

# HPE Aruba ClearPass

Last updated: Jun. 24, 2025

## Overview

Use this guide to set up data ingestion for Aruba ClearPass using a data shipper, such as the Falcon LogScale Collector.

Types of logs generated by this data connector:

- Audit Records
- Insight Logs
- Session Logs
- System Events

## Requirements

**CrowdStrike subscription:** Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB

**CrowdStrike clouds:** Available in **US-1**, **US-2**, **EU-1**, and **US-GOV-1**

**CrowdStrike access and permissions:** Administrator or Connector Manager access to the Falcon console for the respective CID

**Vendor requirements:** Aruba ClearPass UI Admin Access

**System requirements:**

- For the Falcon LogScale Collector, see the list of [supported operating system versions \[https://library.humio.com/falcon-logscale-collector/log-collector-install.html#log-collector-install-compatibility\]](https://library.humio.com/falcon-logscale-collector/log-collector-install.html#log-collector-install-compatibility).
- The size of your Falcon LogScale Collector instance depends on workload. See the [LogScale Collector sizing guide \[https://library.humio.com/falcon-logscale-collector/log-collector-install-sizing.html\]](https://library.humio.com/falcon-logscale-collector/log-collector-install-sizing.html).

## Setup

**Important:** Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

### Step 1: Configure and activate the HPE Aruba ClearPass data connector

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).
2. Click + **Add connection**.
3. In the **Data Connectors** page, filter or sort by **Connector name**, **Vendor**, **Product**, **Connector Type**, **Author**, or **Subscription** to find and select the connector you want to configure.

**Tip:** This data connector's name is located in the header. For example, **Step 1: Configure and activate <the\_data\_connector\_name>**.

4. In **New connection**, review connector metadata, version, and description. Click **Configure**.

**Note:** For connectors that are in a **Pre-production** state, a warning appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, enter a name and optional description to identify the connector.
6. Click the **Terms and Conditions** box, then click **Save**.
7. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate the API key, go to [Data connectors > Data connectors > Data connections \[/data-connectors\]](#), click **Open menu** ⋮ for the data connector, and click **Generate API key**.
8. Copy and safely store the API key and API URL to use during connector configuration.

**Important:** Record your API key somewhere safe as it displays only once during connector setup. For more information about vendor-specific connector setup, see the [Third-party data source integration guides \[/documentation/page/a76b8289/data-connectors#c42a73ec\]](#).

### Step 2: Configure your data shipper

You can use any data shipper that supports the [HEC API \[https://library.humio.com/logscale-api/log-shippers-hec.html\]](https://library.humio.com/logscale-api/log-shippers-hec.html) to complete this step. We recommend using the **Falcon LogScale Collector**.

1. In the Falcon console, navigate to [Support and resources > Resources and tools > Tool downloads \[/support/tool-downloads\]](#).
2. Install the LogScale Collector based on your operating system. For example, LogScale Collector for Windows - X64 vx.x.x.
3. Open the LogScale Collector configuration file in a text editor. For file location, see [Create a configuration - Local \[https://library.humio.com/falcon-logscale-collector/log-collector-config.html#log-collector-config-editing-local\]](https://library.humio.com/falcon-logscale-collector/log-collector-config.html#log-collector-config-editing-local).

4. Edit the config.yaml file. Examples of configuration files for syslog servers:

- Linux

```
dataDirectory: /var/lib/humio-log-collector
sources:
  syslog_udp_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

- Windows

```
dataDirectory: C:\ProgramData\LogScale Collector\
sources:
  syslog_port_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

- Mac

```
dataDirectory: /var/local/logscale-collector
sources:
  syslog_port_514:
    type: syslog
    mode: udp
    port: 514
    sink: humio
sinks:
  humio:
    type: hec
    proxy: none
    token: <generated_during_data_connector_setup>
    url: <generated_during_data_connector_setup>
```

5. Verify the sources and sinks sections are correct.

- Check that no other services are listening on port 514. For example, this command is commonly used to check for listening ports on Linux:

```
sudo netstat -ltn
```

- If port 514 is not available, select a different port and confirm it is not in use. Update the port number.
- If you're configuring multiple sources in the same configuration file, each sink must have a distinct port. For example, you cannot have two Humio sinks listening on port 514.

- Check the local firewall and confirm that the configured port is not being blocked.

**Important:** For Windows Firewall, add the LogScale Collector to your traffic allowlist.

- Add the token and url generated during data connector setup. Remove /services/collector from the end of the url.

6. Save and exit the config.yaml file.

7. Restart the Falcon LogScale Collector.

- For Linux, run this command in your terminal:

```
sudo systemctl start humio-log-collector
```

- For Windows, look for **Services** from the search bar, open **Services**, find **Humio Log Collector** and right-click **Restart**.

- For Mac, run this command in your terminal:

```
sudo launchctl kickstart -k system/com.crowdstrike.logscale-collector
```

## Step 3: Add syslog targets in Aruba ClearPass Policy Manager

1. In the ClearPass Policy Manager, navigate to **Administration > External Servers > Syslog Targets**.

2. Click **Add** and enter these details:

- Host Address:** Enter the IP or hostname of the LogScale collector.
- Description:** Enter a short description.
- Protocol:** Select **TCP**.

d. **Server Port:** Enter the port number specified in the LogScale Collector configuration above.

**Tip:** For more info about adding a syslog target, see

[Syslog Targets \[https://arubanetworking.hpe.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPM\\_UserGuide/Admin/syslogTargets.html\]](https://arubanetworking.hpe.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPM_UserGuide/Admin/syslogTargets.html)

.

3. Click **Save**.

## Step 4: Add syslog export filters in Aruba ClearPass Policy Manager

1. In the ClearPass Policy Manager, navigate to **Administration > External Servers > Syslog Export Filters**.

2. In the **Syslog Export Filters** page, click **Add** and enter these details:

a. **Name:** Enter a name for the syslog export filter.

b. **Description:** Enter a description of the syslog export filter.

c. **Export Template:** Select **Audit Records**.

d. **Export Event Format Type:** Select **RFC 5424**.

e. **Syslog Servers:** Select the Syslog Target you just created.

f. **Local Facility Level:** Select **Local Use 1**.

**Tip:** For more info about adding a syslog export filter, see

[Syslog Export Filters \[https://arubanetworking.hpe.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPM\\_UserGuide/Admin/syslogTargets.html\]](https://arubanetworking.hpe.com/techdocs/ClearPass/6.11/PolicyManager/Content/CPM_UserGuide/Admin/syslogTargets.html)

.

3. Save the configuration.

4. Repeat steps 2-4 for Insight Logs, Session Logs, and Systems Logs in the Export Template.

## Step 5: Verify successful data ingestion

**Important:** Search results aren't generated until an applicable event occurs. Before verifying successful data ingestion, wait until data connector status is **Active** and an event has occurred. Note that if an event timestamp is greater than the retention period, the data is not visible in search.

Verify that data is being ingested and appears in Next-Gen SIEM search results:

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).

2. In the **Status** column, verify data connection status is **Active**.

3. In the **Actions** column, click **Open** menu : and select **Show events** to see all events related to this data connection in **Advanced Event Search**.

4. Confirm that at least one match is generated.

If you need to run a manual search, use this query in Advanced Event Search:

```
#Vendor = "hpe" | #repo = "3pi_hpe_aruba_clearpass" | #event.module = "clearpass"
```



## Data reference

### Parser

The default parser recommended to parse incoming data for this data connector is **aruba-clearpass**.

### Timestamp

**Timestamp Format:** YYYY-MM-DDThh:mm:ss.SSSZ

**Example:** 2019-12-10T10:31:05.868Z

### Structure

Syslog headers with CEF-formatted messages:

```
<log.syslog.priority>log.syslog.version @timestamp log.syslog.hostname log.syslog.appname log.syslog.procid  
log.syslog.msgid syslog.structured_data
```



## Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- [Network:info{failure.success.unknown} \[/documentation/page/q1f14b54/next-gen-siem-data#j0rcmxhx\]](#)

For more information about Next-Gen SIEM events, see [Next-Gen SIEM Data Reference \[/documentation/page/q1f14b54/next-gen-siem-data\]](#).

< [HEC/HTTP Event Connector\[/documentation](#) [Menlo Security Secure Web Gateway](#) > [\[/documentation/page/e21f446/menlo-security-secure-web-gateway\]](#)

