SOURCEFIRE 3D SYSTEM RELEASE NOTES

Version 5.2

Original Publication: June 16, 2013
Last Updated: May 13, 2014

These release notes are valid for Version 5.2 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, as well as product and web browser compatibility. They also contain detailed information on prerequisites, warnings, and specific installation instructions for the following appliances:

- DC750, DC1500, and DC3500 Defense Centers
- 3D7010, 3D7020, 3D7030, 3D7110, 3D7115, 3D7120, 3D7125, 3D8120, and 3D8130 managed devices, in a non-stacked configuration
- 3D8140 and 3D8250 managed devices, either stacked or non-stacked
- 3D8260, 3D8270, and 3D8290 managed devices
- 64-bit virtual Defense Centers and managed devices

To update Series 3 and virtual devices running at least Version 5.1.1.1 of the Sourcefire 3D System to Version 5.2, see the procedures outlined in Updating Your Appliances on page 13.

WARNING! Appliances running Version 4.10.x of the Sourcefire 3D System **cannot** be updated directly to Version 5.2. To update, you must reimage your appliances. Refer to the *Sourcefire 3D System Installation Guide* for reimage instructions. Note that this will result in a loss of all events and configuration data stored on your appliances.

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.

For more information, see the following sections:

- New and Updated Features and Functionality on page 2
- Changed Functionality on page 8
- Updates to Sourcefire Documentation on page 10
- Before You Begin: Important Update and Compatibility Notes on page 11
- Product Compatibility on page 13
- Updating Your Appliances on page 13
- Issues Resolved in Version 5.2 on page 24
- Known Issues on page 29
- 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 5.2 of the Sourcefire 3D System. For detailed information, see the *Sourcefire 3D System User Guide*, *Installation Guide*, and *Virtual Installation Guide*.

Advanced Malware Protection

Version 5.2 adds two new features to enhance the malware protection capabilities of the Sourcefire 3D System: malware blocking and network file trajectory.

Malware Blocking

The Sourcefire 3D System network-based advanced malware detection capabilities added in Version 5.1.1 identifies individual files as they enter your network, creates a fingerprint of each file, checks the fingerprint against the Sourcefire cloud to determine the disposition of the file, and alerts you to files identified as malware.

With the addition of malware blocking in Version 5.2, the Sourcefire 3D System now provides advanced malware protection (AMP). You can now configure file policies to block transfer of known malware files.

Based on the disposition of each detected file and the rules you set in your file policies, the Defense Center instructs a managed device either to block the file or to allow its upload or download. To improve performance, if the system already knows the disposition for a file based on its SHA-256 hash value, the Defense Center uses a cached disposition rather than querying the Sourcefire cloud.

If necessary, you can override dispositions from the cloud on a file-by-file basis with the global malware whitelist. If a file has a disposition in the cloud that you know to be incorrect, you can add the file's SHA-256 value to the whitelist. When the system detects a file from the whitelist, it does not perform a malware lookup

or block the file as malware. You can enable use of the global malware whitelist on a per-file-policy basis.

Several analysis tools let you track AMP events, including the Context Explorer, the dashboard, the event views, and the network file trajectory view. Connection, file, and malware events all reflect when a file is blocked because of malware.

You can perform AMP, which requires Protection and Malware licenses, using any Series 3 managed device or virtual device. You can manage an AMP deployment using any Series 3 or Series 2 Defense Center, except a DC500.

Network File Trajectory

The network file trajectory feature provides a visual, interactive representation of the path an infected file takes across your network, to help you understand the broader impact, context, and spread of malware across the network and endpoints. This view depicts point of entry, propagation, protocols used, and the users or endpoints involved in the transfer. You can use the map to determine which hosts may have transferred malware or are at risk and to observe file transfer trends.

File trajectory information provides standard information about the file (the file name, type, disposition, actions taken by the system, and so on) as well as when it was first and last seen, the number of hosts associated with the file, and the name of any associated threats. The trajectory of a file through your network is illustrated in visual form on the File Trajectory page. You can access the File Trajectory page directly (**Analysis > Files > Network File Trajectory**) or from the Context Explorer, dashboard, or event views of connection, file, or malware events.

You can view network file trajectories on any file where a malware cloud lookup occurred using AMP or on any file detected or quarantined by FireAMP, Sourcefire's endpoint-based advanced malware analysis and protection solution.

Next-Generation Firewall (NGFW)

Several new device management features were added in Version 5.2: high availability state sharing, gateway VPN configuration, policy-based configuration of network address translation (NAT), and clustered stacking.

Clustered State Sharing

The clustered state sharing feature, also referred to as high availability (HA) state sharing, allows clustered devices or clustered stacks to synchronize their states so that, if either device or stack in the cluster fails, the other peer can take over with no interruption to traffic flow. This provides improved failover capability for strict TCP enforcement, unidirectional access control rules, and blocking persistence. Clustered state sharing is supported for VPN and NAT configurations.

With state sharing, devices in the cluster allow TCP sessions to continue after failover without having to reevaluate the connection against your access control rules, even if strict TCP enforcement is enabled.

State sharing also allows the system to transfer the status of allowed connections matching unidirectional access control rules during failover. Without state sharing, if an allowed connection is still active following a failover and the next packet is seen as a response packet, the system denies the connection. With state sharing, a midstream pickup matches the existing connection and the connection continues to be allowed.

Another advantage of state sharing is that while many connections are blocked on the first packet based on access control rules or other factors, there are cases where the system allows some number of packets through before determining that the connection should be blocked. With state sharing, the system immediately blocks the connection on the peer device or stack as well.

You can enable state sharing on clustered Series 3 managed devices with a Control license enabled.

Gateway VPN

You can now configure the Sourcefire 3D System to build secure Virtual Private Network (VPN) tunnels between virtual routers on Sourcefire managed devices and a remote device. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel.

The Sourcefire 3D System builds tunnels using the Internet Protocol Security (IPSec) protocol suite. The system uses the IKE protocol to mutually authenticate the two gateways against each other as well as to negotiate the security association (SA) for the tunnel. Packets across a VPN tunnel are supported for both the Authentication Header (AH) and Encapsulating Security Payload (ESP) security protocols.

The system supports three types of VPN deployments: point-to-point, star, and mesh.

In a point-to-point VPN deployment, two endpoints communicate directly with each other.

In a star VPN deployment, a central endpoint (hub node) establishes a secure connection with multiple remote endpoints (leaf nodes). Star deployments commonly represent a VPN that connects an organization's main and branch office locations using secure connections over the Internet or other third-party network. Star VPN deployments provide all employees with controlled access to the organization's network.

In a mesh VPN deployment, all endpoints can communicate with every other endpoint by means of an individual VPN tunnel. The mesh deployment offers redundancy so that when one endpoint fails, the remaining endpoints can still communicate with each other. This type of deployment commonly represents a VPN that connects a group of decentralized branch office locations.

Note that this feature is only available on Series 3 devices. To deploy VPN, you must enable Protection, Control, and VPN licenses on each of the managed devices used for the VPN.

Policy-Based NAT

Version 5.2 introduces the ability to create a network address translation (NAT) policy. A NAT policy determines how the system performs routing with NAT.

You can now create and use both static and dynamic NAT rules for further flexibility and granular control of NAT configuration. Policy-based NAT supports the following types of rules:

- static, which provide one-to-one translations on destination networks and optionally port and protocol
- dynamic IP, which translate many-to-many source networks, but maintain port and protocol
- dynamic IP and port, which translate many-to-one or many-to-many source networks and port and protocol

You can configure NAT policies in different ways to manage specific network needs:

- to expose an internal server to an external network
- to allow an internal host or server to connect to an external application
- to hide private network addresses from an external network by using a block of IP addresses
- to hide private network addresses from an external network using a limited block of IP addresses and port translation

In previous versions, you could configure NAT through device-based NAT rules. Policy-based NAT replaces that functionality. When you update managed devices to Version 5.2, the device-based NAT rules for that device (formerly configured under **Devices > Device Management > Edit**) become a NAT policy (under the **Devices > NAT** tab on the Defense Center) with equivalent rules.

You can use policy-based NAT on Series 3 managed devices with a Control license enabled.

Clustered Stacking

In addition to the ability to create clustered configurations of managed devices, you can now establish redundancy of networking functionality and configuration data between two identically configured peer device stacks. Just as with paired individual devices in a cluster, clustered stacks provide a backup option if one stack fails. As in the existing clustering feature, all devices in the configuration must have identical licenses and must have Control licenses. When you register or unregister any device in a clustered stack with a Defense Center, the entire clustered stack is registered or unregistered as a group.

All Series 3 devices that support stacking are supported for this feature. However, stacked 3D9900 devices are not supported.

Drop BPDUs Support

The drop Bridge Protocol Data Units (BPDUs) configuration added in Version 5.2 allows you to set up an inline configuration that operates over a single physical link. You can now configure a virtual switch with two logical interfaces; each interface must have a different configured VLAN tag. Additionally, on a third-party switch or other supported device, you must configure two VLANs and two logical interfaces; each interface must be in a different VLAN but configured on the same physical port.

Series 2 Device Reimaging

Series 2 appliances are the second series of Sourcefire physical appliances, which includes the following appliance models:

- 3D500/1000/2000
- 3D2100/2500/3500/4500
- 3D6500
- 3D9900
- DC500/1000/3000

Version 5.2 of the Sourcefire 3D System can now run on Series 2 appliances. Previously, Series 2 devices supported only 4.x versions of the Sourcefire 3D System. Note that Series 2 devices running Version 5.2 must be managed by a Defense Center; they no longer have standalone capabilities. For more information, see the *Sourcefire 3D System User Guide*.

To update any Series 2 appliance to Version 5.2 from Version 4.x, you must reimage the appliance, which discards all events and configuration data stored on those appliances. For more information about reimaging, see the *Sourcefire 3D System Installation Guide*.

Geolocation

The geolocation feature enhances Sourcefire 3D System analysis tools with data about the geographical sources of routable IP addresses (the country, continent, and so on). You can use this data to determine if, for example, connections originate from or terminate in countries unconnected with your organization.

Geolocation information is available in intrusion events, connection events, file events, malware events, host profiles, and user profiles. The Context Explorer and the dashboard can also now include geolocation information.

After you install a geolocation database (GeoDB) update, you can view granular information available for an IP address, such as postal code, coordinates, time zone, Autonomous System Number (ASN), internet service provider (ISP), use type (home or business), organization, domain name, connection type, and proxy information. Note that the system does not retroactively generate data for events logged before the update. You can also pinpoint the detected location with any of four third-party map tools. Note that without a GeoDB update, only the flag icon and ISO3 alpha country code appear.

Network Discovery

Two new areas of functionality have been added to network discovery for Version 5.2: IPv6 support for network discovery and support for user logoff events generated by Version 2.1 of the Sourcefire User Agent.

IPv6 Support

Version 5.2 introduces extensive support for IPv6 addresses in features that were previously limited (partially or completely) to IPv4 addresses. These include adaptive profiles, auditing compliance, correlation, custom fingerprinting, FireSIGHT recommendations, host profiles, intrusion events, IP packet defragmentation, network discovery, the network map, network objects, and the User Agent.

Hosts on your monitored network may now have multiple associated IP addresses (both IPv4 and IPv6). Most parts of the system coordinate data for each of a host's IP addresses to give a full picture of the host's activity and to allow you to take action against an entire host easily.

Sourcefire User Agent Logoff Detection

User Agents monitor users as they log into the network or when accounts authenticate against Active Directory credentials for other reasons and maps users to host IP addresses, to support user access control.

Version 2.1 of the Sourcefire User Agent also now detects logoffs of active directory users. When the agent checks a host and discovers that the expected user is no longer logged in, the agent generates a logoff for that user. When the Defense Center receives the logoff, it unmaps the user from the previously associated IP address.

Access Control

Version 5.2 also adds new functionality in the access control policy: support for source ports and ICMP types and codes in port conditions in access control rules and support for blocking encrypted application traffic using either application conditions or URL conditions.

Source Ports in Access Control Rules

You can now specify source ports as a condition for access control rules; this expands upon the existing capability to specify destination ports. The source ports you specify must be TCP or UDP ports.

ICMP Types and Codes in Access Control Rules

You can now use Internet Control Message Protocol (ICMP) types and codes in access control rules, correlation rules, and port objects. You can also now view ICMP types and codes for all relevant events in the event viewer.

SSL Application Detection

Version 5.2 adds many new application detectors for applications in SSL traffic, allowing you to identify, and optionally block, encrypted application sessions based on the common name from the SSL client certificate used in the session.

URL Blocking based on SSL Common Name

You can now block encrypted application traffic using a URL based on the common name in an SSL certificate.

Updates to API Support

Version 5.2 introduces the ability to request intrusion rule documentation using either eStreamer or the database access feature. In addition, several structures were updated for new features.

eStreamer and Database Access Updates

Version 5.2 contains several data structures updated for IPv6 address support, geolocation changes, changes to support malware blocking, ICMP type and code support, and bug fixes. For more information, see the *Sourcefire 3D System eStreamer Integration Guide* and *Sourcefire 3D System Database Access Guide* for Version 5.2.

Extended Rule Documentation

You can now request intrusion rule documentation using eStreamer. You can also use the database access feature to query intrusion rule documentation.

Changed Functionality

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

- Discovery host profiles now display data about the operating systems of MAC-only hosts.
- The FTP/Telnet preprocessor now has two new configurable fields: **File Get Commands** and **File Put Commands**.
- You can now detect and block files and malware transferred via the FTP (File Transfer Protocol) application protocol and files uploaded using HTTP.
- You can now configure brightness and contrast settings for the LCD screen on Series 3 devices.
- Hyphens (-), dollar signs ($), asterisks (*), and underscores (_) are now supported characters when naming community strings for SNMPv2 alerts (**Policies > Actions > Alerts**).
- You can no longer use semicolons (;) when naming custom rule classifications for intrusion rules (**Policies > Intrusion > Rule Editor**).

- The access control rule display now alerts users automatically when access control rules will be omitted when the policy is applied (for example, when a rule references an empty object group).
- The **Security Event Analyst** and **Security Event Analyst (Read Only)** user roles are now **Security Analyst** and **Security Analyst (Read Only)**, respectively. Their functions and privileges remain the same.
- The system now decodes ERSPAN type 2 and ERSPAN type 3 traffic.
- You can now write correlation rules to respond to network-based malware events based on several new criteria.
- The intrusion event widget now shows **Total Events** by default. In previous versions, it showed **Average Events Per Second** by default. You can modify the widget to show **Average Events Per Second** by editing the widget's preferences.
- Sourcefire now provides default port objects for well-known ports.
- Files now have the disposition `Unavailable` when the Defense Center was unable to perform a malware cloud lookup.
- The host network map now displays all hosts with known MAC addresses or IP addresses.
- You can now filter by **File Name**, **File Type**, **File Type Category**, **File Disposition**, **File SHA256**, and **Malware Threat Name** in the Context Explorer. You can no longer filter by **URL**, **URL category**, or **URL reputation**.
- The health monitor now examines the performance of the RAID controller and the hard disk and triggers a health alert if either are in danger of failing.
- You can now configure browser session timeouts in the user interface settings of your system policy (**System > Local > System Policy**). Note that you cannot configure unlimited sessions for users with the Administrator role.
- The default NAT timeout value is now 3600 seconds (1 hour).
- You can now enter ranges when creating VLAN tag objects (**Objects > Object Management > VLAN Tag**).
- Sourcefire updated the range of values permitted when configuring the maximum transmission unit (MTU) of an interface.

The following list describes changes to the user interface:

- The **Parent File Name** and **Parent File SHA-256** columns in the Applications introducing Malware workflow were renamed **Application File Name** and **Application File SHA-256**, respectively. This does not affect any saved items (such as searches and custom workflows) that include these columns.
- The **Confidence** column was removed from the discovery events table and confidence data is no longer displayed in the service detail view.
- In the connection events table, the **Initiator User** column was moved to the immediate right of the **Initiator Country** column.
- On the **Policies** tab, the **Files** menu item was moved to the immediate right of the **Intrusion** menu item.

- The access control rule editor now shows the status of the intrusion policy, file inspection, and logging for the policy where you are editing a rule.
- The Rule Update Import Log now contains a **Default Action** information column.
- The access control policies page now provides additional information about what causes a policy to be listed as out-of-date.
- The **Client** and **Web Application** columns were added to the file and malware event tables, representing host software (**Client**) and content or requested URL for HTTP traffic (**Web Application**) associated with the malware event.
- You can now configure the remote management port from the **Shared Settings** section of the network settings page (**System > Local > Configuration > Network**).
- The intrusion event packet view now displays the revision of the intrusion rule that matched the packet in the following format, `GID:SID:Rev.`

Updates to Sourcefire Documentation

In Version 5.2, 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 3D System eStreamer Integration Guide*
- *Sourcefire 3D System eStreamer API Guide*
- *Sourcefire 3D System Database Access Guide*
- *Sourcefire 3D500/1000/2000 Quick Start Guide*
- *Sourcefire DC750 Quick Start Guide*
- *Sourcefire DC1500 Quick Start Guide*
- *Sourcefire DC3500 Quick Start Guide*
- *Sourcefire 7000 Series Devices Quick Start Guide*
- *Sourcefire 8000 Series Devices Quick Start Guide*

In addition, the *Sourcefire 3D System User Agent Configuration Guide* was updated for Version 2.1 of the user agent, which was released with Version 5.2.

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 5.2, 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.

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 upgrades. 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, 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 and routing. 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, and NAT are **not** performed during the update process.

Network Traffic Interruption

DEPLOYMENT	NETWORK TRAFFIC INTERRUPTED?
Inline with failopen (**Failopen** 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 failopen option is referred to as configurable bypass in releases after Version 5.1.1.4. It 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, 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 5.2 of the Defense Center to manage Version 5.2 devices. Defense Centers running Version 5.2 can manage devices running Version 5.1. or greater.

Web Browser Compatibility

Version 5.2 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
Firefox 19, 20, and 21	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 8, 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

The following sections help you prepare for and install the Version 5.2 update:

- Planning the Update on page 14
- Updating a Defense Center on page 18

- Updating Managed Devices on page 20
- Using the Shell to Perform the Update on page 22

TIP! You can update Series 3 and virtual devices running at least Version 5.1.1.1 of the Sourcefire 3D System to Version 5.2. To update an appliance running Version 4.10.x, including Series 3 devices, you must restore your appliance. For more information, see the *Sourcefire 3D System Installation Guide*.

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.

WARNING! If your system contains saved searches that reference inactive custom tables, the update may fail. Resolve all broken references in your saved searches before beginning the update.

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 11. To ensure a smooth update process, you must also read the following sections.

Sourcefire 3D System Version Requirements

To update to Version 5.2, an appliance must be running at least Version 5.1.1.1.

A Defense Center must be running at least Version 5.2 to update its managed devices to Version 5.2.

The closer your appliances' current version to the release version (Version 5.2), the less time the update takes.

WARNING! If you plan to restore 3D7110 or 3D7120 managed devices to Version 5.1.1 before updating, you must use an ISO file with build 334 or later. Older versions may cause problems with traffic processing.

Operating System Requirements

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

- VMware ESX/ESXi 4.1
- VMware vSphere Hypervisor 5.0
- VMware vSphere Hypervisor 5.1

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

Time and Disk Space Requirements

The following table provides disk space and time guidelines for the Version 5.2 update. Note that when you update a managed device with the Defense Center, the Defense Center requires additional disk space on its `/Volume` partition.

Time and Disk Space Requirements

Appliance	Space on /	Space on /Volume	Space on /Volume on Manager	Time
DC750, DC1500, and DC3500	220 KB	6.5 GB	n/a	40-60 minutes
physical managed devices, stacked or unstacked	100 KB	3 GB	511 MB	45-65 minutes
virtual Defense Centers	220 KB	6.5 GB	n/a	hardware dependent
virtual managed devices	200 KB	3.9 GB	505 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*.

IMPORTANT! Sourcefire does not support updating or reimaging appliances with more than one hard drive. You must remove additional hard drives before beginning the update.

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.

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 upgrade *after* all of the secondary devices, the stack resumes normal operation when the update completes on the primary device.

After the Installation

After you perform the update on either the Defense Center or managed devices, you **must** reapply device configuration and access control policies. 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
- updating your intrusion rules and vulnerability database (VDB), if necessary

TIP! Version 5.2 adds network discovery support for IPv6 addresses. When you upgrade to Version 5.2, however, the system does not automatically add IPv6 addresses to your discovery rules. To perform discovery on IPv6 traffic, update the rules in your network discovery policy to add IPv6 ranges to the networks to monitor and reapply the policy. To perform network discovery on all IPv6 traffic, add `::/0` as a monitored network.

IMPORTANT! Upon completing the update, install VDB build 156 or later to your Defense Center and reapply your access control policies.

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 5.2 update, Defense Centers reboot.

WARNING! You can update Series 3 and virtual devices running at least Version 5.1.1.1 of the Sourcefire 3D system to Version 5.2. To update an appliance running Version 4.10.x of the Sourcefire 3D System, you must restore your appliance. Note that this will result in a loss of all events and configuration data stored on your appliances. For more information about restoring, see the *Sourcefire 3D System Installation Guide*.

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 5.2 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 11 and Planning the Update on page 14.

2. Download the update from the Sourcefire Support Site:
   `Sourcefire_3D_Defense_Center_S3_Upgrade-5.2.0-838.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 5.2.0. 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*.

    IMPORTANT! For the update to Version 5.2, Sourcefire recommends installing a VDB build 156 or later.

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*.

Updating Managed Devices

After you update your Defense Centers to Version 5.2, 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 5.2 update, all devices reboot. Managed devices do **not** perform traffic inspection, switching, routing, or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow

and Inspection During the Update on page 11.

WARNING! Appliances running Version 4.10.x of the Sourcefire 3D System **cannot** be updated directly to Version 5.2. To update, you must reimage your appliances. Note that this will result in a loss of all events and configuration data stored on your appliances. For more information about reimaging, see the *Sourcefire 3D System Installation Guide*.

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 11 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 18.

3. Download the update from the Sourcefire Support Site:

   - for physical managed devices:

     `Sourcefire_3D_Device_S3_Upgrade-5.2.0-838.sh`

   - for virtual managed devices:

     `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.2.0-838.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 5.2.0.

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 your deployment includes RADIUS-based external user authentication, you **must** use the Defense Center to reapply the system policy to your devices.

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 5.2 update, all appliances reboot. Managed devices do **not** perform traffic inspection, switching, routing, or related functions during the

update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update on page 11.

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 11 and Planning the Update on page 14.

2. Download the appropriate update from the Sourcefire Support Site:
   - for Defense Centers, including virtual Defense Centers: `Sourcefire_3D_Defense_Center_S3_Upgrade-5.2.0-838.sh`
   - for physical managed devices: `Sourcefire_3D_Device_S3_Upgrade-5.2.0-838.sh`
   - for virtual managed devices: `Sourcefire_3D_Device_Virtual64_VMware_Upgrade-5.2.0-838.sh`

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

3. Using SSH, log into the appliance using an account with Administrator privileges. For virtual appliances, log in using the virtual console in the VMware vSphere Client.

4. At the prompt, access root privileges on the appliance:
   - On a Defense Center, type `sudo su -` and provide the password again.
   - On a managed device, type `expert` to display the shell prompt. Then, type `sudo su -` and provide the password again.

   The root prompt appears.

5. Using SCP, transfer the update to the `/var/sf/updates` directory on the appliance.

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

   `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. 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 18
   - Updating Managed Devices on page 20

Issues Resolved in Version 5.2

The following issues are resolved in Version 5.2:

- The command line interface (CLI) command `show traffic-statistics` now displays statistics for virtual as well as physical interfaces. (102347)
- Resolved an issue where clicking the evaluate icon to evaluate an application detector with a packet capture prevented you from activating the detector. (102464)
- Added, modified, and removed numerous preprocessor rules. (102633, 104588, 111941, 113970, 118178, 118500, 118553, 122038)
- Resolved an issue where the intrusion event views incorrectly displayed XFF data. (102655, 110873, 113369)
- Improved the use of colors throughout the user interface. (104562, 112517)
- Report text now supports the ASCII code 8217 quotation mark. (105857)
- When navigating from a Custom Analysis dashboard widget to an event viewer page, a message now appears to clarify any potential event count differences between the two pages. (106867)
- Resolved an issue where, in some cases, the system generated errors on packets when an interface returned to a routed configuration after being temporarily configured as a switched interface. (106986)
- Improved the system's ability to identify intrusion policy validation errors. (107105)
- Resolved an issue where, in some cases, intrusion policies did not save when inline normalization allowed TCP options that contained both commas and blank spaces. (108289)
- Status icons on the Device Management page (**Devices > Device Management**) now indicate whether a device in a clustered configuration is in a degraded state. (108908)
- Improved the performance of the `content` keyword in intrusion rules. (109059, 118112)
- Resolved an issue where custom HTTP response pages for Interactive Block access control rules did not appear consistently or allow users to bypass successfully. (109186, 110109, 110110, 111661)
- Resolved an issue where threshold values of 86400 seconds (24 hours) for the packet view in the event viewer could not be saved successfully. (109187)
- Resolved an issue where, in some cases, the system incorrectly identified a correlation policy as active. (110111)
- Added a new troubleshooting option to the Performance Statistics configuration. (110470)

- Resolved an issue where intrusion rules did not generate events if they defined SIP methods in the `sip_method` keyword that were not already defined in the SIP preprocessor. (110532)
- Resolved an issue where two passive interfaces on appliances with identical access control policy and rule settings, but in different security zones, could produce different connection events from the same traffic. (110575)
- Resolved an issue where, after completing an access control or intrusion policy apply, the system generated extraneous process status health alerts. (110578, 120317)
- Resolved an issue where, in some cases, the primary device in a stack appeared perpetually active in the device management portion of the user interface. (110702)
- Resolved an issue where, in some cases, the system experienced issues with task status reporting during access control policy apply on a Defense Center managing clustered devices. (110704)
- Resolved an issue where reports generated graphs and charts without labels for portscan events. (110828)
- The audit log (**System > Monitoring > Audit**) now provides details about settings that changed during edits to the system policy. (110860)
- Resolved an issue where managed devices continued to store user data purged from their managing Defense Center. (111234)
- Resolved a display issue on the intrusion policy comparison page. (111350)
- Improved accuracy of intrusion policy comparison reports. (111396)
- Resolved an issue where, in some cases, two interfaces viewing the same network traffic experienced issues with application detection. (111554)
- Improved performance of the TCP stream preprocessor. (111871, 120171, 122391)
- Resolved an issue where negated predefined search objects lost the negation after the search was saved. (111912)
- Added an alert to notify users that accented characters may not display properly in custom login banners. (111957)
- Improved performance of custom workflows based on the hosts table. (112204)
- Optimized database queries to improve performance of the connection events table. (112506, 117165)
- Resolved an issue where, in some cases, intrusion events generated from reassembled traffic did not contain packet data. (112519)
- Resolved an issue where physical appliances experienced system issues after running continuously for a minimum of 208 days. (112556, 112765, 112766)

- Improved accuracy of operating system identification in the network map. (112843)
- Resolved an issue where, in some cases, the host profile showed inactive ports and services as pending. (113213)
- Resolved an issue where, in rare cases, the system omitted the first line of text from an uploaded list of security intelligence objects encoded in UTF-8. (113578)
- Resolved an issue where the eStreamer service returned events from before the specified start time if the event request did not contain the `FLAG_DETAIL_REQUEST` flag. (113599)
- Resolved an issue where, in some cases, the system incorrectly sorted the **Status** column of custom report templates created based on the health events table. (113618)
- Improved connection tracking to identify a separate ICMP session for each ICMP type in a packet. (113663)
- If you use a Serial Over LAN (SOL) connection to restore a 3D7010, 3D7020, or 3D7030 managed device to factory settings, and a Lights-Out Management (LOM) user is logged in when you begin the restore, that LOM user is now correctly disconnected and deleted. (113706, 113824)
- Resolved an issue where, in some cases, the system failed to email reports. (114256)
- The system now allows users with either a FireSIGHT license or a RNA Host license to enable FireSIGHT recommendations. The system can alert users if they attempt to enable FireSIGHT recommendations without available hosts. (114430)
- Resolved an issue where, in some cases, the system omitted NetBIOS information from the host profile. (115291)
- Resolved an issue where the system generated health alerts about nonexistent issues with discovery event generation. (115308)
- Resolved an issue where uploading a text file to create a new Security Intelligence list caused the system to identify IP addresses as invalid. (115489)
- Resolved an issue where, in some cases, setting thresholds or suppressions from the intrusion event table caused system errors. (115950)
- Improved the performance of the context menu accessed from the intrusion event views. (116165)
- Resolved an issue where, in passive deployments, the system did not perform network discovery on traffic for networks where you constrained the associated discovery rule by security zone. (116462)
- Resolved an issue where the system restarted during intrusion policy apply due to detected SMTP preprocessor changes, even if there were no changes to the SMTP preprocessor. (116830)

- Resolved an issue where the system incorrectly identified versions of Internet Explorer while the browser operated in compatibility mode. (117530)
- Resolved an issue that prevented you from suppressing a GID 134 rule. (117593)
- Resolved an issue where drilling down to the operating systems table view from the **Network Information** graph in the Context Explorer improperly constrained the data. (117996)
- Improved the performance of the HTTP inspect preprocessor. (118025, 118713, 119009)
- Improved the performance of incident generation and reporting in intrusion policies. (118096, 118121)
- Improved the performance of line charts in dashboard widgets. (118173)
- Resolved an issue where, in rare cases, end-of-connection events were not logged. (118688)
- Resolved an issue where the system truncated text in long syslog messages. (118816)
- Resolved an issue where some TCP connections detected by virtual devices were not logged to the Defense Center. (118827)
- Resolved an issue with the formatting of text files sent with email alerts by the Defense Center. (119267)
- Improved the IP defragmentation preprocessor to avoid a possible evasion using packet fragments. (119531)
- Resolved an issue where TCP connections that were reset took a long time to generate connection events. (119557)
- Resolve an issue where the system experienced issues with packet reassembly when the port configuration in an applied intrusion policy differed from the base intrusion policy. (119714)
- Improved functionality of access control rules with user conditions. (119962)
- Resolved an issue where intrusion rules using the `file_data` keyword did not drop traffic if **Drop when Inline** was disabled in the base intrusion policy. (120156)
- Resolved an issue where the TCP stream preprocessor did not correctly identify the server in HTTP traffic when detected midstream. (120170)
- Improved Teredo traffic decoding. (120292)
- Resolved an issue where, in some cases, intrusion events generated during a network discovery policy apply were associated with incorrect security zones. (120316)
- Resolved an issue with high availability configurations where you could not change the secondary Defense Center to the primary role if the original primary Defense Center was offline. (120327)

- Improved logging of Security Intelligence decisions to the syslog. (120564, 120565, 121050)
- Resolved an issue where, in some cases, URL filtering database updates were not synchronized from the Defense Center to managed devices. (120572)
- Resolved an issue where access control policy apply failed when the default action was **Block All Traffic** and the HOME_NET variable was any. Because this combination is invalid, the system now warns you if you attempt to configure it. (120578)
- Resolved an issue where fragmented IP traffic that would normally match a **Trust** access control rule and pass without further inspection was instead evaluated by the intrusion policy associated with the default action. (120734)
- Resolved an issue where, in some cases, changing the dashboard widget time range caused the widget to display incorrect event statistics. (121009)
- Resolved an issue where the system did not log correlation rules that referenced user logins. (121129)
- Resolved an issue where the system did not detect files transferred in HTTP POST requests. (121204)
- Resolved an issue where, in some cases, intrusion email alerts did not associate events with the correct managed device. (121278)
- Resolved an issue where, in rare cases, very large troubleshooting files did not download successfully. (121471)
- Resolved an issue where, in some cases, adding an interface to a security zone caused access control policy apply to fail. (121511)
- Resolved an issue where, in some cases, eStreamer reported incorrect data for intrusion event record type 207. (121555)
- When viewing packet information for intrusion events, the timestamp now reports the correct time in all cases. (121685)
- Resolved an issue where, in some cases, the Intrusion Events by Impact report template preset reported incorrect impact flag data. (121864)
- When you view intrusion events with a search constraint of **Source IP**, this constraint now appropriately changes to **Sending IP** if you navigate to the Malware or Files tabs. (122034)
- Resolved an issue where, in rare cases, devices failed to process packets and log intrusion events. (122130)
- Improved performance of the Context Explorer when handling large datasets. (122276)
- Resolved an issue where, in some cases, eStreamer logged packets before their associated event records. (122365)
- Resolved an issue where, in some cases, the system did not enable traffic profiles with inactive periods. (122440)

- Resolved an issue in network discovery policies where changes to user protocol detection configuration did not take effect. (122763)
- Improved the system's reporting of error messages generated by the eStreamer client. (122859)
- Resolved an issue with the eStreamer client where SHA-256 values were incorrectly reported by the Defense Center. (122869)
- Resolved an issue where users were not prompted to enable the TCP stream preprocessor when saving an intrusion policy with the rate-based attack prevention preprocessor enabled and the TCP stream preprocessor disabled. (122905)
- Resolved an issue where, in rare cases, intrusion rules that triggered on pruned sessions applied the rule action to current sessions. (122990)

Known Issues

The following known issues were reported in Version 5.2:

- You must use the Defense Center's web interface to unregister a managed device. If you unregister a device from its managing Defense Center using either the device's web interface or, for Series 3 and virtual devices, its command line interface (CLI), it is not removed. (112659, 112709)
- If health alerts generated by the advanced malware protection module show errors, you should check your Defense Center's connection to the Sourcefire cloud. To troubleshoot, ensure the connection from the Defense Center to the Sourcefire cloud (`54.243.248.19` and `54.243.248.162`) on port 32137 is working properly. (112708)
- If multiple files are attached to a single email, the system may incorrectly identify files after the first. (114523)
- If you attempt to create multiple static NAT rules with the same original values, the system may experience issues with traffic mapping. (116148)
- In some cases, the Defense Center may show a cluster in a degraded state when it has already recovered, generating extraneous system alerts. (118122)
- When Lights-Out Management is enabled, the system also enables a web server in the background. The web server does not drain system resources and has no known exploits. (119456)

- Sourcefire documentation currently does not reflect the following:
  - On a Series 3 device, TCP connections matching a Trust access control rule on the first packet generate different events depending on the presence of a Monitor rule. If an active Monitor rule is present, the system generates both a beginning and end-of-connection event, as expected. If no monitor rule is active, the system does not generate a beginning-of-connection event. (121060)
  - 3D2100/2500/3500/4500 managed devices do not have functional serial ports. (123396)
- The current version of Snort running on a Defense Center is not displayed on the About page (**Help > About**). (121228, 123403)
- Do not name security zone objects using the pound sign (#); it may cause errors during device reconfiguration. (121514)
- In some cases, reports may not generate if you uploaded a logo file with a particularly long filename or high resolution to the report template. (121878)
- If you attempt to break a stack that was registered using DNS during a period when DNS is disabled, you will experience system issues. Do **not** attempt this. (122709)
- In some cases, intrusion event counts in the dashboard may not match the counts in the event viewer. (122743, 123040)
- When creating stacks of devices from different device groups, the secondary device in the stack both retains membership in its original group and becomes associated with the stack's primary group. The user interface does not alert the user to this behavior. (122802)
- In some cases, your network discovery policy may not function as expected if you apply two or more network discovery rules that apply to the same zones and networks but are configured to discover different hosts, users, and applications. (122853)
- During an update, a device in a clustered, inline deployment may fail over incorrectly. The issue exists only for the duration of the update and will not disrupt the update process. (123239)
- In some cases, intrusion events may display incorrect VLAN ID information. (123696)
- An access control policy apply may not succeed on a cluster with both state sharing and **Inspect Local Router Traffic** enabled. As a workaround, disable the Inspect Local Router Traffic setting (**Devices > Device Management**). (123710)
- If the managing Defense Center is unavailable, you may be unable to break clusters or stacks from the command line interface (CLI) on the primary device. (123932)
- Hosts without IP addresses may count towards your FireSIGHT host limit, prematurely triggering a health status alert. (124091)

- In rare cases, the system may require up to 3 hours to complete an update to Version 5.2 of the Sourcefire 3D System on a 3D7110 or 3D7120 managed device. Do **not** interrupt the update; allow the post-update reboot to finish completely. (124148)
- If a device group contains an inactive managed device, you may be unable to edit the device group. (124286)
- You can not use IPv6 addresses to configure connections to Sourcefire User Agents (**Policies > Users**). As a workaround, configure the connection using the associated IPv4 addresses instead. (124377)
- Upon completing the update to Version 5.2, Snort will not load if your intrusion policy contains invalid local rules. As a workaround, resolve the intrusion rule syntax errors in all relevant intrusion policies and manually reapply your access control policy. (124935)
- If you finish updating your Defense Center to Version 5.2 to manage devices running Version 5.1.x and you reapply individual intrusion policies instead of your complete access control policies, events will not log on your Defense Center. To resolve this issue, either update your managed devices to Version 5.2 or contact Support for further assistance. (125352)
- Sourcefire documentation does not reflect that when you reimage a device from Version 4.10.x to Version 5.2, if the device has interfaces configured to fail open they will revert to a non-bypass (fail closed) configuration at first boot and remain closed until you configure bypass mode for them. (125957)
- After updating an appliance running Version 5.1.x of the Sourcefire 3D System and Version 2.0.3 of the Sourcefire User Agent to Version 5.2 of the Sourcefire 3D System, the system may generate an extraneous health alert. (127082, 127265)
- If you create a custom analysis dashboard widget based on a saved connection event search that uses data in fields without an asterisk (*), the widget displays incorrect data. Only the fields that constrain connection summaries can constrain custom analysis dashboard widgets based on connection events. (127324, 127327)
- If you apply a VPN deployment on a stack, cluster, or clustered stack and then unregister the stack, cluster, or clustered stack from its managing Defense Center, the VPN deployment remains active on the stack, cluster, or clustered stack when you register the appliances to another Defense Center. Additionally, you cannot manage the VPN deployment from the new Defense Center. As a workaround, remove the VPN deployment from the stack, cluster, or clustered stack before unregistering it from the Defense Center. (128816, 130728)
- In some cases, the system experiences issues with user account management if devices running Version 5.1.1.x are managed by a Defense Center running Version 5.2. As a workaround, update your managed devices to Version 5.2. (130024)

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.

Thank you for using Sourcefire products.

Legal Notices

WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY CISCO-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION. CISCO-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND CISCO DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL CISCO BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO CISCO-CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF CISCO IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU..