Manage Falcon Log Collector Instance Enrollment

Last updated: May 19, 2025

Overview

Enroll Falcon Log Collector instances in fleet management to associate them with a remote configuration. Use enrollment tokens to associate instances of the Falcon Log Collector with the config file. The instance no longer uses a local configuration file, and you can manage its configuration centrally. For more info, see Manage Remote Configurations [/documentation/page/cdf9cac0/manage-remote-configurations].

View enrollment tokens

To see an overview of all enrollment tokens and their configurations:

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

2. Click **Enrollment tokens**.

A list of all the enrollment tokens and their details is displayed.

Enroll a Falcon Log Collector instance

The process of creating a new enrollment token associates an instance of the Falcon Log Collector with a centrally managed configuration file. For more info, see Manage Remote Configurations [/documentation/page/cdf9cac0/manage-remote-configurations].

1. Install the Falcon Log Collector. For more info, see Step 1: Download install the Falcon Log Collector [/documentation/page/q81f4f3a/get-started-with-fleet-management#x7b0acd3].

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

3. Click **Enrollment tokens**.

4. Click **New token**.

5. Enter a unique and descriptive name.

6. Select a configuration from **Assigned config** to assign to the instance of the Falcon Log collector.

7. Click **Create token**.

8. The data directory is written to the start-up config. If you need to place your data directory at a different path, provide the `--data argument`.

9. Click **See enrollment command** for the newly generated token.

10. Click **Copy enrollment command**

    next to the required OS to copy the token to your clipboard. You can add optional settings to this command. For more info, see Enrollment token options [/documentation/page/w55f2d06/manage-falcon-log-collector-instance-enrollment#aaf8defb].

11. Run the script on the machine where you installed the Falcon Log Collector instance.

> **Note:** The enroll command stops and starts the service during the enrollment process. You can override this step by using the `--no-service` flag on the enroll command.

Enroll existing Falcon Log Collector instances

You can enroll existing Falcon Log Collector instances into fleet management to monitor the status of your instances. However, to take full advantage of fleet management, you must enroll the configuration in remote configuration management. For more info, see Fleet Management (fleetManagement) [https://library.humio.com/falcon-logscale-collector/log-collector-config-common-fleet.html].

> **Important:** This procedure deletes the existing configuration YAML file being used by the instances of the Falcon Log Collector.

If you do not already have a configuration in remote configuration for the instances, you can import an existing configuration or create a new configuration. For more info, see Create a Remote Configuration [https://library.humio.com/falcon-logscale-collector/log-collector-fleet-management-remote.html#log-collector-fleet-management-remote-create]
. If you're importing a local configuration file, you may need to remove some local-only sections, which are underlined in the editor.

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

2. Click **Enrollment tokens**.

3. Click **New token**.

4. Enter a unique name.

5. Select the configuration you created to assign to the instance of the Falcon Log collector.

6. Click **Create token**. The token appears on the **Enrollment tokens** page.

7. Click **See enrollment command** for the newly generated token.

8. Click **Copy enrollment command**

8. Click **Copy enrollment command**

   ⧉

   next to the required OS to copy the token to your clipboard. You can add optional settings to this command. For more info, see [Enrollment token options [/documentation/page/w55f2d06/manage-falcon-log-collector-instance-enrollment#aaf8defb]](/documentation/page/w55f2d06/manage-falcon-log-collector-instance-enrollment#aaf8defb).

9. Run the script on the machine where the Falcon Log Collector instance is installed.

Enrollment token options

You can set options related to the configuration when running the enrollment command.

Option	Description	Default Value/Behavior
`--allow-insecure-http`	Enable use of `http://` addresses, see [Enable HTTP [https://library.humio.com/falcon-logscale-collector/log-collector-config-troubles.html#log-collector-config-troubles-http]](https://library.humio.com/falcon-logscale-collector/log-collector-config-troubles.html#log-collector-config-troubles-http)	Not allowed
`--allow-remote-cmd`	Enable the use of CMD sources when using remote configuration	Not allowed
`--ca-cert mycert`	Use CA root certificate from argument. This can be used with a PEM encoded value, the certificate is encoded in the start-up configuration. For example `--ca-cert "-----BEGIN CERTIFICATE-----\n....\n-----END CERTIFICATE-----`	N/A
`--ca-file mycertfile`	Use CA root certificate from file argument and point to a certificate file on disk. The path to the file should be absolute and readable by the service user. The file is read on each start of the Falcon Log Collector. Example: `--ca-file "/opt/ca.crt"`	N/A
`--cfg myfilepath`	Specify a custom configuration file location. The enrollment command overwrites the local file with a start-up remote configuration. If your service used a configuration on a different path, the `--cfg` argument can be used to place the configuration in a different path. The argument only affects the path to where the start-up configuration is written, it does not alter the SystemD or Windows service entry.	The following paths are used by default: • Linux: /etc/logscale-collector/config.yaml /etc/humio-log-collector/config.yaml • Windows: C:\Program Files (x86)\CrowdStrike\Humio Log Collector\config.yaml • macOS: /usr/local/etc/logscale-collector/config.yaml
`--data mydatadirectory`	Specify a custom data directory which is then written to the start-up configuration	The following paths are used by default: • Linux: /var/lib/logscale-collector • Windows: C:\ProgramData\LogScale Collector • macOS: /var/local/logscale-collector
`--ephemeralTimeout mytimeoutinhours`	Unenrolls and removes from the fleet overview if it is offline for the specified duration in hours	N/A
`-h or --help`	Print list of command options that can be used for enrollment	N/A
`--mode mymode`	Mode of enrollment, can be `"full"` or `"localConfig"` where: • full (default): Enroll into fleet management with configuration of the log sources stored and managed centrally in Falcon Next-Gen SIEM. • localConfig: Will enroll into fleet management with configuration of the log sources managed and stored locally on the host in a local yaml file. Fleet overview including metrics from the collector will still be available.	Full
`--no-check-certificate`	Skip TLS certificate validation. Allows insecure connections.	Validation is performed
`--no-permissions`	Data directory permissions are not changed. This option is only relevant for Linux. It prevents the command from changing data directory permissions to align with the standard service user. It should not be used for normal deployments, and is only relevant if for some reason the standard service user is not desired to be used to run the collector.	Changes are made to the permissions of the data directory
`--no-service`	Bypasses stopping and starting the service during the enrollment process	The service stops and starts when the command has run
`--proxy myproxy`	Proxy to use for fleet management where the possible values are: • auto: Tries to determine the system proxy or fallback to none. • system: Attempts to use the system proxy and fails if it cannot be determined. • none: For Windows Server or you can specify, if required, an override proxy	Auto

	configuration for the sink. - a URL such as: http://127.0.0.1:3129 for a HTTP proxy. If your setup requires a proxy to communicate with Falcon Next-Gen SIEM, it can be configured using `--proxy` followed by the proxy.	
`--timeout duration`	Set the timeout of the command. If the processing of the command takes longer than duration, the command fails and exits. This could be caused by a network timeout, for example. Possible values are either 0 or a duration using a format with units. For example, :0: no timeout, 1m30s	Default is 1m0s

Edit an enrollment token

Change the name of a token and switch the configuration assigned to an instance.

1. Go to Next-Gen SIEM > Log management > Data onboarding [/data-connectors].
2. Click **Enrollment tokens**.
3. Click **Options** ⋮ for the token you want to change and select **Edit token**.
4. Edit the name or change the assigned configuration by selecting a configuration file.
5. Click **Save**.

Delete an enrollment token

1. Go to Next-Gen SIEM > Log management > Data onboarding [/data-connectors] and click **Fleet management**.
2. Click **Enrollment token**.
3. Click **Options** ⋮ for the token you want to delete and select **Delete config**.
4. Click **Delete config** to confirm.

< Manage Remote Configurations[/documenta Manage Falcon Log Collector Groups > [/documentation/page/pa9df507/manage-falcon-log-collector-groups]