Photon 400 Installation & Quick Start Guide

Token-Based Authorization

This document describes how to get started using the Photon 400 with token-based authorization. Token-based authorization is performed using a token downloaded from the managing Stellar Cyber server's **Sensor Installation** page.

The steps are as follows:

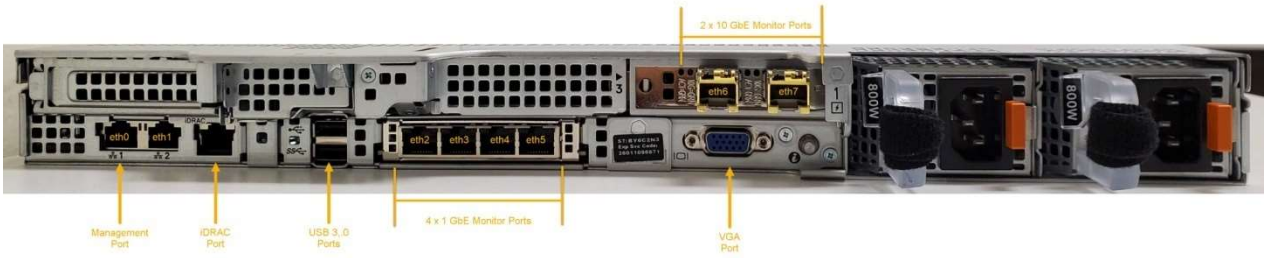
1. Connect power.
2. Connect the Photon 400 to the network.
3. Obtain an installation token from the Stellar Cyber GUI.
4. Access the Photon 400 CLI.
5. Change the management port settings.
6. Apply the installation token in the CLI.

Connecting Power

To connect power to the appliance:

1. Connect the included power cables to the power source.
2. Connect the power cables to the rear of the Photon 400.
3. Press the power button on the front of the Photon 400.

Connecting to the Network



To connect the Photon 400 to the network:

1. Connect the Management port to a network accessible by the DP.

2. Use the monitor ports to connect to data sources (mirror ports or taps). There are four 1 GbE monitor ports (eth2...eth5, from left to right) and 2 10GbE monitor ports (eth6...eth7, left to right).

Obtaining an Installation Token

Some Stellar Cyber deployments use tokens to authorize and configure the installation of a sensor. Tokens point the installed sensor to the correct DP, assign the specified tenant, and authorize the sensor installation.

Use the following procedure to obtain a token in the Stellar Cyber GUI:

1. Navigate to the **System | Deployment | Sensor Installation** page and click on the **Tokens** tab.
2. If a token already exists for the target tenant for the sensor installation, you can either use the **Copy** button to copy it to the clipboard or use the **Download** button to download it as a file.
    - Copy the token if you plan on applying it by pasting it into a `set token string <token>` command in the CLI.
    - Download the token as a file if you plan on hosting the file on an HTTP server and referring to it in a `set token url <token url>` command.
3. If there is not already an unexpired token for the target tenant, click the **Generate** button.
4. Select the tenant for the token from the **Tenant** dropdown. This is the tenant to which all sensors authorized with this token will be automatically assigned. The dropdown lists all tenants configured for your organization in the **System | Tenants** page.
5. Click the **Generate** button. The system generates the token and displays its contents in the **Token** field. The dialog also updates to display the expiration date for the token.
6. You can use the **Copy** button to copy the token to the clipboard immediately, or simply close the dialog and retrieve the token from the **Tokens** tab later on.

Accessing the Photon 400 CLI

You can access the appliance using a VGA monitor and USB keyboard, using SSH to the Management port, or using a virtual console over the iDRAC port. The ports for these connections are all at the rear of the appliance, as illustrated above.

VGA Console Access

For VGA console access, connect a display device to the system using one of the two VGA ports (one is in the front and the other is in the rear. Then, connect a USB keyboard to one of the USB ports (one is in the front and two are in the rear).

SSH Access

The default management IP address on the appliance is **192.168.1.100/24**, and the default gateway IP address is: **192.168.1.1**. The default username and password are as follows:

- Username: **aella**
- Password: **changeme**

For SSH access to the appliance:

```
ssh -l aella 192.168.1.100
```

Virtual Console over iDRAC

The iDRAC feature can be licensed directly from Dell; a free trial is available. There is an iDRAC Direct port on the front of the appliance and a dedicated iDRAC network port on the back.

Change the Management Port Settings

1. You should still be logged in to your sensor from the previous procedure. If you are not, log in now using either SSH or a console connection with the credentials you set in the previous procedure.
2. You can set IP parameters manually using commands similar to the following (substitute your own IP parameters for the ones shown in bold below):
   - `set interface management ip 192.168.14.100/255.255.255.0`
   - `set interface management gateway 192.168.14.1`
   - `set interface management dns 8.8.8.8`
3. Verify the IP settings with the `show interfaces` command.
4. Use the `set ntp` command to specify the NTP server(s) to use for time synchronization.

Applying the Token to the Sensor

Use the following procedure to apply a token to a sensor.

1. Apply the token to the installed sensor from the sensor CLI with the `set token` command. The available techniques are as follows:
   - **Copy and Paste Token String** – Copy the token string from the **Tokens** tab and paste it into the CLI command. The syntax is as follows:
     `set token string <pasted string>`
   - **Host Token on HTTP Server** – Download the token as a file from the **Tokens** tab, upload it to an HTTP server, and reference it in the `set token` command. The syntax is as follows:
     `set token url http://<url to token>`
2. The CLI reports that the Sensor token is successfully set.
   Note: If you receive an error message instead, it's possible that the token has expired. Refer to the **Tokens** tab to see the expiration date. If you are using the File technique, it's also possible that an extra space or line may have crept into your text file – check the file to make sure it includes only the token text.

3. Wait a minute or so. Then, verify that the token was successfully applied using any combination of the following techniques:
    - Check the **System | Sensors** tab in the user interface to see that the sensor has registered itself successfully.
    - Verify that the `show system` command shows all services as running.
    - Verify that the `show receiver` command displays a receiver.
    - Verify that the `show json` command reports some data sent in the `BYTE_SENT` column.

Set the Timezone for the Sensor

You should use the **Edit** feature in the **System | Sensors** page to set the timezone for the sensor.
During installation, the sensor timezone is automatically set to UTC+0. Since the logs for some security products may only include the local time without a timezone, Stellar Cyber strongly recommends that you set the sensor timezone to the same timezone as your security product