



QUICK START GUIDE

Fidelis Network[®] Collector Cluster

Rev-J

Collector Controller2 (HP DL360-G10) and
Collector XA2 (HP DL360-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 (e.g., Direct, Internal, Mail and Web Sensors) and stores it for ongoing analysis. A Fidelis Collector cluster of appliances consist of one or two Collector Controller(s) and typically three or more Collector XA database nodes.




Figure 1: Fidelis Network — Collector Controller (Rev-J)



Figure 2: Fidelis Network — Collector XA2 Appliance (Rev-J)

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) for Admin, DB, SYNC 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. 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 Controller2 Appliance

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

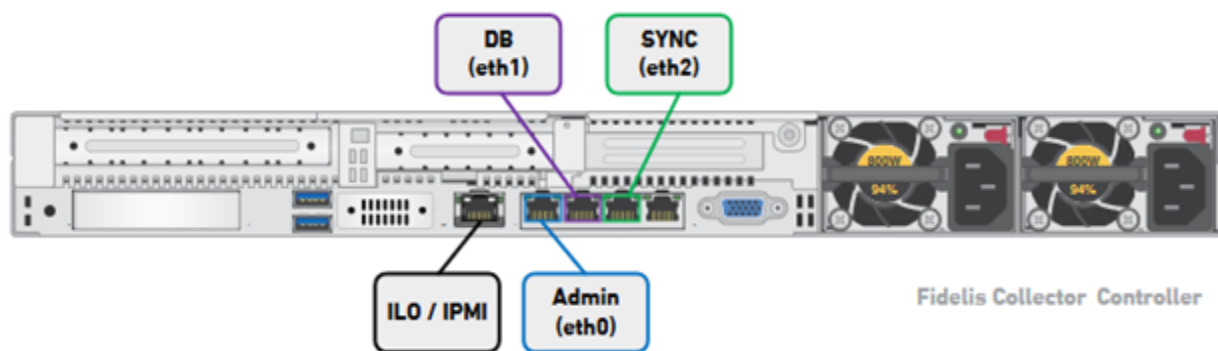


Figure 3: Network Port Assignments — Collector Controller (Rev-J)

Collector XA 2 Database Node

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

DB Net	GbE RJ45 (copper)	Cat 5 patch cable
SYNC net	GbE RJ45 (copper)	Cat 5 patch cable
iLO	GbE RJ45 (copper)	Cat 5 patch cable

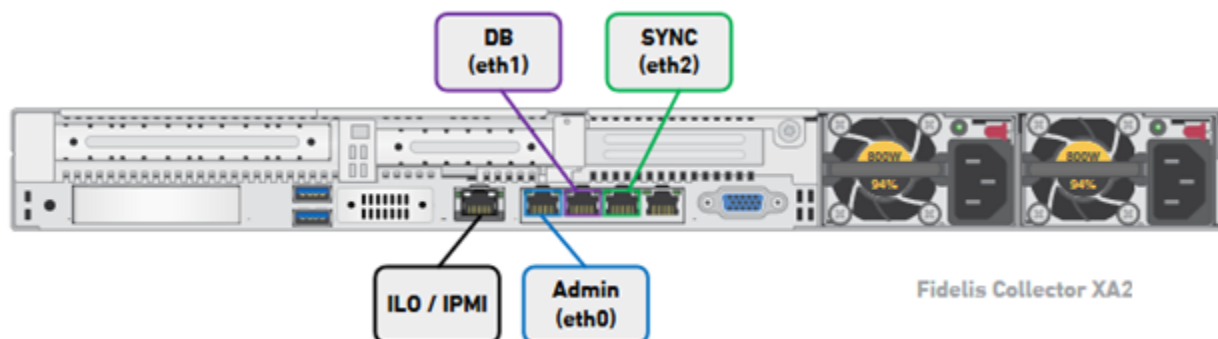


Figure 4: Network Port Assignments — Collector XA2 (Rev J)

4. Collector Networking Environment

The Collector components 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 may intersect.

Use the tables below to identify the count and type of switch ports necessary to support the number of Collector components 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 XA2 nodes to the CommandPost/K2.

Appliance	Switch Port Type	Qty.
Collector Controller	GbE - RJ45/Cat5+ (copper twisted pair)	1
Collector XA2	GbE - RJ45/Cat5+ (copper twisted pair)	1

DB Network

The DB Network allows communication between Collector Controller and Controller XA nodes. This network must be independent from other networks. Only IPv4 addresses are supported.

Appliance	Switch Port Type	Qty.
Collector Controller	GbE - RJ45/Cat5+ (copper twisted pair)	1
Collector XA2	GbE - RJ45/Cat5+ (copper twisted pair)	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	n/a	
Collector XA2	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 Controller	GbE - RJ45/Cat5+ (copper twisted pair)	1
Collector XA2	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. (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			
	Admin/eth0	DB/eth1	SYNC/eth2	iLO/IPMI
Interface				
Hostname (FQDN)	collector-xa1.organization.net.			
Static IP Address	10.1.2.3	192.168.1.3	172.16.1.3	10.2.3.3
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	10.1.2.1			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)			

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.

Appliance Network Cabling

Using the connectors and cables described in sections 3 and 4, begin to connect the appliances to the networks. Reference the Collector Network Diagram below.

To cable the Collector Controller 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. Optionally, connect the iLO port to the ADMIN (or ILO) switch port
4. Repeat for each Collector Controller.

To cable the Collector XA2 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. Optionally, connect the iLO port to the ADMIN (or ILO) switch port.
5. Repeat for each Collector XA2 component.

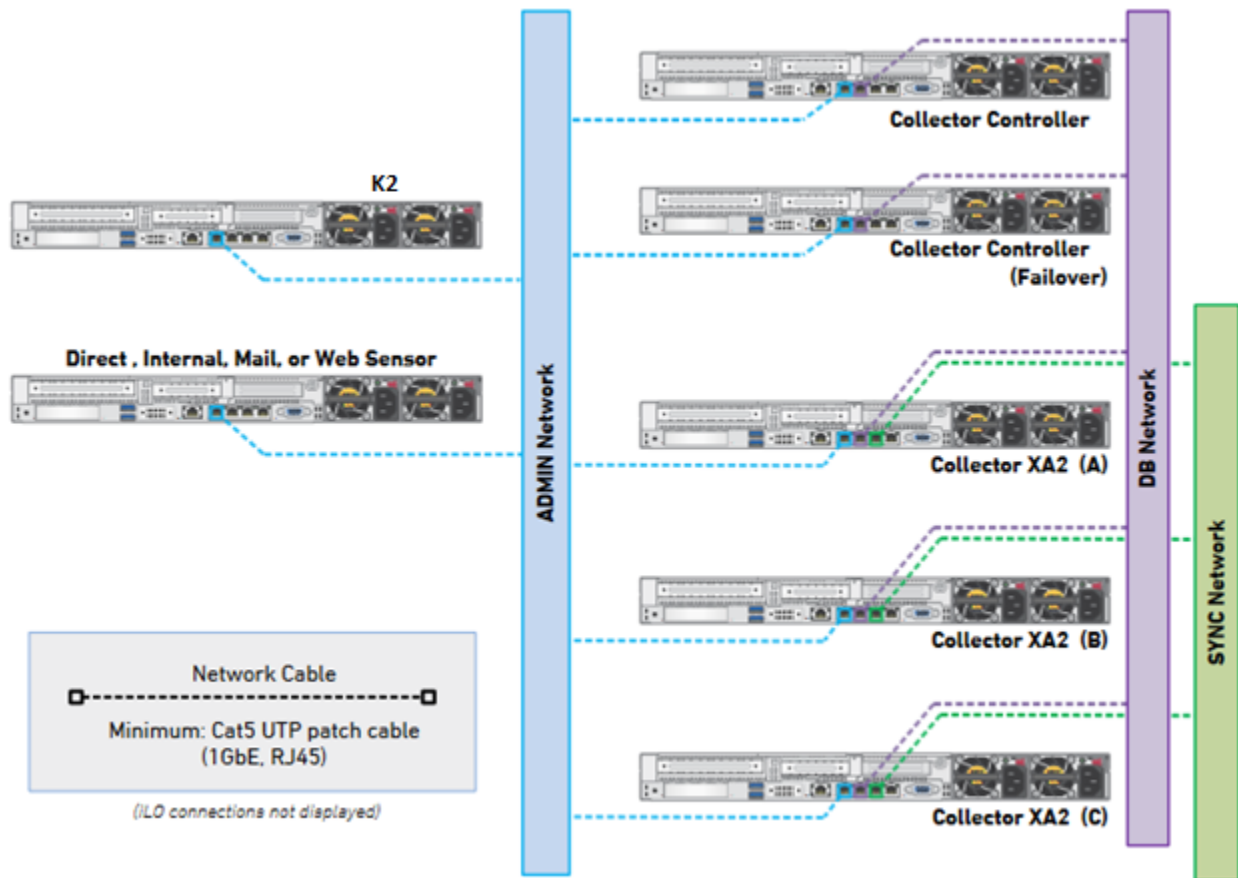
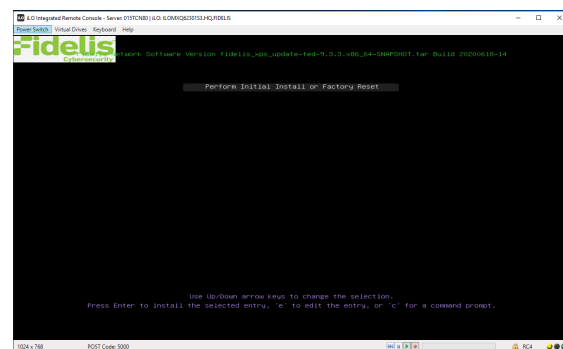


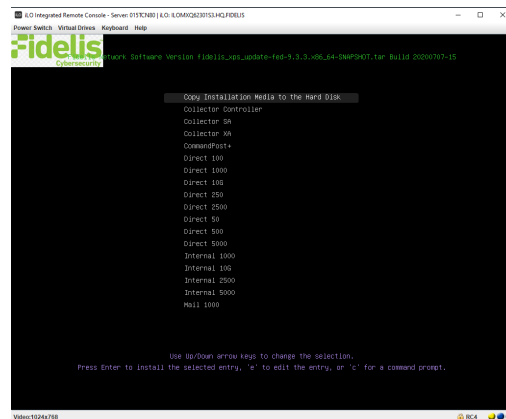
Figure 5: Collector Network Diagram

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](#).



4. Login into 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 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
```
11. Repeat steps for all appliances being added to the Collector cluster.
12. Use the PING command to verify connectivity between the XAs on their SYNC/eth2 interfaces.

8. Cluster Setup

On the Final Collector XA2 Component

If you have not completed setup for the XA2 components in section 6 above, or you are adding an XA2 component to the cluster, follow these steps:

1. On the last XA node of the cluster, log in to the appliance console as user fidelis.
2. Change user account to root:
su root
3. Start the Fidelis Setup program.
/FSS/bin/setup
4. Navigate to **Collector Settings**.
5. At the XA2 count, configure the number of XA2 appliances, and select **Ok**.
6. Review the list of IP addresses. Select **Confirm** if these are correct, else **Edit** to correct them.

9. Fidelis Network Integration

Register Collector Controller with CommandPost/K2

Note: If you are installing a failover set of Collector Controllers, register only the “primary” Collector Controller. Configure Collector Controller failover unit IP address in the Primary Controller’s configuration page within the CommandPost/K2 user interface.

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 Cluster. This is not the fully qualified domain name of the Controller.
Component IP Address	Specify the IP address of the primary Collector Controller2 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.

Link Collector Controller(s) 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, 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 (Primary)

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

Collector Controller (Failover)

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

Collector XA2 (A)

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

Collector XA2 (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 XA2 (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

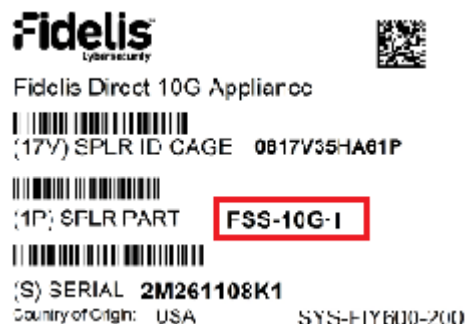
Component Configuration and Resources (Rev-J)

Enterprise Collector Cluster Hardware Specifications (Rev-J)		
	Collector Controller	Collector XA2
Storage Capacity & Configuration	300 GB 2x HDD in RAID-1	300 GB 2x HDD in RAID-1 1.2 TB (3.6TB) 6xHDD, RAID-10
CPU	Dual Intel Xeon Silver 4214 12/24 2.2 GHz	Dual Intel Xeon Gold 6234 8/16 3.2Ghz
Memory	64GB (ECC DDR4 2666Mhz)	128GB (ECC DDR4 2666Mhz)
Network Adapters	4x 1GbE (copper)	
Optional Network Adapters		
Out of Band Management	Integrated Lights Out (ILO) Management	
Performance Power Supply	Dual hot-swap 800w High Efficiency AC power supplies (80+ Platinum Certified)	Dual hot-swap 800w High Efficiency AC power supplies (80+ Platinum Certified)
Form Factor	1U Rack-mount chassis	
Dimensions	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)	
Weight	16.27 kg (35.86 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 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-CXA2-J FNH-CXA2-J	Collector XA

FSS-MAIL-WEB-CC2-J FNH-MAIL-WEB-CC2-J	Collector Controller
--	----------------------

QSC_Fidelis_CE_Rev-J_20200716