Firepower Release Notes, Version 6.2.2.1, Version 6.2.2.2, Version 6.2.2.3, Version 6.2.2.4, and Version 6.2.2.5

First Published: 2017-11-06

Last Modified: 2018-11-27

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

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

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

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

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

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

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

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

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

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

CONTENTS

CHAPTER 6

CHAPTER 7

CHAPTER 1

Welcome to Version 6.2.2.x

Thank you for choosing Firepower.

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

About the Release Notes

The release notes provide critical and release-specific information for Version 6.2.2.x, including upgrade warnings and behavior changes. Read this document even if you are familiar with Firepower releases and have previous experience upgrading Firepower deployments.

Warning You cannot uninstall a Version 6.2.2.2+ patch from a device in CC or UCAPL compliance mode. Instead, you must reimage. Before you begin, we *strongly* recommend backing up event and configuration data to an external location.

Note Devices running Version 6.2.2.1, Version 6.2.2.2, Version 6.2.2.3, and Version 6.2.2.4 that are configured for Threat Grid integration may be unable to pull reports from Threat Grid or submit files manually for analysis, per CSCvj07038. See Patch or Hotfix for New Dynamic Analysis CA Certificate, on page 26 for more information.

Release Dates

Sometimes Cisco releases updated builds. Only the latest build for each platform is available on the Cisco Support & Download site. You should always use the latest build. If you downloaded an earlier build, do not use it. For more information, see Resolved Issues in New Upgrade Packages, on page 63.

Table 1: Dates for Version 6.2.2.x

Version	Build	Date	Platforms
6.2.2.5	57	2018-11-27	All

Version	Build	Date	Platforms
6.2.2.4	43	2018-09-21	FTD/FTDv
	34	2018-07-09	FMC/FMCv Firepower 7000/8000 ASA FirePOWER NGIPSv
	32	2018-06-15	—
6.2.2.3	69	2018-06-19	All
	66	2018-04-24	—
6.2.2.2	109	2018-02-28	All
6.2.2.1	80	2017-12-05	Firepower 2100 series
	78	2017-11-20	—
	73	2017-11-06	FMC/FMCv All devices except Firepower 2100 series

CHAPTER 2

Features and Functionality

Features and functionality introduced in previous versions may be superseded by new features and functionality in later versions.

New or Changed Functionality in Version 6.2.2.x

Version 6.2.2.2

The following features have new or changed functionality in Version 6.2.2.2:

- The audit log now denotes if a policy changed on the Firepower Threat Defense Platform Settings (Devices > Platform Settings) page. (CSCvg79176)
- If an ISE pxgrid deployed in high availability fails or becomes unreachable, the Firepower Management Center now discovers the new active pxgrid faster. (CSCve71562)
- Version 6.2.2.2 increases the memory capacity for lower-end Firepower appliances and reduces the number of health alerts. (CSCvg34306)

CHAPTER 3

Platforms and Environments

The following sections describe the supported platforms and environments in Version 6.2.2.x, as well as compatibility guidelines:

Supported Platforms and Environments

Specific manager-device compatibility depends on the version of both the manager and device. A Firepower Management Center running Version 6.2.2.x can manage the following devices:

- Firepower 2100 series devices—Version 6.2.1, Version 6.2.2
- All other Firepower devices—Version 6.1.0 or later, Version 6.2.0 or later, Version 6.2.2 or later

However, keep in mind that many features depend on the version of the system running on the device. Even if a Firepower Management Center is running Version 6.2.2, your deployment may not support all its features until you also update managed devices to Version 6.2.2.x.

We *strongly* recommend upgrading the Firepower Management Center to the same maintenance release or later as the version you upgrade the managed device to. As an example, we recommend a Firepower Management Center run at least Version 6.2.2.1 before you upgrade a managed device to Version 6.2.2.1.

For smaller deployments, you can manage devices either locally or with a Firepower Management Center. On specific platforms, you can use Firepower Device Manager to manage Firepower Threat Defense. You can also use ASDM to manage ASA FirePOWER modules. You can use only one management method for a device at a time.

Supported Firepower Management Center

The following table lists supported Firepower Management Center platforms, and their operating system or hosting environment requirements.

Platform	OS/Hosting Environments
Firepower Management Center: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500	Firepower Threat Defense
Firepower Management Center Virtual (64-bit)	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0 Amazon Web Services (AWS) VPC/EC2 Kernel-based virtual machine (KVM)

Supported Devices in Version 6.2.2.x

The following table lists supported device platforms and their supported implementations, management methods, and operating system or hosting environment requirements.

Platform	Implementations	Managers	OS/Hosting Environments
Firepower 2110, 2120, 2130, 2140	Firepower Threat Defense	Firepower Device Manager Firepower Management Center	Firepower Threat Defense
Firepower 4110, 4120, 4140, 4150 Firepower 9300 with SM-24, SM-36, or SM-44 modules	Firepower Threat Defense	Firepower Management Center	FXOS 2.2(2) FXOS 2.2(2.x) **Caution** Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. As a workaround, use FXOS Version 2.3.1.58 or later. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Platform	Implementations	Managers	OS/Hosting Environments
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X ASA5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Firepower Threat Defense ASA FirePOWER module	Firepower Device Manager, for Firepower Threat Defense ASDM 7.8(2), for ASA FirePOWER Firepower Management Center, for either	Firepower Threat Defense ASA OS, for ASA FirePOWER: • 9.5(2), 9.5(3) except 5506 models • 9.6(x) • 9.7(x) • 9.8(x) Note that the ASA 5506-X does not support the ASA FirePOWER module when running ASA Version 9.5(x).
ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	ASA FirePOWER module	ASDM 7.8(2) Firepower Management Center	ASA OS: • 9.5(2), 9.5(3) • 9.6(x) • 9.7(x) • 9.8(x)
Virtual: VMware	Firepower Threat Defense Virtual NGIPSv	Firepower Device Manager, for Firepower Threat Defense Firepower Management Center, for either	VMware vSphere/VMware ESXi 5.5 VMware vSphere/VMware ESXi 6.0
Virtual: AWS	Firepower Threat Defense Virtual	Firepower Management Center	Amazon Web Services (AWS) EC2/VPC
Virtual: KVM	Firepower Threat Defense Virtual	Firepower Management Center	Kernel-based virtual machine (KVM)
Virtual: Azure	Firepower Threat Defense Virtual	Firepower Management Center	Microsoft Azure Standard D3 Microsoft Azure Standard D3_v2
Firepower 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	NGIPS	Firepower Management Center	Firepower Management Center

Integrated Product Compatibility

You can integrate a variety of products with Firepower, including:

- Cisco Identity Services Engine (ISE and ISE-PIC)
- Cisco AMP Threat Grid
- Cisco Terminal Services (TS) Agent
- Cisco AnyConnect Secure Mobility Client
- Cisco Firepower System User Agent

See the Firepower System Compatibility Guide for required versions of these integrated products,.

Web Browser Compatibility for Version 6.2.2.5

The Firepower web interfaces for Version 6.2.2.5 have been tested on the following browsers:

Table 2: Supported Web Browsers

Browser	Required Settings
Google Chrome 70	JavaScript, cookies **Caution** The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower system to the trust store of the browser/OS or use another web browser.
Mozilla Firefox 63	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox browser search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.

Browser	Required Settings
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must also disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Web Browser Compatibility for Version 6.2.2.4

The Firepower web interfaces for Version 6.2.2.4 have been tested on the following browsers:

Table 3: Supported Web Browsers

Browser	Required Settings
Google Chrome 66	JavaScript, cookies **Caution** The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower system to the trust store of the browser/OS or use another web browser.
Mozilla Firefox 60	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox browser search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must also disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.

Browser	Required Settings
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Web Browser Compatibility for Version 6.2.2.3

The Firepower web interfaces for Version 6.2.2.3 have been tested on the following browsers:

Table 4: Supported Web Browsers

Browser	Required Settings
Google Chrome 65	JavaScript, cookies **Caution** The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower system to the trust store of the browser/OS or use another web browser.
Mozilla Firefox 59	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox browser search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must also disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Web Browser Compatibility for Version 6.2.2.2

The Firepower web interfaces for Version 6.2.2.2 have been tested on the following browsers:

Table 5: Supported Web Browsers

Browser	Required Settings
Google Chrome 64	JavaScript, cookies **Caution** The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower system to the trust store of the browser/OS or use another web browser.
Mozilla Firefox 58	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The FMC uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the FMC and the Login screen takes a long time to load, enter **about:support** in a Firefox browser search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must also disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Web Browser Compatibility for Version 6.2.2.1

The Firepower web interfaces for Version 6.2.2.1 have been tested on the following browsers:

Table 6: Supported Web Browsers

Browser	Required Settings
Google Chrome 61	JavaScript, cookies **Caution** The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower system to the trust store of the browser/OS or use another web browser.
Mozilla Firefox 55	JavaScript, cookies, Transport Layer Security (TLS) v1.2 The Firepower Management Center uses a self-signed certificate by default; we recommend you replace that certificate with a certificate signed by a trusted certificate authority. For information on replacing server certificates, see the Firepower Management Center Configuration Guide. **Tip** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox browser search bar and click **Refresh Firefox**. You may lose existing Firefox settings when you refresh. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. **Caution** Firefox 56 incorrectly displays HTML instead of the Firepower Management Center UI . We *strongly* recommend using Firefox 55 or earlier or Fireox 57 or later.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, Transport Layer Security (TLS) v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must also disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

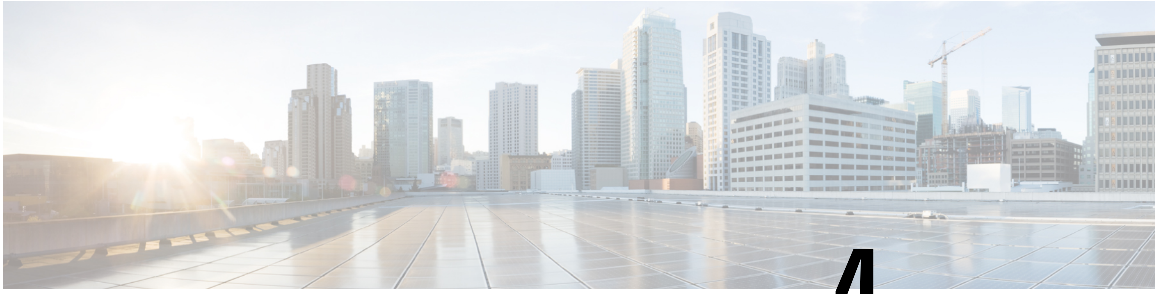
Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Screen Resolution Compatibility

Firepower user interfaces are not compatible with lower screen resolutions than those recommended in the following table:

Table 7: Recommended Screen Resolutions

User Interface	Minimum Recommended Resolution
Firepower Management Center 7000 and 8000 Series devices (limited local web interface) Firepower 4100 and Firepower 9300 devices	At least 1280 pixels wide
ASDM (managing ASA FirePOWER)	1024 pixels wide by 768 pixels high
Firepower Device Manager (managing Firepower Threat Defense)	1024 pixels wide by 768 pixels high



CHAPTER 4

Terminology and Documentation in Version 6.2.2.x

Terminology for Version 6.2.2

The terminology and branding used in Version 6.2.2.x may differ from the terminology used in previous releases, as summarized in the following table. For more information about terminology and branding changes, see the Firepower Compatibility Guide.

Table 8: Product Terminology and Branding in Version 6.2.2.x

Name(s)	Description
Firepower Firepower System	Refers to the product line
Firepower Management Center Management Center	Refers to Firepower management software running on physical or virtual Firepower platforms
Cisco ASA with FirePOWER Services ASA device running an ASA FirePOWER module ASA FirePOWER module	Refers to Firepower software running on an ASA operating system installed on an ASA platform
ASA FirePOWER module managed via ASDM	Refers to ASA FirePOWER module's local configuration interface, accessible with ASDM
Firepower Threat Defense	Refers to Firepower Threat Defense software running on a Firepower operating system installed on an ASA, Firepower 2100 Series, Firepower 4100 Series, Firepower 9300 appliance, or virtual platform

Name(s)	Description
Firepower Device Manager or FDM	Refers to Firepower Threat Defense's local configuration interface, accessible with specific Firepower Threat Defense platforms

Documentation for Version 6.2.2.x

The following documents were updated for Version 6.2.2.x to reflect the addition of new features and functionality and to address reported documentation issues:

For additional information about updating and configuring your system, see the documents in the Cisco Firepower System Documentation Roadmap.

For the ASA documentation roadmap and release notes (including known issues) for parallel ASA versions, see Navigating the Cisco ASA Series Documentation.

For the FXOS documentation roadmap and release notes (including known issues) for parallel FXOS versions, see Navigating the Cisco FXOS Documentation.

Known Documentation Issues in Version 6.2.2.x

- The Firepower Management Center Configuration Guide does not state that if you deploy an access control rule, SSL rule, or identity rule with geolocation network conditions and the system detects an IP address that appears to be moving from country to country, the system incorrectly reports the continent rule as **unknown** country.
- Online help is missing some information about Cisco Threat Intelligence Director configuration. Specifically, the topic **Configure Policies to Support TID** is missing information about SSL. The missing information is: *If you choose Intrusion Prevention as the default action for the access control policy and you want to decrypt traffic for TID detection, associate an SSL policy with the access control policy; see the topic "Associating Other Policies with Access Control* in the *Firepower Management Center Configuration Guide.* The Firepower Management Center Configuration Guide Version 6.2.2 is correct.

CHAPTER 5

Before You Update: Important Notes

Before you update, familiarize yourself with the update process, the system's behavior during the update, compatibility issues, and required pre or post-update configuration changes.

Caution For Firepower 4100/9300 chassis with FTD, do *not* update to FXOS Version 2.3.1.56 if you updated Firepower Threat Defense from Version 6.0.1.x. This can disable FTD and interrupt traffic on your network. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Note Do not enable common criteria (CC) or UCAPL mode on 8000 series devices running Version 6.2.2. If you do, the device may fail file system integrity checks (FSIC) and become unresponsive. If this happens, you must reimage. We recommend you upgrade to Version 6.2.2.1+ before you enable security certifications compliance.

For more information, see:

Update Paths to Version 6.2.2.x

To update to Version 6.2.2.x, you must be running the following Firepower versions:

- Firepower Management Center—Version 6.2.2
- Firepower 2100 series with Firepower Threat Defense—Version 6.2.2
- All other devices—Version 6.2.2

Note Version 6.2.1 is no longer available. We strongly recommend updating Firepower Management Centers or Firepower 2100 Series devices running Version 6.2.1 to Version 6.2.2, and then to a subsequent patch of Version 6.2.2.x to take advantage of resolved defects and vulnerabilities.

If you update from one major update to another, updating may cause or require significant configuration changes that you must address such as more memory or policy configuration. For example, the Version 6.2.0 update eliminates nested correlation rules, and you may need to take action related to this change.

Firepower Management Center Update Paths

The following table describes update paths for Firepower Management Centers, including Firepower Management Center Virtual:

Firepower Management Center Platform	Update Path
MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500 Firepower Management Center Virtual: VMware	Version 5.4.1.1+ > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x **Note** For Firepower Management Centers running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2 > Version 6.2.2.x
Firepower Management Center Virtual: AWS	Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x **Note** For Firepower Management Center Virtual:AWS running running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2 > Version 6.2.2.x
Firepower Management Center Virtual: KVM	Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x **Note** For Firepower Management Center Virtual: KVM running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2 > Version 6.2.2.x

Firepower Threat Defense Update Paths—With Firepower Management Center

This table describes update paths for Firepower Threat Defense devices managed by a Firepower Management Center.

Firepower Threat Defense Platform	Update Path
ASA 5506-X, ASAS 5506H-X, ASA 5506W-X, ASA 5508-X, 16-X ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X Firepower Threat Defense Virtual: VMware Firepower Threat Defense Virtual: AWS Firepower 4110, 4120, 4140 Firepower 9300 with SM-24, SM-36, or SM-44 modules	Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x
Firepower Threat Defense Virtual: KVM Firepower 4150	Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x
Firepower Threat Defense Virtual: Azure	Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x
Firepower 2110, 2120, 2130, 2140	Version 6.2.2 > Version 6.2.2.x **Note** For Firepower 2100 Series devices running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2 > Version 6.2.2.x

Firepower Threat Defense Update Paths—With Firepower Device Manager

This table describes update paths for Firepower Threat Defense devices managed by Firepower Device Manager.

Firepower Threat Defense Platform	Update Path
ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X	Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x
Firepower 2110, 2120, 2130, 2140	Version 6.2.2 > Version 6.2.2.x **Note** For Firepower 2100 Series devices running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2 > Version 6.2.2.x
Firepower Threat Defense Virtual: VMware	Version 6.2.2 > Version 6.2.2.x

NGIPS Update Paths—With Firepower Management Center

This table describes update paths for NGIPS devices (including ASA FirePOWER modules) managed by a Firepower Management Center.

NGIPS Platform	Update Path
Firepower 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125 Firepower 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390 AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390 ASA FirePOWER: ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X ASA FirePOWER: ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60 NGIPSv: VMware	Version 5.4.0.2 > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x
ASA FirePOWER: ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X	Version 5.4.1.1 > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x

NGIPS Update Paths—ASA FirePOWER with ASDM

This table describes update paths for ASA FirePOWER modules managed by ASDM.

ASA FirePOWER NGIPS Platform	Update Path
ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5516-X	Version 5.4.1.1 > Version 6.0.0 Pre-Installation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x
ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-Installation Package > Version 6.1.0 > Version 6.2.0 > Version 6.2.2 > Version 6.2.2.x

Update Sequence Guidelines

The following sections describe update sequences for deployments that include appliances that you linked for performance or redundancy:

Update Sequence for Firepower Management Centers in High Availability

This procedure explains how to upgrade the Firepower software on Firepower Management Centers in a high availability pair.

Do not simultaneously update Firepower Management Centers in a high availaiblity pair. You upgrade peers one at a time. With synchronization paused, first upgrade the standby (or secondary), then the active (or primary). When the standby Firepower Management Center starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade. Do *not* make or deploy configuration changes while the pair is split-brain; your changes will be lost after you upgrade the Firepower Management Centers and restart synchronization.

Step 1 Pause the synchronization of the active Firepower Management Center of the high availability pair with the High Availability tab of the Integration page (**System > Integration**) as described in the Pausing Communication Between Paired Firepower Management Centers topic of the *Firepower Management Center Configuration Guide*.

Step 2 Update the standby Firepower Management Center in the high availability pair. See the Update Firepower Management Centers, on page 37 for more information.

The Firepower Management Center switches from standby to active so both Firepower Management Centers in the high availability pair are active.

Step 3 Update the other Firepower Management Center within the pair.

Step 4 Click **Make-Me-Active** on the High Availability tab of one of the Firepower Management Center web interfaces.

The Firepower Management Center you do not make active automatically switches to standby mode. Communication between the Firepower Management Center pairs automatically restarts.

Update Sequence for High Availability Firepower Threat Defense Devices

Before you update Firepower Threat Defense, update the operating system on high availability Firepower 4100 series and Firepower 9300 devices to the most recent compatible FXOS version. For more information on FXOS versions, see the Firepower System Compatibility Guide.

Make sure you update FXOS to the most recent compatible FXOS version for the *current* Firepower version, that is, the version you are updating *from*. You may have to update FXOS again after you update Firepower to Version 6.2.2.x.

Caution You must always update the FXOS version on the *standby* device of a Firepower Threat Defense high availability pair. Do not update the FXOS version of the active device.

Note Firepower Version 6.2.2.4 does not support upgrading Firepower 2100 devices in high availability from Version 6.2.2. We recommend upgrading to Version 6.2.2.1 and then upgrade to Version 6.2.2.4.

If you upgrade a Firepower 2100 high availability pair from Version 6.2.2 to Version 6.2.2.4 and the upgrade fails, we recommend reimaging the devices. See Reimage Procedures for more information.

Step 1 Update the FXOS version on the standby Firepower Threat Defense device within the high availability pair. See the Cisco FXOS Release Notes for more information.

Step 2 Click the **Switch Active Peer** icon next the high availability pair on the **Devices** > **Device Management** page to switch failover, so the standby Firepower Threat Defense device is now the active device. The Firepower Threat Defense device that was active is now in standby.

Step 3 Update the FXOS version on the new standby Firepower Threat Defense device.

Step 4 Update the Firepower Threat Defense high availability pair to the most recent Firepower version. See Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 40 for more information.

When you install a Firepower update on Firepower Threat Defense devices in a high availability pair, the devices update one at a time. When the update starts, Firepower first applies it to the standby device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. Firepower then updates the active device, which follows the same process.

Update Sequence for Clustered Firepower Threat Defense Devices

When you update Firepower 4100 or Firepower 9300 clusters running Firepower Threat Defense, the system updates the security modules one at a time—first the secondary security modules, then the primary security module. Modules operate in maintenance mode while they are updated.

During the primary security module update, although traffic inspection and handling continues normally, the system stops logging events. Event logging resumes after the full update is completed.

Caution Updating FXOS reboots the device, which can affect traffic in a clustered environment until at least one module comes online. In an intra-chassis cluster, traffic drops if the cluster does not use an optional hardware bypass (fail-to-wire) module or if bypass is disabled. Traffic passes without inspection if bypass is enabled. In an inter-chassis cluster, traffic drops during the reboot if chassis reboots overlap before at least one module comes online; traffic is unaffected if there is no reboot overlap.

For more information, see the Firepower Threat Defense Cluster for the FXOS Chassis chapter of the *Firepower Management Center Configuration Guide* and the About Clustering on the FXOS Chassis chapter of the *Cisco FXOS Firepower Chassis Manager Configuration Guide*.

Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the update is completed. However, if the logging downtime was significant, the system may prune the oldest events before they can be logged.

Update Sequence for 7000 and 8000 Series Devices in High Availability

Note Use the Firepower Management Center to update 7000 or 8000 Series devices in a high availability pair. You cannot update using the devices' web interface.

When you install an update on 7000 and 8000 Series devices in a high availability pair, the system updates the devices one at a time. When the update starts, the system first applies it to the standby device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The system then updates the active device, which follows the same process.

Update Sequence for High Availability 7000 and 8000 Series Devices in Inline Deployment

When you install an update on 7000 Series or 8000 Series devices in high availability configured for inline deployment, the system performs the update on the devices one at a time. The system first applies it to the primary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. While the primary device updates in maintenance mode, the secondary device temporarily becomes primary and does not drop traffic. When the primary device update completes, the primary device moves from maintenance mode to primary mode and the system updates the secondary device.

Update Sequence for Stacked 8000 Series Devices

When you install an update on 8000 Series stacked devices, Firepower updates the stacked devices simultaneously. Each device resumes normal operation when the update is completed. Note the following scenarios:

- If the primary device completes the update before all of the secondary devices, the stack operates in a limited, mixed-version state until all devices have completed the update.
- If the primary device completes the update after all of the secondary devices, the stack resumes normal operation when the update is completed on the active device.

Pre-Update Readiness Checks

Caution Do *not* reboot or shut down an appliance during the readiness check. If your appliance fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

- Checks Firepower software readiness only—The readiness check does not assess preparedness for intrusion rule, VDB, or GeoDB updates.
- Version 6.1+ required—The readiness check was introduced in Version 6.1. A readiness check on the upgrade *to* Version 6.1 may not return accurate results.
- Web interface vs shell—You can use the Firepower Management Center web interface to perform the readiness check on itself and its standalone managed devices only. For clustered devices, stacked devices, and devices in high availability pairs, run the readiness check from each device's shell.
- Time requirements—The time required to run the readiness check varies depending on your appliance model and database size. You may find it expedient to forgo readiness checks if your deployment is large (for example, if your Firepower Management Center manages more than 100 devices).

Run a Readiness Check through the Shell

For clustered devices, stacked devices, and devices in high availability pairs, you *must* use the shell.

Before you begin

- Download the upgrade package for the appliance whose readiness you want to check. Readiness checks are included in upgrade packages.
- Deploy configurations to managed devices whose configurations are out of date. Otherwise, the readiness check may fail.

Step 1 Log into the shell as a user with administrator privileges.

Step 2 Make sure the upgrade package is on the appliance in the correct place:

- Firepower Threat Defense devices: `/ngfw/var/sf/updates`
- All other Firepower appliances: `/var/sf/updates`

On Firepower Management Centers, you can use the web interface to upload the upgrade package.

If you cannot or do not want to use the Firepower Management Center web interface, use SCP to copy the upgrade package to the appliance. Initiate from the Firepower side.

Step 3 Run this command as the root user:

```
sudo install_update.pl --detach --readiness-check full_path_to_update_package
```

Unless you are running the readiness check from the console, use the `--detach` option to ensure the check does not stop if your user session times out. Otherwise, the readiness check runs as a child process of the user shell. If your connection is terminated, the process is killed, the check is disrupted, and the appliance may be left in an unstable state.

Step 4 (Optional) Monitor the readiness check.

If you use the `--detach` option (or begin another shell session), you can use the `tail` or `tail`f command to display logs, for example:

- Firepower Threat Defense devices: `tail /ngfw/var/log/sf/update_package_name/status.log`
- All other Firepower appliances: `tail /var/log/sf/update_package_name/status.log`

If you use `tailf` to display log entries as they occur, you must cancel (Ctrl+C) to return to the command prompt.

Step 5 When the readiness check completes, access the full readiness check report.

- Firepower Threat Defense devices: `/ngfw/var/log/sf/$rpm_name/upgrade_readiness`
- All other Firepower appliances: `/var/log/sf/$rpm_name/upgrade_readiness`

Run a Readiness Check through the Firepower Management Center Web Interface

You can use the Firepower Management Center web interface to perform readiness checks on itself and its standalone managed devices.

Before you begin

- Readiness checks are included in upgrade packages. Note that upgrade packages from Version 6.2.1+ are *signed*, and terminate in .sh.REL.tar instead of just .sh. Do *not* untar signed upgrade packages before performing either a readiness check or the upgrade itself.
- Redeploy configuration changes to any managed devices. Otherwise, the readiness check may fail.

Step 1 On the Firepower Management Center web interface, choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade you want the readiness check to evaluate.

Step 3 Click **Launch Readiness Check**.

Step 4 Monitor the progress of the readiness check in the Message Center.
When the readiness check completes, the system reports success or failure on the Readiness Check Status page.

Step 5 Access the full readiness check report in `/var/log/sf/$rpm_name/upgrade_readiness`.

Pre-Update Configuration and Event Backups

Before you begin the update, we *strongly* recommend that you back up current event and configuration data to an external location. You should also copy any locally stored backups to an external location, because the Firepower Management Center purges locally stored backups from previous updates.

Use the Firepower Management Center to back up event and configuration data for itself and the devices it manages. For more information on the backup and restore feature, see the Firepower Management Center Configuration Guide.

Note Verify that external backups are successful before you begin the update.

Patch or Hotfix for New Dynamic Analysis CA Certificate

Deployments: AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Upgrading from: A patched/hotfixed system with new CA certificates

Directly to: Version 6.2 through 6.2.3

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. In Version 6.1+ deployments, you can obtain a new certificate with a patch or hotfix. For earlier versions, you must upgrade to at least Version 6.1, then patch or hotfix.

If you already patched or hotfixed your deployment, upgrading to a later major version (Version 6.2 through 6.2.3) reverts to the old certificate and disables dynamic analysis. You must patch or hotfix again.

Note If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Managed devices submit files to the cloud for dynamic analysis; the FMC queries for results.

The following table lists the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site. For release notes, see Firepower Release Notes.

Table 9: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC, NGIPS devices
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC, NGIPS devices
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	

Traffic Flow and Inspection During the Update

When you update your sensing devices, traffic either drops throughout the update or traverses the network without inspection depending on how your devices are configured and deployed: routed or transparent, inline versus passive, bypass mode settings, and so on. We *strongly* recommend performing the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

Note When you update devices in a high availability pair, the system performs the update one device at a time to avoid traffic interruption.

This section discusses traffic behavior during the followng update stages:

- The update itself, including related reboots
- FXOS updates on clustered Firepower Threat Defense devices
- Configuration deployments after the update

Traffic Behavior During the Update

The following table describes how updates, including related device reboots, affect traffic flow for different deployments. Note that switching, routing, NAT, and VPN are not performed during the update process, regardless of how you configure any inline sets.

Caution Do *not* update to FXOS Version 2.3.1.56 if you are running an instance of Firepower Threat Defense that has been updated from Version 6.0.1.x of the Firepower System. Doing so may disable your Firepower Threat Defense application, which could interrupt traffic on your network. As a workaround, use FXOS Version 2.3.1.58 or later. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Table 10: Update Traffic Behavior

Device	Deployment	Traffic Behavior
Firepower Threat Defense	inline with optional hardware bypass module; bypass enabled: (**Bypass: Standby** or **Bypass-Force**) or, bypass disabled: (**Bypass: Disabled**)	dropped
Firepower Threat Defense Firepower Threat Defense Virtual	inline with no hardware bypass module; routed, transparent (including EtherChannel, redundant, subinterface)	
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
7000 and 8000 Series	inline with optional hardware bypass module, bypass enabled (**Bypass Mode: Bypass**)	passed without inspection Note that traffic is interrupted briefly at two points: • At the beginning of the update process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the update finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces. The hardware bypass option is *not* supported on nonbypass network modules on Firepower 8000 Series devices, or SFP transceivers on Firepower 7000 Series.
	inline with optional hardware bypass module, bypass disabled (**Bypass Mode: Non-Bypass**)	dropped

Device	Deployment	Traffic Behavior
7000 and 8000 Series NGIPSv	inline with no hardware bypass module	dropped
	inline in tap mode	egress packet immediately, copy not inspected
	passive	uninterrupted, not inspected
	routed, switched	dropped
ASA FirePOWER	routed or transparent, fail-open (**Permit Traffic**)	passed without inspection (requires the latest supported ASA OS version; otherwise, traffic dropped)
	routed or transparent, fail-close (**Close Traffic**)	dropped

⚠

Caution Rebooting the ASA FirePOWER module on an ASA 5585-X, including a reboot that occurs during a module upgrade, causes traffic to drop for up to thirty seconds on the interfaces on the ASA FirePOWER hardware module while the module reboots.

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

Updating FXOS reboots the chassis, which can affect traffic in a clustered environment until at least one module comes online. Whether and how traffic is affected depends on the cluster type:

- **Intra-chassis cluster**—Traffic drops if the cluster does not use an optional hardware bypass (fail-to-wire) module or if bypass is disabled. Traffic passes without inspection if bypass is enabled.
- **Inter-chassis cluster**—Traffic drops during the overlap if multiple chassis reboots overlap before at least one module comes online. Traffic is unaffected if there is no reboot overlap.

  For example, there would be no reboot overlap, and no dropped traffic, if you complete the FXOS update first on one chassis and then on another. Depending on when each update is initiated, there could be reboot overlap (and dropped traffic) if you update multiple chassis simultaneously.

The following table summarizes this behavior.

Table 11: Traffic Behavior During an FXOS Update of Clustered Firepower Threat Defense Devices

Device Model	Deployment	Traffic Behavior
Firepower 9300	intra-chassis cluster without optional hardware bypass module	dropped
	intra-chassis cluster with optional hardware bypass module, bypass disabled	dropped
	intra-chassis cluster with optional hardware bypass module, bypass enabled	passed without inspection
Firepower 9300 Firepower 4100 Series	inter-chassis cluster with no reboot overlap	unaffected
	inter-chassis cluster with reboot overlap before at least one module comes online	dropped

Traffic Behavior During Configuration Deployment

During the upgrade process, you deploy configurations either twice (standalone devices) or three times (devices managed by the Firepower Management Center). When you deploy, resource demands may result in a small number of packets dropping without inspection. In most cases, the deployment immediately after the upgrade restarts the Snort process. During subsequent deployments, the Snort process restarts only if, before deploying, you modify specific policy or device configurations that always restart the process when deployed.

The following table describes how different devices handle traffic during Snort process restarts.

Table 12: Restart Traffic Effects by Managed Device Model

Device Model	Interface Configuration	Restart Traffic Behavior
Firepower Threat Defense, Firepower Threat Defense Virtual	inline, **Snort Fail Open: Down**: enabled	passed without inspection
	inline, **Snort Fail Open: Down**: disabled	dropped
	routed, transparent (including EtherChannel, redundant, subinterface)	dropped
	inline, tap mode	egress packet immediately, copy bypasses Snort
	passive	uninterrupted, not inspected

Device Model	Interface Configuration	Restart Traffic Behavior
7000 and 8000 Series, NGIPSv	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
7000 and 8000 Series	routed, switched, transparent	dropped
ASA FirePOWER	routed or transparent with fail-open (**Permit Traffic**)	passed without inspection
	routed or transparent with fail-close (**Close Traffic**)	dropped

Time and Disk Space Requirements

About Time Estimates

Upgrade time estimates are based on in-house tests.

Estimates for devices are from tests in a Firepower Management Center deployment. This is because raw upgrade times for remotely and locally managed devices are similar, given similar conditions.

Because lower-memory appliances tend to take longer to upgrade, we try to test on those platforms. For virtual platforms, we use the default settings for memory and resources. However, upgrades may still take longer than the provided estimates for any of the following reasons.

Push and Reboot Not Included

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

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

Estimates also do not include reboots. We do not have estimates for readiness checks, separate operating system upgrades, or configuration deploys.

Time Is per Device

Estimates are *per device*. In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device. Stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly longer than upgrading a standalone device.

Affected Configurations and Data

We perform time tests 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.

Version 6.2.2.5 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on FMC	Time
FMC	25 MB	5271 MB	—	From 6.2.2: 60 min From 6.2.2.4: 42 min
FMCv	33 MB	5292 MB	—	Hardware dependent
Firepower 2100 series	9113 MB	9113 MB	2 GB	From 6.2.2: 87 min From 6.2.2.4: 32 min
Firepower 4100/9300 chassis	3325 MB	3325 MB	612 MB	From 6.2.2: 28 min From 6.2.2.4: 12 min
ASA 5500-X series with FTD	226 MB	3809 MB	724 MB	From 6.2.2: 49 min From 6.2.2.4: 25 min
FTDv	226 MB	3809 MB	724 MB	Hardware dependent
Firepower 7000/8000 series	28 MB	566 MB	419 MB	From 6.2.2: 54 min From 6.2.2.4: 12 min
ASA FirePOWER	28 MB	3714 MB	432 MB	From 6.2.2: 215 min From 6.2.2.4: 105 min
NGIPSv	24 MB	3799 MB	98 MB	Hardware dependent

Version 6.2.2.4 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on FMC	Time
FMC	217 MB	4435 MB	—	From 6.2.2: 85 min From 6.2.2.3: 42 min
FMCv	48 MB	3691 MB	—	Hardware dependent
Firepower 2100 series	6965 MB	6965 MB	1 GB	From 6.2.2: 58 min From 6.2.2.3: 34 min
Firepower 4100/9300 chassis	1676 MB	1676 MB	339 MB	From 6.2.2: 24 min From 6.2.2.3: 13 min
ASA 5500-X series with FTD	225 MB	1695 MB	427 MB	From 6.2.2: 142 min From 6.2.2.3: 68 min
FTDv	225 MB	1695 MB	427 MB	Hardware dependent
Firepower 7000/8000 series	36 MB	3343 MB	414 MB	From 6.2.2: 45 min From 6.2.2.3: 19 min
ASA FirePOWER	27 MB	3192 MB	405 MB	From 6.2.2: 182 min From 6.2.2.3: 80 min
NGIPSv	28 MB	444 MB	94 MB	Hardware dependent

Version 6.2.2.3 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on FMC	Time
FMC	205 MB	3766.6 MB	—	From 6.2.2: 66 min From 6.2.2.2: 41 min
FMCv	17.5 MB	3485 MB	—	Hardware dependent
Firepower 2100 series	4486.64 MB	4486.64 MB	132 MB	From 6.2.2: 61 min From 6.2.2.2: 36 min
Firepower 4100/9300 chassis	811.7 MB	811.7 MB	132 MB	From 6.2.2: 20 min From 6.2.2.2: 12 min
ASA 5500-X series with FTD	125.1 MB	1636.6 MB	199 MB	From 6.2.2: 35 min From 6.2.2.2: 20 min
FTDv	125 MB	1810.7 MB	199 MB	Hardware dependent

Platform	Space on /	Space on /Volume	Space on FMC	Time
Firepower 7000/8000 series	17 MB	2775 MB	339 MB	From 6.2.2: 80 min From 6.2.2.2: 42 min
ASA FirePOWER	15.69 MB	2301.5 MB	308 MB	From 6.2.2: 184 min From 6.2.2.2: 100 min
NGIPSv	17.5 MB	576.3 MB	20 MB	Hardware dependent

Version 6.2.2.2 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on FMC	Time
FMC	18 MB	1656 MB	—	From 6.2.2: 34 min From 6.2.2.1: 27 min
FMCv	19 MB	2356 MB	—	Hardware dependent
Firepower 2100 series	2377 MB	2377 MB	497 MB	From 6.2.2: 41 min From 6.2.2.1: 20 min
Firepower 4100/9300 chassis	561 MB	561 MB	41 MB	From 6.2.2: 21 min From 6.2.2.1: 13 min
ASA 5500-X series with FTD	122 MB	984 MB	136 MB	From 6.2.2: 110 min From 6.2.2.1: 70 min
FTDv	122 MB	984 MB	136 MB	Hardware dependent
Firepower 7000/8000 series	16 MB	1706 MB	310 MB	From 6.2.2: 56 min From 6.2.2.1: 40 min
ASA FirePOWER	15 MB	1602 MB	190 MB	From 6.2.2: 113 min From 6.2.2.1: 80 min
NGIPSv	17 MB	170 MB	16 MB	Hardware dependent

Version 6.2.2.1 Time and Disk Space

Platform	Space on /	Space on /Volume	Space on FMC	Time from 6.2.2
FMC	18 MB	480 MB	—	52 min
FMCv	30 MB	775 MB	—	Hardware dependent
Firepower 2100 series	1003 MB	1003 MB	47 MB	28 min

Platform	Space on /	Space on /Volume	Space on FMC	Time from 6.2.2
Firepower 4100/9300 chassis	299 MB	299 MB	47 MB	35 min
ASA 5500-X series with FTD	121 MB	674 MB	69 MB	72 min
FTDv	121 MB	674 MB	69 MB	Hardware dependent
Firepower 7000/8000 series	14 MB	664 MB	61 MB	33 min
ASA FirePOWER	15 MB	758 MB	83 MB	90 min
NGIPSv	17 MB	106 MB	10 MB	Hardware dependent

CHAPTER 6

Update to Version 6.2.2.x

Before you begin, you must thoroughly read and understand these release notes, especially Before You Update: Important Notes, on page 17 and Pre-Update Readiness Checks, on page 23.

If you are unsure whether you should update or perform a fresh install, see Freshly Install Version 6.2.2, on page 55.

Note Updates can require large data transfers from the Firepower Management Center to managed devices. Before you begin, make sure your management network has sufficient bandwidth to successfully perform the transfer. See the Troubleshooting Tech Note at https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html.

The update process differs depending on which component of the system you are updating, and for devices, the implementation and manager. For more information, see the following topics:

Note Devices running Version 6.2.2.1, Version 6.2.2.2, Version 6.2.2.3, and Version 6.2.2.4 that are configured for Threat Grid integration may be unable to pull reports from Threat Grid or submit files manually for analysis, per CSCvj07038. See Patch or Hotfix for New Dynamic Analysis CA Certificate, on page 26 for more information.

- Update Firepower Management Centers, on page 37
- Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 40
- Update ASA FirePOWER Modules Managed with ASDM, on page 42
- Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 43
- Update Firepower Threat Defense Devices with the Firepower Device Manager, on page 46

Update Firepower Management Centers

Use this procedure to update all Firepower Management Centers. If you are using high availability, see Update Sequence for Firepower Management Centers in High Availability, on page 21 before you begin.

This update causes a reboot.

⚠

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.2.x, on page 17.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments, on page 5
- Before You Update: Important Notes, on page 17

Step 3 Download the update from the Support site:

- Upgrade Firepower Management Center (MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500) and Firepower Management Center Virtual:

  Sourcefire_3D_Defense_Center_S3_Patch-6.2.2.x-xxxx.sh.REL.tar

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 4 Upload the update to the Firepower Management Center.

Choose **System** > **Updates**. On the Product Updates tab, click **Upload Update**. Click **Choose File** to browse to the update, then click **Upload**.

The web interface shows the type of update you uploaded, its version number, the date and time it was generated, and whether the update causes a reboot.

Step 5 Deploy configuration changes to the devices you plan to update. Otherwise, eventual device updates may fail.

When you deploy before updating the Firepower Management Center, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Configurations that Restart the Snort Process When Deployed or Activated and Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*.

Step 6 (Optional) Run a readiness check.

See Run a Readiness Check through the Shell, on page 24 or Run a Readiness Check through the Firepower Management Center Web Interface, on page 25.

Caution If you encounter issues with the readiness check that you cannot resolve, do not begin the update. Instead, contact Cisco TAC.

Step 7 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 8 Make sure there are no essential tasks in progress.

Click the system status icon to view the Tasks tab in the Message Center. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages after the update completes.

Step 9 Choose the update you uploaded earlier.

In the **System** > **Updates** page, click the install icon next to the update you are installing.

Step 10 Install the update and monitor its progress.

Choose the Firepower Management Center and click **Install**. Confirm that you want to install the update and reboot.

You can begin monitoring the update's progress on the Tasks tab of the Message Center. However, after the Firepower Management Center completes its necessary pre update checks, you are logged out. When you log back in, the Upgrade Status page displays a progress bar and provides details about the script currently running.

Caution If you encounter issues with the update (for example, if a manual refresh of the Update Status page shows no progress for several minutes, or if the page indicates that the update has failed), do *not* restart the update. Instead, contact Cisco TAC.

Step 11 After the update finishes, clear your browser cache and relaunch the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 12 Log into the Firepower Management Center.

Step 13 Verify update success.

Choose **Help** > **About** and confirm that the software version is listed correctly. Also note the versions of the intrusion rule update and Vulnerability Database (VDB); you will need this information later.

Step 14 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 15 Update intrusion rules and the Vulnerability Database (VDB).

If the intrusion rule update or the VDB available on the Support site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide

When you install the intrusion rule update, you do not need to automatically reapply policies. You will manually deploy configuration changes, which also reapplies policies.

Step 16 Deploy configuration changes to all managed devices.

In most cases, deploying for the first time after you update the Firepower Management Center restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*.

Step 17 Update to the latest patch, if necessary.

You must update to the latest patch to take advantage of product enhancements and security fixes. If a later patch is available on the Support site, use the Firepower System Release Notes for that version to update the system.

Step 18 If you updated Firepower Management Centers in a high availability pair, restart communication.

For more information, see Update Sequence for Firepower Management Centers in High Availability, on page 21.

Update Firepower Threat Defense Devices Using the Firepower Management Center

Use this procedure to update Firepower Threat Defense devices using the Firepower Management Center. You can update multiple devices at once if they use the same update file. If you are using device high availability or clustering, make sure you understand the Update Sequence Guidelines, on page 20 before you begin.

For devices running or hosted on a non-Firepower operating system (for example, ASA OS or FXOS), you *must* update the operating system to the latest supported version. To update the ASA OS version, see Upgrade the ASA. To update the FXOS version, see Cisco FXOS Release Notes.

This update causes a reboot.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.2.x, on page 17.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments, on page 5
- Before You Update: Important Notes, on page 17

Step 3 Update Firepower Management Centers, on page 37.

We *strongly* recommend upgrading the Firepower Management Center to the same maintenance release or later as the version you upgrade the managed device to. As an example, we recommend a Firepower Management Center run at least Version 6.2.2.1 before you upgrade a managed device to Version 6.2.2.1.

Step 4 Deploy configuration changes to the devices you plan to update. Otherwise, eventual device updates may fail.

In most cases, deploying for the first time after you update the Firepower Management Center restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see the Snort® Restart Traffic Behavior section in the *Firepower Management Center Configuration Guide*, Version 6.2.2.

Step 5 For Firepower 4100 series and Firepower 9300 FXOS-based devices, update the operating system to FXOS Version 2.2(2), if you are not already using that version.

See the Cisco FXOS Release Notes for information on updating FXOS. To update FXOS on high availability pairs, update the operating system on the standby, switch failover, then update the new standby; see Update Sequence for High Availability Firepower Threat Defense Devices, on page 21.

Updating FXOS causes an expected disruption in traffic. Updating FXOS also reboots the chassis, which drops traffic or passes it uninspected in an intra-chassis cluster depending on whether the cluster uses an enabled hardware bypass module, and drops traffic in an inter-chassis cluster only if chassis reboots overlap before at least one module comes online.

Step 6 Download the update from the Support site:

- ASA 5500-X Series with Firepower Threat Defense:

  Cisco_FTD_Patch-6.2.2.x-xxxx.sh.REL.tar

- Firepower Threat Defense Virtual (VMware, AWS, KVM, or Microsoft Azure):

  Cisco_FTD_Patch-6.2.2.x-xxxx.sh.REL.tar

- Firepower 4100 series or Firepower 9300 security appliance with Firepower Threat Defense:

  Cisco_FTD_SSP_Patch-6.2.2.x-xxxx.sh.REL.tar

- Firepower 2100 series with Firepower Threat Defense:

  Cisco_FTD_SSP_FP2K_Patch-6.2.2.x-xxxx.sh.REL.tar

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 7 Upload the update to the Firepower Management Center.

Choose **System** > **Updates**. On the Product Updates tab, click **Upload Update**. Click **Choose File** to browse to the update, then click **Upload**.

The web interface shows the type of update you uploaded, its version number, the date and time it was generated, and whether the update causes a reboot.

Step 8 (Optional) Run a readiness check.

See Run a Readiness Check through the Shell, on page 24 or Run a Readiness Check through the Firepower Management Center Web Interface, on page 25.

Caution If you encounter issues with the readiness check that you cannot resolve, do not begin the update. Instead, contact Cisco TAC.

Step 9 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 10 Choose the update you uploaded earlier.

In the **System** > **Updates** page, click the install icon next to the update you are installing.

Step 11 Choose the devices where you want to install the update.

The system does not allow you to choose an ineligible device. If you cannot choose the device you want to update, make sure you downloaded the correct file.

Step 12 Install the update and monitor its progress.

Click **Install**. Confirm that you want to install the update and reboot devices. Devices may reboot twice; this is expected. You can monitor the update's progress on the Tasks tab of the Message Center.

Caution If you encounter issues with the update (for example, if messages on the Tasks tab of the Message Center show no progress for several minutes or indicate that the update has failed), do not restart the update. Instead, contact Cisco TAC.

Step 13 Verify update success.

After the update process completes, choose **Devices** > **Device Management** and verify that the devices you updated have the correct software version.

Step 14 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 15 Deploy configuration changes to all managed devices.

When you deploy for the first time after updating a device, resource demands may result in a small number of packets dropping without inspection. The deploy does not otherwise interrupt traffic inspection unless, since the previous deploy, you have modified specific policy or device configurations that always restart the Snort process when you deploy them. If you have modified any of these configurations, traffic drops or passes without further inspection during the restart depending on how the device handles traffic. For more information, see the Configurations that Restart the Snort Process When Deployed or Activated and Snort® Restart Traffic Behavior sections in the *Firepower Management Center Configuration Guide*, Version 6.2.2.

Step 16 Update to the latest patch, if necessary.

You must update to the latest patch to take advantage of product enhancements and security fixes. If a later patch is available on the Support site, use the Firepower System Release Notes for that version to update the system.

Update ASA FirePOWER Modules Managed with ASDM

Use this procedure to update locally managed ASA FirePOWER modules using ASDM. Resolving issues may require that you **also** update ASA OS to the latest supported version.

This update causes a reboot.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.0.x.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments, on page 5
- Before You Update: Important Notes, on page 17

Step 3 Update to the latest supported ASA OS.
See the ASA/ASDM Release Notes, Cisco ASA Compatibility, and the Firepower Compatibility Guide.

Step 4 Download the update from the Support site:

Cisco_Network_Sensor_Patch-6.2.2.x-xxxx.sh.REL.tar

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 5 Upload the update.

Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**. On the Product Updates tab, click **Upload Update**. Click **Choose File** to browse to the update, then click **Upload**.

Step 6 Deploy configuration changes. Otherwise, the eventual update may fail.

Deploying may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

Step 7 Make sure there are no essential tasks in progress.

Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Task Status**. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages after the update completes.

Step 8 Install the update and monitor its progress.

Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**. On the Product Updates tab, click the install icon next to the update. You can begin monitoring the update's progress in the task queue.

Caution If you encounter issues with the update (for example, if a manual refresh of the task queue shows no progress for several minutes, or if the page indicates that the update has failed), do **not** restart the update. Instead, contact Cisco TAC.

Step 9 After the update finishes, reconnect ASDM to the ASA device as described in the ASA FirePOWER Module Quick Start Guide.

Step 10 Verify update success.

Choose **Configuration** > **ASA FirePOWER Configuration** > **System Information** and confirm that the software version is listed correctly. Also note the versions of the intrusion rule update and Vulnerability Database (VDB); you will need this information later.

Step 11 Update intrusion rules and the Vulnerability Database (VDB).

If the intrusion rule update or the VDB available on the Support site is newer than the version currently running, install the newer version. For more information, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

When you install the intrusion rule update, you do not need to automatically reapply policies. You will manually deploy configuration changes, which also reapplies policies.

Step 12 Deploy configuration changes.

Deploying may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center

Use this procedure to update 7000 and 8000 Series devices, NGIPSv, and ASA FirePOWER modules using the Firepower Management Center. You can update multiple devices at once if they use the same update file. If you are using device high availability, clustering, or stacking, make sure you understand the Update Sequence Guidelines, on page 20 before you begin.

For ASA FirePOWER, resolving issues may require that you *also* update ASA OS to the latest supported version.

This update causes a reboot.

Caution Do *not* manually reboot, shut down the system, or restart the update until you see the login prompt. The system may appear inactive during prechecks; this is expected. If you encounter issues with the update, contact Cisco TAC.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.2.x, on page 17.

Step 2 Read these release notes and complete any pre update tasks.

For more information, see the following topics:

- Platforms and Environments, on page 5
- Before You Update: Important Notes, on page 17

Step 3 Update Firepower Management Centers, on page 37.

We *strongly* recommend upgrading the Firepower Management Center to the same maintenance release or later as the version you upgrade the managed device to. As an example, we recommend a Firepower Management Center run at least Version 6.2.2.1 before you upgrade a managed device to Version 6.2.2.1.

Step 4 Deploy configuration changes to the devices you plan to update. Otherwise, eventual device updates may fail.

In most cases, deploying for the first time after you update the Firepower Management Center restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic. For more information, see Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*.

Step 5 For ASA with FirePOWER Services, update to the latest supported ASA OS.

See the ASA/ASDM Release Notes landing page, Cisco ASA Compatibility, and the Firepower Compatibility Guide.

Step 6 Download the update from the Support site:

- 7000 and 8000 Series:

  Sourcefire_3D_Device_S3_Patch-6.2.2.x-xxxx.sh.REL.tar

- NGIPSv:

  Sourcefire_3D_Device_Virtual64_VMware_Patch-6.2.2.x-xxxx.sh.REL.tar

- ASA with FirePOWER Services:

  Cisco_Network_Sensor_Patch-6.2.2.x-xxxx.sh.REL.tar

Note Download the update directly from the Support site. If you transfer an update file by email, it may become corrupted. Also, keep in mind that many update file names look similar. Make sure you download the correct update.

Step 7 (Optional) Run a readiness check.

See Run a Readiness Check through the Shell, on page 24 or Run a Readiness Check through the Firepower Management Center Web Interface, on page 25.

Caution If you encounter issues with the readiness check that you cannot resolve, do not begin the update. Instead, contact Cisco TAC.

Step 8 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 9 Choose the update you uploaded earlier.

In the **System** > **Updates** page, click the install icon next to the update you are installing.

Step 10 Choose the devices where you want to install the update.

Many update file names look similar. The system does not allow you to choose an ineligible device. If you cannot choose the device you want to update, make sure you downloaded the correct file.

If you are updating stacked 8000 Series devices, choosing one member of the stack automatically chooses the other devices in the stack. You must update members of a stack together.

Step 11 Install the update and monitor its progress.

Click **Install**. Confirm that you want to install the update and reboot devices. Devices may reboot twice; this is expected. You can monitor the update's progress on the Tasks tab of the Message Center.

Caution If you encounter issues with the update (for example, if messages on the Tasks tab of the Message Center show no progress for several minutes or indicate that the update has failed), do not restart the update. Instead, contact Cisco TAC.

Step 12 Verify update success.

After the update process completes, choose **Devices** > **Device Management** and verify that the devices you updated have the correct software version.

Step 13 Verify that the appliances in your deployment are successfully communicating with the managing Firepower Management Center and that there are no issues reported by the health monitor.

Step 14 Deploy configuration changes to all managed devices.

When you deploy for the first time after updating a device, resource demands may result in a small number of packets dropping without inspection. The deploy does not otherwise interrupt traffic inspection unless, since the previous deploy, you have modified specific policy or device configurations that always restart the Snort process when you deploy them. If you have modified any of these configurations, traffic drops or passes without further inspection during the restart depending on how the device handles traffic. For more information, see Configurations that Restart the Snort Process When Deployed or Activated and Snort® Restart Traffic Behavior in the *Firepower Management Center Configuration Guide*.

Step 15 Update to the latest patch, if necessary.

You must update to the latest patch to take advantage of product enhancements and security fixes. If a later patch is available on the Support site, use the Firepower System Release Notes for that version to update the system.

Update Firepower Threat Defense Devices with the Firepower Device Manager

Updating Firepower Threat Defense using this procedure also updates Firepower Device Manager.

Step 1 Download the update from the Support site:

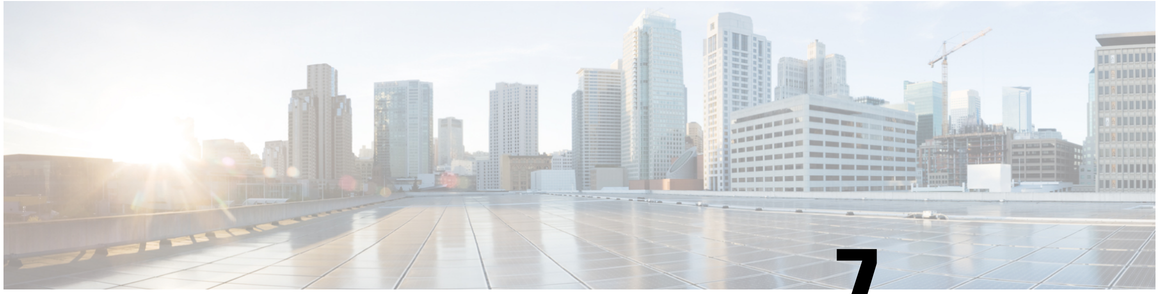
- ASA 5500-X Series with Firepower Threat Defense:

  Cisco_FTD_Patch-6.2.2.x-xxxx.sh.REL.tar

- Firepower 2100 series with Firepower Threat Defense:

  Cisco_FTD_SSP_FP2K_Patch-6.2.2.x-xxxx.sh.REL.tar

Step 2 Follow the instructions for updating Firepower Threat Defense in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.



CHAPTER 7

Uninstall Version 6.2.2.x

Warning If you enabled security certifications compliance before the upgrade, you cannot uninstall Version 6.2.2.2. If you want to go back to an earlier patch, you must either restore from a pre-upgrade backup, or reimage to Version 6.2.2 and then upgrade to your target patch.

Order of Uninstallation

Uninstall the update in the reverse order that you installed it. That is, first uninstall the update from managed devices, then from Firepower Management Centers.

You must uninstall updates locally. You *cannot* use a Firepower Management Center to uninstall the update from a managed device.

Track the Uninstallation

To watch the uninstallation process, access the device through the shell and navigate to the **/var/log/sf/**<*uninstaller file name folder*> directory, then execute the **tail –f main_upgrade_script.log** shell command. Once the uninstallation process is complete, the system generates a upgrade completed message in the file **main_upgrade_script.log**.

Uninstall Firepower Threat Defense Devices in High Availability

Firepower Threat Defense devices in high availability pairs must run the same Firepower version.

You cannot uninstall Firepower Threat Defense devices in high availability. Before you uninstall, you must break the high availability and uninstall each device independently, then reform the high availability pair.

Uninstall from Clustered Firepower Threat Defense Devices

To avoid dropping traffic, uninstall from the slave units before uninstalling from the master unit of a cluster.

Note If the uninstallation process on a clustered device fails, do not restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

Step 1 Verify the Firepower Threat Defense devices within the cluster are healthy and operating normally. Determine which member of the cluster is the master and which member is the slave.

Step 2 Uninstall the update from each slave unit one at a time.

While the slave unit uninstalls, the other slave units and the master unit continue to process traffic.

Step 3 On the master unit, uninstall the software.

While the master unit uninstalls, one of the slave units becomes the master and continues to process traffic.

Step 4 Once the uninstall completes on the master unit, the termporary master unit returns to the slave state and reforms the cluster.

Uninstall the Update from Clustered 7000 and 8000 Series Devices

Clustered devices, devices in high availability pairs and Firepower Management Centers in high availability pairs must run the same Firepower version. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

Note If the uninstallation process on a clustered device fails, do not restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

To ensure continuity of operations, uninstall the update from clustered devices one at a time.

Step 1 Uninstall the update from the secondary appliance.

While the secondary appliance uninstalls, the active appliance continues to forward traffic to the Firepower Management Center.

Step 2 Uninstall the update from the active appliance.

While the active appliance uninstalls, the secondary appliance temporarily becomes active and continues to forward traffic to the Firepower Management Center. Once the uninstall completes, the secondary appliances returns and the appliances reform the cluster.

Step 3 Once the uninstall completes on the secondary unit, the termporary primary unit returns to the secondary state and reforms the cluster.

Uninstall the Update from Stacked 7000 and 8000 Series Devices

All devices in a stack must run the same Firepower version. Uninstalling the update from any of the stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, we recommend you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the uninstallation completes on all devices in the stack.

Uninstall the Update from Devices Deployed Inline

Managed devices do not perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. See Pre-Update Configuration and Event Backups, on page 25 for more information.

Uninstall Firepower Management Centers in High Availability

Firepower Management Centers in high availability pairs must run the same Firepower version. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

Note If the uninstallation process on Firepower Management Centers in a high availability pair fails, do not restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

To ensure continuity of operations, uninstall the update from paired Firepower Management Centers one at a time.

Step 1 Pause high availability synchronization, as described in Pausing Communication Between Paired Firepower Management Centers

Step 2 Uninstall the update from the standby Firepower Management Center first.

The uninstallation completes.

Step 3 Uninstall the update from the active Firepower Management Center.

The uninstallation completes.

Step 4 Resume high availability synchronization, as described in Restarting Communication Between Paired Firepower Management Centers

Step 5 Click **Make Me Active** for the Firepower Management Center you want act as active. The Firepower Management Center you do not make active automatically switches to standby mode. Communication between the Firepower Management Center peers automatically restarts.

After the Uninstall

After you uninstall the update, there are several steps you should take to ensure that your deployment is performing properly, such as verifying that the uninstall succeeded and that all appliances in your deployment are communicating successfully.

Uninstall Firepower Threat Defense Devices and Firepower Threat Defense Virtual Devices Managed by Firepower Management Center

Uninstalling the update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Pre-Update Configuration and Event Backups, on page 25.

Step 1 Read and understand Order of Uninstallation, on page 47.

Step 2 Log into the device as **admin**, via SSH or through the virtual console.

Step 3 Initiate connection between Firepower 2100 Series, Firepower 4100 Series, and Firepower 9300 Security Appliances and the console before you uninstall.

a) For Firepower 2100 Series devices, type **connect ftd** .

b) For Firepower 4100 Series devices and Firepower 9300 Security Appliances, type **connect module <slot number> console** and then **connect ftd** .

Step 4 At the CLI prompt, type **expert** to access the bash shell.

Step 5 At the bash shell prompt, type **sudo su -**.

Step 6 Type the admin password to continue the process with root privileges.

Step 7 At the prompt, enter the following on a single line: **install_update.pl --detach**`/var/sf/updates/filename_Patch_Uninstaller-<version>-<build>.REL.tar`

The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 8 After the uninstallation is complete, the device reboots.

Step 9 Log into the managing Firepower Management Center and select **Devices** > **Device Management**. Confirm that the device where you uninstalled the update has the correct software version.

Step 10 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall ASA FirePOWER Modules Managed by a Firepower Management Center

Uninstalling the update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Pre-Update Configuration and Event Backups, on page 25.

Step 1 Read and understand Order of Uninstallation, on page 47.

Step 2 Log into the device as **admin**, via SSH or through the virtual console.

Step 3 At the CLI prompt, type **session sfr console**.

Step 4 At the CLI prompt, type **expert** to access the bash shell.

Step 5 At the bash shell prompt, type **sudo su -**.

Step 6 Type the admin password to continue the process with root privileges.

Step 7 At the prompt, enter the following on a single line: **install_update.pl --detach**`/var/sf/updates/filename_Patch_Uninstaller-<version>-<build>.REL.tar`

The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 8 After the uninstallation is complete, the device reboots.

Step 9 Log into the managing Firepower Management Center and select **Devices** > **Device Management**. Confirm that the device where you uninstalled the update has the correct software version.

Step 10 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall 7000 Series and 8000 Series Managed devices

Uninstalling the update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Pre-Update Configuration and Event Backups, on page 25.

Step 1 Read and understand Order of Uninstallation, on page 47.

Step 2 Log into the device as **admin**, via SSH or through the virtual console.

Step 3 At the CLI prompt, type **expert** to access the bash shell.

Step 4 At the bash shell prompt, type **sudo su -**.

Step 5 Type the admin password to continue the process with root privileges.

Step 6 At the prompt, enter the following on a single line: **install_update.pl --detach**`/var/sf/updates/filename_Patch_Uninstaller-<version>-<build>.REL.tar`

The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 7 After the uninstallation is complete, the device reboots.

Step 8 Log into the managing Firepower Management Center and select **Devices** > **Device Management**. Confirm that the device where you uninstalled the update has the correct software version.

Step 9 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall NGIPSv Devices

Uninstalling the update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Pre-Update Configuration and Event Backups, on page 25.

Step 1 Read and understand Order of Uninstallation, on page 47.

Step 2 Log into the device as **admin**, via SSH or through the virtual console.

Step 3 At the CLI prompt, type **expert** to access the bash shell.

Step 4 At the bash shell prompt, type **sudo su -**.

Step 5 Type the admin password to continue the process with root privileges.

Step 6 At the prompt, enter the following on a single line: **install_update.pl --detach**`/var/sf/updates/filename_Patch_Uninstaller-<version>-<build>.REL.tar`

The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 7 After the uninstallation is complete, the device reboots.

Step 8 Log into the managing Firepower Management Center and select **Devices** > **Device Management**. Confirm that the device where you uninstalled the update has the correct software version.

Step 9 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall Firepower Management Centers

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the Firepower System Release Notes for that version.

Step 1 Read and understand Order of Uninstallation, on page 47.

Step 2 On the managing Firepower Management Center, make sure that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Step 3 On the managed device, click the system status icon and view the Tasks tab in the Message Center to make sure there are no tasks in progress.

Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the Tasks tab after the uninstallation completes.

Step 4 Choose **System** > **Updates**.

Step 5 Click the install icon next to the uninstaller that matches the update you want to remove, then confirm that you want to uninstall the update and reboot the device.

You can monitor the uninstallation progress in the Tasks tab of the Message Center.

Note Do *not* use the UI to perform any other tasks until the uninstallation is complete and the device reboots. Before the uninstallation completes, the web interface may become unavailable and the device may log you out. This is expected behavior; log in again to view the Tasks tab. If the uninstallation is still running, do *not* use the web interface until the uninstallation is complete. If you encounter issues with the uninstallation (for example, if the Tasks tab indicates that the update has failed or if the Tasks tab shows no progress for several minutes), do *not* restart the uninstallation. Instead, contact Cisco TAC.

Step 6 After the uninstallation is complete, the appliance reboots.

Step 7 Clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 8 Log in to the device.

Step 9 Choose **Help** > **About** and confirm that the correct software version is listed.

Step 10 On the managing Firepower Management Center, verify that the appliances in your deployment successfully communicate with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall ASA FirePOWER Modules Managed By ASDM

Uninstalling the update results in a device running the previous version. For information on uninstalling a previous version, see to the Firepower System Release Notes for that version.

Uninstalling the update reboots the device. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Pre-Update Configuration and Event Backups, on page 25.

Step 1 Read and understand Order of Uninstallation, on page 47.

Step 2 Log into the device as **admin**, through SSH or the virtual console.

Step 3 At the CLI prompt, type **expert** to access the bash shell.

Step 4 At the bash shell prompt, type **sudo su -**.

Step 5 Type the admin password to continue the process with root privileges.

Step 6 At the prompt, enter the following on a single line: **install_update.pl --detach**`/var/sf/updates/filename_Patch_Uninstaller-<version>-<build>.REL.tar`

The uninstallation process begins.

Note If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.

Step 7 After the uninstallation finishes, the device reboots.

Step 8 Verify that the appliances in your deployment are successfully communicating with the Firepower Management Center and that there are no issues reported by the health monitor.

Uninstall Firepower Threat Defense Devices Managed By Firepower Device Manager

You cannot uninstall Firepower Threat Defense devices managed by Firepower Device Manager. You must reimage the appliance. See the Firepower Threat Defense Command Reference Guide for more information.

CHAPTER 8

Freshly Install Version 6.2.2

If you are unable to upgrade a Firepower appliance, or are disinclined to follow the required upgrade path, you can freshly install major Firepower releases. To run a particular patch, install Version 6.2.2, then upgrade.

For more information, see:

Deciding to Freshly Install

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

Note *Always* address licensing concerns before you reimage or switch management of a Firepower appliance. If you are using Cisco Smart Licensing, you may need to manually unregister from the Cisco Smart Software Manager to avoid accruing orphan entitlements.

Table 13: Scenarios: Do You Need a Fresh Install?

Scenario	Solution	Licensing
Upgrade FMC-managed devices from an older Firepower version (5.x, 6.0.x).	The upgrade path from older versions includes intermediate versions. Especially in larger deployments where you must alternate FMC and device upgrade, this multi-step process can be time consuming. To save time, you can reimage older devices instead of upgrading: **1.** Remove the devices from the FMC. **2.** Upgrade the FMC only (5.x → 6.0 → 6.0.1 → 6.1 → 6.2 → 6.2.2). **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 Command Reference for Firepower Threat Defense.	Unregister the device before you switch management. Reassign its license after you add it to the FMC.
Change FTD management from FMC to FDM (remote to local).	Use the **configure manager** CLI command; see Command Reference for Firepower Threat Defense. **Exception:** The device is running or was upgraded from Version 6.0.1. In this case, fresh install.	Remove the device from the FMC to unregister it. Reregister using FDM.
Change ASA FirePOWER management between ASDM and FMC.	Start using the other management method.	Contact Sales for new Classic licenses. ASA FirePOWER licenses are associated with a specific manager.
Replace ASA FirePOWERwith FTD on the *same* physical device.	Fresh install.	Convert Classic to Smart licenses; see the Firepower Management Center Configuration Guide.
Replace NGIPSv with FTDv.	Fresh install.	Contact Sales for new Smart licenses.

Guidelines and Limitations for Fresh Installs

Back Up Event and Configuration Data

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

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

Remove Devices from the Firepower Management Center

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

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

Address Licensing Concerns

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

For more information on licensing, see:

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

Unregistering Smart Licenses

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

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

Unregister from CSSM before you:

- Reimage a Firepower Management Center that manages FTD devices.
- Reimage a Firepower Threat Defense device that is locally managed by FDM.
- Switch a Firepower Threat Defense device from FDM to FMC management.

Do not unregister from CSSM when you:

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

In these two cases, removing the device from the FMC automatically unregisters the device. You do not have to unregister manually as long as you remove the device from the FMC.

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

Unregister a Firepower Management Center

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

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

Step 1 Log into the Firepower Management Center.

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

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

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

Unregister an FTD Device Using FDM

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

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 14: Firepower Management Center Installation Instructions

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

FMC Platform	Guide
FMCv: KVM	Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide
FMCv: AWS	Cisco Firepower Management Center Virtual for the AWS Cloud Quick Start Guide

Table 15: Firepower Threat Defense Installation Instructions

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

Table 16: Firepower 7000/8000 Series, NGIPSv, and ASA FirePOWER Installation Instructions

NGIPS Platform	Guide
Firepower 7000 series	Cisco Firepower 7000 Series Getting Started Guide — Restoring a Device to Factory Defaults
Firepower 8000 series	Cisco Firepower 8000 Series Getting Started Guide — Restoring a Device to Factory Defaults
NGIPSv	Cisco Firepower NGIPSv Quick Start Guide for VMware

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

CHAPTER 9

Known Issues

For known issues, see:

- Version 6.2.2.x Known Issues, on page 61

Version 6.2.2.x 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 your search to bugs affecting specific Firepower platforms and versions, and also search by bug ID, or for specific keywords.

Known Issues in Version 6.2.2.x provides a list of open bugs in Version 6.2.2.x.

CHAPTER 10

Resolved Issues

Bugs listed for a patch were verified as resolved when that patch was initially released.

Resolved Issues in New Upgrade Packages

Sometimes Cisco releases updated builds. Only the latest build for each platform is available on the Cisco Support & Download site. You should always use the latest build. If you downloaded an earlier build, do not use it.

You cannot upgrade from one build to another for the same Firepower version. If a new build would fix your issue, determine if an upgrade or hotfix would work instead. If not, you must uninstall and then reinstall.

Find your platform in the following table to determine if a new Version 6.2.2.x build is available.

Table 17: Version 6.2.2.x Patches with Updated Builds

Version	Updated Build	Released	Platforms	Resolves
6.2.2.4	43	2018-09-21	FTD/FTDv	Resolved multiple issues for FTD paltforms.
	34	2018-07-09	FMC/FMCv NGIPS devices	CSCvk17382: Snort exiting unexpectedly while processing rule evaluation.
6.2.2.3	69	2018-06-19	All	CSCvj25386: Missing default Identity realm EOs causing upgrade failure
6.2.2.1	80	2017-12-05	Firepower 2100 series	CSCvg93011: FTD logical device name mismatch on FPR2100 causes upgrade and HA sync failure

Version 6.2.2.5 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.

- Firepower Management Center
- Firepower Management Center Virtual
- ASA FirePOWER Modules

Caveat ID Number	Description
CSCvd12834	FP Audit Logs do not log passed and failed SSH authentication attempts
CSCvd28906	ASA traceback at first boot in 5506 due to unable to allocate enough LCMB memory
CSCve53415	ASA traceback in DATAPATH thread while running captures
CSCvf54682	sudo : CVE-2017-1000368 : Sudo Parsed tty Information Privilege Escalation Vulnerability
CSCvf96773	Standby ASA has high CPU usage due to extremely large PAT pool range
CSCvg01119	IPV4: Implementing buffered reliability mechanism for routing updates
CSCvg45261	Firepower 2100 high availability pair upgrade failed from 6.2.1-341 to 6.2.3-5305
CSCvg76652	Default DLY value of port-channel sub interface mismatch
CSCvg96103	Including a very large HTML page for the Block response causes all Decrypted sites to fail to load.
CSCvh01213	An ASA may Traceback and reload when processing traffic
CSCvh16252	ASA may traceback and reload in Thread Name: fover_rep during conn replication
CSCvh62705	Firepower 2110 ASA : Shared management across context unable to reach to GW
CSCvh91399	upgrade of ASA5500 series firewalls results in boot loop (not able to get past ROMMON)
CSCvh98781	ASA/FTD Deployment ERROR 'Management interface is not allowed as Data is in use by this instance'
CSCvi03103	BGP ASN cause policy deployment failures.
CSCvi06120	vpn-idle-timeout is not triggered after switching to rebooted failover pair
CSCvi07974	FTD: Layer 2 packets (ex: BPDUs) are dropped during snort restarts (Inline/Passive Interfaces Only)
CSCvi34164	ASA does not send 104001 and 104002 messages to TCP/UDP syslog
CSCvi59968	Firepower 2100 Incorrect reply for SNMP get request 1.3.6.1.2.1.1.2.0

Caveat ID Number	Description
CSCvi84315	Unexpected failures on Firepower 2100 Series devices
CSCvi95544	ASA not matching IPv6 traffic correctly in access control license with "any" keyword configured
CSCvi96442	Slave unit drops UDP/500 and IPSec packets for S2S instead of redirecting to Master
CSCvi97729	To-the-box traffic being routing out a data interface when failover is transitioning on a New Active
CSCvj07038	Firepower devices need to trust Threat Grid certificate
CSCvj15572	Flow-offload rewrite rules not updated when MAC address of interface changes
CSCvj37924	CWE-20: Improper Input Validation
CSCvj42450	ASA traceback in Thread Name: DATAPATH-14-17303
CSCvj43591	Firepower 2110 with ASA DHCP does not work properly
CSCvj49452	sftunnel using weak SSL/TLS versions and ciphers
CSCvj58342	Multicast dropped after deleting a security context
CSCvj72309	FTD does not send Marker for End-of-RIB after a BGP Graceful Restart
CSCvj75793	2100/4100/9300: stopping/pausing capture from Management Center doesn't lower the CPU usage
CSCvj81287	Firepower Threat Defense rejecting syslog server TLS-X509 certificate due to EKU invalid purpose
CSCvj83316	Snort process exits while clearing XFF data.
CSCvj89470	Cisco Adaptive Security Appliance Direct Memory Access Denial of Service Vulnerability
CSCvj91858	Cisco Adaptive Security Appliance Access Control List Bypass Vulnerability
CSCvj92040	TLS client offers some ciphersuites in CC mode that are not allowed by CC
CSCvj93913	SSL Inspection TLS 1.3 downgrade needs to modify client/server random values to be RFC compliant
CSCvk02250	"show memory binsize" and "show memory top-usage" do not show correct information (Complete fix)
CSCvk04592	Flows get stuck in lina conn table in half-closed state
CSCvk06160	SFDC repeatedly exits while Initializing OS Vuln Map
CSCvk18330	Active FTP Data transfers fail with FTP inspection and NAT

Caveat ID Number	Description
CSCvk31035	KVM (FTD): Mapping web server through outside not working consistent with other platforms
CSCvk34648	Firepower 2100 tunnel flap at data rekey with high throughput Lan-to-Lan VPN traffic
CSCvk45443	ASA cluster: Traffic loop on CCL with NAT and high traffic
CSCvk57516	Low DMA memory leading to VPN failures due to incorrect crypto maps
CSCvk66722	Configuring DHCP option 'false' causes DHCP configuration to be not visible from GUI
CSCvk66771	The CPU profiler stops running without having hit the threshold and without collecting any samples.
CSCvk67239	FTD or ASA traceback and reload in "Thread Name: Logger Page fault: Address not mapped"
CSCvm01497	Scheduled reports not stored in correct domain when using another domain's report template
CSCvm03931	software update downloads by Firepower failing due to newer CA certificates not being present
CSCvm09624	Protocol not updated based on AppID when enforcing IPS rules
CSCvm23370	ASA: Memory leak due to PC cssls_get_crypto_ctxt
CSCvm43975	Cisco ASA and FTD Denial of Service or High CPU due to SIP inspection Vulnerability
CSCvm60361	SSH public key auth not working on FTD on 5500
CSCvm80874	ASAv/FP2100 Smart Licensing - Unable to register/renew license
CSCvn08146	Missing audit detail for changes to x509 certificates and keys

Version 6.2.2.4 Resolved Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of resolved bugs for Firepower products. These queries are for Version 6.2.2.4:

- Firepower Management Center
- Firepower Management Center Virtual
- ASA FirePOWER

Table 18: Version 6.2.2.4 Resolved Issues

Bug ID	Description
CSCuv68725	ASA unable to remove ACE with **log disable** option

Bug ID	Description
CSCvc20141	Cisco Firepower System Software Server Message Block File Policy Bypass Vulnerability
CSCvc92934	When SSL decryption is enabled, URL constraints in access control policy are not applied correctly
CSCvd13182	AVT : Missing X-Content-Type-Options in ASA 9.5.2
CSCvd44525	ASA **show tech** some commands twice, show running-config/ak47 detailed/startup-config errors
CSCvd72158	Evaluation of sfims for NTP March 2017
CSCvd86594	Need ability to enable PPTP inspection
CSCve87945	Cannot install new https certificate
CSCve94917	Stale VPN Context issue seen in 9.1 code despite fix for CSCvb29688
CSCvf18160	ASA traceback on failover sync with WebVPN and shared storage-url config
CSCvf39539	Netflow Returns Large Values for Bytes Sent/Received and IP address switch
CSCvf40179	`ERROR: Unable to create crypto map: limit reached`, when adding entry
CSCvf82832	ASA : ICMPv6 syslog messages after upgrade to 962.
CSCvf92262	ASA Webvpn HTTP Strict-Transport-Security Header missing despite fix of CSCvc82150
CSCvf97979	NAT policy deployment failed during generating delta config after changing security zone in rule.
CSCvg05442	ASA traceback due to deadlock between DATAPATH and webvpn processes
CSCvg20782	Identified Vulnerabilities associated with the CVEs from Oracle MySQL Patch Updates
CSCvg37391	Migrated access control policy deploy fails since it has FQDN objects
CSCvg89215	ASA crashed with Thread name DATAPATH-1-27929 in 3 node Firepower 9300 Distributed Cluster
CSCvh14743	IKEv2 MOBIKE session with Strongswan/3rd party client fails due to DPD with NAT detection payload.
CSCvh20742	Cisco Adaptive Security Appliance Clientless SSL VPN Cross-Site Scripting Vulnerability
CSCvh22181	Failures loading websites, such as mail sites, using TLS 1.3 with SSL inspection enabled
CSCvh30261	ASA watchdog traceback during context modification/configuration sync

Bug ID	Description
CSCvh47057	ASA - ICMP flow drops with `no-adjacency` on interface configured in zone when inspection enabled
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
CSCvh62164	Firepower 9300 standby stuck in Bulk-Sync state with high CPS traffics on active
CSCvh63903	Failover of IPv6 addresses on 8000 series pair devices may not succeed
CSCvh75577	Firepower Management Center displays no data for CPU usage even when enabled and deployed in 6.2.2.1
CSCvh81142	Snort Core Generated while running 6.2.3
CSCvh81474	Need to catch malformed JSON to allow rendering of Deploy button and notifications
CSCvh95807	SSL FLow Errors reported when accessing ECDSA signed websites
CSCvh99159	RADIUS authentication/authorization fails for ASDM
CSCvh99414	NFE failure causes Snort to constantly restart
CSCvi01312	webvpn: multiple rendering issues on Confluence and Jira applications
CSCvi03546	User-IP mapping not updated on managed device due to error in updating current map
CSCvi08450	CWS redirection on ASA doesn't treat SSL Client Hello retransmission properly in specific condition
CSCvi16264	ASA traceback and reload due to watchdog timeout when `DATAPATH` accesses compiling ACL structure
CSCvi19263	ASA 9.7.1.15 Traceback while releasing a vpn context spin lock
CSCvi22507	IKEv1 RRI : With Answer-only Reverse Route gets deleted during Phase 1 rekey
CSCvi34137	With SSL decryption enabled and TCP Segmented HTTP requests, Snort does not capture URI correctly
CSCvi37889	Packet Tracer fails with `ERROR: TRACER: NP failed tracing packet,` even after removing captures
CSCvi45567	Not able to do snmpwalk when snmpv1&2c host group configured.
CSCvi47847	Shell application not pin-holing for new tcp port for data transfer as expected
CSCvi55070	IKEv1 RRI : With Originate-only Reverse Route gets deleted during Phase 1 rekey
CSCvi57808	Continuously sfdatacorrelator process terminated unexpectedly
CSCvi58089	Memory leak on webvpn
CSCvi58865	SSL policy with URL category rules specifying decryption can cause browser errors

Bug ID	Description
CSCvi59148	Sessions can remain active on managed device if they are from same IP address but different realms
CSCvi63888	SSL errors might occur when resumed sessions are not decrypted
CSCvi66905	PIM Auto-RP packets are dropped after cluster master switchover
CSCvi76577	`ASA:netsnmp:Snmpwalk` is failed on some group of IPs of a host-group.
CSCvi77352	Illegal update occurs when device removes itself from the cluster
CSCvi82779	ASA generate traceback in DATAPATH thread
CSCvi86799	ASA traceback during output of `show service-policy` with a high number of interfaces and qos
CSCvi95544	ASA not matching IPv6 traffic correctly in ACL with **any** keyword configured
CSCvj07038	Firepower devices need to trust Threat Grid certificate
CSCvj07843	eStreamer using 100% CPU, event processing slows when File/FireAMP events enabled
CSCvj25386	Missing default Identity realm EOs causing upgrade failure
CSCvj43591	Firepower 2110 with ASA DHCP does not work properly
CSCvj56008	Scansafe feature doesn't work at all for HTTPS traffic

Version 6.2.2.3 Resolved Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of resolved bugs for Firepower products. These queries are for Version 6.2.2.3:

- Firepower Management Center
- Firepower Management Center Virtual
- ASA FirePOWER

Table 19: Version 6.2.2.3 Resolved Issues

Bug ID	Description
CSCuu67159	ASA: traceback in **DATAPATH-2-1157**
CSCux17501	SSL inspection blocks traffic with decryption errors for sites with 3072 bit key RSA certificates
CSCvc03899	Firepower Threat Defense managed by Management Center 6.2 - High unmanaged disk usage on **/ngfw**
CSCvc91092	Cisco FireSIGHT System Software Arbitrary Code Execution Vulnerability

Bug ID	Description
CSCve20395	ASA Portal Java plug-ins fail with the latest Java updates
CSCve48087	Deploy policy tab failed to populate the device list from Firepower Management Center
CSCve49722	Can't export if intrusion policy inherits intrusion layer from parent domain
CSCve77286	Intrusion policy rule filter is not working properly
CSCvf53734	access control rules and Categories duplication on Firepower Management Center UI
CSCvf56533	Cannot re-register Firepower 9300 cluster to a different Firepower Management Center
CSCvf81672	ASA Routes flushed after failover when etherchannel fails
CSCvf98631	SSL does not properly re-register with the **IsAppIdRequired** framework on reload
CSCvg00565	ASA crashes in **glib/g_slice** when do **debug menu** self testing
CSCvg05368	Upon joining cluster slave unit generates **ASA-3-202010: NAT/PAT pool exhausted for all PAT'd** conns
CSCvg08988	Access Control Rule is not created in snort if source zone and destination zone are the same
CSCvg23028	REST-API residues on Firepower Threat Defense (2100, 4100, 9300 Series)
CSCvg36672	Need a way to prioritize user driven deployment tasks in Action Queue
CSCvg43389	ASA traceback due to 1550 block exhaustion.
CSCvg45236	Lower-than-expected 256 byte block count with fast-path pre-filter SSL policy
CSCvg56122	SSL handshake fails with large certificate chain size
CSCvg62337	Memory calculation in Snort incorrect for Firepower Threat Defense devices
CSCvg62916	ASA: Software traceback in Thread Name: Dynamic Filter updater
CSCvg65072	Cisco ASA sw, FTD sw, and AnyConnect Secure Mobility Client SAML Auth Session Fixation Vulnerability
CSCvg71421	Archive Cache Pruning May Not Work
CSCvg72583	Archive Cache Loading Could be in Deadlock
CSCvg73042	SSL Cache missing session info leading to **ERR_SSL_PROTOCOL_ERROR** in the browser for SSL websites
CSCvg83924	Traffic not hitting the access control rule which has deprecated Application in it
CSCvg84495	Remote access VPN using an OpenLDAP realm/server doesn't use the correct naming attribute
CSCvg85982	ERSPAN not working on Firepower Threat Defense running 6.2.2

Bug ID	Description
CSCvg99285	[ERROR] Failed to init octeon -- **FATAL ERROR: Can't initialize DAQ oct_ssl (-1)**
CSCvh05081	ASA does not unrandomize the SLE and SRE values for SACK packet generated by ASA module
CSCvh15228	ASA/Firepower Threat Defense Traffic Zone Member Command Causes BGP to Flap
CSCvh19991	User/Group Download fails when an Included Group is missing from the AD Server
CSCvh23531	ASA TLS client connection fails with software DHE
CSCvh23776	Both ASA traceback in high availability pair on 4140 chassis
CSCvh25433	New CLI for Supporting Legacy method SAML Auth using external browser on Endpoint with AC
CSCvh32673	Freed memory not released back to the system quick enough on ASA 5506-x platforms
CSCvh47069	Firepower Management Center Data purge causes managed sensor to wipe out user sessions upon reboot
CSCvh53597	Policy deploy fails if SSL Policy has deprecated AppDetector
CSCvh53616	ASA on Firepower Threat Defense devices traceback due to SSL
CSCvh53901	SFDataCorrelator cores when reading invalid fingerprint type from database
CSCvh54940	ASA traceback with thread name **idfw_proc**
CSCvh55035	Firepower Threat Defense device unable to stablish ERSPAN with Nexus 9000
CSCvh58373	FlexConfig MPF configuration does not deploy all Access-Lists and not redeploying all Class-Maps
CSCvh59884	Notifications about pruned events contains invalid date/time (Thu Jan 1 00:00:01 1970)
CSCvh63896	ASA traceback in threadname CP Processing
CSCvh65500	Firepower 2100 Client in FTP active mode is not able to establish control channel with the Server
CSCvh67981	ASA 9.8.2 Cluster Slave unit traceback when joining cluster and SNMPv3 sync
CSCvh68521	On 8000 series stack, with **Maint on sec fail** setting enabled, stack health is in compromised state
CSCvh69967	5506 traceback when ASA module and RestAPI both enabled
CSCvh70474	SFDataCorrelator/SFDCNotificationd connection log spam after expiring many hosts
CSCvh73582	traceback related to SIP inspection processing
CSCvh75025	ASA traceback when failing over to standby unit

Bug ID	Description
CSCvh77721	Standby SFDataCorrelator fails to connect to Sybase after Management Center pair establish/resume
CSCvh77942	new Certificate configuration of primary unit does not sync to standy unit in a Active/Active setup
CSCvh78133	Firepower 2100 **process_stderr.log** getting flooded with errors causing /ngfw high disk
CSCvh83026	ASA tracebacks intermittently with Thread Name: CTM message handler
CSCvh83145	ASA interface IP and subnet mask changes to 0.0.0.0 0.0.0.0 causing outage of services on interface
CSCvh83934	Memory usage of User-ID component of SNORT exceeds the reserved limit of 10M
CSCvh85246	ssl inspection can be limited by a **do not decrypt** rule specifying one or more common names
CSCvh85514	ASA Traceback in Thread Name: Unicorn Proxy Thread
CSCvh85580	**ids_event_alerter** core when processing connection events
CSCvh89095	Firepower Management Center allows deleting Interface Object being used in SLA monitor object
CSCvh89340	Cisco Firepower Threat Defense SSL Engine High CPU Denial Of Service Vulnerability
CSCvh90947	ASA traceback with Thread Name: **fover_parse**
CSCvh91053	ASA sending DHCP decline | not assiging address to AC clients via DHCP
CSCvh92381	ASA Traceback and goes to boot loop on 9.6.3.1
CSCvh95325	Standby ASA traceback during replication from mate 9.2(4)27
CSCvh95396	Policy deployment failure due to Invalid preprocessor **normalize_tcp** option **ftp**
CSCvh95600	Need consistent identifier for lines of ssl debug log output
CSCvh97216	Mmapped bytes allocated incorrectly accounted in Free Memory of show memory detail
CSCvh97594	ssl inspection cache can become unbalanced, leading to premature removal of recently used items
CSCvi01376	Upon reboot, non-default SSL commands are removed from the FP4100 device
CSCvi02989	Access control policy not able to be edited or deployed after upgrade to Version 6.2.2.1
CSCvi03532	Audit message not generated by: no logging enable
CSCvi07636	ASA: Traceback in Thread Name UserFromCert

Bug ID	Description
CSCvi09305	Some SSL connections slow or fail under a **Do-Not-Decrypt** SSL policy action
CSCvi09811	Traceback in DATAPATH, assertion **0** failed: file **./snp_cluster_transport.h**, line 480
CSCvi12354	Threat Defense member in intra-cluster environment is not able to be re-added in Management Center
CSCvi18602	FSIC failed while downgrade ASA FirePOWER module (5585-x) from 6.2.2.2 to 6.2.2.1
CSCvi29682	ISE-PIC Connection to Firepower Management Center does not work
CSCvi33962	WebVPN rewriter: drop down menu doesn't work in BMC Remedy
CSCvi35805	ASA Cut-Through Proxy allowing user to access website, but displaying **authentication failed**
CSCvi39938	Traffic outage while downloading large number of users and groups
CSCvi53922	Failures loading websites using TLS 1.3 with SSL inspection enabled
CSCvi80849	Cisco Firepower 2100 Series POODLE TLS security scanner alerts

Version 6.2.2.2 Resolved Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of resolved bugs for Firepower products. These queries are for Version 6.2.2.2:

- Firepower Management Center
- Firepower Management Center Virtual
- ASA FirePOWER

Table 20: Version 6.2.2.2 Resolved Security Issues

Bug ID	Description
CSCvd07072	SSL logging denial-of-service vulnerability
CSCve91584	Cisco Firepower Management Console Security Intelligence Objects Denial of Service Vulnerability
CSCvf86435	If **Drop** threshold is configured in Intelligent Application Bypass, all traffic will be trusted
CSCvg35384	snort crash **deleteSessionByKey** found when access control policy edited and malware traffic is sent
CSCvg35618	Cisco Adaptive Security Appliance Remote Code Execution and Denial of Service Vulnerability

Bug ID	Description
CSCvh79732	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81737	Cisco Adaptive Security Appliance Denial of Service Vulnerability
CSCvh81870	Cisco Adaptive Security Appliance Denial of Service Vulnerability

Table 21: Version 6.2.2.2 Resolved Issues

Bug ID	Description
CSCuz25599	Firepower Threat Defense CLI command **system support run-rule-profiling** exits prematurely
CSCuz44985	Erroneous syslog messages cause excessive upgrade times/failures
CSCva42408	Ev AnalysisUI: Domain column disappears after switching to Secondary Firepower Management Center
CSCvb01438	Syslog deployment fails
CSCvb81481	No Input/Output packet for Port-channel in Firepower Threat Defense 4100
CSCvc09017	Show Nat flows on Firepower 7000/8000 series devices displays incorrect data
CSCvc21275	Internal error on editing the NAT policy after import
CSCvc55027	context explorer slow to load due to db deadlocks in **rna_client_app_payload**
CSCvc92854	Firepower Management Center does not detect changes if they are configured via FlexConfig.
CSCvd34694	Enabling SSL Decryption blocks legitimate traffic
CSCvd93621	Unable to edit performance settings in advanced section of Access Control policy
CSCve31387	No CPU alert on 8000 Series, when snort is overwhelmed.
CSCve31938	Changes Made to Objects Referenced Only by FlexConfig not Recognized for Deployment
CSCve34640	SSL policy causing inspection engine (snort) processes stop unexpectedly
CSCve55973	**configure ssh-access-list** command does not work 6.2.x
CSCve58826	Issues with multiple pending UserEnforcementSnapshot tasks
CSCve70416	SSL policy with **Decrypt-Resign** action does not decrypt traffic with ECDSA certificates
CSCve71562	Implement a mechanism to track the status between ISE pxgrid and Management Center pairs
CSCve74524	User Agent does not properly report group names with special characters in the name

Bug ID	Description
CSCve82410	Port Scan does not block scans
CSCve85996	Deployment timeouts after 30 minutes due to expand of ACE during deployment
CSCve86182	Reserved Characters in access control/ Prefilter policy rule name may fail Threat Defense Deployment
CSCve88096	File Events may incorrectly show **Device Not Activated** for capacity handled files
CSCve91343	Firepower Threat Defense: With CC mode enabled, NGFWv IPSec performance degraded 10-20%
CSCve96463	False positives for TCP Session Hijacking in routed deployments
CSCve97046	**threat_name table** prune cannot keep up with insertion
CSCve97395	Syslog and SNMP do not work for Prefilter Policy on Firepower Threat Defense
CSCvf10088	Migration fails when access-list contains vxlan port
CSCvf13106	EIGRP system defined template for every time deployment is not working
CSCvf20259	**ids_event_alerter** output is missing attribute names on Firepower Threat Defense devices
CSCvf20753	Changing text object is not making flex object dirty to be deploy
CSCvf22930	Firepower 9300 running ASA 9.7.1.10 Threat Defense high availability traceback in Datapath
CSCvf23425	SSL handshake error and timeout occurs when HTTPS traffic is passed through GRE tunnel
CSCvf25415	Spaces in IP range in Access Control Policy can cause deploy to fail
CSCvf26676	With SSL inspection, Snort can terminate unexpected in SideChannel
CSCvf27435	SSL Monitor - Event matches wrong access control rule
CSCvf36492	Management Center high availability configuration is not always reflected correctly on sensors
CSCvf36796	Flood of captive portal messages
CSCvf40650	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
CSCvf41773	Threshold configuration files have old unneeded policies
CSCvf44801	Intrusion rule with multiple negations can be trigger false positives
CSCvf47736	TCP connection not reset on when SSL rule action action set to block with reset
CSCvf48889	Memory leak in **ActionQueueScrape.pl** can cause stacked Firepower devices to hang

Bug ID	Description
CSCvf52889	Delay of end of connection events for SSL traffic
CSCvf58260	Categories missing from security intelligence events
CSCvf59214	User sessions without email might cause database issues
CSCvf63022	Application is not being identified for RTP stream
CSCvf63871	Inspection engine CPU usage high if SSL policy or captive portal are enabled
CSCvf64730	Incorrect upper limit for Intrusion Event Database records on Management Center virtual.
CSCvf64831	Firepower Management Center reports incorrect IPv6 addresses and ports
CSCvf67573	Errors during interface creation/deletion and config save
CSCvf69012	Unassigning Flexconfig object that has MPF config removes service-policy and pmap but not class-map
CSCvf70092	Resource Leak in SFTop10Cacher leads to deadlock
CSCvf70381	Malware embedded in an archive may not get blocked
CSCvf72930	Firepowe Threat Defense may traceback in Thread Name **appAgent_monitor_nd_thread** during registration
CSCvf73976	Increase the timeout for interface messages in **ASAConfig.pl**
CSCvf74790	OGS and TCM commands are negated by Firepower Management Center during policy deployment
CSCvf76566	S4000-K9 // Cannot add object to the network group (Firepower Management Center 682412623)
CSCvf77469	Packet loss during Server Hello when SSL policy verdict is **Do Not Decrypt** causes failures
CSCvf78924	Maximum Transmission Unit (MTU) setting ignored on managed devices, leading to dropped packets
CSCvf83436	Management Center Cannot add route-lookup keyword when using **any** as destination interface object
CSCvf86487	Intelligent Application Bypass drop percentage does not work as expected
CSCvf87538	Syslog ID is reset to **111111** when editing syslog settings
CSCvf90350	Firepower Management Center policy deploy fails on using banner values without line breaks
CSCvf91209	SI transaction on sensor should use the same directory for staging
CSCvf92782	PAT pool fails to be enabled on Japanese GUI

Bug ID	Description
CSCvf93232	User can access URLs without active authentication if traffic is not decrypted
CSCvf95108	**Action_queue** tables not pruning successful/failure tasks
CSCvf95494	Routes are not applied on a 7000/8000 series devices in Cluster
CSCvf96656	After creating an access control rule with app filters via REST API, cannot access policy from UI
CSCvf97107	Retransmit delay when first packet lost with **Decrypt-Resign** or **Do Not Decrypt** SSL policy action
CSCvg04071	changing the system hostname in Management Center UI causes Device registration failure on 6.2.2
CSCvg04361	With SafeSearch on, user cannot access some websites using AES-CBC ciphers
CSCvg06695	Firepower 2100 Threat Defense pair reporting failed status due to **Detect service module failure**
CSCvg07052	RealID+TempID in Sybase makes SFDataCorrelator incorrectly assign TempID to new logins
CSCvg08988	Access Control Rule is not created in snort if source zone and destination zone are the same
CSCvg17478	Traceback with Show OSPF Database Commands
CSCvg21478	User/Group Downloads fail with non-ascii characters in included/excluded groups
CSCvg22873	Threat Defense Virtual: Azure, waagent.log file grows without bounds and needs to rotate
CSCvg23287	nfm_exceptiond exited unexpectedly **is_allocator FATAL m_mutex->tryLock** error
CSCvg23401	Firepower Management Center is not displaying VPN configuration.
CSCvg25287	Add **mysql-server.err** file to **logrotate.d** in Firepower Threat Defense
CSCvg25358	Set oom-killer priorities
CSCvg25694	Assert Traceback, thread name : **cli_xml_server**
CSCvg28321	Improve user group lookup handling by broadcasting info to all snort instances
CSCvg32885	Unable to edit or Deployment missing some of the access control rules after upgraded to 6.2.0.3
CSCvg34306	ENH - The memcap for Security Intelligence URL feeds needs to be increased.
CSCvg35384	snort crash **deleteSessionByKey** found when access control policy edited and malware traffic is sent

Bug ID	Description
CSCvg42347	6.2.0.3 upgrade failed on standby 4140 at script **800_post/755_reapply_sensor_policy.pl**
CSCvg42478	SFDaco can sometimes fail to respond to For Policy changes discovered during realm sync
CSCvg43193	Unable to change OSPF md5 key
CSCvg47955	CloudAgent segfault on Firepower Threat Defense
CSCvg52296	Threat Defense 5506 does not send a block page for URL filtering when using BVI switched interfaces
CSCvg53208	Application protocol field missing in connection events
CSCvg54460	**[SFR onbox] ADI.conf** removed on policy deployment
CSCvg55040	Health monitoring for 7000/8000 series devices does not set bypass rules on recovery
CSCvg55713	Search Rules field clears when moved to next page.
CSCvg56106	DHCP relay agents configured not visible on GUI
CSCvg56681	Upgrade framework scripts incorrectly delete rc symlinks
CSCvg56985	If Management Center backup dies in the middle, events are not received on the Management Center
CSCvg58754	Policy Deployment hangs on Threat Defense 6.2.1+ when cluster message and ack comes out of order
CSCvg60323	D/R HTTPS connections fail in browsers that enforce OCSP must staple
CSCvg64722	Firepower Threat Defense in high availability mode in Active-Failed state
CSCvg65044	When network packets are transmitted out-of-order, some SSL sessions may not be established
CSCvg66697	segfault in **ssl_handshake::sig_hash**
CSCvg66706	SFDataCorrelator deadlock core due to slow User Identity event processing
CSCvg66844	Excessive log messages **found no record for Realm** and excessive database queries
CSCvg67206	Traffic loss and **pdts_daq_dext_process** nse interface intialization has not occurred errors
CSCvg71777	Access control rules deleted/added back in every alternate deploy when VXLAN port **UDP:4789** is used
CSCvg72472	user/group download timeout on slow network link - timeout needs to be increased
CSCvg75447	Duplicate User Group Names across AD/Realm causes the user download to fail

Bug ID	Description
CSCvg76542	Correlation rule for connection Reason **is not** should fire when event has no Reason
CSCvg84474	Space in port range for an access control policy rule causes error that prevents rule editing
CSCvg92679	**Use active authentication if passive or VPN identity cannot be established** check gets disabled
CSCvg94742	Force Break from Management for Firepower Threat Defense devices fails to break pair
CSCvg96525	SFDataCorrelator deadlock during whitelist host evaluation
CSCvg97874	FireAMP Cloud events are not available for eStreamer clients
CSCvg99382	Restore backup that was created on remote storage and transferred locally has a problem
CSCvh01083	NAT rules with route-lookup option are exported with different original and translated object names
CSCvh07446	On 7000/8000 devices, many IPs in a single access control rule will match rule incorrectly
CSCvh12075	Firepower Threat Defense devices in high availability might go into reboot loop one after the other
CSCvh12510	system support identity-debug
CSCvh18106	Firepower Management Center- Flexconfig-Removal of EIGRP Authentication every time during deployment
CSCvh21873	SFDataCorrelator on Firepower Management Center repeatedly crashes for corrupt user login event
CSCvh58373	FlexConfig MPF configuration does not deploy all Access-Lists and not redeploying all Class-Maps
CSCvh77330	DOC: Incorrect path for an upgrade to 6.2.2.X
CSCvh91577	**IDSEventAlerter:config** [ERROR] Unrecognized keyword: **ssl_policy_UUID**

Version 6.2.2.1 Resolved Issues

If you have a support contract, you can use the Cisco Bug Search Tool to obtain an up-to-date list of resolved bugs for Firepower products. These queries are for Version 6.2.21:

- Firepower Management Center
- Firepower Management Center Virtual
- ASA FirePOWER

Table 22: Version 6.2.2.1 Resolved Issues

Bug ID	Description
CSCuz68504	Dynamic Analysis Summary not showing full report
CSCvb22670	SFDCNotificationd dumps core if stopped after SFDataCorrelator
CSCvc06133	Firepower Management Center freezes when attempt is made to sort the App Detectors
CSCvc46599	Error message **Unable to translate SSL cipher suite 65535** needs cleaning up
CSCvc59913	Mismatched VLAN tagged traffic has inconsistent access control rule matches.
CSCvc65384	Identity policy not working after import
CSCvc92397	Webpages loads very slowly when URL retry is enabled
CSCvd16631	Excessive logging from sip preprocessor function **SipSessionSnortCallback**
CSCve10708	Upgrade file-transfer from Firepower Management Center to Firepower device times out after one hour
CSCve11915	POP3 payload inspection not proper on snort with the file detection policy
CSCve28417	[NSS] Snort 6 Core - AAB - in SnortPcre of file detection_options.c
CSCve39775	Multiple login messages different username and same realm/IP/timestamp scrambles SFDaco
CSCve46186	Snort memcals for startup memory incorrect on Firepower Threat Defense
CSCve47333	Management Center not deactivating smart licenses for Firepower Threat Defense devices
CSCve47800	Port Scan: IP Protocol scanning not getting detected.
CSCve47868	Snort not triggering Event 123:7 **FRAG3_ANOMALY_BADSIZE_LG**
CSCve55696	UIMP continues to attempt import for deleted users
CSCve58157	Host Input Daemon exits when interface is IPv6 (no IPv4)
CSCve79555	ASA/FTD traceback when clearing capture - assertion **0** failed: file **mps_hash_table_debug.c**
CSCve85240	Access control policy uneditable if copying large Policy, insert/move 50+ rules into category
CSCve85996	Deployment timeouts after 30 minutes due to expand of ACE during deployment
CSCve91343	Firepower Threat Defense: With CC mode enabled, NGFWv IPSec performance degraded 10-20%
CSCve94530	SFDataCorrelator signal-6 core on Firepower Management Center after reconfigure
CSCve95168	Unicode file support over SMB on Firepwer Threat Defense

Bug ID	Description
CSCve99203	256 low block count leads to traffic failures due to alloc to inspect snort
CSCvf09949	Incorrect access control rule is matched in Threat Defense device when it is setup in **passive** mode
CSCvf12124	Third Party Vulnerability Maps won't save
CSCvf14953	Health Alert for CPU usage on cores dedicated to Radware DefensePro service
CSCvf15216	When SSL rules are enabled and sensor is over subscribed, rules are not correctly enforced.
CSCvf15265	SFDataCorrelator takes a long time to start due to large firewall_rule_cache table
CSCvf16799	DH Ephemeral Keys with **Known Key** SSL Policy and session reuse causes client to close session.
CSCvf18368	Long traffic connections matching **Do Not Decrypt** SSL rules may be blocked
CSCvf20259	ids_event_alerter output is missing attribute names on Threat Defense devices
CSCvf22930	FP9300 9.7.1.10 Threat Defense high availability traceback in Datapath
CSCvf38056	SSL flows failing due to Flow tables and Flow ID's overflowing
CSCvf38081	SSL policy Category lookup fails for URLs that aren't in local database
CSCvf40650	Certificates not synced to Standby/All certificates cleared on Standby post deployment failure
CSCvf42713	cannot import web UI HTTPS server certificate on Firepower Management Center or 7000/8000 Series
CSCvf43107	Estreamer Cores - SSLCert length handling
CSCvf50819	AS Path prepend command truncated while deployed
CSCvf52744	cannot activate correlation policy with malware event by network based with file name as condition
CSCvf54853	Large database size for devices upgraded from 6.1.0.x to 6.2.0.x
CSCvf54986	Policy import from SFO or deleting realms fails with unreachable directory servers
CSCvf56267	Environments having multiple user accounts with same email address scrambles/crashs SFDataCorrelator
CSCvf59399	Memory growth in SFDataCorrelator due to User Identity
CSCvf62276	Missing IP address in AMP cloud malware events
CSCvf71086	Port-channel cannot be configured as a passive interface

Bug ID	Description
CSCvf75135	Configure **sysopt connection permit-vpn** using FlexConfig to prevent unintended clear-text traffic
CSCvf75781	Firepower Threat Defense device may leave cluster due to disk space alert
CSCvf76338	Scheduled configuration backup shows missing/wrong information on UI once generated.
CSCvf80717	TCP SACK in conjunction with SSL decryption can cause connections to stuck
CSCvf86080	SFDataCorrelator needs to log incorrect timestamp on bucketized partitioned tables
CSCvf87960	integrity check failure after updating GeoDB on Firepower Management Center
CSCvf89183	Large Deploy Bundles and slow links causes deploy to fail
CSCvg06695	FP2100 Threat Defense pair reporting failed status due to **Detect service module failure**
CSCvg08745	Snort segfaults and coring while processing FTP traffic.
CSCvg17478	traceback with Show OSPF Database Commands
CSCvg25694	Assert Traceback, thread name : **cli_xml_server**
CSCvg32885	Deployment missing some of the access control rules after upgraded to 6.2.0.3
CSCvg42347	6.2.0.3 upgrade failed on standby 4140 at **script 800_post/755_reapply_sensor_policy.pl**

CHAPTER 11

For Assistance

Thank you for choosing Firepower.

- Online Resources, on page 83
- Contact Cisco, on page 83

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/

To receive security and technical information about your products, you can also subscribe to the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and RSS feeds.

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

Contact Cisco

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

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