Cisco Firepower Release Notes, Version 6.3.0

First Published: 2018-12-03

Last Modified: 2022-03-08

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

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

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

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

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

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

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

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

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

CONTENTS

CHAPTER 1 **Welcome** 1

Release Dates 1

Suggested Release 2

CHAPTER 2 **Compatibility** 5

Firepower Management Center 5

Firepower Devices 6

Manager-Device Compatibility 8

Web Browser Compatibility 9

Screen Resolution Requirements 11

CHAPTER 3 **Features and Functionality** 13

Features for Firepower Management Center Deployments 13

New Features in FMC Version 6.3.0 14

Deprecated Features in FMC Version 6.3.0 23

Features for Firepower Device Manager Deployments 25

New Features in FDM Version 6.3.0 25

Deprecated Features in FDM Version 6.3.0 29

About Deprecated FlexConfig Commands 31

Intrusion Rules and Keywords 31

How-To Walkthroughs for the FMC 32

Sharing Data with Cisco 33

CHAPTER 4 **Upgrade the Software** 35

Planning Your Upgrade 35

Minimum Version to Upgrade 36

New Upgrade Guidelines for Version 6.3.0 37
Renamed Upgrade and Installation Packages 38
Reimaging to Version 6.3+ Disables LOM on Most Appliances 39
Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv 40
Reporting Data Removed During FTD/FDM Upgrade 40
RA VPN Default Setting Change Can Block VPN Traffic 40
TLS/SSL Hardware Acceleration Enabled on Upgrade 41
Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER 41
Security Intelligence Enables Application Identification 41
Update VDB after Upgrade to Enable CIP Detection 42
Invalid Intrusion Variable Sets Can Cause Deploy Failure 42
Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade 43
Previously Published Upgrade Guidelines 43
Upgrade Can Unregister FTD/FDM from CSSM 44
Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade 44
Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0 44
Access Control Can Get Latency-Based Performance Settings from SRUs 45
'Snort Fail Open' Replaces 'Failsafe' on FTD 45
Unresponsive Upgrades 46
Traffic Flow and Inspection 46
Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300 47
Firepower Threat Defense Upgrade Behavior: Other Devices 49
Firepower 7000/8000 Series Upgrade Behavior 51
ASA FirePOWER Upgrade Behavior 53
NGIPSv Upgrade Behavior 53
Time and Disk Space Tests 54
Version 6.3.0 Time and Disk Space 56
Upgrade Instructions 56

CHAPTER 5 Install the Software 59
Installation Checklist and Guidelines 59
Unregistering Smart Licenses 61
Installation Instructions 62

CHAPTER 6 Documentation 65

New and Updated Documentation 65

Documentation Roadmaps 67

CHAPTER 7 Resolved Issues 69

Resolved Issues in New Builds 69

Version 6.3.0 Resolved Issues 70

CHAPTER 8 Known Issues 75

Version 6.3.0 Known Issues 75

CHAPTER 9 For Assistance 79

Online Resources 79

Contact Cisco 79

CHAPTER 1

Welcome

This document contains critical and release-specific information.

- Release Dates, on page 1
- Suggested Release, on page 2

Release Dates

Sometimes Cisco releases updated builds. In most cases, only the latest build for each platform is available on the Cisco Support & Download site. We *strongly* recommend you use the latest build. If you downloaded an earlier build, do not use it. For more information, see Resolved Issues in New Builds, on page 69.

Table 1: Version 6.3.0 Dates

Version	Build	Date	Platforms: Upgrade	Platforms: Reimage
6.3.0	85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
6.3.0	84	2018-12-18	FMC/FMCv ASA FirePOWER	—
6.3.0	83	2019-06-27	—	FMC 1600, 2600, 4600
		2018-12-03	All FTD devices except Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices except Firepower 4100/9300

Table 2: Version 6.3.0 Patch Dates

Version	Build	Date	Platforms
6.3.0.5	35	2019-11-18	Firepower 7000/8000 series NGIPSv
	34	2019-11-18	FMC/FMCv All FTD devices ASA FirePOWER
6.3.0.4	44	2019-08-14	All
6.3.0.3	77	2019-06-27	FMC 1600, 2600, 4600
		2019-05-01	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices
6.3.0.2	67	2019-06-27	FMC 1600, 2600, 4600
		2019-03-20	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices
6.3.0.1	85	2019-06-27	FMC 1600, 2600, 4600
		2019-02-18	FMC 750, 1000, 1500, 2000, 2500, 3500, 4000, 4500 FMCv All devices

Suggested Release

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

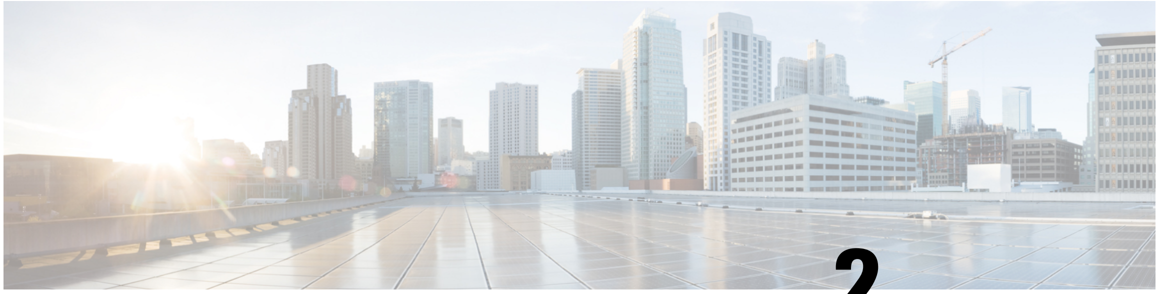
We also list the suggested release in the new feature guides:

- Cisco Firepower Management Center New Features by Release
- Cisco Firepower Device Manager New Features by Release

Suggested Releases for Older Appliances

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

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



CHAPTER 2

Compatibility

For general compatibility information see:

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

For compatibility information for this version, see:

- Firepower Management Center, on page 5
- Firepower Devices, on page 6
- Manager-Device Compatibility, on page 8
- Web Browser Compatibility, on page 9
- Screen Resolution Requirements, on page 11

Firepower Management Center

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

Firepower Management Center

This release supports the following hardware FMC platforms:

- FMC 1600, 2600, 4600
- FMC 1000, 2500, 4500
- FMC 2000, 4000
- FMC 750, 1500, 3500

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)

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 or 6.5

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 8.

Table 3: Firepower Threat Defense in Version 6.3.0

FTD Platform	OS/Hypervisor	Additional Details
Firepower 2110, 2120, 2130, 2140	—	—
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	FXOS 2.4.1.214 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 Firepower 4100/9300 FXOS Release Notes, 2.4(1).
ASA 5508-X, 5516-X ASA 5515-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	Although you do not separately upgrade the operating system on these devices in FTD deployments, you should make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.

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

Table 4: NGIPS/ASA FirePOWER in Version 6.3.0

NGIPS/ASA FirePOWER Platform	OS/Hypervisor	Additional Details
ASA 5508-X, 5516-X ISA 3000	ASA 9.5(2) to 9.16(x)	There is wide compatibility between ASA and ASA FirePOWER versions. However, upgrading allows you to take advantage of new features and resolved issues. See the Cisco ASA Upgrade Guide for order of operations. You should also make sure you have the latest ROMMON image on the ISA 3000, ASA 5508-X and 5516-X. See the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.
ASA 5515-X	ASA 9.5(2) to 9.12(x)	
ASA 5525-X, 5545-X, 5555-X	ASA 9.5(2) to 9.14(x)	
ASA 5585-X-SSP-10, -20, -40, -60	ASA 9.5(2) to 9.12(x)	
NGIPSv	VMware vSphere/VMware ESXi 6.0 or 6.5	For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.
Firepower 7010, 7020, 7030, 7050 Firepower 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140 Firepower 8250, 8260, 8270, 8290 Firepower 8350, 8360, 8370, 8390 AMP 7150, 8050, 8150 AMP 8350, 8360, 8370, 8390	—	—

Manager-Device Compatibility

Firepower Management Center

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

A newer FMC can manage older devices up to a few major versions back, as listed in the following table. However, we recommend you always update your entire deployment. New features and resolved issues often require the latest release on both the FMC and its managed devices.

Table 5: FMC-Device Compatibility

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

Firepower Device Manager

Firepower Device Manager (FDM) is built 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.

Table 6: FDM-FTD Compatibility

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

Adaptive Security Device Manager

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

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

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

Table 7: ASDM-ASA FirePOWER Compatibility

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

Web Browser Compatibility

Browsers

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

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer 11 (Windows only)

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

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

Browser Settings and Extensions

Regardless of browser, you must make sure JavaScript, cookies, and TLS v1.2 remain enabled.

If you are using Microsoft Internet Explorer 11:

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

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

Securing Communications

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

To begin replacing the self-signed certificate:

- Firepower Management Center or 7000/8000 series: Select **System** > **Configuration**, then click **HTTPS Certificates**.
- Firepower Device Manager: Click **Device**, then the **System Settings** > **Management Access** link, then the **Management Web Server** tab.

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

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

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

Browsing from a Monitored Network

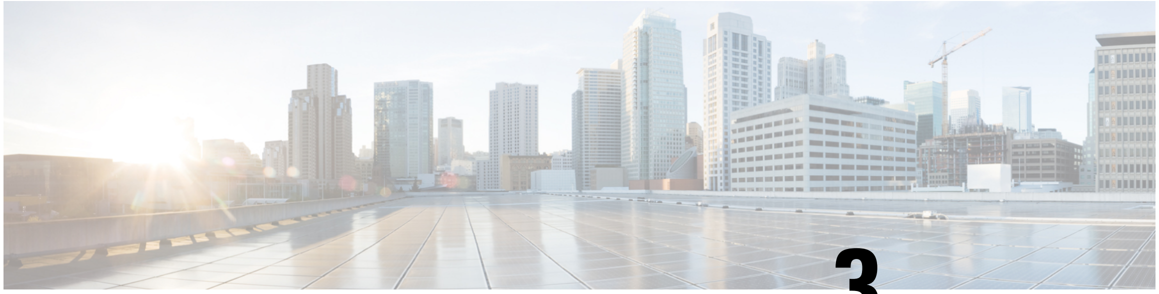
Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using an SSL policy to handle encrypted traffic, and people in your monitored network use browsers with TLS v1.3 enabled, websites that support TLS v1.3 may fail to load.

For more information, see the software advisory titled: *Failures loading websites using TLS 1.3 with SSL inspection enabled*.

Screen Resolution Requirements

Table 8: Screen Resolution Requirements

Interface	Resolution
Firepower Management Center	1280 x 720
7000/8000 series device (limited local interface)	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for the Firepower 4100/9300	1024 x 768



CHAPTER 3

Features and Functionality

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

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

- Features for Firepower Management Center Deployments, on page 13
- Features for Firepower Device Manager Deployments, on page 25
- About Deprecated FlexConfig Commands, on page 31
- Intrusion Rules and Keywords, on page 31
- How-To Walkthroughs for the FMC, on page 32
- Sharing Data with Cisco, on page 33

Features for Firepower Management Center Deployments

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

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

New Features in FMC Version 6.3.0

Table 9:

Feature	Description
Hardware	
FMC models FMC 1600, 2600, and 4600	We introduced the Firepower Management Center models FMC 1600, 2600, and 4600.
ISA 3000 with FirePOWER Services	ISA 3000 with FirePOWER Services is supported in Version 6.3.0 (Protection license only). Although ISA 3000 with FirePOWER Services was also supported in Version 5.4.x, you cannot upgrade to Version 6.3.0. You must reimage.
Firepower Threat Defense: Device Management	
Hardware bypass support on the Firepower 2100 series for supported network modules	Firepower 2100 series devices now support hardware bypass functionality when using the hardware bypass network modules. New/modified pages: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 2100 series
Support for data EtherChannels in On mode	You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode. New/modified Firepower Chassis Manager pages: **Interfaces** > **All Interfaces** > **Edit Port Channel** > **Mode** New/modified FXOS commands: **set port-channel-mode** Supported platforms: Firepower 4100/9300
Firepower Threat Defense: HA and Clustering	

Feature	Description
Multi-instance capability for Firepower 4100/9300 with FTD	You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance. You can use high availability using a container instance on 2 separate chassis. Clustering is not supported. **Note** Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available for FTD. New/modified FMC pages: **Devices** > **Device Management >** edit device **> Interfaces** tab New/modified Firepower Chassis Manager pages: • **Overview** > **Devices** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface** • **Interfaces** > **All Interfaces** > **Type** • **Logical Devices** > **Add Device** • **Platform Settings** > **Mac Pool** • **Platform Settings** > **Resource Profiles** New/modified FXOS commands: **connect ftd***name*, **connect module telnet**, **create bootstrap-key PERMIT_EXPERT_MODE**,**create resource-profile**, **create subinterface**, **scope auto-macpool**, **set cpu-core-count**, **set deploy-type**, **set port-type data-sharing**, **set prefix**, **set resource-profile-name**, **set vlan**, **scope app-instance ftd** *name*, **show cgroups container**, **show interface**, **show mac-address**, **show subinterface**, **show tech-support module app-instance**, **show version** Supported platforms: Firepower 4100/9300

Feature	Description
Cluster control link customizable IP Address for the Firepower 4100/9300	By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. New/modified Firepower Chassis Manager pages: **Logical Devices** > **Add Device** > **Cluster Information** New/modified options: **CCL Subnet IP** field New/modified FXOS commands: **set cluster-control-link network** Supported platforms: Firepower 4100/9300
Improved FTD cluster addition to the FMC	You can now add any unit of a cluster to the FMC, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster with the FMC. Adding a cluster unit is also now automatic. Note that you must delete a unit manually. New/modified pages: • **Devices** > **Device Management > Add** drop-down menu **> Device > Add Device** dialog box • **Devices** > **Device Management > Cluster** tab **> General** area **> Cluster Registration Status > Current Cluster Summary** link **> Cluster Status** dialog box Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Encryption and VPN	
SSL hardware acceleration	Additional FTD devices now support SSL hardware acceleration. Also, this option is now enabled by default. Upgrading to Version 6.3.0 automatically enables SSL hardware acceleration on eligible devices. Using SSL hardware acceleration if you are not decrypting traffic can affect performance. We recommend you disable SSL hardware acceleration on devices that are not decrypting traffic. Supported platforms: Firepower 2100 series, Firepower 4100/9300
RA VPN: RADIUS Dynamic Authorization or Change of Authorization (CoA)	You can now use RADIUS servers for user authorization of RA VPN using dynamic access control lists (ACLs) or ACL names per user. Supported platforms: FTD

Feature	Description
RA VPN: Two-Factor Authentication	Firepower Threat Defense now supports two-factor authentication for RA VPN users using the Cisco AnyConnect Secure Mobility Client. For the two-factor authentication process, we support: • First factor: any RADIUS or LDAP/AD server • Second factor: RSA tokens or DUO passcodes pushed to mobile For more information on Duo multi-factor authentication (MFA) for FTD, see the Cisco Firepower Threat Defense (FTD) VPN with AnyConnect documentation on the Duo Security website. Supported platforms: FTD
Security Policies	
Firepower Threat Defense service policy	You can now configure a Firepower Threat Defense service policy as part of your access control policy advanced options. Use FTD service policies to apply services to specific traffic classes. Features supported include: • TCP State Bypass • Randomizing TCP sequence numbers • Decrementing the time-to-live (TTL) value on packets • Dead Connection Detection • Setting a limit on the maximum number of connections and embryonic connections per traffic class and per client. • Timeouts for embryonic, half closed, and idle connections **Note** Before Version 6.3.0, you could configure connection-related service rules using the TCP_Embryonic_Conn_Limit and TCP_Embryonic_Conn_Timeout predefined FlexConfig objects. You should remove those objects and redo your rules in the FTD service policy. If you created any custom FlexConfig objects to implement any of these connection-related features (that is, **set connection** commands), you should also remove those objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues. The *Threat Defense Service Policies* chapter in the Firepower Management Center Configuration Guide has details on how service policies relate to FlexConfig and other features. New/modified pages: **Policies** > **Access Control** > edit/create policy > **Advanced** tab > **Threat Defense Service Policy** Supported platforms: FTD

Feature	Description
Update interval for URL category and reputation data	**Upgrade impact.** You can now force URL data to expire. There is a tradeoff between security and performance. A shorter interval means you use more current data, while a longer interval can make web browsing faster for your users. If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value. Otherwise, the setting defaults to disabled (the current behavior), meaning that cached URL data does not expire. New/modified pages: **System** > **Integration** > **Cisco CSI** > **Cached URLs Expire** setting Supported platforms: FMC
Event Logging and Analysis	
Cisco Security Packet Analyzer Integration	You can integrate with Cisco Security Packet Analyzer to examine events and display analysis results, or download results for further analysis. New/modified pages: • **System** > **Integration** > **Packet Analyzer** • **Analysis** > **Advanced** > **Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer Supported platforms: FMC
Contextual cross-launch	You can right-click an event in the dashboard or event viewer to look up related information in predefined or custom, public or private URL-based resources. New/modified pages: **Analysis** > **Advanced** > **Contextual Cross-Launch** Supported platforms: FMC

Feature	Description
Unified syslog configuration	**Upgrade impact.** Version 6.3.0 changes and centralizes the way the system logs connection and intrusion events via syslog. Previously, you configured event logging via syslog in multiple places, depending on the event type. You now configure syslog messaging in the access control policy. These configurations affect connection and intrusion event logging for the access control, SSL, prefilter, and intrusion policies, as well as for Security Intelligence. The upgrade does not change your existing settings for connection event logging. However, you may suddenly start receiving intrusion events you did not "expect" via syslog. This is because the intrusion policy now sends syslog events to the destination specified in the access control policy. (Before, you could configure syslog alerting in an intrusion policy to send events to the syslog on the managed device itself rather than to an external host.) For FTD devices, some syslog platform settings now apply to connection and intrusion event messages. For a list, see the *Platform Settings for Firepower Threat Defense* chapter in the Firepower Management Center Configuration Guide. For NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv), messages now use the ISO 8601 timestamp format as specified in RFC 5425. Supported platforms: Any
Fully qualified syslog messages for connection and intrusion events	The format of syslog messages for connection, security intelligence, and intrusion events have the following changes: • Messages from FTD devices now include event type identification numbers. • Fields with empty or unknown values are no longer included, so messages are shorter and important data is less likely to be truncated. • Timestamps now use the ISO 8601 timestamp format as specified in the RFC 5425 syslog format (optional for FTD, required for Classic). Supported platforms: Any
Other syslog improvements for FTD devices	You can send all syslog messages from the same interface (data or management), using the same IP address, using TCP or UDP protocol. Note that secure syslog is supported on data ports only. You can also use the RFC 5424 format for message timestamps. Supported platforms: FTD
Administration and Troubleshooting	

Feature	Description
Export-controlled features for approved customers	Customers whose Smart Accounts are not otherwise eligible to use restricted functionality can purchase term-based licenses, with approval. New/modified pages: **System** > **Licenses** > **Smart Licenses** Supported platforms: FMC, FTD
Specific License Reservation for approved customers	Customers can use Specific License Reservation to deploy Smart Licensing in an air-gapped network. The FMC reserves licenses from your virtual account for a specified duration without accessing the Cisco Smart Software Manager or Smart Software Satellite Server. New/modified pages: **System** > **Licenses** > **Specific Licenses** Supported platforms: FMC, FTD (except ISA 3000)
IPv4 range, subnet, and IPv6 support for SNMP hosts	You can now use IPv4 range, IPv4 subnet, and IPv6 host network objects to specify the SNMP hosts that can access a Firepower Threat Defense device. New/modified pages: **Devices** > **Platform Settings >** create or edit FTD policy **> SNMP > Hosts** tab Supported platforms: FTD
Access control using fully qualified domain names (FQDN)	You can now create fully qualified domain name (FQDN) network objects and use them in access control and prefilter rules. To use FQDN objects, you must also configure DNS server groups and DNS platform settings, so that the system can resolve the domain names. New/modified pages: • **Objects** > **Object Management** > **Network** • **Objects** > **Object Management** > **DNS Server Group** • **Devices** > **Platform Settings >** create or edit FTD policy **> DNS** Supported platforms: FTD
CLI for the FMC	An CLI for the FMC supports a small set of basic commands (change password, show version, reboot/restart, and so on). By default the FMC CLI is disabled, and logging into FMC using SSH accesses the Linux shell. New/modified Classic CLI commands: The **system lockdown-sensor** command has changed to **system lockdown**. This command now works for both devices and FMCs. New/modified pages: **System** > **Configuration** > **Console Configuration** > **Enable CLI Access** check box Supported platforms: FMC, including FMCv

Feature	Description
Copy device configurations	You can copy device configurations and policies from one device to another. New/modified pages: **Devices** > **Device Management >** edit the device **> General** area **> Get/Push Device Configuration** icons. Supported platforms: FMC
Backup/restore FTD device configurations	You can use the FMC web interface to back up configurations for some FTD devices. New/modified pages: **System** > **Tools** > **Backup/Restore** New/modified CLI commands: **restore** Supported platforms: All physical FTD devices, FTDv for VMware
Skip deploying to up-to-date devices when you schedule deploy tasks	**Upgrade impact.** When you schedule a task to deploy configuration changes, you can now opt to **Skip Deployment for up-to-date devices**. This performance-enhancing setting is enabled by default. The upgrade process automatically enables this option on existing scheduled tasks. To continue to force a scheduled deploy to up-to-date devices, you must edit the scheduled task. New/modified pages: **System** > **Tools** > **Scheduling >** add or edit a task **>** choose **Job Type** of **Deploy Policies** Supported platforms: FMC
New health modules	New health modules alert you when: • **Threat Data Updates on Devices**: Threat identification data on managed devices fails to update. • **Realm**: A user is reported to the FMC without being downloaded, or a user logs into a domain that corresponds to a realm not known to the FMC. New/modified pages: • **System > Health > Policy** • **System > Health > Monitor** Supported platforms: FMC
Configurable packet capture size	You can now store up to 10 GB of packet captures. New/modified CLI commands: **file-size**, **show capture** Supported platforms: Firepower 4100/9300
Security and Hardening	

Feature	Description
HTTPS Certificates	The default HTTPS server certificate provided with the system now expires in three years. If your appliance uses a default server certificate that was generated before you upgraded to Version 6.3.0, the server certificate will expire 20 years from when it was first generated. If you are using the default HTTPS server certificate the system now provides the ability to renew it. New/modified pages: **System** > **Configuration** > **HTTPS Certificate** > **Renew HTTPS Certificate** button New/modified Classic CLI commands: **show http-cert-expire-date**, **system renew-http-cert***new_key* Supported platforms: Physical FMCs, 7000/8000 series devices
Improved login security	**Upgrade impact.** Added FMC user configuration settings to improve login security: • **Track Successful Logins**: Track the number of successful logins each FMC account has performed within a specific time period. • **Password Reuse Limit**: Track an FMC user's password history to prevent reuse. • **Max Number of Login Failures** and **Set Time in Minutes to Temporarily Lockout Users**: Limit the number of times in a row an FMC user can enter incorrect web interface login credentials before being temporarily blocked. We also updated the list of supported ciphers and cryptographic algorithms for secure SSH access. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version. New/modified pages: **System** > **Configuration** > **User Configuration** Supported platforms: FMC
Limit SSH login failures on devices	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session. Supported platforms: Any device
Firepower Management Center REST API	

Feature	Description
New REST API services	Added REST API services to support these features: • Site-to-site VPN topology: ftds2svpns, endpoints, ipsecsettings, advancedsettings, ikesettings, ikev1ipsecproposals, ikev1policies, ikev2ipsecproposals, ikev2policies • HA device failover: failoverinterfacemacaddressconfigs, monitoredinterfaces Supported platforms: FMC
Bulk overrides	You can now perform bulk overrides on specific objects. For a full list, see the Cisco Firepower Management Center REST API Quick Start Guide.

Deprecated Features in FMC Version 6.3.0

Table 10:

Feature	Upgrade Impact	Description
EMS extension support for decryption	EMS extension support discontinued until you patch or upgrade.	Version 6.3.0 discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627. In Firepower Management Center deployments, this feature depends on the *device* version. Upgrading the Firepower Management Center to Version 6.3.0 does not discontinue support, as long as the device is running a supported version. However, upgrading the device to Version 6.3.0 does discontinue support. Support is reintroduced in Version 6.3.0.1.
Decryption on passive and inline tap Interfaces	The system stops decrypting traffic in passive deployments.	Version 6.3.0 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. Any inspection of encrypted traffic is necessarily limited.

Feature	Upgrade Impact	Description
Default DNS group FlexConfig objects	You should redo your configurations after upgrade.	Version 6.3.0 deprecates this FlexConfig object for Firepower Threat Defense with FMC: • Default_DNS_Configure And these associated text objects: • defaultDNSNameServerList • defaultDNSParameters These allowed you to configure the Default DNS group, which defines the DNS servers that can be used when resolving fully qualified domain names on the data interfaces. This allowed you to use commands in the CLI, such as **ping**, using host names rather than IP addresses. You can now configure DNS for the data interfaces in the FTD platform settings policy: **Devices** > **Platform Settings >** create or edit FTD policy **>** **DNS**.
Embryonic connection limit and timeout FlexConfig objects	Post-upgrade deployment issues. You should redo your configurations after upgrade.	Version 6.3.0 deprecates these FlexConfig objects for Firepower Threat Defense with FMC: • TCP_Embryonic_Conn_Limit • TCP_Embryonic_Conn_Timeout And these associated text objects: • tcp_conn_misc • tcp_conn_limit • tcp_conn_timeout These allowed you to configure embryonic connection limits and timeouts to protect against SYN Flood Denial of Service (DoS) attacks. You can now configure these features in the FTD service policy: **Policies** > **Access Control** **>** add/edit policy **>** **Advanced** tab > **Threat Defense Service Policy**. **Caution** If you used **set connection** commands to implement connection-related service rules, you should remove the associated objects and implement the features through the FTD service policy. Failure to do so can cause deployment issues.

Feature	Upgrade Impact	Description
Web interface changes	None.	Version 6.3.0 changes these menu options: **Analysis** > **Advanced** > **Whois** is now **Analysis** > **Lookup** > **Whois** **Analysis** > **Advanced** > **Geolocation** is now **Analysis** > **Lookup** > **Geolocation** **Analysis** > **Advanced** > **URL** is now **Analysis** > **Lookup** > **URL** **Analysis** > **Advanced** > **Custom Workflows** is now **Analysis** > **Custom** > **Custom Workflows** **Analysis** > **Advanced** > **Custom Tables** is now **Analysis** > **Custom** > **Custom Tables** **Analysis** > **Hosts** > **Vulnerabilities** is now **Analysis** > **Vulnerabilities** > **Vulnerabilities** **Analysis** > **Hosts** > **Third-Party Vulnerabilities** is now **Analysis** > **Vulnerabilities** > **Third-Party Vulnerabilities**
VMware 5.5 hosting	Upgrade the hosting environment before you upgrade the Firepower software.	Version 6.3.0+ virtual deployments have not been tested on VMware vSphere/VMware ESXi 5.5. This includes FMCv, FTDv, and NGIPSv for VMware.
ASA 5506-X series and ASA 5512-X devices with Firepower software	Upgrade prohibited.	You cannot upgrade to or freshly install Version 6.3.0+ of the Firepower software (both Firepower Threat Defense and ASA FirePOWER) on ASA 5506-X, 5506H-X, 5506W-X, and 5512-X devices.

Features for Firepower Device Manager Deployments

New Features in FDM Version 6.3.0

Feature	Description
High availability configuration.	You can configure two devices as an active/standby high availability pair. A high availability or failover setup joins two devices so that if the primary device fails, the secondary device can take over. This helps you keep your network operational in case of device failure. The devices must be of the same model, with the same number and type of interfaces, and they must run the same software version. You can configure high availability from the **Device** page.

Feature	Description
Support for passive user identity acquisition.	You can configure identity policies to use passive authentication. Passive authentication gathers user identity without prompting the user for username and password. The system obtains the mappings from the identity sources you specify, which can be Cisco Identity Services Engine (ISE)/Cisco Identity Services Engine Passive Identity Connector (ISE PIC), or logins from remote access VPN users. Changes include supporting passive authentication rules in **Policies** > **Identity**, and ISE configuration in **Objects** > **Identity Sources**.
Local user support for remote access VPN and user identity.	You can now create users directly through FDM. You can then use these local user accounts to authenticate connections to a remote access VPN. You can use the local user database as either the primary or fallback authentication source. In addition, you can configure passive authentication rules in the identity policy so that local usernames are reflected in the dashboards and so they are available for traffic matching in policies. We added the **Objects** > **Users** page, and updated the remote access VPN wizard to include a fallback option.
Changed default behavior for VPN traffic handling in the access control policy (**sysopt connection permit-vpn**).	The default behavior for how VPN traffic is handled by the access control policy has changed. Starting in 6.3, the default is that all VPN traffic will be processed by the access control policy. This allows you to apply advanced inspections, including URL filtering, intrusion protection, and file policies, to VPN traffic. You must configure access control rules to allow VPN traffic. Alternatively, you can use FlexConfig to configure the **sysopt connection permit-vpn** command, which tells the system to bypass the access control policy (and any advanced inspections) for VPN-terminated traffic
Support for FQDN-based network objects and data interface support for DNS lookup.	You can now create network objects (and groups) that specify a host by fully-qualified domain name (FQDN) rather than a static IP address. The system looks up the FQDN-to-IP address mapping periodically for any FQDN object that is used in an access control rule. You can use these objects in access control rules only. We added the DNS Group object to the objects page, changed the **System Settings** > **DNS Server** page to allow group assignment to data interfaces, and the access control rule to allow for FQDN network object selection. In addition, the DNS configuration for the management interface now uses DNS groups instead of a set list of DNS server addresses.

Feature	Description
Support for TCP syslog and the ability to send diagnostic syslog messages through the management interface.	In previous releases, diagnostic syslog messages (as opposed to connection and intrusion messages) always used a data interface. You can now configure syslog so that all messages use the management interface. The ultimate source IP address depends on whether you use the data interfaces as the gateway for the management interface, in which case the IP address will be the one from the data interface. You can also configure syslog to use TCP instead of UDP as the protocol. We made changes to the Add/Edit dialog box for syslog servers from **Objects** > **Syslog Servers**.
External Authentication and Authorization using RADIUS for FDM Users.	You can use an external RADIUS server to authenticate and authorize users logging into FDM. You can give external users administrative, read-write, or read-only access. FDM can support 5 simultaneous logins; the sixth session automatically logs off the oldest session. You can forcefully end a FDM user session if necessary. We added RADIUS server and RADIUS server group objects to the **Objects** > **Identity Sources** page for configuring the objects. We added the **AAA Configuration** tab to **Device** > **System Settings** > **Management Access**, for enabling use of the server groups. In addition, the **Monitoring** > **Sessions** page lists the active users and lets an administrative user end a session.
Pending changes view and deployment improvements.	The deployment window has changed to provide a clearer view of the pending changes that will be deployed. In addition, you now have the option to discard changes, copy changes to the clipboard, and download changes in a YAML formatted file. You can also name deployment jobs so they are easier to find in the audit log.
Audit Log.	You can view an audit log that records events such as deployments, system tasks, configuration changes, and administrative user login and logout. We added the **Device** > **Device Administration** > **Audit Log** page.
Ability to export the configuration.	You can download a copy of the device configuration for record keeping purposes. However, you cannot import this configuration into a device. This feature is not a replacement for backup/restore. We added the **Device** > **Device Administration** > **Download Configuration** page.
Improvements to URL filtering for unknown URLs.	If you perform category-based URL filtering in access control rules, users might access URLs whose category and reputation are not defined in the URL database. Previously, you needed to manually enable the option to look up the category and reputation for these URLs from Cisco Collective Security Intelligence (CSI). Now, that option is enabled by default. In addition, you can now set the time-to-live (TTL) for the lookup results, so that the system can refresh the category/reputation for each unknown URL. We updated the **Device** > **System Settings** > **URL Filtering Preferences** page.

Feature	Description
Security Intelligence logging is now enabled by default.	The Security Intelligence policy was introduced in 6.2.3, with logging disabled by default. Starting with 6.3.0, logging is enabled by default. If you upgrade from 6.2.3, your logging settings are preserved, either enabled or disabled. Enable logging if you want to see the results of policy enforcement.
Passive mode interfaces	You can configure an interface in passive mode. When acting passively, the interface simply monitors the traffic from the source ports in a monitoring session configured on the switch itself (for hardware devices) or on the promiscuous VLAN (for FTDv). You can use passive mode to evaluate how the FTDv device would behave if you deployed it as an active firewall. You can also use passive interfaces in a production network if you need IDS (intrusion detection system) services, where you want to know about threats, but you do not want the device to actively prevent the threats. You can select passive mode when editing physical interfaces and when you create security zones.
Smart CLI enhancements for OSPF, and support for BGP.	The Smart CLI OSPF configuration has been enhanced, including new Smart CLI object types for standard and extended ACLs, route maps, AS Path objects, IPv4 and IPv6 prefix lists, policy lists, and standard and expanded community lists. In addition, you can now use Smart CLI to configure BGP routing. You can find these features on the **Device** > **Advanced Configuration** page.
Enhancements for ISA 3000 devices.	You can now configure the following features for the ISA 3000: alarms, hardware bypass, and backup and restore using the SD card. You use FlexConfig to configure the alarms and hardware bypass. For the SD card, we updated the backup/restore pages in FDM.
Support for ASA 5506-X, 5506W-X, 5506H-X, and 5512-X removed starting with FTD 6.3.	You cannot install FTD 6.3 or subsequent releases on the ASA 5506-X, 5506W-X, 5506H-X, and 5512-X. The final supported FTD release for these platforms is 6.2.3.
FTD REST API version 2 (v2).	The FTD REST API for software version 6.3 has been incremented to version 2. You must replace v1 in the API URLs with v2. The v2 API includes many new resources that cover all features added in software version 6.3. 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, change the end of the FDM URL to **/#/api-explorer** after logging in.
Web analytics for providing product usage information to Cisco.	You can enable web analytics, which provides anonymous product usage information to Cisco based on page hits. This information can help Cisco determine feature usage patterns and help Cisco improve the product. All usage data is anonymous and no sensitive data is transmitted. Web analytics is enabled by default. We added Web Analytics to the **Device** > **System Settings** > **Cloud Services** page.

Feature	Description
Installing a Vulnerability Database (VDB) update no longer restarts Snort.	When you install a VDB update, the installation itself no longer restarts Snort. However, Snort continues to restart during the next configuration deployment.
Deploying an Intrusion Rules (SRU) database update no longer restarts Snort.	After you install an intrusion rules (SRU) update, you must deploy the configuration to activate the new rules. The deployment of the SRU update no longer causes a Snort restart.

Deprecated Features in FDM Version 6.3.0

Table 11:

Feature	Upgrade Impact	Description
EMS extension support for decryption	EMS extension support discontinued until you patch or upgrade.	Version 6.3.0 discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the **Decrypt-Resign** and **Decrypt-Known Key** SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627. Support is reintroduced in Version 6.3.0.1.

Feature	Upgrade Impact	Description
FlexConfig commands	You should redo your configurations after upgrade.	Version 6.3.0 deprecates the following FlexConfig commands for Firepower Threat Defense with FDM: • **access-list**: You can now create **extended** and **standard** access lists using the Smart CLI Extended Access List or Standard Access List objects. You can then use them on FlexConfig-supported commands that refer to the ACL by object name, such as **match access-list** with an extended ACL for service policy traffic classes. • **as-path**: You can now create Smart CLI AS Path objects and use them in a Smart CLI BGP object to configure an autonomous system path filter. • **community-list**: You can now create Smart CLI Expanded Community List or Standard Community List objects and use them in a Smart CLI BGP object to configure a community list filter. • **dns-group**: You can now configure DNS groups using **Objects** > **DNS Groups**, and assign the groups using **Device** > **System Settings** > **DNS Server**. • **policy-list**: You can now create Smart CLI Policy List objects and use them in a Smart CLI BGP object to configure a policy list. • **prefix-list**: You can now create Smart CLI IPv4 Prefix List objects and use them in a Smart CLI OSPF or BGP object to configure prefix list filtering for IPv4. • **route-map**: You can now create Smart CLI Route Map objects and use them in a Smart CLI OSPF or BGP object to configure route maps. • **router bgp**: You can now use the Smart CLI templates for BGP.
VMware 5.5 hosting	Upgrade the hosting environment before you upgrade the Firepower software.	Version 6.3.0+ FTDv deployments have not been tested on VMware vSphere/VMware ESXi 5.5.
ASA 5506-X series and ASA 5512-X devices with Firepower Threat Defense	Upgrade prohibited.	You cannot upgrade to or freshly install Firepower Threat Defense Version 6.3.0+ on ASA 5506-X, 5506H-X, 5506W-X, and 5512-X devices.

About Deprecated FlexConfig Commands

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

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

About FlexConfig

Some Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2.0 (FMC deployments) or Version 6.2.3 (FDM deployments), you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

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

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

Intrusion Rules and Keywords

Upgrades can import and auto-enable intrusion rules.

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

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

Supported keywords depend on your Snort version:

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

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

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

How-To Walkthroughs for the FMC

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

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

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

Table 12: Troubleshooting Walkthroughs

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

Sharing Data with Cisco

Web Analytics tracking

In Version 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

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

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

Cisco Success Network

In Version 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support.

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

Cisco Support Diagnostics

In Version 6.5.0+, *Cisco Support Diagnostics* (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

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

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

CHAPTER 4

Upgrade the Software

This chapter provides critical and release-specific information.

- Planning Your Upgrade, on page 35
- Minimum Version to Upgrade, on page 36
- New Upgrade Guidelines for Version 6.3.0, on page 37
- Previously Published Upgrade Guidelines, on page 43
- Unresponsive Upgrades, on page 46
- Traffic Flow and Inspection, on page 46
- Time and Disk Space Tests, on page 54
- Upgrade Instructions, on page 56

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 56.

Table 13: Upgrade Planning Phases

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

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

Minimum Version to Upgrade

You can upgrade directly to Version 6.3.0 as follows. You do not need to be running any specific patch level.

Table 14: Minimum Version to Upgrade to Version 6.3.0

Platform	Minimum Version
Firepower Management Center	6.1.0
Firepower devices with FMC: • Firepower 2100 series • ASA 5500-X series • ISA 3000 • FTDv • Firepower 7000/8000 series • ASA FirePOWER • NGIPSv	6.1.0

Platform	Minimum Version
Firepower devices with FMC: - Firepower 4100/9300	6.2.3 on FXOS 2.3.1.73 or later build (recommended) 6.1.0 on FXOS 2.4.1.214 or later build (required) If you are running Version 6.1.0 and need to upgrade directly to Version 6.3.0, see Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 43. However, if you plan to upgrade "past" 6.3.0, we recommend you use Version 6.2.3 on FXOS 2.3.1 as the intermediate version. From Version 6.2.3, you can upgrade as far as Version 6.6.x.
Firepower devices with FDM	6.2.0
ASA FirePOWER with ASDM	6.2.0

New Upgrade Guidelines for Version 6.3.0

This checklist contains upgrade guidelines that are new or specific to Version 6.3.0.

Table 15: Version 6.3.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Renamed Upgrade and Installation Packages, on page 38	FMC Firepower 7000/8000 series NGIPSv	Any	6.3.0+
	Reimaging to Version 6.3+ Disables LOM on Most Appliances, on page 39	FMC (physical) Firepower 7000/8000 series	Any	6.3.0+
	Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 40	FMC Firepower 7000/8000 series NGIPSv	6.2.3 through 6.2.3.4 6.2.2 through 6.2.2.4 6.2.1 6.2.0 through 6.2.0.6 6.1.0 through 6.1.0.6	6.3.0+
	Reporting Data Removed During FTD/FDM Upgrade, on page 40	FTD with FDM	6.2.0 through 6.2.3.x	6.3.0 only
	RA VPN Default Setting Change Can Block VPN Traffic, on page 40	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	TLS/SSL Hardware Acceleration Enabled on Upgrade, on page 41	Firepower 2100 series Firepower 4100/9300	6.1.0 through 6.2.3.x	6.3.0 only
	Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER, on page 41	FMC ASA FirePOWER with ASDM	6.1.0 through 6.2.3.x	6.3.0 only
	Security Intelligence Enables Application Identification, on page 41	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 42	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 42	Any	6.1.0 through 6.2.3.x	6.3.0+
	Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 43	Firepower 4100/9300	6.1.0.x	6.3.0 only

Renamed Upgrade and Installation Packages

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3+

The naming scheme (that is, the first part of the name) for upgrade, patch, hotfix, and installation packages changed starting with Version 6.3.0, on select platforms.

Note This change causes issues with reimaging older *physical* appliances: DC750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0 or 6.4.0 on one of these appliances, rename the installation package to the "old" name after you download it from the Cisco Support & Download site.

Table 16: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Naming Schemes
FMC	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_3D_Defense_Center_S3
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3

Platform	Naming Schemes
NGIPSv	**New:** Cisco_Firepower_NGIPS_Virtual **Old:** Sourcefire_3D_Device_VMware **Old:** Sourcefire_3D_Device_Virtual64_VMware

Table 17: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	**New:** Cisco_Firepower_Mgmt_Center **Old:** Sourcefire_Defense_Center_M4 **Old:** Sourcefire_Defense_Center_S3
FMCv: VMware	**New:** Cisco_Firepower_Mgmt_Center_Virtual_VMware **Old:** Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	**New:** Cisco_Firepower_Mgmt_Center_Virtual_KVM **Old:** Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 series	**New:** Cisco_Firepower_NGIPS_Appliance **Old:** Sourcefire_3D_Device_S3
NGIPSv	**New:** Cisco_Firepower_NGIPSv_VMware **Old:** Cisco_Firepower_NGIPS_VMware

Reimaging to Version 6.3+ Disables LOM on Most Appliances

Deployments: Physical FMCs, 7000/8000 series devices

Reimaging from: Version 6.0+

Directly to: Version 6.3+

Freshly installing Version 6.3+ now automatically deletes Lights-Out Management (LOM) settings on most appliances, for security reasons. On a few older FMC models, you have the option of retaining LOM settings along with your management network settings.

If you delete network settings during a Version 6.3+ reimage, you *must* make sure you have physical access to the appliance to perform the initial configuration. You cannot use LOM. After you perform the initial configuration, you can reenable LOM and LOM users.

Table 18: Reimage Effect on LOM Settings

Platform	Reimage to Version 6.2.3 or earlier	Reimage to Version 6.3+
MC1600, 2600, 4600 MC1000, 2500, 4500 MC2000, 4000	Never deleted	Always deleted

Platform	Reimage to Version 6.2.3 or earlier	Reimage to Version 6.3+
MC750, 1500, 3500	Deleted if you delete network settings	Deleted if you delete network settings
7000/8000 series	Always deleted	Always deleted

Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv

Deployments: FMC, 7000/8000 series devices, NGIPSv

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

Directly to: Version 6.3.0+

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

Table 19: Patches with Readiness Checks for Version 6.3.0+

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

Reporting Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.x

Directly to: Version 6.3 only

Reporting data for short time periods are removed during the Version 6.3 upgrade. After the upgrade, if you try to query short time ranges on days that fall before the upgrade, the system adjusts your query to match the available data. For example, if you query 1-3 PM for a date, and the system only has 24-hour data, the system reports on the entire day.

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

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

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

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

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

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

TLS/SSL Hardware Acceleration Enabled on Upgrade

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0 only

The upgrade process automatically enables TLS/SSL hardware acceleration (sometimes called *TLS crypto acceleration*) on eligible devices. When it was introduced in Version 6.2.3, this feature was disabled by default on Firepower 4100/9300 chassis, and was not available on Firepower 2100 series devices.

Using TLS/SSL hardware acceleration on a managed device that is not decrypting traffic can affect performance. In Version 6.3.0.x, we recommend you disable this feature on devices that are not decrypting traffic.

To disable, use this CLI command:

```
system support ssl-hw-offload disable
```

Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER

Deployments: Firepower Management Center, ASA FirePOWER (locally managed)

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0-83

Some Firepower Management Centers and locally (ASDM) managed ASA FirePOWER modules experienced upgrade failures with Version 6.3.0, build 83. This issue was limited to a subset of customers who upgraded from Version 5.4.x. For more information, see CSCvn62123 in the Cisco Bug Search Tool.

A new upgrade package is now available. If you downloaded the Version 6.3.0-83 upgrade package, do not use it. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

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

To disable discovery you must:

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

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

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

Directly to: Version 6.3.0+

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

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

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

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

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

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

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

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

Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.1.x on FXOS 2.0.1, 2.1.1, or 2.3.1

Directly to: Version 6.3.0 on FXOS 2.4.1

If your Firepower Management Center is running Version 6.2.3+, we strongly recommend you copy (*push*) Firepower upgrade packages to managed devices before you upgrade. This helps reduce the length of your upgrade maintenance window. For Firepower 4100/9300 with FTD, best practice is to copy before you begin the required companion FXOS upgrade.

Note We recommend that you not upgrade from Version 6.1.0 → 6.3.0. If you are running Version 6.1.0, we recommend upgrading to Version 6.2.3 on FXOS 2.3.1, and proceeding from there. If you do choose to perform this Version 6.1.0 → 6.3.0 upgrade, a push from the FMC before you upgrade FXOS is *required*.

This is because upgrading FXOS to Version 2.4.1 while still running Firepower 6.1.0 causes the device management port to flap, which in turn causes intermittent communication problems between the device and the FMC. Until you upgrade the Firepower software, you may continue to experience management port flaps. You may see 'sftunnel daemon exited' alarms, and any task that involves sustained communications—such as pushing a large upgrade package—may fail.

To upgrade Firepower 4100/9300 with FTD, always follow this sequence:

1. Upgrade the FMC to the target version.
2. Obtain the device upgrade package from the Cisco Support & Download site and upload it to the FMC.
3. Use the FMC to push the upgrade package to the device.
4. After the push completes, upgrade FXOS to the target version.
5. Immediately, use the FMC to upgrade the Firepower software on the device.

Previously Published Upgrade Guidelines

This checklist contains older upgrade guidelines.

Table 20: Version 6.3.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Can Unregister FTD/FDM from CSSM, on page 44	FTD with FDM	6.2.0 through 6.2.2.x	6.2.3 through 6.4.0

✓	Guideline	Platforms	Upgrading From	Directly To
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 44	FTD clusters	6.1.0.x	6.2.3 through 6.4.0
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 44	FTD with FDM	6.2.0 only	6.2.2 through 6.4.0
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 45	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 45	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

Upgrade Can Unregister FTD/FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2 through 6.2.2.x

Directly to: Version 6.2.3 through 6.4.0

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Step 1 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 2 If the device is not registered, click **Register Device**.

Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Version 6.2.3 through 6.4.0

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to `0`) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0

Deployments: FTD with FDM, running on a lower-memory ASA 5500-X series device

Upgrading from: Version 6.2.0

Directly to: Version 6.2.2 through 6.4.0

If you are upgrading from Version 6.2.0, the upgrade may fail with an error of: `Uploaded file is not a valid system upgrade file`. This can occur even if you are using the correct file.

If this happens, you can try the following workarounds:

- Try again.
- Use the CLI to upgrade.
- Upgrade to 6.2.0.1 first.

Access Control Can Get Latency-Based Performance Settings from SRUs

Deployments: FMC

Upgrading from: 6.1.x

Directly to: 6.2.0+

New access control policies in Version 6.2.0+ *by default* get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2.0+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- Default: The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- Custom: The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

'Snort Fail Open' Replaces 'Failsafe' on FTD

Deployments: FTD with FMC

Upgrading from: Version 6.1.x

Directly to: Version 6.2+

In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

Table 21: Migrating Failsafe to Snort Fail Open

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Disabled (default behavior)	**Busy**: Disabled **Down**: Enabled	New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.
Enabled	**Busy**: Enabled **Down**: Enabled	New and existing connections pass without inspection when the Snort process is busy or down.

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

Unresponsive Upgrades

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

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

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

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

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

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

Table 22: Traffic Behavior: FXOS Upgrades

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

Software Upgrades for Standalone Devices

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

Table 23: Traffic Behavior: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (6.1+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (6.1+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices.

- FTD with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

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

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

Note Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see the upgrade path information in the planning chapter of the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Software Uninstall (Patches)

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

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

- FTD with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

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

Table 24: Traffic Behavior: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower Threat Defense Upgrade Behavior: Other Devices

Software Upgrades for Standalone Devices

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

Table 25: Traffic Behavior: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (Firepower 2100 series, 6.3+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (Firepower 2100 series, 6.3+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled** (Firepower 2100 series, 6.3+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability devices.

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

Software Uninstall (Patches)

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

- FTD with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.
- FTD with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

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

Table 26: Traffic Behavior: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Firepower 7000/8000 Series Upgrade Behavior

The following sections describe device and traffic behavior when you upgrade Firepower 7000/8000 series devices.

Standalone 7000/8000 Series: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

Table 27: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, hardware bypass enabled (**Bypass Mode: Bypass**)	Passed without inspection, although traffic is interrupted briefly at two points: • At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces.
Inline, no hardware bypass module,or hardware bypass disabled (**Bypass Mode: Non-Bypass**)	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

7000/8000 Series High Availability Pairs: Firepower Software Upgrade

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

Which peer upgrades first depends on your deployment:

- Routed or switched: Standby 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.
- Access control only: Active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

8000 Series Stacks: Firepower Software Upgrade

In an 8000 series stack, devices upgrade simultaneously. Until the primary device completes its upgrade and the stack resumes operation, traffic is affected as if the stack were a standalone device. Until all devices complete the upgrade, the stack operates in a limited, mixed-version state.

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

Table 28: Traffic Behavior During Deployment: 7000/8000 Series

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
Routed, switched	Dropped

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 29: 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 30: 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 31: Traffic Behavior During NGIPSv Deployment

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

Time and Disk Space Tests

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

Time Tests

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

⚠

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

Table 32: Time Test Conditions for Software Upgrades

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

Disk Space Tests

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

We also report the space needed on the FMC (in /var) for the device upgrade package. If you are using FDM, ignore those values.

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

Table 33: Checking Disk Space

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

Version 6.3.0 Time and Disk Space

Table 34: Version 6.3.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	12.7 GB	29 MB	—	47 min
FMCv: VMware	12.7 GB	29 MB	—	29 min
Firepower 2100 series	13 MB	8.8 GB	930 MB	20 min
Firepower 4100/9300	10 MB	7.6 GB	930 MB	6 min
ASA 5500-X series with FTD	7.9 GB	100 KB	1.1 GB	25 min
FTDv: VMware	7.3 GB	100 KB	1.1 GB	12 min
Firepower 7000/8000 series	7.0 GB	19 MB	920 MB	32 min
ASA FirePOWER	11.3 GB	22 MB	1.2 GB	63 min
NGIPSv	5.7 GB	19 MB	810 MB	16 min

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 35: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0

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, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image.

CHAPTER 5

Install the Software

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

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

- Installation Checklist and Guidelines, on page 59
- Unregistering Smart Licenses, on page 61
- Installation Instructions, on page 62

Installation Checklist and Guidelines

Reimaging returns most settings to factory defaults, including the system password. This checklist highlights actions that can prevent common reimage issues. However, this checklist is *not* comprehensive. See the appropriate installation guide for full instructions: Installation Instructions, on page 62.

Table 36:

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

✓	Action/Check
	Perform backups. Back up before reimaging, when supported. Note that if you are reimaging so that you don't have to upgrade, due to version restrictions you cannot use a backup to import your old configurations. You must recreate your configurations manually. **Caution** We *strongly* recommend you back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance. And especially because backup files are unencrypted, do *not* allow unauthorized access. If backup files are modified, the restore process will fail. Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.
	Determine if you must remove devices from FMC management. If you plan to manually configure the reimaged appliance, remove devices from remote management before you reimage: • If you are reimaging the FMC, remove all its devices from management. • If you are reimaging a single device or switching from remote to local management, remove that one device. If you plan to restore from backup after reimaging, you do not need to remove devices from remote management.
	Address licensing concerns. Before you reimage *any* appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager (CSSM) to avoid accruing orphan entitlements, which can prevent you from reregistering. Or, you may need to contact Sales for new licenses. For more information, see: • The configuration guide for your product. • Unregistering Smart Licenses, on page 61 • Cisco Firepower System Feature Licenses Guide • Frequently Asked Questions (FAQ) about Firepower Licensing

Reimaging Firepower 2100 Series Devices to Earlier Major Versions

We recommend that you perform complete reimages of Firepower2100 series devices. If you use the erase configuration method, FXOS may not revert along with the Firepower Threat Defense software. This can cause failures, especially in high availability deployments.

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

Reimaging Version 5.x Hardware to Version 6.3.0+

The renamed installation packages in Version 6.3+ cause issues with reimaging older *physical* appliances: FMC 750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0, rename the installation package to the "old" name after you download it; see Renamed Upgrade and Installation Packages, on page 38.

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

Unregistering Smart Licenses

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

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

Unregistering removes an appliance from your virtual account 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.
- 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 37: Firepower Management Center Installation Instructions

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

Table 38: Firepower Threat Defense Installation Instructions

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

Table 39: Firepower 7000/8000 Series, NGIPSv, and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
Firepower 7000 series	Cisco Firepower 7000 Series Getting Started Guide: *Restoring a Device to Factory Defaults*

NGIPS Platform	Guide
Firepower 8000 series	Cisco Firepower 8000 Series Getting Started Guide: *Restoring a Device to Factory Defaults*
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 6

Documentation

For Firepower documentation, see:

- New and Updated Documentation, on page 65
- Documentation Roadmaps, on page 67

New and Updated Documentation

The following documentation was updated or is newly available for this release. For links to other documentation, see the Documentation Roadmaps, on page 67.

Firepower Configuration Guides and Online Help

- Firepower Management Center Configuration Guide, Version 6.3 and online help
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.3.0 and online help
- Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.3 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, 2.4(1)
- Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.4(1)
- Cisco Firepower 4100/9300 FXOS Command Reference
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)

Upgrade Guides

- Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
- Cisco ASA Upgrade Guide

Hardware Installation Guides

- Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide ***NEW***
- Cisco Firepower 2100 Series Hardware Installation Guide

Getting Started Guides

- Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide ***NEW***
- Cisco Firepower Management Center Virtual Getting Started Guide ***NEW***
- Cisco ASA 5508-X and 5516-X Getting Started Guide
- Cisco ASA 5508-X and 5516-X Getting Started Guide
- Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Device Manager Quick Start Guide
- Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
- Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide

API and Integration Guides

- Firepower Management Center REST API Quick Start Guide, Version 6.3.0
- Firepower System Event Streamer Integration Guide, Version 6.3.0
- Firepower System Database Access Guide v6.3

Compatibility Guides

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

Licensing and Open Source

- Cisco Firepower System Feature Licenses
- Frequently Asked Questions (FAQ) about Firepower Licensing
- Open Source Used in Firepower Version 6.3.0

Troubleshooting and Configuration Examples

- Cisco Firepower Threat Defense Syslog Messages
- How to Manage a Device with the Firepower Management Center ***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 7

Resolved Issues

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

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

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

- Resolved Issues in New Builds, on page 69
- Version 6.3.0 Resolved Issues, on page 70

Resolved Issues in New Builds

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

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

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

Table 40: Version 6.3.0 New Builds

New Build	Released	Packages	Platforms	Resolves
85	2019-01-22	Upgrade Reimage	Firepower 4100/9300	CSCvo02577: Buffer exhaustion with SSL HW decryption If you already installed or upgraded Firepower Threat Defense to Version 6.3.0-83 on a Firepower 4100/9300 device, apply Hotfix B.

New Build	Released	Packages	Platforms	Resolves
84	2018-12-18	Upgrade	FMC/FMCv ASA FirePOWER	CSCvn62123: Some FMCs and locally (ASDM) managed ASA FirePOWER modules experienced upgrade failures with Version 6.3.0-83. This issue was limited to a subset of customers who upgraded from Version 5.4.x. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

Version 6.3.0 Resolved Issues

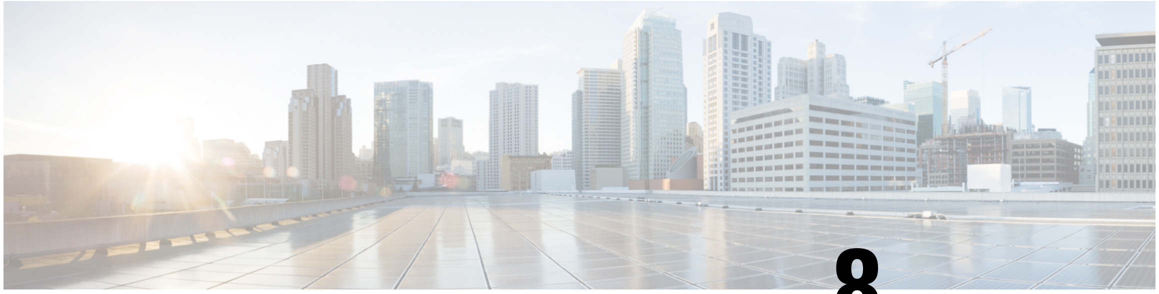
Bug ID	Headline
CSCuy27743	VDB install during firstboot fails because of MySQL dropping out
CSCvb15074	FMC health notifications for interfaces removed or added out-of-band get stuck
CSCvb38753	client hello is getting modified with dnd if application is configured in ssl rule
CSCvb73266	Deploying to devices when upgrade is in failed state causes many problems
CSCvc94589	Evaluation of sfims for OpenSSL Jan 2017
CSCvc99840	Managed device identities out of sync with Firepower Management Center
CSCvd09003	Checking for conflicts in variable sets doesn't work on network groups
CSCvd66558	Inspection engine (Snort) perfomance statistics shows 0 drops, even if there are non-zero drops
CSCvd83685	Obsolete Default SSH Configurations in Firepower Mangement Console
CSCve03169	(1 of 2) ADI process unresponsive during shutdown if bad Realm configuration for LDAP join
CSCve13357	Search filter not working appropriately with Network object groups.
CSCve13816	MEMCACHED software needs to be upgraded to address several security vulnerabilities
CSCve50642	File download from file events fail with "The devices that captured file xxx are not available"
CSCve64511	#sql-*.ibd temporary tables can cause upgrade to fail on 410_check_disk_space
CSCve87925	FMC: Inconsistent interfaces under OSPF interfaces list
CSCvf46888	DNS/URL Security Intelligence blacklisting may not work as expected
CSCvf57596	After policy deploy has failed, ActionQueueScrape process did not exit
CSCvf80217	Rest API explorer does not display device id under "/deployment/deployabledevices"

Bug ID	Headline
CSCvf81997	QP backplane went down after repeating cluster bundle/de-bundle
CSCvf88111	Pigtail should self terminate if not manually terminated.
CSCvf90086	Deployment failure when sub-interface is configured after deleting physical int
CSCvf97412	.REL.tar upgrade file causes System > Updates page in GUI to be slow / unresponsive
CSCvf98187	FDM : Cannot use ";" in the pre-shared-key for Site to Site tunnel
CSCvg10718	Correlation Policy With Traffic Profiles Doesn't Work
CSCvg17746	FXOS CLI and FTD CLI showing different version after upgrade from 6.2.1-341 -> 6.2.3-10587
CSCvg38760	Exporting on Series 3 devices results in Error
CSCvg48641	Missing warning message when AD realm is configured as LDAP realm,
CSCvg50013	Repeated clam update tasks created in AQ, both success and failure status for the same transaction.
CSCvg62301	During device registration, policy discovery can fail, causing the device to unregister
CSCvg74236	Syslog messages for SI events are not sent if syslog alerting for connection events is configured
CSCvg80052	"Tracing enabled by Lina" log optimization
CSCvg82265	AMP server public key is replaced after upgrade
CSCvg85671	Host profile qualification using text host attribute unable to use text as qualifier value
CSCvg90384	High CPU in "top" process when the session is terminated
CSCvg98063	Upgrade/update instructions in the FMC Config Guide are out of date
CSCvh02424	ngfw rules are deployed in incorrect order on sensor
CSCvh12042	Deployment failed because interfaces on device are out of date
CSCvh14518	FMC: Smart license registration may be fail when PID contains hostname
CSCvh23351	HTTP Block Response Page not sending reset packet when 'Block with Reset' is selected in AC Policy
CSCvh59997	ENH: Ability to disable logging for specific Firepower Threat Defense syslog logging message
CSCvh64413	FTD sending "0.0.0.0" NAS-IP-Address attribute when authenticating RA VPN user using Radius Server.
CSCvh77456	Cisco Firepower Threat Defense Software FTP Inspection Denial of Service Vulnerability

Bug ID	Headline
CSCvh87031	Deploy SNMPv3 users in FTD cluster send localized commands
CSCvh95456	Cisco Adaptive Security Appliance Application Layer Protocol Inspection DoS Vulnerabilities
CSCvi03103	BGP ASN cause policy deployment failures.
CSCvi08114	Duplicate pre-filter policy rule getting created at sometime
CSCvi09176	overrides for deleted sensors are left in Network Objects
CSCvi12574	FTD VPN Site-to-Site Deployment fails when IKE preshared password has a "space"
CSCvi12915	Smart license page not displaying licenses
CSCvi21735	Registration incorrectly uses Display Name for hostname lookup
CSCvi28420	DNS SI doesn't send NXDOMAIN for MX and SOA DNS queries
CSCvi56320	The MTU of FTD management interface in BS/QP should be set to 1500 instead of 9000
CSCvi56663	Certain non-ascii characters can prevent downloaded users from getting normal user ids
CSCvi61649	optimize tables marks table as crashed due to .TMM file
CSCvi61815	Logging for External Database Access is not working
CSCvi66676	Object search misbehaving due to search.info corruption
CSCvi74664	Firepower/NGIPS doesn't support adding user/custom snmp configuration
CSCvi80603	Sensor SFDC stuck waiting for snapshots, not receiving any user ip updates
CSCvi81741	"http" is not available for editing in FMC/FTD FlexObject
CSCvi89398	Breaking FTD HA fails with both members of FTD HA Pair in "Standby"
CSCvi92640	FMC cannot establish Remote Storage Server via SSH after restore
CSCvi93701	RA-VPN traffic don't forward to snort
CSCvi93824	Initiating Readiness Check more than once causes stuck notifications
CSCvj08370	FP 2100 Series with FTD Software: LACP mode cannot be change from FMC
CSCvj17008	Negated Original Client IP Search for IPS event with more than one IP excludes events with no XFF.
CSCvj20333	Deployment failed on KP with ERROR: Removal of MIO interfaces is not permitted
CSCvj20963	List of decryptable cipher suites
CSCvj33218	FTD 6.2.2.1: BGP network statements objects are not being pushed properly

Bug ID	Headline
CSCvj36786	FMC won`t show the last IGMP configured interface
CSCvj43939	Invalid Configuration Error when configuring flow-export from FMC GUI
CSCvj46057	FTD HA with virtual macs in the data interfaces while upgrading causes traffic outage
CSCvj56728	ClamAV Integar Overflow Denial of Service Vulnerability
CSCvj67055	Downgrade from IKEv2 to IKEv1 S2S config causes deployment failure
CSCvj76407	Enabling SSL policy slows down deployments by 2 minutes in HA deployment
CSCvj78206	Unable to view all objects if we add network individually
CSCvj80556	A task keep spinning in FMC > Tasks
CSCvj87081	No Connection Events / SFDataCorrelator Exits Unexpectedly during Startup / purge_extra_users
CSCvj89445	Inconsistent deployment status on GUI
CSCvk02250	"show memory binsize" and "show memory top-usage" do not show correct information (Complete fix)
CSCvk03749	Traceback and reload (Process Name: lina)
CSCvk10127	Sensor interfaces reset to no-auto-neg/10m/full-duplex
CSCvk12234	GUI: changing IKEv1 policy switches authentication type to default value
CSCvk12245	GUI: Add button for Network objects doesn't work when you add network group from ACP edit
CSCvk16858	Panic:appAgent_reply_processor_thread-Error: miovif_add_interface_map
CSCvk20497	Network analysis policy showing up as 'Unknown Object '
CSCvk20603	List.pm should not print "warn" message for FTD devices.
CSCvk31035	KVM (FTD): Mapping web server through outside not working consistent with other platforms
CSCvk33923	High disk usage after deleting managed FTD device from FMC
CSCvk34567	Unable to delete local rules with delete_rules.pl script
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
CSCvk38322	Firepower web UI in version 6.2.3 incompatible with Internet Explorer 11 Compatibility View
CSCvk54376	Restore shouln't be permitted until FMC HA is paused
CSCvk58543	FMC receives hm_notifyd exiting health alert

Bug ID	Headline
CSCvk62871	Firepower 2100 FTP Client in passive mode is not able to establish data channel with the Server
CSCvk67239	FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvk69823	FlexConfig objects pushed to device in spite of no changes being made to that on either FMC or FTD
CSCvk72508	QoS Rules do not work with User Defined Application Filters.
CSCvk76274	FMC API Not getting the proper information from Standby Unit in a HA FTD
CSCvm03730	Interface Name field missing on "SLA Monitor Object" menu on FMC
CSCvm07046	Error Message when saving 'Netflow_Delete_Destination' to flexconfig policy
CSCvm10968	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvm39670	Limited charctar in username
CSCvm48220	Fix incorrect check for HA standby in update_snort_attrib_table process
CSCvm59386	Policy Deployment failure because of high disk usage under /ngfw directory
CSCvm81052	local malware detection updates not downloading to FMC due to invalid certificate chain
CSCvn11219	Policy deployment failed with error message "Not a directory"



CHAPTER 8

Known Issues

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

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

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

- Version 6.3.0 Known Issues, on page 75

Version 6.3.0 Known Issues

Table 41: Version 6.3.0 Known Issues

Bug ID	Headline
CSCvk74150	After FDM HA switch the deploy takes longer than 25 minutes on 6.3.0-1376
CSCvm14296	Cisco Firepower Threat Defense Software Multi-Instance Container Escape Vulnerabilities
CSCvm29525	After creating MAX number of LOM users you cannot login remotely using ipmitool
CSCvm32307	Need option to do packet capture on a Port channel Sub-interface
CSCvm37935	Sometimes rule evaluation is aborted on virtual devices due to lower default PPM threshold value
CSCvn07587	Network IPv6 range doesn't deploy correctly to lina
CSCvn12381	4140 Multi-Instance Not Load-Balancing Correctly with 4 Instances
CSCvn19074	MSP -Access Control Rule to Block with Reset for CIP Write application is not blocking

Bug ID	Headline
CSCvn19289	Multiple Vulnerabilities in curl
CSCvn32308	Restoring self backup on secondary requires license re-registrations
CSCvn44222	6.3.0-79: HA upgrade/deployment fails from from missing RAVPN diskfiles on secondary
CSCvn46121	Security Intelligence IP monitor Events are not sent to syslog if default action logs to syslog
CSCvn52181	FMC4500 : Noticed failures related to IPv6 configuration and NTP on console during baseline
CSCvn53145	Policy deploy throws "Variable set has invalid execulded values"
CSCvn67630	Govt UCAPL - Maximum Login Sessions through CLI - test case fails on 6.4.0-1088
CSCvn81898	Device name doesn't exist in a syslog message if syslog alerting for connection events is configured
CSCvo06696	FTD may drop conns through GRE tunnels if firewall receives GRE packet before inner packet
CSCvo15627	Maxfailedlogin for non ucapl user's set to 5 in ucapl mode
CSCvo17612	Return error messages when failing to retrieve objects from database
CSCvo19666	28 Core instance is achieving 20% lower performance than expected
CSCvo31831	Deleting a base policy does not delete the EOs of child policies
CSCvo37273	Adding a validation check in FMC UI to validate the object network configured in static route
CSCvo48771	FMC should check for configuration line length prior to deployment
CSCvo49295	RabbitMQ constantly fails to start with error "case_clause,undefined"
CSCvo49344	RabbitMQ malfunctions and does not recover after SFRemediateD is killed
CSCvo74233	FTD 6.3.0 traceback seen with tftp traffic
CSCvo77796	Slow deployment due to slower IntrusionPolicy step in global snapshot population
CSCvo81219	FP 2100: Reset should be direction aware similar to other platforms
CSCvo87456	Unable to mount SMBv1 share in 6.3.0
CSCvo90413	FTD-REST-API: HTML returned when wrong version passed in URL
CSCvp00236	Upgrading FMC to 6.3.0 fails with error UNABLE TO LOAD stricts.pm and FlyLoader.pm
CSCvp01515	ASA SFR: preprocessors won't be enabled, if enable dependency rules

Bug ID	Headline
CSCvp01542	FMC 6.3 Multitenancy/Domain LDAPS User/Group Download Failure Due to Certificate Location
CSCvp09972	connection event page is not displaying table on UI - max rows user preference is empty
CSCvp11760	Search-Index update fails due to missing Activity Event publish
CSCvp20985	Internet Download Manager detector doesn't match all flows
CSCvp24480	fmc-ha uip snapshot processing stuck in a loop.
CSCvp25581	in FMC-HA user_group_map entries are wiped out in split-brain
CSCvp25782	EventHandler core while pruning metadata cache
CSCvp26548	FDM upgrade fails due to objects validation failure
CSCvp30447	Syslog alerts are not sent to server when Global Rule Thresholding is disabled on Intrusion Policy
CSCvp45786	Not able to upload the STIX or Flat File Manually under Threat Intelligence Director
CSCvp55941	FILE RESUME BLOCK being randomly thrown causing access issues on files from SMB share.
CSCvp95663	InlineResult for IPS event missing metadata "Would have blocked"
CSCvq53902	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq65542	Disable asp load-balance per-packet functionality from fp2100 until all bugs fixed
CSCvq89794	FDM - user downloads not working with LDAPS
CSCvq93768	Lodash lodash Object.prototype Denial of Service Vulnerability
CSCvq93769	Bootstrap collapse Plugin Data-Parent Attribute Cross-Site Scripting V
CSCvq93770	Bootstrap tooltip Plugin Data-Container Property Cross-Site Scripting
CSCvq93771	Bootstrap scrollspy Data-Target Property Cross-Site Scripting Vulnerab
CSCvr06515	Access-control-config hit counter not incrementing
CSCvr33428	FMC generates Connection Events from a SYN flood attack
CSCvr52077	Variable set is not validated at deploy if it is not a part of AC rule
CSCvr72665	FMC upgrading to 6.3/6.4 shouldn't remove existing deprecated flexconfig
CSCvs33392	Known Key SSL decryption and connections can fail when servers are using unsupported TLS options
CSCvs55937	Deployment fails for FDM due to neo4j error

Bug ID	Headline
CSCvt00140	Series 3 sensors fail system restore to 6.3 and 6.4
CSCvt49334	On the 4120 sensor, the task delete is not removing the "task_xx" files from the cron.d directory
CSCvt55927	Unable to break HA in 6.4.0.9-34 FDM
CSCvt86650	Terracotta Quartz Scheduler initDocumentParser XML External Entity Vul
CSCvt86666	Apache Commons Compress ZipArchiveInputStream Denial of Service Vulner
CSCvt87127	Memcached lru Commands NULL Pointer Dereference Vulnerablity
CSCvt87141	GNU Wget set_file_metadata Information Disclosure Vulnerability
CSCvu69541	Query FMC using Ext. DB & unable to extract the 'url_category' from connection_log table as expected
CSCvu86734	FTD Backup and Restore does not restore the hostname of the device locally
CSCvu91792	SNMP IfDiscards OIDs for Internal-Data 0/0 and 0/1 wrong Values
CSCvv03258	FTD/LINA traceback and reload on process name lina
CSCvv54860	backup file can be extremely large when rabbitmq queue backed up

CHAPTER 9

For Assistance

- Online Resources, on page 79
- Contact Cisco, on page 79

Online Resources

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

- 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