FireSIGHT System Release Notes

Version 5.4.1
First Published: February 6, 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 3 Defense Centers (the DC500, DC750, DC1000, DC1500, DC2000, DC3000, DC3500, and the DC4000)
- Cisco ASA with FirePOWER Services (the ASA5506-X, ASA506H-X, ASA5506W-X, ASA5508-X, and ASA5516-X)
- 64-bit virtual Defense Centers

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 5.4.1 of the FireSIGHT System. You can update physical and virtual Defense Centers to Version 5.4.1 .Note that you can update appliances in the following manner:

- Defense Centers (DC500, DC750, DC1000, DC1500, DC2000, DC3000, DC3500, and the DC4000) must be running Version 5.4 to update to Version 5.4.1. If your Defense Center is running an earlier version, you must update to Version 5.4 before updating to Version 5.4.1.

  Note: A Defense Center may update its devices while running Version 5.4, but you will be unable to decrypt or inspect SSL traffic if your Defense Center remains at Version 5.4. If you plan on decrypting or inspecting SSL traffic, update your Defense Center to Version 5.4.1.

  Note: To use the ASA FirePOWER module on the ASA5506-X, ASA506H-X, ASA5506W-X, ASA5508-X, and ASA5516-X devices, you must install the Version 5.4.1 image. 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 5.4.1 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*.

FirePOWER Services Management Capabilities

Centralized Management of Cisco ASA5506-X, ASA5506H-W, ASA5506W-X, ASA5508-X, and ASA5516-X with FirePOWER Services

The Defense Center is now able to manage FirePOWER Services (ASA FirePOWER devices) implementations running on FirePOWER devices in the same way it does on all of the other ASA5500-X devices. This enables the management of multiple FirePOWER devices running ASA FirePOWER devices from a single Defense Center, as long as the ASA platform is running Version 9.3.1 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 FirePOWER 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, ASA5506H-W, ASA5506W-X, ASA5508-X, and ASA5516-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 FirePOWER 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

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

Multiple Management Interfaces

You can now use multiple management interface ports on Series 3 Defense Centers 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.

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.

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 5.4.1.

Table 1 Changes to Terminology

Version 5.4.1 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)
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 on the ASA55XX-X using ASDM
Centralized management	Refers to management of the ASA FirePOWER module on the ASA55XX-X 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

- 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 only configure alerts for retrospective events or network-based malware events from the Advanced Malware Protections Alerts tab on the Alerts page.
- You can now modify thresholds for the latency packet handling and latency rule handling preprocessors from the Advanced tab of the access control policy.

Features and Functionality Introduced in Previous Versions

Features Introduced 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 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 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.

Documentation Updates

You can download all updated documentation from the Support site. In Version 5.4.1, 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 Online Help (SEU)*
- *FireSIGHT System User Guide*
- *FireSIGHT System Installation Guide*
- *FireSIGHT System Virtual Installation Guide*
- *FireSIGHT System eStreamer Integration Guide*

The documentation updated for Version 5.4.1 contains the following errors:

- The *FireSIGHT System User Guide* does not reflect that, on devices with limited memory, the number of intrusion policies may not be paired with more than one variable set. In the case where you can apply an access control policy that references only one intrusion policy, verify every reference to the intrusion policy is paired with the same variable set. Pairing an intrusion policy with different variable sets results in more memory usage.

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.4.1, 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, page 8
- Audit Logging During the Update, page 8
- Version Requirements for Updating to Version 5.4.1, page 8
- .Time and Disk Space Requirements for Updating to Version 5.4.1, page 8
- Product Compatibility After Updating to Version 5.4.1, page 8
- Returning to a Previous Version, page 10

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.

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 5.4.1

To update to Version 5.4.1, a Defense Center must be running at least Version 5.4. If you are running an earlier version, you can obtain updates from the Support site.

.Time and Disk Space Requirements for Updating to Version 5.4.1

The table below provides disk space and time guidelines for the Version 5.4.1 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 2 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Series 3 Defense Centers	59 MB	917 MB	n/a	59 minutes
virtual Defense Centers	59 MB	917 MB	n/a	hardware dependent

Product Compatibility After Updating to Version 5.4.1

To manage an ASA FirePOWER module on a FirePOWER device, you **must** use at least Version 5.4.1 of the Defense Center. Devices must be running the versions identified in the following table to be managed by a Defense Center running Version 5.4.1.

Table 3 Version Requirements for Management

Appliance	Minimum Version to be Managed by a Defense Center Running Version 5.4.1
Series 2 and Series 3 managed devices	Version 5.3 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 5.3.1 of the FireSIGHT System
Cisco ASA with FirePOWER Services on ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, and the ASA5516-X	Version 5.4.1 of the FireSIGHT System

Operating System Compatibility

You can host 64-bit virtual appliances running Version 5.4 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

You can only install ASA FirePOWER modules running Version 5.4.1 on FirePOWER devices running ASA Version 9.3(2) and ASA Version 9.3(3) on the following platforms:

- ASA5506-X
- ASA506H-X
- ASA5506W-X
- ASA5508-X
- ASA5516-X

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

Web Browser Compatibility

Version 5.4.1 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 via **Tools > Internet Options > Security > Custom level**.

Table 4 Supported Web Browsers

Browser	Required Enabled Options and Settings
Chrome 40	JavaScript, cookies
Firefox 35	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.

Returning to a Previous Version

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

To update to Version 5.4.1 from a Version 5.4 image, see Before You Begin: Important Update and Compatibility Notes, page 7 and Installing the Update, page 10.

Download the following files from the Support site:

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

- for Series 3 Defense Center

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

  `Sourcefire_Defense_Center_Virtual64_VMWare-5.4.0-763.tar.gz`
- for ASA FirePOWER module (ASA5506-X, ASA506H-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 the ASA5506-X, see the *Cisco ASA FirePOWER Module Quick Start Guide* for more information on deploying and installing the module

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 7.

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.

To update Defense Centers running at least Version 5.4 to Version 5.4.1, see the guidelines and procedures outlined below:

- Updating Defense Centers, page 12

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.

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

Use the procedure in this section to update your Defense Centers, including virtual Defense Centers. For the Version 5.4.1 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 5.4.1 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:

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 7.

2. Download the update from the Support site:

   – for Series 3 and virtual Defense Centers:

   ```
   Sourcefire_3D_Defense_Center_S3_Upgrade-5.4.1-59.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.

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 completes. 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 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.

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. 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.

    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*.
18. If a patch for Version 5.4.1 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.

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 5.4.1:

- **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 via 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)
- 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 the system reported incorrect intrusion event rate values on the Health Events page. (143833/CSCze94067)
- 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)
- Improved URL blocking capabilities. (144197/CSCze94589)
- 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. (144547/CSCze95535, 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 via 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)
- Improved logging for troubleshooting purposes. (144802/CSCze95504)
- 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 via proxy even if you unchecked the use proxy option. (144968/CSCze95801)
- Resolved an issue where, if you added a stack of devices to a group and added the group to your target list, the system displayed the stack in the group as two targets instead of one target. (145009/CSCze95376)
- 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, if you added a stack of devices to a group and added the group to your target list, the system displayed the stack in the group as two targets instead of one target. (145009/CSCze95376)
- 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 systems running Version 5.3 reported port numbers above **32767** incorrectly. (145184/CSCze95270)
- Resolved an issue where the 40GB fiber NetMod traffic statistics were incorrectly logged traffic on the wrong 40GB port. (145515/CSCze95830)
- Resolved an issue where the system erroneously reported zero events if you attempted to view the first or most recent event events in the table view of Indications of Compromise or the network map of a host profile. (145202/CSCze95825)
- Resolved an issue where, if you attempted to download a zipped malware file from Captured Files on your Defense Center, the system downloaded an invalid zip file. (145251/CSCze96086)
- You can disable the **Session Termination Logging Threshold** by setting the threshold to **0** when you expand the Troubleshooting options of the Transport/Network Layer Preprocessor section in the Advanced tab of the Access Control Policy page (**Policies > Access Control**). (CSCur730080)
- Resolved an issue where the Inline Normalization preprocessor incorrectly resized packets when the **Trim Data to Window** option was enabled. (CSCur80901)
- Resolved an issue where, if you configured with a virtual router as the source IP address and a gateway as the endpoint IP address, and then rebooted the device with the virtual router, the system dropped packets until the gateway IP address was obtained. (CSCus32480, CSCus32488, CSCus32502)
- 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 you were unable to configure yourDefense Center as the network time protocol (NTP) source.(CSCus75305)

Issues Resolved in Previous Versions

Previously resolved issues are listed by version.

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 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 did not report sessions or reported an incorrect time stamp if the session was terminate 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 5.4.1:

- 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 attempt to use the SFR **system restart** CLI command while logged in via 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 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)
- If you edit a local rule on the Intrusion Rule Editor page (**Policies > Intrusion > Rule Editor**), the system displays the current local rule configuration for already-generated event data when viewing rule documentation instead of the rule configuration that triggered them. (145118/CSCze95346)
- 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)
- In some cases, if you generate an intrusion event performance graph (**Overview > Summary > Intrusion Event Performance**) and select **Last Hour** as the time range, the generated graph is blank instead of including data from the intrusion events table view. (145237/CSCze95774)
- 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)
- If you enable remote storage and create a scheduled email alert response on your Defense Center, the scheduled email alert may disable remote storage and remote storage backups may fail. As a workaround, create local backups and manually place the backups into remote storage. (145288/CSCze95993)
- In some cases, access control rules containing web application conditions may not match against web application traffic if users on your network enter a URL that is not lower case into the address bar. (CSCur37364)
- Under certain conditions, you cannot get URL category or reputation information. (CSCur38971, CSCus59492)
- In some cases, if you backup and then restore your Defense Center, the system does not restore locally-created Security Intelligence objects from the backup even though the web interface and the restored policies reference the Security Intelligence objects. As a workaround, recreate your Security Intelligence objects. (CSCur42337, CSCur35624)
- 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 device 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)

- In some cases, if your Defense Center has a file list with SHA-256 file entries and you add a Defense Center in high availability configuration, the secondary Defense Center deletes the existing file list data. (CSCur57708)
- 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, if you configure an inline pair of interfaces including **eth1** and **eth2** on a virtual device and issue the **show traffic-statistics** CLI command, the system will only display traffic statistics for **eth1** and not for **eth2**. (CSCur59771)
- 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)
- If you configure inline sets on a Series 3 managed device with hardware bypass enabled and reboot the device, you may lose interface connectivity for up to 25 seconds. (CSCur64678)
- 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)
- 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 attempt to expand the view of a vulnerability of a host with a client application on the vulnerabilities network map (**Analysis > Hosts > Network Map > Vulnerabilities**), the system does not include the host or any associated hosts in the leaf nodes. (CSCur86191)
- 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 deploy 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)
- You may experience some latency during Snort restart. (CSCus13247)
- 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)

- If you configure remote storage of reports using Windows File Sharing (SMB), the **$User, Host Report: $Host, Attack Report: $Attack SID**, and **Sourcefire FireSIGHT Report: $Customer Name** templates fail to generate reports in the SMB due to unsupported characters in the report names. (CSCus21871)
- 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)
- Some HTTPS traffic classifications may result in false positives. (CSCus32474)
- In some cases, if you create an SSL policy set to **Do Not Decrypt** and attempt to establish a session, the system may erroneously report the session was blocked because of a decryption error even though it was not. (CSCus41127)
- 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)
- 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 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 create a file policy with a Block Malware rule positioned after a rule with a Web Application category condition, the system does not block files identified as malware. As a workaround, position the Block Malware rule before the rule with the Web Application category condition. (CSCus64526)
- 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)

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)
- 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)
- 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 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)
- 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, 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, if you attempt 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 SHA256 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.

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.

For Assistance