Fidelis Network® Sandbox

Quick Start Guide
Rev-K (HPE DL360 Gen10) Platforms

1. System Overview

The Fidelis Sandbox appliance is a 1U appliance that provides users with the ability to submit suspicious files from Fidelis Network sensor alerts to a sandbox for runtime analysis. This capability is not a replacement for any of the other Fidelis detection capabilities already in place, but rather complements them by providing additional information and detections that would not have been possible through other analysis methods. For files and URLs that are determined to be heuristically suspicious, the sandbox appliance can be used to confirm the suspicious or malicious nature of these files. Files already determined to be suspicious can also be sent to the sandbox for generation of execution forensics. In either of these cases, the execution forensics returned by the sandbox appliance can be used for further analysis of events in your network.

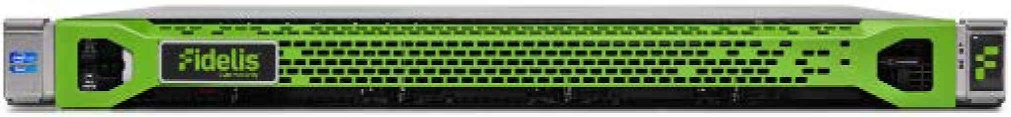


Figure 1: Fidelis Network On-Premises Sandbox Appliance (Rev-K)

Sandbox Setup Checklist

✓	Fidelis CommandPost – 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) for Admin, Routed, and iLO ports (Section 3)
	Network switches with enough physical ports (Section 4)
	Logical network information: IP addresses, hostnames (Section 5, Appendix A)

2. Documentation, Passwords, and Technical Support

Product Documentation

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

Appliance Default Passwords

System	Account	Default Password
Secure Shell (SSH)	fidelis	fidelispass
Admin Secure Shell (SSH)	admin	fidelispass
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. Sandbox Appliance Network Port and Cabling Requirements

You must connect each appliance to the appropriate networks with the proper cabling. The table below describes the physical connection and cable type associated with each port.

Fidelis Sandbox Appliance

Port Label	Physical Connection Type (default)	Cable Type
Admin (eno1)	GbE RJ45 (copper)	Cat 5e patch cable
Routed (eno3)	GbE RJ45 (copper)	Cat 5e patch cable
iLO	GbE RJ45 (copper)	Cat 5e patch cable

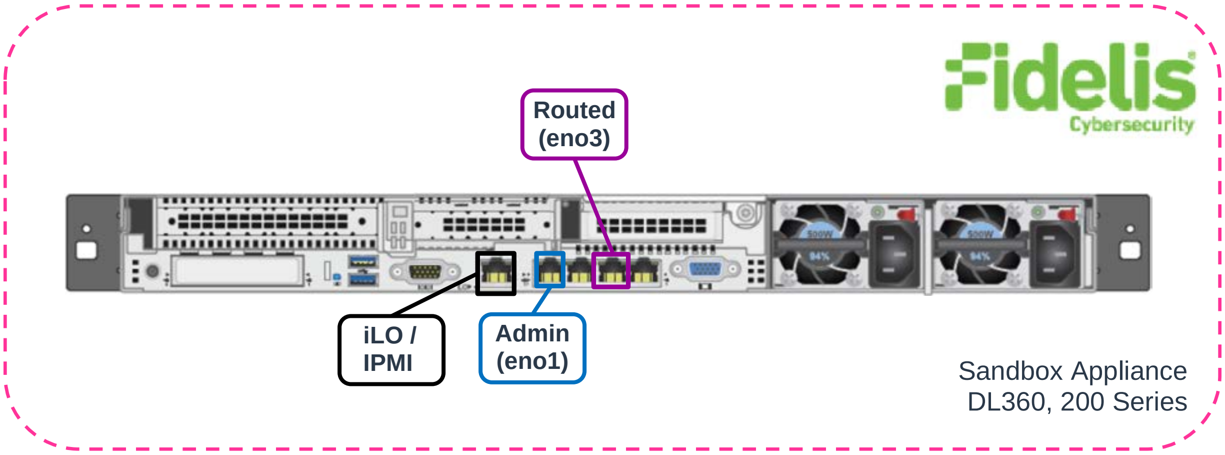


Figure 2: Sandbox Appliance Rear Port Assignments (Rev-K)

4. Sandbox Appliance Networking Environment

The Sandbox appliance may use multiple networks for full operation. The figure above shows the port layout on the Sandbox appliance. The Admin and Routed switches or VLANs must be on different broadcast domains. iLO and Admin networks can intersect.

Admin Network (eno1)

The Admin network interface is used to connect the Sandbox appliance to the Fidelis CommandPost systems.

Appliance	Switch Port Type	Qty
Sandbox Appliance	GbE Copper RJ45 port	1

Non-Attribution Network (Routed Internet Access (eno3))

When the Sandbox appliance is configured in routed mode, this interface is used to allow the malware being executed full Internet access. It is *critical* to understand that any network addresses associated with this interface can be seen by attackers as well as potential IP address blacklisting services. It is highly recommended that some type of non-attributed network, such as a third-party VPN service or separate DSL connection, be used for this.

Appliance	Switch Port Type	Qty
Sandbox Appliance	GbE Copper RJ45 port	1

5. Sandbox Appliance Network Configuration

Each physical connection must be assigned appropriate network configuration based on its role. Before doing the actual installation, it is helpful to build a table of networking information for each appliance. The table below is an example that you can reference during configuration. Appendix A has a worksheet you can use to fill in your information.

Sample Configuration

Network Setting	Assignments		
Interface	Admin (eno1)	Routed (eno3)	iLO / IPMI
Hostname (FQDN)	sandbox.organization.net		
Static IP Address	10.1.2.3	192.168.1.3	10.2.3.4
Subnet Mask	255.255.255.0	255.255.255.0	255.255.252.0
Gateway	10.1.2.1		
Proxy Server	10.5.6.7		10.5.6.7
DNS Servers	8.8.4.4, 8.8.8.8		8.8.4.4, 8.8.8.8
NTP Servers	pool.ntp.org		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. See Appendix B for environmental data.

Power

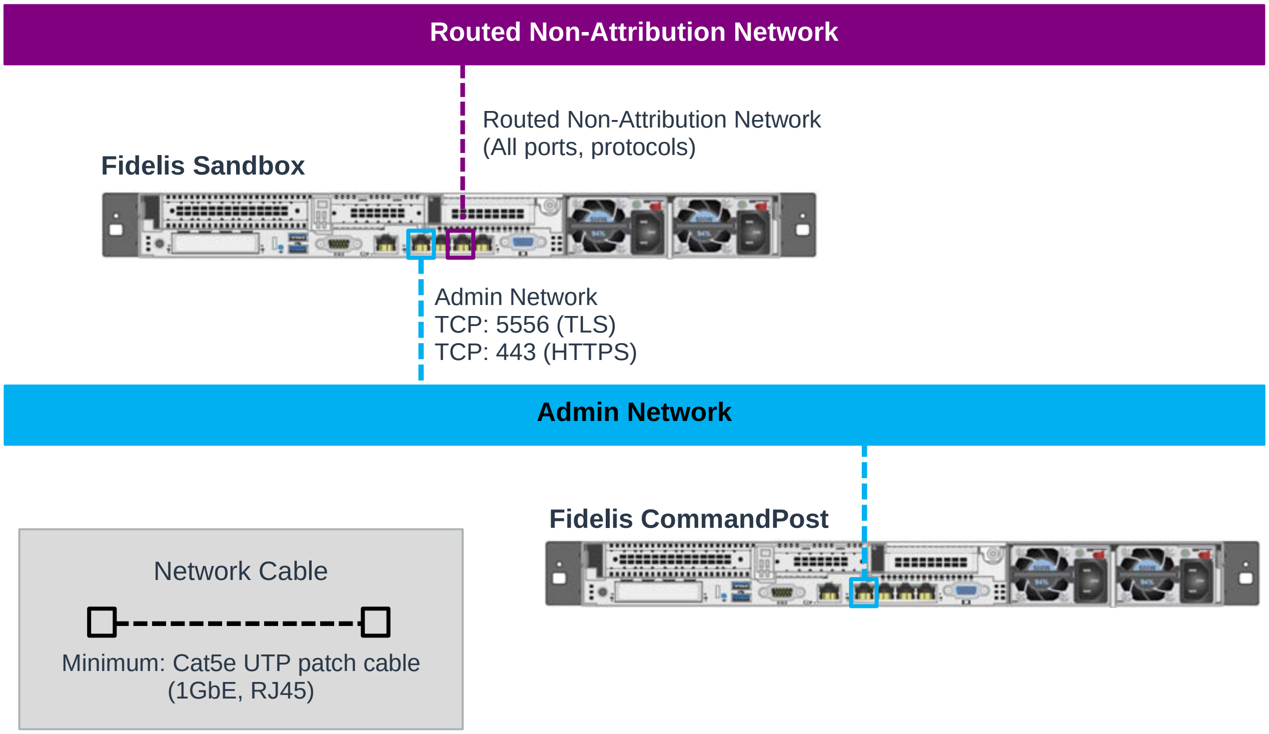
Connect power cables to the power supplies in the back of the appliance.

Network Cabling

Using the connectors and cables described in sections 3 and 4, connect the appliance to the network.

Cable the Sandbox appliance to the switches:

1. Connect the Admin (eno1) port to the ADMIN switch port.
2. Optionally, connect the Routed network (eno3) port to the “Non-Attribution” switch port.
3. Optionally, connect the iLO port to the ADMIN (or iLO) switch port.



(iLO connections not displayed)

Figure 3: Network Cabling Layout

7. Appliance Network Configuration

1. Power on the appliance(s).

2. Connect to the component CLI using via they KVM Console by connecting a keyboard and monitor to the appliance.

3. Directly attach an ethernet cable from a client system such as a laptop to the Admin/eno1 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.

4. Use the following credentials at the login prompt.

   - **user:** fidelis
   - **default password:** fidelispass

5. From the command line, run:

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

6. Within Setup, select **Network Settings**.

7. 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.

   Note: iLO interface is labeled IPMI in Setup.

8. When complete, select **OK** to leave Setup.

9. From the command line, reboot the system:

   ```
   sudo /sbin/reboot
   ```

8. Fidelis Network Integration

Register Sandbox Appliance with a CommandPost

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 **Sandbox**
Name	Specify a “friendly” name for the Sandbxo. This is *not* the fully qualified domain name of the Sandbox.
Description	Optionally, specify a description, for example, a location, business unit, etc.
IP Address	Specify the IP address of the Admin interface of the Sandbox appliance.

4. Click **Add Component**.

5. To register the sensor, click the ⋮ and select **Register**.

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

9. CommandPost Hierarchy Integration

Sandbox can accept sample submissions from multiple CommandPosts. The IP addresses of these CommandPosts need to be connected to the Sandbox appliance. If you have multiple CommandPosts configured in a hierarchical configuration, see the *Fidelis Network and Fidelis Deception User Guide* for more information on how to whitelist the additional CommandPost.

Connect Additional CommandPosts with Sandbox Appliance

1. Log into the user interface of the CommandPost to which the Sandbox is registered.

2. Navigate to: **Administration > Components**

3. In the row for the Sandbox, click the ⚙ icon.

4. On the **Sandbox** tab, connect additional CommandPosts by entering their IP addresses in the **Authorized Client CommandPost IPs** box. Use a comma-delimited list of IP addresses.

5. Click **Save**.

10. Non-Attributed Network Configuration

Optionally, the Sandbox supports Internet connectivity inside the virtual machines that run the potential malware samples. Perform the following steps to enable this connectivity:

1. Set up a connection to the Internet.

   Important! For security purposes, this connection must be on a separate network from the Admin network and must not be your primary connection. When you configure the Sandbox appliance in routed mode, the system uses this interface to allow the malware the Sandbox is executing to have full Internet access. It is *critical* that you understand that attackers can see any network addresses associated with this interface, as well as potential IP address blacklisting services. It is highly recommended that you use some type of non-attributed network, such as a third-party VPN service or separate DSL connection for the interface.

2. Using a RJ45 cable, plug this Internet connection to the Sandbox appliance port eno3, the non-attributed port.

3. Log into the Sandbox appliance via SSH. The default credentials are:

   – **user:** fidelis
   – **default password:** fidelispass

4. Run the following command:

```
sbx net config
```

5. Select interface eno3 and assign an IP/mask/DNS and gateway for the network being used as a non-attribution connection.

6. Log into the CommandPost user interface to which the Sandbox is registered.

7. Navigate to: **Administration > Components**

8. In the row for the Sandbox, click the ⚙ icon.

9. On the left, select **Sandbox**.

10. For **Sandbox Network**, select **Routed**.

11. Click **Save**.

Appendix A: Network Configuration Worksheet

Network Setting	Assignments		
Interface	Admin (eno 1)	Routed (eno 3)	iLO / IPMI
Hostname (FQDN)			
Static IP Address			
Subnet Mask			
Gateway			
Proxy Server			
DNS Servers			
NTP Servers			
Time Zone			

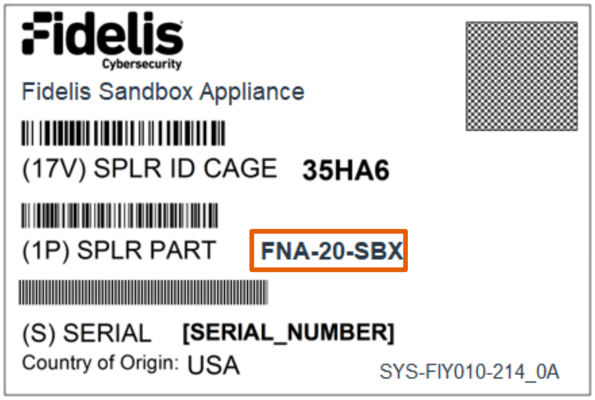
Appendix B: System Specifications

	Sandbox (Rev-K)
Form Factor	1U rack-mount chassis, SFF
CPU	Dual Gold 6246R 16/32-core 3.4Ghz
TPM	TPM 2.0
Memory	256GB ECC DDR4 2933Mhz
Storage Capacity & Configuration	2x HDD 300 GB RAID-1 6x HDD 1.2 TB RAID-10 (3.6 TB Effective)
Network Adapters (Default Config)	4x 1GbE
Out-of-Band Management	Integrated Lights Out Management (iLO)
Power Supply	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)
Weight (approx.)	16.27 kg (35.86 lb)
Operating Temperature	10° to 35°C (50° to 95°F) at sea level
AC Input Requirements	100 - 120 VAC 200 - 240 VAC
BTU Rating (max)	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



Fidelis Cybersecurity

Fidelis Sandbox Appliance

(17V) SPLR ID CAGE **35HA6**

(1P) SPLR PART **FNA-20-SBX**

(S) SERIAL **[SERIAL_NUMBER]**

Country of Origin: USA

SYS-FIY010-214_0A

Appliance SKU	System Type
FNA-20-SBX	Sandbox Appliance

QSG_Sandbox_Rev-K_20220408

Source: Technical Support

About Fidelis Cybersecurity