

TM



QUICK START GUIDE

**Fidelis Network™
CommandPost+
Appliances**

Rev-H

CommandPost (HP DL360-G9) Platforms


1. System Overview

The Fidelis CommandPost+ appliance is the central component for command and control of Fidelis Network components. With CommandPost+, you create and edit sensor policies, craft metadata analytics and automation, and view alerts from connected sensor and Collector components.



Figure 1: Fidelis Network: CommandPost+ 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>

CommandPost 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 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) |

3. CommandPost: 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.

CommandPost Appliance

| Port Label | Physical Connection Type (default) | Cable Type (minimum) |
|------------|------------------------------------|----------------------|
| Admin | GbE RJ45 (copper) | Cat 5 patch cable |
| ILO | GbE RJ45 (copper) | Cat 5 patch cable |

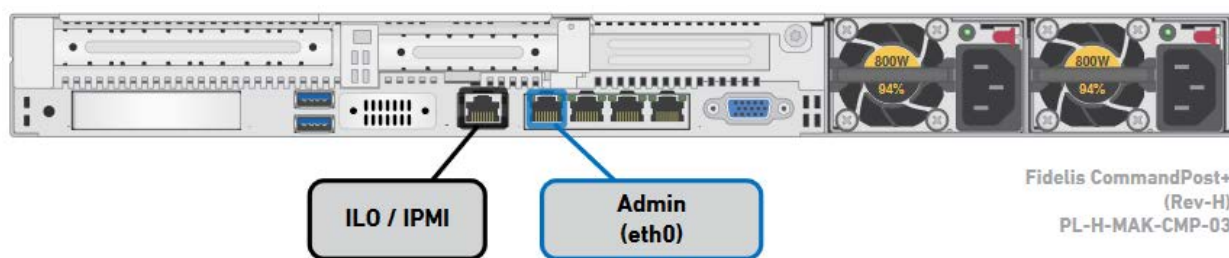


Figure 2: CommandPost+ Rear Port Assignments (Rev-H)

4. CommandPost Networking Environment

The CommandPost+ appliances use the Admin network for service and inter-node communication, and offer the IPMI/ILO interface for optional out-of-band management of the appliance.

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 CommandPost to the Fidelis Network sensors, Collectors, and Sandbox components.

| Appliance | Switch Port Type | Qty. |
|--------------|-------------------|------|
| CommandPost+ | GbE RJ45 (copper) | |

ILO / IPMI Network

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

| Appliance | Switch Port Type | Qty. |
|--------------|-------------------|------|
| CommandPost+ | GbE RJ45 (copper) | |

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 reference this table multiple times during the cluster setup. Appendix A has a worksheet you may use.

Sample Network Configuration Table

| Network Setting | Assignments | |
|-------------------|--------------------------------|---------------|
| Interface: | Admin/eth0 | iLO/IMM |
| Hostname (FQDN) | commandpost1.organization.net. | |
| Static IP Address | 10.1.2.3 | 10.2.3.4 |
| Subnet Mask | 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 | 0.pool1.ntp.org. | |
| Time Zone | UTC (+0) | |

6. Appliance Installation

Rack Installation

Install each appliance in an location with 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.

Cable the **CommandPost+** appliance(s) to the switches:

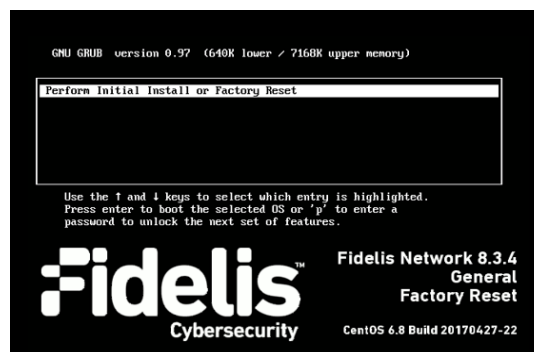
1. Connect **Admin (eth0)** port to the ADMIN switch port.
2. Connect the **iLO port** to the ADMIN (or ILO) switch port (optional).

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 “CommandPost”, and press Enter.

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



4. Use these credentials at the login prompt:
 - user: **fidelis**
 - default password: **fidelispass**
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**

8. Fidelis Licensing — “Air Gap” and “No Feedback” Installations

If your Fidelis Network products are deployed with “Air Gap” or “No Feedback” licenses, you must install them with a license key. 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 / Console / 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 to start 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, Fidelis CommandPost+ is operational and ready for additional Fidelis Network components.

Appendix A: Network Configuration Worksheet

CommandPost+

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

Appendix B: System Specifications

| | CommandPost+ (Rev-H) | CommandPost+ (Rev-G) |
|-----------------------------------|---|---|
| |  |  |
| Form Factor | 1U rack-mount chassis, SFF | 1U rack-mount chassis, SFF |
| CPU | Dual Intel Xeon v3 8-core 2.6 Ghz | 2x Intel Xeon v2 6-core 2.6 Ghz |
| Memory | 96 GB ECC DDR4 2133Mhz | 96 GB ECC DDR3 1600Mhz |
| Storage Capacity & Configuration | 3 TB 6x HDD, RAID-5 | 3 TB 6x HDD, RAID-5 |
| Network Adapters (Default Config) | 4x 1GbE | 4x 1GbE |
| Out of Band Management | Integrated Lights Out Management (ILO) | Integrated Management Module II (IMM2) |
| Power Supply | Dual hot-swap 800W High Efficiency AC power supplies | Dual hot-swap 550W High Efficiency AC power supplies |
| Dimensions | H: 4.32 cm (1.7 in) W: 43.47 cm (17.1 in) D: 69.85 cm (27.5 in) | W: 440 mm (17.3 in) D: 734 mm (28.9 in) H: 43 mm (1.7 in) |
| Weight (appx.) | 15.6 kg (35.5 lb) | 15.6 kg (35.5 lb) |
| Operating Temperature | 10° to 35°C (50° to 95°F) at sea level | 5°C to 40°C (41°F to 104°F) Altitude: 0 to 915 m (3,000 ft) |

QSC_Fidelis_CP_20170524