FireSIGHT System Release Notes

Version 5.3.1.7
First Published: May 2, 2016

Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation and uninstallation instructions for the following appliances:

- Series 3 Defense Centers (the DC750, DC1500, and the DC3500)
- 64-bit virtual Defense Centers
- 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)

Note This update is for Defense Centers and Cisco ASA with FirePOWER Services **only**.

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 5.3.1.7 of the FireSIGHT System. You can update appliances running at least Version 5.3.1 of the FireSIGHT System to Version 5.3.1.7.

For more information, see the following sections:

Cisco Systems, Inc.
www.cisco.com

Changed Functionality

There is no changed functionality in Version 5.3.1.7.

Features and Functionality Added in Previous Releases

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

Management of Cisco ASA with FirePOWER Services

Version 5.3.1 introduces the ability to manage Cisco ASA with FirePOWER Services (ASA FirePOWER devices) with the FireSIGHT Defense Center. Defense Centers running Version 5.3.1 can manage ASA FirePOWER modules on the following ASA devices:

- 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

The ASA FirePOWER module **must** be running Version 5.3.1 to be managed by a Defense Center running Version 5.3.1.1. ASA FirePOWER modules can **only** be installed on the above platforms running Version 9.2.2 or later of the ASA software.

Feature Limitations of Cisco ASA with FirePOWER Services

When you use a Defense Center to manage Cisco ASA with FirePOWER Services devices, the ASA FirePOWER module provides the first-line system policy and passes traffic to the FireSIGHT System for access control, intrusion detection and prevention, discovery, and advanced malware protection.

Regardless of the licenses installed and applied, ASA FirePOWER devices do not support any of the following features through the FireSIGHT System:

- ASA FirePOWER devices do **not** support the FireSIGHT System's hardware-based features, including clustering, stacking, switching, routing, virtual private networks (VPN), and network address translation (NAT).

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

- You **cannot** use the Defense Center web interface to configure ASA FirePOWER interfaces.

- You **cannot** use the Defense Center to shut down, restart, or otherwise manage ASA FirePOWER processes.
- You **cannot** use the Defense Center to create backups from or restore backups to ASA FirePOWER devices.
- You **cannot** write access control rules to match traffic using VLAN tag conditions.

The ASA FirePOWER device does **not** have a FireSIGHT web interface. However, it has software and a CLI specific to the ASA platform. You use these ASA-specific tools to install the system and to perform other platform-specific administrative tasks. For more information, see the ASA FirePOWER module documentation.

Note that if you edit an ASA FirePOWER device and switch from multiple context mode to single context mode (or vise versa), the device renames all of its interfaces. You **must** reconfigure all FireSIGHT System security zones, correlation rules, and related configuration to use the updated ASA FirePOWER interface names.

Note The Defense Center does **not** display ASA interfaces when the ASA FirePOWER device is deployed in SPAN port mode.

Terminology

Version 5.3.1 introduces the ability to manage Cisco ASA with FirePOWER Services using FireSIGHT Defense Centers. If you reference documentation for Version 5.3 or Version 5.3.0.1, you may notice the terminology differs from the documentation for Version 5.3.1.

Table 1 Changes to Terminology

Version 5.3.1 Terminology	Description
Cisco	Formerly *Sourcefire*
FireSIGHT System	Formerly *Sourcefire 3D System*
Defense Center FireSIGHT Defense Center Cisco FireSIGHT Management Center	Formerly *Sourcefire Defense Center*
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

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.

Features Introduced in Previous Versions

Functionality described in previous versions may be superseded by other new functionality or updated through resolved issues.

The following functionality was introduced in Version 5.3.1.3:

- Version 5.3.1.3 no longer supplies default correlation policies. You must create custom policies and rules.

The following features and functionality were introduced in Version 5.3.1.1:

- You can now configure access control rules with the **GRE 47** port condition.
- You can now use the Defense Center's proxy server to communicate with the Cisco Security Manager (CSM).
- You can now reapply device configuration after editing the list of security zones of a cluster, stack or clustered stack of devices from the Object Management page by selecting the apply icon for device changes on the Device Management page (**Devices > Device Management**).
- You can now configure registered ASA FirePOWER devices with advanced options on the advanced tab of the Device Management page (**Devices > Devices Management**).

Documentation Updates

The documentation provided for Version 5.3.1.7 contains the following errors:

- The *FireSIGHT System User Guide* incorrectly states that `You can use Lights-Out Management (LOM) on the default (eth0) management interface on a Serial Over LAN (SOL) connection to remotely monitor or manage Series 3 appliances without logging into the management interface of the appliance` when you cannot.(CSCuu17674)
- The *FireSIGHT System User Guide* incorrectly states the following about devices in a stack: `If a secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to all secondary devices. On failed secondary devices, traffic is dropped. A health alert is generated indicating loss of link.`

  The documentation should specify that, by default, if the secondary device in a stack fails, by default, inline sets with configurable bypass enabled go into bypass mode on the primary device. For all other configurations, the system continues to load balance traffic to the failed secondary device. In either case, a health alert is generated to indicate loss of link. (122708/CSCze88292, 123380/CSCze88692, 138433/CSCze91099)
- The *FireSIGHT System Online Help* does not reflect that:

  The original client IP address that was extracted from an X-Forwarded-For (XFF), True-Client-IP, or custom-defined HTTP header. To display a value for this field, you must enable the HTTP preprocessor Extract Original Client IP Address option in the network analysis policy. Optionally, in the same area of the network analysis policy, you can also specify up to six custom client IP

headers, as well as set the priority order in which the system selects the value for the Original Client IP event field. See *Selecting Server-Level HTTP Normalization Options*, page 25-33 of the *FireSIGHT System User Guide* for more information.

When Extract Original Client IP Address is enabled, specifies the order in which the system processes original client IP HTTP headers. If, on your monitored network, you expect to encounter original client IP headers other than X-Forwarded-For (XFF) or True-Client-IP, you can click Add to add up to six additional Client IP header names to the priority list. Note that if multiple XFF headers appear in an HTTP request, the value for the Original Client IP event field is the header with the highest priority. You can use the up and down arrow icons beside any header type to adjust its priority. (139492/CSCze91210, 141233/CSCze92868, 144139/CSCze95050)

- The *FireSIGHT System Online Help* does not reflect that the system removes interfaces from your security zone configurations when you modify your ASA device security contexts and switch from single context mode to multiple context mode or vice versa. (141050/CSCze92286, 141064/CSCze92547)
- The appliances delivered with *FireSIGHT System Online Help* for Version 5.3.1 list Series 2, Series 3, virtual, and X-Series devices as supported devices. They are not supported. (144113/CSCze95418)
- The *FireSIGHT System User Guide* does not reflect that, if you register a cluster, stack, or clustered stack of devices to a Defense Center, you may have to manually reapply the device configuration. (142411/CSCze92729, 141602/CSCze92992)
- The *FireSIGHT System Online Help* does not reflect that proxies use NT LAN Manager (NTLM) authentication cannot communicate with the Collective Security Intelligence Cloud to receive information. Make sure to configure a different authentication for your proxy if you want to use cloud-based features. (143613/CSCze94827)
- The *FireSIGHT System User Guide* does not reflect:

  A file detected for the first time ever is assigned a disposition after the Defense Center completes a cloud lookup. The system generates a file event, but **cannot** store a file unless the file is immediately assigned a disposition.

  If a previously undetected file matches a file rule with a Block Malware action, the subsequent cloud lookup immediately returns a disposition, allowing the system to store the file and generate events.

  If a previously undetected file matches a file rule with a Malware Cloud Lookup action, the system generates file events but requires additional time to perform a cloud lookup and return a disposition. Due to this delay, the system cannot store files matching a file rule with a Malware Cloud Lookup action until the second time they are seen on your network. (143973/CSCze95101, 144180/CSCze94566)
- The *FireSIGHT System User Guide* does not reflect that you can now choose whether to inspect traffic during policy apply. Inspecting traffic during policy apply on a heavily loaded system may have an impact on network throughput and latency. If this side effect is not ideal for your network setup and connectivity is more important than inspection, unchecking this box will disable inspection temporarily during policy apply and ensure that no packets are dropped during the procedure. After policy apply is successful inspection will resume as normal. (144574/CSCze95159)
- The *FireSIGHT System User Guide* incorrectly states that, when configuring administrative shell access, `Shell users can log in using user names with lowercase, uppercase, or mixed case letters`. The documentation should state that `Shell users can log in using user names with lowercase letters`. (144936/CSCze95327)

- The *FireSIGHT System User Guide* incorrectly refers to the 5.3.1 STIG release notes. The STIG release notes for Version 5.3 should also be used for Version 5.3.1. Contact Support for the 5.3 STIG release notes. (CSCur79089)
- The *FireSIGHT System Virtual Installation Guide* incorrectly states the following about logging in to a virtual device at the VMware console using admin as the username and the new admin account password specified in the deployment setup wizard: `If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use Cisco as the password.` The documentation should state that if you did not change the password using the wizard or you are deploying with a ESXi OVF template, use Sourcefire as the password. (CSCut77002)

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.3.1.7, 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 6
- Traffic Flow and Inspection During the Update, page 6
- Audit Logging During the Update, page 7
- Version Requirements for Updating to Version 5.3.1.7, page 7
- Time and Disk Space Requirements for Updating to Version 5.3.1.7, page 7
- Product Compatibility After Updating to Version 5.3.1.7, page 8

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 (and any uninstallation of the update) reboots ASA FirePOWER 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

- link state

Traffic Inspection and Link State

In an inline deployment, your ASA FirePOWER devices (depending on model) can affect traffic flow via application control, user control, URL filtering, Security Intelligence, and intrusion prevention. In a passive deployment, you can perform intrusion detection and collect discovery data without affecting network traffic flow. 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.

Table 1-2 Network Traffic Interruptions

Deployment	Network Traffic Interrupted?
Inline	Network traffic is blocked throughout the update.
Passive	Network traffic is not interrupted, but also is not inspected during 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 5.3.1.7

To update your appliances to Version 5.3.1.7, a Defense Center must be running at least Version 5.3.0.1. If you are running an earlier version, you can obtain updates from the Support site.

Note This update is **not** supported on managed devices or Sourcefire Software for X-Series.

The closer your appliance's current version to the release version (Version 5.3.1.7), the less time the update takes.

Time and Disk Space Requirements for Updating to Version 5.3.1.7

The table below provides disk space and time guidelines for the Version 5.3.1.7 update. Note that when you use the Defense Center to update an ASA FirePOWER 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 3 Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Series 3 Defense Centers	379 MB	11545 MB	n/a	127 minutes
virtual Defense Centers	379 MB	11545 MB	n/a	hardware dependent
Cisco ASA with FirePOWER Services	63 MB	9699 MB	1482 MB	69 minutes

Product Compatibility After Updating to Version 5.3.1.7

You **must** use at least Version 5.3.0.1 of the Defense Center to manage devices running Version 5.3.1.7. Defense Centers running Version 5.3.1.7 can manage 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 5.3.1.7
physical and virtual managed devices	Version 5.3 of the FireSIGHT System
ASA FirePOWER modules	Version 5.3.1 of the FireSIGHT System

Operating System Compatibility

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

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

You can update the FireSIGHT System on the following ASA platforms running Version 9.2(4.8), Version 9.3(3.9), Version 9.4(2.11), or Version 9.5(2.6):

- 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*.

Web Browser Compatibility

Version 5.3.1.7 of the web interface for the FireSIGHT System has been tested on the browsers listed in the following table.

Table 5 Supported Web Browsers

Browser	Required Enabled Options and Settings
Chrome 49	JavaScript, cookies
Firefox 40	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 Version 5.3.1.1 and later currently does not support including local directory paths when uploading files to your server on Microsoft Internet Explorer 11. Cisco recommends disabling the Internet Explorer **Include local directory path when uploading files to server** option via **Tools > Internet Options > Security > Custom level**.

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 6.

To update appliances running at least Version 5.3.0.1 of the FireSIGHT System to Version 5.3.1.7, see the guidelines and procedures outlined below:

- Updating Defense Centers, page 10
- Updating Cisco ASA with FirePOWER Services, page 13

Note This update is **not** supported on physical or virtual managed devices or Sourcefire Software for X-Series.

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 5.3.1.7, 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 Changed 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 5.3.1.7 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 5.3.1.7 removes existing uninstallers from the appliance.

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 6.

Step 2 Download the update from the Support site:

- for Series 3 and virtual Defense Centers:

  `Sourcefire_3D_Defense_Center_S3_Patch-5.3.1.7-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.

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. You **must** wait until any long-running tasks are complete before you begin the update.

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.

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

Caution Do **not** use the web interface to perform any other tasks until the update completes and the Defense Center reboots. Before the update completes, the web interface may become unavailable and the Defense Center may log you out. This is expected behavior; log in again to view the task queue. If the update is still running, do **not** use the web interface until the update completes. 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 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 5.3.1.7. 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.

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 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 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*.

Step 18 If a patch for Version 5.3.1.7 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.

Note After updating your Defense Center, note that the apply icon for device changes is enabled and turns green to indicate changes that need to be reapplied to your registered devices.

Updating Cisco ASA with FirePOWER Services

After you update your Defense Centers to Version 5.3.1.7, use them to update the ASA FirePOWER devices they manage.

A Defense Center must be running at least Version 5.3.0.1 to update its ASA FirePOWER devices to Version 5.3.1.7.

Updating ASA FirePOWER 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 ASA FirePOWER devices at once, but only if they use the same update file.

For the Version 5.3.1.7 update, all ASA FirePOWER devices reboot. Depending on how your ASA FirePOWER 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 6.

Caution Before you update an ASA FirePOWER device, use its managing Defense Center to reapply the appropriate access control policy to the ASA FirePOWER device. Otherwise, the ASA FirePOWER 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 Cisco ASA with FirePOWER Services:

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 6.

Step 2 Update the software on the ASA FirePOWER devices' managing Defense Center; see Updating Defense Centers, page 10.

Step 3 Download the update from the Support site:

```
Cisco_Network_Sensor_Patch-5.3.1.7-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 ASA FirePOWER devices where you want to install the update.

Step 8 Click **Install**. Confirm that you want to install the update and reboot the ASA FirePOWER 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 ASA FirePOWER 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 ASA FirePOWER devices you updated have the correct software version: Version 5.3.1.7.

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 ASA FirePOWER 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 ASA FirePOWER 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 5.3.1.7 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.

Uninstalling the Update

The following sections help you uninstall the Version 5.3.1.7 update from your appliances:

Planning the Uninstallation

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

Uninstallation Method

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

For all physical appliances and virtual Defense Centers, uninstall the update using the local web interface. Because Cisco ASA with FirePOWER Servicesdo not have a web interface, you **must** use the bash shell to uninstall the update.

Order of Uninstallation

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

Uninstalling the Update from Devices Deployed Inline

ASA FirePOWER devices do **not** perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update, page 6.

Uninstalling the Update and Online Help

Uninstalling the Version 5.3.1.7 update does **not** revert the online help to its previous version. If the version of your online help does not match that of your FireSIGHT System software, your online help may contain documentation for unavailable features and may have problems with context sensitivity and link functionality.

After the Uninstallation

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

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

Uninstalling the Update from a ASA FirePOWER Device

The following procedure explains how to uninstall the Version 5.3.1.7 update from ASA FirePOWER devices. You **cannot** use a Defense Center to uninstall the update from a ASA FirePOWER device.

Uninstalling the Version 5.3.1.7 update results in a device running Version 5.3.1.6. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

Uninstalling the Version 5.3.1.7 update reboots the device. ASA FirePOWER devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Traffic Flow and Inspection During the Update, page 6.

To uninstall the update from a ASA FirePOWER device:

Step 1 Read and understand Planning the Uninstallation, page 15.

Step 2 Log into the device as `admin`, via SSH or through the virtual console.

Step 3 At the CLI prompt, type `expert` to access the bash shell.

Step 4 At the bash shell prompt, type `sudo su -`.

Step 5 Type the admin password to continue the process with root privileges.

Step 6 At the prompt, enter the following on a single line:

```
install_update.pl
/var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-5.3.1.7-xxx.sh
```

The uninstallation process begins.

Caution If you encounter issues with the uninstallation, do not restart the uninstallation. Instead, contact Support.

Step 7 After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 8 Log in to the Defense Center.

Step 9 Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.1.

Step 10 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstalling the Update from a Defense Center

Use the following procedure to uninstall the Version 5.3.1.7 update from Defense Centers and virtual Defense Centers. Note that the uninstallation process reboots the Defense Center.

Uninstalling the Version 5.3.1.7 update results in a Defense Center running Version 5.3.0.1. For information on uninstalling a previous version, refer to the *FireSIGHT System Release Notes* for that version.

To uninstall the update from a Defense Center:

Step 1 Read and understand Planning the Uninstallation, page 15.

Step 2 Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Step 3 View the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

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

Step 4 Select **System > Updates**.

The Product Updates tab appears.

Step 5 Click the install icon next to the uninstaller that matches the update you want to remove.

The Install Update page appears.

Step 6 Select the Defense Center and click **Install**, then confirm that you want to uninstall the update and reboot the device.

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

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

Step 7 After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.

Step 8 Log in to the Defense Center.

Step 9 Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.1.

Step 10 Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Resolved Issues

You can track defects resolved in this release using the Cisco Bug Search Tool (https://tools.cisco.com/bugsearch/). A Cisco account is required. The following sections list the issues resolved in the Version 5.3.1.7 update.

Issues Resolved in Version 5.3.1.7:

- Security Issue Addressed an unauthenticated, arbitrary execution allowing unauthenticated attackers to affect the HTTPS connection during a rule update from support.sourcefire.com, as described in CVE-2015-6357.
- Security Issue Addressed a vulnerability in the third-party product Linux that allowed an authenticated user to cause Denial of Service, as described in CVE-2015-5364.
- Security Issue Addressed an arbitrary HTTP header injection vulnerability allowing unauthenticated, remote attackers to exploit managed devices as described in CVE-2016-1345.
- Resolved an issue where the memory usage health monitor erroneously generated false positives. (144593/CSCze94840)
- Resolved an issue where, if you logged into your system as a user other than the `admin` user and edited the base layer of an intrusion policy, the system incorrectly marked all affected edited intrusion policies as updated by `admin` when it should not have. (CSCur79437)
- Resolved an issue where the /var/home directory on a Defense Center was directed to the wrong directory. (CSCut80381)
- Resolved an issue where, if a host generated an indication of compromise (IOC) and you disabled the IOC for that host on the Host Profile page, the Indications of Compromise by Host dashboard widget incorrectly displayed the IOC. (CSCuv41376)

Issues resolved in Version 5.3.1.6:

- Security Issue Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections, as described in CVE-2014-8275 and CVE-2015-0204.
- Security Issue Addressed multiple vulnerability issues in Linux, NTP, and other third parties, as described in CVE-2011-2699, CVE-2011-4131, CVE-2012-3400, CVE-2013-1944, CVE-22013-4545, CVE-22013-21944, and CVE-22014-29296.
- Security Issue Addressed an arbitrary script injection vulnerability allowing unauthenticated, remote attackers to exploit GNU C library DNS resolution functionality, as described in CVE-2013-7423.
- Resolved an issue where managed devices stopped processing traffic when the Defense Center updated a large security intelligence feed referenced in an access control policy during a policy apply. (CSCus19921)
- Resolved an issue where running the `sudo ips_profile` shell command on a device running at least Version 5.3 that is registered to a Defense Center running at least Version 5.4 caused the rule profiled script to fail. (CSCuu02211)
- Resolved an issue where the Cisco cloud continuously checked for an updated download and caused system issues. (CSCuu04844)
- Resolved an issue where, if you applied an access control policy set to **Block** as the default actions to an ASA FirePOWER device, the system incorrectly reverted the policy's default action to **Reset** instead of **Block**. (CSCuu60713)
- Resolved an issue where the system did not properly encode an edit to a newly added comment to an access control policy rule. (CSCus83065)
- Resolved an issue where the system did not generate a list of vendors in the vendor drop-down menu if you create a product map set and **Add Fix Map**. (CSCuu79373)
- Resolved an issue where the **Send email** check box on Reporting page did not stay selected if you generated a report, navigated away from the Report Templates tab, and then generated another report. (CSCuu97750)
- Resolved an issue where the Product Licensing dashboard widget did not list any URL Filtering licenses even if URL Filtering licenses were present. (CSCuu97762)
- Resolved an issue where the License page incorrectly listed licenses under the wrong devices if you added more than one license to a 3D8250 device and one license to another Series 3 device. (CSCuu99789)

Issues Resolved in Version 5.3.1.5:

- Security Issue Addressed a vulnerability in HTTP connection handling that allowed users to be redirected to malicious websites, as described in CVE-2015-0706.
- Security Issue Addressed multiple vulnerability issues in Linux and other third parties, as described in CVE-2011-1927, CVE-2012-2744. and CVE-2015-1781.
- Security Issue Addressed a cross-site scripting (XSS) vulnerability, as described in CVE-2015-0707.

- Resolved an issue where generated events incorrectly reported file threat scores as a number instead of **Low**, **Medium**, **High**, or **Very High**. (142290/CSCze93722)
- Improved URL blocking and URL filtering. (144198/CSCze94590)
- Resolved an issue where, if you edited the interface security zones on the Object Management page, the stacked device configuration appeared to be up-to-date when it wasn't. (144626/CSCze94847)
- Resolved an issue where, if you edited a local rule on the Intrusion rule Editor page, the system displayed the current local rule configuration for already-generated event data when viewing rule documentation instead of the rule configuration that triggered them. (145118/CSCze95346)
- Resolved an issue where, if you enabled remote storage and scheduled an email alert response on your Defense Center, the scheduler disabled remote storage and remote storage backups failed. (145288/CSCze95993)
- Resolved an issue where if you imported a policy that referenced a shared layer, importing the policy failed. (144946/CSCze96151)
- Resolved an issue where, if you created a correlation rule configured to if **an intrusion event occurs** or **a connection event occurs** and you selected **ingress security zone**, **egress security zone**, i**ngress interfaces**, or **egress interface** as the condition, the system did not recognize the rule and did not trigger traffic matching the rule. (CSCur59840)
- Resolved an issue where the system generated an `Internal Server Error` message if the password for your registered ASA FirePOWER device included an unsupported character. (CSCus68604)
- Resolved an issue where, if your system restarted after a vulnerability database (VDB) install and the **Inspect Traffic During Policy Apply** option in your access control policy was unchecked, your system experienced loss of network connectivity. (CSCut08225)
- Resolved an issue where, if you edited an access control rule with multiple URL category conditions and attempted to remove one of the conditions, the web management interface only removed the first category condition listed. (CSCut25082)
- The system now reports a recovery event for all CPUs when CPU usage changes from a high level to a normal state. (CSCut27600)
- Resolved an issue where the system did not display some web application information in a host profile when only a subset of the networks were monitored. (Resolved an issue where the system did not display some web application information in a host profile when only a subset of the networks were monitored. (CSCut36536))
- Resolved an issue where, if you created and edited a search for generated events, then canceled the search before the search started, the system redirected you to the events page related to the search with the incorrect search name. (CSCut63265)
- The system now generates a `Network file trajectory is not available for malware events due to pruning of the related file events based on configurable maximums` message if the network trajectory file is unavailable due to issues with your current configuration. (CSCut63362)
- Resolved an issue where, if you restarted your ASA5585X device with a large number of subinterfaces configured without also restarting the SFR5585X service card, the SFR5585X service card appeared to fail. (CSCut89619)
- Resolved an issue where RPM page manager (RPM) install history did not reset correctly if you downgraded RPM files starting with Cisco. (CSCut98525)
- Resolved an issue where Defense Centers running Version 5.4.1 were unable to apply policies to devices running Version 5.3.1.5. (CSCuu16406)
- Resolved an issue where, if you changed your system's time zone to a zone east of UTC and added a correlation rule with at least one inactive period to a correlation policy, policy apply failed. (CSCuu37600)

- Resolved an issue where, if you created an access control policy containing a geolocation condition, traffic that should have matched the condition did not. (CSCuu48800)
- Improved stability of SFDataCorrelator. (CSCuu53215)
- Resolved an issue where, if you configured your Defense Center to use a static IPv4 address with an IPv6 address enabled and you accessed the Defense Center's interface via the IPv6 address, the access control policy editor page did not load. (CSCuu83933)

Issues Resolved in Version 5.3.1.4:

- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities. (CSCur25518, CSCus07858, CSCus07875)
- Security Issue Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections, as described in CVE-2014-3569, CVE-2014-3570, CVE-2014-3572, CVE-2015-0204, CVE-2015-0286, CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0293.
- Improved data pruning. (141894/ CSCze92576)
- Resolved an issue where the Defense Center or managed device generated `High Unmanaged Disk Usage` health alerts. (145221/CSCze95877)
- Improved multiple dashboard widgets. (CSCus11068)
- Resolved an issue where, if you applied an access control policy to clustered devices, the access control policy page displayed the status of the policy apply as `pending` even though the action queue task successfully completed. (CSCus86011)

Issues Resolved in Version 5.3.1.3:

- Security Issue Addressed an arbitrary script injection vulnerability allowing unauthenticated, remote attackers to exploit GNU C library. The fix is addressed in CVE-2015-0235.
- Security Issue Addressed multiple vulnerabilities in SSLv3 that allowed external attacks on client connections. The fix is addressed in CVE-2014-3566.
- Security Issue Addressed multiple injection vulnerabilities as described in CVE-2007-6750.
- Security Issue Resolved several cross-site scripting (XSS) vulnerabilities.
- Security Issue Resolved an unauthorized vulnerability in Universal Unique Identifier (UUID) manipulation.
- The *FireSIGHT System Online Help* documents that HTTP X-Forwarded-For (XFF) headers are now a configurable option in the rule editor for intrusion policies. (139492/CSCze91210, 141233/CSCze92868)
- The *FireSIGHT System Online Help* documents that the apply icon for device changes on the Device Management page (**Devices > Device Management**) activates and turns green when out-of-date device configuration policies need to be reapplied. (144142/CSCze95449)
- Resolved an issue where a 3D9900 device running a version older than Version 5.3.0.3 registered to a Defense Center running at least Version 5.3.1 did not generate intrusion events. (144171/CSCze94677)
- Improved the reliability of URL reputation and detection capabilities. (144196/CSCze94549)
- Resolved an issue where the system treated DNS traffic as OpenVPN, QQ, and Viber traffic. (144546/CSCze95528)
- Resolved an issue where, in some cases, the system misidentified SMTP traffic as FTP and caused intrusion events for FTP commands that were false positives. (144591/CSCze95154)

- 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. (145008/CSCze95316)
- Resolved an issue where automatic updates failed if you attempted to download updates while managing an X-Series device. (145045/CSCze95716)
- Resolved an issue where systems running Version 5.3 reported port numbers above 32767 incorrectly. (145183/CSCze95390)
- Resolved an issue where the Defense Center or managed device generated `High Unmanaged Disk Usage` health alerts. (145221/CSCze9587)
- Resolved an issue where the system provided an incorrect patch release if you attempted to update your system using the **Download Updates** button on the **Product Updates** page (**System >Updates**). (145172/CSCze95369)
- Resolved an issue where the system did not provide URL category or reputation information. (CSCur38971)
- 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. (CSCur40263)
- Resolved an issue where the host profile incorrectly displayed multiple IP addresses for a single managed device. (CSCur42027, CSCur59486)
- Resolved an issue where, if you created a custom workflow and attempted to open the packet view of an intrusion event, the system opened the incorrect intrusion event in the packet view. (CSCur48743)
- Resolved an issue where, if you created a scheduled task to install a new version of the database (VDB) and the Defense Center already had a recent VDB installed, the system switched from active to standby mode every time the task occurred. (CSCur59252)
- Resolved an issue where the system did not display the associated hosts if you expanded a vulnerability based on a client application from the vulnerabilities network map. (CSCur86191)
- Improved the optimization of certain event workflows. (CSCus52203
- Improved troubleshooting capabilities. (CSCut12157)
- Improved SFDataCorrelator capabilities. (CSCut23688)
- Resolved an issue where the system ignored source network access control rule conditions when processing traffic. (CSCut23929)
- Troubleshooting generated by a failure now includes IPv6 information. (CSCut48083)

Because you can update your appliances from Version 5.3.1 to Version 5.3.1.7, this update also includes the changes in all updates from Version 5.3.1.7 through Version 5.3.1. Previously resolved issues are listed by version.

Issues Resolved in Version 5.3.1.1:

- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities.
- Security Issue Addressed multiple cross-site request forgery (CSRF) vulnerabilities.
- Security Issue Addressed multiple HTML injection vulnerabilities.
- Security Issue Addressed multiple Denial of Service (DoS) vulnerabilities as described in CVE-2014-0196, and CVE-2014-3153.

- Resolved an issue where, if you added a group of stacked devices targeted by the current access control policy to your Defense Center and reapplied the policy, the system incorrectly displayed the list of managed devices on the Device Management page and prevented you from editing the listed devices. (140710/CSCze92390)
- Resolved an issue where applying a single health policy to 100 or more managed devices caused system issues. (140977/CSCze92388)
- Resolved an issue where, if you registered an ASA FirePOWERdevice to a pair of Defense Centers in a high availability configuration, the secondary Defense Center did not display the CSM Single Sign-On tab on the User Management page (**System > Local > User Management**). (141150/CSCze92615)
- Resolved an issue where syslog alerts contained incorrect intrusion rule classification data when sent as intrusion event notifications. (141213/CSCze92467, 141216/CSCze92474, 141220/CSCze92639)
- Resolved an issue where adaptive profiles failed to take effect if you used a network variable such as `$HOME_NET` as the value for Networks settings. (141225/CSCze92611)
- Resolved an issue where, if you created a configuration-only backup, the backup file included extraneous discovery event data. (141246/CSCze92508)
- Resolved an issue where, if you created a saved search that used a VLAN tag object, the system saved the search with the value `0` in the field where you used the VLAN tag object instead. (141330/CSCze92734)
- Resolved an issue where, if you created a custom workflow with a large number of pages, the time window obscured the link the to the final pages of the workflow. (141336/CSCze92873)
- Resolved an issue where, in rare cases, the system did not generate a health alert when reapplying device configuration failed. (141625/CSCze93130, 141628/CSCze93009)
- Resolved an issue where, one or more unresponsive detection resources on a managed device after installing an update of the vulnerability database (VDB) caused system issues. (141758CSCze93100)
- Resolved an issue where, in rare cases, the system triggered an alert on the first data packet of a TCP session from a server in which the egress interface would not be recorded. (141817/CSCze93047)
- Resolved an issue where, in rare cases, applying multiple access control policies caused system issues and high unmanaged disk usage health alerts. (141830/CSCze92990)
- Resolved a third-party vulnerability in OpenSSL to address CVE-2-014-0224. (141901/CSCze93310)
- Improved the stability of the SMB and DCE/RPC preprocessor. (142199/CSCze93232)
- Resolved an issue where, if you edited an access control policy and policy apply failed, the policy changes from the attempted policy apply were not restored to the previously applied policy. (142907/CSCze94256)
- Resolved a third-party vulnerability in Java to address the following CVEs: CVE-2014-0429, CVE-2013-5907, CVE-2013-5782, CVE-2013-5830, CVE-2013-1537, CVE-2013-0437, CVE-2013-1478, CVE-2013-1480, CVE-2012-5083, CVE-2012-1531, CVE-2012-1713, CVE-2014-0385, CVE-2013-5802, CVE-2013-2461, CVE-2013-2467, CVE-2013-2407, CVE-2014-0460, CVE-2014-0423, CVE-2013-5905, CVE-2013-5906, CVE-2014-4264, CVE-2013-6954, CVE-2013-6629, CVE-2013-5825, CVE-2013-4002, CVE-2013-5823, CVE-2013-2457, CVE-2013-0440, CVE-2013-5780, CVE-2014-4244, CVE-2014-4263, CVE-2014-0453, CVE-2014-0411, CVE-2013-0443, CVE-2013-2451, CVE-2013-5803, CVE-2013-2415, CVE-2013-1489, CVE-2012-5085. (143620/CSCze94657)

- Resolved an issue where, if the system generated file events from the file traffic, the system incorrectly truncated file event filenames with colons on several pages of the web interface. (143666/CSCze94954)
- Resolved an issue where, if the system generated intrusion events matching a rule with a generator ID (GID) other than 1 or 3, syslog alerts contained incorrect messages. (143725/CSCze94300)
- Resolved an issue where, if you disabled any access control rules containing either an intrusion policy or a variable set different from any enabled rules and the access control policy's default action, access control policy apply failed and the system experienced issues. (143870/CSCze94942)
- Resolved an arbitrary injection vulnerability allowing unauthenticated, remote attackers to execute commands via Bash. This addresses CVE-2014-6271 and CVE-2014-7169. For more information, refer to the Cisco Security Advisory page at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash. (144863/CSCze95512, 144942/CSCze95480, 144949/CSCze96202)

Issues Resolved in Version 5.3.1:

- Resolved an issue where, in some cases, the intrusion event packet view displayed a rule message that did not match the rule that generated the event. (138208/CSCze90592)
- Resolved an issue where you could not import an intrusion rule that referenced a custom variable. (138211/CSCze90499)
- Resolved an issue where enabling telnet on a Cisco IOS Null Route remediation module and configuring the username for the Cisco IOS instance to enable by default on the Cisco IOS router caused Cisco IOS Null Route remediations to fail on the Defense Center. (139506/CSCze91607)
- Resolved an issue where the system did not prevent you from creating a network variable with an excluded network value that excluded all (any) networks. (139510/CSCze91770)

Known Issues

The following known issues are reported in Version 5.3.1.7:

- In some cases, if you enable the use of a proxy on your Defense Center and **Create FireAMP Connection** on the Amp Management page (**Amp > Amp Management**), the system does not include `Private Cloud` in the Cloud Name drop-down list when it should. (CSCuu16374)
- In some cases, if you create an LDAP object in the Microsoft Active Directory and add the LDAP object to a user policy, then move the LDAP object, the Defense Center cannot locate the LDAP object. As a workaround, remove the LDAP group containing the LDAP object from the Users Policy page (**Policies > Users**) and **Fetch Groups from the Defense Center**, then add the group and recreate the LDAP object in the user policy. (CSCuu95350)
- If you apply an access control policy with the default action set to **Network Discovery** that contains an access control rule configured to **Block** ICMPv6 traffic to an 8000 Series, the system does not generate events when traffic is blocked when it should. (CSCuw36033)
- In some cases, if you apply an access control policy containing all the **Risk** category conditions, the system does not automatically enable all the necessary detectors if the detectors were not enabled prior to apply the access control policy. (CSCuw41474)
- If a user belongs to a group included in an LDAP user awareness object but the group the user belongs to is set as the primary group on the Active Directory server, the user is not included in the list of access-controlled users downloaded from the Active Directory server and you cannot add that user to an access control rule. (CSCuv03821)

- In some cases, if you generate a report template with a custom logo and create a backup file, then backup and restore the Defense Center, the backup file does not save the custom logo in the report template. (CSCuv44883)
- In some cases, if you apply policy and then compare policies, the policy comparison always generates differences even when there are none. (CSCuv76157)
- If you create an access control rule and set the default action to **Interactive Block**, then edit the interactive block response page on the HTTP Responses tab of the Default Access Control page (**Policies > Access Control**) in Japanese, the interactive block page does not generate a **Continue** button to bypass the interactive block page. (CSCuw21450)
- The system cleans up archived files in no specific order, but attempts to insure that all events are reported to the Defense Center. (CSCuw79989)
- In some cases, if you apply an access control rule that uses more than one VLAN, traffic that should trigger the applied access control rule incorrectly triggers other rules. (CSCuw99834)
- In some cases, updating a managed device fails and the system does not indicate why in Task Status. If you update a device and the update fails without a reason, contact Support. (CSCux56288)
- If you filter intrusion rules on the Rule State page (**Rule Configuration > Rule State**) and search for the `FlowBit` keyword, the system generates inconsistent results. (CSCuy13901)
- If you remove a user from all groups within a realm referenced in the access control policy and deploy configuration changes, then click **Download users and groups** from the Access Control tab, the system does not update the deployed configuration and continues to process traffic as if the group(s) still contained the user. (CSCuy39685)
- In some cases, generating troubleshoot for Series 3, ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, or ASA5585-X device from the Defense Center user interface fails. (CSCuz00468)
- Updating appliances via CLI commands is not supported and you cannot recover the appliance after the update reboot. Cisco strongly recommends updating the Defense Center and all managed devices via the web interface. If you experience issues updating your appliances, contact Support. (CSCuz01827, CSCuz09667)

The following known issues were reported in previous releases:

- In some cases, applying changes to your access control policy, intrusion policy, network discovery policy, or device configuration, or installing an intrusion rule update or update of the vulnerability database (VDB) causes the system to experience a disruption in traffic that uses Link Aggregation Control Protocol (LACP) in fast mode. As a workaround, configure LACP links in slow mode. (112070/CSCze87966)
- If the system generates intrusion events with a **Destination Port/ICMP Code** of `0`, the Top 10 Destination Ports section of the Intrusion Event Statistics page (**Overview > Summary > Intrusion Event Statistics**) omits port numbers from the display. (125581/CSCze88014)
- Defense Center local configurations (**System > Local > Configuration**) are **not** synchronized between high availability peers. You must edit and apply the changes on all Defense Centers, not just the primary. (130612/CSCze89250, 130652)
- In some cases, large system backups may fail if disk space usage exceeds the disk space threshold before the system begins pruning. (132501/CSCze88368)
- In some cases, using the RunQuery tool to execute a `SHOW TABLES` command may cause the query to fail. To avoid query failure, only run this query interactively using the RunQuery application. (132685/CSCze89153)

- If you delete a previously imported local intrusion rule, you cannot re-import the deleted rule. (132865/CSCze88250)
- In rare cases, the system may not generate events for intrusion rules 141:7 or 142:7. (132973/CSCze89252)
- In some cases, remote backups of managed devices include extraneous unified files, generating large backup files on your Defense Center. (133040/CSCze89204)
- You must edit the maximum transmission unit (MTU) on a Defense Center or managed device using the appliance's CLI or shell. You cannot edit MTUs via the user interface. (133802/CSCze89748)
- If you create a URL object with an asterisk (`*`) in the URL, the system does not generate preempted rule warnings for access control policies containing rules that reference the object. Do **not** use asterisks (`*`) in URL object URLs. (134095/CSCze88837, 134097/CSCze88846)
- If you configure your intrusion policy to generate intrusion event syslog alerts, the syslog alert message for intrusion events generated by intrusion rules with preprocessor options enabled is `Snort Alert`, not a customized message. (134270/CSCze88831)
- If the secondary device in a stack generates an intrusion event, the system does not populate the table view of intrusion events with security zone data. (134402/CSCze88843)
- If you configure an Nmap scan remediation with the **Fast Port Scan** option enabled, Nmap remediation fails. As a workaround, disable the **Fast Port Scan** option. (134499/CSCze88810)
- If you generate a report containing connection event summary data based on a connection event table saved search, reports on that table populate with no data. (134541/CSCze89348)
- Scheduling and running simultaneous system backup tasks negatively impacts system performance. As a workaround, stagger your scheduled tasks so only one backup runs at a time. (134575/CSCze89679)
- If you edit a previously configured LDAP connection where user and group access control parameters are enabled, clicking **Fetch Groups** does not populate the Available Groups box. You must re-enter your password when editing an LDAP connection in order to fetch available groups. (134872/CSCze89834)
- In some cases, if you enable **Resolve IP Addresses** in the **Event Preferences** section of the Event View Settings page, hostnames associated with IPv6 addresses may not resolve as expected in the dashboard or event views. (135182/CSCze90155)
- Configuring a proxy server to authenticate with a Message Digest 5 (MD5) password encryption for malware cloud lookups is not supported. (135279/CSCze89442)
- You cannot enter more than 450 characters in the **Base Filter** field when creating an LDAP authentication object. (135314/CSCze89081)
- In some cases, if you schedule a task while observing Daylight Saving Time (DST), the task does not run during periods when you are not observing DST. As a workaround, select **Europe, London** as your local time zone on the Time Zone Preference page (**Admin > User Preferences**) and recreate the task during a period when you are not observing DST. (135480)
- The system requires additional time to reboot appliances or ASA FirePOWER devices 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, the system may generate a false positive for the SSH preprocessor rule 128:1. (135567/CSCze89434)
- If you apply an intrusion policy containing a rule with the **Extract Original Client IP Address** HTTP preprocessor option enabled, the system may populate intrusion events with incorrect data in the **Original Client IP** field if traffic passes through a dedicated proxy server. (135651/CSCze89056)

- If you schedule a task with **Report** as the job type, the system does not attach the report to the emailed status report. (136026/CSCze90265)
- If you apply an access control policy to multiple devices, the Defense Center displays the task status differently on the Task Status page, the Access Control policy page, and the Device Management page of the web interface. The status on the Device Management page (**Devices > Device Management**) is correct. (136364/CSCze87068, 136614/CSCze89936)
- In some cases, if you create a custom workflow based on the health events table, the Defense Center displays conflicting data in the event viewer. (136419/CSCze90336)
- If you import a custom intrusion rule as an `.rtf` file, the system does not warn you that the `.rtf` file type is not supported. (136500/CSCze89991)
- If you configure a Security Intelligence feed and specify a **Feed URL** that was created on a computer running a Windows operating system, the system does not display the correct number of submitted IP addresses in the tooltips on the Security Intelligence tab. As a workaround, use `dos2unix` commands to convert the file from Windows encoding to Unix encoding and click **Update Feeds** on the Security Intelligence page. (136557/CSCze89888)
- If you disable a physical interface, the logical interfaces associated with it are disabled but remain green on the Interfaces tab of the appliance editor for that managed device. (136560/CSCze89894)
- If you create a custom table based on the captured files table, the system generates an error message. The system does not support creating a custom table based on the captured files table. (136844/CSCze89977)
- If you register a managed device with a hostname containing more than 40 characters, device registration fails. (137235/CSCze90144)
- In some cases, the system does not filter objects in the Object Manager as expected if you include 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)
- In some cases, if you enabled Simple Network Management Protocol (SNMP) polling in your system policy, modifying the high availability (HA) link interface configuration on one of your clustered managed devices causes the system to generate inaccurate SNMP polling requests. (137546/CSCze90000)
- In some cases, configuring your access control policy to log blacklisted connections to the syslog or SNMP trap server causes system issues. (137952)
- In some cases, the Operating System Summary workflow displays incorrect DNS server counts, NTP server counts, and DNS port counts if the system receives DNS or NTP packets out of order. (138047/CSCze90930)
- The table view of file events appears to support viewing the file trajectory for ineligible file events. You can only view file trajectories for files with a calculated SHA-256 value. (138155/CSCze90676)
- If you generate a report in HTML or PDF format that includes a chart with **File Name** as the x-axis, the system does not display UTF-8 characters in the x-axis filenames. (138297/CSCze90799)
- In rare cases, if you have ever used your Defense Center to manage more than one device, the system displays inaccurate intrusion event counts in the dashboard. (138298)
- In rare cases, editing and reapplying an intrusion policy hundreds of times causes intrusion rule updates and system updates to require over 24 hours to complete. (138333/CSCze90747)
- If the latest version of the geolocation database (GeoDB) is installed on your Defense Center and you attempt to update the GeoDB with the same version, the system generates an error message. (138348/CSCze90813)

- Connection events logged to the syslog or SNMP trap server may have incorrect **URL Reputation** values. (138504/CSCze91066, 139466/CSCze91510)
- In some cases, if you apply more than one access control policy across your deployment, searching for intrusion or connection events (**Analysis > Search**) matching a specific access control rule may retrieve events generated by unrelated rules in other policies. (138542/CSCze91690)
- You cannot cut and paste access control rules from one policy to another. (138713/CSCze91012)
- In the Security Intelligence Source/Destination metadata (rec_type:281), the eStreamer server identifies the source as the destination and the destination as the source. (138740/CSCze91402)
- In an access control policy, the system processes certain Trust rules before the policy's Security Intelligence blacklist. Trust rules placed before either the first Monitor rule or before a rule with an application, URL, user, or geolocation-based network condition are processed before the blacklist. That is, Trust rules that are near the top of an access control policy (rules with a low number) or that are used in a simple policy allow traffic that should have been blacklisted to pass uninspected instead. (138743, 139017)
- If you disable **Drop When Inline** in your intrusion policy, inline normalization stops modifying packets seen in traffic and the system does not indicate what traffic would be modified. In some cases, other devices or applications on your network may not function in the same way after you re-enable **Drop When Inline**. (139174/CSCze91149, 139177/CSCze91163)
- Security Known Issue Sourcefire is aware of a vulnerability inherent in the Intelligent Platform Management Interface (IPMI) standard (CVE-2013-4786). Enabling Lights-Out Management (LOM) on an appliance exposes this vulnerability. To mitigate the vulnerability, deploy your appliances on a secure management network accessible only to trusted users. To prevent exposure to the vulnerability, do not enable LOM. (139286/CSCze91556)
- In rare cases, the Task Status page (**System > Monitoring > Task Status**) incorrectly reports that a failed system policy apply succeeded. (139428/CSCze92142)
- If you configure and save three or more intrusion policies that reference each other through their base policies, the system does not update the Last Modified dates for all policies on the Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**). As a workaround, wait 5 to 10 minutes and refresh the Intrusion Policy page. (139647/CSCze91353)
- In some cases, if you create a system policy on the primary Defense Center in a high availability configuration and then manually synchronize the secondary Defense Center, the system generates an `ERROR 500 Internal Server Error` message. (139685/CSCze95818)
- In some cases, if you configure and save a report with a time window that includes the transition day from observing Daylight Saving Time (DST) to not observing DST, the system adjusts the time window to begin an hour earlier than you specified. As a workaround, set the time window to begin one hour later. (139713/CSCze91697)
- If you remove an IP address from the global whitelist via the Object Manager page of the Defense Center web interface, the command line interface (CLI) on your Defense Center does not reflect the change. (139784/CSCze91728)
- If you automatically download a patch update by clicking **Download Updates** on the Product Updates page (**System > Updates**), your Defense Center may download the incorrect patch. As a workaround, download patch updates manually by clicking **Upload Update** on the Product Updates page. (141056/CSCze92845)
- If you use Internet Explorer 11 to add a report parameter to the report section title bar while creating a new report template (**Overview > Reporting > Report Templates**), no report fields are added to the template. As a workaround, install and use Internet Explorer 10. (142950/CSCze94011)

- In some cases, the syslog output seen from a managed device reports `SNORT ALERT` as a signature ID instead of the signature ID reported in syslog output seen from the Defense Center. (CSCur40263)
- 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 in the high availability configuration deletes the existing file list data. (CSCur57708)
- In some cases, if you create a new report template with a static time window, the system may not correctly save the time. (CSCur61984)
- You cannot import system-provided Security Intelligence objects to a device that already has system-provided Security Intelligence objects. (CSCur78753)
- In some cases, if you change the selected time zone in the Time Zone Preference tab on the User Preferences page (**Admin > User Preferences > Time Zone Preference**), the system does not calculate daylight savings time for you selected time zone and may display the wrong time. (CSCur92028)
- Resolved an issue where latency may occur on devices with nonpassive interfaces during Snort restart. (CSCus13247)
- The system does not support resetting the password for the admin user on an ASA5585-X device. (CSCus17991)
- If you select **Enable Remote Storage of Reports** from the Reports page (**Overview > Reporting > Reports**) with the Server Message Block (SMB) protocol enabled, the `$User, Host Report: $Host`, `Attack Report: $Attack SID`, and `Sourcefire FireSIGHT Report: $Customer Name` templates fail to generate reports due to unsupported characters in the report names. (CSCus21871)
- In some cases, if you create a file policy containing a Web Application category and a Block Malware rule, the system will not block files identified as malware if the Block Malware rule is positioned after the Web Application category. As a workaround, position the Block Malware rule before the Web Application category. (CSCus64526)
- In some cases, if you place an access control rule referencing a file policy after an access control rule with a web application, the traffic matching the file policy is not identified. As a workaround, position the rule containing the file policy before the rule with the web application. (CSCus64393,CSCus64526)
- In some cases, if you store details in the Clipboard page and create an incident and **Add all to incident**, generate a report from the new incident, then attempt to create a new incident, you are able to add previous clipboard contents to the new incident even though the **Events in your clipboard** section of the Incidents page (**Analysis > Intrusion > Incidents**) is empty. (CSCus67128)
- In some cases, If your system includes an SSL Visibility Appliance (SSLVA) device and you create a file policy containing a Web Application category and a Block Malware rule, your first attempt to download a file over HTTPS may fail. As a workaround, disable the file policy. (CSCus72505)
- In some cases, if you create an access control policy with a rule set to block an object group containing URLs, the system does not block traffic related to the contained URL objects. As a workaround, include the URL(s) to be blocked as individual URL object(s) in the access control rule instead of the object group. (CSCus77551)
- In some cases, if you apply an access control policy to multiple managed devices, the system incorrectly displays the policy status as `pending` when the policy was successfully applied. As a workaround, edit and save the policy, then reapply. (CSCus86011)
- In some cases, if you create an user role, the system may not enable some checkboxes but the options available under the disabled checkboxes are enabled. (CSCus87248)
- If you remove the LSI RegEx card from the top blade of an ASA5585 device, you cannot install the ASA FirePOWER module. (CSCus89754)

- In some cases, if the Defense Center experiences a large amount of data, restoring a backup may fail. (CSCus91552)
- In some cases, if your system experiences a network disruption during a policy apply, and you later attempt to deactivate an unused detector on the Application Detector page (**Policies > Application Detectors**), the system generates a `Failed to deactivate 1 detectors because they are detecting applications used by applied Access Control policies` error. (CSCus91892)
- In some case, if you attempt to restore a backup archive located on a Windows network file server (NFS), backup restoration fails. As a workaround, manually transfer your archived files with WinSCP. (CSCut08317)
- You are unable to block URL's which have not been categorized or assigned a reputation score. (CSCut17683)
- In some cases, if your Defense Center's database experiences system issues, you may be missing your access control policy or your access control policy may be missing rules. If you experience missing rules in your access control policy, contact support. (CSCut30047)
- Access control policy rules currently do not support LDAP group names with 37 or more characters. (CSCut34003)
- The Backup Management tab of the **Managed Device Backup** page (**System > Tools > Backup/Restore > Managed Device Backup**) does not include registered ASA55X5 or ASA55X5-SSP-XX devices as options. (CSCut41338)
- In some cases, if you create an access control policy referencing either a network rule set to block all IPv6 addresses with `::/0` or a network rule set to block all IPv4 addresses with `0.0.0.0/0`, the system incorrectly blocks all traffic. (CSCut58667)
- In some cases, if the system attempts to query an unknown URL, the Cloud Lookup Health Module generates false positive alerts. (CSCut77594)
- If you edit an access control rule with multiple category conditions and attempt to remove one of the conditions, the web management interface only removes the first category condition listed regardless of the condition selected. (CSCuu00585)
- In some cases, if you copy the Top Intrusion Events table from a recently created FireSIGHT Report, the Fields row of the generated table does not include data. As a workaround, manually populate data for the Fields row of the copied table. (CSCuu01020)
- In some cases, if you disable an access control rule referencing an intrusion policy, the Access Control Policy page (**Policies > Access Control**) incorrectly displays the intrusion policy as out-of-date after the access control policy is successfully reapplied. The Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**) displays the correct policy status. (CSCuu15483)
- The system displays the incorrect amount of memory usage on the Memory page (**Overview > Dashboards > Summary Dashboard > Status > System load > Memory**). As a workaround, view the correct memory usage via the Memory Test option in the Memory Usage page (**Health > Health Monitor**). (CSCuu19742)
- In some cases, if you create a file policy and a NAT policy and enable TCP stream preprocessor rules with an HTTP port number that is not an available port from the network access policy's HTTP preprocessor configuration page, the system does not detect malware in traffic that matches the file policy and downloads malware content when it should not. (CSCuu24472)
- In some cases, if you create and delete a custom user role or deactivate and reactivate a user role several times, the system generates extraneous tabs in the web browser. (CSCuu31584)

- In some cases, if you change your system's time zone to a zone east of UTC and add a correlation rule with at least one inactive period to a correlation policy, policy apply fails. As a workaround, delete the old correlation rule and temporarily set your time zone to UTC. Then recreate the correlation rule with the inactive period and apply policy, then reset your time zone and reapply the policy. (CSCuu37600)
- The system does not include audit log entries for login attempts with `<script>alert(1)</script>` as the user name. (CSCuu39516, CSCuu39521)
- In some cases, if your system accumulates large quantities of traffic for an extended period of time, Snort may experience latency and you may experience a disruption in traffic. (CSCuu52545)
- If you experience an error or a failure while updating an appliance from Version 5.3.1 to Version 5.3.1.4 or later, contact Support. (CSCuu54653)
- In some cases, if your device appears to have unapplied changes on the Device Management page (**Devices > Device Management**) and you **Apply Changes**, then click the **View Changes** link from the Apply Device Changes pop-up window, the system generates the Intrusion Policy comparison viewer when it should not. (CSCuu88332)
- In some cases, if you configure a system policy to use remote NTP server to synchronize time to a system with a registered ASA 5500-X device, a Series 2 device, or a Series 3 device running a version older than Version 5.4 and you experience a leap second, your system may use a high amount of CPU. (CSCuv11738)
- In some cases, if you create a new task on the Scheduling page (**System > Tools > Scheduling**) and select the link provided as the Backup Profile, the web page generates as a `HTTP Error 500 Internal server` error page. (CSCuv22624)

Assistance

All new support cases must be opened using the Cisco Technical Assistance Center (TAC) by phone, web or email. To open a TAC case online, you must have a Cisco.com user ID and contract number. If you need assistance opening a case, call the Cisco TAC at 800-553-2447.

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.

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