

Cisco Firepower Release Notes, Version 6.6.0

First Published: 2020-04-06

Last Modified: 2020-07-17

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

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

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

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

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

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

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

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

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

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

© 2020 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Welcome to Version 6.6.0** 1

About the Release Notes 1

Release Dates 1

CHAPTER 2 **Compatibility** 3

Firepower Management Centers 3

Firepower Devices 4

Manager-Device Compatibility 6

Web Browser Compatibility 6

Screen Resolution Requirements 8

Additional Compatibility Resources 8

CHAPTER 3 **Features and Functionality** 9

New Features in Firepower Management Center/Version 6.6.0 9

New Features in Firepower Device Manager/FTD Version 6.6.0 17

Deprecated Features 23

Version 6.6.0 Deprecated Features 24

Version 6.5.0 Deprecated Features 25

Version 6.4.0 Deprecated Features 27

Version 6.3.0 Deprecated Features 28

Deprecated FlexConfig Commands 31

FMC How-To Walkthroughs 32

CHAPTER 4 **Upgrade to Version 6.6.0** 35

Guidelines and Warnings for Version 6.6.0 35

FMCv Requires 28 GB RAM for Upgrade 36

Events Temporarily Unavailable After FMC Upgrade 37
Previously Published Guidelines and Warnings 37
Firepower 1000 Series Devices Require Post-Upgrade Power Cycle 38
Historical Data Removed During FTD/FDM Upgrade 39
New URL Categories and Reputations 39
Pre-Upgrade Actions for URL Categories and Reputations 40
Post-Upgrade Actions for URL Categories and Reputations 41
Guidelines for Rules with Merged URL Categories 42
TLS Crypto Acceleration Enabled/Cannot Disable 45
Readiness Check May Fail on FMC, NGIPSv 45
RA VPN Default Setting Change Can Block VPN Traffic 45
Security Intelligence Enables Application Identification 46
Update VDB after Upgrade to Enable CIP Detection 46
Invalid Intrusion Variable Sets Can Cause Deploy Failure 47
General Guidelines and Warnings 47
Minimum Version to Upgrade 50
Time Tests and Disk Space Requirements 50
About Time Tests 50
About Disk Space Requirements 51
Version 6.6.0 Time and Disk Space 51
Traffic Flow, Inspection, and Device Behavior 52
FTD Upgrade Behavior: Firepower 4100/9300 Chassis 52
FTD Upgrade Behavior: Other Devices 56
ASA FirePOWER Upgrade Behavior 57
NGIPSv Upgrade Behavior 58
Upgrade Instructions 59
Upgrade Packages 59

CHAPTER 5 **Freshly Install the Software** 61
Deciding to Freshly Install 61
Guidelines and Limitations for Fresh Installs 63
Unregistering Smart Licenses 65
Unregister a Firepower Management Center 66
Unregister an FTD Device Using FDM 66

Installation Instructions 66

CHAPTER 6 **Documentation** 69

New and Updated Documentation 69

Documentation Roadmaps 71

CHAPTER 7 **Resolved Issues** 73

Searching for Resolved Issues 73

Version 6.6.0 Resolved Issues 74

CHAPTER 8 **Known Issues** 81

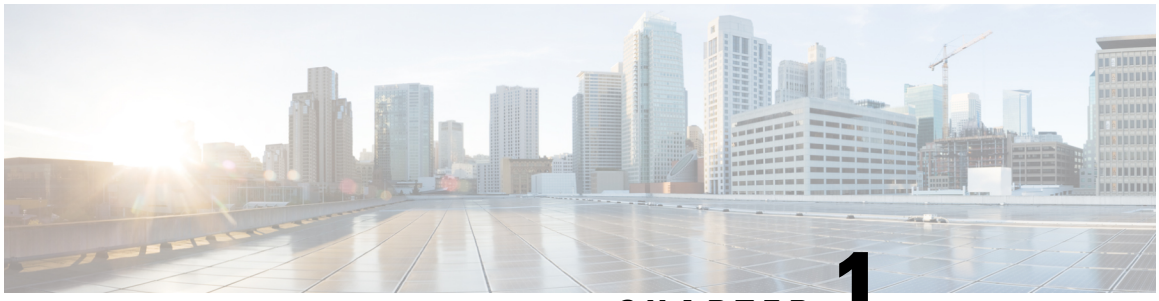
Searching for Known Issues 81

Version 6.6.0 Known Issues 81

CHAPTER 9 **For Assistance** 85

Online Resources 85

Contact Cisco 85



CHAPTER 1

Welcome to Version 6.6.0

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, including upgrade warnings and behavior changes. Read this document even if you are familiar with Firepower releases and have previous experience upgrading Firepower deployments.

For links to upgrade and installation instructions, see:

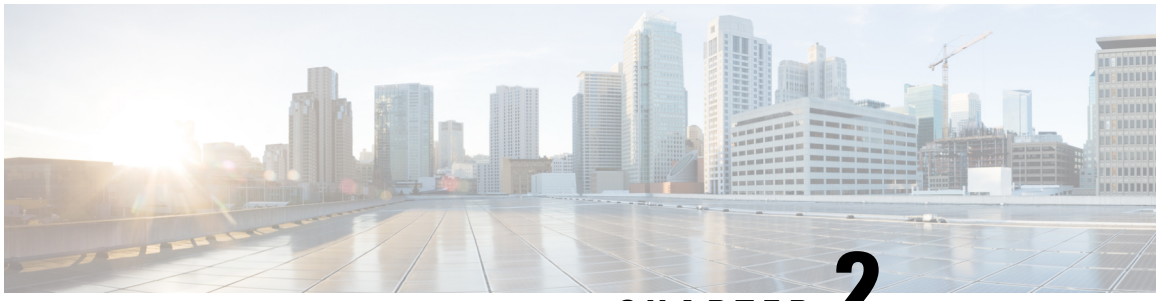
- Upgrade Instructions, on page 59
- Installation Instructions, on page 66

Release Dates

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

Table 1: Version 6.6.0 Dates

Build	Date	Platforms
90	2020-05-08	Firepower 4112
	2020-04-06	FMC/FMCv All devices except Firepower 4112



CHAPTER 2

Compatibility

For detailed compatibility information for all supported Firepower versions, including links to end-of-sale and end-of-life announcements for deprecated platforms, see the Cisco Firepower Compatibility Guide.

For compatibility information for this Firepower version, see:

- Firepower Management Centers, on page 3
- Firepower Devices, on page 4
- Manager-Device Compatibility, on page 6
- Web Browser Compatibility, on page 6
- Screen Resolution Requirements, on page 8
- Additional Compatibility Resources, on page 8

Firepower Management Centers

Firepower Management Center Physical Platforms

Version 6.6.0 FMC software is supported on these physical platforms:

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

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

Firepower Management Center Virtual (FMCv) Platforms:

Version 6.6.0 FMCv software is supported in both on-premises and cloud-based deployments:

- FMCv and FMCv 300 for VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7
- FMCv for Kernel-based virtual machine (KVM)
- FMCv for Amazon Web Services (AWS)
- FMCv for Microsoft Azure

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

Firepower Devices

Cisco Firepower devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules.

About Firepower Devices

Depending on platform, Firepower devices can have different software, operating systems, and management methods:

- **Software:** Some Firepower devices run Firepower Threat Defense (FTD) software; some run NGIPS/ASA FirePOWER software. Some can run either—but not both at the same time.
- **OS/Hypervisor:** Some Firepower implementations bundle the operating system with the software. Others require that you upgrade the operating system yourself. For versions and builds of bundled operating systems, see the *Bundled Components* information in the Cisco Firepower Compatibility Guide.
- **Remote management:** All Firepower devices support remote management with a Firepower Management Center (FMC), which can manage multiple devices.
- **Local management:** Most Firepower devices—especially newer models and versions—support local, single-device management. Use Firepower Device Manager (FDM) to manage Firepower Threat Defense (FTD). Use Cisco Adaptive Security Device Manager (ASDM) to manage ASA FirePOWER.
- **Cloud management:** Firepower Threat Defense devices support Cisco Defense Orchestrator (CDO) concurrently with local FDM management. Although some configurations still require FDM, CDO allows you to establish and maintain consistent security policies across multiple FTD devices without using an FMC.

Supported Firepower Devices

These Firepower Threat Defense devices are supported in Version 6.6.0

Table 2: Firepower Threat Defense Devices in Version 6.6.0

FTD Device Platform	OS/Hypervisor	Management		
		FMC	FDM	CDO
Firepower 1010, 1120, 1140, 1150	—	**YES**	**YES**	**YES**
Firepower 2110, 2120, 2130, 2140	—	**YES**	**YES**	**YES**
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145	FXOS 2.8.1.105+ Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.8(1).	**YES**	**YES**	**YES**

FTD Device Platform	OS/Hypervisor	Management		
		FMC	FDM	CDO
Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	FXOS 2.8.1.105+ Upgrade FXOS first. To resolve issues, you may need to upgrade FXOS to the latest build. To help you decide, see the Cisco FXOS Release Notes, 2.8(1).	**YES**	**YES**	**YES**
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X ISA 3000	—	**YES**	**YES**	**YES**
Firepower Threat Defense Virtual (FTDv)	Any of: • VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7 • KVM: Kernel-based Virtual Machine • AWS: Amazon Web Services • Microsoft Azure For supported instances, see the appropriate FTDv Getting Started guide.	**YES**	**YES**	**YES**

These NGIPS/ASA FirePOWER devices are supported in Version 6.6.0

Table 3: NGIPS/ASA FirePOWER Devices in Version 6.6.0

NGIPS Device Platform	OS/Hypervisor	Management	
		FMC	ASDM
ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X ISA 3000	ASA 9.5(2) to 9.14(x) There is wide compatibility between ASA and ASA FirePOWER versions. However, even if an ASA upgrade is not strictly required, resolving issues may require an upgrade to the latest supported version. See the Cisco ASA Upgrade Guide for order of operations. We recommend you upgrade the ASA 5508-X and 5516-X to the latest ROMMON image; see the instructions in the Cisco ASA and Firepower Threat Defense Reimage Guide.	**YES**	**YES**
NGIPSv	VMware vSphere/VMware ESXi 6.0, 6.5, or 6.7 For supported instances, see the Cisco Firepower NGIPSv Quick Start Guide for VMware.	**YES**	—

Manager-Device Compatibility

The FMC must run at least the same maintenance release (third-digit release) as the devices it manages. Although you can manage a patched device (fourth-digit release) with an unpatched FMC, new features and resolved issues often require the latest patch on *both* the FMC and its managed devices. We *strongly* recommend that you update your entire deployment.

Table 4: FMC-Device Compatibility

Version 6.6.0 FMC	*can manage*	Version 6.2.3 through 6.6.0.x devices.
Version 6.6.0 devices	*require*	Version 6.6.0 FMC.

Table 5: FDM-Device Compatibility

Version 6.6.0 FDM	*can manage*	one FTD device.

Table 6: ASDM-Device Compatibility

Version 7.14.1 ASDM	*can manage*	Version 6.6.0.x and earlier ASA FirePOWER modules. Although there is wide compatibility between ASA, ASDM, and ASA FirePOWER versions, some newer versions of ASDM may not be able to manage ASA FirePOWER modules on older ASA devices. For details, see Cisco ASA Compatibility.
Version 6.6.0 ASA FirePOWER modules	*require*	Version 7.14.1 ASDM.

Web Browser Compatibility

Browsers Tested with Firepower Web Interfaces

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

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

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

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

Browser Settings and Extensions

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

If you are using Microsoft Internet Explorer 11:

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

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

Securing Communications

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

To begin replacing the self-signed certificate:

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

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

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

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

Browsing from a Firepower-Monitored Network

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

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

Screen Resolution Requirements

Table 7: Screen Resolution Requirements for Firepower User Interfaces

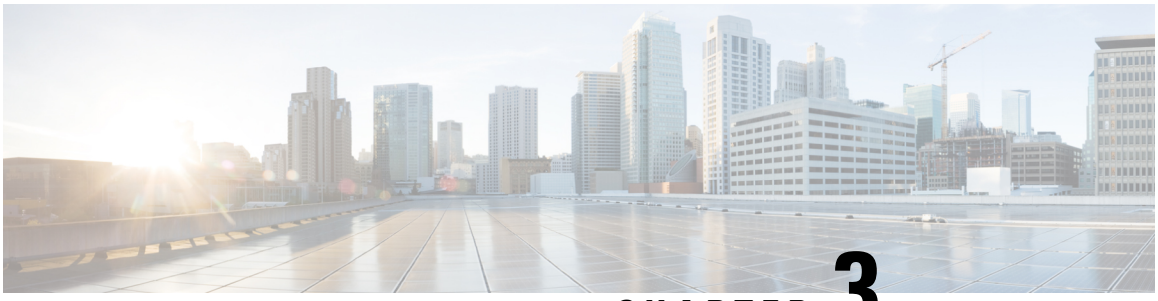
Interface	Resolution
Firepower Management Center	1280 x 720
Firepower Device Manager	1024 x 768
ASDM managing an ASA FirePOWER module	1024 x 768
Firepower Chassis Manager for Firepower 4100/9300 chassis	1024 x 768

Additional Compatibility Resources

This table provides links to release notes and additional compatibility information. For full documentation roadmaps, see Documentation Roadmaps, on page 71.

Table 8: Additional Compatibility Resources

Description	Resources
Compatibility guides provide detailed compatibility information for supported hardware models and software versions, including bundled components and integrated products.	Cisco Firepower Compatibility Guide Cisco ASA Compatibility Cisco Firepower 4100/9300 FXOS Compatibility
Release notes provide critical and release-specific information, including upgrade warnings and behavior changes.	Cisco Firepower Release Notes Cisco ASA Release Notes Cisco Firepower 4100/9300 FXOS Release Notes
Sustaining bulletins provide support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.	Cisco NGFW Product Line Software Release and Sustaining Bulletin



CHAPTER 3

Features and Functionality

Major releases provide new features, functionality, and enhancements to the Firepower software. Major versions can include deprecated features and platforms, menu and terminology changes, changed behavior, and so on.

Because deprecated features are the most likely to cause upgrade issues when skipping versions, the release notes provide historical information for deprecated features. For historical information on new features, read the release notes for the versions you are skipping.

- New Features in Firepower Management Center/Version 6.6.0, on page 9
- New Features in Firepower Device Manager/FTD Version 6.6.0, on page 17
- Deprecated Features, on page 23
- Deprecated FlexConfig Commands, on page 31
- FMC How-To Walkthroughs, on page 32

New Features in Firepower Management Center/Version 6.6.0

The following table lists the new and changed features in Firepower Version 6.6.0 when configured using a Firepower Management Center.

Table 9: Version 6.6.0 New Features: FMC Deployments

Feature	Description
Hardware and Virtual Hardware	
FTD on the 4112	We introduced the Firepower 4112. You can also deploy ASA logical devices on this platform. Requires FXOS 2.8.1.

Feature	Description
Larger instances for AWS deployments	FTDv for AWS adds support for these larger instances: • C5.xlarge • C5.2xlarge • C5.4xlarge FMCv for AWS adds support for these larger instances: • C3.4xlarge • C4.4xlarge • C5.4xlarge All existing FMCv for AWS instance types are now deprecated. You *must* resize your existing FMCv instances before you upgrade. For more information, see FMCv Requires 28 GB RAM for Upgrade, on page 36. Supported platforms: FMCv for AWS, FTDv for AWS
Autoscale for cloud-based FTDv deployments	Version 6.6.0 introduces support for AWS Auto Scale/Azure Autoscale. The serverless infrastructure in cloud-based deployments allow you to automatically adjust the number of FTDv instances in the Auto Scale group based on capacity needs. This includes automatic registering/unregistering to and from the managing FMC. Supported platforms: FTDv for AWS, FTDv for Azure
Firepower Threat Defense: Device Management	
Obtain initial management interface IP address using DHCP	For Firepower 1000/2000 series and ASA-5500-X series devices, the management interface now defaults to obtaining an IP address from DHCP. This change makes it easier for you to deploy a new device on your existing network. This feature is not supported for Firepower 4100/9300 chassis, where you set the IP address when you deploy the logical device. Nor is it supported for FTDv or the ISA 3000, which continue to default to 192.168.45.45. Supported platforms: Firepower 1000/2000 series, ASA-5500-X series
Configure MTU values in CLI	You can now use the FTD CLI to configure MTU (maximum transmission unit) values for FTD device interfaces. The default is 1500 bytes. Maximum MTU values are: • Management interface: 1500 bytes • Eventing interface: 9000 bytes New FTD CLI commands: **configure network mtu** Modified FTD CLI commands: Added the **mtu-event-channel** and **mtu-management-channel** keyword to the **configure network management-interface** command. Supported platforms: FTD

Feature	Description
Get upgrade packages from an internal web server	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades *to* Version 6.6.0, nor is it supported for the FMC or Classic devices. New/modified screens: **System > Updates > Upload Update** button **> Specify software update source** option Supported platforms: FTD
Connection-based troubleshooting enhancements	We made the following enhancements to FTD CLI connection-based troubleshooting (debugging): • **debug packet-module trace**: Added to enable module level packet tracing. • **debug packet-condition**: Modified to support troubleshooting of ongoing connections. Supported platforms: FTD
Firepower Threat Defense: Clustering	
Multi-instance clustering	You can now create a cluster using container instances. On the Firepower 9300, you must include one container instance on each module in the cluster. You cannot add more than one container instance to the cluster per security engine/module. We recommend that you use the same security module or chassis model for each cluster instance. However, you can mix and match container instances on different Firepower 9300 security module types or Firepower 4100 models in the same cluster if required. You cannot mix Firepower 9300 and 4100 instances in the same cluster. New FXOS CLI commands: **set port-type cluster** New/modified Firepower Chassis Manager screens: • **Logical Devices** > **Add Cluster** • **Interfaces** > **All Interfaces** > **Add New** drop-down menu **> Subinterface > Type** field Supported platforms: Firepower 4100/9300
Parallel configuration sync to data units in FTD clusters	The control unit in an FTD cluster now syncs configuration changes with slave units in parallel by default. Formerly, synching occurred sequentially. Supported platforms: Firepower 4100/9300
Messages for cluster join failure or eviction added to **show cluster history**	We added new messages to the **show cluster history** command for when a cluster unit either fails to join the cluster or leaves the cluster. Supported platforms: Firepower 4100/9300
Firepower Threat Defense: Routing	

Feature	Description
Virtual routers and VRF-Lite	You can now create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). The maximum number of virtual routers you can create ranges from five to 100, and depends on the device model. For a full list, see the Virtual Routing for Firepower Threat Defense chapter in the *Firepower Management Center Configuration Guide*. New/modified screens: **Devices > Device Management** > edit device > **Routing** tab New FTD CLI commands: **show vrf**. Modified FTD CLI commands: Added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. Supported platforms: FTD, except Firepower 1010 and ISA 3000
Firepower Threat Defense: VPN	
DTLS 1.2 in remote access VPN	You can now use Datagram Transport Layer Security (DTLS) 1.2 to encrypt RA VPN connections. Use FTD platform settings to specify the minimum TLS protocol version that the FTD device uses when acting as a, RA VPN server. If you want to specify DTLS 1.2, you must also choose TLS 1.2 as the minimum TLS version. Requires Cisco AnyConnect Secure Mobility Client, Version 4.7+. New/modified screens: **Devices > Platform Settings >** add/edit Threat Defense policy **> SSL > DTLS Version** option Supported platforms: FTD, except ASA 5508-X and ASA 5516-X
Site-to-site VPN IKEv2 support for multiple peers	You can now add a backup peer to a site-to-site VPN connection, for IKEv1 and IKEv2 point-to-point extranet and hub-and-spoke topologies. Previously, you could only configure backup peers for IKEv1 point-to-point topologies. New/modified screens: **Devices > VPN > Site to Site >** add or edit a point to point or hub and spoke FTD VPN topology > add endpoint > **IP Address** field now supports comma-separated backup peers Supported platforms: FTD
Security Policies	

Feature	Description
Usability enhancements for security policies	Version 6.6.0 makes it easier to work with access control and prefilter rules. You can now: • Edit certain attributes of multiple access control rules in a single operation: state, action, logging, intrusion policy, and so on. In the access control policy editor, select the relevant rules, right-click, and choose **Edit**. • Search access control rules by multiple parameters. In the access control policy editor, click the **Search Rules** text box to see your options. • View object details and usage in an access control or prefilter rule. In the access control or prefilter policy editor, right-click the rule and choose **Object Details**. Supported platforms: FMC
Object group search for access control policies	While operating, FTD devices expand access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your rules are defined or how they appear in the FMC. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. New/modified screens: **Devices** > **Device Management** > edit device > **Device** tab > **Advanced Settings** > **Object Group Search** option Supported platforms: FTD
Time-based rules in access control and prefilter policies	You can now specify an absolute or recurring time or time range for a rule to be applied. The rule is applied based on the time zone of the device that processes the traffic. New/modified screens: • Access control and prefilter rule editors • **Devices** > **Platform Settings** > add/edit Threat Defense policy > **Time Zone** • **Objects** > **Object Management** > **Time Range** and **Time Zone** Supported platforms: FTD

Feature	Description
Egress optimization re-enabled	Version 6.6.0 fixes CSCvs86257. If egress optimization was: • Enabled but turned off, the upgrade turns it back on. (We turned off egress optimization in some Version 6.4.0.x and 6.5.0.x patches, even if the feature was enabled.) • Manually disabled, we recommend you reenable it post-upgrade: **asp inspect-dp egress-optimization**. Supported platforms: FTD
Event Analysis	
New datastore improves performance	To improve performance, Version 6.6.0 uses a new datastore for connection and Security Intelligence events. After the upgrade finishes and the FMC reboots, historical connection and Security Intelligence events are migrated in the background. For more information, see Events Temporarily Unavailable After FMC Upgrade, on page 37. Supported platforms: FMC
Wildcard support when searching connection and Security Intelligence events for URLs	When searching connection and Security Intelligence events for URLs having the pattern `example.com`, you must now include wildcards. Specifically, use `*example.com*` for such searches. Supported platforms: FMC
Monitor up to 300,000 concurrent user sessions with FTD devices	In Version 6.6.0, some FTD device models support monitoring of additional concurrent user sessions (logins): • 300,000 sessions: Firepower 4130, 4140, 4150, 9300 • 150,000 sessions: Firepower 2140, 4120 All other devices continue to support the old limit of 64,000, except ASA FirePOWER which is limited to 2000. A new health module alerts you when the user identity feature's memory usage reaches a configurable threshold. You can also view a graph of the memory usage over time. New/modified screens: • **System** > **Health** > **Policy** > add or edit health policy > **Snort Identity Memory Usage** • **System** > **Health** > **Monitor** > select a device > **Graph** option for the Snort Identity Memory Usage module Supported platforms: Firepower 2140, 4120, 4130, 4140, 4150, 9300

Feature	Description
Integration with IBM QRadar	You can use the new Cisco Firepower app for IBM QRadar as an alternate way to display event data and help you analyze, hunt for, and investigate threats to your network. Requires eStreamer. For more information, see the Integration Guide for the Cisco Firepower App for IBM QRadar Supported platforms: FMC
Administration and Troubleshooting	
New options for deploying configuration changes	The **Deploy** button on the FMC menu bar is now a menu, with options that add the following functionality: • Status: For each device, the system displays whether changes need to be deployed; whether there are warnings or errors you should resolve before you deploy; and whether your last deploy is in process, failed, or completed successfully. • Preview: See all applicable policy and object changes you have made since you last deployed to the device. • Selective deploy: Choose from the policies and configurations you want to deploy to a managed device. • Deploy time estimate: Display an estimate of how long it will take to deploy to a particular device. You can display estimates for a full deploy, as well as for specific policies and configurations. • History: View details of previous deploys. New/modified screens: • **Deploy > Deployment** • **Deploy > Deployment History** Supported platforms: FMC
Initial configuration updates the VDB and schedules SRU updates	On new and reimaged FMCs, the setup process now: • Downloads and installs the latest vulnerability database (VDB) update. • Enables daily intrusion rule (SRU) downloads. Note that the setup process does *not* enable auto-deploy after these downloads, although you can change this setting. Upgraded FMCs are not affected. New/modified screens: • **System > Updates > Product Updates** (VDB updates) • **System > Updates > Rule Updates** (SRU updates) Supported platforms: FMC

Feature	Description
VDB match no longer required to restore FMC	Restoring an FMC from backup no longer requires the same VDB on the replacement FMC. However, restoring does now replace the existing VDB with the VDB in the backup file. Supported platforms: FMC
HTTPS certificates with subject alternative name (SAN)	You can now request a HTTPS server certificate that secures multiple domain names or IP addresses by using SAN. For more information on SAN, see RFC 5280, section 4.2.1.6. New/modified screens: **System > Configuration > HTTPS Certificate > Generate New CSR > Subject Alternative Name** fields Supported platforms: FMC
Real names associated with FMC user accounts	You can now specify a real name when you create or modify an FMC user account. This can be a person's name, department, or other identifying attribute. New/modified screens: **System > Users > Users > Real Name** field. Supported platforms: FMC
Usability	
FMC web interface Light theme	The FMC now defaults to the Light theme, which was introduced as an experimental feature in Version 6.5.0. Upgrading to Version 6.6.0 automatically switches you to the Light theme. You can switch back to the Classic theme in your user preferences. Although we cannot respond to everybody, we welcome feedback on the Light theme. Use the feedback link on the User Preferences page or contact us at fmc-light-theme-feedback@cisco.com. Supported platforms: FMC
Display time remaining for upgrades	The FMC's Message Center now displays approximately how much time remains until an upgrade will complete. This does not include reboot time. New/modified screens: Message Center Supported platforms: FMC
Security and Hardening	
Default HTTPS server certificate renewals have 800 day lifespans	Unless the current *default* HTTPS server certificate already has an 800-day lifespan, upgrading to Version 6.6.0 renews the certificate, which now expires 800 days from the date of the upgrade. All future renewals have an 800 day lifespan. Your old certificate was set to expire depending on when it was generated. Supported platforms: FMC
FMC REST API	

Feature	Description
New REST API capabilities	Added the following REST API services to support Version 6.6.0 features: • bgp, bgpgeneralsettings, ospfinterface, ospfv2routes, ospfv3interfaces, ospfv3routes, virtualrouters, routemaps, ipv4prefixlists, ipv6prefixlists, aspathlists, communitylists, extendedcommunitylists, standardaccesslists, standardcommunitylists, policylists: Routing • virtualrouters, virtualipv4staticroutes, virtualipv6staticroutes, virtualstaticroutes: Virtual routing • timeranges, globaltimezones, timezoneobjects: Time-based rules • commands: Run a limited set of CLI commands from the REST API • pendingchanges: Deploy improvements Added the following REST API services to support older features: • intrusionrules, intrusionpolicies: Intrusion policies Supported platforms: FMC
Changed REST API service name for extended access lists	The extendedaccesslist (singular) service in the FMC REST API is now extendedaccesslist**s** (plural). Make sure you update your client. Using the old service name fails and returns an Invalid URL error. Request Type: GET URL to retrieve the extended access list associated with a specific ID: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist/{objectId} • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s**/{objectId} URL to retrieve a list of all extended access lists: • Old: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist • New: /api/fmc_config/v1/domain/{domainUUID}/object/extendedaccesslist**s** Supported platforms: FMC

New Features in Firepower Device Manager/FTD Version 6.6.0

Released: April 6, 2020

The following table lists the new features available in FTD 6.6.0 when configured using Firepower Device Manager.

Feature	Description
Platform Features	
FDM support for Firepower Threat Defense Virtual for the Amazon Web Services (AWS) Cloud.	You can configure Firepower Threat Defense on Firepower Threat Defense Virtual for the AWS Cloud using Firepower Device Manager.
FDM for the Firepower 4112	We introduced the FTD for the Firepower 4112. **Note** Requires FXOS 2.8.1.
Firewall and IPS Features	
Ability to enable intrusion rules that are disabled by default.	Each system-defined intrusion policy has a number of rules that are disabled by default. Previously, you could not change the action for these rules to alert or drop. You can now change the action for rules that are disabled by default. We changed the Intrusion Policy page to display all rules, even those that are disabled by default, and allow you to edit the action for these rules.
Intrusion Detection System (IDS) mode for the intrusion policy.	You can now configure the intrusion policy to operate in Intrusion Detection System (IDS) mode. In IDS mode, active intrusion rules issue alerts only, even if the rule action is Drop. Thus, you can monitor or test how an intrusion policy works before you make it an active prevention policy in the network. In FDM, we added an indication of the inspection mode to each intrusion policy on the **Policies** > **Intrusion** page, and an **Edit** link so that you can change the mode. In the FTD API, we added the inspectionMode attribute to the IntrusionPolicy resource.
Support for manually uploading Vulnerability Database (VDB), Geolocation Database, and Intrusion Rule update packages.	You can now manually retrieve update packages for VDB, Geolocation Database, and Intrusion Rules, and then upload them from your workstation to the FTD device using FDM. For example, if you have an air-gapped network, where FDM cannot retrieve updates from the Cisco Cloud, you can now get the update packages you need. We updated the **Device** > **Updates** page to allow you to select and upload a file from your workstation.
FTD API support for access control rules that are limited based on time.	Using the FTD API, you can create time range objects, which specify one-time or recurring time ranges, and apply these objects to access control rules. Using time ranges, you can apply an access control rule to traffic during certain times of day, or for certain periods of time, to provide flexibility to network usage. You cannot use FDM to create or apply time ranges, nor does FDM show you if an access control rule has a time range applied to it. The TimeRangeObject, Recurrence, TimeZoneObject, DayLightSavingDateRange, and DayLightSavingDayRecurrence resources were added to the FTD API. The timeRangeObjects attribute was added to the accessrules resource to apply a time range to the access control rule. In addition, there were changes to the GlobalTimeZone and TimeZone resources.

Feature	Description
Object group search for access control policies.	While operating, the FTD device expands access control rules into multiple access control list entries based on the contents of any network objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in Firepower Device Manager. It impacts only how the device interprets and processes them while matching connections to access control rules. Object group search is disabled by default. In Firepower Device Manager, you must use FlexConfig to enable the **object-group-search access-control** command.
VPN Features	
Backup peer for site-to-site VPN. (FTD API only.)	You can use the FTD API to add a backup peer to a site-to-site VPN connection. For example, if you have two ISPs, you can configure the VPN connection to fail over to the backup ISP if the connection to the first ISP becomes unavailable. Another main use of a backup peer is when you have two different devices on the other end of the tunnel, such as a primary-hub and a backup-hub. The system would normally establish the tunnel to the primary hub. If the VPN connection fails, the system automatically can re-establish the connection with the backup hub. We updated the FTD API so that you can specify more than one interface for outsideInterface in the SToSConnectionProfile resource. We also added the BackupPeer resource, and the remoteBackupPeers attribute to the SToSConnectionProfile resource. You cannot configure a backup peer using FDM, nor will the existence of a backup peer be visible in FDM.
Support for Datagram Transport Layer Security (DTLS) 1.2 in remote access VPN.	You can now use DTLS 1.2 in remote access VPN. This can be configured using the FTD API only, you cannot configure it using FDM. However, DTLS 1.2 is now part of the default SSL cipher group, and you can enable the general use of DTLS using FDM in the AnyConnect attributes of the group policy. Note that DTLS 1.2 is not supported on the ASA 5508-X or 5516-X models. We updated the protocolVersion attribute of the sslcipher resource to accept DTLSV1_2 as an enum value.
Deprecated support for less secure Diffie-Hellman groups, and encryption and hash algorithms.	The following features are deprecated and will be removed in a future release. You should avoid configuring these features in IKE proposals or IPSec policies for use in VPNs. Please transition away from these features and use stronger options as soon as is practical. • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5.

Feature	Description
Routing Features	
Virtual routers and Virtual Routing and Forwarding (VRF)-Lite.	You can create multiple virtual routers to maintain separate routing tables for groups of interfaces. Because each virtual router has its own routing table, you can provide clean separation in the traffic flowing through the device. Virtual routers implement the "light" version of Virtual Routing and Forwarding, or VRF-Lite, which does not support Multiprotocol Extensions for BGP (MBGP). We changed the **Routing** page so you can enable virtual routers. When enabled, the **Routing** page shows a list of virtual routers. You can configure separate static routes and routing processes for each virtual router. We also added the [**vrf** *name* | **all**] keyword set to the following CLI commands, and changed the output to indicate virtual router information where applicable: **clear ospf**, **clear route**, **ping**, **show asp table routing**, **show bgp**, **show ipv6 route**, **show ospf**, **show route**, **show snort counters**. We added the following command: **show vrf**.
OSPF and BGP configuration moved to the Routing pages.	In previous releases, you configured OSPF and BGP in the Advanced Configuration pages using Smart CLI. Although you still configure these routing processes using Smart CLI, the objects are now available directly on the Routing pages. This makes it easier for you to configure processes per virtual router. The OSPF and BGP Smart CLI objects are no longer available on the Advanced Configuration page. If you configured these objects before upgrading to 6.6, you can find them on the Routing page after upgrade.
High Availability Features	
The restriction for externally authenticated users logging into the standby unit of a high availability (HA) pair has been removed.	Previously, an externally-authenticated user could not directly log into the standby unit of an HA pair. The user first needed to log into the active unit, then deploy the configuration, before login to the standby unit was possible. This restriction has been removed. Externally-authenticated users can log into the standby unit even if they never logged into the active unit, so long as they provide a valid username/password.

Feature	Description
Change to how interfaces are handled by the BreakHAStatus resource in the FTD API.	Previously, you could include the **clearIntfs** query parameter to control the operational status of the interfaces on the device where you break the high availability (HA) configuration. Starting with version 6.6, there is a new attribute, **interfaceOption**, which you should use instead of the clearIntfs query parameter. This attribute is optional when used on the active node, but required when used on a non-active node. You can choose from one of two options: • DISABLE_INTERFACES (the default)—All data interfaces on the standby device (or this device) are disabled. • ENABLE_WITH_STANDBY_IP—If you configured a standby IP address for an interface, the interface on the standby device (or this device) is reconfigured to use the standby address. Any interface that lacks a standby address is disabled. If you use break HA on the active node when the devices are in a healthy active/standby state, this attribute applies to the interfaces on the standby node. In any other state, such as active/active or suspended, the attribute applies to the node on which you initiate the break. If you do use the clearIntfs query parameter, clearIntfs=true will act like interfaceOption = DISABLE_INTERFACES. This means that breaking an active/standby pair with clearIntfs=true will no longer disable both devices; only the standby device will be disabled. When you break HA using FDM, the interface option is always set to DISABLE_INTERFACES. You cannot enable the interfaces with the standby IP address. Use the API call from the API Explorer if you want a different result.
The last failure reason for High Availability problems is now displayed on the High Availability page.	If High Availability (HA) fails for some reason, such as the active device becoming unavailable and failing over to the standby device, the last reason for failure is now shown below the status information for the primary and secondary device. The information includes the UTC time of the event.
Interface Features	
PPPoE Support	You can now configure PPPoE for routed interfaces. PPPoE is not supported on High Availability units. New/Modified screens: **Device** > **Interfaces** > **Edit** > **IPv4 Address** > **Type** > **PPPoE** New/Modified commands: **show vpdn group, show vpdn username, show vpdn session pppoe state**
Management Interface acts as a DHCP client by default	The Management interface now defaults to obtaining an IP address from DHCP instead of using the 192.168.45.45 IP address. This change makes it easier for you to deploy an FTD in your existing network. This feature applies to all platforms except for the Firepower 4100/9300 (where you set the IP address when you deploy the logical device), and the Firepower Threat Defense Virtual and ISA 3000 (which still use the 192.168.45.45 IP address). The DHCP server on the Management interface is also no longer enabled. You can still connect to the default inside IP address by default (192.168.1.1).

Feature	Description
HTTP proxy support for FDM management connections.	You can now configure an HTTP proxy for the management interface for use with FDM connections. All management connections, including manual and scheduled database updates, go through the proxy. We added the **System Settings** > **HTTP Proxy** page to configure the setting. In addition, we added the HTTPProxy resource to the FTD API.
Set the MTU for the Management interface	You can now set the MTU for the Management interface up to 1500 bytes. The default is 1500 bytes. New/Modified commands: **configure network mtu, configure network management-interface mtu-management-channel** No modified screens.
Licensing Features	
Smart Licensing and Cloud Services enrollment are now separate, and you can manage your enrollments separately.	You can now enroll for cloud services using your security account rather than your Smart Licensing account. Enrolling using the security account is the recommended approach if you intend to manage the device using Cisco Defense Orchestrator. You can also unregister from cloud services without unregistering from Smart Licensing. We changed how the **System Settings** > **Cloud Services** page behaves, and added the ability to unregister from cloud services. In addition, the Web Analytics feature was removed from the page and you can now find it at **System Settings** > **Web Analytics**. In the FTD API, the CloudServices resources were modified to reflect the new behavior.
Support for Permanent License Reservation.	If you have an air-gapped network, where there is no path to the internet, you cannot register directly with the Cisco Smart Software Manager (CSSM) for Smart Licensing. In this situation, you can now get authorization to use Universal Permanent License Reservation (PLR) mode, where you can apply a license that does not need direct communication with CSSM. If you have an air-gapped network, please contact your account representative and ask for authorization to use Universal PLR mode in your CSSM account, and to obtain the necessary licenses. We added the ability to switch to PLR mode, and to cancel and unregister a Universal PLR license, to the **Device** > **Smart License** page. In the FTD API, there are new resources for PLRAuthorizationCode, PLRCode, PLRReleaseCode, PLRRequestCode, and actions for PLRRequestCode, InstallPLRCode, and CancelReservation.
Administrative and Troubleshooting Features	
FDM direct support for Precision Time Protocol (PTP) configuration for ISA 3000 devices.	You can use FDM to configure the Precision Time Protocol (PTP) on ISA 3000 devices. PTP is a time-synchronization protocol developed to synchronize the clocks of various devices in a packet-based network. The protocol is designed specifically for industrial, networked measurement and control systems. In previous releases, you had to use FlexConfig to configure PTP. We grouped PTP with NTP on the same System Settings page, and renamed the **System Settings** > **NTP** page to **Time Services**. We also added the PTP resource to the FTD API.

Feature	Description
Trust chain validation for the FDM management web server certificate.	When you configure a non-self-signed certificate for the FDM web server, you now need to include all intermediate certificates, and the root certificate, in the trust chain. The system validates the entire chain. We added the ability to select the certificates in the chain on the **Management Web Server** tab on the **Device** > **System Settings** > **Management Access** page.
Support for encrypting backup files.	You can now encrypt backup files using a password. To restore an encrypted backup, you must supply the correct password. We added the ability to choose whether to encrypt backup files for recurring, scheduled, and manual jobs, and to supply the password on restore, to the **Device** > **Backup and Restore** page. We also added the encryptArchive and encryptionKey attributes to the BackupImmediate and BackupSchedule resources, and encryptionKey to the RestoreImmediate resource in the FTD API.
Support for selecting which events to send to the Cisco cloud for use by cloud services.	When you configure the device to send events to the Cisco cloud, you can now select which types of events to send: intrusion, file/malware, and connection. For connection events, you can send all events or just the high-priority events, which are those related to connections that trigger intrusion, file, or malware events, or that match Security Intelligence blocking policies. We changed how the Send Events to the Cisco Cloud Enable button works. The feature is on the **System Settings** > **Cloud Services** page.
FTD REST API version 5 (v5).	The FTD REST API for software version 6.6 has been incremented to version 5. You must replace v1/v2/v3/v4 in the API URLs with v5, or preferentially, use /latest/ to signify you are using the most recent API version that is supported on the device. The v5 API includes many new resources that cover all features added in software version 6.6. Please re-evaluate all existing calls, as changes might have been mode to the resource models you are using. To open the API Explorer, where you can view the resources, log into FDM, then click the more options button (⋮) and choose **API Explorer**.

Deprecated Features

Deprecated features can prevent upgrade or require pre- or post-upgrade configuration changes. If your upgrade path skips versions, review the deprecated features for intermediate releases.



Note Version 6.6.0 is the last major release that will support the Cisco Firepower User Agent software as an identity source. You will not be able to further upgrade FMCs with user agent configurations. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC) now. This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact Sales.

For more information, see the appropriate *Cisco Firepower User Agent Configuration Guide* on the Cisco Firepower Management Center Configuration Guides page.

Version 6.6.0 Deprecated Features

These features were deprecated in Version 6.6.0.

Table 10: Version 6.6.0 Deprecated Features

Feature	Description
Lower-memory instances for cloud-based FMCv deployments	For performance reasons, the following FMCv instances are no longer supported: • c3.xlarge on AWS • c3.2xlarge on AWS • c4.xlarge on AWS • c4.2xlarge on AWS • Standard_D3_v2 on Azure You must resize before you upgrade to Version 6.6.0+. For more information, see FMCv Requires 28 GB RAM for Upgrade, on page 36. **Note** As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances. Affected platforms: FMCv on AWS or Azure
e1000 Interfaces on FTDv for VMware	Version 6.6.0 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device. For more information, see the Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide. Affected platforms: FTDv for VMware

Feature	Description
Less secure Diffie-Hellman groups, and encryption and hash algorithms	Version 6.6.0 deprecates the following features: • Diffie-Hellman groups: 2, 5, and 24. • Encryption algorithms for users who satisfy export controls for strong encryption: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256. DES continues to be supported (and is the only option) for users who do not satisfy export controls. • Hash algorithms: MD5. These features will be removed in a future release. Avoid configuring them in IKE proposals or IPSec policies for use in VPNs. Change to stronger options as soon as possible. Affected platforms: FTD
Custom tables for connection events	Version 6.6.0 ends support for custom tables for connection and Security Intelligence events. After you upgrade, existing custom tables for those events are still 'available' but return no results. We recommend you delete them. There is no change to other types of custom tables. Deprecated options: • **Analysis > Advanced > Custom Tables >** click **Create Custom Table > Tables** drop-down list **> Connection Events** and **Security Intelligence Events** Affected platforms: FMC
Ability to delete connection events from the event viewer	Version 6.6.0 ends support for deleting connection and Security Intelligence events from the event viewer. To purge the database, select **System** > **Tools** > **Data Purge.** Deprecated options: • **Analysis** > **Connections** > **Events > Delete** and **Delete All** • **Analysis** > **Connections** > **Security Intelligence Events > Delete** and **Delete All** Affected platforms: FMC

Version 6.5.0 Deprecated Features

These features were deprecated in Version 6.5.0.

Table 11: Version 6.5.0 Deprecated Features

Feature	Description
Ability to disable the FMC CLI	Version 6.3.0 introduced the FMC CLI, which you had to explicitly enable. In Version 6.5.0, the FMC CLI is automatically enabled, for both new and upgraded deployments. If you want to access the Linux shell (also called *expert mode*), you must log in to the CLI and then use the **expert** command. **Caution** We recommend you do not access Firepower appliances using the shell, unless directed by Cisco TAC. Deprecated options: **System > Configuration > Console Configuration > Enable CLI access** check box Affected platforms: FMC
TLS 1.0 & 1.1	To enhance security: • Captive portal (active authentication) has removed support for TLS 1.0. • Host input has removed support for TLS 1.0 and TLS 1.1. If your client fails to connect with a Firepower appliance, we recommend you upgrade your client to support TLS 1.2. Affected platforms: FMC
TLS crypto acceleration FXOS CLI commands for Firepower 4100/9300	As part of allowing TLS crypto acceleration for multiple container instances on Firepower 4100/9300, we removed the following FXOS CLI commands: • **show hwCrypto** • **config hwCrypto** And this FTD CLI command: • **show crypto accelerator status** For information on their replacements, see the new feature documentation. Affected platforms: Firepower 4100/9300

Feature	Description
Cisco Security Packet Analyzer integration	Version 6.5.0 ends support for FMC integration with Cisco Security Packet Analyzer. Deprecated screens/options: • **System > Integration > Packet Analyzer** • **Analysis > Advanced > Packet Analyzer Queries** • **Query Packet Analyzer** when right-clicking on an event in the dashboard or event viewer Affected platforms: FMC
Default HTTPS server certificates	If you are upgrading from Version 6.4.0.9+, the *default* HTTPS server certificate's lifespan-on-renew returns to 3 years, but this is again updated to 800 days in Version 6.6.0+. Your current default HTTPS server certificate is set to expire depending on when it was generated, as follows: • 6.4.0.9 and later patches: 800 days • 6.4.0 to 6.4.0.8: 3 years • 6.3.0 and all patches: 3 years • 6.2.3: 20 years Supported platforms: FMC/FMCv, FDM
Firepower Management Center models FMC 750, 1500, 3500	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower Management Center software on the FMC 750, FMC 1500, and FMC 3500 models. You cannot manage Version 6.5.0+ devices with these FMCs.
ASA 5515-X and ASA 5585-X series devices with Firepower software	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software (both FTD and ASA FirePOWER) on these models: • ASA 5515-X • ASA 5585-X-SSP-10, -20, -40, -60 You can, however, manage older devices with a newer FMC.
Firepower 7000/8000 series devices	You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software on Firepower 7000/8000 series devices, including AMP models. You can, however, manage older devices with a newer FMC.

Version 6.4.0 Deprecated Features

These features were deprecated in Version 6.4.0.

Table 12: Version 6.4.0 Deprecated Features

Feature	Description
SSL hardware acceleration FTD CLI commands	As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands: • **system support ssl-hw-accel enable** • **system support ssl-hw-accel disable** • **system support ssl-hw-status** For information on their replacements, see the new feature documentation. Affected platforms: FTD
FMC menu changes	These FMC pages have changed location in Version 6.4.0. **System** > **Integration** > **Cloud Services** is now **System** > **Integration** > **Cisco CSI**

Version 6.3.0 Deprecated Features

These features were deprecated in Version 6.3.0.

Table 13: Version 6.3.0 Deprecated Features

Feature	Description
EMS extension support for decryption	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. Support is reintroduced in Version 6.3.0.1. Affected platforms: Any
Decryption on passive and inline tap Interfaces	Version 6.3.0 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. Any inspection of encrypted traffic is necessarily limited. Affected platforms: Any

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

Feature	Description
FlexConfig commands for FTD with FDM	Version 6.3.0 deprecates the following FlexConfig commands for FTD FDM: • **access-list**: You can now create **extended** and **standard** access lists using the Smart CLI Extended Access List or Standard Access List objects. You can then use them on FlexConfig-supported commands that refer to the ACL by object name, such as **match access-list** with an extended ACL for service policy traffic classes. • **as-path**: You can now create Smart CLI AS Path objects and use them in a Smart CLI BGP object to configure an autonomous system path filter. • **community-list**: You can now create Smart CLI Expanded Community List or Standard Community List objects and use them in a Smart CLI BGP object to configure a community list filter. • **dns-group**: You can now configure DNS groups using **Objects** > **DNS Groups**, and assign the groups using **Device** > **System Settings** > **DNS Server**. • **policy-list**: You can now create Smart CLI Policy List objects and use them in a Smart CLI BGP object to configure a policy list. • **prefix-list**: You can now create Smart CLI IPv4 Prefix List objects and use them in a Smart CLI OSPF or BGP object to configure prefix list filtering for IPv4. • **route-map**: You can now create Smart CLI Route Map objects and use them in a Smart CLI OSPF or BGP object to configure route maps. • **router bgp**: You can now use the Smart CLI templates for BGP. Affected platforms: FTD with FDM

Feature	Description
FMC menu options	Version 6.3.0 changes these menu options: **Analysis > Advanced > Whois** is now **Analysis > Lookup > Whois** **Analysis > Advanced > Geolocation** is now **Analysis > Lookup > Geolocation** **Analysis > Advanced > URL** is now **Analysis > Lookup > URL** **Analysis > Advanced > Custom Workflows** is now **Analysis > Custom > Custom Workflows** **Analysis > Advanced > Custom Tables** is now **Analysis > Custom > Custom Tables** **Analysis > Hosts > Vulnerabilities** is now **Analysis > Vulnerabilities > Vulnerabilities** **Analysis > Hosts > Third-Party Vulnerabilities** is now **Analysis > Vulnerabilities > Third-Party Vulnerabilities** Affected platforms: FMC
VMware 5.5 hosting	Version 6.3.0+ 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. Affected platforms: FMCv, FTDv, and NGIPSv for VMware
ASA 5506-X series and ASA 5512-X devices with Firepower software	You cannot upgrade to or freshly install Version 6.3.0+ of the Firepower software (both FTD and ASA FirePOWER) on these models: • ASA 5506-X, 5506H-X, 5506W-X • ASA 5512-X You can, however, manage older devices with a newer FMC.

Deprecated FlexConfig Commands

The release notes list deprecated FlexConfig objects and commands along with the other deprecated features for each version, in Deprecated Features, on page 23.

For a full list of prohibited commands, including those prohibited when FlexConfig was introduced, see your configuration guide.

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

About FlexConfig

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

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

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

FMC How-To Walkthroughs

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

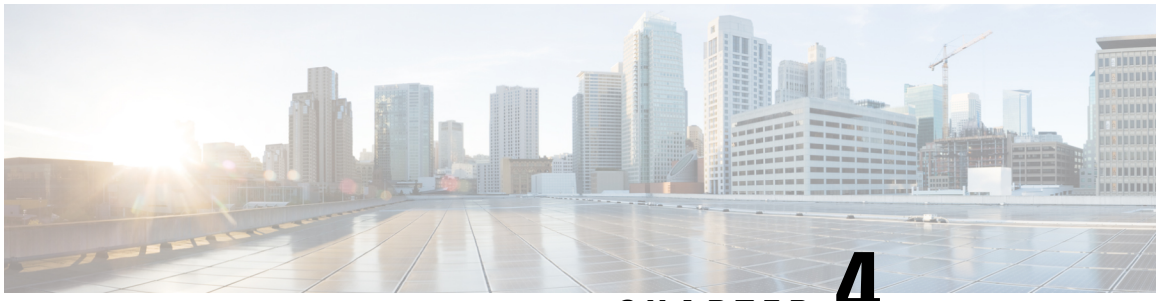
Note FMC walkthroughs are tested on the Firefox and Chrome browsers. If you encounter issues with a different browser, we ask that you switch to Firefox or Chrome. If you continue to encounter issues, contact Cisco TAC.

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

Table 14: Troubleshooting Walkthroughs

Problem	Solution
Cannot find the **How To** link to start walkthroughs.	Make sure walkthroughs are enabled. From the drop-down list under your username, select **User Preferences** then click **How-To Settings**.
Walkthrough appears when you do not expect it.	If a walkthrough appears when you do not expect it, end the walkthrough.
Walkthrough disappears or quits suddenly.	If a walkthrough disappears: • Move your pointer. Sometimes the FMC stops displaying an in-progress walkthrough. For example, pointing to a different top-level menu can make this happen. • Navigate to a different page and try again. If moving your pointer does not work, the walkthrough may have quit.

Problem	Solution
Walkthrough is out of sync with the FMC: • Starts on the wrong step. • Advances prematurely. • Will not advance.	If a walkthrough is out of sync, you can: • Attempt to continue. For example, if you enter an invalid value in a field and the FMC displays an error, the walkthrough can prematurely move on. You may need to go back and resolve the error to complete the task. • End the walkthrough, navigate to a different page, and try again. Sometimes you cannot continue. For example, if you do not click **Next** after you complete a step, you may need to end the walkthrough.



CHAPTER 4

Upgrade to Version 6.6.0

This chapter provides critical and release-specific information.

- Guidelines and Warnings for Version 6.6.0, on page 35
- Previously Published Guidelines and Warnings, on page 37
- General Guidelines and Warnings, on page 47
- Minimum Version to Upgrade, on page 50
- Time Tests and Disk Space Requirements, on page 50
- Traffic Flow, Inspection, and Device Behavior, on page 52
- Upgrade Instructions, on page 59
- Upgrade Packages, on page 59

Guidelines and Warnings for Version 6.6.0

This checklist contains important upgrade guidelines and warnings that are new or specific to this major version.

Table 15: Version 6.6.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	FMCv Requires 28 GB RAM for Upgrade, on page 36	FMCv	6.2.3 through 6.5.0.x	6.6.0+
	Events Temporarily Unavailable After FMC Upgrade, on page 37	FMC	6.2.3 through 6.5.0.x	6.6.0+

To avoid upgrade failure, review these additional guidelines and warnings.

Table 16: Additional Upgrade Guidelines and Warnings

✓	Resource	Details
	Previously Published Guidelines and Warnings, on page 37	Read these if your upgrade skips versions.
	General Guidelines and Warnings, on page 47	Read these even if you are familiar with the upgrade process, as guidelines may have changed.

✓	Resource	Details
	Known Issues, on page 81	Read these and be prepared to work around any bugs that affect upgrade.
	Features and Functionality, on page 9	Read these for additional items that may affect upgrade. If your upgrade skips versions, you should also read the new feature documentation for the versions you skipped, in the Cisco Firepower Release Notes. **Note** Deprecated features especially can require pre-upgrade configuration changes.

FMCv Requires 28 GB RAM for Upgrade

Deployments: FMCv

Upgrading from: Version 6.2.3 through 6.5.0.x

Directly to: Version 6.6.0+

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

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



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

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

Table 17: FMCv Memory Requirements for Version 6.6.0+ Upgrades

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

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

Events Temporarily Unavailable After FMC Upgrade

Deployments: FMC

Upgrading from: Version 6.2.3 through 6.5.0.x

Directly to: Version 6.6.0+

Version 6.6.0 uses a new datastore for connection and Security Intelligence events.

After the upgrade finishes and the FMC reboots, historical connection and Security Intelligence events are migrated in the background, resource constrained. Depending on FMC model, system load, and how many events you have stored, this can take from a few hours up to a day.

Historical events are migrated by age, newest events first. Events that have not been migrated do not appear in query results or dashboards. If you reach the connection event database limit before the migration completes, for example, because of post-upgrade events, the oldest historical events are not migrated.

Tip Monitor event migration progress in the Message Center by clicking the System Status icon on the menu bar.

Previously Published Guidelines and Warnings

These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips versions.

Table 18: Version 6.6.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 38	Firepower 1000 series	6.4.0.x	6.5.0+
	Historical Data Removed During FTD/FDM Upgrade, on page 39	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 39	Any	6.2.3 through 6.4.0.x	6.5.0+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 45	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+
	Readiness Check May Fail on FMC, NGIPSv, on page 45	FMC Firepower 7000/8000 series NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 45	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 46	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 46	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 47	Any	6.1.0 through 6.2.3.x	6.3.0+

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

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

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

Historical Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.3 through 6.4.x

Directly to: 6.5.0+

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

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Cisco Talos Intelligence Group (Talos) has introduced new categories and renamed reputations to classify and filter URLs. For detailed lists of category changes, see the Cisco Firepower Release Notes, Version 6.5.0. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

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

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

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

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

- *Reputationless URLs* can belong to any category.

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

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

Table 19: Deployment Changes on Upgrade

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

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 20: Pre-Upgrade Actions

Action	Details

Make sure your appliances can reach Talos resources.	The system must be able to communicate with the following Cisco resources after the upgrade:
	• https://regsvc.sco.cisco.com/ — Registration
	• https://est.sco.cisco.com/ — Obtain certificates for secure communications
	• https://updates-talos.sco.cisco.com/ — Obtain client/server manifests
	• http://updates.ironport.com/ — Download database (note: uses port 80)
	• https://v3.sds.cisco.com/ — Cloud queries
	The cloud query service also uses the following IP address blocks:
	• IPv4 cloud queries:
	  • 146.112.62.0/24
	  • 146.112.63.0/24
	  • 146.112.255.0/24
	  • 146.112.59.0/24
	• IPv6 cloud queries:
	  • 2a04:e4c7:ffff::/48
	  • 2a04:e4c7:fffe::/48

Identify potential rule issues.	Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section). **Note** You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade. In FMC deployments, we recommend you generate an *access control policy report*, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose **Policies** > **Access Control** , then click the report icon () next to the appropriate policy.

Post-Upgrade Actions for URL Categories and Reputations

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

Table 21: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 42. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

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

Table 22: Guidelines for Rules with Merged URL Categories

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

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

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

Table 23: Examples of Rules with Merged URL Categories

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

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

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

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

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

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

Readiness Check May Fail on FMC, NGIPSv

Deployments: FMC, NGIPSv

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

Directly to: Version 6.3.0+

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

Table 24: Patches with Readiness Checks for Version 6.3.0+

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

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

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

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

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

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

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

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

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

To disable discovery you must:

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

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

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

Directly to: Version 6.3.0+

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

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

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

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

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

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

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

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

General Guidelines and Warnings

These important guidelines and warnings apply to every upgrade. However, this list is not comprehensive. For links to additional important information on the upgrade process, which can include planning upgrade paths, OS upgrades, readiness checks, backups, maintenance windows, and so on, see Upgrade Instructions, on page 59.

Back Up Event and Configuration Data

When supported, we strongly recommend you back up both before and after upgrade:

- Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly.
- After upgrade: This creates a snapshot of your freshly upgraded deployment. We recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

You should back up to a secure remote location and verify transfer success. Upgrades purge locally stored backups. And especially because backup files are unencrypted, do not allow unauthorized access. If backup files are modified, the restore process will fail.

As the first step in any backup, note the appliance model and version, including patch level. For FMCs running Version 6.5.0.x and earlier, note the VDB version. For Firepower 4100/9300 chassis, note the FXOS version. This is important because if you need to restore the backup to a new or reimaged appliance, you may need to update the new appliance first.

Note Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. Careful planning and preparation can help you avoid missteps. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your Firepower product.

Verify NTP Synchronization

Before you upgrade, make sure Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the Time Synchronization Status health module does alert if clocks are out of sync by more than 10 seconds, but you should still check manually.

To check time:

- FMC: Choose **System > Configuration > Time**.
- Devices: Use the **show time** CLI command.

Check Bandwidth

To upgrade a Firepower appliance (or perform a readiness check), the upgrade package must be on the appliance. Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers.

In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. We recommend you manually push (copy) Firepower upgrade packages to managed devices before you upgrade, either from the FMC or, for FTD devices, from your own internal web server. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Appliance Access

Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.

Signed Upgrade Packages

So that Firepower can verify that you are using the correct files, upgrade and hotfix packages are *signed* archives. Do not untar signed (.tar) packages.

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

Disable ASA REST API on ASA FirePOWER Devices

Before you upgrade an ASA FirePOWER module, make sure the ASA REST API is disabled. Otherwise, the upgrade could fail. From the ASA CLI: `no rest api agent`. You can reenable after the uninstall: `rest-api agent`.

Sharing Data with Cisco

Some features involve sharing data with Cisco.

In Version 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support. During upgrades, you may be asked to accept or decline participation. You can also opt in or out at any time.

In Version 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs. Major upgrades enable web analytics tracking, even if your current setting is to opt out. If you do not want Cisco to collect this data, opt out after each major upgrade.

In Version 6.5.0+, *Cisco Support Diagnostics* (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case. During upgrades, you may be asked to accept or decline participation. You can also opt in or out at any time.

Upgrades Can Import and Auto-Enable Intrusion Rules

If a newer intrusion rule uses keywords that are not supported in your current Firepower version, that rule is not imported when you update the intrusion rule database (SRU).

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

Supported keywords depend on the Snort version included with your Firepower software:

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

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

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

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.

Minimum Version to Upgrade

You can upgrade directly to Version 6.6.0 as follows. You do not need to be running any specific maintenance release or patch level.

Table 25: Minimum Version to Upgrade Firepower Software to Version 6.6.0

Platform	Minimum Version
Firepower Management Center	6.2.3
Firepower Threat Defense	6.2.3 FXOS 2.8.1.105+ required for Firepower 4100/9300.
ASA FirePOWER with FMC	6.2.3
ASA FirePOWER with ASDM	6.3.0 Due to CSCvu50400, you should not upgrade ASA FirePOWER with ASDM directly from Version 6.2.3.x to 6.6.0. Although the upgrade will succeed, you will experience significant performance issues and must contact Cisco TAC for a fix. You should instead upgrade to any intermediate release, then to Version 6.6.0.

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 reports of in-house time and disk space tests for reference purposes.

About Time Tests

Time values given here are based on in-house tests.



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

Test Conditions

- Deployment: Values 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.
- Versions: For major upgrades, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version.

- Models: In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
- Virtual settings: We test with the default settings for memory and resources.
- High availability and scalability: We test on standalone devices.

  In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
- Configurations: We test on appliances with minimal configurations and traffic load.

  Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.

Time Is For Upgrade Only

Values represent only the time it takes for the Firepower upgrade script to run on each platform. They do *not* include time for:

- Transferring upgrade packages to managed devices, whether before or during upgrade.
- Readiness checks.
- VDB and SRU updates.
- Deploying configurations.
- Reboots (values may be provided separately).

About Disk Space Requirements

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

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

Version 6.6.0 Time and Disk Space



Note For ASA 5545-X with FirePOWER Services, if the SRU on the device is the *same as* or *newer than* the SRU in the Version 6.6.0 upgrade package (2020-01-16-001-vrt), the upgrade can take longer than expected—more than an hour longer. To determine if this will affect you, log into the Firepower CLI on the device and use the **show version** command to display the **Rules update version**.

Table 26: Version 6.6.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	16.5 GB	71 MB	—	46 min	15 min
FMCv: VMware 6.0	16.7 GB	57 MB	—	36 min	7 min
Firepower 1000 series	410 MB	11.5 GB	1.1 GB	20 min	17 min
Firepower 2100 series	470 MB	10.3 GB	1 GB	14 min	14 min
Firepower 4100 series	61 MB	9.3 GB	980 MB	11 min	9 min
Firepower 4100 series container instance	46 MB	11.3 GB	980 MB	11 min	6 min
Firepower 9300	64 MB	10.5 GB	980 MB	15 min	12 min
ASA 5500-X series with FTD	8.7 GB	70 KB	1.2GB	23 min	26 min
FTDv: VMware 6.0	8.7 GB	70 KB	1.2 GB	14 min	17 min
ASA FirePOWER	11.4 GB	63 MB	1.4 GB	93 min	10 min
NGIPSv: VMware 6.0	6.1 GB	53 MB	860 MB	10 min	5 min

Traffic Flow, Inspection, and Device Behavior

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

- When a device is rebooted.
- When you upgrade the operating system or virtual hosting environment on a device.
- When you upgrade the Firepower software on a device, 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.

Firepower 4100/9300 Chassis: FXOS Upgrade

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

Table 27: Traffic Behavior During FXOS Upgrade

Deployment	Method	Traffic Behavior
Standalone	—	Dropped
High availability	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online
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 FTD Device: Firepower Software Upgrade

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

Table 28: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

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

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force** (6.1+)	Either: • Dropped (6.1 through 6.2.2.x) • Passed without inspection (6.2.3+)
	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 data security module or modules upgrade first, then the control module. Security modules operate in maintenance mode while they upgrade.

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



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

High Availability and Clustering Hitless Upgrade Requirements

Performing hitless upgrades have the following additional requirements.

Flow Offload: Due to bug fixes in the flow offload feature, some combinations of FXOS and FTD do not support flow offload; see the Cisco Firepower Compatibility Guide. To perform a hitless upgrade in a high availability or clustered deployment, you must make sure you are always running a compatible combination.

If your upgrade path includes upgrading FXOS to 2.2.2.91, 2.3.1.130, or later (including FXOS 2.4.1.x, 2.6.1.x, and so on) use this path:

1. Upgrade FTD to 6.2.2.2 or later.
2. Upgrade FXOS to 2.2.2.91, 2.3.1.130, or later.
3. Upgrade FTD to your final version.

For example, if you are running FXOS 2.2.2.17/FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1/FTD 6.4.0, then you can:

1. Upgrade FTD to 6.2.2.5.
2. Upgrade FXOS to 2.6.1.
3. Upgrade FTD to 6.4.0.

Version 6.1.0 Upgrades: Performing a hitless upgrade of an FTD high availability pair to Version 6.1.0 requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.

Traffic Behavior During Deployment

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

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

Table 29: Traffic Behavior During FTD Deployment

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.	Dropped
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 on Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and FTDv.

Standalone FTD Device: Firepower Software Upgrade

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

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

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.	Dropped
IPS-only interfaces	Inline set, fail-to-wire enabled: **Bypass: Standby** or **Bypass-Force** (6.1+)	Either: • Dropped (6.1 through 6.2.2.x) • Passed without inspection (6.2.3+)
	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.

Traffic Behavior During Deployment

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

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all Firepower devices, including

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

Table 31: Traffic Behavior During FTD Deployment

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

ASA FirePOWER Upgrade Behavior

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

Table 32: Traffic Behavior During ASA FirePOWER Upgrade

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

Traffic Behavior During ASA FirePOWER Deployment

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

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

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

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

NGIPSv Upgrade Behavior

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

Firepower Software Upgrade

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 33: Traffic Behavior During NGIPSv Upgrade

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

Traffic Behavior During Deployment

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

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

Table 34: Traffic Behavior During NGIPSv Deployment

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

Upgrade Instructions

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

- Cisco Firepower Management Center Upgrade Guide: Upgrade FMC deployments, including managed devices and companion operating systems.
- Cisco ASA Upgrade Guide: Upgrade ASA FirePOWER modules with ASDM.
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager: Upgrade FTD with FDM.

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
- ASA with FirePOWER Services (ASA 5500-X series): https://www.cisco.com/go/asa-firepower-sw
- ASA with FirePOWER Services (ISA 3000): https://www.cisco.com/go/isa3000-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software

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

Tip An FMC with internet access can download Version 6.6.x maintenance releases (third-digit upgrades) directly from Cisco, about two weeks after they are available for manual download. Direct download from Cisco is not supported for major releases, most patches, or to managed devices—including to devices managed by FDM.

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

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Upgrade-6.6.0-90.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: 6.6.0-90

- File extension: sh.REL.tar

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

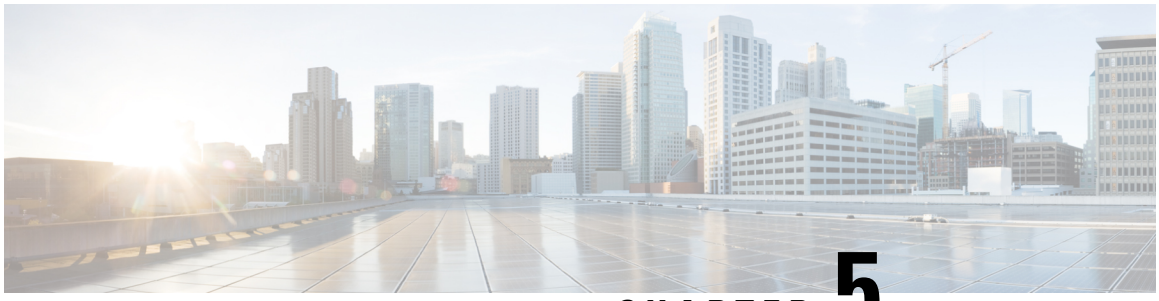
Table 35: Upgrade Package Naming Schemes for Firepower Software

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

Operating System Upgrade Packages

For information on operating system upgrade packages, see the *Planning Your Upgrade* chapters in the following guides:

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



CHAPTER 5

Freshly Install the Software

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

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

- Deciding to Freshly Install, on page 61
- Guidelines and Limitations for Fresh Installs, on page 63
- Unregistering Smart Licenses, on page 65
- Installation Instructions, on page 66

Deciding to Freshly Install

Use this table to identify scenarios where you need to freshly install (also called *reimaging*). Note that for Firepower devices, in all of these scenarios—including switching device management between local and remote—*you will lose device configurations*.

Note Address licensing concerns before you reimage or switch management. If you are using Cisco Smart Licensing, you may need to unregister from the Cisco Smart Software Manager (CSSM) to avoid accruing orphan entitlements. These can prevent you from reregistering.

Table 36: Scenarios: Do You Need a Fresh Install?

Scenario	Solution	Cisco Smart Licensing
Upgrade FMC-managed devices from a much older Firepower version.	The upgrade path from older versions can include 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 to its target version. **3.** Reimage the devices. **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 Cisco Firepower Threat Defense Command Reference.	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 Cisco Firepower Threat Defense Command Reference. **Exception:** The device is running or was upgraded from Version 6.0.1. In this case, reimage.	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.	Reimage.	Convert Classic to Smart licenses; see the Firepower Management Center Configuration Guide.
Replace NGIPSv with FTDv.	Reimage.	Contact Sales for new Smart licenses.
Uninstall an FTD patch with FDM.	Reimage. You cannot uninstall patches in FDM deployments.	Unregister the device before you reimage. Reregister after.
Return to a previous major or maintenance release.	Reimage. You cannot uninstall major or maintenance upgrades. If possible, restore from backup.	Do not unregister before you reimage, and do not remove devices from the FMC. If you do, you must unregister again after you restore, then re-register. Instead, revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Scenario	Solution	Cisco Smart Licensing
Restore a failed FMC or FTD device from backup.	In an RMA scenario, the replacement will arrive configured with factory defaults. However, if the replacement is already configured, we recommend you reimage before you restore.	Do not unregister before you reimage, and do not remove devices from the FMC. If you do, you must unregister again after you restore, then re-register. Instead, revert any licensing changes made since you took the backup. After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

Guidelines and Limitations for Fresh Installs

Careful planning and preparation can help you avoid missteps. Even if you are familiar with Firepower releases and have previous experience reimaging Firepower appliances, make sure you read these guidelines and limitations, as well as the instructions linked in Installation Instructions, on page 66.

Back Up Event and Configuration Data

When supported, we strongly recommend you back up before you reimage.

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

You should back up to a secure remote location and verify transfer success. Reimaging returns most settings to factory defaults, including the system password. It deletes any backups left on the appliance. And especially because backup files are unencrypted, do not allow unauthorized access. If backup files are modified, the restore process will fail.

As the first step in any backup, note the appliance model and version, including patch level. For FMCs running Version 6.5.0 and earlier, note the VDB version. For Firepower 4100/9300 chassis, note the FXOS version. This is important because if you need to restore the backup to a new or reimaged appliance, you may need to update the new appliance first.

Note Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. Careful planning and preparation can help you avoid missteps. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your Firepower product.

Remove Devices from the Firepower Management Center

If you plan to manually configure the reimaged appliance, remove devices from remote management before you reimage:

- If you are reimaging the FMC, remove all its devices from management.

- If you are reimaging a single device or switching from remote to local management, remove that one device.

Note that if you plan to restore from backup after reimaging the FMC or FTD device, you do not need to remove devices from remote management.

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*.

Appliance Access

Reimaging returns most settings to factory defaults.

If you do not have physical access to an appliance, the reimage process lets you keep management network settings. This allows you to connect to the appliance after you reimage to perform the initial configuration. If you delete network settings, you *must* have physical access to the appliance. You cannot use Lights-Out Management (LOM).



Note Reimaging to an earlier major version automatically deletes network settings. In this rare case, you must have physical access.

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

Sharing Data with Cisco

Some features involve sharing data with Cisco.

In Version 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support. During initial setup, you may be asked to accept or decline participation. You can also opt in or out at any time.

In Version 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs. Web analytics tracking is on by default (by accepting the EULA you consent to web analytics tracking), but you can opt out at any time after you complete initial setup. You may also have to opt out again after major upgrades, which can reenable this feature.

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

information from your devices during the course of a TAC case. During initial setup, you may be asked to accept or decline participation. You can also opt in or out at any time.

Reimaging Firepower 1000/2100 Series Devices to Earlier Major Versions

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

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

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). If you later decide to reimage or switch management, you must unregister to avoid accruing orphan entitlements. These can prevent you from reregistering.



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

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

Manually unregister from CSSM before you:

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

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

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

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

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

Unregister a Firepower Management Center

Unless you plan to restore from backup, unregister a Firepower Management Center from CSSM before you reimage. 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 **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 37: Firepower Management Center Installation Instructions

FMC Platform	Guide
FMC 1600, 2600, 4600	Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide

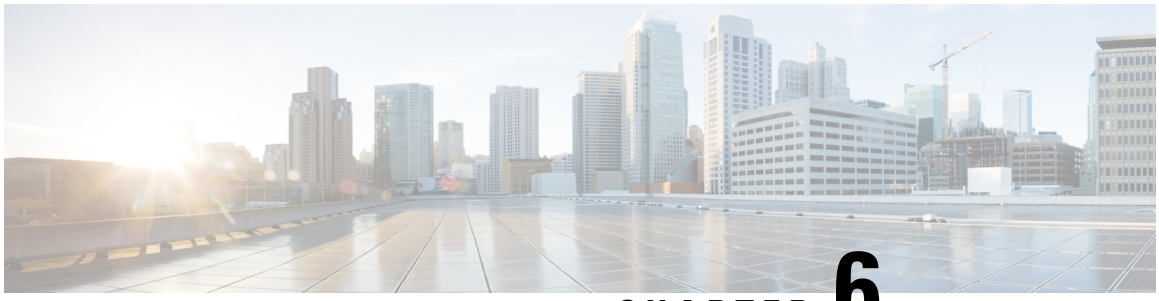
FMC Platform	Guide
FMC 1000, 2500, 4500	Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
FMC 2000, 4000	Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
FMCv and FMCv 300	Cisco Firepower Management Center Virtual Getting Started Guide

Table 38: Firepower Threat Defense Installation Instructions

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

Table 39: NGIPSv and ASA FirePOWER Installation Instructions

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



CHAPTER 6

Documentation

For Firepower documentation, see:

- New and Updated Documentation, on page 69
- Documentation Roadmaps, on page 71

New and Updated Documentation

The following Firepower documentation was updated or is newly available for this release. For links to other Firepower documentation, see the Documentation Roadmaps, on page 71.

Firepower Configuration Guides and Online Help

- Firepower Management Center Configuration Guide, Version 6.6 and online help
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, Version 6.6.0 and online help
- Cisco ASA with FirePOWER Services Local Management Configuration Guide, Version 6.6 and online help
- Cisco Firepower Threat Defense Command Reference

FXOS Configuration Guides and Release Notes

- Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.8(1)
- Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.8(1)
- Cisco Firepower 4100/9300 FXOS Command Reference
- Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1)

Upgrade Guides

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

Hardware Installation Guides

- Cisco Firepower 4112, 4115, 4125, and 4145 Hardware Installation Guide

Getting Started Guides

- Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide
- Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide
- Cisco Firepower Management Center 750, 1500, 2000, 3500 and 4000 Getting Started Guide
- Cisco Firepower Management Center Virtual Getting Started Guide
- Cisco Firepower 1010 Getting Started Guide
- Cisco Firepower 1100 Series Getting Started Guide
- Cisco Firepower 2100 Series Getting Started Guide
- Cisco Firepower 4100 Getting Started Guide
- Cisco Firepower 9300 Getting Started Guide
- Cisco ISA 3000 Getting Started Guide
- Cisco ASA 5508-X and 5516-X Getting Started Guide
- Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide
- Cisco Firepower Threat Defense Virtual for KVM Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the AWS Cloud Getting Started Guide
- Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide

API and Integration Guides

- Firepower Management Center REST API Quick Start Guide, Version 6.6.0
- Cisco Firepower Threat Defense REST API Guide
- Firepower System Event Streamer Integration Guide, Version 6.6.0
- Firepower and Cisco SecureX threat response Integration Guide
- Integration Guide for the Cisco Firepower App for IBM QRadar ***NEW***

Compatibility Guides

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

Licensing and Open Source

- Cisco Firepower System Feature Licenses
- Frequently Asked Questions (FAQ) about Firepower Licensing
- Open Source Used in Firepower Version 6.6.0

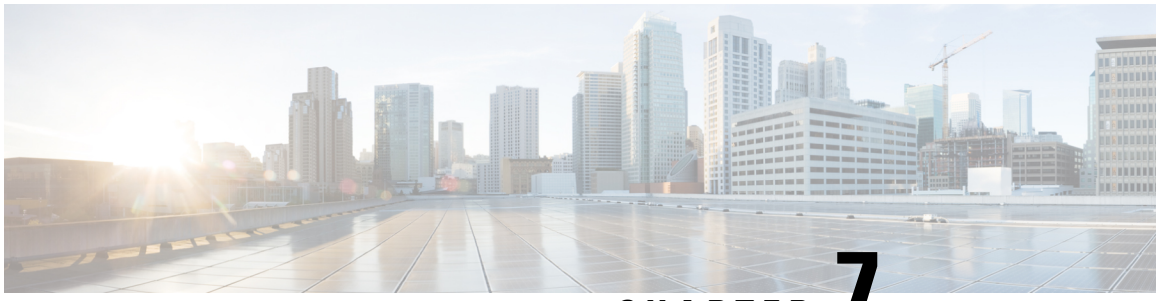
Troubleshooting and Configuration Examples

- Cisco Firepower Threat Defense Syslog Messages
- Using Multi-Instance Capability on the Firepower 4100/9300
- Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability

Documentation Roadmaps

Documentation roadmaps provide links to currently available and legacy documentation:

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



CHAPTER 7

Resolved Issues

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

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

For resolved issues, see:

- Searching for Resolved Issues, on page 73
- Version 6.6.0 Resolved Issues, on page 74

Searching for Resolved Issues

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

These general queries display resolved bugs for Firepower products running Version 6.6.0:

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

Version 6.6.0 Resolved Issues

Table 40: Version 6.6.0 Resolved Issues

Bug ID	Headline
CSCvc05004	Restore failed with an error Unable to clear Lights-Out Managment Users
CSCve93565	Unable to generate certificates using Subject Alternative Name (SAN) in the FMC
CSCvh20050	Cisco Firepower System Software Static Credential Vulnerability - No access vector
CSCvi09009	Import Failure: Out of memory while extracting the import package
CSCvi34123	ENHancement: Cannot add DNS lists that contain _ at the beginning of the list.
CSCvi72863	Deployment instability due to management traffic being inspected with access control policy
CSCvi97028	fmc GUI too slow when configuring unreachable syslog server
CSCvj65880	Blank page when user does not have enough permissions to see rule import log
CSCvm86658	FTD traceback and reload in snap_get_retaddr_mips at snap.h:285
CSCvn28160	Configuring a user with LOM succeeds incorrectly even if LOM isn't updated
CSCvn32473	Troubleshoot file path conflict between FMC and FTD when IPV6 address is used by device
CSCvn81332	Multiple domains with the same netmap_num
CSCvo26597	CLI Banner not seen on FTD
CSCvo66039	Not able to edit portchannel which has ID starting with same number as cluster interface(CCL)
CSCvo80725	vFTD 6.4 fails to establish OSPF adjacency due to "ERROR: ip_multicast_ctl failed to get channel"
CSCvp10983	FMC should not allow invalid ip/range to be entered while creating/editing access policy rule
CSCvp19068	Intrusion event Packet Information for SMTP packet shows truncated field, downloaded pcap is correct
CSCvp20745	Manual time on Secondary FMC always resetting back to 5-Mar-2019 13:57
CSCvp20905	Protocol field is wrongly populated under Policies->Application Detectors for DNS/QQ Apps
CSCvp33033	Elektra uses ext2 instead ext3 or ext4

Bug ID	Headline
CSCvp72518	Cleanup .pyc files during every boot/TID startup to avoid .py files not starting up causing issues
CSCvp95702	CAC login button does not appear on the new FMC GUI
CSCvp98570	FMC is not pushing AAB and snort preserve-connection config to FTD
CSCvp99327	FMC UI Unresponsive After Attempt To Register Smart License With Smart Satellite
CSCvq00138	Documentation states you must update intrusion rules/SRU after FMC restore.
CSCvq07297	Cisco Firepower Threat Defense Software HTTP Filtering Bypass Vulnerability
CSCvq07838	DOC: API example has"forceDeploy" setting in "DeploymentRequest" set to true on the FMC guide.
CSCvq11960	FMC does not allow same IP address value entries within one prefix-list entry
CSCvq12758	FMC shouldn't deploy "strong-encryption-disable" command to FTDs after smart license deregistration
CSCvq24258	Increase number of worker for mojo-server on large appliances
CSCvq28406	Error for a failed import of a certificate in 6.3.0 doesnt appear
CSCvq32660	FlexConfig Must Use Correct Encoding For Special Characters
CSCvq34340	FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature
CSCvq35512	LINA should accept "\" as is without converting it to invalid UTF-8 encoding
CSCvq39344	SNMPv3 GET/WALK not responding successfully.
CSCvq42723	Logging to event viewer gets enabled in GUI even after disabling it.
CSCvq43413	QoS rule using URL list is not pushed to qos.rules file on FTD sensor
CSCvq46674	SRU Update Causes Alert Threshold in Preprocessor Rules being removed
CSCvq51795	FMC didn't cleanup device details when auto-registration fails due to sftunnel issue.
CSCvq52582	DCE/RPC NAP policy has not been updated past Vista
CSCvq52636	Warn of possible policy deployment failure when in route more than one obj should be more specific
CSCvq52770	TSAgent does not work properly with Anti Virus software that proxies web traffic
CSCvq52914	Implement error checking for very large NAT rules that can trigger deployment failures
CSCvq53002	After data purge, users in mysql are still counted into user limit although they are marked deleted

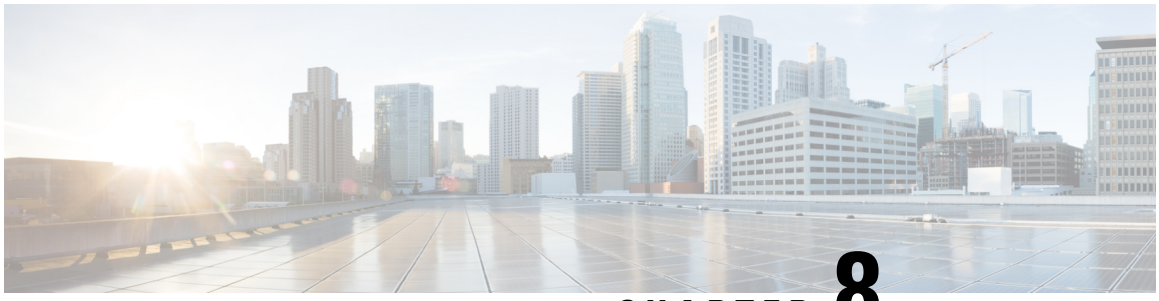
Bug ID	Headline
CSCvq53902	Cisco Firepower Management Center Multiple Cross-Site Scripting Vulnerabilities
CSCvq54176	FTD : A new custom IKE policy not applied or overwrites a default policy
CSCvq55915	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvq55929	Cisco Firepower Management Center Software Stored Cross-Site Scripting Vulnerability
CSCvq72063	Deleting FTD might leave smart licensing in use
CSCvq72292	Failing to deploy multiple site-to-site using aggressive mode
CSCvq74877	DOC: App based rule should be mentioned as a recommendation for FTP traffic
CSCvq76964	Fault Related to Unhealthy module FlexFlash Controller 1 old Firmware
CSCvq80147	ASA SFR: deploy fails as soon as use Network Object Group in VariableSet
CSCvq89794	FDM - user downloads not working with LDAPS
CSCvq95694	Memory leak SSL_ALLOC [ERROR] ssl_alloc.c:113:ssl_alloc_destroy()
CSCvq97698	jQuery Object.prototype Property Injection Vulnerability
CSCvr05934	Error reporting for failed variable set validation during deploy is not sufficient for user.
CSCvr07460	ASA traceback and reload related to crypto PKI operation
CSCvr09468	ASA traceback and reload for the CLI "Show nat pool"
CSCvr17735	SFDataCorrelator high CPU during SI update
CSCvr20893	FTD in HA pair crashes in ids_event_proce process after policy deployment
CSCvr24059	Source SGT correlation doesn't work for FMC and FTD 6.5
CSCvr25152	"Name is invalid" when trying to edit existing external authentication object(add new users)
CSCvr25705	Policy deployment failure incorrectly reported as failed to retrieve config
CSCvr27850	External authentication using LDAP and Radius fails for SSH access on the FTD
CSCvr29638	HA FTD on FPR2110 traceback after deploy ACP from FMC
CSCvr30694	FMC : FMC detect HA Sync Failed
CSCvr30869	Retrospective correlation malware alerts are sent base64 encoded with an unneeded space
CSCvr33239	Incorrect data on dashboard "Security Intelligence Statistics"
CSCvr39556	Segfault in libclamav.so (in the context of SFDataCorrelator)
CSCvr41230	Snort sessions are timing out earlier than configured idle timeouts on SFR module

Bug ID	Headline
CSCvr41377	user download fails when duplicate group names are present
CSCvr43341	FDM 6.5.0 - FPR1000 GUI Unresponsive if upgraded with Trunk Interfaces
CSCvr49229	FMC showing high Cpu in sfmbservice.
CSCvr50621	Policy deployment fails when Standard access list object contains 128.0.0.0/1
CSCvr51955	Estreamer should terminate a connection when not receiving ACKs for a long time
CSCvr51958	Alerting notification on light UI theme keeps spinning forever
CSCvr54250	Many user_ip_map files even though no realm is configured
CSCvr57984	Deployment Failure Due to the Use of MAC Addresses on Unnamed FTD HA Interfaces
CSCvr61575	Error "Object does not belong to current domain" returned, when opening RA VPN in Global domain
CSCvr63858	FTD Upgrade fails at 600_schema/099_pre_multischema.pl
CSCvr67375	Primary FMC 6.3.0.3 in HA stops receiving health alerts suddenly
CSCvr67542	vFMC 6.6.0 requires at least 28GB for upgrade.
CSCvr69380	External Authentication Config for LDAPS Over SSL Failing to Save Cert
CSCvr72372	FMC SLR registration, devices get Unlicensed after migrating from SSMS Satellite
CSCvr72708	6.6 Connection events do not display source sgt for 6.2.3/6.3.0/6.4.0/6.5.0 FTD
CSCvr75274	FTD show tech from troubleshooting files incomplete
CSCvr76029	FTD-HA: after restoring FTD-HA backup file, snort process will be down
CSCvr76044	FTD Snort Rule Profiling does not work consistently - log folder is missing
CSCvr76487	PDF reports failing without any clear error when an image that does not exist is used in the report
CSCvr79008	Session processing delay from FMC wastefully querying all Directory Servers normalizing bad username
CSCvr80621	FMC External Authentication with SecurID RSA fails with banner enabled
CSCvr82372	unable to enable snmpv3 due to license error
CSCvr82716	Insufficient undecryptable site list results in failed TLS connections due to cert pinning
CSCvr82965	DNS entry not showing up in /etc/resolv.conf and 'show-network' , if not configured from FCM
CSCvr89663	Traceback: with thread name: pix_flash_config_thread WM1010 went into reboot loop
CSCvr92327	ASA/FTD may traceback and reload in Thread Name 'PTHREAD-1533'

Bug ID	Headline
CSCvr92596	Upgrade script 470_revert_prep.sh hangs if there are too many partitions, due to grep command
CSCvr92617	NPE in SecurityIntelligenceEoConvertor causes Lucene indexing failure
CSCvr94368	check return status on unmount mysql in 470_revert_prep.sh
CSCvr95581	System 500 Internal Error when trying to access system -> updates page
CSCvr97009	QoS (rate limit) not enforced when using URL categories
CSCvr97778	FTD registration cert is revoked on Standby FMC which is causing devices in pending registration.
CSCvr98194	warn user when disabling a column results in event aggregation
CSCvs00023	port manager crashes with "shutdown" command from clish CLI
CSCvs01422	Lina traceback when changing device mode of FTD
CSCvs04067	Not able to access FMC devices with Chrome on Mac after upgrade to Catalina.
CSCvs04179	ASA - 9.8.4.12 traceback and reload in ssh or fover_rx Thread
CSCvs05084	FTD Cisco Cloud Configuration Failure due to proxy
CSCvs05932	Unable to add ipv6 host objects with /128 or ::/0 FMC 6.3
CSCvs12288	Snort unexpectedly exits with SSL policy enabled and debug_policy_all
CSCvs12946	External Auth from CLI on FMC fails if customer has password limits set.
CSCvs14931	REST API call for GET ftddevicehapairs response shows incorrect FTD-HA status
CSCvs17981	FDM should not allow to change a Network object from Network to Range if object is used in RA VPN
CSCvs19968	Fix consoled from getting stuck and causing HA FTD policy deployment errors.
CSCvs22503	eStreamer repeatedly exits after "Failed to deserialize policy event"
CSCvs23591	FMC should not allow to configure two identical VPN tunnels
CSCvs24295	Certain certificate formats cause ISE FMC Server Certificate dropdown to break
CSCvs25607	addition of netmap_num to constraints causes performance degradation
CSCvs26443	FDM should allow top down approach while configuring sub-interfaces for OSPF
CSCvs32303	SNMP polling fails on Standby FMC as the snmpd process is in Waiting state
CSCvs33297	SSL Rekey Interval is labeled on "seconds" when it should be on "minutes"on FTD managed by FDM.
CSCvs37013	Prevent octeon_init from getting stuck and causing HA FTD policy deployment errors.

Bug ID	Headline
CSCvs37065	Snort crash due to missing data in /ngfw/var/sf/fwcfg/interface_info.conf file
CSCvs39202	Deployment failure when OSPF authentication configuration is pushed
CSCvs40531	AnyConnect 4.8 is not working on the FPR1000 series
CSCvs44149	Reconciliation report not displaying all the networks when adding a large object group
CSCvs47201	GET ALL for devicerecords we get "isPartOfContainer": false for devices part of HA and cluster
CSCvs47880	Firepower Device Manager (FDM) option to change the DNS IP for RA VPN is not reflected on the config
CSCvs50137	Same Security Zone used in ACP rule is Not pushed to NGFW rules
CSCvs50459	Cisco ASA and Cisco FTD Malformed OSPF Packets Processing Denial of Service Vulnerability
CSCvs58934	User already exists for lights-out management error when updating password
CSCvs61392	On firepower devices, hardware rules are not updated after successful policy deployment
CSCvs61421	Reconfigure of SFDataCorrelator taking too long due to long host timeout
CSCvs61549	Deploy fails with "snort validation failed: Unknown error" message, snort core
CSCvs64470	FDM on-box deployment failed with error java.lang.NullPointerException
CSCvs70704	FDM upgrade to 6.5 fails at 100_ftd_onbox_data_import.sh.log(You cannot enable syslog with event...)
CSCvs70864	Analysis / Hosts / Network Map / Application Protocols Loads forever
CSCvs74452	SFDatacorrelator and Snort process cores repeatedly while loading malware seed file
CSCvs77334	FTD failover due to error "Inspection engine in other unit has failed due to snort and disk failure"
CSCvs78252	ASA/Lina Offloaded TCP flows interrupted if TCP sequence number randomizer is enabled and SACK used
CSCvs82369	Threat Data Updates - Cisco Cloud Configuration - Failure
CSCvs88151	FDM Authentication Failure With Custom Tokens
CSCvs88209	Extended community string mismatch between FMC and ASA/LINA
CSCvs91389	FTD Traceback Lina process
CSCvs96054	Unable to register more than 25 devices after migration from virtual FMC to Hardware 2600
CSCvs98634	catalina.<date>.log files can consume all disk space in their partition

Bug ID	Headline
CSCvt01763	Application classification is not retried if a flow is marked brute force failed.
CSCvt03794	Policy deployment failure after SRU update on FTD with passive zone
CSCvt08466	REST API posts using interface ranges are added to the FMC without any check validation
CSCvt10875	Syslog alert shows incorrect hostname due to show running config sync between FTD HA
CSCvt11728	on FDM, vdb updates to current version multiple times
CSCvt27585	Observed Crash in KP while performing Failover Switch from Standby.
CSCvt48941	FTD Standby unit does not join HA due to "HA state progression failed due to APP SYNC timeout"
CSCvt55460	EventHandler memory leak with SNMP alerts
CSCvt80401	FDM GUI unavailable on secondary HA FTD due to high availability sync failing to complete
CSCvt82003	False positive alert for VPN tunnel status
CSCvu12248	ASA-FPWR 1010 traceback and reload when users connect using AnyConnect VPN
CSCvu24784	DOC: Firepower compatibilty pages missing compatibility info for 4112 hardware
CSCvu35427	Intermittent Latency on 5500-X platforms with SFR Module Inspection



CHAPTER 8

Known Issues

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

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

- Searching for Known Issues, on page 81
- Version 6.6.0 Known Issues, on page 81

Searching for Known Issues

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

These general queries display open bugs for Firepower products running Version 6.6.0:

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

Version 6.6.0 Known Issues

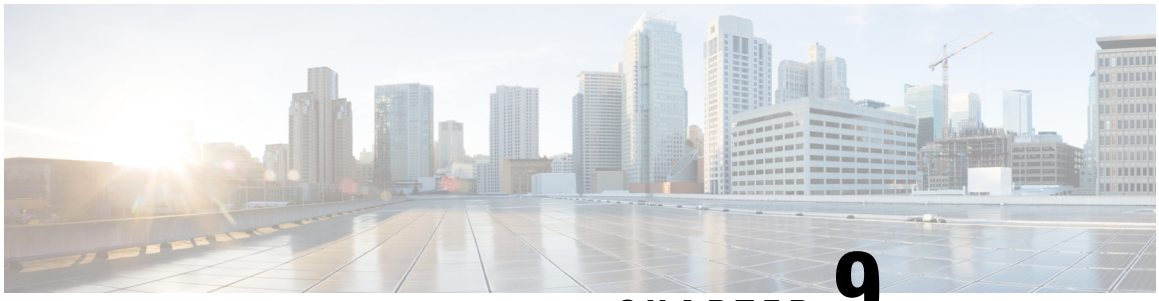
Table 41: Version 6.6.0 Known Issues

Bug ID	Headline
CSCvr90564	Deployment fails when you negate Inter Area OSPF config in user vrf

Bug ID	Headline
CSCvt14898	Deployment failed after upgrade with RAVPN:no split-tunnel-network-list value RA-VPN-policy|splitAcl
CSCvt29546	License is getting unregistered after restoring backup on same box
CSCvt37753	Policy deployments failing on MI Cluster
CSCvt39442	Dashboard widgets not visible due to admin user
CSCvt43431	CLI changes were not updated on UI after changing Management interface config on CLI. OOB sync issue
CSCvt61370	Events may stop coming from a device due to a communication deadlock
CSCvt66906	AppId looks up in dynamic cache even when it finds apps in a session
CSCvt68316	Constant deployment failure after import failure and unable to discard changes
CSCvt68819	Copy to clipboard may fail when copying events that existed before upgrade
CSCvt69260	connection event shows old device name
CSCvt70854	6.6.0-90: [Firepower 1010] Tomcat restarted during SRU update because of out of memory
CSCvt77143	Apache Commons FileUpload HTTP Request Header Value Handling Denial of
CSCvt77210	minimist before 1.2.2 could be tricked into adding or modifying proper
CSCvt78634	FTD Lina traceback during policy deployment with assertion domain_id
CSCvt79988	Policy deployment failure due to snmp configuration after upgrading FMC to 6.6
CSCvt86467	c3p0 0.9.5.2 allows XXE in extractXmlConfigFromInputStream in com/mcha
CSCvt87117	libexpat Improper Parsing Denial of Service Vulnerability
CSCvt87123	Expat libexpat XML Parser Denial of Service Vulnerability
CSCvt89042	dom4j XML Injection Vulnerability
CSCvt89045	Redis redis-cli Buffer Overflow Vulnerability
CSCvt89378	"The database has encountered a critical error, and needs to be restarted." error on UI when login
CSCvt91258	FDM: None of the NTP Servers can be reached - Using Data interfaces as Management Gateway
CSCvt97205	SNMPPOLL/SNMPTRAP to remote end (site-to-site vpn) ASA interface fails on ASA 9.14.1
CSCvt99082	Rest API : Extended Access List URL changed from extendedaccesslist to extendedaccesslists

Bug ID	Headline
CSCvu06882	Hotplug removal of virtio interface from KVM ASAv causes crash
CSCvu12608	ASA5506/5508/5516 devices not booting up properly / Boot loop
CSCvu13287	FDM upgrade fails at 800_post/100_ftd_onbox_data_import.sh
CSCvu16826	FTD snort instances down due to corrupted snort rule after upgrade to release 6.6
CSCvu18510	MonetDB's eventdb crash causes loss of connection events on FMC 6.6.0
CSCvu20690	dom4j before 2.1.3 allows external DTDs and External Entities by defau
CSCvu29145	Snort flow IP profiling cannot be enabled using command 'system support flow-ip-profiling start'
CSCvu30441	FMC 6.6 REST API GUI no response when trying to PUT or POST new access rule
CSCvu30748	ASAv traceback and reload after upgrading to version 9.14.1 on PTHREAD-1859
CSCvu35426	Only one device deploy's policy in Leaf domain schedule deployment
CSCvu35768	After upgrade FMC from 6409-59 to 6.6.0-90 unable to log UI using Radius external user in subdomain.
CSCvu38869	The jQuery framework exchanges data using JavaScript Object Notation - solution not available
CSCvu50400	ASA FirePOWER with ASDM has high CPU usage after upgrading from Firepower 6.2.3.x to 6.6.0
CSCvu62018	Traffic blocked when using max detect IPS with SSL decryption due to rule 129:12 - Snort2
CSCvu65890	FMC unable to switch from MD5 and DES under SNMP3 settings despite not being supported
CSCvu74702	Detection Engine terminated unexpectedly generating a core file post a policy deploy
CSCvu75315	Report does not show intrusion events on bar and pie charts after upgrade to 6.6.0
CSCvu79125	Advanced Malware Risk Report Generation Failed
CSCvu82272	Upgrade on Firepower Management Center may fail due to inactive stale entries of managed devices
CSCvu82578	Light Theme UI FMC - SFR Module long delay loading Interfaces Page
CSCvu84127	Firepower 2100: FTD reboots with no apparent reason
CSCvu84556	Site to Site Dynamic crypto map deployed below RA VPN Dynamic Crypto map
CSCvu96559	Traceback: ASA had an unexpected traceback and generated an incomplete core
CSCvv01558	"unrecognized instance" error from sfhassd on ASA/ Elektra-HA device running 6.6.0-90

Bug ID	Headline
CSCvv04023	FDM (On box manager)Traffic not hit in the proper rule because interface is removed from zones.conf



CHAPTER 9

For Assistance

Thank you for choosing Firepower.

- Online Resources, on page 85
- Contact Cisco, on page 85

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 (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts