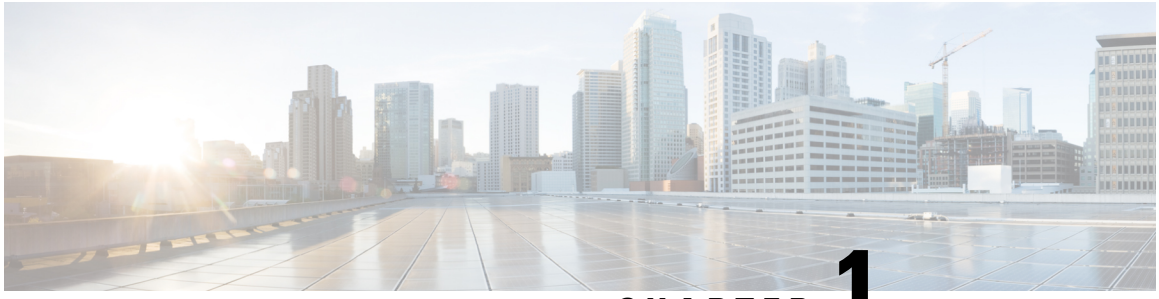
Firepower System Release Notes, Version 6.2.0

First Published: 2017-01-23

Last Modified: 2018-09-27

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

CONTENTS



CHAPTER 1

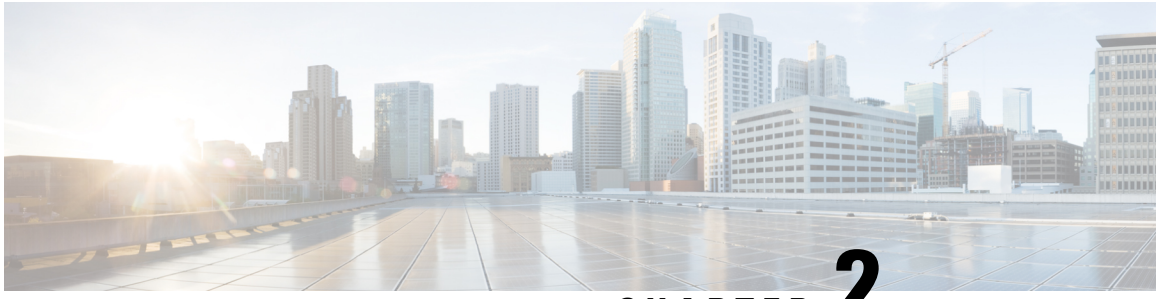
Introduction

This document describes the Version 6.2.0 Firepower update.

Even if you have experience with previous Firepower updates, make sure you thoroughly read and understand this document.

Caution Before you reimage a Firepower Threat Defense device or a Firepower Management Center that manages a Firepower Threat Defense device, you must unregister the managing appliance from the Cisco Smart Software Manager. If you do not unregister the managing appliance, orphan entitlements accrue against your total entitlements in the Smart Software Manager. For more information, see Unregister a Firepower Management Center, on page 63 and Unregister an FTD Device Using FDM, on page 64.

Note Devices running Version 6.2.0 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 the Hotfix BX for more information.



CHAPTER 2

Supported Platforms and Environments in Version 6.2.0

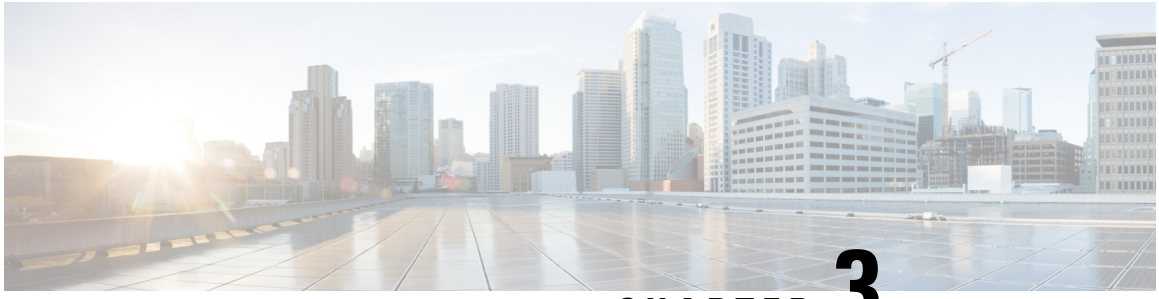
The following table lists the supported platforms for Version 6.2.0:

Table 1: Supported Platforms and Environments

Supported Platform	Supported Environment
Firepower Management Centers: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500	—
64-bit Firepower Management Center Virtual	• VMware vSphere/VMware ESXi 5.5 • VMware vSphere/VMware ESXi 6.0 • Amazon Web Services (AWS) VPC/EC2 • Kernel-based virtual machine (KVM)
7000 and 8000 Series devices: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	—
NGIPSv (virtual managed devices)	• VMware vSphere/VMware ESXi 5.5 • VMware vSphere/VMware ESXi 6.0

Supported Platform	Supported Environment
Cisco ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60 **Note** You can also configure these devices as an ASA FirePOWER module managed by ASDM.	ASA OS, for ASA FirePOWER: • 9.5(2), 9.5(3) except 5506 models • 9.6(x) • 9.7(x) • 9.8(x) **Note** The ASA 5506-X does *not* support the ASA FirePOWER module when running ASA Version 9.5(x). ASDM Version 7.7(1) and later. **Note** The ASA 5506-X, ASA 5508-X, and ASA 5516-X require ROMMON Version 1.1.8 or later.
Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X **Note** You can also configure these devices as Firepower Threat Defense managed by Firepower Device Manager. For more information, see the System Management topic in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.	—
Firepower 9300 appliance with Firepower Threat Defense and the Firepower 4100 series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150	FXOS Version 2.1(1) and later, or Version 2.2(1) and later. **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. For more information, see CSCvh64138 in the Cisco Bug Search Tool. **Note** The Firepower 9300 appliance requires ROMMON Version 1.0.10 or later.

Supported Platform	Supported Environment
Firepower Threat Defense Virtual	• VMware vSphere/VMware ESXi 5.5 • VMware vSphere/VMware ESXi 6.0 • AWS VPC/EC2 • KVM • Microsoft Azure Standard D3 • Microsoft Azure Standard D3_v2



CHAPTER 3

Management Capability in Version 6.2.0

Management Capability: Firepower Management Center

You can use the Firepower Management Center web interface to configure and manage the Firepower Management Center and its managed devices. Alternatively, you can use the UI on specific device platforms to configure and manage those specific device platforms (see Local Management Capability: ASA FirePOWER Module, Firepower Device Manager, and 7000 and 8000 Series Devices).

If a managed device is running Version 6.2.0, you *must* use at least Version 6.2.0 of the Firepower Management Center to manage the device. If a Firepower Management Center is running Version 6.2.0, it can manage devices running the versions specified in the following table.

Table 2: Device Version Requirements to be Managed by Firepower Management Center Running Version 6.2.0

Device	Minimum Required Version for Device
7000 and 8000 Series managed devices	Version 6.1.0
NGIPSv virtual managed devices	Version 6.1.0
ASA with FirePOWER Services on ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60	Version 6.1.0
ASA with FirePOWER Services on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X	Version 6.1.0
Firepower Threat Defense on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Version 6.1.0

Device	Minimum Required Version for Device
Firepower Threat Defense on Firepower 9300 (with SM-24, SM-36, or SM-44 security modules)	Version 6.1.0
Firepower Threat Defense on Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150	Version 6.1.0
Firepower Threat Defense Virtual	On VMware: Version 6.1.0 On AWS: Version 6.1.0 On KVM: Version 6.1.0 On Azure: Version 6.2.0

Local Management Capability: ASA FirePOWER Module, Firepower Device Manager, and 7000 and 8000 Series Devices

On select device platforms tailored for smaller deployments, you can use a GUI to configure and manage the devices. These platforms include the ASA with FirePOWER Services module managed with ASDM or devices running FTD managed by Firepower Device Manager.

Also, you can use a web interface to perform limited configuration on 7000 and 8000 Series devices.

Alternatively, you can use the Firepower Management Center web interface to configure and manage these devices (see Management Capability: Firepower Management Center, on page 7).

ASA FirePOWER Module Managed with ASDM

Supported Platforms: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X, ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60

You can use ASDM to configure and manage an ASA FirePOWER module running Version 6.2.0.

See the Cisco ASA with FirePOWER Services Local Management Configuration Guide for more information.

Firepower Threat Defense Devices Managed by Firepower Device Manager

Supported Platforms: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X

You can use the Firepower Device Manager to configure and manage a FTD device running Version 6.2.0.

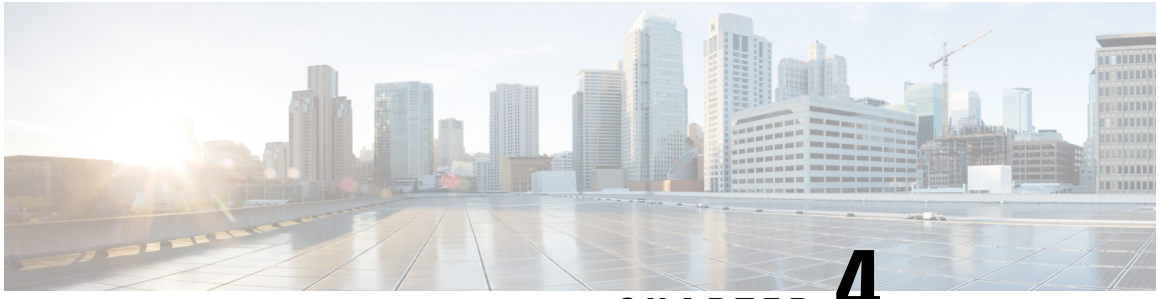
See the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for more information.

7000 and 8000 Series Devices

Supported Platforms: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390

You can use the web interface for a 7000 or 8000 Series device running Version 6.2.0 to manage limited configurations on that device. You must use the Firepower Management Center for some device configurations not accessible from the 7000 and 8000 Series web interface.

See the Firepower Management Center Configuration Guide for more information.



CHAPTER 4

New Features and Functionality

This table includes the new and updated features and functionality included in Version 6.2.0.

Table 3: New Features in Version 6.2.0: Migration Enablers

New Feature	Description	Supported Platforms
Migration Tool	Migrating from Cisco ASA-to-Firepower Threat Defense can be a daunting task for customer is with multiple access control lists (ACLs), Network Address Translation policies, and related configuration objects. The migration tool is specifically designed to assist this migration process. The tool allows you to convert ASA configurations (ACL, NAT and related objects) to Firepower Threat Defense configurations, which you can then import into the Firepower Management Center. The migration tool supports the conversion of up to 600,000 total access rule elements per ASA configuration file.	• 64-bit Firepower Management Center Virtual (VMware and KVM)
REST API	Firepower Version 6.2.0 allows REST clients to create and configure interfaces for Firepower Threat Defense devices through the Firepower Management Center REST API. This feature enables the Firepower Management Center to interact with various Cisco products and services as well as those from third-party vendors. Implementation of these APIs is ideal in the following scenarios: • Large enterprises that want to control policy changes in Firepower through other Cisco systems such as Application Centric Infrastructure (ACI) or through their own proprietary orchestration solutions • Managed security service providers that want to adopt software-defined networking, application-centric infrastructure, and network function virtualization solutions **Note** SDN controllers do not have a way to automatically insert Firepower Threat Defense devices in the traffic path.	• Firepower Management Center • 64-bit Firepower Management Center Virtual

New Feature	Description	Supported Platforms
Packet Tracer and Capture	The Packet Tracer and Capture offers the ability to show all the processing steps that a packet takes, the outcomes, and whether the traffic is blocked or allowed. This allows users to initiate and display output of tracing from the Firepower Management Center. The tracing information includes information from SNORT and preprocessors about verdicts and action taken while processing a packet.	• Firepower Threat Defense

Table 4: New Features for Version 6.2.0: Architecture

New Feature	Description	Supported Platforms
Integrated Routing and Bridging (IRB)	Customers often want to have multiple physical interfaces configured to be part of the same VLAN. The IRB feature meets this demand by allowing users to configure bridges in routed mode, and enables the devices to perform L2 switching between interfaces (including subinterfaces).	• Firepower Threat Defense on ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X • Firepower Threat Defense on Firepower 4100 Series • Firepower Threat Defense on Firepower 9300
Interchassis Clustering	Clustering lets you group multiple FXOS chassis Firepower Threat Defense devices together as a single logical device. A cluster provides all the convenience of a single device (management and integration into a network) while achieving the increased throughput and redundancy of multiple devices. Firepower Version 6.2.0 supports clustering across multiple chassis (interchassis clustering), allowing for higher scalability. You can use the Firepower Management Center to automatically discover all nodes of a cluster.	• Firepower Threat Defense on Firepower 4100 Series • Firepower Threat Defense on Firepower 9300 Appliances

New Feature	Description	Supported Platforms
Policy Change Improvement	Deploying policy changes to a Firepower Threat Defense device can result in restarting the SNORT process and the related loss of some packets. As part of a continuing effort to address this issue, Firepower Version 6.2.0 allows you to configure actions separately for fault conditions, such as SNORT Busy/Overload or SNORT Down. This feature allows you to emphasize either continuity or security by checking a checkbox option in the Firepower Management Center.	Firepower Threat Defense (inline mode only)

Table 5: New Features for Version 6.2.0: Platform/Integration

New Feature	Description	Supported Platforms
Firepower Threat Defense on Microsoft Azure	In Firepower Version 6.2.0, Cisco Firepower Threat Defense Virtual is available in the Microsoft Azure Marketplace. This new platform enables you to secure workloads consistently across the data center and public cloud. Managed centrally by an on-premises Firepower Management Center, Firepower Threat Defense Virtual provides advanced threat protection in the Azure environment without forcing customers to return traffic to the data center.	• Firepower Threat Defense virtual
Firepower Threat Grid API Key Integration	This feature streamlines the process of associating a Threat Grid account with your Firepower Management Center.	• Firepower Management Center • 64-bit Firepower Management Center Virtual

New Feature	Description	Supported Platforms
ISE and SGT tags without Identity	Before Firepower Version 6.2.0, you had to create a realm and identity policy to perform user control based on ISE Security Group Tag (SGT) data, even if you did not want to configure passive authentication using ISE. In Firepower Version 6.2.0, you no longer need to create a realm or identity policy to perform user control based on ISE Security Group Tag (SGT) data.	• Firepower Management Center • Firepower Management Center Virtual • 7000 and 8000 Series • NGIPSv • ASA with FirePOWER Services • Firepower Threat Defense • Firepower Threat Defense Virtual
TS Agent (VDI Identity Support)	To design policies that enforce rules based on the user's identity, you must be able to identify the user correctly. This is a problem in a shared environment, where multiple users are using the same IP address, identifying which user certain traffic applies to becomes difficult. Firepower now provides the ability to better identify individual users in shared environments, such as Citrix's Virtual Desktop Infrastructure (VDI), to accurately enforce user-based policy rules on the firewall. Rather than just associating a user with an IP address, Firepower now associates the user with both the IP address and a port range combination through the use of a new agent deployed on the Windows Terminal Server. The Cisco Terminal Services Agent (TS Agent) intercepts every log in to the terminal server and assigns a port range to every user that logs in. Using RESTful APIs it communicates this information (user, IP address and port range) to the Firepower Management Center, which in turn communicates it to the individual Firepower Threat Defense devices. Now, when **User 1** logs in, Firepower Threat Defense devices not only see the IP address, but also know the port range assigned to the user. Based on the IP address and the port range, Firepower Threat Defense devices properly map the traffic to **User 1**. When **User 2** logs in, a new port range is assigned which enables the Firepower Threat Defense devices to map the appropriate traffic to that user while applying any specific policy rules to that user and their traffic.	• Firepower Management Center • Firepower Management Center Virtual

Table 6: New Features for Version 6.2.0: Firepower Threat Defense and Threat

New Feature	Description	Supported Platforms
Site-to-Site VPN	The site-to-site VPN with public key infrastructure (PKI) support is an addition to the current capability of site-to-site VPN with preshared keys. The Firepower Device Manager (FDM) also allows you to configure site-to-site VPN with pre shared keys.	• Firepower Threat Defense managed by Firepower Management Center • Firepower Threat Defense Virtual
PKI Support for Firepower Management Center	PKI is required to create certificate-based trusted identities for devices establishing site-to-site VPN tunnels. This feature allows you to associate PKI certificate data with devices on the Firepower Management Center.	• Firepower Threat Defense • Firepower Threat Defense Virtual
User-based Indications of Compromise (IOCs)	This feature allows you to generate user-based IOCs from intrusion events or view the associations of users and IOCs. You can also enable and disable eventing of a given IOC per user (against false positives). With this feature, you can correlate IOCs and events to both hosts and users and give them more visibility and alerting options on a per-user basis.	• Firepower Management Center • 64-bit Firepower Management Center Virtual • 7000 and 8000 Series • NGIPSv • ASA with FirePOWER Services • Firepower Threat Defense managed by Firepower Management Center • Firepower Threat Defense Virtual

New Feature	Description	Supported Platforms
URL Lookups	This feature allows you to perform a bulk lookup of URLs (up to 250 URLs at a time) to obtain information such as reputation, category, and matching policy. You can also export the results as a file of comma-separated values. The feature reduces the manual work necessary to determine if your organization is protected against a malicious URL or if you should add a custom rule for a specific IOC. You can use this feature to reduce the number of custom rules, which in turn reduces the chance of performance degradation due to extensive custom rule lists.	• Firepower Management Center Virtual • 64-bit Firepower Management Center Virtual

New Feature	Description	Supported Platforms

FlexConfig	The FlexConfig feature allows you use the Firepower Management Center to deploy ASA CLI template-based functionality to Firepower Threat Defense devices. This feature allows you to enable some of the most valuable ASA functions that are not currently available on Firepower Threat Defense devices. This functionality is structured as templates and objects that work together in a policy. The default templates are officially supported by Cisco TAC.
	
	The targeted features unlocked by FlexConfig potentially include:
	• Non-Inspection Templates:
	  • Routing (EIGRP, PBR, and IS-IS)
	  • Netflow (NSEL) export
	  • MPF connection limits, timeouts (including DCD), and Normalizer settings
	  • Platform sysopt commands
	  • Proxy ARP Neighbor Discovery (**sysopt noproxyarp** *interface*)
	  • IPv6 Prefix Delegation
	  • IPV6
	  • WCCP
	  • VXLAN
	• Application Layer Inspection Templates:
	  • ALGs default configuration
	  • GTPv1/v2 support
	  • Diameter inspection
	  • LISP inspection
	  • SCTP support and inspection
	  • SIP
	  • SS7 inspection
		• Firepower Threat Defense
		• Firepower Threat Defense Virtual

• Changed Functionality, on page 18

Changed Functionality

The following are a few of the changes in Version 6.2.0:

- Version 6.2.0 introduces new functionality related to latency-based performance settings in access control policies. In Version 6.2.0 and later, by default, new access control policies obtain latency-based performance settings from the latest intrusion rule update. You can choose to overwrite these settings with custom settings. For more information, see "Latency-Based Performance Setting Configuration" in the Firepower Management Center Configuration Guide.

  When you update to Version 6.2.0, the system determines whether existing access control policies use default or custom latency-based performance settings and continues as appropriate under the following conditions:

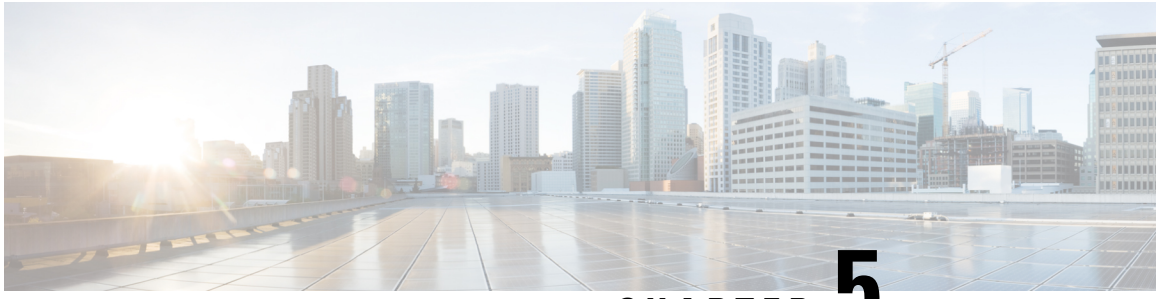
  - If existing policies use default settings, the system sets the **Apply Settings From** option to **Installed Rule Update**. When you deploy the access control policy, the system obtains the latency-based performance settings from the latest intrusion rule update and uses them in that policy.
  - If existing policies do not use default settings, the system sets the **Apply Settings From** option to **Custom** and retains the pre-upgrade settings.

- Version 6.2.0 does not support international characters in URLS for URL objects or inline values in access control policy rules. (CSCux24338)
- Private keys are no longer mandatory when importing certificates. (CSCvb13045)
- Generated troubleshoot now includes captive portal information. (CSCvb26174)
- If you create an access control policy or NAT policy referencing an object or object group that contains an invalid characters in the name, the system now generates an **Unsupported object names are used in the policy for devices** error message and does not save the policy. (CSCvb29308)
- The ASA-to-FTD migration process failed if the ASA configuration file included an access list entry (ACE) with an interface object configured as source network, destination network, or both. Now, the migration tool converts this ASA configuration as a disabled FTD rule. (CSCvb49745)
- Upgrading to Version 6.2.0 from Version 6.1.0.3 or a subsequent 6.1.0.x patch removes the Intelligent Application Bypass (IAB) **All applications including unidentified application** option from the user interface. You must install the Version 6.2.0.1 patch or a subsequent 6.2.0.x patch to restore this option.

  If this option is enabled when you upgrade, and your access control policy does not contain IAB 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 one of the following, depending on which appliance you are using: *deleted* (Firepower Management Center, ASA with FirePOWER Services and *Any Application* (ASA FirePOWER module managed by ASDM).

We recommend deleting *deleted* or *Any Application* from the Selected Applications and Filters window. Installing Version 6.2.0.1 or a subsequent 6.2.0.x version restores the missing option.



CHAPTER 5

Terminology and Documentation for Version 6.2.0

Product Terminology and Branding in Version 6.2.0

The terminology and branding used in Version 6.2.0 may differ from the terminology used in previous releases as summarized in the following table. See the Firepower System Compatibiltiy Guide for more information about terminology and branding changes.

Product Terminology and Branding

Name	Description
Firepower System Firepower	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 a Cisco Adaptive Security Appliance (ASA) operating system installed on an ASA platform.
ASA FirePOWER module managed with ASDM	Refers to ASA FirePOWER module 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 9300 appliance, Firepower 4100 series, or virtual platform.
Firepower Device Manager	Refers to Firepower Threat Defense local configuration interface accessible with specific Firepower Threat Defense platforms.

Documentation for Version 6.2.0

The following documents were updated for Version 6.2.0 to reflect the addition of new features and functionality and to address reported documentation issues:

- Cisco Firepower Management Center Configuration Guide and online help
- Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500, and 4000
- Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500
- Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide
- Cisco Firepower Management Center Virtual for the AWS Cloud Quick Start Guide
- Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide
- Cisco ASA with FirePOWER Services Local Management Configuration Guide and online help
- Cisco Firepower Threat Defense Configuration Guide and online help for Firepower Device Manager
- Firepower Threat Defense Command Reference Guide
- Cisco Firepower Threat Defense Virtual for the Microsoft Azure Cloud Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Management Center Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X Using Firepower Device Manager Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Management Center Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5506-X Series Using Firepower Device Manager Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Management Center Quick Start Guide
- Cisco Firepower Threat Defense for the ASA 5508-X and 5516-X Series Using Firepower Device Manager Quick Start Guide
- Cisco ASA to Firepower Threat Defense Migration Guide
- Firepower System Event Streamer Integration Guide
- Firepower REST API Quick Start Guide
- Terminal Services (TS) Agent Guide
- Cisco Firepower Compatibility Guide

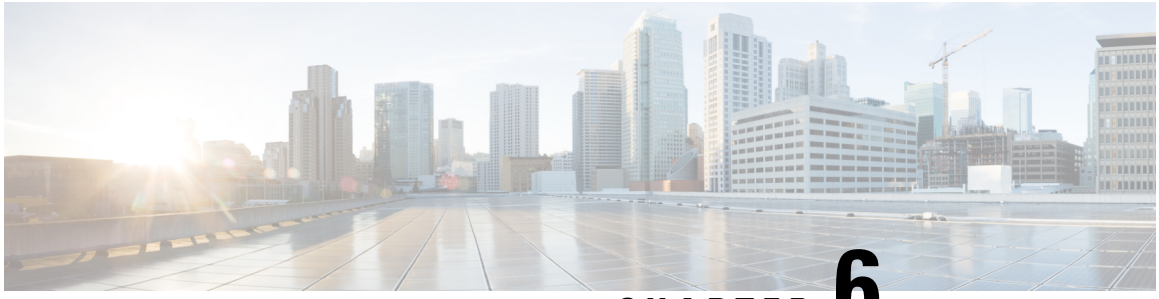
For additional information about updating and configuring your system, see the documents in the Cisco Firepower System Documentation Roadmap.

For parallel ASA versions, see the ASA documentation roadmap and release notes (including known issues).

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

Known Documentation Issues in Version 6.2.0

- The Cisco ASA with FirePOWER Services Local Management Configuration Guide refers to creating new, custom access control and system policies. ASA with FirePOWER Services does not support multiple custom policies. Instead, edit and deploy the system-provided policies.
- 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.
- The Cisco ASA with FirePOWER Services Local Management Configuration Guide states *After you establish remote management and register the Cisco ASA with FirePOWER Services to a Firepower Management Center, you must manage the ASA FirePOWER module from the Firepower Management Center instead of ASDM*. However the guide does not state that once remote management is established, you cannot access the ASA FirePOWER configuration with the ASDM manager.



CHAPTER 6

Product Compatibility in Version 6.2.0

Integrated Product Compatibility

The required versions for the following integrated products vary by Firepower version:

- Cisco Identity Services Engine (ISE)
- Cisco AMP Threat Grid
- Cisco Firepower User Agent

For more information about the required versions, see the Firepower Compatibility Guide.

Web Browser Compatibility

Firepower web UI for Version 6.2.0 has been tested on the browsers listed in the following table:

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.

Table 7: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 55	JavaScript, cookies

Browser	Required Enabled Options and Settings
Mozilla Firefox 50	JavaScript, cookies, TLS v1.1 or v1.2 **Note** 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 web browser search bar and click **Refresh Firefox**. Note that you may lose existing Firefox settings when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. The Firepower Management Center uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a trusted certificate authority. For more information on replacing server certificates, see the section on system configuration in the Firepower Management Center Configuration Guide for your version.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or 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 disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ...**.
Apple Safari 8 and 9	—
Microsoft Edge	—

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.

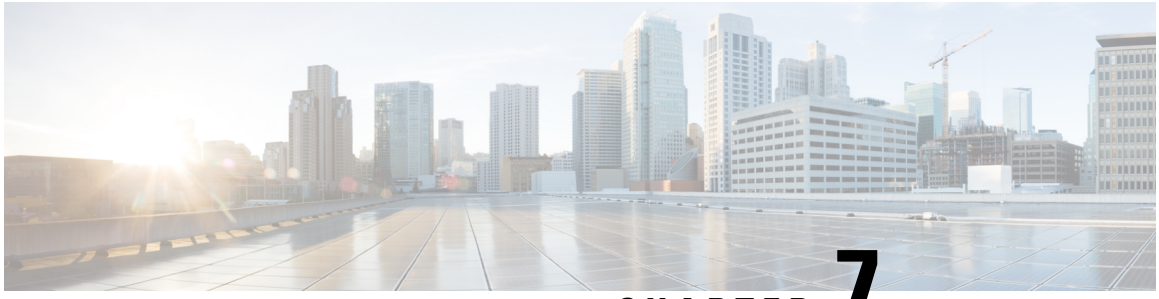
Screen Resolution Compatibility

When you access user interfaces to manage Firepower, we recommend using the screen resolutions in the table below. The user interfaces are compatible with lower resolutions, but a higher resolution optimizes the display.

Table 8: Recommended Screen Resolutions by Web Interface

Web Interface	Recommended Screen Resolution
Firepower Management Centers	At least 1280 pixels wide
7000 and 8000 Series devices	
ASDM (managing ASA FirePOWER)	1024 pixels wide by 768 pixels high

Web Interface	Recommended Screen Resolution
Firepower Device Manager (managing Firepower Threat Defense)	1024 pixels wide by 768 pixels high



CHAPTER 7

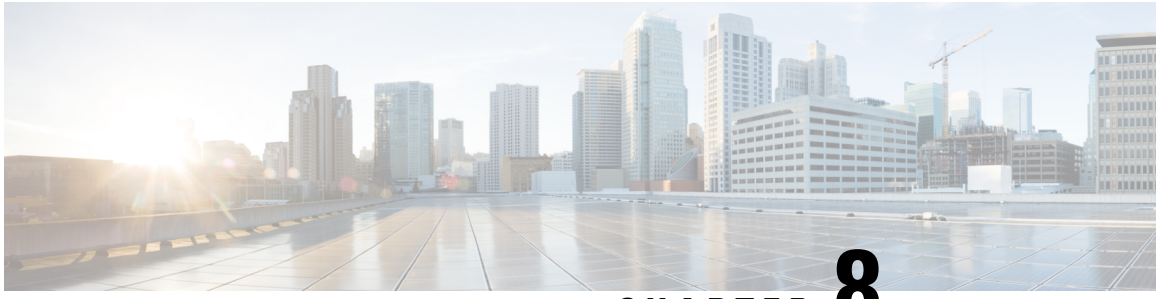
Update vs. Reimage vs. Deploy

In most cases, it is best to perform a traditional update from Version 6.1 to Version 6.2.0 as described in Update Paths to Version 6.2.0, on page 31.

However, the following cases require you to reimage and/or deploy your appliance:

- If you are installing the Firepower on the Firepower Management Centers MC1000, MC2500, or MC4500 you must reimage the appliances to Version 6.2.0. Because those appliances are newly supported in Version 6.2.0, you cannot perform a traditional update on those appliances.
- If you are installing Firepower Threat Defense Virtual in a Microsoft Azure Standard D3 environment, you must deploy the appliances to Version 6.2.0. Because this environment is newly supported in Version 6.2.0, you cannot perform a traditional update on those appliances.
- If you are moving from ASA with FirePOWER Services to Firepower Threat Defense, you must reimage your ASA device to deploy Firepower Threat Defense.
- If you have a Firepower Threat Defense device (physical or virtual) that was installed before version 6.1.0, and you want to switch between managing it with a Firepower Management Center and managing it with the Firepower Device Manager, you must reimage the Firepower Threat Defense.

  New installations of version 6.1.0 and later do not require a reimage.
- If you are recreating a Firepower Threat Defense Virtual device in a different environment than before, you must redeploy your virtual platform to Firepower Threat Defense. For example, if you were using VMware before and now want to deploy in AWS, you must redeploy rather than update.
- If you are unable or disinclined to follow the required update path as described in Update Paths to Version 6.2.0, on page 31, you must reimage and/or deploy your appliance.



CHAPTER 8

Important Update Notes

Before you begin the update process to Version 6.2.0, you should familiarize yourself with the behavior of the system during the update process, as well as with any compatibility issues or required pre- or post update configuration changes.

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. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

Update Paths to Version 6.2.0

To update to Version 6.2.0, you must be running the following Firepower versions:

- Firepower Management Center—Version 6.1.0
- All other devices—Version 6.1.0

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 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
Firepower Management Center Virtual: AWS	Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
Firepower Management Center Virtual: KVM	Version 6.1.0 > Version 6.2.0

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 PreInstallation Package > Version 6.1.0 > Version 6.2.0
Firepower Threat Defense Virtual: KVM Firepower 4150	Version 6.1.0 > Version 6.2.0
Firepower Threat Defense Virtual: Azure	Version 6.2.0

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
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Version 6.1.0 > Version 6.2.0

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: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X ASA FirePOWER: ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60 NGIPSv: VMware	Version 5.4.0.2 > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0
ASA FirePOWER: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	Version 5.4.1.1 > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 Pre-nstallation Package > Version 6.1.0 > Version 6.2.0

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
ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	Version 5.4.1.1 > Version 6.0.0 PreInstallation Package > Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0

ASA FirePOWER NGIPS Platform	Update Path
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60	Version 6.0.0 > Version 6.0.1 Preinstall > Version 6.0.1 > Version 6.1.0 PreInstallation Package > Version 6.1.0 > Version 6.2.0

Update Interface Options

If you are locally managing the ASA FirePOWER module with ASDM, use the ASDM to perform the update. To configure the ASA FirePOWER module through ASDM, see the Cisco ASA with FirePOWER Services Local Management Configuration Guide.

If you are locally managing a Firepower Threat Defense device with the Firepower Device Manager, use the Firepower Device Manager to update your Firepower Threat Defense device. To configure the Firepower Device Manager, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Otherwise, use the Firepower Management Center to update first the Firepower Management Center and then the devices it manages. To configure the Firepower Management Center or its managed devices, see the Firepower Management Center Configuration Guide.

For more information about management, see Management Capability in Version 6.2.0, on page 7.

Update Sequence Guidelines

Update your Firepower Management Center to at least Version 6.2.0 before updating the devices it manages. Then, use the Firepower Management Center to redeploy policies to all managed devices before updating those devices to Version 6.2.0 .

Note the following update sequence complications when you have high availability or device stacking configured:

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.

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 on the High Availability tab of the Integration page (**System** > **Integration**) as described in the Pausing Communication Between Paired Firepower Management Centers topic in the *Firepower Management Center Configuration Guide*, Version 6.2.0.

Step 2 Update the standby Firepower Management Center in the high availability pair.

After the update is completed, 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.

The update is complete.

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

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 Firepower Threat Defense Devices in High Availability

Update the FXOS chassis of Firepower Threat Defense devices in a high availability pair to the most recent compatible FXOS version before installing the most recent Firepower version. For more information on FXOS versions, see the Firepower Compatibility Guide.

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

Note For Firepower Threat Defense high availability in Version 6.2.0, 169.254.0.0/16 and fd00:0:0:*::/64 are internally used subnets and cannot be used for the failover or state links. If you currently use IP addresses in this range, then you must change them to different IP addresses before you upgrade

Step 1 Update the FXOS version on the standby Firepower Threat Defense device within the high availability pair.

Step 2 Switch the active peer so the standby Firepower Threat Defense device is now the active device.

Step 3 Update the FXOS version on the standby Firepower Threat Defense device within the high availability pair.

What to do next

Update the Firepower Threat Defense high availabiltiy pair to the most recent Firepower version.

When you install a Firepower update on Firepower Threat Defense devices in a high availability pair, the devices are updated 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. Once the standby Firepower Threat Defense update is complete, the active Firepower Threat Defense automatically fails over to standby mode and then is updated.

Update Sequence for Clustered FTD Devices

When you update clustered Firepower 9300 or Firepower 4100 series devices 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 About Clustering on the Firepower 4100/9300 Chassis chapter of the *Firepower Management Center Configuration Guide* and the About Clustering on the Firepower 4100/9300 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 complete. However, if the logging downtime was significant, the system may not log some of the oldest events because it may prune them before they can be logged.

Update Sequence for 7000 and 8000 Series Devices in High Availability

Note You cannot locally update 7000 and 8000 Series devices in a high availability pair. You *must* update from the managing Firepower Management Center.

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 standby device then takes over the active role and the system updates the formerly 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 is updated in maintenance mode, the secondary device temporarily becomes primary and does not drop traffic. When the primary device update is complete, 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 complete. Note the following scenarios:

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

Preupdate Readiness Checks

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

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

Run a Readiness Check through the Shell

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

Before you begin

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

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

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

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

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

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

Step 3 Run this command as the root user:

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

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

Step 4 (Optional) Monitor the readiness check.

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

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

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

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

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

Run a Readiness Check through the Firepower Management Center Web Interface

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

Before you begin

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

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

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

Step 3 Click **Launch Readiness Check**.

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

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

Preupdate Modifications to Correlation Policies

If you are updating a Firepower Management Center where you configured correlation policies, follow the rule modifications listed below. If you reimage the Firepower Management Center rather than update it, or if you have not configured correlation policies, the rule modifications listed below are not required.

Version 6.2.0 no longer supports nested correlation rules. In earlier releases, you can use a correlation rule as a trigger for another correlation rule if the rules share a base event type. For example, if you create Rule A and Rule B, which both trigger on an intrusion event, you can use the criteria "Rule A is true" as a constraint for Rule B. In this configuration, Rule A is considered "nested" within Rule B.

The update process flattens certain nested correlation rules by copying settings from the nested correlation rule (Rule A) to the nesting correlation rule (Rule B) and deleting the nested rule. The update copies the host profile/user qualifications and the snooze/inactive periods from the nested rule to the nesting rule.

For all of these settings except inactive periods, the system can copy the settings from the nested rule to the nesting rule only if the settings are absent from the nesting rule. When the system copies inactive periods from the nested rule to the nesting rule, it retains inactive periods from the nesting rule, so that the resulting rule uses settings from both rules originally involved in the nesting configuration.

The update cannot flatten nested rules if the nested and nesting rule have specific types of conflict. In these cases, the update fails.

To avoid this failure, modify your correlation rules as follows before you run the update:

- Remove the host profile qualification, user qualification, and snooze period settings from either the nested rule or the nesting rule, so that only one rule in the nested configuration specifies these settings.
- Remove connection trackers from any nested rules.
- Remove host profile qualifications, user qualifications, snooze periods, and inactive periods from nested rules that do not have to be true; that is, remove those elements from nested rules that are linked to other rule conditions using the OR operator, within the nesting rule.

For information on correlation rules, see the Firepower Management Center Configuration Guide.

Preupdate 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. If you back up to an external location, verify the external backup is successful before updating the system.

The Firepower Management Center purges locally stored backups from previous updates. To retain archived backups, store the backups externally. 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.

Use the Firepower Device Manager to back up event and configuration data for the device it manages. For more information on the backup and restore feature, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

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. For more information, see CSCvh64138 in the Cisco Bug Search Tool.

Table 9: Update Traffic Behavior

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

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

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

Traffic Behavior When Updating FXOS on Clustered Firepower Threat Defense Devices

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

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

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

The following table summarizes this behavior.

Table 10: 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 11: 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**: disabled	Dropped
	Inline, **Snort Fail Open: Down**: enabled	Passed without inspection
	Routed, transparent (including EtherChannel, redundant, subinterface) CLI command: **configure snort preserve-connection enable** (default); this functionality requires Version 6.2.0.2 or a subsequent 6.2.0.x patch	Existing flows: passed without inspection New flows: dropped
	Routed, transparent (including EtherChannel, redundant, subinterface) CLI command, Version 6.2.0.2 or a subsequent 6.2.0.x patch: **configure snort preserve-connection disable**	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

Automatic Modifications to Failsafe Configuration during Update

In Version 6.2.0, the Snort Fail Open configuration replaces the Failsafe option on FTD physical and virtual devices managed by a Firepower Management Center. This new feature provides the same functionality as the Failsafe option, but it also lets you choose whether to drop traffic when the Snort process is down.

When you update a Firepower Management Center to Version 6.2.0, Failsafe is still supported for the following managed devices:

- FTD devices running Version 6.1.x
- 7000 Series, 8000 Series, and NGIPSv devices running Version 6.2.0

When you update a FTD device to Version 6.2.0, the update determines whether Failsafe is enabled and, if so, migrates the Failsafe option to a matching Snort Fail Open configuration. We **strongly** recommend that you consider whether to enable or disable Failsafe before updating your FTD device.

Table 12: Migrating Failsafe to Snort Fail Open

When Version 6.1 Failsafe is…	Snort Fail Open is set to...	
	Busy	**Down**
disabled (default behavior) New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down	disabled New and existing connections drop when the Snort process is busy	enabled New and existing connections pass without inspection when the Snort process is down
enabled New and existing connections pass without inspection when the Snort process is busy or down	enabled New and existing connections pass without inspection when the Snort process is busy	enabled New and existing connections pass without inspection when the Snort process is down

For more information, see the Firepower Management Center Configuration Guide.

Additional Memory Requirements When Version 6.0 is in Your Update Path

If your update path to Verison 6.2.0 begins with Verison 5.4.x or earlier, you may need to update your Firepower Management Center memory before you update to Version 6.0. You must update the Firepower Management Center memory before you update to Verison 6.2.0. See Update Paths to Version 6.2.0, on page 31 for more information.

Firepower Version 6.0 requires more memory than the previous versions for some Firepower Management Center models (previously referred to as the FireSIGHT Management Center or the Defense Center). To be

specific, MC750 requires two 4GB dual in-line memory modules (DIMM). Similarly, MC1500 with 6GB of memory also requires additional memory.

Because the increase in memory was driven by Cisco product requirements, we make memory upgrade kits available for customers with these models. You can order these kits at no cost if you are entitled to run Version 6.0 or later on a qualifying MC750 or MC1500 Firepower Management Center model.

For more information on ordering memory kits, see http://www.cisco.com/c/en/us/support/docs/field-notices/640/fn64077.html. For instructions on replacing the memory after you receive the kit, see "Memory Upgrade Instructions for Firepower Management Centers" in the *Cisco Firepower Management Center 750, 1500, 2000, 3500, 4000, 4500 Hardware Installation Guide*.

Time and Disk Space Requirements for Updating to Version 6.2.0

The following table provides disk space and time guidelines for the Version 6.2.0 update. Note that when you use the Firepower Management Center to update a managed device, the Firepower Management Center requires additional disk space on its **/Volume** partition.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

Note The following guidelines do not include the time required to complete the readiness check. For more information about the readiness check, see Preupdate Readiness Checks, on page 37.

If you encounter issues with the progress of your update, contact Cisco TAC.

Table 13: Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Firepower Management Center	17 MB	10207 MB	–	57 minutes
Firepower Management Center Virtual	17 MB	10207 MB	–	hardware dependent
7000 and 8000 Series managed device	16.5 MB	6129 MB	1.2 GB	27 minutes
NGIPSv device	18 MB	7028 MB	1.3 GB	hardware dependent

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
ASA FirePOWER module	15.6 MB	6619 MB	1.1 GB	165 minutes
Cisco ASA with Firepower Threat Defense	96 KB	5213 MB	938 MB	83 minutes
Firepower 9300 appliance or Firepower 4100 series security appliance running Firepower Threat Defense	5234 MB	5234 MB	734 MB	21 minutes
Firepower Threat Defense Virtual device	1 MB	5663 MB	936 MB	hardware dependent

Post Update Tasks

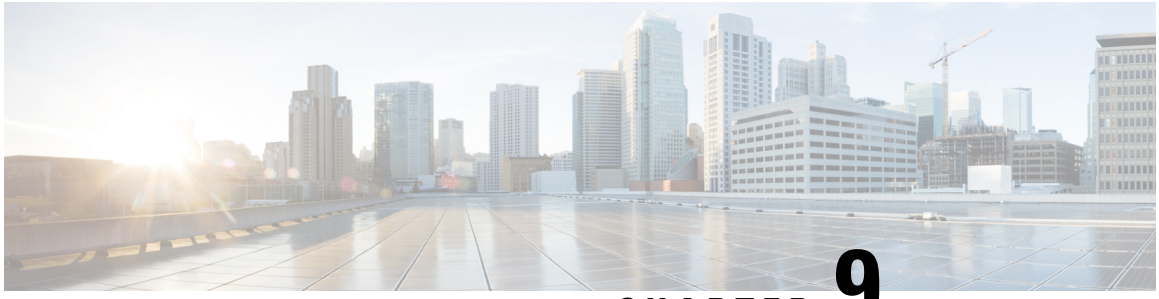
After you perform the update on the Firepower Management Center or managed devices, you must deploy configuration changes to the devices.

Note You must deploy configuration changes first after updating the Firepower Management Center and then again after updating its managed devices.

When you deploy configuration changes, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations requires the Snort process to restart, which temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends how the managed device handles traffic. For more information, see the Firepower Management Center Configuration Guide.

There are several additional post update steps you should take to ensure that your deployment is performing properly, which include the following include:

- Verify that the update succeeded.
- Make sure that all appliances in your deployment are communicating successfully.
- Update your intrusion rules and vulnerability database (VDB) and deploy configuration changes. (See the Firepower Management Center Configuration Guide for details.)
- Make configuration changes based on new features and functionality.
- Redeploy policies and configuration.



CHAPTER 9

Update to Version 6.2.0

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.

Note Devices running Version 6.2.0 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 the Hotfix BX for more information.

Before you begin the update, you must thoroughly read and understand these release notes, especially Important Update Notes, on page 31 and Preupdate Readiness Checks, on page 37.

Update Procedures Listed by Platform

If you want to update:	See:
Firepower Management Centers: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, MC4500	Update Firepower Management Centers and Firepower Management Centers Virtual, on page 50
Firepower Management Center Virtual	

If you want to update:	See:
7000 and 8000 Series devices: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 56
NGIPSv (virtual managed devices)	
Cisco ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60	If managing with the Firepower Management Center: Update 7000 and 8000 Series Devices, NGIPSv, and ASA FirePOWER Modules Using the Firepower Management Center, on page 56 If managing with ASDM: Update ASA FirePOWER Modules Managed with ASDM, on page 58
Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	If managing with the Firepower Management Center: Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 53 If managing with Firepower Device Manager: Update Firepower Threat Defense Devices with the Firepower Device Manager, on page 56
Firepower 9300 with Firepower Threat Defense (with SM-24, SM-36, or SM-44 security modules)	Update Firepower Threat Defense Devices Using the Firepower Management Center, on page 53
Firepower 4100 series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150	
Firepower Threat Defense Virtual	

Update Firepower Management Centers and Firepower Management Centers Virtual

Use the procedure in this section to update your Firepower Management Centers and Firepower Management Center Virtuals. For the Version 6.2.0 update, Firepower Management Centers reboot.

If your appliance is in a high availability configuration, see Update Sequence Guidelines, on page 34.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

Caution Updating Firepower Management Centers in a high availability pair connected by a low bandwidth connection from Version 6.1.0 or later to Version 6.2.0 over a low bandwidth connection may cause system issues and the update may fail. To avoid the update to Version 6.2.0 failing, install Hotfix AJ before updating. Note that this issue may also occur when establishing or reconnecting Version 6.2.0 Firepower Management Centers in a high availability pair.

Step 1 If you want to update Firepower Management Centers in a high availability pair, see Update Sequence for Firepower Management Centers in High Availability, on page 34.

Step 2 Update to the minimum version as described in Update Paths to Version 6.2.0, on page 31.

Step 3 Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0, on page 25
- Update vs. Reimage vs. Deploy, on page 29
- Important Update Notes, on page 31

Step 4 Download the update from the Support site:

- For Firepower Management Center (MC750, MC1500, MC2000, MC3500, MC4000) and Firepower Management Center Virtual:

  Sourcefire_3D_Defense_Center_S3_Upgrade-6.2.0-367.sh

- For Firepower Management Center (MC1000, MC2500, MC4500) :

  Sourcefire_Defense_Center_M4_Upgrade-6.2.0-362.sh

Note Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

Step 5 Upload the update to the Firepower Management Center by choosing **System** > **Updates**, then clicking **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.
The update is uploaded to the Firepower Management Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated.

Step 6 Redeploy configuration changes to any managed devices. Otherwise, the eventual update of the managed devices 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*, Version 6.2.0.

Step 7 (Optional) Run a readiness check on the Firepower Management Center as described in Run a Readiness Check through the Shell, on page 37 and Run a Readiness Check through the Firepower Management Center Web Interface, on page 38.

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

Step 8 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 9 Click the System Status icon and view the **Tasks** tab in the Message Center to make sure that there are no tasks in progress.

You *must* wait until any long-running tasks are complete before you begin the update. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the Tasks tab after the update finishes.

Step 10 On the **System** > **Updates** window, click the install icon next to the update you are installing.

Step 11 Choose the Firepower Management Center and click **Install**. Confirm that you want to install the update and reboot the Firepower Management Center.

The update process begins. You can begin monitoring the update's progress in the **Tasks** tab of the Message Center. However, after the Firepower Management Center finishes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status window displays a progress bar and provides details about the script currently running. Click **show log for current script** to see the update log.

If the update fails for any reason, the page displays an error message indicating the time and date of the failure, which script was running when the update failed, and instructions on how to contact Cisco TAC. Do *not* restart the update.

Caution If you encounter any other issue with the update (for example, if a manual refresh of the Update Status page shows no progress for several minutes), do not restart the update. Instead, contact Cisco TAC.

When the update finishes, the Firepower Management Center displays a success message and reboots.

Step 12 After the update finishes, clear your browser cache and relaunch the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 13 Log into the Firepower Management Center.

Step 14 If prompted, review and accept the **End User License Agreement (EULA)**. Note that you are logged out of the appliance if you do not accept the **EULA**.

Step 15 Choose **Help** > **About** and confirm that the software version is listed correctly: Version 6.2.0. Also note the versions of the intrusion rule update and VDB on the Firepower Management Center; you will need this information later.

Step 16 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 17 If the intrusion rule update available on the Support site is newer than the rule set on your Firepower Management Center, import the newer rule set. Do not autoapply the imported rules when working with Version 6.2.0.

For information on intrusion rule updates, see the Firepower Management Center Configuration Guide.

Step 18 If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not autodeploy VDB updates when working with Version 6.2.0.

Installing a VDB update restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends how the managed device handles traffic. For more information, see the Firepower Management Center Configuration Guide.

Step 19 Redeploy policies to all managed devices.

Click **Deploy** and choose all available devices, then click **Deploy**.

Note You must redeploy configuration changes before updating any managed devices or you may have to reimage your appliances.

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 20 If a later patch is available on the Support site, update to the latest patch as described in the Firepower Release Notes roadmap for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Step 21 If you updated Firepower Management Centers in a high availability pair, see Update Sequence for Firepower Management Centers in High Availability, on page 34

Update Firepower Threat Defense Devices Using the Firepower Management Center

Use this procedure to update Firepower Threat Defense devices running at least Version 6.1.0. A Firepower Management Center must be running at least Version 6.2.0 to update Firepower Threat Defense devices to Version 6.2.0.

You can autodownload files for Firepower Threat Defense devices managed by the Firepower Management Center. You can update multiple devices at once but only if they use the same update file.

If your appliance is in a high availability or clustered configuration, see the Update Sequence Guidelines, on page 34.

Note In Version 6.2.0, the Snort Fail Open configuration replaces the Failsafe option on Firepower Threat Defense physical and virtual devices managed by a Firepower Management Center. This new feature provides the same functionality as the Failsafe option, but it also lets you choose whether to drop traffic when the Snort process is down. When you update a Firepower Threat Defense device to Version 6.2.0, the update determines whether Failsafe is enabled and, if so, migrates the Failsafe option to a matching Snort Fail Open configuration. See Automatic Modifications to Failsafe Configuration during Update, on page 45 for more information.

For devices running or hosted on a non-Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest *supported* version.

Note Switching the management of a Firepower Threat Defense device resets device configuration to system default settings. If you need to switch the management of a Firepower Threat Defense device from the Firepower Management Center to a Firepower Device Manager, execute the **configure manager local** CLI command and register the Firepower Threat Defense device to a Firepower Management Center. Note that switching the management of a Firepower Threat Defense device resets device configuration to system default settings. For more information, see the Firepower Threat Defense Command Reference Guide.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.0, on page 31.

Step 2 Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0, on page 25
- Update vs. Reimage vs. Deploy, on page 29
- Important Update Notes, on page 31

Step 3 Update the software on the device's managing Firepower Management Center; see Update Firepower Management Centers and Firepower Management Centers Virtual, on page 50.

Step 4 Use the managing Firepower Management Center to deploy configuration changes to the managed devices. Otherwise, the eventual update 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 If you are updating a Firepower 9300 appliance or Firepower 4100 series, update to the latest supported FXOS version as described in the Cisco FXOS release notes. See the FXOS release notes landing page, the FXOS Compatibility Guide, and the Firepower Compatibility Guide for more information. If a Firepower 9300 appliance or a Firepower 4100 series device is in a high availability pair, you must update the standby device's FXOS chassis manager before updating the Firepower software. See Update Sequence for Firepower Management Centers in High Availability, on page 34 for more information.

Updating to FXOS Version 2.0.1 or later 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:

- For Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, or any supported virtual platform (VMware, AWS, KVM, Microsoft Azure):

  Cisco_FTD_Upgrade-6.2.0-362.sh

- For Firepower Threat Defense running on the Firepower 4110, Firepower 4120, Firepower 4140, Firepower 4150, Firepower 9300 appliance, and Firepower Threat Defense Virtual:

  Cisco_FTD_SSP_Upgrade-6.2.0-362.sh

  Note Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

Step 7 Upload the update to the Firepower Management Center by choosing **System** > **Updates**, then clicking **Upload Update** on the **Product Updates** tab. Browse to the update and click **Upload**.
The update is uploaded to the Firepower Management Center. The web UI shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.

Step 8 (Optionally) Run a readiness check on the Firepower Threat Defense device as described in Run a Readiness Check through the Shell, on page 37 and Run a Readiness Check through the Firepower Management Center Web Interface, on page 38.

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

Step 9 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 10 On the **System** > **Updates** window, click the install icon next to the update you are installing.

Step 11 Choose the devices on which you want to install the update.

Step 12 Click **Install**. Confirm that you want to install the update and reboot the devices.
The update process begins. You can monitor the update's progress on the **Tasks** tab of the Message Center.

Note that managed devices may reboot twice during the update; this is expected behavior.

Caution If you encounter issues with the update (for example, if messages in 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 After the update process finishes, choose **Devices** > **Device Management** and confirm that the devices you updated have the correct software version.

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

Step 15 Redeploy policies to all managed devices.

Click **Deploy** and choose all available devices, then click **Deploy**.

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*, Version 6.2.0.

Step 16 If a later patch is available on the Support site, update to the latest patch as described in the Firepower Release Notes for that version. You must update to the latest patch to take advantage of product enhancements and security fixes.

Update Firepower Threat Defense Devices with the Firepower Device Manager

Step 1 Download the update from the Support site:

- For Firepower Threat Defense running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X:

  Cisco_FTD_Upgrade-6.2.0-362.sh

Step 2 Follow instructions for updating as described in the System Management topic in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

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 virtual managed devices, and ASA FirePOWER modules running at least Version 6.1.0. A Firepower Management Center must be running at least Version 6.2.0 to update these devices to Version 6.2.0.

You can update multiple devices at once but only if they use the same update file.

If your appliance is in a high availability or stacked configuration, see Update Sequence Guidelines, on page 34.

Note If you are locally managing the ASA FirePOWER module through ASDM, do not update the ASA FirePOWER module using the Firepower Management Center. For more information, see Update ASA FirePOWER Modules Managed with ASDM, on page 58.

Caution Do *not* reboot or shut down your appliance during the update until you see the login prompt. The system may appear inactive during the prechecks; this is expected behavior and does not require you to reboot or shut down your appliance.

For devices running or hosted on a non-Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest *supported* version.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.0, on page 31.

Step 2 Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0, on page 25
- Update vs. Reimage vs. Deploy, on page 29
- Important Update Notes, on page 31

Step 3 Update the software on the device's managing Firepower Management Center; see Update Firepower Management Centers and Firepower Management Centers Virtual, on page 50.

Step 4 Use the managing Firepower Management Center to deploy configuration changes to the managed devices. Otherwise, the eventual update 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*, Version 6.2.0..

Step 5 If you are updating an ASA device, update to the latest supported ASA version as described in the notes for that ASA release. For more information see the ASA/ASDM Release Notes landing page, Cisco ASA Compatibility matrix, and the Firepower Compatibility Guide.

Step 6 Download the update from the Support site:

- For 7000 and 8000 Series:

  Sourcefire_3D_Device_S3_Upgrade-6.2.0-362.sh

- For NGIPSv:

  Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.2.0-362.sh

- For ASA with FirePOWER Services running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, and ASA 5585-X-SSP-60:

  Cisco_Network_Sensor_Upgrade-6.2.0-362.sh

Note Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

Step 7 (Optionally) Run a readiness check on the device as described in Run a Readiness Check through the Shell, on page 37 and Run a Readiness Check through the Firepower Management Center Web Interface, on page 38.

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

Step 8 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 9 On the **System** > **Updates** window, click the install icon next to the update you are installing.

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

If you are updating stacked 7000 and 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 Click **Install**. Confirm that you want to install the update and reboot the devices.
The update process begins. You can monitor the update's progress on the **Tasks** tab of the Message Center.

Note that managed devices may reboot twice during the update; this is expected behavior.

Caution If you encounter issues with the update (for example, if messages in 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 After the update process finishes, choose **Devices** > **Device Management** and confirm that the devices you updated have the correct software version.

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

Step 14 Redeploy policies to all managed devices.

Click **Deploy** and choose all available devices, then click **Deploy**.

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*, Version 6.2.0.

Update ASA FirePOWER Modules Managed with ASDM

Use this procedure to update ASA FirePOWER modules using ASDM running at least Version 6.1.0. Locally managed ASA FirePOWER modules managed with ASDM do not require Firepower Management Centers to update.

Caution Firepower Threat Defense devices managed by the Firepower Device Manager may experience an exhaustion of database handles, which prevents the device from successfully updating to Version 6.2.0. If you locally manage a Firepower Threat Defense devices managed by the Firepower Device Manager, contact Cisco TAC before updating to Version 6.2.0 to enable the update process and restart any appropraite processes.

For devices running or hosted on a non Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest *supported* version.

Step 1 Update to the minimum version as described in Update Paths to Version 6.2.0, on page 31.

Step 2 Read these release notes and complete any preupdate tasks. For more information, see the following sections:

- Product Compatibility in Version 6.2.0, on page 25
- Update vs. Reimage vs. Deploy, on page 29
- Important Update Notes, on page 31

Step 3 If you are updating an ASA device, update to the latest supported ASA version as described in the notes for that ASA release. For more information see the ASA/ASDM Release Notes landing page, Cisco ASA Compatibility matrix, and the Firepower Compatibility Guide.

Step 4 Download the update from the Support site:

Cisco_Network_Sensor_Upgrade-6.2.0-362.sh

Note Download the update package directly from the Support site. If you transfer an update file by email, it may become corrupted.

Step 5 Deploy configuration changes. Otherwise, the eventual update may fail.

Step 6 Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**.

Step 7 Click **Upload Update**.

Step 8 Click **Choose File** to navigate to and choose the update.

Step 9 Click **Upload**.

Step 10 Choose **Monitoring** > **ASA FirePOWER Monitoring** > **Task Status** to view the task queue and make sure that there are no jobs in process.

Tasks that are running when the update begins are stopped and cannot be resumed; you must manually delete them from the task queue after the update finishes. The task queue automatically refreshes every 10 seconds. You must wait until any long-running tasks are complete before you begin the update.

Step 11 Choose **Configuration** > **ASA FirePOWER Configuration** > **Updates**.

Step 12 Click the install icon next to the update you uploaded.

The update process begins. You can begin monitoring the update's progress in the task queue.

Step 13 After the update finishes, reconnect ASDM to the ASA device as described in the ASA Firepower Module Quick Start Guide.

Step 14 Access the ASA FirePOWER module interface and refresh the window. Otherwise, the interface may exhibit unexpected behavior. If you are the first user to access the interface after a major update, the End User License Agreement (EULA) may appear. You must review and accept the EULA to continue.

Step 15 If the intrusion rule update available on the Support site is newer than the rule set on your ASA FirePOWER module, import the newer rule set. Do not autoapply the imported rules when working with Version 6.2.0.

Step 16 If the VDB available on the Support site is newer than the VDB installed during the update, install the latest VDB. Do not autodeploy VDB updates when working with Version 6.2.0.

Installing a VDB update causes 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 17 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.

CHAPTER 10

Reimage or Deploy to Version 6.2.0

Note that you cannot uninstall Version 6.2.0. You *must* reimage your appliance.

Reimaging Firepower on an appliance or deploying Firepower in a virtual environment restores the appliance to the factory defaults.

If you are unsure whether you should perform a traditional Version 6.2.0 installation or reimage or deploy to Version 6.2.0, see Update vs. Reimage vs. Deploy, on page 29 .

Note If you reimage your device to Version 6.2.0, the Firepower password defaults to **Admin123** after the reboot sequence.

Caution Before you reimage a Firepower Threat Defense device or a Firepower Management Center that manages a Firepower Threat Defense device, you must unregister the managing appliance from the Cisco Smart Software Manager. If you do not unregister the managing appliance, orphan entitlements accrue against your total entitlements in the Smart Software Manager. For more information, see Unregister a Firepower Management Center, on page 63 and Unregister an FTD Device Using FDM, on page 64.

For more information, see:

- Reimage or Deploy Existing Platforms, on page 61
- Reimage or Deploy Newly Supported Platforms, on page 63
- Unregister a Firepower Management Center, on page 63
- Unregister an FTD Device Using FDM, on page 64

Reimage or Deploy Existing Platforms

For information about the reimaging and deploying process on existing platforms, see the quick start or getting started guide for the appropriate platform, as described in the following table.

Table 14: Reimaging Documentation by Platform

Platform	Reimaging Documentation
Firepower Management Centers: MC750, MC1000, MC1500, MC2000, MC2500, MC3500, MC4000, and MC4500	Cisco Firepower Management Center Getting Started Guide for Models 750, 1500, 2000, 3500 and 4000
Firepower Management Center Virtual	• Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Giude • Cisco Firepower Management Center Virtual for the AWS Cloud Quick Start Giude • Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide
7000 and 8000 Series devices: 7010, 7020, 7030, 7050, 7110, 7115, 7120, 7125, 8120, 8130, 8140, 8250, 8260, 8270, 8290, 8350, 8360, 8370, 8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, AMP8390	• Firepower 7000 Series Getting Started Guide • Firepower 8000 Series Getting Started Guide
NGIPSv (virtual managed devices)	Firepower NGIPSv Quick Start Guide for VMware
Cisco ASA with FirePOWER Services: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	Reimage the Cisco ASA or Firepower Threat Defense Device
Cisco ASA with FirePOWER Services: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X-SSP-10, ASA 5585-X-SSP-20, ASA 5585-X-SSP-40, ASA 5585-X-SSP-60	Reimage the Cisco ASA or Firepower Threat Defense Device
Cisco ASA with Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5516-X	Reimage the Cisco ASA or Firepower Threat Defense Device
Cisco ASA with Firepower Threat Defense: ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X	Reimage the Cisco ASA or Firepower Threat Defense Device
Firepower 9300 Appliance with Firepower Threat Defense (with SM-24, SM-36, or SM-44 modules)	Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide
Firepower 4100 series with Firepower Threat Defense: Firepower 4110, Firepower 4120, Firepower 4140, and Firepower 4150	Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide

Platform	Reimaging Documentation
Firepower Threat Defense Virtual	• Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide • Cisco Firepower Threat Defense Virtual Quick Start Guide for the AWS Cloud • Cisco Firepower Threat Defense Virtual for VMware Deployment Quick Start Guide

To locate these quick start and getting started guides, see:

- *Navigating the Cisco Firepower System Documentation* (http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html)
- *Navigating the Cisco ASA Series Documentation* (http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html)
- *Navigating the Cisco FXOS Documentation* (http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html)

Reimage or Deploy Newly Supported Platforms

For more information about the reimaging and deploying process for platforms that are newly supported in Version 6.2.0, see the following:

- If you want to reimage Firepower Management Centers MC1000, MC2500, and MC4500, see the Cisco Firepower Management Center Getting Started Guide for Models 1000, 2500, and 4500.
- If you want to deploy Firepower Threat Defense Virtual on Microsoft Azure, see the *Cisco Firepower Threat Defense Virtual for Microsoft Azure Quick Start Guide*.

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 11

Resolved Issues

For devices running or hosted on a non-Firepower appliance (for example, ASA OS or FXOS), resolving an issue may require that you update the operating system *in addition to* Firepower. We recommend you update to the latest **supported** version.

The following defects are resolved in Version 6.2.0:

Caveat ID Number	Description
CSCuw70987, CSCux50957, CSCux86317	Resolved multiple vulnerabilities within the third party Open SSH, as described in CVE-2015-5600, CVE-2015-6565, CVE-2016-0777, and CVE-2016-0778.
CSCuw88390, CSCuw88396, CSCuw89094	Addressed a cross-site scripting (XSS) vulnerability, as described in CVE-2015-6363 and CVE-2016-1294.
CSCux41304, CSCuz52366, CSCvb24543, CSCvb48536	Addressed multiple vulnerabilities that generated denial of service in OpenSSL, as described in CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2016-2105, CVE-2016-2106 CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6305, CVE-2016-6306 CVE-2016-6307 CVE-2016-6308 CVE-2016-6309 CVE-2016-7052 CVE-2015-3194, CVE-2015-3195 and CVE-2015-3196.
CSCux42288	Addressed a vulnerability issue in the third party Java, as described in CVE-2015-6420.
CSCux90163	Resolved a vulnerability where a user without Admin without privileges could delete other users' scheduled tasks.
CSCuy32284	Addressed a vulnerability in the third party GNU C Library, as described in CVE-2015-7547.
CSCuz52939, CSCvb24561, CSCvb24562	Addressed multiple vulnerabilities in the third party product Libxml2, as described in CVE-2016-2073, CVE-2016-444, and CVE-2016-4448.
CSCuz92632	Addressed multiple vulnerabilities in the third party product NTP, as described in CVE-2016-4953, CVE-2016-4954, CVE-2016-4955, CVE-2016-4956, and CVE-2016-4957.

Caveat ID Number	Description
CSCvb24566, CSCvb24564 CSCuz52935	Address multiple vulnerabilities in the Libarchive, as described in CVE-2016-1541, CVE-2016-5844, and CVE-2016-6250.
CSCuu96447	In some cases, if you deleted the permanent license from the Licenses page **System** > **Licenses**, the Device Management page **Devices** > **Device Management** did not display **Unlicensed** for devices the permanent license was deleted from when it should have, and policy deploy would fail.
CSCux64898	In some cases, if you deployed an access control policy with the default action set to **Block** and executed the **configure network management-interface disable-event-channel** CLI command, Firepower continued to generate intrusion and connection events when it should not have.
CSCux78211	Resolved an issue where, if an ASA FirePOWER module in high availability experienced a partial failure, the device did not failover when it should have.
CSCux91934	Resolved an issue where, if you deployed an SSL policy configured with a rule associated with an expired SSL certificate, Firepower used an incorrect SSL rule.
CSCuy28088	Cannot apply FP8130-CTRL-LIC to AMP8050.
CSCuy49371	If you clicked **Create Email Alert** on the Alerts page **Policies** > **Actions** > **Alerts** and enabled **Retrospective Events configuration** on the Advanced Malware Protection Alerts tab, then saved and applied, the email alerts generated by Firepower when the alert was triggered were truncated. Emails should not have been truncated.
CSCuy51566	If you updated a Firepower Management Center from Version 5.4.x to Version 6.0.0 or later and created a new sub domain and deployed a network discovery policy, you could not delete any objects or object groups referenced by the network discovery policy in the global domain.
CSCuy57756	In some cases, if you broke a Firepower Threat Defense high availability pair, one of the devices in the pair stayed in standalone mode and Firepower could not recreate the high availability pair.
CSCuy67210	Not able to disable notifications on the Firesight manager Web interface.
CSCuy68648	Resolved an issue where, if you added a security zone on a Firepower Management Center running Version 5.4.0 or later and updated Firepower to Version 6.0.0 or later and deleted the security zone, Firepower generated an **Object deletion restricted. Remove object from the following: Access control policies** error even if the security zone was not referenced within a rule.
CSCuy83201	Fatal errors on applying policy from 6.0.0.1 with different vulnerability database.
CSCuz17315	Resolved an issue where Firepower generated erroneous **Error found during SSL flow after server certificate** messages for evicted SSL flows.
CSCuz17723	Firepower 9300 devices' high availability status is displayed incorrectly/inconsistent in the Firepower Management Center.

Caveat ID Number	Description
CSCuz24872	Original Client IP does not populate for dropped events when inline normalization enabled.
CSCuz46366	Firepower incorrectly allowed you configure sandbox file sizes from 0 MB to 100 MB on the Files and Malware Settings section on the Advanced tab of the access control editor. Firepower only supports capturing files as large as 10 MB. If you configured the sandbox environment to a file size larger than 10 MB, Firepower did not capture the file.
CSCuz49023	Resolved an issue where despite configuration of impact flag alerting for an eStreamer client, Firepower did not stream impact flag data.
CSCuz54417	If you deployed an SSL policy containing application rule conditions for **SMTPS**, **POP3S**, and **IMAPS** traffic, Firepower might have incorrectly displayed Unknown as the application protocol in the Connection Events page **Analysis** > **Connections** > **Events**.
CSCuz78239	DLL-Load vulnerability in Snort on Windows platforms.
CSCuz92255	Resolved an issue where, if you tested the default storage type on the Remote Stage Device section of the Configuration page **System** > **Configuration**, Firepower incorrectly generated a **Please enter valid host. Please enter a valid Directory path.** error message.
CSCuz92983	Policy deployment fails with mode 10 Gbit Full-Duplex for lag interface.
CSCuz94444	Resolved an issue where the associated client incorrectly rejected resigned certificates for Apple related products and you could not log into iTunes.
CSCuz95008	Resolved an issue where, if you requested pre 6.0.0 metadata from a Firepower Management Center with eStreamer running Version 6.0.0. or later, Firepower incorrectly sent the **userID** field to the eStreamer client instead of the configured LDAP username.
CSCuz99677	Resolved an issue where, if you created a new user with an administrator role and deployed configuration, Firepower incorrectly displayed the default admin user as the user deploying the configuration instead of the newly created user.
CSCva00234	Resolved an issue where policy comparison did not include the high availability health modules when it should have.
CSCva01674	sfestreamer crashes when we have 4 management interfaces on Firepower Management Center.
CSCva12481	Disk manager marks conn-unified as deleted.
CSCva28854	Under rare conditions, when 7000 and 8000 Series devices where firstboot policy apply failed, file handles are depleted on the device which caused health/hardware alarms and a variety of malfunctions.

Caveat ID Number	Description
CSCva29636	Resolved an issue where, if you configure network management for a Firepower Threat Defense virtual device, the console incorrectly provided an HTTPS address to complete the installation when it should not have.
CSCva37443	If your ASA configuration file contained an invalid ICMP service object, the ASA-to-Firepower Threat Defense migration tool failed, but did not log adequate information to troubleshooting logs. Migration no longer fails under this condition. Instead, the tool excludes the invalid ICMP objects from the conversion, converts the related ASA access rules to disabled Firepower Threat Defense rules, and adds a comment to the rules describing the unsupported case.
CSCva38608	Resolved an issue where SHA1 signed certificate with a modern browser and Firepower generated untrusted certificate errors for modern browser.
CSCva41164	Version 6.2.0 does not support access control policy names including the **$** character.
CSCva47456	Resolved an issue where, if Firepower requested a URL lookup and the cloud did not immediately return a URL category, the cached request incorrectly remained marked as **Pending** instead of updating the URL type to **Uncategorzied**.
CSCva49869	Report generation did not give a failed message, continues in queue for week.
CSCva51022	If you deployed a pair of network object groups to a Firepower Threat Defense high availability pair and the network object group IP addresses on either the active and standby device overlapped with the IP addresses on the other device within the pair, deployment failed and Firepower generated a Deployment failed due to configuration error message in the Message Center.
CSCva51662	Resolved an issue where, if you clicked **Launch Readiness Check** while another readiness check is in the queue and closed the dialog window, Firepower incorrectly started a new readiness check task .
CSCva57174	On a Firepower Threat Defense Virtual with RIP and redistribution configured, even if you disabled RIP and redeployed, the device continued to use RIP.
CSCva58269	Resolved an issue where, if you created alerts associated with a domain and then deleted the domain, Firepower did not remove the alerts from the database when it should have.
CSCva58393	User is able to apply smart licenses on AWS HB device.
CSCva58411	Resolved an issue where, if you added smart licenses to a Firepower Threat Defense high availability pair, the smart licensing widget on the dashboard page did not load.
CSCva59135	The ASA-to-Firepower Threat Defense migration tool can convert only one ASA configuration file at a time. If you started a conversion while a conversion task was in progress, Firepower displayed an **Error 500 Internal server** error message. Firepower now displays a warning message that a migration is already in progress.

Caveat ID Number	Description
CSCva63604	Resolved an issue where, if a security module on a Firepower Threat Defense cluster with an access control policy containing more than 10,000 rules reloaded, the security module failed to re-join the cluster and generated a **All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration** warning.
CSCva67943	Resolved an issue where, if you enabled common criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate did not contain serverAuth, Firepower incorrectly passed connections to the syslog server when they should have failed.
CSCva72899	Access control policy report fails if category has span across 50 rules.
CSCva81548	Improved configuration deployment performance.
CSCva82945	The Interfaces tab of the device management page for a Firepower Threat Defense device now displays the current status for interfaces on the device.
CSCva89328	Resolved an issue where, if you deployed an intrusion rule containing an AppID web application condition and a managed device experienced a high volume of traffic containing an excessive amount of similar connection types that did not apply to the AppID application, the application detection process took more time than it normally should and caused latency for other traffic matches.
CSCva89342	If you created an ASA Firepower module high available pair configured for multi-context mode and deployed one or more security zone from the managing Firepower Management Center, then the standby ASA Firepower module within the pair restarted, the standby ASA Firepower module incorrectly removed all security zones and interfaces.
CSCva93408, CSCva93158	Improved the RPC decoder.
CSCva99998	Resolved an issue where Firepower did not restrict read-only users from editing the blacklist page when it should have.
CSCvb02417	Adaptive profiling performance scales badly in some cases.
CSCvb02846	Resolved a rare issue where, if you switched Firepower Management Center high availability peers twice and viewed the Smart Licenses page **System** > **Licenses** > **Licenses** > **Smart Licenses**, the table of devices and any edit windows failed to load.
CSCvb05694	Resolved an issue where, if you deployed an SSL policy and traffic with an HTTP tunnel matched the SSL policy, Firepower dropped some traffic and experienced high CPU use and overall latency.
CSCvb08840	Resolved an issue where, if you enabled automated intrusion rule updates for an ASA Firepower module managed by ASDM, and the device simultaneously deployed automated deployments, the device experienced issues.

Caveat ID Number	Description
CSCvb11574	Resolved an issue where, if you deployed an access control policy containing a custom application detector and deleted the application detector, Firepower did not generate a warning that the application detector must be removed from the access control policy prior to deletion.
CSCvb11642	Resolved an issue where, if you created a network discovery policy configured to detect hosts and a correlation policy containing a rule set to trigger if discovery event occurs and the OS information for a host has changed, then added a condition for if OS name is unknown and added a remediation Nmap scan, discovery events matching the rules did not generated corresponding Nmap scans.
CSCvb11931	Resolved an issue where, if Firepower experienced an issue processing the first session of SMTP traffic between a client and an SMTP server, Firepower did not correctly identify the subsequent SMTP sessions as SMTP for the client-server pair and displayed Unknown in the Application Protocol column of the Connection Events page **Analysis** > **Connections** > **Events**.
CSCvb12453	Resolved an issue where, if you enabled common criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate did not contain host name matching the name of the server, connections to the syslog server incorrectly passed when they should have failed.
CSCvb12791	Resolved an issue where, if you enabled Common Criteria (CC) mode on an appliance for security certifications compliance and the syslog server certificate and/or intermediate certificate(s) have been revoked, Firepower incorrectly established a TLS connection with the syslog server without checking the revocation status.
CSCvb14402	Traffic by Initiator Report for User Renders No Output.
CSCvb19366	Cisco Firepower Management Center Information Disclosure Vulnerability.
CSCvb19716	Resolved an issue where Firepower Management Center high availability synchronization failed if the total size of the database files and logs totaled more than 4GB.
CSCvb20859	Intermittently, if the ASA-to-Firepower Threat Defense migration tool could not migrate an ASA configuration because the access control list was not applied via a valid access-group command, Firepower did not complete internal operations related to that migration, and you could not start another migration.
CSCvb24378	You can now enable or disable default inspection with the command line interface on a Firepower Threat Defense device using **configure inspection <inspection_name> enable|disable**.
CSCvb24768	Resolved an issue where, in some cases, if you updated a system containing at least one security zone to Version 6.1 or later, the Interfaces page **Devices** > **Interfaces** might incorrectly displayed the security zone state as **Unknown** .
CSCvb24807	In rare cases, after you updated the Firepower Management Center to Version 6.10, the dynamic analysis page **AMP** > **AMP Management** would not load.

Caveat ID Number	Description
CSCvb25963	Resolved an issue where, if you formed a Firepower 4100 series series or Firepower 9300 high availability pair with devices containing named interfaces and assigned a portchannel from the FXOS chassis manager, then edited the Interfaces tab of the high availability pair listed on the Device Management page **Devices** > **Device Management** and saved, Firepower did not include the interfaces created for the high availability pair when it should and, in some cases, deployment failed.
CSCvb26266	Resolved an issue where, if you enabled captive portal on a system and updated to Version 6.1.0, captive portal did not work.
CSCvb28158	Workflow set with User Preferences not honored by Search Constraints.
CSCvb28202	False warnings in database Integrity Check for PlatformSettings object.
CSCvb32484	Upgrade to 6.1 fails at 600_schema/000_install_csm.sh.
CSCvb32873	Cannot create new Application Filter Objects 6.1 on ASA managed by ASDM.
CSCvb35499	Resolved an issue where, in some cases, if you updated a system from Version 6.1.0 to Version 6.1.0.x, the update failed.
CSCvb35861	Resolved an issue where, if you created a high availability pair and synchronization requests overload the Tasks tab in the Message Center, Firepower experienced disk space issues and intermittent login issues.
CSCvb36645	Resolved an issue where, if incoming HTTP, TCP, or SSH traffic did not contain an SGT value in the header, traffic matched against the default access control policy instead of any other configured policy.
CSCvb36847	Event QoS in legacy mode does not have an entry for interface stats.
CSCvb39325	Resolved an issue where incoming HTTP and HTTPS traffic containing XFF fields caused system issues.
CSCvb39435	If you updated Firepower from a version earlier than Version 6.1.0 to Version 6.1.0 and immediately exported the access control policy, then imported the policy, importing the access control policy failed.
CSCvb40344	If you deployed a file policy to a device with an excessive amount of endpoints configured, Firepower experienced high CPU and memory use. As a workaround, you could redeploy configuration.
CSCvb41047	Resolved an issue where Firepower generated an incorrect **Health monitoring running behind schedule** health warning if the Firepower Management Center did not receive any health events from registered devices.
CSCvb42559	Firepower Management Center Smart Licensing bypasses Proxy Configuration when in evaluation mode.
CSCvb43868	Upgrade failing for v6.0.1 at 600_schema/000_install_csm.sh.
CSCvb44812	Resolved an issue where Firepower 4100 series series devices generated excessive logging and experienced storage space issues.

Caveat ID Number	Description
CSCvb44268	Resolved an issue where the Appliance Status widget did not load if you had 400 or more devices attached to a Firepower Management Center.
CSCvb46146	If updating Firepower failed and you attempted to update to a different version from the one that failed without resolving the original failure, the new install also failed and could cause Firepower to become unrecoverable.
CSCvb46555	Resolved an issue where, if you enabled **Safe Search** in an access control policy and deployed, Firepower incorrectly generated **Primary Detection Engine Exiting** health alerts.
CSCvb47847	Resolved an issue where, if you updated a system from Version 6.0.1.1 or later to Version 6.1.0, Firepower experienced a variety of issues such as update failure or Firepower Management Center login failure.
CSCvb51077	Resolved an issue where, if you added a remediation as a response to a rule in a correlation policy on a Firepower Management Center and created a high availability pair, then switch high availability peers, the new active Firepower Management Center did not correctly synchronize the correlation policy and the remediation experienced issues.
CSCvb52057	Resolved an issue where, if you deployed an access control policy containing rules with **Safe Search** enabled, some websites experienced latency when loading.
CSCvb57521	Firepower Management Center/FTD - Multiple default routes with same metric or gateway exists.
CSCvb57747	Deploy during intrusion rule update install may cause all subsequent policy applies to fail.
CSCvb60088	FTD policy deployment fails with Syslog Event class **All**.
CSCvb61055	Security Intelligence synchronization failure results in disk becoming full.
CSCvb61156	Resolved an issue where, if a Firepower Management Center running Version 6.1.0 managed a device running a version earlier than Version 6.1.0, Firepower did not generate any new discovery events and removed the network map several days after the Firepower Management Center updated to Version 6.1.0.
CSCvb61480	In some cases, if Firepower processed SIP packets, traffic containing voice or video content might have appeared distorted or experienced latency.
CSCvb61836	Resolved an issue where Firepower logged extraneous policy information during deployment and, in some cases, deploying large policies failed.
CSCvb65648	Resolved an issue where, if you deployed an access control policy containing an identity policy that referenced a realm or access control rules containing groups or users from the realm and you deleted the realm, Firepower incorrectly generated a **System defined Objects cannot be Altered. Please use a different Object** error and you could not edit the access control policy.

Caveat ID Number	Description
CSCvb66591	If you configured a realm for an Active Directory (AD) server to download users and groups, then created a Firepower Management Center high availability pair and the downloads contained large amounts of users and groups, Firepower Management Center high availability registration failed.
CSCvb67568	Resolved a rare issue where, if you created a realm and deployed an access control policy containing rules, then clicked **Download users and groups** and configured a User Agent connection, the user to group mapping became incorrect and access control rules using groups did not match when it should.
CSCvb68226	SFR upgrade to 6.1 causes constant failover between ASA FirePOWER module high availability pair.
CSCvb69742	6.0.0 pre install 5.4.0.999 nfp kernel modules fail to unload followed by outage.
CSCvb69906	Intermittently, if you created a realm and deployed an access control policy containing rules, then downloaded users and groups (including scheduled downloads), the user-to-group mapping could become incorrect, and access control rules using groups might not have matched when they should have.
CSCvb70125	Resolved an issue where policy deploy failed if you configured captive portal on a Firepower Management Center then updated the Firepower Management Center and its managed devices, then tried to redeploy.
CSCvb74873	If you enabled SMB File Inspection in a file policy and deployed to a device managed by theFirepower Management Center, Firepower generated **Primary detection engine exited unexpectedly** warning messages, and Firepower could experience issues.
CSCvb75591	If you deployed a DNS rule with a blacklist action containing a Security Intelligence DNS feed, Firepower did not send the Security Intelligence events to the external syslog if one was configured.
CSCvb78786	Firepower ignored security zone constraints on network discovery rules if the network discovery policy contained rules constrained by zones that included interfaces from multiple devices. This condition was present if the rules used single zones with interfaces from multiple devices (for example, Zone 1 included interfaces from Device 1 and Device 2) or multiple rules used different zones (for example if Rule 1 used Zone 1, which included interfaces from Device 1, and Rule 2 used Zone 2, which included interfaces from Device 2).
CSCvb79079	Resolved an issue where, if you added a syslog alert to an access control rule and deployed on an ASA FirePOWER module managed by ASDM, the device incorrectly generated excessive logging from prefilter policies.
CSCvb80872	Resolved an issue where, in some cases, updating a system to Version 6.1.0 and deploying to a registered device generated a **Deployment failed in policy and object collection. If problem persists after retrying, contact TAC** error message.
CSCvb88561	Resolved an issue where, if Firepower processed HTTP traffic containing XFF headers, Firepower experienced issues and generated erroneous detection engine health warnings.

Caveat ID Number	Description
CSCvb91730	Attempting to change copper SFP interface type (inline/switched/routed) results in error.
CSCvb91613	Snort cores after reload when processing XFF addresses.
CSCvb94411	In some cases, if you deployed an SSL policy containing an SSL rule with the action set to **Do Not Decrypt** placed above an SSL rule with the action set to **Decrypt - Resign**, Firepower incorrectly identified the sessions as undecryptable and matched against the wrong rule with an undecryptable action instead of the correct rule.
CSCvb97742	7000 and 8000 Series devices with low memory could experience a traffic outage and not recover.
CSCvc05323	Resolved an issue where snort restarts caused Firepower to generate extraneous **NGFW Rule Engine Failed to write connection event** log messages.
CSCvc08057	Resolved an issue where FTD devices experienced Snort cores while performing QoS rate limiting on destination interface objects.
CSCvc08912	No input validation on FTD Platform Setting syslog Logging Filter.
CSCvc09761	Cannot delete multiple rules at a time from ASA migrated Prefilter Policies.
CSCvc10655	Resolved an issue where deploying policies to a FTD device failed after updating to a new Firepower version.
CSCvc14561	Resolved an issue where the Firepower Management Center web interface was not available after enabling compliance mode.
CSCvc26880	Resolved an issue where, if a Firepower 8350 device or AMP8350 device produced an unusually large stream of messages on the serial port console or, if you enabled it, the Lights-out Management (LOM) console, the device became unresponsive.
CSCvc30591	eStreamer should use correct datastore for user identity mapping.
CSCvc31852	Resolved an issue where the Firepower Management Center Tasks tab displayed an incorrect amount of time taken for policy deployment.
CSCvc36047	Having **0** at the object service PING service icmp echo 0 causes migration to fail.
CSCvc37923	Resolved an issue where Firepower did not recover from a disk write error caused by disk full even after the disk full issue was resolved, causing excessive logging.
CSCvc37927	Import fails with duplicate object name when the object names differs by case only.
CSCvc44398	URL not extracted from reassembled requests.
CSCvc49641	Snort process segfaults processing traffic in firewall.
CSCvc49789	OptimizeTables.pl always fails on 6.1.0.
CSCvc53628	Available Ports tab hangs when editing prefilter rule ports.

Caveat ID Number	Description
CSCvc54134	Resolved an issue where, when a FTD high availability pair simultaneously rebooted, the pair continuously rebooted until the failover cable was removed.
CSCvc55170	Firepower Management Center login stops working if **resume sync** is selected after upgrade.
CSCvc58398	Firepower Management Center warnings needed during high availability configuration that configuration on the standby Firepower Management Center will be wiped.
CSCvd78303	Version 6.2.0-363 resolved an issue where the FTD device running Version 6.1.0.1 or Version 6.1.0.2 stopped passing traffic after 213 days of uptime and experienced a range of issues from limited connectivity to a traffic outage.

CHAPTER 12

Known Issues in Version 6.2.0

Caveat ID Number	Description
CSCun43602	The configured IPv6 address for an ASA FirePOWER module does not display when you run the **show module 1 details** CLI command.
CSCuw79243	If you deploy an intrusion policy to a clustered or stacked 7000 and 8000 Series devices (in Version 6.0.0 known as a high availability pair), Firepower incorrectly counts all devices in the cluster or stack rather than indicating one device for the cluster or stack.
CSCuv86562	Traceback: ASA crash in thread name fover_health_monitoring_thread.
CSCuy65203	If you deploy an intrusion policy with **Drop when Inline** enabled, intrusion events that use the **detection_filter** keyword and are set to drop and generate now display **Dropped** instead of **Would be dropped**.
CSCux67809	Executing the **show crypto key mypubkey rsa** CLI command on an ASA FirePOWER running Firepower Threat Defense erroneously generates device output.
CSCux64898	In some cases, if you deploy an access control policy with the default action set to **Block** and execute the **configure network management-interface disable-event-channel** CLI command, Firepower continues to generate intrusion and connection events when it should not.
CSCux65770	In some cases, if you attempt to log into Firepower with the incorrect password, Firepower incorrectly locks you out of Firepower after two attempts instead of three attempts.
CSCuz17020	Snort is not able to decode traffic.
CSCuz70987	run_qemu_kvm.sh core dumped on 5506 when device low on memory.
CSCuz81740	The Firepower Threat Defense device overwrites core files configuration of FXOS when it should not.
CSCva40041	If you enable failopen on a series 3 device configured with inline sets and then update the device, the device may incorrectly drop link connectivity for up to 10 seconds before it goes into hardware bypass mode.

Caveat ID Number	Description
CSCva40867	If you switch an ASA FirePOWER module from being managed by ASDM to being managed by an Firepower Management Center and the initial device registration fails, but the device eventually successfully registers to the Firepower Management Center, the network map does not update the status of the device after the failed registration attempt and the Firepower Management Center does not generate an connection events or file events for the device when it should.
CSCva54597	Firepower does not deploy the correct **Regular Expression Limits** default values within the access control policy when you deploy configuration.
CSCva74166	The **show environment** CLI command does not work on Firepower Threat Defense devices.
CSCvb11320	If you edit latency-based performance setting values on the Advanced tab of the access control policy editor page and deploy to a registered Firepower Threat Defense device, Firepower does not save the correct latency rule values when it should.
CSCvb39435	If you deploy a file policy to a device with an excessive amount of endpoints configured, Firepower may experience high CPU use and network latency. As a workaround, redeploy configuration.
CSCvb46169	GRE tunnel flow matches QoS rule ID 0.
CSCvb61021	The **show ipv6 ospf neighbor** CLI command does not work on Firepower Threat Defense devices. As a workaround, execute the **system support diagnostic-cli** CLI command and then execute the **show ipv6 ospf neighbor** CLI command again.
CSCvb61805	Firepower Device Manager 5506 deployment takes about a minute more in Version 6.2.0.
CSCvb62117	You cannot change the master role, remove a unit, or execute on a selected unit from a clustered Firepower Threat Defense device via the following CLI commands: **cluster primary security module**, **cluster exec unit**, and cluster remove unit. To use these commands, you must include the unit number as seen from the output of the show cluster info CLI command: **cluster master unit unit-1-1**.
CSCvb62508	Missing suboptions under capture command from converged cli to capture only blacklisted blocked packets.
CSCvb75308	Rate Limiting **may not** take effect on trusted FTP/TFTP data channel in a cluster deployment.
CSCvb77003	Firepower Device Manager- Unable to filter connection events using zones.
CSCvb79547	If you are using ASDM to manage an ASA FirePOWER module, access control policy comparison does not work. This means you cannot display the differences between your running configuration and your planned changes.
CSCvb80626	In rare cases, Firepower Threat Defense Virtual with low memory allocation does not detect some of intrusion policy violations.

Caveat ID Number	Description
CSCvb88724	The **clear conn** CLI command on the Firepower Threat Defense device only allows you to enter a single IP address for the source or destination; any connections matching the IP address for either the source OR destination are cleared. The CLI help shows that you can enter both a source and destination IP address, but you can only enter 1 address.
CSCvb92548	ASA matches incorrect ACL with object-group-search enabled.
CSCvc01792	Some Firepower Threat Defense commands are model-specific, but may be visible on non-supported models. If you enter an unsupported command, you see the following error: **-ERROR: % Invalid input detected at '^' marker**. Check your command in the Firepower Threat Defense Command Reference Guide for model limitations.
CSCvc03720	The **clear mac-address-table** CLI command is only supported on devices deployed in transparent mode when it should be supported on devices deployed in transparent and routed mode. As a workaround, execute the **system support diagnostic-cli** CLI command for devices deployed in routed mode.
CSCvc05098	If the active Firepower Management Center of a high availability pair fails and the standby Firepower Management Center continues to process traffic while the pair is in a degraded state, then the active Firepower Management Center recovers, Firepower incorrectly displays unknown user for events generated during the degraded state for up to 24 hours before correcting.
CSCvc09167	Firewall rules may not be in sync with firmware rules following policy apply.
CSCvc26721	Management interface receives no traffic after port flap or failover on 5506/5508/5516.
CSCvc35890	If you deploy configuration, Firepower may experience a prolonged amount of time writing syslogs and incorrectly trigger Automatic Application Bypass (AAB) when it should not.
CSCvc38425	ASA with FirePOWER module generates traceback and reloads.
CSCvc41387	If you click the help icon next to the filter textbox, Firepower incorrectly generates an **Error 404: Page not found** error. As a workaround, search the Online Help **Help** > **Online** for intrusion policy keywords.
CSCvc46502	If intra-clustered Firepower Threat Defense devices configured with passive mode or inline tap interfaces experience fragmented traffic, virtual reassembly may fail and the device incorrectly drops traffic. As a workaround, restart the device.
CSCvc50022	Firepower may not be able to process as many HTTP connections in Version 6.2.0 compared to Version 6.1.0.
CSCvc51442	Firepower Threat Defense virtual: ESXi standalone having trouble with serial number.
CSCvc51459	If you run the **managed_pruning.pl** CLI command on an Firepower Management Center and click **Purge Event database & (2)**, the script generates an extraneous warning after purging the database.
CSCvc52879	Reloading Active unit in Active/Standby ASA failover pair is not triggering a failover.

Caveat ID Number	Description
CSCvc53140	OSPF retransmissions and VPN tunnels lost after Active ASA reload.
CSCvc53558	If you add a 10GB management interface to a Firepower Management Center, adding fails and Firepower generates an **unable to change mode for eth2** error.
CSCvc54069	If you create a VPN connection with a reverse route that is same as the already present static route on a Firepower Threat Defense device, then restart the device, the static route breaks and you cannot successfully use the VPN connection.
CSCvc55105	The web interface pages of a Firepower Management Center running Version 6.2.0 takes longer to load than the pages of a Firepower Management Center running Version 6.1.0.x
CSCvc55674	A resource depletion issue can occur on the ASA 5516-X if more than 500 concurrent IPsec or SSL connections are established to the unit. This is unrelated to the maximum IPsec/IKE endpoint count and pertains only to IPsec (either ESP or NAT-T) or SSL connections. The resource depletion will trigger an error and prevent new IPsec or SSL connections from being created to the unit. This issue is specific to the ASA 5506/5508/5516-X family of devices, but is most likely to be seen with the ASA 5516-X. No other ASA FirePOWER modules are affected by this issue.
CSCvc56526	CEP records edit page take minutes to load.
CSCvc56717	In some cases, if Firepower experiences a database error and you attempt to create a domain, you may not be able to delete a domain or move a device to a domain.
CSCvc56746	The Objects page in the FC2000 and FC4000 web interface takes more time to load in Version 6.2 compared to Version 6.1.x.
CSCvc56767	The FC2000 web interface takes more time to save an access control policy in Version 6.2 compared to Version 6.1.x.
CSCvc56919	Traffic drops for reverse UDP/TCP IPv6 traffic over IPv4 tunnel.
CSCvc58132	When upgrading FTD, Firepower may fail to detect applications during the upgrade. Issue will be automatically resolved once deployment is manually triggered post upgrade.
CSCvc58296	In some cases, if you update Firepower and configure Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**), Firepower does not display the available routes when it should. As a workaround, restart the managed device. .
CSCvc58453	FTD devices running FXOS Version 2.1.1(64) do not support Firepower Version 6.1.0.
CSCvc58272	ASA incorrectly processing negative numbers in wrappers, resulting in graphical webvpn issue.
CSCvc58398	Firepower Management Center warnings needed during high availability configuration that configuration on standby will be wiped.

Caveat ID Number	Description
CSCvc59613	If you assign both an active and standby MAC address to a registered Firepower 4100 series or Firepower 9300 high availability pair with the **Add Interface MAC Address** option in the High Availability tab of the Integration page **System** > **Integration** and deploy, then edit the interfaces and delete the interface, Firepower does not delete the MAC address associated with the interface after synchronizing the pair and redeploying fails. As a workaround, delete both the interface and the MAC address associated with the interface, then synchronize changes and redeploy.
CSCvc59811	If you place an access control rule configured to **Allow** a subdomain URL (site.example.com) above an access control rule configured to **Block** the domain URL (example.com), the system may block request to subdomain URL. As a workaround, create an access control to **Allow** each subdomain URL (site.example.com, site2.example.com, etc.) you do not want blocked instead of the rule to block the domain URL, then save and redeploy.
CSCvc60254	SIP: 200 OK messages with multiple seqments not reassembled correctly.
CSCvc62252	Tracking route is up while the reachability is down.
CSCvc62492	ASA: File system becomes read-only after very long up time.
CSCvc62556	Traceback in ASA Cluster Thread Name: qos_metric_daemon.
CSCvc63722	Report Generation of large no of Events is failing.
CSCvc63954	ASA traceback in Thread Name: Event mib process.
CSCvc64050	ASAConfig uses wrong interface IDs after slave unit rejoins multi context ASA cluster.
CSCvc65262	After Snort restart, UDP processing performance may decrease.
CSCvc65409	Traceback observed on gtpv2_process_msg on cluster.
CSCvc65470	In some cases, connection events and security intelligence events generated from identity policy activity show the **Initiator User 0** instead of the username.
CSCvc65528	Pages in the MC4000 web interface take more time to load in Version 6.2.0 compared to Version 6.1.x.
CSCvc68358	The **show lacp** CLI command does not work on ASA 5585-X devices.
CSCvc74395	If you deploy an access control policy containing an access rule with Original Client IP, logging enabled and an SSL rule with the default actions set to **Decrypt - Resign**, Firepower does not display the Action and Access control rule columns of some generated events in the Connection Events page **Analysis** > **Connections** > **Connection Events**.
CSCvc75561	If you use non-ASCII characters in a Flex Config object, the Flex Config policy fails to deploy. As a workaround, replace the non-ASCII characters with the ASCII equivalents.

Caveat ID Number	Description
CSCvc76439	If you create a GID:135 intrusion rule, the rule does not save and Firepower generates a **failed to set the rule state** error.
CSCvc79719	SMB upload - Malware block miss on first attempt.
CSCvc81525	In rare cases, Firepower Threat Defense devices managed by the Firepower Device Manager and ASA with FirePOWER Services devices managed with ASDM can experience an exhaustion of database handles, which prevents any attempt to upgrade to Version 6.2.0. Prior to running the upgrade, contact Cisco TAC to enable upgrade by restarting the appropriate processes.
CSCvc82066	If you update a Firepower Management Center from Version 6.1.0 to 6.2.0 and deploy, deployment may fail and Firepower may generate a **mtu 9188 ^ ERROR: % Invalid input detected at '^' marker.** error message. As a workaround, change the MTU value before you update to Version 6.2.0.
CSCvc92934	If you deploy an access control policy containing an access control rule configured to **Allow** a subdomain URL (site.example.com) placed before an access control rule configured to **Block** the domain URL (example.com) that references an SSL policy with decryption enabled, the system may inconsistently match traffic against the HTTPs certificate instead of the actual URL and navigating to the subdomain may get blocked when it should not.

CHAPTER 13

For Assistance

Thank you for choosing Firepower.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco NGFW and NGIPS devices, see *What's New in Cisco Product Documentation* at: https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

If you have any questions about installing or running Firepower, contact TAC Support:

- Visit the Cisco Support site at https://www.cisco.com/c/en/us/support/index.html.
- Email Cisco Support at mailto:tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.