Firepower Release Notes, Version 6.2.2

First Published: 2017-09-05

Last Modified: 2018-09-28

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.

CONTENTS

CHAPTER 1

Welcome to Version 6.2.2

Thank you for choosing Firepower.

CHAPTER 2

Features and Functionality

For information on the new and changed features and functionality in this release, see:

New Features and Functionality

This section describes the new and updated features and functionality in Version 6.2.2.

Firepower Device Manager on Firepower Threat Defense Virtual for VMware

Supported Platforms: Firepower Threat Defense Virtual for VMware, managed by Firepower Device Manager

Introduced In: Version 6.2.2

You can now use Firepower Device Manager to manage Firepower Threat Defense Virtual hosted on VMware. Because this is a newly supported implementation for Version 6.2.2, you deploy a new virtual device. You cannot update an earlier version of Firepower Threat Defense Virtual and then manage it with Firepower Device Manager.

Cisco Threat Intelligence Director

Supported Platforms: Hosted on any Firepower Management Center with at least 15GB of memory, using Version 6.2.2 devices as elements

Introduced In: Version 6.2.2

The Cisco Threat Intelligence Director (TID) operationalizes custom threat intelligence data, helping you aggregate additional intelligence data, configure defensive actions, and analyze threats in your environment.

By ingesting threat intelligence from third-party threat feeds and threat intelligence platforms, TID correlates enriched observations from Cisco security sensors to detect and alert on security incidents. With fewer false positives, you can focus on actual incidents that have been automatically blocked or monitored.

Unlike security devices that rely solely on proprietary threat intelligence, TIDr can use third-party threat feeds to provide more effective security. By converting intelligence into actionable indicators of compromise, your network defenses can block or monitor more threats, reduce the number of alerts to review, and improve your overall security posture. By operationalizing the ingestion and distribution of additional threat intelligence sources, you reduce management complexity and the need to review and track down false alerts.

Remote Access VPN

Supported Platforms: Firepower Threat Defense, any manager

Introduced In: Version 6.2.2

Firepower Remote Access (RA) VPN allows users to connect to a private business network from a remote location using a computer or an Android or Apple iOS mobile device. Remote users can transfer data securely and confidentially using encryption techniques crucial for data being transferred over shared mediums and the internet. Key capabilities of RA VPN include the following:

- Management—A simple RA VPN wizard provides quick and easy setup of the following:
  - RA VPN policy configurations, including connection profiles, group polices, address pools, and so on.
  - Secure gateways and interfaces where remote users connect.
  - The AnyConnect client image that users download when they initiate a VPN session using a computer. Note that mobile devices obtain AnyConnect from their App Store(s).
- Secured access—Provided by the Cisco AnyConnect VPN client using either SSL or IPsec tunneling and encryption protocols. This presently is the only client supported for remote access connectivity.
- Authenticated and Authorized Access—AAA support for Authentication (LDAP/AD/RADIUS and Client Certificate-based), Authorization (RADIUS Authorization Attributes-DACL, Group Policy, Address Assignment, and so on) and Accounting (RADIUS).
- VPN connectivity—Connection profiles and group policies allow you to define address assignments, split tunneling, the DNS server, timeouts, access hours, client firewall ACLs, and AnyConnect client profiles.
- Monitoring with identity integration—Multiple views, including dashboard widgets, help you track and analyze VPN user activity over time. You can view logon and logout events, see active session status, and can monitor and terminate specific VPN sessions (including forcing a bulk logout).
- Troubleshooting— Troubleshooting logs are useful when you have issues creating or deploying an RA VPN policy, if RA VPN connections or traffic are not as expected, or if events and statistics are not populating properly.
- Availability—Firepower Threat Defense high availability, multiple interfaces (dual ISP), and multiple AAA servers are supported.
- Licensing—Smart Licensing, based on the AnyConnect 4.x model, for Apex, Plus, and VPN-only licenses.

Rate Limiting Enhancements

Supported Platforms: Firepower Threat Defense managed by a Firepower Management Center

Introduced In: Version 6.2.2

Quality of Service (QoS) *rate limits* traffic based on characteristics including network-based criteria (port, network, zone/interface group), applications, URLs, and users, including Cisco Identity Services Engine (ISE) attributes. A QoS policy applied from the Firepower Management Center enforces rate limiting *per interface* on Firepower Threat Defense devices.

Intelligent Application Bypass "All Applications" Option

Supported Platforms: Any device managed by a Firepower Management Center, and ASA FirePOWER modules managed by ASDM

Introduced In: Version 6.0.1.4, Version 6.1.0.3, Version 6.2.0.1, and Version 6.2.2

If you are updating from Version 6.2.0, this release adds the **All applications including unidentified applications** option to the Intelligent Application Bypass settings in the access control policy advanced settings.

If you are updating from a Version 6.2.0.x patch, this option already exists.

When selected, if one of the IAB inspection performance thresholds is met, the system trusts any application that exceeds any flow bypass threshold, regardless of the application type. See the Firepower Management Center Configuration Guide or the Cisco ASA with FirePOWER Services Local Management Configuration Guide for more information.

Packet Capture at Time of Crash

Supported Platforms: Firepower Threat Defense, any manager

Introduced In: Version 6.2.2

Previously, the contents of any active capture on Firepower were not saved when the appliance experienced issues. You can now store active capture contents to flash/disk at the time of an appliance crash to facilitate troubleshooting.

Often, when you troubleshoot a crash that involves traffic, Cisco TAC requires you to specify exactly what traffic causes the crash. Cisco TAC can get this info from a core dump, but the information may be limited by the following factors:

- The packet might have been corrupted so no useful information is present in the core dump.
- The crash is caused by a combination of conditions created by a series of packets, but the core dump offers information from only the last packet.

The system now saves captured packets that go in and out of the Firepower appliance until the crash (if the circular option is specified for capture).

Access Control Rule Creation with REST API

Supported Platforms: Firepower Management Center

Introduced In: Version 6.2.2

Using the REST API, the system now supports bulk access control rule creation. Previously, if you had thousands of rules to create, each rule required a post process that could take anywhere from 5-10 seconds to complete. Now, you can submit all of these rules through a single post process greatly reducing the amount of time it takes to perform this action.

Automatic Application Bypass for Firepower Threat Defense

Supported Platforms: Any device managed by a Firepower Management Center

Introduced In: Version 6.2.2

Automatic Application Bypass (AAB) is now available on Firepower Threat Defense devices managed by a Firepower Management Center. Previously, it was only available on non-Firepower Threat Defense devices.

AAB allows you to limit the time Firepower spends on processing a single packet by bypassing inspection if a time limit is exceeded. If you enable AAB, you can adjust the bypass threshold from 250 milliseconds to 60,000 milliseconds (one minute). By default, the system uses 3,000 milliseconds (3 seconds).

AAB is most valuable in IPS inline deployments so you can balance packet processing delays with your network's tolerance for packet latency. When a malfunction within Snort or a device misconfiguration causes traffic processing time to exceed a specified threshold, AAB causes a partial restart of the Snort process and generates troubleshooting data that can help you determine the cause of the excessive processing time. See the Firepower Management Center Configuration Guide for more information.

Policy Deployment Improvements

Supported Platforms: Any device managed by a Firepower Management Center; ASA with FirePOWER Services managed by ASDM

Introduced In: Version 6.2.2

Deployment improvements significantly reduce the number of dropped or uninspected connections by eliminating Snort restarts when you deploy the following configurations:

- SMTP, POP, and IMAP preprocessor decoding depths
- Various adaptive profile, performance monitor, and advanced access control policy file and malware settings
- Access control rules or SSL rules with category/reputation conditions
- Nonbinary intrusion rule updates
- A change in the total number of intrusion or network analysis policies
- A **Detect Files** or **Block Files** action in a file policy rule

The system also warns you of Snort restarts when you do the following:

- Add a Firepower Threat Defense high availability pair
- Take various actions involving application detectors and user-defined applications

TCP Sequence Randomization Control

Supported Platforms: Firepower Threat Defense, any manager

Introduced In: Version 6.2.2

Each TCP packet carries two sequence numbers. By default, Firepower Threat Defense randomizes the sequence numbers in both the inbound and outbound directions. This feature provides the ability to disable (and if necessary, enable) this randomization with CLI using the **configure tcp-randomization** command.

You can determine if TCP sequence number randomization is disabled by entering the **show running-config policy-map** command and looking for the **set connection random-sequence-number disable** command. If the feature is enabled, there will be no associated command in the running configuration.

Note Although you can disable TCP sequence number randomization when using Firepower Device Manager, each time you deploy the configuration from Firepower Device Manager, the feature is reenabled. If you want to keep TCP sequence number randomization disabled, you must reenter the command after each deployment.

Security Enhancements for Updates: Signed Updates

Supported Platforms: Any

Introduced In: Version 6.2.2

For the system to verify that you are using the correct update file, updates to the system from Version 6.2.2+ are *signed*. Signed update files terminate in **.sh.REL.tar** instead of **.sh**.

If you are updating to Version 6.2.2 from Version 6.2.0 or a later 6.2.0.x patch, those update files are not signed. However, subsequent updates to the system will be.

Note After you upload a signed update file to the Firepower Management Center, the Updates tab on the **System** > **Updates** page can take several minutes to load as the system verifies the update file or files. Remove signed update files after you no longer need them to speed up the display.

Note The U.S. Government changed the name of the Unified Capabilities Approved Products List (UCAPL) to the Department of Defense Information Network ApprovedProducts List (DODIN APL). References to UCAPL in this documentation and the Firepower Management Center UI can be interpreted as references to DODIN APL.

Security Certifications Compliance for Additional Platforms

Supported Platforms: Firepower Management Centers, and all devices managed by Firepower Management Centers.

Introduced In: Version 6.2.2

Firepower Threat Defense devices managed by a Firepower Management Center now support security certifications compliance in Common Criteria (CC) mode or Unified Capabilities Approved Products List (UCAPL) mode using platform settings (**Devices** > **Platform Settings**).

Previously, these modes were available only on Firepower Management Centers and non Firepower Threat Defense devices.

Security Certifications Compliance Enhancements: Boot-Time FSIC

Supported Platforms: Firepower Management Centers, and all devices managed by Firepower Management Centers.

Introduced In: Version 6.2.2

When you boot any appliance that has security certifications compliance enabled, the system performs additional file system integrity checks (FSIC) to ensure the system is secure. If a check fails, the appliance does not boot, SSH access is disabled, and the only access is through the console. If this happens, contact Cisco TAC.

Security Enhancements and Other Updates to FlexConfig Templates

Supported Platforms: Firepower Threat Defense managed by a Firepower Management Center

Introduced In: Version 6.2.2

FlexConfig uses CLI template-based functionality on the Firepower Management Center to enable ASA functions that are not yet supported through the Firepower Management Center user interface.

Government certification requires that sensitive information (like passwords, shared keys in system-provided or user-defined FlexConfig objects) be masked using secret key variables. When you update the Firepower Management Center from Version 6.2.0 to Version 6.2.2, all sensitive information in FlexConfig objects are converted to secret key variable format.

Security Enhancements for Site-to-Site VPN

Supported Platforms: Firepower Threat Defense managed by a Firepower Management Center

Introduced In: Version 6.2.2

The following features were added for IKEv2:

- Transport Mode—To address Government Certificate requirement FCS_IPSEC_EXT.1.3 Refinement, transport mode (also known as host-to-host VPN).
- Hex Support for IKEv2 Preshared Manual Key—To address Government Certificate requirement FIA_PSK_EXT.1.4, we have added support for hex-based preshared key.
- Certificate Map Support—To address Government Certificate requirement FIA_X509_EXT.4.1, we implemented a certificate map used to determine the tunnel to use from the contents of the certificate.
- SA Strength Enforcement—To address Government Certificate requirement FCS_IPSEC_EXT.1.12, we added an option in the Firepower Management Center to ensure that the encryption algorithm used by the child IPsec SA is not higher than the parent IKE.

Security Enhancements in Device Platform Settings

Supported Platforms: Firepower Threat Defense managed by a Firepower Management Center

Introduced In: Version 6.2.2

The following requirements are now supported:

- You can configure console idle timeout for managed Firepower Threat Defense devices.
- You can configure secure syslog and upload Certificate for Firepower Threat Defense syslog-NGTLS.

Security Enhancement to Disable Expert Mode

Supported Platforms: Firepower Threat Defense, any manager

Introduced In: Version 6.2.2

To increase security, you can disable expert mode on Firepower Threat Defense devices. Note that you cannot reverse this command. If you need to restore access to expert mode, you must contact Cisco TAC.

Features and Functionality Introduced in Version 6.2.1

Cisco Firepower Version 6.2.1 has been replaced by Cisco Firepower Version 6.2.2, which offers the same functionality and supports the full set of Firepower platforms. For posterity, this section describes the new and updated features and functionality included in Version 6.2.1:

Table 1: New Features in Version 6.2.1: Core Firewall

Feature	Description	Supported Platforms
Remote Access VPN		• Firepower Management Center

Feature	Description	Supported Platforms
	Firepower Remote Access (RA) VPN allows individual users to connect to a private business network from a remote location using a laptop or desktop computer connected to the internet, or an Android or Apple iOS mobile device. Remote users transfer data securely and confidentially using encryption techniques crucial for data being transferred over shared mediums and the Internet. Key capabilities of RA VPN include: • Secured Access – provided by the Cisco AnyConnect VPN client using either SSL or IPsec tunneling and encryption protocols. This is the only client supported for remote access connectivity. • Authenticated & Authorized Access – AAA support for **Authentication** (LDAP/AD/RADIUS and Client Certificate-based), **Authorization** (RADIUS Authorization Attributes-DACL, Group Policy, Address Assignment, etc.) and **Accounting** (RADIUS). • VPN Connectivity – Connection Profiles and Group Policies allow you to define address assignments, split tunneling, the DNS server, timeouts, access hours, client firewall ACLs, and AnyConnect client profiles. • Monitoring & Troubleshooting – provides multiple analysis views so that VPN user activity can be tracked and analyzed over time. In addition, you can view the Remote Access VPN Troubleshooting Logs. Troubleshooting can be used when having issues creating or deploying a RA VPN policy, if RA VPN connections or traffic is not as expected, or if events and statistics are not populating properly. This feature also provides the capability to bulk logout the currently logged in VPN users. These functions can be used in either the Firepower Management Center or the Firepower Device Manager. • Availability – Firepower Threat Defense high availability, multiple interfaces (dual ISP), and multiple AAA servers are supported. • Licensing – Smart Licensing, based on the AnyConnect 4.x model, for Apex, Plus and VPN-only licenses. • Management – A simple RA VPN wizard on both the Firepower Management Center and the Firepower Device Manager which provides quick and easy set-up of: • RA VPN Policy configuration entities: including Connection Profiles, Group Polices, Address Pools,etc. • secure gateways to which the remote user connects to Firepower Threat Defense devices.	

Feature	Description	Supported Platforms
	- Interfaces on the managed Firepower Threat Defense that users will access to establish VPN connections. - The AnyConnect client image downloaded when a connection is initiated by a desktop or laptop platform. Mobile devices obtain AnyConnect from their App store. • Identity Integration and Monitoring – Seven new dashboard widgets allow you to monitor user VPN activity. This includes logon and logoff events, active session status, and the ability to monitor and terminate specific VPN sessions.	
QoS/Rate Limiting Enhancements	Rate limiting is a mechanism to manage the rate of traffic flowing in and out of network interfaces based on traffic attributes, such as application, file downloading, etc. It can achieve great results when enhanced with the capability to provide bandwidth control based on the traffic attributes, such as source zones, destination zones, source networks, destination networks, source ports, destination ports, applications, users, URLs, and ISE attributes. Network administrators are able to achieve rate limiting per network interface by configuring a QoS (Quality of Service) Policy on their Firepower Device Manager and deploying the policy to Firepower Threat Defense devices. Administrators can do the following in Version 6.2.1: • Rate limit traffic up to 100,000 Mbps (previously 1,000Mbps). • Use customer Security Group Tags (SGTs) in QoS rules. • Use original client network conditions (XFF, True-Client-IP, or custom-defined HTTP headers) in QoS rules.	• Firepower Management Center

Feature	Description	Supported Platforms
Packet Capture at Time of Crash	Previously, the contents of any active capture on Firepower were not saved when the appliance experienced issues. You can now store active capture contents to flash/disk at the time of an appliance crash to facilitate troubleshooting. Often times, when you troubleshoot a crash that involves traffic,Cisco TAC requires exactly what traffic causes the crash. Cisco TAC can get this info from a core dump, but the information may be limited by the following factors: • The packet might have been corrupted so no useful info is present in the core dump. • The crash is caused by combination of conditions createdby a series of packets, but core dump offers information from only the last packet. Version 6.2.1 now saves captured packets that are in and out of the Firepower appliance up until the point of box crash (if circular option is specified for capture).	• Firepower Management Center • Firepower Device Manager
Access Rule Bulk Insert	Using the REST API, Version 6.2.1 now supports bulk access control rule creation. Previously, if you had a thousand access rules to create, each access rule required a post process that could take anywhere from 5-10 seconds to complete. Now, using this API enhancement you can submit all of these rules through a single post process and greatly reducing the amount of time it takes to perform this action.	• Firepower Management Center
Firepower Management Center API Enhancement	The Firepower Management Center API now supports bulk access control rule creation. Previously, if you had a thousand access rules to create, each access rule required a post process that could take anywhere from 5-10 seconds to complete. Now, using this API enhancement you can submit all of these rules through a single post process and greatly reduce the amount of time it takes to perform this action.	• Firepower Management Center
Automatic Application Bypass	Automatic Application Bypass (AAB) provides the ability to limit the amount of time spent processing a single packet through an interface. It enables those packets to bypass detection if the time is exceeded. The feature functions with any deployment; however, it is most valuable in IPS inline deployments to balance packet processing delays with network's tolerance for packet latency. When a malfunction within Snort or a device misconfiguration causes traffic processing time to exceed a specified threshold, AAB causes Snort to restart and generates troubleshooting data that can be analyzed to determine the cause of the excessive processing time. A user can change the bypass threshold if the option is selected. The default setting is 3,000 milliseconds. The valid range is from 250 milliseconds to 60,000 milliseconds.	• Firepower Management Center

Feature	Description	Supported Platforms
FlexConfig Updates	FlexConfig uses CLI template-based functionality on the Firepower Management Center to enable ASA functions that are not yet supported through the Firepower Management Center user interface. As per the Government Certification requirements, all sensitive information like password, shared keys in system-provided or user-defined FlexConfig object should be masked using secret key variables. After you update the Firepower Management Center to Version 6.2.1, all sensitive information in FlexConfigObjects are converted to secret key variable format. In addition, the following new FlexConfig templates are added as part of Version 6.2.1: • **TCP Embryonic connection limit and timeout configuration** template allows you to configure embryonic connection limits/timeout CLIs to protect from SYN Flood DoSAttack. • **Turn on threat detection configure and clear** templates allow you to configure threat detection statistics for attacks intercepted by TCP Intercept. • **IPV6 router header inspection** template allows you to configure of IPV6 inspection header for selectively allow/block certain headers with different types (e.g. allowing RH Type 2,mobile). • **DHCPv6 prefix delegation** template allows you to configure one outside (PD client) and one inside interface (recipient of delegated prefix) for IPv6 prefix delegation.	• Firepower Management Center
Policy Deployment Improvements	Elimination of Snort restarts during configuration deployment of: • SMTP, POP, and IMAP preprocessor decoding depths • HTTP preprocessor compression depths • Affected adaptive profile, performance monitor, and advanced access control policy file and malware settings Warnings of Snort restarts when: • Turning on or breaking Firepower Threat Defense high availability • Activating, deactivating, or modifying application detectors	• Firepower Management Center

Feature	Description	Supported Platforms
CLI Command to Control TCP Sequence Randomization	Each TCP packet carries two sequence numbers. FTD devices, by default, randomizes the sequence numbers in both the inbound and outbound directions. This feature provides the ability to enable and disable this randomization via the command line. If necessary, to confirm TCP randomization is disabled, collect TCP packets on inside and outside interface. For the same packet on inside and outside interface sequence numbers will remain the same.	• Firepower Management Center • Firepower Device Manager

Table 2: New Features in Version 6.2.1: Government Certification Support

Feature	Description	Supported Platform
Government Certificate Support for Site-to-Site VPN	The following features that were added to Site-2-Site VPN that were not supported in Version 6.2.0: • Transport Mode – In order to address Government Certificate requirement FCS_IPSEC_EXT.1.3 Refinement, transport mode (also known as host-to-host VPN). • Hex Support for IKEv2 Pre-shared Manual Key – In order to address Government Certificate requirement FIA_PSK_EXT.1.4, we have added support for hex-based pre-shared key. • Certificate Map Support – In order to address Government Certificate requirement FIA_X509_EXT.4.1, we implemented a certificate map used to determine the tunnel to use from the contents of the certificate. • SA Strength Enforcement - In order to address Government Certificate requirement FCS_IPSEC_EXT.1.12, we added an option in the Firepower Management Center to ensure that the encryption algorithm used by the child IPsec SA is not higher than the parent IKE. **Note** The features supported are for IKEv2only.	• Firepower Management Center • Firepower Device Manager
Platform Setting Enhancements (Compliance Mode Support)	The following requirements have been supported in Version 6.2.1 release of Firepower Management Center: • User should be able to configure console idle timeout for managed Firepower Threat Defense devices. • User can configure secure syslog and should be able to upload Certificate for Firepower Threat Defense syslog-NGTLS.	• Firepower Management Center

Feature	Description	Supported Platform
Ability to Disable Expert Mode for Firepower Threat Defense	In order to increase security, this feature allows you to disable expert mode on Firepower Threat Defense environments.	• Firepower Management Center • Firepower Device Manager
USGv6 FlexConfig: Firepower Management Center Routing Headers	FlexConfig uses CLI template-based functionality on the Firepower Management Center to enable ASA functions that are not yet supported through the Firepower Management Center user interface. The USGv6 NPD:FW certification requires that the USGv6GCT TME selectively allow/block IPv6 Headers of differenttypes (e.g. EH, Routing, etc.). On an ASA FirePOWER module, the user was able touse policy maps to allow this, but you could not figure this on Firepower Management Centers. Now, you are able to develop policy objects and policy groups to configure policies to block/permit/log certain IPv6 headers.The header types now able to be blocked/permitted/logged are: • Authentication extension header • Destination-option extension header • ESP extension header • Fragment extension header • Hop-by-hop extension header • Routing header type 2-225	• Firepower Management Center

The following functionality changed in Version 6.2.1:

- Updating from Version 6.2.0.1 or a subsquent 6.2.0.x patch to Version 6.2.1 removes the Intelligent Application Bypass (IAB) **All applications including unidentified application** option from the user interface.

  If this option is enabled when you update to Version 6.2.1, and your access control policy does not contain bypassable application and filter configurations, the user interface has the following unexpected behaviors:

  - IAB is enabled, but the **All applications including unidentified applications** option is no longer present.
  - The IAB configuration page displays **1 Applications/Filters**, incorrectly indicating that you have configured one application or filter.
  - The Selected Applications and Filters window in the applications and filters editor displays either deleted (Firepower Management Center, ASA with FirePOWER Services) or Any Application (ASA FirePOWER module managed by ASDM).

Changed Behavior and Functionality

The system exhibits the following behavior changes in Version 6.2.2:

URL Filtering on Lower-Memory Devices

Supported Platforms: Lower-memory devices (7000 Family and the following ASA models: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, and ASA 5525-X)

Introduced In: Version 6.1.0.3 and Version 6.2.0.1

If you are updating from Version 6.2.0, you may notice that the system now performs cloud lookups to determine category and reputation for websites not in the local database on lower-memory devices.

If you are updating from Version 6.2.0.1 or a later 6.2.0.x patch the system already exhibits this behavior.

This change was implemented because due to memory limitations, some device models perform most URL filtering with a smaller, less granular, set of categories and reputations. For example, even if a parent URL's subsites have different URL categories and reputations, some devices may store only the parent URL's data.

Deprecated Functionality

The following feature is deprecated functionality in Verison 6.2.2:

- The **configure snort preserve-connections {enable | disable}** CLI command is not available on managed devices running Firepower Threat Defense in Version 6.2.2.

CHAPTER 3

Platforms and Environments

The following sections describe the supported platforms and environments in Version 6.2.2, 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 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.

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

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

The Firepower web interfaces for Version 6.2.2 have been tested on the following browsers:

Table 3: Supported Web Browsers

Browser	Required Settings
Google Chrome 57	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 52	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 Firefox 57 or later.

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.

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 4: 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

Terminology for Version 6.2.2

The terminology and branding used in Version 6.2.2 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 5: Product Terminology and Branding in Version 6.2.2

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
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

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

- Firepower Management Center Configuration Guide and online help
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager and online help
- Command Reference for Firepower Threat Defense
- ASA with FirePOWER Services Local Management Configuration Guide
- Command Reference for Firepower Threat Defense
- Cisco Firepower Threat Defense Virtual Using Firepower Device Manager Deployment Quick Start Guide
- Cisco Firepower 2100 Series Hardware Installation Guide
- Regulatory Compliance and Safety Information—Cisco Firepower 2100 Series
- Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide
- Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Device Manager Quick Start Guide
- Cisco Firepower 2100 Series Faults and Error Messages
- Cisco FXOS Troubleshooting Guide for the Firepower 2100 Series
- Firepower System Event Streamer Integration Guide
- Firepower REST API Quick Start Guide
- Cisco Firepower Compatibility Guide
- Open Source Used in Firepower System Version 6.2.2
- Cisco Firepower System Feature Licenses

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

- 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:

- When to Update versus Reimage/Redeploy, on page 30
- Update Paths to Version 6.2.2, on page 30
- Update Sequence Guidelines, on page 33
- Pre-Update Readiness Checks, on page 36
- Pre-Update Configuration and Event Backups, on page 38
- Patch or Hotfix for New Dynamic Analysis CA Certificate, on page 38
- Traffic Flow and Inspection During the Update, on page 39
- Time and Disk Space Requirements For Version 6.2.2, on page 43

When to Update versus Reimage/Redeploy

In most cases, we recommend you upgrade. However, you must reimage physical devices or redeploy virtual appliances in the following cases:

- Switching device implementations—You want to switch your ASA 5500-X series device between ASA with FirePOWER Services and Firepower Threat Defense.
- Switching management methods—You want to switch management of Firepower Threat Defense between a Firepower Management Center and Firepower Device Manager, and the initially installed version on the device was Version 6.0.1.
- Switching virtual hosting environments—You want to recreate a virtual appliance in a new hosting environment. For example, if you are using Firepower Threat Defense Virtual for VMware but want to deploy in AWS, you must deploy a fresh virtual device.
- New platforms—You want to deploy Firepower Threat Defense Virtual for VMware managed by Firepower Device Manager. This environment is newly supported in Version 6.2.2.
- Other—You are unable or disinclined to follow the required update path as described in Update Paths to Version 6.2.2, on page 30.

For details on reimaging/redeploying, see Reimage or Redeploy Version 6.2.2, on page 55. For details on switching device implementations, management methods, or virtual hosting environments, see Switching Implementation, Management Method, or Hosting.

Update Paths to Version 6.2.2

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

- Firepower Management Center—Version 6.2.0.x or Version 6.2.1
- Firepower 2100 series with Firepower Threat Defense—Version 6.2.1
- All other devices—Version 6.2.0.x

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.

Another example, updating a Firepower Management Center to Version 6.0 may cause traffic outages and system issues if you are are managing devices running X, Y, or earlier. Before you begin the update to Version 6.0, edit the access control policies deployed to those devices, disable the **Retry URL cache miss lookup** option on the Advanced Options section of the Access Control window, then redeploy. To review the release notes for each destination version on your update path, see the Release Notes page.

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 **Note** For Firepower Management Centers running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2
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 **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
Firepower Management Center Virtual: KVM	Version 6.1.0 > Version 6.2.0 > Version 6.2.2 **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

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
Firepower Threat Defense Virtual: KVM Firepower 4150	Version 6.1.0 > Version 6.2.0 > Version 6.2.2

Firepower Threat Defense Platform	Update Path
Firepower Threat Defense Virtual: Azure	Version 6.2.0 > Version 6.2.2
Firepower 2110, 2120, 2130, 2140	Version 6.2.2 **Note** For Firepower 2100 Series devices running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2

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
Firepower 2110, 2120, 2130, 2140	Version 6.2.2 **Note** For Firepower 2100 Series devices running Version 6.2.1, use the following update path: Version 6.2.1 > Version 6.2.2
Firepower Threat Defense Virtual: VMware	Version 6.2.2

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

NGIPS Platform	Update Path
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

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
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

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, on page 33
- Update Sequence for High Availability Firepower Threat Defense Devices, on page 34
- Update Sequence for Clustered Firepower Threat Defense Devices, on page 35
- Update Sequence for 7000 and 8000 Series Devices in High Availability, on page 35
- Update Sequence for High Availability 7000 and 8000 Series Devices in Inline Deployment, on page 35
- Update Sequence for Stacked 8000 Series Devices, on page 36

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 45 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.

⚠ **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.

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 48 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 `tailf` 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 6: 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 7: 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

Device	Deployment	Traffic Behavior
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
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 8: 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 9: 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
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 For Version 6.2.2

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

You must also have enough time to perform the upgrade. We provide estimates of upgrade times for each release. Note that depending on your deployment, upgrades may take longer than the provided estimates. For example, lower-memory appliances and appliances under heavy load may take longer to upgrade. These estimates also do not include the time required to complete a readiness check.

Platform	Space on /	Space on /Volume	Space on Manager	Time
FMC	From 6.2.0: 22 MB From 6.2.1: 21 MB	From 6.2.0: 6467 MB From 6.2.1: 6916 MB	—	From 6.2.0: 52 min From 6.2.1: 61 min

Platform	Space on /	Space on /Volume	Space on Manager	Time
FMCv	From 6.2.0: 24 MB From 6.2.1: 24 MB	From 6.2.0: 6987 MB From 6.2.1: 5975 MB	—	Hardware dependent
Firepower 2100 series	5613 MB	5613 MB	925 MB	57 min
Firepower 9300 chassis	4635 MB	4635 MB	743 MB	14 min
FTDv	.92 MB	3586 MB	987 MB	Hardware dependent
ASA 5500-X series with FTD	.16 MB	3683 MB	987 MB	80 min
Firepower 7000/8000 series	18 MB	6745 MB	1300 MB	27 min
ASA FirePOWER	16 MB	7021 MB	1200 MB	131 min
NGIPSv	18 MB	7261 MB	1300 MB	Hardware dependent

CHAPTER 6

Update to Version 6.2.2

Before you begin, you must thoroughly read and understand these release notes, especially Before You Update: Important Notes, on page 29 and Pre-Update Readiness Checks, on page 36.

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

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 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 38 for more information.

- Update Firepower Management Centers, on page 45
- Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 48
- Update ASA FirePOWER Modules Managed with ASDM, on page 50
- Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 52
- Update Firepower Threat Defense Devices with the Firepower Device Manager, on page 54

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 33 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, on page 30.

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

For more information, see the following topics:

- Platforms and Environments, on page 19
- Before You Update: Important Notes, on page 29

Step 3 Download the update from the Support site:

- Upgrade the Firepower Management Center (MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500) from Version 6.2.1:

  Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.2-xxxx.sh.REL.tar

- Upgrade Firepower Management Center (MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500) and Firepower Management Center Virtual from Version 6.2.0:

  Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.2-xxxx.sh

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 36 or Run a Readiness Check through the Firepower Management Center Web Interface, on page 37.

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 If prompted, review and accept the End User License Agreement (EULA). You must accept to continue.

Step 14 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 15 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 16 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 17 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 18 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 19 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 33.

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 33 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, on page 30.

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

For more information, see the following topics:

- Platforms and Environments, on page 19
- Before You Update: Important Notes, on page 29

Step 3 Update Firepower Management Centers, on page 45.

A Firepower Management Center must be running at least Version 6.2.2 to update a device to Version 6.2.2.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 34.

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_Upgrade-6.2.2-xxxx.sh

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

  Cisco_FTD_Upgrade-6.2.2-xxxx.sh

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

  Cisco_FTD_SSP_Upgrade-6.2.2-xxxx.sh

- Firepower 2100 series with Firepower Threat Defense:

  Cisco_FTD_SSP_FP2K_Upgrade-6.2.2-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 36 or Run a Readiness Check through the Firepower Management Center Web Interface, on page 37.

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.

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

For more information, see the following topics:

- Platforms and Environments, on page 19
- Before You Update: Important Notes, on page 29

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_Upgrade-6.2.2-xxxx.sh

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 If this is the first time installing software on this device, review and accept the End User License Agreement (EULA). You *must* accept to continue.

Step 11 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 12 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 13 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 33 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, on page 30.

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

For more information, see the following topics:

- Platforms and Environments, on page 19
- Before You Update: Important Notes, on page 29

Step 3 Update Firepower Management Centers, on page 45.

A Firepower Management Center must be running at least Version 6.2.2 to update a device to Version 6.2.2.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_Upgrade-6.2.2-xxxx.sh

- NGIPSv:

Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.2.2-xxxx.sh

- ASA with FirePOWER Services:

  Cisco_Network_Sensor_Upgrade-6.2.2-xxxx.sh

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 36 or Run a Readiness Check through the Firepower Management Center Web Interface, on page 37.

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_Upgrade-6.2.2-xxxx.sh

- Firepower 2100 series with Firepower Threat Defense:

  Cisco_FTD_SSP_FP2K_Upgrade-6.2.2-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

Reimage or Redeploy Version 6.2.2

In most cases we recommend updating to Version 6.2.2. However, you can restore the Firepower System to factory defaults by reimaging a physical appliance or redeploying a virtual appliance. If you are not sure what to do, see When to Update versus Reimage/Redeploy, on page 30.

For details on the reimage/redeploy process, see the quick start or getting started guide for your platform. You can find these guides in the appropriate documentation roadmap:

- Cisco Firepower System Documentation Roadmap
- Navigating the Cisco ASA Series Documentation

Before You Reimage or Redeploy Firepower Threat Defense

If you are reimaging or redeploying a Firepower Threat Defense device, avoid accruing orphan entitlements in the Cisco Smart Software Manager by unregistering the device's manager:

- Firepower Management Center—See Unregister a Firepower Management Center, on page 55
- Firepower Device Manager—See Unregister an FTD Device Using FDM, on page 56

After You Reimage or Redeploy

After you reimage or redeploy, update intrusion rules and the vulnerability database (VDB) to the latest version on the Support site. For more information, see the *Firepower Management Center Configuration Guide*.

Restoring to factory defaults returns the system password to **`Admin123`** after the reboot sequence.

- Unregister a Firepower Management Center, on page 55
- Unregister an FTD Device Using FDM, on page 56

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

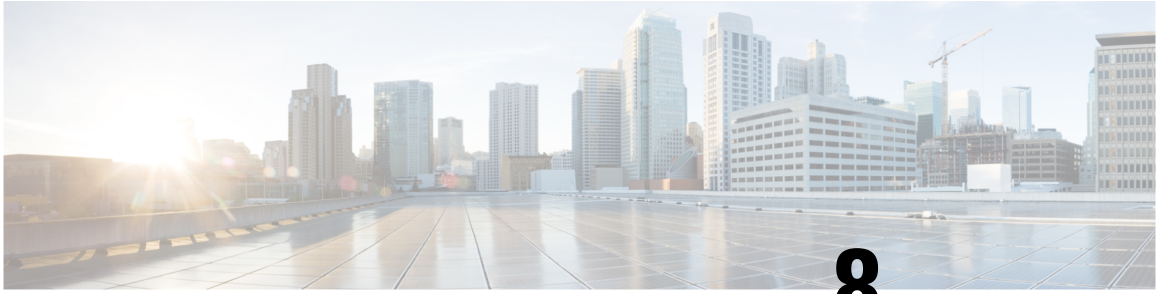
Unregister locally managed Firepower Threat Defense devices from the Cisco Smart Software Manager before you either reimage or switch to remote (FMC) management.

Step 1 Log into the Firepower Device Manager.

Step 2 Click the name of the device in the menu, 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.



CHAPTER 8

Known Issues in Version 6.2.2

The following table addresses known defects at the time of publication of these release notes. For an updated list of known issues, run the provided query in the Bug Search Tool.

If you have a Cisco support contract, use the Firepower Management Center query or the ASA FirePOWER module query as a dynamic search for all open defects with a severity 3 and higher.

Caveat ID Number	Description
CSCvd29174	Allow user to delete TID sources when stuck those on **Downloading**, **Parsing**, or **Scheduled** mode
CSCve54340	ASA 5506-X classic license save throws exception
CSCve89037	Policy name and description are modified in report for Access Control Policy
CSCvf07785	Logout user activity events not being generated when logouts issued from Active Sessions
CSCvf28011	Language changes affects in intrusion rules page for the current user
CSCvf32894	Device name change from device management not reflected on Elements page
CSCvf33988	Unable to verify a expected Troubleshoot file in Firepower Management Center high availability
CSCvf36074	6.2.2: AVC + UDP S2S VPN on SSPs - if pushed past performance limit, performance drops significantly
CSCvf42199	Core seen while running snort restart automated regression suite for more than 14 hours.
CSCvf50556	FlexConfig default value of deployment mode is wrong for new object
CSCvf51410	In production env we might receive observations with modified observable value
CSCvf57485	Group-policy doesn't push webvpn subconfig mode if only ikev2 protocol is selected
CSCvf64831	Incorrect IPv6 event info seen in FP 6.2.2-47
CSCvf75135	Configure **sysopt connection permit-vpn** using FlexConfig to prevent unintended clear-text traffic

Caveat ID Number	Description
CSCvf77429	Upgraded 6.2.2 Firepower Management Center is not showing VPN Troubleshooting events
CSCvf82315	IP address for 10G interfaces cannot be changed from GUI.
CSCvf82316	**System** > **Configuration** > **Management Interfaces** page takes 25 min to load.
CSCvf97412	**.REL.tar** upgrade file causes **System** > **Updates** page in GUI to be slow / unresponsive
CSCvg84495	Remote access VPN using an OpenLDAP realm/server doesn't use the correct naming attribute

CHAPTER 9

Resolved Issues in Version 6.2.2

The following table addresses defects resolved at the time of publication of these release notes. For an updated list of known issues, run the provided query in the Bug Search Tool.

If you have a Cisco support contract, use the Firepower Management Center query or the ASA FirePOWER module query as a dynamic search for all resolved bugs with a severity 3 and higher.

Table 10: Resolved Security Caveats in Version 6.2.2

Caveat ID Number	Description
Security Issue CSCve12652	Cisco Firepower System Software Secure Sockets Layer Policy Bypass Vulnerability

Table 11: Resolved Caveats in Version 6.2.2

Caveat ID Number	Description
CSCuu97541	turn off older SSL/TLS versions and ciphers
CSCux61528	Sensor managed by Management Center thinks it is managed locally
CSCuy08223	Firepower Management Center 6.0.0 User Interface does not show more than 8 User Agents
CSCuy17170	After upgrading to 6.0, you cannot remove tasks from the taskbar
CSCuy50039	In Task Status page the task is stuck/spinning
CSCuy65203	Inline result showing **would have dropped**
CSCva06227	Only 1500 Group Members are downloaded per group for an AD Realm
CSCvb00980	Detection engine, primary detection engine, alerting process health alert
CSCvb16465	Security Intelligence category goes missing from Security Intelligence events after time
CSCvb22670	SFDCNotificationd dumps core if stopped after SFDataCorrelator
CSCvb30960	Large flow introduces latency on all traffic in FirePower Service on ASA

Caveat ID Number	Description
CSCvb34534	access control policy search highlight incorrectly highlights
CSCvb44254	ASA 5506-X Firepower Threat Defense Reset Button
CSCvb57936	Unable to save AD join credentials from edit realm page
CSCvb71265	Firepower: Identity policy shows incorrect warning about Zones
CSCvb72561	Mperf causing high CPU and stays constantly high .
CSCvc06133	Firepower Management Center freezes when attempt is made to sort the App Detectors
CSCvc09167	Firewall rules may not be in sync with firmware rules following policy apply
CSCvc10913	SFDataCorrelator polling for status of file analysis can fail in certain circumstances
CSCvc33269	Document bug: Impact of Leap second on Firepower products
CSCvc37849	Cannot edit intrusion policy after upgrade to 6.1 due to undefined rule state
CSCvc46914	Rule copy and paste reset to top instead of the rule being edited
CSCvc59913	Mismatched VLAN tagged traffic has inconsistent access control rule matches.
CSCvc64185	Task getting created whenever Cloud Management option is selected
CSCvc66770	Mishandled rule index numbers on multipage access control policies with collapsed rule categories
CSCvc84721	Health monitor error: **The cloud databases for these appliances are not synced**
CSCvc90768	Excessive logging from sfbbhealthd process.
CSCvc91394	Making minor changes to included/excluded users in a realm may cause unexpected behavior
CSCvc95382	User identity lost due to limited identity timeout configuration
CSCvd04965	Performance issues related to High Availability
CSCvd11997	Database settings for a fresh deployment were not saved
CSCvd28945	modbus false postive on **MODBUS_BAD_LENGTH**
CSCvd29021	Cannot break Firepower Threat Defense high availability if one of the paired devices has failed
CSCvd35243	C-groups modification during policy apply causes AAB to trigger.
CSCvd35905	upgraded 6.x Management Center incorrectly deploys obsoleted detectors to 6.x devices
CSCvd37120	Snort is unable to map the filename if there are unsupported characters.
CSCvd41054	SSL Trusted CAs not deployed to sensor in some cases

Caveat ID Number	Description
CSCvd51190	Snort reloads cause memory leaks and CPU increase
CSCvd51463	Custom detection/Clean list is incorrect with multiple file polices in use
CSCvd56035	Custom NAP rule with inline normalization enabled does not enable normalization
CSCvd57039	Deadlock in Firepower Management Center high availability syncronization
CSCvd59199	Mismatch between internal database entries prevents correct session propagation
CSCvd61965	micro engine failure failure with msg Microengine heartbeat stopped
CSCvd62536	apache not listening on loopback IPv4 when management interface has only ipv6 configured
CSCvd62879	Repeated same DiskMgr logs flooding messages log - causing small log retention period
CSCvd70549	Query Cisco CSI for Unknown URLs option is not properly synchronized in Management Center pairs
CSCvd73834	Show user information in connection events for flows hitting early deny
CSCvd78338	Correlation Events and Syslog Events show incorrect local rule SID
CSCvd89890	Policy deploy hangs at 40% with the object names end with [_]
CSCvd90569	High availability Status health module should not run on device
CSCvd91019	Unable to delete third party vulnerabilities when the host count associated with them is > 100
CSCvd93722	SSL **Block** action when Extended Master Secret is used with SSL Policy **Known Key Decrypt**
CSCvd94044	7000 and 8000 Series Device with Passive Interface does not Failover when Active device powers off
CSCvd94183	Intermittent failure in User Group lookup.
CSCvd95667	Data channel traffic on windows FTP server aren't matching the pin hole session as expected
CSCvd97249	Firepower Threat Defense: block depletion with continuous SSL traffic and **decrypt resign** enabled.
CSCvd99119	Unable to import if Access Control rules has Realm as matching condition
CSCvd99574	Snort process at 100% and takes excessive amount of time to parse IPS rules.
CSCve02069	2048 byte block depletion with continuous SSL traffic and **decrypt resign** enabled on Threat Defense

Caveat ID Number	Description
CSCve02220	eStreamer certificate generates errors with a McAfee ESM generationQualifier verification failed
CSCve04055	Docs have incorrect commands to suspend or resume Firepower Threat Defense high availability
CSCve08525	URL DB Download Fail with **error -8**
CSCve08961	Stack entering bypass due to disk space health alert
CSCve10406	SFDataCorrelator will not stop on Threat Defense device due to database connection corruption
CSCve11915	POP3 payload inspection not proper on snort with the file detection policy
CSCve13738	Check UUID of Firepower Management Center high availability pair and both having same UUID
CSCve15155	Host input operations can overwhelm high availability transactions
CSCve17116	Access control rule is not matched correctly if src zone and dst zone have different types
CSCve18975	Nothing is shown when clicked on **Policy Assignements**
CSCve20634	Creating ngfw rules with [#] character prevent **event_alerter** from starting.
CSCve30147	Sub-domain SI objects cannot be deleted
CSCve32346	SIGABRT ActionQueueScrape cores in Firepower Management Center high availability
CSCve34090	snort stuck or signal 6 core with interactive block rule
CSCve34181	Static URL/DNS lists are not included in backup
CSCve34792	Threat Defense-NAT:Deployment fails when Auto nat group object values overlapped with interface IP.
CSCve34924	When expanding individual categories in Access Control Policy rule ID changes
CSCve35816	SFDataCorrelator segfault due to null pointer dereference in **handle_host_address_changes()**
CSCve37999	Deployment fails when SSL Platform Settings has deprecated RC4-SHA and RC4-MD5 algorithms configured
CSCve38488	after upgrade, sessions which were deleted were still present in sensor's firewall
CSCve39409	Cannot select **Inherit from base policy** check box
CSCve41306	Firepower Management Center **Interface Type Mismatch with Syslog Server Ip Type** error
CSCve41647	Sessions for local ISE users don't get deleted when delete is attempted

Caveat ID Number	Description
CSCve42702	Device Manager bootstrap aborted - URL category and reputations not populated in URL filtering rules
CSCve44987	eStreamer service sends corrupt messages and spams log files with **Not connected**
CSCve47800	Port Scan: IP Protocol scanning not getting detected.
CSCve47868	Snort not triggering Event 123:7 **FRAG3_ANOMALY_BADSIZE_LG**
CSCve47923	eStreamer log spam **Unable to open directory**
CSCve51315	record_count for interface stats from the sensor are being set to 0, coring SFDatacorrelator.
CSCve51357	5506/5508/5516 Threat Defense console login does not work if console speed set to 115200 in rommon
CSCve53544	Firepower Management Center high availability sync fails if file name contains 2 dots [**..**]
CSCve53812	SFDataCorrelator still in local management mode after deployed from Management Center
CSCve54447	**iprep_proxy.conf** should encode special characters in pass for authetication
CSCve61591	BitTorrent traffic not blocked consistently on resumed sessions.
CSCve64643	REST API internal error when removing AP rule from API that moved via GUI
CSCve64763	eStreamer core when FireAMP event has no SHA
CSCve66196	Editing syslog server platform setting policy and deploy does not push the correct cli to device
CSCve71028	NTP Default Server addresses can be modified
CSCve72760	Missing column netmap_num from the join on **event_extra_data** table.
CSCve73110	Specific mysql statement causing 6.2.1 upgrade failure
CSCve73175	**RPC.conf** not getting properly re-enabled during resumed upgrades
CSCve73601	Threat Defense: Blocking Facebook post/chat/comments/likes application not working for Firefox
CSCve74585	SFDataCorrelator crash or exit when event table **contains large highest index**
CSCve74902	REST identity application and ADI leak File Descriptors
CSCve81576	REST API : PUT - Multiple entries allowed for the same user in Access policy Rule
CSCve82386	Configuring an IP pool for a diagnostic port channel interface on an Threat Defense cluster fails

Caveat ID Number	Description
CSCve84424	Firepower 2110 Firmware version **MISMATCH** error message after upgrade
CSCve84629	Add code to reread **/etc/sf/devicecap.conf** file when moving to local management
CSCve89196	Double byte characters are not rendered correctly for Identity Policy Name and description
CSCve94250	SFDataCorrelator coring due to **ids_event_msg_map** message being null
CSCve94848	MC2000 and MC4000 can rarely hang during boot
CSCve95026	**ids_event_alerter** causes high CPU on Threat Defense device when UUID is missing from EOAttributes
CSCve95168	Unicode file support over SMB on Firepwer Threat Defense
CSCve99153	Access control policy/Pre-filter rules are negated and readded on usage of icmp objects
CSCve99203	256 low block count leads to traffic failures due to alloc to inspect snort
CSCvf01103	SNMP Username on Platform Settings accepts whitespace characters alone as name
CSCvf02208	Management Center: Deleting 1 category in nested access control policy deletes all categories
CSCvf05977	Firepower Threat Defense management interface link flaps when IPv6 gateway is configured
CSCvf09949	Incorrect access control rule is matched in FTD when it is setup in **passive** mode.
CSCvf10781	SFDataCorrelator segfaults repeatedly when processing SSL certificate details
CSCvf12124	Third Party Vulnerability Maps won't save
CSCvf14190	**Multiple routes with same metric or gateway exists** error when configuring ECMP
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
CSCvf16288	after captive portal authentication, packet is incorrectly associated with realm ID 0
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
CSCvf22098	Management interface bootstrap fails with IPv6 only configuratiom and no available DHCPv4 servers
CSCvf30502	Documentation has incorrect info for Max Response Length on Client-Level FTP Options.

Caveat ID Number	Description
CSCvf36025	SFDataCorrelator segfaults during loading of compliance rules
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
CSCvf40350	Static route checking is too restrictive
CSCvf41244	ACT LEDS do not reflect the correct high availability states of the devices
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
CSCvf55850	access-list rules missing after policy deployment on Firepower Threat Defense
CSCvf57891	Need documentation how to view available OS fingerprint in VDB
CSCvf62276	Missing IP address in AMP cloud malware events
CSCvf74015	After a Manual Sync of Smart License, upgrade from 6.2.0-363 to 6.2.2-66 fails
CSCvf74292	Outage caused by process exiting

CHAPTER 10

For Assistance

Thank you for choosing Firepower.

- Online Resources, on page 67
- Contact Cisco, on page 67

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