Fidelis
Cybersecurity

QUICK START GUIDE

Fidelis Network® Sensor Appliances

Rev-J
Fidelis Sensors
(Direct, Internal, Web, and Mail Appliances)
Based on HPE DL360-G10 and DL560-G10 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/K2, and deliver non-selective network session metadata to Fidelis Collector for retrospective analysis.

Figure 1: Fidelis Network – Sensor Appliance (1U) Rev-J

Figure 2: Fidelis Network – Direct / Internal 10G Sensor Appliance – Rev-J

Fidelis Sensors report network alerts and network metadata to your on-premises Fidelis Network Enterprise CommandPost/K2 appliance - or - to the remote Fidelis Network Cloud. Your configuration will depend on which environment you are working with. The following instructions will indicate if they apply to Enterprise (on-prem), Fidelis Network Cloud, or All Environments.

2. Documentation & References

Fidelis Network product documentation, appliance specifications, and instructions can be found at

https://support.fidelissecurity.com or through the 🛈 icon in the CommandPost/K2 user interface.

Appliance Default Passwords

System	Account	Default Password
SSH / Appliance Console	fidelis	fidelispass
CommandPost/K2 User Interface	admin	system
iLO	administrator	*(printed on label, top of server)*

Technical Support

For all technical support related to this product, check with your site administrator to determine support contract details. For support of your product, contact your reseller. If you have a direct support contract with Fidelis Cybersecurity, 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
- Web: https://support.fidelissecurity.com

Sensor Setup Checklist

Check	Fidelis Network Sensor – Appliance Requirements
	Appropriate rack space, power, and cooling (Appendix B)
	Rack tools, rails, and connectors
	Keyboard and video monitor / KVM switch for temporary appliance setup
	Power cables — two per appliance (four for 10G sensor), appropriate for power source and region
	Ethernet cables (cat5 and optical) for Admin, Monitor, and iLO ports (Section 3)
	Network switches with enough physical ports (Section 4)
	Optical transceivers for switches
	Logical network information: IP addresses, hostnames (Section 5, Appendix A)
	For Fidelis Network Software version 9.3.3 and later, the appliance system type (Appendix C)
Check	**…also needed for Fidelis Network Cloud**
	Connection information from Fidelis Customer Support
	Fidelis Network Cloud - Quick Start Guide

3. Sensor: Network Port and Cabling Requirements

Fidelis Network Sensors are designed to process different traffic capacities and different types of network connections, including: 1GbE, 10GbE, 1Gb-SX, and 10Gb-SR. 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

		Cable Type
Admin (eth0)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Prevent (eth1)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Monitor-A (eth2)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Monitor-B (eth3)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Bypass (eth4) *	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Bypass (eth5) *	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Bypass (eth6) *	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Bypass (eth7) *	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
ILO	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable

*Direct and Internal only. For out of band monitoring and inline monitoring
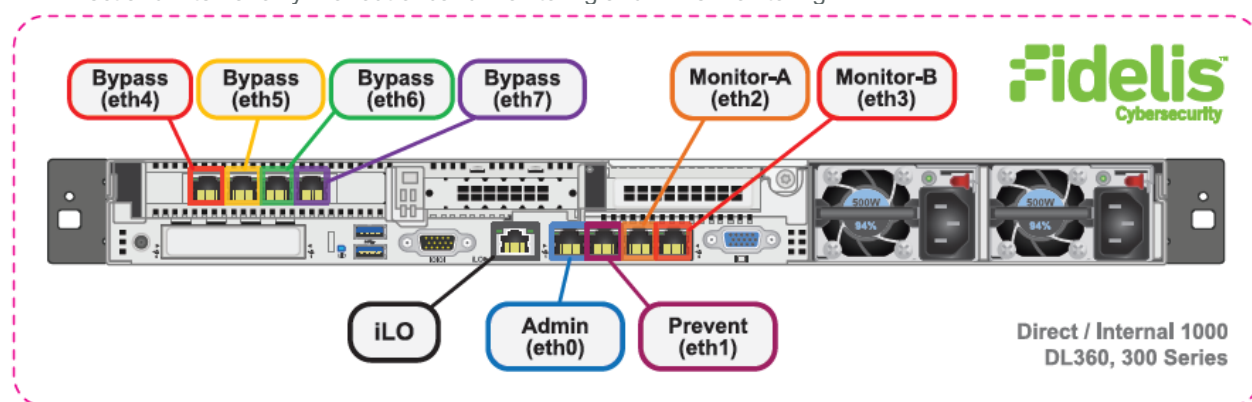

Figure 3: Rear Port Assignments — Sensors rated up to 1Gbps (Direct, Internal, Mail, and Web)

Direct/Internal Sensor Appliances With 10GbE Optical Ports

|		Cable Type
Admin (eth0)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Prevent (eth1)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Monitor-A (eth2)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Monitor-B (eth3)	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
Bypass (eth4)	LC Connector	Fiber SR Patch Cable, Multimode 850nM
Bypass (eth5)	LC Connector	Fiber SR Patch Cable, Multimode 850nM
Bypass (eth6)	LC Connector	Fiber SR Patch Cable, Multimode 850nM
Bypass (eth7)	LC Connector	Fiber SR Patch Cable, Multimode 850nM
ILO	8P8C "RJ45" (copper)	Cat 5/5e/6 patch cable
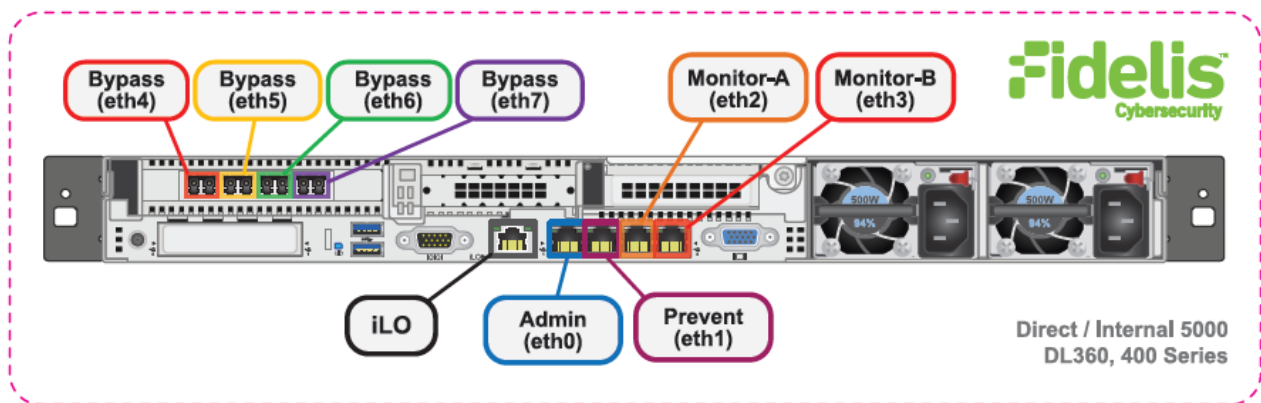
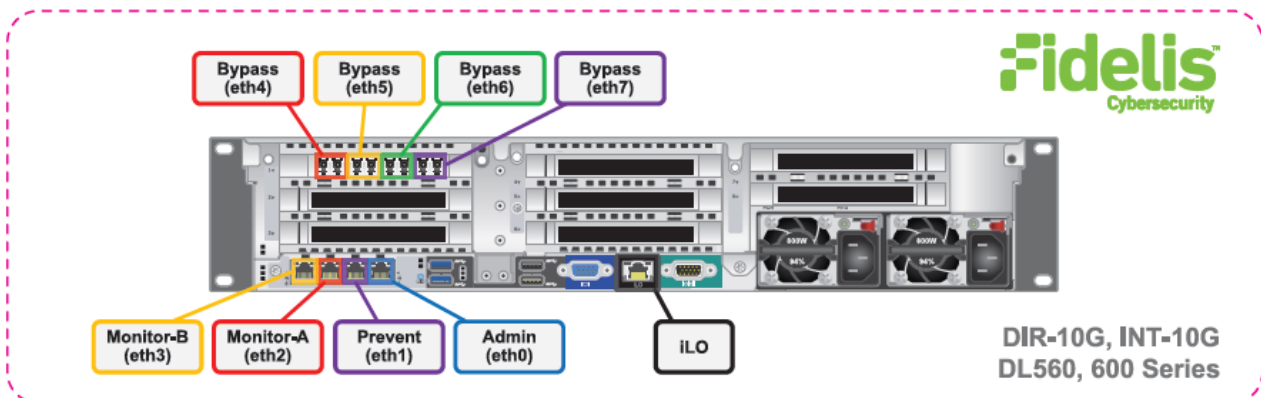Figure 4: Rear Port Assignments — Direct/Internal 5000/2500

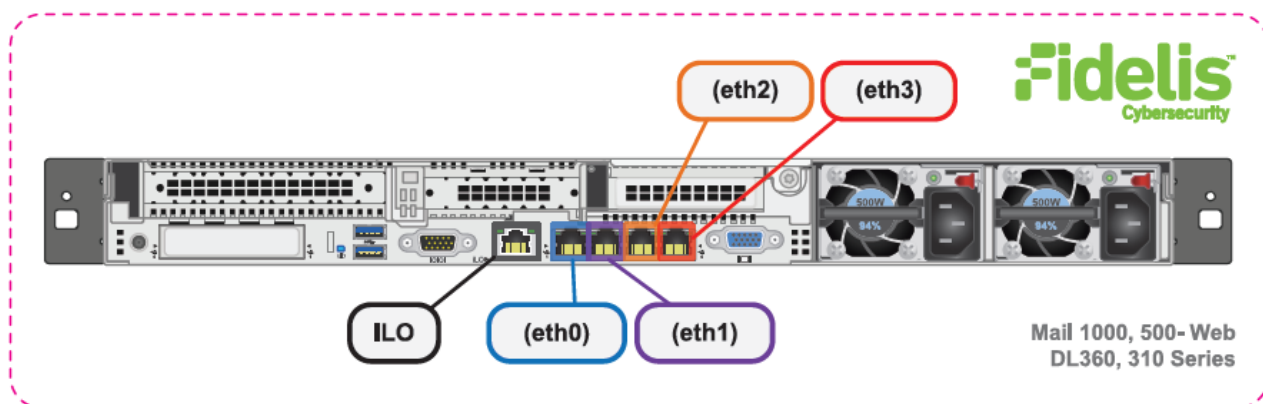Figure 5: Rear Port Assignments — Direct 10G & Internal 10G

Figure 6: Rear Port Assignments — Mail Sensor and Web Sensor

4. Sensor Networking Environment

Sensor appliances may connect to multiple networks for service and monitoring. Use the tables below to identify how many and what type of network switch ports you will need for your deployment.

Admin Network

The Admin Network connects Fidelis Network Sensors to the CommandPost/K2, Collector, and Sandbox. You need one switch port per Sensor appliance for the Admin network.

Appliance	Switch Port Type	Qty.
All Sensors	8P8C "RJ45" (copper)	

Prevent Network

Optional connection that the Sensor uses to deliver TCP Reset and other messages to the production environment. This connection is only used if the Sensor is connected out-of-band to one or more monitored networks. If you use the Prevent port, you will need one additional switch port per Sensor.

Appliance	Switch Port Type	Qty.
All Sensors	8P8C "RJ45" (copper)	

Monitor A and Monitor-B Networks

Optional ports to connect the Sensor appliance to the monitored networks "A" and "B" through network switch mirrored-ports or taps. One additional port for each monitored network.

Appliance	Switch Port Type	Qty.
All Sensors	8P8C "RJ45" (copper)	

Eth4/eth5/eth6/eth7 Networks

Most environments use the eth4/eth5/eth6/eth7 ports (instead of Mon-A and Mon-B) because these ports offer support for higher network throughput and/or support in-line session blocking and prevention / policy enforcement.

For **in-line prevention**, the ports are organized into two pairs (eth4/eth5 and eth6/eth7). Each pair can be connected to one network segment. You will need two switch ports for monitoring each in-line segment. Connect two interfaces in one pair to the same monitored network to allow network data to flow through the device.

In the **out-of-band** configuration, connect the Sensor appliance to the eth4/eth5/eth6/eth7 through network switch mirrored-ports or taps. One additional port for each monitored network.

Appliance	Switch Port Type	Qty.
1GbE Sensors	8P8C "RJ45" (copper)	4
2.5-, 5-, and 10-Gb Sensors	LC Connector	4

ILO / IPMI Network

Optional network for remote/out-of-band server administration. You will need one additional switch port for each IPMI connection.

Appliance	Switch Port Type	Qty.
All Sensors	8P8C "RJ45" (copper)	1

5. Appliance — Logical Network Configuration

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

Direct/Internal Sensor Appliances With 10GbE Optical Ports

Network Setting	Assignments					
Interface	Admin	Prevent	Mon-A	Mon-B	eth4/eth5/ eth6/eth7	ILO / IPMI
Hostname (FQDN)	sensor1.myorganization.int					
Static IP Address	10.1.2.3	n/a*	n/a*	n/a*	n/a*	10.2.3.3
Subnet Mask	255.255.255.0	n/a*	n/a*	n/a*	n/a*	255.255.255.0
Gateway	10.1.2.1	n/a*	n/a*	n/a*	n/a*	10.2.3.1
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)					

*For Alternative Sensor Network Configurations - In-line & ERSPAN

This Quick Start Guide will help you configure a Sensor in "tap" or "out-of-band" mode, where each monitoring interface is connected to a different network. In out-of-band mode, each monitor port is configured in promiscuous mode, and therefore do not need IP network information. Sensors may alternatively be configured to support ERSPAN, which may require IP network configuration. For help with these configurations, please see the **Fidelis Network Enterprise Setup Guide**.

6. Appliance Installation

Rack Installation

Install each appliance in an enclosure/location that has necessary power and cooling. Ensure that the installation environment is within the operating temperature of the appliance.

Refer to **Appendix B** for appliance operating temperature requirements.

Power

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

See **Appendix B** for appliance power specifications.

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:

1. Connect Admin (eth0) port to the ADMIN switch port.

2. 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 KVM Console: Connect a keyboard and monitor to the appliance.

   For Fidelis Network appliances version 9.3.3 or later, the screen on the right is displayed:
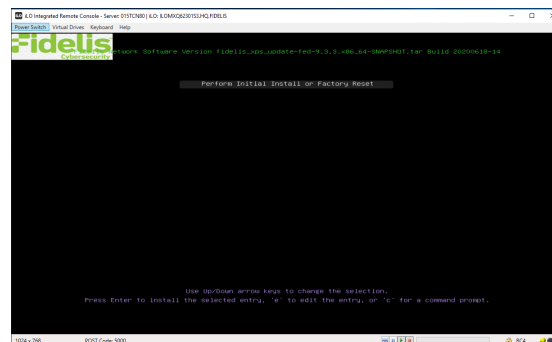
3. If you see the screen above, perform the following steps to apply the software. Otherwise skip to step 4.

   a. With [Perform Initial Install or Factory Reset] selected, press Enter.

   b. Use the Up and Down arrow keys to select the system type (Direct xxxx, Internal xxxx, Mail xxxx or Web), and press Enter.
   If you need help determining the system type, see Appendix C.

4. Login into the system through console or SSH.

   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.

5. Use these credentials at the login prompt:

   user: **fidelis**

   default password: **fidelispass**

6. From the command line, run: **sudo /FSS/bin/setup**

   You will be prompted for the SU (fidelis) password

7. Within Setup, select Network Settings.

8. 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.

9. When complete, select [OK] to leave Setup.

10. From command line, reboot the system: **sudo /fss/bin/shutdown.pl --user admin --reboot**

8. Fidelis Network — On Premises CommandPost/K2 Environments

Register Sensor Appliances with Your Fidelis Enterprise K2

1. Log into the CommandPost/K2 user interface from a web browser.

2. Navigate to the **System > Components** page.

3. Click **Add Component** Sensor.

4. Fill in the Add New Component form:

Component Type	Select **Sensor**
Component Name	Specify a "friendly" name for the sensor. This is not the fully qualified domain name of the sensor.
Component IP address	Specify the IP address of the Admin interface of the sensor appliance
Description	(optional) Specify a description, for example location, business unit, etc.

5. Click **Save**.

6. The Sensor's **Component Name** will appear on the list below Direct/Internal/Mail/Web. Click on the **Component Name** to view the Component Details.

7. Click **Register** and accept the End User License Agreement (EULA). CommandPost/K2 will then communicate with the Sensor at the specified IP address.

9. Fidelis Network Integration - Fidelis Network Cloud Environments

Register Sensor Appliances with Fidelis Network Cloud

Please contact Fidelis Support to connect your Sensors to the Fidelis Network Cloud. Fidelis Support will work with you to configure the Sensors and enable the Fidelis Network Cloud for your environment.

Appendix A: Network Configuration Worksheet

Sensors (All Types)

Network Setting	Assignments					
Interface	Admin	Prevent	Mon-A	Mon-B	eth4/eth5 eth6/eth7	iLO / IPMI
Hostname (FQDN)						
Static IP Address		*n/a**				
Subnet Mask		*n/a**				
Gateway		*n/a**				
Proxy Server						
DNS Servers						
NTP Servers						
Time Zone						

* For in-line or ERSPAN deployments, see the Fidelis Network Enterprise Setup and Configuration Guide.

Appendix B: System Specifications

Direct/Internal 10G & 5000

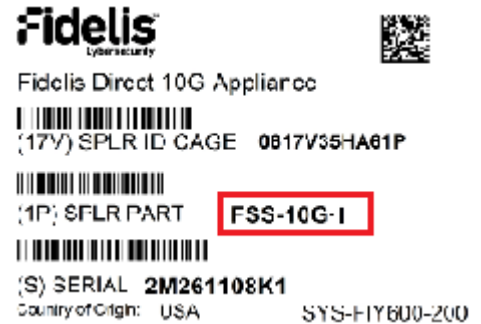|	Direct/Internal 10G	Direct/Internal 5000 Direct/Internal 2500
Form Factor	2U rack-mount chassis	1U rack-mount chassis SFF
CPU	Quad Intel Xeon Gold 6248 20/80-core 2.5 Ghz	Dual Intel Xeon Gold 6248 20/40-core 2.5 Ghz
Memory	384 GB ECC DDR4 2933Mhz	128 GB ECC DDR4 2933Mhz
Storage Capacity & Configuration	480 GB 2x SSD, RAID-1 (240GB)	300 GB 2x HDD, RAID-1
Network Adapters	4x 1GbE 4x 10GbE optical (Inline capable)	4x 1GbE 4x 10GbE optical (inline capable)
Out of Band Management	Integrated Lights Out Management (ILO)	Integrated Lights Out Management (ILO)
Dimensions	H: 8.75 cm (3.44 in) W: 44.54 cm (17.54 in) D: 75.47 cm (29.71 in)	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)
Weight (appx.)	34.12 kg (75.23 lb)	16.27 kg (35.86 lb)
Power Supply	Four hot-swap 800W High Efficiency AC power supplies	Dual hot-swap 800W High Efficiency AC power supplies
Operating Temperature	10° to 35°C (50° to 95°F) at sea level	10° to 35°C (50° to 95°F) at sea level
AC input Requirements	100 – 120 VAC 200 – 240 VAC	100 – 120 VAC 200 – 240 VAC
BTU Rating (max)	3207 BTU/hr (100 VAC) 3071 BTU/hr (200 VAC) 3112 BTU/hr (240 VAC)	3067 BTU/hr (100 VAC) 2958 BTU/hr (200 VAC) 2949 BTU/hr (240 VAC)

Direct/Internal 1000 and below, Mail 1000, 500, 250 and Web

	Direct/Internal 1000 & below	Mail 1000, 500, 250 and Web
Form Factor	1U rack-mount chassis SFF	1U rack-mount chassis SFF
CPU	Dual Intel Xeon-Silver 4214 12/24-core 2.2 Ghz	Dual Intel Xeon-Silver 4214 12/24-core 2.2 Ghz
Memory	64 GB ECC DDR4 2933Mhz	64 GB ECC DDR4 2933Mhz
Storage Capacity & Configuration	300 GB 2x HDD, RAID-1	300 GB 2x HDD, RAID-1
Network Adapters	4x 1GbE 4x 1GbE Copper (inline capable)	4x 1GbE
Out of Band Management	Integrated Lights Out Management (ILO)	Integrated Lights Out Management (ILO)
Dimensions	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)
Weight (appx.)	16.27 kg (35.86 lb)	16.27 kg (35.86 lb)
Power Supply	Dual hot-swap 800W High Efficiency AC power supplies	Dual hot-swap 800W High Efficiency AC power supplies
Operating Temperature	10° to 35°C (50° to 95°F) at sea level	10° to 35°C (50° to 95°F) at sea level
AC input Requirements	100 – 120 VAC 200 – 240 VAC	101 – 120 VAC 200 – 240 VAC
BTU Rating (max)	3067 BTU/hr (100 VAC) 2958 BTU/hr (200 VAC) 2949 BTU/hr (240 VAC)	3067 BTU/hr (100 VAC) 2958 BTU/hr (200 VAC) 2949 BTU/hr (240 VAC)

Appendix C: System Types

For Fidelis Network Software version 9.3.3 and later, the table below shows the software to apply based on the appliance SKU. You can find the SKU in the following locations:
(Note that the SKU starts with "FSS" or "FNH".)

- **Appliance lid UID decal** (see sample on right)
- **Shipping carton UID decal** (see sample on right)
- **Packing list**
- **Purchase Order**

Appliance SKU starts with:	System Type
FSS-1G-J FNH-1G-J	Direct 1000, Direct 500, Direct 250, Direct 100, Direct 50 Internal 1000
FSS-5G-I FNH-5G-J	Direct 5000 Internal 5000
FSS-10G-J FNH-10G-J	Direct 10G Internal 10G
FSS-MAIL-WEB-CC2-J FNH-MAIL-WEB-CC2-J	Mail 1000, Mail 500, Mail 250 Web

QSC_Fidelis_Sensor__Rev-J_20200716