Get Started with Fleet Management

Last updated: Apr. 22, 2025

Overview

Fleet Management gives you options to monitor and manage a fleet of Falcon Log Collector instances that have been either enrolled into remote configurations and those that have only been added to Fleet Management.

> **Note:** You can only see Falcon Log Collector instances that have been configured to work with Fleet Management.

Requirements

Subscription:

- Falcon Next-Gen SIEM 10GB

    ○ Includes 10 GB per day ingestion of third-party data, with 7 days of data retention.

- Falcon Next-Gen SIEM, or Falcon Complete powered by Next-Gen SIEM

    ○ Includes additional third-party data ingestion and data retention capabilities.

LogCollector support: Version 1.7.2 and later

Default roles:

- Connector Manager

- Falcon Administrator

- NG SIEM Administrator

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

Fleet Management setup

Requires complete setup. To use Fleet Management, you must complete all setup steps, including downloading, installing, and enrolling the Falcon Log Collector, configuring the HEC connector, and creating a remote configuration.

Step 1: Download install the Falcon Log Collector

1. Go to **Support and resources > Resources and tools > Tool downloads [/support/tool-downloads]**.

2. Locate the newest version of the LogScale Collector for your operating system and click Download ⤓ .

3. Install the Falcon Log Collector.

    - **Windows:** Execute the installer. The installer guides you through the installation of the Falcon Log Collector. It also creates (but does not start) a Windows service for the Falcon Log Collector.

    - **MacOS:** Double click the installer. You can use the following command to run and enroll your log collector and specify the enrollment token. `$ sudo logscale-collector enroll enrolltoken`

    - **Linux:** Run the following command to install Falcon Log Collector on:

        ○ **Ubuntu:** `shell sudo dpkg -i humio-collector_x.x.x_linux_amd64.deb`

        ○ **RedHat:** `shell $ sudo rpm -i humio-collector.rpm`

Step 2: Enroll the Falcon Log Collector

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

2. Click **Enrollment tokens**.

3. Click **See enrollment command** ◎ .

4. Click **Copy enrollment command** for your operating system.

5. Run the command on your machine where you installed the collector.

Step 3: Set up the HEC/HTTP event connector

Set up data ingestion by configuring the HEC/HTTP Event data connector in the Falcon console. For more info, see
Step 1: Set up the HEC/HTTP Event Data Connector [/documentation/page/bdded008/hec-http-event-connector-guide#g5a3da77].

Step 4: Create a remote configuration

You can create a new configuration, which can then be assigned to multiple Falcon Log Collector instances and managed centrally.

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

2. Click **Config overview**.

3. Click **New config**.

4. Type the name for your new configuration and click either:

   - **Empty config:** Creates a new configuration from scratch.

   - **From template:** Create from template and browse for a previously exported or manually created configuration file (.yaml).

5. Click **Create New**.

6. From the **Draft editor**, configure the file to meet your needs. You can only edit the sources, sinks, and settings. For more info, see
   Sources & Examples [https://library.humio.com/falcon-logscale-collector/log-collector-config-advanced-example.html]. The editor helps by underlining misspelled or incorrectly positioned entities (incorrect level) and by auto-completing entities when you are inserting new entities. You can also hover over entities for useful tips and information.

7. You can perform additional tasks from this page:

   - Click **Test** to view the status of the tests related to this configuration.

   - Export either the draft configuration or the currently published configuration.

   - Import a configuration as a starting point.

8. Once you have finished making changes in the editor you can:

   - Click **Save** to save the changes without publishing.

   - Click **Test** to test your configuration file by publishing it to specific instances.

   - Click **Publish** to save the changes and publish them to all the instances that are using the configuration.

Step 5: Create a group

With groups, you can manage the configuration of multiple instances of the Falcon Log Collector, along with the option to combine configuration snippets to create a configuration that can be applied to all the instances in the group. These features allow you to bulk manage instances.

You can create groups that contain a static list of instances. For example, use the ID of specific machines or dynamic filters based on a subset of the LogScale query language.

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]**.

2. Click **Groups**.

3. Click **New group**.

After a few minutes, the collector instance picks up on the new configuration assigned to it from the group.

About Fleet Management ❯ [/documentation/page/o5a1483c/about-fleet-management]