Sourcefire 3D System Release Notes

Version 5.3.0.3

Original Publication: April 21, 2014

These release notes are valid for Version 5.3.0.3 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 and uninstallation instructions for the following appliances:

- Series 2 and Series 3 Defense Centers (the DC500, DC750, DC1000, DC1500, DC3000, and the DC3500)
- Series 2 and Series 3 managed devices (the 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500, 3D7010, 3D7020, 3D7030, 3D7110, 3D7115, 3D7120, 3D7125, 3D8120, 3D8130, 3D8140, 3D8250, 3D8260, 3D8270, 3D8290, 3D8350, 3D8360, 3D8370, 3D8390, 3D9900, AMP7150, and the AMP8150)
- 64-bit Sourcefire Software for X-Series
- 64-bit virtual Defense Centers and managed devices
- Cisco ASA with FirePOWER Services (the ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, and the ASA5585-X-SSP-60)

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.

To update appliances running at least Version 5.3 of the Sourcefire 3D System to Version 5.3.0.3, see the procedures outlined in Updating Your Appliances on page 5.

For more information, see the following sections:

- Updates to Sourcefire Documentation on page 2
- Before You Begin: Important Update and Compatibility Notes on page 2
- Updating Your Appliances on page 5
- Uninstalling the Update on page 16
- Issues Resolved in Version 5.3.0.3 on page 23
- Known Issues on page 32
- Features Introduced in Previous Versions on page 39
- For Assistance on page 46

Updates to Sourcefire Documentation

In Version 5.3.0.3, 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 Online Help (SEU)*
- *Sourcefire 3D System Installation Guide*
- *Sourcefire 3D System Virtual Installation Guide*
- *Sourcefire 3D System eStreamer API Guide*

Before You Begin: Important Update and Compatibility Notes

Before you begin the update process for Version 5.3.0.3, 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.

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 3
- Traffic Flow and Inspection During the Update on page 3
- Product Compatibility on page 4

Configuration and Event Backup Guidelines

Before you begin the update, Sourcefire **strongly** recommends that you back up current event and configuration data to an external location. This data is **not** backed up as part of the update process.

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 locally stored backups from previous updates. To retain archived backups, store the backups externally.

Traffic Flow and Inspection During the Update

The update process (and any uninstallation of the update) reboots 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, Sourcefire Software for X-Series, 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.

Product Compatibility

You must use at least Version 5.3 of the Defense Center to manage devices running Version 5.3.0.3.

Defense Centers running Version 5.3.0.3 can manage physical devices and virtual devices running Version 5.2.0.4 or greater and Sourcefire Software for X-Series running Version 5.3 or greater.

Web Browser Compatibility

Version 5.3.0.3 of the web interface for the Sourcefire 3D System has been tested on the browsers listed in the following table.

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

Web Browser Compatibility

Browser	Required Enabled Options and Settings
Chrome 33	JavaScript, cookies
Firefox 30	JavaScript, cookies, Secure Sockets Layer (SSL) v3
Microsoft Internet Explorer 9, 10, and 11	JavaScript, cookies, Secure Sockets Layer (SSL) v3, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically**

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.

Updating Your Appliances

To update appliances running at least Version 5.3 of the Sourcefire 3D System to Version 5.3.0.3, see the procedures outlined below. The following sections help you to prepare for and install the Version 5.3.0.3 update:

- Planning the Update on page 5
- Updating a Defense Center on page 9
- Updating Managed Devices and Sourcefire Software for X-Series on page 12
- Using the Shell to Perform the Update on page 15

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.

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

Sourcefire 3D System Version Requirements

To update to Version 5.3.0.3, an appliance must be running at least Version 5.3. 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 5.3.0.2 to update its managed devices to Version 5.3.0.3.

The closer your appliances' current version to the release version (Version 5.3.0.3), 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 the X-Series platform 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 5.3.0.3 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	5 MB	2913 MB	n/a	87 minutes
Series 2 managed devices	1 MB	2606 MB	557 MB	173 minutes
Series 3 Defense Centers	53 MB	2999 MB	n/a	69 minutes
Series 3 managed devices	80 MB	4180 MB	847 MB	63 minutes
3D9900 managed devices	3 MB	2806 MB	577 MB	172 minutes
Sourcefire Software for X-Series	461 MB	1 MB on /mnt/aplocal disk	1240 MB	19 minutes
virtual Defense Centers	53 MB	2999 MB	n/a	hardware dependent
virtual managed devices	486 MB	67 MB	1917 MB	hardware dependent

Configuration and Event Backup Guidelines

Before you begin the update, Sourcefire **strongly** recommends that you back up current event and configuration data to an external location. This data is **not** backed up as part of the update process.

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.

Order of Installation

Update your Defense Centers before updating the devices they manage.

Installing the Update on Paired Defense Centers

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

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

Installing the Update on Clustered Devices

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

Installing the Update on Stacked Devices

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

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

Installing the Update on X-Series Devices

To update to Version 5.3.0.3, Sourcefire Software for X-Series must be running at least Version 5.3.

You **cannot** update Sourcefire Software for X-Series running Version 4.10.x to Version 5.3.0.3. Instead, you must uninstall the previous version and then install Version 5.3 before updating to Version 5.3.0.3. For detailed instructions, see the *Sourcefire Software for X-Series Installation and Configuration Guide*.

Updating the Sourcefire Software for X-Series reloads the affected VAPs. If your Sourcefire Software for X-Series is deployed inline and you are using multi-member VAP groups, Sourcefire recommends that you update the VAPs

one at a time. This allows the other VAPs in the group to inspect network traffic while the VAP that is being updated reloads. If you are using single-VAP VAP groups in an inline deployment, reloading the VAP causes an interruption in network traffic. Make sure you plan the update for a maintenance window or other time when it will have the least impact on your deployment.

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, if necessary
- updating your vulnerability database (VDB) to at least version 220
- making any required configuration changes based on the information in Updates to Sourcefire Documentation 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 5.3.0.3 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.

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 2 and Planning the Update on page 5.

2. Download the update from the Sourcefire Support Site:
   - for Series 2 Defense Centers:
     `Sourcefire_3D_Defense_Center_Patch-5.3.0.3-56.sh`
   - for Series 3 and virtual Defense Centers:
     `Sourcefire_3D_Defense_Center_S3_Patch-5.3.0.3-56.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 monitor the update's progress in the task queue (**System > Monitoring > Task Status**).

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

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. Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.0.3. Also note the versions of the rule update and VDB on the Defense Center; you will need this information later.
12. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
13. 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*.
14. 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*.
15. 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.

16. 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. If this side effect is not ideal for your network setup and connectivity is more important than inspection unchecking this box will disable inspection temporarily during policy apply and ensure that no packets are dropped during the procedure. After policy apply is successful inspection will resume as normal. For more information, see the *Sourcefire 3D System User Guide*.

Updating Managed Devices and Sourcefire Software for X-Series

After you update your Defense Centers to Version 5.3.0.3, use them to update the devices they manage.

A Defense Center must be running at least Version 5.3.0.2 to update its managed devices to 5.3.0.3. Because they do not have a web interface, you must use the Defense Center to update Sourcefire Software for X-Series and virtual managed devices.

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 5.3.0.3 update, all devices reboot; Sourcefire Software for X-Series VAP groups reload. 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 3.

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.

TIP! If your Sourcefire Software for X-Series is deployed inline and you are using multi-member VAP groups, Sourcefire recommends that you update the VAPs one at a time. This allows the other VAPs in the group to inspect network traffic while the VAP that is being updated reloads. If you are using single-VAP VAP groups in an inline deployment, reloading the VAP causes an interruption in network traffic. Make sure you plan the update for a maintenance window or other time when it will have the least impact on your deployment.

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 2 and Planning the Update on page 5.

2. Update the Sourcefire software on the devices' managing Defense Center; see Updating a Defense Center on page 9.

3. Download the update from the Sourcefire Support Site:
   - for Series 2 managed devices:
     `Sourcefire_3D_Device_Patch-5.3.0.3-56.sh`
   - for Series 3 managed devices:
     `Sourcefire_3D_Device_S3_Patch-5.3.0.3-56.sh`

- for 3D9900 managed devices:
  `Sourcefire_3D_Device_x900_Patch-5.3.0.3-56.sh`
- for virtual managed devices:
  `Sourcefire_3D_Device_Virtual64_VMware_Patch-5.3.0.3-56.sh`
- for Sourcefire Software for X-Series:
  `Sourcefire_3D_XOS_Device_Patch-5.3.0.3-56.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.

   For Sourcefire Software for X-Series deployed inline, traffic is interrupted while VAPs reload.

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 5.3.0.3.

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*.

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.

IMPORTANT! Do **not** use the shell to update a fresh, unconfigured (Version 5.3) installation of the Sourcefire 3D System. Before you update an appliance using the shell, make sure that you complete its initial setup using its web interface.

IMPORTANT! Do **not** use the shell to update Sourcefire Software for X-Series. Instead, use the managing Defense Center as described in Updating Managed Devices and Sourcefire Software for X-Series on page 12.

For the Version 5.3.0.3 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 3.

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 2 and Planning the Update on page 5.

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

   - for Series 2 Defense Centers:
     `Sourcefire_3D_Defense_Center_Patch-5.3.0.3-56.sh`
   - for Series 3 and virtual Defense Centers:
     `Sourcefire_3D_Defense_Center_S3_Patch-5.3.0.3-56.sh`
   - for Series 2 managed devices:
     `Sourcefire_3D_Device_Patch-5.3.0.3-56.sh`

- for Series 3 managed devices:
  `Sourcefire_3D_Device_S3_Patch-5.3.0.3-56.sh`
- for 3D9900 managed devices:
  `Sourcefire_3D_Device_9900_Patch-5.3.0.3-56.sh`
- for virtual managed devices:
  `Sourcefire_3D_Device_Virtual64_VMware_Patch-5.3.0.3-56.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 9
   - Updating Managed Devices and Sourcefire Software for X-Series on page 12

Uninstalling the Update

The following sections help you uninstall the Version 5.3.0.3 update from your appliances:

- Planning the Uninstallation on page 17
- Uninstalling the Update from a Managed Device on page 18
- Uninstalling the Update from a Virtual Managed Device on page 20
- Uninstalling the Update from Sourcefire Software for X-Series on page 20
- Uninstalling the Update from a Defense Center on page 21

Planning the Uninstallation

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

Uninstallation Method

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

For all physical appliances and virtual Defense Centers, uninstall the update using the local web interface. Because virtual managed devices and Sourcefire Software for X-Series do not have a web interface, you must use the bash shell to uninstall the update.

Order of Uninstallation

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

Uninstalling the Update from Clustered or Paired Appliances

Clustered devices and Defense Centers in high availability pairs must run the same version of the Sourcefire 3D System. Although the uninstallation process triggers an automatic failover, appliances in mismatched pairs or clusters do not share configuration information, nor do they install or uninstall updates as part of their synchronization. If you need to uninstall an update from redundant appliances, plan to perform the uninstallations in immediate succession.

To ensure continuity of operations, uninstall the update from clustered devices and paired Defense Centers one at a time. First, uninstall the update from the secondary appliance. Wait until the uninstallation process completes, then immediately uninstall the update from the primary appliance.

WARNING! If the uninstallation process on a clustered device or paired Defense Center fails, do **not** restart the uninstall or change configurations on its peer. Instead, contact Support.

Uninstalling the Update from Stacked Devices

All devices in a stack must run the same version of the Sourcefire 3D System. Uninstalling the update from any of the stacked devices causes the devices in that stack to enter a limited, mixed-version state.

To minimize impact on your deployment, Sourcefire recommends that you uninstall an update from stacked devices simultaneously. The stack resumes normal operation when the uninstallation completes on all devices in the stack.

Uninstalling the Update from Devices Deployed Inline

Managed devices do **not** perform traffic inspection, switching, routing, or related functions while the update is being uninstalled. Depending on how your devices are configured and deployed, the uninstallation process may also affect traffic flow and link state. For more information, see Traffic Flow and Inspection During the Update on page 3.

Uninstalling the Update from Sourcefire Software for X-Series

You must uninstall the update from each VAP group individually in order to fully uninstall the update from Sourcefire Software for X-Series. Uninstalling the Version 5.3.0.3 update of the Sourcefire 3D System reloads the affected VAP. If your Sourcefire Software for X-Series is deployed inline and you are using multi-member VAP groups, Sourcefire recommends that after you uninstall the update from a VAP, you allow that VAP to reload before you uninstall the update from additional VAPs.

This allows the other VAPs in the group to inspect network traffic while the affected VAP reloads. If you are using single-VAP VAP groups in an inline deployment, reloading the VAP causes an interruption in network traffic. Make sure you plan the uninstallation for a maintenance window or other time when it will have the least impact on your deployment.

After the Uninstallation

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

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

Uninstalling the Update from a Managed Device

The following procedure explains how to use the local web interface to uninstall the Version 5.3.0.3 update from managed devices. You **cannot** use a Defense Center to uninstall the update from a virtual managed device.

Uninstalling the Version 5.3.0.3 update results in a device running Version 5.3. For information on uninstalling a previous version, refer to the release notes for that version.

Uninstalling the Version 5.3.0.3 update reboots the device. 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 3.

To uninstall the update:

1. Read and understand Planning the Uninstallation on page 17.
2. On the managing Defense Center, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
3. On the managed device, view the task queue (**System > Monitoring > Task Status**) to make sure that there are no tasks in progress.

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

   The Product Updates tab appears.
5. Click the install icon next to the uninstaller that matches the update you want to remove, then confirm that you want to uninstall the update and reboot the device.

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

   WARNING! Do **not** use the web interface to perform any other tasks until the uninstallation has completed and the device reboots. Before the uninstallation completes, the web interface may become unavailable and the device may log you out. This is expected behavior; log in again to view the task queue. If the uninstallation is still running, do **not** use the web interface until the uninstallation has completed. If you encounter issues with the uninstallation (for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress for several minutes), do **not** restart the uninstallation. Instead, contact Support.
6. After the uninstallation finishes, clear your browser cache and force a reload of the browser. Otherwise, the user interface may exhibit unexpected behavior.
7. Log in to the device.
8. Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.
9. On the managing Defense Center, verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstalling the Update from a Virtual Managed Device

The following procedure explains how to uninstall the Version 5.3.0.3 update from virtual managed devices. You **cannot** use a Defense Center to uninstall the update from a managed device.

Uninstalling the Version 5.3.0.3 update results in a device running Version 5.3. For information on uninstalling a previous version, refer to the release notes for that version.

Uninstalling the Version 5.3.0.3 update reboots the device. Virtual managed devices do **not** perform traffic inspection or related functions during the update. Depending on how your devices are configured and deployed, the update process may also affect traffic flow. For more information, see Traffic Flow and Inspection During the Update on page 3.

To uninstall the update:

1. Read and understand Planning the Uninstallation on page 17.
2. Log into the device as `admin`, via SSH or through the virtual console.
3. At the CLI prompt, type `expert` to access the bash shell.
4. At the bash shell prompt, type `sudo su -`.
5. Type the `admin` password to continue the process with root privileges.
6. At the prompt, enter the following on a single line:

   ```
   install_update.pl /var/sf/updates/Sourcefire_3D_
   Device_Virtual64_VMware_Patch_Uninstaller-5.3.0.3-56.sh
   ```

   The uninstallation process begins.

   WARNING! If you encounter issues with the uninstallation, do **not** restart the uninstallation. Instead, contact Support.

7. After the uninstallation finishes, log into the managing Defense Center and select **Devices > Device Management**. Confirm that the device where you uninstalled the update has the correct software version: Version 5.3.
8. Verify that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Uninstalling the Update from Sourcefire Software for X-Series

The following procedure explains how to uninstall the Version 5.3.0.3 update from Sourcefire Software for X-Series. You cannot use a Defense Center to uninstall the update. You must complete the following procedure from each VAP group individually in order to fully uninstall the update from Sourcefire Software for X-Series.

Uninstalling the Version 5.3.0.3 update results in the Sourcefire Software for X-Series running Version 5.3.

To uninstall the update:

1. Read and understand Planning the Uninstallation on page 17.
2. Log into a VAP where you want to uninstall the update.

   For example, to log into the first VAP in the intrusion VAP group:

   ```
   CBS# unix su
   [root@machine admin]# rsh intrusion_1
   ```
3. At the prompt, run the following command to configure your session environment to run Sourcefire scripts:

   ```
   source /opt/sf/profile
   ```
4. At the prompt, type the following on a single line and press **Enter**:

   ```
   install_update.pl
   /var/sf/updates/Sourcefire_3D_XOS_Device_Patch_Uninstaller-
   5.3.0.3-56.sh
   ```

   The update is removed and the VAP reloads. If your Sourcefire Software for X-Series is deployed inline, traffic to that VAP is interrupted while the VAP reloads. Note, however, that if there are other VAPs in the VAP group, traffic is load balanced among the other VAPs.
5. On the managing Defense Center, select **Devices > Device Management** and confirm that the software version is listed correctly: Version 5.3.
6. Verify that the Sourcefire Software for X-Series is successfully communicating with the Defense Center.
7. Repeat steps 1 through 6 for each VAP in the VAP group.

Uninstalling the Update from a Defense Center

Use the following procedure to uninstall the Version 5.3.0.3 update from Defense Centers and virtual Defense Centers. Note that the uninstallation process reboots the Defense Center.

Uninstalling the Version 5.3.0.3 update results in a Defense Center running Version 5.3. For information on uninstalling a previous version, refer to the release notes for that version.

To uninstall the update:

1. Read and understand Planning the Uninstallation on page 17.
2. Make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

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

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

4. Select **System > Updates**.

   The Product Updates tab appears.

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

   The Install Update page appears.

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

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

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

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

8. Log in to the Defense Center.

9. Select **Help > About** and confirm that the software version is listed correctly: Version 5.3.

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

Issues Resolved in Version 5.3.0.3

Cisco recently changed caveat tracking systems and issues addressed in Version 5.3.0.2 and forward are tracked via Cisco Defect Tracking System (CDETS). To view bugs addressed in older versions, refer to the previous caveat tracking system.The following issues are resolved in Version 5.3.0.3:

- Security Issue Addressed an arbitrary injection vulnerability allowing unauthenticated, remote attackers to execute commands via Bash to address CVE-2014-6271 and CVE-2014-7169. (144862/CSCze95477, 144941/CSCze95479, 144948/CSCze96159)
- Resolved an issue where, if you edited any of the applied intrusion policies, the system marked all intrusion policies as out-of-date. (134066, 140135/CSCze91908)
- Improved responsiveness of link state propagation. (137773/CSCze90606)
- Resolved an issue where the documentation did not reflect that, if you registered a cluster, stack, or clustered stack of devices to a Defense Center, you had to manually reapply the device configuration. (141624/CSCze93129, 142412/CSCze92735)
- Resolved a rare issue where, when your system triggered an alert on the first data packet of a TCP session from a server, the alert failed to specify the egress interface. (141817/CSCze93047)
- Improved the stability of the SMB and DCE/RPC preprocessor. (142199/CSCze93232)
- Resolved an issue where, if you edited an access control policy and policy apply failed, the policy changes from the attempted policy apply were not restored to the previously applied policy. (142908/CSCze93586)
- Resolved an issue where, if a user named `admin` is not established during the first initialization of the baseboard management controller of a managed device, the system did not let you change the default password and you could not log into the device. (143053/CSCze94371)
- Improved and accelerated policy apply. (143318/CSCze93668)
- Resolved an issue where, if the system generated intrusion events matching a rule with a GID other than `1` or `3`, alerts sent to your syslog server contained incorrect messages. (143465/CSCze95013)
- Resolved an issue where the host profile incorrectly displayed multiple IP addresses for a single managed device. (143470/CSCze94629)
- Resolved an issue where, if you configured a 3D71xx or 3D70xx managed device with passive interfaces, connection events generated on those interfaces may have reported incorrect egress zone information. (143532/CSCze94988)

- You can now reapply device configuration after editing the list of security zones of a cluster, stack or clustered stack of devices from the Object Management page by selecting the green apply icon for device changes on the Device Management page (**Devices > Device Management**). (143535/CSCze94906)
- Resolved an issue where, if you disabled any access control rules containing either an intrusion policy or a variable set different from any enabled rules and the access control policy's default action, policy apply failed and the system experienced issues. (143809/CSCze94944)
- Improved diskmanager cleanup during report generation. (143900/CSCze94192)
- Resolved an issue where, in some cases, if you applied an access control policy to your Defense Center, policy apply failed and caused system issues. (143974/CSCze95108)
- Improved reliability of URL reputation and device detection capabilities. (144169/CSCze94611)
- Resolved an issue where, in some cases, if you created an intrusion policy with the FTP preprocessor enabled, the system incorrectly identified traffic matching rules referencing the FTP preprocessor as FTP files even if they were not. (144315/CSCze94630)

Issues Resolved in Previous Updates

You can track defects resolved in this release using the Cisco Defect Tracking System (CDETS). To view defects addressed in older versions, refer to the legacy caveat tracking system. Because you can update your appliances from Version 5.3 to Version 5.3.0.3, this update also includes the changes from Version 5.3. Previously resolved issues are listed by version.

Version 5.3.0.2

- Security Issue Addressed multiple cross-site scripting (XSS) vulnerabilities.
- Security Issue Addressed multiple cross-site request forgery (CSRF) vulnerabilities.
- Security Issue Addressed multiple injection vulnerabilities, including HTML and command line injections.
- Security Issue Addressed multiple vulnerability issues in cURL, Linux, MySQL, strongSwan, and Wireshark, including those described in CVE-2013-1944, CVE-2013-2237, CVE-2013-3783, CVE-2013-2338, CVE-2013-5718, CVE-2013-5719, CVE-2013-5720, CVE-2013-5721, and CVE-2013-5722.
- Resolved an issue where the system delayed the generation of end-of-connection events for packets transmitted via a protocol other than TCP or UDP. (131526/CSCze89194)

- Resolved an issue where, in some cases, the intrusion event packet view displayed a rule message that did not match the rule that generated the event. (138011/CSCze90972)
- Resolved an issue where you could not import an intrusion rule that referenced a custom variable. (138077/CSCze90689)
- Resolved an issue where, if the system dropped the connection between the Defense Center and its managed device while completing a backup, the managed device failed to send the finished backup files to the Defense Center, and the Task Status page (**System > Monitoring > Task Status**) reported that the backup was still in progress. (138102/CSCze90708)
- Resolved an issue where connection events logged to an external syslog or SNMP trap server had incorrect URL Reputation values. (138504/CSCze91066, 139466/CSCze91510)
- Resolved an issue where, in rare cases, the system displayed incorrect, extremely high packet counts in the dashboard and event views for Series 3 managed devices. (138608/CSCze91081)
- Improved the stability of clustered state sharing on 3D8250 and 3D8350 managed devices. (139141/CSCze91387)
- Resolved an issue where, if you enabled telnet on a Cisco IOS Null Route remediation module and configured the username for the Cisco IOS instance to enable by default on the Cisco IOS router, Cisco IOS Null route remediation failed on the Defense Center. (139387/CSCze91484)
- Resolved an issue where, if one of your network variables in a variable set excluded `::` or `::0` addresses and you referenced the variable set in an access control policy, applying your access control (or an intrusion policy referenced by your access control policy) failed. (139406/CSCze91378)
- Improved the stability of Snort when a nightly intrusion event performance statistics rotation occurred at the same time as an intrusion policy apply. (139958/CSCze91909)
- Resolved an issue where, when creating a network address translation (NAT) policy on a 70xx Family managed device and positioning a dynamic NAT rule specifying a destination port range before a second dynamic NAT rule specifying a destination port included in the first range, the system did not match traffic against the second dynamic rule if the traffic did not match the first dynamic rule. (140216/CSCze91789, 140307)
- Resolved an issue where, if you deleted a managed device from a Defense Center, then added a different device, then reapplied an access control policy with an intrusion policy associated with the default action, the system indicated that the intrusion policy was out of date on more devices than the Defense Center managed. (140525/CSCze92023)
- Resolved an issue where, in some cases, you could not create new scheduled tasks on managed devices. (140557/CSCze92065)
- Resolved an issue where managing 100 or more managed devices with a single Defense Center caused system issues. (140566/CSCze92086)

- Resolved an issue where, if you added a device stack to a group of devices and edited the applied access control policy, the system removed all targeted devices from the policy, prevented you from adding new devices, and corrupted the policy name. (140605/CSCze92048)
- Resolved an issue where, in rare cases, applying a single health policy to 100 or more managed devices caused system issues. (140976/CSCze92387)
- Resolved an issue where the system experienced a memory issue if eStreamer retrieved a large number of file events. (141075/CSCze92527)
- Resolved an issue where, if you created an access control or intrusion rule that blocked traffic, then applied the access control or intrusion policy to a virtual managed device that used an inline interface set, you experienced a disruption in traffic until you restarted the appliance. (141111/CSCze92684)
- Resolved an issue where querying the external database to access packet data from intrusion events on a Defense Center returned incorrect data. (141144/CSCze92564)
- Resolved an issue where creating a saved search that used a VLAN tag object caused the system to save the search with the value **0** in the field where you used the VLAN tag object. (141195/CSCze92623)
- Resolved an issue where, in some cases, syslog alerts sent as intrusion event notifications contained incorrect intrusion rule classification data. (141212/CSCze92570, 141215/CSCze92540, 141219/CSCze92633)
- Resolved an issue where adaptive profiles failed if you used a network variable as your **Networks** value when configuring adaptive profiles. (141224/CSCze92604)
- Resolved an issue where, if you created a custom workflow with a large number of pages, the time window in the top right portion of the page obscured the link to the final pages of the workflow. (141335/CSCze92830)
- Resolved an issue where, in some cases, FireSIGHT rule recommendations attempted to activate a preprocessor rule that was already active, causing system problems. (141439/CSCze92747)
- Resolved an issue where, in rare cases, if you added multiple passive interfaces to a security zone, then referenced the security zone in a managed device configuration, the configuration apply failed and the system experienced a disruption in detection. (141624/CSCze93129, 141627/CSCze92961)
- Resolved an issue where, if one or more detection resources were unresponsive on a managed device, installing an update of the vulnerability database (VDB) caused system issues. (141757/CSCze93059)
- Improved efficiency and memory management of the disk manager. (141795/CSCze92912)
- Improved the stability of Snort when inspecting traffic transmitted via Real Time Streaming Protocol (RTSP). (141815/CSCze93105)

- Resolved an issue where completing a large number of access control policy applies caused the system to experience a memory issue and generate multiple `High unmanaged disk usage` health alerts. (141830/CSCze92990)
- Resolved an issue where, in some cases, revisions to the network address translation (NAT) policy caused system problems. (142003/CSCze93329)
- Resolved an issue where, in rare cases, Series 3 devices experienced delays during device shutdown. (142033/CSCze93287)

Version 5.3.0.1

- Resolved an issue where, in rare cases, configuring an intrusion policy that contained local intrusion rules in a layer that was shared with another intrusion policy caused intrusion policy exports to fail. (132312)
- Resolved an issue where, in rare cases, Snort stopped processing packets if any of your intrusion rules contained the Sensitive Data (sdf) rule classification. (132600)
- Resolved an issue where, in rare cases, Snort drained system resources if you created and applied an access control policy with rules that specified an unusually large range of ports and contained other rule conditions that would cause the Defense Center to send them to the device in expanded form. (132998)
- Resolved an issue where the Security Intelligence page of your access control policy did not display more than 100 available security zones. (133418)
- Resolved an issue where configuring a proxy server to authenticate with a user name and Message Digest 5 (MD5) password encryption caused communication issues with the Defense Center. (133727, 135041)
- Resolved an issue where you could not use the command line interface (CLI) to register a managed device to a pair of Defense Centers in a high availability configuration. (133825)
- Resolved a memory issue on managed devices where the system omitted data from Intrusion Event Performance graphs. (133944)
- Resolved an issue where the system generated an abnormally high count for the **Total Packets Received** Snort real-time statistic. (134036)
- Resolved an issue where the system did not prevent you from reapplying any of your intrusion policies (individually or as part of an access control policy reapply) a total of 4096 or more times on a single managed device. (134231)
- Resolved an issue where, in rare cases, the system generated an extraneous **Module Disk Usage: Frequent drain of Connection Events** health alert. (134355)

- Resolved an issue where the system did not mark your access control policy **out-of-date** after you applied a new version of the vulnerability database (VDB) if your access control policy contained application detectors related to the FireSight Detector Updates identified in the VDB advisory notice. (134458)
- Resolved an issue where, in some cases, scheduled geolocation updates failed if Greenwich Mean Time (GMT, also known as UTC) was not your local timezone. (134742)
- Security Issue Resolved multiple cross-site scripting (XSS) vulnerabilities in application detection, access control, and correlation rule management. (135011, 135629, 135632)
- Improved the stability of Snort when access control rules included URL conditions. (135071, 136833)
- Resolved an issue where, if your managed device originated at Version 5.1.1.x and you updated it to Version 5.2.x and then to Version 5.3, the system generated extraneous health alerts for **high unmanaged disk usage**. (135689)
- Resolved an issue where, if you updated an appliance from Version 5.2.x to Version 5.3 and later created a backup, you could not restore the backup on Defense Centers that were reimaged to Version 5.3. (135869)
- Resolved an issue where the system displayed multiple unique hosts that shared an IP address as a single host with multiple actual MAC addresses in the host profile. (135956, 135992)
- Resolved an issue where the system restricted access to the User Management page (**System > Local > User Management**) on physical managed devices. (136079)
- Security Issue Eliminated an XSS vulnerability (CVE-2014-2012) in the intrusion rule editor pages that could allow an attacker to access and disclose information, imitate user actions and requests, or execute arbitrary JavaScript. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136542)
- Security Issue Eliminated a cross-site request forgery (CSRF) vulnerability (CVE-2014-2011) in the User Configuration page that could allow an attacker to add or edit user accounts. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136911)
- Security Issue Eliminated a CSRF vulnerability (CVE-2014-2028) in the User Management page that could allow an attacker to activate, deactivate, edit, or delete user accounts. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136914)
- Resolved an issue where the system provided incorrect speed data for fiber interfaces with speeds of 4GB and faster. (137484)

- Security Issue Eliminated an XSS vulnerability (CVE-2014-2275) in the Scheduling page, the Health Monitor page, and the event viewers that could allow an attacker to access and disclose information, imitate user actions and requests, or execute arbitrary JavaScript. Special thanks to Adi Volkovitz Check Point Security Research Team for reporting this issue. (137850, 137853, 137856)
- Resolved an issue where, after you disconnected and reconnected the fiber interfaces on a Series 3 managed device, the system did not reestablish the network connection. (138099)

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 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 multiple 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)
- Resolved an issue where, if you configured a custom table populated with data from the **Correlation Events** table and the **Applications** table, then selected **Source IP** as a common field, updates to Version 5.3 failed. (135735)
- Resolved an issue where, in some cases, if you configured 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 did not generate end-of-connection events for matching SSH-encrypted traffic. (135952)

Known Issues

The following known issues are reported in Version 5.3.0.3:

- The *Sourcefire 3D System User Guide* incorrectly states that, in a high availability deployment: `If a secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to all secondary devices. On failed secondary devices, traffic is dropped. A health alert is generated indicating loss of link.`

  The documentation should specify that, if the secondary device in a stack fails, by default, inline sets with configurable bypass enabled go into bypass mode on the primary device. For all other configurations, the system continues to load balance traffic to the failed secondary device. In either case, a health alert is generated to indicate loss of link. (138432)
- If you create a new report (**Overview > Reporting > Report Templates**) and attempt to **Insert Report Parameter** while viewing the web interface with Internet Explorer 11, no report parameters are added to the report section description. As a workaround, install and use Internet Explorer 10. (142950/CSCze94011)
- The *Sourcefire 3D System User Guide* does not reflect that if your Defense Center loses connectivity to the Internet, the system may take up to 30 minutes to generate an Advanced Malware Protection health alert. (143070/CSCze94138)
- The *Sourcefire 3D System User Guide* does not reflect that you can now choose whether to inspect traffic during policy apply. Inspecting traffic during policy apply on a heavily loaded system may have an impact on network throughput and latency. If this side effect is not ideal for your network setup and connectivity is more important than inspection unchecking this box will disable inspection temporarily during policy apply and ensure that no packets are dropped during the procedure. After policy apply is successful inspection will resume as normal. (143295/CSCze94372)
- In some cases, if your Defense Center and managed devices experience high volumes of traffic, the system generates incorrect CPU health alerts. (143986/CSCze95067)
- The *Sourcefire 3D System User Guide* does not reflect that, if you enable inline normalization, the blocked packets graph on the Block Packets page (**Overview > Summary > Intrusion Event Performance >Blocked Packets**) should be described as the number of packets blocked as a result of rules set to drop in an inline deployment instead of the number of packets blocked as the result of TCP normalization. (144360/CSCze95222)
- If you cluster Series 3 devices and configure the shared Sourcefire Resolution Protocol (SFRP) configuration so the primary device is configured as the backup SFRP with a non-SFRP IP address and the secondary device is configured as the active SFRP with a SFRP IP address, both devices attempt to respond to Address Resolution Protocol (ARP)

requests for incoming addresses that matches rules in the applied network analysis policy and experience a disruption in traffic. As a workaround, ensure the primary device of a cluster is configured as an active SFRP with an SFRP IP address. (CSCur55568)

Known Issues Reported in Previous Releases

The following is a list of known issues that were reported in previous releases of the Sourcefire 3D System:

- In some cases, applying changes to your access control policy, intrusion policy, network discovery policy, or device configuration, or installing an intrusion rule update or update of the vulnerability database (VDB), causes the system to experience a disruption in traffic that uses Link Aggregation Control Protocol (LACP) in fast mode. As a workaround, configure LACP links in slow mode. (112070/CSCze87966)
- In some cases, the system includes extraneous data about dropped packets in intrusion event performance graphs. (124934/CSCze87728)
- If the system generates intrusion events with a Destination Port/ICMP Code of 0, the Top 10 Destination Ports section of the Intrusion Event Statistics page (**Overview > Summary > Intrusion Event Statistics**) omits port numbers from the display. (125581/CSCze88014)
- Defense Center local configurations (**System > Local > Configuration**) are **not** synchronized between high availability peers. You must edit and apply the changes on all Defense Centers, not just the primary. (130612/CSCze89250, 130652)
- In some cases, large system backups may fail if disk space usage exceeds the disk space threshold before the system begins pruning. (132501/CSCze88368)
- In some cases, using the RunQuery tool to execute a `SHOW TABLES` command may cause the query to fail. To avoid query failure, only run this query interactively using the RunQuery application. (132685/CSCze89153)
- If you 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/CSCze89273)
- If you delete a previously-imported local intrusion rule, you cannot re-import the deleted rule. (132865/CSCze88250)
- In rare cases, the system may not generate events for intrusion rules 141:7 or 142:7. (132973/CSCze89252)
- In some cases, remote backups of managed devices include extraneous unified files, generating large backup files on your Defense Center. (133040/CSCze89204)

- You must edit the maximum transmission unit (MTU) on a Defense Center or managed device using the appliance's CLI or shell. You cannot edit the MTU on a Defense Center or managed device via the user interface. (133802/CSCze89748)
- If you create a URL object with an asterisk (*) in the URL, the system does not generate preempted rule warnings for access control policies containing rules that reference the object. Do **not** use asterisks (*) in URL object URLs. (134095/CSCze88837, 134097/CSCze88846)
- If you configure your intrusion policy to generate intrusion event syslog alerts, the syslog alert message for intrusion events generated by intrusion rules with preprocessor options enabled is `Snort Alert`, not a customized message. (134270/CSCze88831)
- If the secondary device in a stack generates an intrusion event, the system does not populate the table view of intrusion events with security zone data. (134402/CSCze88843)
- If you configure an Nmap scan remediation with the **Fast Port Scan** option enabled, Nmap remediation fails. As a workaround, disable the **Fast Port Scan** option. (134499/CSCze88810)
- If you generate a report containing connection event summary data based on a connection event table saved search, reports on that table populate with no data. (134541/CSCze89348)
- Scheduling and running simultaneous system backup tasks negatively impacts system performance. As a workaround, stagger your scheduled tasks so only one backup runs at a time. (134575/CSCze89679)
- If you edit a previously-configured LDAP connection where user and group access control parameters are enabled, clicking **Fetch Groups** does not populate the Available Groups box. You must re-enter your password when editing an LDAP connection in order to fetch available groups. (134872/CSCze89834)
- In some cases, if you enable **Resolve IP Addresses** in the **Event Preferences** section of the Event View Settings page, hostnames associated with IPv6 addresses may not resolve as expected in the dashboard or event views. (135182/CSCze90155)
- You cannot enter more than 450 characters in the **Base Filter** field when creating an LDAP authentication object. (135314/CSCze89081)
- In some cases, if you schedule a task while observing Daylight Saving Time (DST), the task does not run during periods when you are not observing DST. As a workaround, select **Europe, London** as your local time zone on the Time Zone Preference page (**Admin > User Preferences**) and recreate the task during a period when you are not observing DST. (135480)
- The system requires additional time to reboot appliances running Version 5.3 or later due to a database check. If errors are found during the database check, the reboot requires additional time to repair the database. (135564, 136439)

- In some cases, the system may generate a false positive for the SSH preprocessor rule 128:1. (135567/CSCze89434)
- If you apply an intrusion policy containing a rule with the **Extract Original Client IP Address** HTTP preprocessor option enabled, the system may populate intrusion events with incorrect data in the **Original Client IP** field if traffic passes through a dedicated proxy server. (135651/CSCze89056)
- If the maximum transmission unit (MTU) setting on an 8000 Series managed device triggers IP datagram fragmentation, the system may experience NMSB connection issues. (135731/CSCze89504)
- If you schedule a task with **Report** as the job type, the system does not attach the report to the emailed status report. (136026/CSCze90265)
- If you apply an access control policy to multiple devices, the Defense Center displays the task status differently on the Task Status page, the Access Control policy page, and the Device Management page of the web interface. The status on the Device Management page (**Devices > Device Management**) is correct. (136364/CSCze87068, 136614/CSCze89936)
- In some cases, if you create a custom workflow based on the health events table, the Defense Center displays conflicting data in the event viewer. (136419/CSCze90336)
- If you import a custom intrusion rule as an `.rtf` file, the system does not warn you that the `.rtf` file type is not supported. (136500/CSCze89991)
- If you configure a Security Intelligence feed and specify a **Feed URL** that was created on a computer running a Windows operating system, the system does not display the correct number of submitted IP addresses in the tooltips on the Security Intelligence tab. As a workaround, use `dos2unix` commands to convert the file from Windows encoding to Unix encoding and click **Update Feeds** on the Security Intelligence page. (136557/CSCze89888)
- If you disable a physical interface, the logical interfaces associated with it are disabled but remain green on the Interfaces tab of the appliance editor for that managed device. (136560/CSCze89894)
- If you create a custom table based on the Captured Files table, the system generates an error message. The system does not support creating a custom table based on the Captured Files table. (136844/CSCze89977)
- If you register a managed device with a hostname containing more than 40 characters, device registration fails. (137235/CSCze90144)
- In some cases, the system does not filter objects in the Object Manager as expected if you include any of the following special characters in the filter criteria: dollar sign (`$`), caret (`^`), asterisk (`*`), brackets (`[ ]`), vertical bar (`|`), forward slash (`\`), period (`.`), and question mark (`?`). (137493/CSCze90413)

- In some cases, if you enabled Simple Network Management Protocol (SNMP) polling in your system policy, modifying the high availability (HA) link interface configuration on one of your clustered managed devices causes the system to generate inaccurate SNMP polling requests. (137546/CSCze90000)
- In some cases, configuring your access control policy to log blacklisted connections to the syslog or SNMP trap server causes system issues. (137952/CSCze90538)
- In some cases, the Operating System Summary workflow displays incorrect DNS server counts, NTP server counts, and DNS port counts if the system receives DNS or NTP packets out of order. (138047/CSCze90930)
- The table view of file events appears to support viewing the file trajectory for ineligible file events. You can only view file trajectories for files with a calculated SHA-256 value. (138155/CSCze90676)
- If you generate a report in HTML or PDF format that includes a chart with **File Name** as the x-axis, the system does not display UTF-8 characters in the x-axis filenames. (138297/CSCze90799)
- In rare cases, if you have ever used your Defense Center to manage more than one device, the system displays inaccurate intrusion event counts in the dashboard. (138298)
- In rare cases, revising and reapplying an intrusion policy hundreds of times causes intrusion rule updates and system updates to require over 24 hours to complete. (138333/CSCze90747)
- If the latest version of the geolocation database (GeoDB) is installed on your Defense Center and you attempt to update the GeoDB with the same version, the system generates an error message. (138348/CSCze90813)
- In some cases, if you apply more than one access control policy across your deployment, searching for intrusion or connection events (**Analysis > Search**) matching a specific access control rule may retrieve events generated by unrelated rules in other policies. (138542/CSCze91690)
- In some cases, rebooting a Series 3 managed device after a failed system update causes a hardware issue. If a system update fails, contact Support and do **not** reboot the appliance. (138684/CSCze90977)
- You cannot cut and paste access control rules from one policy to another. (138713/CSCze91012)
- In the Security Intelligence Source/Destination metadata (rec_type:281), the eStreamer server identifies the source as the destination and the destination as the source. (138740/CSCze91402)

- In an access control policy, the system processes certain Trust rules before the policy's Security Intelligence blacklist. Trust rules placed before either the first Monitor rule or before a rule with an application, URL, user, or geolocation-based network condition are processed before the blacklist. That is, Trust rules that are near the top of an access control policy (rules with a low number) or that are used in a simple policy allow traffic that should have been blacklisted to pass uninspected instead. (138743, 139017)
- If you disable **Drop When Inline** in your intrusion policy, inline normalization stops modifying packets seen in traffic and the system does not indicate what traffic would be modified. In some cases, other devices or applications on your network may not function in the same way after you re-enable **Drop When Inline**. (13917/CSCze911494, 139177/CSCze91163)
- 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 prevent exposure to the vulnerability, do not enable LOM. To mitigate the vulnerability, deploy your appliances on a secure management network accessible only to trusted users and use a complex, non-dictionary-based password. If you enable LOM and expose this vulnerability, change the complex password every three months. For LOM password requirements, see the *Sourcefire 3D System User Guide*. (139286/CSCze91556, 140954)
- In rare cases, the Task Status page (**System > Monitoring > Task Status**) incorrectly reports that a failed system policy apply succeeded. (139428/CSCze92142)
- In some cases, the system does not enforce the maximum transmission unit (MTU) setting on Series 2 or virtual devices. (139620/CSCze91705)
- If you configure and save three or more intrusion policies that reference each other through their base policies, the system does not update the **Last Modified** dates for all policies on the Intrusion Policy page (**Policies > Intrusion > Intrusion Policy**). As a workaround, wait 5-10 minutes and refresh the Intrusion Policy page. (139647/CSCze91353)
- In some cases, if you configure and save a report with a time window that includes the transition day from observing Daylight Saving Time (DST) to not observing DST, the system adjusts the time window to begin an hour earlier than you specified. As a workaround, set the time window to begin one hour later. (139713/CSCze91697)
- If you remove an IP address from the global whitelist via the Object Manager page of the Defense Center web interface, the command line interface (CLI) on your Defense Center does not reflect the change. (139784/CSCze91728)

- The system does not prevent an externally authenticated user from modifying the LDAP password via the User Preferences page. If an externally authenticated user does this, the user becomes an internally authenticated user. (140143/CSCze91938)
- You can only import a HTTPS certificate once. Modifying or re-importing a server certificate fails. (140283/CSCze92162)
- Although you cannot enable bypass mode for clustered devices, the option still appears in the web interface. (140604/CSCze92047)
- If you create a report in bar graph report form that shows data organized by day, only a maximum of 10 days can appear in the graph. As a workaround, create multiple reports in 10-day increments. (140833/CSCze92405)
- In some cases, the **Password Lifetime** column on the User Management page (**Operations > User Management**) may display a negative value if a user's password has expired. (140839/CSCze92338)
- If you disable an access control rule that invokes an intrusion policy, then reapply your access control policy, the system incorrectly indicates that the appliances' intrusion policy is out of date. As a workaround, delete access control rules that use intrusion policies instead of disabling those rules. (141044/CSCze92012)
- You cannot delete vulnerabilities from the third-party vulnerabilities table (**Analysis > Vulnerabilities > Third-Party Vulnerabilities**). (141103/CSCze92621)
- Files that are intentionally not stored by the system (such as files seen for the first time, or files outside the size limit) incorrectly appear with a **File Storage** value of `Failed`. (141196/CSCze92629, 141505/CSCze92908)
- If you create a configuration-only backup, the backup file includes extraneous discovery event data. (141246/CSCze92508)
- The system-provided saved search **Public Addresses Only** incorrectly includes the private 172.x.x.x IP address range. (141285/CSCze92654)
- When you update your appliances to a new software version, the update overwrites any changes you made to default dashboard pages. As a workaround, perform a system backup before updating, then restore the backup. (141363/CSCze92812)
- Reports do not resolve DNS names for IP addresses, even if you have configured them to do so. (141393/CSCze92797)

- When you configure a device inline between a host and a web server, block the web server by URL in your access control policy, enable the Cisco-provided block response page, then attempt to access the web server from the host, a session timeout may result if the open connection limit of the server's operating system is reached. (141440/CSCze92753)
- In some cases, excessive saved revisions to the intrusion policy may cause system performance issues. (141501/CSCze92792, 141754/CSCze92960)
- On 3D9900 devices, passive interfaces not in security zones do not generate intrusion or connection events. As a workaround, create and specify a security zone for all passive interfaces on this device model. (141663/CSCze93022)
- When you edit a saved search, the previously configured name of the search does not appear in the **Name** field; the field is empty. (142060/CSCze93463)
- When the system sends a file for sandbox analysis and the cloud does not respond within 50 minutes, the file's status still appears as **Sent for Analysis** instead of indicating that analysis has timed out. (142309/CSCze93757)
- When you are using two Defense Centers in a high availability configuration, you cannot generate troubleshooting reports for a Defense Center from the web interface of its high availability peer. You must generate troubleshooting reports directly from the Defense Center you need the reports for. (142645/CSCze93908)

Features Introduced in Previous Versions

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

5.3.0.x

The following features and functionality were introduced in Version 5.3.0.x:

- As of Version 5.3.0.1, LDAP usernames are not case-sensitive. In Version 5.3, usernames were case-sensitive.
- As of Version 5.3.0.1, you can no longer perform joins using the `application_tag_id` field in the `application_host_map` table when querying the external database.

5.3

The following features and functionality were introduced in Version 5.3:

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 introduced 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 provided 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.

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 provided 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 introduced 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**).

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 introduced 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 introduced 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.

Geolocation and Access Control

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

Version 5.3 introduced 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.

8300 Family of Series 3 FirePOWER Appliances

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

Version 5.3 introduced 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 introduced 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.

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.

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

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

- 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 identifies traffic referred by a web server as the web application for referred connections as of Version 5.3. 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 use IPv6 addresses to create authentication objects as of Version 5.3. Note that you cannot use authentication objects with IPv6 addresses to authenticate shell accounts.
- As of Version 5.3 you can 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 (#).
- As of Version 5.3 you can 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 includes file policy UUID metadata for type 502 intrusion events as of Version 5.3.
- 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.
- As of Version 5.3 the system alerts you if you attempt to install a version of the Sourcefire Geolocation Database (GeoDB) already installed on your system.
- As of Version 5.3 you can create correlation rules with **Application Protocol Category**, **Client Category**, and **Web Application Category** conditions.

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

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.