Cisco Firepower Release Notes, Version 6.7.0

First Published: 2020-11-02

Last Modified: 2021-08-03

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

CHAPTER 1

Welcome to Version 6.7.0

Thank you for choosing Firepower.

About the Release Notes

The release notes provide critical and release-specific information, including upgrade warnings and behavior changes.

For links to upgrade and installation instructions, see:

- Upgrade Instructions, on page 75
- Installation Instructions, on page 86

Highlights

Snort 3 for Firepower Device Manager Deployments

Snort 3 is now the default inspection engine for new Version 6.7.0+ Firepower Threat Defense (FTD) deployments when managed with Firepower Device Manager (FDM).

If you upgrade to Version 6.7.0 from an older release, Snort 2 remains the active inspection engine, but you can switch. For more information on this and other new features for FTD with FDM, see New Features in FDM Version 6.7.0, on page 39.

You can also visit the Snort 3 website: https://snort.org/snort3.

Release Dates

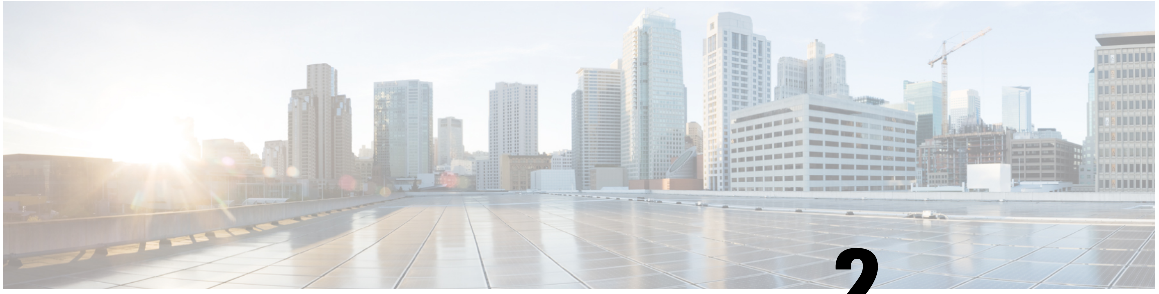
For a list of all platforms available with this version, see Compatibility, on page 3.

Table 1: Version 6.7.0/6.7.x Dates

Version	Build	Date	Platforms
6.7.0	65	2020-11-02	All

Table 2: Version 6.7.0/6.7.x Patch Dates

Version	Build	Date	Platforms
6.7.0.2	24	2021-05-11	All
6.7.0.1	13	2021-03-24	All



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

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
- Firepower Management Center Virtual for Google Cloud Platform (GCP)
- Firepower Management Center Virtual for Oracle Cloud Infrastructure (OCI)

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 6.

Table 3: Firepower Threat Defense in Version 6.7.0/6.7.x

FTD Platform	OS/Hypervisor	Additional Details
Firepower 1010, 1120, 1140, 1150 Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	FXOS 2.9.1.131 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, 2.9(1).

FTD Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-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. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
Firepower Threat Defense Virtual (FTDv)	Any of: • AWS: Amazon Web Services • Azure: Microsoft Azure • GCP: Google Cloud Platform • OCI: Oracle Cloud Infrastructure • 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 6.7.0/6.7.x

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. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
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 Firepower devices support remote management with a Firepower Management Center (FMC), 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
7.0.0/7.0.x	6.4.0
6.7.0/6.7.x	6.3.0
6.6.0/6.6.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 an FMC, many Firepower Threat Defense devices support FDM and CDO management:

- Firepower Device Manager (FDM) is build into FTD and can manage a single device.

  FDM 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.

  CDO allows you to establish and maintain consistent security policies across your deployment without using an 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 FDM also support CDO concurrently.

Table 6: FDM/CDO Compatibility with Firepower Threat Defense

FTD Platform	FDM Compatibility	CDO Compatibility
Firepower 1000 series	6.4.0+	6.4.0+
Firepower 2100 series	6.2.1+	6.4.0+

FTD Platform	FDM Compatibility	CDO Compatibility
Firepower 4100/9300	6.5.0+	6.5.0+
ASA 5500-X series	6.1.0+	6.4.0+
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 GCP	—	—
FTDv for KVM	6.2.3+	6.4.0+
FTDv for OCI	—	—
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
7.0.0/7.0.x	7.16.1
6.7.0/6.7.x	7.15.1
6.6.0/6.6.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

Minimum Version to Upgrade

You can upgrade directly to Version 6.7.0 as follows. You do not need to be running any specific maintenance release or patch level.

Table 8: Minimum Version to Upgrade to Version 6.7.0/6.7.x

Platform	Minimum Version
Firepower Management Center	6.3.0 You cannot upgrade to Version 6.7.0 from Version 6.6.5 or later maintenance release. This is because the Version 6.6.5 data store is newer than the Version 6.7.0 data store. If you are running Version 6.6.5, we recommend you upgrade directly to Version 7.0.0 or later.
Firepower devices	6.3.0 FXOS 2.9.1.131 or later build required for the Firepower 4100/9300.

Web Browser Compatibility

Browsers Tested with Firepower Web Interfaces

Firepower web interfaces are tested with the latest versions of the following popular browsers, running on currently supported versions of macOS and Microsoft Windows:

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

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

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

Browser Settings and Extensions

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

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

Securing Communications

When you first log in to a Firepower web interface, 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 to the Firepower web interface, we do recommend that you replace the self-signed certificate with a certificate signed by a globally known or internally trusted certificate authority (CA).

To begin replacing the self-signed certificate:

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

For detailed procedures, see the online help or the configuration guide for your Firepower 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 Firepower-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 9: Screen Resolution Requirements for Firepower User Interfaces

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 Firepower 4100/9300 chassis	1024 x 768

CHAPTER 3

Features and Functionality

Major releases contain new features, functionality, and enhancements to the Firepower software. 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

New Features in FMC Version 6.7.0

Table 10:

Feature	Description
Hardware and Virtual Appliances	
Oracle Cloud Infrastructure (OCI) virtual deployments	We introduced FMCv and FTDv for Oracle Cloud Infrastructure.
Google Cloud Platform (GCP) virtual deployments	We introduced FMCv and FTDv for Google Cloud Platform.

Feature	Description
High availability support on FMCv for VMware	FMCv for VMware now supports high availability. You use the FMCv web interface to establish HA, just as you would on hardware models. In an FTD deployment, you need two identically licensed FMCv's, as well as one FTD entitlement for each managed device. For example, to manage 10 FTD devices with an FMCv10 HA pair, you need two FMCv10 entitlements and 10 FTD entitlements. If you are managing Classic devices only (7000/8000 series, NGIPSv, ASA FirePOWER), you do not need FMCv entitlements. Note that this feature is not supported on FMCv 2 for VMware—that is, an FMCv licensed to manage only two devices. Supported platforms: FMCv 10, 25, and 300 for VMware
Auto Scale improvements for FTDv for AWS	Version 6.7.0 includes the following Auto Scale improvements for FTDv for AWS: • Custom Metric Publisher. A new Lambda function polls the FMC every second minute for memory consumption of all FTDv instances in the Auto Scale group, then publishes the value to CloudWatch Metric. • A new scaling policy based on memory consumption is available. • FTDv private IP connectivity for SSH and Secure Tunnel to the FMC. • FMC configuration validation. • Support for opening more Listening ports on ELB. • Modified to Single Stack deployment. All Lambda functions and AWS resources are deployed from a single stack for a streamlined deployment. Supported platforms: FTDv for AWS
Auto Scale improvements for FTDv for Azure	The FTDv for Azure Auto Scale solution now includes support for scaling metrics based on CPU and memory (RAM), not just CPU. Supported platforms: FTDv for Azure
Firepower Threat Defense: Device Management	

Feature	Description
Manage FTD on a data interface	You can now configure FMC management of the FTD on a data interface instead of using the dedicated management interface. This feature is useful for remote deployment when you want to manage the FTD at a branch office from an FMC at headquarters and need to manage the FTD on the outside interface. If the FTD receives a public IP address using DHCP, then you can optionally configure Dynamic DNS (DDNS) for the interface using the web type update method. DDNS ensures the FMC can reach the FTD at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes. **Note** FMC access on a data interface is not supported with clustering or high availability. New/modified pages: • **Devices** > **Device Management** > **Device** > **Management** section • **Devices** > **Device Management** > **Interfaces** > **FMC Access** • **Devices** > **Device Management** > **DHCP** > **DDNS** > **DDNS Update Methods** page New/modified FTD CLI commands: **configure network management-data-interface**, **configure policy rollback** Supported platforms: FTD
Update the FMC IP address on the FTD	If you change the FMC IP address, you can now use the FTD CLI to update the device. New/modified FTD CLI commands: **configure manager edit** Supported platforms: FTD

Feature	Description
Synchronization between the FTD operational link state and the physical link state for the Firepower 4100/9300	The Firepower 4100/9300 chassis can now synchronize the FTD operational link state with the physical link state for data interfaces. Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The FTD application interface admin state is not considered. Without synchronization from FTD, data interfaces can be in an Up state physically before the FTD application has completely come online, for example, or can stay Up for a period of time after you initiate an FTD shutdown. For inline sets, this state mismatch can result in dropped packets because external routers may start sending traffic to the FTD before the FTD can handle it. This feature is disabled by default, and can be enabled per logical device in FXOS. **Note** This feature is not supported for clustering, container instances, or an FTD with a Radware vDP decorator. It is also not supported for ASA. New/modified Firepower Chassis Manager pages: **Logical Devices** > **Enable Link State** New/modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** Supported platforms: Firepower 4100/9300
Firepower 1100/2100 series SFP interfaces now support disabling auto-negotiation	**Upgrade impact.** You can now configure a Firepower 1100/2100 series SFP interface to disable flow control and link status negotiation. Previously, when you set an SFP interface speed (1000 or 10000 Mbps) on these devices, flow control and link status negotiation was automatically enabled. You could not disable it. Now, you can select **No Negotiate** to disable flow control and link status negotiation. This also sets the speed to 1000 Mbps, regardless of whether you are configuring a 1 GB SFP or 10 GB SFP+ interface. You cannot disable negotation at 10000 Mbps. New/modified pages: **Devices** > **Device Management** > **Interfaces** > edit interface > **Hardware Configuration** > **Speed** Supported platforms: Firepower 1100/2100 series
Firepower Threat Defense: Clustering	

Feature	Description
New cluster management functionality on the FMC	You can now use the FMC to perform the following cluster management tasks, where previously you had to use the CLI: • Enable and disable cluster units. • Show cluster status from the Device Management page, including History and Summary per unit. • Change the role to the control unit. New/modified pages: • **Devices** > **Device Management** > **More** menu • **Devices** > **Device Management** > **Cluster** > **General** area > **Cluster Live Status** link > **Cluster Status** Supported platforms: Firepower 4100/9300
Faster cluster deployment	Cluster deployment now completes faster. Also, for most deployment failures, it fails more quickly. Supported platforms: Firepower 4100/9300

Feature	Description
Changes to PAT address allocation in clustering. The PAT pool **Flat Port Range** option is now enabled by default and it is not configurable.	**Upgrade impact.** The way PAT addresses are distributed to the members of a cluster is changed. Previously, addresses were distributed to the members of the cluster, so your PAT pool would need a minimum of one address per cluster member. Now, the control instead divides each PAT pool address into equal-sized port blocks and distributes them across cluster members. Each member has port blocks for the same PAT addresses. Thus, you can reduce the size of the PAT pool, even to as few as one IP address, depending on the amount of connections you typically need to PAT. Port blocks are allocated in 512-port blocks from the 1024-65535 range. You can optionally include the reserved ports, 1-1023, in this block allocation when you configure PAT pool rules. For example, in a 4-node cluster, each node gets 32 blocks with which it will be able to handle 16384 connections per PAT pool IP address compared to a single node handling all 65535 connections per PAT pool IP address. As part of this change, PAT pools for all systems, whether standalone or operating in a cluster, now use a flat port range of 1024–65535. Previously, you could use a flat range by enabling the **Flat Port Range** option in a PAT pool rule (Pat Pool tab in an FTD NAT rule). The **Flat Port Range** option is now ignored: the PAT pool is now always flat. You can optionally select the **Include Reserved Ports** option to include the 1–1023 port range within the PAT pool. Note that if you configure port block allocation (the **Block Allocation** PAT pool option), your block allocation size is used rather than the default 512-port block. In addition, you cannot configure extended PAT for a PAT pool for systems in a cluster. This change takes effect automatically. You do not need to do anything before or after upgrade. Supported platforms: FTD
Firepower Threat Defense: Encryption and VPN	

Feature	Description
AnyConnect module support for RA VPN	FTD RA VPN now supports AnyConnect modules. As part of your RA VPN group policy, you can now configure a variety of optional modules to be downloaded and installed when a user downloads the Cisco AnyConnect VPN client. These modules can provide services such as web security, malware protection, off-network roaming protection, and so on. You must associate each module with a profile containing your custom configurations, created in the AnyConnect Profile Editor and uploaded to the FMC as an AnyConnect File object. New/modified pages: • Upload module profiles: We added new **File Type** options to **Objects** > **Object Management** > **VPN** > **AnyConnect File** > **Add AnyConnect File** • Configure modules: We added **Client Modules** options to **Objects** > **Object Management** > **VPN** > **Group Policy** > add or edit a Group Policy object > **AnyConnect** settings Supported platforms: FTD
AnyConnect management VPN tunnels for RA VPN	FTD RA VPN now supports an AnyConnect management VPN tunnel that allows VPN connectivity to endpoints when the corporate endpoints are powered on, not just when a VPN connection is established by the end user. This feature helps administrators perform patch management on out-of-the-office endpoints, especially devices that are infrequently connected by the user, via VPN, to the office network. Endpoint operating system login scripts which require corporate network connectivity also benefit. Supported platforms: FTD
Single sign-on for RA VPN	FTD RA VPN now supports single sign-on (SSO) for remote access VPN users configured at a SAML 2.0-compliant identity provider (IdP). New/modified pages: • Connect to an SSO server: **Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server** • Configure SSO as part of RA VPN: We added **SAML** as an authentication method (AAA settings) when configuring an RA VPN connection profile. Supported platforms: FTD

Feature	Description
LDAP authorization for RA VPN	FTD RA VPN now supports LDAP authorization using LDAP attribute maps. An LDAP attribute map equates attributes that exist in the Active Directory (AD) or LDAP server with Cisco attribute names. Then, when the AD or LDAP server returns authentication to the FTD device during remote access VPN connection establishment, the FTD device can use the information to adjust how the AnyConnect client completes the connection. Supported platforms: FTD
Virtual Tunnel Interface (VTI) and route-based site-to-site VPN	FTD site-to-site VPN now supports a logical interface called Virtual Tunnel Interface (VTI). As an alternative to policy-based VPN, a VPN tunnel can be created between peers with Virtual Tunnel Interfaces configured. This supports route-based VPN with IPsec profiles attached to the end of each tunnel. This allows dynamic or static routes to be used. Using VTI does away with the requirement of configuring static crypto map access lists and mapping them to interfaces. Traffic is encrypted using static route or BGP. You can create a routed security zone, add VTI interfaces to it, and define access control rules for the decrypted traffic control over the VTI tunnel. VTI-based VPNs can be created between: • Two FTD devices • An FTD device and a public cloud • An FTD device and another FTD device with service provider redundancy New/modified pages: • **Devices** > **Device Management** > **Interfaces** > **Add Interfaces** > **Virtual Tunnel Interface** • **Devices** > **VPN** > **Site To Site** > **Add VPN** > **Firepower Threat Defense Device** > **Route Based (VTI)** Supported platforms: FTD
Dynamic RRI support for site-to-site VPN	FTD site-to-site VPN now supports Dynamic Reverse Route Injection (RRI) supported with IKEv2-based static crypto maps in site-to-site VPN deployments. This allowed static routes to be automatically inserted into the routing process for networks and hosts protected by a remote tunnel endpoint. New/modified pages: We added the **Enable Dynamic Reverse Route Injection** advanced option when adding an endpoint to a site-to-site VPN topology. Supported platforms: FTD

Feature	Description
Enhancements to manual certificate enrollment	You can now obtain signed CA certificates and identity certificates from a CA authority independently of each other. We made the following changes to PKI certificate enrollment objects, which store enrollment parameters for creating Certificate Signing Requests (CSRs) and obtaining identity certificates: • We added the **CA Only** option to the manual enrollment settings for PKI certificate enrollment objects. If you enable this option, you will receive only a signed CA certificate from the CA authority, and not the identity certificate. • You can now leave the **CA Certificate** field blank in the manual enrollment settings for PKI certificate enrollment objects. If you do this, you will receive only the identity certificate from the CA authority, and not the signed CA certificate. New/modified pages: **Objects** > **Object Management** > **PKI** > **Cert Enrollment** > **Add Cert Enrollment** > **CA Information** > **Enrollment Type** > **Manual** Supported platforms: FTD
Enhancements to FTD certificate management	We made the following enhancements to FTD certificate management: • You can now view the chain of certifying authorities (CAs) when viewing certificate contents. • You can now export certificates. New/modified pages: • **Devices** > **Certificates** > **Status** column > **View** icon (magnifying glass) • **Devices** > **Certificates** > **Export** icon Supported platforms: FTD
Access Control: URL Filtering, Application Control, and Security Intelligence	

Feature	Description
URL filtering and application control on traffic encrypted with TLS 1.3 (TLS Server Identity Discovery)	You can now perform URL filtering and application control on traffic encrypted with TLS 1.3, by using information from the server certificate. You do not have decrypt the traffic for this feature to work. **Note** We recommend enabling this feature if you want to perform URL filtering and application control on encrypted traffic. However, it can affect device performance, especially on lower-memory models. New/modified pages: We added a **TLS Server Identity Discovery** warning and option to the access control policy's Advanced tab. New/modified FTD CLI commands: We added the B flag to the output of the **show conn detail** command. On a TLS 1.3-encrypted connection, this flag indicates that we used the server certificate for application and URL detection. Supported platforms: FTD
URL filtering on traffic to websites with unknown reputation	You can now perform URL filtering for websites that have an unknown reputation. New/modified pages: We added an **Apply to unknown reputation** check box to the access control, QoS, and SSL rule editors. Supported platforms: FMC
DNS filtering enhances URL filtering	**Beta.** *DNS filtering* enhances URL filtering by determining the category and reputation of requested domains earlier in the transaction, including in encrypted traffic—but without decrypting the traffic. You enable DNS filtering per access control policy, where it applies to all category/reputation URL rules in that policy. **Note** DNS filtering is a Beta feature and may not work as expected. Do not use it in production environments. New/modified pages: We added the **Enable reputation enforcement on DNS traffic** option to the access control policy's Advanced tab, under General Settings. Supported platforms: FMC

Feature	Description
Shorter update frequencies for Security Intelligence feeds	The FMC can now update Security Intelligence data every 5 or 15 minutes. Previously, the shortest update frequency was 30 minutes. If you configure one of these shorter frequencies on a custom feed, you must also configure the system to use an md5 checksum to determine whether the feed has updates to download. New/modified pages: We added new options to **Objects** > **Object Management** > **Security Intelligence** > **Network Lists and Feeds** > edit feed > **Update Frequency** Supported platforms: FMC
Access Control: User Control	
pxGrid 2.0 with ISE/ISE-PIC	**Upgrade impact.** Use pxGrid 2.0 when you connect the FMC to an ISE/ISE-PIC identity source. If you are still using pxGrid 1.0, switch now. That version is deprecated. For use with pxGrid 2.0, Version 6.7.0 introduces the Cisco ISE Adaptive Network Control (ANC) remediation, which applies or clears ISE-configured ANC policies involved in a correlation policy violation. If you used the Cisco ISE Endpoint Protection Services (EPS) remediation with pxGrid 1.0, configure and use the ANC remediation with pxGrid 2.0. ISE remediations will not launch if you are using the 'wrong' pxGrid. The ISE Connection Status Monitor health module alerts you to mismatches. For detailed compatibility information for all supported Firepower versions, including integrated products, see the Cisco Firepower Compatibility Guide. New/modified pages: • **Policies** > **Actions** > **Modules** > **Installed Remediation Modules** list • **Policies** > **Actions** > **Instances** > **Select a module type** drop-down list Supported platforms: FMC
Realm sequences	You can now group realms into ordered *realm sequences*. Add a realm sequence to an identity rule in the same way as you add a single realm. When applying the identity rule to network traffic, the system searches the Active Directory domains in the order specified. You cannot create realm sequences for LDAP realms. New/modified pages: **System** > **Integration** > **Realm Sequences** Supported platforms: FMC

Feature	Description
ISE subnet filtering	Especially useful on lower-memory devices, you can now use the CLI to exclude subnets from receiving user-to-IP and Security Group Tag (SGT)-to-IP mappings from ISE. The Snort Identity Memory Usage health module alerts when memory usage exceeds a certain level, which by default is 80%. New device CLI command: **configure identity-subnet-filter** {**add** | **remove**} Supported platforms: FMC-managed devices
Access Control: Intrusion and Malware Prevention	
Improved preclassification of files for dynamic analysis	**Upgrade impact.** The system can now decide not to submit a suspected malware file for dynamic analysis, based on the static analysis results (for example, a file with no dynamic elements). After you upgrade, in the Captured Files table, these files will have a Dynamic Analysis Status of Rejected for Analysis. Supported platforms: FMC
S7Commplus preprocessor	The new S7Commplus preprocessor supports the widely accepted S7 industrial protocol. You can use it to apply corresponding intrusion and preprocessor rules, drop malicious traffic, and generate intrusion events. New/modified pages: • Enable the preprocessor: In the network analysis policy editor, click **Settings** (you must *click* the word 'Settings'), and enable **S7Commplus Configuration** under SCADA Preprocessors. • Configure the preprocessor: In the network analysis policy editor, under **Settings**, click **S7Commplus Configuration**. • Configure S7Commplus preprocessor rules: In the intrusion policy editor, click **Rules** > **Preprocessors** > **S7 Commplus Configurations**. Supported platforms: all FTD devices, including ISA 3000

Feature	Description
Custom intrusion rule import warns when rules collide	The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the FMC would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely. On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip. Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers. We recommend you read the best practices for importing local intrusion rules in the Firepower Management Center Configuration Guide. New/modified pages: We added a warning icon to **System** > **Updates** > **Rule Updates**. Supported platforms: FMC
Access Control: TLS/SSL Decryption	
ClientHello modification for Decrypt - Known Key TLS/SSL rules	**Upgrade impact.** If you configure TLS/SSL decryption, when a managed device receives a ClientHello message, the system now attempts to match the message to TLS/SSL rules that have the Decrypt - Known Key action. Previously, the system only matched ClientHello messages to Decrypt - Resign rules. The match relies on data from the ClientHello message and from cached server certificate data. If the message matches, the device modifies the ClientHello message in specific ways; see the *ClientHello Message Handling* topic in the Firepower Management Center Configuration Guide. This behavior change occurs automatically after upgrade. If you use Decrypt - Known Key TLS/SSL rules, make sure that encrypted traffic is being handled as expected. Supported platforms: Any device
Event Logging and Analysis	

Feature	Description
Remote data storage and cross-launch with an on-prem Stealthwatch solution	You can now store large volumes of Firepower event data off-FMC, using an on-premises Stealthwatch solution: Cisco Security Analytics and Logging (On Premises). When viewing events in FMC, you can quickly cross-launch to view events in your remote data storage location. The FMC uses syslog to send connection, Security Intelligence, intrusion, file, and malware events. **Note** This on-prem solution is supported for FMCs running Version 6.4.0+. However, contextual cross-launch requires Firepower Version 6.7.0+. This solution also depends on availability of the Security Analytics and Logging On Prem app for the Stealthwatch Management Console (SMC), which must be running Stealthwatch Enterprise (SWE) version 7.3. Supported platforms: FMC
Quickly add Stealthwatch contextual cross-launch resources	A new page on the FMC allows you to quickly add contextual cross-launch resources for your Stealthwatch appliance. After you add Stealthwatch resources, you manage them on the general contextual cross-launch page. This is where you continue to manually create and manage non-Stealthwatch cross-launch resources. New/modified pages: • Add Stealthwatch resources: **System** > **Logging** > **Security Analytics and Logging** • Manage resources: **Analysis** > **Advanced** > **Contextual Cross-Launch** Supported platform: FMC

Feature	Description
New cross-launch options field types	You can now cross-launch into an external resource using the following additional types of event data: • Access control policy • Intrusion policy • Application protocol • Client application • Web application • Username (including realm) New/modified pages: • New variables when creating or editing cross-launch query links: **Analysis** > **Advanced** > **Contextual Cross-Launch**. • New data types in the dashboard and event viewer now offer cross-launch on right click. Supported platforms: FMC
National Vulnerability Database (NVD) replaces Bugtraq	**Upgrade impact.** Bugtraq vulnerability data is no longer available. Most vulnerability data now comes from the NVD. To support this change, we made the following changes: • Added the **CVE ID** and **Severity** fields to the Vulnerabilities table. Right-clicking the CVE ID in the table view allows you to view details about the vulnerability on the NVD. • Renamed the **Vulnerability Impact** field to **Impact** (in the table view only). • Removed the obsolete/redundant **Bugtraq ID**, **Title**, **Available Exploits**, **Technical Description**, and **Solution** fields. • Removed the **Bugtraq ID** filtering option from the Hosts network map. If you export vulnerability data, make sure any integrations are working as expected after the upgrade. Supported platforms: FMC
Upgrade	

Feature	Description
Pre-upgrade compatibility check	**Upgrade impact.** In FMC deployments, Firepower appliances must now pass pre-upgrade compatibility checks before you can run more complex readiness checks or attempt to upgrade. This check catches issues that *will* cause your upgrade to fail—but we now catch them earlier and block you from proceeding. The checks are as follows: • You cannot use the FMC to upgrade a Firepower 4100/9300 chassis to Version 6.7.0+ until you upgrade FXOS to the new release's companion FXOS version. Upgrade is blocked as long as you are upgrading the device to Version 6.7.0 or later. For example, you are *not* blocked from attempting a Firepower 4100/9300 upgrade from 6.3 → 6.6.x, even if the device is running a version of FXOS that is too old for Firepower Version 6.6.x. • You cannot use the FMC to upgrade a device if that device has out-of-date configurations. Upgrade is blocked as long as the FMC is running Version 6.7.0 or later, and you are upgrading a managed device to a valid target. For example, you *are* blocked from upgrading a device from 6.3.0 → 6.6.x if the device has outdated configurations. • You cannot upgrade an FMC *from* Version 6.7.0+ if its devices have out-of-date configurations. Upgrade is blocked as long as the FMC is running Version 6.7.0 or later. For upgrades from earlier versions (including *to* Version 6.7.0), you must make sure you deploy yourself. When you select an upgrade package to install, the FMC displays compatibility check results for all eligible appliances. The new Readiness Check page also displays this information. You cannot upgrade until you fix the issues indicated. New/modified pages: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the upgrade package • **System** > **Update** > **Product Updates** > **Readiness Checks** Supported platforms: FMC, FTD

Feature	Description
Improved readiness checks	**Upgrade impact.** Readiness checks assess a Firepower appliance's preparedness for a software upgrade. These checks include database integrity, file system integrity, configuration integrity, disk space, and so on. After you upgrade the FMC to Version 6.7.0, you will see the following improvements to FTD upgrade readiness checks: • Readiness checks are faster. • Readiness checks are now supported on high availability and clustered FTD devices, without having to log into the device CLI. • Readiness checks for FTD device upgrades to Version 6.7.0+ no longer require the upgrade package to reside on the device. Although we still recommend you push the upgrade package to the device before you begin the upgrade itself, you no longer have to do so before you run the readiness check. • When you select an upgrade package to install, the FMC now shows the readiness status for all applicable FTD devices. A new Readiness Checks page allows you to view the results of readiness checks for the FTD devices in your deployment. You can also re-run readiness checks from this page. • Readiness check results include the estimated upgrade time (but do not include reboot time). • Error messages are better. You can also download success/failure logs from the Message Center on the FMC. Note that these improvements are supported for FTD upgrades from Version 6.3.0+, as long as the FMC is running Version 6.7.0+. New/modified pages: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the upgrade package • **System** > **Update** > **Product Updates** > **Readiness Checks** • **Message Center > Tasks** Supported platforms: FTD

Feature	Description
Improved FTD upgrade status reporting and cancel/retry options	**Upgrade impact.** You can now view the status of device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified pages: • **System** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center > Tasks** New FTD CLI commands: • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry** Supported platforms: FTD

Feature	Description
Upgrades postpone scheduled tasks	**Upgrade impact.** FMC upgrades now postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for all upgrades *from* a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades *to* a supported version from an unsupported version. Supported platforms: FMC
Upgrades remove PCAP files to save disk space	**Upgrade impact.** To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. Upgrades now remove locally stored PCAP files. Supported platforms: Any
Deployment and Policy Management	
Configuration rollback	**Beta.** You can now "roll back" configurations on an FTD device, replacing them with the previously deployed configurations. **Note** Rollback is a Beta feature, and is not supported in all deployment types and scenarios. It is also a disruptive operation. Make sure you read and understand the guidelines and limitations in the *Policy Management* chapter of the Firepower Management Center Configuration Guide. New/modified pages: **Deploy** > **Deployment History** > **Rollback** column and icons. Supported platforms: FTD
Back up and restore FTD container instances	You can now use the FMC to back up FTD container instances. Supported platforms: Firepower 4100/9300
Deploy intrusion and file policies independently of access control policies	You can now select and deploy intrusion and file policies independently of access control policies, unless there are dependent changes. New/modified pages: **Deploy** > **Deployment** Supported platforms: FMC

Feature	Description
Search access control rule comments	You can now search within access control rules comments. New/modified pages: In the access control policy editor, we added the **Comments** field to the **Search Rules** drop-down dialog. Supported platforms: FMC
Search and filter FTD NAT rules	You can now search for rules in an FTD NAT policy to help you find rules based on IP addresses, ports, object names, and so forth. Search results include partial matches. Searching on criteria filters the rule table so only matching rules are displayed. New/modified pages: We added a search field above the rule table when you edit an FTD NAT policy. Supported platforms: FTD
Copy and move rules between access control and prefilter policies	You can copy access control rules from one access control policy to another. You can also move rules between an access control policy and its associated prefilter policy. New/modified pages: In the access control and prefilter policy editors, we added **Copy** and **Move** options to each rule's right-click menu. Supported platforms: FMC
Bulk object import	You can now bulk-import network, port, URL, VLAN tag, and distinguished name objects onto the FMC, using a comma-separated-values (CSV) file. For restrictions and specific formatting instructions, see the *Reusable Objects* chapter of the Firepower Management Center Configuration Guide. New/modified pages: **Objects** > **Object Management** > choose an object type > **Add [Object Type]** > **Import Object** Supported platforms: FMC

Feature	Description
Interface object optimization for access control and prefilter policies	You can now enable interface object optimization on specific FTD devices. During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance. Interface object optimization is disabled by default. If you enable it, you should also enable **Object Group Search**—which now applies to interface objects in addition to network objects—to reduce memory usage on the device. New/modified pages: **Devices** > **Device Management** > **Device** > **Advanced Settings** section **> Interface Object Optimization** check box Supported platforms: FTD
Administration and Troubleshooting	
FMC single sign-on	The FMC now supports single sign-on (SSO) for external users configured at any third-party SAML 2.0-compliant identity provider (IdP). You can map user or group roles from the IdP to FMC user roles. New/modified pages: • **Login** > **Single Sign-On** • **System** > **Users** > **SSO** Supported platforms: FMC
FMC logout delay	When you log out of the FMC, there is an automatic five-second delay and countdown. You can click **Log Out** again to log out immediately. Supported platforms: FMC

Feature	Description
Health monitoring enhancements	We enhanced health monitoring as follows: • Health Status summary page that provides an at-a-glance view of the health of the Firepower Management Center and all of the devices that the FMC manages. • The Monitoring navigation pane allows you to navigate the device hierarchy. • Managed devices are listed individually, or grouped according to their geolocation, high availability, or cluster status where applicable. • You can view health monitors for individual devices from the navigation pane. • Custom dashboards to correlate interrelated metrics. Select from predefined correlation groups, such as CPU and Snort; or create a custom correlation dashboard by building your own variable set from the available metric groups. Supported platforms: FMC

Feature	Description
Health module updates	We replaced the CPU Usage health module with four new modules: • CPU Usage (per core): Monitors the CPU usage on all of the cores. • CPU Usage Data Plane: Monitors the average CPU usage of all data plane processes on the device. • CPU Usage Snort: Monitors the average CPU usage of the Snort processes on the device. • CPU Usage System: Monitors the average CPU usage of all system processes on the device. We added the following health modules to track memory use: • Memory Usage Data Plane: Monitors the percentage of allocated memory used by data plane processes. • Memory Usage Snort: Monitors the percentage of allocated memory used by the Snort process. We added the following health modules to track statistics: • Connection Statistics: Monitors connection statistics and NAT translation counts. • Critical Process Statistics: Monitors the state of critical processes, their resource consumption, and the restart counts. • Deployed Configuration Statistics: Monitors statistics about the deployed configuration, such as the number of ACEs and IPS rules. • Snort Statistics: Monitors Snort statistics for events, flows, and packets. Supported platforms: FMC
Search Message Center	You can now filter the current view in the Message Center. New/modified pages: We added a **Filter** icon and field to the Message Center, under the **Show Notifications** slider. Supported platforms: FMC
Usability and Performance	

Feature	Description
Dusk theme	**Beta.** The FMC web interface defaults to the Light theme, but you can also choose a new Dusk theme. **Note** The Dusk theme is a Beta feature. If you encounter issues that prevent you from using a page or feature, switch to a different 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
Search FMC menus	You can now search the FMC menus. New/modified pages: We added a **Search** icon and field to the FMC menu bar, to the left of the **Deploy** menu. Supported platforms: FMC
Firepower Management Center REST API	

Feature	Description
New REST API services	We added the following FMC REST API services/operations to support new and existing features. Authorization services: • ssoconfig: GET and PUT operations to retrieve and modify FMC single-sign on. Health services: • metrics: GET operation to retrieve metrics for the health monitor. • alerts: GET operation to retrieve health alerts. • deploymentdetails: GET operation to retrieve deployment health details. Deployment services: • jobhistories: GET operation to retrieve deployment history. • rollbackrequests: POST operation to request a configuration rollback. Device services: • metrics: GET operation to retrieve device metrics. • virtualtunnelinterfaces: GET, PUT, POST, and DELETE operations to retrieve and modify virtual tunnel interfaces. Integration services: • externalstorage: GET, GET by ID, and PUT operations to retrieve and modify external event storage configuration. Policy services: • intrusionpolicies: POST and DELETE operations to modify intrusion policies. Update services: • cancelupgrades: POST operation to cancel a failed upgrade. • retryupgrades: POST operation to retry a failed upgrade. Supported platforms: FMC

Deprecated Features in FMC Version 6.7.0

Table 11:

Feature	Upgrade Impact	Description
Cisco Firepower User Agent software and identity source	Prevents Firepower Management Center upgrade.	You cannot upgrade a Firepower Management Center with user agent configurations to Version 6.7.0+. Version 6.6.0/6.6.x is the last release to support the Cisco Firepower User Agent software as an identity source. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC). To convert your license, contact Sales. 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. Deprecated FTD CLI commands: **configure user agent**
Cisco ISE Endpoint Protection Services (EPS) remediation	ISE remediations can stop working.	The Cisco ISE Endpoint Protection Services (EPS) remediation does not work with pxGrid 2.0. Configure and use the new Cisco ISE Adaptive Network Control (ANC) remediation instead. ISE remediations will not launch if you are using the 'wrong' pxGrid to connect the Firepower Management Center to an ISE/ISE-PIC identity source. The ISE Connection Status Monitor health module alerts you to mismatches.

Feature	Upgrade Impact	Description
Less secure Diffie-Hellman groups, and encryption and hash algorithms	Prevents Firepower Management Center upgrade.	You may not be able to upgrade a Firepower Management Center if you use any of the following Firepower Threat Defense features: • Diffie-Hellman groups: 2, 5, and 24. Group 5 continues to be supported in Firepower Management Center deployments for IKEv1, but we recommend you change to a stronger option. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • The NULL "encryption algorithm" (authentication without encryption, for testing purposes) continues to be supported in Firepower Management Center deployments for both IKEv1 and IKEv2 IPsec proposals. However, it is no longer supported in IKEv2 policies. • Hash algorithms: MD5. If you are still using these features in IKE proposals or IPsec policies, change and verify your VPN configuration before you upgrade.

Feature	Upgrade Impact	Description
Appliance Configuration Resource Utilization heath module (temporary deprecation)	Possible post-upgrade errors in the health monitor	Version 6.7.0 *partially* and *temporarily* deprecates support for the Appliance Configuration Resource Utilization health module, which was introduced in Version 6.6.3 and is supported in all later 6.6.x releases. Version 6.7.0 support is as follows: • Firepower Management Center upgraded to Version 6.7.0 from Version 6.6.3+ Continues to support the module, but only if the devices remain at Version 6.6.3/6.6.x. If you upgrade the devices to Version 6.7.0, the module stops working and the health monitor displays an error. To resolve the error, use the Firepower Management Center to disable the module and reapply policies. • Firepower Management Center upgraded to Version 6.7.0 from Version 6.3.0–6.6.1, *or* Firepower Management Center freshly installed to Version 6.7.0. Does not support the module . In the rare case that you add a Version 6.6.3/6.6.x device that has the module enabled to a Firepower Management Center where the module is not supported, the health monitor displays an error that you cannot resolve. This error is safe to ignore. Full support will return in later releases, , where the module is renamed to Configuration Memory Allocation.
Other health modules (permanent deprecation)	None.	Version 6.7.0 deprecates the following health modules: • CPU Usage: Replaced by four new modules; see New Features in FMC Version 6.7.0, on page 11. • Local Malware Analysis: This module was replaced by the Threat Data Updates on Devices module in Version 6.3.0. A Version 6.7.0+ Firepower Management Center can no longer manage any devices where the older module applies. • User Agent Status Monitor: Cisco Firepower User Agent is no longer supported.
Walkthroughs with the Classic theme	None.	Version 6.7.0 discontinues Firepower Management Center walkthroughs (*how-tos*) for the Classic theme. You can switch themes in your user preferences.

Feature	Upgrade Impact	Description
Bugtraq	If you export vulnerability data, make sure any integrations are working as expected after the upgrade.	Version 6.7.0 removes database fields and options for Bugtraq. Bugtraq vulnerability data is no longer available. Most vulnerability data now comes from the National Vulnerability Database (NVD). For more information, see New Features in FMC Version 6.7.0, on page 11.
Microsoft Internet Explorer	You should switch browsers.	We no longer test Firepower web interfaces using Microsoft Internet Explorer. We recommend you switch to Google Chrome, Mozilla Firefox, or Microsoft Edge. For more information, see Web Browser Compatibility, on page 8
ASA 5525-X, 5545-X, and 5555-X devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.7.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5525-X, 5545-X, and 5555-X devices.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.7.0

Feature	Description
Platform Features	
Support ends for the ASA 5525-X, 5545-X, and 5555-X. The last supported release is FTD 6.6.	You cannot install FTD 6.7 on an ASA 5525-X, 5545-X, or 5555-X. The last supported release for these models is FTD 6.6.
Firewall and IPS Features	
TLS server identity discovery for access control rule matching.	TLS 1.3 certificates are encrypted. For traffic encrypted with TLS 1.3 to match access rules that use application or URL filtering, the system must decrypt the TLS 1.3 certificate. We recommend that you enable **TLS Server Identity Discovery** to ensure encrypted connections are matched to the right access control rule. The setting decrypts the certificate only; the connection remains encrypted. We added the **Access Control Settings** (⚙) button and dialog box to the **Policy** > **Access Control** page.

Feature	Description
External trusted CA certificate groups.	You can now customize the list of trusted CA certificates used by the SSL decryption policy. By default, the policy uses all system-defined trusted CA certificates, but you can create a custom group to add more certificates, or replace the default group with your own, more limited, group. We added certificate groups to the **Objects** > **Certificates** page, and modified the SSL decryption policy settings to allow the selection of certificate groups.
Active Directory realm sequences for passive identity rules.	You can create a realm sequence, which is an ordered list of Active Directory (AD) servers and their domains, and use them in a passive authentication identity rule. Realm sequences are useful if you support more than one AD domain and you want to do user-based access control. Instead of writing separate rules for each AD domain, you can write a single rule that covers all of your domains. The ordering of the AD realms within the sequence is used to resolve identity conflicts if any arise. We added the AD realm sequence object on the **Objects** > **Identity Sources** page, and the ability to select the object as a realm in a passive authentication identity rule. In the FTD API, we added the **RealmSequence** resource, and in the **IdentityRule** resource, we added the ability to select a realm sequence object as the realm for a rule that uses passive authentication as the action.
FDM support for Trustsec security group tag (SGT) group objects and their use in access control rules.	In FTD 6.5, support was added to the FTD API to configure SGT group objects and use them as matching criteria in access control rules. In addition, you could modify the ISE identity object to listen to the SXP topic published by ISE. Now, you can configure these features directly in FDM. We added a new object, SGT groups, and updated the access control policy to allow their selection and display. We also modified the ISE object to include the explicit selection of topics to subscribe to.
Snort 3.0 support.	For new systems, Snort 3.0 is the default inspection engine. If you upgrade to 6.7 from an older release, Snort 2.0 remains the active inspection engine, but you can switch to Snort 3.0. For this release, Snort 3.0 does not support virtual routers, time-based access control rules, or the decryption of TLS 1.1 or lower connections. Enable Snort 3.0 only if you do not need these features. You can freely switch back and forth between Snort 2.0 and 3.0, so you can revert your change if needed. Traffic will be interrupted whenever you switch versions. We added the ability to switch Snort versions to the **Device** > **Updates** page, in the **Intrusion Rules** group. In the FTD API, we added the IntrusionPolicy resource action/toggleinspectionengine. In addition, there is a new audit event, Rules Update Event, that shows which intrusion rules were added, deleted, or changed in a Snort 3 rule package update.

Feature	Description
Custom intrusion policies for Snort 3.	You can create custom intrusion policies when you are using Snort 3 as the inspection engine. In comparison, you could use the pre-defined policies only if you use Snort 2. With custom intrusion policies, you can add or remove groups of rules, and change the security level at the group level to efficiently change the default action (disabled, alert or drop) of the rules in the group. Snort 3 intrusion policies give you more control over the behavior of your IPS/IDS system without the need to edit the base Cisco Talos-provided policies. We changed the **Policies** > **Intrusion** page to list intrusion policies. You can create new ones, and view or edit existing policies, including adding/removing groups, assigning security levels, and changing the action for rules. You can also select multiple rules and change their actions. In addition, you can select custom intrusion policies in access control rules.
Multiple syslog servers for intrusion events.	You can configure multiple syslog servers for intrusion policies. Intrusion events are sent to each syslog server. We added the ability to select multiple syslog server objects to the intrusion policy settings dialog box.
URL reputation matching can include sites with unknown reputations.	When you configure URL category traffic-matching criteria, and select a reputation range, you can include URLs with unknown reputation in the reputation match. We added the **Include Sites with Unknown Reputation** check box to the URL reputation criteria in access control and SSL decyption rules.
VPN Features	
Virtual Tunnel Interface (VTI) and route-based site-to-site VPN.	You can now create route-based site-to-site VPNs by using a Virtual Tunnel Interface as the local interface for the VPN connection profile. With route-based site-to-site VPN, you manage the protected networks in a given VPN connection by simply changing the routing table, without altering the VPN connection profile at all. You do not need to keep track of remote networks and update the VPN connection profile to account for these changes. This simplifies VPN management for cloud service providers and large enterprises. We added the **Virtual Tunnel Interfaces** tab to the Interface listing page, and updated the site-to-site VPN wizard so that you can use a VTI as the local interface.
FTD API support for Hostscan and Dynamic Access Policy (DAP) for remote access VPN connections.	You can upload Hostscan packages and the Dynamic Access Policy (DAP) rule XML file, and configure DAP rules to create the XML file, to control how group policies are assigned to remote users based on attributes related to the status of the connecting endpoint. You can use these features to perform Change of Authorization if you do not have Cisco Identity Services Engine (ISE). You can upload Hostscan and configure DAP using the FTD API only; you cannot configure them using FDM. See the AnyConnect documentation for information about Hostscan and DAP usage. We added or modified the following FTD API object models: dapxml, hostscanpackagefiles, hostscanxmlconfigs, ravpns.

Feature	Description
Enabling certificate revocation checking for external CA certificates	You can use the FTD API to enable certificate revocation checking on a particular external CA certificate. Revocation checking is particularly useful for certificates used in remote access VPN. You cannot configure revocation checking on a certificate using FDM, you must use the FTD API. We added the following attributes to the ExternalCACertificate resource: revocationCheck, crlCacheTime, oscpDisableNonce.
Support removed for less secure Diffie-Hellman groups, and encryption and hash algorithms.	The following features were deprecated in 6.6 and they are now removed. If you are still using them in IKE proposals or IPsec policies, you must replace them after upgrade before you can deploy any configuration changes. We recommend that you change your VPN configuration prior to upgrade to supported DH and encryption algorithms to ensure the VPN works correctly. • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5.
Custom port for remote access VPN.	You can configure the port used for remote access VPN (RA VPN) connections. If you need to connect to FDM on the same interface used for RA VPN, you can change the port number for RA VPN connections. FDM uses port 443, which is also the default RA VPN port. We updated the global settings step of the RA VPN wizard to include port configuration.
SAML Server support for authenticating remote access VPN.	You can configure a SAML 2.0 server as the authentication source for a remote access VPN. Following are the supported SAML servers: Duo. We added SAML server as an identity source on the **Objects** > **Identity Sources** page, and updated remote access VPN connection profiles to allow its use.
FTD API Support for AnyConnect module profiles.	You can use the FTD API to upload module profiles used with AnyConnect, such as AMP Enabler, ISE Posture, or Umbrella. You must create these profiles using the offline profile editors that you can install from the AnyConnect profile editor package. We added the anyConnectModuleType attribute to the AnyConnectClientProfile model. Although you can initially create AnyConnect Client Profile objects that use module profiles, you will still need to use the API to modify the objects created in FDM to specify the correct module type.
Routing Features	

Feature	Description
EIGRP support using Smart CLI.	In previous releases, you configured EIGRP in the Advanced Configuration pages using FlexConfig. Now, you configure EIGRP using Smart CLI directly on the Routing page. If you configured EIGRP using FlexConfig, when you upgrade to release 6.7, you must remove the FlexConfig object from the FlexConfig policy, and then recreate your configuration in the Smart CLI object. You can retain your EIGRP FlexConfig object for reference until you have completed the Smart CLI updates. Your configuration is not automatically converted. We added the EIGRP Smart CLI object to the Routing pages.
Interface Features	
ISA 3000 hardware bypass persistence	You can now enable hardware bypass for ISA 3000 interface pairs with the persistence option: after power is restored, hardware bypass remains enabled until you manually disable it. If you enable hardware bypass without persistence, hardware bypass is automatically disabled after power is restored. There may be a brief traffic interruption when hardware bypass is disabled. The persistence option lets you control when the brief interruption in traffic occurs. New/Modified screen: **Device** > **Interfaces** > **Hardware Bypass** > **Hardware Bypass Configuration**
Synchronization between the FTD operational link state and the physical link state for the Firepower 4100/9300	The Firepower 4100/9300 chassis can now synchronize the FTD operational link state with the physical link state for data interfaces. Currently, interfaces will be in an Up state as long as the FXOS admin state is up and the physical link state is up. The FTD application interface admin state is not considered. Without synchronization from FTD, data interfaces can be in an Up state physically before the FTD application has completely come online, for example, or can stay Up for a period of time after you initiate an FTD shutdown. This feature is disabled by default, and can be enabled per logical device in FXOS. **Note** This feature is not supported for an FTD with a Radware vDP decorator. New/Modified Firepower Chassis Manager screens: **Logical Devices > Enable Link State** New/Modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** Supported platforms: Firepower 4100/9300
Firepower 1100 and 2100 SFP interfaces now support disabling auto-negotiation	You can now configure a Firepower 1100 and 2100 SFP interface to disable auto-negotiation. For 10GB interfaces, you can configure the speed down to 1GB without auto-negotiation; you cannot disable auto-negotiation for an interface with the speed set to 10GB. New/Modified screen: **Device > Interfaces > Edit Interface > Advanced Options > Speed** Supported platforms: Firepower 1100 and 2100
Administrative and Troubleshooting Features	

Feature	Description
Ability to cancel a failed FTD software upgrade and to revert to the previous release.	If an FTD major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the FTD API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the FTD CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.
Custom HTTPS port for FDM/FTD API access on data interfaces.	You can change the HTTPS port used for FDM or FTD API access on data interfaces. By changing the port from the default 443, you can avoid conflict between management access and other features, such as remote access VPN, configured on the same data interface. Note that you cannot change the management access HTTPS port on the management interface. We added the ability to change the port to the **Device** > **System Settings** > **Management Access** > **Data Interfaces** page.
Low-touch provisioning for Cisco Defense Orchestrator on Firepower 1000 and 2100 series devices.	If you plan on managing a new Firepower Threat Defense device using Cisco Defense Orchestrator (CDO), you can now add the device without completing the device setup wizard or even logging into FDM. New Firepower 1000 and 2100 series devices are initially registered in the Cisco cloud, where you can easily claim them in CDO. Once in CDO, you can immediately manage the devices from CDO. This low-touch provisioning minimizes the need to interact directly with the physical device, and is ideal for remote offices or other locations where your employees are less experienced working with networking devices. We changed how Firepower 1000 and 2100 series devices are initially provisioned. We also added auto-enrollment to the **System Settings** > **Cloud Services** page, so that you can manually start the process for upgraded devices or other devices that you have previously managed using FDM.
FTD API support for SNMP configuration.	You can use the FTD API to configure SNMP version 2c or 3 on an FDM or CDO managed FTD device. We added the following API resources: SNMPAuthentication, SNMPHost, SNMPSecurityConfiguration, SNMPServer, SNMPUser, SNMPUserGroup, SNMPv2cSecurityConfiguration, SNMPv3SecurityConfiguration. **Note** If you used FlexConfig to configure SNMP, you must redo your configuration using the FTD API SNMP resources. The commands for configuring SNMP are no longer allowed in FlexConfig. Simply removing the SNMP FlexConfig object from the FlexConfig policy will allow you to deploy changes; you can then use the object as reference while you use the API to reconfigure the feature.

Feature	Description
Maximum backup files retained on the system is reduced from 10 to 3.	The system will retain a maximum of 3 backup files on the system rather than 10. As new backups are created, the oldest backup file is deleted. Please ensure that you download backup files to a different system so that you have the versions required to recover the system in case you need to.
FTD API Version backward compatibility.	Starting with FTD Version 6.7, if an API resource model for a feature does not change between releases, then the FTD API can accept calls that are based on the older API version. Even if the feature model did change, if there is a logical way to convert the old model to the new model, the older call can work. For example, a v4 call can be accepted on a v5 system. If you use “latest” as the version number in your calls, these “older” calls are interpreted as a v5 call in this scenario, so whether you are taking advantage of backward compatibility depends on how you are structuring your API calls.
FTD REST API version 6 (v6).	The FTD REST API for software version 6.7 is version 6. You can use v6 in the API URLs, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. 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**.

Deprecated Features in FDM Version 6.7.0

Table 12:

Feature	Upgrade Impact	Description
Less secure Diffie-Hellman groups, and encryption and hash algorithms	Prevents post-upgrade deploy.	You may not be able to deploy post-upgrade with if you use any of the following Firepower Threat Defense features: • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5. If you are still using these features in IKE proposals or IPsec policies, change and verify your VPN configuration before you upgrade.

Feature	Upgrade Impact	Description
FlexConfig commands	Prevents post-upgrade deploy. You should redo your configurations after upgrade.	Version 6.7.0 deprecates the following FlexConfig CLI commands for Firepower Threat Defense with FDM: • **router eigrp**: You can now create and use Smart CLI EIGRP objects directly on the Routing page: **Device** > **Routing** > **EIGRP**. • **snmp-server**: You can now use the FTD API to configure SNMP version 2c or 3. You cannot deploy post-upgrade until you remove any associated FlexConfig objects.
Backup file retention	None. Upgrades always purge local backups.	Version 6.7.0 reduces the number of stored backup files from 10 to 3. Note that we always recommend you back up to a secure remote location and verify transfer success. Upgrades purge locally stored backups.
Microsoft Internet Explorer	You should switch browsers.	We no longer test Firepower web interfaces using Microsoft Internet Explorer. We recommend you switch to Google Chrome, Mozilla Firefox, or Microsoft Edge. For more information, see Web Browser Compatibility, on page 8
ASA 5525-X, 5545-X, and 5555-X devices with Firepower Threat Defense	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.7.0+ of the Firepower Threat Defense software on ASA 5525-X, 5545-X, and 5555-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/LSPs) provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. If a newer intrusion rule uses keywords that are not supported in your current Firepower version, that rule is not imported when you update the SRU/LSP.

After you upgrade the Firepower software 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 the Snort version included with your Firepower software:

- 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 13: 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**. Version 6.7.0 discontinues walkthroughs for the Classic theme. You can switch themes in your user preferences.
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.

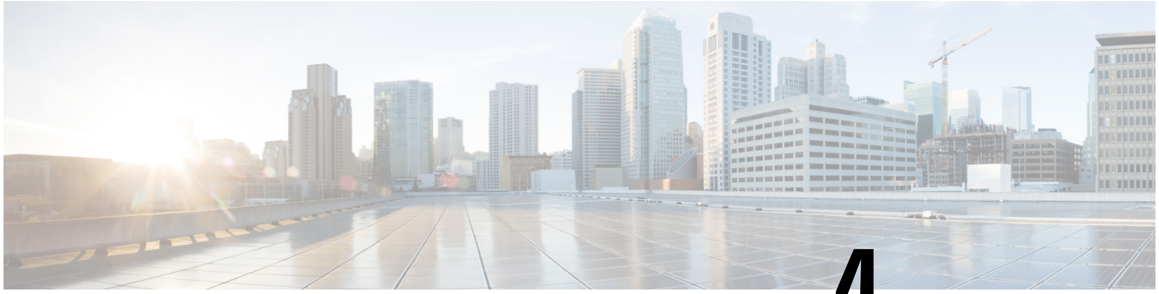
During initial setup and upgrades, you may be asked to enroll. You can also change your enrollment at any time.

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.

Upgrade Checklist

This pre-upgrade checklist highlights actions that can prevent common issues. However, we still recommend you refer to the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 75.

Important At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported. Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. In most cases, do *not* restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, there may be something you can do — see the Note on Unresponsive Upgrades.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 14:

✓	Action/Check
	Assess your deployment. Before you upgrade any Firepower appliance, determine the current state of your deployment. Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your devices are configured for high availability/scalability, and if they are deployed passively, as an IPS, as a firewall, and so on.
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In Firepower Management Center deployments, you usually upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first.
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Upgrade guidelines can appear in multiple places. Make sure you read them all. They include: • New Guidelines for Version 6.7.0, on page 57: Important upgrade guidelines that are new or specific to this release. • Previously Published Guidelines, on page 58: Older guidelines that may apply to your upgrade. • Known Issues, on page 107: Be prepared to work around any bugs that affect upgrade. • Features and Functionality, on page 11: New and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. **Important** If your upgrade skips versions, you may also be directed to older Firepower release notes or other resources for historical guidelines and upgrade impact.
	Check appliance access. Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, 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
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In Firepower Management Center deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 15:

✓	Action/Check
	Upload Firepower upgrade packages. In Firepower Management Center deployments, upload Firepower Management Center and all Classic device (ASA FirePOWER, NGIPSv) upgrade packages to the Firepower Management Center. For Firepower Threat Defense devices, you can either upload upgrade packages to the Firepower Management Center, or configure your own internal web server as the source for Firepower Threat Defense upgrade packages. In Firepower Management Center high availability deployments, you must upload the Firepower Management Center upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.
	Copy Firepower upgrade packages to managed devices. In Firepower Management Center deployments, we recommend you copy (*push*) upgrade packages to managed devices before you initiate the device upgrade. **Note** For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

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 Firepower product.

⚠ **Caution** We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 16:

✓	Action/Check
	Back up Firepower software. Back up before and after upgrade, when supported: • Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly. • After upgrade: This creates a snapshot of your freshly upgraded deployment. In Firepower Management Center deployments, we recommend you back up the Firepower Management Center after you upgrade its managed devices, so your new Firepower Management Center backup file 'knows' that its devices have been upgraded.
	Back up FXOS on the Firepower 4100/9300. Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations before and after upgrade, including logical device and platform configuration settings.
	Back up ASA for ASA with FirePOWER Services. Use ASDM or the ASA CLI to back up configurations and other critical files before and after upgrade, especially if there is an ASA configuration migration.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 17:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major Firepower upgrade.

✓	Action/Check
	Upgrade FXOS on the Firepower 4100/9300. If needed, upgrade FXOS before you upgrade the Firepower software. This is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in Firepower Threat Defense high availability pairs and inter-chassis clusters *one chassis at a time*. **Note** Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: Cisco Firepower 4100/9300 FXOS Release Notes.
	Upgrade ASA on ASA with FirePOWER Services. If desired, upgrade ASA. There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. For standalone ASA devices, upgrade the ASA FirePOWER module just *after* you upgrade ASA and reload. For ASA clusters and failover pairs, to avoid interruptions in traffic flow and inspection, fully upgrade these devices *one at a time*. Upgrade the ASA FirePOWER module just *before* you reload each unit to upgrade ASA. **Note** Before you upgrade ASA, make sure you read all upgrade guidelines and plan configuration changes. Start with the ASA release notes: Cisco ASA Release Notes.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 18:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization. Make sure Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In Firepower Management Center deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • Firepower Management Center: Choose **System** > **Configuration** > **Time**. • Devices: Use the **show time** CLI command.

✓	Action/Check
	Check disk space. Run a disk space check for the Firepower software upgrade. Without enough free disk space, the upgrade fails. See Time Tests and Disk Space Requirements, on page 66.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In Firepower Management Center high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See Traffic Flow, Inspection, and Device Behavior, on page 69.
	Check running tasks. Make sure essential tasks are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them. **Note** In some deployments, upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. This feature is currently supported for Firepower Management Centers running Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. Note that this feature is supported for all upgrades *from* a supported version. This feature is not supported for upgrades *to* a supported version from an unsupported version.
	Run Firepower software readiness checks. We recommend compatibility and readiness checks. These checks assess your preparedness for a Firepower software upgrade.

Note on Unresponsive Upgrades

Starting with major and maintenance Firepower Threat Defense device upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades:

- Firepower Management Center deployments: Use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center.
- Firepower Device Manager deployments: Use the System Upgrade panel.

You can also use the Firepower Threat Defense CLI.

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

If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

New Guidelines for Version 6.7.0

This checklist contains upgrade guidelines that are new or specific to Version 6.7.0.

Table 19: Version 6.7.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0, on page 57	FMC	6.6.5 or later 6.6.x release	6.7.0 only
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 57	Firepower 1010	6.4.0 through 6.6.x	6.7.0+

Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0

Deployments: FMC

Upgrading from: Version 6.6.5 or later maintenance release.

Directly to: Version 6.7.0 only

You cannot upgrade to Version 6.7.0 from Version 6.6.5 or any later 6.6.x maintenance release. This is because the Version 6.6.5 data store is newer than the Version 6.7.0 data store. If you are running Version 6.6.5+, we recommend you upgrade directly to Version 7.0.0 or later.

Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs

Deployments: Firepower 1010

Upgrading from: Version 6.4.0 through 6.6.x

Directly to: Version 6.7.0+

For the Firepower 1010, FTD upgrades to Version 6.7.0+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Previously Published Guidelines

This checklist contains older upgrade guidelines.

Table 20: Version 6.7.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 58	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	FMCv Requires 28 GB RAM for Upgrade, on page 59	FMCv	6.2.3 through 6.5.0.x	6.6.0+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle	Firepower 1000 series	6.4.0.x	6.5.0+
	Historical Data Removed During FTD/FDM Upgrade, on page 60	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 60	Any	6.2.3 through 6.4.0.x	6.5.0+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 66	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+

Upgrade Failure: FMC with Email Alerting for Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.2.3 through 6.7.0.x

Directly to: Version 6.6.0, 6.6.1, 6.6.3, or 6.7.0, as well as any patches to these releases

Related bugs: CSCvw38870, CSCvx86231

If you configured email alerting for individual intrusion events, fully disable it before you upgrade a Firepower Management Center to any of the versions listed above. Otherwise, the upgrade will fail.

You can reenable this feature after the upgrade. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

To fully disable intrusion email alerting:

1. On the Firepower Management Center, choose **Policies** > **Actions** > **Alerts**, then click **Intrusion Email**.
2. Set the **State** to **off**.

3. Next to **Rules**, click **Email Alerting per Rule Configuration** and deselect any rules.

   Note which rules you deselected so you can reselect them after the upgrade.

Tip If reselecting rules would be too time consuming, contact Cisco TAC *before* you upgrade. They can guide you through saving your selections, so you can quickly reimplement them post-upgrade.

4. Save your configurations.

FMCv Requires 28 GB RAM for Upgrade

Deployments: FMCv

Upgrading from: Version 6.2.3 through 6.5.0.x

Directly to: Version 6.6.0+

All FMCv implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB to the virtual appliance. After upgrade, the health monitor will alert if you lower the memory allocation.

These new memory requirements enforce uniform requirements across all virtual environments, improve performance, and allow you to take advantage of new features and functionality. We recommend you do not decrease the default settings. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. For details on FMCv memory requirements, see the Cisco Firepower Management Center Virtual Getting Started Guide.

Note As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.

This table summarizes pre-upgrade requirements for lower-memory FMCv deployments.

Table 21: FMCv Memory Requirements for Version 6.6.0+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.

Platform	Pre-Upgrade Action	Details
AWS	Resize instances: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

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 detailed lists of category changes, see the Cisco Firepower Release Notes, Version 6.5.0. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

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

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

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

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

- *Reputationless URLs* can belong to any category.

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

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

Table 22: 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.
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 23: 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 24: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 63. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

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

Table 25: 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 26: 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.

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.

Time Tests and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. You must also have enough time to perform the upgrade. We provide reports of in-house time and disk space tests for reference purposes.

About Time Tests

Time values are based on in-house tests.

Although we report the *slowest* time of all upgrades tested for a particular platform/series, your upgrade will likely take longer than the provided times for multiple reasons, as follows.

Table 27: Time Test Conditions

Condition	Details
Deployment	Values are from tests in a Firepower Management Center deployment. 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.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual settings	We test with the default settings for memory and resources.

Condition	Details
High availability and 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	Values represent *only* the time it takes for the Firepower software upgrade script. They do not include time for: • Operating system upgrades. • Transferring upgrade packages. • Readiness checks. • VDB and intrusion rule (SRU/LSP) updates. • Deploying configurations. • Reboots, although reboot time may be provided separately.

About Disk Space Requirements

Space estimates are the *largest* reported for all Firepower software upgrades. For releases after early 2020, they are:

- Not rounded up (under 1 MB).
- Rounded up to the next 1 MB (1 MB - 100 MB).
- Rounded up to the next 10 MB (100 MB - 1GB).
- Rounded up to the next 100 MB (greater than 1 GB).

Values represent *only* the space needed to upload and run the Firepower software upgrade script. They do not include values for operating system upgrades, VDB or intrusion rule (SRU/LSP) updates, and so on.

Note When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in /Volume for the device upgrade package (unless you configure an internal web server where your devices can get the package; requires Firepower Threat Defense Version 6.6.0+) .

Checking Disk Space

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.

To check disk space:

- Firepower Management Center and its managed devices: Use the **System** > **Monitoring** > **Statistics** page on the FMC. After you select the appliance you want to check, under Disk Usage, expand the By Partition details.
- Firepower Threat Defense with Firepower Device Manager: Use the **show disk** CLI command.
- ASA FirePOWER with ASDM: Use the **Monitoring** > **ASA FirePOWER Monitoring** > **Statistics** page. Under Disk Usage, expand the By Partition details.

Version 6.7.0 Time and Disk Space

Table 28: Version 6.7.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	13.6 GB	70 MB	—	46 min	9 min
FMCv: VMware 6.0	15.5 GB	64 MB	—	35 min	8 min
Firepower 1000 series	430 MB	11 GB	2 GB	17 min	16 min
Firepower 2100 series	500 MB	11 GB	1.1 GB	15 min	16 min
Firepower 9300	64 MB	11.1 GB	1.1 GB	13 min	12 min
Firepower 4100 series	10 MB	10 GB	1.1 GB	10 min	12 min
Firepower 4100 series container instance	8 MB	9.5 GB	1.1 GB	10 min	9 min
ASA 5500-X series with FTD	8.7 GB	96 KB	1.1 GB	26 min	13 min
FTDv: VMware 6.0	8.1 GB	26 KB	1.1 GB	14 min	18 min
ASA FirePOWER	10.3 GB	64 MB	1.3 GB	62 min	11 min
NGIPSv: VMware 6.0	5.5 GB	54 MB	840 MB	10 min	6 min

Traffic Flow, Inspection, and Device Behavior

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When a device is rebooted.
- When you upgrade the operating system or virtual hosting environment on a device.
- When you upgrade the Firepower software on a device.
- When you uninstall or revert the Firepower software on a device.
- When you deploy configuration changes as part of the upgrade or uninstall process (Snort process restarts).

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) 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

This section describes device and traffic behavior when you upgrade a Firepower 4100/9300 chassis with FTD.

These scenarios also apply to patch uninstall in Firepower Management Center deployments. However, revert is performed simultaneously on all units; that is, revert treats every device as a standalone device, regardless of your high availability/scalability configuration. Therefore, interruptions to traffic flow and inspection during revert depend on interface configurations only. Support for revert begins in Version 6.7.0 for Firepower Device Manager deployments.

Firepower 4100/9300 Chassis: FXOS Upgrade

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 29: Traffic Behavior During FXOS Upgrade

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.

Deployment	Method	Traffic Behavior
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.

Standalone FTD Device: Firepower Software Upgrade

Firepower devices/security modules 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.

This table also applies to device revert, regardless of your high availability/scalability configuration.

Table 30: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

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, 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.

High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The standby device upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Clusters: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in Firepower Threat Defense clusters. To ensure continuity of operations, they upgrade one at a time. The data security module or modules upgrade first, then the control module. Security modules operate in maintenance mode while they upgrade.

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.

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 on all Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 31: Traffic Behavior During FTD Deployment

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, **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

This section describes device and traffic behavior when you upgrade Firepower Threat Defense, with the exception of the Firepower 4100/9300.

These scenarios also apply to patch uninstall in Firepower Management Center deployments. However, revert is performed simultaneously on all units; that is, revert treats every device as a standalone device, regardless of your high availability/scalability configuration. Therefore, interruptions to traffic flow and inspection during revert depend on interface configurations only. Support for revert begins in Version 6.7.0 for Firepower Device Manager deployments.

Standalone FTD Device: Firepower Software Upgrade

Firepower 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.

This table also applies to device revert, regardless of your high availability/scalability configuration.

Table 32: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

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.

High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The standby device upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

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 on all Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 33: Traffic Behavior During FTD Deployment

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, **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 34: 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 35: 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 36: 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

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 37: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide

Task	Guide
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
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.

Upgrade Packages

Firepower software packages are available on the Cisco Support & Download site.

- Firepower Management Center, including Firepower Management Center Virtual: https://www.cisco.com/go/firepower-software
- Firepower Threat Defense (ISA 3000): https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense (all other models, including Firepower Threat Defense Virtual): https://www.cisco.com/go/ftd-software
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software

To find a Firepower software upgrade package, select or search for your Firepower appliance model, then browse to the Firepower software download page for your current version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.

Tip A Firepower Management Center with internet access can download select releases directly from Cisco, some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors.

You use the same upgrade package for all Firepower models in a family or series. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and Firepower version. Maintenance releases use the upgrade package type.

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Upgrade-6.7.0-999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: 6.7.0-999
- File extension: sh.REL.tar

So that Firepower can verify that you are using the correct files, upgrade packages from Version 6.2.1+ are *signed* tar archives (.tar). Do not untar signed (.tar) packages. And, do not transfer upgrade packages by email.

Note After you upload a signed upgrade package, the Firepower Management Center GUI can take several minutes to load as the system verifies the package. To speed up the display, remove these packages after you no longer need them.

Firepower Software Upgrade Packages

Table 38:

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center
Firepower 1000 series	Cisco_FTD_SSP-FP1K
Firepower 2100 series	Cisco_FTD_SSP-FP2K
Firepower 4100/9300	Cisco_FTD_SSP
ASA 5500-X series with FTD ISA 3000 with FTD FTDv	Cisco_FTD
ASA FirePOWER	Cisco_Network_Sensor
NGIPSv	Cisco_Firepower_NGIPS_Virtual

ASA and FXOS Upgrade Packages

For information on operating system upgrade packages, see the planning topics in the following guides:

- Cisco ASA Upgrade Guide, for ASA OS
- Cisco Firepower 4100/9300 Upgrade Guide, for FXOS

CHAPTER 5

Uninstall an Upgrade

You can revert major and maintenance upgrades to Firepower Threat Defense in FDM deployments. This returns the device to its state just before the upgrade. Revert is not supported in Firepower Management Center or ASDM deployments.

Uninstall, Revert, or Reimage?

This table describes the options for removing a successfully completed Firepower upgrade, in order of most to least drastic. These options depend on your deployment and the type of upgrade you want to remove. Note that you should not attempt to uninstall a hotfix. Instead, contact Cisco TAC.

Note Reverting/uninstalling is for situations where the upgrade succeeds, but the upgraded system does not function to your expectations. This is not the same as canceling a failed or in-progress upgrade, which also returns the device to its pre-upgrade state.

Table 39: Options for Returning to a Previous Release

Platform	Method	Version Restrictions	Description
Any	Reimage	To major or maintenance releases only. You cannot reimage to a patch level.	Returns the appliance to factory defaults, with very few exceptions. After reimaging, you must reconfigure entirely from scratch. You may be able to import previously exported configurations, or restore from backup. For details on reimaging, see Install the Software, on page 83.

Platform	Method	Version Restrictions	Description
Firepower Threat Defense with FDM	Revert	Major and maintenance upgrades only.	Returns the device to its state just before the last major or maintenance upgrade (also called a *snapshot*). Reverting after patching necessarily removes patches as well. After reverting, you must redo any configuration changes you made between the upgrade and the revert.
Firepower Management Center Firepower Threat Defense with FMC NGIPS devices with FMC ASA FirePOWER with ASDM	Uninstall	Patches only.	Returns the appliance to whatever patch level it was running before the upgrade. Does not change configurations. For details on uninstalling patches, see the patch release notes.

Revert in Firepower Device Manager Deployments

Guidelines for Revert with Firepower Device Manager

In Version 6.7.0+ Firepower Device Manager deployments, you can revert major and maintenance upgrades to Firepower Threat Defense. Revert is not supported in Firepower Management Center or ASDM deployments.

Revert Is a Snapshot

Reverting returns the Firepower software to its state just before the last major or maintenance upgrade, also called a *snapshot*. Reverting after patching necessarily removes patches as well. After reverting, you must redo any configuration changes you made between the upgrade and the revert.

You can delete the snapshot in order to save disk space, but this removes your ability to revert.

Revert Does Not Downgrade FXOS

For the Firepower 4100/9300 chassis, major Firepower versions have a specially qualified and recommended companion FXOS version. This means that after you revert the Firepower software, you may be running a non-recommended version of FXOS (too new).

Although newer versions of FXOS are backwards compatible with older Firepower versions, we do perform enhanced testing for the recommended combinations. You cannot downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

For more information, see the Cisco Firepower Compatibility Guide.

Revert High Availability Units Simultaneously

If you need to revert both units in a Firepower Threat Defense high availability pair, we recommend you initiate the revert on both units at the same time. Open sessions with both units, verify that revert is possible on each, then start the processes.

Revert an Upgrade with Firepower Device Manager

Use this procedure to revert Firepower Threat Defense with Firepower Device Manager.

If you cannot get into FDM, use the **upgrade revert** FTD CLI command. You can use the **show upgrade revert-info** command to see what version the system will revert to.

Before you begin

Read and understand the Guidelines for Revert with Firepower Device Manager, on page 80.

Step 1 Select **Device**, then click **View Configuration** in the **Updates** summary.

Step 2 In the **System Upgrade** section, click the **Revert Upgrade** link.

You are presented with a confirmation dialog box that shows the current version and the version to which the system will revert. If there is no available version to revert to, there will not be a **Revert Upgrade** link.

Step 3 If you are comfortable with the target version (and one is available), click **Revert**.

CHAPTER 6

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.

Guidelines for Fresh Installs

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.

Reimage Checklist

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. Refer to the appropriate installation guide for full instructions: Installation Instructions, on page 86.

Table 40:

✓	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 Firepower Management Center deployments, you should also able to access the Firepower Management Center management interface without traversing the device.
	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 Firepower product.
	Determine if you must remove devices from Firepower Management Center management. If you plan to manually configure the reimaged appliance, remove devices from remote management before you reimage: • If you are reimaging the Firepower Management Center, 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.

✓	Action/Check
	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 85 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

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 41: 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
FMCv	Cisco Firepower Management Center Virtual Getting Started Guide

Table 42: 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: GCP	Cisco Firepower Threat Defense Virtual for the Google Cloud Platform Getting Started Guide
FTDv: KVM	Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
FTDv: OCI	Cisco Firepower Threat Defense Virtual for the Oracle Cloud Infrastructure Getting Started Guide

FTD Platform	Guide
FTDv: VMware	Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide

Table 43: NGIPSv and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware
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 7

Documentation

For Firepower documentation, see:

- New and Updated Documentation, on page 89
- Documentation Roadmaps, on page 91

New and Updated Documentation

The following Firepower documentation was updated or is newly available for this release. For links to other Firepower documentation, see the Documentation Roadmaps, on page 91.

Firepower Configuration Guides and Online Help

- Firepower Management Center Configuration Guide, Version 6.7 and online help
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.7.0 and online help
- Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.7 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, 2.9(1)
- Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.9(1)
- Cisco Firepower 4100/9300 FXOS Command Reference
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.9(1)

Upgrade Guides

- Cisco Firepower Management Center Upgrade Guide
- Cisco Firepower 4100/9300 Upgrade Guide
- Cisco ASA Upgrade Guide

Hardware Installation Guides

- Cisco Firepower 1010 Hardware Installation Guide
- Cisco Firepower 1100 Series Hardware Installation Guide
- Cisco Firepower 2100 Series Hardware Installation Guide

Getting Started Guides

- Cisco Firepower Management Center Virtual Getting Started Guide
- Cisco Firepower 1010 Getting Started Guide
- Cisco Firepower 1100 Series Getting Started Guide
- Cisco Firepower 2100 Series Getting Started Guide
- Cisco Firepower 4100 Getting Started Guide
- Cisco Firepower 9300 Getting Started Guide
- Cisco ISA 3000 Getting Started Guide
- Cisco ASA 5508-X and 5516-X Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the AWS Cloud Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the Google Cloud Platform Getting Started Guide ***NEW***
- Cisco Firepower Threat Defense Virtual for the Oracle Cloud Infrastructure Getting Started Guide ***NEW***
- Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

API and Integration Guides

- Firepower Management Center REST API Quick Start Guide, Version 6.7.0
- Cisco Firepower Threat Defense REST API Guide
- Firepower System Database Access Guide v6.7
- Cisco Security Analytics and Logging On Premises: Firepower Event Integration Guide ***NEW***

Compatibility Guides

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

Licensing

- Cisco Firepower System Feature Licenses
- Frequently Asked Questions (FAQ) about Firepower Licensing

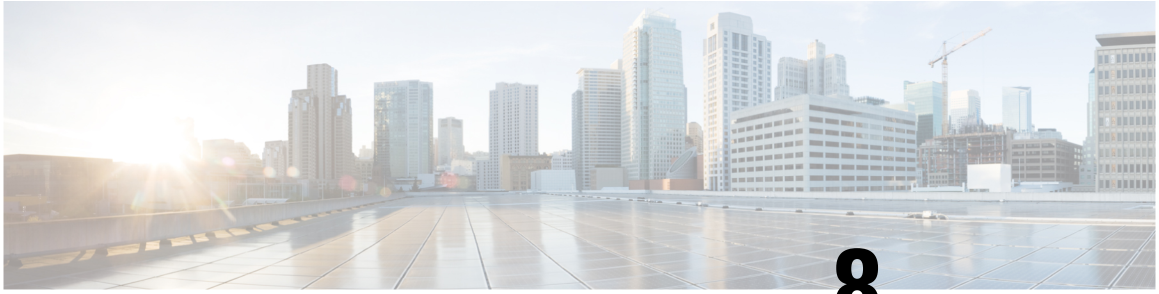
Troubleshooting and Configuration Examples

- Cisco Firepower Threat Defense Syslog Messages
- FMC and FTD Management Network Administration ***NEW***
- Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability
- Deploy the FTD at a Remote Branch Office with FMC ***NEW***

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 8

Resolved Issues

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

Note This list is auto-generated *once* and is 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.'

Searching for Resolved Issues

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

These general queries display resolved bugs for Firepower products running Version 6.7.0:

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- Firepower Threat Defense Virtual
- ASA with FirePOWER Services
- NGIPSv

Version 6.7.0 Resolved Issues

Table 44: Version 6.7.0 Resolved Issues

Bug ID	Headline
CSCuq33233	Clustering: Overlapping PAT IPs in NAT rules prevent xlates from replicating
CSCvd09106	Editing SNMP/Syslog/Email Alert Configuration causes in use count to increase
CSCvf34107	False positive alerts for High Unmanaged Disk usage on /Volume
CSCvg01007	https pdf attachment issues
CSCvg74990	Need to update Online documentation for Archive Inspection feature limitations
CSCvh65500	Firepower 2100 Client in FTP active mode is not able to establish control channel with the Server
CSCvi47847	Shell application not detected through Firepower
CSCvi51189	ENH: FDM should allow custom non-UDP/TCP 443 port for webvpn/AnyConnect
CSCvi92162	DOC: Need explanation about App and URL inspection of HTTPS traffic on each Firepower version
CSCvi96835	No validation err when changing host thats part of a group object used in a routing policy, to Range
CSCvj87597	Import fails when Flex Config contains a Security Zone.
CSCvj91418	Cisco FTD Software SMB Protocol Preprocessor Detection Engine Low System Memory DoS Vuln
CSCvk16568	AppID stop processing traffic if Application ID has been detected
CSCvk21405	shell application not pin holing new connection from server
CSCvk40714	Unable to configure SSH option for Remote Storage
CSCvk56513	Tor not blocked when traffic is passed through proxy.
CSCvk62871	Firepower 2100 FTP Client in passive mode is not able to establish data channel with the Server
CSCvm69294	Standby FMC sending Flood of SNMP traps
CSCvm99989	SNMP OID for SystemUpTime show incorrect value
CSCvn08417	ENH: FlexConfig should not blacklist crypto commands
CSCvn49854	Subsequent HTTP requests not retrieving URL and XFF
CSCvn73530	Scheduled deployment task on KP devices were stuck for more than 50+ hours.

Bug ID	Headline
CSCvn78597	Firepower block page not displayed on MS IE11 and Edge for HTTPS blocked sites when proxy is enabled
CSCvn94888	FTD registered to FMC returns "Service Unavailable"
CSCvo33348	Mysql traffic on non standard port is not correctly classified
CSCvp06526	Manage the sfhassd thread CPU affinity to match the Snort CPU affinity
CSCvp29817	Fail to update login history when converting TempID to RealID. 1x log per ID, history lost
CSCvp80474	OpenSSL vulnerability CVE-2019-1559 on SFOS
CSCvq23896	TLS 1.3 traffic whitelisted by SSL preprocessor when pending for AppID
CSCvq39888	Cisco Firepower Threat Defense Software Non-Standard Protocol Detection Bypass Vuln
CSCvq39955	Cisco Firepower Threat Defense Software Stream Reassembly Bypass Vulnerability
CSCvq54551	Failed to load error on Intelligence Page for FMC for CAC User
CSCvq67965	ENH:Need the ability to disable auto negotiation in SFP - Fp2k
CSCvq76964	Fault Related to Unhealthy module FlexFlash Controller 1 old Firmware
CSCvq95058	IPSEC SA is deleted by failover which is caused by link down
CSCvr01675	Multiple Cisco Products Snort HTTP Detection Engine File Policy Bypass Vulnerability
CSCvr09399	Dynamic flow-offload can't be disabled
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"
CSCvr13762	NGFWHA Missing EO UUID on FMC
CSCvr39217	Fxos Snmp-user is not persistent after reboot
CSCvr49729	Fail-to-Wire ports showing down for FPR2100, FTW configuration API takes long to finish
CSCvr49833	Cisco Firepower 2100 Series Security Appliances ARP Denial of Service Vulnerability
CSCvr55535	Phase 3 of policy deployment takes a long time due to only working on 10 packages at a time
CSCvr57051	Policy deployment failed with error "Can't use an undefined value as a HASH reference "
CSCvr66067	Provide the backup and restore steps for FMC in high availability deployment mode
CSCvr66798	DNS Application Detector sometimes fails to detect DNS traffic

Bug ID	Headline
CSCvr68885	FXOS fault F0479 Virtual Interface link state is down
CSCvr74896	Cannot update Security intelligence when AC Policy is imported to FMC with cloud feeds disabled
CSCvr74901	AppAG encoding for FXOS logical device bootstrap
CSCvr86077	ASA Traceback/pagefault in Datapath due to re_multi_match_ascii
CSCvr86213	CD is required to ignore Cluster-Msg-Delivery-Confirmation in Cluster Node Release Lina State
CSCvr98881	Traceback: FTD ZeroMQ memory assertion
CSCvs05066	Snort file mempool corruption leads to performance degradation and process failure.
CSCvs06043	TunnelClient for CSM_CCMservice on ngfwManager not reading ACK sent from CSM_CCM service on FMC
CSCvs13950	REST API Network Object Validation
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.
CSCvs21705	admin user is not authorized to access the device routing configuration inside the domain.
CSCvs29494	Hub and spoke VPN, dynamic crypto map, auto-generated PSK is the same for static and dynamic peers
CSCvs31114	Warning about not supported bypass revocation checking for FTD 6.5 and higher
CSCvs33392	Known Key SSL decryption and connections can fail when servers are using unsupported TLS options
CSCvs34851	Continuous link flapping leading to snm_log corefile
CSCvs37266	Reviewed intrusion events belonging to a subdomain show the reviewer as Unknown
CSCvs39253	Firepower 7000 & 8000 cannot sent emails on version 6.4
CSCvs39368	DME process may traceback due to memory leak on Firepower 4100/9300
CSCvs39388	FTD not sending system syslog messages in CC mode
CSCvs41883	Deployment fails after upgrading to 6.4.0.x if ND policy refs are missing
CSCvs42203	hostname transmission: Hostname is null, Device sends hostname as "none" to SA
CSCvs42388	Gratuitous logging of string: "Memory stats information for preprocessor is NULL"
CSCvs42577	user download may fail due to password not sent
CSCvs42799	After FXOS upgrade, App Instance failed to start with Checksum Verification Fail

Bug ID	Headline
CSCvs44109	FMC: PPPoE password restrictions are too strict; should match the underlying code
CSCvs44149	Reconciliation report not displaying all the networks when adding a large object group
CSCvs52227	Firewall engine debug logs being produced in syslog without actually enabling debugs.
CSCvs59866	Remove unsupported fast mode lacppolicy configuration from FXOS on Firepower 2100
CSCvs64510	Deployment failure with message (Can't call method "binip" on unblessed reference)
CSCvs68576	Deploy failure when deleting auto nat rule due to double negate
CSCvs71578	FMC upgrade [6.2.3.10 to 6.4.0] got stuck at 400_run_troubleshoot.sh, upgrade was hung
CSCvs72390	Cisco Firepower Management Center Cross-Site Scripting Vulnerability
CSCvs74586	Firepower FTD transparent does not decode non-ip packets
CSCvs74747	FTD registration state shows "pending" after a backup is restored
CSCvs76604	SNMP not working over Management Interface in 6.6.0-1430
CSCvs81871	Remove CCL MTU Pop-Up Warning When Editing Data Interfaces
CSCvs85348	Object validation is validating interfaces from different devices.
CSCvs85640	Unable to supress Audit logs on the FMC
CSCvs86765	rule impact regeneration should not terminated on single rule errors
CSCvs90447	FXOS 8x1G FTW continuous link flap
CSCvs91270	Inspect Interruption - Error in deployment page.
CSCvs92044	FXOS L3 Egress Object Resource Leak due to Port-Channel Member Interface Flaps
CSCvs92077	wrong impact flag for local rules with impact flag not red
CSCvs94061	NTP script error leading to clock drift and traffic interruption
CSCvs98373	FMC is unable to detect classic licenses intermittently
CSCvt01397	Deployment is marked as success although LINA config was not pushed
CSCvt03320	VLAN interfaces should be configurable for DHCP-related configuration on an FMC
CSCvt04377	When vlan encapsulation is exceeded decoding errors are depleting disk space.
CSCvt06091	FXOS displays a WSP-Q40GLR4L transceiver from show interface as type QSFP-40G-LR4
CSCvt06743	FTW watch-dog kick delays which might cause inline sets to go down/Bypass-Fail

Bug ID	Headline
CSCvt08514	SFDataCorrelator:FPReplicationCommunicationRabbit unable to connect without restarting sfipproxy
CSCvt10420	DomainSearchNameValidator class needs updated regex for DOMAIN_NAME_PATTERN
CSCvt10604	Validation Check when two objects with different mask but same network is used in route without ECMP
CSCvt11885	Running the migration script exits with an out of memory error
CSCvt15062	FTD 2100: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted
CSCvt16642	FMC not sending some audit messages to remote syslog server
CSCvt16723	log rotation for ngfw-onbox logs NOT happening at expected log size
CSCvt17448	OSPF multicast mac getting removed from l2-table causing OSPF to fail
CSCvt18337	Failover got disabled on HA node after upgrade
CSCvt20235	Firepower 4100 series all FTW interfaces link flap at the same time but occur rarely
CSCvt20709	Wrong direction in SSL-injected RESET causes it to exit through wrong interface, causing MAC flap
CSCvt21986	Inconsistent allocation of cores for snort and lina between instances
CSCvt22254	Auto Deploy fails after Restore if FDM cannot reach update server
CSCvt25599	Deprecated Flexconfig should block deployment not just warn
CSCvt25647	sru and tid update failures caused by missing rabbitmq device accounts
CSCvt26530	FTD failed over due to 'Inspection engine in other unit has failed due to snort failure'
CSCvt34160	"Link not connected" error after reboot when using WSP-Q40GLR4L transceiver on FPR9K-NM-4X40G
CSCvt34894	Snort consumes excessive memory which is leading to performance problems.
CSCvt34973	SFNotificationd may cause excessive logging in 'messages' files
CSCvt35053	Cisco Firepower Management Center Software Cross-Site Scripting Vulnerabilities
CSCvt35134	FPR4100/9300: Packet drops during the transition of BYPASS to NON-BYPASS when device is rebooted
CSCvt35233	Excessive logging from the daq modules process_snort_verdict verdict blacklist
CSCvt35366	Excessive logging of lua detector invalid LUA (null)
CSCvt35730	FDM deployment error if 2nd tunnel has overlapping crypto ACL

Bug ID	Headline
CSCvt35897	Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software DoS Vuln
CSCvt37881	Block page for https not working
CSCvt37913	serviceability - when breaking FMC HA EOs authority stays with former primary
CSCvt38279	Erase disk0 on ISA3000 causes file system not supported
CSCvt39292	LDAPS External users can't 'sudo su' on Firepower 4110
CSCvt39349	Registration of device should be allowed as long as deploy status = DEPLOYED or FAILED
CSCvt39897	FP 4120 svc_sam_dcosAG crashed with crash type:139
CSCvt40306	ASA:BVI interface of standby unit stops responding after reload
CSCvt45206	Event search may fail when searching events that existed before upgrade
CSCvt46784	clish configure ssh-accesslist command fails silently if iptables is corrupt
CSCvt46999	EventHandler does not process connection events after CLI command to enable/disable ramdisk
CSCvt48260	Standby unit traceback at fover_parse and boot loop when detecting Active unit
CSCvt50528	Warning Message for default settings with Installation of Certificates in ASA/FTD - CLI
CSCvt51039	Handling license cleanup
CSCvt52604	Interfaces page from Objects section of the FMC does not load (domains page is likely affected also)
CSCvt52607	Reduce SSL HW mode flow table memory usage to reduce the probability of Snort going in D state
CSCvt52844	AMP cloud lookup using legacy port on upgraded FDM, 6.6.0-1621
CSCvt54267	Cisco Firepower Management Center Software Denial of Service Vulnerability
CSCvt54279	FDM: Deploy fails with: Missing license for object: Sensitive_data requires the URLFILTERING license
CSCvt54943	extra "Local Disk 3" displayed on FPR9300 (improved solution)
CSCvt59770	FTD: Failure to retrieve certificate via SCEP will cause outage
CSCvt61196	ASA on multicontext mode, deleting a context does not delete the SSH keys.
CSCvt61229	Deployment should not fail for special characters in rule comments
CSCvt61370	Events may stop coming from a device due to a communication deadlock

Bug ID	Headline
CSCvt63293	Disk Usage Health monitor not working for any appliance without 2 Hard Drives
CSCvt64642	FMC -Deployment Failure- Anyconnect - "Certificate Map" using "DC (Domain Component)" to match cert.
CSCvt64822	Cisco Adaptive Security Appliance Software SSL/TLS Denial of Service Vulnerability
CSCvt67638	restore is failing with error unable to extract metadata
CSCvt68486	FXOS: svc_sam_dcosAG process crash on FirePower 4100/9300
CSCvt69260	connection event shows old device name
CSCvt70879	"clear configure access-list" on ACL used for vpn-filter breaks access to resources
CSCvt72683	NAT policy configuration after NAT policy deployment on FP 8130 is not seen
CSCvt73808	Handling for longer header length messages going from DAQ to Oct driver
CSCvt75677	Configuring logical name as TRUE or FALSE on interface disappears all static routes from FMC UI
CSCvt78809	Instance start failed due to VNIC configuration error
CSCvt79471	GET to ../deployment/deployabledevices fails with 500 internal error on 6.2.3.13 FMC.
CSCvt79777	duplicate ip addresses in sfipproxy.conf
CSCvt79863	FTD upgrade incorrectly declared successful despite failure due to IO errors
CSCvt79988	Policy deployment failure due to snmp configuration after upgrading FMC to 6.6
CSCvt80104	Memcached software needs to be upgraded to address CVE-2018-1000115
CSCvt80172	Supervisor software needs to be upgraded to address CVE-2017-11610
CSCvt83121	Cisco ASA and FTD Software OSPFv2 Link-Local Signaling Denial of Service Vulnerability
CSCvt83133	Unable to access anyconnect webvpn portal from google chrome using group-url
CSCvt85815	Policy Deployment fails after enabling "Sensitive Data Detection"
CSCvt86807	Web Analytics (Google Analytics) is re-enabled after major upgrade
CSCvt89587	Deployment failing with error : Input line size exceeded available buffer
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt93177	Disable Full Proxy to Light Weight Proxy by Default. (FP2LWP) on FTD Devices
CSCvt93999	FMC shouldn't allow a second upgrade on same device if upgrade is going on
CSCvt94383	Invalid gid permissions causing HA sync and device registration issues

Bug ID	Headline
CSCvu01083	Add RabbitMQ log cleaning exception to avoid process restart
CSCvu02594	Snort taking long time to terminate, because of too many async sessions
CSCvu05216	cert map to specify CRL CDP Override does not allow backup entries
CSCvu08802	FTD HA configuration lost on FMC after FMC upgrade from 6.4.0.7 to 6.5.0.4
CSCvu09379	During reimage FMC will get stuck in a loop when using FTP transfer without password
CSCvu09496	DNS data collected and exported multiple times while same DNS policy referenced in many ACP's
CSCvu09723	FDM: Default Action's logging doesn't reflect on LINA side
CSCvu10900	Tons of ssl-certs-unified.log files, contributing to 9GB in troubleshoot
CSCvu11868	"Link not connected" error after reboot when using QSFP-40G-LR4 transceiver on FPR9K-NM-4X40G
CSCvu12307	FTD-HA: "ERROR: The specified AnyConnect Client image does not exist."
CSCvu12608	ASA5506/5508/5516 devices not booting up properly / Boot loop
CSCvu13287	FDM unable to import certificate with no subject or issuer - fails upgrade as well
CSCvu14647	Unable to stop config database error during FMC HA sync
CSCvu14772	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, pa
CSCvu15611	FTD-HA: Standby failed to join HA "CD App Sync error is App Config Apply Failed"
CSCvu16201	Data Correlator terminated unexpectedly on FMC during CheckClientAppVulnerability
CSCvu22377	An extra whitespace in cluster group name of FTD causing Slave to be kicked out.
CSCvu23289	Disk filled by numerous neostore.transaction.db.* files, causing neo4j issues
CSCvu26658	SFDataCorrelator can drop events during backup operations
CSCvu29660	Block exhaustion snapshot not created when available blocks goes to zero
CSCvu30549	Document all 3 URL entry options for "Manual URL Filtering"
CSCvu30572	Document syntax and semantics of URL when "Enter URL" textbox of "Add Rule" is used
CSCvu30585	Document "URL Object" format and feature operation
CSCvu30588	Document "URL List and Feeds Object" format and feature operation of "Security Intelligence"
CSCvu30756	User Identity does not correctly handle identical sessions in different netmaps

Bug ID	Headline
CSCvu31167	DOC: File policy automatically enables inline normalization with Normalize TCP Payload option
CSCvu32449	FDM: AnyConnect "Validation failed due to duplicate name:"
CSCvu36539	Upgrade will fail if a smart licensed device is upgraded from 6.2.2 -> 6.4.0 -> 6.6.0.
CSCvu40531	FXOS LACP packet logging to pktmgr.out and lacp.out fills up /opt/cisco/platform/logs to 100%
CSCvu43827	ASA & FTD Cluster unit traceback in thread Name "cluster config sync" or "fover_FSM_thread"
CSCvu53585	Elektra onbox policy deployment failure after upgrade to 6.6.0
CSCvu54000	Firepower 4100 FTP Client in EPSV passive mode is not able to establish data channel with the Server
CSCvu54221	Add hardware requirement for FMC HA
CSCvu54706	Cisco Firepower Management Center CWE-772 - Slow HTTP POST vulnerability
CSCvu55469	FTD - Connection idle timeout doesn't reset
CSCvu57825	Snort down: Reconfiguring Detection Error
CSCvu57834	syslog-ng process utilizing 100% CPU
CSCvu58153	Display RADIUS port representation as little-endian instead of big-endian
CSCvu60923	Editing the IP in a Radius Server Group object results in unintended values for the IP address
CSCvu65085	[DOC] Route-map object Set Clauses do not include EIGRP k-values.
CSCvu65890	FMC unable to switch from MD5 and DES under SNMP3 settings despite not being supported
CSCvu65936	FDM 6.6.0 upgrade(or)configImport fail with EtherChannelInterface as failoverlink validation failure
CSCvu66119	URL rules are incorrectly promoted on series 3 resulting in traffic matching the wrong rule.
CSCvu70529	Binary rules (SO rules) are not loaded when snort reloads
CSCvu75581	Cisco ASA and FTD Web Services Interface Cross-Site Scripting Vulnerabilities
CSCvu77689	FTP to FileZilla miscategorized as SMTP
CSCvu79129	FTD-API/FDM: Smart License Base License is Lost
CSCvu82272	Upgrade on Firepower Management Center may fail due to inactive stale entries of managed devices

Bug ID	Headline
CSCvu82578	Light Theme UI FMC - SFR Module long delay loading Interfaces Page
CSCvu82743	Encoded Rule Plugin SID: value, GID: 3 not registered properly. Disabling this rule
CSCvu82918	HA sync fails on standby with unexpected error
CSCvu83389	ASA drops GTPV1 Forward relocation Request message with Null TEID
CSCvu83629	Number Of URLs in Security Intelligence for URL List file may not appear in new UI (Ligth Theme)
CSCvu84556	Site to Site Dynamic crypto map deployed below RA VPN Dynamic Crypto map
CSCvu85127	Unable to deploy if device with same UUID is trying to connect
CSCvu85381	HA Re-formation fails following a policy deploy failure on standby
CSCvu87879	Deployment gets stuck when HA continually changes state due to interface monitoring
CSCvu88005	FMC REST API user permission for GET taskstatus
CSCvu91292	Snort restarts repeatedly when new custom apps are identified using nmap
CSCvu96927	Not able to remove FQDN object once it is assigned within a NAT group
CSCvu98197	HTTPS connections matching 'Do not decrypt' SSL decryption rule may be blocked
CSCvv02925	OSPF neighbourship is not establising
CSCvv09180	NTP "Server Status" is blank in Firepower Chassis Manager when more than one NTP server configured
CSCvv10901	vFTD on VMware documentation should recommend disabling hyperthreading
CSCvv10948	FDM upgrade - There are no visible pending changes on UI -- but upgrade is not starting
CSCvv11981	Lina side of changes required for bug CSCvr98881 in unified-logging.
CSCvv12988	tomcat does not recover gracefully after getting killed during backup
CSCvv13672	CPU load graph may show incomplete CPU data for longer time period selected
CSCvv14442	FMC backup restore fails if it contains files/directories with future timestamps
CSCvv15013	FXOS sending additional internal VLAN TAG leading to ARP update failure on devices.
CSCvv16245	Cisco Firepower Management Center Software Common Access Card Authentication Bypass Vuln
CSCvv17893	Bad uip snapshot and log file causes FTD to repeatedly requests catchup, and exhausts file handlers

Bug ID	Headline
CSCvv18936	CAC login button doesn't appear on new UI, after session timeout
CSCvv21045	Database doesn't accept any new connections causing event processing to stop
CSCvv21782	6.6.1: Prefilter Policy value shown as Invalid ID for all the traffic in ASA SFR Platform
CSCvv23370	Observed traceback in FPR2130 while running webVPN, SNMP related traffic.
CSCvv26683	"configure high-availability disable" command when executed from CLI causes exception in next HAJoin
CSCvv27113	ProcessMetadata for intrusion event uses wrong local_sid constraint to lookup entry
CSCvv29851	FMC - High Availabilty page not loading after Migration from Virtual to Physical device
CSCvv31197	File names not showing up correctly for the file events for decrypted ssl traffic
CSCvv33013	FDM: Unable to add the secret key with the character ^ @ _
CSCvv34888	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 92)
CSCvv36915	"Show NTP" command does not work on multi-instance FTD
CSCvv38482	FDM UI fails to load after an upgrade
CSCvv40316	FDM - Unable to add the BGP 11th neighbor using smart CLI routing object
CSCvv43864	Preview change log is blank when changes are made to the policy
CSCvv45500	Version 6.6.0.1 FTD Upgrade with FDM Suspends HA
CSCvv46984	Upgrade to 660 fails in HA standby device managed through data interface
CSCvv52591	DMA memory leak in ctm_hw_malloc_from_pool causing management and VPN connections to fail
CSCvv55066	FPR1010: Internal-Data0/0 and data interfaces are flapping during SMB file transfer
CSCvv57476	CSS Styles loading issue in Chrome 85, IE and Edge browsers
CSCvv58604	Reset not sent when traffic matches AC-policy configured with block/reset and SSL inspection
CSCvv64302	DOC: Documentation incorrectly states Logging Events to Ramdisk is not enabled on lower end devices
CSCvv69708	DOC: FTD Improve Platform Settings DNS Resolution configuration guide
CSCvv70096	Snort 2: Memory Leak in SSL Decrypt & Resign Processing
CSCvv73540	Create a monitor to drop file cache once it exceeds a certain limit
CSCvv74951	Disable memory cgroups when running the system upgrade scripts

Bug ID	Headline
CSCvv79705	Upgrade to 6.6.0 or 6.6.1 failed on 800_post/100_ftd_onbox_data_import.sh
CSCvv91486	Memory leak during reload in stream
CSCvv99517	FMC: Unable to save interface config and "An internal error occurred while processing your request"
CSCvw07003	Unable to edit Site-to-Site VPN configuration by a leaf domain admin user
CSCvw07352	SFDataCorrelator log spam, metadata fails after Sybase connection status 0
CSCvw17084	In Firepower Module 6.3, app status is down after restore

CHAPTER 9

Known Issues

For your convenience, the release notes list known bugs for this version.

If your upgrade skips versions, you should also read the known issues for the major versions you are skipping. See the appropriate Cisco Firepower Release Notes.

Note This list is auto-generated *once* and is 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.'

Searching for Known Issues

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

These general queries display open bugs for Firepower products running Version 6.7.0:

- Firepower Management Center
- Firepower Management Center Virtual
- Firepower Threat Defense
- Firepower Threat Defense Virtual
- ASA with FirePOWER Services
- NGIPSv

Version 6.7.0 Known Issues

Table 45: Version 6.7.0 Known Issues

Bug ID	Headline
CSCvv59527	Unresponsive pxGridv2 endpoint download hangs ADI, SFDataCorrelator
CSCvv95130	FTD device (ASA 5500-X & Firepower 1000/2100 series) does not respond after restore from backup
CSCvv99419	[6.7.0] FDM Snort 3 SSL Policy addition/removal causing Snort to restart w/o UI warning
CSCvw20092	File Policy not set in eStreamer event for malware event created by a retrospective event
CSCvw41726	FMC Monitoring Syslog setting manually the Page works erratically
CSCvw46630	FTD: NLP path dropping return ICMP destination unreachable messages
CSCvw48743	Performance Degradation observed with connection based debugging
CSCvw51105	6.7.0 FMC pxGrid connection to ISE 3.0 does not work when ipv6 is configured
CSCvx71029	Speed autonegotiation may need to be disabled on switch connected to FPR device with SFP link

CHAPTER 10

For Assistance

Thank you for choosing Firepower.

Online Support Resources

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

- 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