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 consist of one or two Collector Controller(s) and typically three or more Collector XA database nodes.

![Figure 1: Fidelis Network — Collector Controller (Rev-I)](image1)

![Figure 2: Fidelis Network — Collector XA2 Appliance (Rev-I)](image2)

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.

<table>
<thead>
<tr>
<th>System</th>
<th>Account</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH / Appliance Console</td>
<td>fidelis</td>
<td>fidelispass</td>
</tr>
<tr>
<td>CommandPost/K2 user interface</td>
<td>admin</td>
<td>system</td>
</tr>
<tr>
<td>iLO</td>
<td>administrator</td>
<td><em>(printed on label, top of server)</em></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Check</th>
<th>Fidelis Network Sensor – Appliance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Appropriate rack space, power, and cooling (<a href="#">Appendix B</a>)</td>
</tr>
<tr>
<td></td>
<td>Rack tools, rails, and connectors</td>
</tr>
<tr>
<td></td>
<td>Keyboard and video monitor / KVM switch for temporary appliance setup</td>
</tr>
<tr>
<td></td>
<td>Power cables — two per appliance, appropriate for power source and region</td>
</tr>
<tr>
<td></td>
<td>Ethernet cables (cat5) for Admin, DB, SYNC and iLO ports (<a href="#">Section 3</a>)</td>
</tr>
<tr>
<td></td>
<td>Network switches with enough physical ports (<a href="#">Section 4</a>)</td>
</tr>
<tr>
<td></td>
<td>Logical network information: IP addresses, hostnames (<a href="#">Section 5, Appendix A</a>)</td>
</tr>
<tr>
<td></td>
<td>For Fidelis Network Software version 9.0.5 and later, the appliance system type (<a href="#">Appendix C</a>)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port Label</th>
<th>Physical Connection Type (default)</th>
<th>Cable Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>GbE RJ45 (copper)</td>
<td>Cat 5 patch cable</td>
</tr>
<tr>
<td>DB Net</td>
<td>GbE RJ45 (copper)</td>
<td>Cat 5 patch cable</td>
</tr>
<tr>
<td>iLO</td>
<td>GbE RJ45 (copper)</td>
<td>Cat 5 patch cable</td>
</tr>
</tbody>
</table>

![Figure 3: Network Port Assignments — Collector Controller (Rev-I)](image-url)
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 can 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.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Switch Port Type</th>
<th>Qty.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Controller</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
<tr>
<td>Collector XA2</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
</tbody>
</table>
**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.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Switch Port Type</th>
<th>Qty.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Controller</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
<tr>
<td>Collector XA2</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Switch Port Type</th>
<th>Qty.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Controller</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Collector XA2</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
</tbody>
</table>

**iLO / IPMI Network**
Optional network for remote/out-of-band server administration.

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Switch Port Type</th>
<th>Qty.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collector Controller</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
<tr>
<td>Collector XA2</td>
<td>GbE - RJ45/Cat5+ (copper twisted pair)</td>
<td>1</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Admin/eth0</td>
</tr>
<tr>
<td>Hostname (FQDN)</td>
<td>collector-xa1.organization.net.</td>
</tr>
<tr>
<td>Static IP Address</td>
<td>10.1.2.3</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.252.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.1.2.1</td>
</tr>
<tr>
<td>Proxy Server</td>
<td>10.5.6.7</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>8.8.4.4, 8.8.8.8</td>
</tr>
<tr>
<td>NTP Servers</td>
<td>pool.ntp.org.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>UTC (+0)</td>
</tr>
</tbody>
</table>

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**.
      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:
   ```bash
   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
    ```

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 7 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:

<table>
<thead>
<tr>
<th>Component Type</th>
<th>Specify Collector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Name</td>
<td>Specify a “friendly” name for the Collector Cluster. This is not the fully qualified domain name of the Controller.</td>
</tr>
<tr>
<td>Component IP Address</td>
<td>Specify the IP address of the primary Collector Controller appliance</td>
</tr>
<tr>
<td>Description</td>
<td>(optional) Specify a description, for example location, business unit, etc.</td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Admin/eth0</td>
</tr>
<tr>
<td></td>
<td>DB/eth1</td>
</tr>
<tr>
<td></td>
<td>iLO/IMM</td>
</tr>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Static IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Proxy Server</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td></td>
</tr>
<tr>
<td>NTP Servers</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
</tbody>
</table>

#### Collector Controller (Failover)

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Admin/eth0</td>
</tr>
<tr>
<td></td>
<td>DB/eth1</td>
</tr>
<tr>
<td></td>
<td>iLO/IMM</td>
</tr>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Static IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Proxy Server</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td></td>
</tr>
<tr>
<td>NTP Servers</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
</tbody>
</table>
# Collector XA2 (A)

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Admin/eth0</td>
</tr>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Static IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Proxy Server</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td></td>
</tr>
<tr>
<td>NTP Servers</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
</tbody>
</table>

# Collector XA2 (B)

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Admin/eth0</td>
</tr>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Static IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Proxy Server</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td></td>
</tr>
<tr>
<td>NTP Servers</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
</tbody>
</table>
### Collector XA2 (C)

<table>
<thead>
<tr>
<th>Network Setting</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Admin/eth0</td>
</tr>
<tr>
<td></td>
<td>DB/eth1</td>
</tr>
<tr>
<td></td>
<td>SYNC/eth2</td>
</tr>
<tr>
<td></td>
<td>iLO/IMM</td>
</tr>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Static IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Proxy Server</td>
<td></td>
</tr>
<tr>
<td>DNS Servers</td>
<td></td>
</tr>
<tr>
<td>NTP Servers</td>
<td></td>
</tr>
<tr>
<td>Time Zone</td>
<td></td>
</tr>
</tbody>
</table>

### Appendix B: System Specifications

#### Component Configuration and Resources (Rev-I)

**Collector Cluster Hardware Specifications (Rev-I)**

<table>
<thead>
<tr>
<th></th>
<th>Collector Controller</th>
<th>Collector XA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Capacity &amp;</td>
<td>Integrated 6Gbps hardware RAID</td>
<td>Integrated 6Gbps hardware RAID</td>
</tr>
<tr>
<td>Configuration</td>
<td>• 480GB* on 2x SSD in RAID-1 (240GB)</td>
<td>• 3.6 TB* on 6x HDD in RAID-10 (DB)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 480GB* on 2x SSD in RAID-1 , 240 GB (OS)</td>
</tr>
<tr>
<td>CPU</td>
<td>Dual Intel Xeon Silver 4114 - 2.2Ghz 10c v3 (20 cores total)</td>
<td>Dual - Intel Gold 6134 3.2Ghz 8c (16 cores total)</td>
</tr>
<tr>
<td>Memory</td>
<td>64GB (ECC DDR4 2666Mhz)</td>
<td>128GB (ECC DDR4 2666Mhz)</td>
</tr>
<tr>
<td>Network Adapters</td>
<td>4x 1GbE (copper)</td>
<td></td>
</tr>
<tr>
<td>Optional Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adapters</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out of Band Management</td>
<td>Integrated Lights Out (ILO) Management</td>
<td></td>
</tr>
<tr>
<td>Performance Power</td>
<td>Dual hot-swap 800w High Efficiency AC power supplies (80+ Platinum Certified)</td>
<td>Dual hot-swap 800w High Efficiency AC power supplies (80+ Platinum Certified)</td>
</tr>
<tr>
<td>Supply</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Form Factor</td>
<td>1U Rack-mount chassis</td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td>H: 4.29 cm (1.69 in) W: 43.46 cm (17.11 in) D: 70.7 cm (27.83 in)</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>16.27 kg (35.86 lb)</td>
<td></td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>10° to 35°C (50° to 95°F) at sea level</td>
<td></td>
</tr>
</tbody>
</table>

*Raw capacity listed. A portion of the storage capacity is dedicated to the operating system.
# 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

<table>
<thead>
<tr>
<th>Appliance SKU with:</th>
<th>System Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSS-CXA2-I</td>
<td>Collector XA</td>
</tr>
<tr>
<td>FNH-CXA2-I</td>
<td>Collector XA</td>
</tr>
<tr>
<td>FSS-MAIL-WEB-CC2-I</td>
<td>Collector Controller</td>
</tr>
<tr>
<td>FNH-MAIL-WEB-CC2-I</td>
<td>Collector Controller</td>
</tr>
</tbody>
</table>

QSC_Fidelis_CE_Rev-l_20190509