



QUICK START GUIDE

Fidelis Network[®] High Capacity Collector

Rev-1

Collector Controller 10G (HP DL360-G10) and
Collector XA4 (DL380-G10) 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 (i.e., Direct, Internal, Mail, and Web sensors) and stores it for ongoing analysis. A Fidelis Collector cluster of appliances consists of one or two Collector Controllers and typically three or more Collector XA database nodes.




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



Figure 2: Fidelis Network — Collector XA4 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	<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: <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 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 9.0.5 and later, the appliance system type (Appendix C)

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

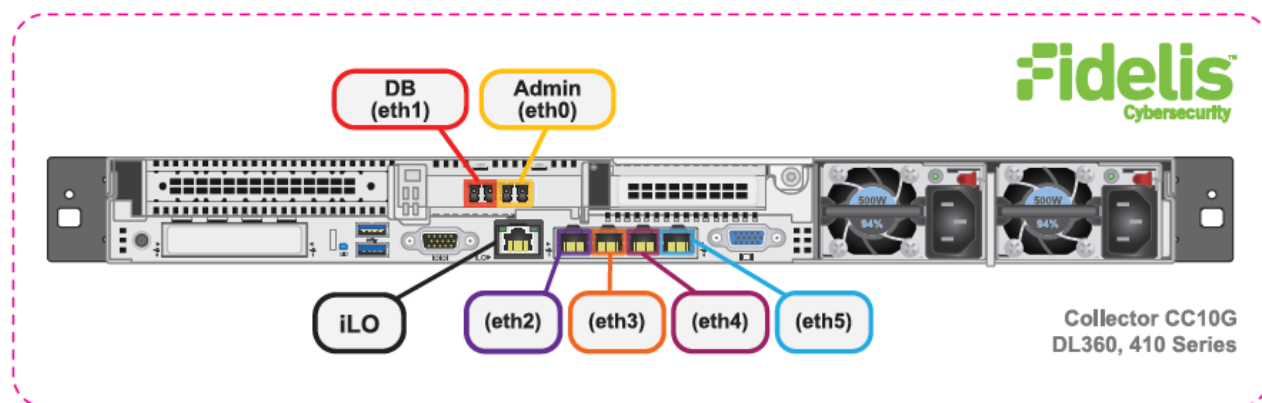


Figure 3: Network Port Assignments — Collector Controller 10G (Rev-I)

Collector XA4 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

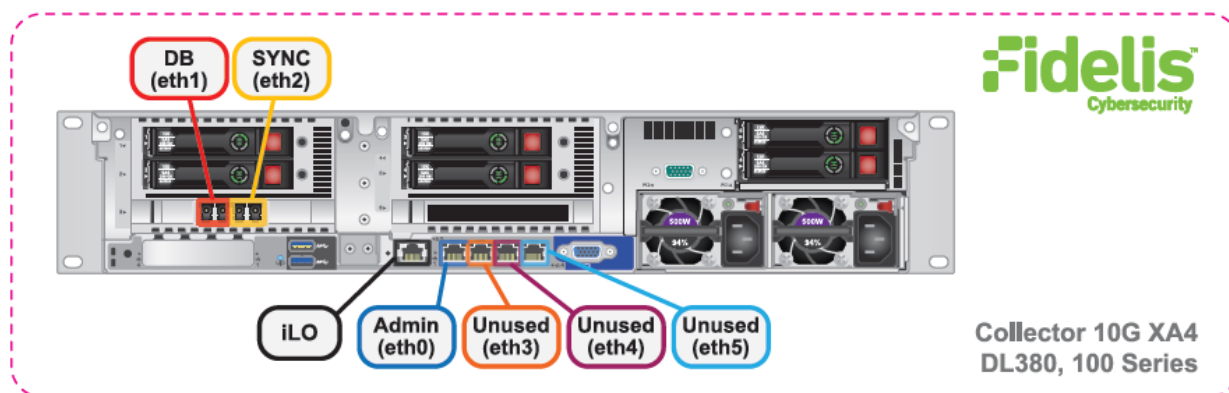


Figure 4: Network Port Assignments — Collector XA4 (Rev-1)

4. Collector Networking Environment

The Collector appliances use multiple networks for service and inter-node communication. You can deploy networks 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 can 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/K2 systems. Also connects the Collector XA nodes to the CommandPost/K2.

Appliance	Switch Port Type	Qty.
Collector Controller 10G	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	1
Collector XA4	GbE - Copper Cat5 RJ45 port	1

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)	1
Collector XA4	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	1

SYNC Network

The SYNC Network provides transport for database node synchronization. This network must be independent from other networks. Only IPv4 addresses are supported.

Appliance	Switch Port Type	Qty.
Collector Controller 10G	n/a	
Collector XA4	10GbE Fiber SR, LC connector (may require SFP+ transceiver)	1

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	1
Collector XA4	GbE - Copper Cat5 RJ45 port	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 (see the sample table below). [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	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 3 and 4, begin to connect the appliances to the networks. Refer to the Collector Network Diagram below.

To cable the Collector Controller 10G appliance(s) to the switches:

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

To cable the Collector XA4 Node appliances to the switches:

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

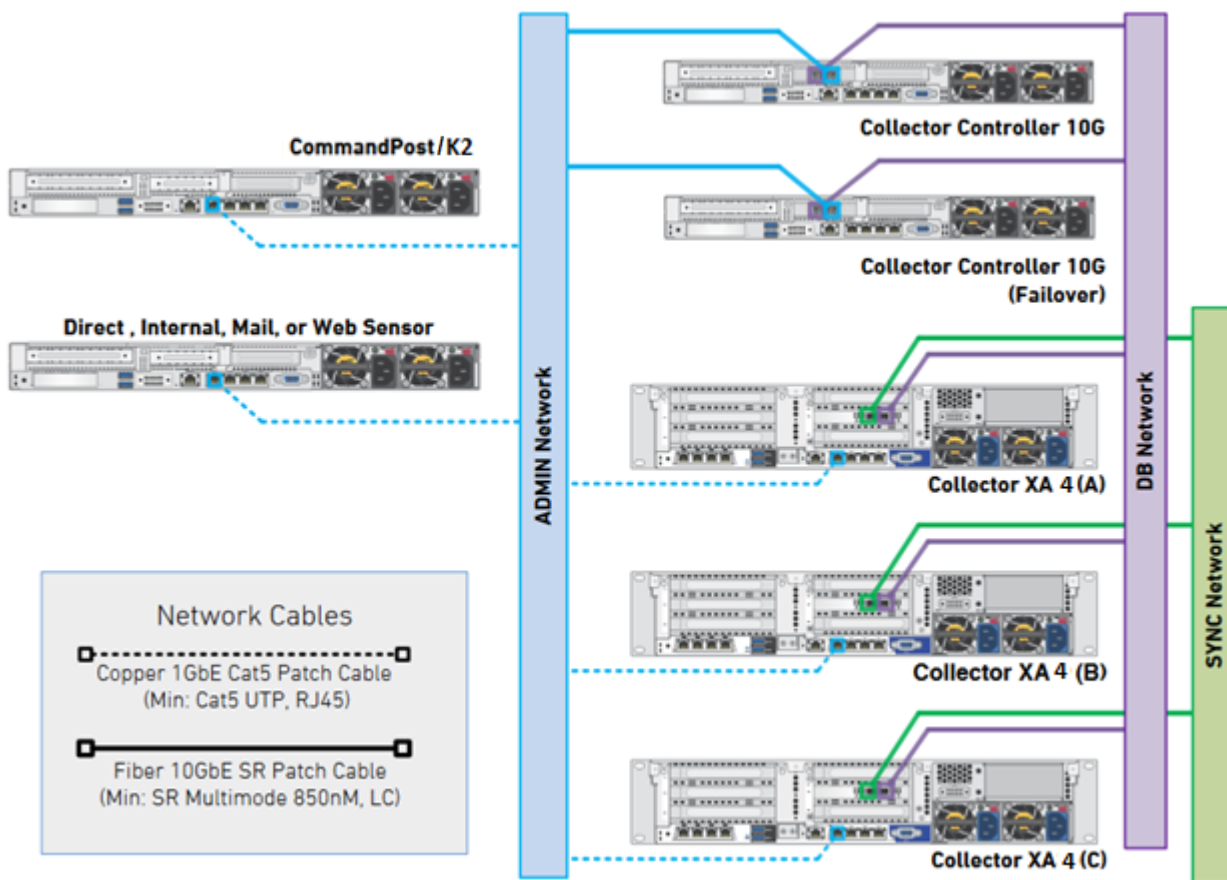
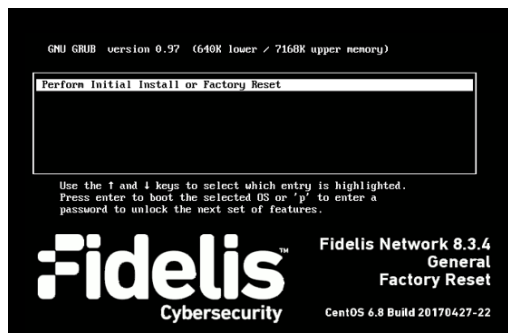


Figure 5: Collector Network Diagram

7. Appliance Network Configuration

1. Power on the appliance(s).
2. Connect to the component CLI using one of the following methods:

- **Via 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:

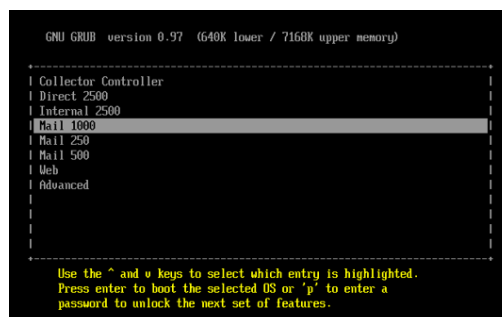


3. If you see the screen above, perform the following steps to apply the software. Otherwise skip to step 4.

- 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 Controller** (or **Collector XA** for cluster), 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.
5. Use these credentials at the login prompt:
 - user: **fidelis**
 - default password: **fidelispass**
6. Change to root using the default password.
7. From the command line, run:

```
/bin/bpctl_start
```

```
/bin/bypass_util all set_force_bypass off
```

8. Run the following to start the Fidelis Setup program:

```
/FSS/bin/setup
```

9. Within Setup, select **Network Settings**.
10. 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.

11. When complete, select **OK** to leave Setup.
12. From command line, run the following to reboot the system:

```
sudo /fss/bin/shutdown.pl --user admin --reboot
```
13. Repeat the previous steps for all appliances being added to the Collector cluster.
14. Use the PING command to verify connectivity between the XAs on their SYNC/eth2 interfaces.

8. Cluster Setup

On the Final Collector XA4 Appliance

If you have not completed setup for the XA4 appliances in section 7 above, or you are adding an XA4 appliance to the Collector, follow these steps:

1. Login via KVM console.
2. Use these credentials at the login prompt:
 - user: **fidelis**
 - default password: **fidelispass**
2. Change to root using the default password.
3. From the command line, run

```
/bin/bpctl_start
```

```
/bin/bypass_util all set_force_bypass off
```
4. From the command line, run: `/FSS/bin/setup`
5. Navigate to **Collector Settings**.
6. At the XA4 count, enter the number of XA4 appliances, and select **Ok**.
7. 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/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. This is not the fully qualified domain name of the Controller.
Component IP Address	Specify the IP address of the primary Collector Controller 10G appliance
Description	(optional) Specify a description, for example location, business unit, etc.

5. Click **Save**.
6. Register the Collector to the 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.

Register Collector Controller 10Gs with the 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, Mail, or Web 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 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 XA4 (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 XA4 (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 XA4 (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 XA4
		
Form Factor	1U rack-mount chassis SFF	2U rack-mount chassis SFF
CPU	Dual Intel Xeon Gold 6148 20-core 2.4 Ghz	Dual Intel Xeon Gold 6136 12-core 3.0 Ghz
Memory	128 GB ECC DDR4 2666Mhz	192 GB ECC DDR4 2666Mhz
Storage Capacity & Configuration	480 GB 2x SSD, RAID-1 (240GB)	480 GB 2x SSD, RAID-1(240GB) ----- 26.4 TB 22x HDD, RAID-10 (13.2TB)
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: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)	H: 8.73 cm (3.44 in) W: 44.54 cm (17.54 in) D: 67.94 cm (26.75 in)
Weight (appx.)	16.27 kg (35.86 lb)	24.5 kg (54 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: 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



Fidelis Direct 10G Appliance



(17Y) SPLR ID CAGE 0817V35HA61P



(1P) SFLR PART

FSS-10G-I



(S) SERIAL 2M261108K1

Country of Origin: USA

SYS-FHY600-200

Appliance SKU with:	System Type
FSS-CXA4-I FNH-CXA4-I	Collector XA
FSS-CC10G-I FNH-CC10G-I	Collector Controller

QSC_Fidelis_CHC_Rev-I_20190509