Fidelis Cybersecurity

QUICK START GUIDE

# Fidelis Sandbox Appliance

Rev-J

Sandbox Appliance (HP D360-G10) Platforms

www.fidelissecurity.com

# 1. System Overview

The Fidelis Sandbox Appliance, shown in Figure 1 below, 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 the 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 — Sandbox Appliance (Rev-J)**

# 2. Documentation & References

Fidelis product documentation, appliance specifications, and instructions can be found here https://support.fidelissecurity.com/ or through the icon in the CommandPost GUI.

## Sandbox Default Passwords

| System | Account | 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. Contact your reseller or if you have a direct support contract, contact the Fidelis Security support team at:

- Phone: +1 301.652.7190
- Toll-free in the US: 1.800.652.4020 — Use the customer support option.
- Email: support@fidlissecurity.com
- Web: https://support.fidelissecurity.com

### Sandbox Setup Checklist

| Required for the Sandbox Appliance: | Check |
|---|---|
| Rack space, power, and cooling for each component (Appendix B) | |
| Rack tools, rails, and connectors | |
| Keyboard and video monitor / KVM switch for temporary appliance setup | |
| Power cables — two per component, appropriate for power source and region | |
| Ethernet cables 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) | |

## 3. Sandbox Appliance Network Port and Cabling Requirements

Each component must be connected 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 | GbE RJ45 (copper) | Cat 5 patch cable |
| ROUTED | GbE RJ45 (copper) | Cat 5 patch cable |
| ILO | GbE RJ45 (copper) | Cat 5 patch cable |

## 4.Sandbox Appliance Networking Environment

The Sandbox Appliance may use multiple networks for full operation. Figure 2 below shows the port layout on the Sandbox Appliance (Rev J). The ADMIN and Routed switches or VLANs must be on different broadcast domains. iLO and ADMIN networks may intersect.

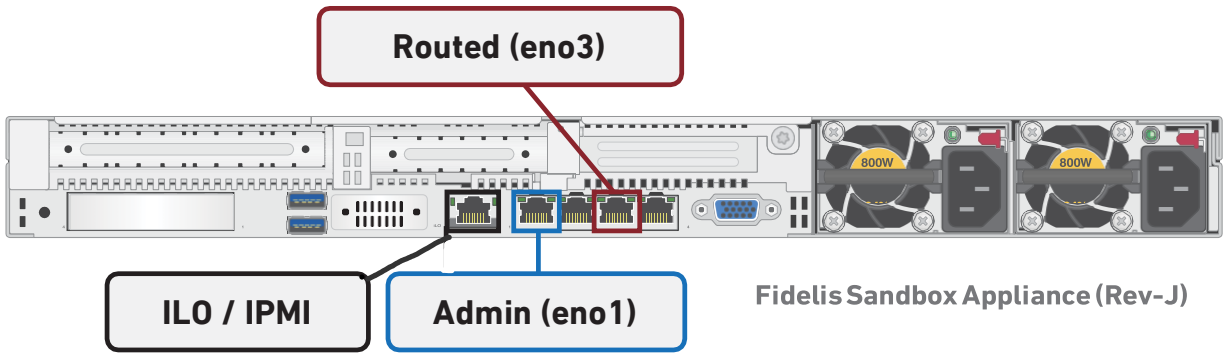



Figure 2: Sandbox Appliance Port Layout

**Use the information below to identify the type of switch ports necessary to support the deployment.**

### Admin Network (eno1)

The ADMIN Network interface is used to connect the Sandbox appliance to the Fidelis Network CommandPost/K2 systems.

| Component | Switch Port Type | Qty. |
|---|---|---|
| Sandbox Appliance | GbE - RJ45/Cat5+ (copper twisted pair) | 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 may 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 3rd party VPN service or separate DSL connection be used for this.

| Component | Switch Port Type | Qty. |
|---|---|---|
| Sandbox Appliance | GbE - RJ45/Cat5+ (copper twisted pair) | 1 |

# 5. Sandbox Appliance Network Configuration

Each physical connection must be assigned appropriate network configuration based on its role. Before doing the actual install, it may be helpful to build a table of the networking information for each appliance. The table below is an example that you can reference during configuration. You can find an empty table in Appendix A: Network Configuration Worksheet.

### Example Network Configuration Table

| 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. Component Installation

## Rack Installation

Install each component in an enclosure/location that has necessary power and cooling. See Appendix B: System Specifications and Environmental Information for environmental data.

## Power

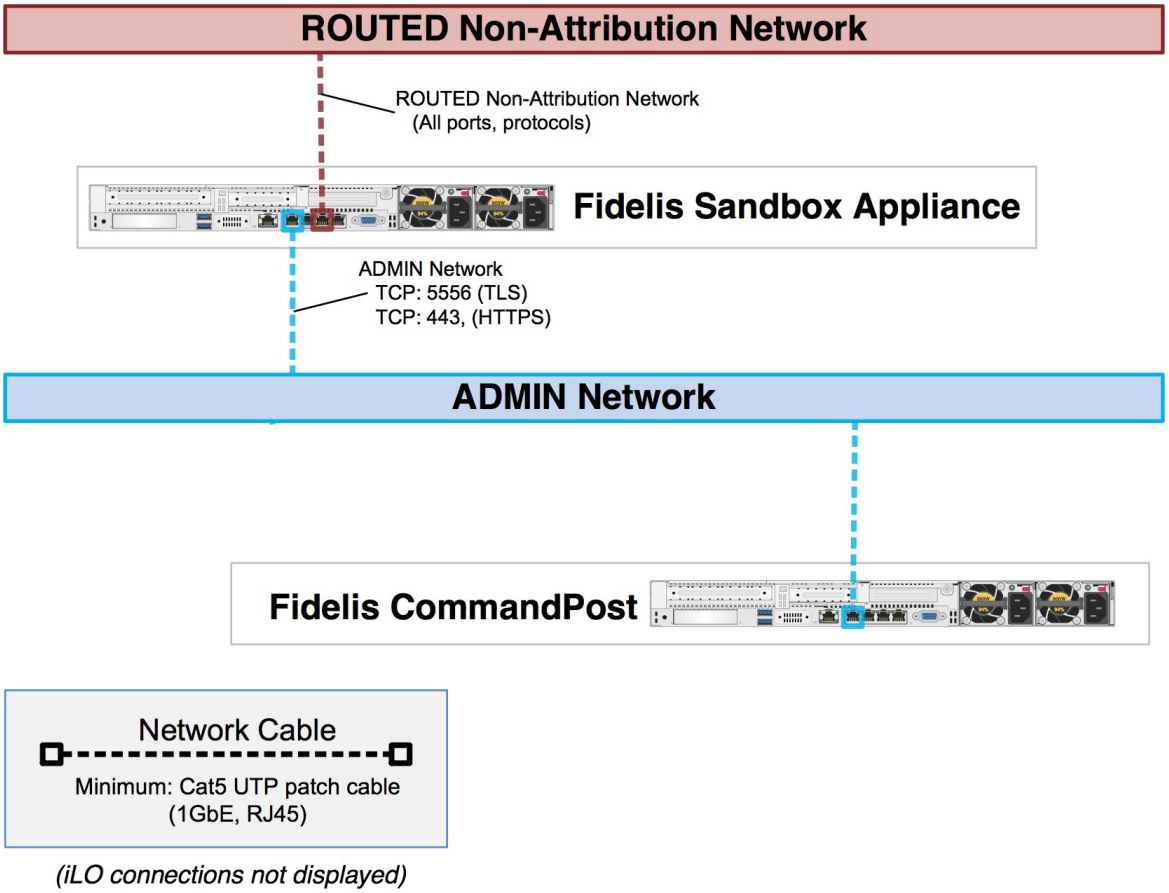
Connect power cables to the power supplies in the back of the component.

## Network Cabling

Using the connectors and cables described in section 3, connect the appliance to the network. Please use Figure 3 for a reference for this section.

Cable the Sandbox appliance to the switches:

1. Connect **Admin (eno1)** port to the "ADMIN" switch port
2. (optional) Connect **Routed Network (eno3)** port to the "Non-Attribution" switch port
3. (optional) Connect the **iLO port** to the ADMIN (or ILO) switch port




*(iLO connections not displayed)*

**Figure 3: Network Cabling Layout**

# 7. Component Network Configuration

1. If you have not done so, power on the component(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/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.
   - **Via Console:** Connect a keyboard and monitor to the appliance.
3. Use these credentials at the login prompt:
   - user: **fidelis**
   - default password: **fidelispass** (default)
4. From the command line, run: **sudo /FSS/bin/setup**
5. Within Setup, select Network Settings.
6. 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. (Note: iLO interface is labeled “IPMI” in Setup.)
7. When complete, select [OK] to leave Setup.
8. From command line, reboot the system: **sudo /sbin/reboot**

# 8. CommandPost/K2 Integration

### Registering Sandbox appliance with a CommandPost/K2

1. Log into the CommandPost/K2 GUI from a web browser.
2. Add the Sandbox appliance to the CommandPost/K2 at the System>Components page. Click [Add Component].
3. Select “Sandbox” from the pick list. Complete the form:
   - name – this is a “friendly” name for the Sandbox, not the FQDN of the Sandbox.
   - IP address of the ADMIN interface of the Sandbox appliance
   - (optional) description – e.g. location, business unit, etc.
   - click [Save].
4. Register the Sandbox to the CommandPost/K2. Click [Register] and accept the End User License Agreement (EULA). The CommandPost/K2 will then communicate with the Sandbox at the specified IP address.

# 9. CommandPost/K2 Hierarchy Integration

Sandbox can accept sample submissions from multiple CommandPost/K2s. The IP addresses of these CommandPost/K2 need to be connected to the Sandbox appliance. If you have multiple CommandPost/K2s configured in a hierarchical configuration, please see the user’s guide for more information on how to whitelist the additional CommandPost/K2.

### Connect additional CommandPost/K2s with Sandbox appliance

1. Log into the Registered CommandPost/K2 GUI from a web browser.
2. Configure the Sandbox appliance to the CommandPost/K2 at the System>Components> Sandbox page. Click [Config].
3. In Sandbox> tab, enter additional comma-delimited CommandPost/K2 IP addresses in [Authorized Client CommandPost/K2 IPs] window. Click [Save] to save the configuration.
4. In the whitelisted CommandPost/K2 web GUIs, add the Sandbox appliance at the System>Components page.

## 10. Non-attributed Network Configuration

The Sandbox optionally supports internet connectivity inside the VMs that run the potential malware samples. Enabling this requires the following steps:

1. Setup a connection to the internet. This connection should be on a separate network from the ADMIN network and should not be your primary connection for security purposes. 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 may 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 3rd party VPN service or separate DSL connection be used for this.
2. Using an RJ45 cable, plug this internet connection to the Sandbox appliance port eno3, the non-attributed port.
3. Log into the Sandbox appliance via ssh (default user: fidelis, default password: fidelispass).
4. Enter the console command: “sbx net config”.
5. Select interface eno3 and give it a configuration that corresponds to your network and operating system routing.
6. Log into the CommandPost/K2 to which the sandbox is registered.
7. Go to the System -> Components page.
8. Expand the sandbox and click on the Config button.
9. In the left tab, click “Sandbox”.
10. Where it says “Sandbox Network”, change isolated to routed and click save.

When complete, the Fidelis Sandbox appliance will be operational and ready to analyze malware samples submitted from the CommandPost/K2.

# Appendix A: Network Configuration Worksheet

## Sandbox Appliance

| Network Setting | Assignments | | |
|---|---|---|---|
| Interface: | ADMIN/eno1 | ROUTED/eno3 | iLO/IPMI |
| Hostname (FQDN) | | | |
| Static IP Address | | | |
| Subnet Mask | | | |
| Gateway | | | |
| Proxy Server | | | |
| DNS Servers | | | |
| NTP Servers | | | |
| Time Zone | | | |

# Appendix B: System Specifications

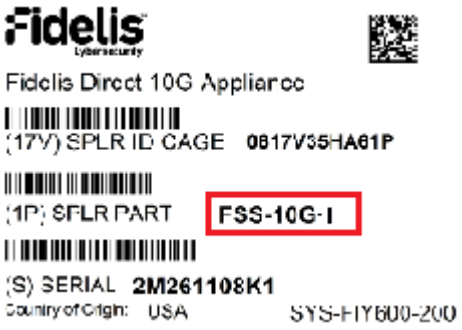
## Component Configuration and Resources (Rev-J)

| | Sandbox (Rev-J) |
|---|---|
| |  |
| Form Factor | 1U rack-mount chassis, SFF |
| CPU | Dual Intel Xeon Gold 6246<br>12/24-core 3.3 Ghz |
| Memory | 192 GB<br>ECC DDR4 2933Mhz |
| Storage Capacity & Configuration | 300GB<br>2x HDD, RAID-1<br>1.2 TB<br>6x HDD, RAID-10 (3.6TB) |
| Network Adapters (Default Config) | 4x 1GbE |
| Out of Band Management | Integrated Lights Out Management (ILO) |
| Power Supply | Dual hot-swap<br>800W High Efficiency<br>AC power supplies |
| Dimensions | H: 4.29 cm ( 1.69 in)<br>W: 43.46 cm (17.11 in)<br>D: 70.7 cm (27.83 in) |
| Weight (appx.) | 16.27 kg (35.85 lb) |
| Operating Temperature | 10° to 35°C (50° to 95°F) at sea level |

# Appendix C: System Types

For Fidelis Network Software version 9.3.3 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-SB-CollSA2-J<br>FNH-SB-CollSA2-J | Sandbox |

QSC_Fidelis_CE_20201103