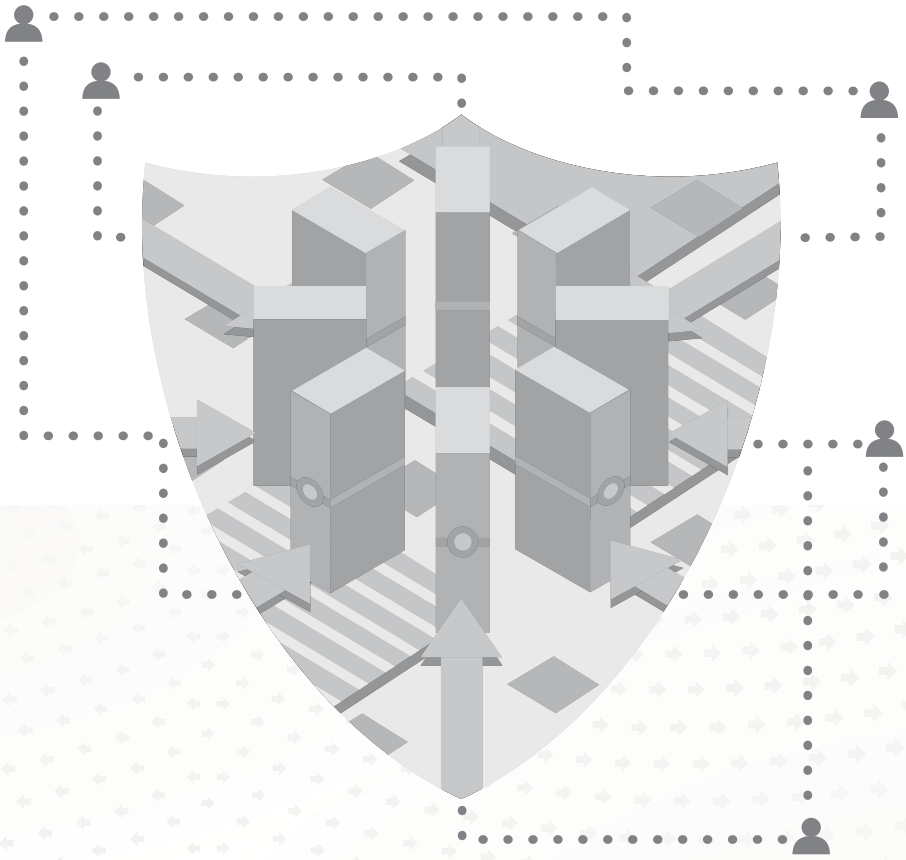
Sourcefire 3D System

Installation Guide

Version 5.2



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

Legal Notices

Cisco, the Cisco logo, Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, and certain other trademarks and logos are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Cisco or its subsidiaries (collectively, "Cisco") or any Sourcefire-provided or Cisco-provided products. Sourcefire and Cisco products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

The copyright in the Documentation is owned by Cisco and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Cisco's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

No part of the Documentation may be used in a compilation or otherwise incorporated into another work or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of Cisco. Cisco reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms.

Disclaimers

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

2014-Mar-25 11:52

Table of Contents

Chapter 1
Introduction to the Sourcefire 3D System

The Sourcefire 3D® System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on detected applications, users, and URLs. You can also use Sourcefire appliances to serve in a switched, routed, or hybrid (switched and routed) environment; to perform network address translation (NAT); and to build secure virtual private network (VPN) tunnels among the virtual routers on Sourcefire managed devices, or from managed devices to remote devices or other third-party VPN endpoints.

The Sourcefire Defense Center® provides a centralized management console and database repository for the Sourcefire 3D System. Managed devices installed on network segments monitor traffic for analysis.

Devices in a passive deployment monitor traffic flowing across a network, for example, using a switch SPAN, virtual switch, or mirror port. Passive sensing interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.

Devices in an inline deployment allow you to protect your network from attacks that might affect the availability, integrity, or confidentiality of hosts on the network. Inline interfaces receive all traffic unconditionally, and traffic received on these interfaces is retransmitted unless explicitly dropped by some configuration in your deployment. Inline devices can be deployed as a simple intrusion prevention system. You can also configure inline devices to perform access control as well as manage network traffic in other ways.

This installation guide provides information about deploying, installing, and setting up Sourcefire appliances (devices and Defense Centers). It also contains

hardware specifications and safety and regulatory information for Sourcefire appliances.

TIP! You can host virtual Defense Centers and devices, which can manage and be managed by physical appliances. However, virtual appliances do not support any of the system's hardware-based features: redundancy, switching, routing, and so on. For detailed information, see the *Sourcefire 3D System Virtual Installation Guide*.

The topics that follow introduce you to the Sourcefire 3D System and describe its key components:

- Sourcefire 3D System Appliances on page 9
- Sourcefire 3D System Components on page 16
- Licensing the Sourcefire 3D System on page 19
- Security, Internet Access, and Communication Ports on page 23

Sourcefire 3D System Appliances

A Sourcefire *appliance* is either a traffic-sensing managed *device* or a managing *Defense Center*:

Physical devices are fault-tolerant, purpose-built network appliances available with a range of throughputs and capabilities. Defense Centers serve as central management points for these devices, and automatically aggregate and correlate the events they generate. There are several *models* of each physical appliance type; these models are further grouped into *series* and *family*.

Many Sourcefire 3D System capabilities are appliance dependent. For more information, see the following sections:

- Defense Centers on page 9
- Managed Devices on page 10
- Understanding Appliance Series, Models, and Capabilities on page 10

Defense Centers

The Defense Center provides a centralized management point and event database for your Sourcefire 3D System deployment. Defense Centers, which can be physical or virtual, aggregate and correlate intrusion, file, malware, discovery, connection, and performance data. This allows you to monitor the information that your devices report in relation to one another, and to assess and control the overall activity that occurs on your network.

Key features of the Defense Center include:

- device, license, and policy management
- display of event and contextual information using tables, graphs, and charts
- health and performance monitoring
- external notification and alerting
- real-time threat response using correlation and remediation features
- reporting

For many physical Defense Centers, a high availability (redundancy) feature can help you ensure continuity of operations.

Managed Devices

Physical Sourcefire devices are fault-tolerant, purpose-built network appliances available in a range of throughputs. You can also host virtual devices. Devices deployed passively help you gain insight into your network traffic. Deployed inline, you can use Sourcefire devices to affect the flow of traffic based on multiple criteria. You must manage Sourcefire devices with a Defense Center.

Depending on model and license, managed devices:

- gather detailed information about your organization's hosts, operating systems, applications, users, files, networks, and vulnerabilities
- block or allow network traffic based on various network-based criteria, as well as other criteria including applications, users, URLs, IP address reputations, and the results of intrusion or malware inspections
- have switching, routing, DHCP, NAT, and VPN capabilities, as well as configurable bypass interfaces, fast-path rules, and strict TCP enforcement
- have clustering (redundancy) to help you ensure continuity of operations, and stacking to combine resources from multiple devices

Understanding Appliance Series, Models, and Capabilities

Version 5.2 of the Sourcefire 3D System is available on two series of physical appliances, as well as virtual appliances. Many Sourcefire 3D System capabilities are appliance dependent. For more information, see:

- Series 2 Appliances on page 11
- Series 3 Appliances on page 11
- Virtual Appliances on page 12
- Appliances Delivered with Version 5.2 on page 12
- Supported Capabilities by Appliance Model on page 13

Series 2 Appliances

Series 2 is the second series of Sourcefire physical appliances. Because of resource and architecture limitations, Series 2 devices support a restricted set of Sourcefire 3D System features.

Although Sourcefire does not deliver Version 5.2 on Series 2 appliances other than 3D500/1000/2000 devices, you can restore the following Series 2 devices and Defense Centers to Version 5.2:

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

There is no update path from Version 4.10.x to Version 5.2; you must use an ISO image to restore your appliances. Reimaging results in the loss of **all** configuration and event data on the appliance. You **cannot** import this data onto an appliance after a reimage. For more information, see Restoring a Sourcefire Appliance to Factory Defaults on page 198.

IMPORTANT! Only reimage your appliances during a maintenance window. Reimaging resets devices in inline deployments to a non-bypass configuration and disrupts traffic on your network. For more information, see Traffic Flow During the Restore Process on page 199.

When running Version 5.2, Series 2 devices automatically have most of the capabilities associated with a Protection license: intrusion detection and prevention, file control, and basic access control. However, Series 2 devices cannot perform Security Intelligence filtering, advanced access control, or advanced malware protection. You also cannot enable other licensed capabilities on a Series 2 device. With the exception of the 3D9900, which supports fast-path rules, stacking, and tap mode, Series 2 devices do not support any of the hardware-based features associated with Series 3 devices: switching, routing, NAT, and so on.

When running Version 5.2, DC1000 and DC3000 Series 2 Defense Centers support all the features of the Sourcefire 3D System; the DC500 has more limited capabilities.

Series 3 Appliances

Series 3 is the third series of Sourcefire physical appliances. All 7000 Series and 8000 Series devices are Series 3 appliances. 8000 Series devices are more powerful and support a few features that 7000 Series devices do not.

Virtual Appliances

You can host 64-bit virtual Defense Centers and devices on VMware ESX/ESXi. Virtual Defense Centers can manage up to 25 physical or virtual devices; physical Defense Centers can manage virtual devices.

Regardless of the licenses installed and applied, virtual appliances do not support any of the system's hardware-based features: redundancy, switching, routing, and so on. Also, virtual devices do not have web interfaces. For detailed information on virtual appliances, see the *Sourcefire 3D System Virtual Installation Guide*.

Appliances Delivered with Version 5.2

The following table lists the appliances that Sourcefire delivers with Version 5.2 of the Sourcefire 3D System.

Version 5.2 Sourcefire Appliances

Models/Family	Series	Type
Series 2 devices: 3D500, 3D1000, and 3D2000	Series 2	device
70xx Family: 3D7010, 3D7020 and 3D7030	Series 3 (7000 Series)	device
71xx Family: 3D7110, 3D7115, 3D7120m and 3D7125	Series 3 (7000 Series)	device
81xx Family: 3D8120/8130/8140	Series 3 (8000 Series)	device
82xx Family: 3D8250, 3D8260, 3D8270, and 3D8290	Series 3 (8000 Series)	device
virtual devices	none	device
Series 3 Defense Centers: DC750/1500/3500	Series 3	Defense Center
virtual Defense Centers	none	Defense Center

Although Sourcefire does not deliver Version 5.2 on Series 2 appliances other than 3D500, 3D1000m and 3D2000 devices, you can reimage the following Series 2 devices and Defense Centers to Version 5.2:

- 3D2100/2500/3500/4500
- 3D6500

- 3D9900
- DC500/1000/3000

Reimaging results in the loss of **all** configuration and event data on the appliance. See Restoring a Sourcefire Appliance to Factory Defaults on page 198 for more information.

Supported Capabilities by Appliance Model

Many Sourcefire 3D System capabilities are appliance dependent. The table below matches the major capabilities of the system with the appliances that support those capabilities, assuming you have the correct licenses installed and applied. For a brief summary of these features and licenses, see Supported Capabilities by Appliance Model on page 13 and Licensing the Sourcefire 3D System on page 19.

The Defense Center column for device-based capabilities (such as stacking, switching, and routing) indicates whether that Defense Center can manage and configure devices to perform their functions. For example, you can use a Series 2 DC1000 to manage NAT on Series 3 devices. Also, a blank cell means the feature is unsupported, while `n/a` marks certain Defense Center-based features that are not relevant to managed devices.

Supported Capabilities by Appliance Model

Feature	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center	Virtual Device	Virtual Defense Center
network discovery: host, application, and user	✓	✓	✓	✓	✓	✓
geolocation data	✓	DC1000, DC3000	✓	✓	✓	✓
intrusion detection and prevention (IPS)	✓	✓	✓	✓	✓	✓
Security Intelligence filtering		DC1000, DC3000	✓	✓	✓	✓
access control: basic network control	✓	✓	✓	✓	✓	✓
access control: applications		✓	✓	✓	✓	✓
access control: users		DC1000, DC3000	✓	✓	✓	✓

Supported Capabilities by Appliance Model (Continued)

Feature	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center	Virtual Device	Virtual Defense Center
access control: literal URLs		✓	✓	✓	✓	✓
access control: URL filtering by category and reputation		DC1000, DC3000	✓	✓	✓	✓
file control: by file type	✓	✓	✓	✓	✓	✓
network-based advanced malware protection (AMP)		DC1000, DC3000	✓	✓	✓	✓
FireAMP integration	n/a	✓	n/a	✓	n/a	✓
fast-path rules	3D9900	✓	8000 Series	✓		✓
strict TCP enforcement		✓	✓	✓		✓
configurable bypass interfaces	✓	✓	except where hardware limited	✓		✓
tap mode	3D9900	✓	✓	✓		✓
switching and routing		✓	✓	✓		✓
NAT policies		✓	✓	✓		✓
VPN		✓	✓	✓		✓
high availability	n/a	DC1000, DC3000	n/a	DC1500, DC3500	n/a	
device stacking	3D9900	✓	3D8140, 82xx Family	✓		✓

Supported Capabilities by Appliance Model (Continued)

Feature	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center	Virtual Device	Virtual Defense Center
device clustering		✓	✓	✓		✓
clustered stacks		✓	3D8140, 82xx Family	✓		✓
interactive CLI			✓		✓	

Series 3 Device Chassis Designations

The following section lists the 7000 Series and 8000 Series devices and their respective chassis hardware codes. The chassis code appears on the regulatory label on the outside of the chassis, and is the official reference code for hardware certifications and safety.

7000 Series Chassis Designations

The 7000 Series Chassis Models table lists the chassis designations for the 7000 Series models available world-wide.

7000 Series Chassis Models

3D Device Model	Hardware Chassis Code
3D7010, 3D7020, and 3D7030	CHRY-1U-AC
3D7110 and 3D7120 (Copper)	GERY-1U-8-C-AC
3D7110 and 3D7120 (Fiber)	GERY-1U-8-FM-AC
3D7115 and 3D7125	GERY-1U-4C8S-AC

8000 Series Chassis Designations

The 8000 Series Chassis Models table lists the chassis designations for the Series 3 models available world-wide.

8000 Series Chassis Models

3D Device Model	Hardware Chassis Code
3D8120, 3D8130, and 3D8140 (AC power)	CHAS-1U-AC
3D8120, 3D8130, and 3D8140 (DC power)	CHAS-1U-DC
3D8250, 3D8260, 3D8270, and 3D8290 (AC power)	CHAS-2U-AC
3D8250, 3D8260, 3D8270, and 3D8290 (DC power)	CHAS-2U-DC

Sourcefire 3D System Components

The sections that follow describe some of the key capabilities of the Sourcefire 3D System that contribute to your organization's security, acceptable use policy, and traffic management strategy.

TIP! Many Sourcefire 3D System capabilities are appliance model, license, and user role dependent. Where needed, Sourcefire documentation outlines the requirements for each feature and task.

Redundancy and Resource Sharing

The redundancy and resource-sharing features of the Sourcefire 3D System allow you to ensure continuity of operations and to combine the processing resources of multiple physical devices:

- Defense Center high availability allows you to designate redundant DC1000, DC1500, DC3000, or DC3500 Defense Centers to manage devices.
- Device stacking allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration.
- Device clustering allows you to establish redundancy of networking functionality and configuration data between two or more Series 3 devices or stacks.

Network Traffic Management

The Sourcefire 3D System's network traffic management features allow Series 3 devices to act as part of your organization's network infrastructure. You can:

- configure a Layer 2 deployment to perform packet switching between two or more network segments
- configure a Layer 3 deployment to route traffic between two or more interfaces
- perform network address translation (NAT)
- build secure VPN tunnels from virtual routers on managed devices to remote devices or other third-party VPN endpoints

FireSIGHT

FireSIGHT™ is Sourcefire's discovery and awareness technology that collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities, in order to provide you with a complete view of your network.

You can use the Defense Center's web interface to view and analyze data collected by FireSIGHT. You can also use this data to help you perform access control and modify intrusion rule states.

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that traverses your network. As part of access control, the Security Intelligence feature allows you to blacklist—deny traffic to and from—specific IP addresses before the traffic is subjected to deeper analysis.

After Security Intelligence filtering occurs, you can define which and how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. You can trust, monitor, or block traffic, or perform further analysis, such as:

- intrusion detection and prevention
- file control
- file tracking and network-based advanced malware protection (AMP)

Intrusion Detection and Prevention

Intrusion detection and prevention is a policy-based feature, integrated into access control, that allows you to monitor your network traffic for security violations and, in inline deployments, to block or alter malicious traffic. An intrusion policy contains a variety of components, including:

- rules that inspect the protocol header values, payload content, and certain packet size characteristics
- rule state configuration based on FireSIGHT recommendations

- advanced settings, such as preprocessors and other detection and performance features
- preprocessor rules that allow you to generate events for associated preprocessors and preprocessor options

File Tracking, Control, and Malware Protection

To help you identify and mitigate the effects of malware, the Sourcefire 3D System's file control, network file trajectory, and advanced malware protection components can detect, track, and optionally block the transmission of files (including malware files) in network traffic.

File control is a policy-based feature, integrated into access control, that allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.

Network-based advanced malware protection (AMP) allows the system to inspect network traffic for malware in specific types of files. When a managed device detects one of these file types, the Defense Center obtains the file's disposition from the Sourcefire cloud. The managed device uses this information to track and then block or allow the file.

FireAMP is Sourcefire's enterprise-class, endpoint-based AMP solution. If your organization has a FireAMP subscription, individual users install FireAMP Connectors on their computers and mobile devices. These lightweight agents communicate with the Sourcefire cloud, which in turn communicates with the Defense Center. In this way, you can use the Defense Center to view malware detection and quarantines on the endpoints in your organization, as well as to track the malware's trajectory.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs):

- The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Sourcefire appliance to a custom-developed client application.
- The database access feature allows you to query several database tables on a Defense Center, using a third-party client that supports JDBC SSL connections.
- The host input feature allows you to augment the information in the network map by importing data from third-party sources using scripts or command-line files.
- Remediations are programs that your Defense Center can automatically launch when certain conditions on your network are met. This can not only automatically mitigate attacks when you are not immediately available to address them, but can also ensure that your system remains compliant with your organization's security policy.

Licensing the Sourcefire 3D System

You can license a variety of features to create an optimal Sourcefire 3D System deployment for your organization. You must use the Defense Center to control licenses for itself and the devices it manages.

Sourcefire recommends you add the licenses your organization has purchased during the initial setup of your Defense Center. Otherwise, any devices you register during initial setup are added to the Defense Center as unlicensed. You must then enable licenses on each device individually after the initial setup process is over. For more information, see Setting Up a Sourcefire 3D System Appliance on page 86.

A FireSIGHT license is included with each Defense Center purchase, and is required to perform host, application, and user discovery. The FireSIGHT license on your Defense Center also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as how many users you can use to perform user control. FireSIGHT host and user license limits are model specific, as listed in the following table.

FireSIGHT Limits by Defense Center Model

Defense Center Model	FireSIGHT Host and User Limit
DC500	1000 (no user control)
DC750	2000
DC1000	20,000
DC1500	50,000
DC3000	100,000
DC3500	300,000

If your Defense Center was previously running Version 4.10.x, you may be able to use legacy RNA Host and RUA User licenses instead of a FireSIGHT license. For more information, see Using Legacy RNA Host and RUA User Licenses on page 22.

Additional model-specific licenses allow your managed devices to perform a variety of functions, as follows:

Protection

A Protection license allows managed devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering.

Control

A Control license allows managed devices to perform user and application control. It also allows devices to perform switching and routing (including DHCP relay), NAT, and to cluster devices and stacks. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows managed devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A URL Filtering license requires Protection and Control licenses.

Malware

A Malware license allows managed devices to perform network-based advanced malware protection (AMP), that is, to detect and block malware in files transmitted over your network. It also allows you to view trajectories, which track files transmitted over your network. A Malware license requires a Protection license.

VPN

A VPN license allows you to build secure VPN tunnels among the virtual routers on Sourcefire managed devices, or from managed devices to remote devices or other third-party VPN endpoints. A VPN license requires Protection and Control licenses.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. In general, you cannot license a capability that a device does not support; see Supported Capabilities by Appliance Model on page 13.

The following table summarizes which licenses you can add to your Defense Center and apply to each device model. The Defense Center rows (for all licenses except FireSIGHT) indicate whether that Defense Center can manage devices using those licenses. For example, you can use a Series 2 DC1000 to create a VPN deployment using Series 3 devices, but you cannot use a DC500 to perform category and reputation-based URL filtering, regardless of the devices it

manages. Also, a blank cell means the license is unsupported, while n/a marks Defense Center-based licenses that are not relevant to managed devices.

Supported Licenses by Model

Models	FireSIGHT	Protection	Control	URL Filtering	Malware	VPN
Series 2 devices: • 3D500/1000/2000 • 3D2100/2500/3500/4500 • 3D6500 • 3D9900	n/a	automatic, no Security Intelligence				
Series 3 devices: • 7000 Series • 8000 Series	n/a	✓	✓	✓	✓	✓
virtual devices	n/a	✓	no support for hardware features	✓	✓	
DC500 Series 2 Defense Center	✓	no Security Intelligence	no user control			✓
DC1000/3000 Series 2 Defense Centers	✓	✓	✓	✓	✓	✓
DC750/1500/3500 Series 3 Defense Centers	✓	✓	✓	✓	✓	✓
virtual Defense Centers	✓	✓	✓	✓	✓	✓

In addition to the information in the table, note that:

- Series 2 devices automatically have Protection capabilities, with the exception of Security Intelligence filtering.
- Although you can enable a Control license on a virtual device, a virtual device does not support any of the hardware-based features granted by that license, such as switching or routing.
- Although the DC500 can manage devices with Protection and Control licenses, you cannot perform Security Intelligence filtering or user control.

For detailed information on licensing, see the Licensing the Sourcefire 3D System chapter in the *Sourcefire 3D System User Guide*.

Using Legacy RNA Host and RUA User Licenses

In Version 4.10.x of the Sourcefire 3D System, RNA Host and RUA User feature licenses determined your monitored host and user limits, respectively. If your Defense Center was previously running Version 4.10.x, you can use your legacy host and user licenses instead of a FireSIGHT license.

Version 5.2 Defense Centers using legacy licenses use the RNA Host limit as the FireSIGHT host limit and the RUA User limit as both the FireSIGHT user and authoritative user limit. The FireSIGHT Host License Limit health module alerts appropriately for your licensed limit.

Note that RNA Host and RUA User limits are cumulative. That is, you can add multiple licenses of each type to the Defense Center to monitor the total number of hosts or users allowed by the licenses.

If you later add a FireSIGHT license, the Defense Center uses the higher of the limits. For example, the FireSIGHT license on the DC1500 supports up to 50,000 hosts and users. If the RNA Host limit on your Version 4.10.x DC1500 was higher than 50,000, using that legacy host license on the same Defense Center running Version 5.2 gives you the higher limit. For your convenience, the web interface displays only the licenses that represent the higher limits.

IMPORTANT! Because FireSIGHT license limits are matched to the hardware capabilities of Defense Centers, Sourcefire does **not** recommend exceeding them when using legacy licensing. For guidance, contact Sourcefire Support.

Because there is no update path from Version 4.10.x to Version 5.2, you must use an ISO image to "restore" the Defense Center. Note that reimaging results in the loss of **all** configuration and event data on the appliance. You **cannot** import this data onto an appliance after a reimage. For more information, see Restoring a Sourcefire Appliance to Factory Defaults on page 198.

IMPORTANT! Only reimage your appliances during a maintenance window. Reimaging resets devices in an inline deployment to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process on page 199.

During the restore process, you are prompted to delete license and network settings. Keep these settings, although you can re-add them later if you accidentally delete them. Note that Version 5.2 Defense Centers cannot manage Version 4.10.x devices. You can, however, restore and update supported Version 4.10.x devices to the latest version. For more information, see Restoring a Sourcefire Appliance to Factory Defaults on page 198.

Security, Internet Access, and Communication Ports

To safeguard the Defense Center, you must install the Defense Center on a protected internal network. Although the Defense Center is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it from outside the firewall.

If the Defense Center and the managed device reside on the same network, you can connect the management interface on the device to the same protected internal network as the Defense Center. This allows you to securely control the device from the Defense Center and aggregate the event data generated on the managed device's network segment. By using the Defense Center's filtering capabilities, you can analyze and correlate data from attacks across your network to evaluate how well your security policies are being implemented.

Note, however, that Sourcefire appliances are configured to directly connect to the Internet. Specific features of the Sourcefire 3D System require this direct connection, and others support use of a proxy server. Additionally, the system requires that certain ports remain open for basic intra-appliance communication, as well as to allow you to access appliances' web interfaces. By default, several other ports are open to allow the system to take advantage of additional features and functionality.

For more information, see:

- Internet Access Requirements on page 23
- Open Communication Ports Requirements on page 24

Internet Access Requirements

By default, Sourcefire appliances are configured to directly connect to the Internet. Specific features of the Sourcefire 3D System require this direct connection, while others support use of a proxy server; see the Configuring s chapter in the *Sourcefire 3D System User Guide*.

TIP! You can manually upload system software, intrusion rule, GeoDB, and VDB updates to appliances.

To ensure continuity of operations, both Defense Centers in a high availability pair must have Internet access. For specific features, the primary Defense Center contacts the Internet, then shares information with the secondary during the synchronization process. Therefore, if the primary fails, you should promote the secondary to primary as described in the Managing Devices chapter in the *Sourcefire 3D System User Guide*.

The following table describes the Internet access requirements of the Sourcefire 3D System.

Sourcefire 3D System Internet Access Requirements

For...	Internet access is required to...	High Availability Considerations	Proxy?
RSS Feed dashboard widget	download RSS feed data from an external source, including Sourcefire.	Feed data is not synchronized.	✓
Security Intelligence feeds	download Security Intelligence feed data from an external source, including the Sourcefire Intelligence Feed.	The primary Defense Center downloads feed data and shares it with the secondary. In case of primary failure, you must switch roles.	✓
URL filtering data	download cloud-based URL category and reputation data for access control, and perform lookups for uncategorized URLs.	The primary Defense Center downloads URL filtering data and shares it with the secondary. In case of primary failure, you must switch roles.	✓
malware cloud lookups (Malware licensed)	perform cloud lookups to determine if files detected in network traffic contain malware.	Paired Defense Centers perform cloud lookups independently, although file policies are synchronized.	
FireAMP integration (FireAMP subscription)	receive endpoint-based malware events from the Sourcefire cloud.	Cloud connections are not synchronized. Configure them on both Defense Centers.	
system, intrusion rule, GeoDB, and VDB updates	download or schedule the download of an intrusion rule, GeoDB, VDB, or system update directly to the appliance.	Rule, GeoDB, and VDB updates are synchronized; system updates are not. All appliances that download updates must have Internet access.	✓
obtaining whois information using the IP address context menu	obtain whois information.	Any appliance requesting whois information must have Internet access.	✓

Open Communication Ports Requirements

The Sourcefire 3D System requires that ports 443 (inbound) and 8305 (inbound and outbound) remain open for basic intra-appliance communication, as well as to allow you to access appliances' web interfaces.

By default, several other ports are open to allow the system to take advantage of additional features and functionality. The following table lists these ports. Note that DHCP is disabled by default on ports 67 and 68.

Sourcefire 3D System Open Communication Ports Requirements

Ports	Description	Protocol	Direction	Open the port to...
22	SSH/SSL	TCP	Bidirectional	allow a secure remote connection to the appliance.
25	SMTP	TCP	Outbound	send email notices and alerts from the appliance.
53	DNS	TCP	Outbound	use DNS.
67, 68	DHCP	UDP	Outbound	use DHCP. **Disabled by default.**
80	HTTP	TCP	Outbound or Bidirectional	allow the RSS Feed dashboard widget to connect to a remote web server; use for auto-update. Adding inbound access allows the Defense Center to update custom and third-party Security Intelligence feeds via HTTP, and to download URL filtering information.
161, 162	SNMP	UDP	Bidirectional (161); Outbound (162)	provide access if you enabled SNMP polling (inbound) and SNMP traps (outbound).
389, 636	LDAP	TCP	Outbound	track user activity and for authentication.
443	HTTPS/AMPQ	TCP	Inbound or Bidirectional	access the appliance. **Required.** Adding outbound access allows the Defense Center to download or receive software updates, VDB and GeoDB updates, URL filtering information, secure Security Intelligence feeds, and endpoint-based (FireAMP) malware events.
514	syslog	UDP	Outbound	send alerts to a remote syslog server.
623	SOL/LOM	UDP	Bidirectional	allow you to perform Lights-Out Management (LOM) using a Serial Over LAN (SOL) connection on a Series 3 appliance.

Sourcefire 3D System Open Communication Ports Requirements (Continued)

Ports	Description	Protocol	Direction	Open the port to...
1500, 2000	database access	TCP	Inbound	access the Defense Center if external database access is enabled.
1812, 1813	RADIUS	UDP	Outbound or Bidirectional	use RADIUS. Adding inbound access ensures that RADIUS authentication and accounting function correctly. Ports 1812 and 1813 are the default, but you can configure RADIUS to use other ports instead. For more information, see the *Sourcefire 3D System User Guide*.
3306	Sourcefire User Agent	TCP	Inbound	allow communication between the Defense Center and Sourcefire User Agents.
8302	eStreamer	TCP	Bidirectional	use for an eStreamer client.
8305	device management	TCP	Bidirectional	communicate between the Defense Center and managed devices. **Required**.
8307	Host Input Client API	TCP	Bidirectional	communicate with the Defense Center during client/server authentication.
32137	malware cloud lookups	TCP	Outbound	allow the Defense Center to perform cloud lookups to determine if a file detected in network traffic contains malware, and to track file trajectories.

CHAPTER 2
UNDERSTANDING DEPLOYMENT

The Sourcefire 3D System can be deployed to accommodate the needs of each unique network architecture. The Defense Center provides a centralized management console and database repository for the Sourcefire 3D System. Devices are installed on network segments to collect traffic connections for analysis.

Devices in a passive deployment monitor traffic flowing across a network using a switch SPAN, virtual switch, or mirror port to collect data about the nature of the traffic traversing your network. Devices in an inline deployment allow you to monitor your network for attacks that might affect the availability, integrity, or confidentiality of hosts on the network. A device can be deployed in an inline, switched, routed, or hybrid (Layer 2/Layer3) environment.

To learn more about your deployment options, see the following sections for more information:

- Understanding Deployment Options on page 28 provides some factors to consider when designing your deployment.
- Understanding Interfaces on page 28 explains the different between interfaces and how they function in your deployment.
- Connecting Devices to Your Network on page 32 describes how to use a hub, span, and network tap in your deployment.
- Deployment Options on page 36 describes a basic deployment and identifies the primary functional locations within it.
- Deploying with Access Control on page 43 describes the advantages of using access control in an inline deployment.

- Using a Multi-Port Managed Device on page 48 explains how to use a managed device for multiple networks or for use as a virtual router or virtual switch in your network deployment.
- Complex Network Deployments on page 50 explains advanced deployment scenarios, such as using a VPN or having multiple entry points.

For additional information about deployments, consult the *Best Practices Guide*, available from the Sourcefire sales department.

Understanding Deployment Options

Your deployment decisions will be based on a variety of factors. Answering these questions can help you understand the vulnerable areas of your network and clarify your intrusion detection and prevention needs:

- Will you be deploying your managed device with passive or inline interfaces? Does your device support a mix of interfaces, some passive and others inline? See Understanding Interfaces on page 28 for more information.
- How will you connect the managed devices to the network? Hubs? Taps? Spanning ports on switches? Virtual switches? See Connecting Devices to Your Network on page 32 for more information.
- Do you want to detect every attack on your network, or do you only want to know about attacks that penetrate your firewall? Do you have specific assets on your network such as financial, accounting, or personnel records, production code, or other sensitive, protected information that require special security policies? See Deployment Options on page 36 for more information.
- Do you provide VPN or modem access for remote workers? Do you have remote offices that also require an IPS deployment? Do you employ contractors or other temporary employees? Are they restricted to specific network segments? Do you integrate your network with the networks of other organizations such as customers, suppliers, or business partners? See Complex Network Deployments on page 50 for more information.

Understanding Interfaces

The sections that follow describe how different interfaces affect the capabilities of the Sourcefire 3D System. In addition to passive and inline interfaces, you can

also have routed, switched, and hybrid interfaces. See the following sections for more information:

- Passive Interfaces on page 29
- Inline Interfaces on page 29
- Switched Interfaces on page 30
- Routed Interfaces on page 31
- Hybrid Interfaces on page 32

Passive Interfaces

LICENSE: Any
SUPPORTED DEVICES: Any

You can configure a passive IPS deployment to monitor traffic flowing across a network using a switch SPAN, virtual switch, or mirror port, allowing traffic to be copied from other ports on the switch. Passive interfaces allow you to inspect traffic within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and do not retransmit received traffic.

You can configure one or more physical ports on a managed device as passive interfaces. For more information, see Connecting Devices to Your Network on page 32.

Inline Interfaces

LICENSE: Any
SUPPORTED DEVICES: Any

You configure an inline IPS deployment transparently on a network segment by binding two ports together. Inline interfaces allow you to install a device in any network configuration without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, then retransmit all traffic received on these interfaces except traffic explicitly dropped.

You can configure one or more physical ports on a managed device as inline interfaces. You must assign a pair of inline interfaces to an inline set before they can handle traffic in an inline deployment.

IMPORTANT! If you configure an interface as an inline interface, the adjacent port on its NetMod automatically becomes an inline interface as well to complete the pair.

Configurable bypass inline sets allow you to select how your traffic is handled if your hardware fails completely (for example, the device loses power). You may determine that connectivity is critical on one network segment, and, on another

network segment, you cannot permit uninspected traffic. Using configurable bypass inline sets, you can manage the traffic flow of your network traffic in one of the following ways:

- *Bypass*: an interface pair configured for bypass allows all traffic to flow if the device fails. The traffic bypasses the device and any inspection or other processing by the device. Bypass allows uninspected traffic across the network segment, but ensures that the network connectivity is maintained.
- *Non-bypass*: an interface pair configured for non-bypass stops all traffic if the device fails. Traffic that reaches the failed device does not enter the device. Non-bypass does not permit traffic to pass uninspected, but the network segment loses connectivity if the device fails. Use non-bypass interfaces in deployment situations where network security is more important than loss of traffic.

Configure the inline set as bypass to ensure that traffic continues to flow if your device fails. Configure the inline set as non-bypass to stop traffic if the device fails. Note that reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process on page 199.

All appliances can contain configurable bypass interfaces. The 8000 Series appliances can also contain NetMods with interfaces that cannot be configured for bypass. For more information on NetMods, see 8000 Series Modules on page 185.

Advanced options vary by appliance and can include tap mode, propagate link state, transparent inline mode, and strict TCP mode. For information on how to configure your inline interface sets, see Configuring Inline Sets in the *Sourcefire 3D System User Guide*. For more information on using inline interfaces, see Connecting Devices to Your Network on page 32.

Switched Interfaces

LICENSE: Control
SUPPORTED DEVICES: Series 3

You can configure switched interfaces on a managed device in a Layer 2 deployment to provide packet switching between two or more networks. You can also configure virtual switches on managed devices to operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets.

Switched interfaces can have either a physical or logical configuration:

- *Physical switched interfaces* are physical interfaces with switching configured. Use physical switched interfaces to handle untagged VLAN traffic.
- *Logical switched interfaces* are an association between a physical interface and a VLAN tag. Use logical interfaces to handle traffic with designated VLAN tags.

Virtual switches can operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets. When you configure a virtual switch, the switch initially broadcasts packets through every available port on the switch. Over time, the switch uses tagged return traffic to learn which hosts reside on the networks connected to each port.

You can configure your device as a virtual switch and use the remaining interfaces to connect to network segments you want to monitor. To use a virtual switch on your device, create physical switched interfaces and then follow the instructions for Setting Up Virtual Switches in the *Sourcefire 3D System Guide*.

Routed Interfaces

LICENSE: Control
SUPPORTED DEVICES: Series 3

You can configure routed interfaces on a managed device in a Layer 3 deployment so that it routes traffic between two or more interfaces. You must assign an IP address to each interface and assign the interfaces to a virtual router to route traffic.

You can configure routed interfaces for use with a gateway virtual private network (gateway VPN) or with network address translation (NAT). For more information, see Deploying a Gateway VPN on page 41 and Deploying with Policy-Based NAT on page 42.

You can also configure the system to route packets by making packet forwarding decisions according to the destination address. Interfaces configured as routed interfaces receive and forward the Layer 3 traffic. Routers obtain the destination from the outgoing interface based on the forwarding criteria, and access control rules designate the security policies to be applied.

Routed interfaces can have either a physical or logical configuration:

- *Physical routed interfaces* are physical interfaces with routing configured. Uses physical routed interfaces to handle untagged VLAN traffic.
- *Logical switched interfaces* are an association between a physical interface and a VLAN tag. Use logical interfaces to handle traffic with designated VLAN tags.

To use routed interfaces in a Layer 3 deployment, you must configure virtual routers and assign routed interfaces to them. A virtual router is a group of routed interfaces that route Layer 3 traffic.

You can configure your device as a virtual router and use the remaining interfaces to connect to network segments you want to monitor. You can also enable strict TCP enforcement for maximum TCP security. To use a virtual router on your device, create physical routed interfaces on your device and then follow the instructions for Setting Up Virtual Routers in the *Sourcefire 3D System User Guide*.

Hybrid Interfaces

LICENSE: Control
SUPPORTED DEVICES: Series 3

You can configure logical hybrid interfaces on managed devices that allow the Sourcefire 3D System to bridge traffic between virtual routers and virtual switches. If IP traffic received on interfaces in a virtual switch is addressed to the MAC address of an associated hybrid logical interface, the system handles it as Layer 3 traffic and either routes or responds to the traffic depending on the destination IP address. If the system receives any other traffic, it handles it as Layer 2 traffic and switches it appropriately.

To create a hybrid interface, you first configure a virtual switch and virtual router, then add the virtual switch and virtual router to the hybrid interface. A hybrid interface that is not associated with both a virtual switch and a virtual router is not available for routing, and does not generate or respond to traffic.

You can configure hybrid interfaces with network address translation (NAT) to pass traffic between networks. For more information, see Deploying with Policy-Based NAT on page 42.

If you want to use hybrid interfaces on your device, define a hybrid interface on the device and then follow the instructions for Setting Up Hybrid Interfaces in the *Sourcefire 3D System User Guide*.

Connecting Devices to Your Network

You can connect your managed devices to your network in several ways. Configure a hub or network tap using either passive or inline interfaces, or a span port using passive interfaces. The following sections describe supported connection methods and cabling considerations:

Using a Hub

An Ethernet hub is a simple way to ensure that the managed device can see all the traffic on a network segment. Most hubs of this type take the IP traffic meant for any of the hosts on the segment and broadcast it to all the devices connected to the hub. Connect the interface set to the hub to monitor all incoming and outgoing traffic on the segment. Using a hub does not guarantee that the detection engine sees every packet on a higher volume network because of the potential of packet collision. For a simple network with low traffic, this is not likely to be a problem. In a high-traffic network, a different option may provide better results. Note that if the hub fails or loses power, the network connection is broken. In a simple network, the network would be down.

Some devices are marketed as hubs but actually function as switches and do not broadcast each packet to every port. If you attach your managed device to a hub, but do not see all the traffic, you may need to purchase a different hub or use a switch with a Span port.

Using a Span Port

Many network switches include a span port that mirrors traffic from one or more ports. By connecting an interface set to the span port, you can monitor the combined traffic from all ports, generally both incoming and outgoing. If you already have a switch that includes this feature on your network, in the proper location, then you can deploy the detection on multiple segments with little extra equipment cost beyond the cost of the managed device. In high-traffic networks, this solution has its limitations. If the span port can handle 200Mbps and each of three mirrored ports can handle up to 100Mbps, then the span port is likely to become oversubscribed and drop packets, lowering the effectiveness of the managed device.

Using a Network Tap

Network taps allow you to passively monitor traffic without interrupting the network flow or changing the network topology. Taps are readily available for different bandwidths and allow you to analyze both incoming and outgoing packets on a network segment. Because you can monitor only a single network segment with most taps, they are not a good solution if you want to monitor the traffic on two of the eight ports on a switch. Instead, you would install the tap between the router and the switch and access the full IP stream to the switch.

By design, network taps divide incoming and outgoing traffic into two different streams over two different cables. Managed devices offer multi-port options that recombine the two sides of the conversation so that the entire traffic stream is evaluated by the decoders, the preprocessors, and the detection engine.

Cabling Inline Deployments on Copper Interfaces

If you deploy your device inline on your network and you want to use your device's bypass capabilities to maintain network connectivity if the device fails, you must pay special attention to how you cable the connections.

If you deploy a device with fiber bypass capable interfaces, there are no special cabling issues beyond ensuring that the connections are securely fastened and the cables are not kinked. However, if you are deploying devices with copper rather than fiber network interfaces, then you must be aware of the device model that you are using, because different device models use different network cards. Note that some 8000 Series NetMods do not allow bypass configuration.

The network interface cards (NICs) in the device support a feature called Auto-Medium Dependent Interface Crossover (Auto-MDI-X), which allows network interfaces to configure automatically whether you use a straight-through or crossover Ethernet cable to connect to another network device. The Devices and Bypass Characteristics table lists the various devices and whether they bypass as straight-through or crossover connections.

Devices and Bypass Characteristics

DEVICE	FAILS OPEN AS...
3D500/1000/2000	straight-through
7000 Series	crossover
8000 Series	crossover

For a managed device that bypasses with a straight-through connection, wire the device as would normally be done with the device live on the network. In most cases you should use one straight-through cable and one crossover cable to connect the device to the two endpoints.

Straight-Through Bypass Connection Cabling

For a managed device that bypasses with a crossover connection, wire the device as would normally be done without a device deployed. The link should work with power to the device removed. In most cases you should use two straight-through cables to connect the device to the two endpoints.

Crossover Bypass Connection Cabling

The Valid Configurations for Hardware Bypass and table indicates where you should use crossover or straight-through cables in your hardware bypass configurations. Note that a Layer 2 port functions as a straight-through (MDI) endpoint in the deployment, and a Layer 3 port functions as a crossover (MDIX) endpoint in the deployment. The total crossovers (cables and appliances) should be an odd number for bypass to function properly.

Valid Configurations for Hardware Bypass

Endpoint 1	Cable	Managed Device	Cable	Endpoint 2
MDIX	=	=	=	MDI
MDI	X	=	=	MDI
MDI	=	=	X	MDI
MDI	=	=	=	MDIX
MDIX	=	X	=	MDIX
MDI	=	X	=	MDI
MDI	X	X	X	MDI
MDIX	X	X	=	MDI

IMPORTANT! In the Valid Configurations for Hardware Bypass table, = indicates a straight-through cable or managed device bypass connection, and X indicates a crossover cable or managed device bypass connection.

Note that every network environment is likely to be unique, with endpoints that have different combinations of support for Auto-MDI-X. The easiest way to

confirm that you are installing your device with the correct cabling is to begin by connecting the device to its two endpoints using one crossover cable and one straight-through cable, but with the device powered down. Ensure that the two endpoints can communicate. If they cannot communicate, then one of the cables is the incorrect type. Switch one (and only one) of the cables to the other type, either straight-through or crossover.

After the two endpoints can successfully communicate with the inline device powered down, power up the device. The Auto-MDI-X feature ensures that the two endpoints will continue to communicate. Note that if you have to replace an inline device, you should repeat the process of ensuring that the endpoints can communicate with the new device powered down to protect against the case where the original device and its replacement have different bypass characteristics.

The Auto-MDI-X setting functions correctly only if you allow the network interfaces to auto-negotiate. If your network environment requires that you turn off the Auto Negotiate option on the Network Interface page, then you must specify the correct MDI/MDIX option for your inline network interfaces. See Configuring Inline Interfaces in the *Sourcefire 3D System User Guide* for more information.

Special Cases

Connecting 8000 Series Devices

8000 Series managed devices do not support half duplex network links; they also do not support differences in speed or duplex configurations at opposite ends of a connection. To ensure a stable network link, you must either auto-negotiate on both sides of the connection, or set both sides to the same static speed.

Changing Your Remote Console

When you change your remote console from Physical Serial Port to Lights-Out Management or from Lights-Out Management to Physical Serial Port on 70xx Family devices, you may have to reboot the appliance twice to see the expected LILO boot prompt.

TIP! 3D2100/2500/3500/4500 devices do not have functional serial ports.

Deployment Options

When you place your managed device on a network segment, you can monitor traffic using an intrusion detection system or protect your network from threats using an intrusion prevention system.

You can also deploy your managed device to function as a virtual switch, virtual router, or gateway VPN. Additionally, you can use policies to route traffic or control access to traffic on your network. For more information, see the following sections:

- Deploying with a Virtual Switch on page 37
- Deploying with a Virtual Router on page 38
- Deploying with Hybrid Interfaces on page 40
- Deploying a Gateway VPN on page 41
- Deploying with Policy-Based NAT on page 42
- Deploying with Access Control on page 43

Deploying with a Virtual Switch

LICENSE: Control
SUPPORTED DEVICES: Series 3

You can create a *virtual switch* on your managed device by configuring inline interfaces as switched interfaces. The virtual switch provides Layer 2 packet switching for your deployment. Advanced options include setting a static MAC address, enabling spanning tree protocol, enabling strict TCP enforcement, and dropping bridge protocol data units (BPDUs) at the domain level. For information on switched interfaces, see Switched Interfaces on page 30.

A virtual switch must contain two or more switched interfaces to handle traffic. For each virtual switch, the system switches traffic only to the set of ports configured as switched interfaces. For example, if you configure a virtual switch with four switched interfaces, when the system receives traffic packets through one port it only broadcasts these packets to the remaining three ports on the switch.

To configure a virtual switch to allow traffic, you configure two or more switched interfaces on a physical port, add and configure a virtual switch, and then assign the virtual switch to the switched interfaces. The system drops any traffic received on an external physical interface that does not have a switched interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical switched interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical switched interface, it also drops the packet.

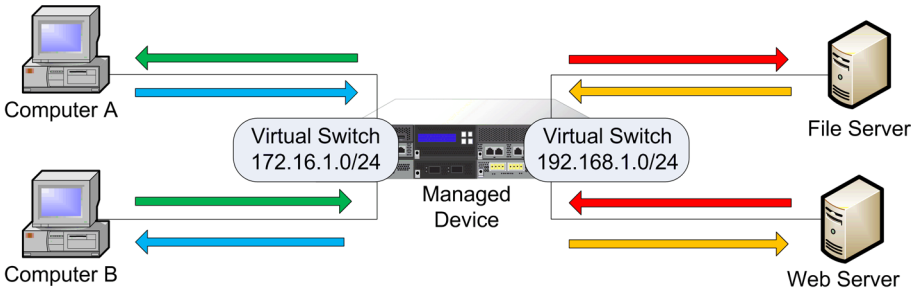
You can define additional logical switched interfaces on the physical port as needed, but you must assign a logical switched interface to a virtual switch to handle traffic.

Virtual switches have the advantage of scalability. When you use a physical switch, you are limited by the number of available ports on the switch. When you replace your physical switch with a virtual switch, you are limited only by your bandwidth and the level of complexity you want to introduce to your deployment.

Use a virtual switch where you would use a Layer 2 switch, such as workgroup connectivity and network segmentation. Layer 2 switches are particularly effective where workers spend most of their time on their local segment. Larger deployments (for example, deployments that contain broadcast traffic, Voice-over-IP, or multiple networks) can use virtual switches on smaller network segments of the deployment.

When you deploy multiple virtual switches on the same managed device, you can maintain separate levels of security as dictated by the needs of each network.

Virtual Switches on a Managed Device



In this example, the managed device monitors traffic from two separate networks, 172.16.1.0/20 and 192.168.1.0/24. Although both networks are monitored by the same managed device, the virtual switch passes traffic only to those computers or servers on the same network. Traffic can pass from computer A to computer B through the 172.16.1.0/24 virtual switch (indicated by the blue line) and from computer B to computer A through the same virtual switch (indicated by the green line). Similarly, traffic can pass to and from the file and web servers through the 192.168.1.0/24 virtual switch (indicated by the red and orange lines). However, traffic cannot pass between the computers and the web or file servers because the computers are not on the same virtual switch as the servers.

For more information on configuring switched interfaces and virtual switches, see Setting Up Virtual Switches in the *Sourcefire 3D System User Guide*.

Deploying with a Virtual Router

LICENSE: Control
SUPPORTED DEVICES: Series 3

You can create a *virtual router* on a managed device to route traffic between two or more networks, or to connect a private network to a public network (for example, the Internet). The virtual router connects two routed interfaces to provide Layer 3 packet forwarding decisions for your deployment according to the destination address. Optionally, you can enable strict TCP enforcement on the virtual router. For more information on routed interfaces, see Routed Interfaces on page 31. You must use a virtual router with a gateway VPN. For more information, see Deploying a Gateway VPN on page 41.

A virtual router can contain either physical or logical routed configurations from one or more individual devices within the same broadcast domain. You must associate each logical interface with a VLAN tag to handle traffic received by the physical interface with that specific tag. You must assign a logical routed interface to a virtual router to route traffic.

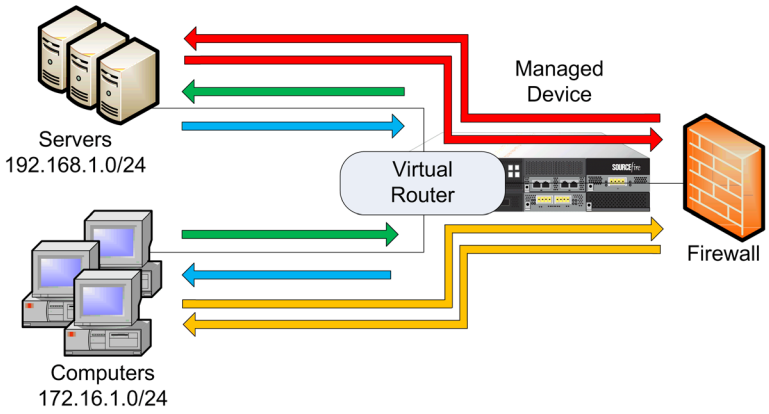
To configure a virtual router, you set up routed interfaces with either physical or logical configurations. You can configure physical routed interfaces for handling untagged VLAN traffic. You can also create logical routed interfaces for handling traffic with designated VLAN tags. The system drops any traffic received on an external physical interface that does not have a routed interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical routed interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical routed interface, it also drops the packet.

Virtual routers have the advantage of scalability. Where physical routers limit the number of networks you can connect, multiple virtual routers can be configured on the same managed device. Putting multiple routers on the same device reduces the physical complexity of your deployment, allowing you to monitor and manage multiple routers from one device.

Use a virtual router where you would use a Layer 3 physical router to forward traffic between multiple networks in your deployment, or to connect your private network to a public network. Virtual routers are particularly effective in large deployments where you have many networks or network segments with different security requirements.

When you deploy a virtual routers on your managed device, you can use one appliance to connect multiple networks to each other, and to the Internet.

Virtual Routers on a Managed Device



In this example, the managed device contains a virtual router to allow traffic to travel between the computers on network 172.16.1.0/20 and the servers on network 192.168.1.0/24 (indicated by the blue and green lines). A third interface

on the virtual router allows traffic from each network to pass to the firewall and back (indicated by the red and orange lines).

For more information, see Setting Up Virtual Routers in the *Sourcefire 3D System User Guide*.

Deploying with Hybrid Interfaces

LICENSE: Control
SUPPORTED DEVICES: Series 3

You can create a *hybrid interface* on a managed device to route traffic between Layer 2 and Layer 3 networks using a virtual switch and a virtual router. This provides one interface that can both route local traffic on the switch and route traffic to and from an external network. For best results, configure policy-based NAT on the interface to provide network address translation on the hybrid interface. See Deploying with Policy-Based NAT on page 42.

A hybrid interface must contain one or more switched interfaces and one or more routed interfaces. A common deployment consists of two switched interfaces configured as a virtual switch to pass traffic on a local network and virtual routers to route traffic to networks, either private or public.

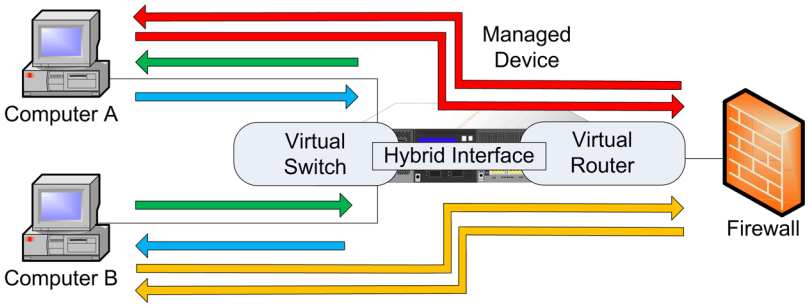
To create a hybrid interface, you first configure a virtual switch and virtual router, then add the virtual switch and virtual router to the hybrid interface. A hybrid interface that is not associated with both a virtual switch and a virtual router is not available for routing, and does not generate or respond to traffic.

Hybrid interfaces have the advantage of compactness and scalability. Using a single hybrid interface combines both Layer 2 and Layer 3 traffic routing functions in a single interface, reducing the number of physical appliances in the deployment and providing a single management interface for the traffic.

Use a hybrid interface where you need both Layer 2 and Layer 3 routing functions. This deployment can be ideal for small segments of your deployment where you have limited space and resources.

When you deploy a hybrid interface, you can allow traffic to pass from your local network to an external or public network, such as the Internet, while addressing separate security considerations for the virtual switch and virtual router in the hybrid interface.

Hybrid Interface on a Managed Device



In this example, computer A and computer B are on the same network and communicate using a Layer 2 virtual switch configured on the managed device (indicated by the blue and green lines). A virtual router configured on the managed device provides Layer 3 access to the firewall. A hybrid interface combines the Layer 2 and Layer 3 capabilities of the virtual switch and virtual router to allow traffic to pass from each computer through the hybrid interface to the firewall (indicated by the red and orange lines).

For more information, see Setting Up Hybrid Interfaces in the *Sourcefire 3D System User Guide*.

Deploying a Gateway VPN

LICENSE: VPN
SUPPORTED DEVICES: Series 3

You can create a *gateway virtual private network* (gateway VPN) connection to establish a secure tunnel between a local gateway and a remote gateway. The secure tunnel between the gateways protects communication between them.

You configure the Sourcefire 3D System to build secure VPN tunnels from the virtual routers of Sourcefire managed devices to remote devices or other third-party VPN endpoints using the Internet Protocol Security (IPSec) protocol suite. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. The VPN endpoints authenticate each other with either the Internet Key Exchange (IKE) version 1 or version 2 protocol to create a security association for the tunnel. The system runs in either IPSec authentication header (AH) mode or the IPSec encapsulating security payload (ESP) mode. Both AH and ESP provide authentication, and ESP also provides encryption.

A gateway VPN can be used in a point-to-point, star, or mesh deployment:

- Point-to-point deployments connect two endpoints with each other in a direct one-to-one relationship. Both endpoints are configured as peer devices, and either device can initiate the secured connection. At least one device must be a VPN-enabled managed device.

  Use a point-to-point deployment to maintain your network security when a host at a remote location uses public networks to connect to a host in your network.

- Star deployments establish a secure connection between a hub and multiple remote endpoints (leaf nodes). Each connection between the hub node and an individual leaf node is a separate VPN tunnel. Typically, the hub node is the VPN-enabled managed device, located at the main office. Leaf nodes are located at branch offices and initiate most of the traffic.

  Use a star deployment to connect an organization's main and branch office locations using secure connections over the Internet or other third-party network to provide all employees with controlled access to the organization's network.

- Mesh deployments connect all endpoints together by means of VPN tunnels. This offers redundancy in that when one endpoint fails, the remaining endpoints can still communicate with each other.

  Use a mesh deployment to connect a group of decentralized branch office locations to ensure that traffic can travel even if one or more VPN tunnels fails. The number of VPN-enabled managed devices you deploy in this configuration controls the level of redundancy.

For more information on gateway VPN configuration and deployments, see Gateway VPN in the *Sourcefire 3D System User Guide*.

Deploying with Policy-Based NAT

License: Control
Supported Devices: Any

You can use *policy-based network address translation* (NAT) to define policies that specify how you want to perform NAT. You can target your policies to a single interface, one or more devices, or entire networks.

You can configure static (one-to-one) or dynamic (one-to-many) translation. Note that dynamic translations are order-dependent where rules are searched in order until the first matching rule applies.

Policy-based NAT typically operates in the following deployments:

- Hide your private network address.

  When you access a public network from your private network, NAT translates your private network address to your public network address. Your specific private network address is hidden from the public network.

- Allow access to a private network service.

  When a public network accesses your private network, NAT translates your public address to your private network address. The public network can access your specific private network address.

- Redirect traffic between multiple private networks.

  When a server on a private network accesses a server on a connected private network, NAT translates the private addresses between the two private networks to ensure there is no duplication in private addresses and traffic can travel between them.

Using policy-based NAT removes the need for additional hardware and consolidates the configuration of your intrusion detection or prevention system and NAT into a single user interface. For more information, see Using NAT Policies in the *Sourcefire 3D System User Guide*.

Deploying with Access Control

LICENSE: Any
SUPPORTED DEVICES: Any

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can enter, exit, or travel within your network. The following section describes how access control can function in your deployment. See the *Sourcefire 3D System User Guide* for more information on this feature.

An access control policy determines how the system handles traffic on your network. You can add access control rules to your policy to provide more granular control over how you handle and log network traffic.

An access control policy that does not include access control rules uses one of the following default actions to handle traffic:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection
- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only
- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

Access control rules further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule action, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

Access control can filter traffic based on Security Intelligence data, a feature that allows you to specify the traffic that can traverse your network, per access control policy, based on the source or destination IP address. This feature can create a blacklist of disallowed IP addresses whose traffic is blocked and not inspected.

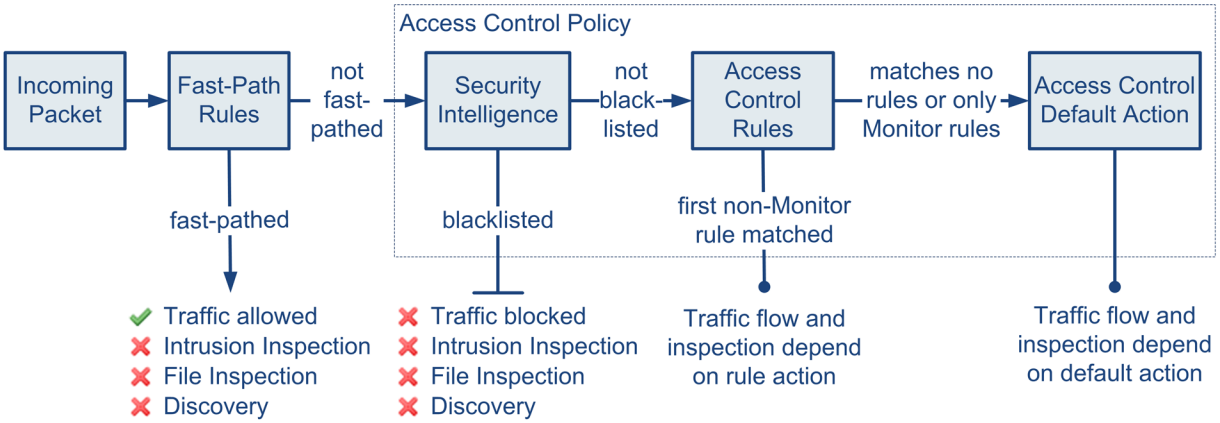
The sample deployment illustrates common network segments. Deploying your managed devices in each of these locations serves different purposes. The following sections describe typical location recommendations:

- Inside the Firewall on page 44 explains how access control functions on traffic that passes through the firewall.
- On the DMZ on page 45 explains how access control within the DMZ can protect outward-facing servers.
- On the Internal Network on page 46 explains how access control can protect your internal network from intentional or accidental attack.
- On the Core Network on page 46 explains how an access control policy with strict rules can protect your critical assets.
- On a Remote or Mobile Network on page 47 explains how access control can monitor and protect the network from traffic at remote locations or on mobile devices.

Inside the Firewall

Managed devices inside the firewall monitor inbound traffic allowed by the firewall or traffic that passes the firewall due to misconfiguration. Common network segments include the DMZ, the internal network, the core, mobile access, and remote networks.

The diagram below illustrates traffic flow through the Sourcefire 3D System, and provide some details on the types of inspection performed on that traffic. Note that the system does not inspect fast-pathed or blacklisted traffic. For traffic handled by an access control rule or default action, flow and inspection depend on the rule action. Although rule actions are not shown in the diagram for simplicity, the system does not perform any kind of inspection on trusted or blocked traffic. Additionally, file inspection is not supported with the default action.



An incoming packet is first checked against any fast-path rules. If there is a match, the traffic is fast-pathed. If there is no match, Security Intelligence-based filtering determines if the packet is blacklisted. If not, any access control rules are applied.

If the packet meets the conditions of a rule, traffic flow and inspection depend on the rule action. If no rules match the packet, traffic flow and inspection depend on the default policy action. (An exception occurs with Monitor rules, which allow traffic to continue to be evaluated.) The default action on each access control policy manages traffic that has not been fast-pathed or blacklisted, or matched by any non-Monitor rule. Note that fast-path is available only for 8000 Series and 3D9900 devices.

You can create access control rules to provide more granular control over how you handle and log network traffic. For each rule, you specify an action (trust, monitor, block, or inspect) to apply to traffic that meets specific criteria.

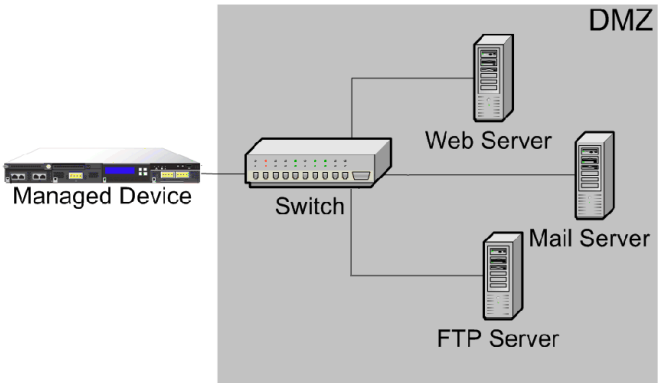
On the DMZ

The DMZ contains outward-facing servers (for example, web, FTP, DNS, and mail), and may also provide services such as mail relay and web proxy to users on the internal network.

Content stored in the DMZ is static, and changes are planned and executed with clear communication and advance notice. Attacks in this segment are typically inbound and become immediately apparent because only planned changes should occur on the servers in the DMZ. An effective access control policy for this segment tightly controls access to services and searches for any new network events.

Servers in the DMZ can contain a database that the DMZ can query via the network. Like the DMZ, there should be no unexpected changes, but the database content is more sensitive and requires greater protection than a web site or other DMZ service. A strong intrusion policy, in addition to the DMZ access control policy, is an effective strategy.

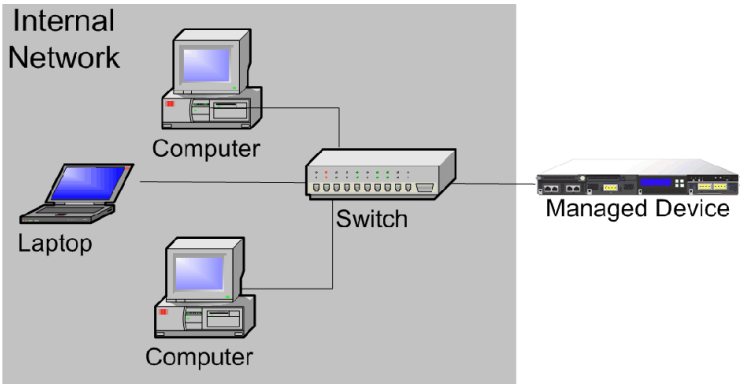
A managed device deployed on this segment can detect attacks directed to the Internet that originate from a compromised server in the DMZ. Monitoring network traffic using Network Discovery can help you monitor these exposed servers for changes (for example, an unexpected service suddenly appearing) that could indicate a compromised server in the DMZ.



On the Internal Network

A malicious attack can originate from a computer on your internal network. This can be a deliberate act (for example, an unknown computer appears unexpectedly on your network), or an accidental infection (for example, a work laptop infected off-site is connected to the network and spreads a virus). Risk on the internal network can also be outbound (for example, a computer sends information to a suspicious external IP address).

This dynamic network requires a strict access control policy for all internal traffic in addition to outbound traffic. Add access control rules to tightly control traffic between users and applications.

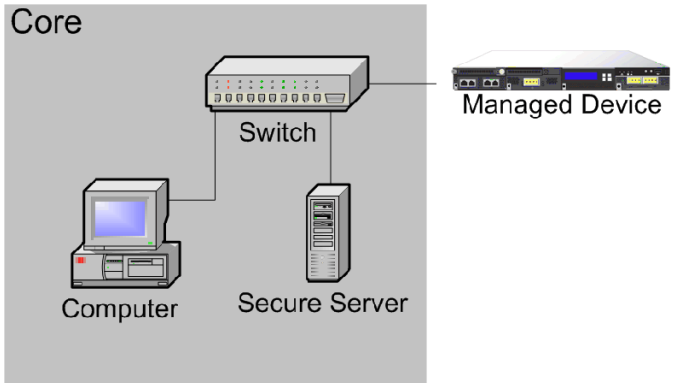


On the Core Network

Core assets are those assets critical to the success of your business and must be protected at all cost. Although core assets vary depending on the nature of your business, typical core assets include financial and management centers or intellectual property repositories. If the security on the core assets is breached, your business can be destroyed.

Although this segment must be readily available for your business to function, it must be tightly restricted controlled. Access control should ensure that these assets cannot be reached by those network segments with the highest risk, such

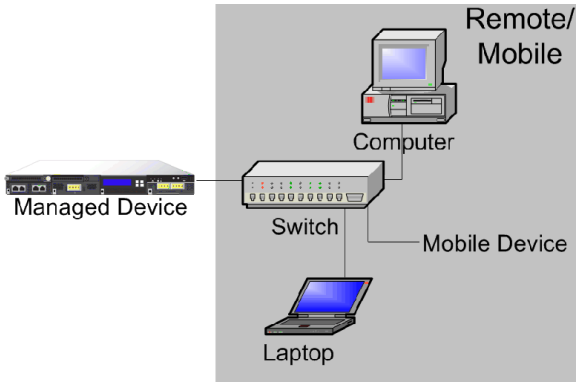
as remote networks or mobile devices. Always use the most aggressive control on this segment, with strict rules for user and application access.



On a Remote or Mobile Network

Remote networks, located off-site, often use a virtual private network (VPN) to provide access to the primary network. Mobile devices and the use of personal devices for business purposes (for example, using a "smart phone" to access corporate email) are becoming increasingly common.

These networks can be highly dynamic environments with rapid and continual change. Deploying a managed device on a dedicated mobile or remote network allows you to create a strict access control policy to monitor and manage traffic to and from unknown external sources. Your policy can reduce your risk by rigidly limiting how users, network, and applications access core resources.



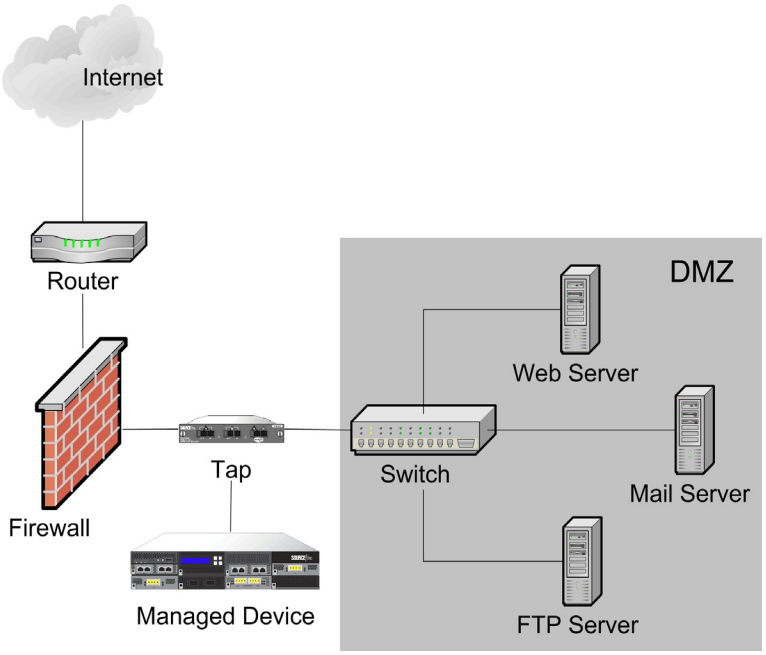
Using a Multi-Port Managed Device

The managed device offers multiple sensing ports on its network modules. You can use the multi-port managed devices to:

- recombine the separate connections from a network tap
- capture and evaluate traffic from different networks
- perform as a virtual router
- perform as a virtual switch

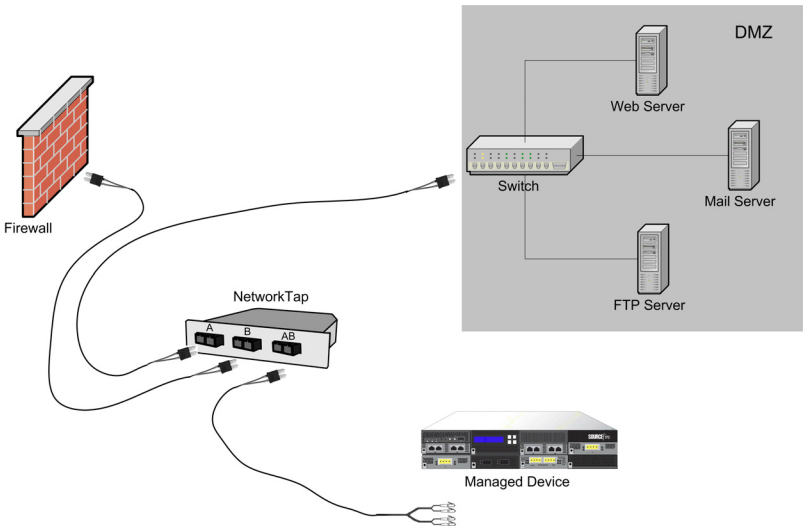
IMPORTANT! Although each port is capable of receiving the full throughput for which the device is rated, the total traffic on the managed device cannot exceed its bandwidth rating without some packet loss.

Deploying a multi-port managed device with a network tap is a straightforward process. The following diagram shows a network tap installed on a high-traffic network segment.

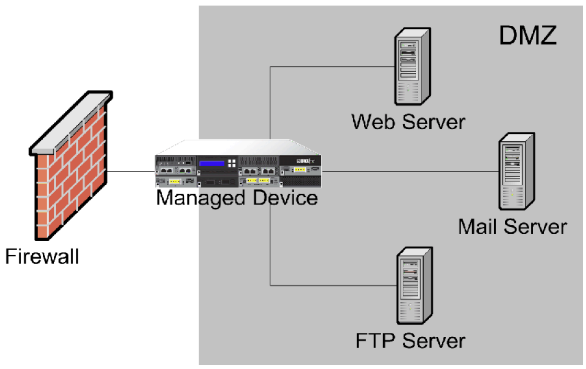


In this scenario, the tap transmits incoming and outgoing traffic through separate ports. When you connect the multi-port adapter card on the managed device to the tap, the managed device is able to combine the traffic into a single data stream so that it can be analyzed.

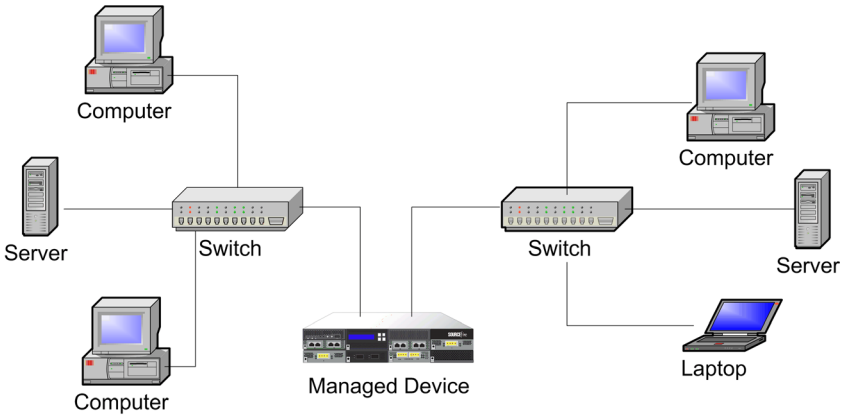
Note that with a gigabit optical tap, as shown in the illustration below, both sets of ports on the managed device are used by the connectors from the tap.



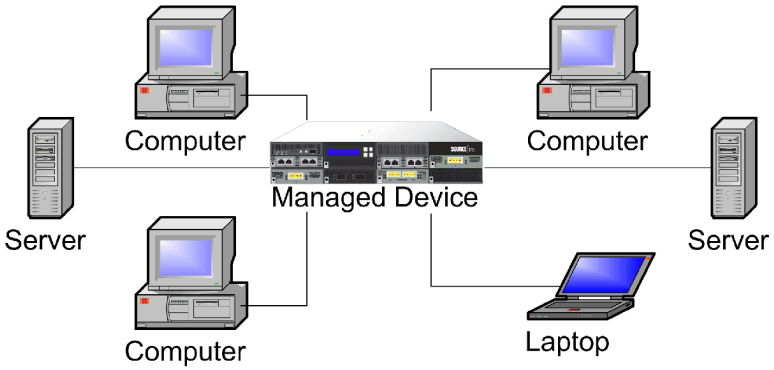
You can use the virtual switch to replace both the tap and the switch in your deployment. Note that if you replace the tap with a virtual switch, you lose the tap packet delivery guarantee.



You can also create interfaces to capture data from separate networks. The following diagram shows a single device with a dual-port adapter and two interfaces connected to two networks.



In addition to using one device to monitor both network segments, you can use the virtual switch capability of the device to replace both switches in your deployment.



Complex Network Deployments

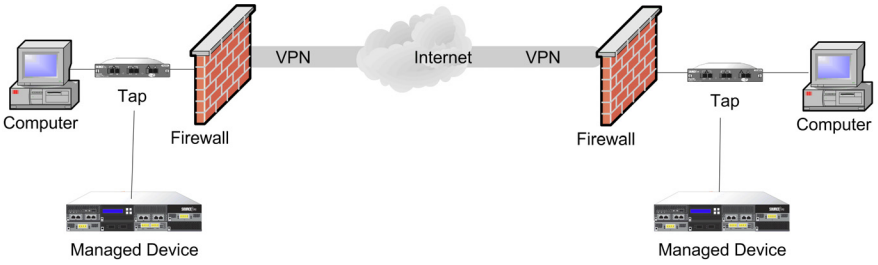
Your enterprise's network may require remote access, such as using a VPN, or have multiple entry points, such as a business partner or banking connection. The following sections describe some of the issues involved with these deployments:

- Integrating with VPNs on page 51
- Detecting Intrusions on Other Points of Entry on page 51
- Deploying in Multi-Site Environments on page 53
- Integrating Managed Devices within Complex Networks on page 55

Integrating with VPNs

Virtual private networks, or VPNs, use IP tunneling techniques to provide the security of a local network to remote users over the Internet. In general, VPN solutions encrypt the data payload in an IP packet. The IP header is unencrypted so that the packet can be transmitted over public networks in much the same way as any other packet. When the packet arrives at its destination network, the payload is decrypted and the packet is directed to the proper host.

Because network appliances cannot analyze the encrypted payload of a VPN packet, placing managed devices outside the terminating endpoints of the VPN connections ensures that all packet information can be accessed. The following diagram illustrates how managed devices can be deployed in a VPN environment.

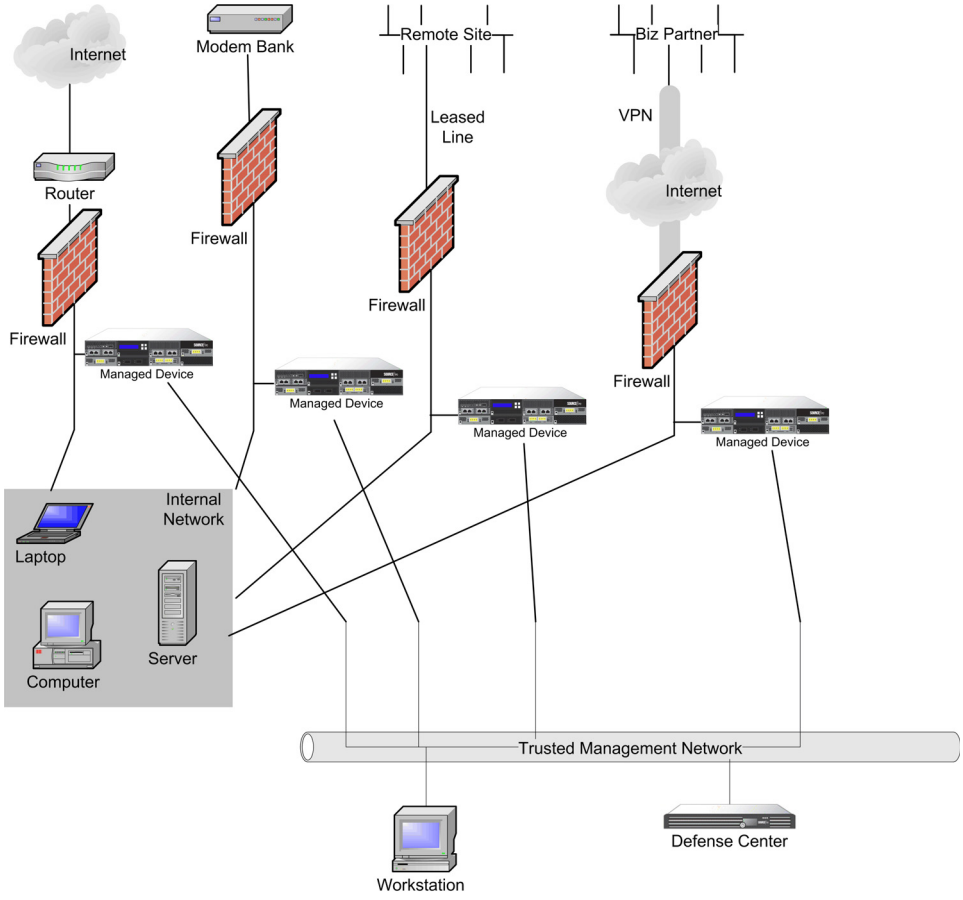


You can replace the firewall and the tap on either side of the VPN connection with the managed device. Note that if you replace the tap with a managed device, you lose the tap packet delivery guarantee.

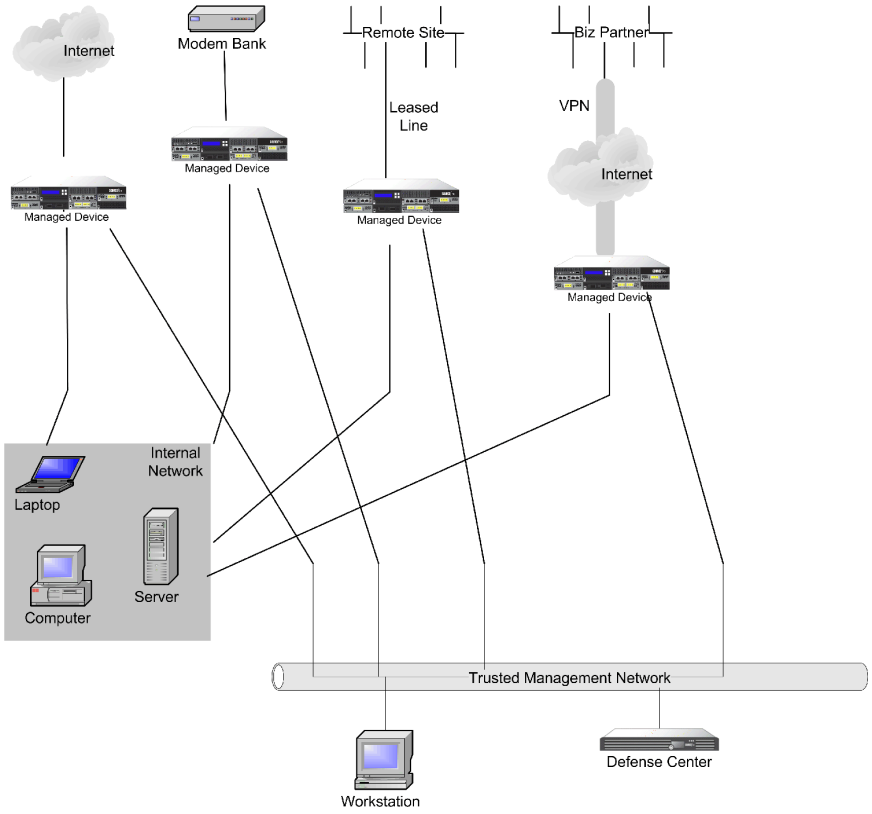
Detecting Intrusions on Other Points of Entry

Many networks include more than one access point. Instead of a single border router that connects to the Internet, some enterprises use a combination of the Internet, modem banks, and direct links to business partner networks. In general, you should deploy managed devices near firewalls (either inside the firewall, outside the firewall, or both) and on network segments that are important to the integrity and confidentiality of your business data. The following diagram shows

how managed devices can be installed at key locations on a complex network with multiple entry points.



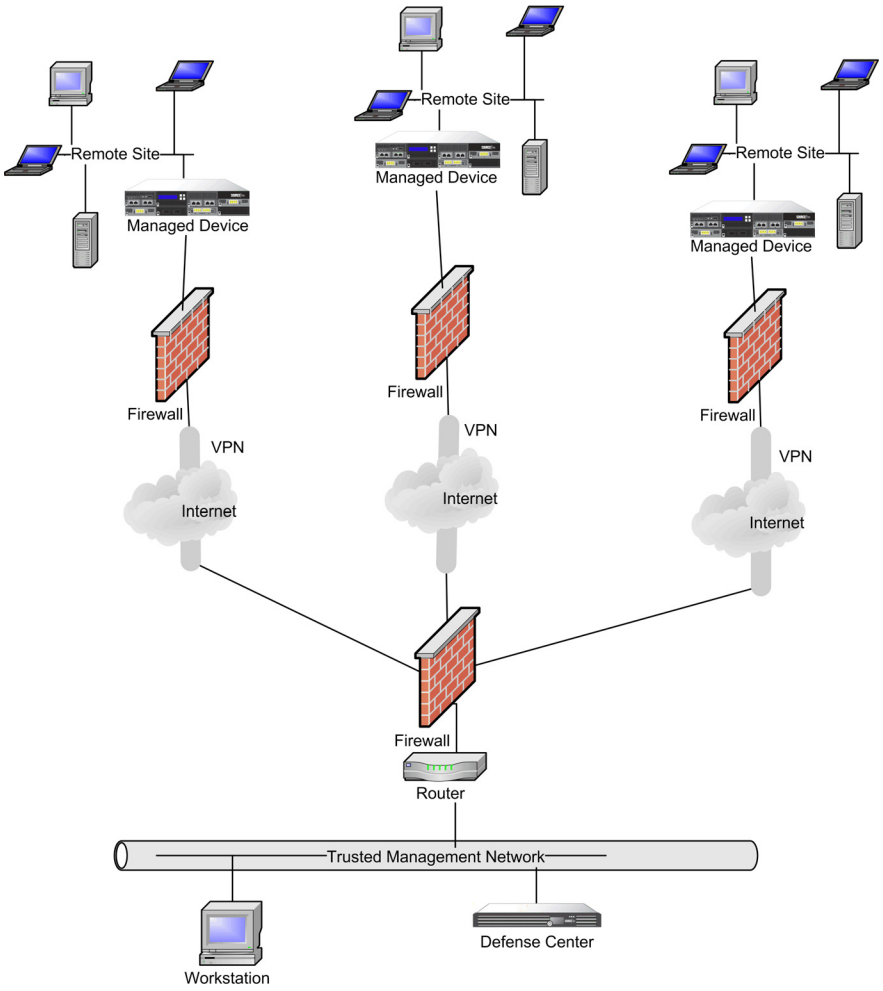
You can replace the firewall and the router with the managed device deployed on that network segment.



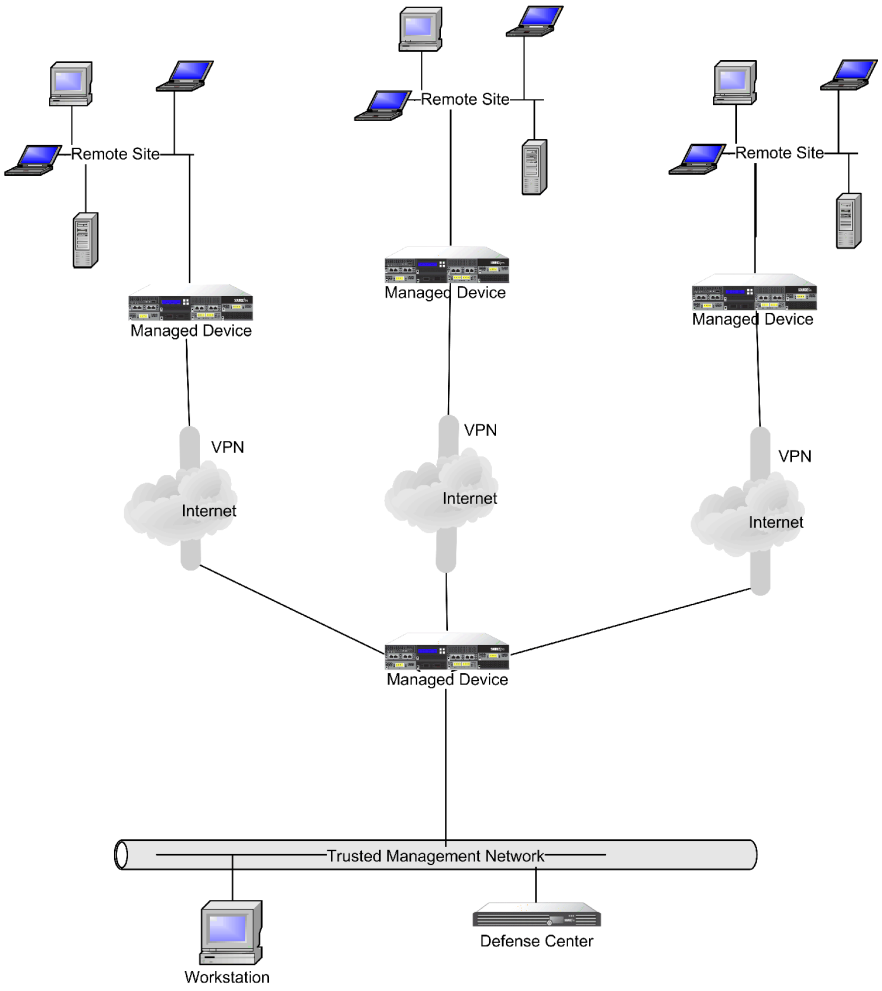
Deploying in Multi-Site Environments

Many organizations want to extend intrusion detection across a geographically disparate enterprise and then analyze all the IPS data from one location. The Sourcefire 3D System supports this by offering the Defense Center, which aggregates and correlates events from managed devices deployed throughout the organization's many locations. Unlike deploying multiple managed devices and Defense Centers in the same geographic location on the same network, when deploying managed devices in disparate geographic locations, you must take precautions to ensure the security of the managed devices and the data stream. To secure the data, you must isolate the managed devices and Defense Center from unprotected networks. You can do this by transmitting the data stream from

the managed devices over a VPN or with some other secure tunneling protocol as shown in the following diagram.



You can replace the firewalls and routers with the managed device deployed in each network segment.



Integrating Managed Devices within Complex Networks

You can deploy managed devices in more complex network topologies than a simple multi-sector network. This section describes the issues surrounding network discovery and vulnerability analysis when deploying in environments where proxy servers, NAT devices, and VPNs exist, in addition to information about using the Sourcefire Defense Center to manage multiple managed devices and the deployment and management of managed devices in a multi-site environment.

Integrating with Proxy Servers and NAT

Network address translation (NAT) devices or software may be employed across a firewall, effectively hiding the IP addresses of internal hosts behind a firewall. If managed devices are placed between these devices or software and the hosts being monitored, the system may incorrectly identify the hosts behind the proxy or NAT device. In this case, Sourcefire recommends that you position managed devices inside the network segment protected by the proxy or NAT device to ensure that hosts are correctly detected.

Integrating with Load Balancing Methods

In some network environments, "server farm" configurations are used to perform network load balancing for services such as web hosting, FTP storage sites, and so on. In load balancing environments, IP addresses are shared between two or more hosts with unique operating systems. In this case, the system detects the operating system changes and cannot deliver a static operating system identification with a high confidence value. Depending on the number of different operating systems on the affected hosts, the system may generate a large number of operating system change events or present a static operating system identification with a lower confidence value.

Other Detection Considerations

If an alteration has been made to the TCP/IP stack of the host being identified, the system may not be able to accurately identify the host operating system. In some cases, this is done to improve performance. For instance, administrators of Windows hosts running the Internet Information Services (IIS) Web Server are encouraged to increase the TCP window size to allow larger amounts of data to be received, thereby improving performance. In other instances, TCP/IP stack alteration may be used to obfuscate the true operating system to preclude accurate identification and avoid targeted attacks. The likely scenario that this intends to address is where an attacker conducts a reconnaissance scan of a network to identify hosts with a given operating system followed by a targeted attack of those hosts with an exploit specific to that operating system.

CHAPTER 3
INSTALLING A SOURCEFIRE 3D SYSTEM APPLIANCE

Sourcefire appliances are easily installed on your network as part of a larger Sourcefire 3D System deployment. You install devices on network segments to inspect traffic and generate intrusion events based on the intrusion policy applied to it. This data is transmitted to a Defense Center, which manages one or more devices to correlate data across your full deployment, and coordinate and respond to threats to your security.

See the following sections for more information about installing a Sourcefire appliance:

Included Items

The following is a list of components that ship with Sourcefire appliances. As you unpack the system and the associated accessories, check that your package contents are complete as follows:

- one Sourcefire appliance
- power cord (two power cords are included with appliances that include redundant power supplies)
- Category 5e Ethernet straight-through cables: one for a Defense Center; two for a managed device
- one rack-mounting kit (not applicable to the 3D500/1000/2000; required tray and rack-mounting kit available separately for the 3D7010/7020/7030)

Security Considerations

Before you install your appliance, Sourcefire recommends that you consider the following:

- Locate your Sourcefire 3D System appliance in a lockable rack within a secure location that prevents access by unauthorized personnel. Place a desktop device (3D500/1000/2000) within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the Sourcefire appliance.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access.
- Identify the specific workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using Access Lists within the appliance's system policy. For more information, see the *Sourcefire 3D System User Guide*.

Identifying the Management Interfaces

You connect each appliance in your deployment to the network using the management interface. This allows the Defense Center to communicate with and administer the devices it manages.

Sourcefire appliances are delivered on different hardware platforms. Make sure you refer to the correct illustration for your appliance as you follow the installation procedure:

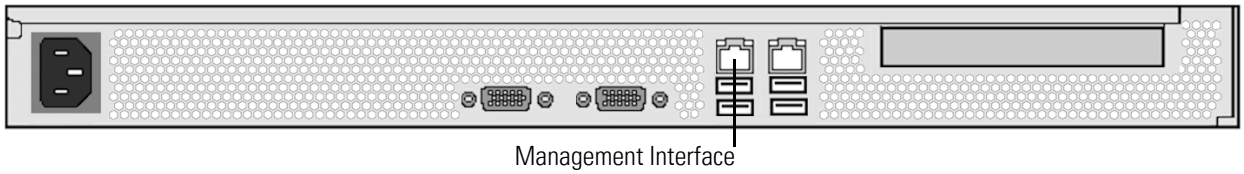
- Sourcefire Defense Center 750 on page 59
- Sourcefire Defense Center 1500 on page 59
- Sourcefire Defense Center 3500 on page 60

Sourcefire Defense Center 750

The DC750 is available as a 1U appliance.

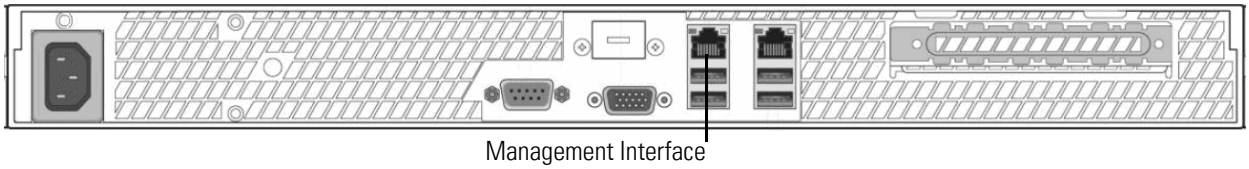
The following illustration of the rear of the chassis indicates the location of the management interface on a DC750 (Rev 1).

DC750 (Rev 1)



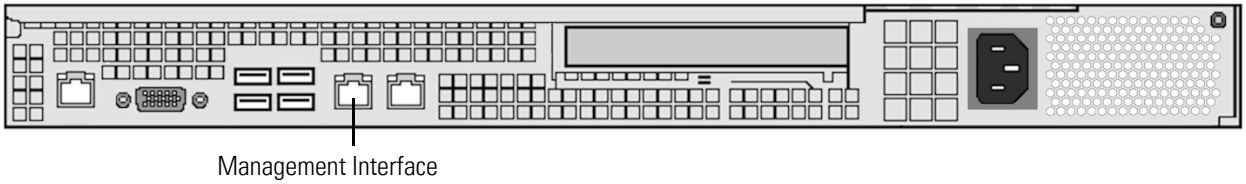
The following illustration of the rear of the chassis indicates the location of the management interface on a DC750 (Rev 2).

DC750 (Rev 2)



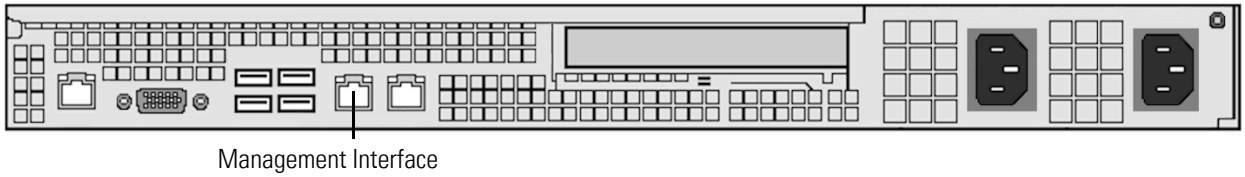
Sourcefire Defense Center 1500

The DC1500 is available as a 1U appliance. The following illustration of the rear of the chassis indicates the location of the management interface.



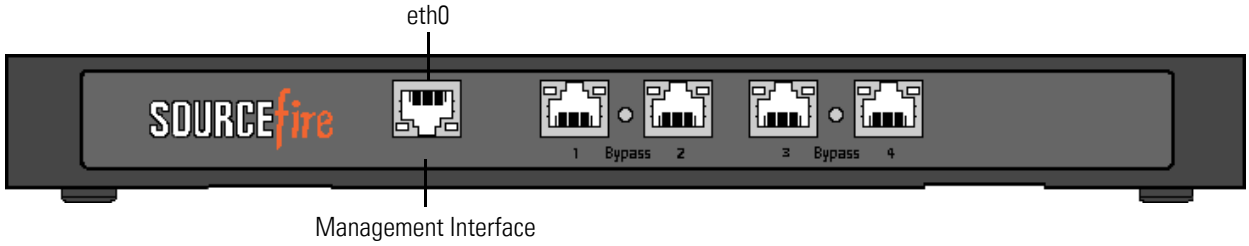
Sourcefire Defense Center 3500

The DC3500 is available as a 1U appliance. The following illustration of the rear of the chassis indicates the location of the management interface.



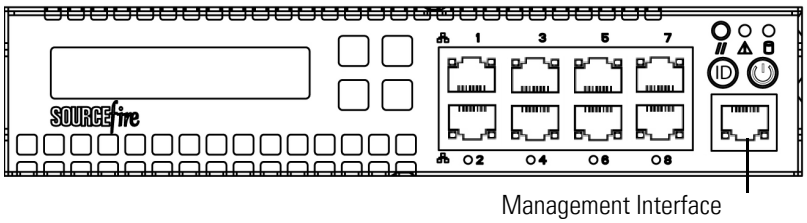
Sourcefire 3D500/1000/2000

The 3D500/1000/2000 is available as a desktop appliance. The following illustration indicates the location of the management interface.

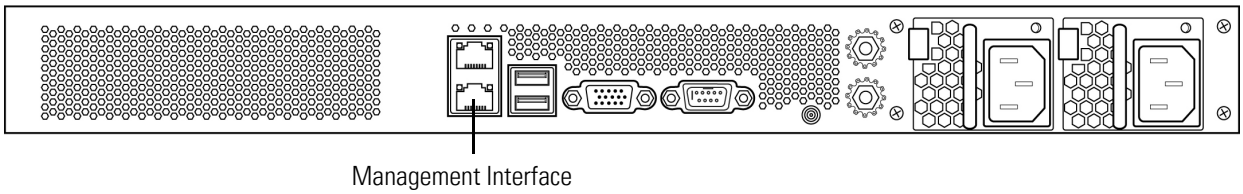


Sourcefire 7000 Series

The 3D7010, 3D7020, and 3D7030 are 1U appliances that are one-half the width of the chassis tray. The following illustration of the front of the chassis indicates the management interface.

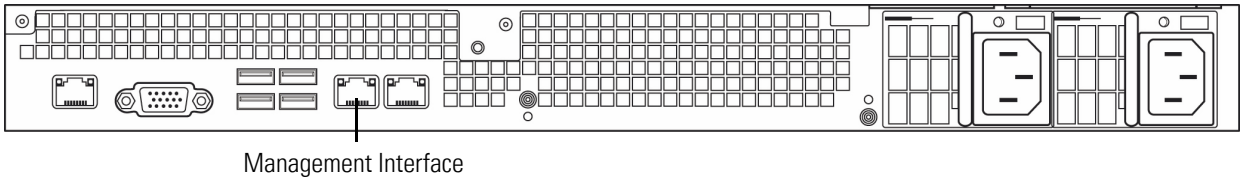


The 3D7110/7120 and the 3D7115/7125 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the management interface.

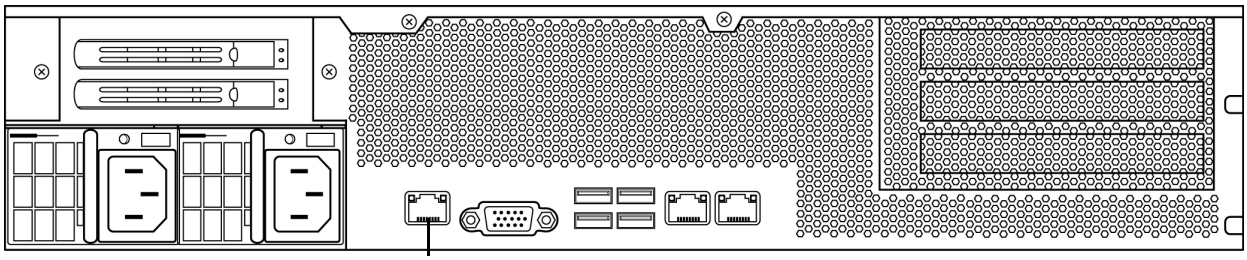


Sourcefire 8000 Series

The 3D8120/8130/8140 is available as a 1U appliance. The following illustration of the rear of the chassis indicates the location of the management interface.



The 3D8250 is available as a 2U appliance. The 3D8260/8270/8290 is available as a 2U appliance with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the management interface for each 2U appliance.



Identifying the Sensing Interfaces

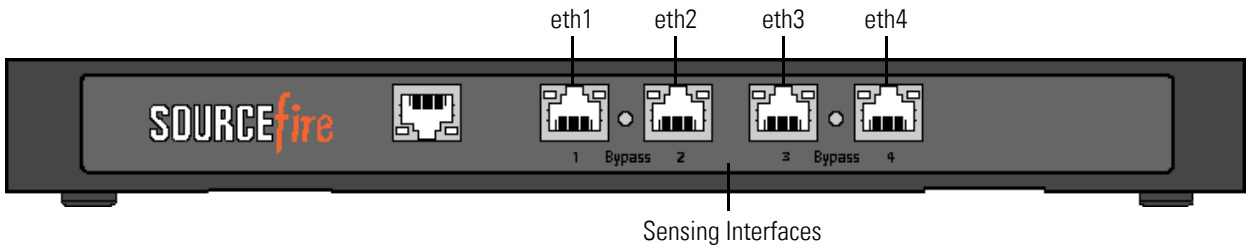
Managed devices connect to network segments using sensing interfaces. The number of segments each device can monitor depends on the number of sensing interfaces on the device and the type of connection (passive, inline, routed, or switched) that you want to use on the network segment.

The following sections describe the sensing interfaces for each managed device. For information on connection types, see Understanding Interfaces on page 28.

- To locate the sensing interfaces on the 3D500/1000/2000, see Sourcefire 3D500/1000/2000 on page 62.
- To locate the sensing interfaces on the 7000 Series, see Sourcefire 7000 Series on page 63.
- To locate the module slots on the 8000 Series on the Sourcefire 8000 Series on page 67.
- To locate the sensing interfaces on the 8000 Series NetMods, see 8000 Series Modules on page 68.

Sourcefire 3D500/1000/2000

The 3D500/1000/2000 is available as a desktop appliance. The following illustration indicates the locations of the sensing interfaces.



You can use the sensing interfaces to passively sense up to four separate network segments.

You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system. The 3D500 can monitor one network when deployed inline, while the 3D1000 and 3D2000 can monitor two networks inline.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left (eth1 and eth2) or the two interfaces on the right (eth3 and eth 4) to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure the interface set as inline with bypass.

If you configure the interfaces as inline without using the bypass capability, you can use any two of the interfaces on the device as an inline pair.

IMPORTANT! By default, the initial setup process supports one inline bypass interface pair for eth1 and eth2. For more information, see the *Sourcefire 3D System User Guide*.

Sourcefire 7000 Series

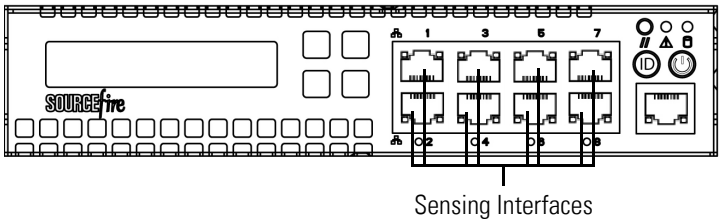
The Sourcefire 7000 Series is available in the following configurations:

- 1U device one-half the width of the rack tray with eight copper interfaces, each with configurable bypass capability.
- 1U device with either eight copper interfaces or eight fiber interfaces, each with configurable bypass capability
- 1U device with four copper interfaces with configurable bypass capability and eight small form-factor pluggable (SFP) ports without bypass capability

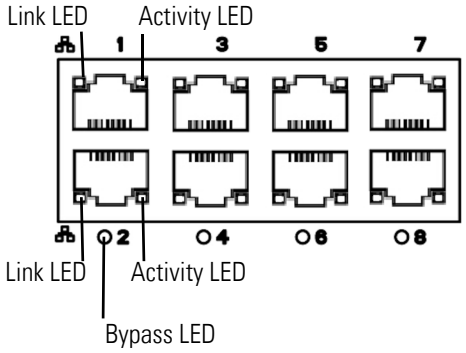
3D7010/7030/7030

The 3D7010/7020/7030 is delivered with eight copper port sensing interfaces, each with configurable bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

Eight Port 1000BASE-T Copper Configurable Bypass Interfaces



You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

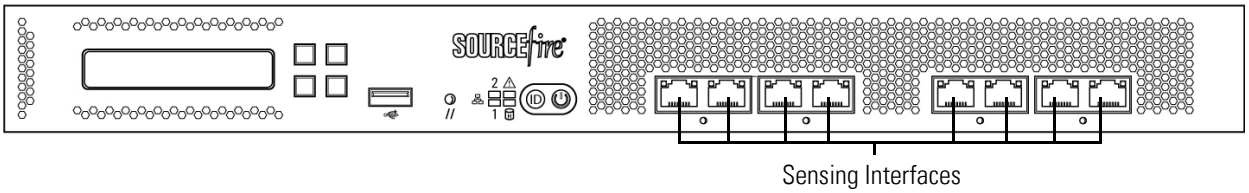


If you want to take advantage of the device's automatic bypass capability, you must connect two interfaces vertically (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

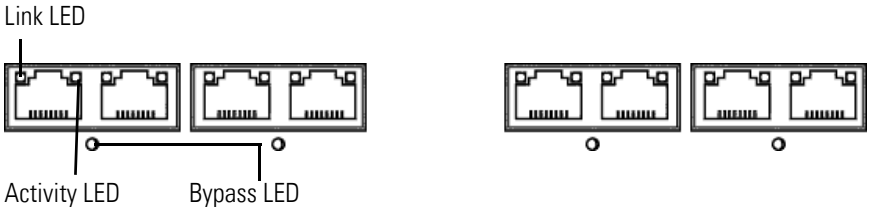
3D7110/7120

The 3D7110/7120 is delivered with eight copper port sensing interfaces, or eight fiber port sensing interfaces, each with configurable bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

3D7110/7120 Copper Interfaces



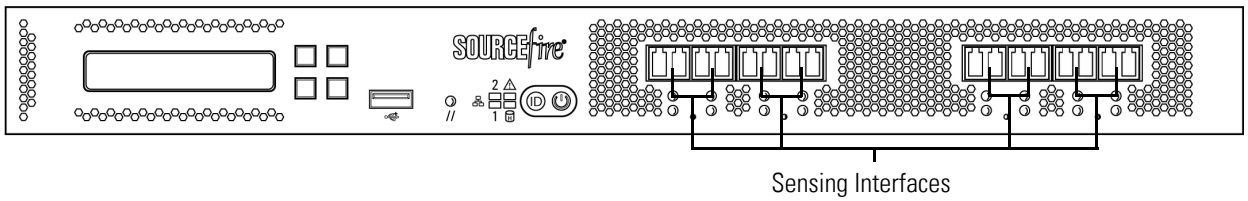
Eight-Port 1000BASE-T Copper Interfaces



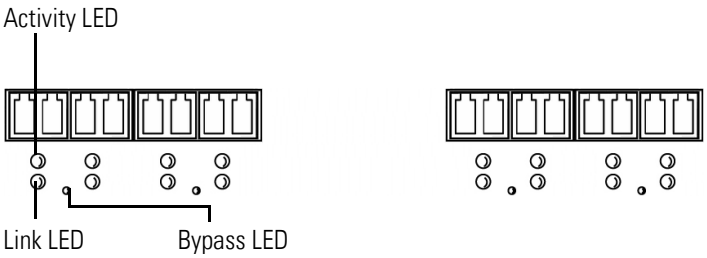
You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

3D7110/7120 Fiber Interfaces



Eight-Port 1000BASE-SX Fiber Configurable Bypass



The eight-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to eight separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to four networks.

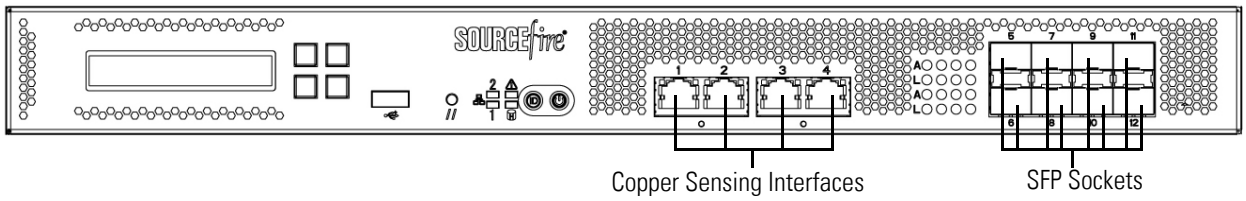
TIP! For best performance, use the interface sets consecutively. If you skip any interfaces, you may experience degraded performance.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

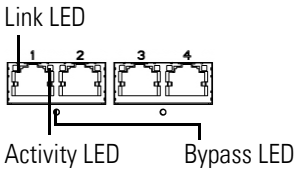
3D7115/7125

The 3D7115 and 3D7125 devices are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability. The following illustration of the front of the chassis indicates the location of the sensing interfaces.

3D7115/7125 Copper and SFP Interfaces



Four 1000BASE-T Copper Interfaces



You can use the copper interfaces to passively monitor up to four separate network segments. You can also use paired interfaces in inline or inline with bypass mode to deploy the device as an intrusion prevention system on up to two networks.

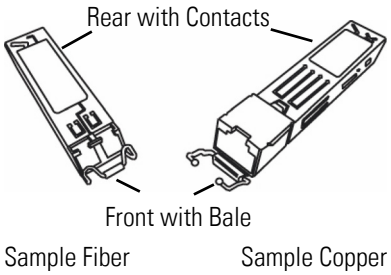
If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. Automatic bypass capability allows traffic to flow even if the device fails or loses power. After you cable the interfaces, you use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

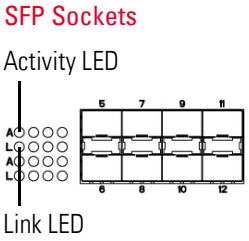
SFP Interfaces

When you install Sourcefire SFP transceivers into the SFP sockets, you can passively monitor up to eight separate network segments. You can also use paired interfaces in inline, non-bypass mode to deploy the device as an intrusion detection system on up to four networks.

Sourcefire SFP transceivers are available in 1G copper, 1G short range fiber, or 1G long range fiber, and are hot-swappable. You can use any combination of copper or fiber transceivers in your device in either passive or inline configuration. Note that SFP transceivers do not have bypass capability and should not be used in intrusion prevention deployments. To ensure compatibility, use only SFP transceivers available from Sourcefire. See Using SFP Transceivers on a 3D7115 or 3D7125 on page 251 for more information.

Sample SFP Transceivers





Sourcefire 8000 Series

The Sourcefire 8000 Series is available as a 1U device with a 10G network switch or a 2U device with either a 10G or a 40G network switch. This device can be shipped fully assembled, or you can install the network modules (NetMods) that contain the sensing interfaces.

IMPORTANT! If you install a NetMod in an incompatible slot on your device (for example, inserting a 40G NetMod in slots 1 and 4 on a 3D8250) or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface of the managing Defense Center when you attempt to configure the NetMod. Contact Sourcefire Support for assistance.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only)

The following modules contain non-bypass sensing interfaces:

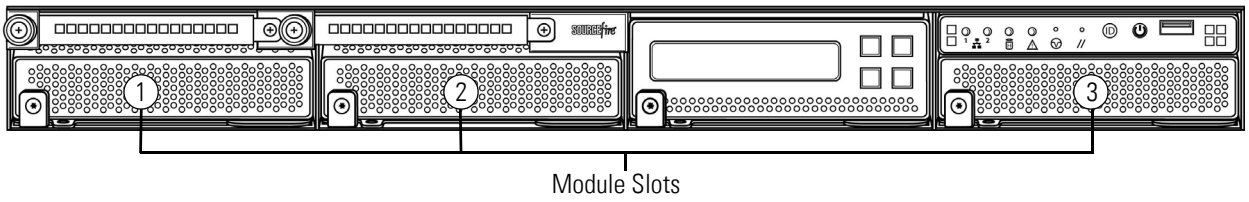
- a quad-port 1000BASE-T copper interface without bypass capability
- a quad-port 1000BASE-SX fiber interface without bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability

In addition, a stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the 3D8140 and 3D8250, and is provided in the 3D8260/8270/8290 stacked configurations.

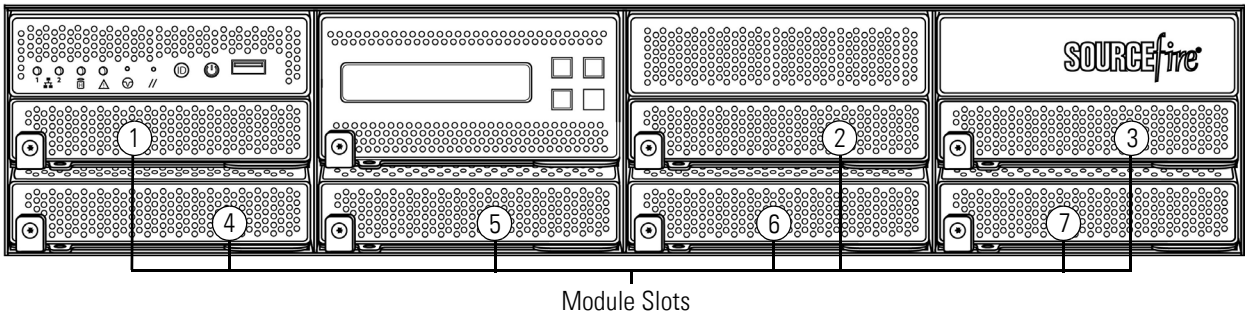
WARNING! Modules are **not** hot-swappable. See Inserting and Removing 8000 Series Modules on page 255 for more information.

The following illustrations of the front of the chassis indicates the location of the module slots that contain the sensing interfaces.

81xx Family Front Chassis View



82xx Family Front Chassis View



8000 Series Modules

The 8000 Series can be delivered with the following modules with configurable bypass capability:

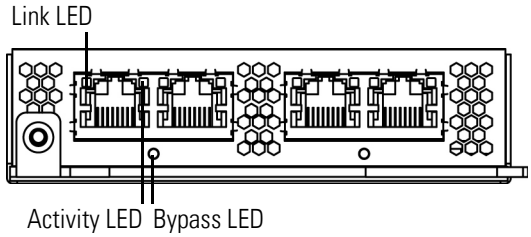
- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Quad-Port 1000BASE-T Copper Configurable Bypass NetMod on page 69 for more information.
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod on page 69 for more information.
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod on page 70 for more information.
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability. See Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod on page 71 for more information.

The 8000 Series can be delivered with the following modules without configurable bypass capability:

- a quad-port 1000BASE-T copper interface without bypass capability. See Quad-Port 1000BASE-T Copper Non-Bypass NetMod on page 72 for more information.
- a quad-port 1000BASE-SX fiber interface without bypass capability. See Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod on page 72 for more information.
- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod on page 72 for more information.

A stacking module is optional on the 3D8140 and 3D8250, and is provided in the 3D8260/8270/8290 stacked configurations. See 8000 Series Stacking Module on page 73 for more information.

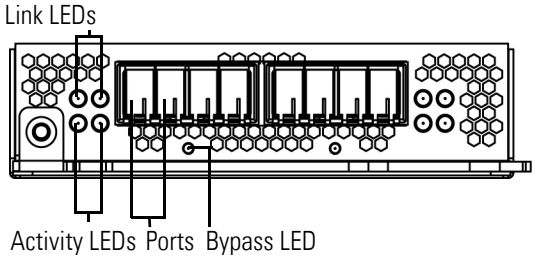
Quad-Port 1000BASE-T Copper Configurable Bypass NetMod



You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on up to two networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod



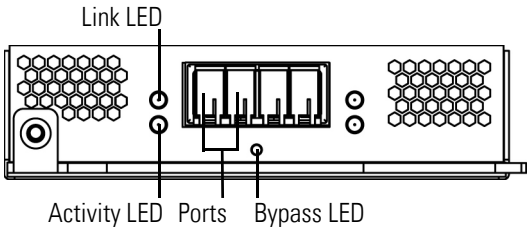
The quad-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use this configuration to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on up to two separate networks.

TIP! For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod



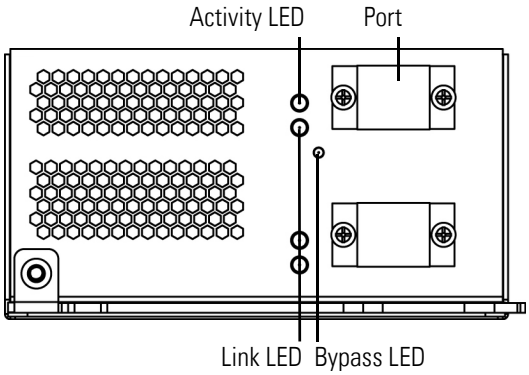
The dual-port 10GBASE fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers. Note that these can be either MMSR or SMLR interfaces.

You can use this configuration to passively monitor up to two separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on a single network.

TIP! For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect two interfaces to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod



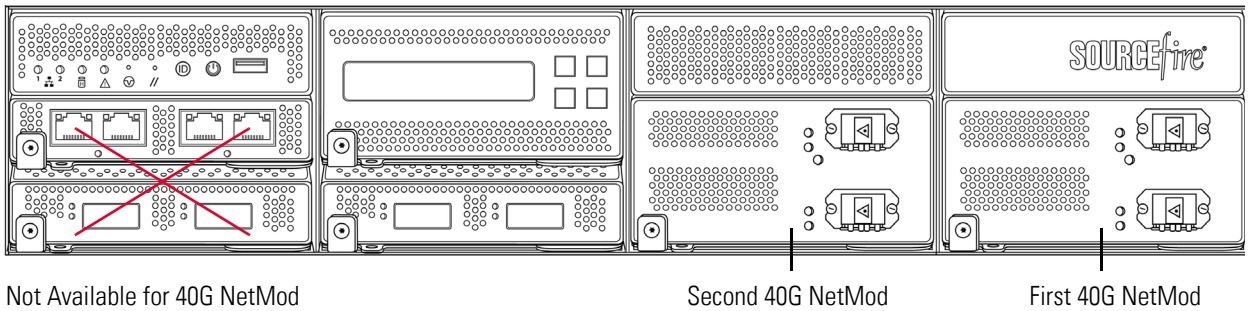
The dual-port 40GBASE-SR4 fiber configurable bypass configuration uses MPO (Multiple-Fiber Push On) connector optical transceivers.

You can use the 40G NetMod only in the 3D8270/8290 or a 40G-capable 3D8250/8260. If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Defense Center web interface displays red. A 40G-capable device displays "3D 8250-40G" on the LCD Panel.

You can use this configuration to passively monitor up to two separate network segments. You also can use the paired interface in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on one network.

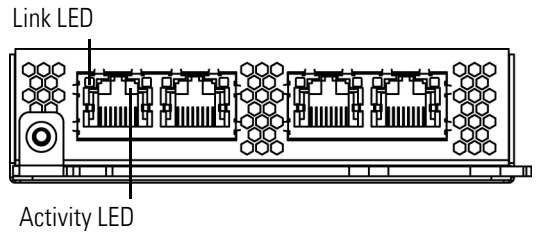
You can use up to two 40G NetMods. Install the first 40G NetMod in slots 3 and 7, and the second in slots 2 and 6. You cannot use a 40G NetMod in slots 1 and 4.

40G NetMod Placement



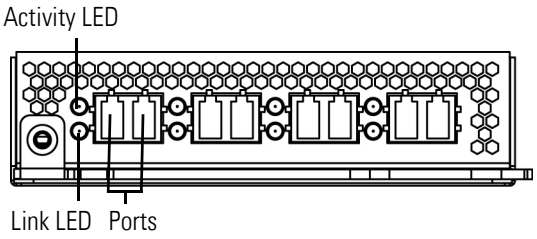
If you want to take advantage of a device's automatic bypass capability, you must use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Quad-Port 1000BASE-T Copper Non-Bypass NetMod



You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod

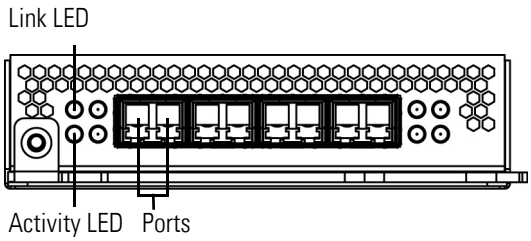


The quad-port 1000BASE-SX fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

TIP! For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod



The quad-port 10GBASE fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers with either MMSR or SMLR interfaces.

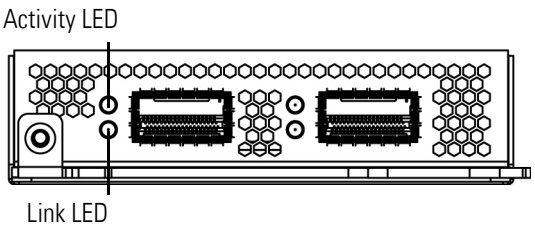
WARNING! The quad-port 10G BASE non-bypass NetMod contains non-removable small form-factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

TIP! For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

8000 Series Stacking Module

A stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the 3D8140 and 3D8250, and is provided in the 3D8260/8270/8290 stacked configurations.



The stacking module allows you to combine the resources of two devices, using one as the primary device and one as the secondary. Only the primary device has sensing interfaces.

- The 3D8140 and 3D8250 can be delivered with the stacking module.
- The 3D8260 is delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The 3D8270 is delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The 3D8290 is delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.

For more information on using stacked devices, see Using Devices in a Stacked Configuration.

Using Devices in a Stacked Configuration

You can increase the amount of traffic inspected on network segments by combining the resources of identically configured devices in a stacked configuration. One device is designated as the primary device and is connected to the network segments. All other devices are designated secondary devices, and are used to provide additional resources to the primary device. A Defense Center creates, edits, and manages the stacked configuration.

The primary device contains sensing interfaces and one set of stacking interfaces for each secondary device connected to it. You connect the sensing interfaces on the primary device to the network segments you want to monitor in the same way as a non-stacked device. You connect the stacking interfaces on the primary device to the stacking interfaces on the secondary devices using the stacking cables. Each secondary device is connected directly to the primary device using the stacking interfaces. If a secondary device contains sensing interfaces, they are not used.

You can stack devices in the following configurations:

- two 3D8140s
- up to four 3D8250s
- a 3D8260 (a 10G-capable primary device and a secondary device)
- a 3D8270 (a 40G-capable primary device and two secondary devices)
- a 3D8290 (a 40G-capable primary device and three secondary devices)

For the 3D8260 and 3D8270, you can stack additional devices for a total of four devices in the stack.

One device is designated as the primary device and is displayed on the Defense Center's web interface with the primary role. All other devices in the stacked configuration are secondary and displayed in the web interface with the secondary role. You use the combined resources as a single entity except when viewing information from the stacked devices.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single 3D8140 or 3D8250. Connect the secondary devices to the primary device as indicated in the stack cabling diagram.

After the devices are physically connected to the network segments and to each other, use a Defense Center to establish and manage the stack.

The following sections provide more information on how to connect and manage stacked devices:

- Connecting the 3D8140 on page 75
- Connecting the 3D8250/8260/8270/8290 on page 75
- Using the 8000 Series Stacking Cable on page 79
- Managing Stacked Devices on page 79

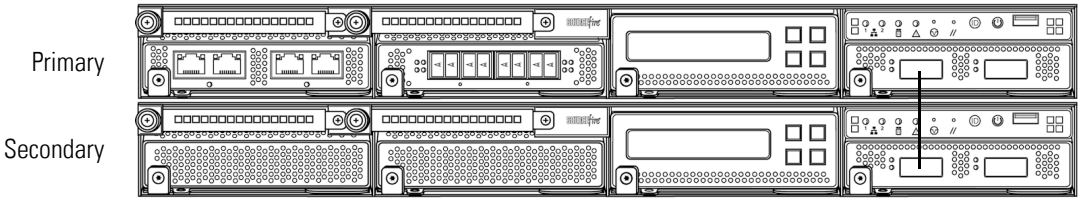
Connecting the 3D8140

You can connect two 3D8140s in a stacked configuration. You must use one 8000 Series stacking cable to create the physical connection between the primary device and the secondary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable on page 79.

Install the devices in your rack so you can easily connect the cable between the stacking modules. You can install the secondary device above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single 3D8140. Connect the secondary device directly to the primary device.

The following graphic shows a primary device with a secondary device installed below the primary device.



To connect a 3D8140 secondary device:

- Use an 8000 Series stacking cable to connect the left stacking interface on the primary device to the left stacking interface on the secondary device, then use the Defense Center that manages the devices to establish the stacked device relationship in the system. Note that the right stacking interface is not connected. See Managing Stacked Devices on page 79.

Connecting the 3D8250/8260/8270/8290

You can connect any of the following configurations:

- up to four 3D8250s
- a 3D8260 (a 10G-capable primary device and a secondary device)
- a 3D8270 (a 40G-capable primary device and two secondary devices)
- a 3D8290 (a 40G-capable primary device and three secondary devices)

For the 3D8260 and 3D8270, you can stack additional devices for a total of four devices in the stack.

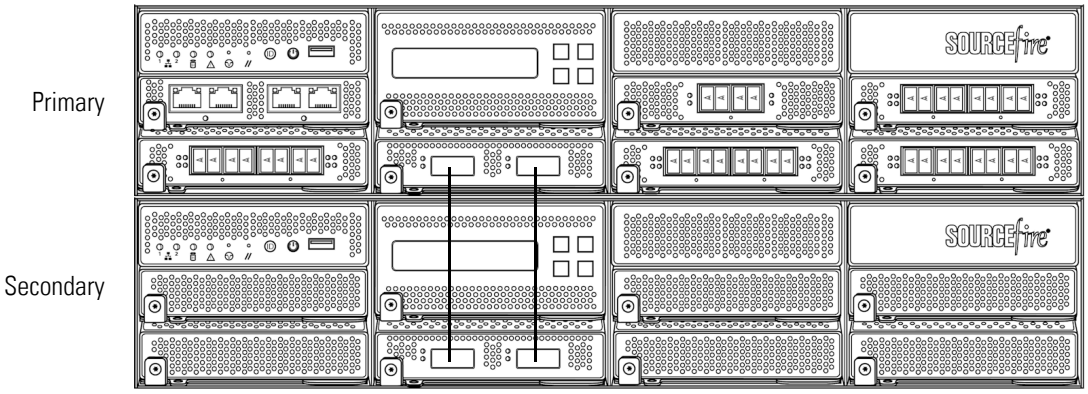
You must use two 8000 Series stacking cables for each secondary device you want to connect to the primary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable on page 79.

Install the devices in your rack so you can easily connect the cables between the stacking modules. You can install the secondary devices above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single 3D8250. Connect each secondary device directly to the primary device as required for the number of secondary devices in the configuration.

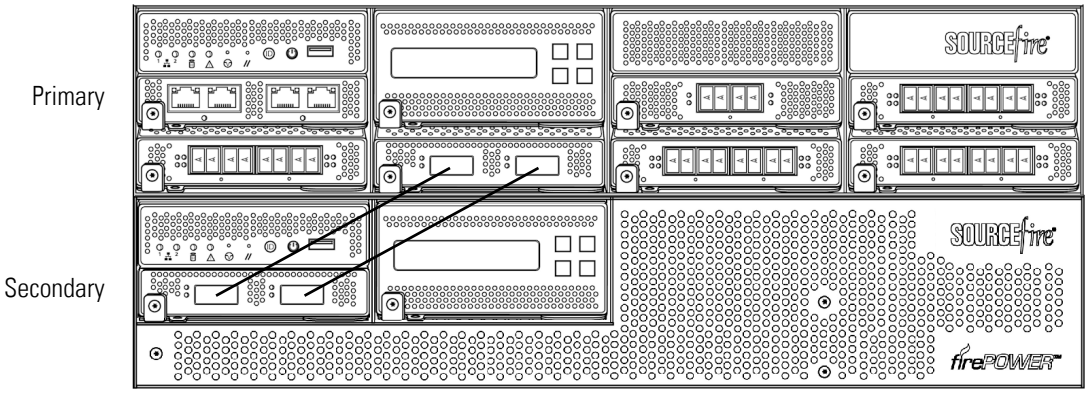
3D8250 Primary Device with One Secondary Device

The following example shows a 3D8250 primary device and one secondary device. The secondary device is installed below the primary device. Note that the secondary device contains no sensing interfaces.



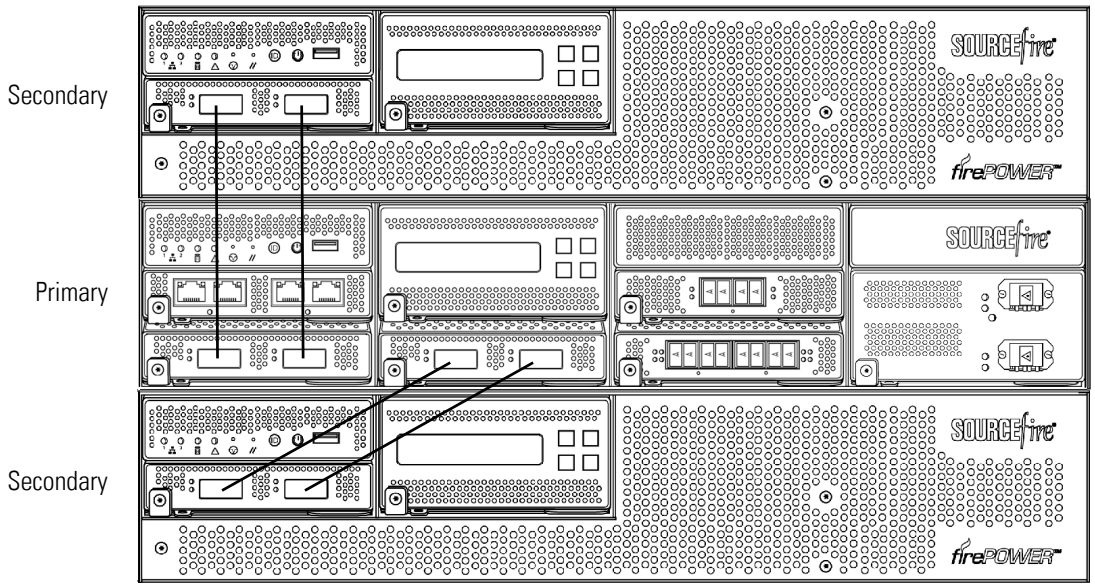
3D8260 - 3D8250 Primary Device and One Secondary Device

The following example shows a 3D8260 configuration, which includes a 10G-capable 3D8250 primary device and one dedicated secondary device. The secondary device is installed below the primary device.



3D8270 - 3D8250 (40G) Primary Device and Two Secondary Devices

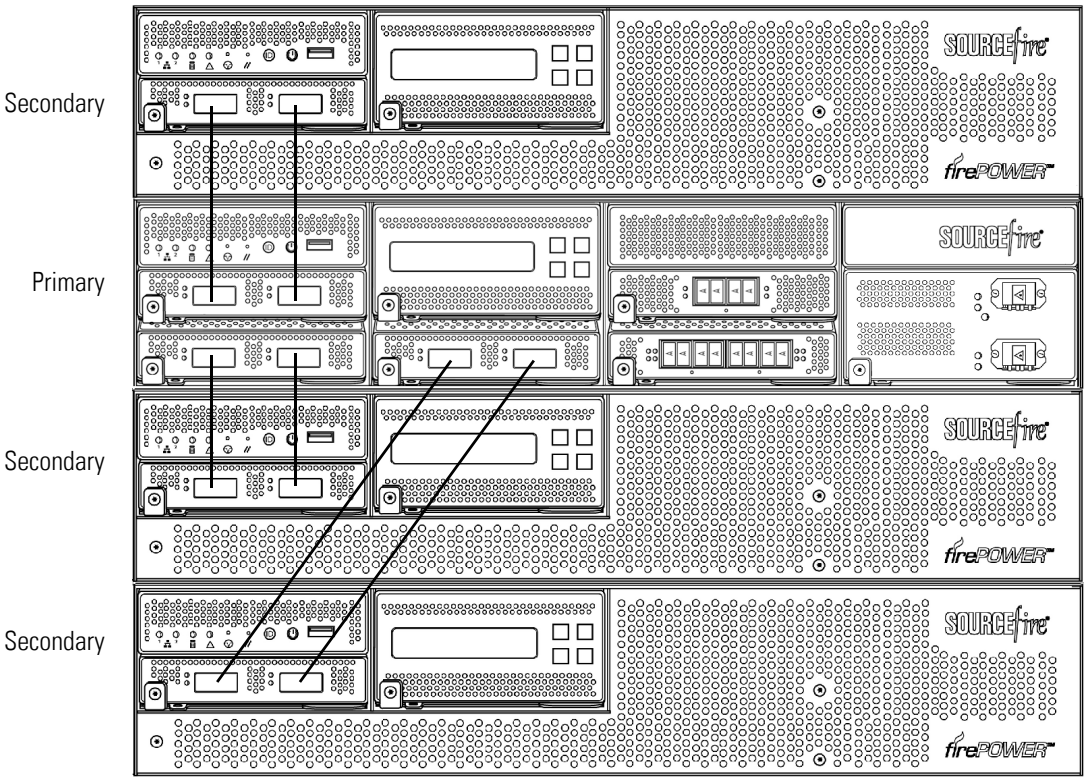
The following example shows a 3D8270, which includes a 40G-capable 3D8250 primary device and two dedicated secondary devices. One secondary device is installed above the primary device and the other is installed below the primary device.



3D8290 - 3D8250 (40G) Primary Device and Three Secondary Devices

The following example shows a 3D8290, which includes a 40G-capable 3D8250 primary device and three dedicated secondary devices. One secondary device is

installed above the primary device and two secondary devices are installed below the primary device.

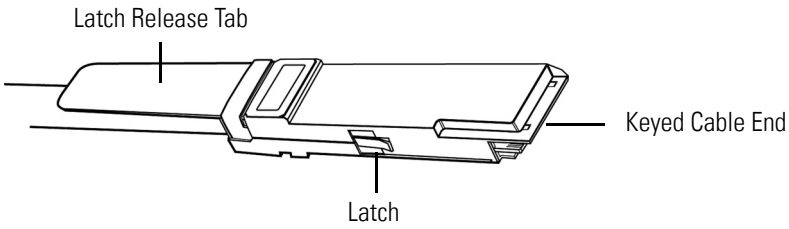


To connect a 3D8250 secondary device:

1. Use an 8000 Series stacking cable to connect the left interface on the stacking module on the primary device to the left interface on the stacking module on the secondary device.
2. Use a second 8000 Series stacking cable to connect the right interface on the stacking module on the primary device to the right interface on the stacking module on the secondary device.
3. Repeat steps 1 and 2 for each secondary device you want to connect.
4. Use the Defense Center that manages the devices to establish the stacked device relationship and manage their joint resources. See Managing Stacked Devices on page 79.

Using the 8000 Series Stacking Cable

The 8000 Series stacking cable has identically-keyed ends, each with a latch to secure the cable in the device and a latch release tab.



Use 8000 Series stacking cables to create the physical connection between the primary device and each secondary device as required for each device configuration. The 3D8250/8260/8270/8290 requires two cables per connection and the 3D8140 requires one cable. Devices do not need to be powered down to insert or remove the stacking cable.

WARNING! Use only the Sourcefire 8000 Series stacking cable when cabling your devices. Using unsupported cables can create unforeseen errors.

Use the Defense Center to manage the stacked devices after you have physically connected the devices.

To insert an 8000 Series stacking cable:

- To insert the cable, hold the cable end with release tab facing up, then insert the keyed end into the port on the stacking module until you hear the latch click into place.

To remove an 8000 Series stacking cable:

- To remove the cable, pull on the release tab to release the latch, then remove the cable end.

Managing Stacked Devices

A Defense Center establishes the stacked relationship between the devices, controls the interface sets of the primary device, and manages the combined resources in the stack. You cannot manage interface sets on the local web interface of a stacked device.

After the stacked relationship is established, each device inspects traffic separately using a single, shared detection configuration. If the primary device fails, traffic is handled according to the configuration of the primary device (that is, as if the stacked relationship did not exist). If the secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to the failed secondary device where the traffic is dropped.

For information on establishing and managing stacked devices, see Managing Stacked Devices in the *Sourcefire 3D System User Guide*.

Installing the Appliance in a Rack

The Sourcefire 3D System is delivered on different hardware platforms. You can rack-mount all Sourcefire appliances, including the 3D500/1000/2000 desktop devices (with purchase of a 1U mounting kit). When you install an appliance, you must also make sure that you can access the appliance's console. To access the console for initial setup, connect to a Sourcefire appliance in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to any Sourcefire appliance, which is useful for rack-mounted appliances connected to a keyboard, video, and mouse (KVM) switch.

Ethernet Connection to Management Interface

Configure a local computer, which must not be connected to the internet, with the following s:

- IP address: `192.168.45.2`
- netmask: `255.255.255.0`
- default gateway: `192.168.45.1`

Using an Ethernet cable, connect the network interface on the local computer to the management interface on the appliance. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. The settings for this software are 9600 baud, 8 data bits, no parity checking, 1 stop bit, and no flow control.

Note that the management interface on a physical Sourcefire appliance is preconfigured with a default IPv4 address. However, you can reconfigure the management interface with an IPv6 address as part of the setup process.

After initial setup, you can access the console in the following additional ways:

Serial Connection/Laptop

You can use a serial cable to connect a computer to any Sourcefire appliance except the 3D2100/2500/3500/4500 devices. To interact with the appliance, use terminal emulation software as described above.

Lights-Out Management Using Serial over LAN

The LOM feature allows you to perform a limited set of management actions on a Series 3 appliance, including restoring to factory defaults, using a Serial over LAN (SOL) connection. For more information, see Setting up Lights-Out Management on page 219.

By default, Sourcefire appliances direct initialization status, or *init*, messages to the VGA port. If you want to use the physical serial port or SOL to access the console, Sourcefire recommends you redirect console output to the serial port after you complete initial setup. For more information, see Redirecting Console Output on page 82.

To install the appliance:

1. Mount the appliance in your rack using the mounting kit and its supplied instructions.

   Optionally, you can deploy the 3D500/1000/2000 as a desktop device.

2. Connect to the appliance using either a keyboard and monitor or Ethernet connection.

3. If you are using a keyboard and monitor to set up the appliance, use an Ethernet cable now to connect the management interface to a protected network segment.

   If you plan to perform the initial setup process by connecting a computer directly to the appliance's physical management interface, you will connect the management interface to the protected network when you finish setup.

4. For a managed device, connect the sensing interfaces to the network segments you want to analyze using the appropriate cables for your interfaces:

   - Copper Sensing Interfaces: If your device includes copper sensing interfaces, make sure you use the appropriate cables to connect them to your network; see Cabling Inline Deployments on Copper Interfaces on page 34.
   - Fiber Adapter Card: For devices with a fiber adapter card, connect the LC connectors on the optional multimode fiber cable to two ports on the adapter card in any order. Connect the SC plug to the network segment you want to analyze.
   - Fiber Tap: If you are deploying the device with an optional fiber optic tap, connect the SC plug on the optional multimode fiber cable to the "analyzer" port on the tap. Connect the tap to the network segment you want to analyze.
   - Copper Tap: If you are deploying the device with an optional copper tap, connect the A and B ports on the left of the tap to the network segment you want to analyze. Connect the A and B ports on the right of the tap (the "analyzer" ports) to two copper ports on the adapter card.

   For more information about options for deploying the managed device, see Understanding Deployment Options on page 28.

   Note that if you are deploying a device with bypass interfaces, you are taking advantage of your device's ability to maintain network connectivity even if the device fails. See Testing an Inline Bypass Interface Installation on page 83 for information on installation and latency testing.

5. Attach the power cord to the appliance and plug into a power source.

   If your appliance has redundant power supplies, attach power cords to both power supplies and plug them into separate power sources. Note that the 3D500/1000/2000 does not have a power switch. This device turns on when you connect the power supply.

6. Turn on the appliance.

   If you are using a direct Ethernet connection to set up the appliance, confirm that the link LED is on for both the network interface on the local computer and the management interface on the appliance. If the management interface and network interface LEDs are not lit, try using a crossover cable. For more information, see Cabling Inline Deployments on Copper Interfaces on page 34.

7. Continue with the next chapter, Setting Up a Sourcefire 3D System Appliance on page 86.

Redirecting Console Output

By default, Sourcefire appliances direct initialization status, or *init*, messages to the VGA port. If you restore an appliance to factory defaults and delete its license and network settings, the restore utility also resets console output to VGA. If you want to use the physical serial port or SOL to access the console, Sourcefire recommends you redirect console output to the serial port after you complete initial setup.

TIP! 3D2100/2500/3500/4500 devices do not have functional serial ports.

To redirect console output, run a script from the appliance's shell. The following table lists the console you should use depending on the way you plan to access the appliance.

Console Redirection Options

Appliance	VGA (Default)	Physical Serial	LOM via SOL
3D500/1000/2000	`tty0`	`ttyS0`	n/a
3D2100/2500/3500/4500	`tty0`	n/a	n/a
3D6500	`tty0`	`ttyS1`	n/a
3D9900	`tty0`	`ttyS1`	n/a

Console Redirection Options (Continued)

Appliance	VGA (Default)	Physical Serial	LOM via SOL
Series 2 Defense Centers	`tty0`	`ttyS0`	n/a
all Series 3 appliances	`tty0`	`ttyS0`	`ttyS0`

Note that while all Series 3 appliances support LOM, 7000 Series devices do not support LOM and physical serial access at same time. However, the console setting is the same regardless of which you want to use.

To redirect the console output:

Access: Admin

1. Using your keyboard/monitor or serial connection, log into the appliance using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.

   The prompt for the appliance appears.

2. At the prompt, access `root` privileges on the appliance:
   - On a Defense Center or Series 2 managed device, type `sudo su -` and provide the password again.
   - On a Series 3 managed device, type `expert` to display the shell prompt. Then, type `sudo su -` and provide the password again.

   The root prompt appears.

3. Set the console output by typing the following:

   ```
   /usr/local/sf/bin/set_console.sh -c console_value
   ```

   where *`console_value`* represents the way you plan to access the appliance, as described in the Console Redirection Options table above.

4. To implement your changes, reboot the appliance by typing `reboot`.

   The appliance reboots.

Testing an Inline Bypass Interface Installation

Managed devices with bypass interfaces provide the ability to maintain network connectivity even when the device is powered off or inoperative. It is important to

ensure that you properly install these devices and quantify any latency introduced by their installation.

IMPORTANT! Your switch's spanning tree discovery protocol can cause a 30-second traffic delay. Sourcefire recommends that you disable the spanning tree during the following procedure.

The following procedure, applicable only to copper interfaces, describes how to test the installation and ping latency of an inline bypass interface. You will need to connect to the network to run ping tests and connect to the managed device console.

To test a device with inline bypass interface installation:

Access: Admin

1. Ensure that the interface set type for the appliance is configured for inline bypass mode.

   See Configuring Inline Sets in the *Sourcefire 3D System User Guide* for instructions on configuring an interface set for inline bypass mode.

2. Set all interfaces on the switch, the firewall, and the device sensing interfaces to auto-negotiate.

   IMPORTANT! Cisco devices require auto-negotiate when using auto-MDIX on the device.

3. Power off the device and disconnect all network cables.

   Reconnect the device and ensure you have the proper network connections. Check cabling instructions for crossover versus straight-through from the device to the switches and firewalls, see Cabling Inline Deployments on Copper Interfaces on page 34.

4. With the device powered off, ensure that you can ping from the firewall through the device to the switch.

   If the ping fails, correct the network cabling.

5. Run a continuous ping until you complete step 10.

6. Power the device back on.

7. Using your keyboard/monitor or serial connection, log into the device using an account with Administrator privileges. The password is the same as the password for the device's web interface.

   The prompt for the device appears.

8. Shut down the device:
   - On a Series 2 device, type `sudo su -`, then type your password again. At the root prompt, shut down the appliance by typing `shutdown -h now`.
   - On a Series 3 device, type `system shutdown`.

   You can also shut down the device using its web interface; see the Managing Devices chapter in the *Sourcefire 3D System User Guide*. As most devices power off, they emit an audible click sound. The click is the sound of relays switching and the device going into hardware bypass.
9. Wait 30 seconds.

   Verify that your ping traffic resumes.
10. Power the device back on, and verify that your ping traffic continues to pass.
11. For appliances that support tap mode, you can test and record ping latency results under the following sets of conditions:
    - device powered off
    - device powered on, policy with no rules applied, inline intrusion policy protection mode
    - device powered on, policy with no rules applied, inline intrusion policy protection tap mode
    - device powered on, policy with tuned rules applied, inline intrusion policy protection mode

    Ensure that the latency periods are acceptable for your installation. For information on resolving excessive latency problems, see Configuring Packet Latency Thresholding and Understanding Rule Latency Thresholding in the *Sourcefire 3D System User Guide*.

CHAPTER 4
SETTING UP A SOURCEFIRE 3D SYSTEM APPLIANCE

After you deploy and install a Sourcefire appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a device, you can change its configuration at any time using the Defense Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

For more information on each of the steps in the initial setup process, see the following sections:

- Understanding the Setup Process on page 87 outlines the setup process, which depends on the appliance's model and whether you have physical access to the appliance.

IMPORTANT! If you are not already familiar with the setup process, Sourcefire **strongly** recommends you read this section first.

- Configuring Network Settings Using a Script on page 90 explains how to use a script to specify network settings that allow a new appliance to communicate on your management network. This step is required for all Defense Centers and Series 2 devices that you are accessing using a keyboard and monitor.
- Performing Initial Setup on a Series 3 Device Using the CLI on page 91 explains how to use an interactive command line interface (CLI) to perform the setup process on a Series 3 device.
- Initial Setup Page: Devices on page 93 explains how to use any device's web interface to complete its initial setup.
- Initial Setup Page: Defense Centers on page 100 explains how to use a Defense Center's web interface to complete its initial setup.
- Next Steps on page 109 contains guidance on the post-setup tasks you may want to perform as you set up your Sourcefire 3D System deployment.

WARNING! The procedures in this chapter explain how to set up an appliance without powering it down. However, if you need to power down for any reason, use the procedure in the Managing Devices chapter in the *Sourcefire 3D System User Guide*, the `system shutdown` command from the CLI on a Series 3 device, or the `shutdown -h now` command from an appliance's shell (sometimes called expert mode).

Understanding the Setup Process

After you deploy and install a new Sourcefire appliance, as described in earlier chapters of this guide, you must complete a setup process. Before you begin the setup, make sure that you can meet the following conditions.

Appliance Model

You must know which appliance you are setting up. A Sourcefire *appliance* is either a traffic-sensing managed *device* or a managing *Defense Center*. There are several *models* of each appliance type; these models are further grouped into *series* and *family*. For more information, see Understanding Appliance Series, Models, and Capabilities on page 10.

Access

To set up a new appliance, you must connect using either keyboard and monitor/KVM (keyboard, video, and mouse) or a direct Ethernet connection to the appliance's management interface. After initial setup, you can configure the appliance for serial access. For more information, see Installing the Appliance in a Rack on page 80.

Information

You have, at minimum, the information needed to allow the appliance to communicate on your management network: an IPv4 or IPv6 management IP address, a netmask or prefix length, and a default gateway.

If you know how the appliance is deployed, the setup process is also a good time to perform many initial administrative-level tasks, including registration and licensing.

TIP! If you are deploying multiple appliances, set up your devices first, then their managing Defense Center. The initial setup process for a device allows you to preregister it to a Defense Center; the setup process for a Defense Center allows you to add and license preregistered managed devices.

After you complete setup, you will use the Defense Center's web interface to perform most management and analysis tasks for your deployment. Physical managed devices have a restricted web interface that you can use only to perform basic administration. For more information, see Next Steps on page 109.

For details on how to set up each type of Sourcefire appliance, see:

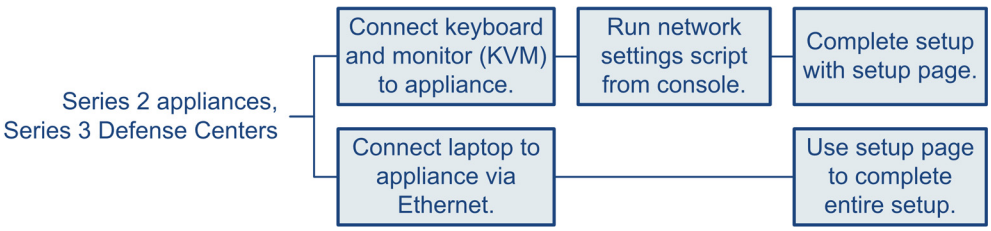
- Setting Up a Series 2 Appliance or Series 3 Defense Center on page 88
- Setting Up a Series 3 Device on page 89

TIP! If you are setting up an appliance after restoring it to factory defaults (see Restoring a Sourcefire Appliance to Factory Defaults on page 198) and you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. Skip to Initial Setup Page: Devices on page 93 or Initial Setup Page: Defense Centers on page 100.

Setting Up a Series 2 Appliance or Series 3 Defense Center

SUPPORTED DEVICES: Series 2
SUPPORTED DEFENSE CENTERS: Series 2, Series 3

The following diagram illustrates the choices you can make when setting up Series 2 devices and Defense Centers, as well as Series 3 Defense Centers:



To set up any Series 2 appliance or a Series 3 Defense Center:

ACCESS: Admin

1. If you are using a keyboard and monitor, run a script that helps you configure settings to allow the appliance to communicate on your management network; see Configuring Network Settings Using a Script on page 90.

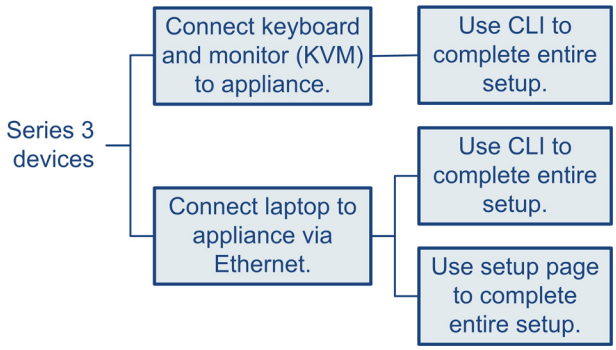
   If you are setting up a reimaged appliance and you kept your network settings as part of the restore process, or if you are accessing the appliance via a direct Ethernet connection, skip to the next step.

2. Complete the setup process by browsing to the appliance's web interface from a computer on your management network:
   - To complete the setup of a managed device using its web interface, see Initial Setup Page: Devices on page 93.
   - To complete the setup of a Defense Center using its web interface, see Initial Setup Page: Defense Centers on page 100.

Setting Up a Series 3 Device

SUPPORTED DEVICES: Series 3

The following diagram illustrates the choices you can make when setting up Series 3 devices:



Your access to a Series 3 device determines how you set it up. You have the following options:

- Regardless of how you are connected to the device, you can use the CLI to set it up; see Performing Initial Setup on a Series 3 Device Using the CLI on page 91.
- If you are accessing the appliance via a direct Ethernet connection, you can browse to the appliance's web interface from a local computer; see Initial Setup Page: Devices on page 93.

If you are setting up a reimaged device and you kept your network settings as part of the restore process, you can access the CLI via SSH or a Lights-Out

Management (LOM) connection. You can also browse to the device's web interface from a computer on your management network.

Configuring Network Settings Using a Script

SUPPORTED DEVICES: Series 2

After you install a new Defense Center or Series 2 device, or delete its network settings as part of a reimage, you must configure the appliance to communicate on your management network. Complete this step by running a script at the console.

The Sourcefire 3D System provides a dual stack implementation for both IPv4 and IPv6 management environments. First, the script prompts you to configure (or disable) IPv4 management settings, then IPv6. For IPv6 deployments, you can retrieve settings from a local router. You must provide the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway.

When following the script's prompts, for multiple-choice questions, your options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the script prompts you for much of the same setup information that the appliance's setup web page does. For more information, see Network Settings on page 96 (device) and Network Settings on page 103 (Defense Center).

To configure network settings using a script:

ACCESS: Admin

1. At the console, log into the appliance.

   Use `admin` as the username and `Sourcefire` as the password.

2. At the admin prompt, switch to the root user by typing `sudo su -`, then typing the password again if prompted.

3. At the root prompt, run the following script:

   ```
   /usr/local/sf/bin/configure-network
   ```

4. Follow the script's prompts.

   Configure (or disable) IPv4 management settings first, then IPv6. If you manually specify network settings, you must:

   - enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.
   - enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

5. Confirm that your settings are correct.

   If you entered settings incorrectly, type `n` at the prompt and press Enter. You can then enter the correct information. The console may display messages as your settings are implemented.

6. Log out of the appliance.
7. Your next step depends on the appliance:
   - To complete the setup of a managed device using its web interface, continue with Initial Setup Page: Devices on page 93.
   - To complete the setup of a Defense Center using its web interface, continue with Initial Setup Page: Defense Centers on page 100.

Performing Initial Setup on a Series 3 Device Using the CLI

SUPPORTED DEVICES: Series 3

Optionally, you can use the CLI to configure Series 3 devices instead of using the device's web interface. When you first log in to a newly configured device using the CLI, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, configure the device's network settings and detection mode. Finally, register the device to the Defense Center that will manage it.

When following the setup prompts, options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a device's setup web page does. For detailed information on these options, see Initial Setup Page: Devices on page 93.

To complete the initial setup on a Series 3 device using the CLI:

ACCESS: Admin

1. Log into the device. Use `admin` as the username and `Sourcefire` as the password.
   - For a Series 3 device attached to a monitor and keyboard, log in at the console.
   - If you connected a computer to the management interface of a Series 3 device using an Ethernet cable, SSH to the interface's default IPv4 address: 192.168.45.45.

   The device immediately prompts you to read the EULA.
2. Read and accept the EULA.
3. Change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

   Sourcefire recommends that you use strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary. For more information, see Change Password on page 95.

4. Configure network settings for the device.

   First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

   - enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.
   - enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

   For more information, see Network Settings on page 96. The console may display messages as your settings are implemented.

5. Select whether you want to allow changing of the device's network settings using the LCD panel.

   WARNING! Enabling this option can present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see Using the LCD Panel on a Series 3 Device on page 111.

6. Specify the detection mode based on how you deployed the device.

   For more information, see Detection Mode on page 98. The console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Defense Center, and displays the CLI prompt.

7. To use the CLI to register the device to the Defense Center that will manage it, continue with the next section, Registering a Series 3 Device to a Defense Center Using the CLI.

   You must manage devices with a Defense Center. If you do not register the device now, you must log in later and register it before you can add it to a Defense Center.

8. Log out of the appliance.

Registering a Series 3 Device to a Defense Center Using the CLI

SUPPORTED DEVICES: Series 3

If you configured a Series 3 device using the CLI, Sourcefire recommends that you use the CLI to register the device to a Defense Center at the conclusion of the setup script. It is easiest to register a device to its Defense Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique alphanumeric registration key is always required to register a device to a Defense Center. This is a simple key that you specify, and is not the same as a license key.

In most cases, you must provide the Defense Center's hostname or the IP address along with the registration key, for example:

```
configure manager add DC.example.com my_reg_key
```

However, if the device and the Defense Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the hostname, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

To register a device to a Defense Center:

Access: CLI Configuration

1. Log in to the device as a user with Configuration CLI access level:
   - If you are performing the initial setup from the console, you are already logged in as the `admin` user, which has the required access level.
   - Otherwise, SSH to the device's management IP address or host name.
2. At the prompt, register the device to a Defense Center using the `configure manager add` command, which has the following syntax:

   ```
   configure manager add {hostname | IPv4_address |
   IPv6_address | DONTRESOLVE} reg_key [nat_id]
   ```

   where:
   - `{`*`hostname`* | *`IPv4_address`* | *`IPv6_address`* | `DONTRESOLVE}` specifies either the fully qualified host name or IP address of the Defense Center. If the Defense Center is not directly addressable, use `DONTRESOLVE`.
   - *`reg_key`* is the unique alphanumeric registration key required to register a device to the Defense Center.
   - *`nat_id`* is an optional alphanumeric string used during the registration process between the Defense Center and the device. It is required if the hostname is set to `DONTRESOLVE`.
3. Log out of the appliance.

   The device is ready to be added to a Defense Center.

Initial Setup Page: Devices

For all managed devices (except Series 3 devices that you configured using the CLI; see Performing Initial Setup on a Series 3 Device Using the CLI on page 91), you must complete the setup process by logging into the device's web interface and specifying initial configuration options on a setup page.

You must change the administrator password, specify network settings if you have not already, and accept the EULA. You can also preregister the device to a Defense Center and specify a detection mode; the detection mode and other options you choose during registration determine the default interfaces, inline

sets, and zones that the system creates, as well as the policies that it initially applies to managed devices.

To complete the initial setup on a physical managed device using its web interface:

Access: Admin

1. Direct your browser to `https://mgmt_ip/`, where *mgmt_ip* is the IP address of the device's management interface.
   - For a device connected to a computer with an Ethernet cable, direct the browser on that computer to the default management interface IPv4 address: `https://192.168.45.45/`.
   - For a device where network settings are already configured, use a computer on your management network to browse to the IP address of the device's management interface.

   The login page appears.

2. Log in using `admin` as the username and `Sourcefire` as the password.

   The setup page appears. See the following sections for information on completing the setup:
   - Change Password on page 95
   - Network Settings on page 96
   - Series 3 Device LCD Panel Configuration on page 97
   - Remote Management on page 97
   - Time Settings on page 98
   - Detection Mode on page 98
   - Automatic Backups on page 100
   - End User License Agreement on page 100

3. When you are finished, click **Apply**.

   The device is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role.

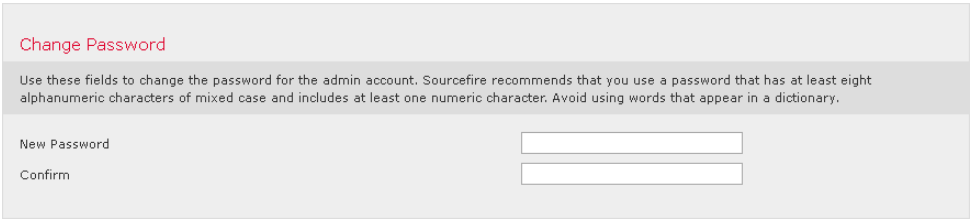
4. Log out of the device.

   The device is ready to be added to its managing Defense Center.

IMPORTANT! If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the device's management interface to the management network. If you need to access the device's web interface at any time, direct a browser on a computer on the management network to the IP address or host name that you configured during setup.

Change Password

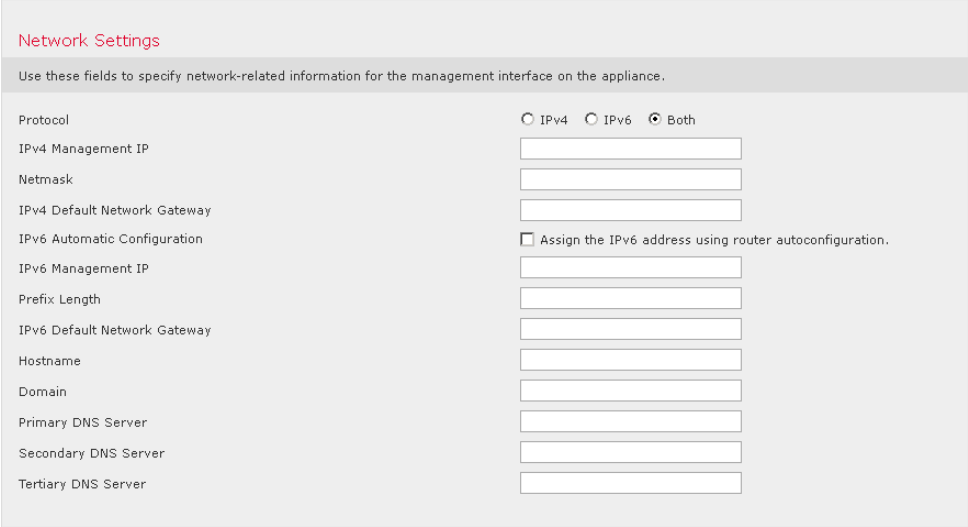
You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.



Sourcefire recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A device's network settings allow it to communicate on your management network. If you already configured the device's network settings, this section of the page may be pre-populated.



The Sourcefire 3D System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

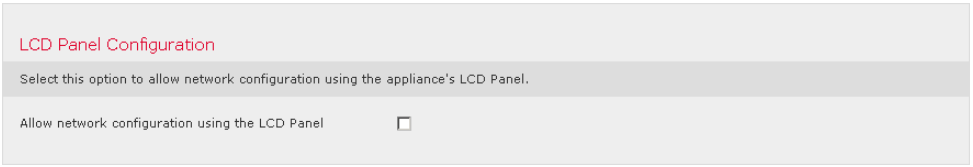
- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of 255.255.0.0).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of 112).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Series 3 Device LCD Panel Configuration

SUPPORTED DEVICES: Series 3

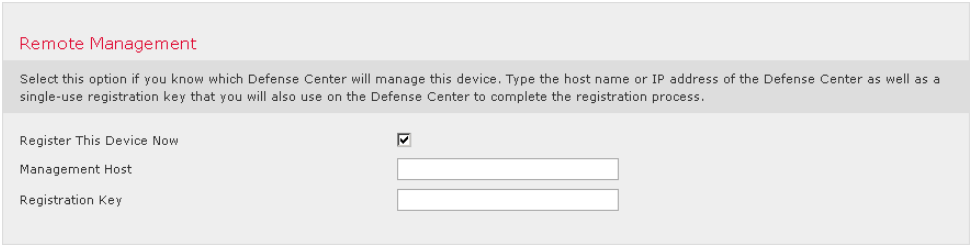
If you are configuring a Series 3 device, select whether you want to allow changing of the device's network settings using the LCD panel.



WARNING! Enabling this option can represent a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see Using the LCD Panel on a Series 3 Device on page 111.

Remote Management

You must manage a Sourcefire device with a Defense Center. For your convenience, the setup page allows you to preregister the device to the Defense Center that will manage it.

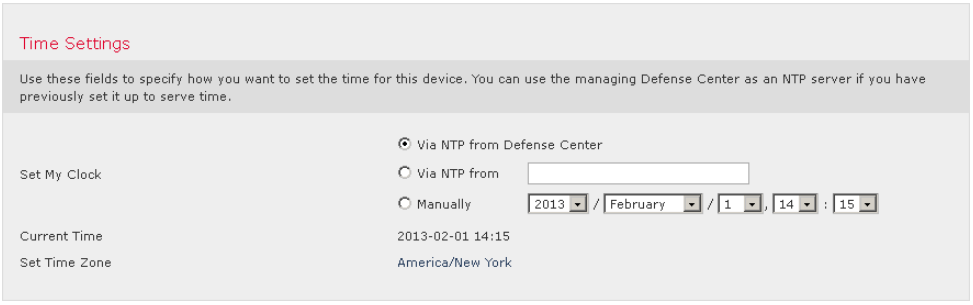


Leave the **Register This Device Now** check box enabled, then specify the IP address or fully qualified domain name of the managing Defense Center as the **Management Host**. Also, type the alphanumeric **Registration Key** you will later use to register the device to the Defense Center. Note that this is a simple key that you specify, and is not the same as the license key.

IMPORTANT! If the device and Defense Center are separated by a network address translation (NAT) device, defer device registration until after you complete the initial setup. See the Managing Devices chapter in the *Sourcefire 3D System User Guide* for more information.

Time Settings

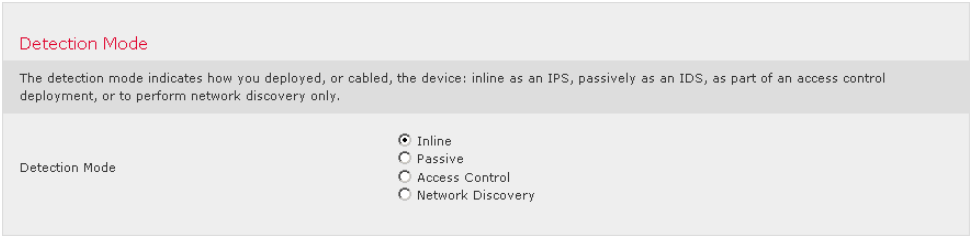
You can set the time for a device either manually or via network time protocol (NTP) from an NTP server, including the Defense Center. Sourcefire recommends that you use the Defense Center as the NTP server for its managed devices.



You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Detection Mode

The detection mode you choose for a device determines how the system initially configures the device's interfaces, and whether those interfaces belong to an inline set or security zone.



The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device's initial configurations. In general, you should choose a detection mode based on how your device is deployed:

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, you can perform file and malware detection, Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system (IPS). An IPS usually fails *open* and *allows* non-matching traffic.

In an inline deployment, you can also perform network-based advanced malware protection (AMP), file control, Security Intelligence filtering, and network discovery.

Although you can select the inline mode for any device, keep in mind that inline sets using the following interfaces lack bypass capability:

- non-bypass NetMods on 8000 Series devices
- SFP transceivers on 71xx Family devices

IMPORTANT! Reimaging resets devices in inline deployments to a non-bypass configuration; this disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process on page 199.

Access Control

Choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails *closed* and *blocks* non-matching traffic. Rules explicitly specify the traffic to pass.

You should also choose this mode if you want to take advantage of your device's specific hardware-based capabilities, which include (depending on model): clustering, strict TCP enforcement, fast-path rules, switching, routing, DHCP, NAT, and VPN.

In an access control deployment, you can also perform malware protection, file control, Security Intelligence filtering, and network discovery.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone

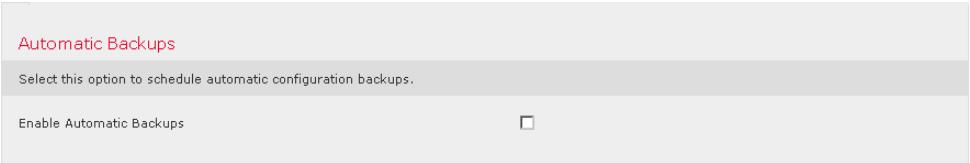
Initial Configurations Based on Detection Mode (Continued)

Detection Mode	Security Zones	Inline Sets	Interfaces
Access Control	none	none	none
Network Discovery	Passive	none	first pair assigned to Passive zone

Note that security zones are a Defense Center-level configuration which the system does not create until you actually register the device to the Defense Center. Upon registration, if the appropriate zone (Internal, External, or Passive) already exists on the Defense Center, the registration process adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *Sourcefire 3D System User Guide*.

Automatic Backups

The device provides a mechanism for archiving data so that configuration and event data can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.



Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**. The device is configured according to your selections and is ready to be added to its managing Defense Center.

Initial Setup Page: Defense Centers

For all Defense Centers, you must complete the setup process by logging into the Defense Center's web interface and specifying initial configuration options on a setup page. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.

The setup process also allows you to register and license devices. Before you can register a device, you must complete the setup process on the device itself, as well as add the Defense Center as a remote manager, or the registration will fail.

Keep the following points in mind when setting up a DC500 Defense Center after a reimage:

- The DC500 cannot use URL Filtering or Malware licenses.
- Although the DC500 can manage devices with Protection and Control licenses, you cannot perform Security Intelligence filtering or user control.
- The DC500 cannot display geolocation information.

For more information, see Supported Capabilities by Appliance Model on page 13 and Licensing the Sourcefire 3D System on page 19.

To complete the initial setup on a Defense Center using its web interface:

Access: Admin

1. Direct your browser to `https://mgmt_ip/`, where *mgmt_ip* is the IP address of the Defense Center's management interface.
   - For a Defense Center connected to a computer with an Ethernet cable, direct the browser on that computer to the default management interface IPv4 address: `https://192.168.45.45/`.
   - For a Defense Center where network settings are already configured, use a computer on your management network to browse to the IP address of the Defense Center's management interface.

   The login page appears.

2. Log in using `admin` as the username and `Sourcefire` as the password.

   The setup page appears. See the following sections for information on completing the setup:
   - Change Password on page 102
   - Network Settings on page 103
   - Time Settings on page 104
   - Recurring Rule Update Imports on page 104
   - Recurring Geolocation Updates on page 105

- Automatic Backups on page 105
- License Settings on page 105
- Device Registration on page 107
- End User License Agreement on page 109

3. When you are finished, click **Apply**.

   The Defense Center is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role.

   IMPORTANT! If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the Defense Center's management interface to the management network. Use a browser on a computer on the management network to access the Defense Center at the IP address or host name that you just configured, and complete the rest of the procedures in this guide.

4. Use the Task Status page (**System > Monitoring > Task Status**) to verify that the initial setup was successful.

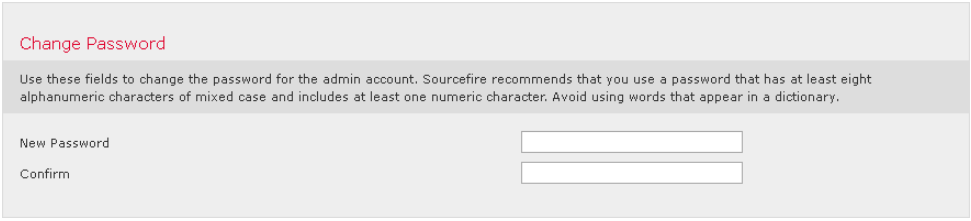
   The page auto-refreshes every ten seconds. Monitor the page until it lists a status of **Completed** for the initial device registration and policy apply tasks. If, as part of setup, you configured an intrusion rule or geolocation update, you can also monitor those tasks.

   The Defense Center is ready to use. See the *Sourcefire 3D System User Guide* for more information on configuring your deployment.

5. Continue with Next Steps on page 109.

Change Password

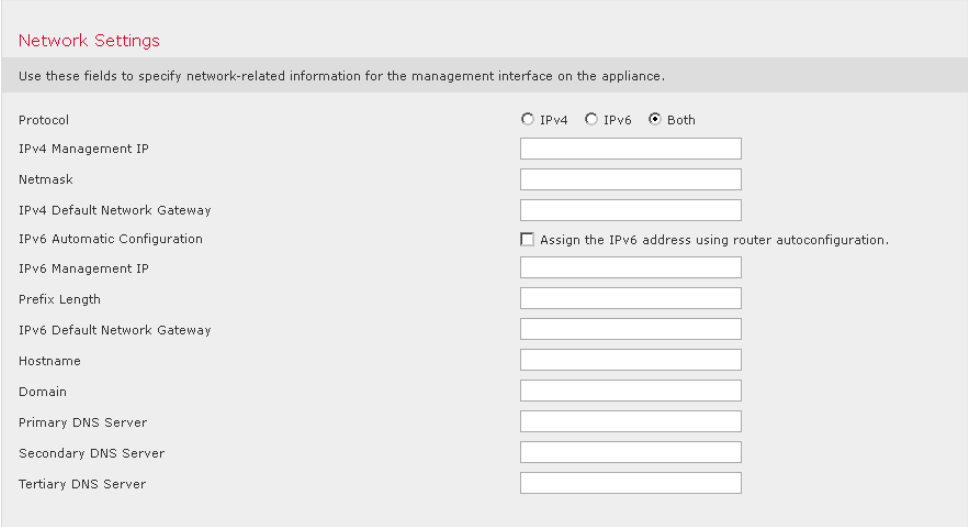
You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.



Sourcefire recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A Defense Center's network settings allow it to communicate on your management network. If you already configured the network settings, this section of the page may be pre-populated.



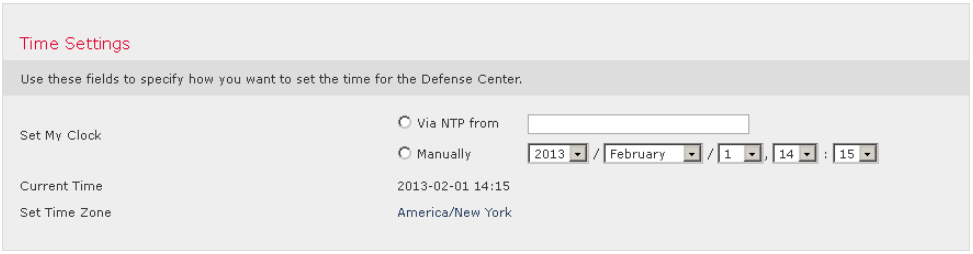
The Sourcefire 3D System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of 255.255.0.0).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of 112).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Time Settings

You can set the time for a Defense Center either manually or via network time protocol (NTP) from an NTP server.



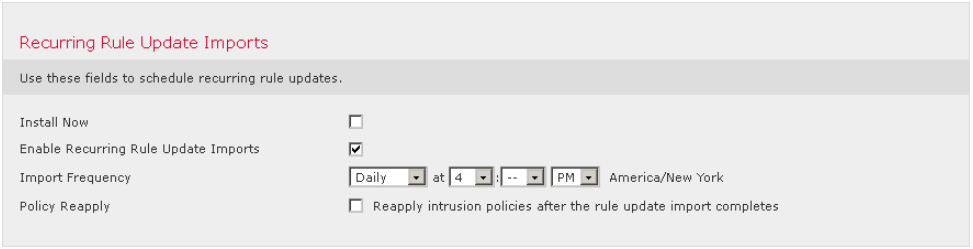
You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Recurring Rule Update Imports

LICENSE: Protection

As new vulnerabilities become known, the Sourcefire Vulnerability Research Team (VRT) releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables.

If you plan to perform intrusion detection and prevention in your deployment, Sourcefire recommends that you **Enable Recurring Rule Update Imports**.



You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, select **Install Now**.

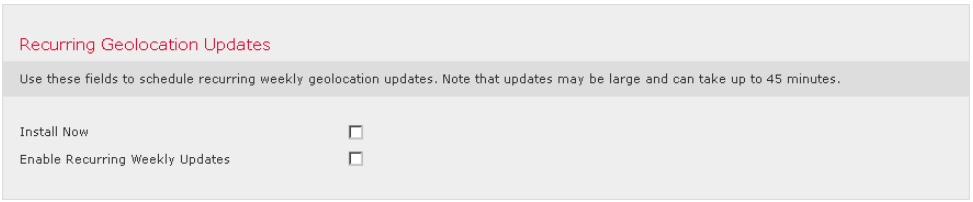
IMPORTANT! Rule updates may contain new binaries. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, rule updates may be large, so make sure to import rules during periods of low network use.

Recurring Geolocation Updates

SUPPORTED DEFENSE CENTERS: Any except DC500

You can use most Defense Centers to view geographical information about the routed IP addresses associated with events generated by the system, as well as monitor geolocation statistics in the dashboard and Context Explorer.

The Defense Center's geolocation database (GeoDB) contains information such as an IP address's associated internet service provider (ISP), connection type, proxy information, and exact location. Enabling regular GeoDB updates ensures that the system uses up-to-date geolocation information. If you plan to perform geolocation-related analysis in your deployment, Sourcefire recommends that you **Enable Recurring Weekly Updates**.



You can specify the weekly update frequency for the GeoDB. Click the time zone to change it using a pop-up window. To download the database as part of the initial configuration process, select **Install Now**.

IMPORTANT! GeoDB updates may be large and may take up to 45 minutes to install after download. You should update the GeoDB during periods of low network use.

Automatic Backups

The Defense Center provides a mechanism for archiving data so configurations can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.

Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the Defense Center.

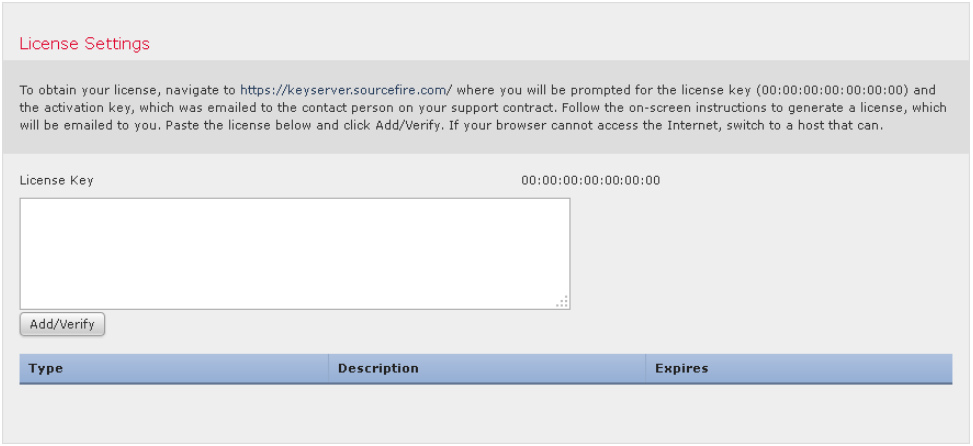
License Settings

You can license a variety of features to create an optimal Sourcefire 3D System deployment for your organization. A FireSIGHT license on the Defense Center is required to perform host, application, and user discovery. Additional

model-specific licenses allow your managed devices to perform a variety of functions. Because of architecture and resource limitations, not all licenses can be applied to all managed devices; see Supported Capabilities by Appliance Model on page 13 and Licensing the Sourcefire 3D System on page 19.

Sourcefire recommends that you use the initial setup page to add the licenses your organization has purchased. If you do not add licenses now, any devices you register during initial setup are added to the Defense Center as unlicensed; you must license each of them individually after the initial setup process is over. Note that if you are setting up a reimaged appliance and you kept your license settings as part of the restore process, this section may be pre-populated.

If you have not already obtained your licenses, click the link to navigate to `https://keyserver.sourcefire.com/` and follow the on-screen instructions. You need your license key (listed on the initial setup page), as well as the activation key previously emailed to the contact associated with your support contract.



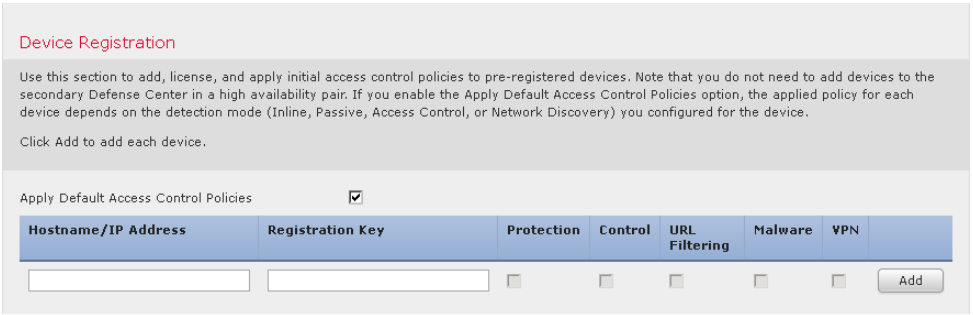
Add a license by pasting it into the text box and clicking **Add/Verify**. After you add a valid license, the page updates so you can track which licenses you have added. Add licenses one at a time.

Maximum 3D8250 Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	0	5
Maximum Virtual Device 64bit Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	5	0
Maximum DC1500 Licenses				
FireSIGHT Host	FireSIGHT User			
50000	50000			

Type	Description	Expires
3D8250	5 Protection License(s)	Never
3D8250	5 Control License(s)	Never
3D8250	5 VPN License(s)	Never
Virtual Device 64bit	5 Malware License(s)	2013-09-16 18:58:01
Virtual Device 64bit	5 Control License(s)	Never
Virtual Device 64bit	5 Protection License(s)	Never
DC1500	50000 FireSIGHT Host, 50000 FireSIGHT User License(s)	Never

Device Registration

A Defense Center can manage any device, physical or virtual, currently supported by the Sourcefire 3D System. You can add most pre-registered devices (see Remote Management on page 97) to the Defense Center during the initial setup process. However, if a device and the Defense Center are separated by a NAT device, you must add it after the setup process completes.



When registering devices, leave the **Apply Default Access Control Policies** check box enabled if you want to automatically apply access control policies to devices upon registration. Note that you cannot choose which policy the Defense Center applies to each device, only whether to apply them. The policy that is applied to

each device depends on the detection mode (see Detection Mode on page 98) you chose when configuring the device, as listed in the following table.

Default Access Control Policy Applied Per Detection Mode

Detection Mode	Default Access Control Policy
Inline	Default Intrusion Prevention
Passive	Default Intrusion Prevention
Access Control	Default Access Control
Network Discovery	Default Network Discovery

An exception occurs if you previously managed a device with a Defense Center and you changed the device's initial interface configuration. In this case, the policy applied by this new Defense Center page depends on the changed (current) configuration of the device. If there are interfaces configured, the Defense Center applies the Default Intrusion Prevention policy. Otherwise, the Defense Center applies the Default Access Control policy.

To add a device, type its **Hostname** or **IP Address**, as well as the **Registration Key** you specified when you registered the device. Remember this is a simple key that you specified, and is not the same as a license key.

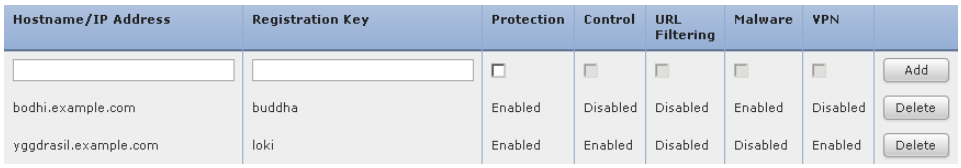
Then, use the check boxes to add licensed capabilities to the device. You can only select licenses you have already added to the Defense Center; see License Settings on page 105.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. However, the setup page does **not** prevent you from enabling unsupported licenses on managed devices, or enabling a capability for which you do not have a model-specific license. This is because the Defense Center does not determine the device model until later. The system cannot enable an invalid license, and attempting to enable an invalid license does not decrement your available license count.

For more information on licensing, including which Defense Centers you can use to apply each license to each device model, see Supported Capabilities by Appliance Model on page 13 and Licensing the Sourcefire 3D System on page 19.

IMPORTANT! If you enabled **Apply Default Access Control Policies**, you must enable a Protection license on the devices where you chose an **Inline** or **Passive** detection mode. You must also enable Protection on any previously managed device that has configured interfaces. Otherwise, the default policy (which requires Protection in those cases) will fail to apply.

After you enable licenses, click **Add** to save the device's registration settings and, optionally, add more devices.



If you selected the wrong options or mis-typed a device name, click **Delete** to remove it. You can then re-add the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**.

The Defense Center is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role. Continue with step 3 in Initial Setup Page: Defense Centers on page 100 to complete the initial setup of the Defense Center.

Next Steps

After you complete the initial setup process for an appliance and verify its success, Sourcefire recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Sourcefire 3D System User Guide*.

TIP! If you want to use a serial or LOM/SOL connection to access your appliance's console, you should redirect console output; see Redirecting Console Output on page 82. If you want to use LOM specifically, you must enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users on page 221.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Sourcefire recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Defense Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Sourcefire recommends that you use the Defense Center to apply the same system policy to itself and all the devices it manages.

By default, the Defense Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Sourcefire recommends that you use the Defense Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Sourcefire recommends that all the appliances in your deployment run the most recent version of the Sourcefire 3D System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

WARNING! Before you update any part of the Sourcefire 3D System, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

CHAPTER 5
USING THE LCD PANEL ON A SERIES 3 DEVICE

Series 3 devices allow you to view device information or configure certain settings using an LCD panel on the front of the device instead of the system's web interface.

The LCD panel has a display and four multi-function keys, and operates in multiple modes that show different information and allow different configurations depending on the state of the device.

For more information, see the following sections:

- Understanding LCD Panel Components on page 112 explains how to identify the components of the LCD panel and display the panel's main menu.
- Using the LCD Multi-Function Keys on page 113 explains how to use the multi-function keys on the LCD panel.
- Idle Display Mode on page 114 describes how the LCD panel displays various system information when the device is idle.
- Network Configuration Mode on page 115 explains how to use the LCD panel to configure the s for the device's management interface: the IPv4 or IPv6 address, subnet mask or prefix, and default gateway.

WARNING! Allowing reconfiguration using the LCD panel can present a security risk. You need only physical access, not authentication, to configure s using the LCD panel. For more information, see Using the LCD Panel on a Series 3 Device on page 111.

- System Status Mode on page 118 explains how you can view monitored system information, such as link state propagation, bypass status, and system resources, as well as change the LCD panel brightness and contrast.
- Information Mode on page 119 explains how you can view identifying system information such as the device's chassis serial number, IP address, model, and software and firmware versions.
- Error Alert Mode on page 121 describes how the LCD panel communicates error or fault conditions; for example, bypass, fan status, or hardware alerts.

IMPORTANT! The device must be powered on to use the LCD panel. For information on how to safely power on or shut down the device, see the Managing Devices chapter in the *Sourcefire 3D System User Guide.*

Understanding LCD Panel Components

The LCD panel on the front of a Series 3 device has a display and four multi-function keys:

- The display contains two lines of text (up to 17 characters each), as well as the multi-function key map. The map indicates, with symbols, the actions that you can perform with the corresponding multi-function keys.
- The multi-function keys allow you to view system information and complete basic configuration tasks, which vary according to the mode of the LCD panel. For more information, see Using the LCD Multi-Function Keys on page 113.

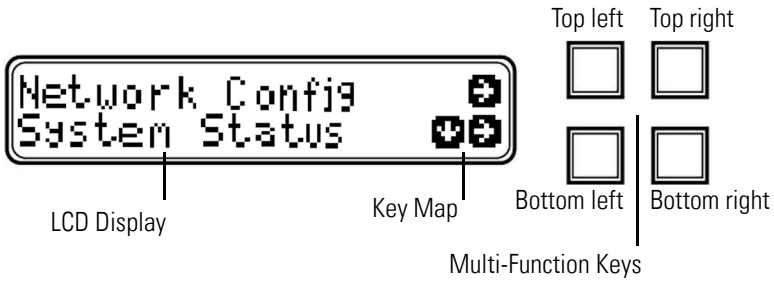
The following graphic shows the panel's default Idle Display mode, which does not include a key map.

LCD Panel, Idle Display mode

In Idle Display mode, the panel alternates between displaying the CPU utilization and free memory available, and the chassis serial number. You can access the Network Configuration, System Status, and Information modes by interrupting Idle Display mode to show the LCD panel's main menu.

The following graphic shows the main menu, which has a key map that corresponds to the four multi-function keys (top left, top right, bottom left, and bottom right).

LCD Panel, main menu



To access the main menu:

▶ In Idle Display mode, press any multi-function key.

The main menu appears.

- To change the device's s, see Network Configuration Mode on page 115.
- To view monitored system information or adjust the LCD panel brightness and contrast, see System Status Mode on page 118.
- To view identifying system information, see Information Mode on page 119.

IMPORTANT! Pressing a multi-function key as the LCD panel enters Idle Display mode can cause the panel to display an unexpected menu.

Using the LCD Multi-Function Keys

Four multi-function keys allow you navigate the menus and options on a Series 3 device's LCD panel. You can use the multi-function keys when a key map appears on the display. A symbol's location on the map corresponds to the function and location of the key used to perform that function. If no symbol is displayed, the corresponding key has no function.

TIP! The function of a symbol, and therefore the key map, varies according the LCD panel mode. If you do not get the result you expect, check the mode of the LCD panel.

The following table explains the multi-function key functions.

LCD Panel Multi-Function Keys

SYMBOL	DESCRIPTION	FUNCTION
↑	Up arrow	Scrolls up the list of current menu options.
↓	Down arrow	Scrolls down the list of current menu options.
←	Left arrow	Performs one of the following actions: • Takes no action and displays the LCD panel menu. • Moves the cursor to the left. • Re-enables editing.
→	Right arrow	Performs one of the following actions: • Enters the menu option displayed on that line. • Moves the cursor to the right. • Scrolls through continued text.
X	Cancel	Cancels the action.
+	Add	Increases the selected digit by one.
-	Subtract	Decreases the selected digit by one.
✓	Check mark	Accepts the action.

Idle Display Mode

The LCD panel enters Idle Display mode after 60 seconds of inactivity (you have not pressed any multi-function keys) with no detected errors. If the system detects an error, the panel enters Error Alert mode (see Error Alert Mode on page 121) until the error is resolved. Idle Display mode is also disabled when you are editing your s or running diagnostics.

In Idle Display mode, the panel alternates (at five second intervals) between displaying the CPU utilization and free memory available and the chassis serial number.

A sample of each display might look like this:

```
CPU: 50%
FREE MEM: 1024 MB
```

or:

```
Serial Number:
3D99-101089108-BA0Z
```

In Idle Display mode, press any multi-function key to enter the main menu; see Understanding LCD Panel Components on page 112.

IMPORTANT! Pressing a multi-function key as the LCD panel enters Idle Display mode can cause the panel to display an unexpected menu.

Network Configuration Mode

The Sourcefire 3D System provides a dual stack implementation for both IPv4 and IPv6 management environments. In Network Configuration mode, you can use the LCD panel to configure the s for a Series 3 device's management interface: the IP address, subnet mask or prefix, and default gateway.

By default, the ability to change s using the LCD panel is disabled. You can enable it during the initial setup process, or using the device's web interface. For more information, see Allowing Network Reconfiguration Using the LCD Panel on page 117.

WARNING! Enabling this option can present a security risk. You need only physical access, not authentication, to configure s using the LCD panel.

To configure s using Network Configuration mode:

1. In Idle Display mode, press any multi-function key to enter the main menu.

   The main menu appears:

   ```
   Network Config          →
   System Status        ↓ →
   ```

2. Press the right arrow (à) key on the top row to access Network Configuration mode.

   The LCD panel displays the following:

   ```
   IPv4                 ↓ →
   IPv6                   →
   ```

3. Press the right arrow key to select the IP address you want to configure.
   - For IPv4, the LCD panel might display the following:

     ```
     IPv4 set to DHCP.    ←
     Enable Manual?       →
     ```

   - For IPv6, the LCD panel might display the following:

     ```
     IPv6 Disabled.       ←
     Enable Manual?       →
     ```

4. Press the right arrow key to manually configure the network.
   - For IPv4, the LCD panel displays the IPv4 address. For example:

     ```
     IPv4 Address:      - +
     194.170.001.001    X →
     ```

   - For IPv6, the LCD panel displays a blank IPv6 address. For example:

     ```
     IPv6 Address:      - +
     0000:0000:0000:00  X →
     ```

   The first line on the panel indicates whether you are editing the IPv4 or IPv6 address. The second line displays the IP address you are editing. A cursor underlines the first digit, and represents the digit you are editing. The two symbols correspond with the multi-function keys to the right of each row.

   Note that the IPv6 address does not fit completely on the display. As you edit each digit and move the cursor to the right, the IPv6 address scrolls to the right.

5. Edit the digit underlined by the cursor, if needed, and move to the next digit in the IP address.
   - To edit the digit, press the minus (-) or plus (+) keys on the top row to decrease or increase the digit by one.
   - To move to the next digit in the IP address, press the right arrow key on the bottom row to move the cursor to the next digit to the right.

   With the cursor on the first digit, the LCD panel displays the cancel and right arrow symbols at the end of the IP address. With the cursor on any other digit, the LCD panel displays the left and right arrow symbols.

6. When you finish editing the IPv4 or IPv6 address, press the right arrow key again to display the check mark (✓) key to accept the changes.

   Before you press the right arrow key, the function symbols on the display looks like the following sample:

   ```
   IPv4 Address:      - +
   194.170.001.001    X →
   ```

   After you press the right arrow key, the function symbols on the display looks like the following sample:

   ```
   IPv4 Address:      X ✓
   194.170.001.001    ←
   ```

7. Press the check mark key to accept the changes to the IP address.

   For IPv4, the LCD panel displays the following:

   ```
   Subnet Mask:       - +
   000.000.000.000    X →
   ```

   For IPv6, the LCD panel displays the following:

   ```
   Prefix:            - +
   000.000.000.000    X →
   ```

8. Edit the subnet mask or prefix the same way you edited the IP address, and press the check mark key to accept the changes.

   The LCD panel displays the following:

   ```
   Default Gateway    - +
   000.000.000.000    X →
   ```

9. Edit the default gateway the same way you edited the IP address, and press the check mark key to accept the changes.

   The LCD panel displays the following:

   ```
   Save?              ✓
                      X
   ```

10. Press the check mark key to save your changes.

Allowing Network Reconfiguration Using the LCD Panel

Because it presents a security risk, the ability to change s using the LCD panel is disabled by default. You can enable it during the initial setup process (see Setting Up a Series 3 Device on page 89), or using the device's web interface as described in the following procedure.

To allow network reconfiguration using a device's LCD panel:

ACCESS: Admin

1. After you complete the initial setup of the device, log into the device's web interface using an account with Administrator privileges.
2. Select **System > Local > Configuration**.

   The Information page appears.
3. Click **Network**.

   The s page appears.
4. Under LCD Panel, select the **Allow reconfiguration of s** check box. When the security warning appears, confirm that you want to enable this option.

   TIP! For information on the other options on this page, see the *Sourcefire 3D System User Guide*.

5. Click **Save**.

   The s are changed.

System Status Mode

The LCD panel's System Status mode displays monitored system information, such as link state propagation, bypass status, and system resources. You can also change the LCD panel's brightness and contrast in System Status mode.

The following table describes the information and options available in this mode.

System Status Mode Options

Option	Description
Resources	Displays the CPU utilization and free memory available. Note that Idle Display mode also shows this information.

Link State	Displays a list of any inline sets currently in use and the link state status for that set. The first line identifies the inline set, and the second line displays its status (normal or tripped). For example:
	`eth2-eth3:`
	`normal`

Fail Open	Displays a list of the bypass inline sets in use and the status of those pairs, either normal or in bypass.
Fan Status	Displays a list and the status of the fans in the device.
Diagnostics	Accessible after pressing a specific key sequence available from Sourcefire Support. **Warning!** Do **not** access the diagnostics menu without the guidance of Sourcefire Support. Accessing the diagnostics menu without specific instructions from Sourcefire Support can damage your system.
LCD Brightness	Allows you to adjust the brightness of the LCD display.
LCD Contrast	Allows you to adjust the contrast of the LCD display.

To enter System Status mode and view monitored system information:

1. In Idle Display mode, press any multi-function key to enter the main menu.

   The main menu appears:

   ```
   Network Config          →
   System Status        ↓  →
   ```

2. Press the right arrow (→) key on the bottom row to access System Status mode.

   The LCD panel displays the following:

   ```
   Resources          ↓ →
   Link State         ↓ →
   ```

3. Scroll through the options by pressing the down arrow (↓) key. Press the right arrow key in the row next to the status you want to view.

   Depending on the option you chose, the LCD panel displays the information listed in the System Status Mode Options table on page 118. To change the LCD panel brightness or contrast, see the next procedure.

To adjust the LCD panel brightness or contrast:

1. In System Status mode, scroll through the options by pressing the down arrow (↓) key until the LCD panel displays the LCD Brightness and LCD Contrast options:

   ```
   LCD Brightness     ↓ →
   LCD Contrast       ↓ →
   ```

2. Press the right arrow key in the row next to the LCD display feature (brightness or contrast) you want to adjust.

   The LCD panel displays the following:

   ```
   Increase             →
   Decrease           ↓ →
   ```

3. Press the right arrow key to increase or decrease the display feature you have selected.

   The LCD display changes as you press the keys.

4. Press the down arrow to display the Exit option:

   ```
   Decrease           ↓ →
   Exit                 →
   ```

5. Press the right arrow key in the Exit row to save the setting and return to the main menu.

Information Mode

The LCD panel's Information mode displays identifying system information such as the device's chassis serial number, IP address, model, and software and firmware versions. Sourcefire Support may require this information if you call for assistance.

The following table describes the information available in this mode.

Information Mode Options

OPTION	DESCRIPTION
IP address	Displays the IP address of the device's management interface.
Model	Displays the device's model.
Serial number	Displays the device's chassis serial number.
Versions	Displays the device's system software and firmware versions. Use the multi-function keys to scroll through the following information: • Product version • NFE version • Micro Engine version • Flash version • GerChr version

To enter Information mode and view identifying system information:

1. In Idle Display mode, press any multi-function key to enter the main menu.

   The main menu appears:

   ```
   Network Config        →
   System Status      ↓  →
   ```

2. Scroll through the modes by pressing the down arrow (↓) key until the LCD panel displays Information mode:

   ```
   System Status      ↓  →
   Information        ↓  →
   ```

3. Press the right arrow (→) key on the bottom row to access Information mode.
4. Scroll through the options by pressing the down arrow (↓) key. Press the right arrow key in the row next to the information you want to view.

   Depending on the option you chose, the LCD panel displays the information listed in the Information Mode Options table on page 120.

Error Alert Mode

When an error or fault condition occurs, Error Alert mode interrupts Idle Display mode. In Error Alert mode, the LCD display flashes and displays one or more of the errors listed in the following table.

LCD Panel Error Alerts

Error	Description
Hardware alarm	Alerts on hardware errors
Link state propagation	Displays the link state of paired interfaces
Bypass	Displays the status of inline sets configured in bypass mode
Fan status	Alerts when a fan reaches a critical condition

To view multiple error alerts:

Access:

- Use the multi-function keys to scroll through the list of error alerts.

  For more information, see the LCD Panel Multi-Function Keys table on page 114.

To exit Error Alert mode:

- Press the appropriate multi-function key as indicated on the LCD display.

  If you exit Error Alert mode before you resolve the error that triggered the alert, the LCD panel returns to Error Alert mode.

CHAPTER 6
HARDWARE SPECIFICATIONS

The Sourcefire 3D System is delivered on a variety of appliances to meet the needs of your organization. See the Rack and Cabinet Mounting Options on page 122 for information on installing the appliance in a rack.

The hardware specifications for each of the appliances are described in the following sections:

Rack and Cabinet Mounting Options

You can mount Sourcefire appliances in racks and server cabinets. The appliance comes with a rack-mounting kit except for the 3D500, 3D7010, 3D7020, and 3D7030. For information on mounting the appliance in a rack, refer to the instructions delivered with the rack-mounting kit.

The 3D500 is a desktop device and can be rack-mounted. The 3D7010, 3D7020, and 3D7030 require a tray and rack-mounting kit, available separately. You can purchase rack and cabinet mounting kits for other appliances separately.

Sourcefire Defense Centers

See the following sections for more information about your Defense Center.

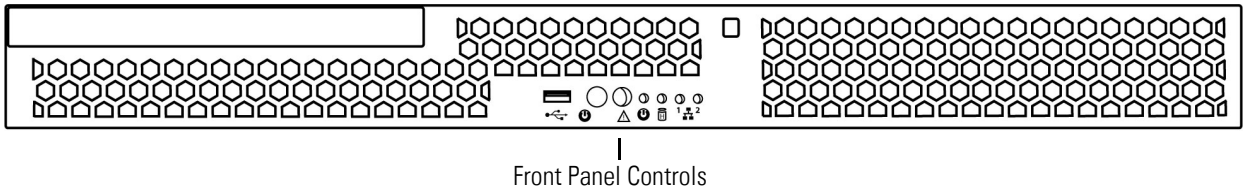
Sourcefire DC750

The DC750 is a 1U appliance delivered on two different chassis (Rev 1 and Rev 2). Specifications vary but the appliances function identically. See the following sections for more information about the appliance:

DC750 Chassis Front View

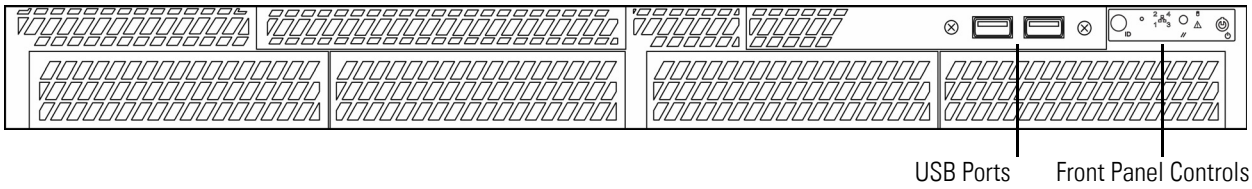
The front of the DC750 (Rev 1) chassis contains the front panel controls.

DC750 (Rev 1)



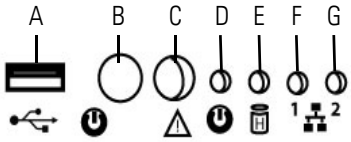
The front of the DC750 (Rev 2) chassis contains the front panel controls.

DC750 (Rev 2)



The following diagram illustrates the front panel controls and LEDs for the DC750 (Rev 1).

DC750 (Rev 1)

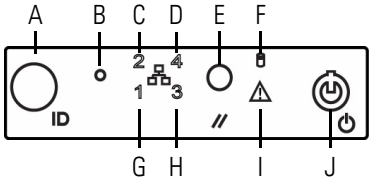


Front Panel Components (Rev 1)

A	USB port	E	Fixed disk drive status LED
B	Power button	F	NIC 1 activity status LED
C	System status LED	G	NIC 2 activity status LED
D	Power LED		

The following diagram illustrates the front panel controls and LEDs for the DC750 (Rev 2). The hard disk drive and system status icons, the numbers for the NIC (1, 2, 3, and 4) activity status, and the power button are also the LEDs.

DC750 (Rev 2)



Front Panel Components (Rev 2)

A	ID button with ID LED	F	Hard disk drive status LED
B	Non-maskable interrupt button	G	NIC 1 activity status LED
C	NIC 2 activity status LED	H	NIC 3 activity status LED
D	NIC 4 activity status LED	I	System status LED
E	Reset button	J	Power button with power LED

The front panel of the chassis houses five LEDs which you can view to display the system's operating state. The DC750 Front Panel LEDs table describes the LEDs on the front panel.

DC750 Front Panel LEDs

LED	DESCRIPTION
System status	Indicates system status: • A green light indicates the system is operating normally. • A blinking green light indicates the system is operating in a degraded condition. DC750 (Rev 1) only: • An amber light indicates the system is in a critical or non-recoverable condition. • A blinking amber light indicates the system is in a non-critical condition. **IMPORTANT!** The amber status light takes precedence over the green status light. When the amber light is on or blinking, the green light is off. For more information, see the DC750 System Status table on page 126.
Power	Indicates whether the system has power or is sleeping: • A green light indicates the system is operating normally. • No light indicates the system is off. • A blinking green light indicates the system is sleeping. The sleep indication is maintained on standby by the chipset. If the system is powered down without going through BIOS, the state in effect at the time of power off will be restored when the system is powered on until the BIOS clears it. If the system is not powered down normally, it is possible that the power light will be blinking at the same time that the system status light is off due to a failure or configuration change that prevents the BIOS from running.
Hard drive activity	Indicates hard drive activity: • A blinking green light indicates the fixed disk drive is active. • No light indicates no drive activity, or the system is powered off or sleeping. DC750 (Rev 1) only: An amber light indicates there is a fixed disk drive fault. Drive activity is determined from the onboard hard disk controllers. The server board also provides a header giving access to this light for add-in controllers.
NIC activity	Indicates activity between the system and the network: • A blinking green light indicates there is activity. • No light indicates there is no activity.

The DC750 System Status table describes the conditions where the system status LED might be lit.

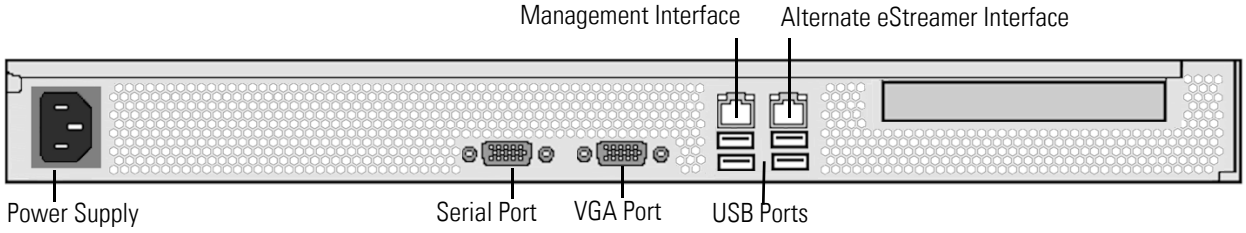
DC750 System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • the system is unable to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • BIOS has disabled or mapped out some of the system memory

DC750 Chassis Rear View

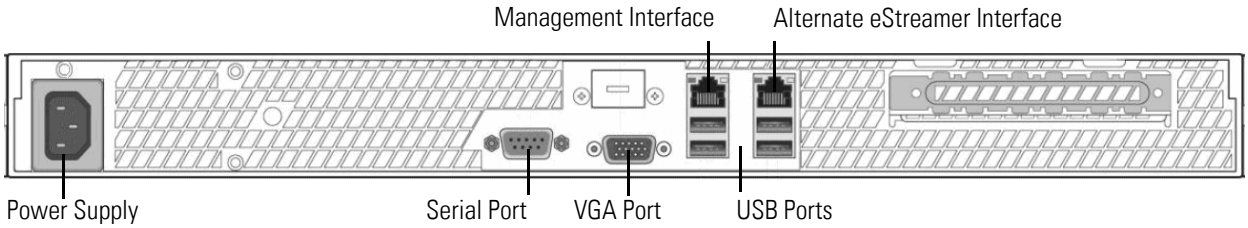
The rear of the chassis contains the power supply and connection ports for the DC750 (Rev 1).

DC750 (Rev 1)



The rear of the chassis contains the power supply and connection ports for the DC750 (Rev 2).

DC750 (Rev 2)



The DC750 System Components: Rear View table describes the features that appear on the rear of the appliance.

DC750 System Components: Rear View

Feature	Description
Power supply	Provides power to the Defense Center through an AC power source
Serial port, VGA port USB ports	Allows you to attach a monitor, keyboard, and mouse to the device
10/100/1000Mbps Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Alternate eStreamer interface	Provides an alternate interface for the eStreamer client

The 10/100/1000Mbps management interface is located on the rear of the appliance. The DC750 Management Interface LEDs table describes the LEDs associated with the management interface.

DC750 Management Interface LEDs

LED	Description
Left (link)	Indicates whether the link is up: • If the light is on, the link is up. • No light indicates there is no link.
Right (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no link.

DC750 Physical and Environmental Parameters

The DC750 (Rev 1) Physical and Environmental Parameters table describes the physical attributes and the environmental parameters for the appliance.

DC750 (Rev 1) Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	20.0 in. x 16.93 in. x 1.67 in. (50.8 cm x 43.0 cm x 4.24cm)
Max weight	33 lbs. (15 kg)
Power supply	350 W power supply for 120 VAC 9.5 Ampere maximum at 110 volts, 50/60 Hz 4.75 Ampere maximum at 220 volts, 50/60 Hz
Operating temperature	50°F to 95°F (10°C to 35°C) with the maximum rate of change not to exceed 18°F (10°C) per hour
Non-operating temperature	-40°F to +158°F (-40°C to +70°C)
Non-operating humidity	90%, non-condensing at 95°F (35°C)
Acoustic noise	<7.0 dBA (rack mount) in an idle state at typical office ambient temperature
Operating shock	No errors with half a sine wave shock of 2G (with 11 msec. duration)
Package shock	Operational after 24 in. (60 cm) free fall although cosmetic damage may be present; chassis weight of 40 to 80 lbs. (18 to 36 kg)
ESD	+/- 12 kV for air discharge and 8 K for contact
Airflow	Front to back
System cooling requirements	1660 BTU/hour

The DC750 (Rev 2) Physical and Environmental Parameters table describes the physical attributes and the environmental parameters for the appliance.

DC750 (Rev 2) Physical and Environmental Parameters

PARAMETER	DC750 (REV 2)
Form factor	1U
Dimensions (D x W x H)	21.8 in. x 17.25 in. x 1.67 in. (55.37 cm x 43.82 cm x 4.24 cm)
Max weight	33 lbs. (15 kg)
Power supply	250 W power supply for 120 VAC 6.0 Ampere maximum at 110 volts, 50/60 Hz 3.0 Ampere maximum at 220 volts, 50/60 Hz
Operating temperature	50°F to 95°F (10°C to 35°C) with the maximum rate of change not to exceed 18°F (10°C) per hour
Non-operating temperature	-40°F to +158°F (-40°C to +70°C)
Non-operating humidity	90%, non-condensing at 95°F (35°C)
Acoustic noise	7.0 dBA in an idle state at typical office ambient temperature (23 +/- 2°C, 73 +/- 4°F
Operating shock	No errors with half a sine wave shock of 2G (with 11 msec. duration)
Package shock	Operational after 24 in. (60 cm) free fall although cosmetic damage may be present; chassis weight of 40 to 80 lbs. (18 to 36 kg)
ESD	+/- 12 kV for air discharge and 8 K for contact
Airflow	Front to back
System cooling requirements	1660 BTU/hour

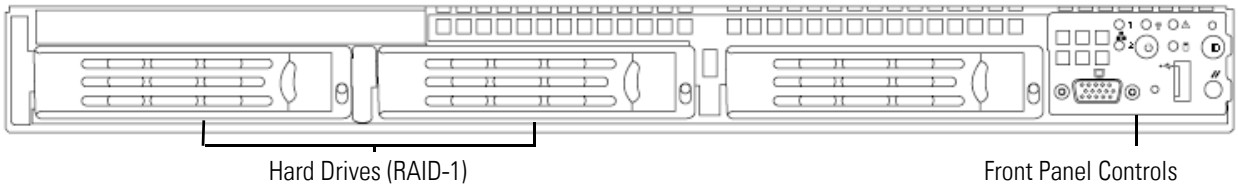
Sourcefire DC1500

The DC1500 is a 1U appliance. See the following sections for more information about the appliance:

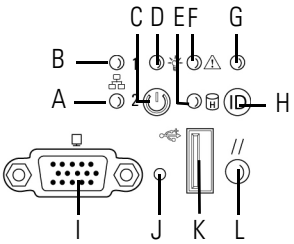
- DC1500 Chassis Front View on page 130
- DC1500 Chassis Rear View on page 132
- DC1500 Physical and Environmental Parameters on page 134

DC1500 Chassis Front View

The front of the chassis contains the hard drives and the front panel controls.



The following diagram illustrates the front panel controls and LEDs.



Front Panel Components

A	NIC 2 activity LED	G	ID LED
B	NIC 1 activity LED	H	ID button
C	Power button	I	Video connector (not available)
D	Power/sleep LED	J	Non-maskable interrupt button
E	Fixed disk drive status	K	USB 2.0 connector
F	System status LED	L	Reset button

The front panel of the chassis houses six LEDs, which you can view with or without the front bezel to display the system's operating state. The DC1500 Front Panel LEDs table describes the LEDs on the front panel.

DC1500 Front Panel LEDs

LED	Description
NIC 1 activity NIC 2 activity	Indicates activity between the system and the network: • A blinking green light indicates activity. • No light indicates no activity.

DC1500 Front Panel LEDs (Continued)

LED	DESCRIPTION
Power/sleep	Indicates whether the system has power or is sleeping: • A green light indicates the system is operating normally. • A blinking green light indicates the system is sleeping. • No light indicates the system does not have power. The sleep indication is maintained on standby by the chipset. If the system is powered down without going through BIOS, the state in effect at the time of power off will be restored when the system is powered on until the BIOS clears it. If the system is not powered down normally, it is possible that the power light will be blinking at the same time that the system status light is off due to a failure or configuration change that prevents the BIOS from running.
Hard drive activity	Indicates hard drive activity: • A blinking green light indicates the fixed disk drive is active. • An amber light indicates there is a fixed disk drive fault. • No light indicates there is no drive activity, or the system is powered off or sleeping. Drive activity is determined from the onboard hard disk controllers. The server board also provides a header giving access to this light for add-in controllers.
System status	Indicates system status: • A green light indicates the system is operating normally. • A blinking green light indicates the system is operating in a degraded condition. • An amber light indicates the system is in a critical or non-recoverable condition. • A blinking amber light indicates the system is in a non-critical condition. • No light indicates the Power On Self Tests (POST) is underway or the system has stopped. **IMPORTANT!** The amber status light takes precedence over the green status light. When the amber light is on or blinking, the green light is off. For more information, see the DC750 System Status table on page 126.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.

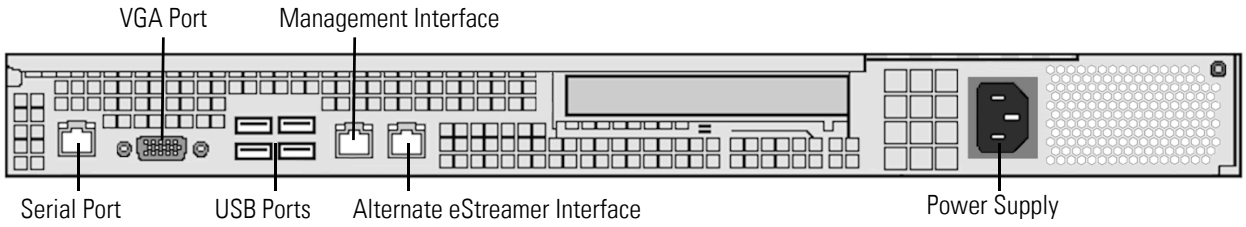
The DC1500 System Status table describes the conditions under which the system status LED might be lit.

DC1500 System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • the system is unable to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • BIOS has disabled or mapped out some of the system memory

DC1500 Chassis Rear View

The rear of the chassis contains the connection ports and power supply.



The DC1500 System Components: Rear View table describes the features that appear on the rear of the appliance.

DC1500 System Components: Rear View

Feature	Description
Power supply	Provides power to the Defense Center through an AC power source.
VGA port USB ports	Allows you to attach a monitor, keyboard, and mouse to the Defense Center.
10/100/1000Mbps Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Alternate eStreamer interface	Provides an alternate interface for the eStreamer client
RJ45 serial port	Allows you to establish a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the appliance. The RJ45 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic. See the DC1500 Serial Port Pin Assignments table on page 134. **IMPORTANT!** You cannot use the front and the rear panel serial ports at the same time.

The 10/100/1000Mbps management interface is located on the rear of the appliance. The DC1500 Management Interface LEDs table describes the LEDs associated with the management interface.

DC1500 Management Interface LEDs

LED	Description
Left (link)	Indicates whether the link is up: • If the light is on, the link is up. • No light indicates there is no link.
Right (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.

The DC1500 Serial Port Pin Assignments table describes the signal present on the DB-9 connector.

DC1500 Serial Port Pin Assignments

Pin	Signal	Description
1	DCD	Carrier detect
2	RD	Received data
3	TD	Transmitted data
4	DTR	Data terminal ready
5	GND	Ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

DC1500 Physical and Environmental Parameters

The DC1500 Physical and Environmental Parameters table describes the physical attributes and the environmental parameters for the appliance.

DC1500 Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	27.2 in.x 16.93 in. x 1.7 in. (69.1 cm x 43.0 cm x 4.3 cm)
Max weight	34 lbs. (15.4 kg)
Power supply	600 W power supply for 120 VAC 9.5 Ampere maximum at 110 volts, 50/60 Hz 4.75 Ampere maximum at 220 volts, 50/60 Hz
Operating temperature	50°F to 95°F (10°C to 35°C)
Non-operating temperature	-40°F to +158°F (-40°C to +70°C)

DC1500 Physical and Environmental Parameters (Continued)

Parameter	Description
Non-operating humidity	90%, non-condensing at 82.4°F (28°C)
Acoustic noise	<7.0 dBA (rack mount) in an idle state at typical office ambient temperature
Operating shock	No errors with half a sine wave shock of 2G (with 11 msec. duration)
Package shock	Operational after 24 in. (60 cm) free fall although cosmetic damage may be present; chassis weight of 40 to 80 lbs. (18 to 36 kg)
ESD	+/- 15 kV (I/O port +/-8 KV) per Intel environment test specification
Airflow	Front to back
System cooling requirements	2550 BTU/hour

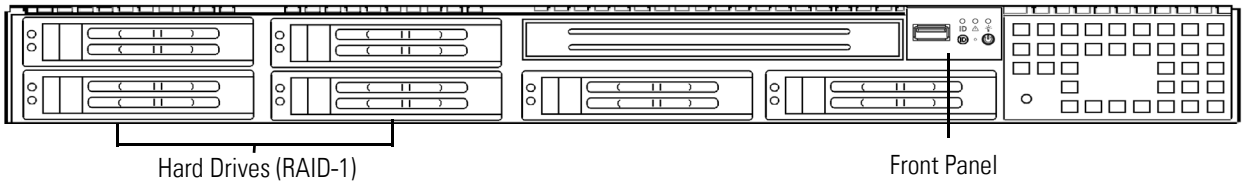
Sourcefire DC3500

The DC3500 is a 1U appliance. See the following sections for more information about the appliance:

- DC3500 Chassis Front View on page 135
- DC3500 Chassis Rear View on page 138
- DC3500 Physical and Environmental Parameters on page 141

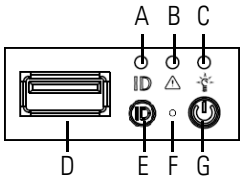
DC3500 Chassis Front View

The front of the chassis contains the hard drives and the front panel.



The front of the appliance includes controls and LED displays for the front panel.

The following diagram illustrates the front panel controls and LEDs.



Front Panel Components

A	ID LED	E	ID button
B	System status LED	F	Reset button
C	Power LED	G	Power button
D	USB port		

The front panel of the chassis houses three LEDs, which display the system's operating state. The DC3500 Front Panel LEDs table describes the LEDs on the front panel.

DC3500 Front Panel LEDs

LED	DESCRIPTION
Power	Indicates whether the system has power. • A green light indicates that the system has power. • No light indicates the system does not have power.
System status	Indicates the system status. • A green light indicates the system is operating normally. • A blinking green light indicates the system is operating in a degraded condition. • A blinking amber light indicates the system is in a non-critical condition. • An amber light indicates the system is in a critical or non-recoverable condition. • No light indicates the system is starting up or off. **IMPORTANT!** The amber status light takes precedence over the green status light. When the amber light is on or blinking, the green light is off. See the DC3500 System Status table on page 137 for more information.
Hard drive activity	Indicates the hard drive status. • A blinking green light indicates the fixed disk drive is active. • An amber light indicates a fixed disk drive fault. • No light indicates there is no drive activity or the system is powered off.

DC3500 Front Panel LEDs (Continued)

LED	Description
NIC activity	Indicates whether there is any network activity. • A green light indicates there is network activity. • No light indicates there is no network activity.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.

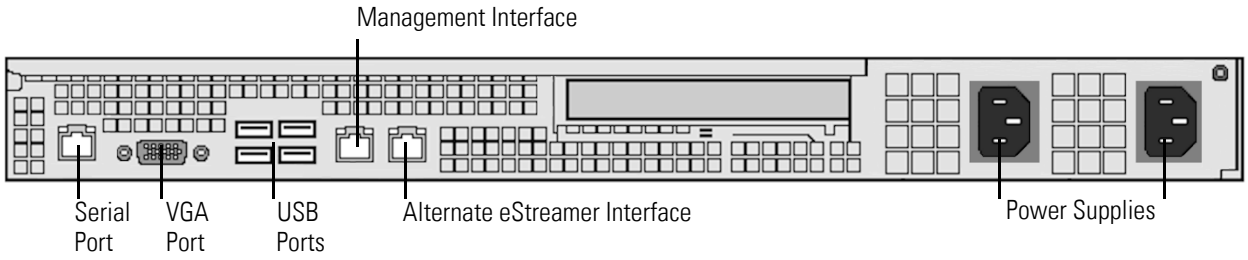
The DC3500 System Status table describes the conditions under which the system status LED might be lit.

DC3500 System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **TIP!** If you observe a degraded condition indication, check your power supply connections first. Power down the appliance, disconnect both power cords, reconnect the power cords to re-seat them, and then restart the appliance. **Warning!** To power down safely, use the procedure in the Managing Devices chapter in the *Sourcefire 3D System User Guide*, or the `shutdown -h now` command from the Defense Center's shell.

DC3500 Chassis Rear View

The rear of the chassis contains the connection ports and power supplies.



The DC3500 System Components: Rear View table describes the features that appear on the rear of the appliance.

DC3500 System Components: Rear View

FEATURE	DESCRIPTION
PS/2 mouse connector PS/2 keyboard connector VGA port USB ports	Allows you to attach a monitor, keyboard, and mouse to the appliance, as an alternative to using the RJ45 serial port, to establish a direct workstation-to-appliance connection. You also must use a USB port to restore the appliance to its original factory-delivered state, using the thumb drive delivered with the appliance.
RJ45 serial port	Allows you to establish a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the appliance. The RJ45 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic. See the DC3500 Serial Port Pin Assignments table on page 140. **IMPORTANT!** You cannot use the front and the rear panel serial ports at the same time.
10/100/1000Mbps Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Alternate eStreamer interface	Provides an alternate interface for the eStreamer client
Redundant power supplies	Provides power to the appliance through an AC power source

The 10/100/1000Mbps management interface is located on the rear of the appliance. The DC3500 Management Interface LEDs table describes the LEDs associated with the management interface.

DC3500 Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The DC3500 Power Supply LEDs table describes the LEDs associated with the dual power supplies.

DC3500 Power Supply LEDs

LED	Description
Off	The power supply is not plugged in.
Amber	No power supplied to this module. OR A power supply critical event such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking amber	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

The DC3500 Serial Port Pin Assignments table describes the signal present on the DB-9 connector.

DC3500 Serial Port Pin Assignments

Pin	Signal	Description
1	DCD	Carrier detect
2	RD	Received data
3	TD	Transmitted data
4	DTR	Data terminal ready
5	GND	Ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

The DC3500 Internal USB Connector Pin-Out table describes the signal present on the USB Connector.

DC3500 Internal USB Connector Pin-Out

Pin	Signal Name	Description
1	USB2_VBUS4	USB power (port4)
2	USB2_VBUS5	USB power (port 5)
3	USB_ICH_P4N_CONN	USB port 4 negative signal
4	USB_ICH_P5N_CONN	USB port 5 negative signal
5	USB_ICH_P4P_CONN	USB port 4 positive signal
6	USB_ICH_P5P_CONN	USB port 5positive signal
7	Ground	
8	Ground	

DC3500 Internal USB Connector Pin-Out (Continued)

Pin	Signal Name	Description
9	Key	No pin
10	TP_ISB_ICH_NC	Test point

DC3500 Physical and Environmental Parameters

The DC3500 Physical and Environmental Parameters table describes the physical attributes and the environmental parameters for the appliance.

DC3500 Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	26.2 in. x 16.93 in. x 1.7 in. (66.5 cm x 43.0 cm x 4.3 cm)
Weight	38 lbs. (17.2 kg)
Power supply	Dual 650 W redundant power supplies for 120 VAC 8.5 Amp max at 110 volts, 50/60 Hz 4.2 Amp max at 220 volts, 50/60 Hz
Operating temperature	50°F to 95°F (10°C to 35°C)
Non-operating temperature	-40°F to 158°F (-40°C to 70°C)
Operating humidity	5% to 85%
Non-operating humidity	90%, non-condensing at 95°F (35°C)
Acoustic noise	< 7.0 BA (rack mount) in an idle state at typical office ambient temperature
Operating shock	No errors with half a sine wave shock of 2G (with 11 msec. duration)
Packaged shock	Operational after 24 in. (60 cm) free fall although cosmetic damage may be present; chassis weight of 40 to 80 lbs (18 to 36 kg)
ESD	+/- 15KV (I/O port +/-8KV) per Intel environment test specification

DC3500 Physical and Environmental Parameters (Continued)

Parameter	Description
Airflow	Front to back
System cooling requirements	2550 BTU/hr
RoHS	Complies with RoHS Directive 2002/95/EC

Sourcefire Series 2 Devices

Series 2 devices are available new on the 3D500/1000/2000. Other Series 2 devices can be upgraded from 4.10 to 5.2 using the process described in Restoring a Sourcefire Appliance to Factory Defaults on page 198.

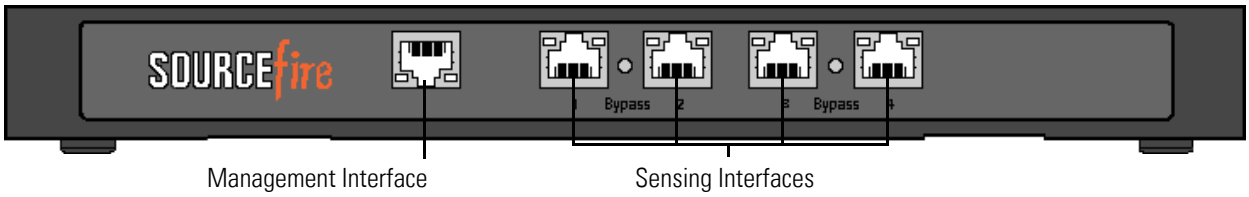
Sourcefire 3D500, 3D1000 and 3D2000 Devices

The 3D500, 3D1000, and 3D2000 devices are delivered as desktop devices. Optionally, you can rack-mount the device using a 1U rack-mounting kit. See the following sections for more information about the appliance:

- 3D500, 3D1000, or 3D2000 Chassis Front View on page 142
- 3D500, 3D1000, and 3D2000 Chassis Rear View on page 144
- 3D500/1000/2000 Physical and Environmental Parameters on page 145

3D500, 3D1000, or 3D2000 Chassis Front View

The front of the chassis contains the management and sensing interfaces.



The following table describes the features on the front of the appliance.

3D500, 3D1000, and 3D2000 System Components: Front View

Feature	Description
10/100 Ethernet Management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Gigabit sensing interfaces	Allows you to use four gigabit copper Ethernet bypass interfaces in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system. The 3D500 can monitor one network as an IPS, while the 3D1000 and 3D2000 can monitor two networks as an IPS. If you want to take advantage of the device's automatic bypass capability, you must use the two interfaces on the left or the two interfaces on the right as paired interfaces on a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure the interface set as inline with bypass.

The 10/100 management interface is located on the front of the appliance. The following table describes the LEDs associated with the management interface.

3D500, 3D1000, and 3D2000 Management Interface LEDs

LED	Description
Left (link)	Indicates whether the link is up. If the light is on, the link is up. If the light is off, there is no link.
Right (activity)	Indicates activity on the port. If the light is blinking, there is activity. If the light is off, there is no activity.

The following table describes how the LEDs function.

3D500, 3D1000, and 3D2000 Bypass LEDs

Status	Description
On	The interface has link and is passing traffic.
Off	The interface pair is in bypass mode; that is, it has failed open. OR The interface pair is not an inline bypass interface set.

3D500, 3D1000, and 3D2000 Chassis Rear View

The rear of the chassis contains the connection ports and power supply.

The following table describes the features that appear on the rear of the appliance.

3D500, 3D1000, and 3D2000 System Components: Rear View

Feature	Description
Power supply	Provides power to the appliance through an AC power source.
Serial port	Allows you to establish a direct workstation-to-appliance connection. This gives you direct access to all of the appliance's management services.
VGA port	Allows you to attach a monitor to the appliance, as an alternative to using the serial port to establish a direct workstation-to-appliance connection.
USB ports	Allows you to attach a monitor to the appliance, as an alternative to using the serial port to establish a direct workstation-to-appliance connection. You must also use a USB port to restore the appliance to its original factory-delivered state, using the thumb drive delivered with the appliance.
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.

The following table describes the signal present on the DB-9 connector.

3D500, 3D1000, and 3D2000 Serial Port Pin Assignments

Pin	Signal	Description
1	DCD	Carrier detect
2	RD	Received data
3	TD	Transmitted data
4	DTR	Data terminal ready

3D500, 3D1000, and 3D2000 Serial Port Pin Assignments (Continued)

Pin	Signal	Description
5	GND	Ground
6	DSR	Data set ready
7	RTS	Request to send
8	CTS	Clear to send
9	RI	Ring indicator

3D500/1000/2000 Physical and Environmental Parameters

The following table describes the physical attributes and the environmental parameters for the appliance.

3D500, 3D1000, and 3D2000 Physical and Environmental Parameters

Parameter	Description
Form factor	1U rack-mounted or desktop device
Dimensions (D x W x H)	6.7 in. x 11.8 in. x 1.25 in. (17 cm x 30 cm x 3.2 cm)
Power Adapter	AC Input: 1.6 Ampere maximum at 100-240 Volts, 50/60 Hz DC Output: 5 Ampere maximum at 12 Volts
Copper 1000BASE-T	Gigabit copper ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Operating temperature	0°C to 40°C (32°F to 104°F)
Non-operating temperature	-20°C to 75°C (-4°F to 167°F)
Non-operating humidity	5% to 90%, non-condensing at 45°C (113°F)
Acoustic noise	No noise
Cooling requirements	Designed to operate in an air-conditioned environment.

Sourcefire 7000 Series Devices

All 7000 Series Devices have an LCD panel on the front of the appliance where you can view and, if enabled, configure your appliance.

See the following sections for information about your device:

- Sourcefire 3D7010, 3D7020, and 3D7030 on page 146
- Sourcefire 3D7110 and 3D7120 on page 153
- Sourcefire 3D7115 and 3D7125 on page 162

Sourcefire 3D7010, 3D7020, and 3D7030

The 3D7010, 3D7020, and 3D7030, also called the 70xx Family, are 1U appliances, one-half the width of the rack tray, and delivered with eight copper interfaces, each with configurable bypass capability. See Sourcefire Series 3 Information on page 232 for safety considerations for 70xx Family appliances.

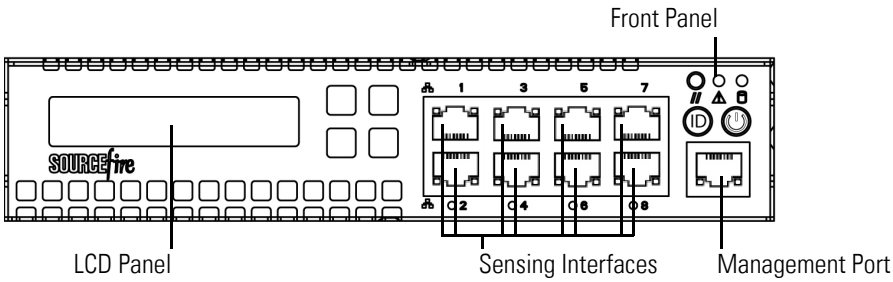
See the following sections for more information:

- 70xx Family Front View on page 146
- 70xx Family Rear View on page 151
- 70xx Family Physical and Environmental Parameters on page 152

70xx Family Front View

The front of the chassis contains the LCD panel, sensing interfaces, front panel, and management port.

70xx Family (Chassis: CHRY-1U-AC) Front View

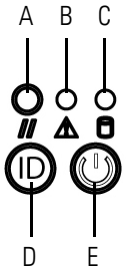


The 70xx Family System Components: Front View table describes the features on the front of the appliance.

70xx Family System Components: Front View

FEATURE	DESCRIPTION
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Series 3 Device on page 111.
Sensing interfaces	Contain the sensing interfaces that connect to the network. For information, see Sensing Interfaces on page 149.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Front panel	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see 3D7110 and 3D7120 Front Panel Components on page 154.

70xx Family Front Panel



Front Panel Components

A	Reset button	D	System ID button
B	System status LED	E	Power button and LED
C	Hard drive activity LED		

The front panel of the chassis houses LEDs, which display the system's operating state. The 70xx Family Front Panel LEDs table describes the LEDs on the front panel.

70xx Family Front Panel LEDs

LED	DESCRIPTION
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.
System status	Indicates the system status: • A green light indicates the system is powered up and operating normally, or powered down and attached to AC power. • An amber light indicates a system fault. See the 70xx Family System Status table on page 149 for more information.
Hard drive activity	Indicates the hard drive status: • A blinking green light indicates the fixed disk drive is active. • If the light is off, there is no drive activity or the system is powered off.
System ID	When pressed, the ID button displays a blue light, and a blue light is visible at the rear of the chassis.
Power button and LED	Indicates whether the appliance has power: • A green light indicates that the appliance has power and the system is on. • No light indicates the system is shut down or does not have power.

The 70xx Family System Status table describes the conditions under which the system status LEDs might be lit.

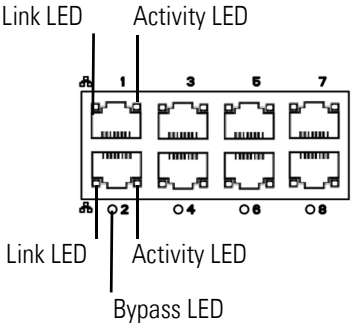
70xx Family System Status

CONDITION	DESCRIPTION
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional

Sensing Interfaces

The 70xx Family appliances are delivered with eight copper interfaces, each with configurable bypass capability.

Eight-Port 1000BASE-T Copper Interfaces



Use the 70xx Family Copper Link/Activity LEDs table to understand the activity and link LEDs on the copper interfaces.

70xx Family Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the 70xx Family Copper Bypass LEDs table to understand bypass LEDs on the copper interfaces.

70xx Family Copper Bypass LEDs

Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

The 10/100/1000 management interface is located on the front of the appliance. The 70xx Family Management Interface LEDs table describes the LEDs associated with the management interface.

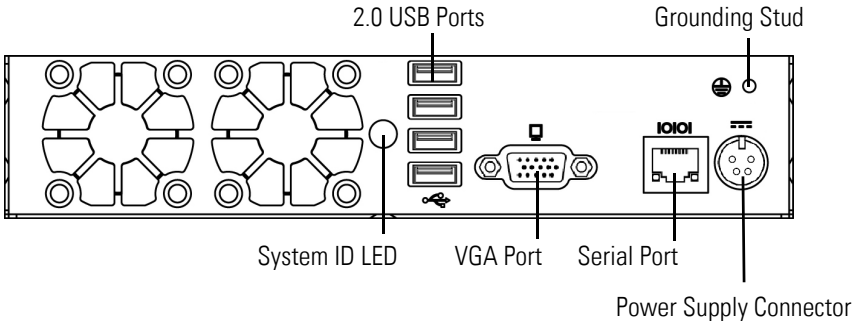
70xx Family Management Interface LEDs

LED	Description
Left (link)	Indicates whether the link is up. If the light is on, the link is up. If the light is off, there is no link.
Right (activity)	Indicates activity on the port. If the light is blinking, there is activity. If the light is off, there is no activity.

70xx Family Rear View

The rear of the chassis contains the system ID LED, connection ports, grounding stud, and power supply connector.

70xx Family (Chassis: CHRY-1U-AC) Rear View



The 70xx Family System Components: Rear View table describes the features that appear on the rear of the appliance.

70xx Family System Components: Rear View

Feature	Description
System ID LED	Helps identify a system installed in a high-density rack with other similar systems. The blue LED indicates that the ID button is pressed.
2.0 USB ports VGA port Serial port	Allows you to attach a monitor, keyboard, and mouse to the device, as an alternative to using the RJ45 serial port, to establish a direct workstation-to-appliance connection.
Grounding stud	Allows you to connect the appliance to the common bonding network. See the Power Requirements for Sourcefire Devices on page 240 for more information.
12V Power supply connector	Provides a power connection to the device through an AC power source.

70xx Family Physical and Environmental Parameters

The 70xx Family Physical and Environmental Parameters table describes the physical attributes and the environmental parameters for the appliance.

70xx Family Physical and Environmental Parameters

Parameter	Description
Form factor	1U, half rack width
Dimensions (D x W x H)	Single chassis: 12.49 in. x 7.89 in. x 1.66 in. (31.74 cm x 20.04 cm x 4.21 cm) 2-Chassis Tray: 25.05 in. x 17.24 in. x 1.73 in. (63.62 cm x 43.8 cm x 4.44 cm)
Chassis weight maximum installed	Chassis: 7 lbs. (3.17 kg) Single chassis and power supply in tray: 17.7 lbs. (8.03 kg) Double chassis and power supplies in single tray: 24.7 lbs. (11.2 kg)
Copper 1000BASE-T	Gigabit copper ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Power supply	200 W AC power supply Voltage: 100 VAC to 240 VAC nominal (90 VAC to 264 VAC maximum) Current: 2A maximum over the full range Frequency range: 50/60 Hz nominal (47 Hz to 63 Hz maximum)
Operating temperature	0°C to 40°C (32°F to 104°F)
Non-operating temperature	-20°C to 70°C (-29°F to 158°F)
Operating humidity	5% to 95%, noncondensing Operation beyond these limits is not guaranteed and not recommended.
Non-operating humidity	0% to 95%, non-condensing Store the unit below 95% non-condensing relative humidity. Acclimate below maximum operating humidity at least 48 hours prior to placing the unit in service.
Altitude	0 ft (sea level) to 5905 ft (0 to 1800 m)
Cooling requirements	682 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.

70xx Family Physical and Environmental Parameters (Continued)

PARAMETER	DESCRIPTION
Acoustic noise	53 dBA when idle. 62 dBA at full processor load.
Operating shock	No errors with half a sine wave shock of 5G (with 11 msec. duration)
Airflow	20 ft^3 (0.57 m^3) per minute Airflow through the appliance enters at the front and exits at the rear, with no side ventilation.

Sourcefire 3D7110 and 3D7120

The 3D7110 and 3D7120 devices, part of the 71xx Family, are 1U appliances, and are delivered with eight copper or eight fiber interfaces, each with configurable bypass capability. See Sourcefire Series 3 Information on page 232 for safety considerations for 71xx Family appliances.

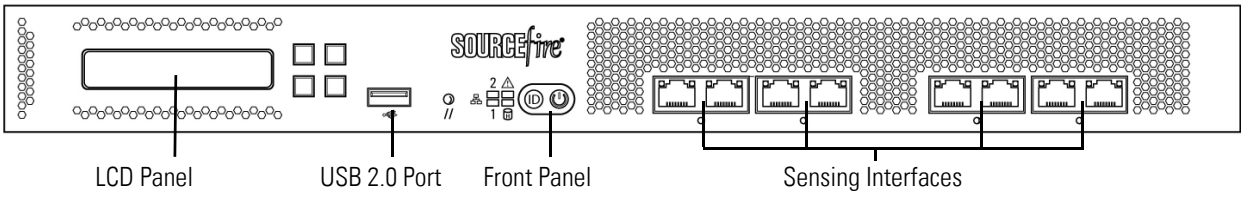
See the following sections for more information:

- 3D7110 and 3D7120 Chassis Front View on page 153
- 3D7110 and 3D7120 Chassis Rear View on page 159
- 3D7110 and 3D7120 Physical and Environmental Parameters on page 161

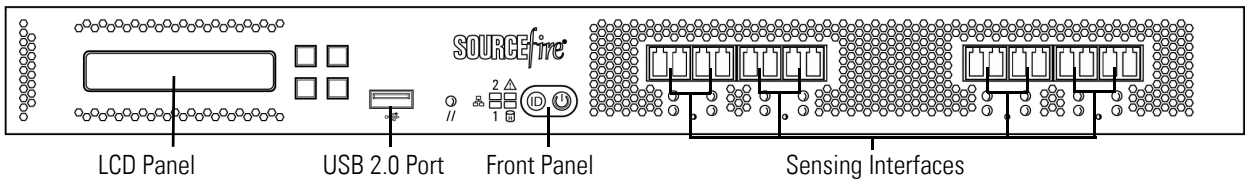
3D7110 and 3D7120 Chassis Front View

The front of the chassis contains the LCD panel, USB port, front panel, and either copper or fiber sensing interfaces.

3D7110 and 3D7120 with Copper Interfaces (Chassis: GERY-1U-8-C-AC)



3D7110 and 3D7120 with Fiber Interfaces (Chassis: GERY-1U-8-FM-AC)

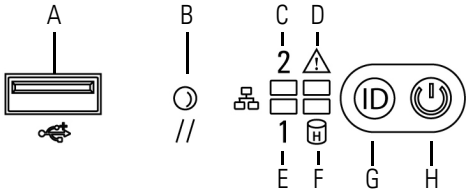


The 3D7110 and 3D7120 System Components: Front View table describes the features on the front of the appliance.

3D7110 and 3D7120 System Components: Front View

FEATURE	DESCRIPTION
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Series 3 Device on page 111.
Front panel USB 2.0 port	Allows you to attach a keyboard to the device.
Front panel	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see 3D7110 and 3D7120 Front Panel on page 154.
Sensing interfaces	Contain the sensing interfaces that connect to the network. For more information, see 3D7110 and 3D7120 Sensing Interfaces on page 157.

3D7110 and 3D7120 Front Panel



3D7110 and 3D7120 Front Panel Components

A	USB 2.0 connector	E	NIC1 activity LED
B	Reset button	F	Hard drive activity LED
C	NIC2 activity LED	G	ID button
D	System status LED	H	Power button and LED

The front panel of the chassis houses LEDs, which display the system's operating state. The 8000 Series Front Panel Components table describes the LEDs on the front panel.

3D7110 and 3D7120 Front Panel LEDs

LED	Description
NIC activity (1 and 2)	Indicates whether there is any network activity: • A green light indicates there is network activity. • No light indicates there is no network activity.
System status	Indicates the system status: • No light indicates the system is operating normally, or is powered off. • A red light indicates a system error. See the 3D7110 and 3D7120 System Status on page 156 for more information.
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.
Hard drive activity	Indicates the hard drive status: • A blinking green light indicates the fixed disk drive is active. • An amber light indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the appliance has power: • A green light indicates that the appliance has power and the system is on. • A blinking green light indicates that the appliance has power and is shut down. • If the light is off, the system does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

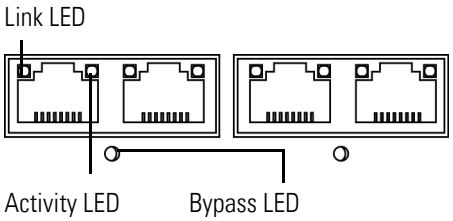
3D7110 and 3D7120 System Status

CONDITION	DESCRIPTION
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set fault indication command from system BIOS; the BIOS may use the command to indicate additional non-critical status such as system memory or CPU configuration changes
Degraded	Any degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **TIP!** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, then restart the device. **WARNING!** To power down safely, use the procedure in the Managing Devices chapter in the *Sourcefire 3D System User Guide*, or the `system shutdown` command from the CLI.

3D7110 and 3D7120 Sensing Interfaces

The 3D7110 and 3D7120 devices are delivered with eight-port copper or eight-port fiber interfaces, each with configurable bypass capability.

Eight-Port 1000BASE-T Copper Interfaces



Use the following table to understand the activity and link LEDs on the copper interfaces

3D7110 and 3D7120 Copper Link/Activity LEDs

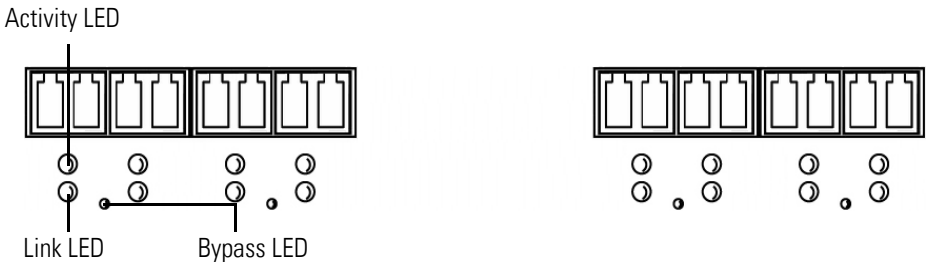
Status	Description
Both LEDs off	The interface does not have link.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the following table to understand the bypass LED on the copper interfaces.

3D7110 and 3D7120 Copper Bypass LED

Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

Eight-Port 1000BASE-SX Fiber Configurable Bypass Interfaces



Use the following table to understand the link and activity LEDs on the fiber interfaces.

3D7110 and 3D7120 Fiber Link/Activity LEDs

STATUS	DESCRIPTION
Top (activity)	For an inline interface: the light is on when the interface has activity. If dark, there is no activity. For a passive interface: the light is non-functional.
Bottom (link)	For an inline or passive interface: the light is on when the interface has link. If dark, there is no link.

Use the following table to understand the activity and link LEDs on the fiber interfaces.

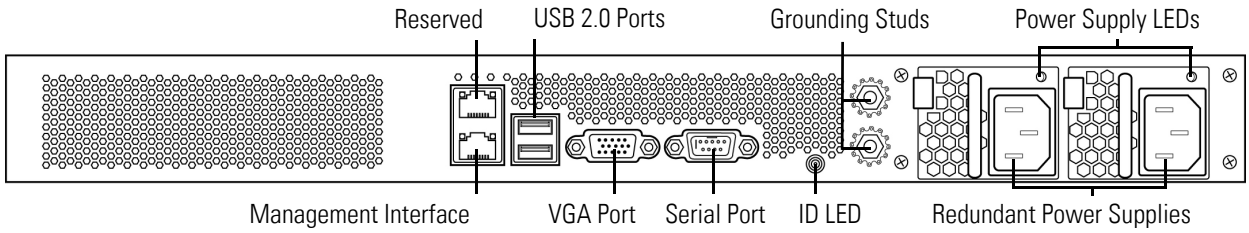
3D7110 and 3D7120 Fiber Bypass LEDs

STATUS	DESCRIPTION
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

3D7110 and 3D7120 Chassis Rear View

The rear of the chassis contains the management port, connection ports, grounding studs, and power supplies.

3D7110 and 3D7120 (Chassis: GERY-1U-8-C-AC or GERY-1U-8-FM-AC) Rear View



The following table describes the features that appear on the rear of the appliance.

3D7110 and 3D7120 System Components: Rear View

FEATURES	DESCRIPTION
VGA port USB port	Allows you to attach a monitor, keyboard, and mouse to the device to establish a direct workstation-to-appliance connection.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposed **only** and is not intended to carry service traffic.
System ID LED	Helps identify a system installed in a high-density rack with other similar systems. The blue light indicates that the ID button is pressed.
Grounding studs	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Sourcefire Devices on page 240 for more information.
Redundant power supplies	Provides power to the device through an AC power source.
Power supply LEDs	Indicates the status of the power supply. See 3D7110 and 3D7120 Power Supply LED on page 160.

The 10/100/1000 management interface is located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

3D7110 and 3D7120 Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The following table describes the LED associated with the power supply.

3D7110 and 3D7120 Power Supply LED

LED	Description
Off	The power cord is not plugged in.
Red	No power supplied to this module. OR A power supply critical event, such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking red	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

3D7110 and 3D7120 Physical and Environmental Parameters

The following table describes the physical attributes and the environmental parameters for the appliance.

3D7110 and 3D7120 Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	21.6 in. x 19.0 in. x 1.73 in. (54.9 cm x 48.3 cm x 4.4 cm)
Weight maximum installed	27.5 lbs. (12.5 kg)
Copper 1000BASE-T	Gigabit copper Ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 1000BASE-SX	Fiber bypass-capable interfaces with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)
Power supply	450 W dual redundant (1+1) AC power supplies Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) Current: 3A maximum for 90 VAC to 132 VAC, per supply 1.5A maximum for 187 VAC to 264 VAC, per supply Frequency range: 47 Hz to 63 Hz
Operating temperature	5°C to 40°C (41°F to 104°F)
Non-operating temperature	-20°C to 70°C (-29°F to 158°F)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 28°C (82°F) at temperatures from 25°C to 35°C (77°F to 95°F) Store the unit below 95% non-condensing relative humidity. Acclimate below maximum operating humidity at least 48 hours before placing the unit in service.
Altitude	0ft (sea level) to 5905 ft (1800 m)

3D7110 and 3D7120 Physical and Environmental Parameters (Continued)

Parameter	Description
Cooling requirements	900 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	64 dBA at full processor load, normal fan operation Meets GR-63-CORE 4.6 Acoustic Noise
Operating shock	Complies with Bellecore GR-63-CORE standards
Airflow	140 ft^3 (3.9 m^3) per minute Airflow through the appliance enters at the front and exits at the rear with no side ventilation.

Sourcefire 3D7115 and 3D7125

The 3D7115 and 3D7125 devices, part of the 71xx Family, are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability. To ensure compatibility, use only Sourcefire SFP transceivers. See Sourcefire Series 3 Information on page 232 for safety considerations for 71xx Family appliances.

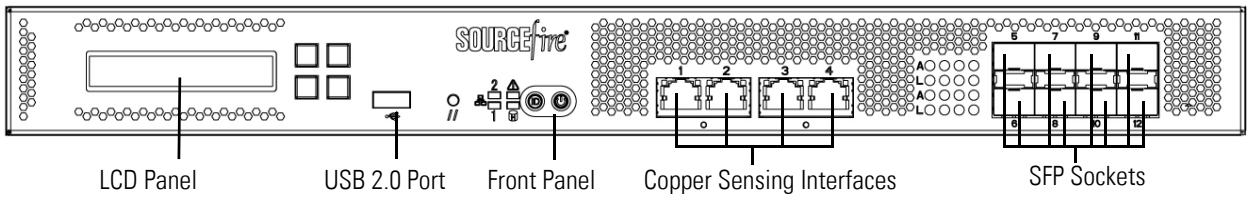
See the following sections for more information:

- 3D7115 and 3D7125 Chassis Front View on page 162
- 3D7115 and 3D7125 Chassis Rear View on page 168
- 3D7115 and 3D7125 Physical and Environmental Parameters on page 170

3D7115 and 3D7125 Chassis Front View

The front of the chassis contains the LCD panel, USB port, front panel, copper sensing interfaces, and SFP sockets.

3D7115 and 3D7125 (Chassis: GERY-1U-8-4C8S-AC) Front View

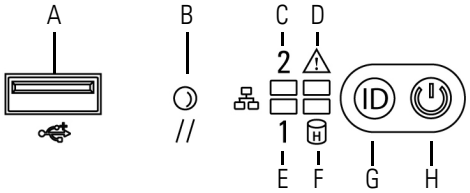


The following table describes the features on the front of the appliance.

3D7115 and 3D7125 System Components: Front View

FEATURE	DESCRIPTION
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Series 3 Device on page 111.
Front panel USB 2.0 port	Allows you to attach a keyboard to the device.
Front panel	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see 3D7115 and 3D7125 Front Panel on page 163.
Sensing interfaces	Contain the sensing interfaces that connect to the network. For more information, see 3D7115 and 3D7125 Sensing Interfaces on page 165.

3D7115 and 3D7125 Front Panel



3D7115 and 3D7125 Front Panel Components

A	USB 2.0 connector	E	NIC1 activity LED
B	Reset button	F	Hard drive activity LED
C	NIC2 activity LED	G	ID button
D	System status LED	H	Power button and LED

The front panel of the chassis houses LEDs, which display the system's operating state. The following table describes the LEDs on the front panel.

3D7115 and 3D7125 Front Panel LEDs

LED	DESCRIPTION
NIC activity (1 and 2)	Indicates whether there is any network activity: • A green light indicates there is network activity. • No light indicates there is no network activity.
System status	Indicates the system status: • No light indicates the system is operating normally, or is powered off. • A red light indicates a system error. See the 3D7115 and 3D7125 System Status on page 165 for more information.
Reset button	Allows you to reboot the appliance without disconnecting it from the power supply.
Hard drive activity	Indicates the hard drive status: • A blinking green light indicates the fixed disk drive is active. • An amber light indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the appliance has power: • A green light indicates that the appliance has power and the system is on. • A blinking green light indicates that the appliance has power and is shut down. • No light indicates the system does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

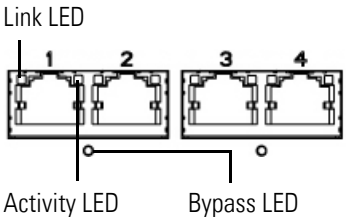
3D7115 and 3D7125 System Status

CONDITION	DESCRIPTION
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional non-critical status such as system memory or CPU configuration changes
Degraded	Any degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **TIP!** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, then restart the device. **WARNING!** To power down safely, use the procedure in the Managing Devices chapter in the *Sourcefire 3D System User Guide*, or the `system shutdown` command from the CLI.

3D7115 and 3D7125 Sensing Interfaces

The 3D7115 and 3D7125 devices are delivered with four-port copper interfaces with configurable bypass capability, and eight hot-swappable small form-factor pluggable (SFP) ports without bypass capability.

Four 1000BASE-T Copper Interfaces



Use the following table to understand the link and activity LEDs on copper interfaces.

3D7115 and 3D7125 Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the following table to understand the bypass LED on copper interfaces.

3D7115 and 3D7125 Copper Bypass LED

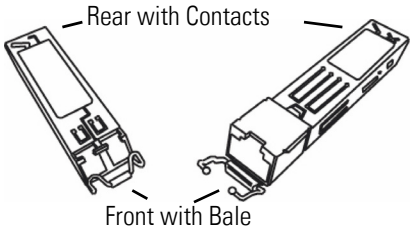
Status	Description
Off	The interface pair is not in bypass mode or has no power.
Steady green	The interface pair is ready to enter bypass mode.
Steady amber	The interface pair has been placed in bypass mode and is not inspecting traffic.
Blinking amber	The interface pair is in bypass mode; that is, it has failed open.

SFP Interfaces

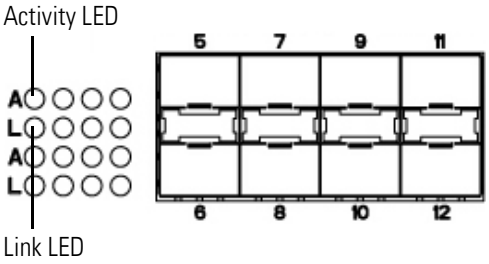
You can install up to eight hot-swappable Sourcefire SFP transceivers, available in 1G copper, 1G short range fiber, or 1G long range fiber. SFP transceivers do not have bypass capability and should not be used in intrusion prevention deployments. See Using SFP Transceivers on a 3D7115 or 3D7125 on page 251

for more information.

Sample SFP Transceivers



Sample Fiber Sample Copper



Use the following table to understand the fiber LEDs.

3D7115 and 3D7125 SFP Socket Activity/Link LEDs

Status	Description
Top (activity)	For an inline interface: the light is on when the interface has activity. If dark, there is no activity. For a passive interface: the light is non-functional.
Bottom (link)	For an inline or passive interface: the light is on when the interface has link. If dark, there is no link.

Use the following table to understand the specifications of the SFP optical transceivers.

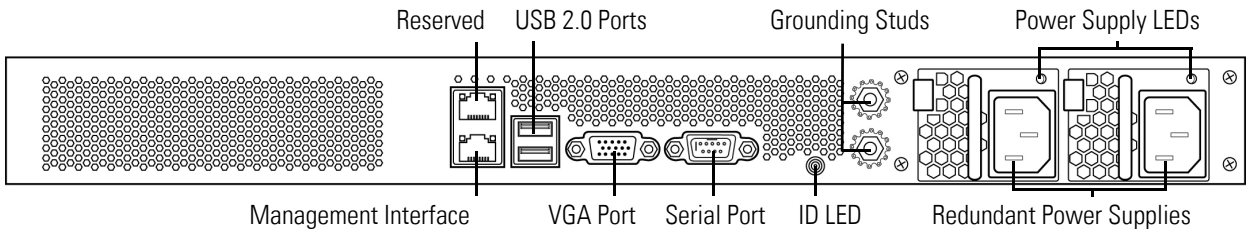
3D7115 and 3D7125 SFP Optical Parameters

PARAMETER	1000BASE-SX	1000BASE-LX
Optical connectors	LC duplex	LC duplex
Bit rate	1000Mbps	1000Mbps
Baud rate/encoding/tolerance	1250Mbps / 8b/10b encoding	1250Mbps / 8b/10b encoding
Optical interface	Multimode	Single mode only
Operating distances	200 m (656 ft) for 62.5 µm/125 µm fiber 500 m (1640 ft) for 50 µm/125 µm fiber	10 km (6.2 miles) for 9 µm/125 µm fiber
Transmitter wavelength	770-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	0 dBm	-3 dBm
Minimum average launch power	-9.5 dBm	-11.5 dBm
Maximum average power at receiver	0 dBm	-3 dBm
Receiver sensitivity	-17 dBm	-19 dBm

3D7115 and 3D7125 Chassis Rear View

The rear of the chassis contains the management interface, connection ports, grounding studs, and power supplies.

3D7115 and 3D7125 (Chassis: GERY-1U-8-4C8S-AC) Rear View



The following table describes the features that appear on the rear of the appliance.

3D7115 and 3D7125 System Components: Rear View

Features	Description
VGA port USB port	Allows you to attach a monitor, keyboard, and mouse to the device to establish a direct workstation-to-appliance connection.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposed **only** and is not intended to carry service traffic.
System ID LED	Helps identify a system installed in a high-density rack with other similar systems. The blue light indicates that the ID button is pressed.
Grounding studs	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Sourcefire Devices on page 240for more information.
Redundant power supplies	Provides power to the device through an AC power source.
Power supply LEDs	Indicates the status of the power supply. See 3D7115 and 3D7125 Power Supply LED on page 170.

The 10/100/1000 management interface is located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

3D7115 and 3D7125 Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The following table describes the LED associated with the power supply.

3D7115 and 3D7125 Power Supply LED

LED	Description
Off	The power cord is not plugged in.
Red	No power supplied to this module. OR A power supply critical event, such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking red	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

3D7115 and 3D7125 Physical and Environmental Parameters

The following table describes the physical attributes and the environmental parameters for the appliance.

3D7115 and 3D7125 Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	21.6 in. x 19.0 in. x 1.73 in. (54.9 cm x 48.3 cm x 4.4 cm)
Weight maximum installed	29.0 lbs. (13.2 kg)
Copper 1000BASE-T	Gigabit copper ethernet bypass-capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Copper 1000BASE-T SFP	Gigabit copper ethernet non-bypass capable interfaces in a paired configuration Cable and distance: Cat5E at 50 m

3D7115 and 3D7125 Physical and Environmental Parameters (Continued)

Parameter	Description
Fiber 1000BASE-SX SFP	Fiber non-bypass capable interfaces with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard) 200 m (656 ft) for 62.5 µm/125 µm fiber 500 m (1640 ft) for 50 µm/125 µm fiber
Fiber 1000BASE-LX SFP	Fiber non-bypass capable interfaces with LC connectors Cable and distance: LX is single mode fiber (1310 nm) at 10 km for 9 µm/125 µm fiber (standard)
Power supply	450 W dual redundant (1+1) AC power supplies Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) Current: 3A maximum for 90 VAC to 132 VAC, per supply 1.5A maximum for 187 VAC to 264 VAC, per supply Frequency range: 47 Hz to 63 Hz
Operating temperature	5°C to 40°C (41°F to 104°F)
Non-operating temperature	-20°C to 70°C (-29°F to 158°F)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 28°C (82°F) at temperatures from 25°C to 35°C (77°F to 95°F) Store the unit below 95% non-condensing relative humidity. Acclimate below maximum operating humidity at least 48 hours before placing the unit in service.
Altitude	0ft (sea level) to 5905 ft (1800 m)
Cooling requirements	900 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.

3D7115 and 3D7125 Physical and Environmental Parameters (Continued)

PARAMETER	DESCRIPTION
Acoustic noise	64 dBA at full processor load, normal fan operation Meets GR-63-CORE 4.6 Acoustic Noise
Operating shock	Complies with Bellecore GR-63-CORE standards
Airflow	140 ft^3 (3.9 m^3) per minute Airflow through the appliance enters at the front and exits at the rear with no side ventilation.

Sourcefire 8000 Series Devices

The 8000 Series devices use network modules (NetMods) that contain either copper or fiber sensing interfaces. The devices can be shipped fully assembled or you can install the modules. Assemble your device before installing the Sourcefire 3D System. See the assembly instructions shipped with your modules.

Some 8000 Series devices can be stacked to increase the capability of the system. For each stacking kit, you replace a NetMod with a stacking module and cable the devices together using the 8000 Series stacking cable. See Using Devices in a Stacked Configuration on page 74 for more information.

The 8000 Series device can be delivered on a variety of chassis:

- 3D8120/8130/8140, also known as the 81xx Family, is a 1U chassis and can contain up to three modules. For the 3D8140 only, you can add a stacking kit for a total 2U configuration.
- 3D8250, part of the 82xx Family, is 2U chassis and can contain up to seven modules. You can add up to three stacking kits for a total 8U configuration.
- 3D8260, part of the 82xx Family, is a 4U configuration with two 2U chassis. The primary chassis contains one stacking module and up to six sensing modules. The secondary chassis contains one stacking module. You can add up to two stacking kits for a total 8U configuration.
- 3D8270, part of the 82xx Family, is a 6U configuration with three 2U chassis. The primary chassis contains two stacking modules and up to five sensing modules. Each secondary chassis contains one stacking module. You can add one stacking kit for a total 8U configuration.
- 3D8290, part of the 82xx Family, is an 8U configuration with four 2U chassis. The primary chassis contains three stacking modules and up to four sensing modules. Each secondary chassis contains one stacking module. This model is fully configured and does not accept a stacking kit.

See the following sections for more information:

- 8000 Series Chassis Front View on page 173
- 8000 Series Chassis Rear View on page 178
- 8000 Series Physical and Environmental Parameters on page 181
- 8000 Series Modules on page 185

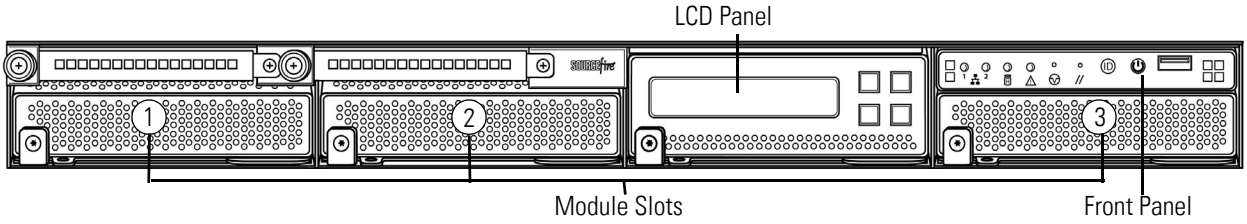
8000 Series Chassis Front View

The 8000 Series chassis can be in the 81xx Family or 82xx Family. See Sourcefire Series 3 Information on page 232 for safety considerations for 81xx Family and 82xx Family appliances.

81xx Family Chassis Front View

The front view of the chassis contains the LCD panel, front panel, and three module slots.

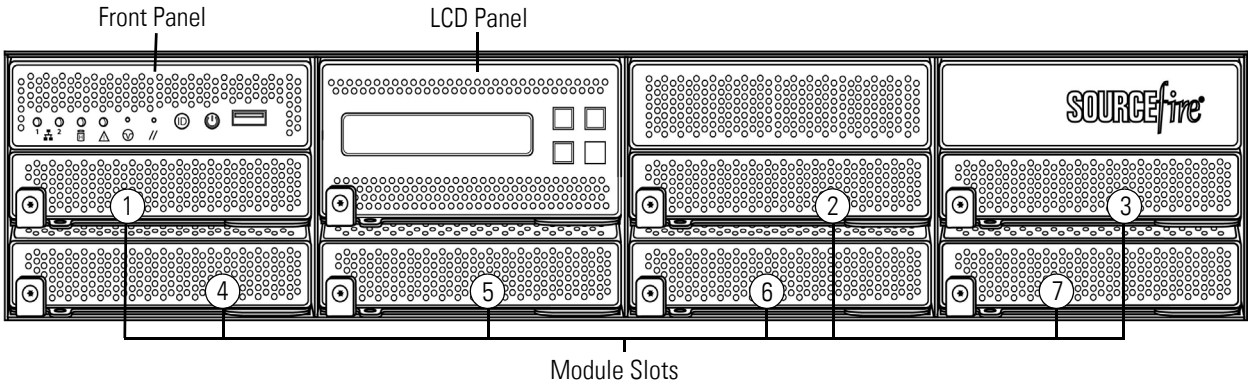
81xx Family (Chassis: CHAS-1U-AC/DC) Front View



82xx Family Chassis Front View

The front view of the chassis contains the LCD panel, front panel, and seven module slots.

82xx Family (Chassis: CHAS-2U-AC/DC) Front View



The 8000 Series System Components: Front View table describes the features on the front of the appliance.

8000 Series System Components: Front View

FEATURE	DESCRIPTION
Module slots	Contain the modules. For information on available modules, see 8000 Series Modules on page 185.
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Series 3 Device on page 111.
Front panel controls	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see 82xx Family Front Panel on page 175.
Front panel USB port	The USB 2.0 port allows you to attach a keyboard to the device.

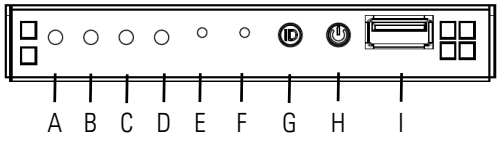
See the following sections for more information:

- 8000 Series Front Panel on page 174
- 8000 Series Chassis Rear View on page 178

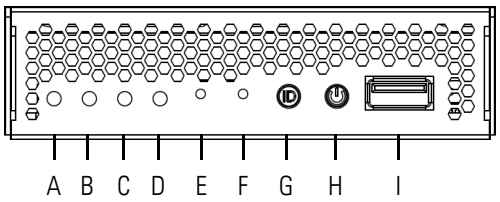
8000 Series Front Panel

The front panel for the 81xx Family and 82xx Family contain the same components.

81xx Family Front Panel



82xx Family Front Panel



8000 Series Front Panel Components

A	NIC activity LED	F	Reset button
B	Reserved	G	ID button
C	Hard drive activity LED	H	Power button and LED
D	System status LED	I	USB 2.0 connector
E	Non-maskable interrupt button		

The front panel of the chassis houses LEDs, which display the system's operating state. The 8000 Series Front Panel LEDs table describes the LEDs on the front panel

8000 Series Front Panel LEDs

LED	DESCRIPTION
NIC activity	Indicates whether there is any network activity. • Green indicates there is network activity. • If the light is off, there is no network activity.
Hard drive activity	Indicates the hard drive status. • Blinking green indicates the fixed disk drive is active. • Amber indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.
System status	Indicates the system status. • Green indicates the system is operating normally. • Blinking green indicates the system is operating in a degraded condition. • Blinking amber indicates the system is in a non-critical condition. • Amber indicates the system is in a critical or non-recoverable condition, or the system is starting up. • If the light is off, the system is starting up or off. **IMPORTANT!** The amber status light takes precedence over the green status light. When the amber light is on or blinking, the green light is off. See the 8000 Series System Status table on page 177 for more information.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the system has power. • Green indicates that the system has power. • If the light is off, the system does not have power.

The 8000 Series System Status table describes the conditions under which the system status LEDs might be lit.

8000 Series System Status

CONDITION	DESCRIPTION
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **TIP!** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, and then restart the device. **WARNING!** To power down safely, use the procedure in the Managing Devices chapter in the *Sourcefire 3D System User Guide*, or the `system shutdown` command from the CLI.

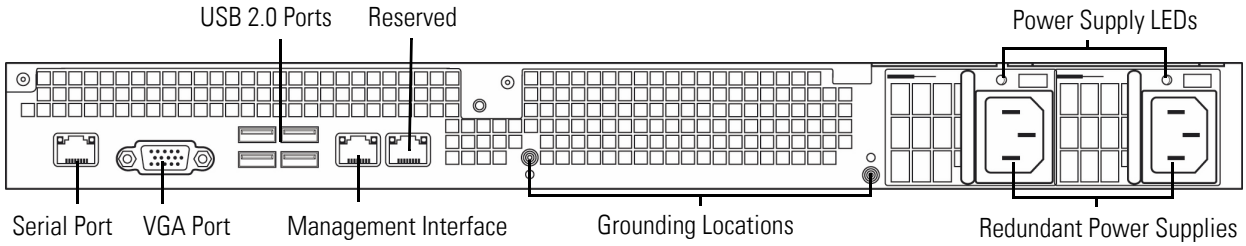
8000 Series Chassis Rear View

The 8000 Series chassis can be in the 81xx Family or 82xx Family.

81xx Family Chassis Rear View

The rear view of the chassis contains connection ports, the management interface, and the power supplies.

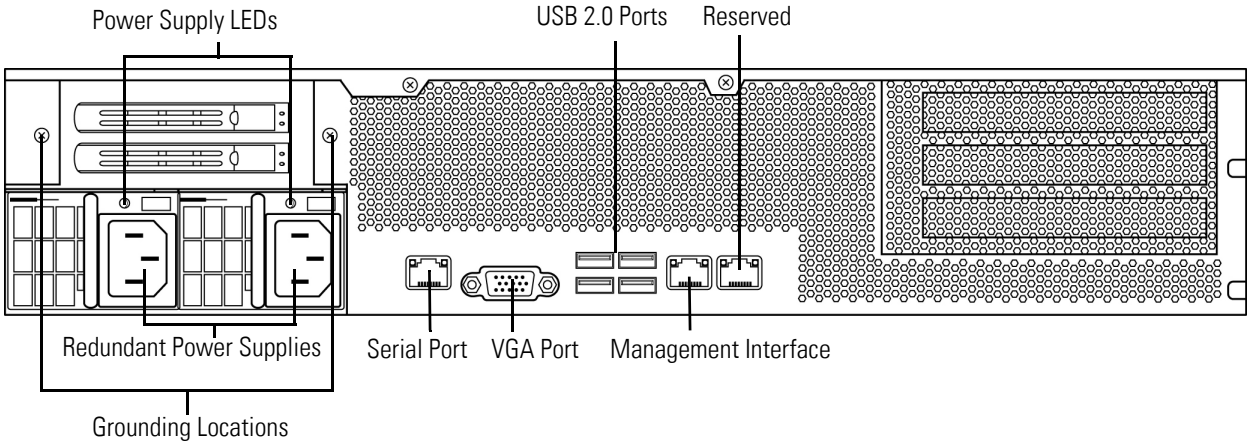
81xx Family (Chassis: CHAS-1U-AC/DC) Rear View



82xx Family Chassis Rear View

The rear view of the chassis contains power supplies, connection ports, and the management interface.

82xx Family (Chassis: CHAS-2U-AC/DC) Rear View



The 8000 Series System Components: Rear View table describes the features that appear on the rear of the appliance.

8000 Series System Components: Rear View

FEATURE	DESCRIPTION
VGA port USB 2.0 ports	Allows you to attach a monitor, keyboard, and mouse to the device, as an alternative to using the RJ45 serial port, to establish a direct workstation-to-appliance connection.
RJ45 serial port	Allows you to establish a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the device. The RJ45 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic. See the 8000 Series RJ45 to DB-9 Adapter Pin-Out table on page 180
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Redundant power supplies	Provides power to the device through an AC power source.
Grounding locations	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Sourcefire Devices on page 240for more information.

The 10/100/1000 management interface is located on the rear of the appliance. The 8000 Series Management Interface LEDs table describes the LEDs associated with the management interface.

8000 Series Management Interface LEDs

LED	DESCRIPTION
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The 8000 Series Power Supply LEDs table describes the LEDs associated with the management interface.

8000 Series Power Supply LEDs

LED	Description
Off	The power supply is not plugged in.
Amber	No power supplied to this module. OR A power supply critical event such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking amber	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

The 8000 Series RJ45 to DB-9 Adapter Pin-Out table list the signals on a typical DB-9 serial connector and the corresponding pins on the device's RJ45 serial connectors. You can use this table to construct an adapter for serial connections.

8000 Series RJ45 to DB-9 Adapter Pin-Out

DB-9 Pin	Signal	Description	RJ45 Pin
1	DCD/DSR	Data carrier detect/data set ready	7
2	RD	Receive data	6
3	TD	Transmit data	3
4	DTR	Data terminal ready	2
5	GND	Ground	4 & 5
6		No connection	
7	RTS	Request to send	1

8000 Series RJ45 to DB-9 Adapter Pin-Out (Continued)

DB-9 Pin	Signal	Description	RJ45 Pin
8	CTS	Clear to send	8
9		No connection	

8000 Series Physical and Environmental Parameters

The following table describes the physical attributes and environmental parameters for 81xx Family devices.

81xx Family Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	28.7″ x 17.2″ x 1.73″ (72.8 cm x 43.3 cm x 4.4 cm)
Weight maximum installed	43.5 lbs (19.8 kg)
Copper 1000BASE-T configurable bypass NetMod	Quad-port Gigabit copper ethernet configurable bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE configurable bypass MMSR or SMLR NetMod	Dual-port fiber configurable bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX configurable bypass NetMod	Quad-port fiber configurable bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)
Copper 1000BASE-T non-bypass NetMod	Quad-port Gigabit copper ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE non-bypass MMSR or SMLR NetMod	Quad-port fiber non-bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX non-bypass NetMod	Quad-port fiber non-bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)

81xx Family Physical and Environmental Parameters (Continued)

Parameter	Description
Power supply	Dual 650 W redundant power supplies designed for AC or DC. AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) AC Current: 10A maximum over the full range, per supply 5A maximum for 187 VAC to 264 VAC, per supply AC Frequency range: 47 Hz to 63 Hz DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum DC Current: 20A maximum, per supply
Operating temperature	10°C to 35°C (50°F to 95°F)
Non-operating temperature	-20°C to 70°C (-29°F to 158°F)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 28°C at temperatures from 25°C to 35°C (77°F to 95°F)
Altitude	0ft (sea level) to 6000 ft (0 to 1800 m)
Cooling requirements	1725 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	Max normal operating noise is 87.6 dB LWAd (high temperature) Typical normal operating noise is 80 dB LWAd.
Operating shock	No errors with half a sine wave shock of 2G (with 11 msec. duration)
Airflow	160 ft^3 (4.5 m^3) per minute Restriction of the airflow such as blocking the front or back or enclosing the unit in a cabinet without sufficient clearance may cause the unit to overheat, even if the ambient temperature is in the operating range. Airflow through the appliance enters at the front and exits at the rear. The minimum recommended clearance in the front and back is 7.9” (20 cm). This minimum can only be used if you can ensure a supply of low temperature air at the front of the appliance.

The following table describes the physical attributes and environmental parameters for 82xx Family devices.

82xx Family Physical and Environmental Parameters

Parameter	Description
Form factor	2U
Dimensions (D x W x H)	29.0″ x 17.2″ x 3.48″ (73.5 cm x 43.3 cm x 88.2 cm)
Weight maximum installed	58 lbs (25.3 kg)
Copper 1000BASE-T configurable bypass NetMod	Quad-port Gigabit copper ethernet configurable bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE MMSR or SMLR configurable bypass NetMod	Dual-port fiber configurable bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX configurable bypass NetMod	Quad-port fiber configurable bypass interfaces1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)
Fiber 40GBASE-SR4 configurable bypass NetMod	Dual-port fiber configurable bypass interfaces with OTP/MTP connectors Cable and distance: OM3: 100 m at 850 nm Multimode OM4: 150 m at 850 nm Multimode
Copper 1000BASE-T non-bypass NetMod	Quad-port Gigabit copper ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE non-bypass MMSR or SMLR NetMod	Quad-port fiber non-bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX non-bypass NetMod	Quad-port fiber non-bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)

82xx Family Physical and Environmental Parameters (Continued)

PARAMETER	DESCRIPTION
Power supply	Dual 750 W redundant power supplies designed for AC or DC. AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum) AC Current: 10A maximum over the full range, per supply 5A maximum for 187 VAC to 264 VAC, per supply AC Frequency range: 47 Hz to 63 Hz DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum DC Current: 20A maximum, per supply
Operating temperature	10°C to 35°C (50°F to 95°F)
Non-operating temperature	-20°C to 70°C (-29°F to 158°F)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 28°C at temperatures from 25°C to 35°C (77°F to 95°F)
Altitude	0 ft (sea level) to 6000 ft (0 to 1800 m)
Cooling requirements	up to 2225 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	Max normal operating noise is 81.6 dB LWAd (High temp.) Typical normal operating noise is 81.4 dB LWAd.
Operating shock	No errors with half a sine wave shock of 2G (with 11 msec. duration)
Airflow	Front to back, 210 ft^3 (6 m^3) per minute Restriction of the airflow such as blocking the front or back or enclosing the unit in a cabinet without sufficient clearance may cause the unit to overheat, even if the ambient temperature is in the operating range. Airflow through the appliance enters at the front and exits at the rear. The minimum recommended clearance in the front and back is 7.9" (20cm). This minimum can only be used if you can ensure a supply of low temperature air at the front of the appliance.

8000 Series Modules

The sensing interfaces for the 8000 Series appliances can be delivered with copper or fiber interfaces.

WARNING! Modules are **not** hot-swappable. See Inserting and Removing 8000 Series Modules on page 255 for more information.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Quad-Port 1000BASE-T Copper Configurable Bypass NetMod on page 186.
- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod on page 187 for more information.
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod on page 188 for more information.
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only). See Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod on page 191 for more information.

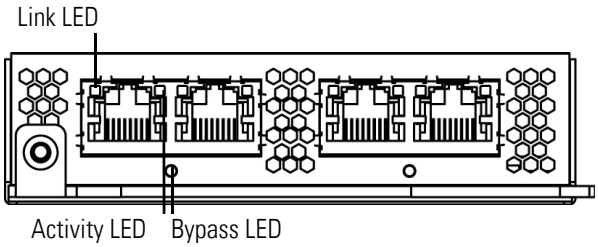
The following modules contain non-bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface without bypass capability. See Quad-Port 1000BASE-T Copper Non-Bypass NetMod on page 193 for more information.
- a quad-port 1000BASE-SX fiber interface without bypass capability. See Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod on page 194 for more information.
- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod on page 195 for more information.

In addition, you can use a stacking module to connect two 3D8140 or up to four 3D8250 devices to combine their processing power and increase throughput. See Stacking Module on page 197 for more information.

Quad-Port 1000BASE-T Copper Configurable Bypass NetMod

The quad-port 1000BASE-T copper configurable bypass NetMod contains four copper ports and link, activity, and bypass LEDs.



Use the Copper Link/Activity LEDs table to understand the link and activity LEDs on copper interfaces.

Copper Link/Activity LEDs

Status	Description
Both LEDs off	The interface does not have link and is not in bypass mode.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

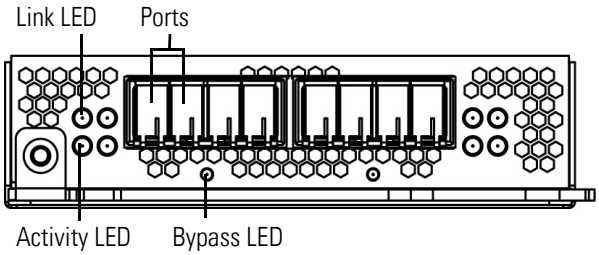
Use the Copper Bypass LEDs table to understand the bypass LEDs on copper interfaces.

Copper Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod

The quad-port 1000BASE-SX fiber configurable bypass NetMod contains four fiber ports and link, activity, and bypass LEDs.



Use the Fiber Link/Activity LEDs table to understand link and activity LEDs of the fiber interfaces.

Fiber Link/Activity LEDs

Status	Description
Top	For an inline or passive interface: • A blinking light indicates the interface has activity. No light indicates there is no activity.
Bottom	For an inline interface: • A light indicates the interface has activity. • No light indicates there is no activity. For a passive interface, the light is always on.

Use the Fiber Bypass LEDs table to understand bypass LEDs on the fiber interfaces.

Fiber Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

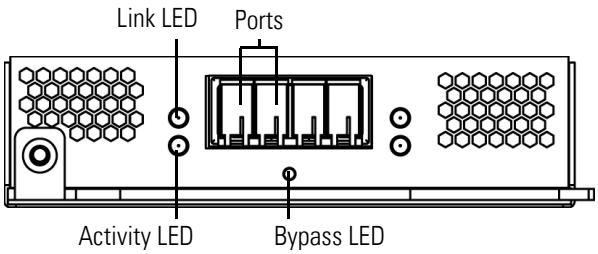
Use the 1000BASE-SX NetMod Optical Parameters table to understand the optical specifications of the fiber interfaces.

1000BASE-SX NetMod Optical Parameters

PARAMETER	1000BASE-SX
Optical connectors	LC duplex
Bit rate	1000Mbps
Baud rate/encoding/tolerance	1250Mbps / 8b/10b encoding
Optical interface	Multimode
Operating distances	200 m (656 ft) for 62.5 µm/125 µm fiber 500 m (1640 ft) for 50 µm/125 µm fiber
Transmitter wavelength	770-860 nm (850 nm typical)
Maximum average launch power	0 dBm
Minimum average launch power	-9.5 dBm
Maximum average power at receiver	0 dBm
Receiver sensitivity	-17 dBm

Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod

The dual-port 10GBASE (MMSR or SMLR) fiber configurable bypass NetMod contains two fiber ports and link, activity, and bypass LEDs.



Use the Fiber Link/Activity LEDs table to understand link and activity LEDs of the fiber interfaces.

Fiber Link/Activity LEDs

STATUS	DESCRIPTION
Top	For an inline or passive interface: • A blinking light indicates the interface has activity. No light indicates there is no activity.
Bottom	For an inline interface: • A light indicates the interface has activity. • No light indicates there is no activity. For a passive interface, the light is always on.

Use the Fiber Bypass LEDs tables to understand the bypass LEDs on the fiber interfaces.

Fiber Bypass LEDs

STATUS	DESCRIPTION
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

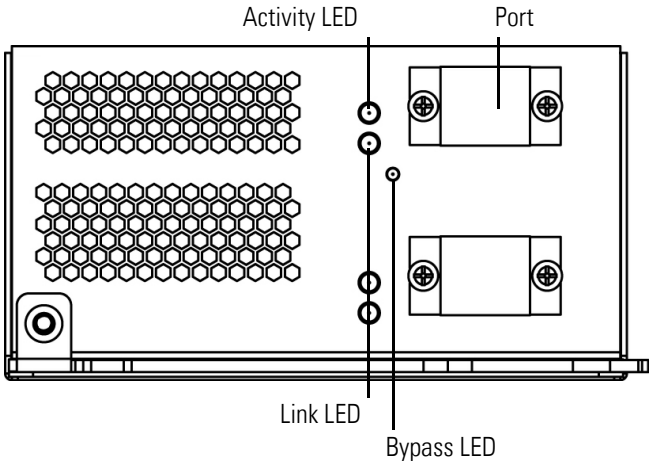
Use the 10GBASE MMSR and SMLR NetMod Optical Parameters table to understand the optical parameters of the fiber interfaces.

10GBASE MMSR and SMLR NetMod Optical Parameters

PARAMETER	10GBASE MMSR	10GBASE SMLR
Optical connectors	LC duplex	LC duplex
Bit rate	10.000Gbps	10.000Gbps
Baud rate/ encoding/tolerance	10.3125Gbps / 64/66b encoding / +/- 100 ppm	10.3125Gbps / 64/166b encoding / +/- 100 ppm
Optical interface	Multimode	Single mode only
Operating distance	840-860 nm (850 nm typical) 26m (85 ft) to 33 m (108 ft) for 62.5 µm/125 µm fiber (modal BW 160 to 200 respectively) 66 m (216 ft) to 82 m (269 ft) for 50 µm/125 µm fiber (modal BW 400 to 500 respectively) Distances to 300 m (980 ft) are available with higher quality (OM3) fiber. Minimum distances (all): 2 m (6ft)	1270-1355 nm (1310 nm typical) 2 m to 10 km (6 ft to 6.2 miles) for 9 µm/125 µm fiber
Transmitter wavelength	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	-1 dBm	-0.5 dBm
Minimum average launch power	-7.3 dBm	-8.2 dBm
Maximum average power at receiver	-1 dBm	-0.5 dBm
Receiver sensitivity	-9.9 dBm	-14.4 dBm

Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod

The dual-port 40GBASE-SR4 fiber configurable bypass NetMod contains two fiber ports and link, activity, and bypass LEDs.



You can use the 40G NetMod only in the 3D8270/8290 or a 40G-capable 3D8250/8260. If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Defense Center web interface displays red. A 40G-capable device displays 3D 8250-40G on the LCD panel. See 8000 Series Modules on page 68 for placement information.

Use the Fiber Link/Activity LEDs table to understand link and activity LEDs of the fiber interfaces.

Fiber Link/Activity LEDs

STATUS	DESCRIPTION
Top (activity)	The light flashes when the interface has activity. If dark, there is no activity.
Bottom (link)	The light is on when the interface has link. If dark, there is no link.

Use the Fiber Bypass LED table to understand bypass LED of the fiber interfaces.

Fiber Bypass LED

STATUS	DESCRIPTION
Off	The interface pair does not have link and is not in bypass mode, or has no power.
Steady green	The interface pair has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Use the and 40GBASE-SR4 NetMod Optical Parameters table to understand optical parameters of the fiber interfaces.

40GBASE-SR4 NetMod Optical Parameters

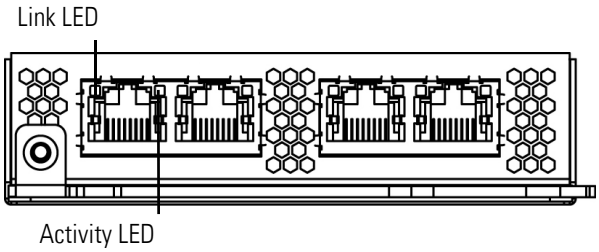
PARAMETER	40GBASE-SR4
Optical connectors	OTP/MTP single row twelve fiber positions. Only the outer eight fibers are used
Bit rate	40.000Gbps
Baud rate/encoding/tolerance	10.3125Gbps / 64/66b encoding / +/- 100 ppm
Optical interface	Multimode
Operating distances	100 m (320 ft) for 50 µm/125 µm fiber (OM3) Minimum distance: 0.5 m (2 ft) 40G optics are carried on eight fiber cables utilizing MPO connectors.
Transmitter wavelength	840-860 nm (850 nm typical)
Maximum average launch power	2.4 dBm
Minimum average launch power	-7.8 dBm

40GBASE-SR4 NetMod Optical Parameters (Continued)

PARAMETER	40GBASE-SR4
Maximum average power at receiver	2.4 dBm
Receiver sensitivity	-9.5 dBm

Quad-Port 1000BASE-T Copper Non-Bypass NetMod

The quad-port 1000BASE-T copper non-bypass NetMod contains four copper ports, and link and activity LEDs.



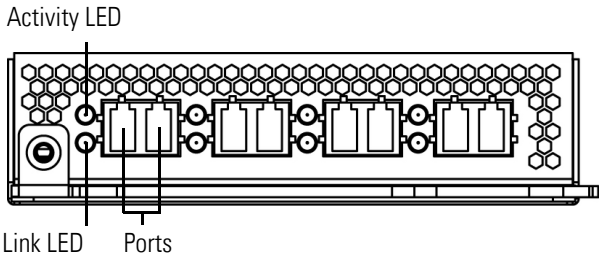
Use the Non-Bypass Copper Link/Activity LEDs table to understand copper LEDs.

Non-Bypass Copper Link/Activity LEDs

STATUS	DESCRIPTION
Both LEDs Off	The interface does not have link.
Link Amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link Green	The speed of the traffic on the interface is 1Gb.
Activity Blinking Green	The interface has link and is passing traffic.

Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod

The quad-port 1000BASE-SX fiber non-bypass NetMod contains four fiber ports, and link and activity LEDs.



Use the Non-Bypass Fiber Link/Activity LEDs table to understand the link and activity LEDs on the fiber interfaces.

Non-Bypass Fiber Link/Activity LEDs

Status	Description
Top (Activity)	For an inline or passive interface: the light flashes when the interface has activity. If dark, there is no activity.
Bottom (Link)	For an inline interface: the light is on when the interface has link. If dark, there is no link. For a passive interface: the light is always on.

Use the 1000BASE-SX NetMod Optical Parameters table to understand the optical parameters of the fiber interfaces.

1000BASE-SX NetMod Optical Parameters

Parameter	1000BASE-SX
Optical connectors	LC duplex
Bit rate	1000Mbps
Baud rate/encoding/tolerance	1250Mbps / 8b/10b encoding
Optical interface	Multimode
Operating distances	200 m (656 ft) for 62.5 µm/125 µm fiber 500 m (1640 ft) for 50 µm/125 µm fiber

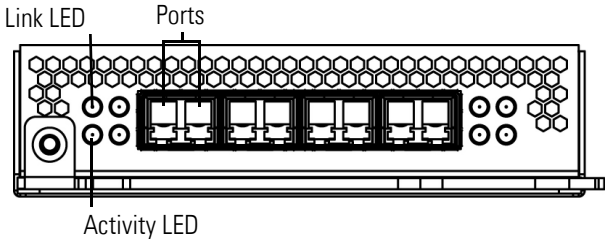
1000BASE-SX NetMod Optical Parameters (Continued)

PARAMETER	1000BASE-SX
Transmitter wavelength	770-860 nm (850 nm typical)
Maximum average launch power	0 dBm
Minimum average launch power	-9.5 dBm
Maximum average power at receiver	0 dBm
Receiver sensitivity	-17 dBm

Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod

The quad-port 10GBASE (MMSR or SMLR) fiber non-bypass NetMod contains four fiber ports, and link and activity LEDs.

WARNING! The quad-port 10GBASE non-bypass NetMod contains non-removable SFPs. Any attempt to remove the SFP can damage the module.



Use the Fiber Link/Activity LEDs table to understand the link and activity LEDs on fiber interfaces.

Fiber Link/Activity LEDs

STATUS	DESCRIPTION
Top	For an inline or passive interface: the light flashes when the interface has activity. If dark, there is no activity.
Bottom	For an inline interface: the light is on when the interface has link. If dark, there is no link. For a passive interface: the light is always on.

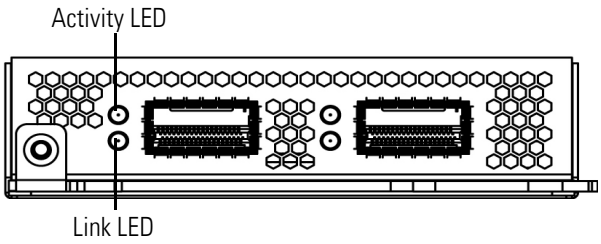
Use the 10GBASE MMSR and SMLR NetMod Optical Parameters table to understand the optical parameters of the fiber interfaces.

10GBASE MMSR and SMLR NetMod Optical Parameters

PARAMETER	10GBASE MMSR	10GBASE SMLR
Optical connectors	LC duplex	LC duplex
Bit rate	10.000Gbps	10.000Gbps
Baud rate/ encoding/tolerance	10.3125Gbps / 64/66b encoding / +/- 100 ppm	10.3125Gbps / 64/66b encoding / +/- 100 ppm
Optical interface	Multimode	Single mode only
Operating distance	840-860 nm (850 nm typical) 26 m (85 ft) to 33 m (108 ft) for 62.5 µm/125 µm fiber (modal BW 160 to 200 respectively) 66 m (216 ft) to 82 m (269 ft) for 50 µm/125 µm fiber (modal BW 400 to 500 respectively) Distances to 300 m (980 ft) are available with higher quality (OM3) fiber. Minimum distances (all): 2 m (6ft)	1270-1355 nm (1310 nm typical) 2 m to 10 km (6 ft to 6.2 miles) for 9 µm/125 µm fiber
Transmitter wavelength	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	-1 dBm	-0.5 dBm
Minimum average launch power	-7.3 dBm	-8.2 dBm
Maximum average power at receiver	-1 dBm	-0.5 dBm
Receiver sensitivity	-9.9 dBm	-14.4 dBm

Stacking Module

The stacking module contains two connection ports for the 8000 Series stacking cable, and activity and link LEDs.



Use the Stacking LEDs table to understand the stacking LEDs. Note that the stacking module is available for the 3D8140 and 3D8250, and is included in the 3D8260, 3D8270, and 3D8290.

Stacking LEDs

Status	Description
Top	Indicates activity on the interface: • A blinking light indicates there is activity on the interface. • No light indicates there is no activity.
Bottom	Indicates whether the interface has link: • A light indicates the interface has link. • No light indicates there is no link.

CHAPTER 7
RESTORING A SOURCEFIRE APPLIANCE TO FACTORY DEFAULTS

Sourcefire provides ISO images on its Support Site for restoring, or reimaging, Defense Centers and managed devices to their original factory settings.

For more information, see the following sections:

Before You Begin

Before you begin restoring your appliances to factory defaults, you should familiarize yourself with the expected behavior of the system during the restore process.

Configuration and Event Backup Guidelines

Before you begin the restore process, Sourcefire recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

Restoring your appliance to factory defaults results in the loss of almost **all** configuration and event data on the appliance. Although the restore utility can retain the appliance's license, network, console, and Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

Traffic Flow During the Restore Process

To avoid disruptions in traffic flow on your network, Sourcefire recommends restoring your appliances during a maintenance window or at a time when the interruption will have the least impact on your deployment.

Restoring a managed device that is deployed inline resets the device to a non-bypass (fail closed) configuration, disrupting traffic on your network. Traffic is blocked until you configure bypass-enabled inline sets on the device.

For more information about editing your device configuration to configure bypass, see the Managing Devices chapter of the *Sourcefire 3D System User Guide*.

Understanding the Restore Process

A Sourcefire *appliance* is either a traffic-sensing managed *device* or a managing *Defense Center*. There are several *models* of each appliance type; these models are further grouped into *series* and *family*. For more information, see Understanding Appliance Series, Models, and Capabilities on page 10.

The precise steps you take to restore an appliance depend on the appliance's model and whether you have physical access to the appliance, but the general process is the same.

IMPORTANT! Only reimage your appliances during a maintenance window. Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process on page 199.

To restore a Sourcefire appliance:

Access: Admin

1. Determine the model of the appliance (device or Defense Center) you want to restore.
2. Obtain the correct restore ISO image from the Support Site.

3. Copy the image to an appropriate storage medium.
4. Connect to the appliance.
5. Reboot the appliance and invoke the restore utility.
6. Install the ISO image.

For your convenience, you can install system software and intrusion rule updates as part of the restore process on most appliances.

The following table summarizes how to restore the different models of Sourcefire appliances.

Supported Restore Methods by Appliance Model

Models	Restore Method	Physical Access Required?	Update during Restore?
DC1000 DC3000	Use a Sourcefire-provided CD-ROM with the ISO image pre-loaded, or create your own CD.	yes, to load the CD	no
DC500 all Series 2 devices (except 3D9900)	Boot from a Sourcefire-provided external USB drive and use an interactive menu to download and install the ISO image on the appliance.	yes, to insert the USB drive	yes
3D9900 Series 3 appliances	Boot from the appliance's internal flash drive and use an interactive menu to download and install the ISO image on the appliance.	no; a remote KVM switch (all) or LOM (Series 3) allows you to restore remotely	yes

Note that you **cannot** restore an appliance using its web interface. To restore an appliance, you must connect to it in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to any Sourcefire appliance, which is useful for rack-mounted appliances connected to a KVM (keyboard, video, and mouse) switch. If you have a KVM that is remote-accessible, you can restore Series 3 appliances and the 3D9900 without having physical access.

Serial Connection/Laptop

You can use a serial cable to connect a computer to any Sourcefire appliance except the 3D2100/2500/3500/4500 devices. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. The settings for this software are 9600 baud, 8 data bits, no parity checking, 1 stop bit, and no flow control.

Lights-Out Management Using Serial over LAN

The LOM feature allows you to perform a limited set of actions on a Series 3 appliance, using a Serial over LAN (SOL) connection. If you need to restore a LOM-capable appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. After you connect to an appliance using LOM, you issue commands to the restore utility as if you were using a physical serial connection. For more information, see Setting up Lights-Out Management on page 219.

Obtaining the Restore ISO and Update Files

Sourcefire provides ISO images for restoring appliances to their original factory settings. Before you restore an appliance, obtain the correct ISO image from the Sourcefire Support Site.

The ISO image you should use to restore an appliance depends on when Sourcefire introduced support for that appliance model. Unless the ISO image was released with a minor version to accommodate a new appliance model, ISO images are usually associated with major versions of the system software (for example, 5.1 or 5.2). To avoid installing an incompatible version of the system, Sourcefire recommends that you always use the most recent ISO image available for your appliance.

Most Sourcefire appliances use an external USB or internal flash drive to boot the appliance so you can run the restore utility. However, DC1000 and DC3000 Defense Centers require a restore ISO CD. If you have a DC1000 or DC3000, Sourcefire provided you with an ISO image on CD-ROM when you purchased the appliance. If you want to restore the appliance to a different version, you can download the appropriate ISO image and create a new restore ISO (not data) CD, which you can then use to restore the appliance.

Sourcefire also recommends that you always run the latest version of the system software supported by your appliance. After you restore an appliance to the latest supported major version, you should update its system software, intrusion rules, and Vulnerability Database (VDB). For more information, see the release notes for the update you want to apply, as well as the Updating System Software chapter in the *Sourcefire 3D System User Guide*.

For your convenience, you can install system software and intrusion rule updates as part of the restore process on most appliances. For example, you could restore a device to Version 5.2, and also update the device to Version 5.2.0.1 as part of that process. Keep in mind that only Defense Centers require rule updates.

Note that because you use a CD to restore DC1000 and DC3000 Defense Centers, you cannot install updates as part of the restore process on those appliances. Instead, update the appliances afterward.

To obtain the restore ISO and other update files:

Access: Any

1. Using the user name and password for your support account, log into the Sourcefire Support Site (https://support.sourcefire.com/).
2. Click **Downloads**, select the **3D System** tab on the page that appears, and then click the major version of the system software you want to install.

   For example, to download a Version 5.2 or Version 5.2.1 ISO image, you would click **Downloads > 3D System > 5.2**.
3. Find the image (ISO image) that you want to download.

   You can click one of the links on the left side of the page to view the appropriate section of the page. For example, you would click **5.2.1 Images** to view the images and release notes for Version 5.2.1 of the Sourcefire 3D System.
4. Click the ISO image you want to download.

   The file begins downloading.
5. Optionally, download system software and intrusion rule updates:
   - System software updates are on the same page of the Support Site as the ISO images. You can click one of the links on the left side of the page to view the appropriate section of the page. For example, you would click **5.2.1** to view the updates and release notes for Version 5.2.1 of the Sourcefire 3D System.
   - To download a rule update, select **Downloads > Rules & VDB > Rules**. The most recent rule update is at the top of the page.

   Remember that if you are restoring a DC1000 or DC3000 you must install updates after the restore process completes.
6. How are you going to restore the appliance?
   - For most appliances—those that you restore with a USB or internal flash drive—copy the files to an HTTP (web) server, FTP server, or SCP-enabled host that the appliance can access on its management network.
   - For the DC1000 and DC3000, create a restore CD using the ISO image.

WARNING! Do **not** transfer ISO or update files via email; the files can become corrupted. Also, do **not** change the names of the files; the restore utility requires that they be named as they are on the Support Site.

Beginning the Restore Process

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

For all appliances except the DC1000 and DC3000 Defense Centers, begin the restore process by booting the appliance from either an external USB or internal flash drive, depending on the appliance model; see the Supported Restore Methods by Appliance Model table on page 200.

After you make sure that you have the appropriate level of access and connection to an appliance, as well the correct ISO image, use one of the following procedures to restore your appliance:

- Starting the Restore Utility Using KVM or Physical Serial on page 203 explains how to start the restore process for an appliance that does not support LOM, or where you do not have LOM access. You can use this method to restore any appliance except a DC1000 or DC3000 Defense Center.
- Starting the Restore Utility Using Lights-Out Management on page 205 explains how use LOM to start the restore process for a Series 3 appliance, via an SOL connection.
- Restoring a DC1000 or DC3000 Using a CD on page 217 explains how to restore a DC1000 or DC3000 Defense Center using a CD.

WARNING! The procedures in this chapter explain how to restore an appliance without powering it down. However, if you need to power down for any reason, use the procedure in the Managing Devices chapter in the *Sourcefire 3D System User Guide*, the `system shutdown` command from the CLI on a Series 3 device, or the `shutdown -h now` command from an appliance's shell (sometimes called expert mode).

Starting the Restore Utility Using KVM or Physical Serial

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

For all appliances except DC1000 and DC3000 Defense Centers, Sourcefire provides a restore utility on either an external USB or internal flash drive, depending on the appliance model; see the Supported Restore Methods by Appliance Model table on page 200.

TIP! If you need to restore a Series 3 appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. See Starting the Restore Utility Using Lights-Out Management on page 205.

To start the restore utility:

Access: Admin

1. If you are using a USB drive to restore a DC500 or any Series 2 device except the 3D9900, insert the USB drive into an available USB port on the appliance.

   Otherwise, skip to the next step.

2. Using your keyboard/monitor or serial connection, log into the appliance using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.

   The prompt for the appliance appears.

3. Reboot the appliance:

   - On a Defense Center or Series 2 managed device, type `sudo su -`, then type your password again. At the root prompt, reboot the appliance by typing `reboot`.
   - On a Series 3 managed device, type `system reboot`.

   The appliance reboots. On a DC500 Defense Center or 3D500/1000/2000 device, a Sourcefire splash screen appears.

4. Monitor the reboot status:

   - On a DC500 Defense Center or 3D500/1000/2000 device, press Ctrl + U slowly and repeatedly when the splash screen appears.
   - For all other appliances that use a keyboard and monitor connection, a red LILO boot menu appears. Quickly press one of the arrow keys to prevent the appliance from booting the currently installed version of the system.
   - For all other appliances that use a serial connection, when you see the BIOS boot options, press Tab slowly and repeatedly (to prevent the appliance from booting the currently installed version of the system). The LILO boot prompt appears:

     ```
     LILO 22.8 boot:
     3D-5.2 System_Restore
     ```

5. Indicate that you want to restore the system:

   - On a DC500 Defense Center or 3D500/1000/2000 device, press Enter.
   - For all other appliances that use a keyboard and monitor connection, use the arrow keys to select `System_Restore` and press Enter.
   - For all other appliances that use a serial connection, type `System_Restore` at the prompt and press Enter.

   The `boot` prompt appears after the following choices:

   ```
   0. Load with standard console
   1. Load with serial console
   ```

6. Select a display mode for the restore utility's interactive menu:
   - For a keyboard and monitor connection, type `0` and press Enter.
   - For a serial connection, type `1` and press Enter.

   If you do not select a display mode, the restore utility defaults to the standard console after 10 seconds.

   Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.

   The restore utility copyright notice appears.
7. Press Enter to confirm the copyright notice and continue with Using the Interactive Menu to Restore an Appliance on page 207.

Starting the Restore Utility Using Lights-Out Management

SUPPORTED DEVICES: Series 3
SUPPORTED DEFENSE CENTERS: Series 3

If you need to restore a Series 3 appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process.

IMPORTANT! Before you can restore an appliance using LOM, you must enable the feature; see Setting up Lights-Out Management on page 219.

To start the restore utility using Lights-Out Management:

ACCESS: Admin

1. At your computer's command prompt, enter the IPMI command to start the SOL session and display the prompt for the appliance:
   - For IPMItool, type:

     `ipmitool -I lanplus -H` *`IP_address`* `-U` *`username`* `sol activate`
   - For ipmiutil, type:

     `ipmiutil sol -a -V4 -J3 -N` *`IP_address`* `-U` *`username`* `-P` *`password`*

   Where *`IP_address`* is the IP address of the management interface on the appliance, *`username`* is user name of an authorized LOM account, and *`password`* is the password for that account. Note that IPMItool prompts you for the password after you issue the `sol activate` command.

2. Reboot the appliance:
   - For a Defense Center, type `sudo su -`, then type your password again. At the `root` prompt, reboot the appliance by typing `reboot`.
   - For a Series 3 device, type `system reboot`.

   The appliance reboots.
3. Monitor the reboot status. When you see the BIOS boot options, press Tab slowly and repeatedly (to prevent the appliance from booting the currently installed version of the system) until the LILO boot prompt appears:

   ```
   LILO 22.8 boot:
   3D-5.2 System_Restore
   ```
4. At the `boot` prompt, start the restore utility by typing `System_Restore`.

   The `boot` prompt appears after the following choices:

   ```
   0. Load with standard console
   1. Load with serial console
   ```
5. Type `1` and press Enter to load the interactive restore menu via the appliance's serial connection.

   IMPORTANT! If you do not select a display mode, the restore utility defaults to the standard console after 10 seconds.

   Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.

   The restore utility copyright notice appears.
6. Press Enter to confirm the copyright notice and continue with Using the Interactive Menu to Restore an Appliance on page 207.

Using the Interactive Menu to Restore an Appliance

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

The restore utility for most Sourcefire appliances uses an interactive menu to guide you through the restoration.

TIP! If you are restoring a DC1000 or DC3000 with a CD, skip to Restoring a DC1000 or DC3000 Using a CD on page 217.

IMPORTANT! Only reimage your appliances during a maintenance window. Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process on page 199.

The menu displays the options listed in the following table.

Restore Menu Options

OPTION	DESCRIPTION	FOR MORE INFORMATION, SEE...
1 IP Configuration	Specify network information about the management interface on the appliance you want to restore, so that the appliance can communicate with the server where you placed the ISO and any update files.	Identifying the Appliance's Management Interface on page 209
2 Choose the transport protocol	Specify the location of the ISO image you will use to restore the appliance, as well as any credentials the appliance needs to download the file.	Specifying ISO Image Location and Transport Method on page 210
3 Select Patches/Rule Updates	Specify a system software and intrusion rules update to be applied after the appliance is restored to the base version in the ISO image.	Updating System Software and Intrusion Rules During Restore on page 211
4 Download and Mount ISO	Download the appropriate ISO image and any system software or intrusion rule updates. Mount the ISO image.	Downloading the ISO and Update Files and Mounting the Image on page 212

Restore Menu Options (Continued)

Option	Description	For more information, see...
5 Run the Install	Invoke the restore process.	Invoking the Restore Process on page 213
6 Save Configuration 7 Load Configuration	Save any set of restore configurations for later use, or load a saved set.	Saving and Loading Restore Configurations on page 215
8 Wipe Contents of Disk	Securely scrub the hard drive to ensure that its contents can no longer be accessed.	Scrubbing the Contents of the Hard Drive on page 219

Navigate the menu using your arrow keys. To select a menu option, use the up and down arrows. Use the right and left arrow keys to toggle between the **OK** and **Cancel** buttons at the bottom of the page.

The menu presents two different kinds of options:

- To select a numbered option, first highlight the correct option using the up and down arrows, then press Enter while the **OK** button at the bottom of the page is highlighted.
- To select a multiple-choice (radio button) option, first highlight the correct option using the up and down keys, then press the space bar to mark that option with an x. To accept your selection, press Enter while the **OK** button is highlighted.

In most cases, complete menu options **1**, **2**, **4**, and **5**, in order. Optionally, add menu option **3** to install system software and intrusion rule updates during the restore process.

If you are restoring an appliance to a different major version from the version currently installed on the appliance, a two-pass restore process is required. The first pass updates the operating system, and the second pass installs the new version of the system software.

If this is your second pass, or if the restore utility automatically loaded the restore configuration you want to use, you can start with menu option **4**: Downloading the ISO and Update Files and Mounting the Image on page 212. However, Sourcefire recommends you double-check the settings in the restore configuration before proceeding.

TIP! To use a previously saved configuration, start with menu option **6**: Saving and Loading Restore Configurations on page 215. After you load the configuration, skip to menu option **4**: Downloading the ISO and Update Files and Mounting the Image on page 212.

To restore an appliance using the interactive menu, select:

ACCESS: Admin

1. **1 IP Configuration** — see Identifying the Appliance's Management Interface on page 209.
2. **2 Choose the transport protocol** — see Specifying ISO Image Location and Transport Method on page 210.
3. **3 Select Patches/Rule Updates** (optional) — Updating System Software and Intrusion Rules During Restore on page 211.
4. **4 Download and Mount ISO** — see Downloading the ISO and Update Files and Mounting the Image on page 212.
5. **5 Run the Install** — see Invoking the Restore Process on page 213.

Identifying the Appliance's Management Interface

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

The first step in running the restore utility is to identify the management interface on the appliance you want to restore, so that the appliance can communicate with the server where you copied the ISO and any update files. If you are using LOM, remember that the management IP address for the appliance is **not** the LOM IP address.

To identify the appliance's management interface:

ACCESS: Admin

1. From the main menu, select **1 IP Configuration**.

   The Pick Device page appears.
2. Select the appliance's management interface (generally **eth0**).

   The IP Configuration page appears.
3. Select the protocol you are using for your management network: **IPv4** or **IPv6**.

   Options for assigning an IP address to the management interface appear.
4. Select a method to assign an IP address to the management interface: **Static** or **DHCP**.
   - If you select **Static**, a series of pages prompts you to manually enter the IP address, network mask or prefix length, and default gateway for the management interface.
   - If you select **DHCP**, the appliance automatically detects the IP address, network mask or prefix length, and default gateway for the management interface, then displays the IP address.

5. When prompted, confirm your settings.

   If prompted, confirm the IP address assigned to the appliance's management interface. The main menu appears again.

6. Continue with the next section, Specifying ISO Image Location and Transport Method.

Specifying ISO Image Location and Transport Method

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

After you configure the management IP address that the restore process will use to download files it needs, you must identify which ISO image you will use to restore the appliance. This is the ISO image that you downloaded from the Support Site (see Obtaining the Restore ISO and Update Files on page 201), and stored on a web server, FTP server, or SCP-enabled host.

The interactive menu prompts you to enter any necessary information to complete the download, as listed in the following table.

Information Needed to Download Restore Files

TO USE...	YOU MUST PROVIDE...
HTTP	• IP address for the web server • full path to the ISO image directory (for example, `/downloads/ISOs/`)
FTP	• IP address for the FTP server • path to the ISO image directory, relative to the home directory of the user whose credentials you want to use (for example, `mydownloads/ISOs/`) • authorized user name and password for the FTP server
SCP	• IP address for the SCP server • authorized user name for the SCP server • full path to the ISO image directory • password for the user name you entered earlier Note that before you enter your password, the appliance may ask you to add the SCP server to its list of trusted hosts. You must accept to continue.

Note that the restore utility will also look for update files in the ISO image directory.

To specify the restore files' location and transport method:

ACCESS: Admin

1. From the main menu, select **2 Choose the transport protocol**.
2. On the page that appears, select either **HTTP**, **FTP**, or **SCP**.
3. Use the series of pages presented by the restore utility to provide the necessary information for the protocol you chose, as described in the Information Needed to Download Restore Files table on page 210.

   If your information was correct, the appliance connects to the server and displays a list of the Sourcefire ISO images in the location you specified.
4. Select the ISO image you want to use.
5. When prompted, confirm your settings.

   The main menu appears again.
6. Do you want to install a system software or intrusion rule update as a part of the restore process?
   - If yes, continue with the next section, Updating System Software and Intrusion Rules During Restore.
   - If no, continue with Downloading the ISO and Update Files and Mounting the Image on page 212. Note that you can use the system's web interface to manually install updates after the restore process completes.

Updating System Software and Intrusion Rules During Restore

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

Optionally, you can use the restore utility to update the system software and intrusion rules after the appliance is restored to the base version in the ISO image. Note that only Defense Centers require rule updates.

The restore utility can only use one system software update and one rule update. However, system updates are cumulative back to the last major version; rule updates are also cumulative. Sourcefire recommends that you obtain the latest updates available for your appliance; see Obtaining the Restore ISO and Update Files on page 201.

If you choose not to update the appliance during the restore process, you can update later using the system's web interface. For more information, see the release notes for the update you want to install, as well as the Updating System Software chapter in the *Sourcefire 3D System User Guide*.

To install updates as part of the restore process:

ACCESS: Admin

1. From the main menu, select **3 Select Patches/Rule Updates**.

   The restore utility uses the protocol and location you specified in the previous procedure (see Specifying ISO Image Location and Transport Method on page 210) to retrieve and display a list of any system software update files in that location. If you are using SCP, enter your password when prompted to display the list of update files.

2. Select the system software update, if any, you want to use.

   You do not have to select an update; press Enter without selecting an update to continue. If there are no system software updates in the appropriate location, the system prompts you to press Enter to continue.

   The restore utility retrieves and displays a list of rule update files. If you are using SCP, enter your password when prompted to display the list.

3. Select the rule update, if any, you want to use.

   You do not have to select an update; press Enter without selecting an update to continue. If there are no rule updates in the appropriate location, the system prompts you to press Enter to continue.

   Your choices are saved and the main menu appears again.

4. Continue with the next section, Downloading the ISO and Update Files and Mounting the Image.

Downloading the ISO and Update Files and Mounting the Image

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

The final step before you invoke the restore process is to download the necessary files and mount the ISO image.

TIP! Before you begin this step, you may want to save your restore configuration for later use. For more information, see Saving and Loading Restore Configurations on page 215.

To download and mount the ISO image:

ACCESS: Admin

1. From the main menu, select **4 Download and Mount ISO**.

2. When prompted, confirm your choice. If you are downloading from an SCP server, enter your password when prompted.

   The appropriate files are downloaded and mounted. The main menu appears again.

3. Continue with the next section, Invoking the Restore Process.

Invoking the Restore Process

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

After you download and mount the ISO image, you are ready to invoke the restore process. If you are restoring an appliance to a different major version from the version currently installed on the appliance, a two-pass restore process is required. The first pass updates the operating system, and the second pass installs the new version of the system software.

First Pass of Two (Changing Major Versions Only)

When restoring an appliance to a different major version, a first pass by the restore utility updates the appliance's operating system, and, if necessary, the restore utility itself.

IMPORTANT! If you are restoring an appliance to the same major version, or if this is your second pass through the process, skip to the next procedure: Second or Only Pass on page 214.

To perform the first pass of a two-pass restore process:

ACCESS: Admin

1. From the main menu, select **5 Run the Install**.
2. When prompted (twice), confirm that you want to reboot the appliance.

IMPORTANT! For appliances you are restoring using an external USB drive, if the drive has a restore utility associated with a different version of the system, you must update the utility on the drive to continue. When prompted, type `yes` to update the utility (and delete any saved restore configurations). Then, confirm that you want to reboot from the updated drive. If you do not update the USB drive, the appliance reboots. You cannot restore the appliance using this drive.

3. Monitor the reboot and invoke the restore process again:
   - For a keyboard and monitor connection, a red LILO boot menu appears. Quickly press one of the arrow keys to prevent the appliance from booting the currently installed version of the system.
   - For a serial or SOL/LOM connection, when you see the BIOS boot options, press Tab slowly and repeatedly until the LILO boot prompt appears:

     ```
     LILO 22.8 boot:
     3D-5.2 System_Restore
     ```

4. Indicate that you want to restore the system:
   - For a keyboard and monitor connection, use the arrow keys to select `System_Restore` and press Enter.
   - For a serial or SOL/LOM connection, type `System_Restore` at the prompt and press Enter.

   In either case, the `boot` prompt appears after the following choices:

   ```
   0. Load with standard console
   1. Load with serial console
   ```

5. Select a display mode for the restore utility's interactive menu:
   - For a keyboard and monitor connection, type `0` and press Enter.
   - For a serial or SOL/LOM connection, type `1` and press Enter.

   If you do not select a display mode, the restore utility defaults to the standard console after 10 seconds.

   Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.

   The restore utility copyright notice appears.

6. Press Enter to confirm the copyright notice, then begin the second pass of the process, starting with Using the Interactive Menu to Restore an Appliance on page 207.

Second or Only Pass

Use the following procedure to perform the second or only pass through the restore process.

To perform the second or only pass through the restore process:

Access: Admin

1. From the main menu, select **5 Run the Install**.
2. Confirm that you want to restore the appliance and continue with the next step.

3. Choose whether you want to delete the appliance's license and network settings. Deleting these settings also resets display (console) settings and, for Series 3 appliances, LOM.

   In most cases, you do not want to delete these settings, because it can make the initial setup process shorter. Changing settings after the restore and subsequent initial setup is often less time consuming than trying to reset them now. For more information, see Next Steps on page 218.

4. If you are using a USB drive to restore the appliance, remove the drive when the restore utility prompts you to type your final confirmation that you want to restore the appliance.

5. Type your final confirmation that you want to restore the appliance.

   The final stage of the restore process begins. When it completes, if prompted, confirm that you want to reboot the appliance.

WARNING! Make sure you allow sufficient time for the restore process to complete. On appliances with internal flash drives, the utility first updates the flash drive, which is then used to perform other restore tasks. If you quit (by pressing Ctrl + C, for example) during the flash update, you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, do **not** quit. Instead, contact Support.

IMPORTANT! Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process on page 199.

6. Continue with Next Steps on page 218.

Saving and Loading Restore Configurations

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

For most appliances, you can use the restore utility to save a restore configuration to use if you need to restore the appliance again. Although the restore utility

automatically saves the last configuration used, you can save multiple configurations, which include:

- network information about the management interface on the appliance; see Identifying the Appliance's Management Interface on page 209
- the location of the restore ISO image, as well as the transport protocol and any credentials the appliance needs to download the file; see Specifying ISO Image Location and Transport Method on page 210
- the system software and intrusion rules updates, if any, that you want to apply after the appliance is restored to the base version in the ISO image; see Updating System Software and Intrusion Rules During Restore on page 211

SCP passwords are not saved. If the configuration specifies that the utility must use SCP to transfer ISO and other files to the appliance, you will have to re-authenticate to the server to complete the restore process.

The best time to save a restore configuration is after you provide the information listed above, but before you download and mount the ISO image. Note that if you update a restore USB drive to be compatible with a different major version of the system, any saved restore configurations are lost.

To save a restore configuration:

Access: Admin

1. From the restore utility's main menu, select **6 Save Configuration**.

   The utility displays the settings in the configuration you are saving.
2. When prompted, confirm that you want to save the configuration.
3. When prompted, enter a name for the configuration.

   Your configuration is saved and the main menu appears again.
4. If you want to use the configuration you just saved to restore the appliance, continue with Downloading the ISO and Update Files and Mounting the Image on page 212.

To load a saved restore configuration:

Access: Admin

1. From the main menu, select **7 Load Configuration**.

   The utility presents a list of saved restore configurations. The first option, **default_config**, is the configuration you last used to restore the appliance. The other options are restore configurations that you have saved.
2. Select the configuration you want to use.

   The utility displays the settings in the configuration you are loading.

3. When prompted, confirm that you want to load the configuration.

   The configuration is loaded. If prompted, confirm the IP address assigned to the appliance's management interface. The main menu appears again.

4. To use the configuration you just loaded to restore the appliance, continue with Downloading the ISO and Update Files and Mounting the Image on page 212.

Restoring a DC1000 or DC3000 Using a CD

SUPPORTED DEVICES: None
SUPPORTED DEFENSE CENTERS: DC1000, DC3000

For DC1000 and DC3000 Defense Centers, which have CD-ROM drives, Sourcefire provided a restore CD when you purchased the appliance. If you want to restore the appliance to a different version, you can download the appropriate ISO image and create a new ISO (not data) restore CD, which you can then use to restore the system; see Obtaining the Restore ISO and Update Files on page 201.

Note that because you use a CD to restore these Defense Centers, you cannot install updates as part of the restore process on those appliances. Instead, update the appliances afterward.

To restore a DC1000 or DC3000 using a CD:

ACCESS: Admin

1. Place the restore CD in the Defense Center's CD tray.

   If the appliance is off, power it on to open the tray.

2. Using your keyboard/monitor or serial connection, log into the Defense Center using an account with Administrator privileges. The password is the same as the password for the Defense Center's web interface.

   The prompt for the Defense Center appears.

3. At the prompt, access root privileges: type `sudo su -`, press Enter, then provide your password.

4. At the `root` prompt, reboot the Defense Center by typing `reboot`.

   The Defense Center boots from the CD. This can take several minutes.

5. When prompted, confirm that you want to restore the Defense Center.

6. Choose whether you want to delete the appliance's license and network settings. Deleting these settings also resets display (console) settings.

   In most cases, you do not want to delete these settings, because it can make the initial setup process shorter. Changing settings after the restore and subsequent initial setup is often less time consuming than trying to reset them now. For more information, see Next Steps on page 218.

7. Type your final confirmation that you want to restore the appliance.

   The restore process begins and shows its progress on the screen.

   WARNING! Make sure you allow sufficient time for the restore process to complete. In rare cases, If you quit (by pressing Ctrl + C or powering down the appliance, for example), you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, do **not** quit. Instead, contact Support.

8. When prompted, press Enter to continue.

   The Defense Center ejects the CD. Remove the CD and close the tray.

9. When prompted again, press Enter to confirm that the restoration is complete and that you want to reboot the appliance.

   The appliance reboots.

10. Continue with Next Steps.

Next Steps

Restoring your appliance to factory default settings results in the loss of almost **all** configuration and event data on the appliance, including bypass configurations for devices deployed inline. For more information, see Traffic Flow During the Restore Process on page 199.

After you restore an appliance, you must complete an initial setup process:

- If you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. For more information, see Initial Setup Page: Devices on page 93 and Initial Setup Page: Defense Centers on page 100.
- If you deleted license and network settings, you must configure the appliance as if it were new, beginning with configuring it to communicate on your management network. See the next chapter, Setting Up a Sourcefire 3D System Appliance on page 86.

Note that deleting license and network settings also resets display (console) settings and, for Series 3 appliances, LOM settings. After you complete the initial setup process:

- If you want to use a serial or SOL/LOM connection to access your appliance's console, you should redirect console output; see Redirecting Console Output on page 82.
- If you want to use LOM, you must re-enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users on page 221.

Scrubbing the Contents of the Hard Drive

SUPPORTED DEVICES: Any
SUPPORTED DEFENSE CENTERS: Any except DC1000/3000

You can securely scrub the hard drive on most Sourcefire appliances to ensure that its contents can no longer be accessed. For example, if you need to return a defective appliance that contains sensitive data, you can use this feature to overwrite the data.

This mode of scrubbing the disk meets the following military standard:

STANDARDS

The DoD scrub sequence is compliant with the DoD 5220.22-M procedure for sanitizing removable and non-removable rigid disks which requires overwriting all addressable locations with a character, its complement, then a random character, and verify. Please refer to the DoD document for additional constraints.

WARNING! Scrubbing your hard drive results in the loss of **all** data on the appliance, which is rendered inoperable.

To scrub the hard drive:

ACCESS: Admin

1. Follow the instructions in one of the following sections to display the restore utility's interactive menu, depending on how you are accessing the appliance:
   - Starting the Restore Utility Using KVM or Physical Serial on page 203
   - Starting the Restore Utility Using Lights-Out Management on page 205

   Note that the DC1000 and DC3000 do not support this feature.
2. From the main menu, select **8 Wipe Contents of Disk**.
3. When prompted, confirm that you want to scrub the hard drive.

   The hard drive is scrubbed. The scrub process may take several hours to complete; larger drives take longer.

Setting up Lights-Out Management

SUPPORTED DEVICES: Series 3
SUPPORTED DEFENSE CENTERS: Series 3

If you need to restore a Series 3 appliance to factory defaults and do not have physical access to the appliance, you can use Lights-Out Management (LOM) to perform the restore process. You **cannot** restore a Series 2 appliance using LOM. Only Series 3 appliances support LOM.

The LOM feature allows you to perform a limited set of actions on a Series 3 Defense Center or managed device, using a Serial over LAN (SOL) connection. With LOM, you use a command line interface on an out-of-band management connection to perform tasks such as viewing the chassis serial number, or monitoring conditions such as fan speed and temperature.

The syntax of LOM commands depends on the utility you are using, but LOM commands generally contain the elements listed in the following table.

LOM Command Syntax

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
`ipmitool`	`ipmiutil`	Invokes the IPMI utility.
n/a	`-V4`	For ipmiutil only, enables admin privileges for the LOM session.
`-I lanplus`	`-J3`	Enables encryption for the LOM session.
`-H` *`IP_address`*	`-N` *`IP_address`*	Specifies the IP address of the management interface on the appliance.
`-U` *`username`*	`-U` *`username`*	Specifies the user name of an authorized LOM account.
n/a (prompted on login)	-P *`password`*	For ipmiutil only, specifies the password for an authorized LOM account.
`command`	*`command`*	The command you want to issue to the appliance. Note that where you issue the command depends on the utility: • For IPMItool, type the command last. • For ipmiutil, type the command first.

Therefore, for IPMItool:

```
ipmitool -I lanplus -H IP_address -U username command
```

Or, for ipmiutil:

```
ipmiutil command -V4 -J3 -N IP_address -U username -P
password
```

For a full list of LOM commands supported by the Sourcefire 3D System, see the Configuring Appliance Settings chapter in the *Sourcefire 3D System User Guide*.

IMPORTANT! Before you can connect to a 7000 Series device using SOL, you must disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to the device's management interface.

Before you can restore an appliance using LOM, you must enable LOM for both the appliance and the user who will perform the restore. Then, use a third-party Intelligent Platform Management Interface (IPMI) utility to access the appliance. You must also make sure you redirect the appliance's console output to the serial port.

For more information, see the following sections:

- Enabling LOM and LOM Users on page 221
- Installing an IPMI Utility on page 222
- Redirecting Console Output on page 82

Enabling LOM and LOM Users

SUPPORTED DEVICES: Series 3
SUPPORTED DEFENSE CENTERS: Series 3

Before you can use LOM to restore an appliance, you must enable and configure the feature. You must also explicitly grant LOM permissions to users who will use the feature.

You configure LOM and LOM users on a per-appliance basis using each appliance's local web interface. That is, you cannot use the Defense Center to configure LOM on a managed device. Similarly, because users are managed independently per appliance, enabling or creating a LOM-enabled user on the Defense Center does not transfer that capability to users on managed devices.

LOM users also have the following restrictions:

- You must assign the Administrator role to the user.
- The user name may have up to 16 alphanumeric characters. Hyphens and longer user names are not supported for LOM users.

- The password may have up to 20 alphanumeric characters. Longer passwords are not supported for LOM users. A user's LOM password is the same as that user's system password.
- Series 3 Defense Centers and 8000 Series devices can have up to 13 LOM users. 7000 Series devices can have up to eight LOM users.

TIP! For detailed instructions on the following tasks, see the Configuring Appliance Settings chapter in the *Sourcefire 3D System User Guide*.

To enable LOM:

Access: Admin

1. Select **System > Local > Configuration**, then click **Console Configuration**.
2. Your next step depends on your appliance model:
   - To enable LOM on Defense Centers and 8000 Series devices, enable remote access using the **Physical Serial Port** before you can specify the LOM IP address, netmask, and default gateway (or use DHCP to have these values automatically assigned).
   - On 7000 Series devices, select **Lights Out Management** to configure LOM settings. 7000 Series devices do not support LOM and physical serial access at the same time.

IMPORTANT! The LOM IP address must be different from the management interface IP address of the appliance.

To enable LOM capabilities for a Sourcefire 3D System user:

Access: Admin

1. Select **System > Local > User Management**, then either edit an existing user to add LOM permissions, or create a new user that you will use for LOM access to the appliance.
2. On the User Configuration page, enable the **Administrator** role if it is not already enabled.
3. Enable the **Allow Lights-Out Management Access** check box and save your changes.

Installing an IPMI Utility

You use a third-party IPMI utility on your computer to create an SOL connection to the appliance.

If your computer is running Linux or Mac OS, use IPMItool. Although IPMItool is standard with many Linux distributions, you must install IPMItool on a Mac. First,

confirm that your Mac has Apple's xCode developer tools package installed. Also, make sure the optional components for command line development are installed ("UNIX Development" and "System Tools" in newer versions, or "Command Line Support" in older versions). Finally, install MacPorts and IPMItool. For more information, use your favorite search engine or see these sites:

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

For Windows environments, use ipmiutil, which you must compile yourself. If you do not have access to a compiler, you can use ipmiutil itself to compile. For more information, use your favorite search engine or see this site:

```
http://ipmiutil.sourceforge.net/
```

Chapter 8
Safety and Regulatory Information

Sourcefire appliances are delivered on multiple hardware platforms. General Safety Guidelines are applicable to all appliances. Regulatory Information for each appliance is described in its own section. Please read the following sections prior to installing the appliance and follow all guidelines when working with the appliance.

Sourcefire strongly recommends that you follow industry guidelines for general safety and electromagnetic emissions. The following sections include more information:

General Safety Guidelines

Follow these rules to ensure general safety:

1. Observe good housekeeping in the area of the machines during and after maintenance.
2. At all times, keep the chassis area free from dust.

3. When lifting any heavy object:
   - Lifting the chassis may require two people.
   - Ensure you can stand safely without slipping.
   - Distribute the weight of the object equally between your feet.
   - Use a slow lifting force. Never move suddenly or twist when you attempt to lift.
   - Lift by standing or by pushing up with your leg muscles; this action removes the strain from the muscles in your back. Do not attempt to lift any objects that weigh more than 16 kg (35 lb) or objects that you think are too heavy for you.
4. Do not perform any action that causes hazards or makes the equipment unsafe.
5. Before you start the machine, ensure that other service representatives and the customer's personnel are not in a hazardous position.
6. Place removed covers and other parts in a safe place, away from all personnel, while you are servicing the machine.
7. Keep your tool case away from walk areas so that other people do not trip over it.
8. Do not wear loose clothing that can be trapped in the moving parts of a machine. Ensure that your sleeves are fastened or rolled up above your elbows. If your hair is long, fasten it.
9. Insert the ends of your necktie or scarf inside clothing or fasten it with a nonconductive clip, approximately 8 centimeters (3 inches) from the end.
10. The appliance must be properly grounded when connecting power to the AC outlet.
11. Do not wear jewelry, chains, metal-frame eyeglasses, or metal fasteners for your clothing.

WARNING! **Remember:** Metal objects are good electrical conductors.

12. To avoid electrical shock, do not open or remove chassis covers or metal parts without proper instruction.
13. Wear safety glasses when you are: hammering, drilling, soldering, cutting wire, attaching springs, using solvents, or working in any other conditions that might be hazardous to your eyes.
14. There must be ample clearance on all sides of the chassis for the cooling air inlet and exhaust ports, as well as for access to the network interface modules (no less than 2 inches).

15. Remove all factory packaging before using the appliance.
16. Do not cover or block vents, or otherwise enclose the appliance.

Safety Warning Statements

Before installing this product, read the safety information in this section.

Statement 1

DANGER! Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.
- Connect all power cords to a properly wired and grounded electrical outlet.
- Connect to properly wired outlets any equipment that will be attached to this product.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.
- Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.

To connect:

1. Turn everything OFF.
2. Attach all cables to devices.
3. Attach signal cables to connectors.
4. Attach power cords to outlet.
5. Turn device ON.

To disconnect:

1. Turn everything OFF.
2. Remove power cords from outlet.
3. Remove signal cables from connectors.
4. Remove all cables from devices.

Statement 2

CAUTION! When replacing the lithium battery, use only an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of.

Do not:

- Throw or immerse into water.
- Heat to more than 100° C (212° F).
- Repair or disassemble.

Dispose of the battery as required by local ordinances or regulations.

Statement 3

CAUTION! When laser products (such as CD-ROMs, DVD drives, fiber optic devices, or transmitters) are installed, note the following:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

DANGER! Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following. Laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam.

Statement 4

CAUTION! Use safe practices when lifting.

Statement 5

CAUTION! The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

Statement 6

CAUTION! Never remove the cover on a power supply or any part that has the following label attached.

Hazardous voltage, current, and energy levels are present inside any component that has this label attached. There are no serviceable parts inside these components. If you suspect a problem with one of these parts, contact a service technician.

Statement 7

CAUTION! The following label indicates a hot surface nearby.

Statement 8

DANGER! Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed the branch circuit protection requirements.

Statement 9

CAUTION! Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the following label is attached.

Statement 10

CAUTION! Make sure that the rack is secured properly to avoid tipping when the server unit is extended.

Statement 11

CAUTION! Some accessory or option board outputs exceed Class 2 or limited power source limits and must be installed with appropriate interconnecting cabling in accordance with the national electric code.

Statement 12

CAUTION! The following label indicates moving parts nearby.

WARNING! Handling the cord on this product or cords associated with accessories sold with this product, will expose you to lead, a chemical known to the State of

California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Statement 13

WARNING! The following label indicates this product contains hazardous moving parts. Keep away from moving fan blades.

Regulatory Information

The regulatory information for each of the appliances is described in its own section:

- Sourcefire Defense Center 750/1500/3500 Information on page 229
- Sourcefire 3D500 Information on page 230
- Sourcefire Series 3 Information on page 232

Sourcefire Defense Center 750/1500/3500 Information

This product complies with the following safety standards and certifications:

Safety Standards

The following information applies to the DC750/1500/3500:

- UL60950 - CSA 60950(USA / Canada)
- EN60950 (Europe)
- IEC60950 (International)
- CB Certificate & Report, IEC60950 (report to include all country national deviations)
- GS License (Germany)
- GOST R 50377-92 - License (Russia)
- Belarus License (Belarus)
- Ukraine License (Ukraine)
- CE - Low Voltage Directive 73/23/EEE (Europe)
- IRAM Certification (Argentina)
- GB4943- CNCA Certification (China)
- FCC (Class A Verification) - Radiated & Conducted Emissions (USA)
- CISPR 22 - Emissions (International)

- EN55022 - Emissions (Europe)
- EN55024 - Immunity (Europe)
- EN61000-3-2 - Harmonics (Europe)
- EN61000-3-3 - Voltage Flicker (Europe)
- CE - EMC Directive 89/336/EEC (Europe)
- VCCI Emissions (Japan)
- AS/NZS 3548 Emissions (Australia / New Zealand)
- BSMI CNS13438 Emissions (Taiwan)
- GOST R 29216-91 Emissions (Russia)
- GOST R 50628-95 Immunity (Russia)
- Belarus License (Belarus)
- Ukraine License (Ukraine)
- RRL MIC Notice No. 1997-41 (EMC) & 1997-42 (EMI) (Korea)
- GB 9254 - CNCA Certification (China)
- GB 17625 - (Harmonics) CNCA Certification (China)

Certifications/Registrations/Declarations

The following information applies to the DC750/1500/3500:

- UL Certification (US/Canada)
- CE Declaration of Conformity (CENELEC Europe)
- FCC/ICES-003 Class A Attestation (USA/Canada)
- VCCI Certification (Japan)
- C-Tick Declaration of Conformity (Australia)
- MED Declaration of Conformity (New Zealand)
- BSMI Certification (Taiwan)
- GOST R Certification / License (Russia)
- Belarus Certification / License (Belarus)
- RRL Certification (Korea)
- IRAM Certification (Argentina)
- CNCA Certification (China)
- Ecology Declaration (International)

Sourcefire 3D500 Information

This appliance complies with the following electromagnetic compatibility (EMC) regulations:

Federal Communications Commission (FCC) statement

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Sourcefire is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

ATTENTION: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

NOTICE TO CUSTOMERS: This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformance with the protection requirements of European Council Directive EMC 2004/108/EC.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

ATTENTION: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Sourcefire Series 3 Information

The following section list the Series 3 devices by series, family, and chassis hardware codes. The chassis code appears on the regulatory label on the outside of the chassis, and is the official reference code for hardware certifications and safety.

Series 3 Device Families

SERIES	FAMILY	APPLIANCES
7000 Series	70xx Family	3D7010
		3D7020
		3D7030
7000 Series	71xx Family	3D7110
		3D7115
		3D7120
		3D7125
8000 Series	81xx Family	3D8120
		3D8130
		3D8140
8000 Series	82xx Family	3D8250
		3D8260
		3D8270
		3D8290

The following safety and regulatory information applies to the 7000 Series and 8000 Series devices:

Safety and Regulatory Compliance

The following sections describe the safety and regulatory compliance of the Series 3 appliances

70xx Family Appliances

The following information applies to all 70xx Family appliances:

Emissions:

- FCC, 47 CFR Part 15, Class A digital device
- EN 55022:2010, Class A
- EN 55024:2010
- EN61000-3-2:2006
- EN61000-3-3:2008
- BSMI CNS 13438

Safety:

- IEC 60950-1
- UL/CSA 60950-1:2nd Edition – 2011
- EN 60950-1: 2006/A11:2009
- EC Council Directive 2001/95/EC
- BSMI CNS 14336-1
- UL CB scheme
- These Sourcefire units are also in conformity with:
- Directive 2011/65/EU, Restriction of Hazardous Substances (RoHS)
- Directive 1907/2006EC, Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)

71xx Family and 8000 Series Appliances Safety and Regulatory Compliance

This 71xx Family and 8000 Series appliances comply with the following safety standards:

71xx Family and 8000 Series Safety and Regulatory Compliance

Regulation	Description
IEC 60950-1	Safety of Information Technology Equipment
UL/CSA 60950-1:2nd Edition – 2007	Safety of Information Technology Equipment
EN 60950-1: 2006/A11:2009	Safety of Information Technology Equipment
AS/NZS 60950-1: 2001	Safety of Information Technology Equipment
AS/NZS CISPR22:2022	Information Technology Equipment - Radio Disturbance Characteristics
FCC, 47 CFR Part 15, Class A digital device	Radio Frequency Devices – Subpart B – Unintentional Radiators
ICES-003 Issue 4 – Feb 2004, Class A	Interference-Causing Equipment Standards – Digital Apparatus
EN 55022:2006, Class A	Information Technology Equipment – Radio Disturbance Characteristics
EN 55024:1998 + A1:2001 + A2:2003	Information Technology Equipment – Immunity Characteristics
CISPR 22:2005 + A1:2005+A2:2006, Class A	Information Technology Equipment – Radio Disturbance Characteristics
CISPR 24:1997	Information Technology Equipment – Immunity Characteristics
EN61000-3-2:2006	Power Line Harmonics
EN61000-3-3:2008	Flicker and Voltage Fluctuations
ANSI C63.4	Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment
EC Council Directive 2001/95/EC	Safety

71xx Family and 8000 Series Safety and Regulatory Compliance (Continued)

Regulation	Description
EC Council Directive 2006/95/EC	LVD
EC Council Directive 2004/108/EC	Electromagnetic compatibility

Chassis and NetMod Designations

The following sections list the 7000 Series and 8000 Series appliance chassis, hardware chassis codes, and the Korean KC certification registration number for appliances available in the Republic of Korea:

7000 Series Chassis Designations

The 7000 Series Chassis Models - World-Wide and Korean Designations table lists the chassis designations for the 7000 Series models available world-wide, and in the Republic of Korea.

7000 Series Chassis Models - World-Wide and Korean Designations

3D Device Model	Hardware Chassis Code	Korean KC Certification Registration Number
3D7010/7020/7030	CHRY-1U-AC	KCC-REM-SFi-CHRY1UAC
3D7110/3D7120	GERY-1U-8-C-AC	KCC-REM-SFi-GERY1U8CAC
3D7110/3D7120	GERY-1U-8-FM-AC	KCC-REM-SFi-GERY1U8FMAC
3D7115/7125	GERY-1U-4C8S-AC	KCC-REM-SFi-GERY1U4C8SAC

8000 Series Chassis Designations

The 8000 Series Chassis Models - World-Wide Designation table lists the chassis designations for the Series 3 models available world-wide.

8000 Series Chassis Models - World-Wide Designation

3D Device Model	Hardware Chassis Code
3D8120 / 3D8130 / 3D8140 (AC power)	CHAS-1U-AC
3D8120 / 3D8130 / 3D8140 (DC power)	CHAS-1U-DC
3D8250 / 3D8260 / 3D8270 / 3D8290 (AC power)	CHAS-2U-AC
3D8250 / 3D8260 / 3D8270 / 3D8290 (DC power)	CHAS-2U-DC

The 8000 Series Chassis Models - Korean Designation table lists the chassis designations for the Series 3 models available in the Republic of Korea. Please note a blank (empty position) may be substituted for a network module for each slot listed.

8000 Series Chassis Models - Korean Designation

3D Device Model	Hardware Chassis Code	Korean KC Certification Registration Number	Network Module Configuration
3D8120 / 3D8130 / 3D8140 (AC power)	CHAS-1U-AC-0003	KCC-REM-SFi-CHAS1UAC0003	Slot 1: NM-C4-0 (or blank) Slot 2: NM-C4-0 (or blank) Slot 3: NM-FX4-0 (or blank)
3D8120 / 3D8130 / 3D8140 (DC power)	CHAS-1U-DC-0003	KCC-REM-SFi-CHAS1UDC0003	Slot 1: NM-C4-0 (or blank) Slot 2: NM-C4-0 (or blank) Slot 3: NM-FX4-0 (or blank)
3D8120 / 3D8130 / 3D8140 (AC power)	CHAS-1U-AC-0004	KCC-REM-SFi-CHAS1UAC0004	Slot 1: SF-3D-CLST-MOD-0(or blank) Slot 2: NM-*R2-0 (or blank)[1] Slot 3: NM-*R2-0 (or blank)[1]

8000 Series Chassis Models - Korean Designation (Continued)

3D Device Model	Hardware Chassis Code	Korean KC Certification Registration Number	Network Module Configuration
3D8120 / 3D8130 / 3D8140 (DC power)	CHAS-1U-DC-0004	KCC-REM-SFi-CHAS1UDC0004	Slot 1: SF-3D-CLST-MOD-0 (or blank) Slot 2: NM-*R2-0 (or blank)[1] Slot 3: NM-*R2-0 (or blank)[1]
3D8250 / 3D8260 / 3D8270 / 3D8290 (AC power)	CHAS-2U-AC-0005	KCC-REM-SFi-CHAS2UAC0005	Slot 1: SF-3D-CLST-MOD-0 (or blank) Slot 2: NM-*R2-0 (or blank)[1] Slot 3: NM-C4-0 (or blank) Slot 4: NM-FX4-0 (or blank) Slot 5: NM-FX4-0 (or blank) Slot 6: NM-*R2-0 (or blank)[1] Slot 7: NM-C4-0 (or blank)
3D8250 / 3D8260 / 3D8270 / 3D8290 (DC power)	CHAS-2U-DC-0005	KCC-REM-SFi-CHAS2UDC0005	Slot 1: SF-3D-CLST-MOD-0 (or blank) Slot 2: NM-*R2-0 (or blank)[1] Slot 3: NM-C4-0 (or blank) Slot 4: NM-FX4-0 (or blank) Slot 5: NM-FX4-0 (or blank) Slot 6: NM-*R2-0 (or blank)[1] Slot 7: NM-C4-0 (or blank)

[1]This network module can be either an NM-SR2-0 or an NM-LR2-0.

NetMod Designations for Korea

The 8000 Series NetMod Designation for Korea table lists the NetMod designations for the Series 3 models available in the Republic of Korea.

8000 Series NetMod Designation for Korea

NetMod Model	Korean KC Certification Registration Number
SF-3D-CLST-MOD-0	KCC-REM-SFi-SF3DCLSTMOD0
NM-C4-0	KCC-REM-SFi-NMC40
NM-FX4-0	KCC-REM-SFi-NMFX40
NM-SR2-0	KCC-REM-SFi-NMSR20
NM-LR2-0	KCC-REM-SFi-NMLR20

Safety Notices

The following sections list the safety notices for Korea, Japan, and Taiwan:

Safety Notice for Korea

Required statement indicating that Sourcefire's equipment is Class A.

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Safety Notice for Japan

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Safety Notice for Taiwan

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Waste Electrical and Electronic Equipment Directive (WEEE)

Sourcefire is compliant with the Waste Electrical and Electronic Equipment Directive (WEEE), Directive 2002/96/EC, as amended by 2003/108/EC. European Union customers who wish to dispose of a Sourcefire product may send it to Sourcefire for proper disposal.

For more information, contact:

Sourcefire EMEA
C/O Seko Benelux BV - Operations
Valkweg 1
1118 EC Schiphol
The Netherlands

Tel: +31-(0)20-8201193
Fax: +31-(0)20-6583 359

APPENDIX A
POWER REQUIREMENTS FOR SOURCEFIRE DEVICES

The following section describes the power requirements for the Sourcefire 3D System devices and related information:

Warnings and Cautions

This document contains both warnings and cautions. Warnings are safety related. Failure to follow warnings may lead to injury or equipment damage. Cautions are requirements for proper function. Failure to follow cautions may result in improper operation.

Interface Connections

WARNING! The intra-building ports of the equipment or subassembly are suitable for connection to intra-building or exposed wiring or cabling only. The intra-building ports of the equipment or subassembly **must not** be metallically connected to interfaces that connect outside the plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of the primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Static Control

CAUTION! Electrostatic discharge control procedures, such as using grounded wrist straps and an ESD work surface, must be in place before unpacking, installing, or moving the appliance. Excessive electrostatic discharges can damage the appliance or cause unintended operation.

3D7010/7020/7030

The 3D7010/7020/7030 (CHRY-1U-AC) is suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies. Note that this device is available only as an AC appliance.

Sourcefire recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See Installation on page 241 for circuit installation, voltage, current, frequency range, and power cord information.
- See Grounding/Earthing Requirements on page 242 for bonding locations, recommended terminals, and ground wire requirements.

Installation

The Sourcefire 3D System appliances must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook and local electrical codes.

The appliance uses a single power supply. An external surge protection device must be used at the input of the network equipment where the Sourcefire 3D System is to be installed.

The circuit must be rated for the full rating of the appliance.

Voltage

The power supply works with 100VAC to 240VAC nominal (90VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

Current

The labeled current rating is 2A maximum over the full range. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cord

The power connection on the power supply is an IEC C14 connector and accepts IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cord supplied with the appliance is a 16 AWG, UL-recognized cord with NEMA 515P plug. Contact the factory about other power cords.

IMPORTANT! Do **not** cut the cord on the power supply.

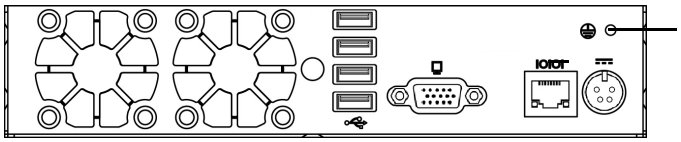
Grounding/Earthing Requirements

The appliance must be grounded to the common bonding network.

Bonding Location

A ground bonding location is provided on the rear of the chassis. An M4 stud is provided. An outside-toothed lock washer is provided for attaching a ring terminal. A standard ground symbol is available by each stud.

The following illustration indicates the bonding location on the chassis.



Recommended Terminals

You must use a UL-Approved terminal for the ground connection. A ring terminal with a clearance hole for #6 (M3.5) stud may be used. For 16 AWG wire, AMP/Tyco 36151 is recommended. This is a UL-approved ring terminal with a hole for a #6 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. See Current on page 241.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

3D7110/7120 and 3D7115/7125

This section describes the power requirements for the following Sourcefire devices:

- 3D7110/7120 (GERY-1U-8-AC)
- 3D7115/7125 (GERY-1U-4C8S-AC)

These Sourcefire devices are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies. Note that this device is available only as an AC appliance.

Sourcefire recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See Installation on page 243 for circuit installation, voltage, current, and frequency range, and power cord information.
- See Grounding/Earthing Requirements on page 244 for bonding locations, recommended terminals, and ground wire requirements.

Installation

The Sourcefire 3D System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook and local electrical codes.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Sourcefire 3D System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

Current

The labeled current rating for each supply is: 10A maximum over the full range, per supply 5A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

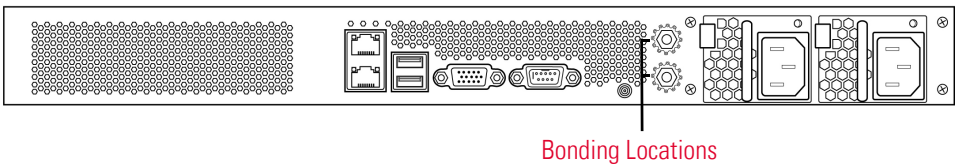
Grounding/Earthing Requirements

The Sourcefire 3D System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the chassis.



Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. See Current on page 241.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

3D8120/8130/8140 and 3D8250/8260/8270/8290

Devices included in this section are:

- 3D8120/8130/8140 (CHAS-1U-AC, CHAS-1U-DC, or CHAS-1U-AC/DC)
- 3D8250/8260/8270/8290 (CHAS-2U-AC, CHAS-2U-DC, or CHAS-2U-AC/DC)

These Sourcefire devices are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Sourcefire recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation on page 245 for circuit installation, voltage, current, and frequency range, and power cord information.
- See DC Installation on page 247 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.
- See Grounding/Earthing Requirements on page 249 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Sourcefire 3D System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook and local electrical codes.

WARNING! Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Sourcefire 3D System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 10A maximum over the full range, per supply 5A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16

AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

WARNING! Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Sourcefire 3D System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 20A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 20A, as stated on the label.

WARNING! Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN.
- -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

20A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320"). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay*. Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.

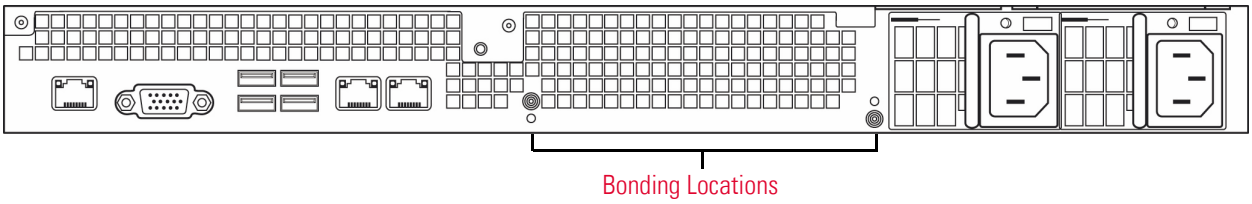
Grounding/Earthing Requirements

The Sourcefire 3D System must be grounded to the Common Bonding Network.

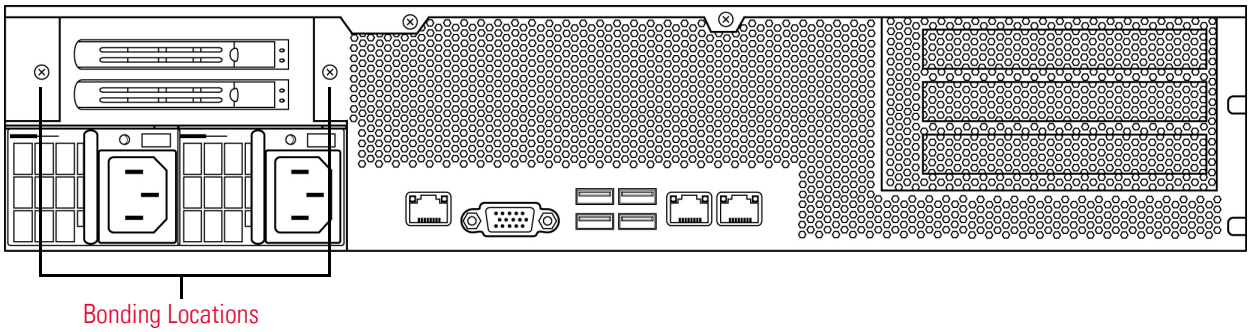
Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 1U chassis.



The following illustration indicates the bonding locations on the 2U chassis.



Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see Current on page 241. For DC currents, see DC Current on page 248.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

The ground wire should be sized to match the breaker for the circuit.

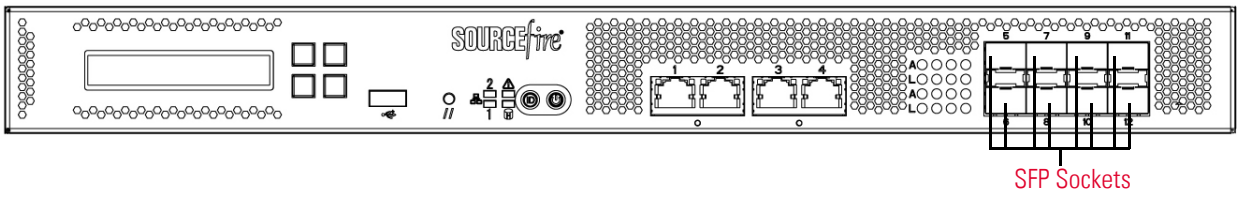
APPENDIX B
USING SFP TRANSCEIVERS ON A 3D7115 OR 3D7125

The following sections provide more information on using the small form-factor pluggable (SFP) sockets and transceivers in a 3D7115 and 3D7125:

3D7115 and 3D7125 SFP Sockets and Transceivers

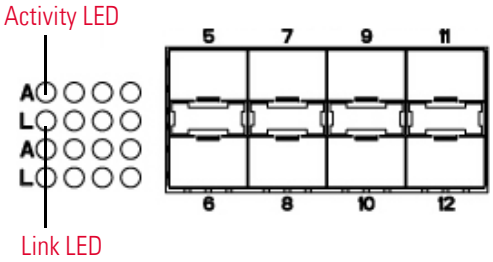
The 3D7115 and 3D7125 contain eight small form-factor pluggable (SFP) sockets and can house up to eight SFP transceivers.

3D7115 and 3D7125 Front View



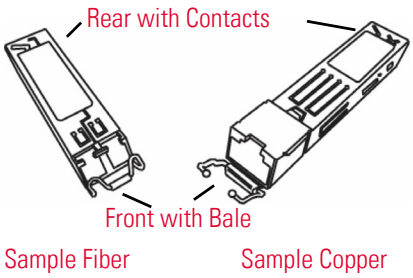
3D7115 and 3D7125 SFP Sockets

The eight SFP sockets are numbered from 5 through 12 in a vertical pattern, and oriented in a tab-to-center configuration (the upper row faces up and the lower row faces down).



The accompanying LEDs to the left of the sockets display information on activity and link for each interface. See 3D7115 and 3D7125 SFP Socket Activity/Link LEDs on page 167 for more information.

Sample SFP Transceivers



The 3D7115 and 3D7125 can support up to eight SFP transceivers in any combination of three formats:

- SFP-C-1: copper transceiver
- SFP-F-1-SR: short range fiber transceiver
- SFP-F-1-LR: long range fiber transceiver

Use only Sourcefire SFP transceivers in the 3D7115 and 3D7125. Non-Sourcefire SFP transceivers can jam in the socket and can cause permanent damage to the transceiver, the chassis, or both.

You can insert or remove transceivers while the device remains functioning. Refresh the user interface on the Defense Center to see the change in configuration.

SFP transceivers do not have bypass capability. Use these transceivers in a passive deployment or an inline deployment where you want your device to stop all traffic if the device fails or loses power (for example, virtual switches, virtual routers, and some access control policies).

For a passive deployment, you can use any combination of transceivers in up to eight sockets to monitor up to eight network segments. For an inline deployment, you can use any combination (copper, fiber, or mixed) of transceivers in vertically sequential sockets (5 and 6, 7 and 8, 9 and 10, or 11 and 12) to monitor up to four network segments.

Use the Defense Center that manages your device to configure the ports on the transceivers.

Inserting an SFP Transceiver

Use appropriate electrostatic discharge (ESD) procedures when inserting the transceiver. Avoid touching the contacts at the rear, and keep the contacts and ports free of dust and dirt.

WARNING! Do not force an SFP transceiver into a socket as this can jam the transceiver and can cause permanent damage to the transceiver, the chassis, or both.

To insert an SFP transceiver:

1. Taking care not to touch the contacts in the rear, use your fingers to grasp the sides of the bale and slide the rear of the transceiver into a socket on the chassis. Note that sockets on the upper row face up and sockets on the lower row face down.
2. Gently push the bale toward the transceiver to close the bale and engage the locking mechanism, securing the transceiver in place.

3. Follow the procedure in Installing a Sourcefire 3D System Appliance on page 57 to configure the port on the transceiver.

   Note that if you insert a transceiver into a device currently in operation, you must refresh the user interface on the Defense Center to view the change.

Removing an SFP Transceiver

Use appropriate electrostatic discharge (ESD) procedures when removing the transceiver. Avoid touching the contacts at the rear, and keep the contacts and ports free of dust and dirt.

To remove an SFP transceiver:

1. Disconnect all cables from the transceiver you want to remove from the device.
2. Using your fingers, gently pull the bale of the transceiver away from the chassis to disengage the connecting mechanism.

   For transceivers in the upper row, pull down. For transceivers in the lower row, lift up.
3. Using your fingers, grasp the sides of the bale and use the bale as a handle to gently pull the transceiver out of the chassis, taking care not to touch the contacts at the back of the transceiver.

APPENDIX C
INSERTING AND REMOVING 8000 SERIES MODULES

The 8000 Series appliances allow for modular flexibility in your deployment. Use the steps in this section to:

- insert a new module into an appliance
- remove or replace a preinstalled module on an appliance

The following sections describe how to insert, remove, or replace an 8000 Series module:

Module Slots on the 8000 Series Appliances

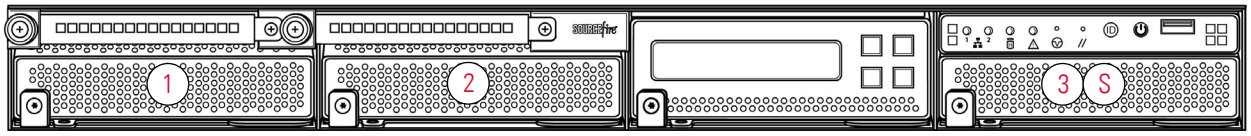
The 8000 Series appliances can use the modules in the following slots:

After you insert the modules into your appliance, see the following sections for more information on using the modules:

- For information on configuring the sensing interfaces, see Identifying the Sensing Interfaces on page 61.
- For information on using the stacking module, see Using Devices in a Stacked Configuration on page 74.

81xx Family

The 81xx Family appliances can use the modules in the following slots:



Slots 1-3: NetMods
Slot S: Stacking module

Stacking Configuration Considerations

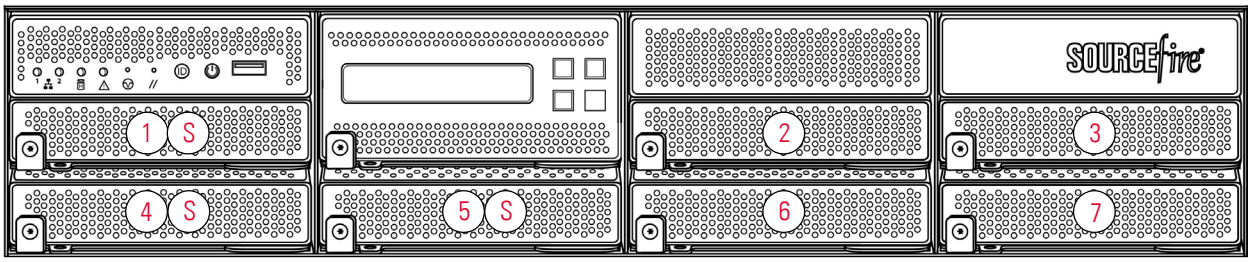
Configure the modules as follows for stacked devices:

- Install NetMods on the primary device only.
- Install one stacking module on the primary device and one stacking module on the secondary device.

82xx Family

The 82xx Family appliances can use the modules in the following slots:

82xx Family Primary Device



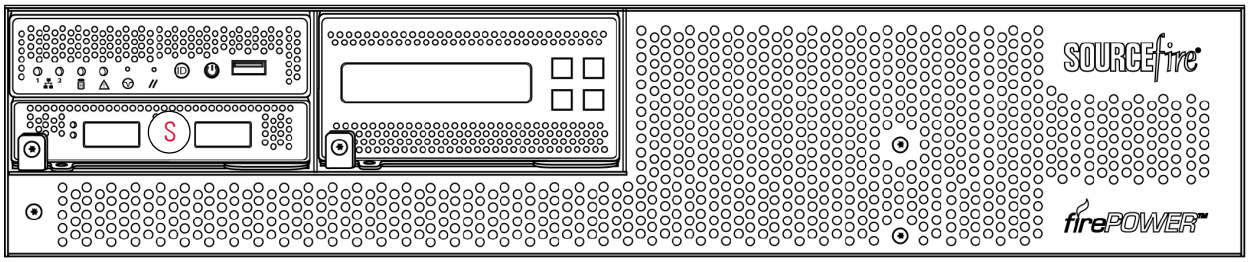
Slots 1-7: NetMods
Slot S: Stacking modules

Stacking Configuration Considerations

Configure the modules as follows for stacked devices:

- Install NetMods on the primary device only.
- Install one stacking module on the primary device for each stacked secondary device, and one stacking module on each secondary device.

82xx Family Secondary Device



Slot S: Stacking module

Included Items

Your module assembly kit includes a T8 Torx screwdriver and one or more of the following modules:

- quad-port 1000BASE-T copper configurable bypass NetMod. For more information, see Quad-Port 1000BASE-T Copper Configurable Bypass NetMod on page 186.
- quad-port 1000BASE-SX fiber configurable bypass NetMod. For more information, see Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod on page 187.
- dual-port 10GBASE (MMSR or SMLR) fiber configurable bypass NetMod. For more information, see Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod on page 188.
- dual-port 40GBASE-SR4 fiber configurable bypass NetMod. For more information, see Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod on page 191.

IMPORTANT! Use this dual-slot NetMod only on the 40G-capacity 3D8250. If you need to upgrade your 3D8250, see the *Sourcefire 8000 Series Device 40G Capacity Upgrade Guide*.

- quad-port 1000BASE-T copper non-bypass NetMod. For more information, see Quad-Port 1000BASE-T Copper Non-Bypass NetMod on page 193.

- quad-port 1000BASE-SX fiber non-bypass NetMod.quad-port 1000BASE-SX fiber non-bypass NetMod. For more information, see Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod on page 194.
- quad-port 10GBASE (MMSR or SMLR) fiber non-bypass NetMod. For more information, see Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod on page 195.

WARNING! The quad-port 10GBASE fiber non-bypass NetMod contains non-removable small form factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

- stacking module. For more information, see Stacking Module on page 197.

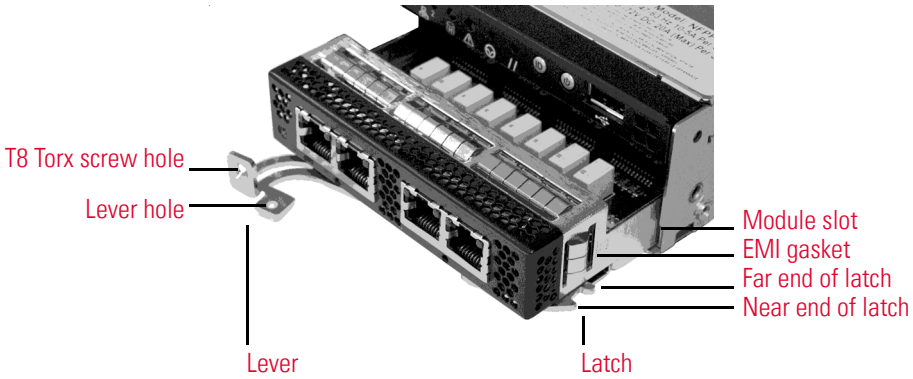
If you install a NetMod in an incompatible slot on your appliance or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface on the managing Defense Center when you attempt to configure the NetMod. Contact Sourcefire support for assistance.

IMPORTANT! Replacing a NetMod can alter the configuration of a fully configured Korean-certified (KCC mark) appliance. For more information, see the original configuration documentation for your appliance and Chassis and NetMod Designations on page 235.

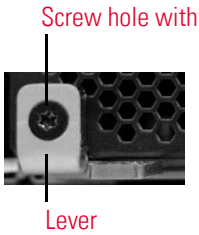
Identifying the Module Parts

All modules contain the same parts, regardless of sensing interface, speed, or size of the module.

Sample Module or Slot Cover (open)



Sample Module Lever (closed with screw in hole)



Before You Begin

Prepare to insert or remove your module using the following guidelines:

- Identify all appliance and module parts.
- Identify the slots where you want to install your NetMods.

> **TIP!** You can insert the NetMod into any available, compatible slot.

- Identify the correct slots for your stacking modules. See Using Devices in a Stacked Configuration on page 74.
  - 3D8140: slot 3
  - 3D8250/8260 primary slot: slot 5
  - 3D8270 primary slots: slots 5 and 1
  - 3D8290 primary slots: slots 5, 1, and 4
  - 3D82xx secondary: slot S
- Confirm that the EMI gaskets are in place.
- Unplug all power cords from the appliance.

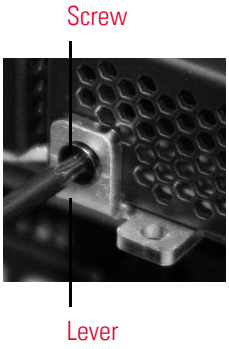
> **WARNING!** You **cannot** hot-swap modules. You must power down and unplug **both** power cords from the appliance before inserting or removing modules.

Removing a Module or Slot Cover

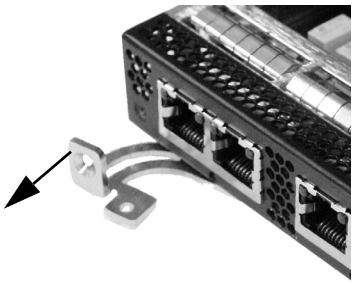
Use proper electrostatic discharge (ESD) practices such as wearing wrist straps and using an ESD work surface when handling the modules. Store unused modules in an ESD bag or box to prevent damage.

To remove a module or slot cover:

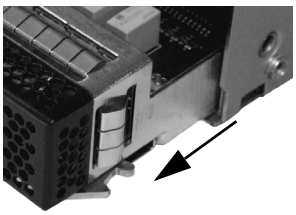
1. Remove and reserve the T8 Torx screw from the lever of the module using the included screwdriver.



2. Pull the lever away from the module to release the latch.



3. Slide the module out of the slot.

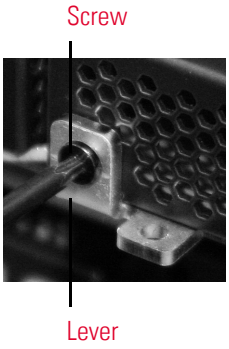


Inserting a Module or Slot Cover

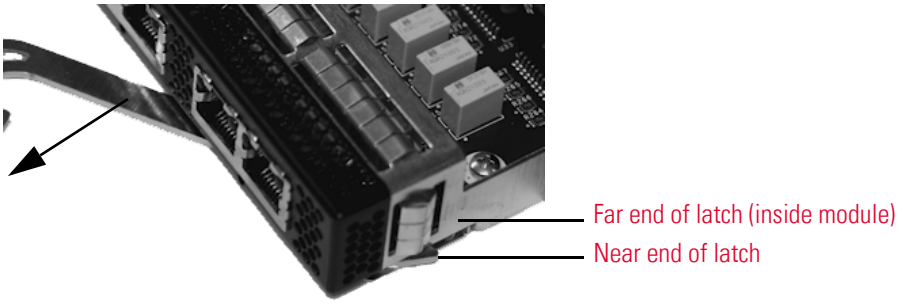
Remove the existing module or slot cover to prepare the slot for a new module. See Removing a Module or Slot Cover on page 259 for more information.

To insert a module or slot cover:

1. Remove and reserve the T8 Torx screw from the lever of the module using the included screwdriver.

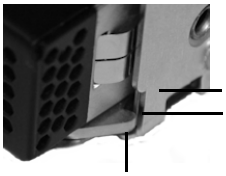


2. Pull the lever away from the module to open the latch. The near end of the latch is visible. The far end of the latch is inside the module.

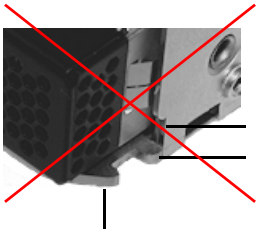


3. Insert the module into the slot until the far end of the latch is inside the slot and the near end of the latch touches the outside of the module slot.

Correct module alignment



Incorrect module alignment

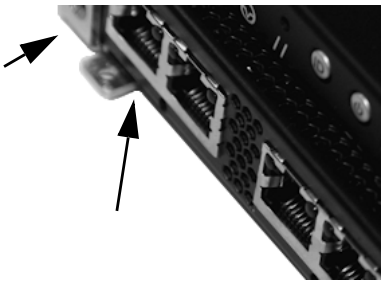


4. Push the lever toward the module so that the latch engages and pulls the module into the slot.

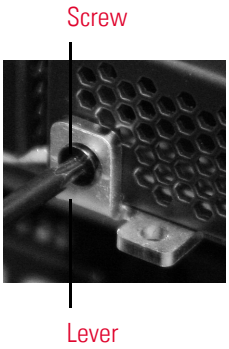
WARNING! Do **not** use excessive force. If the latch does not engage, remove and realign the module, and then try again.

5. Press firmly on the screw hole to push the lever fully against the module to secure the latch.

   The lever is fully against the module, and the module is flush with the chassis.



6. Insert and tighten the reserved T8 Torx screw into the lever.



Glossary

7000 Series	A group of Series 3 Sourcefire managed devices. The devices in this series include the 70xx Family (the 3D7010, 3D7020, and 3D7030 models) and the 71xx Family (the 3D7110, 3D7115, 3D7120, and 3D7125 models).
8000 Series	A group of Series 3 Sourcefire managed devices. The devices in this series include the 81xx Family (the 3D8120/8130/8140 models) and the 82xx Family (the 3D8250/8260/8270/8290 models). 8000 Series devices are generally more powerful than the 7000 Series devices.
access control	A feature of the Sourcefire 3D System that allows you to specify, inspect, and log the traffic that can traverse your network. Access control includes the intrusion detection and prevention, file control, and advanced malware protection features, and also determines the traffic you can inspect with the discovery feature.
access control policy	A policy that you apply to managed devices to perform access control on the network traffic monitored by those devices. An access control policy may include multiple access control rules; it also specifies a default action, which determines the handling and logging of traffic that does not meet the criteria of any of those rules. An access control policy can also specify HTTP response page, Security Intelligence, and other advanced settings.
access control rule	A set of conditions the Sourcefire 3D System uses to examine your monitored network traffic and which allows you to achieve granular access control. Access control rules, which populate an access control policy, may perform simple IP address matching, or may characterize complex connections involving different

	users, applications, ports, and URLs. The access control rule action determines how the system handles traffic that meets the rule's conditions. Other rule settings determine how (and whether) the connection is logged, and whether an intrusion policy or file policy inspects matching traffic.
access list	A list of IP addresses, configured in the system policy, that represents the hosts that can access an appliance. By default, anyone can access the web interface of an appliance using port 443 (HTTPS), as well as the command line using port 22 (SSH). You can also add SNMP access using port 161.
advanced malware protection	Abbreviated AMP, the Sourcefire 3D System's network-based malware detection and malware cloud lookup feature. Compare this functionality with FireAMP, Sourcefire's endpoint-based AMP tool that requires a FireAMP subscription.
advanced setting	A preprocessor or other intrusion policy feature that requires specific expertise to configure. Advanced settings typically require little or no modification and are not common to every deployment.
alert	A notification that the system has generated a specific event. You can alert based on intrusion events (including their impact flags), discovery events, malware events, correlation policy violations, health status changes, and connections logged by specific access control rules. In most cases, you can alert via email, syslog, or SNMP trap.
appliance	A Defense Center or managed device. An appliance can be physical or virtual.
application	A detected network asset, communications method, or HTTP content against which you can write access control rules. The system detects three types of application: application protocol, client application, and web application.
application control	A feature that, as part of access control, allows you to specify which application traffic can traverse your network.
application protocol	A type of application that represents application protocol traffic detected during communications between server and client applications on hosts; for example, SSH or HTTP.
apply	The action you take to have a policy, or changes to that policy, take effect. You apply most policies from the Defense Center to its managed devices; however, you activate and deactivate correlation policies because they do not involve changes to the configuration of managed devices.
bypass mode	A characteristic of an inline set that allows traffic to continue flowing if the sensing interfaces in the set fail for any reason.
CLI	See command line interface.

client	Also called a client application, an application that runs on one host and relies on another host (a server) to perform some operation. For example, email clients allow you to send and receive email. When the system detects that a user on a host is using a specific client to access another host, it reports that information in the host profile and network map, including the name and version (if available) of the client.
client application	See client.
clustering	A feature that allows you to achieve redundancy of networking functionality and configuration data between two peer Series 3 devices or stacks. Clustering provides a single logical system for policy applies, system updates, and registration. Compare with high availability, which allows you to configure redundant Defense Centers.
command line interface	A restricted text-based interface on Series 3 and virtual devices. The commands that CLI users can run depend on the users' assigned level of access.
configurable bypass	A characteristic of an inline set that allows you to configure bypass mode.
connection	A monitored session between two hosts. You can log connections detected by managed devices in the access control policy; you configure NetMod connection logging in the network discovery policy.
Context Explorer	A page that displays detailed, interactive graphical information about your monitored network, using intrusion, connection, file, geolocation, malware, and discovery policy. Distinct sections present information in the form of vivid line, bar, pie, and donut graphs, accompanied by detailed lists. You can easily create and apply custom filters to fine-tune your analysis, and you can examine data sections in more detail by clicking or hovering your cursor over graph areas. Compared with a dashboard, which is highly customizable, compartmentalized, and updates in real time, the Context Explorer is manually updated, designed to provide broader context for its data, and has a single, consistent layout designed for active user exploration.
context menu	A pop-up menu, available on many of the pages in the web interface, that you can use as a shortcut for accessing other features in the Sourcefire 3D System. The contents of the menu depend on several factors, including the page you are viewing, the specific data you are investigating, and your user role. Context menu options include links to intrusion rule, event, and host information; various intrusion rule settings, quick links to the Context Explorer; options to add a host to the Security Intelligence global blacklist or global whitelist by its IPS address; and options to add a file to the global whitelist by its SHA-256 hash value.
Control license	A license that allows you to implement user control and application control by adding user and application conditions to access control rules. It also allows you to configure your managed devices to perform switching and routing (including DHCP relay and NAT), as well as clustering managed devices.

correlation	A feature you can use to build a correlation policy that responds in real time to threats on your network. The remediation component of correlation provides a flexible API that allows you to create and upload your own custom remediation modules to respond to policy violations.
custom user role	A user role with specialized access privileges. Custom user roles may have any set of menu-based and system permissions, and may be completely original or based on a predefined user role.
dashboard	A display that provides at-a-glance views of current system status, including data about the events collected and generated by the system. To augment the dashboards delivered with the system, you can create multiple custom dashboards, populated with the dashboard widgets you choose. Compare with the Context Explorer, which offers a broad, brief, and colorful picture of how your monitored network looks and acts.
dashboard widget	A small, self-contained dashboard component that provides insight into an aspect of the Sourcefire 3D System.
database access	A feature that allows read-only access to the Defense Center database by a third-party client.
decoder	A component of intrusion detection and prevention that places sniffed packets into a format that can be understood by a preprocessor.
default action	As part of an access control policy, determines how to handle traffic that does not meet the conditions of any rule in the policy. When you apply an access control policy that does not contain any access control rules or Security Intelligence settings, the default policy action determines how non-fast-pathed traffic on your network is handled. You can set the default action to block or trust traffic without further inspection, or inspect it with a network discovery policy or intrusion policy.
Defense Center	A central management point that allows you to manage devices and automatically aggregate and correlate the events they generate.
device	A fault-tolerant, purpose-built appliance available in a range of throughputs. Depending on the licensed capabilities you enable on your devices, you can use them to passively monitor traffic to build a comprehensive map of your network assets, application traffic, and user activity, perform intrusion detection and prevention, perform access control, and configure switching and routing. You must manage devices with a Defense Center.
device clustering	See clustering.
device stacking	See stacking.
discovery	A component of the Sourcefire 3D System that uses managed devices to monitor your network and provide you with a complete, persistent view of your network.

Network discovery determines the number and types of hosts (including network devices and mobile devices) on your network, as well as information about the operating systems, active applications, and open ports on those hosts. You can also configure Sourcefire managed devices to monitor user activity on your network, which allows you to identify the source of policy breaches, attacks, or network vulnerabilities.

discovery policy See network discovery policy.

endpoint A computer or mobile device where your users install a FireAMP Connector as part of your organization's advanced malware protection strategy.

eStreamer A component of the Sourcefire 3D System that allows you to stream event data from a Defense Center or managed device to external client applications.

event A collection of details about a specific occurrence that you can view in the event viewer, using workflows. Events may represent attacks on your network, changes in your detected network assets, violations of your organization's security and network use policies, and so on. The system also generates events that contain information about the changing health status of appliances, your use of the web interface, rule updates, and launched remediations. Finally, the system presents certain other information as events, even though these "events" do not represent particular occurrences. For example, you can use the event viewer to view detailed information about detected hosts, applications, and their vulnerabilities.

event viewer A component of the system that allows you to view and manipulate events. The event viewer uses workflows to present a broad, then a more focused event view that contains only the events of interest to you. You can constrain the events in an event view by drilling down through the workflow, or by using a search.

Event Streamer See eStreamer.

fast-path rule A rule that you configure at a device's hardware level, using a limited set of criteria, to allow traffic that does not need to be analyzed to bypass processing.

feed See Security Intelligence feed.

file control A feature that, as part of access control, allows you to specify and log the types of files that can traverse your network.

file policy A policy that the system uses to perform file control and advanced malware protection. Populated by file rules, a file policy is invoked by an access control rule within an access control policy.

file trajectory See network file trajectory.

file type A specific type of file format, such as PDF, EXE, or MP3.

FireAMP	Sourcefire's enterprise-class, endpoint-based, advanced malware analysis and protection solution that discovers, understands, and blocks malware outbreaks, persistent threats, and targeted attacks. If your organization has a FireAMP subscription, individual users install lightweight FireAMP Connectors on endpoints (computers, mobile devices), which then communicate with the Sourcefire cloud. This allows you to quickly identify and quarantine malware, as well as identify outbreaks when they occur, track their trajectory, understand their effects, and learn how to successfully recover. You can also use the FireAMP portal to create custom protections, block execution of certain applications, and create custom whitelists. Compare with network-based advanced malware protection.
FireAMP Connector	A lightweight agent that users in a subscription-based FireAMP deployment install on endpoints, such as computers and mobile devices. Connectors communicate with the Sourcefire cloud, exchanging information that allow you to quickly identify and quarantine malware throughout your organization.
FireAMP portal	The website, http://amp.sourcefire.com/, where you can configure your organization's subscription-based FireAMP deployment.
FireAMP subscription	A separately purchased subscription that allows your organization to use FireAMP as an advanced malware protection (AMP) solution. Compare with a Malware license, which you enable on managed devices to perform network-based AMP.
FireSIGHT license	The default license on the Defense Center, which allows you to perform host, application, and user discovery. The FireSIGHT license also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as the number of access-controlled users you can use in access control rules to perform user control.
GeoDB	See geolocation database.
geolocation	A feature that provides data on the geographical source of routable IP addresses detected in traffic on your monitored network including connection type, internet service provider, and so on. You can see geolocation information which is stored in the geolocation database, in connection events, intrusion events, file events, and malware events, as well as in host profiles.
geolocation database	Also called the GeoDB, a regularly updated database of known geolocation data associated with routable IP addresses.
health module	A test of a particular performance aspect, such as CPU usage or available disk space, of the appliances in your deployment. Health modules, which you enable in a health policy, generate health events when the performance aspects they monitor reach a certain level.

health monitor	A feature that continuously monitors the performance of the appliances in your deployment. The health monitor uses health modules within an applied health policy to test the appliances.
health policy	The criteria used when checking the health of an appliance in your deployment. Health policies use health modules to indicate whether your Sourcefire 3D System hardware and software are working correctly. You can use the default health policy or create your own.
high availability	A feature that allows you to configure redundant physical Defense Centers to manage groups of devices. Event data streams from managed devices to both Defense Centers and most configuration elements are maintained on both Defense Centers. If your primary Defense Center fails, you can monitor your network without interruption using the secondary Defense Center. Compare with clustering, which allows you to designate redundant devices.
host	A device that is connected to a network and has a unique IP address. To the Sourcefire 3D System, a host is any identified host that is not categorized as a mobile device, bridge, router, NAT device, or logical interface.
host input	A feature that allows you to import data from third-party sources using scripts or command-line files to augment the information in the network map. The web interface also provides some host input functionality; you can modify operating system or application protocol identities, validate or invalidate vulnerabilities, and delete various items from the network map, including clients and server ports.
hybrid interface	A logical interface on a managed device that allows the system to bridge traffic between a virtual router and a virtual switch.
import	A method that you can use to transfer various configurations from appliance to appliance. You can import configurations that you previously exported from another appliance of the same type.
inline deployment	A deployment of the Sourcefire 3D System where your managed devices are placed inline on a network. In this configuration, devices can affect network traffic flow using switching, routing, access control, and intrusion detection and prevention.
inline interface	A sensing interface configured to handle traffic in an inline deployment. You must add inline interfaces to inline sets in pairs.
inline set	One or more pairs of inline interfaces.
intrusion	A security breach, attack, or exploit that occurs on your network.
intrusion detection and prevention	The monitoring of your network traffic for security policy violations, and, in inline deployments, the ability to block or alter malicious traffic. In the Sourcefire 3D

	System, you perform intrusion detection and prevention when you associate an intrusion policy with an access control rule or default action.
intrusion event	An event that records an intrusion policy violation. Intrusion event data includes the date, time, and the type of exploit, as well as other contextual information about the attack and its target.
intrusion policy	A variety of components that you can configure to inspect your network traffic for intrusions and security policy violations. These components include intrusion rules that inspect the protocol header values, payload content, and certain packet size characteristics; variables commonly used in intrusion rules; a FireSIGHT recommended rules configuration; advanced settings such as preprocessors and other detection and performance features; and preprocessor rules that allow you to generate events for associated preprocessor options. When your network traffic meets the conditions in an access control rule, you can inspect that traffic with an intrusion policy; you can also associate an intrusion policy with the default action.
intrusion rule	A set of keywords and arguments that, when applied to monitored network traffic, identify potential intrusions, security policy violations, and security breaches. The system compares packets against rule conditions. If the packet data matches the conditions, the rule triggers and generates an intrusion event. Intrusion rules include drop rules and pass rules.
layer	A complete set of intrusion rule, preprocessor rule, and advanced setting configurations within an intrusion policy. You can add custom user layers to the built-in layer or layers in your policy. A setting in a higher layer in an intrusion policy overrides a setting in a lower layer.
LDAP authentication	A form of external authentication that verifies user credentials by comparing them to a Lightweight Directory Access Protocol (LDAP) directory stored on an LDAP directory server.
Lights-Out-Management (LOM)	A Series 3 feature that allows you to use an out-of-band Serial over LAN (SOL) management connection to remotely monitor or manage appliances without logging into the web interface of the appliance. You can perform limited tasks, such as viewing the chassis serial number or monitoring such conditions as fan speed and temperature.
link state propagation	An option for inline sets in bypass mode that automatically brings down the second interface in a pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up also. In other words, if the link state of a paired interface changes, the link state of the other interface changes automatically to match it.
list	See Security Intelligence list.

logical interface	A virtual subinterface that you define to handle traffic with specific VLAN tags as the tagged traffic passes through a physical interface.
malware blocking	A component of Sourcefire's network-based advanced malware protection (AMP) solution. After malware detection yields a malware disposition for a detected file, you can either block the file or allows its upload or download. Compare this functionality with FireAMP, Sourcefire's endpoint-based AMP tool that requires a FireAMP subscription.
malware cloud lookup	A process by which the Defense Center communicates with the Sourcefire cloud to determine the malware disposition of a file detected in network traffic, based on the file's SHA-256 hash value.
malware detection	A component of Sourcefire's network-based advanced malware protection (AMP) solution. File policies applied to managed devices as part of your overall access control configuration inspect network traffic. The Defense Center then performs malware cloud lookups for specific detected file types, and generates events that alert you to the files' malware dispositions. AMP malware blocking follows and either blocks the file or allows its upload or download. Compare this functionality with FireAMP, Sourcefire's endpoint-based AMP tool that requires a FireAMP subscription.
malware event	An event generated by one of Sourcefire's advanced malware protection solutions. Network-based malware events are generated when the Sourcefire cloud returns a malware disposition for a file detected in network traffic; retrospective malware events are generated when that disposition changes. Compare with endpoint-based malware events, which are generated when a deployed FireAMP Connector detects a threat, blocks malware execution, or quarantines or fails to quarantine malware.
Malware license	A license that allows you to perform advanced malware protection (AMP) in network traffic. Using a file policy, you can configure the system to perform malware cloud lookups on specific file types detected by managed devices. Compare with FireAMP subscription.
malware protection	See advanced malware protection.
managed device	See device.
management interface	The network interface that you use to administer a Sourcefire 3D System appliance. In most deployments, the management interface is connected to an internal protected network. Compare with sensing interface.
mobile device	In the Sourcefire 3D System, a host identified by the discovery feature as a mobile, handheld device (such as a mobile phone or tablet). The system can often detect whether a mobile device is jailbroken.

monitor	In an access control policy, a way to log traffic that matches a Security Intelligence blacklist or access control rule, but allows the system to continue to evaluate the traffic rather than immediately allowing or blocking it.
NAT	Network address translation, a feature most commonly used to share a single internet connection among multiple hosts on a private network. Using discovery, the system can identify network devices as logical interfaces. In addition, in a Layer 3 deployment of the Sourcefire 3D System, you can configure routing with NAT using a NAT policy.
NAT policy	A policy that uses NAT rules to perform routing with NAT.
NetMod	A module that you install in the chassis of a managed device that contains the sensing interfaces for that device.
network device	In the Sourcefire 3D System, a host identified as a bridge, router, NAT device, or logical interface.
network discovery	See discovery.
network discovery policy	A policy that specifies the kinds of discovery policy (including host, user, and application data) the system collects for specific network segments, including networks monitored by NetMod-enabled devices. The network discovery policy also manages import resolution preferences and active detection source priorities.
network file trajectory	A visual representation of a file's path as hosts transfer it across your network. For any file with an associated SHA-256 hash value, the trajectory map displays the IP addresses of all hosts that have transferred the file, the time the file was detected, the file's malware disposition, associated file events and malware events, and so on.
network map	A detailed representation of your network. The network map allows you to view your network topology in terms of the hosts, mobile devices, and network devices running on your network, as well as their associated host attributes, application protocols, and vulnerabilities.
non-bypass mode	A characteristic of an inline set that blocks traffic if the sensing interfaces in the set fail for any reason.
passive detection	The collection of discovery policy through analysis of traffic passively collected by managed devices. Compare with active detection.
passive interface	A sensing interface configured to analyze traffic in a passive deployment.
physical interface	An interface that represents a physical port on a NetMod.

policy	A mechanism for applying settings, most often to an appliance. See access control policy, correlation policy, file policy, health policy, intrusion policy, network discovery policy, and system policy.
preprocessor	A feature that normalizes traffic inspected by an intrusion policy and that helps identify network layer and transport layer protocol anomalies by identifying inappropriate header options, defragmenting IP datagrams, providing TCP stateful inspection and stream reassembly, and validating checksums. Preprocessors can also render specific types of packet data in a format that the system can analyze; these preprocessors are called data normalization preprocessors, or application layer protocol preprocessors. Normalizing application layer protocol encoding allows the system to effectively apply the same content-related intrusion rules to packets whose data is represented differently and obtain meaningful results. Preprocessors generate preprocessor rules whenever packets trigger preprocessor options that you configure.
preprocessor rule	An intrusion rule associated with a preprocessor or with the portscan flow detector. You must enable preprocessor rules if you want them to generate events. Preprocessor rules have a preprocessor-specific GID (generator ID).
protected network	Your organization's internal network that is protected from users of other networks by a device such as a firewall. Many of the intrusion rules delivered with the Sourcefire 3D System use variables to define the protected network and the unprotected (or outside) network.
Protection license	A license for Series 3 and virtual devices that allows you to perform intrusion detection and prevention, file control, and Security Intelligence filtering. Without a license, Series 2 devices automatically have Protection capabilities, with the exception of Security Intelligence.
RADIUS authentication	Remote Authentication Dial In User Service, a service used to authenticate, authorize, and account for user access to network resources. You can create an external authentication object to allow Sourcefire 3D System users to authenticate through a RADIUS server.
remediation	An action that mitigates potential attacks on your system. You can configure remediations and, within a correlation policy, associate them with correlation rules and compliance white lists so that when they trigger, the Defense Center launches the remediation. This can not only automatically mitigate attacks when you are not immediately available to address them, but can also ensure that your system remains compliant with your organization's security policy. The Defense Center ships with predefined remediation modules, and you also can use a flexible API to create custom remediations.
reputation (IP address)	See Security Intelligence.

routed interface	An interface that routes traffic in a Layer 3 deployment. You can set up physical routed interfaces for handling untagged VLAN traffic, and logical routed interfaces for handling traffic with designated VLAN tags. You can also add static Address Resolution Protocol (ARP) entries to routed interfaces.
router	A network device, located at a gateway, that forwards packets between networks. Using network discovery, the system can identify routers. In addition, you can configure managed devices as virtual routers that route traffic between two or more interfaces.
rule	A construct, usually within a policy, that provides criteria against which network traffic is examined.
rule action	A setting that determines how the system handles network traffic that meets the conditions of a rule. See access control rule and file rule action.
rule state	Whether an intrusion rule is enabled (set to Generate Events or Drop and Generate Events), or disabled (set to Disable) within an intrusion policy. If you enable a rule, it is used to evaluate your network traffic; if you disable a rule, it is not used.
rule update	An as-needed intrusion rule update that contains new and updated standard text rules, shared object rules, and preprocessor rules. A rule update may also delete rules, modify default intrusion policy settings, and add or delete system variables and rule categories.
scheduled task	An administrative task that you can schedule to run once or at recurring intervals.
Security Intelligence	A feature that allows you to specify the traffic that can traverse your network, per access control policy, based on the source or destination IP address. This is especially useful if you want to blacklist—deny traffic to and from—specific IP addresses, before the traffic is subjected to analysis by access control rules. Optionally, you can use a monitor setting for Security Intelligence filtering, which allows the system to analyze connections that would have been blacklisted, but also logs the match to the blacklist.
Security Intelligence feed	One of the types of Security Intelligence objects, a dynamic collection of IP addresses that the system downloads on a regular basis, at an interval you configure. Because feeds are regularly updated, using them ensures that the system uses up-to-date information to filter your network traffic using the Security Intelligence feature. See also Sourcefire Intelligence Feed.
Security Intelligence list	A simple static collection of IP addresses that you manually upload to the Defense Center as a Security Intelligence object. Use lists to augment and fine-tune Security Intelligence feeds as well as the global blacklist and global whitelist.

security policy	An organization's guidelines for protecting its network. For example, your security policy might forbid the use of wireless access points. A security policy may also include an acceptable use policy (AUP), which provides employees with guidelines of how they may use their organization's systems.
security policy violation	A security breach, attack, exploit, or other misuse of your network.
security zone	A grouping of one or more inline, passive, switched, or routed interfaces that you can use to manage and classify traffic flow in various policies and configurations. The interfaces in a single zone may span multiple devices; you can also configure multiple security zones on a single device. You must assign each interface you configure to a security zone before it can handle traffic, and each interface can belong to only one security zone.
sensing interface	A network interface on a device that you use to monitor a network segment. Compare with management interface.
Series 2	The second series of Sourcefire appliance models. Because of resource, architecture, and licensing limitations, Series 2 appliances support a restricted set of Sourcefire 3D System features. Series 2 devices include the 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500, and 3D9900. Series 2 Defense Centers include the DC500, DC1000, and DC3000.
Series 3	The third series of Sourcefire appliance models. Series 3 appliances include 7000 Series and 8000 Series devices, as well as the DC750, DC1500, and DC3500 Defense Centers.
server	The server application (compare with client application) installed on a host, identified by application protocol traffic.
SFP module	A small form-factor pluggable transceiver that is inserted into a network module on a 71xx Family device. Sensing interfaces on SFP modules do not allow configurable bypass.
Sourcefire cloud	Sometimes called *cloud services*, a Sourcefire-hosted external server where the Defense Center can obtain up-to-date, relevant information including malware, Security Intelligence, and URL filtering data. See also malware cloud lookup.
Sourcefire Intelligence Feed	A collection of regularly updated lists of IP addresses determined by the Sourcefire VRT to have a poor reputation. Each list in the feed represents a specific category: open relays, known attackers, bogus IP addresses (bogon), and so on. In an access control policy, you can blacklist any or all of the categories using Security Intelligence. Because the intelligence feed is regularly updated, using it ensures that the system uses up-to-date information to filter your network traffic.
Sourcefire VRT	Sourcefire's Vulnerability Research Team.

stack	Two to four connected devices that share detection resources.
stacking	A feature that allows you to increase the amount of traffic inspected on a network segment by connecting two to four physical devices in a stacked configuration. When you establish a stacked configuration, you combine the resources of each stacked device into a single, shared configuration.
switch	A network device that acts as a multiport bridge. Using network discovery, the system identifies switches as bridges. In addition, you can configure managed devices as virtual switches, performing packet switching between two or more networks.
switched interface	An interface that you want to use to switch traffic in a Layer 2 deployment. You can set up physical switched interfaces for handling untagged VLAN traffic, and logical switched interfaces for handling traffic with designated VLAN tags.
system policy	Settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Use the Defense Center to apply a system policy to itself and its managed devices.
table view	A type of workflow page that displays event information, with one column for each of the fields in the database table. When performing event analysis, you can use drill-down pages to constrain the events you want to investigate before moving to the table view that shows you the details about the events you are interested in. The table view is often the next-to-last page in workflows delivered with the system.
tap mode	An advanced inline set option available on 3D9900 and Series 3 devices where a copy of each packet is analyzed and the network traffic flow is undisturbed instead of passing through the device. Because you are working with copies of packets rather than the packets themselves, the device cannot affect the packet stream even if you configure access control and intrusion policies to drop, modify, or block traffic.
task queue	A queue of jobs that the appliance needs to perform. When you apply a policy, install software updates, and perform other long-running jobs, the jobs are queued and their status reported on the Task Status page. The Task Status page provides a detailed list of jobs and refreshes every ten seconds to update their status.
transparent inline mode	An advanced inline set option that allows a device to act as a "bump in the wire" and to forward all the network traffic it sees, regardless of its source and destination.
URL category	A general classification for a URL, such as malware or social networking.
URL filtering	A feature that allows you to write access control rules that determine the traffic that can traverse your network based on URLs requested by monitored hosts,

	correlated with URL category and URL reputation information about those URLs, which is obtained from the Sourcefire cloud by the Defense Center. You can also achieve more granular, custom control over web traffic by specifying individual URLs or groups of URLs to allow or block.
URL Filtering license	A license that allows you to perform URL filtering based on URL category and URL reputation information. URL Filtering licenses may expire.
user	A user whose network activity has been detected by a managed device or User Agent.
user activity	An event generated when the system detects a user login (optionally, including some failed login attempts) or the addition or deletion of a user record from the Defense Center database.
User Agent	An agent you install on a server to monitor users as they log into the network or when they authenticate against Active Directory credentials for any other reason. User activity for access-controlled users is used for access control only when reported by a User Agent.
user awareness	A feature that allows your organization to correlate threat, endpoint, and network intelligence with user identity information, and that allows you to perform user control.
user control	A feature that, as part of access control, allows you to specify and log the user-associated traffic that can enter your network, exit it, or cross from within without leaving it.
user role	The level of access granted to a user of the Sourcefire 3D System. For example, you can grant different access privileges to the web interface for event analysts, the administrator managing the Sourcefire 3D System, users accessing the Defense Center database using third-party tools, and so on. You can also create custom roles with specialized access privileges.
UTC time	Coordinated Universal Time. Also known as Greenwich Mean Time (GMT), UTC is the standard time common to every place in the world. The Sourcefire 3D System uses UTC, although you can set the local time using the Time Zone feature.
VDB	See vulnerability database.
virtual Defense Center	A Defense Center that you can deploy on your own equipment in a virtual hosting environment.
virtual device	A managed device that you can deploy on your own equipment in a virtual hosting environment. You cannot configure a virtual device as a virtual switch or virtual router.

virtual router	A group of routed interfaces that route Layer 3 traffic. In a Layer 3 deployment, you can configure virtual routers to route packets by making packet forwarding decisions according to the destination IP address. You can define static routes, configure Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) dynamic routing protocols, as well as implement Network Address Translation (NAT).
virtual switch	A group of switched interfaces that process inbound and outbound traffic through your network. In a Layer 2 deployment, you can configure virtual switches on managed devices to operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access and control (MAC) address from a host to determine where to send packets.
VLAN	Virtual local area network. VLANs map hosts not by geographic location, but by some other criterion, such as by department or primary use. A monitored host's host profile shows any VLAN information associated with the host. VLAN information is also included in intrusion events, as the innermost VLAN tag in the packet that triggered the event. You can filter intrusion policies by VLAN and target compliance white lists by VLAN. In Layer 2 and Layer 3 deployments, you can configure virtual switches and virtual routers on managed devices to appropriately handle VLAN-tagged traffic.
VPN	A feature that allows you to build secure VPN tunnels among the virtual routers on Sourcefire managed devices, or from managed devices to remote devices or other third-party VPN endpoints.
VPN license	A license that allows you to build secure VPN tunnels among the virtual routers on Sourcefire managed devices, or from managed devices to remote devices or other third-party VPN endpoints.
VRT	See Sourcefire VRT.
vulnerability	A description of a specific compromise to which a host is susceptible. The Defense Center provides information on the vulnerabilities to which each of your hosts is vulnerable in the hosts' host profiles. In addition, you can use the vulnerabilities network map to obtain an overall view of the vulnerabilities that the system has detected on your entire monitored network. If you deem a host or hosts no longer vulnerable to a specific compromise, you can deactivate, or mark as invalid, a specific vulnerability.
vulnerability database	Also called the VDB, a database of known vulnerabilities to which hosts may be susceptible. The system correlates the operating system, application protocols, and clients detected on each host with the VDB to help you determine whether a particular host increases your risk of network compromise. VDB updates may contain new and updated vulnerabilities, as well as new and updated application detectors.

web application	A type of application that represents the content of, or requested URL for, HTTP traffic.
widget	See dashboard widget.
zone	See security zone.