QUICK START GUIDE

Fidelis Network® Collector SA

Rev-I
Collector SA Appliances
Based on HP DL360-G10 Platforms

1. System Overview

The Fidelis Collector is the security analytics database for Fidelis Network. The Fidelis Collector SA receives network metadata from Fidelis Network sensors (i.e., Direct, Internal, Mail, and Web sensors) and stores it for ongoing analysis. The Collector SA appliance Rev-I is also referred to as Collector SA2.

Figure 1: Fidelis Network — Collector SA Appliance (Rev-I)

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

Collector 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, appropriate for power source and region
	Ethernet cables (cat5) for Admin and iLO ports (Section 3)
	Network switches with enough physical ports (Section 4)
	Logical network information: IP addresses, hostnames (Section 5, Appendix A)
	For Fidelis Network Software version 9.0.5 and later, the appliance system type (Appendix C)

3. Collector: Network Port and Cabling Requirements

Each component must be connected to the various networks with appropriate cables. The tables below describe the physical connection and cable type associated with each port.

Collector SA Appliance

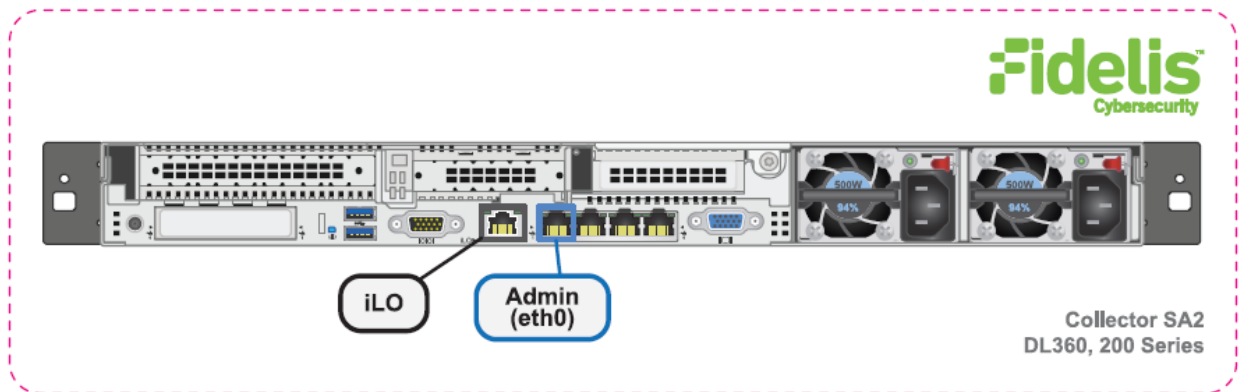| Port Label	Physical Connection Type (default)	Cable Type
Admin	GbE RJ45 (copper)	Cat 5 patch cable
iLO	GbE RJ45 (copper)	Cat 5 patch cable

Figure 3: Network Port Assignments — Collector SA (Rev-I)

4. Collector SA Networking Environment

The Collector SA appliances use the Admin network for service and inter-node communication. The appliances also offer the IPMI/iLO interface for optional out-of-band management of the appliance.

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 the Collector SA to the Fidelis Network sensors and CommandPost/K2 systems.

Appliance	Switch Port Type	Qty.
Collector SA	GbE - RJ45/Cat5+ (copper twisted pair)	1

iLO / IPMI Network

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

Appliance	Switch Port Type	Qty.
Collector SA	GbE - RJ45/Cat5+ (copper twisted pair)	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 that you can reference during configuration. Appendix A has a worksheet you can use to build your own Network Configuration table that you will reference multiple times during setup.

Sample Network Configuration Table

Network Setting	Assignments	
Interface:	Admin/eth0	iLO/IMM
Hostname (FQDN)	CollectorSA-1.organization.net.	
Static IP Address	10.1.2.3	10.2.3.4
Subnet Mask	255.255.255.0	255.255.255.0
Gateway	10.1.2.1	
Proxy Server	10.5.6.7	
DNS Servers	8.8.4.4, 8.8.8.8	
NTP Servers	0.pool1.ntp.org.	
Time Zone	UTC (+0)	

6. Appliance Installation

Rack Installation

Install each appliance in a location with 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.

To cable the Collector SA appliance(s) 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 9.0.5 or later, the screen on the right is displayed:
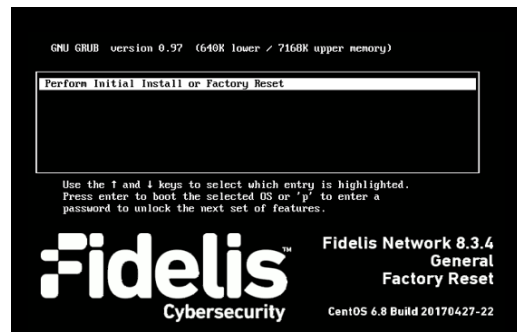
3. If you see the screen above, perform the following steps to apply the software. Otherwise skip to step 4.

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

   b. Use the Up and Down arrow keys to select the system type **Collector SA**, and press Enter.

      If you need help determining the system type, see Appendix C.

      The system displays a screen with the message "Congratulations, your CentOS installation is complete."
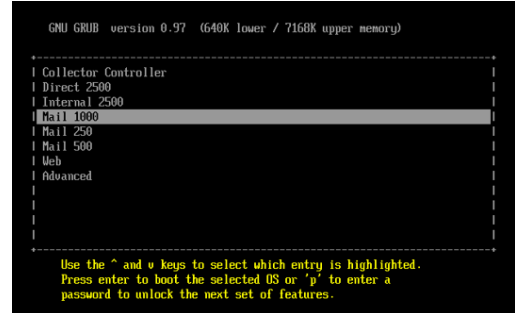
   c. Click **Reboot**.

4. Login to the appliance using 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.

   − Use the Network Configuration table you prepared earlier.

   − 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 Integration

Register Collector SA with CommandPost/K2

1. Log into the CommandPost/K2 user interface from a web browser.
2. Navigate to **System > Components**.
3. Click **Add Component**.
4. Fill in the Add New Component form:

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

5. Click **Save**.
6. Register the Collector to CommandPost/K2. Click **Register** and accept the End User License Agreement (EULA).

   CommandPost/K2 will then communicate with the Collector at the specified IP address.

Link Collector to Fidelis Sensors

1. Log into the CommandPost/K2 user interface from a web browser.
2. Navigate to **System > Components**.
3. Select the appropriate Direct, Internal, or Mail sensor to expand its details and then click **Config**.
4. In the left navigation, select the appropriate item for the sensor **Direct**, **Internal**, or **Mail**.
5. Click the **Advanced** or **Metadata** tab for the sensor.
6. In the **Send metadata to collector** list, select the Collector from the list.
7. Repeat for each Fidelis sensor.

Appendix A: Network Configuration Worksheet

Collector SA

Network Setting	Assignments	
Interface:	Admin/eth0	iLO/IMM
Hostname (FQDN)		
Static IP Address		
Subnet Mask		
Gateway		
Proxy Server		
DNS Servers		
NTP Servers		
Time Zone		

Appendix B: System Specifications

Component Configuration and Resources (Rev-I)

	Collector SA (Rev-I)
Form Factor	1U rack-mount chassis, SFF
CPU	Dual Intel Xeon Gold 6136 12/24-core 3.0 Ghz
Memory	192 GB ECC DDR4 2666Mhz
Storage Capacity & Configuration	480GB 2x SSD, RAID-1 (240GB) 7.2 TB HDD 6x HDD, RAID-10 (3.6TB)
Network Adapters (Default Config)	4x 1GbE
Out of Band Management	Integrated Lights Out Management (ILO)
Power Supply	Dual hot-swap 800W High Efficiency AC power supplies
Dimensions	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 (35.85 lb)
Operating Temperature	10° to 35°C (50° to 95°F) at sea level

Appendix C: System Types

For Fidelis Network Software version 9.0.5 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 typically 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 with:	System Type
FSS-SB-CollSA2-I FNH-SB-CollSA2-I	Collector SA

QSC_Fidelis_CE_Rev-I_20190509