

# Data Connectors

*Last updated: Jul. 16, 2025*

## Overview

Create data connectors in the Falcon console to automate and manage ingestion from third-party data sources. You can seamlessly bring in data from a range of CrowdStrike Store applications for downstream analysis and processing in Falcon to unlock insights and enhance your overall security posture.

## Requirements

**Subscription:** Falcon Next-Gen SIEM or Falcon Next-Gen SIEM 10GB

**Default roles:**

- Connector Manager: Can create, view, and manage connectors, parsers, alerts, and alerts settings.
- Connector Viewer: Can view connectors, parsers, alerts, and alerts settings.
- Falcon Administrator: Can create, view, and manage connectors, parsers, alerts, and alerts settings.

**Custom role permissions:**

- Third Party Ingest:
  - Read data connector
  - Write data connector
  - Read data connectors alerts
  - Write data connectors alerts
  - Read data connectors notification preferences
  - Write data connectors notification preferences
  - Read permission on parser
  - Write permission on parser
- Marketplace Services:
  - Activate store app
  - Read store app
  - Create app config
  - Delete app config
  - Read app config
  - Update app config
  - Read app config schema

**CrowdStrike clouds:** Available in US-1, US-2, and EU-1. For info about the availability of data connectors in US-GOV-1, see the documentation specific to the data connector.

## Understanding third-party connectors

Connectors offload the complexity around setting up and managing data ingestion pipelines from sources outside of Falcon. You create connectors in the Falcon console and configure settings on the data source that set up the service-to-service integration between the third-party system and the Falcon cloud. The connector facilitates secure access to the data source, automates ingestion, and sends ingested data to a predefined destination in Falcon for processing.

## Data sources

Data connectors support data ingestion from select data sources. You can view the supported data connectors available for configuration from the Falcon console at [Next-Gen SIEM > Log management > Data onboarding \[/data-connectors\]](#) or [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).

## Connector types

Falcon uses two types of connectors, which are defined by the way data is served up from the source. Based on the nature of the interaction between Falcon and the data source, a connector operates in either a push- or pull-based manner.

- Push-based connectors: Push connectors let other systems send, or “push,” data to Falcon. The data source drives the transfer operation and pushes new data to a CrowdStrike-provided URL whenever it’s available.
- Pull connectors manually retrieve, or “pull,” data from a source. Data is pulled from a third-party data source, such as a vendor’s API. The schedule and frequency of the data retrieval depends on the data connector.

# Provisioning

Part of the connector setup process includes configuration at the data source level. Each provider has its own unique settings and details that are required. Depending on the connector type, this configuration occurs at a different point in the workflow and in either the Falcon console or the provider interface.

## Pull connectors

Pull connectors contain a **Data source configuration** model with provider-specific fields that define how Falcon should access and retrieve data from the source. When creating a new connector in the Falcon console, the system prompts you to create a data source configuration and presents you with the fields required by your data source. This configuration is saved in Falcon and can be reused in other connectors your organization creates for the data source. For more info, see [Add a pull-based connector. \[/documentation/page/a76b8289/data-connectors#za3a529d\]](#) To learn more about specific provider configuration field requirements, see the [CrowdStrike third-party integration documentation \[/documentation/page/a76b8289/data-connectors#c42a73ec\]](#) for your data source.

## Push connectors

Falcon assigns each push connector a unique ingest URL and key. After creating a connector in the Falcon console, you enter this info and configure other settings directly on the third-party system that define how to push data on the URL with the key. You can find more info about required configuration steps in the [CrowdStrike third-party integration documentation \[/documentation/page/a76b8289/data-connectors#c42a73ec\]](#) for your data source.

# Third-party data source integration guides

Find detailed information about data ingestion configuration in the CrowdStrike documentation for your data source.

- [Third-Party Data Sources \[/documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations\]](#)
- Falcon Insight for ChromeOS: [Set up data ingestion \[/documentation/page/efac85ed/falcon-insight-for-chromeos#sf522067\]](#)

## Limits

Each data connector has data ingestion limits for both size and rate. These limits can vary by type of connector as well as per product or vendor.

For specific information about each connector's limits, refer to the connector's setup documentation at [Third-Party Data Sources \[/documentation/category/je6a45b3/next-gen-siem/third-party-integration-and-data-connectors/third-party-integrations\]](#).

## Event truncation behaviors

When events are too large to be ingested, they can be truncated. Truncation behavior differs depending on the connector type, ingestion endpoint, vendor configuration, and other factors.

- **Simple removal:** Data from the end of the event is removed until the event is within the size limit.
- **Field removal:** If the event contains fields, the fields are sorted and removed in reverse alphabetical order (z-a) until the event is within the size limit. Tags are not removed from the event. If the event does not contain fields, or if the event is still too large after structured fields are removed, data from the end of the event is removed until the event is within the size limit.
- **Discarded:** If the event is larger than the size limit, the event is not ingested.

To identify events that have been truncated, look for these indicators:

- The raw message ends with an ellipsis (...).
- An extra field, **@error\_msg**, is appended to the event.
- The event field **@error** has the value **True**.

## Limits for push-based connectors

For push-based connectors, the data ingestion limits are different depending on which data ingestion URL the connector uses.

Endpoint	Max payload size	Max event size	Event truncation behavior	Max tag key length	Max tag value length
/hec/<datasource_id>/v1/services/collector/event /hec/v1/services/collector/event https://<datasource_id>.<baseURL>/services/collector	16,000,000 bytes / ~16 MB	950,000 bytes / ~1 MB	Field removal	65535	65535
/hec/<datasource_id>/v1/services/collector /hec/v1/services/collector	16,000,000 bytes / ~16 MB	950,000 bytes / ~1 MB	Field removal	65535	65535
/hec/<datasource_id>/v1/services/collector/raw /hec/v1/services/collector/raw	16,000,000 bytes / ~16 MB	950,000 bytes / ~1 MB	Simple removal	Not applicable	Not applicable
/humio/<datasource_id>/v1/humio-structured	16,000,000 bytes / ~16 MB	950,000 bytes / ~1 MB	Field removal	65535	65535
/humio/<datasource_id>/v1/humio-unstructured	16,000,000 bytes / ~16 MB	950,000 bytes / ~1 MB	Field removal	65535	65535

/humio/<datasource_id>/v1/raw	1 MB	950,000 bytes / ~1 MB	Simple removal	Not applicable	Not applicable
-------------------------------	------	-----------------------	----------------	----------------	----------------

There is no limit per connector on the number of events ingested per second.

### Limits for pull-based connectors

For pull-based connectors, polling frequency limits are different for each connector depending on the third-party vendor's configurations.

Data connector	Polling frequency limit	Max event size	Event truncation behavior
1Password Business Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Abnormal Security Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Akamai Secure Internet Access Enterprise (SIA) Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Armis Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Cisco Duo MFA Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft Defender XDR Alerts & Incidents	Every 10 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft DLP	Every 10 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft Exchange Online	Every 5 mins	950,000 bytes	Simple removal
Data Connector built for Microsoft Graph API, providing data for Microsoft Azure AD Directory Audits	Every 5 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft Graph API, providing data for Microsoft Azure AD SignIns	Every 5 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft Graph API, providing data for Microsoft Defender Identity	Every 10 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft Graph API, providing data for Microsoft Defender O365 Email	Every 10 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft O365 Message Trace	Every 10 minutes	950,000 bytes	Simple removal
Data Connector built for Microsoft Sharepoint	Every 10 minutes	950,000 bytes	Simple removal
ForgeRock Data Connector	Every 5 minutes	950,000 bytes	Simple removal
Menlo Security Data Connector	Every 5 minutes	950,000 bytes	Simple removal
Mimecast Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Netskope Data Connector	Every 10 minutes	950,000 bytes	Simple removal
Okta Data Connector	Every minute	950,000 bytes	Simple removal
Proofpoint Data Connector	Every 10 minutes	950,000 bytes	Simple removal

### Limits for streaming-based connectors

For streaming-based connectors, the data ingestion limits are different depending on the third-party vendor.

Data connector	Max event size	Event truncation behavior
Data Connector built for Azure Virtual Machines	950,000 bytes	Simple removal
Data Connector built for Generic Microsoft Azure Event Hubs	950,000 bytes	Simple removal
Data Connector built for Generic Microsoft Azure Event Hubs	950,000 bytes	Simple removal
Data Connector built for Microsoft Azure Firewall	950,000 bytes	Simple removal
Data Connector built for Microsoft Azure Network Security Groups	950,000 bytes	Simple removal
Data Connector built for Microsoft Azure VPN Gateway	950,000 bytes	Simple removal
Data Connector built for Microsoft Defender for Cloud	950,000 bytes	Simple removal
Data Connector built for Microsoft Defender for Identity	950,000 bytes	Simple removal
Data Connector built for Microsoft Defender XDR Events	950,000 bytes	Simple removal

Data Connector built for Microsoft Entra ID	950,000 bytes	Simple removal
Google Cloud Audit Logs Data Connector	950,000 bytes	Simple removal
Google Cloud Pub/Sub Data Connector	950,000 bytes	Simple removal
Google Workspace Data Connector	950,000 bytes	Simple removal
Netskope Transaction Logs Data Connector	950,000 bytes	Simple removal

### Limits for AWS S3-based connectors

For AWS S3-based connectors, the data ingestion limits are different depending on the third-party vendor and product.

Data connector	Max event size	Event truncation behavior
Amazon CloudWatch Data Connector	950,000 bytes	Simple removal
Amazon GuardDuty Data Connector	950,000 bytes	Simple removal
Amazon S3 Access Log Data Connector	950,000 bytes	Simple removal
Amazon S3 Data Connector	950,000 bytes	Simple removal
Amazon Security Lake Data Connector	950,000 bytes	Simple removal
AWS Cloudtrail Data Connector	950,000 bytes	Simple removal
AWS Config Data Connector	950,000 bytes	Simple removal
AWS Network Firewall Data Connector	950,000 bytes	Simple removal
AWS Security Hub Data Connector	950,000 bytes	Simple removal
AWS VPC Flow Data Connector	950,000 bytes	Simple removal
AWS WAF Data Connector	950,000 bytes	Simple removal
Cisco Umbrella Data Connector	950,000 bytes	Simple removal

## Manage connectors

**Important:** New data connector setup and configuration features are currently being released in phases across CrowdStrike clouds. Setup instructions may not fully reflect your Falcon console environment.

### Add a new connector

Connectors are configured from the Falcon console at [Next-Gen SIEM > Log management > Data onboarding \[/data-connectors\]](#) or [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).


The process is different for data that must be pushed or pulled from the source. For more info, see [Add a push-based connector \[/documentation/page/a76b8289/data-connectors#i942acfc\]](#) and [Add a pull-based connector \[/documentation/page/a76b8289/data-connectors#za3a529d\]](#).

**Tip:** You can also create a data connection using a parser from the **Parsers** tab in [Next-Gen SIEM > Log management > Data onboarding \[/data-connectors\]](#). For more info, see [Add a data connection using a parser \[/documentation/page/n00d51ed/parsers#i811cfd9\]](#).

### Add a pull-based 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.
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 dialog appears. Click **Accept** to continue configuration.

5. In the **Add new connector** page, click **Manage configurations**.
6. Create a configuration by entering values for the required fields in the configuration window or select an existing configuration. To edit a configuration from this window, select **Edit** , then modify the field values.

**Important:** For information about the required vendor-specific configuration fields, see the [Third-party data source integration guides \[/documentation/page/a76b8289/data-connectors#c42a73ec\]](#). Modifications to a configuration are applied anywhere the configuration is used.

7. Enter a name and an optional description to identify the connector.
8. Click the **Terms and Conditions** box, then click **Save**.

## Add a push-based 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 \[/documentation/page/a76b8289/data-connectors#c42a73ec\]](#).

## View and manage connections

**Status of connections:** View total counts per status and number of data connections.

**Data ingest:** In this chart, compare 30-day average and measured data ingest volumes, to optimize storage, costs, and resources.

- **Next-Gen SIEM:** View the daily data ingest volume as a 30-day moving average, for Next-Gen SIEM only. Click **Other** to update the chart with ingest totals from other Falcon subscriptions, like [Falcon Discover for IoT \[/documentation/category/db2748e6/xiot-security/xiot-asset-management\]](#) and [Endpoint Security \[/documentation/category/b67b4178/endpoint-security\]](#).

**Connections:** See a summary information and access management capabilities for each connection.

- **Connection name:** The name you gave the connection when you configured it.
- **Vendor:** The name and logo of the company that the data source belongs to.
- **Product:** The name of the product to which the data source belongs to.
- **Connector type:** The type of connection defined by ingestion type. Ingestion type is either **Push** or **Pull**.
- **Status:** The status of the connection.
  - **Pending:** A connection whose configuration is still in progress and not completed.
  - **Disconnected:** The connection is down and data is not being ingested.
  - **Paused:** The data connection is paused and cannot ingest or receive data.
  - **Active:** A data connection receiving data with no error (has received data at least in one hour).
  - **Idle:** A data connection that did not receive any data in the last one hour is an idle data connection.
  - **Error:** A data connection that encountered an error in the last one hour is set to state Error. Click the **Error** link to see all errors for the selected data connection in **Advanced Event Search**. For more info about errors, see [Show error history](#).
- **Ingest (24h):** The volume of data ingested by a connector in the last 24 hours, displayed in bytes.




**Note:** A returned quantity of zero indicates the data connector has not ingested any data and might be misconfigured. For troubleshooting suggestions, see [Data connection errors \[/documentation/page/a76b8289/data-connectors#u5bae034\]](#).

- **Parser:** The parser used by the data connection.
- **Subscription:** The part of the Falcon platform that is receiving the data, based on your Falcon subscription. Subscriptions include [Falcon Next-Gen SIEM \[/documentation/category/f090d800/next-gen-siem\]](#), [Falcon Discover for IoT \[/documentation/category/db2748e6/xiot-security/xiot-asset-management\]](#), and [Endpoint Security \[/documentation/category/b67b4178/endpoint-security\]](#).
- **Actions:** Options to view and manage a connection. Click **Open menu** ⋮ to see available actions. The list of actions changes based on the type of connector. For example, the **Generate API key** action is only available for Push-based connectors. The full list of actions includes **Show details**, **Edit connection**, **Generate API key**, **Regenerate API key**, **Show error history**, **Show events**, and **Regenerate CFT URL**.

## View connection details

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).
2. In the **Actions** column, click **Open menu** ⋮ and select **Show details**.
3. In the **Connection details** page, review the connection name, description, status, data source, and the time and size of the last data ingestion. See either


the API URL for push connectors or the data source configuration name for pull connectors.

4. You can also manage connections, such as **Edit**  or **Delete**  connections, or Regenerate an API key  for push-based connectors, from this page.

## Edit a connection

You can edit the name and description of an existing connection. For pull-based connection, you can also modify the data source configuration if you want to ingest a different dataset. If your connection has **Enable parser selection** available, you can also change which parser is used to transform incoming data. For more info on parsers, see [Manage parsers \[documentation/page/a76b8289/data-connectors#v43a2825\]](#).

**Note:** The connector's data source and the assigned API URL (push-based connectors) cannot be changed.

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[data-connectors\]](#).
2. In the **Actions** column, click **Open menu**  and select **Edit connection**. The **Connection details** page opens.
3. Make changes to the connection name, description, selected parser, or for pull-based connections make data source configurations as needed.
4. Click **Save changes**.

## Generate a push connector API key

You generate an API key when you configure a **Push** connector. If you lose your API key or suspect that it's been compromised, you can generate a new one.


1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[data-connectors\]](#).
2. In the **Actions** column, click **Open menu**  and select **Generate API key**. If you need to regenerate an API key, select **Regenerate API key**.

**Important:** When you regenerate an API key, the old key is no longer active. You must configure any third-party systems or data shippers with the new API key. All access tokens issued before regenerating the API key are immediately invalidated when the new key is created.

## Pause a connection

**Note:** This action is only available for **Push** type connectors with a **Status** of **Active**, **Error**, or **Idle**.

Pausing a data connection stops the flow of data from your applications until resumed. You can temporarily pause a connection from the **Connections** table:


1. In the **Actions** column, click **Open menu**  and select **Pause connection**.
2. In the **Pause connection** dialog, click **Pause connection**.

When a connection is paused, the **Actions** menu shows the **Resume connection** option. Click **Resume connection** to enable the flow of data from your application to Next-Gen SIEM.

## Delete a connection


You can delete a connection that you no longer need.

**Important:** After a connection is deleted it's permanently removed from the system and cannot be restored.

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[data-connectors\]](#).
2. In the **Actions** column, click **Open menu**  and select **Delete connection**.
3. A confirmation prompt appears. Click **Delete connection** to confirm deletion.

## Show error history


You can learn more about errors generated by a data connection by accessing **Advanced Event Search** from the **Data Connections** page.

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[data-connectors\]](#).
2. In the **Actions** column, click **Open menu**  and select **Show error history**.
3. The **Advanced event search** page opens and an error query is run.
4. Review **Results** to learn more about an error.

To learn more about investigating errors, see [Data connection errors \[documentation/page/a76b8289/data-connectors#u5bae034\]](#).

## Show events

You can see a full list of events generated by a data connection by accessing **Advanced Event Search** from the **Data Connections** page.

1. In the Falcon console, go to **Data connectors > Data connectors > Data connections**.
2. In the **Actions** column, click **Open menu**  and select **Show events**.
3. The **Advanced event search** page opens and an events query is run.
4. Review **Results** to learn more about an event.

## View audit logs

You can review third-party data connection activities in the Falcon console as audit logs:

1. Go to [Audit logs > Audit logs > Falcon UI \[/audit-log/falcon-console/\]](#).
2. From the **Category** filter, select **Third party data connections**.

Audit logs for third-party data connections display this information:

- **Time:** The action's date and time.
- **Analyst:** The email address associated with the action.
- **Action:** The action's type. These actions generate logs:
  - Data connection creation
  - Data connection update
  - Data connection pause
  - Data connection resume
  - Data connection deletion
  - API key generation
  - API key regeneration
  - Data connection state update
  - Alert status update
- **Activity details:** The data connection name and ID associated with the action.

**Note:** For the **Data connection update** action only, change details about connection properties are also available. For example, "Name": {"Old": "user\_hec1", "New": "user\_hec2"}.

- **User IP, City, State, Country, and Company:** Location and company details where the change occurred.

## Manage alerts for third-party data connectors

You can receive alerts as email notifications and view your alerts in the Falcon console when a third-party data connector in your environment is disconnected or has not received data for the past 24 hours.

### Manage alerts

Go to [Data connectors > Data connectors > Alerts \[/data-connectors/alerts\]](#) to view and manage your third-party data connector alerts and alerts settings.

#### View alerts

Your alerts are displayed in the **Alerts** table. You can search for alerts by name, filter alerts by the impacted connector name or alert status, or sort them by when they last occurred. Alerts can be in **New**, **In review**, or **Resolved** status.

The count on the **Alerts** tab displays the current number of new alerts.

**Note:** The **Alerts** table filters and displays **New** and **In review** alerts by default. To view all alerts, click **Clear all** to remove all filters.

#### View alert details

To view details for an alert, click the alert name or click **Open menu**  and then click **View alert details**.

#### Resolve common issues

Review the alert log on an alert's detail page. The alert log varies for each alert and each connector. For common issues, take these remediation actions:

Alert log error code	Remediation action
401	Verify and update your third-party data source credentials (API key, token, app ID, and so on) and data connector configuration.
403	Ensure that your connector configuration is authorized to connect to the third-party data source.


#### View connector details

To view details for a connector you received an alert for, click the name of the connector in the **Alerts** table.

You are taken to the connector's details page in the [My connectors \[/data-connectors/connectors\]](#) tab. Verify info about the connector's current status, last data ingestion time and quantity, and API authorization URL. See [View connector details \[/documentation/page/a76b8289/data-connectors#a357f777\]](#) for more info.

#### Update alert status

Your alerts can be in **New**, **In review**, or **Resolved** status. This helps other users in your environment determine which alerts are new and need attention, are currently under review, or have been reviewed.

To update a new alert's status, click **Open menu**  for the alert in the **Alerts** table and then click **Mark as in review** or **Mark as resolved**.

To update an in-review alert's status, click **Open menu** ⋮ for the alert in the **Alerts** table and then click **Mark as resolved**.

## Manage alerts settings

Go to [Data connectors > Data connectors > Alerts \[/data-connectors/alerts\]](#) and then click **Manage alerts settings**.

Alerts settings

Manage all of your connector alerts from one place.

Notification preferences

Notify by

Email

Recipients

user@crowdstrike.com

System alerts

Automatically resolve alerts within 30 days

On

Alert if connector is disconnected

On

Alert if connector receives no data in 24 hours

On

### Set email notification preferences

1. In the **Notification preferences** section of the **Alerts settings** dialog, click **Edit** ✎.
2. In the **Recipients** field, enter up to 10 email addresses for users in your environment who should receive email alerts.

**Note:** Specified recipients must have email addresses ending in your organization's domain.

3. Click **Save changes**.

**Note:** If you do not enter any email recipients, the first 10 Falcon Admins in your environment, in alphabetical order of email addresses, are sent email notifications for alerts.

### Set alerts

In the **System alerts** section of the **Alerts settings** dialog, update these settings:

1. Enable the **Automatically resolve alerts within 30 days** setting to automatically set the status of alerts older than 30 days as **Resolved**.
2. Enable the **Alert if connector is disconnected** setting to receive alerts when a connector in your environment is disconnected.
3. Enable the **Alert if connector receives no data in 24 hours** to receive alerts when a connector in your environment has not received any data for the past 24 hours.

**Note:** The **Automatically resolve alerts within 30 days**, **Alert if connector is disconnected**, and **Alert if connector receives no data in 24 hours** settings are enabled by default. If you disable these alerts settings, it may take up to 1 minute for alerts to appear when you enable them again.

Click **Close** ✕ to close the **Alert settings** dialog.

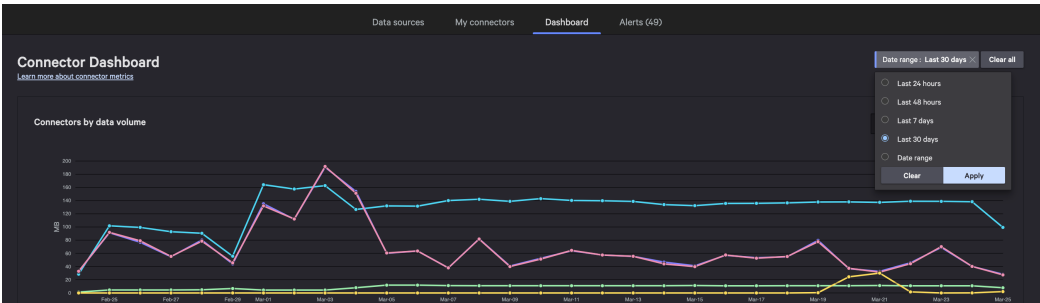
## View ingestion volume dashboard for third-party data connectors

The **Connector Dashboard** displays near real-time information to monitor the amount of data ingested from third-party sources over a period of time for your CID. Gain insight on how your data ingestion volume compares to your subscribed data ingestion volume limit.

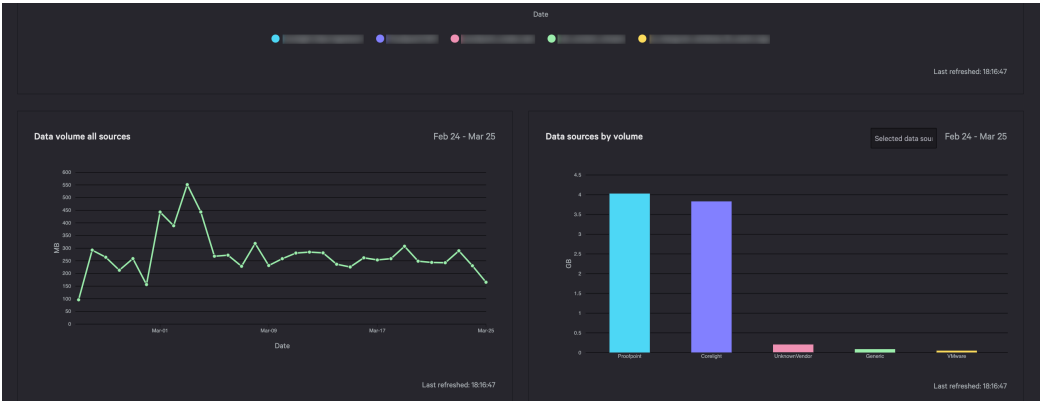
**Note:** The **Connector Dashboard** only displays info for your current CID.

To view the ingestion volume dashboard, go to [Data connectors > Data connectors > Dashboard \[/data-connectors/dashboard\]](#). The default time period for the ingestion volume dashboard is **Last 30 days**. To specify a different time period, click **Date Range** and select a time period from these options:

- **Last 24 hours**
- **Last 48 hours**
- **Last 7 days**
- **Last 30 days**
- **Date Range:** Specify a time period up to 90 days by selecting a start and end date.







Each section of the **Connector Dashboard** displays relevant info:

Section	Description and usage
Connectors by data volume	The volume of data ingested by each connector over a specified time period. Click <b>Select connectors</b> in this section to search for and select data sources.
Data volume all sources	Total volume of data ingested by all your connectors over a specified time period.
Data sources by volume	The total volume of data ingested from each data source over a specified period of time. Click <b>Select data sources</b> in this section to search for and select data sources.

## Manage parsers

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 [Parsers \[documentation/page/n00d51ed/parsers\]](#) and [Parsing Data \[https://library.humio.com/data-analysis/parsers.html\]](#).

## Manage Third-Party Detection Exclusions

If the Falcon console is showing detections generated from ingested third-party data that you don't want to see, you can create exclusions. These exclusions prevent detections from being generated, based on criteria you specify. For more info, see [Third-Party Detection Exclusions \[documentation/page/i499c81a/third-party-detection-exclusions-0\]](#).

## Common issues

### Data connection errors

Connection errors occur for multiple reasons. For example, data may be invalid or missing, or resources required for configuration may be missing, or the data connection may not be authorized to authenticate with a third-party system.

In the **Data Connections** page, the **Error** status is displayed for connections that encounter data ingestion errors in the last hour. Begin your error investigation from this page.

1. In the Falcon console, go to [Data connectors > Data connectors > Data connections \[data-connectors\]](#).
2. Run the automatically generated error query in **Advanced Event Search**. In the **Status** column, click **Error** or in the **Actions** column, click **Open menu** : and select **Show error history**. An example of an error query:

```
#repo.cid = <customer-id> | #repo = 3pi_connection_errors | @dataConnectionID = <id_of_connection>
```

**Tip:** If you need to troubleshoot parser errors, you can run this query, which includes the parser errors and excludes the connection errors:  
`#repo.cid = <customer-id> | #error=true | #repo != 3pi_connection_errors | @dataConnectionID=<id_of_connection>.`

- `#repo.cid = <customer-id>`: Scopes errors to a specific customer ID (CID).
- `#repo=3pi_connection_errors`: The repository where all data connection errors are stored.
- `@dataConnectionID=<id_of_connection>`: The ID of a data connection.

3. In **Advanced Event Search**, the error query runs and results are returned.
4. In the **Results** tab, review the **Field List** content to learn more about an error.

```
#error:true
#repo:3pi_connection_errors
#repo.cid:82769abc90834def088bg688ccd5h123
#type:json
@dataConnectionID:b1234b5dc67a408c912e34f7ab12c8d9
@error:true
@error_msg: Ingest credentials don't have permissions. Verify all required permissions as per
connector integration guide have been granted
@event_parsed:false
@id:5abcdXY9RkMnA3stuvWxPyZ3_12_345_1234567890
@ingesttimestamp:1739570223511
```

```
@rawstring:{@error_msg::Ingest credentials don't have permissions. verify all required permissions
as per connector integration guide have been
granted","status_code":404,"@error":true,"@timestamp":"2025-02-14T21:57:02Z","error_count":1}
```

- Error field definitions

- @error\_msg: The string provided by the third-party system. This string can be plain text or JSON. You can click any **Field List** entry and click **Message** to view the error message. An error message provides more details about an error that stems from a third-party system. For example, an error message can notify you of permissions or misconfiguration issues in a third-party system.
- status\_code: The status code received from the third-party system.
- error\_count: The number of times an error occurs in a short period of time. For example, if you misconfigured the LogScale Collector or another data shipper during data connector setup, this appears as one event in search. However, the associated error count reflects the total number of requests that are reported as failed.
- @timestamp: When the error occurred. If not provided, the timestamp is set to the current time. A timestamp can be used to correlate errors with changes that might have occurred in your environment around that time. For example, if an error occurs not long after you changed a client or access token in a Pull-based connector configuration or modified settings in a third-party system.

## Reference

Use these reference materials to help plan for setup and configuration of multiple data connectors.

## Microsoft connectors

Use the data in this table to streamline the set up and configuration of multiple Microsoft connectors:

- Learn which connectors ingest the types of data you're already using.
- See which connectors use the same transport protocol, like Azure Event Hubs, to help with configuration and avoid duplicate data ingestion.

Details about the categories included in this table:

- **Type:** The connector type, as listed in the **Data Connections** page. For more info, see [View and manage connections](#) [/documentation/page/a76b8289/data-connectors#r7b8be88]. Data connectors either push or pull data from a source. To learn more, see [Connector types](#) [/documentation/page/a76b8289/data-connectors#l86520cd].
- **Transport protocol:** The protocol used by the data connector to retrieve data from Microsoft.
- **Data Collected:** The type of data collected by each connector, such as logs, events, or alerts.
- **Parser:** The name of the parser associated with the data connector.
- **Notes:** Helpful information related to set up, configuration, and management of each data connector.

Integration Guide	Type	Transport Protocol	Data Collected	Parser	Notes
<a href="#">Data Connector built for Microsoft Defender XDR Events</a> [/documentation/page/j06b4388/data-connector-built-for-microsoft-defender-xdr]	Push	Azure Event Hubs using the <a href="#">Streaming API</a> [https://learn.microsoft.com/en-us/defender-xdr/streaming-api]	All Advanced Hunting events and alerts. For more info, see <a href="#">Hunting tables support status in Event Streaming API</a> [https://learn.microsoft.com/en-us/defender-xdr/supported-event-types#hunting-tables-support-status-in-event-streaming-api].	microsoft-defendero365-eventhubs	
<a href="#">Data Connector built for Microsoft Defender XDR Alerts &amp; Incidents</a> [/documentation/page/iab821ac/data-connector-built-for-microsoft-defender-xdr-alerts-incidents]	Pull	<a href="#">Microsoft Graph API</a> [https://learn.microsoft.com/en-us/graph/use-the-api]	Defender XDR alerts and Defender XDR incidents. For more info, see <a href="#">alert resource type</a> [https://learn.microsoft.com/en-us/graph/api/resources/security-alert?view=graph-rest-1.0] and <a href="#">incident resource type</a> [https://learn.microsoft.com/en-us/graph/api/resources/security-incident?view=graph-rest-1.0].	microsoft-defendero365-graphapi	
<a href="#">Data Connector built for Microsoft Defender for Cloud</a> [/documentation/page/ze713e6a/data-connector-built-for-microsoft-defender-for-cloud]	Push	Azure Event Hubs using <a href="#">Continuous Export</a> [https://learn.microsoft.com/en-us/azure/defender-for-cloud/benefits-of-continuous-export]	Defender for Cloud security alerts. For more info, see <a href="#">Security alerts - a reference guide</a> [https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference].	microsoft-defender-cloud	Not necessary if Defender XDR Events Connector is already enabled.
<a href="#">Data Connector built for Microsoft Defender for Cloud Apps</a> [/documentation/page/z39d761a/data-connector-built-for-microsoft-defender-for-cloud-apps]	Push	HEC Push using a <a href="#">SIEM Agent</a> [https://learn.microsoft.com/en-us/defender-cloud-apps/siem] over syslog	Defender for Cloud Apps alerts and Defender for Cloud Apps activity logs. For more info, see <a href="#">Sample activity logs</a> [https://learn.microsoft.com/en-us/defender-cloud-apps/siem#sample-activity-logs].	microsoft-defender-cloudapps	Not necessary if Defender XDR Events Connector is already enabled.

<a href="#">Data Connector built for Microsoft Defender for Identity</a> [ <a href="#">/documentation/page/qa99cc3d/data-connector-built-for-microsoft-defender-for-identity</a> ]	Push	Azure Event Hubs using the <a href="#">Streaming API</a> [ <a href="#">https://learn.microsoft.com/en-us/defender-xdr/streaming-api</a> ]	Identity-specific Advanced Hunting events: <ul style="list-style-type: none"> <li>• IdentityDirectoryEvents</li> <li>• IdentityInfo</li> <li>• IdentityLogonEvents</li> <li>• IdentityQueryEvents</li> </ul> For more info, see <a href="#">Supported Microsoft Defender XDR streaming event types in event streaming API</a> [ <a href="#">https://learn.microsoft.com/en-us/defender-xdr/supported-event-types</a> ] .	microsoft-defender-identity	Not necessary if Defender XDR Events Connector is already enabled.
<a href="#">Data Connector built for Microsoft Entra ID</a> [ <a href="#">/documentation/page/zd4ca92c/data-connector-built-for-microsoft-entra-id</a> ]	Push	Azure Event Hubs	Entra ID activity logs: <ul style="list-style-type: none"> <li>• AuditLogs</li> <li>• SignInLogs</li> <li>• ProvisioningLogs</li> <li>• MicrosoftGraphActivityLogs</li> <li>• NonInteractiveUserSignInLogs</li> <li>• RiskyUsers</li> <li>• UserRiskEvent</li> <li>• ManagedIdentitySignInLogs</li> <li>• ServicePrincipalSignInLogs</li> </ul> For more info, see <a href="#">Log categories</a> [ <a href="#">https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-configure-diagnostic-settings#log-categories</a> ] .	microsoft-entra-id	
<a href="#">Data Connector built for Azure Virtual Machines</a> [ <a href="#">/documentation/page/m22bf272/data-connector-built-for-azure-virtual-machines</a> ]	Push	Azure Event Hubs using <a href="#">Log Analytics Workspace</a> [ <a href="#">https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview</a> ]	Windows events and Syslog events.	microsoft-azure-vm	
<a href="#">Data Connector built for Microsoft Azure Firewall</a> [ <a href="#">/documentation/page/jd3ba8c7/data-connector-built-for-microsoft-azure-firewall</a> ]	Push	Azure Event Hubs	All Azure Firewall Resource logs. For more info, see <a href="#">Resource logs</a> [ <a href="#">https://learn.microsoft.com/en-us/azure/firewall/monitor-firewall-reference#resource-logs</a> ] .	microsoft-azure-firewall	
<a href="#">Data Connector built for Microsoft Azure WAF</a> [ <a href="#">/documentation/page/ec3f3acd/data-connector-built-for-microsoft-azure-waf</a> ]	Push	Azure Event Hubs with two ways to deploy. For more info, see <a href="#">Supported service</a> [ <a href="#">https://learn.microsoft.com/en-us/azure/web-application-firewall/overview#supported-service</a> ] .	WAF resource logs for Application Gateway or WAF resource logs for FrontDoor. Application Gateway logs: <ul style="list-style-type: none"> <li>• Application Gateway Access Logs</li> <li>• Application Gateway Performance Logs</li> <li>• Application Gateway Firewall Logs</li> </ul> For more info, see <a href="#">Enabling logging through the Azure portal</a> [ <a href="#">https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/web-application-firewall-logs#enable-logging-through-the-azure-portal</a> ] . Front Door logs: <ul style="list-style-type: none"> <li>• FrontDoor Access Logs</li> <li>• FrontDoor Health Probe Logs</li> <li>• FrontDoor WebApplicationFirewall Logs</li> </ul> For more info, see <a href="#">Logs and diagnostics</a> [ <a href="#">https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-monitor? pivots=front-door-standard-premium#logs-and-diagnostics</a> ]	microsoft-azure-waf	

			.		
<a href="#">Data Connector built for Azure Network Security Groups [/documentation/page/k1116054/data-connector-built-for-azure-network-security-groups]</a>	Push	Azure Event Hubs	<p>Network Security Group resource logs:</p> <ul style="list-style-type: none"> <li>Event</li> <li>Rule Counter</li> </ul> <p>For more info, see <a href="#">Log categories [https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log#log-categories]</a></p> <p>.</p>	microsoft-azure-nsg	
<a href="#">Data Connector built for Azure NSG Flow Logs [/documentation/page/v76acf23/data-connector-built-for-azure-nsg-flow-logs]</a>	Push	HEC Push using an <a href="#">ARM Template [https://learn.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema#alert-category]</a>	<p>NSF Flow Logs. For more info, see <a href="#">Flow logging for network security groups [https://learn.microsoft.com/en-us/azure/network-watcher/nsg-flow-logs-overview]</a></p> <p>.</p>	microsoft-azure-nsg	
<a href="#">Data Connector built for Microsoft Azure VPN Gateway [/documentation/page/v252d2d9/data-connector-built-for-microsoft-azure-vpn-gateway]</a>	Push	Azure Event Hubs	<p>VPN Gateway resource logs:</p> <ul style="list-style-type: none"> <li>Gateway Diagnostic Logs</li> <li>Tunnel Diagnostic Logs</li> <li>IKE Diagnostic Logs</li> <li>Route Diagnostic Logs</li> <li>P2S Diagnostic Logs</li> <li>VPN Gateway Activity Logs</li> <li>Related alerts</li> </ul> <p>For more info, see <a href="#">Supported Microsoft Defender XDR streaming event types in event streaming API [https://learn.microsoft.com/en-us/defender-xdr/supported-event-types]</a> and <a href="#">Alert category [https://learn.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-schema#alert-category]</a></p> <p>.</p>	microsoft-azure-vpn	
<a href="#">Data Connector built for Generic Microsoft Azure Event Hubs [/documentation/page/g8dab5ba/data-connector-built-for-generic-microsoft-azure-event-hubs]</a>	Push	Azure Event Hubs	<p>Logs depend on the parser selected during connector configuration.</p>	This data connector allows you to select any compatible parser.	
<a href="#">Data Connector built for Microsoft Event Hubs [/documentation/page/gcd5959e/data-connector-built-for-microsoft-event-hubs]</a>	Push	Azure Event Hubs using the <a href="#">Streaming API [https://learn.microsoft.com/en-us/defender-xdr/streaming-api]</a>	<p>All Advanced Hunting events. For more info, see <a href="#">Hunting tables support status in Event Streaming API [https://learn.microsoft.com/en-us/defender-xdr/supported-event-types#hunting-tables-support-status-in-event-streaming-api]</a></p> <p>.</p>	microsoft-defendero365-eventhubs	Do not use this connector. Use the Microsoft Defender XDR Events connector instead.
<a href="#">Data Connector built for Microsoft Graph API [/documentation/page/c71b146b/data-connector-built-for-microsoft-graph-api]</a>	Pull	<a href="#">Microsoft Graph API [https://learn.microsoft.com/en-us/graph/use-the-api]</a>	<p>Entra audit logs, sign-in logs, and Defender alerts:</p> <ul style="list-style-type: none"> <li>Entra DirectoryAudit</li> <li>Entra signIn</li> <li>Defender for Identity Alerts</li> <li>Defender for o365 Email Alerts</li> </ul> <p>For more info, see <a href="#">Directory audit logs [https://learn.microsoft.com/en-us/graph/api/resources/azure-ad-auditlog-overview?view=graph-rest-1.0#directory-audit-logs]</a></p> <p>.</p>	microsoft-azure-ad	Do not use this connector. Use the Microsoft Defender XDR Events and Microsoft Entra ID connector instead.