

TM



## QUICK START GUIDE

# Fidelis Network<sup>TM</sup> Sensor Appliances

Rev-H 2016 (Applies to Fidelis Network  
— Direct, Internal, Web, and Mail Sensor  
Appliances Based on HP DL360-G9 and  
DL380-G9 Platforms)

## 1. System Overview

Fidelis sensors are the components that monitor the network environment for activities that may indicate advanced threat, malware, and data theft. Fidelis sensors analyze network traffic, deliver alerts and session data to CommandPost+, and deliver non-selective network session metadata to Fidelis Collector for retrospective analysis.




Figure 1: Fidelis Network — Sensor Appliance (1U) Rev-H



Figure 2: Fidelis Network — Direct / Internal 10G Sensor Appliance — Rev-H

## 2. Documentation & References

Fidelis Network product documentation, appliance specifications, and instructions can be found here <http://fidelissecurity.com/customer-support/login> or through the  icon in the CommandPost GUI.

### Appliance Default Passwords

System	Account	Password
SSH / Appliance Console	fidelis	fidelispass
CommandPost GUI	admin	system
ILO	administrator	<i>(printed on label, top of server)</i>

### Technical Support

For all technical support related to this product, check with your site administrator to determine support contract details. Contact your reseller or if you have a direct support contract, contact the Fidelis Cybersecurity support team at:

- Phone: +1 301.652.7190
- Toll-free in the US: 1.800.652.4020 — Use the customer support option.
- Email: [support@fidelissecurity.com](mailto:support@fidelissecurity.com)
- Web: <http://www.fidelissecurity.com/customer-support/login>

## Things You Need

Required for Each Appliance	Status
Appropriate rack space, power, and cooling ( <a href="#">Appendix B</a> )	
Rack tools, rails, and connectors	
Keyboard and video monitor / KVM switch for temporary appliance setup	
Power cables — two per appliance, appropriate for power source and region	
Ethernet cables (cat5 and optical) for Admin, Monitor, and iLO ports ( <a href="#">Section 3</a> )	
Network switches with enough physical ports ( <a href="#">Section 4</a> )	
Optical transceivers for switches	
Logical network information: IP addresses, hostnames ( <a href="#">Section 5</a> , <a href="#">Appendix A</a> )	

## 3. Sensor Appliances: Network Port and Cabling Requirements

Each appliance must be connected to the various networks with appropriate cables and in some cases, SFP+ transceivers. The tables below describe the physical connection and cable type associated with each port on the appliance.

### Direct/Internal Appliances With 1GbE rj45/Copper Ports

Port Label	Physical Connection Type (Default)	Cable Type
ADMIN	GbE RJ45 (copper)	Cat 5 patch cable
MON-A	GbE RJ45 (copper)	Cat 5 patch cable
MON-B	GbE RJ45 (copper)	Cat 5 patch cable
ILO	GbE RJ45 (copper)	Cat 5 patch cable

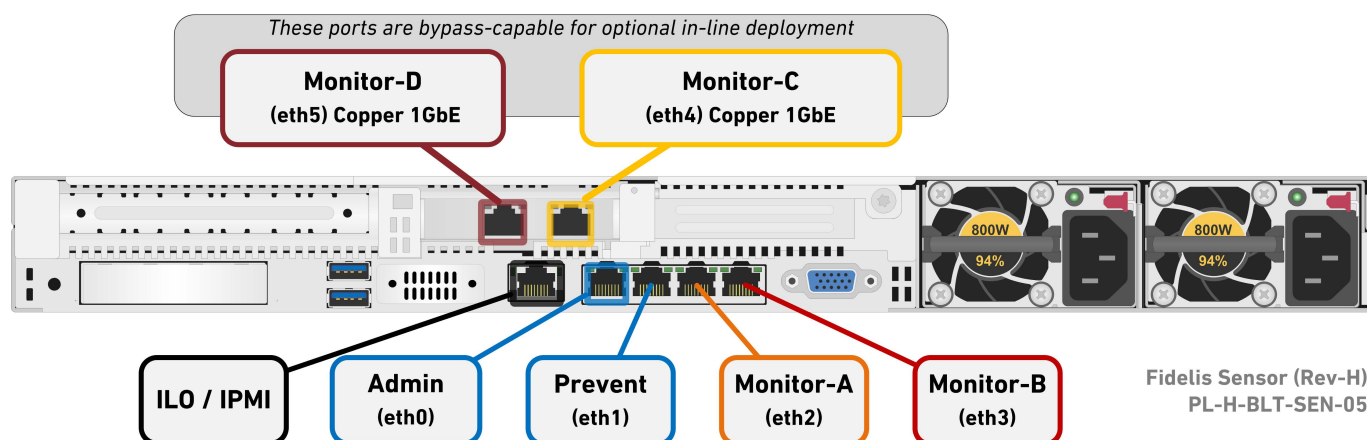


Figure 3: Rear Port Assignments — Sensors rated up to 1Gbps (Direct, Internal, Mail, and Web)

## Direct/Internal Sensor Appliances With 10GbE Optical Ports

Port Label	Physical Connection Type (Default)	Cable Type
ADMIN	GbE RJ45 (copper)	Cat 5 patch cable
MON-A	10GbE LC connector	Fiber SR Patch Cable, Multimode 850nm
MON-B	10GbE LC connector	Fiber SR Patch Cable, Multimode 850nm
ILO	GbE RJ45 (copper)	Cat 5 patch cable

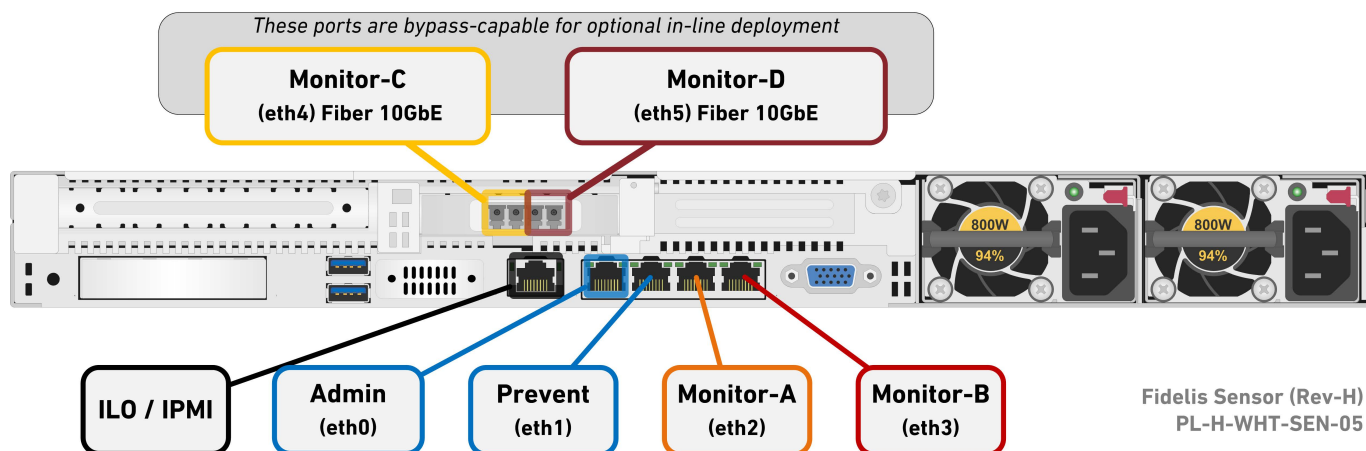


Figure 4: Rear Port Assignments — Direct/Internal 2500, 5000

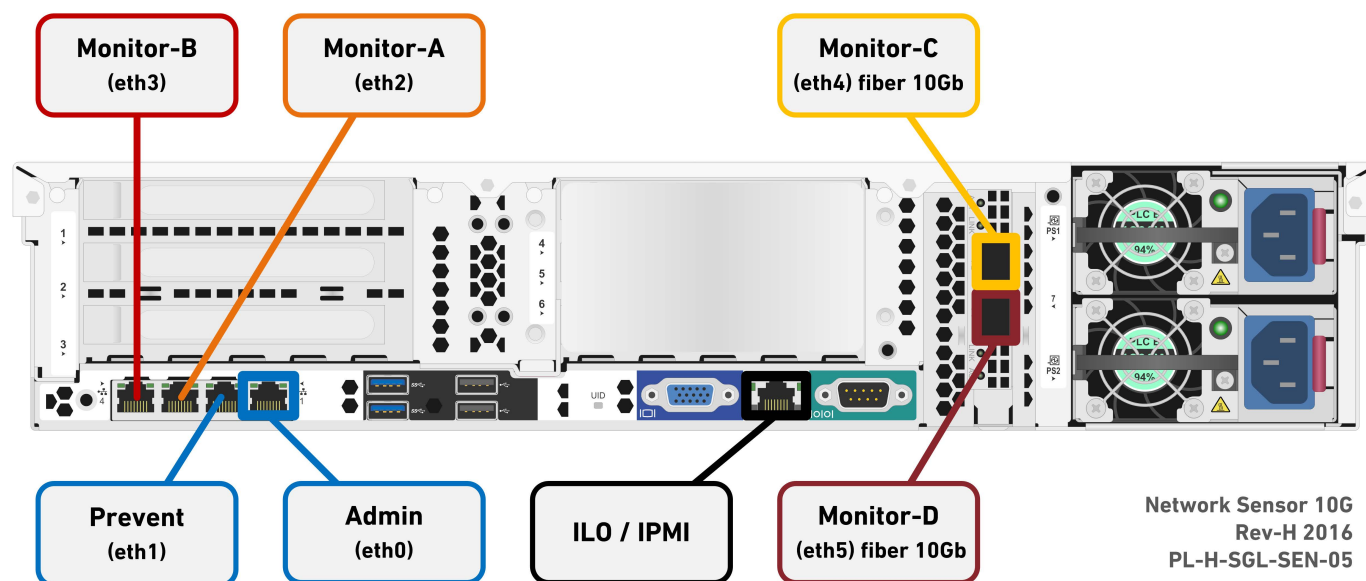


Figure 5: Rear Port Assignments — Direct 10G & Internal 10G

## 4. CommandPost and Sensor Networking Environment

Sensor appliances use multiple networks for service and monitoring. Use the tables below to identify the count and type of switch ports necessary to support the number of appliances for your deployment.

### ADMIN Network

The ADMIN Network connects Fidelis Network sensors to the CommandPost, Collector, and Sandbox.

Appliance	Switch Port Type	Qty.
All Sensors	GbE - Copper Cat5 RJ45 port	

### Monitor A Network

The Monitor A Network connects the sensor appliance to the monitored network environment — typically through a network switch mirror port or tap. In the out-of-band configuration, this port is connected to a single network environment for monitoring — Network A. In Inline Configuration, use this monitor port in pair with Monitor B to allow network data to flow through the device.

Appliance	Switch Port Type	Qty.
1-GbE sensors	GbE - Copper Cat5 RJ45 port	
10Gb sensors	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	

### Monitor B Network

The Monitor B (optional) similar to Monitor A above. connects the sensor to the monitored network environment. In the out-of-band configuration, this port is connected to a single network environment for monitoring — that is Network B. In Inline Configuration, use this monitor port in pair with Monitor B to allow network data to flow through the device.

Appliance	Switch Port Type	Qty.
1-GbE sensors	GbE - Copper Cat5 RJ45 port	
10Gb sensors	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	

### ILO Network

Optional network for remote/out-of-band server administration.

Appliance	Switch Port Type	Qty.
All sensors	GbE - Copper Cat5 RJ45 port	

## 5. Appliance — Logical Network Configuration

Each physical connection must be assigned logical network information. Build a table of the logical information for each appliance (sample below) that you can reference during configuration. Appendix A includes a worksheet for you. You will reference this table multiple times during the cluster setup.

**Sample Network Configuration Table**

Network Setting	Assignments			
Interface:	ADMIN/eth0	Monitor A	Monitor B	iLO/IMM
Hostname (FQDN)	sensor1.organization.net.			
Static IP Address	10.1.2.3	n/a	n/a	10.2.3.4
Subnet Mask	255.255.252.0	n/a	n/a	255.255.252.0
Gateway	10.1.2.1			
Proxy Server	10.5.6.7			
DNS Servers	8.8.4.4, 8.8.8.8			
NTP Servers	pool.ntp.org.			
Time Zone	UTC (+0)			

## 6. Appliance Installation

### Rack Installation

Install each appliance in an enclosure/location that has necessary power and cooling.

### Power

Connect power cables to the power supplies in the back of the appliance.

### Network Cabling

Using the connectors and cables described in sections 3 and 4, begin to connect the appliances to the networks.

Cable the Sensor appliances to the switches:

- Connect **Admin (eth0)** port to the ADMIN switch port.
- Connect the **iLO port** to the ADMIN (or ILO) switch port (optional).

## 7. Appliance Network Configuration

1. Power on the Appliance(s)
2. Connect to the component CLI using one of the following methods:
  - **Via SSH:** Directly attach an Ethernet cable from a client system such as a laptop to the Admin/eth0 port on the appliance. The default IP address is 192.168.42.11/24. Assign a static IP from the same subnet to the network interface on the client system and connect to the appliance using SSH.
  - **Via KVM Console:** Connect a keyboard and monitor to the appliance.
3. Use these credentials at the login prompt:
  - user: **fidelis**
  - default password: **fidelispass**
4. From the command line, run: `>sudo /FSS/bin/setup`
  - a. You will be prompted for the SU (fidelis) password
5. Within Setup, select Network Settings.
6. Configure the network parameters for the system and each active network interface.
  - a. Use the Network Configuration table you prepared earlier.
  - b. When complete, return to the top menu.
7. When complete, select [OK] to leave Setup.
8. From command line, reboot the system: `>sudo /sbin/shutdown -r now`

## 8. Fidelis Network Integration

### Register Sensor Appliances With CommandPost

1. Log into the CommandPost GUI from a web browser.
2. Add the Sensor to the CommandPost at the System>Components page. Click [Add Component].
3. Select Sensor from the drop down. Complete the form:
  - name — this is a user-friendly name for the sensor, not the FQDN of the sensor.
  - IP address of the ADMIN interface of the sensor appliance
  - (optional) description — e.g. location, business unit, etc.
  - click [Save].
4. Register the sensor to CommandPost. Click [Register] and accept the End User License Agreement (EULA). CommandPost will then communicate with the sensor at the specified IP address.

## 9. Fidelis Licensing

To use Fidelis Network sensor appliances, you must license them. The CommandPost GUI shows the Host ID for the Fidelis Network hardware, the current license key, and the expiration date. To access the License page:

1. Log into the CommandPost.
2. Click System>Components>[component name]>Config.
3. Click the License tab.

If your license key shows <no license> or <invalid>. Refer to Request a License for more information.

### Request a License

1. Click Request License or click the Host ID.
2. This sends an email to [license@fidelissecurity.com](mailto:license@fidelissecurity.com) that includes the product type, serial number, and Host ID.
3. Include in the body of the email:
  - contact name and phone number
  - organization name and site location

Fidelis Cybersecurity will respond within one business day with a license key.

### Enter a License Key

After receiving a response to a license request:

1. Copy the license key exactly into the License Key box.
2. Click Save.

When complete, Fidelis Network sensor appliances will be operational and ready to monitor the network.



## Appendix A: Network Configuration Worksheet

### Sensors (All Types)

Network Setting	Assignments			
Interface:	ADMIN/eth0	Mon-A (eth4)	Mon-B (eth5)	iLO
Hostname (FQDN)				
Static IP Address		n/a	n/a	
Subnet Mask		n/a	n/a	
Gateway		n/a	n/a	
DNS Servers				
NTP Servers				
Time Zone				

## Appendix B: System Specifications

	Direct/Internal 10G	Direct & Internal 5000, 2500	Direct 1000, 500, 250, 100, 50; Internal 1000	Mail 1000, 500 250; Web
				
Form Factor	2U rack-mount chassis	1U rack-mount chassis SFF	1U rack-mount chassis SFF	1U rack-mount chassis SFF
CPU	Quad Intel Xeon v3 18-core 2.1Ghz	Dual Intel Xeon v3 14-core 2.6 Ghz	Dual Intel Xeon v3 10-core 2.6 Ghz	Dual Intel Xeon v3 10-core 2.6 Ghz
Memory	256GB ECC DDR4 2133Mhz	128GB ECC DDR4 2133Mhz	96GB ECC DDR4 2133Mhz	96GB ECC DDR4 2133Mhz
Storage Capacity & Configuration	500 GB 2x HDD, RAID-1	300 GB 2x HDD, RAID-1	300 GB 2x HDD, RAID-1	300 GB 2x HDD, RAID-1
Network Adapters (Default Config)	4x 1GbE 2x 10GbE optical	4x 1GbE 2x 10GbE optical (inline capable)	4x 1GbE 2x 1GbE (inline capable)	4x 1GbE 2x 1GbE (inline capable)
Out of Band Management	Integrated Lights Out Management (ILO)	Integrated Lights Out Management (ILO)	Integrated Lights Out Management (ILO)	Integrated Lights Out Management (ILO)
Dimensions	H: 8.73 cm ( 3.44 in) W: 44.55 cm (17.54 in) D: 73.60 cm (28.97 in)	H: 4.32 cm ( 1.7 in) W: 43.47 cm (17.1 in) D: 69.85 cm (27.5 in)	H: 4.32 cm ( 1.7 in) W: 43.47 cm (17.1 in) D: 69.85 cm (27.5 in)	H: 4.32 cm ( 1.7 in) W: 43.47 cm (17.1 in) D: 69.85 cm (27.5 in)
Weight (appx.)	32.18 kg (70.94 lb)	15.6 kg (35.5 lb)	15.6 kg (35.5 lb)	15.6 kg (35.5 lb)
Power Supply	Dual hot-swap 1200W High Efficiency AC power supplies	Dual hot-swap 800W High Efficiency AC power supplies	Dual hot-swap 800W High Efficiency AC power supplies	Dual hot-swap 800W High Efficiency AC power supplies
Operating Temp	10° to 35°C (50° to 95°F) at sea level	10° to 35°C (50° to 95°F) at sea level	10° to 35°C (50° to 95°F) at sea level	10° to 35°C (50° to 95°F) at sea level



Fidelis Cybersecurity is creating a world where attackers have no place left to hide. We reduce the time it takes to detect attacks and resolve security incidents. Our Fidelis Network™ and Fidelis Endpoint™ products look deep inside your traffic and content where attackers hide their exploits. Then, we pursue them out to your endpoints where your critical data lives. With Fidelis you'll know when you're being attacked, you can retrace attackers' footprints and prevent data theft. To learn more about Fidelis Cybersecurity products and incident response services, please visit [www.fidelissecurity.com](http://www.fidelissecurity.com) and follow us on Twitter [@FidelisCyber](https://twitter.com/FidelisCyber).