SOURCEFIRE 3D SYSTEM RELEASE NOTES

Version 5.3

Original Publication: April 21, 2014

These release notes are valid for Version 5.3 of the Sourcefire 3D System. Even if you are familiar with the update process, make sure you thoroughly read and understand these release notes, which describe supported platforms, new and changed features and functionality, known and resolved issues, and product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation instructions for the following appliances:

- Series 2 and Series 3 Defense Centers (the DC500 Rev 1 and 2, DC750 Rev 1 and 2, DC1000 Rev 1 and 2, DC1500, DC3000, and the DC3500)
- Series 2 and Series 3 managed devices (the 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500, 7000 Series, 8000 Series, 3D9900, AMP7150, and the AMP8150)
- Sourcefire Software for X-Series
- 64-bit virtual Defense Centers and managed devices

TIP! For detailed information on the Sourcefire 3D System, refer to the online help or download the *Sourcefire 3D System User Guide* from the Support Site.

If you completed a migration from Version 4.10.3.x (patch 4.10.3.5 or later) to Version 5.2, you must update to Version 5.2.0.3 before beginning the update process to Version 5.3. For more information about migration, see the *Sourcefire 3D System Migration Guide*.

To install Version 5.3 of the Sourcefire Software for X-Series on X-Series appliances, you must uninstall any previous versions and remove any existing

Sourcefire software packages. For update information, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

To update all other appliances running at least Version 5.2.0.4 of the Sourcefire 3D System to Version 5.3, see the procedures outlined in Updating Your Appliances on page 13.

For more information, see the following sections:

- New and Updated Features and Functionality on page 2
- Updates to Sourcefire Documentation on page 10
- Before You Begin: Important Update and Compatibility Notes on page 10
- Product Compatibility on page 13
- Updating Your Appliances on page 13
- Issues Resolved in Version 5.3 on page 25
- Known Issues on page 27
- For Assistance on page 32

New and Updated Features and Functionality

This section of the release notes summarizes the new and updated features and functionality included in Version 5.3 of the Sourcefire 3D System.

- Advanced Malware Protection Features on page 2
- Next-Generation Intrusion Prevention (NGIPS) Features on page 5
- Next-Generation Firewall (NGFW) Features on page 6
- FirePOWER Appliance Features on page 6
- Platform Support Features on page 7
- Changed Functionality on page 8

For detailed information, see the *Sourcefire 3D System User Guide*, *Installation Guide*, *Virtual Installation Guide*, and *Sourcefire Software for X-Series Installation and Configuration Guide*.

Advanced Malware Protection Features

File Capture and Storage

LICENSE: Malware
SUPPORTED DEVICES: Series 3, Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Any except DC500

The file capture feature provides the ability to automatically carve files of interest out of network traffic based on the file type or the file disposition. Once captured, the files can either be stored locally on FirePOWER appliances or automatically

submitted for additional malware analysis using Sourcefire's cloud-based sandboxing technology, dynamic analysis.

File capture is configured as part of a file policy and each file has a SHA-256 calculated to uniquely identify files and reduce duplicates in file storage. Captured files are stored on the primary hard drive of the FirePOWER appliance.

You can manually submit captured files for dynamic analysis or download them from the FirePOWER appliance through event table views, the network file trajectory feature, and the captured files table view.

Dynamic Analysis, Threat Scores, and Summary Reports

LICENSE: Malware
SUPPORTED DEVICES: Series 3, Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Any except DC500

Version 5.3 introduces dynamic analysis, a feature that maximizes your ability to quickly identify new zero-day malicious behavior on your network through the use of cloud-based technology. When configured, you can submit previously unseen files with an unknown disposition to the Sourcefire cloud for an in-depth analysis of the file's behavior. Based on that behavior, a threat score is determined and communicated back to the Defense Center. The higher the threat score, the more likely the file is malicious and action can be taken based on threat score levels.

Sourcefire also provides a related dynamic analysis summary report that provides details on the analysis and why the threat score was assigned to the file. This additional information helps you identify malware and fine tune your detection capabilities.

You can configure your system to automatically capture and send files for dynamic analysis, or you can submit them for analysis on demand. For more information about the file capture feature, see File Capture and Storage on page 2.

Custom Detection

LICENSE: Malware
SUPPORTED DEVICES: Series 3, Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Any except DC500

Custom file detection can be used to identify and block any files moving around your network, even if Sourcefire has not identified the file as malicious. You do not need a cloud connection to perform these lookups, so custom file detection is ideal for use with any type of private intelligence data you have.

If you have identified a malicious file, you can automatically block it by adding its unique SHA-256 value to the custom file detection list. You can use the custom detection list in combination with the clean list, which lets you mark specific files as clean.

Together, the custom file detection list and clean list help you customize your malware protection approach to your specific environment. The custom file

detection list and clean list are included by default in every file policy, and you can opt not to use either or both lists on a per-policy basis.

Spero Engine

LICENSE: Malware
SUPPORTED DEVICES: Series 3, Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Any except DC500

The Spero engine feature provides another cloud-based method for detecting suspicious and potentially new malware in executable files using big data. Spero creates a signature of an executable file based on the structural information of that file, the dynamic-link libraries (DLL) that are referenced, and the metadata from the Portable Executable (PE) header. This feature print then runs through the machine learned data trees for analysis and determines whether the file contains malware. The Spero analysis result is considered jointly with the file disposition to generate a final disposition for the executable file.

SMB File Detection

LICENSE: Protection
SUPPORTED DEVICES: Feature dependent
SUPPORTED DEFENSE CENTERS: Feature dependent

As of Version 5.3, you can now detect, inspect, and block files transferred in NetBIOS-ssn traffic, including files transferred over Server Message Block (SMB).

AMP Cloud Connectivity

LICENSE: Malware, URL Filtering
SUPPORTED DEFENSE CENTERS: Any except DC500

Prior to Version 5.3, to connect to the Sourcefire cloud you had to use TCP Port 32137 and a direct connection from the Defense Center to the cloud.

Version 5.3 introduces proxy support for connecting to the Sourcefire cloud to do malware detection and dynamic analysis. Previously, you had to use TCP port 32137, but now the default connection is made over TCP port 443 to allow more organizations to connect and use Sourcefire's advanced malware intelligence. Use of port 32137 is still supported, but is no longer the default.

Note that if you are updating to Version 5.3 from a previous version of the Sourcefire 3D System, use of legacy port 32137 is enabled by default. If you want to connect via port 443 after updating, deselect the checkbox on the Cloud Services page (**System > Local > Configuration > Cloud Services**).

Next-Generation Intrusion Prevention (NGIPS) Features

Host and Event Correlation IOC Style (Indications of Compromise)

LICENSE: FireSIGHT + Protection or FireAMP subscription
SUPPORTED DEVICES: Feature dependent
SUPPORTED DEFENSE CENTERS: Feature dependent

Host and event correlation introduces the ability to pinpoint the hosts on your network that may have been compromised by an attack. Host and event correlation aggregates data from intrusion events, connection events, Security Intelligence events, and FireAMP events to help you quickly diagnose and contain security breaches on your network.

This feature introduces Sourcefire-provided Indications of Compromise (IOC) rules that allow you to control whether the system generates IOC events for particular types of compromise and correlates those events with the host involved. At the time of event generation, the system sets an IOC tag on the affected host impacted by that IOC event. Hosts that have the most IOC events associated with them from unique detection sources are those that are most likely compromised. Once you have resolved the breach, the IOC tags are removed. IOC events and host tags are viewable in the host profile, network map, Context Explorer, dashboard, and event viewers.

Enhanced Security Intelligence Event Storage and Views

LICENSE: Protection
SUPPORTED DEVICES: Series 3, Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Any except DC500

If your system is configured to blacklist traffic or monitor blacklisted traffic based on Security Intelligence data, you can now view Security Intelligence events in dashboards and in the Context Explorer. Security Intelligence events, although similar to connection events, are stored and pruned separately and have their own event view, workflows, and Custom Analysis dashboard widget presets.

Simplified Intrusion Policy Variable Management

LICENSE: Protection
SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any

The addition of variable sets streamlines and centralizes variable management in the object manager. You create custom variable sets and customize the default variable set to suit your network environment. The default variable set functions as a master key, containing both Sourcefire-provided default variables and user-created custom variables, and can be used to populate custom variable sets. Customizing a variable in this set propagates the change to all other variable sets containing that variable.

The update from Version 5.2 to Version 5.3 automatically transitions existing variables into variable sets. Existing system level variables become custom

variables within the default variable set. Custom variables configured at the intrusion policy level are grouped by intrusion policy into new custom variable sets.

Next-Generation Firewall (NGFW) Features

Geolocation and Access Control

LICENSE: FireSIGHT
SUPPORTED DEVICES: Series 3, Virtual
SUPPORTED DEFENSE CENTERS: Any except DC500

Version 5.3 introduces the ability to filter traffic by source or destination countries from within your access control policy. To take advantage of geolocation filtering, specify the individual countries or reference a geolocation object in an access control policy rule.

Geolocation objects are configured in the object manager and represent one or more countries that your system has identified in traffic on your monitored network. Create geolocation objects to save and organize custom groupings of countries.

URL Filtering License Change

LICENSE: Protection + URL Filtering
SUPPORTED DEVICES: Series 3, Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Any except DC500

Sourcefire no longer requires a Control license to enable URL filtering. Only a Protection license is required. After you add a URL Filtering license for the first time, the Defense Center automatically enables URL filtering and automatic updates.

FirePOWER Appliance Features

8300 Family of Series 3 FirePOWER Appliances

SUPPORTED DEVICES: 3D8350, 3D8360, 3D8370, 3D8390

Version 5.3 introduces the high-powered 8300 Family of Series 3 FirePOWER managed devices. The 8300 Family supports stacking, clustering, all existing NetMods, and all other features of the existing Series 3 8000 Series managed devices. They also provide increased power for faster connection speeds: 15Gbps on the 3D8350, 30Gbps on the 3D8360, 45Gbps on the 3D8370, and 60Gbps on the 3D8390.

Dedicated AMP Appliances

SUPPORTED DEVICES: AMP7150 and AMP8150

Version 5.3 also introduces two new Series 3 FirePOWER managed devices designed with additional processing power to maximize the performance of Sourcefire's AMP features. The AMP7150 is a 71xx Family device with support for small form-factor pluggable (SFP) transceiver with 32GB of RAM and a 120GB hard drive. The AMP8150 is an 81xx Family device with 96GB of RAM, 2 CPUs, 24 cores, and a 400GB hard drive.

Disk Manager Improvements

LICENSE: Any
SUPPORTED DEVICES: Series 2, Series 3, X-Series
SUPPORTED DEFENSE CENTERS: Series 2, Series 3

In Version 5.3, Sourcefire improved disk space management and file pruning on all appliances. These improvements support the file capture feature and enhance overall performance. For more information, see File Capture and Storage on page 2.

Malware Storage Packs

SUPPORTED DEVICES: 8000 Series

Sourcefire now supports the installation of a Sourcefire-supplied second hard drive, or *malware storage pack*, to provide local storage for captured files and free space on the main hard drive for event and configuration storage. You can add a malware storage pack to any 8000 Series managed device (except for the AMP8150, which is shipped with additional storage). Malware storage packs are also supported on stacked or clustered 8000 Series devices (except for the AMP8150).

Compatible managed devices detect if a malware storage pack is added and automatically transfer existing file captures to the added drive, freeing space on the main drive. For more information, see File Capture and Storage on page 2.

WARNING! Do **not** attempt to install third-party hard drives. Installing an unsupported hard drive may damage the device.

Platform Support Features

Sourcefire Software for X-Series

SUPPORTED DEVICES: X-Series

Version 5.3 of the Sourcefire 3D System is now supported on X-Series appliances running X-Series Operating System (XOS) Version 9.7.2 (and later) and Version 10.0 (and later). If you are using an earlier version of XOS, contact Blue Coat

Systems Support. For more information about X-Series, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

Virtual Appliance Initial Setup Improvements

LICENSE: Any
SUPPORTED DEVICES: Virtual, X-Series
SUPPORTED DEFENSE CENTERS: Virtual

As of Version 5.3, you can perform the initial setup on virtual devices without leaving the vCloud workflow by using the vSphere Hypervisor or the vCloud Director. You no longer need to connect to the virtual device console to change the default password, configure networking, set the initial detection mode, and configure the managing Defense Center during initial setup. Those configuration steps can now all be performed during the vCloud deployment workflow. Note that you can still deploy using ESXi, but that it requires additional setup on the VMware console.

Changed Functionality

The following list describes changes to existing features of the Sourcefire 3D System:

- You can now use a shell-based query management tool to locate and stop long-running queries. The query management tool allows you to locate queries running longer than a specified number of minutes and stop those queries. The tool logs an event to the audit log and to syslog when you stop a query.

  Note that only administrative users with shell access rights on the Defense Center can access this tool. For more information, type `query_manager -h` on the Defense Center shell or see Stopping Long-Running Queries in the *Sourcefire 3D System User Guide*.
- Sourcefire now identifies traffic referred by a web server as the web application for referred connections. For example, if an advertisement accessed via advertising.com is actually referred by CNN.com, Sourcefire identifies CNN.com as the web application.
- You can no longer configure access control rules containing any of the following port conditions: `IP 0`, `IP-ENCAP 4`, `IPv6 41`, `IPv6-ROUTE 43`, `IPv6-FRAG 44`, `GRE 47`, `ESP 50`, or `IPv6-OPTS 60`.

  If you are updating from an earlier version of the Sourcefire 3D System, the access control policy rule editor marks invalid rules with a warning and the object manager resets invalid port object values to TCP.
- If you break a stack or cluster, the devices now remain in the primary device's group. Before Version 5.3, the system reverted the devices to the groups they belonged to before they joined a stack or cluster.

- Improved the performance and stability of NetFlow data collection and logging. Sourcefire also added the following new fields for connections exported by NetFlow–enabled devices: **NetFlow Destination/Source Autonomous System**, **NetFlow Destination/Source Prefix**, **NetFlow Destination/Source TOS**, and **NetFlow SNMP Input/Output**.
- You can now use IPv6 addresses to create authentication objects. Note that you cannot use authentication objects with IPv6 addresses to authenticate shell accounts.
- You can now identify unique **Initiator** and **Responder** IP addresses when creating IPv6 fast-path rules on Series 3 managed devices. Before Version 5.3, the fields were fixed and set to Any.
- For fresh installations of Version 5.3 on Series 3 managed devices, the Automatic Application Bypass (AAB) feature is enabled by default. If you update from a previous version of the Sourcefire 3D System, your AAB settings are not affected. Note that AAB activates only when a preset amount of time is spent processing a single packet. If AAB engages, the system kills the affected Snort processes.
- During the update to Version 5.3, the system now stores your currently applied access control policy and up to 10 saved but unapplied revisions to the access control policy, retaining your changes.
- If you schedule multiple report generation tasks at the same time, the system queues the tasks. You can view them on the Task Status page (**System > Monitoring > Task Status**).
- You cannot name security zone objects using the pound sign (#).
- You can now use -1 as the minimum value in intrusion rule `icode` argument ranges. Selecting -1 as the minimum value allows you to include the ICMP code 0 in the range.
- Added a new SMTP preprocessor alert to detect attacks against Cyrus SASL authentication.
- The system now includes file policy UUID metadata for type 502 intrusion events.
- The file disposition Neutral is now Unknown. Files with an Unknown disposition indicate that a malware cloud lookup occurred before the cloud assigned a disposition.
- Added several new Snort decoder rules to identify packets containing malformed authentication headers.
- You can no longer configure custom analysis dashboard widgets based on the **Ingress Interface**, **Ingress Security Zone**, **Egress Interface**, or **Egress Security Zone** fields of the connection summary table.
- The system now alerts you if you attempt to install a version of the Sourcefire Geolocation Database (GeoDB) already installed on your system.

- You can now create correlation rules with **Application Protocol Category**, **Client Category**, and **Web Application Category** conditions.
- As of Version 5.3, LDAP usernames are case-sensitive. Before Version 5.3, usernames were not case-sensitive.

Updates to Sourcefire Documentation

In Version 5.3, the following documents were updated to reflect the addition of new features and changed functionality and to address reported documentation issues:

- *Sourcefire 3D System User Guide*
- *Sourcefire 3D System Online Help*
- *Sourcefire 3D System Installation Guide*
- *Sourcefire 3D System Virtual Installation Guide*
- *Sourcefire Software for X-Series Installation and Configuration Guide*
- *Sourcefire 3D System eStreamer Integration Guide*
- *Sourcefire 3D System Database Access Guide*
- *Sourcefire 3D System Malware Storage Pack Guide*
- *Sourcefire 8000 Series Devices Quick Start Guide*

In addition, the *Sourcefire 3D System User Agent Configuration Guide* was updated for Version 2.2 of the agent, which was released with Version 5.3.

You can download all updated documentation from the Sourcefire Support site.

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.3, you should familiarize yourself with the behavior of the system during and after the update process, as

well as with any compatibility issues or required pre- or post-update configuration changes.

IMPORTANT! The update to Version 5.3 fails if your configuration includes a custom table populated with data from the **Correlation Events** table and the **Applications** table with **Source IP** selected as a common field. If your configuration includes a custom table of this type, delete the custom table and recreate it after completing the update to Version 5.3.

WARNING! Sourcefire **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 on page 11
- Traffic Flow and Inspection During the Update on page 11
- Audit Logging During the Update on page 12
- Returning to a Previous Version on page 13

Configuration and Event Backup Guidelines

Before you begin the update, Sourcefire **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 *Sourcefire 3D System User Guide*.

IMPORTANT! The Defense Center purges backups from previous updates. To retain archived backups, store the backups externally.

Traffic Flow and Inspection During the Update

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

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

Note that when you update clustered devices, the system performs the update one device at a time to avoid traffic interruption.

Traffic Inspection and Link State

In an inline deployment, your managed devices (depending on model) can affect traffic flow via application control, user control, URL filtering, Security Intelligence, and intrusion prevention, as well as switching, routing, NAT, and VPN. 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 *Sourcefire 3D System Installation Guide*.

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

Network Traffic Interruption

DEPLOYMENT	NETWORK TRAFFIC INTERRUPTED?
Inline with configurable bypass (**Configurable bypass** option enabled for inline sets)	Network traffic is interrupted at two points during the update: • At the beginning of the update process, traffic is briefly interrupted while link goes down and up (flaps) and the network card switches into hardware bypass. Traffic is not inspected during hardware bypass. • After the update finishes, traffic is again briefly interrupted while link flaps and the network card switches out of bypass. After the endpoints reconnect and reestablish link with the sensor interfaces, traffic is inspected again. **IMPORTANT!** The configurable bypass option is **not** supported on virtual devices, non-bypass NetMods on 8000 Series devices, or SFP transceivers on 71xx Family devices.
Inline	Network traffic is blocked throughout the update.
Passive	Network traffic is not interrupted, but also is not inspected during the update.

Switching and Routing

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

Audit Logging During the Update

When updating appliances that have a web interface, after the Sourcefire 3D 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.

Product Compatibility

You must use at least Version 5.3 of the Defense Center to manage devices running Version 5.3.

Defense Centers running Version 5.3 can manage physical and virtual devices running Version 5.2.0.4 or greater and Sourcefire Software for X-Series running Version 5.3.

Web Browser Compatibility

Version 5.3 of the web interface for the Sourcefire 3D System has been tested on the browsers listed in the following table.

Web Browser Compatibility

Browser	Required Enabled Options and Settings
Chrome 30	JavaScript, cookies
Firefox 24	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 9 and 10	JavaScript, cookies, Secure Sockets Layer (SSL) v3, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically**

Screen Resolution Compatibility

Sourcefire 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 Sourcefire 3D System for any reason, contact Sourcefire Support for more information.

Updating Your Appliances

You **cannot** update appliances running Version 4.10.x of the Sourcefire 3D System directly to Version 5.3. Instead, you must reimage physical appliances and recreate virtual appliances. Note that reimaging results in the loss of almost **all** configuration and event data on the appliance. For more information about

reimaging and recreating appliances, see the *Sourcefire 3D System Installation Guide*.

TIP! If you want to retain essential configuration and event data, you can perform a limited migration from Version 4.10.3.x (patch 4.10.3.5 or later) to Version 5.2.0.x, then update your migrated deployment to Version 5.3. Before updating your migrated deployment to Version 5.3, your system must be running Version 5.2.0.3. For more information, see the *Sourcefire 3D System Migration Guide*.

To install Version 5.3 of the Sourcefire Software for X-Series on X-Series appliances, you must uninstall any previous versions and remove any existing Sourcefire software packages. For update information, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

To update all other appliances running at least Version 5.2.0.4 of the Sourcefire 3D System to Version 5.3, see the procedures outlined below. The following sections help you to prepare for and install the Version 5.3 update:

- Planning the Update on page 14
- Updating a Defense Center on page 19
- Updating Managed Devices on page 21
- Using the Shell to Perform the Update on page 23

WARNING! 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.

TIP! The system may generate an extraneous **Module Disk Usage: Frequent drain of Connection Events** health alert. You can safely ignore the health alert if you see it during the update to Version 5.3.

Planning 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 on page 10. To ensure a smooth update process, you must also read the following sections.

Sourcefire 3D System Version Requirements

To update to Version 5.3, an appliance must be running at least Version 5.2.0.4. If you are running an earlier version, you can obtain updates from the Sourcefire Support Site.

A Defense Center must be running at least Version 5.3 to update its managed devices to Version 5.3.

The closer your appliances' current version to the release version (Version 5.3), the less time the update takes.

Operating System Requirements

You can host 64-bit virtual Sourcefire 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

For more information, see the *Sourcefire 3D System Virtual Installation Guide*.

You can run Sourcefire Software for X-Series on X-Series appliances running XOS Version 9.7.2 and later and Version 10.0 and later. For more information, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

Time and Disk Space Requirements

The following table provides disk space and time guidelines for the Version 5.3 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.

Do **not** restart the update or reboot your appliance at any time during the update process. Sourcefire 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.

TIP! 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 Sourcefire Support.

Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
Series 2 Defense Centers	50 MB	5.5 GB	n/a	40-55 minutes
Series 2 managed devices	40 MB	2.2 GB	268 MB	45-60 minutes
Series 3 Defense Centers	150 MB	4.3 GB	n/a	50-65 minutes
Series 3 managed devices	50 MB	3 GB	388 MB	30-45 minutes
3D9900 managed devices	75 MB	2 GB	388 MB	55-70 minutes
virtual Defense Centers	150 MB	388 MB	n/a	hardware dependent
virtual managed devices	50 MB	3 GB	388 MB	hardware dependent

Configuration and Event Backup Guidelines

Before you begin the update, Sourcefire **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.

You can 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 *Sourcefire 3D System User Guide*.

When to Perform the Update

Because the update process may affect traffic inspection, traffic flow, and link state, Sourcefire **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.

You **cannot** update X-Series appliances running Version 4.10.x to Version 5.3. Instead, you must uninstall the previous version and then install Version 5.3. For

detailed instructions, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

Order of Installation

You must update your Defense Centers before you can update the devices they manage.

Installing the Update on Paired Defense Centers

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

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

Installing the Update on Clustered Devices

When you install an update on clustered devices, the system performs the update on the devices one at a time. When the update starts, the system first applies it to the secondary device, which goes into maintenance mode until any necessary processes restart and the device is processing traffic again. The system then applies the update to the primary device, which follows the same process.

Installing the Update on Stacked Devices

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

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

X-Series Devices

You **cannot** update X-Series appliances running Version 4.10.x to Version 5.3. Instead, you must uninstall the previous version and then install Version 5.3. For detailed instructions, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

After the Installation

After you perform the update on either the Defense Center or managed devices, you **must** reapply device configuration and access control policies. Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Sourcefire 3D 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
- checking the Support site to see if a patch is available for Version 5.3
- updating your intrusion rules and vulnerability database (VDB), if necessary

> **IMPORTANT!** After you complete the system software update, install VDB build 156 or later to your Defense Center and reapply your access control policies.

- making any required configuration changes based on the information in New and Updated Features and Functionality on 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 a Defense Center

Use the procedure in this section to update your Defense Centers, including virtual Defense Centers. For the Version 5.3 update, Defense Centers reboot.

WARNING! Before you update the Defense Center, reapply access control policies to any managed devices. Otherwise, the eventual update of the managed device may fail.

WARNING! 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.

IMPORTANT! Updating a Defense Center to Version 5.3 removes existing uninstallers from the appliance.

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 on page 10 and Planning the Update on page 14.

2. Download the update from the Sourcefire Support Site:
   - for Series 2 Defense Centers:
     `Sourcefire_3D_Defense_Center_Upgrade-5.3.0-XXX.sh`
   - for Series 3 and virtual Defense Centers:
     `Sourcefire_3D_Defense_Center_S3_Upgrade-5.3.0-XXX.sh`

   IMPORTANT! 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.

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.

   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.

6. Select **System > Updates**.

   The Product Updates tab appears.

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

   The Install Update page appears.

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 being run.

   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.

   WARNING! 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 5.3.0. 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.

    For information on rule updates, see the *Sourcefire 3D 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 *Sourcefire 3D System User Guide*.

16. Reapply device configurations to all managed devices.

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

17. Reapply access control policies to all managed devices.

    WARNING! 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 *Sourcefire 3D System User Guide*.

18. If a patch for Version 5.3 is available on the Support site, apply the latest patch as described in the *Sourcefire 3D System Release Notes* for that version.

Updating Managed Devices

After you update your Defense Centers to Version 5.3, use them to update the devices they manage.

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

For the Version 5.3 update, all devices reboot. Managed devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see

Traffic Flow and Inspection During the Update on page 11.

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

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

To update managed devices:

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

   For more information, see Before You Begin: Important Update and Compatibility Notes on page 10 and Planning the Update on page 14.

2. Update the Sourcefire software on the devices' managing Defense Center; see Updating a Defense Center on page 19.

3. Download the update from the Sourcefire Support Site:

   - for Series 2 managed devices:
     `Sourcefire_3D_Device_Upgrade-5.3.0-XXX.sh`
   - for Series 3 managed devices:
     `Sourcefire_3D_Device_S3_Upgrade-5.3.0-XXX.sh`
   - for 3D9900 managed devices:
     `Sourcefire_3D_Device_x900_Upgrade-5.3.0-XXX.sh`
   - for virtual managed devices:
     `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.3.0-XXX.sh`

   IMPORTANT! Download the update directly from the Support Site. If you transfer an update file by email, it may become corrupted.

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.

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

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

   The Install Update page appears.

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

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

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

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

   Note that managed devices may reboot twice during the update; this is expected behavior.

   WARNING! 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.

9. Select **Devices > Device Management** and confirm that the devices you updated have the correct software version: Version 5.3.0.

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

11. Reapply device configurations to all managed devices.

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

12. Reapply access control policies to all managed devices.

    Applying an access control policy may cause a short pause in traffic flow and processing, and may also cause a few packets to pass uninspected. For more information, see the *Sourcefire 3D System User Guide*.

13. If a patch for Version 5.3 is available on the Support site, apply the latest patch as described in the *Sourcefire 3D System Release Notes* for that version.

Using the Shell to Perform the Update

Although Sourcefire recommends that you use the web interface on your Defense Centers to perform updates, there may be rare situations where you need to update the appliance using the bash shell.

For the Version 5.3 update, all appliances reboot. Managed devices do **not** perform traffic inspection, switching, routing, NAT, VPN, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update on page 11.

Sourcefire has seen failures in specific circumstances and plans to resolve them in an upcoming patch. If you see an error message that

To install the update using the shell:

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

   For more information, see Before You Begin: Important Update and Compatibility Notes on page 10 and Planning the Update on page 14.

2. Download the appropriate update from the Sourcefire Support Site:

   - for Series 2 Defense Centers:
     `Sourcefire_3D_Defense_Center_Upgrade-5.3.0-XXX.sh`
   - for Series 3 and virtual Defense Centers:
     `Sourcefire_3D_Defense_Center_S3_Upgrade-5.3.0-XXX.sh`
   - for Series 2 managed devices:
     `Sourcefire_3D_Device_Upgrade-5.3.0-XXX.sh`
   - for Series 3 managed devices:
     `Sourcefire_3D_Device_S3_Upgrade-5.3.0-XXX.sh`
   - for 3D9900 managed devices:
     `Sourcefire_3D_Device_x900_Upgrade-5.3.0-XXX.sh`
   - for virtual managed devices:
   - `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.3.0-XXX.sh`

   IMPORTANT! Download the update directly from the Support Site. If you transfer an update file by email, it may become corrupted.

3. Log into the appliance's shell using an account with Administrator privileges.

   For virtual appliances, log in using the virtual console in the VMware vSphere Client. Note that on a Series 3 or virtual managed device, you must type expert to display the shell prompt.

4. At the prompt, run the update as the root user, providing your password when prompted:

   `sudo install_update.pl /var/sf/updates/`*`update_name`*

   where *`update_name`* is the file name of the update you downloaded earlier.

   The update process begins.

5. When the update is complete, the appliance reboots. You can monitor the update and complete any post-update steps as described in the following sections:

   - Updating a Defense Center on page 19
   - Updating Managed Devices on page 21

Issues Resolved in Version 5.3

The following issues are resolved in Version 5.3:

- Improved the performance and stability of VPN. (116996, 119698, 123636)
- Resolved an issue where modifying the device configuration on a clustered stack and immediately applying the changes caused the apply to fail and the system to display an error message in the task status queue. (121625)
- Resolved an issue where, in some cases, installing a new intrusion rule update caused custom intrusion rule classifications referenced by correlation rules to revert to predefined classifications. (122163)
- Resolved an issue where, in some cases, network discovery policies did not function as expected if you applied two or more network discovery rules constrained by the same zones and networks that were configured to discover a different combination of hosts, users, and applications. (122853)
- Resolved an issue where LDAP authentication could fail if the DNS entries in your network environment for your LDAP server's hostname and IP address did not match. (123447)
- Resolved an issue where updates of the Sourcefire 3D System required upwards of three hours on Series 3 appliances. (124148)
- Resolved an issue where, in some cases, you could not edit a device group if it contained an inactive managed device. (124286)
- The system now generates an error message when you attempt to install an intrusion rule update while the system is already running an update of the Sourcefire 3D System. (124290)
- Resolved an issue where, in rare cases, the Defense Center did not back up events onto remote storage. (124350)
- Resolved an issue where, in some cases, the system displayed an erroneous **Please wait, loading...** message. (124918)
- Improved the performance of Nmap scans. (124999)
- Resolved an issue where the system incompletely terminated failed intrusion rule updates. (125368)
- Resolved an issue where the system generated false positive alerts on the SMTP preprocessor rules 124:1, 124:3, or 124:10. (125449)
- Security Issue Resolved multiple packet display issues. (125531, 132258)
- Improved the performance of sensitive data analysis. (125588, 126167)
- Resolved an issue where the system ran an Nmap scan from a device even if you used a remediation where **Scan from reporting device** was disabled. (125608)
- Resolved an issue where the system generated false positive alerts in reassembly traffic if you enabled any of the auto-detect DCE/RPC preprocessor options. (125737)

- Resolved an issue where, after importing a new intrusion rule update, the number of imported rules in an intrusion policy did not match the number of rules in the import log. (125900)
- Security Issue Resolved an issue where the system granted incorrect access privileges to users with limited user roles. (126016, 127428, 127779)
- Resolved multiple synchronization issues on managed devices in clustered, stacked, and clustered and stacked configurations. (126106, 128724)
- Improved the stability of syslog alert responses when sending connection events to the syslog. (127682)
- Resolved an issue where the system generated events on intrusion rule 135:2 for incomplete (SYN-only) connections when you enabled the TCP stream preprocessor option **Require TCP 3-Way Handshake** and you configured the rate-based attack prevention preprocessor to limit excessive simultaneous connections. (127803)
- Resolved an issue where, if you configured a traffic profile and a correlation rule to trigger on traffic spikes at or above two standard deviations, the system did not generate a correlation event. (128107)
- Resolved an issue where the system generated false positive alerts on intrusion rule 1:24490. (128304)
- Resolved a hardware issue where, in rare cases, the 3D8120, 3D8130, 3D8140, and 3D8250 experienced system issues and required a reboot. (128689)
- Resolved an issue where if you disabled user detection in LDAP traffic using your network discovery policy, the Defense Center stopped logging User Agent login data. (128741)
- Resolved an issue where, in some cases, you could not perform on-demand user data retrieval and download if you scheduled automatic LDAP user data retrieval. (128962)
- Security Issue Resolved cross-site scripting (XSS) vulnerabilities in the object manager and rule editor. (129052, 132023)
- Resolved an issue where, in some cases, if you viewed reviewed intrusion events and drilled down to the packet view, there were no visible events and the reviewed constraint was removed. (129257)
- Resolved an issue where, in some cases, the system incorrectly identified SMTP traffic and generated a connection event with missing application information if the SMTP server responded with a connection error. (130085)
- Resolved an access control policy synchronization issue on Defense Centers in a high availability configuration. (130475)
- Resolved an issue where, in rare cases, the system generated critical health alert emails containing indecipherable messages. (130518)
- Resolved multiple display issues on the security zones page in the object manager. (130569, 130631, 130632)

- Resolved an issue where drilling down in a custom workflow redirected you to the incorrect packet view page for an intrusion event. (130620)
- Resolved an issue where, in some cases, the system restore boot option did not output to the serial port on managed devices even if you selected **Physical Serial Port** as the remote console access option. (130772)
- Improved the stability of clustered managed devices when failing over after a hardware failure. (130811, 130812, 131031, 133088, 130602)
- Resolved a failover synchronization issue on clustered managed devices. (130829)
- Improved the system's malware analysis and blocking capabilities when handling file transfer protocol (FTP) traffic. (130888, 133134)
- Resolved an issue where, in rare cases, the intrusion policy page failed to display. (131181)
- Resolved an issue where, in rare cases, the table view of servers (**Analysis > Hosts > Servers**) duplicated servers and produced inaccurate server counts. (131329)
- Resolved an issue where, in some cases, if you configured static routes as described in KB article 000001950 and made a subsequent change to the network configuration, the system dropped the static routes until after the next system reboot. (131646)
- Improved the stability of stacking three managed devices in a Tri-Stack. (131836, 131896)
- Resolved an issue where the system misplaced the home directory files for user accounts after updating to a major version of the Sourcefire 3D System. (132503)
- Resolved an issue where disabling the **Quoted-Printable Decoding Depth** advanced option in your intrusion policy did not prevent the system from generating events on intrusion rule 124:11. (132538)

Known Issues

The following known issues are reported in Version 5.3:

- 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)
- 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, 130652)

- In rare cases, configuring an intrusion policy that contains local intrusion rules in a layer that is shared with another intrusion policy may cause intrusion policy exports to fail. As a workaround, create a backup copy of each shared layer and remove the shared layers from the intrusion policies before exporting. After the export finishes, re-add the shared layers to the intrusion policies. (132312)
- In some cases, large system backups may fail if disk space usage exceeds the disk space threshold before the system begins pruning. (132501)
- In rare cases, Snort may stop processing packets if any of your intrusion policy rules contain the sensitive data rule classification. (132600)
- 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)
- If you reboot a Series 3 managed device after a Sourcefire 3D System update fails, subsequent updates may fail even after you resolve the original issue. (132700)
- If you delete a previously-imported local intrusion rule, you cannot re-import the deleted rule. (132865)
- In rare cases, the system may not generate events for intrusion rules 141:7 or 142:7. (132973)
- In rare cases, Snort drains system resources if you create and apply an access control policy with rules that specify an unusually large range of ports and contain other rule conditions that would cause the Defense Center to send them to the device in expanded form. (132998)
- In some cases, remote backups of managed devices include extraneous unified files, generating large backup files on your Defense Center. (133040)
- The Security Intelligence page of your access control policy cannot display more than 100 available security zones. (133418)
- In some cases, configuring a proxy server to authenticate with Message Digest 5 (MD5) authentication causes communication issues with the Defense Center. As a workaround, configure basic or NLTM authentication. (133727, 135041, 135076)
- You must edit the maximum transmission unit (MTU) on a managed device using the appliance's CLI or shell. You cannot edit the MTU on a managed device via the user interface. (133802)
- If you use the command line interface (CLI) to register a Series 3 or virtual managed device to a Defense Center in a high availability configuration, device registration fails for the second Defense Center. As a workaround, run the `add_manager.pl` script from the managed device's shell to register it to the Defense Center. (133825)

- 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, 134097)
- Reapplying any of your intrusion policies (individually or part of an access control policy reapply) a total of 4096 or more times on a single managed device causes system issues. (134231)
- 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)
- In rare cases, the system generates an extraneous **Module Disk Usage: Frequent drain of Connection Events** health alert. You can safely ignore the health alert if you see it during the update to Version 5.3. (134355, 137660)
- Sourcefire documentation incorrectly states that you can perform geolocation-based traffic filtering in access control policies using Sourcefire Software for X-Series. You **cannot** perform geolocation-based traffic filtering in access control policies on X-Series. (134400)
- 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)
- Sourcefire documentation does not reflect that the system does not match traffic or generate events on access control rules referencing user groups unless the user group was previously seen in traffic and entered into the cache. If the access control policy default action is set to **Block All Traffic**, the system may block an allowed user group the first time traffic from a user in that group is seen on your network. (134440)
- If you install a version of the vulnerability database (VDB) and you previously enabled NAVL detectors in your access control policy, the system may not mark your access control policy as out-of-date. To synchronize the NAVL detectors between your Defense Center and managed devices, reapply your access control policy completely after installing a new version of the VDB. (134458)
- 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)
- 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)
- 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)

- If Greenwich Mean Time (GMT, also known as UTC) is not your local timezone, scheduled geolocation updates may fail. If your local timezone is +X number of hours from GMT, schedule geolocation updates for X:00 or later. If your local timezone is -X number of hours from GMT, schedule geolocation updates for (24:00 - X) or earlier. For example, if your local timezone is UTC-5, schedule updates before 19:00 local time. (134742)
- When querying the database, you cannot perform joins using **host_id** or **application_tag_id** fields in the application_host_map table. (134791)
- 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)
- 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)
- You cannot enter more than 450 characters in the **Base Filter** field when creating an LDAP authentication object. (135314)
- 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 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)
- 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)
- If you update a managed device from Version 5.1.1.x to Version 5.2.x and then to Version 5.3, the system generates extraneous health alerts for **high unmanaged disk usage**. (135689)
- If you configure a custom table populated with data from the **Correlation Events** table and the **Applications** table, then select **Source IP** as a common field, updates to Version 5.3 fail. As a workaround, delete the custom table and recreate it after updating to Version 5.3. (135735)
- If you update an appliance from Version 5.2.x to Version 5.3 and later create a backup, you **cannot** restore the backup on appliances that were reimaged to Version 5.3. (135869)

- In some cases, if you configure an access control policy with a Monitor rule (which forces end-of-connection logging) and a Trust rule with **Log at Beginning of Connection** enabled, the system may not generate end-of-connection events for matching SSH-encrypted traffic. As a workaround, configure the rules as stated above and add an Allow rule directly above the Trust rule. Configure the Allow rule with the same conditions as your Trust rule, with both **Log at Beginning of Connection** and **Log at End of Connection** enabled, and with an application condition that matches SSH-encrypted traffic. (135952)
- If you schedule a task with **Report** as the job type, the system does not attach the report to the emailed status report. (136026)
- In some cases, the system restricts access to the User Management page (**System > Local > User Management**) on physical managed devices. As a workaround, access the User Management page as the `admin` user by manually entering the URL: `https://`*`appliance`*`/admin/user/view/cgi`, where *`appliance`* is the IP address or name of the appliance. (136079)
- 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, 136614)
- 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)
- 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)
- 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)
- Connection events logged to the syslog or SNMP trap server may have incorrect **URL Reputation** values. (138504)
- 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, 139177)
- Security 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)

For Assistance

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

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

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

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

Thank you for using Sourcefire products.

Legal Notices

Disclaimers