



Fidelis Network[®] Collector Appliances

Quick Start Guide

Rev-K Collector Controller (CC2) and Collector XA2
(HPE DL360 Gen10) Platforms

1. System Overview

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



Figure 1: Fidelis Network – Collector Controller (CC2) Appliance – Rev-K



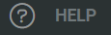
Figure 2: Fidelis Network – Collector XA2 Appliance – Rev-K

Collector Setup Checklist

✓	Fidelis Collector – 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 power source and region
	Ethernet cables (cat5e and optical) 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 software version 9.4.1 and later, the appliance type (Appendix C)

2. Documentation, Passwords, and Technical Support

Product Documentation

You can find Fidelis Network product documentation, appliance specifications, and instructions at <https://support.fidelissecurity.com> or through the  navigation item in the CommandPost user interface.

Appliance Default Passwords

System	Account	Default Password
SSH / Appliance Console	fidelis	fidelispass
CommandPost 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 Fidelis Cybersecurity Technical support at:

- Phone: +1.301.652.7190
- Toll-free in the US and Canada: 1.800.652.4020
- Email: support@fidelissecurity.com
- Web: <https://support.fidelissecurity.com>

3. Collector: Network Port and Cabling Requirements

You must connect each appliance to the various networks using 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 (CC2) Appliance

Port Label	Physical Connection Type (default)	Cable Type (minimum)
Admin (eth0)	GbE RJ45 (copper)	Cat 5e patch cable
DB (eth1)	GbE RJ45 (copper)	Cat 5e patch cable
iLO	GbE RJ45 (copper)	Cat 5e patch cable

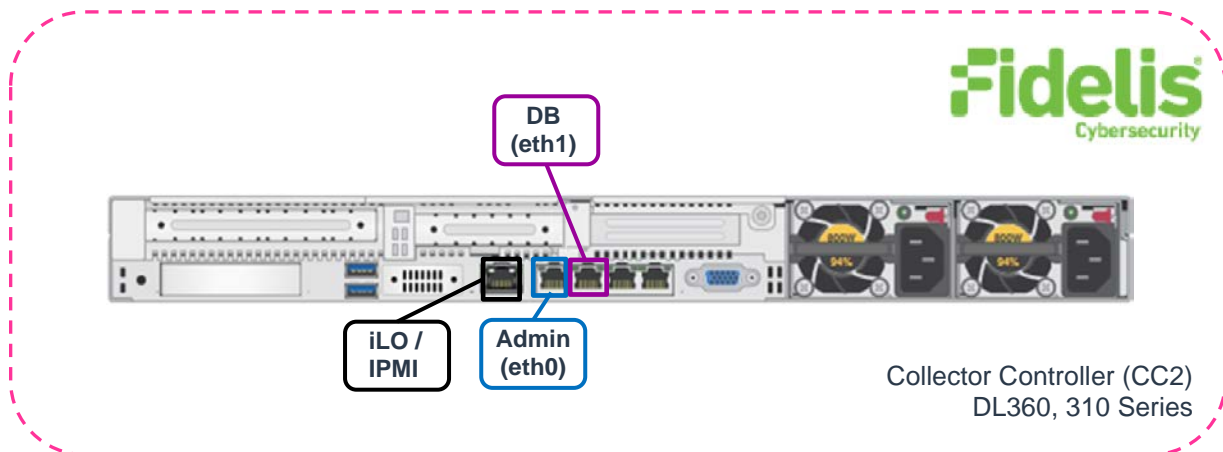


Figure 3: Rear Port Assignments – Collector Controller (CC2) (Rev-K)

Collector XA2 Database Node

Port Label	Physical Connection Type (default)	Cable Type (minimum)
Admin (eth0)	GbE RJ45 (copper)	Cat 5e patch cable
DB (eth1)	GbE RJ45 (copper)	Cat 5e patch cable
SYNC (eth2)	GbE RJ45 (copper)	Cat 5e patch cable
iLO	GbE RJ45 (copper)	Cat 5e patch cable

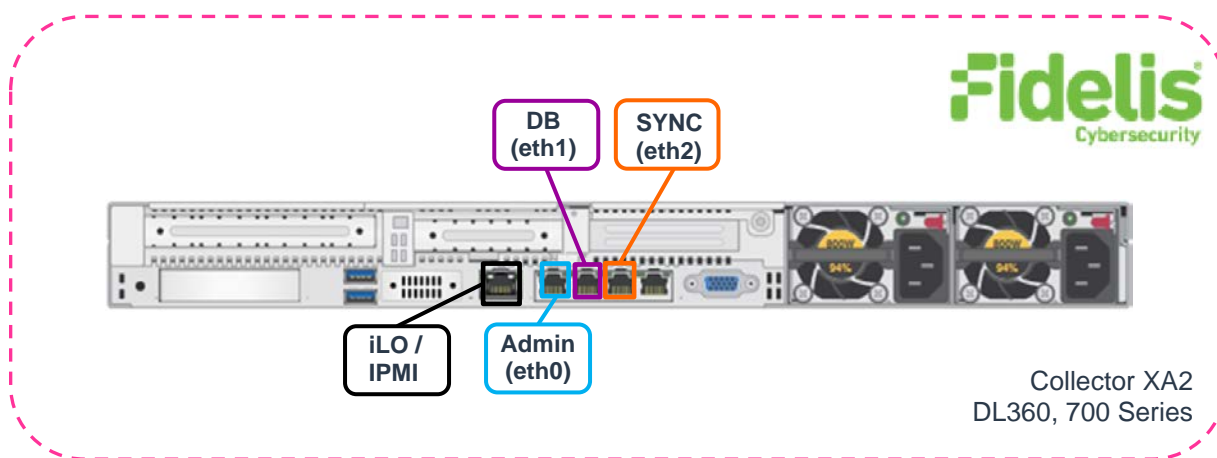


Figure 4: Rear Port Assignments – Collector XA2 (Rev-K)

4. Collector Networking Environment

The Collector appliances use multiple networks for service and inter-node communication. You can deploy the Admin network, DB network, and SYNC network 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. The Admin and iLO 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.

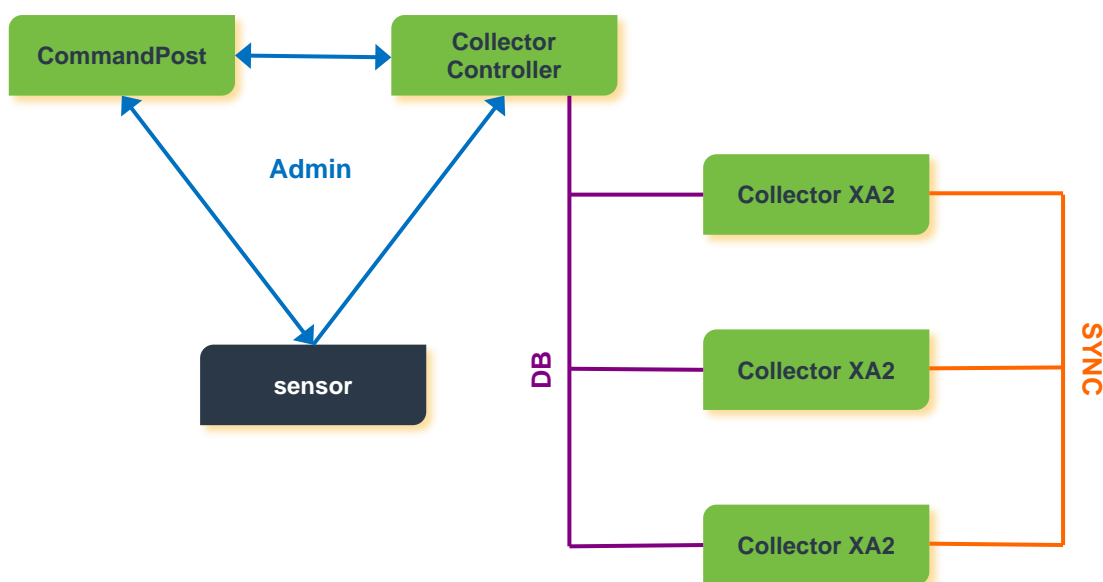


Figure 5: Independent networks: Admin, DB, and SYNC

Admin Network

The Admin network connects the Collector Controller to the Fidelis sensors and CommandPost systems. Optionally, you can connect Collector XA2 nodes to the CommandPost.

Appliance	Switch Port Type	Qty
Collector Controller (CC2)	GbE Copper RJ45 port	1
Collector XA2	GbE Copper RJ45 port	1

DB Network

The DB network allows communication between the Collector Controller and the Collector XA2 nodes. This network *must* be independent from other networks. You must use IPv4 addressing only.

Appliance	Switch Port Type	Qty
Collector Controller (CC2)	GbE Copper RJ45 port	1
Collector XA2	GbE Copper RJ45 port	1

SYNC Network

The SYNC network provides transport for database node synchronization. This network *must* be independent from other networks. You must use IPv4 addressing only.

Appliance	Switch Port Type	Qty
Collector Controller (CC2)	n/a	
Collector XA2	GbE Copper RJ45 port	1

iLO / IPMI Network

The iLO / IPMI network is an optional network for remote/out-of-band server administration.

Appliance	Switch Port Type	Qty
Collector Controller (CC2)	GbE Copper RJ45 port	1
Collector XA2	GbE Copper RJ45 port	1

5. Appliance – Logical Network Configuration

You must assign logical network information to each physical connection. Build a table of the logical information for each appliance (sample below) that you can reference during configuration. [Appendix A](#) has a worksheet you can use.

Sample Network Configuration Table: Collector Controller (CC2)

Network Setting	Assignments		
Interface	Admin (eth0)	DB (eth1)	iLO / IPMI
Hostname (FQDN)	collector-controller.organization.net		
Static IP Address	10.1.2.3	192.168.1.3	10.2.3.3
Subnet Mask	255.255.255.0	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	pool.ntp.org		
Time Zone	UTC (+0)		

Sample Network Configuration Table: Collector XA2

Network Setting	Assignments			
Interface	Admin (eth0)	DB (eth1)	SYNC (eth2)	iLO / IPMI
Hostname (FQDN)	collector-xa.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			
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. Ensure that the installation environment is within the operating temperature of the appliance. See [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 requirements.

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 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 a Collector XA2 node appliance to the switches:

1. Optionally, 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 XA2.

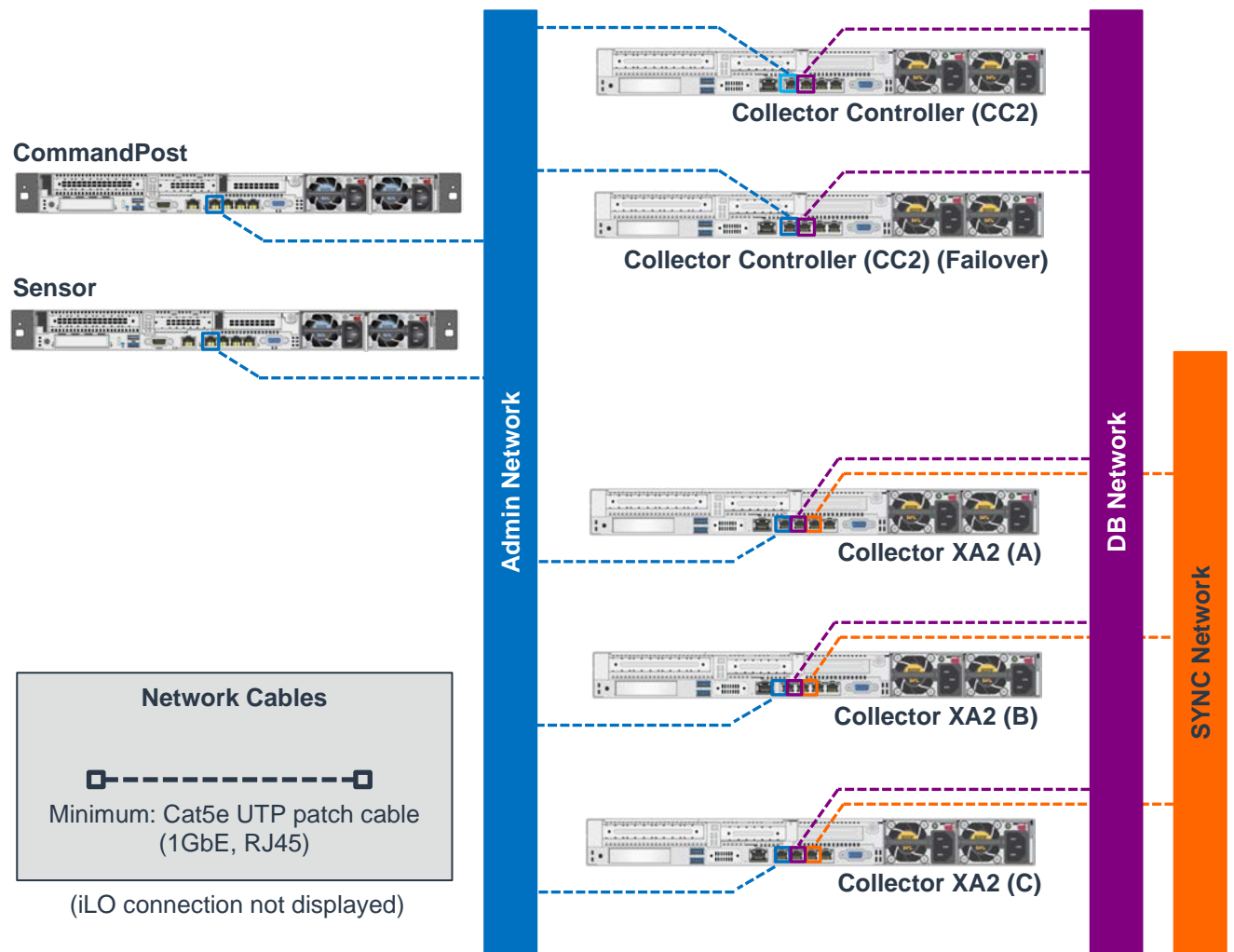


Figure 6: Collector Network Diagram

7. Appliance Network Configuration

Start the Appliance Network Configuration

1. Power on the appliance(s).
2. Connect to the component CLI using one of the following methods:
 - Via KVM Console, see [Option 1: Connect to the Component CLI Using KVM Console](#)
 - Via iLO, see [Option 2: Connect to the Component CLI Using iLO](#)

Option 1: Connect to the Component CLI Using KVM Console

1. Connect a keyboard and monitor to the appliance.
2. Continue with [Complete the Appliance Network Configuration](#).

Option 2: Connect to the Component CLI Using iLO

iLO supports DHCP by default. If you need a static IP address, before performing this procedure, first follow [Configuring iLO to Use a Static IP Address](#).

1. Log into the iLO console:

`https://<IP address>`

where <IP address> is the iLO IP address

2. Specify the credentials:
 - Username - Administrator
 - Password - A random eight-character string
 - DNS name - ILOXXXXXXXXXXXX, where the X characters represent the server serial number.

The iLO firmware is configured with a default username, password, and DNS name. The default information is on the serial label pull tab attached to the server that contains the iLO management processor. Use these values to access iLO remotely from a network client by using a web browser.

3. In the iLO web interface, navigate to **iLO Integrated Remote Console**.
4. Select **Power & Thermal**.
5. Click **Reset**.

The system shuts down and restarts. For Fidelis Network appliances version 9.4.1 or later, a screen similar to below is displayed. If you do not see this screen, contact Fidelis Customer Support.

6. Continue with [Complete the Appliance Network Configuration](#).

Configuring iLO to Use a Static IP Address

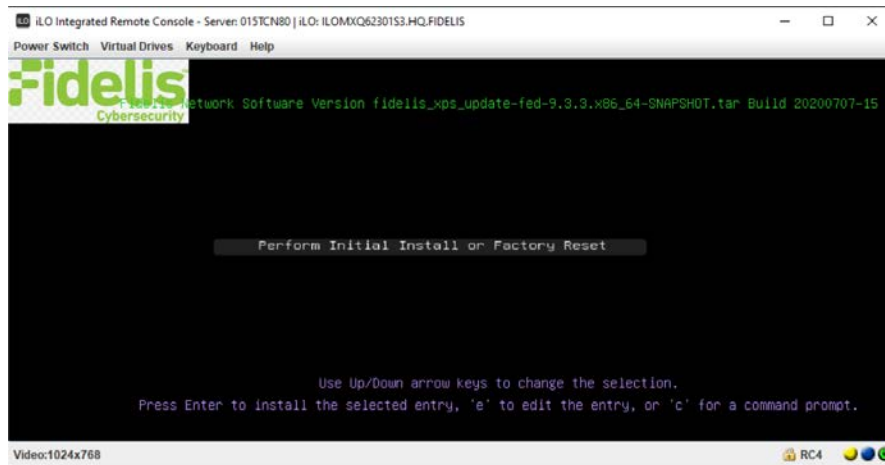
Use this procedure only if you want to connect to the component CLI using iLO and you need a static IP address. Note that iLO supports DHCP by default.

1. Directly attach an ethernet cable from a client system, such as a laptop to the iLO port on the appliance.
2. Restart the machine.
3. Press F9 in the server POST screen.
The UEFI System Utilities start.
4. Click **System Configuration**.
5. Click **iLO 5 Configuration Utility**.
6. Disable DHCP:
 - a. Click **Network Options**.
 - b. Select **OFF** in the **DHCP Enable** menu.
The **IP Address**, **Subnet Mask**, and **Gateway IP Address** boxes become editable. When DHCP Enable is set to **ON**, you cannot edit these values.
7. Enter values in the **IP Address**, **Subnet Mask**, and **Gateway IP Address** boxes. (See [Section 5 / Appendix A](#)).
8. To save the changes and exit, press F12.
The iLO 5 Configuration Utility prompts you to confirm that you want to save the pending configuration changes.
9. To save and exit, click **Yes - Save Changes**.
The iLO 5 Configuration Utility notifies you that iLO must be reset in order for the changes to take effect.
10. Click **OK**.
iLO resets, and the iLO session is automatically ended. You can reconnect in approximately 30 seconds.
11. Resume the normal boot process:
 - a. Start the iLO remote console.
The iLO 5 Configuration Utility is still open from the previous session.
 - b. Press ESC several times to navigate to the System Configuration page.
 - c. To exit the System Utilities and resume the normal boot process, click **Exit** and resume system boot.

iLO is configured to use a static IP address. Continue with [Option 2: Connect to the Component CLI Using iLO](#).

Complete the Appliance Network Configuration

1. After connecting using either KVM Console or iLO, you should see this screen for Fidelis Network appliances version 9.4.1 or later.



If you do not see the screen above, contact [Fidelis Technical Support](#).

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



3. Use the Up and Down arrow keys to select the system type **Collector Controller** or **Collector XA**, 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*. The system will automatically reboot.

4. 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 the following credentials at the login prompt. You will be required to change the password immediately.
 - **user:** fidelis
 - **default password:** fidelisspass

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

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

You will be prompted for the fidelis password.

7. With 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 ([Appendix A](#)).
 - When complete, return to the top menu.
9. When complete, select **OK** to leave Setup.
10. From the 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 XA nodes on their SYNC (eth2) interfaces.

8. Cluster Setup – For the Final Collector XA2 Appliance

If you have not completed setup for the Collector XA2 appliances, follow the steps in [section 7](#) above.

For the final Collector XA2 appliance or if you are adding and additional Collector XA2 appliance, follow these steps:

1. Log into the appliance console as user fidelis.
2. Change to root using the default password.

`su root`
3. Run the following to start the Fidelis Setup program:

`sudo /FSS/bin/setup`
4. Navigate to **Collector Settings**.
5. At the XA2 count, enter the number of Collector XA2 appliances, and select **Ok**.
6. Review the list of IP addresses. Select **Confirm** if these are correct or edit **Edit** to make corrections.

9. Fidelis Network Integration

Register Collector Controller (CC2) with CommandPost

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 user interface.

1. From the CommandPost user interface, navigate to: **Administration > Components**
2. Click **Add Component**.
3. Fill in the Add New Component popup:

Component Type	Select Collector
Name	Specify a "friendly" name for the Controller. This is <i>not</i> the fully qualified domain name of the Controller.
Description	Optionally, specify a description, for example, a location, business unit, etc.
IP Address	Specify the IP address of the Admin interface of the Controller appliance.

4. Click **Add Component**.
5. To register the Collector Controller to the CommandPost, click the  and select **Register**.

Accept the End User License Agreement (EULA). The CommandPost begins communicating with the Collector at the specified IP address.

Link Collector Controller (CC2) to Fidelis Sensors

1. From the CommandPost user interface, navigate to: **Administration > Components**
2. For each sensor:

- a. In the row for the sensor, click the  icon.

The system displays the Configure Component popup.

- b. In the Configure Component popup, select **Direct**, **Internal**, **Mail**, or **Web** from the navigation on the left (based on the type of sensor).
- c. Select the **Advanced** or **Metadata** tab.
- d. In the **Send Metadata to Collector** field, select the Collector from the list.

Appendix A: Network Configuration Worksheet

Collector Controller 10G (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 10G (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 XA4 (A)

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



Collector XA4 (B)

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

Collector XA4 (C)

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				

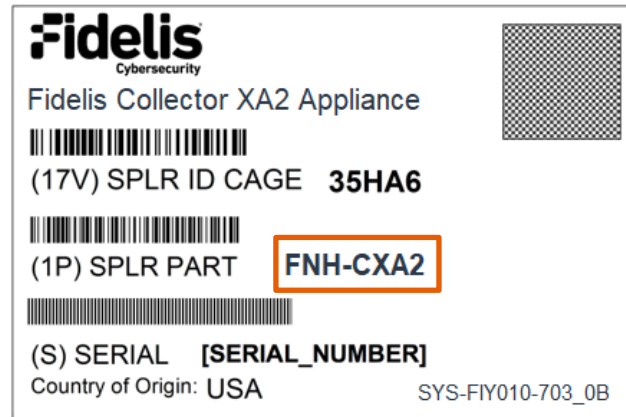
Appendix B: System Specifications

	Collector Controller (CC2) (Rev-K)	Collector XA2 (Rev-K)
		
Form Factor	1U rack-mount chassis SFF	1U rack-mount chassis SFF
CPU	Dual Intel Xeon Silver 4214R 12/24-core 2.4Ghz	Single Intel Xeon Gold 6246R 16-core 3.4Ghz
TPM	TPM 2.0	TPM 2.0
Memory	64GB ECC DDR4 2933Mhz	128 GB ECC DDR4 2933Mhz
Storage Capacity & Configuration	2x HDD 300 GB RAID-1 (300 GB Effective)	2x HDD 300 GB RAID-1 6x HDD 1.2 TB RAID-10 (3.6 TB Effective)
Network Adapters (Default Config)	4x 1GbE	4x 1GbE
Out-of-Band Management	Integrated Lights Out Management (iLO)	Integrated Lights Out Management (iLO)
Power Supply	Dual hot-swap 800W High Efficiency AC power supplies	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)	H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)
Weight (approx.)	16.27 kg (35.86 lb)	16.27 kg (35.86 lb)
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)	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 versions 9.4.1 and later, the table below shows the software to apply based on the appliance SKU. (Note the SKU typically starts with “FNH”). You can find the SKU in the following locations:

- Appliance lid UID decal (see sample on right)
- Shipping carton decal (see sample on right)
- Packing list
- Purchase order
- Maintenance certificate



Appliance SKU	System Type
FNH-CXA2	Collector XA2
FNH-Mail-Web-CC2-J	Collector Controller (CC2)

QSG_Collector-Cluster_Rev-K_20221201

Source: Technical Support

About Fidelis Cybersecurity

Fidelis Cybersecurity, the industry innovator in Active XDR and proactive cyber defense solutions, safeguards modern IT environments with unparalleled detection, deception, response, cloud security, and compliance capabilities. We offer full visibility across hybrid environments via deep, dynamic asset discovery, multi-faceted context, and risk assessment. These features help minimize attackable surface areas, automate exposure prevention, threat detection, and incident response, and provide the context, accuracy, speed, and portability security professionals need to find and neutralize adversaries earlier in the attack lifecycle. Fidelis Cybersecurity is dedicated to helping clients become stronger and more secure. Fidelis is trusted by many top commercial, enterprise, and government agencies worldwide. For more information, please visit www.fidelissecurity.com

