

Firepower Release Notes, Version 6.3.0

First Published: 2018-12-03

Last Modified: 2019-01-23

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

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

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

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

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

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

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

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

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

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

© 2018–2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Welcome to Version 6.3.0** 1

About the Release Notes 1

Release Dates 1

CHAPTER 2 **Compatibility** 3

Supported Firepower Management Centers 3

Supported Devices by Manager 3

FMC Deployments 4

FDM Deployments 5

ASDM Deployments 5

Manager-Device Version Compatibility 6

Integrated Product Compatibility 7

Web Browser Compatibility 7

Screen Resolution Requirements 8

CHAPTER 3 **New Features and Functionality** 11

New Features in FMC/Firepower Version 6.3.0 11

New Features in Firepower Device Manager/FTD Version 6.3.0 17

CHAPTER 4 **Upgrade to Version 6.3.0** 23

Upgrade Warnings for All Releases 23

Appliance Access During Upgrade 23

Unresponsive Upgrades 23

Cisco Smart Licensing: Check Status After Upgrade 23

Upgrade Warnings for Version 6.3.0 24

Upgrade Warnings from Intermediate Versions 24

Renamed Upgrade and Installation Packages 24
Preinstallation Hotfix for MC1000, 2500, and 4500 (Required) 25
Push Firepower Package Before FXOS Upgrade on Firepower 4100/9300 (Required) 26
Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER May Fail 27
Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv 27
Updated Security for Appliance Access 28
Firepower Management Center Menu Changes 28
SSL Hardware Acceleration Enabled on Upgrade 28
EMS Extension Support for SSL Decryption Disabled on Upgrade 29
Security Intelligence Enables Application Identification 29
Invalid Intrusion Variable Sets Can Cause Deploy Failure 29
RA VPN Default Setting Change Can Block VPN Traffic 30
Timeouts for the URL Filtering Cache Can Change 30
Syslog Behavior Changes for Connection and Intrusion Events 31
Reporting Data Removed During FTD/FDM Upgrade 31
EOS: Decryption on Passive and Inline Tap Interfaces 31
EOS: VMware vSphere/VMware ESXi 5.5 32
EOS: Firepower on ASA 5512-X and ASA 5506-X Series 32
Blacklisted FlexConfig Commands for FTD 32
Version 6.3.0 Deprecated FlexConfig Objects 33
Version 6.3.0 Blacklisted CLI Commands 33
Version Requirements to Upgrade 34
Time Tests and Disk Space Requirements 34
About Time Tests 35
About Disk Space Requirements 35
Version 6.3.0 Time and Disk Space 36
Traffic Flow, Inspection, and Device Behavior During Upgrade 36
FTD Upgrade Behavior: Firepower 4100/9300 Chassis 36
FTD Upgrade Behavior: Other Devices 39
Firepower 7000/8000 Series Upgrade Behavior 40
ASA FirePOWER Upgrade Behavior 42
NGIPSv Upgrade Behavior 42
Upgrade Instructions 43
Upgrade Packages 43

CHAPTER 5 **Freshly Install Version 6.3.0** 45

Deciding to Freshly Install 45

Guidelines and Limitations for Fresh Installs 46

Unregistering Smart Licenses 47

Unregister a Firepower Management Center 48

Unregister an FTD Device Using FDM 48

Installation Instructions 49

CHAPTER 6 **Documentation** 51

Updated Documentation 51

Documentation Roadmaps 53

CHAPTER 7 **Resolved Issues** 55

Searching for Resolved Issues 55

Resolved Issues in New Builds 55

Version 6.3.0 Resolved Issues 56

CHAPTER 8 **Known Issues** 61

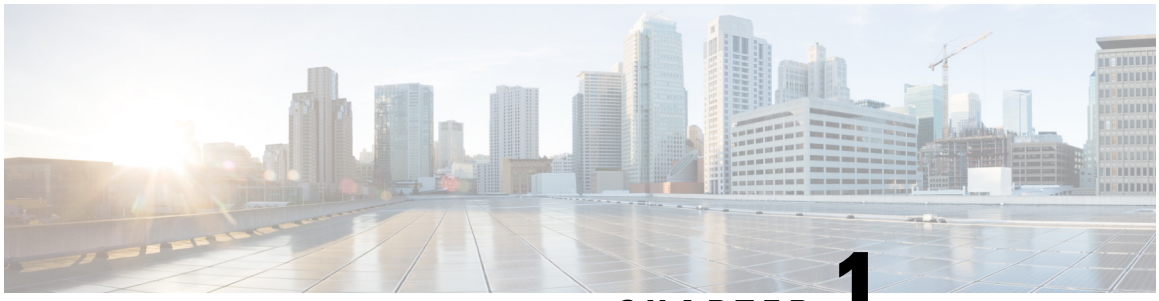
Searching for Known Issues 61

Version 6.3.0 Known Issues 61

CHAPTER 9 **For Assistance** 63

Online Resources 63

Contact Cisco 63



CHAPTER 1

Welcome to Version 6.3.0

Thank you for choosing Firepower.

- About the Release Notes, on page 1
- Release Dates, on page 1

About the Release Notes

The release notes provide critical and release-specific information for Version 6.3.0, including upgrade warnings and behavior changes. Read this document even if you are familiar with Firepower releases and have previous experience upgrading Firepower deployments.

The release notes do not contain upgrade or installation instructions. Upgrading or freshly installing (reimaging) a Firepower deployment can be a complex process. Rather than provide instructions here, the release notes point you to the appropriate resources.

For links to upgrade and installation instructions, see:

- Upgrade Instructions, on page 43
- Installation Instructions, on page 49

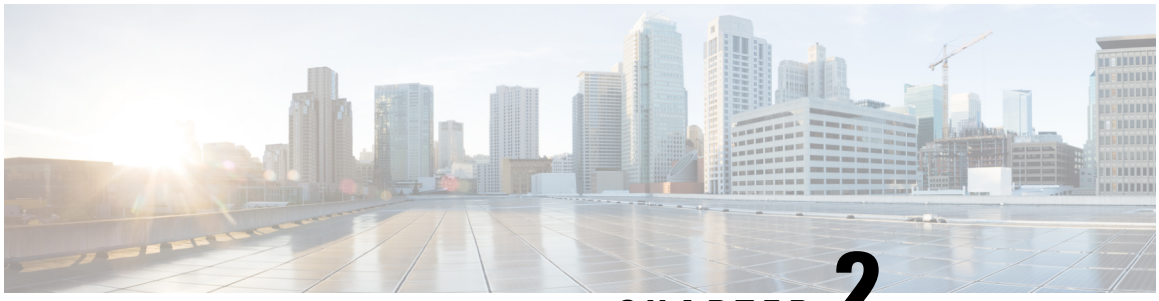
Release Dates

Sometimes Cisco releases updated builds. Only the latest build for each platform is available on the Cisco Support & Download site. You should always 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 55.

Table 1: Dates for Version 6.3.0

Build	Date	Platforms: Upgrade	Platforms: Fresh Install
85	2019-01-22	Firepower 4100/9300	Firepower 4100/9300
84	2018-12-18	FMC/FMCv ASA FirePOWER	—

Build	Date	Platforms: Upgrade	Platforms: Fresh Install
83	2018-12-03	All FTD devices except Firepower 4100/9300 Firepower 7000/8000 NGIPSv	FMC/FMCv All devices except Firepower 4100/9300



CHAPTER 2

Compatibility

These topics provide compatibility information for this Firepower version.

- Supported Firepower Management Centers, on page 3
- Supported Devices by Manager, on page 3
- Manager-Device Version Compatibility, on page 6
- Integrated Product Compatibility, on page 7
- Web Browser Compatibility, on page 7
- Screen Resolution Requirements, on page 8

Supported Firepower Management Centers

Firepower Management Center:

- MC 1000, 2500, 4500
- MC 2000, 4000
- MC 750, 1500, 3500

Firepower Management Center Virtual:

- VMware vSphere/VMware ESXi 6.0 and 6.5
- Kernel-based virtual machine (KVM)
- Amazon Web Services (AWS) VPC/EC2

Supported Devices by Manager

You can manage a Firepower device *either* locally (FDM/ASDM) or with a Firepower Management Center. You can use only one management method for a device at a time.

FMC Deployments

Firepower Threat Defense Devices with Firepower Management Center

Firepower Threat Defense Platform	Operating System
Firepower 2100 series: • Firepower 2110, 2120, 2130, 2140	FXOS 2.4.1.216 Automatic upgrade—bundled.
Firepower 4100/9300 chassis: • Firepower 4110, 4120, 4140, 4150 • Firepower 9300 with SM-24, SM-36, SM-44 modules	FXOS 2.4.1.214 Separate upgrade. Upgrade FXOS first.
ISA 3000 ASA 5500-X series: • ASA 5508-X, 5516-X • ASA 5515-X, 5525-X, 5545-X, 5555-X	ASA 9.10(1.3) Automatic upgrade—bundled.
Firepower Threat Defense Virtual: • VMware vSphere/VMware ESXi 6.0 and 6.5 • Kernel-based virtual machine (KVM) • Amazon Web Services (AWS) EC2/VPC • Microsoft Azure Standard D3 and D3_v2	See the documentation for your virtual hosting environment.

NGIPS Devices with Firepower Management Center

NGIPS Platform	Operating System
Firepower 7000/8000 series: • 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	Firepower. Automatic upgrade—bundled.

NGIPS Platform	Operating System
ASA with FirePOWER Services: • ISA 3000 • ASA 5508-X, 5516-X • ASA 5515-X, 5525-X, 5545-X, 5555-X • ASA 5585-X-SSP-10, -20, -40, -60	Any of: • ASA 9.5(2), 9.5(3) • ASA 9.6(x) through 9.10(x) Separate upgrade. See the Cisco ASA Upgrade Guide for order of operations.
NGIPSv: • VMware vSphere/VMware ESXi 6.0 and 6.5	See the documentation for your virtual hosting environment.

FDM Deployments

Firepower Threat Defense Devices with Firepower Device Manager

Firepower Threat Defense Platform	Operating System
Firepower 2100 series: • Firepower 2110, 2120, 2130, 2140	FXOS 2.4.1.216 Automatic upgrade—bundled.
ISA 3000 ASA 5500-X series: • ASA 5508-X, 5516-X • ASA 5515-X, 5525-X, 5545-X, 5555-X	ASA 9.10(1.3) Automatic upgrade—bundled.
Firepower Threat Defense Virtual: • VMware vSphere/VMware ESXi 6.0 and 6.5 • Kernel-based virtual machine (KVM)	See the documentation for your virtual hosting environment.

ASDM Deployments

Use ASDM 7.10.1 to manage Version 6.3.0 of the ASA FirePOWER module.

ASA FirePOWER with ASDM

ASA with FirePOWER Services Platform	Operating System
ISA 3000 ASA 5500-X series: • ASA 5508-X, 5516-X • ASA 5515-X, 5525-X, 5545-X, 5555-X • ASA 5585-X-SSP-10, -20, -40, -60	Any of: • ASA 9.5(2), 9.5(3) • ASA 9.6(x) through 9.10(x) Separate upgrade. See the Cisco ASA Upgrade Guide for order of operations.

Manager-Device Version Compatibility

This section provides manager-device compatibility for Version 6.3.0.

Firepower Management Center Deployments

We *strongly* recommend the FMC run *at least* the same version as its managed devices. Although you can use a major-version FMC to manage devices running patches to that major version, features and resolved issues often depend on the Firepower version running on the device.

Version	Platform	Capability/Requirement
Version 6.3.0	FMC	Can manage these Firepower devices: • Version 6.1.x • Version 6.2.x • Version 6.3.0
Version 6.3.0	Managed device	Requires this FMC: • Version 6.3.0

Firepower Device Manager Deployments

Firepower Device Manager is built into Firepower Threat Defense. There is no concept of manager-device compatibility in this type of deployment.

Version	Platform	Capability/Requirement
Version 6.3.0	FDM	Can manage one Firepower Threat Defense device.

ASDM Deployments

Version	Platform	Capability/Requirement
Version 7.10(1)	ASDM	Can manage these ASA FirePOWER modules: • Version 5.3.x through Version 6.3.0

Version	Platform	Capability/Requirement
Version 6.3.0	ASA FirePOWER module	Requires this ASDM: • Version 7.10(1)

Integrated Product Compatibility

You can integrate a variety of Cisco products with Firepower.

Table 2: Firepower Version 6.3.0 Compatibility with Integrated Products

Product	Version
Cisco Firepower System User Agent	2.3
Cisco Identity Services Engine: ISE	2.3 2.3 patch 2 2.4
Cisco Identity Services Engine: ISE-PIC	2.2 patch 1 2.4
Cisco Terminal Services (TS) Agent	1.1 1.2
Cisco AMP Threat Grid	2.1.4+
Cisco AnyConnect Secure Mobility Client	4.0+
Cisco Security Packet Analyzer	Any

Web Browser Compatibility

Browsing the Web from a Firepower-Monitored Network

Many browsers use Transport Layer Security (TLS) v1.3 by default. If you are using a Firepower 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*.

Using Firepower Web Interfaces

Firepower web interfaces are tested with various popular browsers. If you encounter issues with a browser that is not listed, we ask that you switch to a tested browser. If you continue to encounter issues, contact Cisco TAC.

Note SSL certificates allow the FMC (and 7000/8000 series devices) to establish an encrypted channel between the appliance and your browser. By default, the system comes with a self-signed HTTPS server certificate. We recommend that you replace it with a certificate signed by a globally known or internally trusted certificate authority (CA). You can generate custom server certificate requests and import custom server certificates on the HTTPS Certificates page; choose **System** > **Configuration**, then click **HTTPS Certificates**. For more information, see the online help or the Firepower Management Center Configuration Guide.

Browsers Tested with Firepower Web Interfaces

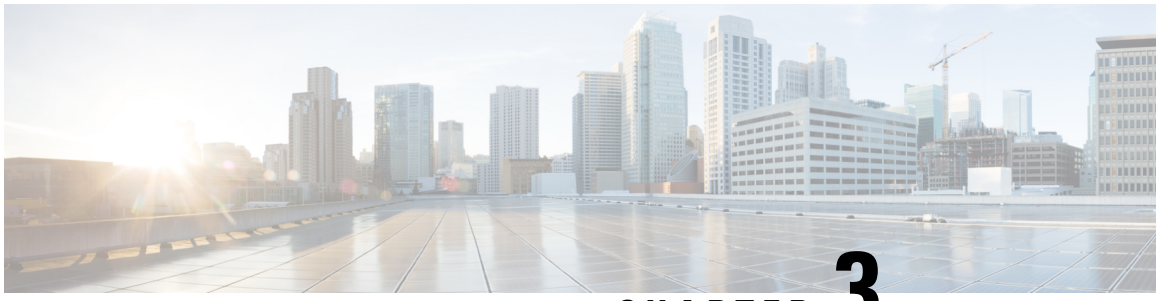
Browser	Required Settings and Additional Warnings
Google Chrome	JavaScript, cookies Chrome does not cache static content, such as images, CSS, or JavaScript, with the system-provided self-signed certificate. Especially in low bandwidth environments, this can extend page load times. If you do not want to replace the self-signed certificate, you can instead add it to the trust store of the browser/OS.
Mozilla Firefox	JavaScript, cookies, TLS v1.2 When it updates, Firefox sometimes stops trusting the system-provided self-signed certificate. If you do not want to replace the certificate, and the login page does not load, refresh Firefox. Type `about:support` in the Firefox search bar and click **Refresh Firefox**. You will lose some settings; see the Refresh Firefox support page.
Microsoft Internet Explorer 10 and 11 (Windows)	JavaScript, cookies, TLS v1.2, 128-bit encryption 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 (Internet Explorer 11 only). Enable Compatibility View for the Firepower web interface IP address/URL.
Apple Safari 10 and 11 (MacOS)	Tested with Firepower Device Manager only.
Microsoft Edge (Windows)	Not tested.

Screen Resolution Requirements

Firepower user interfaces require the following resolutions.

Interface	Resolution
Firepower Management Center	1280 pixels wide
7000/8000 series device (limited local interface)	1280 pixels wide

Interface	Resolution
Firepower Device Manager	1024 pixels wide by 768 pixels high
ASDM managing an ASA FirePOWER module	1024 pixels wide by 768 pixels high
Firepower Chassis Manager for Firepower 4100/9300 chassis	1024 pixels wide by 768 pixels high



CHAPTER 3

New Features and Functionality

These topics provide an overview of the new features and functionality available in Firepower Version 6.3.0.

- New Features in FMC/Firepower Version 6.3.0, on page 11
- New Features in Firepower Device Manager/FTD Version 6.3.0, on page 17

New Features in FMC/Firepower Version 6.3.0

This table summarizes the new features available in Firepower Version 6.3.0 when configured using a Firepower Management Center. For details, see the appropriate installation, quick start, or configuration guide. Updated documentation is linked from Updated Documentation, on page 51.

Feature	Description
Hardware	
ISA 3000 with FirePOWER Services	ISA 3000 with FirePOWER Services is supported in Version 6.3.0. 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. Supported platforms: ISA 3000
Licensing	
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 screens: **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 screens: **System** > **Licenses** > **Specific Licenses** Supported platforms: FMC, FTD
Interface Features	

Feature	Description
Hardware bypass support on the Firepower 2100 for supported network modules	Firepower 2100 devices now support hardware bypass functionality when using the hardware bypass network modules. New/Modified screens: **Devices** > **Device Management** > **Interfaces** > **Edit Physical Interface** Supported platforms: Firepower 2100
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 screens: **Interfaces** > **All Interfaces** > **Edit Port Channel** > **Mode** New/Modified FXOS commands: **set port-channel-mode** Supported platforms: Firepower 4100/9300
Access Control	
Update interval for URL category and reputation data	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. Upgrading to Version 6.3.0 does not change system behavior. The setting defaults to disabled (the current behavior), meaning that cached URL data does not expire. New/Modified screens: **System** > **Integration** > **Cisco CSI** > **Cached URLs Expire** setting
High Availability and Scalability	

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 screens: **Devices** > **Device Management >** edit device **> Interfaces** tab New/Modified Firepower Chassis Manager screens: • **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
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 screens: **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

Feature	Description
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 screens: • **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
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
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
Events, 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 screens: • **System** > **Integration** > **Packet Analyzer** • **Analysis** > **Advanced** > **Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer

Feature	Description
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 screens: **Analysis** > **Advanced** > **Contextual Cross-Launch**
Unified syslog configuration	Previously, you configured event logging via syslog in multiple places, depending on the event type. In Version 6.3.0, 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. 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*. Supported platforms: feature dependent
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).
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	
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 screens: **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 and 8000 Series devices
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 screens: **Devices** > **Platform Settings** > create or edit FTD policy > **SNMP** > **Hosts** tab Supported platforms: FTD

Feature	Description
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 screens: • **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 screens: **System** > **Configuration** > **Console Configuration** > **Enable CLI Access** check box Supported platforms: FMC, including FMCv
Improved login security	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. New/Modified screens: **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: Managed devices
Copy device configurations	You can copy device configurations and policies from one device to another. New/Modified screens: **Devices** > **Device Management >** edit the device **> General** area **> Get/Push Device Configuration** icons.
Backup/restore FTD device configurations	You can use the FMC web interface to back up configurations for some FTD devices. New/Modified screens: **System** > **Tools** > **Backup/Restore** New/Modified CLI commands: **restore** Supported platforms: All physical FTD devices, FTDv on VMware

Feature	Description
Skip deploying to up-to-date devices when you schedule deploy tasks	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 screens: **System** > **Tools** > **Scheduling >** add or edit a task **>** choose **Job Type** of **Deploy Policies**
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 screens: • **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
Firepower Management Center REST API	
New objects	The FMC REST API supports new objects for site-to-site VPN topology and HA device failover. New objects for site-to-site VPN topology: ftds2svpns, endpoints, ipsecsettings, advancedsettings, ikesettings, ikev1ipsecproposals, ikev1policies, ikev2ipsecproposals, ikev2policies New objects for HA device failover: failoverinterfacemacaddressconfigs, monitoredinterfaces
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*.

New Features in Firepower Device Manager/FTD Version 6.3.0

Released: December 3, 2018

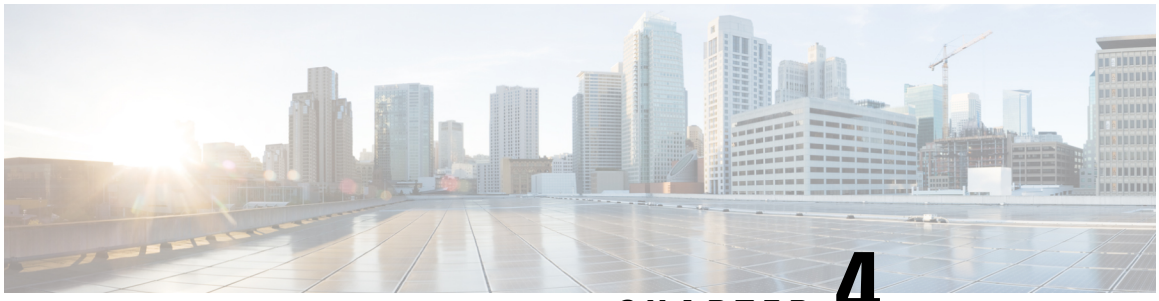
The following table lists the new features available in FTD 6.3.0 when configured using Firepower Device Manager.

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.
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 Firepower Device Manager. 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 Firepower Device Manager Users.	You can use an external RADIUS server to authenticate and authorize users logging into Firepower Device Manager. You can give external users administrative, read-write, or read-only access. Firepower Device Manager can support 5 simultaneous logins; the sixth session automatically logs off the oldest session. You can forcefully end a Firepower Device Manager 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 Firepower Threat Defense Virtual). You can use passive mode to evaluate how the Firepower Threat Defense Virtual 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 Firepower Device Manager.
Support for ASA 5506-X, 5506W-X, 5506H-X, and 5512-X removed starting with FTD 6.3.	You cannot install Firepower Threat Defense 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 Firepower Device Manager 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.



CHAPTER 4

Upgrade to Version 6.3.0

These topics provide critical and release-specific information for Version 6.3.0.

- Upgrade Warnings for All Releases, on page 23
- Upgrade Warnings for Version 6.3.0, on page 24
- Version Requirements to Upgrade, on page 34
- Time Tests and Disk Space Requirements, on page 34
- Traffic Flow, Inspection, and Device Behavior During Upgrade, on page 36
- Upgrade Instructions, on page 43
- Upgrade Packages, on page 43

Upgrade Warnings for All Releases

These important warnings apply to every upgrade.

Appliance Access During Upgrade

Before you upgrade a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firepower Management Center deployments, you should also able to access the FMC management interface without traversing the device.

This is because Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails.

Unresponsive Upgrades

Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do *not* restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Cisco Smart Licensing: Check Status After Upgrade

Deployments: Firepower Device Manager

In some cases, upgrading a Firepower Threat Defense device managed by Firepower Device Manager unregisters the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

1. Click **Device**, then click **View Configuration** in the Smart License summary.
2. If the device is not registered, click **Register Device**.

Upgrade Warnings for Version 6.3.0

These important warnings apply to Version 6.3.0.

Upgrade Warnings from Intermediate Versions

These release notes provide warnings that are *new* to Version 6.3.0.

You can upgrade to Version 6.3.0 from several previous major versions. Unless you are upgrading from the most recent major version or one of its patches (Version 6.2.3.x), you *must* review the warnings and guidelines from intermediate versions. Even if your upgrade path skips a version, its guidelines may still apply. For example, if an intermediate upgrade auto-enables an option, so will this one.

Table 3: Resources for Intermediate-Version Warnings

Resource	When Upgrading to Version 6.3.0				
	***from* 6.2.3.x**	**6.2.2.x**	**6.2.1**	**6.2.0.x**	**6.1.0.x**
Version 6.3.0 Release Notes (this document)	Yes	Yes	Yes	Yes	Yes
Version 6.2.3 Release Notes	—	Yes	Yes	Yes	Yes
Version 6.2.2 Release Notes	—	—	Yes	Yes	Yes
Version 6.2.0 Release Notes	—	—	—	—	Yes

Renamed Upgrade and Installation Packages

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1 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, on select platforms.

Table 4: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Packages
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
NGIPSv	**New:** Cisco_Firepower_NGIPS_Virtual **Old:** Sourcefire_3D_Device_VMware **Old:** Sourcefire_3D_Device_Virtual64_VMware

Table 5: Naming Schemes: Installation Packages

Platform	New
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

Preinstallation Hotfix for MC1000, 2500, and 4500 (Required)

Deployments: Firepower Management Center models MC1000, 2500, and 4500

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

You must apply a preinstallation hotfix before you upgrade an MC1000, MC2500, or MC4500 from Version 6.2.x to Version 6.3+. This hotfix updates the firmware for the RAID controller. Without the hotfix, affected upgraded FMCs running Version 6.3+ can experience performance issues. Do not apply the hotfix to any other appliance, including new or reimaged Version 6.3+ FMCs.

The hotfix is available on the Cisco Support & Download site, in the same location as the upgrade and installation packages for your *current* version. Use the regular upgrade page (**System** > **Updates**) to apply the hotfix.

Table 6: Preinstallation Hotfix Packages

Current Version	Hotfix	Package
6.3+	—	Contact Cisco TAC if you upgraded to 6.3+ without the hotfix.
6.2.3.x	Hotfix AJ	Sourcefire_3D_Defense_Center_S3_Hotfix_AJ-6.2.3.999-5.sh.REL.tar
6.2.2.x	Hotfix BY	Sourcefire_3D_Defense_Center_S3_Hotfix_BY-6.2.2.999-1.sh.REL.tar
6.2.1	—	Upgrade to Version 6.2.3 and apply Hotfix AJ.
6.2.0.x	Hotfix CD	Sourcefire_3D_Defense_Center_S3_Hotfix_CD-6.2.0.999-1.sh

Push Firepower Package Before FXOS Upgrade on Firepower 4100/9300 (Required)

Deployments: Firepower 4100/9300 with FTD

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

Directly to: Version 6.3+ running on FXOS 2.4.1+

We strongly recommend you use the FMC to push (copy) 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 push before you begin the required companion FXOS upgrade.

Note If you are upgrading a Firepower 4100/9300 device from Version 6.1 directly to Version 6.3, this push is *required*. You *must* push before you upgrade FXOS.

This is because upgrading FXOS to Version 2.4.1+ while still running Firepower 6.1 can make the device management port flap, which in turn causes intermittent communication problems between the device and the FMC. 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.

Before you begin

Make sure you have the bandwidth to perform a large data transfer from the FMC to the devices. The time to push an upgrade package depends on your management network's bandwidth. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Step 1 Upgrade the FMC to the target version.

The FMC must be running at least Version 6.2.3 to push to managed devices.

Step 2 Obtain the device upgrade package from the Cisco Support & Download site and upload it to the FMC.

Step 3 Use the FMC to push the upgrade package to the device.

Step 4 After the push completes, upgrade FXOS to the target version.

Step 5 Immediately, use the FMC to upgrade the Firepower software on the device.

Until you upgrade the Firepower software, you may continue to experience management port flaps.

Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER May Fail

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

Upgrading from: Version 6.1 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; see Resolved Issues in New Builds, on page 55. 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.

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

Deployments: FMC, 7000/8000 series, NGIPSv

Upgrading from: Version 6.1 through 6.1.0.6, Version 6.2 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+

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. To run the readiness check, you must be running one of the following patches.

Table 7: Patches with Readiness Checks for Version 6.3+

Readiness Check Not Supported	First Patch with Fix
6.1 through 6.1.0.6	6.1.0.7
6.2 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

Updated Security for Appliance Access

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

To enhance security, in Version 6.3 we 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.

Firepower Management Center Menu Changes

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

Version 6.3 changes the menu paths on the FMC web interface for the following pages.

Table 8: Changed FMC Menu Paths in Version 6.3+

Old Menu Path	New Menu Path
Analysis > Lookup > Whois	**Analysis > Advanced > Whois**
Analysis > Lookup > Geolocation	**Analysis > Advanced > Geolocation**
Analysis > Lookup > URL	**Analysis > Advanced > URL**
Analysis > Custom > Custom Workflows	**Analysis > Advanced > Custom Workflows**
Analysis > Custom > Custom Tables	**Analysis > Advanced > Custom Tables**
Analysis > Vulnerabilities > Vulnerabilities	**Analysis > Hosts > Vulnerabilities**
Analysis > Vulnerabilities > Third-Party Vulnerabilities	**Analysis > Hosts > Third-Party Vulnerabilities**

SSL Hardware Acceleration Enabled on Upgrade

Deployments: FTD on Firepower 2100 series & Firepower 4100/9300 chassis

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0 only

The upgrade process automatically enables SSL hardware 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 SSL hardware acceleration on a managed device that is not decrypting traffic can affect performance. We recommend you disable SSL hardware acceleration on devices that are not decrypting traffic.

To disable, use this CLI command:

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

EMS Extension Support for SSL Decryption Disabled on Upgrade

Deployments: Any

Upgrading from: Version 6.2.3.8+

Directly to: Version 6.3.0

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 FMC deployments, this feature depends on the *device* version. Upgrading the FMC 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.

We will reintroduce support in a patch.

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.

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, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the following 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.

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.

Timeouts for the URL Filtering Cache Can Change

Deployments: Any

Upgrading from: Version 6.2.3.x

Directly to: Version 6.3+

New for Version 6.3, the GUI allows you configure a timeout value for the URL filtering cache. To minimize instances of URLs matching on stale data, you can set URLs in the cache to expire. If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value.

After the upgrade completes:

- FMC: Choose **System** > **Integration**, click the Cisco CSI tab, and evaluate the **Cached URLs Expire** setting.

- FDM: Choose **System Settings** > **Traffic Settings** > **URL Filtering Preferences** and evaluate the **URL Time to Live** setting.

Syslog Behavior Changes for Connection and Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

Version 6.3 changes and centralizes the way the system logs connection and intrusion events via syslog. You can access these settings on the new Logging tab in the access control policy. The upgrade does not change your existing settings for connection event logging, however:

- Intrusion events: Before Version 6.3, enabling syslog alerting in an intrusion policy sent all intrusion events to the syslog, either on the managed device itself or to an external host or hosts. If you did not specify an external host, obviously no events were sent. After you upgrade to Version 6.3+, the intrusion policy uses the destination on the Logging tab of the access control policy. This means you can suddenly start receiving intrusion events you did not "expect" via syslog,
- Timestamps: Messages sent from Classic devices (7000/8000 series, ASA FirePOWER, NGIPSv) now use the ISO 8601 timestamp format as specified in RFC 5425.

Reporting Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.x

Directly to: Version 6.3

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.

EOS: Decryption on Passive and Inline Tap Interfaces

Deployments: Any device with interfaces in passive or inline tap mode, where you have configured SSL decryption

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

Version 6.3 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. If you configure SSL decryption, any encrypted traffic on these interfaces is handled by the SSL policy's **Undecryptable Action** setting (FMC) or its default action (FDM). Any subsequent inspection of the still-encrypted traffic is necessarily limited.

EOS: VMware vSphere/VMware ESXi 5.5

Deployments: Any virtual appliance hosted on VMware vSphere/VMware ESXi 5.5

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

Version 6.3 virtual deployments have not been tested on VMware vSphere/VMware ESXi 5.5. We recommend you upgrade the hosting environment before you upgrade the Firepower software.

EOS: Firepower on ASA 5512-X and ASA 5506-X Series

Deployments: ASA 5506-X series and ASA 5512-X devices

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

You cannot upgrade to or freshly install Version 6.3+ of the Firepower software (both FTD and ASA FirePOWER) on these models:

- ASA 5506-X, 5506H-X, 5506W-X
- ASA 5512-X

For information on compatibile Firepower versions, see the Cisco Firepower Compatibility Guide.

Blacklisted FlexConfig Commands for FTD

Some Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2, you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.

FTD upgrades can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can blacklist FlexConfig commands that you are currently using. Although your existing configurations continue to work and you can still deploy, you cannot assign or create FlexConfig objects using the newly blacklisted commands.

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

The following topics list newly blacklisted or changed FlexConfig configurations. For full lists, see the FlexConfig topics in your configuration guide or online help.

Version 6.3.0 Deprecated FlexConfig Objects

Table 9: Version 6.3.0 Deprecated FlexConfig Objects for FMC

Object	Description	New Location	Associated Text Objects
Default_DNS_Configure	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.	Configure DNS for the data interfaces in the FTD platform settings policy.	defaultDNSNameServerList defaultDNSParameters
TCP_Embryonic_Conn_Limit TCP_Embryonic_Conn_Timeout	Configure embryonic connection limits and timeouts to protect against SYN Flood Denial of Service (DoS) attacks.	Configure these features in the FTD service policy, which you can find on the Advanced tab of the access control policy assigned to the device.	tcp_conn_misc tcp_conn_limit tcp_conn_timeout

Version 6.3.0 Blacklisted CLI Commands

Table 10: Version 6.3.0 Blacklisted CLI Commands for FDM

Command	Comments
access-list	Partially blocked. • You can create **ethertype** access lists. • You cannot create **advanced** access lists, which the system uses with the **access-group** command. Instead, use **Policies** > **Access Control** to configure access rules. • You cannot create **webtype** access lists.
as-path	Create Smart CLI AS Path objects and use them in a Smart CLI BGP object to configure an autonomous system path filter.
community-list	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	Configure DNS groups using **Objects** > **DNS Groups**, and assign the groups using **Device** > **System Settings** > **DNS Server**.
domain-name	Configure DNS groups using **Objects** > **DNS Groups**, and assign the groups using **Device** > **System Settings** > **DNS Server**.

Command	Comments
ipv6	You can configure **ipv6 ospf** and **ipv6 router ospf** commands, but all other **ipv6** commands are prohibited. Create Smart CLI IPv6 Prefix List objects and use them in a Smart CLI BGP object to configure prefix list filtering for IPv6.
logging	Use **Objects** > **Syslog Servers** and **Device** > **System Settings** > **Logging Settings**. However, you can configure the **logging history** command in FlexConfig.
policy-list	Create Smart CLI Policy List objects and use them in a Smart CLI BGP object to configure a policy list.
prefix-list	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	Create Smart CLI Route Map objects and use them in a Smart CLI OSPF or BGP object to configure route maps.
router bgp	Use the Smart CLI templates for BGP.

Version Requirements to Upgrade

This table lists the versions of the Firepower software that support direct upgrade to Version 6.3.0. You do *not* need to be running the latest patch of the previous version to upgrade to the next major version.

Appliance	Managed By	Version to Upgrade
Firepower Management Center	—	6.1.0+
7000 and 8000 series device NGIPSv ASA FirePOWER module	Firepower Management Center	6.1.0+
Firepower Threat Defense device	Firepower Management Center	6.1.0+
	Firepower Device Manager	6.2.0+
ASA FirePOWER module	ASDM	6.2.0+

Time Tests and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. When you use the Firepower Management Center to upgrade a managed device, the FMC requires additional disk space in its /Volume partition, for the device upgrade package.

You must also have enough time to perform the upgrade. We provide estimates of upgrade times for each release.

About Time Tests

Time values given here are based on in-house tests. Values for devices are from tests in a Firepower Management Center deployment. This is because raw upgrade times for remotely and locally managed devices are similar, given similar conditions. Because lower-memory appliances tend to take longer to upgrade, we try to test on those platforms. For virtual platforms, we use the default settings for memory and resources.



Note Although we report the slowest time of all upgrades tested, your upgrade will likely take longer than the provided times for any/all of the following reasons.

Push and Reboot Not Included

Values represent *only* the time it took for the Firepower upgrade script itself to run. Values do not include the time required to upload upgrade packages to a locally managed device or to the FMC, nor the time to copy (*push*) upgrade packages from the FMC to a managed device.

In FMC deployments, insufficient bandwidth between the FMC and managed devices can extend upgrade time or even cause the upgrade to time out. Make sure you have the bandwidth to perform a large data transfer from the FMC to its devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Values also do not include reboots, readiness checks, operating system upgrades, or configuration deploys.

Time Is For Single Devices

Values are *per device*. 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.

Note that stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly longer than upgrading a standalone device.

Affected Configurations and Data

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.

About Disk Space Requirements

Space estimates are the *largest* reported for all upgrades, and are:

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

Version 6.3.0 Time and Disk Space

For Version 6.3, we tested upgrades from all eligible previous major versions: Version 6.1 to Version 6.2.3. In most cases, we tested on the lowest-end models in each series, and sometimes on multiple models in a series. For virtual appliances, we used VMware vCenter Server, Version 6.0. For the ISA 3000, refer to the ASA 5500-X series estimates.

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

Traffic Flow, Inspection, and Device Behavior During Upgrade

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

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

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions. We *strongly* recommend performing any upgrade or uninstall in a maintenance window or at a time when any interruption will have the least impact on your deployment.

FTD Upgrade Behavior: Firepower 4100/9300 Chassis

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

Chassis: FXOS Upgrade

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

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)	Fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection
	Fail-to-wire disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online
	No fail-to-wire module.	Dropped until at least one module is online

Standalone Device: Firepower Software Upgrade

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

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, fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Either: • Passed without inspection (6.2.3+) • Dropped (6.1 through 6.2.2.x)
	Inline set, fail-to-wire disabled: **Bypass: Disabled**. (6.1+)	Dropped
	Inline set, no fail-to-wire module	Dropped
	Inline set, tap mode	Egress packet immediately, copy not inspected
	Passive, ERSPAN passive	Uninterrupted, not inspected

High Availability Pairs: Firepower Software Upgrade

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

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

Clusters: Firepower Software Upgrade

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

The slave security module or modules upgrade first, then the master. Security modules operate in maintenance mode while they upgrade.

During the master 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.



Note Upgrading an inter-chassis cluster from Version 6.2.0, Version 6.2.0.1, or Version 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. The Snort process 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 Firepower Threat Defense standalone devices, high availability pairs, and clusters. Your interface configuration determines whether traffic drops or passes without inspection during the interruption.

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 - 6.1.0.x)	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

FTD Upgrade Behavior: Other Devices

This section describes device and traffic behavior when you upgrade Firepower Threat Defense devices with bundled operating systems: Firepower 2100 series, ASA 5500-X series, ISA 3000, and FTDv.

Standalone Devices: Firepower Software Upgrade

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

High Availability Pairs: Firepower Software Upgrade

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

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

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying,

you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on Firepower Threat Defense standalone devices and high availability pairs. Your interface configuration determines whether traffic drops or passes without inspection during the interruption.

Table 11: Traffic Behavior During Deployment: FTD Devices with Bundled OS

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 - 6.1.0.x)	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 and 8000 series devices.

Standalone Devices: Firepower Software Upgrade

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

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.

Interface Configuration	Traffic Behavior
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

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. The Snort process 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, resources demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on Firepower standalone devices, high availability pairs, and 8000 series stacks. Your interface configuration determines whether traffic drops or passes without inspection during the interruption.

Interface Configuration	Restart 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

Interface Configuration	Restart Traffic Behavior
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.

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 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. The Snort process 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.

When you deploy, resources 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

Your interface configurations determine how NGIPSv handles traffic during the Firepower software 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. Your interface configuration determines whether traffic drops or passes without inspection during the interruption.

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

Upgrade Instructions

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

- Firepower Management Center Upgrade Guide—Upgrade Firepower Management Center deployments, including managed devices and companion operating systems.
- Cisco ASA Upgrade Guide—Upgrade ASA FirePOWER modules managed by ASDM.
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager—Upgrade a Firepower Threat Defense device with Firepower Device Manager.

Upgrade Packages

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

- Firepower Management Center, including FMCv: https://www.cisco.com/go/firepower-software
- Firepower Threat Defense (ISA 3000): https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense (all other models, including FTDv): https://www.cisco.com/go/ftd-software
- Firepower 7000 series: https://www.cisco.com/go/7000series-software
- Firepower 8000 series: https://www.cisco.com/go/8000series-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software

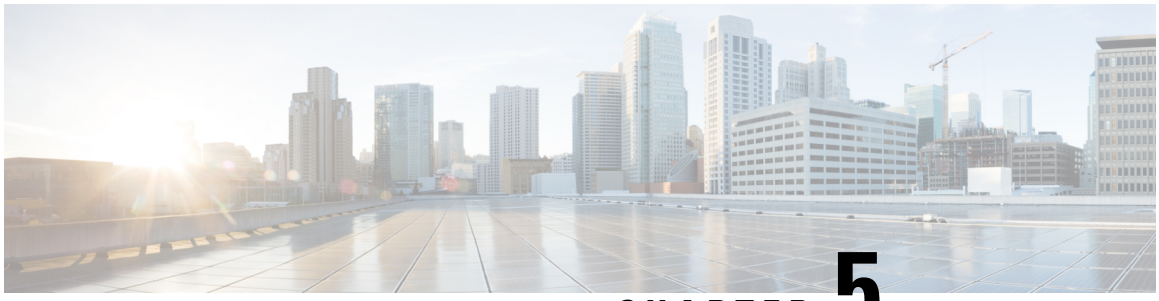
Upgrade packages from Version 6.2.1+ are signed tar archives (.tar). Do not untar.

Table 12: Upgrade Packages from Version 6.2.1+

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP_FP2K_Upgrade-*version-build*.sh.REL.tar
Firepower 4100/9300 chassis	Cisco_FTD_SSP_Upgrade-*version-build*.sh.REL.tar
ASA 5500-X series with FTD ISA 3000 with FTD Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-*version-build*.sh.REL.tar
Firepower 7000/8000 series AMP models	Cisco_Firepower_NGIPS_Appliance_Upgrade-*version-build*.sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh.REL.tar
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh.REL.tar

Table 13: Upgrade Packages from Version 6.1.x or 6.2.0.x

Platform	Package
FMC/FMCv	Cisco_Firepower_Mgmt_Center_Upgrade-*version-build*.sh
Firepower 4100/9300 chassis	Cisco_FTD_SSP_Upgrade-*version-build*.sh
ASA 5500-X series with FTD Firepower Threat Defense Virtual	Cisco_FTD_Upgrade-*version-build*.sh
Firepower 7000/8000 series AMP models	Cisco_Firepower_NGIPS_Appliance_Upgrade-*version-build*.sh
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade-*version-build*.sh
ASA FirePOWER	Cisco_Network_Sensor_Upgrade-*version-build*.sh



CHAPTER 5

Freshly Install Version 6.3.0

If you are unable to upgrade a Firepower appliance, or are disinclined to follow the required upgrade path, you can freshly install major Firepower releases.

- Deciding to Freshly Install, on page 45
- Guidelines and Limitations for Fresh Installs, on page 46
- Unregistering Smart Licenses, on page 47
- Installation Instructions, on page 49

Deciding to Freshly Install

Use this table to identify scenarios where you need to freshly install. In all of these scenarios—including switching device management between local and remote—*you will lose device configurations*.

Note *Always* address licensing concerns before you reimage or switch management of a Firepower appliance. If you are using Cisco Smart Licensing, you may need to manually unregister from the Cisco Smart Software Manager to avoid accruing orphan entitlements. If you do not manually unregister, you may not be able to register a device if it is still registered with smart licensing

Table 14: Scenarios: Do You Need a Fresh Install?

Scenario	Solution	Licensing
Upgrade FMC-managed devices from an older Firepower version (5.x, 6.0.x).	The upgrade path from older versions includes intermediate versions. Especially in larger deployments where you must alternate FMC and device upgrade, this multi-step process can be time consuming. To save time, you can reimage older devices instead of upgrading: **1.** Remove the devices from the FMC. **2.** Upgrade the FMC only (5.x → 6.0 → 6.0.1 → 6.1 → 6.2.3+). **3.** Reimage the devices. You cannot reimage Version 5.x devices directly to Version 6.3. You must reimage to 6.2.3 first; see Guidelines and Limitations for Fresh Installs, on page 46. **4.** Re-add the devices to the FMC.	Removing devices from the FMC unregisters them. Reassign licenses after you re-add the devices.
Change FTD management from FDM to FMC (local to remote).	Use the **configure manager** CLI command; see Command Reference for Firepower Threat Defense.	Unregister the device before you switch management. Reassign its license after you add it to the FMC.
Change FTD management from FMC to FDM (remote to local).	Use the **configure manager** CLI command; see Command Reference for Firepower Threat Defense. **Exception:** The device is running or was upgraded from Version 6.0.1. In this case, fresh install.	Remove the device from the FMC to unregister it. Reregister using FDM.
Change ASA FirePOWER management between ASDM and FMC.	Start using the other management method.	Contact Sales for new Classic licenses. ASA FirePOWER licenses are associated with a specific manager.
Replace ASA FirePOWERwith FTD on the *same* physical device.	Fresh install.	Convert Classic to Smart licenses; see the Firepower Management Center Configuration Guide.
Replace NGIPSv with FTDv.	Fresh install.	Contact Sales for new Smart licenses.

Guidelines and Limitations for Fresh Installs

Back Up Event and Configuration Data

Freshly installing returns all settings to factory defaults, including the system password (Admin123). Before you begin, we *strongly* recommend backing up event and configuration data to an external location.

Note, however, if you are freshly installing so that you don't have to upgrade, you cannot use a backup to import your old configurations. You can restore a backup only from an appliance of the same model *and Firepower version*.

Remove Devices from the Firepower Management Center

Always remove devices from remote management before you reimage. If you are:

- Reimaging the FMC, remove all its devices from management.
- Reimaging a single device or switching from remote to local management, remove that one device.

Address Licensing Concerns

Before you reimage *any* Firepower appliance, address licensing concerns. You may need to unregister from the Cisco Smart Software Manager, or you may need to contact Sales for new licenses. See Deciding to Freshly Install to determine what you need to do, depending on your scenario.

For more information on licensing, see:

- Cisco Firepower System Feature Licenses Guide
- Frequently Asked Questions (FAQ) about Firepower Licensing
- The licensing chapter in your *Configuration Guide*.

Reimaging Version 5.x Hardware to Version 6.3+

You cannot freshly install Version 6.3+ on a *physical* Firepower appliance that is currently running Version 5.x. This occurs because the old system restore process is incompatible with newer installation packages.

Affected appliances are:

- DC750, DC1500, DC3500
- DC2000, DC4000
- 7000/8000 series devices, including AMP models

In this case, the quickest path to Version 6.3+ is:

1. Freshly install Version 6.2.3.
2. Freshly install (or upgrade to) Version 6.3+.

After you reimage a FMC (Defense Center) from Version 5.x to Version 6.2.3, 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 devices, whether locally (Firepower Device Manager) or remotely (Firepower Management Center) managed, use Cisco Smart Licensing. To use licensed features, you must register with Cisco Smart Software Manager (CSSM). Before you reimage or switch management, you must manually unregister to avoid accruing orphan entitlements.

Unregistering removes an appliance from your virtual account, and also 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.

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.

Do not unregister from CSSM when you:

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

In these two cases, removing the device from the FMC 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.

Unregister a Firepower Management Center

Unregister a Firepower Management Center from the Cisco Smart Software Manager before you reimage the FMC. This also unregisters any managed Firepower Threat Defense devices.

If the FMC is configured for high availability, licensing changes are automatically synchronized. You do not need to unregister the other FMC.

Step 1 Log into the Firepower Management Center.

Step 2 Choose **System** > **Licenses** > **Smart Licenses**.

Step 3 Next to Smart License Status, click the stop sign ( ).

Step 4 Read the warning and confirm that you want to unregister.

Unregister an FTD Device Using FDM

Unregister locally managed Firepower Threat Defense devices from the Cisco Smart Software Manager before you either reimage or switch to remote (FMC) management.

If the device is configured for high availability, you must log into the other unit in the high availability pair to unregister that unit.

Step 1 Log into the Firepower Device Manager.

Step 2 Click **Device**, then click **View Configuration** in the Smart License summary.

Step 3 Select **Unregister Device** from the gear drop-down list.

Step 4 Read the warning and confirm that you want to unregister.

Installation Instructions

The release notes do not contain installation instructions. Instead, see one of the following documents. Installation packages are available on the Cisco Support & Download site.

Table 15: Firepower Management Center Installation Instructions

FMC Platform	Guide
FMC 750, 1500, 2000, 3500, 4000	Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500, and 4000 — Restoring a Firepower Management Center to Factory Defaults
FMC 1000, 2500, 4500	Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500 — Restoring a Firepower Management Center to Factory Defaults
FMCv	Cisco Firepower Management Center Virtual Deployment Guide

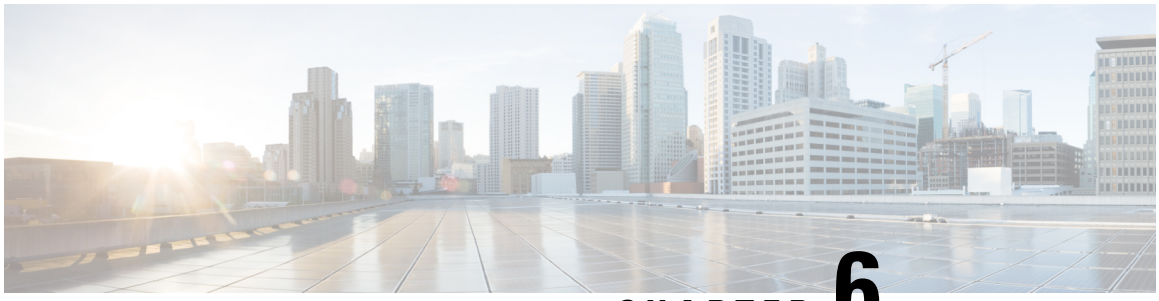
Table 16: Firepower Threat Defense Installation Instructions

FTD Platform	Guide
Firepower 2100 series	Reimage the Cisco ASA or Firepower Threat Defense Device *and* Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series Running Firepower Threat Defense
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guides — Image Management chapters
ASA 5500-X series ISA 3000	Reimage the Cisco ASA or Firepower Threat Defense Device
FTDv: VMware, with FMC	Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide
FTDv: VMware, with FDM	Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for VMware Deployment Quick Start Guide
FTDv: KVM, with FMC	Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide
FTDv: KVM, with FDM	Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start Guide

FTD Platform	Guide
FTDv: AWS	Cisco Firepower Threat Defense Virtual Quick Start Guide for the AWS Cloud
FTDv: Azure	Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

Table 17: 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
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	Reimage the Cisco ASA or Firepower Threat Defense Device *and* ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide — Managing the ASA FirePOWER Module



CHAPTER 6

Documentation

The following topics provide links to Firepower documentation:

- Updated Documentation, on page 51
- Documentation Roadmaps, on page 53

Updated Documentation

The following Firepower documentation was updated or is newly available for Version 6.3.0. For links to documentation not updated or newly available with this release, see the Documentation Roadmaps, on page 53.

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
- Command Reference for Firepower Threat Defense

FXOS Configuration Guides

- 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

Upgrade Guides

- Firepower Management Center Upgrade Guide
- Cisco ASA Upgrade Guide

Hardware Installation Guides

- Cisco Firepower 2100 Series Hardware Installation Guide

Quick Start Guides

Quick Start: Firepower Management Center

- Firepower Management Center Virtual Deployment Guide ***NEW***

Quick Start: Firepower Threat Defense with FMC

- Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series 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 Management Center Quick Start Guide
- Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide
- Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide

Quick Start: Firepower Threat Defense with FDM

- Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Device Manager 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 Using Firepower Device Manager for VMware Deployment Quick Start Guide
- Cisco Firepower Threat Defense Virtual Using Firepower Device Manager for KVM Deployment Quick Start 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 Guide
- Cisco FXOS Compatibility Guide

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

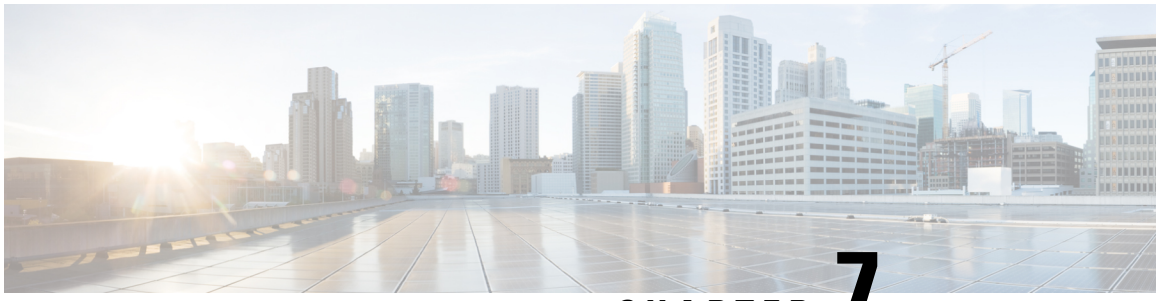
Troubleshooting and Configuration Examples

- 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

Bugs listed here were verified as resolved when this Firepower version was initially released.

- Searching for Resolved Issues, on page 55
- Resolved Issues in New Builds, on page 55
- Version 6.3.0 Resolved Issues, on page 56

Searching for Resolved Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of resolved bugs for Firepower products. These general queries display resolved bugs for Firepower products running Version 6.3.0:

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

You can further constrain your search to bugs affecting specific Firepower platforms and versions. You can also search by bug ID, or for specific keywords.

Resolved Issues in New Builds

Sometimes Cisco releases updated builds. Only the latest build for each platform is available on the Cisco Support & Download site. You should always 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 you have an issue with a currently installed "old" build, determine if an upgrade, patch, or hotfix will address that issue. If none of these are available, you must reimage.

Table 18: Version 6.3.0 New Builds

New Build	Released	Platforms	Packages	Resolves
85	2019-01-22	Firepower 4100/9300	Upgrade Fresh Install	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.
84	2018-12-18	FMC/FMCv ASA FirePOWER	Upgrade	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

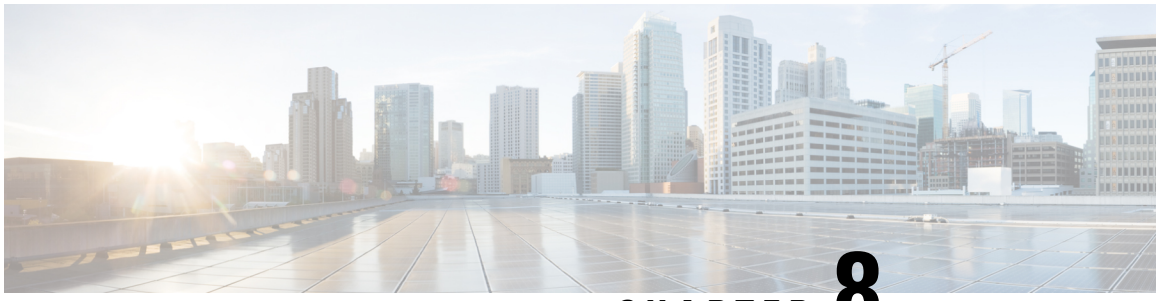
Bug ID	Title
CSCuy27743	VDB install during firstboot fails because of MySQL dropping out
CSCvb15074	FMC health notifications for interfaces removed or added out-of-band get stuck
CSCvb38753	client hello is getting modified with dnd if application is configured in ssl rule
CSCvb73266	Deploying to devices 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

Bug ID	Title
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"
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

Bug ID	Title
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
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

Bug ID	Title
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
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

Bug ID	Title
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
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

Bugs listed here were known to exist when this Firepower version was initially released.

- Searching for Known Issues, on page 61
- Version 6.3.0 Known Issues, on page 61

Searching for Known Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of open bugs for Firepower products. These general queries display open bugs for Firepower products running Version 6.3.0:

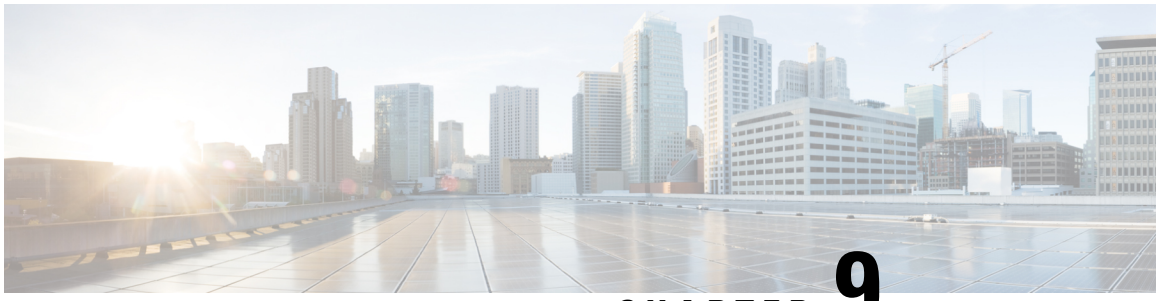
- Firepower Management Center
- Firepower Management Center Virtual
- NGIPSv

You can further constrain your search to bugs affecting specific Firepower platforms and versions. You can also search by bug ID, or for specific keywords.

Version 6.3.0 Known Issues

Bug ID	Title
CSCvk74150	After FDM HA switch the deploy takes longer than 25 minutes on 6.3.0-1376
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
CSCvm53619	Failover interface MAC address does not get updated correctly
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	Title
CSCvn19289	Multiple Vulnerabilities in curl
CSCvn32308	Restoring self backup on secondary requires license re-registrations
CSCvn44222	6.3.0-79: While doing HA upgrade from 6.3.0-79 to 6.4.0-1058, upgrade failed
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"



CHAPTER 9

For Assistance

Thank you for choosing Firepower.

- Online Resources, on page 63
- Contact Cisco, on page 63

Online Resources

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

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

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC: 1.408.526.7209 or 1.800.553.2447