FireSIGHT System Release Notes

Version 5.4
First Published: March 24, 2015
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 instructions for the following appliances:

- Series 2 and Series 3 Defense Centers (the DC500, DC750, DC1000, DC1500, DC2000, DC3000, DC3500, and the DC4000)
- Series 2 and Series 3 managed devices (the 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500, 3D7010, 3D7020, 3D7030, 3D7050, 3D7110, 3D7115, 3D7120, 3D7125, 3D8120, 3D8130, 3D8140, 3D8250, 3D8260, 3D8270, 3D8290, 3D8350, 3D8360, 3D8370, 3D8390, 3D9900, AMP7150, AMP8050, AMP8150, and the AMP8350)
- Cisco ASA with FirePOWER Services (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)
- Cisco NGIPS for Blue Coat X-Series
- 64-bit virtual Defense Centers and managed devices

Note You cannot update Cisco NGIPS for Blue Coat X-Series running Version 5.3.0.x of the FireSIGHT System directly to Version 5.4. Instead, you must uninstall the previous version and install Version 5.4. Note that this results in the loss of all configuration and event data on the X-Series installation. For more information, see the *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*.

Note To reduce the time to update to Version 5.4.0, install the Version 5.4.0 Pre-Installation Package before you update. For more information, see FireSIGHT System Release Notes for the Version 5.4.0 Pre-Installation Package.

Cisco Systems, Inc.
www.cisco.com

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 of the FireSIGHT System. You can update Series 2 devices and Series 3 devices running at least Version 5.3.0.1 of the FireSIGHT System to Version 5.4. You can update Defense Centers and ASA FirePOWER modules running at least Version 5.3.1 to Version 5.4.

Caution

If you plan to use SSL policies, you must update your Version 5.4 managed devices to Version 5.4.0.1 and your Version 5.4 Defense Centers to Version 5.4.1.

For more information, see the following sections:

- New Features and Functionality, page 2
- Documentation Updates, page 7
- Before You Begin: Important Update and Compatibility Notes, page 8
- Installing the Update, page 12
- Resolved Issues, page 18
- Known Issues, page 22
- For Assistance, page 24

New Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 5.4 of the FireSIGHT System:

- Detection and Security Enhancements, page 2
- Platform Enhancements, page 3
- Enhancements for International Compatibility, page 4
- Changed Functionality, page 5
- Terminology, page 6

For detailed information, see the *FireSIGHT System User Guide*, *FireSIGHT System Installation Guide*, *FireSIGHT System Virtual Installation Guide*, and *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*.

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.

Caution If you plan to use SSL policies, you must update your Version 5.4 managed devices to Version 5.4.0.1 and your Version 5.4 Defense Centers to Version 5.4.1.

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.

Caution If you had either the latency packet handling or latency rule handling preprocessors disabled in a previously applied access control policy, updating your Defense Center to Version 5.4 automatically enables both preprocessors with high thresholds. To modify either preprocessor settings so they are no longer enabled, upgrade your Defense Center to Version 5.4.1 and disable either the **Packet Handling** option or the **Rule Handling** option in the Advanced Tab of the access control policy, then reapply your policies.

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 IoOC support from FireAMP Connectors

The list of Indicators of Compromise 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.

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 With the FireSIGHT System, Version 5.4, the supported ESXi versions are upgraded to 5.0, 5.1, and 5.5.

Support for vmxet3 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.

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.

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.

Dedicated AMP Appliances

Version 5.4 also introduces two 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 as the AMP8360, AMP8370, and AMP8390, for 2, 3, and 4 stacks, respectively.

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.

Enhancements for International Compatibility

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.

Changed Functionality

- SSL licenses are not available in Version 5.4. If you plan on using SSL policies, you must update your devices to Version 5.4.0.1 and your Defense Centers to Version 5.4.1.
- 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 via 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 via 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 via 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.

Terminology

If you reference documentation for Version 5.3.1.x or Version 5.3.0.x, you may notice the terminology differs from the documentation for Version 5.4.

Table 1 Changes to Terminology

Version 5.4 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*
Cisco NGIPS for Blue Coat X-Series	Formerly FireSIGHT software for X-Series or *Sourcefire Software for X-Series*
FireSIGHT managed devices	Refers to all devices managed by a FireSIGHT Defense Center (managed devices and ASA devices)

Table 1 Changes to Terminology

Version 5.4 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

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.

Documentation Updates

You can download all updated documentation from the Support site. In Version 5.4, 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*
- *FireSIGHT System Installation Guide*
- *FireSIGHT System Virtual Installation Guide*
- *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*
- *FireSIGHT System eStreamer Integration Guide*
- *FireSIGHT System Remediation API Guide*
- *FireSIGHT System Database Access Guide*
- *FireSIGHT System Host Input API Guide*

The documentation updated for Version 5.4 contains the following errors:

- The documentation for Version 5.4 does not reflect support for the new AMP8050 and AMP8350 models. For information on installation, specifications, and feature support for these models, refer to the documentation for the 3D8130 and the 3D8350, respectively. Note, however, that the AMP8050 and the AMP8350 contain a pre-installed malware storage pack SSD not included with those models. For information on use of the AMP8350 in a stacked configuration, see the information on the 3D8360, 3D8370, and 3D8390.

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.4, 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.

Note To reduce the time to update to Version 5.4.0, install the Version 5.4.0 Pre-Installation Package before you update. For more information, see FireSIGHT System Release Notes for the Version 5.4.0 Pre-Installation Package.

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, page 8
- Traffic Flow and Inspection During the Update, page 8
- Audit Logging During the Update, page 9
- Version Requirements for Updating to Version 5.4, page 9
- Time and Disk Space Requirements for Updating to Version 5.4, page 10
- Product Compatibility After Updating to Version 5.4, page 11
- Installing the Update, page 12

Configuration and Event Backup Guidelines

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

Use the 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.

Traffic Flow and Inspection During the Update

The update process reboots managed devices. Depending on how your devices are configured and deployed, the following capabilities are affected:

- traffic inspection, including application awareness and 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 devices, the system performs the update one device at a time to avoid traffic interruption.

Traffic Inspection and Link State

In an inline deployment, your managed devices (depending on model) can affect traffic flow via application control, user control, URL filtering, Security Intelligence, and intrusion prevention, as well as switching, routing, NAT, and VPN. For more information on appliance capabilities, see the *FireSIGHT System Installation Guide*.

The following table provides details on how traffic flow, inspection, and link state are affected during the update, depending on your deployment. Note that regardless of how you configured any inline sets, switching, routing, NAT, and VPN are **not** performed during the update process.

Table 1-2 Network Traffic Interruptions

Deployment	Network Traffic Interrupted?
Inline with configurable bypass (**Configurable bypass** option enabled for inline sets)	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 virtual devices, Cisco NGIPS for Blue Coat X-Series, Cisco ASA with FirePOWER Services, non-bypass NetMods on 8000 Series devices, or SFP transceivers on 71xx Family devices.
Inline	Network traffic is blocked throughout the update.
Passive	Network traffic is not interrupted, but also is not inspected during the update.

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 completes its pre-update tasks and the streamlined update interface page appears, login attempts to the appliance are not reflected in the audit log until the update process is complete and the appliance reboots.

Version Requirements for Updating to Version 5.4

A Defense Center must be running at least Version 5.3.1 to update to Version 5.4. If you are running an earlier version, you can obtain updates from the Support site.

A Defense Center must be running at least Version 5.4 to update its managed devices to Version 5.4.

The closer your appliances' current version to the release version (Version 5.4), the less time the update takes.

Time and Disk Space Requirements for Updating to Version 5.4

The table below provides disk space and time guidelines for the Version 5.4 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 Support.

Table 1-3 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Series 2 managed devices	1 MB	2.1 GB	477 MB	90-120 minutes
3D9900 managed devices	1 MB	1.6 GB	538 MB	70-90 minutes
Series 2 Defense Centers	1 MB	3 GB	n/a	80-100 minutes
Series 3 managed devices	1 MB	2 GB	545 MB	90-110 minutes
Series 3 Defense Centers	1 MB	2.8 GB	n/a	80-100 minutes
virtual Defense Centers	1 MB	2.8 GB	n/a	hardware dependent
virtual managed devices	1 MB	2.7 GB	538 MB	hardware dependent
ASA FirePOWER modules	1 MB	2.1 GB	428 MB	30-45 minutes

Product Compatibility After Updating to Version 5.4

You **must** use Version 5.4 of the Defense Center to manage devices running Version 5.4. Defense Centers running Version 5.4 can manage managed devices and ASA FirePOWER modules installed on ASA devices. Devices must be running the versions identified in the following table to be managed by a Defense Center.

Table 4 Version Requirements for Management

Appliance	Minimum Version to be Managed by a Defense Center Running Version 5.4
physical and virtual managed devices	Version 5.3.0.1 of the FireSIGHT System
Cisco NGIPS for Blue Coat X-Series	Version 5.3.0.1 of the FireSIGHT System
ASA FirePOWER modules	Version 5.3.1 of the FireSIGHT System

Note You cannot update Cisco NGIPS for Blue Coat X-Series running Version 5.3.0.x of the FireSIGHT System directly to Version 5.4. Instead, you must uninstall the previous version and install Version 5.4. Note that this results in the loss of all configuration and event data on the X-Series installation. For more information, see the *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*.

Operating System Compatibility

You can host 64-bit virtual appliances running Version 5.4 on the following hosting environments:

- VMware vSphere Hypervisor/VMware ESXi 5.0
- VMware vSphere Hypervisor/VMware ESXi 5.1
- VMware vSphere Hypervisor/VMware ESXi 5.5
- VMware vCloud Director 5.1

You can install ASA FirePOWER modules running Version 5.4 on the following ASA platforms running ASA Version 9.2(2.4) and later, ASA Version 9.2(3) and later, and ASA Version 9.2(4)and later:

- 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

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

You can run Version 5.4 of the Cisco NGIPS for Blue Coat X-Series on the X-Series platform running XOS Version 9.7.2 and later and Version 10.0 and later. For more information, see the *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*.

Web Browser Compatibility

Version 5.4 of the web interface for the FireSIGHT System has been tested on the browsers listed in the following table.

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

Table 5 Supported Web Browsers

Browser	Required Enabled Options and Settings
Chrome 40	JavaScript, cookies
Firefox 36	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**

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

Screen Resolution Compatibility

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.

Installing 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 8.

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

You can update Defense Centers and ASA FirePOWER modules running at least Version 5.3.1 of the FireSIGHT System to Version 5.4. You can update Series 2 devices running at least Version 5.3.1 of the FireSIGHT System to Version 5.4. To update your appliances to Version 5.4, see the guidelines and procedures outlined below:

- Updating Defense Centers, page 14

- Updating Managed Devices and ASA FirePOWER Modules, page 16

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.

Order of Installation

Update your Defense Centers before updating the devices they manage.

Installing the Update on Paired Defense Centers

When you begin to update one Defense Center in a high availability 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.

Installing the Update on Clustered Devices

When you install an update on clustered 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. The system then applies the update to the primary device, which follows the same process.

Installing the Update on Stacked Devices

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

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

Installing the Update on Cisco NGIPS for Blue Coat X-Series

You cannot update Cisco NGIPS for Blue Coat X-Series running Version 5.3.0.x of the FireSIGHT System directly to Version 5.4. Instead, you must uninstall the previous version and install Version 5.4. Note that this results in the loss of all configuration and event data on the X-Series installation. For more information, see the *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*.

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. Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *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, 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.

Updating Defense Centers

Note To reduce the time to update to Version 5.4.0, install the Version 5.4.0 Pre-Installation Package before you update. For more information, see FireSIGHT System Release Notes for the Version 5.4.0 Pre-Installation Package.

Use the procedure in this section to update your Defense Centers, including virtual Defense Centers. For the Version 5.4 update, Defense Centers reboot.

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 removes existing uninstallers from the appliance.

Note If you have inline normalization enabled and you update a Defense Center currently running Version 5.3.x to Version 5.4, the update process does not change the behavior of your policies. The system now adds user layers as necessary to preserve the settings that carried over.

To update a Defense Center:

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

For more information, see Before You Begin: Important Update and Compatibility Notes, page 8.

Step 2 Download the update from the Support site:

- for Series 2 Defense Centers:

  `Sourcefire_3D_Defense_Center_Upgrade-5.4.0-xxx.sh`
- for Series 3 and virtual Defense Centers:

  `Sourcefire_3D_Defense_Center_S3_Upgrade-5.4.0-xxx.sh`

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

Step 3 Upload the update to the 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.

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

Step 5 View the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

You **must** wait until any long-running tasks are complete before you begin the update. 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 completes. The task queue automatically refreshes every 10 seconds.

Step 6 Select **System > Updates**.

The Product Updates tab appears.

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

The Install Update page appears.

Step 8 Select the 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 completes its necessary pre-update checks, you are logged out. When you log back in, the Upgrade Status page appears. The Upgrade Status page displays a progress bar and provides details about the script currently running.

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

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

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

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

Step 10 Log into the Defense Center.

Step 11 Review and accept the End User License Agreement (EULA). Note that you are logged out of the appliance if you do not accept the EULA.

Step 12 Select **Help > About** and confirm that the software version is listed correctly: Version 5.4. Also note the versions of the rule update and VDB on the Defense Center; you will need this information later.

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

Step 14 If the rule update available on the Support site is newer than the rules on your 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*.

Step 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*.

Step 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.

Step 17 Reapply access control policies to all managed devices.

⚠

Caution If you disabled either the latency packet handling or latency rule handling preprocessors in an access control policy prior to updating your Defense Center to Version 5.4 and do not want the preprocessors automatically enabled, **do not** reapply access control policies after updating your Defense Center to Version 5.4. To modify either preprocessor setting so they are no longer enabled, upgrade your Defense Center to Version 5.4.1 and disable either the **Packet Handling** option or the **Rule Handling** option in the Advanced Tab of the access control policy, then reapply your policies.

⚠

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

Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *FireSIGHT System User Guide*.

Step 18 If a patch for Version 5.4 is available on the Support site, apply the latest patch as described in the *FireSIGHT System Release Notes* for that version.

⚠

Caution If you plan to use SSL policies, you must update your Version 5.4 managed devices to Version 5.4.0.1 and your Version 5.4 Defense Centers to Version 5.4.1.

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

Updating Managed Devices and ASA FirePOWER Modules

After you update your Defense Centers to Version 5.4, 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. Because they do not have a web interface, you must use the Defense Center to update your virtual managed devices. ASA FirePOWER modules do not have a web interface you can use to update the ASA FirePOWER modules. To update your physical and virtual ASA FirePOWER modules, use your Defense Center.

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.

For the Version 5.4 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 8.

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

To update managed devices and ASA FirePOWER modules:

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

For more information, see Before You Begin: Important Update and Compatibility Notes, page 8.

Step 2 Update the software on the devices' managing Defense Center; see Updating Defense Centers, page 14.

Step 3 Download the update from the Support site:

- for Series 2 managed devices:

  `Sourcefire_3D_Device_Upgrade-5.4.0-xxx.sh`
- for Series 3 managed devices:

  `Sourcefire_3D_Device_S3_Upgrade-5.4.0-xxx.sh`
- for 3D9900 managed devices:

  `Sourcefire_3D_Device_9900_Upgrade-5.4.0-xxx.sh`
- for virtual managed devices:

  `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.4.0-xxx.sh`
- for ASA FirePOWER modules:

  `Cisco_Network_Sensor_Upgrade-5.4.0-xxx.sh`

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

Step 4 Upload the update to the 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.

Step 5 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

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

The Install Update page appears.

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

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

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

Step 9 The update process begins. You can monitor the update's progress in the 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 Support.

Step 10 Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 5.4.

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

Step 12 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.

Step 13 Reapply access control policies to all managed devices.

Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *FireSIGHT System User Guide*.

Step 14 If a patch for Version 5.4 is available on the Support site, apply the latest patch as described in the *FireSIGHT System Release Notes* for that version.

⚠ **Caution** If you plan to use SSL policies, you must update your Version 5.4 managed devices to Version 5.4.0.1 and your Version 5.4 Defense Centers to Version 5.4.1.

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

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. The following sections list the issues resolved in the Version 5.4 update.

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, and CVE-2013-7265
- Security Issue Addressed multiple injection vulnerabilities, including HTML and command line.
- 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 via 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 reported an incorrect time stamp if the session was terminated. (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 enabled, 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 only be imported 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 drop-down 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:

- 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)
- You cannot 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. (134385/CSCze89030)
- Configuring a proxy server to authenticate with Message Digest 5 (MD5) password encryption for malware cloud lookups is not supported. (135279/CSCze89442)
- 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 some cases, if you create an intrusion rule and add a `file_type` and a `file_group` to your detection options, moving the `file_type` detection option up or down in order clears the selection you made for `file_group` when it should not. (139441/CSCze91218)
- In some cases, if you disable the IPV6 support option on a virtual router and save, the system generates an error and does not save the router configuration. (141718/CSCze93309)
- In some cases, if you view the threat score of some files from generated events, the system may incorrectly report the threat score as a number instead of Low, Medium, High, or Very High. (142290/CSCze93722)
- In some cases, if you create an SSL rule with logging enabled, the connection events page (**Analysis > Connections > Events**) does not display the URL category or URL reputation values. (142878/CSCze93434)
- 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)
- The *FireSIGHT System User Guide* does not reflect that if your Defense Center loses connectivity to the Internet, the system may take up to 30 minutes to generate an Advanced Malware Protection health alert. (143070/CSCze94138)
- In some cases, if you create an SSL policy with the **Session Not Cached** option under the Undecryptable Actions tab set to **Do Not Decrypt** or **Block** and SSL session reuse is enabled, when the session is refreshed, the system may display `uncached session` errors in the **SSL Status** column of the Connection Events table view. Cisco recommends creating an SSL policy with the **Session Not Cached** option set to **Do Not Decrypt** so traffic is not blocked. (143335/CSCze93608)
- If you register a managed device running Version 5.3.x to a Defense Center running Version 5.4, the system does not display data for the **Network Analysis Policy** column of the Intrusion Events table view and the Connection Events table view. (143349/CSCze94484)
- 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 Support 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, the system incorrectly displays file names containing colons (`:`) on the file events table view page (**Analysis > Files > File Events**). (143666/CSCze94954)
- In some cases, if you add users to an ASA managed device running a fresh installation of Version 5.4, the system does not include `show users` as a supported CLI command. (144400/CSCze95719)
- 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 should generate an HTTP response page, you are unable to access the same web page in additional tabs on the same browser. (144419/CSCze95694)
- If you create a custom network variable that is named identically to a default variable but contains different capitalization, the system incorrectly assumes the custom variable is the default variable and you cannot delete it. (144488/CSCze95591)
- In some cases, if you configure the local configuration of your Defense Center or managed device so `eth1` is enabled for DHCP and Event Only Traffic, the system incorrectly saves the configuration with both `eth0` and `eth1` enabled for DHCP when only `eth1` should be configured for DHCP. (144525/CSCze95666)

- In some cases, if you apply an access control policy with archive file types enabled on a device running an older vulnerability database (VDB), policy apply fails. As a workaround, update your device with the latest VDB and reapply the policy. (144533/CSCze95570)
- The Appliance Information dashboard widget does not display the status for all active management interfaces. (144567/CSCze95021)
- In some cases, if you create link aggregation group (LAG) interfaces on a NetMod connected to an 8000 Series managed device and remove the NetMod after powering down the device, the device attempts to load the configured interfaces from the NetMod instead of deleting the interface groups and generates an `Unable to load container` error. (144576/CSCze95166)
- If you remove the URL Filtering license from your system, the traffic sent to the cloud is disrupted. Do not remove your URL Filtering license from your system. (144578/CSCze95183)
- If you want to configure alerts for retrospective events or network-based malware events, you must configure both a discovery event alert and an Advanced Malware Protection alert. (144657/CSCze95041)
- In some cases, if you create an HTML report and use Mozilla Firefox to open the report, Firefox displays the report data as binary data when it should not. (144667/CSCze95195)
- The system does not stop intrusion rule updates if there are errors during the installation process. Contact Support if you do not see any imported rules in the rule update import log. (145039/CSCze95385)
- In some cases, if you backup and then restore your Defense Center, the system does not restore any locally-created Security Intelligence (SI) objects from the backup even though web interface display and the restored policies reference the SI objects. As a workaround, re-create your SI objects. (CSCur42337)
- In some cases, if the system attempts to download a file but the download is blocked and the file is downloaded again, the system either does not identify the file type or the system generates incorrect SHA-256 values. (CSCus87799)
- In some cases, if you attempt to upgrade a pair of Defense Centers in high availability from a version older than Version 5.4 directly to Version 5.4.1 without syncing the Defense Centers at Version 5.4, the system generates an error and all access control policies are corrupted. As a workaround, upgrade the Defense Centers in high availability to Version 5.4 and sync the pair of Defense Centers before upgrading to Version 5.4.1. (CSCut60825)

For Assistance

Thank you for choosing the FireSIGHT System.

Sourcefire Support

If you are a new customer, please visit https://support.sourcefire.com/ to download the Sourcefire Support Welcome Kit, a document to help you get started with Sourcefire Support and set up your Customer Center account.

If you have any questions, want to download updated documentation, or require assistance with the Sourcefire Defense Center or managed devices, please contact Sourcefire Support:

- Visit the Sourcefire Support site at https://support.sourcefire.com/.
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 410.423.1901 or 1.800.917.4134.

If you have any questions or require assistance with Cisco NGIPS for Blue Coat X-Series, please visit the Blue Coat Support site at: https://www.bluecoat.com/support/contactsupport/.

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.

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

♲ Printed in the USA on recycled paper containing 10% postconsumer waste.