# Firepower System Release Notes

**Version 6.0**
**First Published: November 11, 2015**
**Last Updated: December 5, 2017**

These release notes are valid for Version 6.0 of the Firepower System. Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, management platform-managed device compatibility, and known and resolved issues. They also contain detailed information on prerequisites, warnings, and specific installation instructions.

**Tip** To access the full documentation for the Firepower System, see the documentation roadmap at http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html.

**Caution: You must install the FireSIGHT System Version 6.0.0 Pre-Installation package prior to updating to Version 6.0. For more information, see the *FireSIGHT System Release Notes Version 6.0 Pre-Installation*.**

For more information, see the following sections:



# Supported Platforms and Compatibility

Supported platforms, minimum originating versions, and operating systems vary by version. For more information, see:



## Supported Platforms

You can run Version 6.0 on the platforms specified in the following table. For minimum Firepower System version requirements, see Firepower Version Requirements for Updating to Version 6.0, page 13.

**Note:** Version 6.0 of the Firepower 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.

**Table 2-1** Platform Support in Version 6.0

| Supported platforms in Version 6.0 | Capability in Version 6.0 | Other requirements to run Version 6.0 |
|---|---|---|
| Firepower Management Center (the MC750, MC1500, MC3500, MC2000, and the MC4000) | management | ■ MC750 requires two 4GB dual in-line memory modules (DIMM)<br>■ MC1500 requires at least 8GB of memory |
| 64-bit Firepower Management Center Virtual | management | hosted on:<br>■ VMware vSphere Hypervisor/VMware ESXi 5.1<br>■ VMware vSphere Hypervisor/VMware ESXi 5.5<br>■ VMware vCloud Director 5.1 |
| Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390) | managed device | n/a |
| Cisco ASA with FirePOWER Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, AS A5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) | managed device | running:<br>■ ASA Version 9.4(x)<br>*No ASDM or captive portal*<br>■ ASA Version 9.5(1.5)<br>*No captive portal*<br>■ ASA Version 9.5(2)<br>■ ASA Version 9.5(3)<br>■ ASA Version 9.6(x) |
| NGIPSv (virtual managed device) | managed device | hosted on:<br>■ VMware vSphere Hypervisor/VMware ESXi 5.1<br>■ VMware vSphere Hypervisor/VMware ESXi 5.5<br>■ VMware vCloud Director 5.1 |

# Management Platform-Managed Device Compatibility

Management capability varies by version. The following tables detail available management platforms and the devices that those platforms can manage:

**Table 2-2** Management Platform-Compatibility by Management Platform

| Supported management platforms | What can you manage using this management platform? |
|---|---|
| Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) | All of the following, running at least Version 5.4.0.2:<br>■ Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390)<br>■ NGIPSv (virtual managed devices)<br>■ Cisco ASA with Firepower Services (the 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, and the ASA 5585-X-SSP-60)<br>**Caution: Updating a Firepower Management Center managing devices running Version 5.4.0.6, Version 5.4.1.5, or earlier to Version 6.0 may cause traffic outages and system issues. You must disable the Retry URL cache miss lookup option in the Advanced Options section of the Access Control page to managed devices running Version 5.4.0.6, Version 5.4.1.5, or earlier prior to deploying configuration.**<br>All of the following, Running Version 5.4.1.1:<br>■ Cisco ASA with Firepower Services (the ASA 5506X- ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and the ASA 5516-X)<br>All of the following, running Version 6.0:<br>■ Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390)<br>■ NGIPSv (virtual managed devices)<br>■ Cisco ASA with FirePOWER Services (the 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, and the ASA 5585-X-SSP-60) |

**Table 2-2** Management Platform-Compatibility by Management Platform

| Supported management platforms | What can you manage using this management platform? |
|---|---|
| ASDM version 7.5(1.112) and later | All of the following, running Version 6.0:<br>■ Cisco ASA with FirePOWER Services (the 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, and the ASA 5585-X-SSP-60) |
| 64-bit Firepower Management Centers Virtual | All of the following, running at least Version 5.4.0.2:<br>■ Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390)<br>■ NGIPSv (virtual managed devices)<br>■ Cisco ASA with Firepower Services (the 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, and the ASA 5585-X-SSP-60)<br>**Caution: Updating a Firepower Management Center managing devices running Version 5.4.0.6, Version 5.4.1.5, or earlier to Version 6.0 may cause traffic outages and system issues. You must disable the Retry URL cache miss lookup option in the Advanced Options section of the Access Control page to managed devices running Version 5.4.0.6, Version 5.4.1.5, or earlier prior to deploying configuration.**<br>All of the following, Running Version 5.4.1.1:<br>■ Cisco ASA with Firepower Services (the ASA 5506X- ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and the ASA 5516-X)<br>All of the following, running Version 6.0:<br>■ Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390)<br>■ NGIPSv (virtual managed devices)<br>■ Cisco ASA with FirePOWER Services (the 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, and the ASA 5585-X-SSP-60) |

**Table 2-3** Management Platform-Managed Device Compatibility by Managed Device

| Supported Managed Devices | What can you use to manage this device? |
|---|---|
| Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390) | All of the following, running Version 6.0:<br>■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000)<br>■ 64-bit Firepower Management Centers Virtual |
| Cisco ASA with FirePOWER Services (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 the ASA 5585-X-SSP-60) | All of the following, running Version 6.0:<br>■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000)<br>■ 64-bit Firepower Management Centers Virtual<br>■ ASDM (the 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, and the ASA 5585-X-SSP-60) |
| NGIPSv (virtual managed devices) | All of the following, running Version 6.0:<br>■ Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000)<br>■ 64-bit virtual Firepower Management Centers |

# New Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 6.0 of the Firepower System:



## New Features

The following features are introduced in Version 6.0:

### Expanded Threat Protection

#### URL and DNS-based Security Intelligence

New Security Intelligence feeds based on URLs and Domain Name System (DNS) servers are provided to enhance the existing IP-based Security Intelligence capability. Currently, IP-based intelligence is used to control access to known malware, phishing, command & control, and Bot sites. New attack methods designed to defeat IP-based intelligence (e.g., fast flux) abuse DNS load balancing features in an effort to hide the actual IP address of a malicious server. While the IP addresses associated with the attack are frequently swapped in and out, the domain name will rarely change. The URL-based intelligence will supplement the IP-based intelligence in addressing this kind of attack, and the DNS-based intelligence will help identify known DNS servers that are complicit in these kinds of attacks. Access control policies can be created using these new intelligence feeds and new dashboards provide visibility and analysis. In addition, both URL-based and

DNS-based Security Intelligence events will also feed in to the Indications of Compromise (IoC) correlation feature. These new feeds are provided through regular updates from the Cisco Talos Security Intelligence and Research Group and, like the IP-based Security Intelligence feature, are part of the base product and do not require a separate license.

### DNS Inspection and Sinkholes

The same way that attackers use the SSL protocol to hide their activity, attackers use the DNS protocol with the same intentions. For that reason, and as another way to address fast flux-type attacks, the Firepower system provides the ability to intercept DNS traffic requests and take appropriate action based on the policy setting. A DNS policy allows for requests to known command & control, spam, phishing, etc., sites to be blocked, to return a `Domain Not Found` message, or have the traffic directed to a pre-configured sinkhole. This last option routes the traffic directly through the Firepower managed device and gives information about the endpoint that could result in an IoC alert.

## Enhanced Network Visibility and Control

### SSL Decryption for Cisco ASA with FirePOWER Services Managed Via ASDM

Cisco's next-generation firewall (NGFW), Cisco ASA with FirePOWER Services, now has the ability to locally manage SSL communications and decrypt the traffic before performing attack, application, and malware detection against it. This is the same capability we introduced in Version 5.4 for Cisco's Firepower next-generation IPS (NGIPS) appliances. SSL decryption can be deployed in both passive and inline modes, and supports HTTPS and StartTLS-based applications (e.g., SMTPS, POP3S, FTPS, IMAPS, TelnetS). Decryption policies can be configured to exert granular control over encrypted traffic logging and handling, such as limiting decryption based on URL categories to enforce privacy concerns. It also provides the ability to block self-signed encrypted traffic, or on SSL version, specific Cipher Suites, and/or unapproved mobile devices.

### Support for OpenAppID-Defined Applications

OpenAppID is Cisco's open source, application-focused detection language that enables users to create, share and implement new application detection signatures for custom, localized, and cloud applications, without being dependent upon a NGFW vendor's release cycle or roadmap. In Version 6.0, the Firepower application detection engine that identifies and controls access to over 3,000 applications has been enhanced to recognize OpenAppID-defined applications. In the same way that Snort was an effort to open source the intrusion detection game, OpenAppID is a way to open source the application detection game. Support for OpenAppId-defined applications demonstrates Cisco's commitment to the open source initiatives and the flexibility that it provides to our customers.

### Captive Portal and Active Authentication

In order to provide better visibility in mapping users to IP addresses and their associated network events, the Captive Portal and Active Authentication feature can be configured to require users to enter their credentials when prompted through a browser window. The mapping also allows policies to be based on a user or group of users. This feature supplements the existing Sourcefire User Agent (SUA) integration with Active Directory to address non-Windows environments, BYOD users, and guests.

**Note:** Cisco ASA with FirePOWER Services only supports the Captive Portal and Active Authentication feature when running ASA version 9.5(2) or later.

### Integration with Cisco Identity Services Engine (ISE)

The integration with Cisco ISE enhances the user identity data available to the system to use in analysis and policy control. By subscribing to Cisco's Platform Exchange Grid (PxGrid), the Firepower Management Center is able to download additional user data, device type data, device location data, and Security Group Tags (SGTs —a method used by ISE to provide network access control). Beyond the added visibility into the users on your network, this data is also actionable intelligence because it extends the control you can provide by creating policies based on SGTs, or on device type, or any of the other information provided by ISE.

**Note:** In Version 6.0, you cannot use ISE to automatically quarantine an infected endpoint. This functionality will be added in a later release.

## Improved Threat Defense Against Advanced Persistent Threats

### Local Malware Checks

This feature provides the ability to identify popular/common malware directly on the Firepower appliance, and reduces the need to send files for dynamic analysis (sandboxing), either in the cloud or on-prem (see Intergration with AMP Threat Grid). Using high-fidelity ClamAV signatures, files whose SHA-256 lookup return a disposition of `Unknown` will be analyzed locally on the Firepower appliance to identify common characteristics associated with malware, reducing the need for dynamic analysis.

### File Property Analysis

Because certain file types support nested content that can be used to hide malware, this feature provides local analysis of files to determine the viability of malware hidden within. For example, a PDF file can contain different types of files nested inside the file. A file composition report is then run that identifies if nested data exists within the file, what file types those nested files represent, and how likely each nested file is to contain malware. Based on this information, you can choose whether or not to send the file on for dynamic analysis.

### Integration with AMP Threat Grid

Cisco's acquisition of ThreatGrid in June 2014 increased our abilities in helping our customers address advanced persistent threats, and that technology has now been fully integrated in Firepower v6.0. AMP Threat Grid now provides our sandboxing capabilities in the cloud when using our **AMP for Firepower** option. Files sent to the cloud for dynamic analysis are securely analyzed and correlated against hundreds of millions of other analyzed malware artifacts to provide a global view of malware attacks, campaigns, and their distribution. Detailed reports identify key behavioral indicators and determine threat scores for faster prioritization and recovery from advanced attacks.

In addition, we have greatly expanded the file types we support for automatic dynamic analysis from just executable files to include PDF and Office documents.

## Expanded Management Functionality

### Multiple Domain Management

To address the service provider market which must manage separate customer environments, as well as enterprises with acquisitions (resulting in overlapping IP addresses) or geographic business units that need to be managed separately, the Firepower Management Center now has the ability to create multiple management domains. These domains (up to 50) enable separate management environments and are administered using granular role-based access control (RBAC). Each domain provides separate event data, reporting, and network maps.

### Policy Hierarchy and Inheritance

To support multiple domain management and make policy administration more efficient, Version 6.0 provides the ability to create a hierarchy of policies. Global policies (e.g., access control) can be established that will apply to all management environments. A policy hierarchy can then be constructed underneath the global policy level to represent different environments, different companies, different business units, or different parts of the organization. Each of these policy environments will inherit the policies of the hierarchy above it, allowing for more consistent and efficient policy management.

### Expanded ASDM Management Availability

Cisco's Adaptive Security Device Manager (ASDM) is the local management feature for Cisco ASA with FirePOWER Services. It was introduced as part of the Cisco ASA 5506-X, ASA 5508-X, and ASA 5516-X appliances. With Firepower v6.0, ASDM is now available on the remaining Cisco ASA with FirePOWER Services appliances (ASA 5512-X / ASA 5515-X / ASA 5525-X / ASA 5545-X / ASA 5555-X / ASA 5585-X).

# Changed Functionality

- The default password for Firepower Management Center and Firepower Management Center virtual appliances changes from `Sourcefire` to `Admin123` in Version 6.0 and later. For more information, see the Firepower Management Center Quick Start Guide.
- You cannot compare policies on the following pages: the NAT Policy page, the Platform Settings page, and the SSL Policy page.

- Version 6.0 does not support AMP for Firepower signature lookups with the private AMP cloud. In Version 6.0, the system automatically submits SHA-256 signatures to the public AMP cloud. If you have a private AMP cloud and are receiving events from endpoints, the Version 6.0 Firepower Management Center will continue to receive those events without any additional changes to your configuration.
- Syslog messages for connection events now populate information for the following fields: HTTP Referrer, User Agent, and Referenced Host.
- Version 6.0 does not support Discovery Event Health Monitoring.)
- You can now edit Automatic Application Bypass (AAB) settings on ASA modules running FirePOWER services.

# Updated Terminology

The terminology used in Version 6.0 may differ from the terminology used in previous releases. For more information, see the *Firepower Compatibility Guide*.

# Updated Documentation

To access the full documentation for the Firepower System, see the documentation roadmap at http://www.cisco.com/c/en/us/td/docs/security/firesight/roadmap/firesight-roadmap.html. In Version 6.0, the following documents were updated to reflect the addition of new features and changed functionality and to address reported documentation issues:

- *Firepower Management Center Online Help*
- *ASA FirePOWER Module Online Help*
- *Firepower Management Center Configuration Guide*
- *Firepower Management Center Installation Guide*
- *Firepower System Virtual Installation Guide*
- *Firepower System eStreamer Integration Guide*
- *Firepower System Remediation API Guide*
- *Firepower System Database Access Guide*
- *Firepower System Host Input API Guide*
- *Firepower NGIPSv for VMware Quick Start Guide*
- *Firepower NGIPSv and Firepower Management Center for VMware Quick Start Guide*
- *Cisco ASA FirePOWER Services Local Management Configuration Guide*
- *Firepower 7000 and 8000 Series Installation Guide*

The documentation updated for Version 6.0 contains the following errors:

- The *Firepower Management Center Configuration Guide* does not reflect that in a multidomain deployment, when you create a DNS policy, the Descendant Whitelists for DNS rule and Descendant Blacklists for DNS rule are disabled by default. You can enable each rule by editing them. (CSCuw62140)
- The online help incorrectly states that the default intrusion policy instead of the currently deployed access control policy inspects traffic during policy deployment if you deploy your configuration changes with Inspect traffic during policy apply enabled and no specific configuration requires a snort restart.

**Note:** The online help content may differ from the *Firepower Management Center Configuration Guide* content. The *Firepower Management Center Configuration Guide* content is updated more regularly than the online help.

# Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 6.0, 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: You `must` install the FireSIGHT System Version 6.0.0 Pre-Installation package prior to updating the Version 6.0. For more information, see the *FireSIGHT System Release Notes Version 6.0 Pre-Installation*.**

**Caution: Cisco strongly recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.**

For more information, see the following sections:



## Configuration and Event Backup Guidelines

Before you begin the update, Cisco strongly recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

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*.

Version 6.0 does not support AMP for Firepower signature lookups with the private AMP cloud. In Version 6.0, the system automatically submits SHA-256 signatures to the public AMP cloud. If you have a private AMP cloud and are receiving events from endpoints, the Version 6.0 Firepower Management Center will continue to receive those events without any additional changes to your configuration.

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

## Applying the Version 6.0 Pre-Installation Package

Apply the Version 6.0 Pre-Installation Package before updating to Version 6.0 if your appliances are running the following versions:

- Firepower Management Centers running Version 5.4.1.1, Version 5.4.1.2, Version 5.4.1.3, Version 5.4.1.4, or Version 5.4.1.5
- Series 3 devices running Version 5.4.0.2, Version 5.4.0.3, Version 5.4.0.4, Version 5.4.0.5, or Version 5.4.0.6
- ASA FirePOWER modules (ASA FirePOWER modules (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, and the ASA 5585-X-SSP-60) running Version 5.4.0.2, Version 5.4.0.3, Version 5.4.0.4, Version 5.4.0.5, or Version 5.4.0.6
- ASA FirePOWER modules (ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, and ASA 5516-X) running Version 5.4.1.1, Version 5.4.1.2, Version 5.4.1.3, Version 5.4.1.4, or Version 5.4.1.

Applying the Version 6.0 Pre-Installation Package before updating to Version 6.0 is **not** required for appliances running the following versions, but we strongly recommend applying the Version 6.0 Pre-Installation Package as it optimizes updating Firepower Management Centers to Version 6.0.0 and decreases the time the update takes to complete:

- Firepower Management Centers running Version 5.4.1.6 or later (not required, but strongly recommended)
- Series 3 devices running Version 5.4.0.7 or later
- ASA FirePOWER modules (ASA FirePOWER modules (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, and the ASA 5585-X-SSP-60) running Version 5.4.0.7 or later
- ASA FirePOWER modules (ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, and ASA 5516-X) running Version 5.4.1.6 or later

## Break Firepower Management Center High Availability Prior to Upgrade

Version 6.0 does not support Firepower Management Centers in a high availability pair. In order to update Firepower Management Centers in a high availability environment, you must break the pair and update each Firepower Management Center individually. In order to update to Version 6.0, you must break the high availability pair.

## Update Firepower Management Center Memory for MC750 and MC1500 and Management Centers Virtual

Version 6.0 of the Firepower 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, Cisco is making memory upgrade kits available for customers with these models. These kits can be ordered at no cost by customers who are entitled to run Version 6.0 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 *Firepower Management Center Installation Guide*.

In addition, Management Centers Virtual require a minimum of 8GB of memory to update to Version 6.0.

## Update Management Center HTTPS Certificates to Version 6.0

Use of a certificate with an `RSASSA-PSS` signature algorithm on a Firepower Management Center is not currently supported in Version 6.0. If you update a Firepower Management Center using such a certificate to Version 6.0 or add such a certificate in Version 6.0, the system does not allow you to log into the Management Center web interface and generates an `Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator` error.

Prior to updating, generate and install an HTTPS certificate with either a `sha1WithRSAEncryption` or `sha256WithRSAEncryption` algorithm and restart the Firepower Management Center, or use the default Firepower Management Center certificate and restart the appliance.

Similarly, if the certificate used by the Firepower Management Center was generated using a public server key larger than 2048 bits, you will not be able to log into the Management Center web interface after updating to Version 6.0.

If you are unable to log into the Management Center web interface with a public server key with more than 2048 bits, replace certificates that were created with larger public keys by generating a server certificate request (CSR) and then applying a certificate generated using that request to the Firepower Management Center. After installing the new certificate, restart the appliance.

**Note:** For information on correctly generating a certificate on a Version 5.4.x appliance, see Using Custom HTTPS Certificates in the *FireSIGHT System User Guide*, Version 5.4.1.

If you lose access to the web interface after updating to Version 6.0 or after uploading a certificate, contact Support.

# 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 vs passive, bypass mode settings, and so on. We strongly recommend performing the update in a maintenance window or at a time when the interruptions will have the least impact on your deployment.

**Note:** When you update 8000 Series clusters or stack pairs, the system performs the update one device at a time to avoid traffic interruption. When you update clustered Cisco ASA with FirePOWER Services devices, apply the update one device at a time, allowing the update to complete before updating the second device.

This section discusses traffic behavior during the following update stages:

- The update itself, including related reboots
- 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 appliances do not perform switching, routing, NAT, and VPN during the update process, regardless of how you configure any inline sets.

**Table 4** Update Traffic Behavior

| Device | Deployment | Traffic Behavior |
|---|---|---|
| 7000 and 8000 Series | inline with optional hardware bypass module, bypass enabled **(Bypass Mode**: **Bypass**) | passed without inspection<br>Network traffic is interrupted briefly at two points :<br>■ At the beginning of the update process, as link goes down and up (flaps) and the network card switches into hardware bypass.<br>■ 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.<br>The hardware bypass option is **not** supported on nonbypass network modules on ASA with FirePOWER Services 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 |

**Table 4** Update Traffic Behavior

| 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<br>(requires at least the minimum supported ASA OS version; otherwise, traffic dropped) |
| | routed or transparent, fail-close (**Close Traffic**) | 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 5** Restart Traffic Effects by Managed Device Model

| Device Model | Interface Configuration | Restart Traffic Behavior |
|---|---|---|
| 7000 and 8000 Series, NGIPSv | inline, **Failsafe** enabled or disabled | passed without inspection<br>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 |

## Audit Logging During the Update

When updating appliances that have a web interface, after the system completes its pre-update tasks and the streamlined update interface page appears, login attempts to the appliance are not reflected in the audit log until the update process is complete and the appliance reboots.

## Time and Disk Space Requirements for Updating to Version 6.0

The table below provides disk space and time guidelines for the Version 6.0 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 restart the update or reboot your appliance at any time during the update process. Cisco provides time estimates as a guide, but actual update times vary depending on the appliance model, deployment, and configuration. Note that the system may appear inactive during the pre-checks portion of the update and after rebooting; this is expected behavior.**

The reboot portion of the update includes a database check. If errors are found during the database check, the update requires additional time to complete. System daemons that interact with the database do not run during the database check and repair.

**Note:** The closer your appliance's current version to the release version (Version 6.0), the less time the update takes.

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

**Table 2-6** Time and Disk Space Requirements

| Appliance | Space on / | Space on /Volume | Space on /Volume on Manager | Time |
|---|---|---|---|---|
| Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) | 16 MB | 8022 MB | 1.5 GB | 58 minutes |
| 64-bit Firepower Management Centers Virtual | 16 MB | 8022 MB | 1.5 GB | hardware dependent |
| 7000 Series and 8000 Series devices (the 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, AMP8380, and the AMP8390) | 16 MB | 6496 MB | 1.2 GB | 94 minutes |
| Cisco ASA with FirePOWER Services (the 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, and the ASA 5585-X-SSP-60) | 32 MB | 7644 MB | 1.2 GB | 41 minutes |
| NGIPSv (virtual managed devices) | 17 MB | 6046 MB | 1.2 GB | hardware dependent |

# Firepower Version Requirements for Updating to Version 6.0

Appliances must be running the minimum versions specified in the following table in order to update to Version 6.0 of the Firepower System. For minimum operating system requirements and information about management platform-managed device compatibility, see Supported Platforms and Compatibility, page 1.

**Note:** A Firepower Management Center must be running at least Version 6.0 if you want to use it to update its managed devices to Version 6.0.

*Table 7 Platform Support in Version 6.0*

| Platform | Minimum version required to update to Version 6.0 |
|---|---|
| Firepower Management Centers (the MC750, MC1500, MC3500, MC2000, and the MC4000) | Version 5.4.1.1 |
| 64-bit Firepower Management Centers Virtual | Version 5.4.1.1 |
| Firepower 7000 Series and 8000 Series (the 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, AMP8380, and the AMP8390) | Version 5.4.0.2 |
| Cisco ASA with FirePOWER Services (the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and the ASA 5516-X) | Version 5.4.1 |
| Cisco ASA with FirePOWER Services (the 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, and the ASA 5585-X-SSP-60) | Version 5.4.0.2 |
| NGIPSv (virtual managed devices) | Version 5.4.0.2 |

# Web Browser and Screen Resolution Compatibility in Version 6.0

Note the following to optimize your experience using the web interface.

### Web Browser Compatibility

Version 6.0 of the web interface for the Firepower System has been tested on the browsers listed in the following table.

**Note:** 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 a self-signed certificate to the trust store of the browser/OS or use another web browser.

**Note:** If you use the Microsoft Internet Explorer 11 browser, you must disable the **Include local directory path when uploading files to server** option in your Internet Explorer settings via **Tools > Internet Options > Security > Custom level**.

*Table 8 Supported Web Browsers*

| Browser | Required Enabled Options and Settings |
|---|---|
| Chrome 46 | JavaScript, cookies |
| Firefox 41 | JavaScript, cookies, Secure Sockets Layer (SSL) v3 |
| Microsoft Internet Explorer 10 and 11 | JavaScript, cookies, Secure Sockets Layer (SSL) v3, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** |

### Screen Resolution Compatibility

Cisco recommends selecting a screen resolution that is at least 1280 pixels wide. The user interface is compatible with lower resolutions, but a higher resolution optimizes the display.

# Integrated Product Compatibility in Version 6.0

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

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

For more information, see the *Firepower System Compatibility Guide*.

# Installing the Update

Before you begin the update, you must thoroughly read and understand these release notes, especially Supported Platforms and Compatibility, page 1 and Before You Begin: Important Update and Compatibility Notes, page 9.

**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.

For minimum Firepower System version requirements, see Firepower Version Requirements for Updating to Version 6.0, page 13. To update your appliances, see the guidelines and procedures outlined below:

- Updating Firepower Management Centers, page 16
- Updating Managed Devices and ASA FirePOWER Modules, page 18

**Caution: Do not reboot or shut down your appliances during the update until you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.**

**Note:** Version 6.0 of the Firepower 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. For more information see Update Firepower Management Center Memory for MC750 and MC1500 and Management Centers Virtual, page 10 and the *Firepower Management Center Installation Guide*.

### When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, Cisco **strongly** recommends you perform the update in a maintenance window or at a time when the interruption will have the least impact on your deployment.

### Installation Method

You `must` install the FireSIGHT System Version 6.0.0 Pre-Installation package prior to updating the Version 6.0. For more information, see the *FireSIGHT System Release Notes Version 6.0.0 Pre-Installation Package*.

Use the Firepower Management Center's web interface to perform the update. Update the Firepower Management Center first, then use it to update the devices it manages.

### Order of Installation

Update your Firepower Management Centers before updating the devices they manage.

**Caution: URL category determination can introduce up to two seconds of delay in packet delivery, depending on local network conditions. If such delay is not acceptable, URL retry should not be allowed. Note that without URL retry, URL filtering may not be effective until such time as URL category and reputation determination completes for each URL. Until that time, packets that would have been filtered based on the URL's category or reputation will be filtered based on the Uncategorized category. For more information on preventing URL retry, see Preventing URL Cache Miss Lookup Retries, page 18.**

### Installing the Update on Paired Firepower Management Centers

Updating Firepower Management Center in a high availability pair is not supported in Version 6.0. In order to update Firepower Management Centers in a high availability environment, you must break the pair and update each Firepower Management Center individually.In order to update to Version 6.0, you must break the high availability pair.

### Installing the Update on Clustered Devices

When you install an update on clustered devices (in Version 6.0, 7000 Series or 8000 Series devices or device stacks in a high-availability pair), the system performs the update on the devices one at a time. When the update starts, the system applies the update one device at a time.

### Installing the Update on Stacked Devices

When you install an update on stacked devices, the system performs the updates simultaneously. Each device resumes normal operation when the update completes. Note that:

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

### After the Installation

After you perform the update on either the Firepower Management Center or managed devices, you **must** redeploy your configurations. Deployment 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 *Firepower Management Center Configuration Guide*.

There are several additional post-update steps you should take to ensure that your appliances are performing properly. These include:

- verifying that the update succeeded
- making sure that all appliances in your deployment are communicating successfully
- updating to the latest patch for Version 6.0, if available, to take advantage of the latest enhancements and security fixes
- optionally, updating your intrusion rules and vulnerability database (VDB) and redeploying your configurations
- making any required configuration changes based on the information in New Features and Functionality, page 5

The next sections include detailed instructions not only on performing the update, but also on completing any post-update steps. Make sure you complete all of the listed tasks.

## Updating Firepower Management Centers

**Caution: You `must` install the FireSIGHT System Version 6.0.0 Pre-Installation package prior to updating the Version 6.0. For more information, see the *FireSIGHT System Release Notes Version 6.0.0 Pre-Installation*.**

Use the procedure in this section to update your Firepower Management Centers, including virtual Firepower Management Centers. For the Version 6.0 update, Firepower Management Centers reboot.

**Caution: Before you update the Firepower Management Center, redeploy your configurations to any managed devices. Otherwise, the managed device update may fail.**

**Caution: Do not reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.**

**Note:** Updating a Firepower Management Center to Version 6.0 removes existing uninstallers from the appliance.

**Note:** The default password for Firepower Management Center and Firepower Management Center virtual appliances changes from `Sourcefire` to `Admin123` in Version 6.0 and later. For more information, see the Firepower Management Center Quick Start Guide.

### To update a Firepower Management Center:

**Step 1** Read these release notes and complete any required pre-update tasks.

**Note:** If the Firepower Management Center is running Version 5.4.1.1, Version 5.4.1.2, Version 5.4.1.3, Version 5.4.1.4, or Version 5.4.1.5 prior to updating to Version 6.0, you **must** install the Version 6.0 Pre-Installation Package prior to updating to Version 6.0. For more information, see Applying the Version 6.0 Pre-Installation Package, page 9.

**Note:** You need to break your Firepower Management Center high availability pairs and may need to install additional memory on your MC750, MC1500, or Firepower Management Center Virtual appliances prior to update. If your Firepower Management Center uses a custom HTTPS certificate that uses a `RSASSA-PSS` signature algorithm or was generated using a public key with more than 2048 bits, you may also need to generate and upload a new certificate or you will not be able to access the user interface on the Firepower Management Center after upgrade. For more information, see Before You Begin: Important Update and Compatibility Notes, page 9.

**Step 2** Download the update from the Support site:

- for Firepower Management Centers and Firepower Management Centers Virtual:

  `Sourcefire_3D_Defense_Center_S3_Upgrade-6.0.0-1010.sh`

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

**Step 3** Upload the update to the Firepower Management Center by selecting **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 4** Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 5** View the task queue (**System > Monitoring > Task Status**) 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. After the system update completes, to reduce clutter, remove the messages for these tasks from the Message Center.

**Step 6** Select **System > Updates**.

The Product Updates tab appears.

**Step 7** Click the install icon next to the update you uploaded.

The Install Update page appears.

**Step 8** Select 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 task queue (**System > Monitoring > Task Status**). However, after the Firepower Management Center completes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status page displays a progress bar and provides details about the script currently running.

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 Support. 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 Support.**

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

**Step 9** After the update finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

**Step 10** Log into the Firepower Management Center.

**Step 11** 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 12** Select **Help > About** and confirm that the software version is listed correctly: Version 6.0. Also note the versions of the intrusion rule update and VDB on the Firepower Management Center; you will need this information later.

**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** If the rule update available on the Support site is newer than the rules on your Firepower Management Center, import the newer rules. Do not auto-apply the imported rules at this time.

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

**Step 15** If the VDB available on the Support site is newer than the VDB on your Firepower Management Center, install the latest VDB.

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 *Firepower Management Center Configuration Guide*.

**Step 16** Redeploy your configurations to all managed devices.

Deployment 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 *Firepower Management Center Configuration Guide*.

**Step 17** If a patch for Version 6.0 is available on the Support site, apply the latest patch as described in the for that version.

**Caution: Updating a Firepower Management Center to Version 6.0 with managed devices running Version 5.4.0.6, Version 5.4.1.5, or earlier to Version 6.0 may cause traffic outages and system issues. You must disable the Retry URL cache miss lookup option in the Advanced Options section of the Access Control page to managed devices running Version 5.4.0.6, Version 5.4.1.5, or earlier prior to deploying configuration. For more information, see Preventing URL Cache Miss Lookup Retries, page 18.**

You **must** update to the latest patch to take advantage of the latest enhancements and security fixes.

# Preventing URL Cache Miss Lookup Retries

URL category determination can introduce up to two seconds of delay in packet delivery, depending on local network conditions. If such delay is not acceptable, URL retry should not be allowed.

When you allow URL retry, the system delays packets for URLs that have not been previously seen by the firewall while the URL category and reputation are determined so URL filtering rules can be resolved. Until the lookup of the URL category and reputation is completed, or the lookup request times out, in inline, routed, or transparent deployments the packet will be held at the firewall. If a two second time limit is reached without the category and reputation determination completing, the URL category Uncategorized is used with no reputation, and rule evaluation proceeds. Note that without URL retry, URL filtering may not be effective until such time as URL category and reputation determination completes for each URL. Until that time, packets that would have been filtered based on the URL's category or reputation will be filtered based on the Uncategorized category.

To disable URL retry on managed devices, disable the **Retry URL cache miss lookup** option in the General advanced settings of the access control policy (**Policies > Access Control > edit policy > Advanced >edit General Settings**) and redeploy the access control policy to the device. Note that this option is enabled and URL retry is not allowed by default.

# Updating Managed Devices and ASA FirePOWER Modules

After you update your Firepower Management Centers to Version 6.0, use them to update the devices they manage.

**Caution: Updating the system with managed devices running Version 5.4.0.5 or earlier to Version 6.0 may cause traffic outages and system issues. Prior to updating to Version 6.0, you `must` update managed devices to Version 5.4.0.6 or later prior to updating to Version 6.0.**

You must use a Firepower Management Center running Version 6.0 to update any managed device that does not have its own web interface. For ASA FirePOWER modules running on the ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X, you can update the module using the Firepower Management Center or connect to the ASA device and update the ASA FirePOWER module using local management via ASDM. For more information see the *Cisco ASA with FirePOWER Services Local Management Release Notes*.

Updating managed devices is a two-step process. First, download the update from the Support site and upload it to the managing Firepower Management Center. Next, install the software. You can update multiple devices at once, but only if they use the same update file.

For the Version 6.0 update, all devices reboot. 7000 Series and 8000 Series devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update, page 11.

**Caution: Before you update a managed device, use its managing Firepower Management Center to redeploy your configuration to the managed device. Otherwise, the managed device update may fail.**

**Caution: Do not reboot or shut down your appliances during the update until after you see the login prompt. The system may appear inactive during the pre-checks portion of the update; this is expected behavior and does not require you to reboot or shut down your appliances.**

### To update managed devices and ASA FirePOWER modules:

**Step 1** Read these release notes and complete any required pre-update tasks.

For more information, see Before You Begin: Important Update and Compatibility Notes, page 9.

**Note:** If the Series 3 deivces , NGIPSv devices, and ASA FirePOWER modules (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, and the ASA 5585-X-SSP-60) are running Version 5.4.0.2, Version 5.4.0.3, Version 5.4.0.4, Version 5.4.0.5, Version 5.4.0.6 or if the ASA FirePOWER modules (ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X) are running Version 5.4.1.1, Version 5.4.1.2, Version 5.4.1.3, Version 5.4.1.4, or Version 5.4.1.5, you **must** install the Version 6.0 Pre-Installation Package prior to updating to Version 6.0. For more information, see Applying the Version 6.0 Pre-Installation Package, page 9.

**Step 2** Update the software on the devices' managing Firepower Management Center; see Updating Firepower Management Centers, page 16.

**Step 3** Download the update from the Support site:

- for 7000 Series and 8000 Series managed devices:

  `Sourcefire_3D_Device_S3_Upgrade-6.0.0-1005.sh`

- for virtual managed devices:

  `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-6.0.0-1005.sh`

- for ASA FirePOWER modules :

  `Cisco_Network_Sensor_Upgrade-6.0.0-1005.sh`

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

**Step 4** Upload the update to the Firepower Management Center by selecting **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 5** Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 6** Click the install icon next to the update you are installing.

The Install Update page appears.

**Step 7** Select the devices where you want to install the update.

If you are updating a stacked pair, selecting one member of the pair automatically selects the other. You must update members of a stacked pair together.

**Step 8** Click **Install**. Confirm that you want to install the update and reboot the devices.

**Step 9** The update process begins. You can monitor the update's progress in the Firepower Management Center's task queue by clicking the System Status icon, then clicking the Tasks tab.

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 the Message Center indicates that the update has failed, or shows no progress on the update task for several minutes), do not restart the update. Instead, contact Support.**

**Step 10** Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 6.0.

**Step 11** Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 12** Redeploy your configurations to all managed devices.

Deployment 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 *Firepower Management Center User Guide*.

**Step 13** If a patch for Version 6.0 is available on the Support site, apply the latest patch as described in the for that version.

# Resolved Issues

You can view defects resolved in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required.

The following issues are resolved in Version 6.0:

- Security Issue Addressed a cross-site request forgery (CSRF) vulnerability.
- Security Issue Addressed a vulnerability that allowed an authenticated user can access system files using path traversal.
- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities, including those described in CVE-2015-0737, CVE-2015-4270, and CVE-2015-6353.
- Security Issue Addressed multiple cross-site scripting (XSS) and arbitrary HTML injection vulnerabilities including those described in CVE-2015-0707.
- Security Issue Addressed multiple vulnerability issues in MYSQL, DNS, NTP, and OpenSSL as described in CVE-2010-3614, CVE-2014-3569, CVE-2014-3570, CVE-2014-3572, CVE-2014-6568, CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296, CVE-2014-9297, CVE-2014-9298, CVE-2015-0205, CVE-2015-0287, CVE-2015-0292, CVE-2015-0374, CVE-2015-0381, CVE-2015-0382, CVE-2015-0385, CVE-2015-0391, CVE-2015-0409, CVE-2015-0411, CVE-2015-0432, CVE-2015-0498, CVE-2015-0505, CVE-2015-0506, CVE-2015-0507, CVE-2015-0511, CVE-2015-1798, CVE-2015-1799, CVE-2015-1499, CVE-2015-2566, CVE-2015-2567, CVE-2015-3405, CVE-2015-3676.
- Security Issue Addressed multiple vulnerability issues that generated denial of service in MYSQL, Linux, GNU C Library, NTP, XML, OpenSSL, and other third parties as described in CVE-2009-0696, CVE-2011-1155, CVE-2012-0876, CVE-2012-2807, CVE-2012-287, CVE-2012-3509, CVE-2012-3400, CVE-2012-3480, CVE-2012-5134, CVE-2013-0242, CVE-2013-1914, CVE-2013-4332, CVE-2013-4458, CVE-2014-3512, CVE-2014-3571, CVE-2014-3660, CVE-2014-6040, CVE-2014-8502, CVE-2015-0206, CVE-2015-0286, CVE-2015-0288, CVE-2015-0293, CVE-2015-1473, CVE-2015-1781, CVE-2015-1819.
- Security Issue Addressed multiple arbitrary script injection vulnerabilities allowing unauthenticated, remote attackers to exploit or overwrite functionality as described in CVE-2008-3075, CVE-2008-4101, CVE-2010-2252, CVE-2010-4494, CVE-2010-4651, CVE-2011-2716, CVE-2011-3102, CVE-2014-047, CVE-2014-4877, CVE-2014-5119, CVE-2014-7817, CVE-2015-1472, CVE-2015-6307.
- Security Issue Addressed multiple vulnerabilities in HTTP connection handling that allowed users to be redirected to malicious websites as described in CVE-2012-1033 and CVE-2015-0706.

- Security Issue Addressed multiple vulnerabilities that allowed unauthenticated, remote attacker to disclose sensitive information on an affected system, including those described in CVE-2011-1098 and CVE-2015-3153.
- Security Issue Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections, as described in CVE-2014-3556.
- Security Issue Addressed multiple parameter manipulation and misconfiguration vulnerabilities, including those described in CVE-2009-0025, CVE-2009-4022, and CVE-2015-0773.
- Security Issue Resolved multiple vulnerabilities where managed devices experienced microengine failure when processing traffic, including those described in CVE-2015-6307.
- Resolved an issue where, if the device did not process sufficient traffic, the system failed to generate complete performance graphs. (108348/CSCze87001)
- Resolved an issue where the intrusion performance graph incorrectly reported the minimum packets received instead of the actual number of packets received. (124331/CSCze87003)
- Resolved an issue where deploying a policy with a policy identification number greater than `4096` failed. (134385/CSCze89030)
- Resolved an issue which could have artificially limited the number of active dynamic NAT translations. (134561/CSCze87078)
- Resolved an issue where, in some cases, the front panel LCD informational screen of Firepower 7000 Series and 8000 Series devices incorrectly displayed some software errors as hardware errors. (140386/CSCze91939)
- Resolved an issue where the system did not display the number of failed login attempts. (140400/CSCze87152)
- Improved data pruning. (141894/ CSCze92576)
- Improved link state propagation responsiveness for Firepower 7000 Series and 8000 Series devices (143860/CSCze87386)
- Resolved an issue where, if you disabled an access control rule using an intrusion policy or variable set not used in any other rule and attempted to deploy the policy, deployment failed. (143872/CSCze87308)
- Improved URL filtering. (144198/CSCze94590, 144199/CSCze94758, 144685/CSCze94805)
- Resolved an issue where, if updating failed and you attempted to update again, some drives did not mount correctly during install. (144553/CSCze95696)
- Improved reporting. (145102/CSCze95656)
- Resolved an issue where the Discovery Statistics page did not include any events in the following rows of the statistics summary: **Total Events**, **Total Events Last Hour**, or **Total Events Last Day**. (145153/CSCze95751)
- Improved troubleshooting for Firepower 7000 Series and 8000 Series devices. (145187/CSCze95510)
- Resolved an issue where removing the URL Filtering license from your system caused a disruption in cloud connectivity. (144578/CSCze95183)
- Corrected the calculation used by the memory usage health monitor to prevent false alerts. (144593/CSCze94840)
- Resolved an issue where the passive interfaces on Firepower 7000 Series devices reported incorrect egress security zones and interfaces. (144624/CSCze95206)
- Resolved an issue where, if you edited the interface security zones on the Object Management page, the stacked device configuration appeared to be up-to-date when it wasn't. (144626/CSCze94847)
- Resolved an issue where, if you deployed to a cluster or device stack of Firepower 7000 Series or 8000 Series devices, the system only deployed to the primary device if the clustered or stacked devices contained out-of-date policies prior to latest policy apply. (144646/CSCze95167)
- Resolved an issue where, if you created an HTML report, the web browser incorrectly displayed the report as binary data.(144737/CSCze95180, 144738/CSCze95205)
- Resolved an issue where decrypted SSL sessions displayed URLs in connection logs as http:// instead of https://. (144785/CSCze95781)

- Resolved an issue where, if you created a custom network variable named identically to a default variable but with different capitalization, the system incorrectly assumed the custom variable and the default variable were the same and prevented you from deleting the custom variable. (44788/CSCze96160)
- Resolved an issue where the system treated DNS traffic as OpenVPN, QQ, and Viber traffic. (144789/CSCze96154)
- Resolved an issue where if you imported a policy that referenced a shared layer, importing the policy failed. (144946/CSCze96151)
- Improved disk space utilization. (145012/CSCze95309)
- Improved reliability of hardware acceleration in Firepower 7000 Series and 8000 Series devices. (145035/CSCze95433, 145509/CSCze95994, CSCus68624, CSCut53335, CSCut80043)
- Resolved an issue where, if you edited a local rule on the intrusion rule editor when viewing rule documentation, the system displayed the current local rule configuration for already-generated event data instead of the rule configuration that triggered it. (145118/CSCze95346)
- Resolved an issue where, if you generated an intrusion even performance graph with **Last Hour** set as the time range, the system incorrectly generated a blank graph. (145237/CSCze95774)
- Resolved an issue where, if you enabled remote storage and created a scheduled email alert response on your Firepower Management Center, the scheduled email alert disabled remote storage and remote storage backups failed. (145288/CSCze95993)
- Resolved an issue where, if you attempted to view the first or last event of an Indication of Compromise (IoC), the system did not locate the event. (145486/CSCze95786)
- Resolved an issue where the 40GB fiber NetMod traffic statistics incorrectly logged traffic on the wrong 40GB port. (145515/CSCze95830)
- Resolved an issue where access control rules containing web application conditions did not match against traffic if users on your network entered a URL into the address bar that was not all lowercase. (CSCur37364)
- Resolved an issue where the file trajectory page failed to load due to invalid subtypes. (CSCur38623)
- Resolved an issue where, in some cases, you were not able to retrieve URL category or URL reputation information. (CSCur38971)
- Resolved an issue where, if you did not deactivate a traffic profile before deleting it, the deleted profile continued to use resources when it should not. (CSCur48345)
- Resolved an issue where, if you created a custom workflow and attempted to open the packet view of an intrusion event, the system opened the incorrect intrusion event in the packet view. (CSCur48743)
- Resolved an issue where, in some cases, you could not edit your access control policy and the system generated an `Unknown Error (9999): Couldn't get a lock on /var/tmp/.ac_lock` error message. (CSCur55338)
- Resolved an issue where, if you created a scheduled task to install a new version of the vulnerability database (VDB) on a Firepower Management Center already running that version of the VDB, the system reinstalled the VDB and switched from active mode to standby mode every time the task was scheduled. (CSCur59252)
- Resolved an issue where, if you created a correlation rule to trigger when an intrusion event or connection event occurs and the condition matches an ingress security zone, egress security zone, ingress interfaces, or egress interface as the condition, the system did not recognize the rule and failed to generate events for traffic matching the rule. (CSCur59840)
- Resolved an issue on Firepower 7000 Series and 8000 Series managed devices where the system lost inline connectivity for up to 25 seconds on bypass-enabled inline sets during device reboot. (CSCur64678)
- You can now disable session termination logging to decrease disk space requirements. (CSCur73008)
- Resolved an issue where the system did not display the associated hosts if you expanded a vulnerability based on a client application from the vulnerabilities tab of the Network Map. (CSCur86191)
- Resolved an issue where, if you configured a routed interface on clustered Firepower 7000 Series or 8000 Series managed devices to both a private IP address and a Cisco Redundancy Protocol (SFRP) IP address, the system did not recognize which IP address was the primary address and did not establish an Open Shortest Path First (OSPF) connection. (CSCur86355)
- Resolved an issue where, if you changed the selected time zone in the Time Zone Preference tab on the User Preferences page, the system did not include daylight savings time. (CSCur92028)

- Resolved an issue where the system did not generate complete troubleshoot files if the system contained a large database. (CSCur97450)
- Resolved an issue where, in some cases, the host did not always display the block page if one of your access control rule actions was set to **Block** or **Interactive Block**. (CSCus06868)
- Resolved an issue where the system incorrectly duplicated the number of registered targets on the Intrusion Policy page. (CSCus08840)
- Resolved an issue where the system occasionally experienced latency during Snort restart. (CSCus11068)
- Resolved an issue where, an ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X device configured in monitor-only mode experienced a fail over if the device processed a high amount of traffic. (CSCus15229)
- Resolved an issue where the system did not support generating multiple report types when using Windows File Sharing (SMB) due to unsupported characters in the report name. (CSCus21871)
- Resolved an issue where, if you configured a domain name without a DNS entry, the web interface page did not load. (CSCus28155, CSCut89714)
- Resolved an issue where importing intrusion rules failed if you edited an intrusion policy. (CSCus29526)
- Resolved an issue where, if you created an SSL policy with the default actions set to **Do Not Decrypt** and attempted to establish a session, the system erroneously reported the session was blocked when it was not. (CSCus41127)
- Resolved an issue where, if you added a Cisco IOS remediation to your Cisco IOS Null Route instance and entered your password to log into the router, the device did not accept the password and remediation failed. (CSCus45769)
- Improved the optimization of certain event workflows. (CSCus52203)
- Resolved an issue where, if the intrusion policy had a sufficiently complex configuration, the system truncated the configuration and intrusion policy deployment failed. (CSCus53911)
- Improved memory utilization. (CSCus59008, CSCuu38535, CSCuu81679)
- Resolved an issue where, if you created an access control rule referencing a file policy with a **Block Malware** rule positioned after an access control rule containing a web application condition, the system did not identify malware files. (CSCus64393, CSCus6452)
- Resolved an issue where the system generated an `Internal Server Error` message if the password for your registered ASA FirePOWER module included an unsupported character. (CSCus68604)
- Resolved an issue where, if you configured both malware blocking and SSL decryption, you could not download files via HTTPS even if the files did not contain malware. (CSCus72505)
- Improved communication between Firepower Management Centers and managed devices. (CSCus79643)
- You can now deploy an access control policy containing both SSL policies and URL category conditions on a Firepower Management Center with a registered Firepower 7030 device. (CSCut02823)
- Resolved an issue where the system experienced latency when you deleted hosts from the network map. (CSCut02913)
- Improved pruning for correlation event tables. (CSCut02984)
- Resolved an issue where, if you created a file policy with Spero analysis and file capture enabled, the system did not capture files detected in incoming traffic. (CSCut06837)
- Resolved an issue where, if you restored a backup archive located on a Windows network file server (NFS), backup restoration failed. (CSCut08317)
- Resolved an issue where, if you deployed an access control policy referencing an SSL policy to a managed device with **Inspect Local Router Traffic** enabled, the system generated errors and experienced issues. (CSCut12631)
- Resolved an issue where deploying to a cluster of devices (in Version 6.0, known as high availability) caused the system to fail over when it should not. (CSCut12919)
- Resolved an issue where, if you created an access control rule configured to send connection events to an external syslog server and the rule matched an excessive amount of traffic, the managed device stopped sending events to the external syslog server. (CSCut14629)

- Resolved an issue where, if your intrusion policy layers shared identical names and you performed a system update, the system experienced issues. (CSCut16772)
- Improved network mapping generation when processing historical email and eStreamer events. (CSCut23688)
- Resolved an issue where, if you edited an access control rule with multiple URL category conditions and attempted to remove one of the conditions, the system removed only the first category condition listed. (CSCut25082)
- Resolved an issue where, in some cases, the Firepower Management Center experienced system issues and failed to load access control rules. (CSCut30047)
- Resolved an issue where, if you created a passive zone on a Firepower 8000 Series device and performed the `show fastpath-rules` CLI command, the system reported intrusion rules as inactive. (CSCut32479)
- Improved the reliability of backup and restore. (CSCut34456)
- The system generates a `Having Inspect traffic during policy apply disabled may cause network disruptions until deployment completes` warning if you deploy without enabling **Inpsect traffic during policy apply**. (CSCut36078)
- Resolved an issue where, if you created a file policy configured to **Inspect Archives**, the system experienced issues and stopped processing traffic. (CSCut39253, CSCuu14892)
- Resolved an issue where, if you selected one or more cells of the Original Client IP column in the intrusion events table view to review or copy, the system generated an error and did not display the rows you selected. (CSCut41458)
- Resolved an issue where the system experienced latency and did not match traffic if you created an access control rule targeting users in an LDAP group that contains a large number of access-controlled users. (CSCut56233)
- Resolved an issue where, if you created and edited a search for generated events, then canceled it before the search started, the system redirected you to the events page related to the search with the incorrect search name. (CSCut63265)
- Improved disk manager functionality. (CSCut65740)
- Resolved an issue where the system experienced issues if the last entry in the map list was a duplicate. (CSCut65738)
- Resolved an issue where importing intrusion rule updates caused system issues. (CSCut65772)
- Resolved an issue where, in some cases, the system dropped database communication and experienced errors. (CSCut71816)
- Resolved an issue where, in some cases, deploying on a Firepower Management Center with registered Firepower 7000 Series and 8000 Series devices in a high-availability pair caused a fail over. (CSCut72278)
- Improved health alert notifications for Cloud Lookup failures. (CSCut77594)
- Resolved an issue where, if your system experienced two sequential failures, the system was placed into bypass mode even if you did not enable bypass mode. (CSCut80892)
- Resolved an issue where the message column of the Retrospective Malware Events table view did not include the old disposition or the new disposition values of a retrospective malware event. (CSCut83512)
- Resolved an issue where, if you restarted your ASA 5585-X device with a large number of subinterfaces configured without also restarting the SFR5585-X service card, the SFR5585-X service card appeared to fail. (CSCut89619)
- Resolved an issue where using the `show managers` CLI command on a device registered to a system with multiple interfaces configured caused the system displayed the incorrect IP address. (CSCut95947)
- Resolved an issue where, in some cases, update failure did not get caught in time. (CSCuu01055)
- Resolved an issue where, if you experienced system issues, the cloud continuously checked for a new update. (CSCuu04844)
- Resolved an issue where, if you created an access control policy with a URL category condition and the network map failed to load a complete database, the system experienced issues. (CSCuu06714)
- Resolved an issue where the vulnerability database (VDB) install took an unexpectedly long time. (CSCuu06786)
- Resolved an issue where, in some cases, your Firepower Management Center stopped receiving health events from a registered device. (CSCuu18450)

- Resolved an issue where the system experienced latency if you created a link aggregation group (LAG) on a Firepower 7000 Series or 8000 Series device when connected to a Cisco Nexus 7000 switch. (CSCuu31626)
- Resolved an issue where, if you changed your system's time zone to a UTC+ zone and added a correlation rule with at least one inactive period to a correlation policy, activating the correlation rule failed. (CSCuu37600)
- Resolved an issue where you experienced connectivity issues if you created a routed interface on your clustered Firepower 7000 Series or 8000 Series device (known as high availability in Version 6.0). (CSCuu37668)
- Resolved an issue where the Cisco Redundancy Protocol (SFRP) router advertisement value appeared to be configurable when you added or edited a routed IP address when it was not. (CSCuu37687)
- Resolved an issue where, if you enabled two or more management interfaces and web client lost connectivity to one of the interfaces, the system defaulted to an incorrect gateway IP address and you could not access the interface. (CSCuu44020)
- Resolved an issue where, if you created an access control policy with a geolocation condition, traffic that should have matched the condition did not. (CSCuu48800)
- Improved network map generation. (CSCuu53215, CSCuu94784, CSCuv72386, CSCuw06359)
- Improved load time for access control rules with manual URL conditions referenced in an access control policy. (CSCuu55853)
- Resolved an issue where ASA Firepower modules (ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and ASA 5516-X) running the minimum ASA version 9.3.2.2 or later did not enforce the mpf-policy-map-class mode. (CSCuu68273)
- Resolved an issue where creating a search for an intrusion event with an original client IP using a negated subnet IP address caused the system to incorrectly exclude intrusion events with no original client IP. (CSCuu68438)
- Resolved an issue where, in rare cases, the system appeared unstable and did not recover from a reboot. (CSCuu93154)
- Resolved an issue where a drive failure on some DC4000 appliances caused RAID controller failure and data loss. (CSCuu93159)
- Improved eStreamer performance. (CSCuu94902)
- Resolved an issue where the system did not display the correct number of bytes in the Top Web Applications Seen and Top Client Applications Seen widgets on the Summary Dashboard if you viewed high-volume media such as video streaming on your web browser. (CSCuu97036)
- Resolved an issue where, if you deployed an SSL policy set to **Decrypt-Resign** on a managed device, the decrypted traffic that egressed from one interface set switched or routed so the traffic ingressed into a different interface set on the same managed device and the system experienced a disruption in SSL traffic. (CSCuu97712)
- Resolved an issue where the **Send email** check box on the Report Templates tab of the Reporting page did not stay selected and you stopped receiving reports via email if you generated a report, navigated away from the Report Templates tab, and then generated another report. (CSCuu97750, CSCuu41580, CSCuv43116)
- Resolved an issue where clicking **Continue** on interactive block web page did not always redirect you to the blocked web page. (CSCuu97934, CSCuu97946)
- Resolved an issue where, in some cases, updating failed. (CSCuu99337)
- Resolved an issue where the system did not acknowledge users as members of their primary LDAP groups. (CSCuv03821)
- Resolved an issue where, if you generated a connection event report and modified the **Maximum Results** value, the system did not save the new value and generated the report with the default value. (CSCuv06557)
- Resolved an issue where, if you configured the system to use a remote NTP server to synchronize time to a system with a managed device running a version older than Version 5.4 and you experienced a leap second, your system used a high amount of CPU. (CSCuv11738)
- Resolved an issue where, if you created an access control rule configured with an Interactive Block action and you viewed a blocked webpage in a Chrome web browser, the **Continue** button to bypass the block page did not work. (CSCuv21748)
- Resolved an issue where generated internal CA certificates were valid for only 30 days instead of 10 years. (CSCuv29004)

- Resolved an issue where, if a host generated an Indication of Compromise (IoC) and you disabled the IoC for that host on the Host Profile page, the Indications of Compromise by Host dashboard widget incorrectly displayed the IoC when it should not. (CSCuv41376)
- Resolved an issue where, if you created an SSL policy default action set to **Decrypt - Known Key** or **Decrypt - Resign** on a 7000 Series or 8000 Series device and you choose to resume the SSL session with a different source IP address, SSL inspection failed and the connection log displayed an incorrect SSL policy default action. (CSCuv48689)
- Improved file detection and blocking. (CSCuv59181)
- Improved memory utilization for port ranges in access control rules. (CSCuv64114)
- Resolved an issue where, if you registered many devices or configured many interfaces on a managed device or created many VPN deployments, the system did not generate information for all of the devices or interfaces or VPN deployments on their respective pages. (CSCuv76287)
- Improved Health Monitor alerting. (CSCuv96121)
- Resolved an issue where merging intrusion policy layers generated errors. (CSCuw34380)
- Improved email notification reliability. (CSCuw36354)
- Resolved an issue where, in some cases, the system experienced errors caused by invalid username values. (CSCuw39725)
- Resolved an issue where, if you switched from Serial Over Lan (SOL) to Lights-out-Management (LOM) on a MC4000, or vice versa, the system's console port did not work. (CSCuw67319)
- Resolved an issue where, if you enabled SSL debug logging via the `system support ssl-debug` or `system support debug-DAQ-NSE` CLI command and your system experienced a high amount of traffic for an extended amount of time, the system experienced disk space issues. (CSCuw68004)
- Resolved an issue where, if you deployed a file policy with the default action set to **Malware Block** and the system detected SMB traffic, the system experienced issues. (CSCux49653)

# Known Issues

You can view known issues reported in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required.

The following known issues are reported in Version 6.0:

- If you plan on updating the Firepower Management Center from Version 5.4.0.2 or later to Version 6.0, we **strongly** recommend installing the FireSIGHT System Version 6.0.0 Pre-Installation package prior to updating the Version 6.0. For more information, see the *FireSIGHT System Release Notes Version 6.0.0 Pre-Installation Package*.
- You may experience latency if you use Firefox version 38.0.1 to view your Firepower Management Center's interface. As a workaround, use Firefox 41 or later or use a different web browser. (CSCuv11830)
- In some cases, if you create an access control policy when registering a device on a subdomain, the system creates the access control policy in the global domain instead of the subdomain when it should not. (CSCut56951)
- In some cases, if you edit the default network access policy in the advanced tab of the Access Control page (**Policies > Access Control**), the system incorrectly displays the default network access policy as an intrusion policy on the deployment dialog window. (CSCuv48221)
- Online help does not open if you click the help icon on the Select Comparison page (**ASA FirePOWER Configuration > Policies > Files > Compare Policies**) of an ASA FirePOWER module managed via ASDM. (CSCuw21863)
- In some cases, if you view **All Events (Not Dropped)** in the Intrusion Events table view page of a Firepower 7000 Series or 8000 Series device and sort the table by a maximum of six fields including **Review By** and **Count** and then generate a report, report generation fails. As a workaround, exclude either the **Review By** and **Count** field values or, if you include both the **Review By** and **Count** fields, only nor more than three additional field values when generating a report from the intrusion events page. (CSCuw29993)

- You cannot name a device group with a name that includes the plus ( `+` ) character even though the system generates a `This field contains invalid characters. Only alphanumerics, hyphen ( - ), underscore ( _ ), period ( . ), and plus ( + ) are allowed` message. (CSCuw44373)
- In some cases, if you edit the browser and shell timeout threshold values on the Shell Timeout page (**System > Configuration > Shell Timeout**) and redeploy, the system logs out of inactive Firepower Management Centers up to one minute after the configured threshold values. (CSCuw48568)
- In some cases, editing a file list in a domain causes any file policy in that domain to be marked out-of-date. (CSCuw52764)
- The Device Management page (**Devices > Device Management**) does not display device override values in the tooltip for device objects. (CSCuw53371)
- External certificates from Version 5.4.x are not supported in Version 6.0: the only curves supported in Version 6.0 are `prime192v1`, `prime256v1`,`secp384r1` and `secp521r1`. You must update your system to Version 6.0 to obtain supported external certificates. (CSCuw54749)
- In some cases, if you create an access control policy referencing both a file policy containing a file rule configured to **Detect Files** and an SSL policy configured to **Decrypt--Resign** or **Decrypt--known key** on a system sending and receiving emails with Outlook 2013, the Connection Events page (**Analysis > Connections > Events**) does not include email file attachments in generated events. (CSCuw65152)
- In some cases, if you refresh the tabs in the Device Management page (**Devices > Device Management**) or the NAT page (**Devices > NAT**) or the VPN page (**Devices > VPN**), the system does not clear the cache on the page being refreshed and the **Save** button is un-operational. As a workaround, cancel any edits made to the page or tab and select the device you want to edit again. (CSCuw75367)
- In some cases, if you create an SSL policy containing a certificate with more than one status, such as expired or revoked, the Certificate Status column of the Connection Events page (**Analysis > Connections > Events**) does not display a status. (CSCuw76040)
- In rare cases, if you create or edit a device interface on the Device Management page (**Devices > Devices Management**), the system generates a `No cache exists to discard and resume` error and you cannot deploy. As a workaround, refresh the Device Management page and redeploy. (CSCuw77505)
- In some cases, if you incorrectly configure OSPFv3, RIP or Border Gateway Protocol on a device's virtual router page (**Devices > Devices Management > Virtual Router**) and leave the configuration page without saving changes, the system generates a **To revert back the configuration** pop-up; click **Yes** to clean the virtual router configuration page of any edits or click **No** causes the system to generate the **To revert back the configuration** pop-up multiple times before saving the virtual router configuration page without any edits. (CSCuw78916)
- If you deploy a network discovery policy to a clustered or stacked Firepower 7000 Series or 8000 Series devices (in Version 6.0 known as a high availability pair), the system incorrectly counts all devices in the cluster or stack rather than indicating one device for the cluster or stack. (CSCuw79241, CSCuw79243)
- After initial setup on a Firepower Management Center, Firepower 7000 Series, or 8000 Series device, if you are connecting to the appliance from behind a network address translator (NAT) device, the system provides a redirect URL containing the IP address for the IP address you configured for the appliance rather than the NAT IP you are connecting to, and the session times out. As a workaround, correct the URL to use the NAT IP used to connect via web. (CSCuw79967)
- If you uninstall Version 5.4.1.3 or later to an earlier 5.4.x version and then update the system to Version 6.0, the update to Version 6.0 fails. Update your system to the latest version prior to updating your system to Version 6.0. (CSCuw81780)
- In some cases, if you do not select the required licenses for a device prior to device registration, the system generates an `Initial policy deployment not started due to validation errors. For details, redeploy manually` message. For more information on the correct licenses to select for your device, see the Licensing the FireSIGHT System chapter of the *Firepower Management Center Configuration Guide*. (CSCuw85743)
- In some cases, if you deploy a NAT policy containing rules targeted to Firepower 7000 Series or 8000 Series managed devices' routed interfaces and then cluster the managed devices (known is Version 6.0 as a high-availability pair), some NAT rules continue to target a managed device's routed interface instead of changing to target a high availability interface when it should. As a workaround, edit the rule containing the individual interface, manually create a high availability interface, then redeploy. (CSCuw89223)
- The HTTP Listing page (**Device > Platform Settings > Firepower Threat Defense Platform Settings > HTTP**) lists **Authentication Certificate** as a configurable field when it is not. (CSCuw89605)

- In some cases, the system generates events for large amounts of HTTP traffic processed by a port that is not specified in the HTTP preprocessor rule. As a workaround, add the port to the HTTP preprocessor rule with GID `119` and SID `15`. (CSCuw90033)
- If you initiate deployment while backing up the Firepower Management Center, a message does not appear to indicate that the communication channel is blocked and the policy cannot deploy. Wait until backup process is complete and then deploy. (CSCuw90629)
- In some cases, if you create an access control policy that has an intrusion policy as the default action, the variable set icon next to the default action does not display properly. As a workaround, change the default action to use a different intrusion policy, which makes the icon show up, and then change your default action back to the previous intrusion policy. (CSCuw94067)
- In some cases, the Firepower Management Center's Deploy window displays an incorrect timestamp after you update the Firepower Management Center to Version 6.0 and deploy configuration changes. (CSCuw94083)
- In some cases, if you create an OSPFv3 router but do not configure a manual router-id in the Advanced Settings tab of the router page (**Devices > Device Management > Router**), the system does not use unnamed IPv4 IP addresses and generates an `OPSFv3 router process will not start as no router ID has been configured. Neither router ID in OSPFv3 nor IPv4 address configured in Interfaces` error message. (CSCuw95485)
- If you create a correlation rule configured to match a **MAC Vendor is** condition, the system generates a `Warning: no vendors match this string` warning and does not execute the correlation rule. As a workaround, update your vulnerability database (VDB). If the VDB update does not resolve the issue, use the **MAC Vendor contains** condition instead of the **MAC Vendor is** condition. (CSCuw96022)
- The link to the Cisco Smart Software Manager from the Firepower Management Center Smart Licensing user interface page (**System > Local > System Policy**) directs to an updated link, which also redirects. As a workaround, if the redirect does not occur quickly enough, connect to https://software.cisco.com/#module/SmartLicensing. (CSCuw96552)
- In some cases, deploy fails on a device running Version 5.4.0 that is registered to a Firepower Management Center running Version 6.0 if you deploy an access control policy that references a file policy configured for malware protection. (CSCuw97809)
- In some cases, if you enable sensitive data detection in the Advanced Settings on the Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**), then switch to another domain before saving, the system does not reload the Intrusion Policy page in the destination domain when it should. As a workaround, save or manually reload the Intrusion Policy page. (CSCuw97864)
- In some cases, if the time configured on a device running Version 6.0 is set ahead of the time configured on a Firepower Management Center, registering the managed device to the Firepower Management Center causes issues restoring connectivity. As a workaround, execute the `/etc/rc.d/init.d/pm restart` CLI command. If you continue to experience connectivity issues, contact Support. (CSCuw97948)
- In some cases, if the time configured on a device running Version 6.0 is set ahead of the time configured on a Firepower Management Center, registering the managed device to the Firepower Management Center causes connectivity issues and the system may not be able to restore connectivity. As a workaround, execute the `/etc/rc.d/init.d/pm restart` CLI command. If you continue to experience connectivity issues, contact Support. (CSCuw97948)
- In some cases, if your user interface initiates a restore, the session will be disconnected and you must log in again to see the status of restore operation. (CSCuw98296)
- In some cases, if you create two subdomains on a Firepower Management Center running Version 6.0 and register a 7000 Series or 8000 Series device, create a network object override and deploy an access control policy, then move the device from one subdomain to another subdomain, the system deletes the override value from the Object page. (CSCuw98708)
- Version 6.0 does not support the Safari web browser on systems running the MAC OS. Use Firefox, Chrome, or Internet Explorer. (CSCuw98876)
- In some cases, if the system hosting a virtual device experiences a high amount of traffic, deploying to the virtual device may cause temporary network issues. (CSCux00380)
- In some cases, intrusion events do not display the correct source IP address or the correct destination IP address. As a workaround, view the Connection Events page (**Analysis > Connections > Events**) to view the correct source and destination IP addresses of an intrusion event. (CSCux00385)
- In some cases pinholes are not created for Real-time Transport Protocol (RTP) connections established by calls using the Session Initiation Protocol (SIP), which prevents the VOIP channel creation for the SIP call. (CSCux03758, CSCux09765)

- Although an application detector is available for the Skinny (SCCP) protocol, pinholes are not created for RTP connections established by SCCP packets. (CSCux05468)
- In some cases, when deploying policies to a large number of devices, policy deployment times out and fails when Snort fails to restart. (CSCux07861)
- If you deploy a NAT policy which resides in a subdomain to a Firepower 7000 Series or 8000 Series device and move the device to new domain, deploy fails. As a workaround, create a new NAT policy in a new domain and target the correct device, then redeploy. (CSCux10651)
- In some cases, if you create a VPN deployment on a registered device and move the device from one domain to another domain, then deploy, deploy fails and the system generates a `Pre-deploy Global Configuration Generation. Cannot find policy information` error message. As a workaround, remove the VPN configuration prior to moving the device to another domain. An alternative workaround is to unregister and then register the device to the Firepower Management Center, then create a VPN deployment and deploy. (CSCux10820)
- Use of a certificate with an RSASSA-PSS signature algorithm on a Firepower Management Centerr is not supported in Version 6.0. If you update a Firepower Management Center using such a certificate to Version 6.0 or add such a certificate in Version 6.0, the system does not allow you to log into the Management Center web interface and generates an `Unable to authorize access. If you continue to have difficulty accessing this device, please contact the system administrator` error. As a workaround, prior to update, generate and install an SSL certificate with either a `sha1WithRSAEncryption` or `sha256WithRSAEncryption` algorithm and restart the Firepower Management Center, or use the default Firepower Management Center certificate and restart the appliance. If you are unable to access the user interface on your Firepower Management Center, contact Support. (CSCux30610)
- In some cases, if you create an access control policy referencing an SSL policy that contains a network object with multiple entries on a managed Firepower appliance running Version 5.4 or later and you update the system to Version 6.0, deploying the policy fails on a Firepower Management Center running Version 6.0. As a workaround, edit the SSL policy after updating the system to Version 6.0 and remove the network object, then add the network object and redeploy. (CSCux31618)
- If the certificate used by your Firepower Management Center was generated using a public server key larger than 2048 bits, you will not be able to log into the Firepower Management Center web interface after updating to Version 6.0. As a workaround, replace certificates that were created with larger public keys by generating a server certificate request and then applying a certificate generated using that request to the Firepower Management Center. You can do the server certificate request and the certificate upload through the local configuration settings on the Firepower Management Center (**System > Local > Configuration > HTTPS Certificate**). If you generate a certificate without using a CSR from the Firepower Management Center, use a public key of 2048 bits or less. If you generate a certificate that contains more than 2048 bits and lose access to the Management Center web interface, contact Support. (CSCux35430)
- In some cases, if you deployed an access control policy that contains a custom URL, the CPU experienced high usage and the system experienced issues. (CSCux35554)
- If a device running Firepower Threat Defense is registered to a Firepower Management Center running Version 6.0 ten days or more, the system experiences the following issues: registering a new device the Firepower Management Center generates a `CSM failed state: (2) CSM can not provide device state (2)` error and device registration fails; updating the Firepower Management Center from 6.0.0 to a later version generates an `Installation failed. Peer discovery incomplete. Please retry after few moments` error and the update fails; backing up the Firepower Management Center generates a `Registration or CSM state are blocking backup` error and backup fails; attempting to create, update, or delete a domain on the Firepower Management Center generates an A `sensor registration process is running. Please wait until process completes.` error and the system does not successfully create, update, or delete the selected domain. As a workaround, download the install file for Version 6.0 through the Firepower Management Center and execute the `/usr/local/sf/bin/install_update.pl /var/sf/updates/[UPGRADE_PKG_NAME].sh` CLI command as the root user to update the Firepower Management Center to Version 6.0 instead of updating through the web interface. (CSCux89875)
- Environments with multiple user accounts with same email address scrambles/crashes SFDataCorrelator. (CSCvf56267)
- 256 low block count leads to traffic failures due to alloc to inspect snort. (CSCvg45236)

# For Assistance

Thank you for choosing the Firepower System.

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about the Firepower System, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/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 or require assistance with the Firepower System, please contact Cisco Support:

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.