

Parsers

Last updated: Jun. 25, 2025

Overview

Parsers use scripts written in CrowdStrike Query Language to transform incoming data into searchable events that trigger detections in Next-Gen SIEM. You can use default parsers to parse incoming data in common formats. To parse incoming data in other formats, create and manage your own custom parsers. For more info on parsing data, see [Parsing Data \[https://library.humio.com/data-analysis/parsers.html\]](https://library.humio.com/data-analysis/parsers.html).

View parsers

The **Parsers** table displays a list of all available parsers.

In the Falcon console, go to [Data connectors > Data connectors > Parsers \[data-connectors/parsers\]](#). You can complete these tasks in the **Parsers** table:

Note: Parsers in **Active** status are parsers that are currently in use by a data connector. Parsers in **Inactive** status are parsers that are not currently in use by any data connector.

- View details for each parser, such as name, data source, type, current status, and the number of data connectors using the parser.
- Search for a parser by name.
- Filter parsers by data source, type, and current status.
- Sort the table by parser names in alphabetical order and current status.
- Create a new data connection using a parser.

Click a parser's name to see its summary page with details such as current status, data source, parser script, and associated tests.

Default parsers

Parse data in common incoming formats using the default parsers listed in this table.

The **Parsers** table displays a list of all available parsers. To see all default parsers, follow these steps:

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors\]](#) and click the **Parsers** tab.
2. Set the **Type** filter to **Default** and click **Apply**.

Note: For more info about built-in parsers for the LogScale Collector, see [Built-in Parsers \[https://library.humio.com/data-analysis/parsers-built-in.html\]](https://library.humio.com/data-analysis/parsers-built-in.html).

Add a new parser

Create a new parser from a blank template, a clone of an existing parser, or a YAML file.

1. In the Falcon console, go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.
2. Click **Add new parser**.
3. In **Create new parser**, enter a name for your parser.
4. In the dropdown, select the method you want to use to create your parser.
 - Blank template: Create a parser from scratch.
 - Clone existing: Select an existing parser to clone.
 - Import: Import a parser by uploading a YAML file. To export an existing parser, see [Export a parser \[documentation/page/n00d51ed/parsers#g7db68d5\]](#).
5. Click **Create**. The **Edit parser** page opens.
6. In the **Parser script** section, enter your parser script in CrowdStrike Query Language. For more info on writing parser scripts, see [Creating a parser \[https://library.humio.com/data-analysis/parsers-create.html\]](https://library.humio.com/data-analysis/parsers-create.html).

Note: Next-Gen SIEM detections expect fields that are normalized to a common schema according to the [CrowdStrike Parsing Standard \[https://library.humio.com/integrations/packages-pasta.html\]](https://library.humio.com/integrations/packages-pasta.html).



7. Optional. In the **Test data** section, add, delete, and run tests using sample data.
8. Click **Save and exit**.

To create a new data connection using a parser, follow the steps in [Add a data connection using a parser \[documentation/page/n00d51ed/parsers#i811cfd9\]](#).

Add a data connection using a parser

Create a new data connection using a parser.

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.
2. In the **Parsers** table, search or filter for your parser.
3. Click **Open menu**  for the parser.
4. In the menu, click **Create connection from parser**.
The **New connection** dialog opens.
5. In the **New connection** dialog, select the delivery method for your third-party data. For example, you can ingest data using Cribl Stream or the HEC protocol.
6. Click **Next**.
The **Add a new connector page** opens.
7. In the **Add new connector** page, enter a name and optional description to identify the connector.
8. Click the **Terms and Conditions** box, then click **Save**.
9. 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**.
10. 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 \[documentation/page/a76b8289/data-connectors#c42a73ec\]](#).

Generate a parser with AI

In addition to creating a parser from scratch, cloning an existing parser, or importing your parser, you can now generate a new parser with AI by simply uploading a sample log file. For more info on creating parsers, see [Manage parsers \[documentation/page/a76b8289/data-connectors#v43a2825\]](#).

Parsers use scripts written in CrowdStrike Query Language to transform incoming data into searchable events that trigger detections in Next-Gen SIEM. You can use default parsers to parse incoming data in common formats. For more info on parsing data, see [Parsing Data \[https://library.humio.com/data-analysis/parsers.html\]](#). For more information on CrowdStrike Query Language, see [Get Started with CrowdStrike Query Language \[documentation/category/nbb7a91/event-investigation/get-started-with-crowdstrike-query-language\]](#).

Create a new parser

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors\]](#) and click the **Parsers** tab.
2. Click **Add new parser**.
3. In **Create new parser**, enter a name for your parser.
4. In the dropdown, ensure **blank template** is selected.
5. Click **Create**. The **Edit parser** page opens.

Generate a parser

Important: The LLM powering this feature is hosted in the US region, and the inputted sample logs are transmitted to this LLM.

1. Click **Generate parser**. The **Generate a parser with AI** dialog opens.
2. Upload a TXT or CSV sample log file of the data from which you want to create a parser.

Note: Files should be set up as newline delimited and must not exceed 10,000 characters.

3. Select the log format of your sample log file:

- NDJSON
- Unstructured (for example, syslog)
- CSV

4. Add keywords such as the source of the log file, technology, or version info.

Note: Keywords must be at most 1,000 characters.

5. Select **Generate Parser**. The **Generate a parser with AI** build window opens. You can expect the parser generation to take up to 5 minutes.

Note: You can only minimize the build window, not close it. If you minimize the window, the parser generation will continue to run in the background until complete. You will not be able to do any other work in the Falcon console until the build is complete.

The **Edit parser** page reappears with the AI-generated parser in the Parser script section.

Note: Next-Gen SIEM detections expect fields that are normalized to a common schema according to the [CrowdStrike Parsing Standard \[documentation/page/u05f69c9/crowdstrike-parsing-standard\]](#).

Verify the parser

1. In the Test data section, add, delete, and run tests using sample data to verify the generated parser.

Note: Select **Use CPS** as an additional verification test. Based on the test data results, make changes to the parser.


2. Reject and regenerate the parser.

3. Once you have zero errors, click **Save and exit**.

For more info about associating the parser with a data connector, see [Data Connectors \[documentation/page/a76b8289/data-connectors\]](#).

Clone a parser

Clone an existing parser.

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.
2. In the **Parsers** table, click **Open menu**  for the parser you want to clone.
3. Click **Clone parser**.
4. In **Create new parser**, enter a name for your new parser.
5. Click **Create**. The **Edit parser** page opens.
6. In the **Parser script** section, enter your parser script in CrowdStrike Query Language. For more info on writing parser scripts, see [Creating a parser \[https://library.humio.com/data-analysis/parsers-create.html\]](#).


Note: Next-Gen SIEM detections expect fields that are normalized to a common schema according to the [CrowdStrike Parsing Standard \[https://library.humio.com/integrations/packages-pasta.html\]](#).

7. Optional. In the **Test data** section, add, delete, and run tests using sample data.
8. To save your changes, click **Save and exit**.

Edit a parser

Edit a custom parser's script.

Note: Only custom parsers are editable.


1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.
2. In the **Parsers** table, click **Open menu**  menu for the parser you want to edit.
3. Click **Edit parser**. The **Edit parser** page opens.
4. In the **Parser script** section, enter your parser script in CrowdStrike Query Language. For more info on writing parser scripts, see [Creating a parser \[https://library.humio.com/data-analysis/parsers-create.html\]](#).

Note: Note: Next-Gen SIEM detections expect fields that are normalized to a common schema according to the [CrowdStrike Parsing Standard \[https://library.humio.com/integrations/packages-pasta.html\]](#).

5. Optional. In the **Test data** section, add, delete, and run tests using sample data.
6. To save your changes, click **Save and exit**.

Export a parser


Export a parser as YAML to use when creating a new parser.

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.
2. In the **Parsers** table, click **Open menu**  for the parser you want to export as a YAML file.
3. Click **Export parser**.
4. Select a name and destination for your parser script.
5. Click **Save**.

Delete a parser

Delete a custom or inactive parser.

Note: You cannot delete default parsers or parsers that are currently in use.

1. Go to [Next-Gen SIEM > Log management > Data onboarding \[data-connectors/parsers\]](#) and click the **Parsers** tab.
2. In the **Parsers** table, click **Open menu**  for the parser you want to delete.
3. Click **Delete parser**, and then click **Delete parser**.

< [Data Connectors\[documentation/page/a76b8289/data-connectors\]](#)