

TM



QUICK START GUIDE

Fidelis Network™ High Capacity Collector

Rev-H

Collector Controller Appliances

Based on HP DL360-G9 and DL380-G9

Platforms

1. System Overview

The Fidelis Collector is the security analytics database for Fidelis Network. The Fidelis Collector receives network metadata from Fidelis Network sensors (e.g., Direct, Internal, and Mail Sensors) and stores it for ongoing analysis. A Fidelis Collector is a cluster of appliances consisting of one or two Collector Controller(s) and typically three or more Collector XA database nodes.




Figure 1: Fidelis Network — Collector Controller 10G (Rev-H)



Figure 2: Fidelis Network — Collector XA3 Appliance (Rev-H)

2. Documentation & References

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

Appliance Default Passwords

System	Account	Default Password
SSH / Appliance Console	fidelis	fidelispass
CommandPost GUI	admin	root
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. 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: <http://www.fidelissecurity.com/customer-support/login>

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 and optical) for Admin, DB, SYNC 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 8.3.4 and later, the appliance system type (Appendix D)

3. Collector: Network Port and Cabling Requirements

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

Collector Controller 10G Appliance

Port Label	Physical Connection Type (default)	Cable Type
Admin	10GbE LC connector	Fiber SR Patch Cable, Multimode 850nM
DB Net	10GbE LC connector	Fiber SR Patch Cable, Multimode 850nM
ILO	GbE RJ45 (copper)	Cat 5/5e/6 patch cable

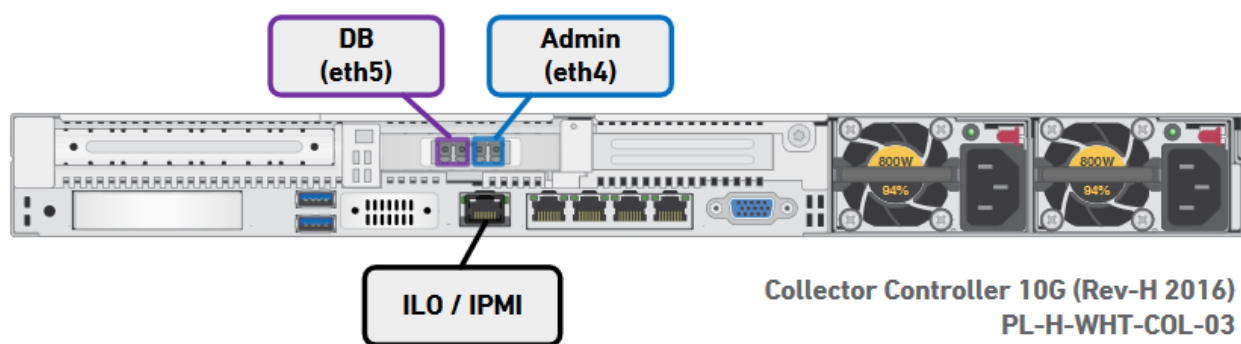


Figure 3: Network Port Assignments — Collector Controller 10G (Rev-H)

Collector XA3 Database Node

Port Label	Physical Connection Type (default)	Cable Type
Admin	GbE RJ45 (copper)	Cat 5 patch cable
DB Net	10GbE SFP+ w/ LC Connector	Fiber SR Patch Cable, Multimode 850nM
SYNC net	10GbE SFP+ w/ LC Connector	Fiber SR Patch Cable, Multimode 850nM
ILO	GbE RJ45 (copper)	Cat 5 patch cable

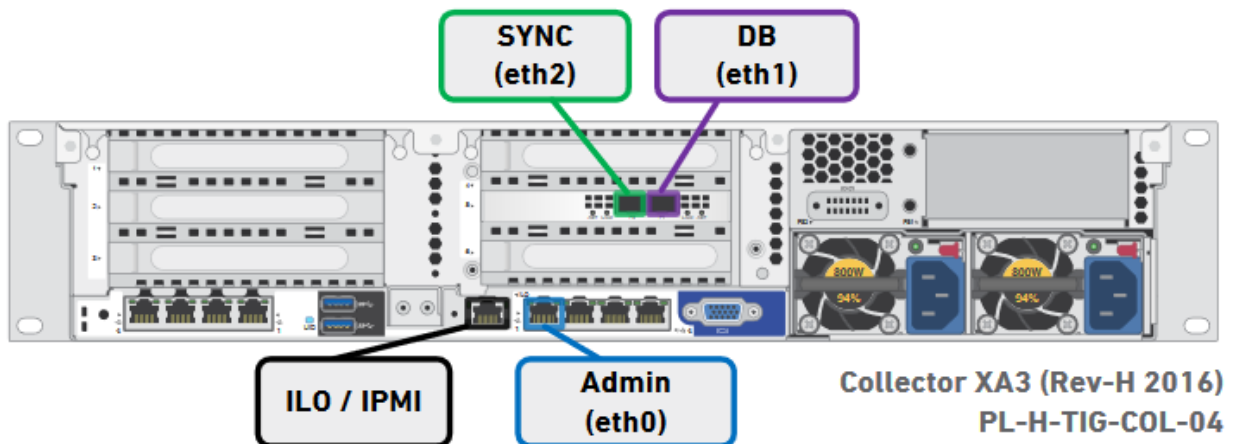


Figure 4: Network Port Assignments — Collector XA3 (Rev-H)

4. Collector Networking Environment

The Collector appliances use multiple networks for service and inter-node communication. Networks may be deployed as three independent physical switches — or — multiple independent VLANs on the same switch fabric. The ADMIN, DB, and SYNC switches or VLANs must be different broadcast domains. (iLO and ADMIN networks may intersect)

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 Controller to the Fidelis Network sensors and CommandPost systems. Also connects the Collector XA nodes to the CommandPost.

Appliance	Switch Port Type	Qty.
Collector Controller 10G	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	
Collector XA3	GbE - Copper Cat5 RJ45 port	

DB Network

The DB Network allows communication between Collector Controller and Controller XA nodes. This network must be independent from other networks. IPv4 addressing only.

Appliance	Switch Port Type	Qty.
Collector Controller 10G	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	
Collector XA3	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	

SYNC Network

Most environments use the Monitor-C and -D ports (instead of -A and -B) because these ports offer support for higher network throughput and/or support in-line session blocking and prevention / policy enforcement.

Appliance	Switch Port Type	Qty.
Collector Controller 10G	n/a	
Collector XA3	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	

ILO / IPMI Network

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

Appliance	Switch Port Type	Qty.
Collector Controller 10G	GbE - Copper Cat5 RJ45 port	
Collector XA3	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. You will refer to this table multiple times during setup. Appendix A has a worksheet you may use.

Sample Network Configuration Table

Network Setting	Assignments			
Interface	Admin/eth0	DB/eth1	SYNC/eth2	iLO/IMM
Hostname (FQDN)	collector-xa1.organization.net.			
Static IP Address	10.1.2.3	192.168.1.3	172.16.1.3	10.2.3.4
Subnet Mask	255.255.252.0	255.255.255.0	255.255.255.0	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 4 and 5, begin to connect the appliances to the networks. Refer to the Collector network diagram for this section.

Cable the **Collector Controller 10G** appliance(s) to the switches:

1. Connect **Admin (eth0)** port to the “ADMIN” switch port
2. Connect **DB (eth1)** port to the “DB” switch port
3. Connect the **iLO port** to the ADMIN (or ILO) switch port (optional)
4. Repeat for each Collector Controller.

Cable the **Collector XA3 Node** appliances to the switches:

1. Connect **Admin (eth0)** port to the “ADMIN” switch port.
2. Connect **DB (eth1)** port to the “DB” switch port.
3. Connect **SYNC (eth2)** port to the “SYNC” switch port.
4. Connect the **iLO port** to the ADMIN (or ILO) switch port. (optional)
5. Repeat for each Collector XA.

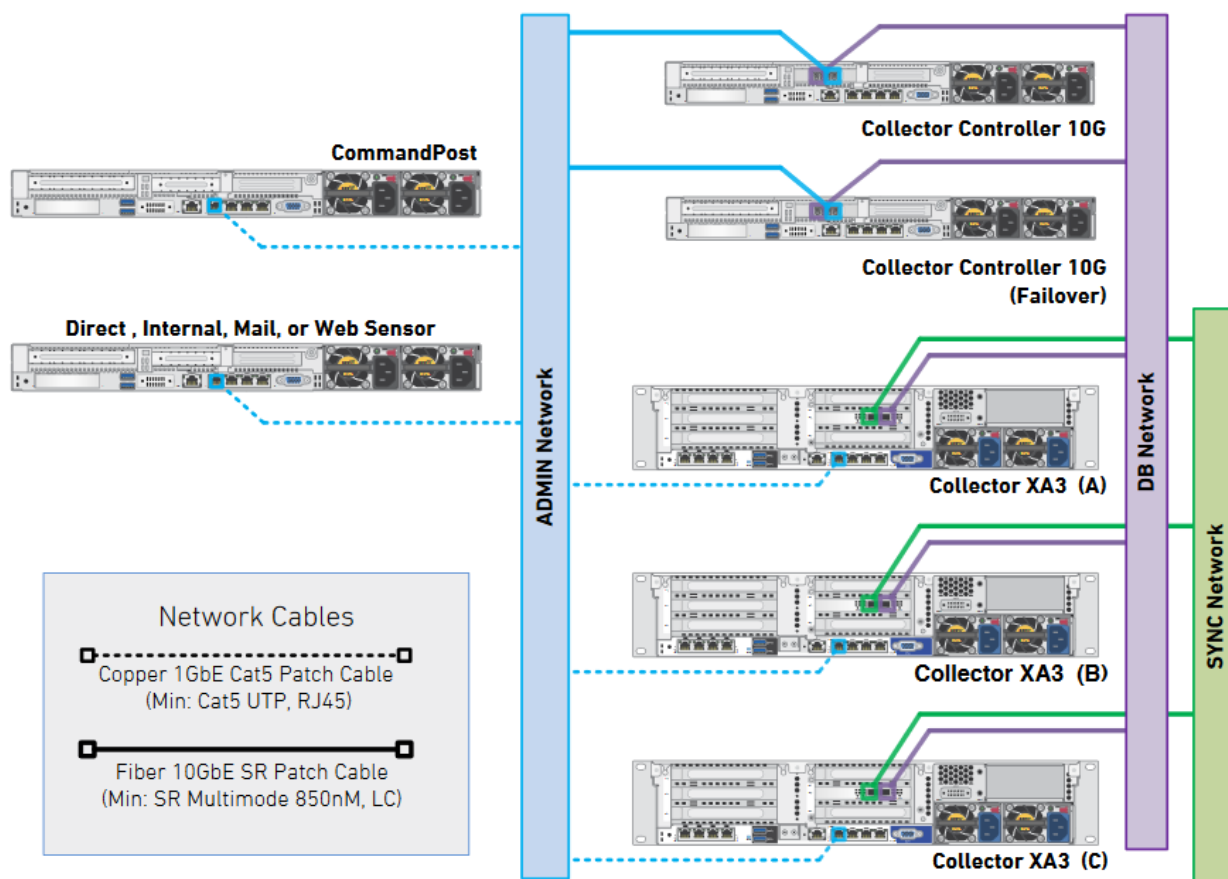
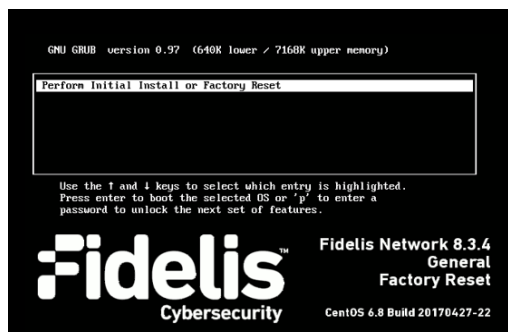


Figure 5: Collector Network Diagram

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.

For Fidelis Network appliances version 8.3.4 or later, the screen on the right is displayed:

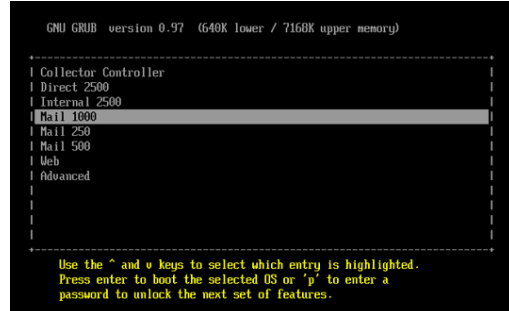


3. If you see the screen above, perform the following steps to apply the software. Otherwise skip to step 4.

- a. With [Perform Initial Install or Factory Reset] selected, press Enter.
- b. Use the Up and Down arrow keys to select the system type, and press Enter.
If you need help determining the system type, see [Appendix D](#).

The system displays a screen with the message “Congratulations, your CentOS installation is complete.”

- c. Click Reboot.



4. Use these credentials at the login prompt:
 - user: **fidelis**
 - default password: **fidelisspass**
 5. From the command line, run: **sudo /FSS/bin/setup**
You will be prompted for the SU (fidelis) password
 6. Within Setup, select Network Settings.
 7. 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.
 8. When complete, select [OK] to leave Setup.
 9. From command line, reboot the system: **sudo /fss/bin/shutdown.pl --user admin --reboot**
- Repeat steps for all appliances being added to the Collector cluster.
10. Use the PING command to verify connectivity between the XAs on their SYNC/eth2 interfaces.

8. Cluster Setup

On the Final Collector XA3 Appliance

If you have not completed setup for the XA3 appliances in section 7 above, or you are adding an XA3 appliance to the Collector, follow these steps:

1. Login via SSH or KVM console.
2. From the command line, run: **su - root -c /FSS/bin/setup**
3. Navigate to Collector Settings.
4. At the XA3 count, enter the number of XA3 appliances, and select Ok.
5. Review the list of IP addresses. Select Confirm if these are correct, or select Edit to correct them.

9. Fidelis Network Integration

Register Collector Controller 10G with CommandPost

1. Log into the CommandPost GUI from a web browser.
2. Add the Collector to the CommandPost at the System>Components page. Click Add Component.
3. Select Collector from the drop down menu. Complete the form:
 - name — this is a user-friendly name for the Collector, not the FQDN of the Controller.
 - IP address of the ADMIN interface of the primary Collector Controller 10G appliance
 - (optional) description — e.g. location, business unit, etc.
 - Click Save.
4. Register the Collector to CommandPost. Click Register and accept the End User License Agreement (EULA). CommandPost will then communicate with the Collector at the specified IP address.

Register Collector Controller 10Gs with the Fidelis Sensors

1. Log into the CommandPost GUI from a web browser.
2. Select the appropriate Direct, Internal, or Mail sensor and click Config.
3. Click the Advanced page for the sensor and select a Collector at the drop down box.
4. Repeat for each sensor.

10. Fidelis Licensing

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.
This sends an email to license@fidelissecurity.com that includes the product type, serial number, and Host ID.
2. 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, Collector and Collector appliances will be operational and storing network metadata for analysis.

Appendix A: Network Configuration Worksheet

Collector Controller 10G (Primary)

Network Setting	Assignments		
Interface	Admin/eth0	DB/eth1	iLO/IMM
Hostname (FQDN)			
Static IP Address			
Subnet Mask			
Gateway			
Proxy Server			
DNS Servers			
NTP Servers			
Time Zone			

Collector Controller 10G (Failover)

Network Setting	Assignments		
Interface	Admin/eth0	DB/eth1	iLO/IMM
Hostname (FQDN)			
Static IP Address			
Subnet Mask			
Gateway			
Proxy Server			
DNS Servers			
NTP Servers			
Time Zone			

Collector XA3 (A)

Network Setting	Assignments			
Interface	Admin/eth0	DB/eth1	SYNC/eth2	iLO/IMM
Hostname (FQDN)				
Static IP Address				
Subnet Mask				
Gateway				
Proxy Server				
DNS Servers				
NTP Servers				
Time Zone				



Collector XA3 (B)

Network Setting	Assignments			
Interface	Admin/eth0	DB/eth1	SYNC/eth2	iLO/IMM
Hostname (FQDN)				
Static IP Address				
Subnet Mask				
Gateway				
Proxy Server				
DNS Servers				
NTP Servers				
Time Zone				

Collector XA3 (C)

Network Setting	Assignments			
Interface	Admin/eth0	DB/eth1	SYNC/eth2	iLO/IMM
Hostname (FQDN)				
Static IP Address				
Subnet Mask				
Gateway				
Proxy Server				
DNS Servers				
NTP Servers				
Time Zone				

Appendix B: System Specifications

	Collector Controller 10G	Collector XA3
		
Form Factor	1U rack-mount chassis SFF	2U rack-mount chassis SFF
CPU	Dual Intel Xeon v3 14-core 2.6 Ghz	Dual Intel Xeon v3 10-core 3.1 Ghz
Memory	128 GB ECC DDR3 1600Mhz	256 GB ECC DDR3 1600Mhz
Storage Capacity & Configuration	300 GB 2x HDD, RAID-1	300 GB 2x HDD, RAID-1 ----- 9.9 TB 22x HDD, RAID-10
Network Adapters	4x 1GbE 2x 10GbE optical	4x 1GbE 2x 10GbE optical
Out of Band Management	Integrated Lights Out Management (ILO)	Integrated Lights Out Management (ILO)
Dimensions	H: 4.32 cm (1.7 in) W: 43.47 cm (17.1 in) D: 69.85 cm (27.5 in)	H: 8.73 cm (3.44 in) W: 44.55 cm (17.54 in) D: 67.94 cm (26.75 in)
Weight (appx.)	15.6 kg (35.5 lb)	23.6 kg (51.5 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

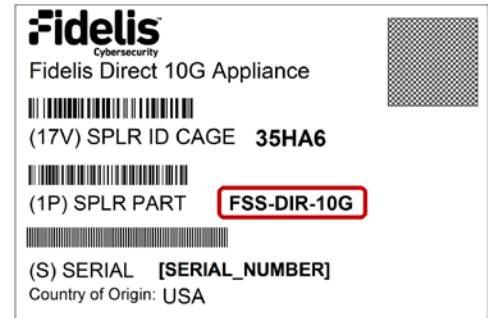
Appendix C: Collector — Internet Socket Communication Ports (TCP, UDP)

Network	Ports
Admin	TCP: 22 (SSH), 443 (HTTPS), 5556 TLS, 5557 TLS 5558 TLS, 5559 UDP: 123 (NTP), 5560 (IP2ID)
DB	TCP: 22 (SSH), 5433, 5556 TLS
SYNC	TCP: 22 (SSH), 5433, 5434, 5444, 5450, 4803, UDP: 4803, 4804, 4805, 5433

Appendix D: System Types

For Fidelis Network Software version 8.3.4 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”.)

- 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-CXA3	Collector
FSS-CXA4	Collector
FSS-CC10G	Collector Controller

QSC_Fidelis_CHC_20170524