

Falcon LogScale Collector

Last updated: Jul. 2, 2025

Overview

The Falcon LogScale Collector Data Connector can ingest logs from different sources, depending on the parser you select during setup. For more details about sources, see [Sources & Examples \[https://library.humio.com/falcon-logscale-collector/log-collector-config-advanced-example.html\]](https://library.humio.com/falcon-logscale-collector/log-collector-config-advanced-example.html).

Use this connector to streamline setup and configuration of the Falcon LogScale Collector for data sources that require a data shipper for data transport to the Falcon console.

Requirements

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.

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

Step 1: Configure and activate the Falcon LogScale Collector 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 **Falcon LogScale Collector Data Connector**.
4. In the **New connection** dialog, review connector metadata, version, and description. Click **Configure**.

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

5. In the **Add new connector** page, enter or select these details:

- **Vendor:** Select the vendor name for the data source.
- **Product:** Select the product name for the data source.
- **Connector name:** Enter a name to identify the connector.
- **Description:** Optional. Enter a description of the connector.
- **Parsers:** Select a parser to parse incoming data.
 - In the Parsers dropdown menu, search for an existing parser that aligns with the data source.
 - If such a parser does not exist, you need to create a custom parser. To create a custom parser, click **Create new parser**. For more info, see [Add a new parser \[documentation/page/n00d51ed/parsers#v2187748\]](#). For custom parser requirements, see [Understanding the CrowdStrike Parsing Standard \[documentation/page/u05f69c9/crowdstrike-parsing-standard#gc82e70d\]](#).

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**, 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.

Note: Record your API key somewhere safe as it displays only once during connector setup. For more information about vendor-specific connector setup, see [Third-Party Data Sources \[documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations\]](#).

Step 2: Create a new configuration file

In the Falcon console, create a new configuration file for your instance of the Falcon LogScale Collector.

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors\]](#) and click **Fleet Management**.
2. On the **Config overview** tab, click + **New config**.

3. Enter a name for the config and select **Empty config**.

Tip: If you're already using the Falcon LogScale Collector and have a `config.yaml` file you'd like to use, select **From Template** and upload the file.

4. Click **Create new**. The **Draft editor** appears.

5. Edit the sinks section to include these details:

- Replace `<ingest-token>` with the API key provided in [Step 1: Configure and activate the Falcon LogScale Collector Data Connector](#) [documentation/page/u496e28e/falcon-logscale-collector#ie508d39].
- Replace `<ingest-url>` with the API URL provided in [Step 1: Configure and activate the Falcon LogScale Collector Data Connector](#) [documentation/page/u496e28e/falcon-logscale-collector#ie508d39].
- Replace `humio` with `hec`.

6. Edit additional sources and sinks fields based on your environment. For example configurations, see [Sources & examples](#) [https://library.humio.com/falcon-logscale-collector/log-collector-config-advanced-example.html]. Important areas to keep in mind:

- If setting up a syslog source, check that no other services are listening on port 514. This is the default port for the Falcon LogScale Collector. If port 514 is in use, select a different port and confirm it is not in use. Add this new port number to the config file.
- If you plan to configure multiple sources in the same config 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. For Windows Firewall, add the Falcon LogScale Collector to your traffic allowlist.

7. Click **Publish**.

Step 3: Install the Falcon LogScale Collector

1. Go to [Next-Gen SIEM > Log management > Data onboarding](#) [data-connectors] and click **Fleet Management**.

2. On the **Fleet overview** tab, click **Get LogScale Collector**.

3. We recommend following the **Full install** instructions:

Note: **Full install** allows for configuring and updating the Falcon LogScale Collector within the Falcon UI and a robust fleet management system with metrics. Custom install requires local updates through a systems package manager. If you need custom install instructions, see [Create a configuration - Local](#) [https://library.humio.com/falcon-logscale-collector/log-collector-config.html#log-collector-config-editing-local].

- Select your operating system:** `macOS/Linux` or `Windows`.
- Select an enrollment token:** An enrollment token associates instances of the Falcon Log Collector with the config file. A **Default Collector install token** is provided and selected. No additional action is required.
- Run the provided `curl` command in your terminal to download and install the Falcon LogScale Collector.
- Close the **Get Falcon LogScale Collector** window.


4. In **Fleet overview**, confirm your Falcon LogSale Collector is now available.

Step 4: Assign the configuration to your instance of the Falcon LogScale Collector or Groups

On the **Fleet overview** tab, you can assign the config you created in

[Step 2: Create a new configuration file](#) [documentation/page/u496e28e/falcon-logscale-collector#e9d073c6] to the instance of the Falcon LogScale Collector you just installed.

There are two ways to do this depending on your use case. If you only need to assign the configuration to a single instance of the Falcon LogScale Collector, follow these steps:

- In the row of the Falcon LogScale Collector you just installed, click the **Open**  menu and select **Extend config**. The **Extend configuration** window appears.
- Select the config you created in [Step 2: Create a new configuration file](#) [documentation/page/u496e28e/falcon-logscale-collector#e9d073c6].
- Click **Save**.

If you need to associate a config file with multiple instances of the Falcon LogScale Collector, you can create **Groups** in **Fleet Management**.

Instances when creating a group might be helpful:

- Managing a large fleet of collectors.
- Assigning multiple instances of the Falcon LogScale Collector to the same config file.
- Upgrading or downgrading multiple instances of the Falcon LogScale Collector at the same time.

Filters can also be added to groups. These filters query instances of the Falcon LogScale Collector and automatically add them to your group. For example, you can create a filter that groups all instances of the Falcon LogScale Collector running on Linux. For more info, see [Manage Falcon Log Collector Groups](#) [documentation/page/pa9df507/manage-falcon-log-collector-groups].

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:

#repo=3pi_auto_raptor_* | #type=<parser_selected_during_setup>

Note: This query contains a placeholder value. Replace the placeholder values with your parser. For example, if your parser is named MyParser, you would enter this query: #repo=3pi_auto_raptor_* | #type=MyParser.