

QUICK START GUIDE 7000 SERIES DEVICES

Thank you for choosing Sourcefire!

Before installing this device, download and follow the instructions in the Sourcefire Support Welcome Kit (<https://support.sourcefire.com>) to get started with Sourcefire Support, and to set up your Customer Center account.

Included items:

- one of the following Sourcefire 7000 Series models:
 - Sourcefire 3D7010/7020/7030
 - Sourcefire 3D7110/7120
 - Sourcefire 3D7115/7125
 - Sourcefire AMP7150

Each model group (3D7010/7020/7030, 3D7110/7120, 3D7115/7125, and AMP7150) has identical chassis. To confirm which model you have, see your packing list.

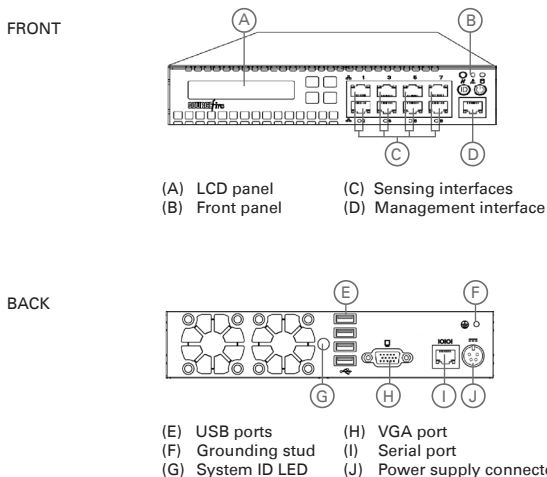
- two power cords (3D7010/7020/7030 only: one power cord)
- two straight-through Cat 5e Ethernet cables
- rack-mounting kit

Required items:

- flathead and Phillips screwdrivers for the rack-mounting kit
- 3D7010/7020/7030 only: chassis tray, available separately
- 3D7115/7125, AMP7150 only: small form-factor pluggable (SFP) transceivers, available separately (optional)

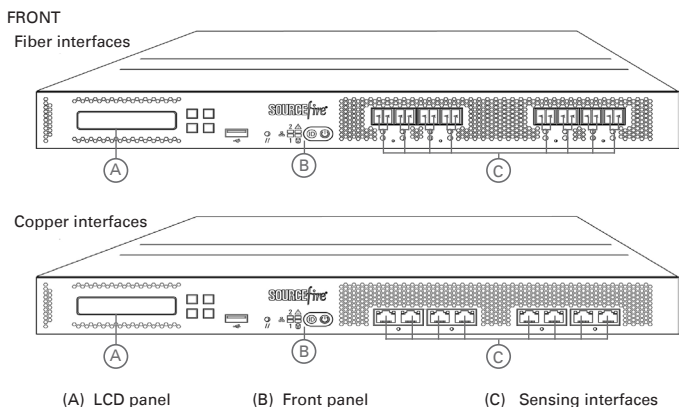
3D7010/7020/7030

(Chassis: CHRY-1U-AC)

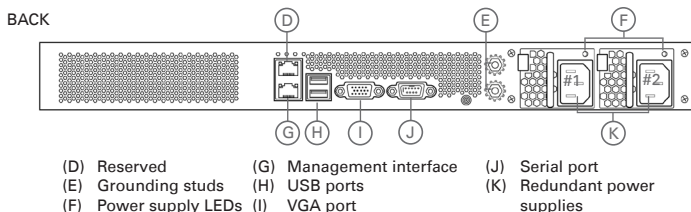


3D7110/7120

(Chassis: GERY-1U-8-C-AC / GERY-1U-8-FM-AC)

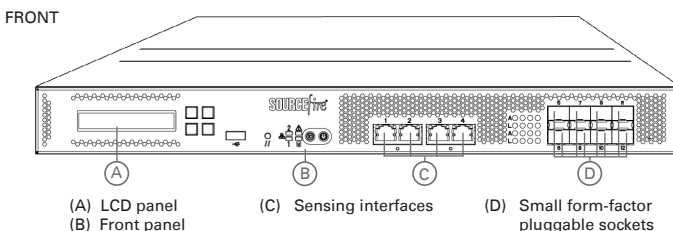


3D7110/7120



3D7115/7125, AMP7150

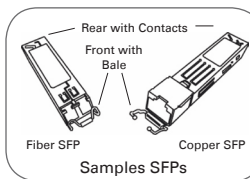
(Chassis: GERY-1U-4C8S-AC)



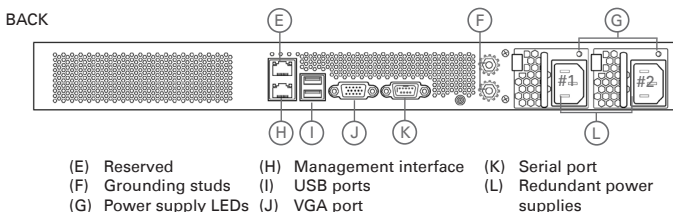
SMALL FORM-FACTOR PLUGGABLE TRANSCEIVERS

The 3D7115/7125 and AMP7150 support only Sourcefire SFP transceivers:

- SFP-F-1-SX
- SFP-F-1-LX
- SFP-C-1



3D7115/7125, AMP7150



Deploying the Device

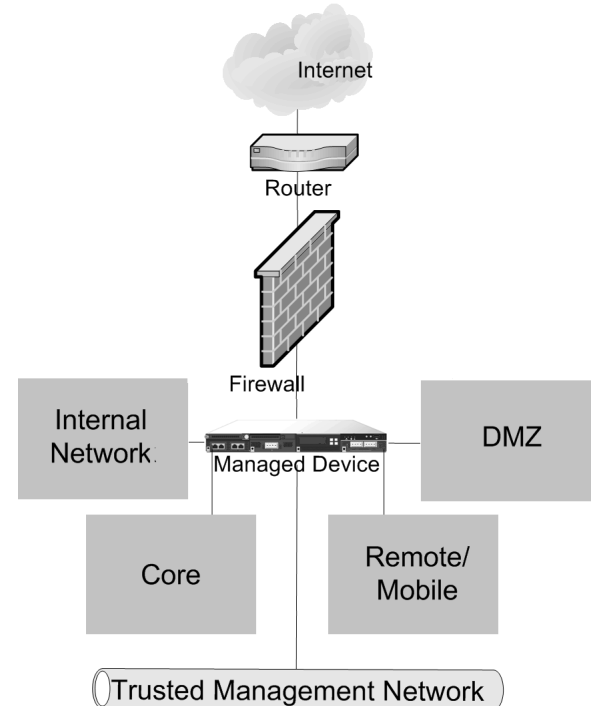
Your device is typically deployed inside a firewall, where it is connected to your trusted management network and the various network segments you want to monitor.

In a simple deployment scenario, you connect the management interface on your device to your trusted management network using an Ethernet cable, then connect the sensing interfaces to the network segments you want to monitor using the appropriate cables (copper or fiber) in either a passive or inline cabling configuration.

The trusted management network (a restricted network protected from unauthorized access) may have a single secure connection to the Internet for security updates and similar functions, but is separate from the rest of your network and is not accessible to hosts used in daily business operations.

You can connect sensing interfaces to different network segments dedicated to particular components of your business that have distinct security requirements to target policies based on the needs for specific segments. These segments can include the DMZ (outward-facing servers, such as mail, ftp, and web hosts), your internal network (hosts used in daily operation and similar applications), and the core (hosts reserved for critical business assets), and can also include segments dedicated to remote locations, mobile access, or other functions.

How you cable your sensing interfaces determines your configuration options. If you use passive cabling, you can configure passive sensing interfaces. If you use inline cabling, you can create passive, inline, inline with fail-open, virtual switch, virtual router, or hybrid sensing interfaces on your device. For more information on deployment options and interface configurations and how they affect product features, see the *Sourcefire 3D System User Guide* and the *Sourcefire 3D System Installation Guide*.



Cabling the Device

You can cable your device to configure passive or inline interfaces, depending on your deployment needs.

Use passive cabling if you want to:

- monitor traffic
- collect information about hosts, operating systems, applications, users, files, networks, and vulnerabilities

Use inline cabling if you want to use the same features as a passive deployment, plus:

- configure a virtual switch, virtual router, or hybrid interface
- perform network address translation (NAT)
- use policies to block traffic based on access control features such as application control, user control, security intelligence, URL dispositions, file control, malware detection, or intrusion prevention

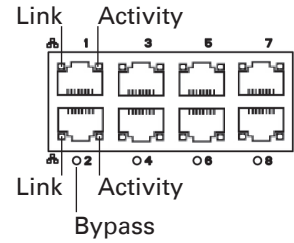
Use the appropriate cables (as indicated by your interface) and cabling diagram for the interface you want to configure, then use the web interface on the Defense Center to configure the interfaces. See *Connecting the Sensing Interfaces* on page 4.

Understanding the Sensing Interfaces

3D7010/7020/7030

The 3D7010/7020/7030 is a 1U device one-half the width of the rack tray with eight copper sensing interfaces, each with bypass capability.

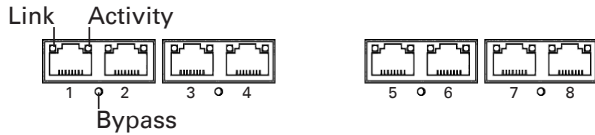
You can use these interfaces to passively monitor up to eight separate network segments. You can also use paired interfaces in an inline configuration on up to four network segments.



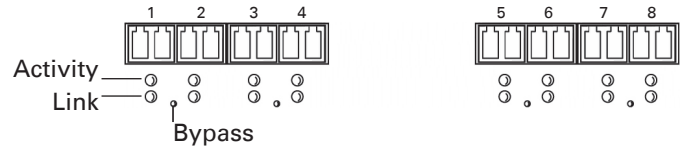
3D7110/7120

The 3D7110/7120 is a 1U device with eight copper or eight fiber sensing interfaces, each with bypass capability.

EIGHT-PORT 1000BASE-T COPPER



EIGHT-PORT 1000BASE-SX FIBER



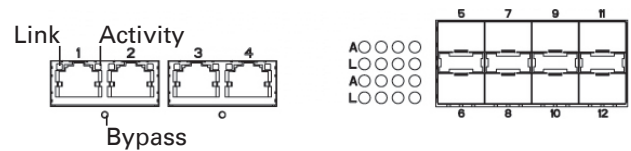
You can use these interfaces to passively monitor up to eight separate network segments. You can also use paired interfaces in an inline configuration on up to four network segments.

3D7115/7125, AMP7150

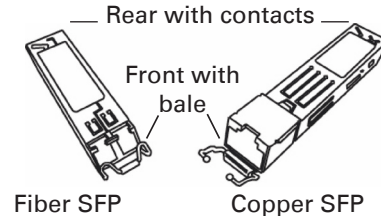
The 3D7115/7125 and AMP7150 are 1U devices with four copper sensing interfaces with bypass capability and eight small form-factor pluggable (SFP) sockets without bypass capability.

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

You can insert up to eight SFP transceivers (any combination of copper, fiber, or both) and use their interfaces to monitor up to eight separate network segments. You can also use any combination of transceivers on sequentially paired interfaces (interfaces 5 and 6, 7 and 8, 9 and 10, or 11 and 12) in an inline deployment. Note that SFP interfaces do not have bypass capabilities.



SAMPLE SFP TRANSCEIVERS



Inserting or Removing a Small Form-Factor Pluggable (SFP) Transceiver

The 3D7115/7125 and AMP7150 contain eight SFP sockets in a “tab toward center” configuration. Cable the interface on the transceiver after the transceiver is inserted into the chassis.

Use appropriate electrostatic discharge (ESD) procedures when inserting or removing the transceiver. Avoid touching the contacts, and keep the contacts and interfaces free of dust and dirt.

To insert an SFP transceiver into the chassis SFP socket:

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 engage the locking mechanism, securing the transceiver in place.

CAUTION! 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.

Use only Sourcefire SFP transceivers. Non-Sourcefire transceivers may jam in the socket and can cause permanent damage to the transceiver, the chassis, or both.

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 locking mechanism.
For transceivers in the upper row, pull down. For transceivers in the lower row, lift up.
3. Gently slide the transceiver directly out of the socket, taking care not to touch the contacts at the back of the transceiver.
If the transceiver does not slide out easily, push the transceiver back into the socket and try again, using the bale as a handle.

Connecting the Sensing Interfaces

This section describes the physical connection of the sensing interfaces. After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the device's sensing interfaces as passive, inline, inline with fail-open, switched, routed, or hybrid. Use only the interfaces on the front of the device as sensing interfaces.

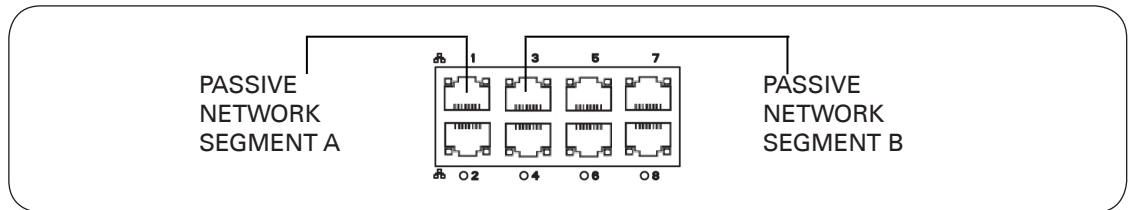
See the *Sourcefire 3D System Installation Guide* for detailed information on planning your deployment. After you have selected a deployment model, cable the sensing interfaces as needed for your configuration.

Passive Interface Cabling

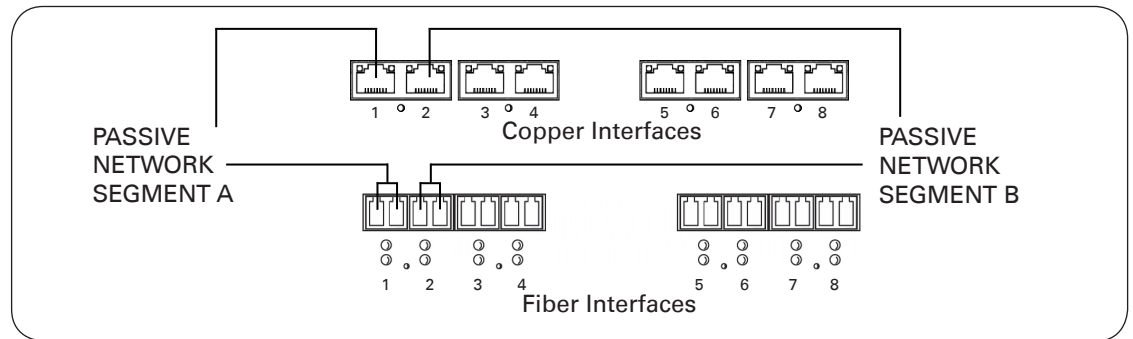
For each network segment you want to monitor passively, connect the appropriate cables (either copper or fiber) to one sensing interface.

Use this cabling when you want to configure passive interfaces.

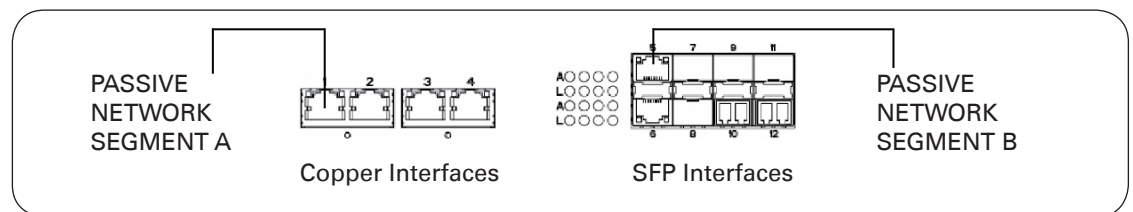
3D7010/7020/7030



3D7110/7120



3D7115/7125, AMP7150

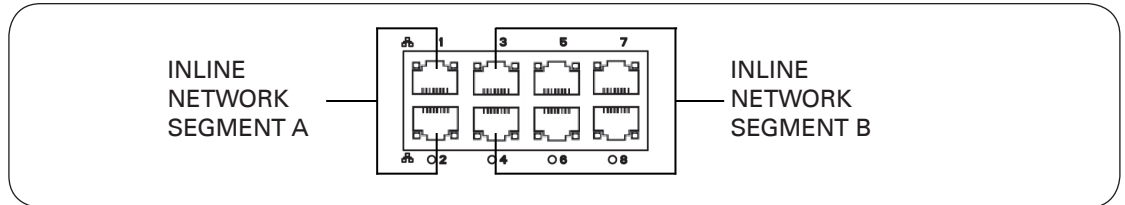


Inline Interface Cabling

For each network segment you want to monitor inline, connect the appropriate cables (either copper or fiber sequentially to pairs of sensing interfaces.

Use this cabling when you want to configure inline, inline with fail-open, switched, routed, or hybrid interfaces.

3D7010/7020/7030

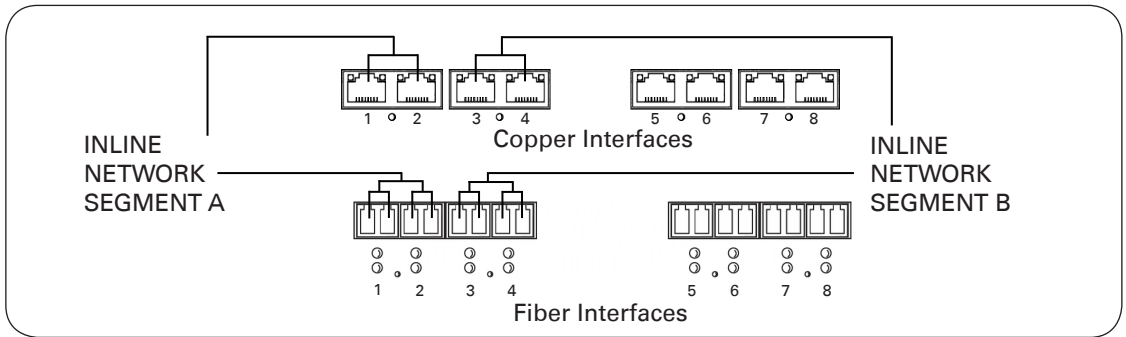


Inline with Fail-Open Configuration

If you want to take advantage of the device's configurable fail-open capability, you must cable a sequential pair of vertical interfaces (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment.

After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the interface as inline with fail-open. See Setting Up an IPS Device in the *Sourcefire 3D System User Guide*.

3D7110/7120

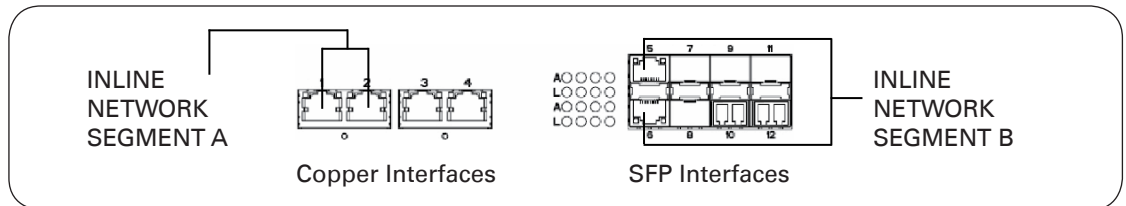


Inline with Fail-Open Configuration

If you want to take advantage of the device's configurable fail-open capability, you must cable a sequential pair of interfaces (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment.

After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the interface as inline with fail-open. See Setting Up an IPS Device in the *Sourcefire 3D System User Guide*.

3D7115/7125, AMP7150



Inline with Fail-Open Configuration

You can configure SFP interfaces inline, but SFP interfaces do not have inline fail-open capability. If you want to take advantage of the device's configurable fail-open capability, you must cable a sequential pair of copper interfaces (interfaces 1 and 2, or 3 and 4) to a network segment.

After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the interface as inline with fail-open. See Setting Up an IPS Device in the *Sourcefire 3D System User Guide*.

Installing the Device

The Sourcefire 3D System is delivered on different hardware platforms that you can rack-mount. When you install a device, make sure that you can access the device's console for initial setup.

You can access the console for initial setup using a keyboard and monitor with KVM, or using an Ethernet connection to the management interface.

Keyboard and Monitor/KVM

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

IMPORTANT! Do not use a KVM switch with USB mass storage to access the device because the device may attempt to use the mass storage device as a boot device.

Ethernet Connection to Management Interface

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

- 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 device. To interact with the device, use terminal emulation software such as HyperTerminal or XModem with the following software settings:

- 9600 baud
- 8 data bits
- no parity checking
- 1 stop bit
- no flow control

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

To install the device:

1. Mount the device in your rack using the mounting kit and its supplied instructions.
2. Connect to the device using either a keyboard and monitor or an Ethernet connection.
 - If you are using a keyboard and monitor to set up the device, 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 device's physical management interface, you will connect the management interface to the protected network when you finish setup.
3. Connect the sensing interfaces to the network segments you want to analyze using the appropriate cables for your interfaces: See *Connecting the Sensing Interfaces* on page 4.
4. Attach the power cord to the device and plug into a power source.

If your device has redundant power supplies, attach power cords to both power supplies and plug them into separate power sources.
5. Turn on the device.
 - If you are using a keyboard and monitor to set up the device, continue with *Configuring Network Settings Using a Script* in the *Sourcefire 3D System Installation Guide*.
 - If you are using a direct Ethernet connection to set up the device, confirm that the link LED is on for both the network interface on the local computer and the management interface on the device. 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* in the *Sourcefire 3D System Installation Guide*.
6. After you have configured network settings, make sure the device is connected to the protected management network with an Ethernet cable and continue the initial setup with *Initial Setup: Devices* in the *Sourcefire 3D System Installation Guide*.

You can find detailed information on additional configuration options (such as testing an inline bypass configuration, reconfiguring your console output, and so on) in the *Sourcefire 3D System Installation Guide*.

LEDS

Front Panel LEDs	
3D7010/7020/7030	
	A Reset button B System status LED C Hard drive activity LED D System ID button E Power button and LED
LED	Description
Reset button	When pressed, the system immediately reboots.
System status	Indicates the system status: <ul style="list-style-type: none"> A green light indicates the system is powered up and operating normally, or powered down and attached to power. An amber light indicates an active system fault. No light indicates the system is not attached to power.
Hard drive activity	Indicates the hard drive status: <ul style="list-style-type: none"> A green light indicates the hard 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 bright blue LED is illuminated on the rear of the chassis to help identify the device when it is installed in a high-density rack with other similar systems.
Power button and LED	Indicates whether the device has power: <ul style="list-style-type: none"> A green light indicates that the device has power and the system is on. No light indicates the system is shut down or does not have power.
3D7110/7120, 3D7115/7125, and AMP7150	
	A USB 2.0 connector B Reset button C NIC2 activity LED D System status LED E NIC1 activity LED F Hard drive activity LED G System ID button H Power button and LED
LED	Description
NIC1 and NIC2 activity	Indicates whether there is any network activity: <ul style="list-style-type: none"> A green light indicates there is network activity. No light indicates there is no network activity.
Hard drive activity	Indicates the hard drive status: <ul style="list-style-type: none"> A green light indicates the hard drive is active. An amber light indicates a hard drive fault. No light indicates there is no drive activity, or the system is powered off.
System status	Indicates the system status: <ul style="list-style-type: none"> No light indicates the system is operating normally, or is powered off. A red light indicates a system error.
Reset button	When pressed, the system immediately reboots.
System ID	When pressed, the ID button displays a blue light, and a bright blue LED is illuminated on the rear of the chassis to help identify the device when it is installed in a high-density rack with other similar systems.
Power button and LED	Indicates whether the device has power: <ul style="list-style-type: none"> A green light indicates that the device has power and the system is on. No light indicates the system is shut down or does not have power.
Management Interface LEDs (all)	
Left (activity)	Indicates activity on the port: <ul style="list-style-type: none"> A blinking light indicates activity. No light indicates there is no link.
Right (link)	Indicates whether the link is up: <ul style="list-style-type: none"> A light indicates the link is up. No light indicates there is no link.

Sensing Interface LEDs	
3D7010/7020/7030 EIGHT-PORT 1000 BASE-T COPPER INTERFACES	
3D7110/7120 EIGHT-PORT 1000BASE-T COPPER	
EIGHT-PORT 1000BASE-SX FIBER	
3D7115/7125, AMP7150 FOUR-PORT 1000 BASE-T COPPER INTERFACES with EIGHT-PORT SMALL FORM-FACTOR PLUGGABLE SOCKETS	
Copper Link/Activity LEDs	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.
Fiber Activity/Link LEDs	Description
Activity (top)	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
Link (bottom)	For an inline or passive interface: the light is on when the interface has link. If dark, there is no link.
Bypass LED (all)	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 Activity/Link LEDs	Description
3D7115/7125, AMP7150 SFPs only	
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.

Hardware Specifications

Physical and Environmental Parameters			
Parameter	3D7010/7020/7030	3D7110/7120	3D7115/7125, AMP7150
Form factor	1U, half-rack width	1U	
Dimensions (D x W x H)	Single chassis: 12.49" x 7.89" x 1.66" (31.74 cm x 20.04 cm x 4.21 cm) 2-Chassis Tray: 25.05" x 17.24" x 1.73" (63.62 cm x 43.8 cm x 4.44 cm)	21.6 x 19.0 x 1.73 inches (54.9 x 48.3 x 4.4 cm)	
Weight (max installed)	Chassis: 7 pounds (3.17 kg) Single chassis and power supply in tray: 17.7 pounds (8.03 kg) Double chassis and power supplies in single tray: 24.7 pounds (11.2 kg)	29.0 pounds (13.2kg)	
Copper 1000BASE-T	Gigabit copper ethernet fail-open interfaces in a paired configuration Cable and distance: Cat5E at 50m	Gigabit copper ethernet fail-open interfaces in a paired configuration Cable and distance: Cat5E at 50m	
Fiber 1000BASE-SX	Not applicable	Fiber bypass with LC connectors Cable and distance: SX is multimode fiber (850nm) at 550m (standard)	Not applicable
Copper 1000BASE-T SFP	Not applicable	Not applicable	Gigabit copper ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50m
Fiber 1000BASE-SX SFP	Not applicable	Not applicable	Fiber non-bypass with LC connectors Cable and distance: SX is multimode fiber (850nm) at 550m (standard) 200m (656 ft) for 62.5µm/125µm fiber 500m (1640 ft) for 50µm/125µm fiber
Fiber 1000BASE-LX SFP	Not applicable	Not applicable	Fiber non-bypass with LC connectors Cable and distance: LX is single mode fiber (1310nm) at 10km for 9µm/125µm fiber (standard)
Power supply	200W AC power supply Voltage: 100VAC to 240VAC nominal (90VAC to 264VAC maximum) Current: 2A maximum over the full range Frequency range: 50/60 Hz nominal (47Hz to 63Hz maximum)	450W dual redundant (1+1) AC power supplies Voltage: 100VAC to 240VAC nominal (85VAC to 264VAC maximum) Current: 3A maximum for 90VAC to 132VAC, per supply 1.5A maximum for 187VAC to 264VAC, per supply Frequency range: 47Hz to 63Hz	
Operating temperature	0°C to 40°C (32°F to 104°F)	5°C to 40°C (41°F to 104°F)	
Non-operating temperature	-20°C to 70°C (-4°F to 158°F)	-20°C to 70°C (-4°F to 158°F)	
Operating humidity	5% to 95%, noncondensing Operation beyond these limits is not guaranteed and not recommended.	5% to 85%, non-condensing 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.	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 prior to placing the unit in service.	
Altitude	0 ft (sea level) to 5905 ft (0 to 1800m)	0 ft (sea level) to 5905 ft (0 to 1800m)	
Cooling requirements	682 BTU/hour You must provide sufficient cooling to maintain the device within its required operating temperature range. Failure to do this may cause a malfunction or damage to the device.	900 BTU/hour You must provide sufficient cooling to maintain the device within its required operating temperature range. Failure to do this may cause a malfunction or damage to the device.	
Acoustic noise	53 dBA when idle. 62 dBA at full processor load.	64 dBA at full processor load, normal fan operation Meets GR-63-CORE 4.6 Acoustic Noise	
Operating shock	No errors with half a sine wave shock of 5G (with 11 msec. duration)	Complies with Bellecore GR-63-CORE standards	
Airflow	20 ft ³ (0.57m ³) per minute Airflow through the device enters at the front and exits at the rear, with no side ventilation.	140 ft ³ (3.9m ³) per minute Airflow through the device enters at the front and exits at the rear with no side ventilation.	

Regulatory Conformance

This Sourcefire device conforms to multiple national and international standards. For a full list of regulatory compliance, see the *Sourcefire 3D System Installation Guide*.

Security Considerations

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

- Locate your device in a lockable rack within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the device.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access.

**WARNING!**

This Sourcefire device should be installed and maintained by qualified personnel only. Keep in mind the following safety information to avoid system damage or personal injury:

- Remove all factory packaging before using the device.
- Provide adequate ventilation to prevent overheating. Do not cover or block vents, or otherwise enclose the device.
- The device must be properly grounded when connecting power to the power outlet.
- At all times, keep the chassis area free from dust.
- Lifting the chassis for rack installation may require two people, as the unit is heavy.
- To avoid electrical shock, do not open or remove the chassis covers or metal parts without proper instruction.

SOURCEfire®

9770 Patuxent Woods Drive
Columbia, MD 21046 USA
800.917.4134 | +1.410.423.1901
support@sourcefire.com

©2014 Cisco and/or its affiliates.
All rights reserved.