FireSIGHT System Release Notes

Version 5.4.0.10 and Version 5.4.1.9
First Published: March 6, 2017
Last Updated: September 17, 2020

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, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation and uninstallation instructions for the following appliances:

- Series 3 Defense Centers (the DC750, DC1500, DC2000, DC3500, and the DC4000)
- Series 3 managed devices (the 3D7010, 3D7020, 3D7030, 3D7050, 3D7110, 3D7115, 3D7120, 3D7125, 3D8120, 3D8130, 3D8140, 3D8250, 3D8260, 3D8270, 3D8290, 3D8350, 3D8360, 3D8370, 3D8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, and the AMP8390)
- Cisco ASA with FirePOWER Services (the ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60, and the ISA 3000)
- 64-bit virtual Defense Centers and managed devices

Tip: For detailed information on the FireSIGHT System, refer to the online help or download the *FireSIGHT System User Guide* from the Support site.

These release notes are valid for Version 5.4.0.10 and Version 5.4.1.9 of the FireSIGHT System. You can update physical and virtual managed devices to Version 5.4.0.10. You can update Cisco ASA FirePOWER modules, physical Defense Center, and virtual Defense Centers to Version 5.4.1.9. Note that you can update appliances in the following manner:

- Defense Centers (the DC750, DC1500, DC2000, DC3500, and the DC4000) must be running Version 5.4.0 to update to Version 5.4.1.9. If your Defense Center is running an earlier version, you must update to Version 5.4.0 before updating to Version 5.4.1.9.

  Note: A Defense Center may update its devices while running Version 5.4.0, but you will be unable to decrypt or inspect SSL traffic if your Defense Center remains at Version 5.4.0. If you plan on decrypting or inspecting SSL traffic, update your Defense Center to Version 5.4.1 or later.

- Series 3 devices (the 3D7010, 3D7020, 3D7030, 3D7050, 3D7110, 3D7115, 3D7120, 3D7125, 3D8120, 3D8130, 3D8140, 3D8250, 3D8260, 3D8270, 3D8290, 3D8350, 3D8360, 3D8370, 3D8390, AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, and the AMP8390) must be running Version 5.4.0.5 to update to Version 5.4.0.10. If your Series 3 device is running an earlier version, you must update to Version 5.4.0.5 before updating to Version 5.4.0.10.
- ASA FirePOWER modules (the ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60) must be running at least Version 5.4.0.5 to update to Version 5.4.0.10. If your ASA FirePOWER module is running an earlier version, you must update to Version 5.4.0.5 before updating to Version 5.4.0.10.

- ASA FirePOWER modules (ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X) must be running at least Version 5.4.1.4 before updating to Version 5.4.1.9. The ISA 3000 must be running at least Version 5.4.1.7 before updating to Version 5.4.1.9. See the *Cisco ASA FirePOWER Module Quick Start Guide* for more information on deploying and installing the module.

For more information, see the following sections:

New Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 5.4.0.10 and Version 5.4.1.9 of the FireSIGHT System:

For detailed information, see the *FireSIGHT System User Guide*, *FireSIGHT System Installation Guide*, *FireSIGHT System Virtual Installation Guide*, and *Installation and Configuration Guide*.

Terminology

The terminology used in Version 5.4.1.9 and Version 5.4.0.10 may differ from the terminology used in previous releases. For more information, see the Firepower Compatibility Guide.

Table 1 Changes to Terminology

Version 5.4.0.10 and Version 5.4.1.9 Terminology	Description
Cisco	Formerly *Sourcefire*
FireSIGHT System	Formerly *Sourcefire 3D System*
Defense Center FireSIGHT Defense Center Cisco FireSIGHT Management Center	Formerly *Sourcefire Defense Center*
device managed device	Formerly *Sourcefire managed device*
FireSIGHT managed devices	Refers to all devices managed by a FireSIGHT Defense Center (managed devices and ASA devices)

Table 1 Changes to Terminology (continued)

Version 5.4.0.10 and Version 5.4.1.9 Terminology	Description
Cisco Adaptive Security Appliance (ASA) ASA device	Refers to the Cisco ASA hardware
Cisco ASA with FirePOWER Services	Refers to ASA devices with the ASA FirePOWER module installed
ASA FirePOWER module	Refers to the hardware and software modules installed on compatible ASA devices
ASA software	Refers to the base software installed on Cisco ASA devices
Adaptive Security Device Management (ASDM)	Refers to the Adaptive Security Device Manager used to manage ASA functionality
Direct management	Refers to management of the ASA FirePOWER module using ASDM
Centralized management	Refers to management of the ASA FirePOWER module using a FireSIGHT Defense Center

Tip: Cisco documentation may refer to the Defense Center as the FireSIGHT Management Center. The Defense Center and the FireSIGHT Management Center are the same appliance.

Changed Functionality

There is no changed functionality in Version 5.4.0.10 or Version 5.4.1.9.

Features and Functionality Introduced in Previous Versions

Version 5.4.1.1

Dedicated AMP Appliances

Version 5.4 introduces a new Series 3 FirePOWER managed devices designed with additional processing power to maximize the performance of the FireSIGHT System's AMP features. The AMP8050 is a 81xx Family device with support for Netmods and includes the additional storage necessary to function as a dedicated AMP appliance. The AMP8350 is an 83xx Family device also with support for Netmods and the additional storage required for AMP functionality. The AMP8350 model can be used as a stacked unit with the AMP8360, AMP8370, and AMP8390, for 2, 3, and 4 stacks, respectively.

Version 5.4.1

FirePOWER Services Management Capabilities

Centralized Management of Cisco ASA5506-X with FirePOWER Services

The Defense Center is now able to manage FirePOWER Services (ASA FirePOWER devices) implementations running on ASA5506-X devices in the same way it does on all of the other ASA5500-X devices. This enables the management of multiple ASA5506-X devices running ASA FirePOWER devices from a single Defense Center, as long as the ASA platform is running Version 9.3.2.2 or later and the ASA FirePOWER device is running Version 5.4.1 or later. Administrators will be able to configure intrusion detection and prevention policies, advanced malware protection, application control, user and group control, file control, and URL filtering and then apply those configurations to multiple ASA5506-X devices all at once. In addition, Defense Centers provide critical dashboards, event views, alerting capabilities, and reporting from all of your ASA FirePOWER devices in a single view.

Direct Management of Cisco ASA5506-X with FirePOWER Services

Cisco's Adaptive Security Device Manager (ASDM) can be used to perform the same ASA FirePOWER management functions listed above, but only on one ASA5506-X device at a time. In addition, you can manage system policies, licensing, and back up and restore directly.

Management Limitations of Cisco ASA with FirePOWER Services

At the current time, the Cisco ASA FirePOWER product consists of two different products tightly integrated with each other: the ASA Firewall and the FirePOWER Next-Generation Intrusion Prevention System (NGIPS). Whereas critical data sharing between the two has been accomplished, a unified management platform is still in development.

For this reason, the Cisco ASA functionality is currently managed through the Cisco Security Manager (CSM) or the Adaptive Security Device Manager (ASDM), and the FirePOWER Services functionality is managed through the Cisco Defense Center. As a result, the Defense Center does not support any of the following capabilities:

- Cisco ASA hardware-based features, including clustering, stacking, switching, routing, virtual private networks (VPN), and network address translation (NAT).
- Configuring ASA interfaces. In addition, when FirePOWER Services are deployed in SPAN port mode, any ASA interfaces that have been configured will not be displayed.
- Shutting down, restarting or otherwise managing ASA processes.
- Creating or restoring backups from ASA devices.
- Writing access control rules to match traffic using VLAN tag conditions.

Note: The ASA platform provides these features, configured using the ASA command line interface (CLI) and ASDM. For more information, see the ASA FirePOWER module documentation.

Platform Enhancements

VMware Tool Support

You can now use VMware Tools with FireSIGHT System virtual appliances. This enhances compatibility with the VMware environment and improves management of virtual devices by enabling soft power down, migration, and other virtual specific capabilities. VMware tools are supported on:

- 64-bit Virtual Defense Center
- 64-bit Virtual managed device

Note: As of Version 5.4 of the FireSIGHT System, the system supports ESXi Version 5.0, 5.1, and 5.5.

Support for VMXNET3 Interfaces in VMware Virtual Appliances

VMXNET3 interface types are now supported on virtual devices. This allows you to use high-speed network interfaces, up to 10Gbits/s.

Multiple Management Interfaces

You can now use multiple management interface ports on Series 3 Defense Centers, FirePOWER (Series 3) managed devices, and virtual Defense Centers. You can set one interface for management traffic and another interface for event traffic. This improves deployment options in some environments.

Series 3 Support

Version 5.4 introduces the 3D7050 as a 70xx Family device with a dual core quad thread processor, 8GB of RAM, and a 80GB hard drive.

LACP Support

FirePOWER (Series 3) devices are now able to take part in Link Aggregation Control Protocol (LACP) (IEEE 802.3ad) negotiation to aggregate multiple links together into one. This allows both link redundancy and bandwidth sharing.

Defense Center 2000 (DC2000)

The DC2000 is a new Defense Center appliance platform that offers double the performance and capacity of the DC1500.

Defense Center 4000 (DC4000)

The DC4000 is a new Defense Center appliance platform that offers double the performance and capacity of the DC3500.

International Compatibility Enhancements

Unicode Support

The system now displays the names of files detected through file detection, malware detection, and FireAMP file events. This allows the display of non-Western characters, including those that are double-byte encoded.

Geolocation and Security Intelligence Data in Correlation Rules

The correlation rules engine has been updated to make connection, geolocation, and Security Intelligence data available. This allows you to generate correlated events or take correlated actions based on these two new constraints. For example, if an `Impact 1` intrusion event is detected from a specific country, you can set up an alert to log that information to an external syslog server.

Support for Private FireAMP Cloud

With Version 5.4, you can use a private FireAMP cloud rather than the Cisco public cloud. This requires installation of a private cloud virtual appliance. The private cloud mediates interactions with the public cloud so you can gather collected threat information from the public cloud without exposing information from your network.

The following features and functionality were updated in Version 5.4:

Detection and Security Enhancements

Integrated SSL Decryption

FirePOWER (Series 3) devices can now identify SSL communications and decrypt the traffic before applying attack, application, and malware detection. You can use SSL decryption in any of the supported Series 3 device deployment modes, including inline and passive. SSL policies control characteristics of SSL in use within the enterprise, with SSL rules to exert granular control over encrypted traffic logging and handling.

Simplified Normalization and Preprocessor Configuration

You now configure traffic normalization and preprocessing in the access control policy, rather than the intrusion policy. This simplifies configuration, especially for new users. The sensitive data preprocessor, rule states, alerting, and event thresholds can still be configured at an individual intrusion policy level.

New file_type Keyword in the Snort Rule Language

A new **file_type** keyword is available in the Snort rules language that enables the specification of a file type for detection. This is a streamlined alternative to the existing **flowbits**-driven method.

Expanded IoC support from FireAMP Connectors

The list of Indicators of Compromise (IoC) provided by FireAMP is now dynamic and data-driven. As new IoCs become available, they are automatically supported by the Defense Center. This enhances the IoC correlation capability in any deployment where FireAMP is used.

Protected Rule Content

A new capability of the Snort rule language is available for use in high-security environments. You can now create a Snort content match using hashed data. This allows the rule writer to specify what content to search for, but never exposes the content in plain text.

Previously Changed Functionality

The following functionality was introduced in Version 5.4.0.7 and 5.4.1.6:

- SCADA preprocessor now supports processing Common Industrialist Protocol (CIP) traffic. CIP configuration is not enabled by default. For more information, see the Configuring SCADA Preprocessing section of the FireSIGHT System User guide. (CSCux85466, CSCuy08100, CSCuy08741)

The following functionality was introduced in Version 5.4.0.6 and 5.4.1.5:

- If the system detects a URL and cannot categorize the requested URL from prior lookup results, the system attempts a secondary URL lookup method. If the URL cannot be categorized within two seconds using the secondary URL lookup method, the system assigns the URL the Uncategorized category and processes the URL.
- The SMTP preprocessor now generates an alert for multi-line authentication command overflow attempts.
- The system now restricts reassembly of packets once the system reaches the max HTTP server flow depth and decreases latency in traffic processing.

The following functionality was introduced in Version 5.4.0.5 and Version 5.4.1.4:

- VLAN tags are now limited to integers between 0 and 4095.
- The system now supports matching SSL traffic on all port values, including values 32,768 and larger.

If the system detects a URL and cannot categorize the requested URL from prior lookup results, the system attempts a secondary URL lookup method. If the URL can not be categorized within two seconds using the secondary URL lookup method, the system assigns the URL the **Uncategorized** category and processes the URL.

The following functionality was introduced in Version 5.4.0.3 and Version 5.4.1.2:

- You must apply the same access control policy to all devices that you plan to stack or cluster before you configure the stack or cluster except in cases where an applied configuration requires the Snort process to restart. See the How Snort Restarts Affect Traffic section in the *FireSIGHT System User Guide*.
- You are now able to choose to inspect traffic during policy apply to prevent network disruption.
- The system no longer reports the discovery event status to the Health Policy page.
- You can now create an access control policy that references either an access control rule network condition set to block all IPv6 addresses with ::/0 or a network rule set to block all IPv4 addresses with 0.0.0.0/0 is now supported.
- The system now reports an event for all CPU reports when CPU usage changes from a high level to a normal state.

The following functionality was introduced in Version 5.4.0.2 and Version 5.4.1.1:

- The system now clears all intrusion policy locks when you upload intrusion rules or install intrusion rule updates.

The following functionality was introduced in Version 5.4.1:

- Registered ASA devices now have configurable advanced options on the Advanced tab of the Device Management page (**Devices > Device Management**).
- The **show users** CLI command is now supported on ASA devices.
- You can configure alerts only for retrospective events or network-based malware events from the Advanced Malware Protections Alerts tab on the Alerts page.

The following features and functionality were updated in Version 5.4:

- You can now view VLAN tags for connection events in the event viewer (**Analysis > Connections > Events**).
- The system now identifies login attempts over the FTP, HTTP, and MDNS protocols.

- You can now select archived connection events separately from discovery events for transmission to the eStreamer client.
- The Discovery Event Health Monitor is no longer available in health policies.
- Expand Packet View, previously available in Version 4.10.x, is now a configurable option in Version 5.4 with the Event View Settings tab (**Admin > User Preferences > Event View Settings**).
- Importing a custom intrusion rule as an **.rtf** file now generates an **Invalid Rules File 'rtf_rule.rtf': Must be a plain text file that is ASCII or UTF-8 encoded** warning.
- You can now generate the following intrusion event performance graphs with the Intrusion Event Graphs page (**Overview > Summary > Intrusion Event Graphs**):
  - ECN Flags Normalized in TCP Traffic/Packet
  - ECN Flags Normalized in TCP Traffic/Session
  - ICMPv4 Echo Normalizations
  - ICMPv6 Echo Normalizations
  - IPv4 DF Flag Normalizations
  - IPv4 Options Normalizations
  - IPv4 Reserved Flag Normalizations
  - IPv4 Resize Normalizations
  - IPv4 TOS Normalizations
  - IPv4 TTL Normalizations
  - IPv6 TTL Normalizations
  - IPv6 Options Normalizations
  - TCP Header Padding Normalizations
  - TCP No Option Normalizations
  - TCP NS Flag Normalizations
  - TCP Options Normalizations
  - TCP Packets Blocked by Normalization
  - TCP Reserved Flags Normalizations
  - TCP Segment Reassembly Normalizations
  - TCP SYN Option Normalizations
  - Total TCP Filtered Packets
  - TCP Timestamp ECR Normalizations
  - Total UDP Filtered Packets
  - TCP Urgent Flag Normalizations

- You can now configure the **HTTP Referrer** and **User Agent** fields in the Connection Events table view and the Security Intelligence Events table view when configuring the displayed columns.
- You can now view warnings associated with the individual rules of your access control policy with the Access Control Policy page (**Policies > Access Control**). In the access control policy editor, view a warning by hovering your pointer over the alert icon next to the rule name and reading the warning in the tooltip text, or by selecting the **Show Warnings** button at the top of the page to view the warnings associated with all the rules referenced in your access control policy.
- In Version 5.4, inline normalization is automatically enabled when you create a network analysis policy with **Inline Mode** enabled. In previous versions, you had to manually enable inline normalization in your inline intrusion policies. Note that the update from Version 5.3.x to Version 5.4 does not change your inline normalization settings.
- You can now add access control rule port conditions that specify unassigned protocol numbers not included in the **Protocol** drop-down list.
- You no longer need a secondary rule to control FTP Data Channel in your access control policy.
- The new **Decompress SWF File (LZMA)**, **Decompress SWF File (Deflate)**, and **Decompress PDF File (Default) HTTP** Inspect preprocessor options offer enhanced decompression support for PDF and SWF file content.
- The TCP stream preprocessor now has enhanced protocol-awareness for SMTP, POP3, and IMAP.
- The system now provides enhanced detection of information in application traffic, including detection of application data in DNS traffic and detection of users in additional protocols.
- You can now configure LDAP authentication to use Common Access Cards (CACs) to associate the card with a user name so a user can log directly into the system using the card.
- The system now offers enhanced GPRS Tunneling Protocol (GTP) support.
- You can now force 8000 Series stacked devices into maintenance mode when any member of the stack fails. For more information, contact Cisco TAC. (CSCuy92530)

Documentation Updates

You can download all updated documentation from the Support site. In Version 5.4.0.10 and Version 5.4.1.9, the following documents were updated to reflect the addition of new features and changed functionality and to address reported documentation issues:

- *FireSIGHT System Online Help*
- *FireSIGHT System User Guide*

The documentation updated for Version 5.4.0.10 and Version 5.4.1.9.contains the following errors:

- The *FireSIGHT System User Guide* incorrectly states that **Cisco does not recommend enabling more than one non-SFRP IP address on a clustered Series 3 device's routed or hybrid interface where one SFRP IP address is already configured. The system does not perform NAT if clustered Series 3 devices experience failover while in standby mode.** The system does perform NAT if clustered Series 3 devices experience failover while in standby mode.
- The *FireSIGHT System User Guide* incorrectly states that you can **use Lights-Out Management (LOM) on the default (eth0) management interface on a Serial Over LAN (SOL) connection to remotely monitor or manage Series 3 appliances**. Using the same IP address for LOM and for a SOL connection to your Series 3 device is not currently supported.

- The *FireSIGHT System Virtual Installation Guide* incorrect states the following about logging in to a virtual device at the VMware console using admin as the username and the new admin account password specified in the deployment setup wizard: **If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use Cisco as the password.** The documentation should state that if you did not change the password using the wizard or you are deploying with an ESXi OVF template, use **Sourcefire** as the password.

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.4.0.10 and Version 5.4.1.9, 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: 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.

Before you begin the update, Cisco strongly recommends that you back up current event and configuration data to an external location. This data is not backed up as part of the update process.

Use the Defense 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 *FireSIGHT System User Guide*.

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

Caution: BIOS Version 2.0.1b must be running on DC2000 and DC4000 appliances in order to update to Version 5.4.1.1 and later. If updating your appliances fails due to an incompatible BIOS version, contact Cisco TAC.

Caution: Prior to updating an ASA FirePOWER module running FirePOWER Services or a Cisco ASA managed by ASDM, set the device clock to the correct time. If an ASA device clock is set to the incorrect time before updating, the Access Control Licensing page does not load.

Traffic Flow and Inspection During the Update

The update process reboots managed devices and might restart the Snort process. Depending on how your devices are configured and deployed, the following capabilities could be affected

- traffic inspection, including application awareness and control, user control, URL filtering, Security Intelligence, intrusion detection and prevention, and connection logging
- traffic flow, including switching, routing, NAT, VPN, and related functionality
- link state

Note that when you update clustered 7000 or 8000 Series devices or device stacks, the system performs the update one device at a time to avoid traffic interruption. When you update clustered devices, apply the update one device at a time, allowing the update to complete before updating the second device.

The following table explains how Snort restarts affect traffic inspection. It is reasonable to anticipate that the product update could affect traffic similarly.

Table 2 Snort Restart Traffic Effects by Managed Device Model

On this managed device model...	Configured as...	Traffic during restart is...
Series 3 and virtual	Inline with **Failsafe** enabled or disabled, or inline tap mode	Passed without inspection (a few packets might drop if **Failsafe** is disabled and Snort is busy but not down)
	Passive	Uninterrupted and not inspected
Series 3	Routed, switched, or transparent	Dropped
Cisco ASA with FirePOWER Services	Routed or transparent with fail-open (**Permit Traffic**)	Passed without inspection
	Routed or transparent with fail-close (**Close Traffic**)	Dropped

Link State

In 7000 Series and 8000 Series inline deployments with **Bypass** enabled, network traffic is interrupted at two points during the update:

- At the beginning of the update process, traffic is briefly interrupted while link goes down and up (flaps) and the network card switches into hardware bypass. Traffic is not inspected during hardware bypass.
- After the update finishes, traffic is again briefly interrupted while link flaps, and the network card switches out of bypass. After the endpoints reconnect and reestablish link with the sensor interfaces, traffic is inspected again.

Note: The configurable **Bypass** option is **not** supported on Cisco ASA with FirePOWER Services, non-bypass NetMods on 8000 Series devices, or SFP transceivers on 71xx Family devices.

Switching and Routing

Series 3 devices do **not** perform switching, routing, NAT, VPN, or related functions during the update. If you configured your devices to perform only switching and routing, network traffic is blocked throughout the update.

Audit Logging During the Update

When updating appliances that have a web interface, after the system finishes 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.

Version Requirements for Updating to Version 5.4.0.10 and Version 5.4.1.9

To update to Version 5.4.1.9, a Defense Center must be running at least Version 5.4.0. Defense Centers running Version 5.4.1 and later can manage devices running Version 5.4.0.10 and Version 5.4.1.9. If you are running an earlier version, you can obtain updates from the Support site.

Caution: BIOS Version 2.0.1b must be running on DC2000 and DC4000 appliances in order to update to Version 5.4.1.1 or later. If updating your appliances fails due to an incompatible BIOS version, contact Cisco TAC.

Series 3 devices must be running at least Version 5.4.0.5 to update to Version 5.4.0.10.

Cisco ASA with FirePOWER Services (ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60) must be running at least Version 5.4.0.5 to update to Version 5.4.0.10.

Cisco ASA with FirePOWER Services (ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X) must be running at least Version 5.4.1.4 to update to Version 5.4.1.9. The ISA3000 device must be running Version 5.4.1.7 to update to Version 5.4.1.9.

The closer your device's or ASA module's current version to the release version (Version 5.4.0.10 or Version 5.4.1.9), the less time the update takes.

Time and Disk Space Requirements for Updating to Version 5.4.0.10 and Version 5.4.1.9

The table below provides disk space and time guidelines for the Version 5.4.0.10 and Version 5.4.1.9 update. Note that when you use the Defense Center to update a managed device, the Defense 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.

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

Table 3 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update from Version 5.4.0	Time to Update from Version 5.4.0.9 or Version 5.4.1.8
Series 3 managed devices	469 MB	10483 MB	1786 MB	80 minutes	17 minutes
Series 3 Defense Centers	681 MB	22129 MB	n/a	180 minutes	29 minutes
virtual Defense Centers	676372 MB	23186788 MB	n/a	hardware dependent	

Table 3 Time and Disk Space Requirements (continued)

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time to Update from Version 5.4.0	Time to Update from Version 5.4.0.9 or Version 5.4.1.8
virtual managed devices	439116 MB	13069900 MB	2275 MB	hardware dependent	
Cisco ASA with FirePOWER Services on ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60	56 MB	13158 MB	2330 MB	260 minutes	80 minutes
Cisco ASA with FirePOWER Services on ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X, and the ISA 3000	90 MB	16172 MB	2776 MB	246 minutes	14 minutes

Caution: If you update a Defense Center from Version 5.4.0 to Version 5.4.1.9, the system re-installs all intrusion rule updates instead of the latest intrusion rule update and the update takes much longer than the projected time listed in the Time and Disk Space Requirements for Updating to Version 5.4.0.10 and Version 5.4.1.9, page 11. To reduce update time, Cisco **strongly** recommends updating to Version 5.4.1.2, then updating from Version 5.4.1.2 to Version 5.4.1.9.

Product Compatibility After Updating to Version 5.4.0.10 and Version 5.4.1.9

You **must** use at least Version 5.4.1 of the Defense Center to manage devices running Version 5.4.1.9. To manage an ASA FirePOWER module on an ASA5506-X,ASA5506W-X, ASA5506H-X, ASA5508-X, or ASA5516-X device, you **must** use at least Version 5.4.1 of the Defense Center.

Table 4 Version Requirements for Management

Appliance	Minimum Version to be Managed by a Defense Center Running Version 5.4.1.9
Series 3 FirePOWER managed devices	Version 5.4.0.5 of the FireSIGHT System
Cisco ASA with FirePOWER Services on ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60	Version 5.4.0.5 of the FireSIGHT System
Cisco ASA with FirePOWER Services on ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X	Version 5.4.1.4 of the FireSIGHT System
ISA3000	Version 5.4.1.7 of the FireSIGHT System

Caution: If you update a Defense Center from Version 5.4.0 to Version 5.4.1.9, the system re-installs all intrusion rule updates instead of the latest intrusion rule update and the update takes much longer than the projected time listed in the Time and Disk Space Requirements for Updating to Version 5.4.0.10 and Version 5.4.1.9, page 11. To reduce update time, Cisco **strongly** recommends updating to Version 5.4.1.2, then updating from Version 5.4.1.2 to Version 5.4.1.9.

Operating System Compatibility

You can host 64-bit virtual appliances running Version 5.4.1.9 on the following hosting environments:

- VMware vSphere VMware ESXi 5.0

- VMware vSphere VMware ESXi 5.1
- VMware vSphere VMware ESXi 5.5
- VMware vCloud Director 5.1

YYou can install ASA FirePOWER modules running Version 5.4.0.10 on the following ASA platforms running ASA Version 9.3(2), ASA Version 9.3(3), ASA Version 9.4(x) and later, ASA Version 9.5(1.5), ASA Version 9.5(2), ASA Version 9.5(3), ASA Version 9.6(x) and later, ASA Version 9.7(x), ASA Version 9.8(x), and ASA Version 9.9(x):

- ASA5512-X
- ASA5515-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and ASA5585-X-SSP-60

You can install ASA FirePOWER modules running Version 5.4.1.9 on the following AA platforms running ASA Version 9.4(x), ASA 9.5(1.5), ASA Version 9.5(2), ASA Version 9.5(3), ASA Version 9.6(x), ASA Version 9.7(x), ASA Version 9.8(x), and ASA Version 9.9(x):

- ASA5506-X
- ASA5506W-X
- ASA5506H-X
- ASA5508-X
- ASA5516-X
- ISA 3000

Note that you can install Version 5.4.1.9 on ASA5506-X platforms running ASA Version 9.3(2), ASA Version 9.3(3) as well.

For more information, see the *FireSIGHT System Installation Guide* or the *FireSIGHT System Virtual Installation Guide*.

Web Browser Compatibility

Version 5.4.0.10 and Version 5.4.1.9 of the web interface for the FireSIGHT 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 FireSIGHT System-provided self-signed certificate. This may cause FireSIGHT 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 through **Tools > Internet Options > Security > Custom level**.

Table 5 Supported Web Browsers

Browser	Required Enabled Options and Settings
Chrome 56	JavaScript, cookies
Firefox 51	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 9, 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**

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

Screen Resolution Compatibility

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.

Return to a Previous Version

If you need to return your appliance to a previous release of the FireSIGHT System for any reason, contact Cisco TAC for more information.

Reimage Appliances

If you need to reimage your appliances to the current release of the FireSIGHT System for any reason, refer to the *FireSIGHT System Virtual Installation Guide* for virtual appliances, and the Restoring a FireSIGHT System Appliance to Factory Defaults section of the *FireSIGHT System Installation Guide* for all other appliances.

Caution Reimaging always involves at least one system reboot.

To update to Version 5.4.0.10 or Version 5.4.1.9 from a Version 5.4.1 or Version 5.4.0 image, see Before You Begin: Important Update and Compatibility Notes, page 9 and Install the Update, page 15.

Download the following files from the Support site:

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

- for Series 3 Defense Center:

  `Sourcefire_Defense_Center_S3-5.4.0-763-Restore.iso`
- for virtual Defense Centers:

  `Sourcefire_Defense_Center_Virtual64_VMWare-5.4.0-763.tar.gz`
- for Series 3 managed devices:

  `Sourcefire_3D_Device_S3-5.4.0-763-Restore.iso`
- for virtual managed devices:

  `Sourcefire_3D_Device_Virtual64_VMWare-5.4.0-763.tar.gz`
- for ASA FirePOWER modules:

  `asasfr-sys-5.4.0-763.pkg`

- for Cisco ASA with FirePOWER Services (ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, and ASA5516-X):

  ```
  asasfr-5500X-boot-5.4.1-211.img
  asafr-sys-5.4.1-211.pkg
  ```

  Note: To install the ASA FirePOWER module Version 5.4.1 image on an ASA device, see the *Cisco ASA FirePOWER Module Quick Start Guide* for more information on deploying and installing the module.

Install the Update

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

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.

To update Defense Centers running at least Version 5.4.1 to Version 5.4.1.9, ASA FirePOWER modules (ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, and ASA5516-X) running at least Version 5.4.1 to update Version 5.4.1.9, the ISA3000 must be running at least Version 5.4.1.7 to update to Version 5.4.1.9, and managed devices and ASA FirePOWER modules (ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and ASA5585-X-SSP-60) running at least Version 5.4.0 of the FireSIGHT System to Version 5.4.0.10, see the guidelines and procedures outlined below:

- Update Defense Centers, page 16
- Update Managed Devices, 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.

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

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

Caution: If you update a Defense Center from Version 5.4.0 to Version 5.4.1.9, the system re-installs all intrusion rule updates instead of the latest intrusion rule update and the update takes much longer than the projected time listed in the Time and Disk Space Requirements for Updating to Version 5.4.0.10 and Version 5.4.1.9, page 11. To reduce update time, Cisco **strongly** recommends updating to Version 5.4.1.2, then updating from Version 5.4.1.2 to Version 5.4.1.9.

Order of Installation

Update your Defense Centers before updating the devices they manage.

Install the Update on Paired Defense Centers

When you begin to update one Defense Center within a pair, the other Defense Center in the pair becomes the primary, if it is not already. In addition, the paired Defense Centers stop sharing configuration information; paired Defense Centers do **not** receive software updates as part of the regular synchronization process.

To ensure continuity of operations, do **not** update paired Defense Centers at the same time. First, complete the update procedure for the secondary Defense Center, then update the primary Defense Center.

Install the Update on Clustered Devices

When you install an update on clustered 7000 Series or 8000 Series devices the system performs the update on the devices one at a time. When the update starts, the system first applies it to the secondary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. Apply the updated one device at a time, allowing the update to complete before updating the second device.

Install 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 finishes. Note that:

- If the primary device finishes 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 finishes the update after all of the secondary devices, the stack resumes normal operation when the update finishes on the primary device.

After the Installation

After you perform the update on either the Defense Center or managed devices, you **must** reapply device configuration and access control policies. When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. For more information, see the Configurations that Restart the Snort Process section of the *FireSIGHT System User Guide*.

There are several additional post-update steps you should take to ensure that your deployment is 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 5.4.1.9, if available, to take advantage of the latest enhancements and security fixes
- optionally, updating your intrusion rules and vulnerability database (VDB) and reapplying your access control policies
- making any required configuration changes based on the information in New Features and Functionality, page 2

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.

Update Defense Centers

Use the procedure in this section to update your Defense Centers, including virtual Defense Centers. For the Version 5.4.1.9 update, Defense Centers reboot.

Caution: BIOS Version 2.0.1b must be running on DC2000 and DC4000 appliances in order to update to Version 5.4.1.1 or later. If updating your appliances fails due to an incompatible BIOS version, contact Cisco TAC.

Caution: Before you update the Defense Center, reapply access control policies to any managed devices. Otherwise, the eventual update of the managed device 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 Defense Center to Version 5.4.1.9 removes existing uninstallers from the appliance.

Caution: If you update a Defense Center from Version 5.4.0 to Version 5.4.1.9, the system re-installs all intrusion rule updates instead of the latest intrusion rule update and the update takes much longer than the projected time listed in the Time and Disk Space Requirements for Updating to Version 5.4.0.10 and Version 5.4.1.9, page 11. To reduce update time, Cisco **strongly** recommends updating to Version 5.4.1.2, then updating from Version 5.4.1.2 to Version 5.4.1.9.

To update a Defense Center:

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.

2. Download the update from the Support site:

   – for Series 3 and virtual Defense Centers:

   ```
   Sourcefire_3D_Defense_Center_S3_Patch-5.4.1.9-53.sh
   ```

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

3. Upload the update to the Defense 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 Defense Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.

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

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. Tasks that are running when the update begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the task queue after the update finishes. The task queue automatically refreshes every 10 seconds.

6. Select **System > Updates**.

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

8. Select the Defense Center and click **Install**. Confirm that you want to install the update and reboot the Defense Center.

   The update process begins. You can begin monitoring the update's progress in the task queue (**System > Monitoring > Task Status**). However, after the Defense Center finishes 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 Cisco TAC. Do **not** restart the update.

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

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

   The update process begins. You can monitor the update's progress in the task queue (**System > Monitoring > Task Status**).

Caution: Do **not** use the web interface to perform any other tasks until the update finishes and the Defense Center reboots. Before the update finishes, the web interface may become unavailable and the Defense Center may log you out. This is expected behavior; log in again to view the task queue. If the update is still running, do **not** use the web interface until the update finishes. If you encounter issues with the update (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the update. Instead, contact Cisco TAC.

9. After the update finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
10. Log into the Defense Center.
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**.
12. Select **Help > About** and confirm that the software version is listed correctly: Version 5.4.1.9. Also note the versions of the rule update and VDB on the Defense Center; you will need this information later.
13. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
14. If the rule update available on the Support site is newer than the rules on your Defense Center, import the newer rules. Do not auto-apply the imported rules at this time.

    For information on rule updates, see the *FireSIGHT System User Guide*.
15. If the VDB available on the Support site is newer than the VDB on your Defense 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 *FireSIGHT System User Guide*.
16. Reapply device configurations to all managed devices.

    To reactivate a grayed-out **Apply** button, edit any interface in the device configuration, then click **Save** without making changes.
17. Reapply access control policies to all managed devices.

    Caution: Do **not** reapply your intrusion policies individually; you must reapply all access control policies completely.

    When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. For more information, see the Configurations that Restart the Snort Process section of the *FireSIGHT System User Guide*.
18. If a patch for Version 5.4.1.9 is available on the Support site, apply the latest patch as described in the *FireSIGHT System Release Notes* for that version. You **must** update to the latest patch to take advantage of the latest enhancements and security fixes.

Update Managed Devices

After you update your Defense Centers to Version 5.4, Version 5.4.1, or Version 5.4.1.9, use them to update the devices they manage.

A Defense Center must be running at least Version 5.4 to update its managed devices to Version 5.4.1.9. Because they do not have a web interface, you must use the Defense Center to update your virtual managed devices, and ASA FirePOWER modules.

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

When you updated clustered Cisco ASA with FirePOWER Services apply the update one device at a time and allow the update to complete before updating the second device.

Before you update an ASA FirePOWER module, set the device clock to the correct time. If an ASA device clock is set to the incorrect time before updating, the Access Control Licensing page does not load.

For the Version 5.4.0.10 update, all devices reboot. Series 3 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 9.

Caution: Before you update a managed device, use its managing Defense Center to reapply the appropriate access control policy to the managed device. Otherwise, the managed device update may fail.

Caution: Installing the updates and applying policies can interrupt traffic inspection due to Snort restarts and system restarts. How these interruptions affect traffic depends on the model of the managed device and how it handles traffic. For more information, see Traffic Flow and Inspection During the Update, page 9.

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:

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

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

Caution: Failing to set the device clock of an ASA FirePOWER module running FirePOWER Services or a Cisco ASA managed by ASDM to the correct time prior to updating the device causes the Access Control Licensing page to not load.

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

2. Update the software on the devices' managing Defense Center; see Update Defense Centers, page 16.
3. Download the update from the Support site:
   - for Series 3 managed devices:

     `Sourcefire_3D_Device_S3_Patch-5.4.0.10-53.sh`

   - for virtual managed devices:

     `Sourcefire_3D_Device_Virtual64_VMware_Patch-5.4.0.10-53.sh`

   - for ASA FirePOWER modules (ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and ASA5585-X-SSP-60):

     `Cisco_Network_Sensor_Patch-5.4.0.10-53.sh`

   - for ASA FirePOWER modules (ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X, and the ISA 3000):

     `Cisco_Network_Sensor_Patch-5.4.1.9-49.sh`

Caution: ASA FirePOWER modules (ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and ASA5516-X) must be running at least Version 5.4.1 before updating to Version 5.4.1.9. The ISA 3000 must be running at least Version 5.4.1.7 before updating to Version 5.4.1.9. See the *Cisco ASA FirePOWER Module Quick Start Guide* for more information on deploying and installing the module.

4. Upload the update to the Defense 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 Defense Center. The web interface shows the type of update you uploaded, its version number, and the date and time it was generated. The page also indicates whether a reboot is required as part of the update.

5. Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
6. Click the install icon next to the update you are installing.
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.

8. Click **Install**. Confirm that you want to install the update and reboot the devices.
9. The update process begins. You can monitor the update's progress in the Defense Center's task queue (**System > Monitoring > Task Status**).

   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 task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do not restart the update. Instead, contact Cisco TAC.

10. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 5.4.0.10 or Version 5.4.1.9.
11. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
12. Reapply device configurations to all managed devices.

    Tip: To reactivate a grayed-out **Apply** button, edit any interface in the device configuration, then click **Save** without making changes.

13. Reapply access control policies to all managed devices.

    Caution: When you apply an access control policy, resource demands may result in a small number of packets dropping without inspection. Additionally, applying some configurations requires the Snort process to restart, which interrupts traffic inspection. Whether traffic drops during the interruption or passes without further inspection depends on the model of the managed device and how it handles traffic.For more information, see the Configurations that Restart the Snort Process section in the *FireSIGHT System User Guide*.

14. If a patch for Version 5.4.0.10 or Version 5.4.1.9 is available on the Support site, apply the latest patch as described in the *FireSIGHT System Release Notes* for that version.

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

Uninstall the Update

The following sections help you uninstall the Version 5.4.1.9 update from your appliances:

Plan the Uninstallation

Before you uninstall the update, you must thoroughly read and understand the following sections.

Uninstallation Method

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

For all physical appliances and virtual Defense Centers, uninstall the update using the local web interface. Because virtual managed devices do not have a web interface, you **must** use the bash shell to uninstall the update.

Order of Uninstallation

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

Uninstall the Update from Clustered or Paired Appliances

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

To ensure continuity of operations, uninstall the update from clustered devices and paired Defense Centers one at a time. First, uninstall the update from the secondary appliance. Wait until the uninstallation process finishes, then immediately uninstall the update from the primary appliance.

Caution: If the uninstallation process on a clustered device or paired Defense Center fails, do **not** restart the uninstall or change configurations on its peer. Instead, contact Cisco TAC.

Uninstall the Update from Stacked Devices

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

To minimize impact on your deployment, Cisco recommends that you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the uninstallation finishes on all devices in the stack.

Uninstall the Update from Devices Deployed Inline

Managed devices do **not** perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update, page 9.

Uninstall the Update and Online Help

Uninstalling the Version 5.4.1.9 update does **not** revert the online help to its previous version. If the version of your online help does not match that of your FireSIGHT System software, your online help may contain documentation for unavailable features and may have problems with context sensitivity and link functionality.

After the Uninstallation

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

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.

Uninstall the Update from a Managed Device

The following procedure explains how to use the local web interface to uninstall the Version 5.4.0.10 update from managed devices. You **cannot** use a Defense Center to uninstall the update from a managed device.

Uninstalling the Version 5.4.0.10 update results in a device running Version 5.4.0.9. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

Uninstalling the Version 5.4.1.9 update reboots the device. Managed devices do **not** perform traffic inspection, switching, routing, 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 9.

To uninstall the update from a managed device:

1. Read and understand Plan the Uninstallation, page 21.
2. On the managing Defense Center, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
3. On the managed device, view the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

   Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the task queue after the uninstallation finishes. The task queue automatically refreshes every 10 seconds. You **must** wait until any long-running tasks are complete before you begin the uninstallation.
4. Select **System > Updates**.
5. Click the install icon next to the uninstaller that matches the update you want to remove, then confirm that you want to uninstall the update and reboot the device.

   The uninstallation process begins. You can monitor the uninstallation progress in the task queue (**System > Monitoring > Task Status**).

   Caution: Do **not** use the web interface to perform any other tasks until the uninstallation has completed and the device reboots. Before the uninstallation finishes, the web interface may become unavailable and the device may log you out. This is expected behavior; log in again to view the task queue. If the uninstallation is still running, do **not** use the web interface until the uninstallation has completed. If you encounter issues with the uninstallation (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the uninstallation. Instead, contact Cisco TAC.
6. After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
7. Log in to the device.
8. Select **Help > About** and confirm that the software version is listed correctly: Version 5.4.0.9.
9. On the managing Defense Center, verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstall the Update from a Virtual Managed Device

The following procedure explains how to uninstall the Version 5.4.1.9 update from virtual managed devices. You **cannot** use a Defense Center to uninstall the update from a managed device.

Uninstalling the Version 5.4.1.9 update results in a device running Version 5.4.1.8. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

Uninstalling the Version 5.4.1.9 update reboots the device. Virtual managed devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Traffic Flow and Inspection During the Update, page 9.

To uninstall the update from a virtual managed device:

1. Read and understand Plan the Uninstallation, page 21.
2. Log into the device as `admin`, with SSH or through the virtual console.
3. At the CLI prompt, type `expert` to access the bash shell.
4. At the bash shell prompt, type `sudo su -`.
5. Type the admin password to continue the process with root privileges.
6. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach
   /var/sf/updates/Sourcefire_3D_Device_Virtual64_VMware_Patch_Uninstaller-5.4.1.9-49.sh
   ```

   Caution: If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Cisco TAC.
7. After the uninstallation finishes, log into the managing Defense Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 5.4.1.8.
8. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstall the Update from a Cisco ASA with FirePOWER Services

The following procedure explains how to uninstall the Version 5.4.1.9 update from virtual managed devices. You **cannot** use a Defense Center to uninstall the update from a managed device.

Uninstalling the Version 5.4.1.9 update results in a device running Version 5.4.1.8. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

Uninstalling the Version 5.4.1.9 update reboots the device. Virtual managed devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Traffic Flow and Inspection During the Update, page 9.

To uninstall the update from a virtual managed device:

1. Read and understand Plan the Uninstallation, page 21.
2. Log into the device as `admin`, with SSH or through the virtual console.
3. At the CLI prompt, type `expert` to access the bash shell.
4. At the bash shell prompt, type `sudo su -`.
5. Type the admin password to continue the process with root privileges.
6. At the prompt, enter the following on a single line:

   ```
   install_update.pl --detach
   /var/sf/updates/Sourcefire_3D_Device_Virtual64_VMware_Patch_Uninstaller-5.4.1.9-49.sh
   ```

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

7. After the uninstallation finishes, log into the managing Defense Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 5.4.1.8.
8. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstall the Update from a Defense Center

Use the following procedure to uninstall the Version 5.4.1.9 update from Defense Centers and virtual Defense Centers. Note that the uninstallation process reboots the Defense Center.

Uninstalling the Version 5.4.1.9 update results in a Defense Center running Version 5.4.1.8. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

To uninstall the update from a Defense Center:

1. Read and understand Plan the Uninstallation, page 21.
2. Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
3. View the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

   Tasks that are running when the uninstallation begins are stopped, become failed tasks, and cannot be resumed; you must manually delete them from the task queue after the uninstallation finishes. The task queue automatically refreshes every 10 seconds. You **must** wait until any long-running tasks are complete before you begin the uninstallation.
4. Select **System > Updates**.
5. Click the install icon next to the uninstaller that matches the update you want to remove.
6. Select the Defense Center and click **Install**, then confirm that you want to uninstall the update and reboot the device.

   The uninstallation process begins. You can monitor the uninstallation progress in the task queue (**System > Monitoring > Task Status**).

   Caution: Do **not** use the web interface to perform any other tasks until the uninstallation has completed and the Defense Center reboots. Before the uninstallation finishes, the web interface may become unavailable and the Defense Center may log you out. This is expected behavior; log in again to view the task queue. If the uninstallation is still running, do **not** use the web interface until the uninstallation has completed. If you encounter issues with the uninstallation (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the uninstallation. Instead, contact Cisco TAC.
7. After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
8. Log in to the Defense Center.
9. Select **Help > About** and confirm that the software version is listed correctly: Version 5.4.1.8.
10. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Resolved Issues

You can track defects resolved in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required. To view defects addressed in older versions, refer to the legacy caveat tracking system.

Issues Resolved in Version 5.4.0.10 and Version 5.4.1.9:

- **Security Issue** Addressed multiple vulnerabilities that generated denial of service in OpenSSL, Libxml2, and SSH, as described in CVE-2010-5298, CVE-2013-4353, CVE-2014-3507, CVE-2014-3510, CVE-2015-3194, CVE-2015-3195, CVE-2015-3196, CVE-2016-1907, CVE-2016-2073, CVE-2016-2105, CVE-2016-2106, CVE-2016-2107, CVE-2016-2108, CVE-2016-2109, CVE-2016-2176, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-4448, CVE-2016-4449, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6305, CVE-2016-6306, CVE-2016-6307, CVE-2016-6308, CVE-2016-6309, and CVE-2016-7052.
- **Security Issue** Addressed a vulnerability issue in the third party products OpenSSL, Linux, and GNU libc, as described in CVE-2013-4237, CVE-2014-0076, CVE-2014-0160, CVE-2014-3508, CVE-2014-3509, CVE-2014-3511, CVE-2015-2808, CVE-2016-2183, and CVE-2016-5696.**Security Issue** Addressed a cross-site scripting (XSS) vulnerability, as described inCVE-2016-6395.
- **Security Issue** Resolved a vulnerability where arbitrary HTTP header injection allowed unauthenticated, remote attackers to bypass configured rules used by snort detection, as described in CVE-2016-1463.
- **Security Issue** Resolved a vulnerability where, if you applied a file policy with the default action set to **Block Malware** and enabled **Inspect HTTP Responses**, the system assigned an incorrect SHA value to malware files and did not block the file when it should, as described in CVE-2016-9209.
- **Security Issue** Resolved an issue where, if you configured the Email Notification option on the Configuration page (**System > Configuration**) using Authentication, the system incorrectly stored the email account password as plain text on the system. (CSCuz17452)
- Resolved an issue where the Real Time Eventing page (**Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**) does not load in the ASDM interface window. (CSCus11216)
- The system allowed you to create user passwords containing the [**$**] character even though special characters are not supported, and subsequent login attempts fails. (CSCut27442)
- Resolved an issue where, if you selected all the application filters within the Application Filters page (**Object > Object Management > Application Filters**) by selecting the first available application filter and using the keyboard command **shift+click** on the last available application filter on a Chrome browser, only the two applications filters you selected remained checked. (CSCut86012)
- Removed support for deprecated configurations of the Secure Sockets Layer (SSL) web browser option. (CSCuu97541, CSCuz52366)
- Improved LDAP performance. (CSCuv05876)
- Resolved an issue where, if you configured a system policy to use remote NTP server to synchronize time to a system with a registered ASA 5500-X device or a Series 3 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 a new task on the Scheduling page (**System > Tools > Scheduling**) and selected the link provided as the backup profile, the link generated a **500 Internal Server Error.** (CSCuv22624)
- Resolved an issue where, if you created a scheduled task to download and install a geolocation database (GeoDB) on a Day of Week, the system did not execute the scheduled task when it should have. (CSCuv44836)
- Resolved an issue where, if you generated a report template with a custom logo and created a backup file, then backed up and restored the Defense Center, the backup file did not save the custom logo in the report template. (CSCuv44883)
- Updated the local time zone for Europe/Istanbul. (CSCuw73747)
- Resolved an issue where, if you switched as ASA FirePOWER module from being managed by a Defense Center to being managed by ASDM, intrusion events did not consistently display in the ASDM event viewer. (CSCuv97332)

- Resolved an issue where, if you edited the time synchronization window on the System Policy page (**System > Local > System Policy**) and configured the **Set My Clock** option to use the Defense Center as the NTP server, the system did not use the Defense Center's local time when it should have. (CSCuw92124)
- Resolved an issue where, if you reboot a managed NGIPSv device and added multiple vmxnet3 interfaces, the system incorrectly added the interfaces causing pre-existing interfaces to experience issues. (CSCux15018)
- Resolved an issue where, if you created a security zone containing an active interface without saving device configuration and applied an access control policy referencing the security zone in some or all of the access control rules, all the rules referencing the security zone were not included in the applied access control rule. (CSCux38908)
- Resolved an issue where you could not generate troubleshooting for the secondary Defense Center in a high availability configuration from the primary Defense Center. (CSCux46182)
- Resolved an issue where, if you updated a system running Version 5.4.1.4 or earlier to Version 5.4.1.5 or later, the system experienced a fatal error and update failed. (CSCux48859)
- Resolved an issue where, if you disabled the **Sensitive Data Detection** option in the Advanced Settings section of the Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**), the system incorrectly enabled the detection option every time you download a new intrusion rule update. (CSCux57338)
- Resolved an issue where the system did not generate alerts for rate-based traffic, like TCP SYN flood, when it should have. (CSCux59107)
- Improved the stability of using IPv6 IP addressed with Cisco redundancy protocol (SFRP) functionality. (CSCux67113)
- Improved update process from Version 5.4.1.2. (CSCuy00310)
- Improved detection on GRE tunneled flows. (CSCuy01267)
- Improved updating from Version 5.4.1.5 or later to Version 6.0.0. (CSCuy07477)
- Resolved an issue where, if you applied an access control policy referencing an intrusion policy and an SSL policy with the action set to **Decrypt-Resign**, the system did not generate downloadable packet information on the packet view of the Intrusion Events page (**Analysis > Intrusion > Events**). (CSCuy34078)
- Resolved an issue where, if you enabled **Inspect HTTP Responses** as a server-level HTTP normalization option, the system did not detect files containing 16,000 or more non-printable characters. (CSCuy43369)
- Resolved an issue where the system did not detect files if the client dropped packets. (CSCuy45196)
- Resolved an issue where, if you allowed cloud communications enable both **Enable URL Filtering** and **Query Cloud for Unknown URLs** on the Cloud Services page (**Configuration > ASA FirePOWER Configuration > Local > Configuration > Cloud Service**) on an ASA Firepower device managed by ASDM and the device requested a URL lookup for an unknown URL, the system did not assign a category when it should. (CSCuy79984)
- Resolved an issue where, if you configured Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virttual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**) of an ASA FirePOWER module, the OSPF incorrectly reported all interfaces as available even if they were not. (CSCuy64096)
- Resolved an issue where, if you enabled the SMTP preprocessor, the system experienced issues. (CSCuy66901)
- Resolved a rare issue where the SIP preprocessor was not properly enabled even if you manually enabled the preprocessor. (CSCuy89897)
- Resolved an issue where, if you enabled adaptive profiles in the Advanced tab of the access control policy editor page and repeatedly deploy configuration, the system did not prune expired information and experienced memory issues. (CSCuz03171)
- Resolved an issue where, if you create an intrusion policy layer on a system running Version 5.4.0.X and updated the system to Version 6.0.0, then shared the intrusion policy layer, the system displayed an error. (CSCuz07954)

- Resolved an issue where, if you had a large number of intrusion policies and each policy contained more than one layer, the intrusion rule update failed. (CSCuz25692)
- Resolved an issue where the system logged zip files containing malicious child files incorrectly. (CSCuz30018, CSCuz30074)
- Resolved an issue where the system allowed you to create and save a file policy, then delete the name of the policy and save. The system now checks policies for empty requirements, such as policy name, prior to saving. (CSCuz60341)
- Resolved an issue where the system generated extraneous **High Unmanaged Disk Usage** health alerts. (CSCuz66563)
- The data dictionary for the DBcheck is not updated in both Version 5.4.0.x and Version 5.4.1.x. (CSCuz69497)
- Improved general network performance for SSL traffic. (CSCuz72548)
- Resolved an issue where, if you deployed a file policy with the default action set to **Block Malware** and attempted to download a malware file via FTP, the system did not block the download and generated an event in the Connection Events page (**Analysis > Connections > Events**) even though the file was successfully downloaded. (CSCuz80431)
- Resolved an issue where, if you deployed an SSL policy with decryption enabled and the system processed SSL traffic, the system experienced issues. (CSCuz83354)
- Resolved an issue where updatingDefense Center virtuals with less than 8GB of memory running Version 5.4.0 or later to Version 6.0.0 Pre-Install or Version 6.0.0 failed. (CSCuz93339)
- Resolved an issue where, if you deployed a file policy with **Archive Inspection** enabled for ARJ compressed files enabled during the inspection of traffic containing malformed ARJ compressed files, the system experienced issues such as geolocation database and URL database update failures. (CSCuz99094)
- Resolved an issue where, if you updated an 5500x series device while it is registered to a Defense Center, all Malware Cloud Lookup requests timed out (CSCva00693)
- Resolved an issue where a system with an updated firmware will not appear to support Lights-out Management in the web interface. (CSCva09177)
- Resolved an issue where device autoregistration to the standby Defense Center in a high -availability pair failed. (CSCva10398)
- Resolved an issue where, if the system experienced an issue when processing the first session of SMTP traffic between a client and an SMTP server, the system did not correctly identify the subsequent SMTP sessions as SMTP for the client-server pair and displayed **Unknown** in the Application Protocol column of the Connection Events page (**Analysis > Connections > Events**). (CSCva10980)
- Resolved an issue where, if a link for stacked Series 3 devices dropped, the system took up to 30 seconds to acknowledge the down link. (CSCva13792)
- Resolved an issue where, in some cases, Series 3 devices configured with static routes experienced issues and used 100% of the CPU. (CSCva15195)
- FTP Normalization is automatically enabled when you deploy a file policy in Version 6.1.0 or later, even if inline normalization is disabled in a network analysis policy. (CSCva20916)
- Resolved an issue where Defense Center did not send events to external clients through eStreamer if some of the events contained information about SSL certificates. (CSCva27436)

- Resolved an issue where, if you applied the Microsoft updates KB3161606 or KB3172614 to a system running either Windows 8.1 and Windows Server 2012 R2 or Microsoft updates KB3161608 or KB3172605 to a system running Windows 7 SP and Windows Server 2008 R2 SP1, then used a certificate to connect to a User Agent server via TLS, the User Agent failed to complete any SSL connections to the Defense Center. (CSCva32331)
- Improved SSL inspection processes. (CSCva42950)
- Resolved a rare issue where, if an authoritative and non-authoritative logon for the same user/IP arrived at the Defense Center at approximately the same time, the non-authoritative had a later timestamp but was processed first. (CSCva43120)
- Resolved an issue where, if you deployed an access control policy containing an SSL policy with the default action set to **Decrypt - Resign** and a file policy with the default action set to either **Block** or **Block with reset** for PDF file types, the system did not block FTPS traffic containing PDFs when it should have. (CSCva84390)
- Resolved an issue where the detection_filter keyword did not count events in the expected manner. (CSCvb22338)
- Resolved an issue where FTP servers do not support filenames or file paths containing non-English characters. (CSCvb22610)
- Resolved an issue where, if you created a realm for Active Directory (AD) and **Download users and groups**, then added a user from the downloaded group to an access control policy and deployed to an ASA FirePOWER module, the system did not block the user when it should. (CSCvb26230)
- Resolved an issue where the DHCP Relate agent did not start if you configured a RHCP Relate agent on a virtual router with more than 21 interfaces. (CSCvb40343)
- Improved general memory usage and reduced latency when processing high volumes of traffic against access control policies configured with URL filter conditions and user groups. (CSCvb50368)
- Resolved an issue where updating an ASA FirePOWER module from Version 5.4.1.8 or later to Version 6.0 or if you uninstall Version 5.4.1.8 or later on a ASA FirePOWER module to Version 5.4.1.7 and attempt to update the device to Version 6.0 failed. (CSCvb62987)
- Resolved an issue where, in some cases, Series 3 device stacks experienced issues and required a reboot. (CSCvb66334)
- Resolved a rare issue where, another instance of Process Manager could be started while there was already an instance running, causing processes to both traffic outages and processes repeatedly stopping and starting. (CSCvb92968)
- Resolved an issue where, if you performed URL control and enabled **Retry URL cache miss lookup** in the access control policy, the system incorrectly generated multiple connection events for the same connection. (CSCvc08844)
- Resolved an issue where, if a 3D8350 device or AMP8350 device produced an unusually large stream of messages on the serial port console or, if you enabled it, the Lights-out Management (LOM) console, the device became unresponsive. (CSCvc26880)
- The Version 6.0 pre-install incorrectly stopped the update when the pre-install script checked Defense Centers for exactly 8G RAM. (CSCvc98418)

Issues Resolved in Previous Versions

Previously resolved issues are listed by version.

Issues resolved in Version 5.4.0.9 and Version 5.4.1.8:

- Resolved an issue where, if you enabled the use of a proxy on your Defense Center and **Create FireAMP Connection** on the AMP Management page (**AMP> AMP Management**), the system did not include Private Cloud in the Cloud Name drop-down list. (CSCuu16374)

- Resolved an issue where, if you created an LDAP object in the Microsoft Active Directory and added the LDAP object to a user policy, then moved the LDAP object, the Defense Center could not locate the LDAP object. (CSCuu95350)
- Resolved an issue where, if you attempted to delete a security zone from the Security Zones page (**Objects > Object Management > Security Zones**) referenced in the applied access control policy of an ASA 5500-X Series device, the system did not save the changes and did not delete the security zone. (CSCuv40232)
- Resolved an issue where, if you applied a policy that included a rule with security zone conditions and then compared policies, the policy comparison generated differences even when there were none. (CSCuv76157)
- Resolved an issue where, if you manually configured the time to a future time or date while deploying configuration and then deployed another configuration with the current time or date to the same appliance, the device did not save the second configuration when it should have. (CSCuw01691)
- Improved email notification reliability. (CSCuw36354)
- Resolved an issue where, if you deployed a network discovery policy and enabled host discovery, the system incorrectly detected hosts from networks not defined in the network discovery policy. (CSCuw51866)
- Resolved an issue where, if you clicked **Create Custom Workflow** on the Custom Workflows page (**Analysis > Custom > Custom Workflows**) for intrusion events and included **HTTP URI**, **HTTP Hostname**, and/or **Original Client IP** fields, marking intrusion events as reviewed generated an database error and the events did not get marked as reviewed. (CSCuw90541)
- Resolved an issue where, if user IP and group mappings streamed to a managed device while the mappings were updated on the Defense Center, the network map on the managed device did not update correctly and did not match the network map on the Defense Center. (CSCux12245)
- Resolved an issue where, if you configured a backup LDAP server on the LDAP Connections page (**Policies > Users > LDAP Connections**), the system did not recognize the backup LDAP server and any attempt to **Fetch Groups** or **Download Users** failed if the primary LDAP server was unreachable. (CSCux24855)
- Resolved an issue where, if you applied an access control policy that generated more than 32,000 rules, then added either a network address translation (NAT) policy or a VPN policy containing a static rule and reapplied, the rules became corrupted and policy apply failed. (CSCux74877)
- Resolved an issue where, if you deployed an access control policy containing a user group within a realm and the system submitted a high volume of URL lookups, network mapping dropped messages related to some users and did not match against deployed access control rules when it should have. (CSCuy15844)
- Resolved an issue where, if you deployed an access control policy containing a file policy set to **Block Malware** and an SSL policy set to **Decrypt - Known key**, the system did not successfully complete the initial file transfer for incoming traffic when it should have. (CSCuy22114)
- Resolved an issue where the system displayed incorrect frame collision counts for the **show portstats** CLI command on a physical Series 3 device. (CSCuy33294)
- Resolved an issue where the system experienced issues if processes exceeded memory limits. (CSCuy36889)
- Resolved an issue where, if you configure inline sets to go into bypass mode on a Series 3 device running Version 5.4.0 or later and update the device to Version 5.4.0.2 or later, the device experienced loss of link on sensing interfaces for an extended period of time after the device rebooted during the update. (CSCuy74958, CSCva86844)
- Resolved an issue where, if you updated a Defense Center pair to at least Version 5.4.1.5 with multiple clustered devices registered and expanded the last cluster of devices listed on the Device Management page (**Devices > Device Management**), the system did not display all the devices within the cluster. (CSCuy79012)
- Improved general performance of network mapping. (CSCuy83259)
- Improved event threshold functionality. (CSCuy85993)

- Resolved an issue where, if you deployed an access control rule containing applications detected by NMAP scan, the system could not find a detector for the applications and redeploying the access control policy containing the rule with the risk application generated a **Policy has rules with missing detectors. The following rules specify applications for which a detector is not defined** error. (CSCuy87939)
- Resolved an issue where, if you updated a managed Series 3 or ASA FirePOWER module to Version 5.4.0.5 or later, the update failed even though the Defense Center displayed the update successful. (CSCuy94873)
- Resolved an issue where, if you registered multiple devices to a Defense Center, deploying an intrusion policy randomly failed on one of the registered devices. (CSCuz01826)
- Improved Defense Center application reports. (CSCuz04049)
- Resolved an issue where, in some cases, the system experienced memory issues if you applied a SSL rule containing an application identification, URL category, or common name condition. (CSCuz09961)
- Resolved an issue where, if you installed a vulnerability database (VDB) update on a Defense Center managing a device with no licenses or policies, the VDB update appeared to fail even though it successfully completed. (CSCuz11048)
- Generated malware events no longer contain extraneous linebreak characters. (CSCuz16055)
- Resolved an issue where, if you deployed an SSL policy to a device managed by a Defense Center running Version 6.0.0 and updated the Defense Center to Version 6.0.1.1, then redeployed configuration and the system experienced a high volume of traffic, the system experienced a disruption in traffic. (CSCuz19469)
- Resolved an issue where, if you updated a Defense Center to Version 5.4.1.6 or later and applied policy to a registered device running Version 5.3.x, policy apply failed. (CSCuz52737)
- Resolved an issue where, if you applied an SSL rule, the system applied the inherited default action for handshake errors instead of the traffic that matched the rule. (CSCuz54524)
- Resolved an issue where updating a Defense Center from Version 5.4.0 to Version 5.4.1.7 caused the system to reinstall all intrusion rule updates instead of the latest intrusion rule update. (CSCuz68570)
- Resolved an issue where, if you deployed an SSL policy set to **Decrypt - Resign** and the system immediately restarted, the system experienced issues. (CSCuz79056)
- If you apply an access control policy containing an excessive amount of access control rules with the default action set to **Trust**, the system may incorrectly generate events for traffic matching any of the rules set to **Trust** when it should not. (CSCuz83816)
- Resolved an issue where, if fragmented UDP packets with different VLAN tags traveled through the same inline set on a Series 3 device, the fragmented packets experienced a 10 second delay and the system dropped traffic. (CSCva03312)
- Resolved an issue where memory issues on stacked 8000 Series devices caused processes to terminate. (CSCva39997)

Issues Resolved in Version 5.4.0.8 and 5.4.1.7:

- Resolved an issue where, if you registered a device to a pair of a Defense Centers and applied an access control policy with URL rules and turned on URL cloud query, the managed device did not successfully request a URL lookup. (CSCus99059)
- Resolved an issue where, if you clicked the **Email Status to:** link on the Scheduling page (**System > Tools > Scheduling**), the web browser incorrectly displayed a **500 Internal Server Error** message. (CSCuv22590)
- Resolved an issue where the FSIC incorrectly checked extraneous files. (CSCuv55284)
- Resolved an issue where, in some cases, attempting to backup and restore a Defense Center failed. (CSCuv95657, CSCuw71197)

- Improved general appliance functionality. (CSCuw44360)
- Resolved an issue where the system incorrectly allowed you to cluster a 3D8260 device with a 3D8270 device. (CSCuw92248)
- Resolved an issue where, if you configured Cisco Redundancy Protocol (SFRP) with an IPv6 address on a Series 3 pair with routed or hybrid interfaces, and the system experienced a fail-over, the system incorrectly handled sessions shared between pair members. (CSCux73498)
- Resolved an issue where resuming a failed upgrade for a Defense Center pair caused an incomplete upgrade, broken HA state and an inability edit the access control policy. (CSCuy05808)
- Resolved an issue where the network map experienced issues if the last entry in the RNA map list was a duplicate. (CSCuy01269)
- Resolved an issue where flash files that use LZMA compression were not decompressed. (CSCuy22393)
- Resolved an issue where, if you created a file policy and enabled the HTTP preprocessor, and the system detected a malware file containing a custom **SHA256** value, the system did not block the malware file. (CSCuy32815)
- Resolved an issue where, if you edited a base intrusion policy used by one or more child policies, the system did not mark the child policies as out-of-date when it should. (CSCuy32822)
- Resolved an issue where intrusion policies continuously and unsuccessfully attempted to sync paired Defense Centers due to taking longer than a configured timeout. (CSCuy33982)
- Resolved an issue where, if a registered ASA FirePOWER module experienced memory corruption, the system suffered a network outage and restarted. (CSCuy37234)
- Resolved an issue where, if you removed a user from all the groups within a LDAP connection referenced in the access control policy and applied configuration changes, then clicked **Download users and groups** from the Users page (**Policies > Users**), the system did not update the applied configuration and continued to process traffic as if the group(s) still contained the user. (CSCuy39685)
- Improved CIP traffic detection on mid-stream sessions. (CSCuy43852)
- Resolved an issue where if you enabled the use of a proxy on the Defense Center and submitted captured files to the Cisco cloud for dynamic analysis, the system generated a **Dynamic Analysis Failed (Network Issue)** error and did not successfully submit the files for analysis. (CSCuy49613)
- Resolved an issue where, if you applied an intrusion rule set to **Drop and Generate Events** and enabled **Sensitive Data Detection** in the Advanced Settings tab of the intrusion Edit Policy page (**Policies > Intrusion > Intrusion Policy**), then edited the Sensitive Data Detection page and checked **Masks**, the system did not correctly mask some sensitive data generated in intrusion events. (CSCuy56094)
- Resolved an issue where access control rules did not function correctly for web applications and URLs that were SPDY-enabled. (CSCuy65157)
- Resolved an issue where updating a DC750 from Version 5.4 to Version 5.4.1.6 or later failed. (CSCuy72106)
- Resolved an issue where creating a stack on a Defense Center failed, the Device Management page (**Devices > Device Management**) and the Policies page did not load, and the system generated a Task failure **(3c428400-ebb6-11e5-b1fb-4696ad84e4e4) Update stack : Unable to load SF::PeerManager::ClusterMgmt: Attempt to reload SF/PeerManager/ClusterMgmt.pm aborted.** error. (CSCuy79698)

Issues Resolved in Version 5.4.0.7 and 5.4.1.6:

- **Security Issue** Addressed an arbitrary script injection vulnerability allowing unauthenticated, remote attackers to exploit GNU libc or libpng, as described in CVE-2014-7547 and CVE-2015-8126.

- **Security Issue** Addressed a vulnerability issue that generated denial of service in GNU utilities, as described in CVE-2015-7547.
- **Security Issue** Addressed a cross-site scripting (XSS) and arbitrary HTML injection vulnerabilities, as described in CVE-2015-0737.
- **Security Issue** Addressed an arbitrary HTTP header injection vulnerability allowing unauthenticated, remote attackers to exploit managed devices as described in CVE-2016-0737.
- Resolved an issue where, if you generated an intrusion event performance graph with **Last Hour** set as the time range, the system incorrectly generated a blank graph. (145237/CSCze95774)
- Resolved an issue where updating the vulnerability database (VDB) on a paired Defense Center incorrectly switched the peer of the pair from active to standby and from standby to active when it should not. (CSCur59343)
- Resolved an issue where, if you configured Open Shortest Path First (OSPF) in the Dynamic Routing tab of the Virtual router page (**Devices > Devices Management > Virtual routers > Dynamic Routing**) and added an **Area**, then changed the value of the **Cost** column and deployed changes, the system did not update the OSPF. (CSCus31735)
- Resolved an issue where Snort generated reporting statistics at inconsistent intervals. (CSCus42306)
- Resolved an issue where, if you created an access control rule configured with an **Interactive Block** action and you viewed a blocked web page in a Chrome web browser, the **Continue** button to bypass the block page did not work. (CSCuu53237, CSCuv21748)
- 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 you could not manually set the time zone on an ASA FirePOWER module managed by ASDM. (CSCuu70250)
- Resolved an issue where internal CA certificates generated on the Object Management page (**Objects > Object Management > PKI**) remained valid for 30 days when they should be valid for ten years. (CSCuv29004)
- Resolved an issue where, if you deployed an SSL policy and enabled SSL decryption, the system experienced a disruption in traffic after a few hours of decrypting SSL traffic. (CSCux75036)
- Resolved an issue where, if you attempted to update the system with less than the required amount of free space, the update failed and the system incorrectly appeared to have a negative amount of space available. (CSCuv43019)
- Improved Simple Mail Transfer Protocol (SMTP) traffic detection. (CSCuy44141)
- Resolved an issue where, if you suppressed a rule in an intrusion policy with the Suppression Type set to either **Source** or **Destination** IP address with a custom variable, then deleted the custom variable and applied policy, policy apply failed the system did not indicate why. (CSCuv44581)
- You can now execute the **Show user** CLI command on ASA FirePOWER modules. (CSCuv45343)
- Resolved an issue where selecting **network file system 4(NFS4)** storage as a remote storage type from the Storage Type drop-down menu on the Remote Storage device tab of the Local Configuration page (**System > Local > Configuration**) erroneously generated an error. (CSCuv50519)
- Optimized firewall rules count limit. (CSCuv86743)
- Resolved an issue where the 7000 Series or 8000 Series devices may have changed the outermost Ether type for **IEEE 802.1Q VLAN** traffic they inspected from **88a8** to **8100**, which prevented endpoints from receiving those frames. (CSCuw57916)
- Resolved an issue where, if you removed a DNS entry from a management interface and saved the configuration without replacing or adding another DNS entry, then attempted to login to web interface, the web page generated a blank login screen. (CSCuw68408)

- Resolved an issue where health events caused excessive logging and the system experienced disk space issues. (CSCuw84304)
- Resolved an issue where if you created a logical interface that referenced a link aggregated group (LAG) to a Series 3 device and added, removed, or replaced the existing NetMod on the device, the system did not recognize any referenced objects. (CSCux03639)
- Resolved an issue where the Defense Center's health monitor generated extraneous **Warning** (yellow) and **Critical** (red) health alerts when there were no alerts. (CSCux04564)
- Resolved an issue where, if you enabled **Automatic Rule Update** on a Defense Center pair and installed a rule update, then applied policies, the Defense Center incorrectly displayed the access control policy as out-of-date when it was not. (CSCux21111)
- Resolved an issue where disabling interface **eth0** caused system issues. (CSCux22564, CSCux35301)
- Resolved an issue where, if you edited a registered device's name to include a character larger than 8-bit and configured passive mode interfaces, then enabled **Inline Normalization** and applied the access control policy, the system did not generate the policy deploy dialog. (CSCux23227)
- Resolved an issue where, if you update a system running Version 5.4 to Version 5.4.1 or later with STIG mode enabled, update failed. (CSCux23487)
- Resolved an issue where, if you logged into the FirePOWER system and deleted an **In queue** or a **Report Generation Failed** report from the reports tab of the Reporting page (**Overview > Reporting**) as a user other than the user who created the report, the system did not delete the report when it should have. (CSCux27304)
- Improved HTTP traffic processing and reduced the chance of dropped packets when processing large HTTP POST events. (CSCux30861)
- Resolved an issue where, if you created a system policy containing an external authentication server with the Attribute field set to **string**, policy apply failed and the system generated an error. (CSCux31226)
- Resolved an issue where, if you created an access control policy referencing an SSL policy containing a network object with multiple entries on a managed Firepower appliance running Version 5.4 or later and you updated the system to Version 6.0, policy apply failed. (CSCux31618)
- Resolved a rare issue where the system did not properly process HTTP POST data with incorrect headers. (CSCux40517)
- Resolved an issue where, in some cases, the system database integrity check failed and you could not upgrade the system to Version 6.0. (CSCux52218)
- Resolved an issue where, if you edited and deployed an intrusion policy that was created in Version 5.4 or earlier, intrusion layers may have become corrupted. (CSCux57697)
- Resolved an issue where, if you deployed an intrusion policy and enabled Sensitive Data Detection, the system did not consistently mask content in traffic containing sensitive data. (CSCux61562)
- Improved packet reassembly for HTTP traffic containing chunked encoding. (CSCux61630)
- Improved HTTP inspection of gzip compressed data when there is no Content-Length header present in the HTTP Response. (CSCux76518)
- Resolved an issue where, graphs generated from the Intrusion Event Performance page (**Overview > Summary > Intrusion Event Performance**) displayed incorrect or no data. (CSCux91742)
- Resolved an issue where, if you deployed an access control policy containing an SSL rule, the system eventually dropped the majority of incoming traffic and caused a network outage. (CSCux95913)

- Resolved an issue where, if you applied an intrusion rule set to **Drop and Generate Events** and enabled **Sensitive Data Detection** in the Advanced Settings tab of the intrusion Edit Policy page (**Policies > Intrusion > Intrusion Policy**), then edited the Sensitive Data Detection page and checked **Masks**, the system did not correctly mask some sensitive data generated in intrusion events. (CSCuy43629)
- Resolved an issue where, if you applied policies after importing the 2016-02-28-001 rule update, the system did not correctly apply policies. (CSCuy56212)

Issues Resolved in Version 5.4.0.6 and Version 5.4.1.5:

- **Security Issue** Addressed multiple vulnerability issues in Linux, MYSQL, DNS, NTP, OpenSSL, and other third parties, as described in CVE-2013-1944, CVE-2013-4545, CVE-2014-0139, CVE-2014-9296, CVE-2015-0405, CVE-2015-0423, CVE-2015-0433, CVE-2015-0438, CVE-2015-0439, CVE-2015-0441, CVE-2015-0500, CVE-2015-0501, CVE-2015-0503, CVE-2015-0508, CVE-2015-1793, CVE-2015-2568, CVE-2015-2571, CVE-2015-2573, CVE-2015-2575, CVE-2015-6335, CVE-2015-7855, and CVE-2015-7871.
- **Security Issue** Addressed an arbitrary script injection vulnerability allowing unauthenticated, remote attackers to exploit GNU C library DNS resolution functionality, as described in CVE-2013-7423.
- **Security Issue** Addressed multiple vulnerabilities in OpenSSL that allowed external attacks on client connections, as described in CVE-2014-8275 and CVE-2015-0204.
- **Security Issue** Addressed multiple cross-site scripting (XSS) and arbitrary HTML injection vulnerabilities, including those described in CVE-2015-6353.
- **Security Issue** Addressed multiple vulnerability issues that generated denial of service in NTP, XML, OpenSSL, and other third parties as described in CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7704, CVE-2015-7705, CVE-2015-7848, CVE-2015-7850, CVE-2015-7853.
- **Security Issue** Addressed multiple arbitrary script injection vulnerabilities allowing unauthenticated, remote attackers to exploit or overwrite functionality as described in CVE-2015-7703.
- **Security Issue** Addressed a vulnerability that allowed an authenticated user can access system files using path traversal as described in CVE-2015-7851.
- Improved inspection of traffic tagged by the Cisco Identity Service Engine (ISE). (143060/CSCze94478)
- Resolved an issue where the memory usage health monitor erroneously generated false positives. (144593/CSCze94840)
- Resolved an issue where, if you created an intrusion rule with the source IP set to **!$HOME_NET** and added the intrusion rule to an intrusion policy, then changed the rule state to **Drop and Generate Events**, the system does not allow you to save the intrusion policy. (CSCur53155)
- Resolved an issue where the **show traffic-statistics** CLI command did not display data for the second interface of an inline pair on a virtual device. (CSCur59771)
- Resolved an issue where the system generated excessive and extraneous logs in the system log (syslog). (CSCur75622)
- 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 reflect daylight savings time. (CSCur92028)
- Resolved an issue where the system included both raw HTTP packets and reassembled packets in event counts. (CSCus68893)
- Resolved an issue where, if you applied an access control rule containing a network object or group that had been previously deleted from a primary or active Defense Center in a high availability configuration, the secondary or passive system did not recognize the network object or group as deleted and experienced issues. (CSCut54187)
- Resolved an issue where, if you applied a NAT policy to a pair of clustered devices, policy apply on the secondary device failed and the system separated the cluster. (CSCut98774)

- Resolved an issue where, if you created an access control policy with a URL category condition and the system loaded a partial database, the system experienced issues. (CSCuu06714)
- Resolved an issue where an SSH session did not time out when it should. (CSCuu21037)
- Resolved an issue where, in some cases, creating traffic profiles generated multiple errors. (CSCuu22704)
- Resolved an issue where, if you enabled at least two management interfaces and your system lost connectivity to one of the interfaces, the system defaulted to an incorrect gateway IP address and you could not access the interface. (CSCuu44020)
- Improved eStreamer performance. (CSCuu94902)
- Syslog messages now populate information for the following fields: **HTTP Referrer**, **User Agent**, and **Referenced Host**. (CSCus18179)
- The system only supports one normal IP address for virtual router interfaces on clustered Series 3 devices. (CSCut58601)
- Improved health alert notifications for failed malware cloud lookups. (CSCut77594)
- Resolved an issue where, if the system experienced two sequential system failures, the system fell into bypass mode even if you configured non-bypass mode. (CSCut80892)
- Resolved an issue where using the **show managers** CLI command on a device registered to a system with multiple interfaces configured caused the system to display the incorrect IP address. (CSCut95947)
- Resolved an issue where, if you created a file policy configured to **Inspect Archives**, the network map experienced issues and the system stopped processing traffic. (CSCuu14892)
- Resolved an issue where, if you created an access control policy with the default action set to **Block with Reset** that referenced a file policy with the default action set to **Block Malware**, the system did not block the first malware file detected. (CSCuu81183)
- Resolved an issue where, if a backup filename contained a space, applying the backup to a Defense Center failed. (CSCuu99818)
- 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 in the Report Templates page with a modified **Maximum Results** value, the system generated the report with the default value instead of the configured value. (CSCuv06557)
- Resolved an issue where the system did not deploy VPN when it should have. (CSCuv20623)
- 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. (CSCuv41376)
- Improved health monitor alerts. (CSCuv96121)
- The system now supports UTF-8 characters when creating LDAP objects and downloading groups and users in access control and system policies. (CSCuv27375)
- Resolved an issue where, if you registered many devices, 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)
- Resolved an issue where policy apply on Series 3 devices and ASA FirePOWER modules experiencing high volumes of traffic failed due to a memory limitation. (CSCuv99982)

- Resolved an issue where, if you created a new identity in a Microsoft Active Directory session with a **Department** value containing double quotes (**“ ”**) and immediately logged into a system, the system was unable to retrieve the new user profile. (CSCuw03498)
- Improved the stability of the network map. (CSCuw06359)
- Resolved an issue where, if you configured a static route on your appliance and reapplied your system policy, the system incorrectly deleted the static route. (CSCuw07826)
- Resolved an issue where the system displayed the incorrect device name in correlation events generated by a correlation rule on malware events. (CSCuw11056)
- Resolved an issue where registering and managing multiple devices on a DC4000 caused system connection issues. (CSCuw11462)
- Resolved an issue where, if you registered a device to the primary Defense Center in a high availability environment and renamed the device to a name containing 40 characters or more before device synchronization completed, device registration to the secondary Defense Center failed. (CSCuw27368)
- Resolved an issue where, if you created an access control rule with the default action set to either **Interactive Block** or **Interactive Block with Reset**, clicking **Continue** on the interactive block page did not redirect to a HTTPS page. (CSCuw28868)
- Resolved an issue where, if you used a Windows OS computer to access the web interface and created an SSL policy, the firewall incorrectly blocked sessions even if you did not set the default action to **Block**. (CSCuw36519)
- Resolved an issue where the system with an applied file policy failed to detect and process FTP traffic. (CSCuw49257)
- Resolved an issue where deleting third-party vulnerabilities with a host input client connection caused system issues. (CSCuw56215)
- Resolved an issue where, if you applied an access control policy referencing four or more file policies to a Cisco ASA FirePOWER module, the system incorrectly processed Simple Mail Transfer Protocol (SMTP) traffic and experienced issues. (CSCuw65202)
- Resolved an issue where systems with enabled traffic profiles experienced disk space issues. (CSCuw74528)
- Resolved an issue where, if you executed host input commands on a Defense Center in a high availability configuration, the system failed to apply the host input commands to the secondary Defense Center in the pair. (CSCuw98376)
- Resolved an issue where, after resolving a disk space issue, the system continued to experience issues storing events and logged **All shard connections are busy for partition** errors. (CSCux00142)

Issues resolved in Version 5.4.0.5 and Version 5.4.1.4:

- **Security Issue** Resolved an issue where the system did not properly encode a newly added comment to an access control policy rule.
- **Security Issue** Addressed multiple cross-site request forgery (CSRF) vulnerabilities as described in CVE-2015-4242.
- Resolved an issue where, if you logged into your system as a user other than the **admin** user and edited the base layer of an intrusion policy, the system incorrectly marked all affected edited intrusion policies as updated by **admin** when it should not have. (CSCur79437)
- Resolved an issue where, if you configured a system policy to use remote NTP server to synchronize time to a system with registered devices and you disabled device management, NTP failed to sync updated time to the device after the system enabled device management. (CSCur97671)

- Resolved an issue where, in some cases, the Defense Center experienced system issues and failed to load access control rules. (CSCut30047)
- Resolved an issue where the system experienced latency while downloading large number of groups and users from Microsoft Active Directory Server and the system did not match traffic to the access control rule referencing LDAP groups. (CSCut56233)
- Resolved an issue where the system incorrectly handled static routes configured on Series 3 devices with multiple interfaces. (CSCut84953)
- Resolved an issue where the system displayed an internal server error if you viewed the Discovery Statistics page on a Defense Center that did not have any discovery events. (CSCuu00749)
- In some cases, the system does not generate intrusion event performance graphs (**Overview > Summary > Intrusion Event Performance**). (CSCuu15447)
- Resolved an issue where, if you backed up your Defense Center and restored the backup to a different Defense Center, the Defense Center with the restored backup did not allow you to log in. (CSCuu35238)
- Resolved an issue where, if you downloaded LDAP users or an LDAP group to a Defense Center without a FireSIGHT license, the download failed and the system generated a user limit reached error. (CSCuu35615)
- Resolved an issue where the Cisco Redundancy Protocol (SFRP) advertisement interval value appeared to be configurable when you added or edited a routed IP address when it was not. (CSCuu37687)
- Resolved an issue where ASA FirePOWER modules 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 the system incorrectly disabled your configured static route, virtual router, or virtual router filter if you configured a static or virtual router on a managed device with clustered interfaces. (CSCuu47325)
- Resolved an issue where the system did not generate a list of vendors if you created a product map and selected the **Add Fix Map** option. (CSCuu79373)
- Resolved an issue where, if you applied an SSL policy with the default actions set to **Decrypt-Resign**, decrypted traffic that egressed from one interface set was switched or routed so it ingressed into a different interface set on the same managed device. (CSCuu97712)
- Resolved an issue where the License page incorrectly listed licenses under the wrong devices if you added more than one license to a 3D8250 device and one license to another Series 3 device. (CSCuu99789)
- Resolved an issue where DC2000 and DC4000 BIOS settings could not be configured using **ucsfg** Cisco UCS Configuration Utility commands. (CSCuv03352)
- Resolved an issue where the system did not include data from X-Forward-For, True-Client-IP, and other packet data in generated intrusion events. (CSCuv03727)
- Resolved an issue where, if you applied an intrusion policy to a managed device that was not set to **drop when inline**, the system did not block files with a malware disposition when it should. (CSCuv12647)
- Resolved an issue where troubleshoot generation from the Health Monitor page failed if you enabled both IPv6 IP addresses. (CSCuv27328)
- Resolved an issue where the system incorrectly saved **blacklist** as the priority list when configuring the priority settings of the reputation preprocessor even if you set the configuration to whitelist. (CSCuv52955)
- Improved memory utilization for access control rule memory with port ranges. (CSCuv64114)
- Resolved an issue where, if you modified an attribute setting in a host profile, the system did not retain the host's attribute setting after the host IP address changed. (CSCuv69748)

- Improved network map generation. (CSCuv72386)
- Resolved an issue where the system did not include new user accounts not mapped to a host IP address, and grouped access control rules configured to detect user traffic by group failed. (CSCuv78458)
- Resolved an issue where your network analysis policy did not correctly load after a system update. (CSCuw44448)

Issues resolved in Version 5.4.0.4 and Version 5.4.1.3:

- **Security Issue** Addressed a vulnerability issue in Linux, as described in CVE-2011-4131.
- **Security Issue** Resolved an issue where managed devices experienced microengine failure when processing corrupted traffic. (CSCuu86214)
- Resolved an issue where you could not reapply an intrusion policy (individually or as part of an access control policy reapply) a total of 4096 or more times to a single managed device was not supported. (134385/CSCze89030)
- Resolved an issue where, if you imported an intrusion policy referenced by another policy as a shared layer or as a base policy, importing the intrusion policy failed. (144946/CSCze96151)
- Resolved an issue where the system incorrectly listed twice the number of registered targets on the Intrusion Policy list page. (CSCus08840)
- Resolved an issue where you could add old events from the clipboard to a new incident, even though the events in your clipboard section of the Incidents page appeared empty. (CSCus67128)
- Resolved an issue where, if you edited an access control rule with multiple category conditions and attempted to remove one of the conditions, the system only removed the first listed category condition. (CSCut25082)
- Resolved an issue where the system reported intrusion rules as inactive if the rule targeted a passive zone on an 8000 Series device and performed the **show fastpath-rules** CLI command. (CSCut32479)
- Resolved an issue where configuring a file policy with **Inspect Archives** enabled caused Snort to stop passing traffic. (CSCut39253, CSCuu60621)
- Improved troubleshooting. (CSCut43542)
- Improved Disk manager reliability. (CSCut65740)
- Improved correlation rule performance. (CSCut97938)
- Resolved an issue where downgrading RPM packet manager (RPM) files starting with Cisco did not correctly reset the RPM install history. (CSCut98525)
- Resolved an issue where policy apply failed if you reapplied an active access control policy to an ASA FirePOWER module without editing the policy. (CSCuu14839)
- Improved error message warning against use of overlapping port settings in DCE/RPC advanced settings. (CSCuu18577)
- Resolved an issue where connectivity to the AMP cloud may be lost after using the system for an extended period of time. (CSCuu24587)
- Resolved an issue where the system experienced a disruption in traffic if you created a link aggregation group (LAG) on a physical Series 3 device connected to a Cisco Nexus 7000 switch. (CSCuu31626)
- Resolved an issue where, if you changed your system's time zone to a zone east of UTC and added a correlation rule with at least one inactive period to a correlation policy, policy apply failed. (CSCuu37600)
- Resolved an issue where creating a routed interface on your clustered Series 3 device caused connectivity issues. (CSCuu37668)

- Resolved an issue where the **Send email** check box on the Report Templates tab of the Reporting page did not stay selected if you generated a report, navigated away from the Report Templates tab, and then generated another report. (CSCuu97750)
- Improved tracking of the number of monitored hosts. (CSCuu77263)
- Resolved an issue where, if you configured your Defense Center to use a static IPv4 address with an IPv6 address enabled and you accessed the Defense Center's interface using the IPv6 address, the Access Control Policy page did not load. (CSCuu83933)
- Resolved an issue where, in rare cases, your system appeared unstable and did not recover from a hard reset. (CSCuu93154)
- Resolved an issue where a drive failure on some DC4000 appliances caused RAID controller failure and data loss. (CSCuu93159)
- Resolved an issue where the Product Licensing dashboard widget did not list any URL Filtering licenses even if URL Filtering licenses were present. (CSCuu97762)
- Improved network mapping performance. (CSCuv48373)

Issues resolved in Version 5.4.0.3 and Version 5.4.1.2:

- **Security Issue** Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections, as described in CVE-2015-0286,CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, and CVE-2015-0293.
- **Security Issue** Addressed a cross-site scripting (XSS) vulnerability, as described in CVE-2015-0707.
- **Security Issue** Addressed multiple vulnerability issues in Linux and other third parties, as described in CVE-2011-2699, CVE-2012-2744, CVE-2012-3400, and CVE-2015-1781.
- **Security Issue** Addressed a vulnerability in HTTP connection handling that allowed users to be redirected to malicious websites, as described in CVE-2015-0706.
- **Security Issue** Resolved an issue where the system can experience a microengine fault based on malformed packet data in traffic inspected by a FirePOWER 7000 or 8000 Series managed device. (CSCuu10871, CSCuu26678)
- When routing is configured on a Series 3 device, the system may forward source-routing IPv4 packets, which direct the packet along a different path than configured on the router and can be used to bypass network security measures. (132121/CSCze88520)
- Resolved an issue where, if you viewed the threat score of some files from generated events, the system incorrectly reported the threat score as a number instead of **Low**, **Medium**, **High**, or **Very High**. (142290/CSCze93722)
- Improved URL filtering. (144198/CSCze94590)
- Resolved an issue where the passive interfaces on 7000 Series devices reported incorrect egress security zones and interfaces. (144624/CSCze95206)
- Resolved an issue where, if you edited the interface security zones from 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 enabled remote storage and created a scheduled email alert response on your Defense Center, the scheduled email alert disabled remote storage and remote storage backups failed. (145288/CSCze95993)
- 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 lowercase. (CSCur37364)
- Resolved an issue where adding a Defense Center in a high availability configuration to your system caused the secondary Defense Center to overwrite the existing SHA-256 values in the system's file list. (CSCur57708)

- Resolved an issue where, if you created aa 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)
- Improved multiple dashboard widgets. (CSCus11068)
- Resolved an issue where your system occasionally experienced latency during Snort restart. (CSCus13247)
- Resolved a bug where file names of uuencoded email attachments was not displayed in file events and malware events. (CSCus30831)
- Resolved an issue where some HTTPS traffic inspections resulted in false positives. (CSCus32474)
- Resolved an issue where the system generated an **Internal Server Error** message if the password for your registered ASA FirePOWER device included an unsupported character. (CSCus68604)
- Resolved an issue where the system generated a malware alert on the second attempt to download a suspicious file over HTTP instead of generating an alert on the first attempt to download the file. (CSCus83151**)**
- Resolved an issue where, if you created an user role in the Custom User Role tab of the User Management page, the system disabled some check-boxes but enabled some options available under the disabled check boxes. (CSCus87248)
- Resolved an issue where, if you attempted to download a file but the download was blocked and the file was downloaded again, the system either did not identify the file type or the system generated incorrect SHA-256 values. (CSCus87799)
- If your system restarts or reloads after a VDB install and the **Inspect Traffic During Policy Apply** option in your firewall policy is unchecked, you may experience loss of network connectivity during the restart process. (CSCut08225)
- Resolved an issue where, if you created an access control rule configured to send events to an external syslog server and the system detected multiple truncated unified files, the device stopped sending connection events to the syslog server. (CSCut14629)
- Improved SFDatacorrelator performance when processing historical email and eStreamer alerts. (CSCut23688)
- Resolved an issue where the FirePOWER fiber ports on the 4-Port 10Gbps non-bypass network modules would not reliably achieve link connectivity with APCON IntellaFlex or IntellaPatch brand devices. (CSCut24654)
- Resolved an issue where the system displayed incorrect file type information on the Network File Trajectory page. (CSCut27978)
- Resolved an issue where enabling the Original Client IP column in the Intrusion Events table view and reviewing one or more row generated errors. (CSCut41458)
- Resolved issues where the system exposed plain text passwords in syslog messages in the web interface and in log files accessible with the shell. (CSCut80473)
- Resolved an issue where the Retrospective Malware Events table did not include the old disposition or the new disposition fields of a retrospective malware event. (CSCut83512)
- Resolved an issue where, if you restarted your ASA5585-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, if you configured a domain name without a DNS entry, the web interface page did not load. (CSCut89714)
- Resolved an issue where, if you removed a malware license from your Defense Center while the Defense Center experienced a disruption in cloud connectivity, the system continuously generated **Cannot connect to cloud** Health Monitor alerts. (CSCut95470)

- Resolved an issue where configuring a Windows TGM Proxy caused a disruption in detection preprocessors. (CSCut95588)
- Disabling one of management interfaces from a multiple manager interface configuration no longer disables the communication channel. (CSCut95915)
- Resolved an issue where, if you configured a link aggregated group (LAG) to use link aggregation control protocol (LACP) and the LAG interfaces experienced heavy broadcast traffic, the LAG interfaces entered a forced down state. (CSCuu04209)
- Resolved an issue where you experienced system issues if the cloud continuously checked for a new update. (CSCuu04844)
- The system will generate an alert if you attempt to create two correlation policies with an identical name. (CSCuu14720)
- Resolved an issue where, if you downgrade an ASA5585-X device to an older version, Linux did not downgrade when it should have. (CSCuu14965)
- Resolved an issue where the system displayed the incorrect amount of memory usage on the System Load dashboard widget. (CSCuu19742)
- Improved CPU performance reporting for the Simple Network Management Protocol (SNMP) agent on physical Series 3 devices. (CSCuu31029)
- Improved CPU performance. (CSCuu35011)
- Resolved an issue where, if an ASA5506-X device running ASA platform Version 9.3(3) or 9.4(1) experienced issues, the device stopped processing traffic. (CSCuu38535)
- Resolved an issue where excessive memory usage caused the system to restart processes that potentially caused loss of network connectivity. (CSCuu88135)
- Resolved an issue where, if you clicked the Edit icon near the configurable **Relay Host** option while generating a report from the Report page, the web browser redirected to a internal server error web page. (CSCuv01286)

Issues resolved in Version 5.4.1.1 and Version 5.4.0.2:

- **Security Issue** Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections, as described in CVE-2014-3569, CVE-2014-3570, CVE-2014-3572, and CVE-2015-0204.
- **Security Issue** Addressed an arbitrary script injection vulnerability allowing unauthenticated, remote attackers to exploit GNU C library DNS resolution functionality, as described in CVE-2015-0235.
- **Security Issue** Resolved multiple cross-site scripting (XSS) and arbitrary HTML injection vulnerabilities. (CSCus03591, CSCus03762, CSCus04436, CSCus07858, CSCus07875)
- **Security Issue** Resolved a vulnerability in Universal Unique Identifier (UUID) manipulation. (CSCus06097)
- 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 backed up and restored a Defense Center, Security Intelligence objects were not backed up or restored. (CSCur42337, CSCur35624)
- Resolved an issue on Series 3 managed devices where inline connectivity could be lost for up to 25 seconds on bypass-enabled inline sets during device reboot. (CSCur64678)
- Resolved an issue where, in some cases, you were not able to get URL category or URL reputation information. (CSCur38971, CSCus59492)

- 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, 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 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 create an SSL policy 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 placed an access control rule referencing a file policy with a Block Malware rule positioned after an access control rule with a web application condition, the system did not identify malware files. (CSCus64393, CSCus64526)
- Resolved an issue where, if both the management interface and the control interface of your system used the same VLAN and the management interface used an IPv6 address, the management interface was inoperable. (CSCus64678)
- Resolved an issue where, if your system included an SSL Visibility Appliance (SSLVA) or a Cisco SSL Appliance and you created a file policy containing a web application category and a Block Malware rule, your first attempt to download a file over HTTPS failed. Note that this issue is resolved when the SSL appliance is running Version 3.8.4. (CSCus72505)
- Resolved an issue where the system experiences issues if you applied an access control policy referencing a URL Filtering license, Security Intelligence license, and an SSL policy configured for inspection on any of the following devices: the 7000 Series, ASA5506-X, ASA5506H-X, and the ASA5506W-X. (CSCut02823)
- 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)
- When an applied access control policy with a rule set has all source IPv4 addresses, the system evaluates traffic with an IPv6 source address as if source addresses were not set in the rules. When an applied access control policy with a rule set has all source IPv6 addresses, the system evaluates traffic with an IPv4 source address as if source addresses were not set in the rules. When an applied access control policy with a rule set has all destination IPv4 addresses, the system evaluates traffic with an IPv6 destination address as if destination addresses were not set in the rules. When an applied access control policy with a rule set has all destination IPv6 addresses, the system evaluates traffic with an IPv4 destination address as if destination addresses were not set in the rules. (CSCut48596)
- Resolved a rare issue where, if a Series 3 device detected traffic targeted for stacked devices, the system experienced issues and could not process traffic. (CSCut53335)

Issues resolved in Version 5.4.1:

- **Security Issue** Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections. The fix addresses CVE-2014-3566.
- **Security Issue** Addressed an arbitrary script injection vulnerability allowing unauthenticated, remote attackers to execute commands through Bash. The fix addresses CVE-2014-6271 and CVE-2014-7169.
- **Security Issue** Resolved an unauthorized vulnerability in Universal Unique Identifier (UUID) manipulation.
- **Security Issue** Resolved cross-site scripting (XSS) vulnerabilities in the host attribute.
- **Security Issue** Resolved an HTML injection vulnerability.
- Improved the speed of reloading Snort configurations during access control policy apply. (112070/CSCze87966, CSCur19687)

- Resolved an issue where, if you created an SSL policy with the Session Not Cached option set to **Do Not Decrypt** or **Block** and SSL session reuse enabled, the system displayed uncached session errors in the **SSL Status** column of the Connection Events table view when the session refreshed. (143335/CSCze93608).
- Resolved an issue where the system did not display data for the **Network Analysis Policy** column of the Intrusion Events table view and the Connection Events table view if you registered a device running Version 5.3.X to a Defense Center running Version 5.4. (143349/CSCze94484)
- Resolved an issue where the system failed to recover if you attempted to reboot your clustered Series 3 devices after the devices went to maintenance mode and experienced a power failure. (143504/CSCze94928)
- Updated the *FireSIGHT System User Guide* to reflect that applying an access control policy may cause a short pause in traffic flow and processing. (143514/CSCze94971)
- Access control policies now have logging capabilities for **Log at Beginning and End of Connection**, **Log at End of Connection**, and **No Logging at Connection**. (143507/CSCze94975)
- Resolved an issue where, if the system generated file events, the system incorrectly truncated file event filenames containing colons on several pages of the web interface. (143666/CSCze94954)
- Resolved an issue where, if you disabled an access control rule containing either an intrusion policy or a variable set that was different from any enabled access control rules, policy apply failed and the system experienced issues. (143871/CSCze94114, 144635/CSCze95200)
- Improved diskmanager cleanup during report generation. (143933/CSCze94240, 143934/CSCze94286)
- Resolved an issue where multiple IP addresses were incorrectly displayed for a single host profile. (144259/CSCze94623)
- Resolved an issue where decrypted SSL sessions displayed URLs in connection logs as **http://** instead of **https://**. (144485/CSCze95739)
- 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. (144488/CSCze95591, 144544/CSCze95599)
- Resolved an issue where, if you enabled your Defense Center or managed device's **eth1** for DHCP, the system incorrectly saved the configuration with DHCP enabled for both **eth0** and **eth1**. (144525/CSCze95666)
- Resolved an issue where, if you applied an access control policy with archive file types enabled on a device running a vulnerability database (VDB) older than Version 211, policy apply failed. (144533/CSCze95570)
- Resolved an issue where the system treated DNS traffic as OpenVPN, QQ, and Viber traffic. (144548/CSCze95536)
- Resolved an issue where rule or packet latency thresholding timers could not be disabled. (144555/CSCze95704)
- Resolved an issue where, if you created a link aggregation group (LAG) interface on a NetMod connected to an 8000 Series managed device and then powered down the device, removing the NetMod after powering down caused errors. (144576/CSCze95166)
- Resolved an issue where removing the URL Filtering license from your system caused a disruption in cloud connectivity. (144578/CSCze95183)
- Resolved an issue where, if you used the SFR **system restart** CLI command on the ASA5506-X device while logged in through the ASA session command, the device stopped processes and did not restart them. (144609/CSCze94873)
- Resolved an issue where, if you created an HTML report, the web browser incorrectly displayed the report as binary data. (144667/CSCze95195)

- Resolved an issue where importing and exporting Defense Center policies failed. (144806/CSCze95396, 144905/CSCze96093)
- Resolved an issue where defining a large range of ports for source ports or destination ports caused policy apply to fail. (144933/CSCze95305)
- Resolved an issue where the system experienced a FSIC failure during update. (144964/CSCze95780)
- Resolved an issue where, if you attempted to establish a private cloud connection without utilizing the proxy option, the system attempted to connect to the private cloud with proxy even if you unchecked the use proxy option. (144968/CSCze95801)
- Resolved an issue where automatic update failed if you attempted to download updates while managing an X-Series device. (145060/CSCze95372)
- Resolved an issue where the user interface provided the incorrect patch release when you attempted to update your system with the **Download Updates** button. (145174/CSCze95284)
- Resolved an issue where, at altitudes of 2000 feet or higher, the AMP8150 emitted excessive noise due to inlet fans running at 20,000 RPM or faster, despite reported fan speeds as low as 0 RPM. Updating the BMC firmware or applying this update resolves the issue in the firmware, but to resolve temporarily until you can update, use the **ipmi mc reset cold** CLI command to reset the AMP8150 Baseboard Management Controller (BMC). Note that you must reestablish your Serial Over Lan (SOL) session after reset. (CSCus59936)
- Resolved an issue where the Inline Normalization preprocessor incorrectly resized packets when the **Trim Data to Window** option was enabled. (CSCur80901)

Issues resolved in Version 5.4:

- **Security Issue** Addressed multiple vulnerability issues in Linux and other third parties as described in CVE-2013-0343, CVE-2013-2164, CVE-2013-2206, CVE-2013-2232, CVE-2013-2234, CVE-2013-2888, CVE-2013-3552, CVE-2013-4387, CVE-2013-4470, CVE-2013-4786, CVE-2007-6750, CVE-2013-7263, CVE-2013-7265.
- **Security Issue** Addressed multiple injection vulnerabilities, including HTML and command line injections.
- **Security Issue** Addressed multiple cross-site scripting (XSS) vulnerabilities.
- **Security Issue** Addressed multiple cross-site request forgery (CSRF) vulnerabilities.
- **Security Issue** Addressed multiple parameter manipulation and misconfiguration vulnerabilities.
- If you configure an access control rule to **Block, Block with reset, Interactive block, Interface Block with reset**, or **Monitor**, selecting a reputation level also selects all reputations more severe than the selected level. If you configure an access control rule to **Allow** or **Trust**, selecting a reputation level also selects all reputations less severe than the selected level. (111747/CSCze87908)
- The system now prevents you from using IPv6 addresses to configure connections to the User Agent. (124377/CSCze88700)
- Resolved an issue where, in some cases, the system included extraneous data in intrusion event performance graphs. (124934/CSCze87728)
- Improved the functionality of eStreamer performance metrics. (129840/CSCze89231)
- Resolved an issue where large system backups failed if disk space usage exceeded the disk space threshold before pruning. (132501/CSCze88368)
- Resolved an issue where using the RunQuery tool to execute a **SHOW TABLES** command caused the query to fail. (132685/CSCze89153)
- Resolved an issue where, in some cases, performing remote backups of managed devices generated large backup files on your Defense Center. (133040/CSCze89204)

- You can now edit the maximum transmission unit (MTU) of a managed device through the Interface tab of the Management Interfaces page (**System > Local > Configuration > Management Interfaces**) on the managed device's web interface. You can no longer edit the MTU of management interfaces of managed devices from the Defense Center. (133802/CSCze89748)
- Resolved an issue where the syslog alert message for events generated by intrusion rules with preprocessor options enabled caused a `Snort Alert` message instead of a customized message. (134270/CSCze88831)
- Resolved an issue where remediation failed if you configured an Nmap scan remediation with the **Fast Port Scan** and the **Use Port from Event** options enabled. (134499/CSCze88810)
- Resolved an issue where, if you enabled end-of-connection logging on a system in high availability, the system did not report sessions or reported an incorrect time stamp if the session was terminated prematurely. (134806/CSCze89822)
- Resolved an issue where communication issues between the Defense Center and cloud did not generate a health alert. (134888/CSCze90122)
- Resolved an issue where the system did not resolve host names associated with IPv6 addresses as expected in the dashboard or event views if you enabled **Resolve IP Addresses** from the Event View Settings page. (135182/CSCze90155)
- Custom HTTP response pages now support up to 50,000 plaintext characters. (136295/CSCze90383)
- Resolved an issue where the system displayed an incorrect number of submitted IP addresses in the tooltips on the Security Intelligence tab if you specified a Feed URL previously created on a computer running a Windows operating system. (136557/CSCze89888)
- Resolved an issue where, if you disabled a physical interface on a managed device, the status of the logical interfaces associated with the physical interface remained green on the Interfaces tab of the editor even though they were disabled. (136560/CSCze89894)
- Resolved an issue where the Defense Center displayed different task statuses on the Task Status page, the Access Control Policy page, and the Device Management page of the web interface if you applied an access control policy to multiple devices. (136614/CSCze89936)
- Resolved an issue where a custom intrusion rule with a TCP protocol condition generated events based on UDP traffic instead of TCP traffic. (136843/CSCze89941)
- Resolved an issue where the captured files table was erroneously listed as an option for a custom table base. (136844/CSCze89977)
- Resolved an issue where the system generated false positives for the 145:1, 145:2, 145:3, 145:4, 145:5, and 145:6 DNP3 preprocessor rules. (137145/CSCze90786)
- Resolved an issue where, if you registered a managed device with a hostname containing more than 40 characters, device registration failed. (137235/CSCze90144)
- Resolved an issue where the system did not correctly filter objects in the Object Manager if you included any of the following special characters in the filter criteria: dollar sign ($), caret (^), asterisk (*), brackets ([ ]), vertical bar (|), forward slash (\), period (.), and question mark (?). (137493/CSCze90413)
- Resolved an issue where, if you enabled Simple Network Management Protocol (SNMP) polling in your system policy and modified the interface configuration on one of your clustered managed devices, the system generated inaccurate SNMP polling requests. (137546/CSCze90000)
- Resolved an issue where enabling syslog or Simple Network Management Protocol (SNMP) connection logging in an access control rule caused system issues. (137952/CSCze90538)

- Resolved an issue where the table view of file events appeared to support viewing the file trajectory by file name even without a calculated SHA256 value. (138155/CSCze90676)
- Resolved an issue where the system did not display UTF-8 characters in the x-axis filenames if you generated a report in HTML or PDF format that included a chart with **File Name** as the x-axis. (138297/CSCze90799)
- Resolved an issue where, in rare cases, revising and reapplying an intrusion policy hundreds of times caused intrusion rule updates and system updates to require over 24 hours to complete. (138333/CSCze90747)
- Resolved an issue where the system generated an error message if you attempted to update the geolocation database (GeoDB) to the version already installed on your Defense Center. (138348/CSCze90813)
- Resolved an issue where connection events logged to an external syslog or Simple Network Management Protocol (SNMP) trap server had incorrect **URL Reputation** values. (138504/CSCze91066)
- Resolved an issue where applying more than one access control policy across your deployment and searching for intrusion or connection events matching a specific access control rule retrieved events generated by unrelated rules in other policies. (138542/CSCze91690)
- Resolved an issue where cutting and pasting access control rules appeared to be supported. (138713/CSCze91012)
- Resolved an issue where, if your Defense Center was running Version 5.3 with eStreamer running Version 5.3, the security intelligence events on your Defense Center incorrectly reversed the values of the destination IP and the source IP. (138740/CSCze91402)
- Resolved an issue where the system did not generate a warning about ignored inline normalization settings if you applied an intrusion policy set to **drop when inline** to a device with passive interfaces. (139177/CSCze91163)
- Resolved an issue where, in rare cases, the Task Status page incorrectly reported a failed system policy apply was successful. (139428/CSCze92142)
- Resolved an issue where the system did not enforce the maximum transmission unit (MTU) setting on Series 2 or virtual devices. (139620/CSCze91705)
- Resolved an issue where, if you configured and saved three or more intrusion policies that referenced each other through their base policies, the system did not update the **Last Modified** dates for the policies on the Intrusion Policy page. (139647/CSCze91353)
- Resolved an issue where, if you configured and saved a report with a time window that included the transition day from observing Daylight Saving Time (DST) to not observing DST, the system adjusted the time window to begin an hour earlier than specified. (139713/CSCze91697)
- Resolved an issue where, if you switched interfaces between the virtual routers on your managed devices, the system did not activate the dormant static route for the switched interfaces. (139929/CSCze91619)
- Resolved an issue where, if you did not register a device to your Defense Center and your Defense Center had no data, viewing the Intrusion Events Graph page (**Overview > Summary > Intrusion Event Graphs**) caused a **WARNING: normalizations disabled because not inline** error. (140117/CSCze92324)
- Resolved an issue where the system did not prevent an externally authenticated user from modifying their password using the FireSIGHT System web interface. (140143/CSCze91938)
- Resolved an issue where custom HTTPS certificates could be imported only once. (140283/CSCze92162)
- Resolved an issue where creating a new task on the Scheduling page (**System > Tools > Scheduling**) caused the system to display an authorization error message. (140575/CSCze92225)
- Resolved an issue where bypass mode appeared as an option for clustered devices even though the option could not be enabled. (140604/CSCze92047)
- Resolved an issue where reports created in bar graph form displayed a maximum of 10 days. (140833/CSCze92405)

- Resolved an issue where the **Password Lifetime** column on the User Management page displayed a negative value if a user's password expired. (140839/CSCze92338)
- Resolved an issue where, if you disabled an access control rule referencing an intrusion policy and then reapplied your access control policy, the system incorrectly indicated the appliance's intrusion policy was out of date. (141044/CSCze92012)
- Resolved an issue where you could not delete third-party vulnerabilities. (141103/CSCze92621)
- Resolved an issue where files intentionally not stored by the system incorrectly appeared with a **Failed File Storage** value in the event viewer and dashboard. (141196/CSCze92629)
- Resolved an issue where the system-provided saved search **Public Addresses Only** included the private 172.16.0.0/12 IP address range. (141285/CSCze92654)
- Resolved an issue where, if you updated your Defense Center to Version 5.4, the update wrote over any changes made to the Connection Summary dashboard (**Overview > Dashboards > Connection Summary**). (141363/CSCze92812)
- Resolved an issue where reports did not resolve host names for IP addresses. (141393/CSCze92797)
- Resolved an issue where, if you enabled **HTTP Block Response** in an access control policy and the web server's operating host reached its open connection limit, HTTP Block Response caused sessions to remain open and the web server to time out. (141440/CSCze92753)
- Resolved an issue where excessive saved revisions to the intrusion policy caused system performance issues. (141501/CSCze92792)
- Resolved an issue where the passive interfaces not in security zones on 3D9900 devices did not generate intrusion or connection events. (141663/CSCze93022)
- You can now enable rules from the packet view of a generated event when you select the **Set this rule to generate events in all locally created policies** option from the actions menu. (142058/CSCze93416)
- Resolved an issue where, in rare cases, Series 3 devices experienced delays during device shutdown. (142110/CSCze93561)
- Resolved an issue where, if the Defense Center sent a file to the cloud to perform a dynamic analysis in a sandbox environment and the cloud was not available within 50 minutes, the file's status remained **Sent for Analysis** instead of a timed out status. (142309/CSCze93757)
- Resolved an issue where, if the Defense Center incorrectly assigned an invalid serial header, the Defense Center failed to send events to the eStreamer client. (143201/CSCze93686)
- Resolved an issue where, if you clicked on an application in the Denied Connections by Application dashboard widget, the system did not properly constrain the resulting event view to blocked connections. (143376/CSCze93645)
- Resolved an issue where, if you generated a report in CSV format only, report section queries would ignore the option to inherit the time window. (143403/CSCze94376)
- Resolved an issue where the Modbus preprocessor failed to generate events after the system missed or dropped a packet. (142450/CSCze95921)
- Resolved an issue where, if you created an access control policy that referenced an SSL policy set to decrypt traffic, policy apply failed. (144518/CSCze94864)
- Resolved an issue where, if you created an intrusion policy or network analysis policy and added a shared layer to it, then exported and imported the new policy the system generated a **Back-end failed for import** error and did not import the policy. (144905/CSCze96093)

Known Issues

The following known issues are reported in Version 5.4.0.10 and Version 5.4.1.9:

- If you change the DNS settings on an ASA FirePOWER module (ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X), the changes do not take effect unless network services are restarted. (CSCuu91139)
- If you configure inline set to bypass and restart the device, the device incorrectly takes the inline set out of bypass mode when it should not. (CSCuw82385)
- The system does not send an alert when someone logs in to a FireSIGHT appliance or Defense Center console. (CSCuy63018)
- If you uninstall a Version 5.4.x patch, the uninstallation process does not warn you to not reboot the device during the uninstallation when it should. (CSCuy74827)
- If you configure global thresholding on a pair of Defense Centers in high-availability mode, the system may not send all thresholded intrusion events to both Defense Centers in the pair and the primary Defense Center may appear to generate more intrusion events than the secondary Defense Center. (CSCuy79899)
- Captured files are seeing being pruned from disk randomly instead of oldest first. This is causing some recently captured files to be unable to be send for analysis when older files can. (CSCuz76009)
- If you generate troubleshoot on 3D8140 or 3D8250 devices, the troubleshoot may not detect all hardware errors when it should. (CSCuz82318)
- If you execute the **show fastpath-rules** CLI command on a 8000 series device, the system incorrectly displays **Default Domain** for each fast path rule instead of the actual domain name. (CSCva03481)
- If you select **Inspect Archive** in the advance settings of file policy rule and enable **Block Uninspectable Archives**, downloading any GZ archive file of a text document getting blocked with file events on Defense Center showing Archive Block (Failed to Inspect). As a workaround, disable **Block Uninspectable Archives** in the file policy rule. (CSCva10734)
- The second port, **eht2**, of an NGIPSv device configured for inline mode does not show traffic statistics when it should. (CSCva90898)
- The Asia/Sakhalin timezone is incorrectly displayed as GMT+10 instead of FMT+11. (CSCvb25965)
- CPU wait time is consistently higher then expected. (CSCvb97471)
- If you deploy a NAT policy to a Series 3 device and execute the **show NAT flows <allocator #** CLI command, the series 3 device displays incorrect information. (CSCvc09017)
- Firewall rules may not be in sync with firmware rules following policy apply. (CSCvc09167)
- Managed devices running Version 5.4.0.9 or later may experience extraneous syslog messages and, in rare cases, may cause general latency or system issues. (CSCvc11205), CSCvc11209
- URL filtering does not work as expected if the URL database from Version 5.4.0 on a managed device updates. (CSCvc17167)
- The memory usage values displayed in the generated health events may not match the configured threshold values when it should. (CSCvc49476)
- If you switch an ASA FirePOWER module to multi-context mode and a context name contains lag, such as flag, and deploy at least one access control rule containing security zones, traffic does not match against rules with security zones when it should. As a workaround, delete the existing context and copy the configuration to a context that does not have lag in the context name. (CSCvc53358)
- (CSCvc63125)

- The /var/log/messages directory on a managed device may incorrectly fill up with extraneous network map messages. (CSCvc66614)
- If the health monitor may generate a **The cloud databases for these appliances are not synced** health alert and the system contains an out-of-date cloud database file on the sensor, contact Cisco TAC. (CSCvc84721)
- If a stack has entered maintenance mode due to an issue or failure on a secondary unit, use of the manage_procs.pl script can bring that stack out of maintenance mode even if the issue has not been resolved. (CSCvc94207)
- If you configure a stacked 3D8370 for inline mode and the secondary device experiences a failure, the primary device within the stack goes into maintenance mode as expected. If you execute the manage_procs.pl script and select options 3 and 5) to fix the issue, with Defense Center moves the primary device within the stack out of maintenance mode when it should not and the stack experiences an outage. (CSCvd05708)
- Time stamp does not show for SHA list files if description has double quotes or if it is too long. (CSCvd09165)
- The system may generate extraneous error messages in the **/var/log/messages** directory and syslog. (CSCvd12448)
- If you click **Add Device** or **Connect** in the Device Management panel on left side of ASDM dashboard, the ASDM interface generates a generic **Can't Connect to Device** message when trying to add or connect to the ASA FirePOWER module. instead of providing why the action fails. (CSCvd13575)
- If you enable STIG, the Defense Center web interface allows you to disable STIG in Single Mode when it should not. To correctly disable STIF, contact Cisco TAC. (CSCvd20895)
- If you enable the modbus preprocessor and deploy an intrusion policy, the system generates intrusion events with the incorrect **MODBUS_BAD_LENGTH** type. (CSCvd28945)
- If you plan to update the system to Version 6.0, you must install the FireSIGHT System Version 6.0 Pre-Installation package before you update to Version 6.0. For more information, see the *FireSIGHT System Release Notes Version 6.0 Pre-Installation Package*.

The following known issues were reported in previous releases:

- In some cases, if a Microsoft Windows update occurs on a client transferring a file, detection of that file fails because the client transmits pieces of the file in separate sessions that the system cannot reassemble to detect the complete file. (112284/CSCze88424)
- The system requires additional time to reboot appliances or ASA FirePOWER modules running Version 5.3 or later due to a database check. If errors are found during the database check, the reboot requires additional time to repair the database. (135564, 136439)
- In rare cases, if you request archived eStreamer events, the system may not return all the events between the requested timestamp and the current time. Requesting current eStreamer events functions correctly. (142742/CSCze94012)
- If you create a new report (**Overview > Reporting > Report Templates**) and attempt to insert a report parameter while viewing the web interface with Internet Explorer 11, no report parameters are added to the report section description. As a workaround, use Internet Explorer 10. (142950/CSCze94011)
- In some cases, your system may generate extraneous health alarms if your RAID controller is placed into power saving mode. (142214/CSCze87267)
- In some cases, if you attempt to use the SFR **system restart** CLI command while logged in with the ASA session command, the device may stop processes and not restart them. This affects all devices except the ASA5506-X. (143135/CSCze94403)

- In some cases, if you create an access control rule set with an interactive block action and enable beginning-of-connection logging or both beginning-of-connection and end-of-connection logging, the system does not log beginning-of-connection events with the reason **User Bypass**. (143357/CSCze93672, 144167/CSCze94675)
- In some cases, if your clustered Series 3 devices go into maintenance mode, then experience a power failure and you attempt to reboot the devices, the system does not recover. Contact Cisco TAC if your device does not successfully recover from maintenance mode. (143504/CSCze94928)
- In some cases, if you create an access control rule set to allow traffic that references an SSL rule set to **Decrypt-Resign** and an intrusion rule set to drop when inline, the system incorrectly displays the SSL Status as `Unknown` in the intrusion events table view (**Analysis > Intrusion > Events**). (143665/CSCze94947)
- In some cases, your access control policies may appear as out-of-date even when they are not. (14412/CSCze95029)
- In some cases, if you apply an access control policy referencing two intrusion policies to two devices, then edit the first intrusion policy, then reapply the policy to one device and cluster the two devices, the modified intrusion policy is marked out-of-date on the second device. As a workaround, apply a different access control policy with the same intrusion policies to the second device. (144136/CSCze95126)
- In some cases, if you create an access control policy referencing a rule with the HTTP response page set with an Interactive Block action and you attempt to access a URL that generates an HTTP response page, you are unable to access the same web page in additional tabs on the same browser. (144419/CSCze95694)
- In some cases, the system may not display policy-related information for the following columns on the Connection Events table view (**Analysis > Connections > Events**): **Action, Reason, Access Control Policy, Access Control Rule**, and **Network Analysis Policy**. (145142/CSCze95299)
- In some cases, the system does not display any events in the **Total Events**, **Total Events Last Hour**, or **Total Events Last Day** rows of the statistics summary of the Discovery Statistics page (**Overview > Summary > Discovery Statistics**). (145153/CSCze95751)
- Your device may experience a prolonged wait period when powering on. (145248/CSCze96068)
- In some cases, if you enable a fail-open Cisco Redundancy Protocol (SFRP) set to monitor-only on a ASA 5515 module in a high availability configuration and your device experiences a failover, your module may change from active to standby mode several times when it should not. (145256/CSCze95812)
- If you configure an ASA FirePOWER module running Version 5.0 or later with network address translation (NAT), the system incorrectly processes data channels matching applied access control, intrusion, and network discovery policies. (145274/CSCze96017)
- In some cases, if you make changes on the Advanced Malware Protection Alerts tab of the Alerts page (**Policies > Actions > Alerts**) on a system configured with high availability, the changes may not be synchronized properly between the appliances. (CSCur46711)
- In some cases, if you create an intrusion rule set to block Multiprotocol Label Switching (MPLS) traffic and specify either a source IP address or a destination IP address, the system does not block matching traffic. (CSCur46880)
- If you do not deactivate a traffic profile before deleting it, the system allows the deleted profile to continuously use resources without generating traffic. (CSCur48345)
- In some cases, if you configure your cluster of routed Series 3 managed devices with Cisco Redundancy Protocol (SFRP) and apply a network address translation (NAT) rule, both the primary and secondary devices of the cluster respond to the address resolution protocol (ARP) detected in matching traffic when only the primary device should respond. As a workaround, designate the SFRP interface on the primary device as the master interface and the SFRP on the secondary device as the backup interface when creating a NAT rule for your clustered devices. (CSCur55568)

- If you create a scheduled task to install a new version of the vulnerability database (VDB) on your Defense Center, the system will not alert you if you already have a recent VDB version installed and the Defense Center switches from active to standby mode every time the task is scheduled. Cisco does not recommend scheduling automatic VDB updates. (CSCur59252)
- If you use an invalid IP address when configuring the DNS preprocessor in an intrusion policy on an 81xx Family device, system functionality may slow down exponentially. To resolve this issue, enter a valid IP address and reapply the intrusion policy. (CSCur59598)
- In some cases, the Device tab of the Device Management page (**Devices > Device Management**) displays **yes** for licenses that may have expired or been removed from the registered device when it should display **no**. (CSCur61884)
- In some cases, if you delete a protection license from the licenses page (**System > Licenses**), the system does not decrement the number of used licenses when it should. As a workaround, disable the license from the Device Management page (**Devices > Device Management**). (CSCur61927)
- You cannot apply an existing intrusion policy that is not referenced in the currently-applied access control policy. (CSCur72904)
- An intrusion detected on the ASA5506-X device may not generate alerts for gzip compressed HTTP traffic or chunked HTTP response data where the decompressed or non-chunked data would match. (CSCur77397)
- In some cases, if your system loses connectivity between the Defense Center and device during policy apply, the Network Discovery page (**Policies** > **Network Discovery**) displays **apply to devices**. As a workaround, edit the network discovery policy and reapply. (CSCur81583)
- If you create an intrusion policy referencing a network analysis policy that is set to **Ignore Audio/Video Data Channel**, the system generates alerts for session initiation protocol (SIP) audio data when it should not. (CSCur83184)
- If you manually configure the time of the Defense Center or managed device into the past, the Health Monitor page (**Health > Health Monitor**) does not display alerts. (CSCur85894)
- In some cases, if you configure the router interface of your clustered Series 3 managed devices to both a private IP address and a Cisco Redundancy Protocol (SFRP) IP address, the system does not recognize which IP address is the primary address and does not establish an Open Shortest Path First (OSPF) connection. (CSCur86355)
- In some cases, if you create a network analysis policy with the HTTP preprocessor enabled and **Unlimited Decompression** enabled, and an intrusion rule set to alert for data within gzip compressed HTTP traffic, the system may not generate alerts for traffic matching the applied intrusion rule beyond 65535 bytes of decompressed data. (CSCur87659)
- In some cases, if you change the selected time zone in the Time Zone Preference tab on the User Preferences page (**Admin > User Preferences > Time Zone Preference**), the system may not incorporate daylight savings time and may display the wrong time. (CSCur92028)
- In some cases, if you apply a large database and attempt to create a troubleshoot file on your Defense Center, the system utilizes extraneous memory for the task and generates an **Out of memory!** error. (CSCur97450)
- If BIOS Version 2.0.1b is not running on your DC2000 and DC4000 appliances before updating to Version 5.4.1.1 or later, the update fails. If the update fails due to an earlier BIOS Version running on your Defense Centers, contact Cisco TAC. (CSCus10407)
- You may encounter false positives on the detection of the Sametime application. (CSCus17165)
- You cannot reset the password for the admin user on the ASA5585-X device. (CSCus17991)
- Running troubleshooting on your system may cause latency. (CSCus19876)

- In some cases, indications of compromise (IOC) cannot be removed or resolved from the IOC table view (**Analysis > Hosts > Indications of Compromise**) if the host associated with the event has been retired. (CSCus24116)
- In some cases, if you have a single trusted certificate authority (CA) group or object referenced in your applied SSL policy, the system does not allow you to remove the group or object from the policy. As a workaround, add a different CA group or object to the policy and remove the trusted CA group or object from the current SSL policy. (CSCus42239)
- In some cases, if you add an Cisco IOS Null Route instance to your Cisco IOS remediation and enable your password to log into the router, the device does not enable the password and the remediation fails. As a workaround, do not select to enable the password. (CSCus45769)
- If you apply an access control policy referencing Security Intelligence (SI) objects and policy apply fails, reapply you access control policy. If you are still unable to apply policy, contact Cisco TAC. (CSCus50470)
- If your ASA5506-X device running Version 5.4.1 does not have a URL license installed or if the license is unavailable, the Cloud Services page (**System > Local > Configuration**) erroneously displays a **Last URL filtering update** message with a timestamp. (CSCus51935)
- In some cases, if you create an URL individual object and add the individual object to an URL group object, then modify the group object, the tooltip for the individual object does not reflect the updated value of the group object. (CSCus51943)
- In some cases, if your URL license is unavailable or deleted and you attempt to add a new URL license, the **Enable Automatic Updates** option on the Cloud Services page (**System > Local > Configuration**) is not checked by default when it should. (CSCus53842)
- In some cases, if you deploy a network analysis policy (NAP) and enable inline mode, connection events generated by HTTPS traffic does not display the correct total bytes value. (CSCus59142)
- In some cases, if you install the new intrusion rule update and then restore a backup to your device, the system erroneously generates an **Intrusion Policy is out-of-date** message whether the intrusion policy existed before or after the rule update. (CSCus59479)
- In some cases, if your access control policy includes a source and destination address that contains **::/0**, the connection events table view (**Analysis > Connections > Events**) contains events generated from IPv4 and IPv6 traffic when only IPV6 traffic should be allowed. (CSCus63549)In some cases, if you change the order of access control rules and apply, policy apply fails. (CSCus64721)
- If you cannot connect to the Cisco cloud through your authorization proxy but you can connect through direct connection, contact Cisco TAC. (CSCus83379)
- In some cases, if you apply an access control policy to an ASA5506-X device from a Defense Center, and the policy is associated with multiple intrusion policies where many rules are enabled, policy apply fails. As a workaround, use fewer policies. Each unique combination of an intrusion policy and variable set counts as a policy, and the network access policy associated with the access control policy counts as a policy. (CSCus95519)
- Resolved an issue where, if you created an access control policy containing a file policy with dynamic analysis enabled, the connectivity to the Collective Security Intelligence Cloud needed for dynamic analysis failed if the proxy port was configured to be port 80. (CSCut01361)
- In some cases, if you create an access control policy that references an SSL policy with **Inspect Local Router Traffic** enabled, the system experiences issues. As a workaround, do not enable the **Inspect Local Router Traffic** option. (CSCut12631)
- The Backup Management tab of the Backup/Restore page (**System > Tools > Backup/Restore**) does not include registered ASA55X5 or ASA55X5-SSP-XX devices as options. (CSCut41338)
- In some cases, if you set up a scan instance for a Nmap module, the Remote Operating System Detection may incorrectly identify the version of detected operating system. As a workaround, refer to the Host Script Output for the correct OS. (CSCut23654)

- If you apply an access control policy with an associated policy that requires a firewall preprocessor, then apply an access control policy that does not require the firewall preprocessor, the firewall preprocessor remains enabled when it should not. As a workaround, apply the access control policy that does not require the firewall preprocessor again, such as a basic access control policy or the default access control policy. (CSCuu53467)
- In some cases, if you update a pair of Defense Center in a high availability configuration, the secondary Defense Center's access control policies may appear up-to-date while the primary Defense Center's access control policies are not. Note that the system should report the correct status for objects and policies referenced by the access control policies. (CSCut63260)
- In some cases, if you create and edit a search for generated events, then cancel the search before the search starts, the system redirects you to the events page related to the search and displays an incorrect search name. (CSCut63265/CSCuu97738)
- In some cases, the network map experiences issues if the last entry in the rna map list is a duplicate. If you experience issues with SFDatacorrelator performance, contact Cisco TAC. (CSCut65738)
- In some cases, if you edit the Interfaces page (**Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**) of an ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, or ASA 5516-X and add a security zone, then click **Store ASA FirePOWER Changes**, the system generates an **Unable to load container (311014dd-c9b1-4ae4-b566-ad2b128a7d57)** error. (CSCut85300)
- FirePOWER services are unavailble during the update process if you update the following Cisco ASA with FirePOWER Servicesfrom Version 5.4.1 to Version 5.4.1.1: ASA5506-X, ASA506H-X, ASA5506W-X, ASA5508-X, ASA5516-X. FirePOWER services are available after updating your devices. As a workaround, use the **tail -f /var/log/sf/Cisco_network_sensor_Patch-5.4.1.1_main_upgrade_script.log** command through SSH to observe the update process and restart the Adaptive Security Device Manager (ASDM) on your ASA module after the update finishes. (CSCut89599)
- In some cases, if the sensing interfaces configured for inline deployment are down while the system restarts, Snort continuously restarts. (CSCut93464)
- In some cases, your 3D8xx device may experience an error and lose control and info channels. (CSCut98395)
- If you break a cluster of devices containing a NAT policy with the **Remove the interface configurations on <device name>** option selected, then policy apply on the secondary device fails after breaking the cluster. As a workaround, de-select **Remove the interface configurations on <device name>** when separating the clustered devices. (CSCut98774)
- If you attempt to update your device and experience system issues after updating, such as not being able to access your device, contact Cisco TAC. (CSCuu01055)
- If you use the **system support run-rule-profiling** CLI command and a stack trace occurs, reapply the access control policy. (CSCuu02211)
- In some cases, a clustered ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, or ASA 5555-X device is separated from the cluster due to an erroneous health check failure. As a workaround, if the device status is healthy, add the device in the cluster again. (CSCuu10394
- In some cases, if you disable an access control rule referencing an intrusion policy, the Access Control page (**Policies** > **Access Control**) incorrectly displays the intrusion policy as out-of-date after the access control policy is successfully re-applied. The Intrusion Policy page (**Policies** > **Intrusion** > **Intrusion Policy**) will display the correct policy status. (CSCuu15483)
- In some cases, if you enable the use of a proxy on your Defense Center and **Create FireAMP Connection** on the Amp Management page (**Amp > Amp Management**), the system does not include **Private Cloud** in the Cloud Name drop-down list when it should. (CSCuu16374)
- The File Trajectory page (**Analysis** > **Files** > **Network File Trajectory**) displays the first and last host icons of a host with an indication of compromise as a blue icon instead of a red icon. (CSCuu17950)

- In some cases, if you register a ASA FirePOWER module to your Defense Center and reboot the ASA FirePOWER module, the data channel connection between the Defense Center and the VMware tool on the virtual ASA device experiences a disruption in connectivity. As a workaround, re-register your ASA device. (CSCuu18450)
- Adding an IP address to the Security Intelligence Global Whitelist does not add the IP address to an Access Control Policy as a Trust Rule. Adding an IP address to the Security Intelligence Global Blacklist will block all traffic to or from the identified IP address. (CSCuu20110)
- In some cases, if you create a file policy and a NAT policy and enable TCP stream preprocessor rules with a HTTP port number that is not an available port from the network access policy's HTTP preprocessor configuration page, the system does not detect malware in traffic that matches the file policy's configured action and downloads malware content when it should not. (CSCuu24472)
- The asterisk **(*)** character is a supported character in the **system file secure-copy** CLI command. (CSCuu25329)
- The system does not include audit log entries for login attempts with **<script>alert(1)</script>** as the user name. (CSCuu39516)
- The send email check box on the Report Templates tab of the Reporting page (**Overview > Reporting**) does not stay selected if you generate a report and then navigate away from the Report Templates tab. (CSCuu41580, CSCuv43116)
- In rare cases, if you apply an access control policy to an ASA FirePOWER module during the debug process, the system does not apply the access control rules even though the Defense Center's Task Status displays the apply successful. As a workaround, unregister the device from the Defense Center, register the device again, and reapply policy. (CSCuy25189)
- The system incorrectly allows an intrusion policy with a missing layer to be saved and does not generate a warning when it should. (CSCuy69895)
- If you apply more than one license to a clustered stack registered to a Defense Center and then move the clustered stack from one Defense Center to another Defense Center, not all of the licenses are successfully added during device registration and the Defense Center does not apply the access control policy to the cluster. As a workaround, manually apply the license to the clustered stack and then reapply policy. (CSCuy83290)
- If you install the Version 6.0.0 Pre-Installation Package on an appliance running Version 5.4 and then uninstall the Version 6.0.0 Pre-Installation Package, the system generates an I**nstallation failed: Unable to uninstall 5.4.1.999-2, only the last update (Sourcefire_3D_Defense_Center_S3_6.0.0_Pre-install-2) is eligible to be uninstalled at this time. Please uninstall it first** error message and you cannot uninstall the package. If you need to uninstall the Version 6.0.0 Pre-Installation Package from an appliance, contact Cisco TAC. (CSCuy85826)
- FirePOWER appliance SCP does not support reimage files 1GB or later. If you need to reimage an appliance and the reimage file is larger than 1GB, use alternative methods such as HTTP or FTP. (CSCuy88158)
- If you apply an access control policy with logging enabled, the system may not correctly identify the access control policy during the apply and generates **Unknown Object** errors in the Access Control Policy column of the Connection Events page (**Analysis > Connections > Events**). The system correctly identifies the access control policy for generated events after a successful policy apply. (CSCuy90101)
- In some cases, if you create an access control policy containing a geolocation condition, traffic that should match the condition fails to match. (CSCuu48800)
- In some cases, if you register a device to your Defense Center and then update the device, using the **configure manager <IP address> add** CLI command disables the Defense Center from managing the device. As a workaround, waiting for the device to automatically register to the Defense Center after updating. (CSCuu44265)
- In some cases, if you register and manage more than 100 devices on your Defense Center, the access control policy page may take up to several minutes to load. (CSCuu44646)
- In some cases, if you use the **system file copy** CLI command on a device, you may be unable to exit the CLI prompt. As a workaround, use **ctr+c** to exit the command back to the prompt. (CSCuu48793)

- In some cases, if your system accumulates large quantities of traffic for an extended period of time, you may experience latency and you may experience a disruption in traffic. (CSCuu52545)
- In some cases, if you create an access control policy referencing a network analysis policy and disable the Modbus Preprocessor, then enable all the Modbus rules in the Modbus preprocessor listed on the Rule Editor page (**Policies > Intrusion > Rule Editor**), the system does not automatically enable the Modbus preprocessor when it should. (CSCuu66121)
- In some cases, if you baseline a managed device to Version 5.4.x with the latest vulnerability database (VDB) and apply a network discovery policy, then browse with Internet Explorer Version 11, the Host Profile pop-window of any event and the Connection Events page (**Analysis > Connections > Events**) incorrectly reports the event with Internet Explorer 7. (CSCuu67292)
- In some cases, the system truncates user names or group names that contain 36 characters or more and are assigned to an access control policy even though documentation states 36 or more characters is supported. (CSCuu70235)
- If you configure a host input host using a MAC address, the system does not correctly store the MAC address and does not generate the MAC Address field in the Discovery Events page (**Analysis > Hosts > Discovery Events**). (CSCuu90757)
- If you have multiple devices registered to your Defense Center, the connection attempts to MySQL may fail. (CSCuu94784)
- In some cases, if you create an LDAP object in the Microsoft Active Directory and add the LDAP object to a user policy, then move the LDAP object, the Defense Center cannot locate the LDAP object. As a workaround, remove the LDAP group containing the LDAP object from the Users Policy page (**Policies > Users**) and **Fetch Groups** from the Defense Center, then add the group and recreate the LDAP object to the user policy. (CSCuu95350)
- In some cases, if you delete the permanent license from the Licenses page (**System > Licenses**), the Device Management page (**Devices > Device Management**) does not display **Unlicensed** for devices the permanent license was deleted from when it should and policy apply fails. As a workaround, edit the Licenses section of the Device page (**Devices > Device Management > Device**) and apply changes. (CSCuu96447)
- In some cases, the system does not display the correct number of bytes in the Top Web Applications Seen and Top Client Applications Seen widgets on the Summary Dashboard (**Overview > Dashboard > Summary Dashboard**) when your web browser is being used for high-volume media, such as video streaming. (CSCuu97036)
- In some cases, if you create a virtual router filter, the system incorrectly saves the virtual router OSPF Path Type as **Ext-2** instead of **Ext-1**. (CSCuv08158)
- In some cases, if you add a cluster and edit the interfaces, you are unable to edit the secondary interface and the system generates an **Unable to load container** error. (CSCuv25142)
- If you click the name of a file that contains extended characters in the table view for the Captured File Summary workflow (**Analysis** > **Files** > **Captured Files**), an internal server error occurs. (CSCuv40941)
- If you open the Discovery Statistics page (**Overview** > **Summary** > **Discovery Statistics**) on a Defense Center that does not have any discovery events, an internal server error occurs. (CSCuv42327)
- In some cases, if you create a file policy and enable the HTTP preprocessor, and the system detects a malware file containing a custom **SHA256** value, the system does not block the malware file when it should. (CSCuv59181)
- In some cases, if you remove a device registered to a Defense Center running Version 6.0 to a Defense Center running Version 5.4.1.2 or later, applying policy from the Defense Center running Version 5.4.1.2 fails. (CSCuv65650)
- In some cases, the system does not generate events for rules with the generator ID (GID) of **134** if the rule is configured to alert and latency-based performance settings are enabled in the access control policy. Note that latency-based performance is enabled by default (CSCuv70840)

- In some cases, if you apply policy and then compare policies, the access control policy comparison always generates differences even when there are none. (CSCuv76157)
- In some cases, if you create an access control rule configured with all countries selected as the destination or source country, the system does not match IPv6 traffic. As a workaround, create an access control rule configured with a single country selected as the destination or source country. (CSCuv93913)
- In some cases, policy apply to a registered Series 2 device may cause a network outage for up to 10 minutes. As a workaround, apply policy to registered Series 2 devices in the maintenance window. (CSCuv95966)
- In some cases, if you manually configure the time to a future time or date while applying a device configuration and then apply another device configuration with the current time or date to the same appliance, the device does not save the second device configuration when it should. (CSCuw01691)
- External authentication login to the Radius server does not support usernames with capitalized characters. (CSCuw19529)
- If you create an access control rule and set the default action to **Interactive Block**, then edit the interactive block response page on the HTTP Responses tab of the Default Access Control page (**Policies > Access Control**) in Japanese, the Interactive Block page does not generate a **Continue** button to bypass the interactive block page. (CSCuw21450)
- In some cases, if you view **All Events (Not Dropped)** in the Intrusion Events table view page of a 7000 Series or 8000 Series device and sort the table up to six fields including **Review By** and **Count** and then generate a report, report generation fails. As a workaround, exclude the **Review By** or **Count** field values or, if you include both the **Review By** and **Count** fields, include no more than three additional field values when generating a report from the intrusion events page. (CSCuw29993)
- In some cases, the system generates extraneous errors if you merge intrusion policy layers. (CSCuw34380)
- In some cases, the SFDatacorrelator experiences issue and does not correctly handle Snort messages. (CSCuw34423)
- The update process to Version 5.4.0 terminates existing login sessions on a serial or Lights-out Management (LOM) console and disables additional sessions until the update finishes. If you initiate the update with shell from a serial over LAN or LOM console without the **--detach** option, the update to Version 5.4.0 fails. (CSCuw65158)
- In some cases, your login session on a Defense Center during a system update expires before the update process finishes and your system does not successfully update. As a workaround, either click on different tabs in the web interfaces or create a scheduled task to download updates at an hourly interval to avoid session timeout. (CSCuw26878, CSCux04478)
- If you update at least one physical and at least one virtual device simultaneously, the update may fail and the devices that failed to update may be incorrectly placed into maintenance mode. As a workaround, reboot the devices that failed to update, unregister the devices and then register the devices to the Defense Center. Update devices once it is successfully registered to the Defense Center. (CSCux93946)
- The system cannot successfully apply policies if the detection engine is not running. (CSCuw44047)
- In some cases, if you form a cluster with two devices and break the cluster, then delete the devices from the Defense Center and re-register the devices, you are unable to successfully register the device that was previously the secondary peer of the cluster. (CSCuw48594)
- If you change the SSL CA certificate that is used for decryption in an SSL policy and apply an SSL policy containing a rule to a Cisco ASA with FirePOWER Services device or an ASA with Firepower Threat Defense device, the lock icon in the SSL Status column in the table view of the Connection Events page (**Analysis > Connections > Events**) is incorrectly grayed out for events generated by the SSL rule. As a workaround, disable the re-enable the SSL rule. (CSCuw51847)
- In some cases, if you change the management IP address through the web interface, the system does not update the configured broadcast address of the interface configuration for an ASA FirePOWER module. (CSCuw59460)

- In some cases, if you **Create Custom Workflow** on the Custom Workflows page (**Analysis > Custom > Custom Workflows**) for intrusion events and include **HTTP URI**,**HTTP Hostname**, and/or **Original Client IP** fields, marking intrusion events as reviewed generates an database error and the events do not get marked as reviewed. As a workaround, do not include the **HTTP URI**,**HTTP Hostname**, and/or **Original Client IP** fields when making a custom workflow to intrusion events. (CSCuw90541)
- If you update a Series 3 device from Version 5.4.0 to 5.4.0.2 or later and the system time is incorrectly set to date that is before **Oct 3, 2014**, the install fails. As a workaround, set the system date to the correct date prior to installing. (CSCuw62108)
- In some cases, updating virtual Defense Centers running VMware from a Version 5.4.x to a later Version of 5.4.x fails. As a workaround, individually install all the required patches to the virtual Defense Center. (CSCuw65577)
- In some cases, if you cluster two stacks of 3D8250 devices and apply an access control policy containing an intrusion policy, then the secondary stack in the cluster goes into maintenance mode and you edit the access control policy, applying the modified access control policy causes the system to incorrectly remove the access control policy from the active stack in the cluster. (CSCuw73470)
- In some cases, if you create an access control rule set with **Interactive Block** action, the system blocks only websites that end in **.com**. (CSCuw92220)
- In some cases, Cisco PIX Shun remediation through SSH is not successful on ASA FirePOWER modules that have **enable mode** passwords configured. As a workaround, disable the device password and resubmit the remediation. (CSCuw97173)
- In some cases, if you apply an access control rule that uses more than one VLAN, traffic that should trigger the applied access control rule incorrectly triggers other rules. (CSCuw99834)
- In some cases, if you view the Traffic by Initiator User widget on the Traffic tab of the Connection Summary page **(Overview > Dashboards > Connection Summary**) in a Firefox web browser running Version 43, the system does not display any data when it should. As a workaround, use an earlier version of Firefox or a different web browser to view the Connection Summary page. (CSCuw99854)
- If the Defense Center runs out of disk space but resolves the issue on its own, the system may still fail to store and display new event information and generate **All shard connections are busy for partition** errors in the Syslog page (**System > Monitoring > Syslog**). As a workaround, reboot the system. If the system continues to experience issues, contact Cisco TAC. (CSCux00142)
- In some cases, if you configure automated policy apply for an extended period of time and attempt to manually apply a policy, policy apply fails and the system generates a **the table 'EOContainerStore' is full** error in the Health Events page (**Health > Health Events**). (CSCux00455)
- The system may experience dropped packets if you edit the access control policy to an intrusion preventative default action and apply to registered devices configured with routed, transparent, or inline interfaces. (CSCux02726)
- In some cases, if you add a security zone to an access control policy and apply, the system does not correctly process traffic. If you add security zones to your applied access control policy and suspect your traffic is being incorrectly processed or blocked, disable the security zones in your access control policy. (CSCux05653)
- In some cases, if you configure 3D8250 or 3D8350 devices with a virtual switch and the system experiences a failover, the IP and MAC address switch from the primary device to the secondary device and ARP traffic that passed through a specific interface on the switch before the failover is incorrectly processed when passed through a difference interface on the switch. (CSCux11121)
- In some cases, if user IP and group mappings are being streamed to a managed device while the mappings are being updated on the Defense Center, the network map on the managed device may not update correctly and may not match the network map on the Defense Center. If your Defense Center and managed devices appear to have different network maps, contact Cisco TAC. (CSCux12245)

- In rare cases, the ASDM user interface does not successfully load the configuration page or the statstics page and you cannot access ASA FirePOWER module logging. As a workaround, restart the ASDM. (CSCux12539)
- In some cases, if you baseline a device to Version 5.3 and update to Version 5.4.0 and apply an access control policy configured with inline normalization or if you configure a managed device's available interfaces to passive mode and apply an access control policy configured with inline normalization, the system does not generate a warning when it should. (CSCux23258)
- In some cases, if you enable automatic application bypass (AAB) on your 3D7010 device and generate troubleshoot, AAB activates when it should not. (CSCux46403)
- The system does not automatically trim oversized UDP packets to match the configured MTU value when it should and over time drops traffic that is oversized. (CSCux51826)
- In some cases, updating a managed device fails and the system does not indicate why in Task Status. If you update a device and the update fails without a reason, contact Cisco TAC. (CSCux56288)
- In some cases, if you configure two intrusion policies to share layers and you compare the two policies without editing either policy, the system incorrectly displays differences between the two policies when there should be no changes. (CSCux59094)
- In some cases, if you set the default time zone to **Europe** and **Moscow** on the Time Zone Preference tab (**User Name > User Preferences > Time Zone Preference**), the system displays an incorrect timestamp on generated events. (CSCux66887)
- If you hover the mouse cursor over the **Last Contacted** icon in the Management tab of the Device Management page (**Devices > Device Management**), the system incorrectly displays the timestamp without a colon separating the hour from the minutes. (CSCux68570)
- If you download the **Sourcefire EventStreamer SDK 5.4.0** file from the Cisco Support site and attempt to install on a device running Windows OS, the install fails. As a workaround, remove **2> /dev/null** from line 58 of the **SFPkcs12.pm** file, located in the EventStreamerSDK-5.4.0\examples\perl_client directory and install. (CSCux76998)
- In some cases, if you apply a file policy set to **Detect Files** or **Block Malware** to a virtual device configured with inline sets, the system inconsistently detects or blocks packets containing PDF, zip, gzip bzip exe file types. (CSCux81938)
- In some cases, if you apply a file rule with the action set to **Detect Files** or **Block Files** to a device registered to a system running Version 5.4.0.4 or later, the system may not correctly detect and block the file types or decompress the archives correctly, as can be seen on the File Summary page (**Analysis > Files > Events**) and the Connection Events page (**Analysis > Connections > Events**). (CSCux81952)
- In some cases, if you stack two 3D8350 devices and apply an access control rule containing a large number of network objects, the system generates erroneous **Error sending cluster heartbeat from NFE0 to NFE0 on member 0:: Heartbeat timeout reached before ACK received** errors and does not successfully apply. As a workaround, disable the access control rule containing the large number of network objects and reapply, or delete the rule and create a new rule containing fewer network objects. (CSCux89473)
- In some cases, if you register a device running at least Version 5.4.0.2 or Version 5.4.1.1 to a Defense Center running Version 6.0, then de-register the device and register it to a Defense Center running at least Version 5.4.1.4, applying a policy from the Defense Center running 5.4.1.4 fails and the action queue displays a **Not a HASH reference** error. (CSCuy01340)
- In some cases, the system incorrectly deletes local report files even though the disk usage is not high and does not generate a warning or message. As a workaround, use remote storage for local reports. For more information, see the Using Remote Storage for Reports section of the *FireSIGHT System User Guide*. (CSCuy11976)
- If you filter intrusion rules on the Rule State page (**Rule Configuration > Rule State**) and search for the **FlowBit** keyword, the system generates inconsistent results. (CSCuy13901)

- If you apply an access control policy containing a file policy set to **Block Malware** and an SSL policy set to **Decrypt - Known key**, the system does not successfully complete the initial file transfer for incoming traffic when it should. As a workaround, download the file a second time. (CSCuy22114)
- If you update a system running Version 5.3.x to Version 5.4.0 or later, the system automatically sets the link mode to **Autonegotiate** even if the managed device does not support autonegotiation. As a workaround, manually set the link mode on the Device Management page (**Devices > Device Management**) and save. (CSCuy28028, CSCuy36266)
- If you modify a load balancing configuration with a CLI command and then apply policy, the system does not retain the load balancing configuration after a successful policy apply. You must execute the CLI command again to modify the load balancing configuration after each policy apply. (CSCuy30534)
- If you apply an SSL rule with the rule action set to **Decrypt-Resign** and browse decrypted websites using Chrome Version 40 or later, the browser generates alerts for the decrypted websites. As a workaround, use the Internet Explorer or Firefox web browser. (CSCuy30988)
- If you remove a user from all groups within a realm referenced in the access control policy and apply configuration changes, then click **Download users and groups** from the Access Control tab, the system does not update the applied configuration and continues to process traffic as if the group(s) still contained the user. (CSCuy39685)
- If you **Create Email Alert** on the Alerts page (**Policies > Actions > Alerts**) and enable the **Retrospective Events** configuration option on the Advanced Malware Protection Alerts tab, then save and apply, the system generates truncated emails when the alert is triggered when the emails should not be. (CSCuy49371)
- In some cases, if you enable the use of a proxy on the Defense Center and submit captured files to the Cisco cloud for dynamic analysis, the system generates a **Dynamic Analysis Failed (Network Issue)** error and does not successfully submit the files for analysis. (CSCuy49613)
- If you configure a manager on a Series 3 device and register the device to a Defense Center, then configure a second manager to the same Series 3 device, the second manager is successfully configured when it should not be and the device generates a **This sensor is already managed** warning. (CSCuy51043)
- In some cases, if you backup the system or files to a remote server with SCP and the connection to the remote server experiences latency, the backup fails. (CSCuy56306)
- In some cases, access control rules were not working for web applications and URLs that are SPDY-enabled. (CSCuy65157)
- The backup and restoration feature does not backup user login or user logout activity. (CSCuy87658)
- In some cases, if you create routed interfaces in the Interfaces tab of the Device Management page (**Devices > Device Management**) and edit the Ipv6 address assigned to routed interface configuration multiple times, applying configuration changes eventually fails. As a workaround, set the interface to **none** and apply changes, then assign the IPv6 address to the recreated routed interface and save. (CSCuy89243)
- In some cases, if you update a managed Series 3 or Cisco ASA with FirePOWER Services to Version 5.4.0.5 or later, the update fails even though the Defense Center displays the update successful. If you experience issues after updating a Series 3 or Cisco ASA with FirePOWER Services to Version 5.4.0.5 or later, contact Cisco TAC. (CSCuy94873)
- If you schedule a task on the Scheduling page (**System > Tools > Scheduling**) for **12:30 AM**, the web interface incorrectly displays the scheduled time as 12:00 AM even though the task will occur at the configured time. (CSCuz06444)
- In some cases, troubleshoot generation fails on a device with high quantities of files stored from a file inspection policy. (CSCuz13054)
- If you apply a network address translation (NAT) policy containing an excess of 32,000 rules, policy apply may fail. If policy apply fails after applying more than 32,000 NAT rules, contact Cisco TAC. (CSCuz21956, CSCva20501)

- In some cases, if you apply an access control policy with connection logging enabled and create a search from the Connection Events page (**Analysis > Connections > Connection Events**) for a **Traffic (KB)** field value, the system returns incorrect results. (CSCuz22965)
- If you create a correlation rule based on a malware event and include a filename containing a space as a condition, the system saves the correlation rule but you cannot edit the rule after the initial save. As a workaround, if you include a filename as a condition for a correlation rule based on malware events, do not include a space in the filename. (CSCuz23093)
- In some cases, the system experiences issues if the Automated application Bypass (AAB) is activated and policy apply fails. As a workaround, restart the device and increase the AAB timeout value, then reapply policy. (CSCuz52270, CSCuy56781)
- If you enable Lights-out Management (LOM) and use an IPv4 address when configuring the physical serial port for LOM, you are unable to ping the LOM interface even though LOM functionality operates normally. As a workaround, enable the DHCP option on the LOM Configuration page (**System > Local > Configuration > Console Configuration > Lights-Out Management Settings > IPv4 settings > Configuration**) and save, then disable the DHCP option and apply policy. (CSCuz62007)
- If the secondary Defense Center in a pair does not contain the same intrusion policy layers as the primary Defense Center, or if the Defense Centers within a pair do not successfully complete syncing before the active switches to inactive, updating the Defense Center pair to Version 6.0.1 fails. (CSCuz72271)
- In some cases, if a Defense Center managing a stack of devices terminates Snort processes to free local memory space, the primary device of the registered stack stops sending heartbeats and the system generates health alerts. (CSCuz85435)
- You cannot edit the management interface speed on the Management Interfaces page (**System > Configuration > Management Interfaces**) on a DC2000 or DC4000. The system defaults to autonegotiate speed. (CSCva00537)
- In some cases, if you deploy an intrusion policy to an inline deployment and the intrusion rule threshold is triggered by traffic, the system correctly blocks traffic but generates connection events without the correct tag and appears to incorrectly allow traffic. (CSCva01799)
- If the secondary Defense Center within a pair does not contain the same intrusion policy layers as the primary Defense Center, or if the Defense Centers within a pair do not successfully complete synchronizing before the active Defense Center switches to inactive, updating the Defense Center pair fails. (CSCva18657)
- If you apply an SSL policy containing application rule conditions for SMTPS, POP3S, and IMAPS traffic, the system may incorrectly display **Unknown** as the application protocol in the Connection Events page (**Analysis > Connections > Events**). (CSCva20528)
- In rare cases, applying a policy for the first time to a 7000 Series or 8000 Series device with a fresh configuration fails and may cause additional health alerts. If policy apply to a registered 7000 Series or 8000 Series device after a fresh installation fails, contact Cisco TAC. (CSCva28854)
- If you are managing ASA with FirePOWER Services using ASDM, you may have issues with large update files (2GB+). If you attempt to upload a large update file to a device and receive a **Bad Gateway** error, use SCP or another secure method to **/var/sf/updates**. For assistance, contact Cisco TAC. (CSCva30354)
- If you enable failopen on a Series 3 device configured with inline sets and then update the device, the device may incorrectly drop link connectivity for up to 10 seconds before it goes into hardware bypass mode. (CSCva40041)
- In some cases, if a non-authoritative logon arrives at the Defense Center, and logoff does not occur, and then an authoritative logon arrives at the Defense Center for the same user/IP, the new authoritative logon is not sent to the managed devices. (CSCva43130)
- If you apply a file policy with logging to a device with Automatic Application Bypass (AAB) enabled, excessive logging may incorrectly trigger AAB. (CSCva62240)

- If you configure a physical serial port on the Console Configuration page (**System > Local > Configuration > Console Configuration**) of a DC4000 and save, but cancel the option to reboot the system, the system incorrectly defaults to Lights-out Management after rebooting. (CSCva72374)
- If you create an LDAP connection for user awareness and add a corrupt SSL certificate or an SSL certificate containing a **.txt** file extension, then update the system, the update fails. As a workaround, check the SSL certificate prior to updating the system. If the certificate is corrupted, remove the LDAP connection or remove the corrupted certificate from the LDAP connection prior to updating the system. If you update the system and the update fails, contact Cisco TAC. (CSCva98606)
- The status of the inactive device of a Defense Center pair on the High Availability page (**System > Registration > High Availability**) incorrectly states **This DC became inactive** instead of when the device was last synchronized. (CSCvb09634)
- If you deploy an access control policy with an intrusion policy added from the I**ntrusion Policy used before Access Control rule is determined** drop-down menu in the Advanced tab of the Access Control Policy page (**Policies > Access Control**), the system does not execute the action of the intrusion policy. (CSCvb27856)
- If you apply an SSL policy with the default action set to **Decrypt - Resign**, traffic from certain servers is not decrypted when it should be and causes a handshake error. (CSCvb27930, CSCvb28005)
- If you change the hostname of a registered device in the Device Management page (**Devices > Device Management**) and save, the Defense Center does not synchronize the new hostname in generated Health Monitor Alerts. As a workaround, restart the Defense Center. (CSCvb28289)
- If you include a tab space in a NAT rule name and apply policy, policy apply fails. As a workaround, manually remove the tab space from the NAT rule name and save, then reapply policy. If you continue to have issues, contact Cisco TAC. (CSCvb30980)
- Defense Center pairs managing very large numbers of sensors may incorrectly use an excessive amount of memory and synchronization may fail. (CSCvb36330)
- Adding more than one manager to an appliance with CLI and then registering the device to the Defense Center is not supported and causes device registration to fail. Only add one manager with CLI before registered to a Defense Center. (CSCvb40559)
- If you import a custom Security Intelligence feed, the Network Lists and Feed page (**Objects > Object Management > Security Intelligence > Network Lists and Feeds**) does not update the timestamp of the imported feed. (CSCvb54229)
- If you execute rule profiling with CLI and the sessions times out before the rule profiling finishes, the system does not generate the files from the rule profiling. As a workaround, set the access control policy's Shell Timeout value in the Shell Timeout page (**Devices > Platforms Settings > Shell Timeout**) to a longer value prior to executing rule profiling with CLI. (CSCvb56061)
- Version 5.4.0.9 and Version 5.4.1.8 do not install the correct intrusion rule updates. After updating the system to Version 5.4.0.9 or Version 5.4.1.8, you must download the latest intrusion rule update from Version 5.4.1.7 (2016-05-17 and later) from the Cisco Support page. (CSCvb57781)
- If you configure a manager on a device with the **configure manager add** CLI command, manager configuration may fail and the device will not register to the Defense Center. If the **configure manager add** CLI command fails, contact Cisco TAC. (CSCvb58876)

For Assistance

Thank you for choosing the FireSIGHT System.

Cisco Support

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information about Cisco ASA devices, 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 Cisco ASA devices, 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.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.