

Cloudflare

Last updated: Jul. 14, 2025

Overview

Enhance Next-Gen SIEM detections with data from Cloudflare products:

- [Cloudflare Application Services](#) [/documentation/page/zb514465/cloudflare#edeb7d2d]
- [Cloudflare Area 1](#) [/documentation/page/zb514465/cloudflare#n7381ba7]
- [Cloudflare Zero Trust](#) [/documentation/page/zb514465/cloudflare#s9f85572]

Important: This data connector can be configured for multiple Cloudflare products. Each Cloudflare product that you integrate with requires a new setup of the Cloudflare data connector. Give your new data connector a name to help distinguish between multiple Cloudflare product connectors. For example, *Area 1*.

Setup

Important: Some of these steps are performed in third-party products. CrowdStrike does not validate any third-party configurations in customer environments. Perform the following steps with care, and validate your settings and values before finalizing configurations in the Falcon console.

Cloudflare Application Services

Set up Cloudflare Core data ingestion through the Cloudflare Application Services UI. For more info, see [Enable HTTP destination](https://developers.cloudflare.com/logs/get-started/enable-destinations/http/) [https://developers.cloudflare.com/logs/get-started/enable-destinations/http/].

Requirements

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

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

Vendor requirements:

- Access to the Cloudflare dashboard to retrieve account information.
 - **Auth_email:** The email address used to sign in to Cloudflare.
 - **Auth_token:** The API Token page.
 - **Zone ID:** The Overview page.
 - **Domain:** Your customer domain.

Other requirements:

- Your environment must include a functioning deployment of Cloudflare Application Services.
- A host machine with internet activity to execute curl commands.

Configuration summary

[Step 1: Configure and activate the Cloudflare data connector](#) [/documentation/page/zb514465/cloudflare#f8f5acac]

[Step 2: Retrieve the Cloudflare API key](#) [/documentation/page/zb514465/cloudflare#b14c28ba]

[Step 3: Configure log forwarding](#) [/documentation/page/zb514465/cloudflare#c744fc13]

[Step 4: Confirm and enable new Logpush job](#) [/documentation/page/zb514465/cloudflare#h0b559bd]

[Step 5: Verify successful data ingestion](#) [/documentation/page/zb514465/cloudflare#r803a192]

Step 1: Configure and activate the Cloudflare data connector

1. Go to [Data connectors > Data connectors > Data connections](#) [/data-connectors].
2. Click the **Cloudflare Data Connector** tile.
3. Enter a name and optional description to identify the connector.
4. Accept the Terms and Conditions then click **Save**.
5. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate an API key and API URL, navigate to [Data connectors > Data connectors > My connectors](#) [/data-connectors/connectors], click on the three dot menu for the data connector, and click **Generate API key**.
6. Copy and safely store both to use when configuring log forwarding.

Step 2: Retrieve the Cloudflare API key

These steps are performed in the administration interface for your instance of Cloudflare Application Services. For more detailed info, see the Cloudflare product documentation.

1. In the Cloudflare dashboard, on the **Accounts** page, select your account.
2. On the **Home** page, select the active domain.
3. On the **Overview** page, in the **API** section, save the **Zone ID** to enter in a later step.
4. Go to **My Profile > API Tokens**.
5. Under the **API Keys** section, click **View** for **Global API Key**.
6. Enter your Cloudflare account password and click **View** to retrieve the API key.
7. Save the **API Key** to enter when configuring log forwarding.

Important: The **Zone ID** and **API Key** pose a security risk if compromised. We recommend deleting them after you enter them in a later step.

Step 3: Configure log forwarding

Important: It is possible to choose which data to send to the Falcon console. However, CrowdStrike does not assist customers in choosing and configuring which data to send. Perform custom configuration with care, and validate your settings and values before finalizing configurations in Falcon.

1. Copy the command and replace these values with your own information before executing the curl command:

```
curl -s https://api.cloudflare.com/client/v4/zones/Enter_Zone_ID/logpush/jobs -X POST -d '{
  "name": "Enter_your_Domain",
  "logpull_options": "fields=RayID,EdgeStartTimestamp&timestamps=rfc3339",
  "destination_conf": "Enter_the_API_URL?
header_Authorization=Bearer%20Enter_the_CrowdStrike_API_key&tags=host:Enter_your_domain,dataset:http_requests",
  "max_upload_bytes": 5000000,
  "max_upload_records": 1000,
  "dataset": "http_requests",
  "enabled": true
}' \
-H "X-Auth-Email: user@domain.com" \
-H "X-Auth-Key: Enter_the_Cloudflare_API_Key"
```

- a. {Enter_Zone_ID}
 - b. Enter_your_Domain
 - c. Enter_the_API_URL
 - d. Enter_the_CrowdStrike_API_key
 - e. Enter_your_domain
 - f. user@domain.com
 - g. Enter_the_Cloudflare_API_Key.
2. To ingest additional data sets, replace http_requests with the listed data sets and repeat the curl request:

- a. dns_logs
- b. firewall_events
- c. http_requests
- d. nel_reports
- e. page_shield_events
- f. spectrum_events

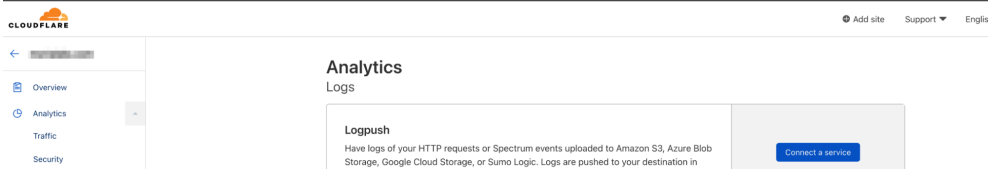
Step 4: Confirm and enable new Logpush job

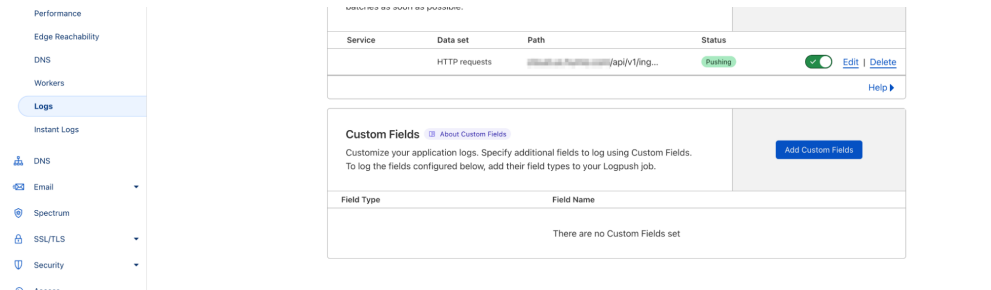
These steps are performed in the administration interface for your instance of Cloudflare Application Services. For more detailed info, see the Cloudflare product documentation.

1. In the Cloudflare dashboard, on the **Accounts** page, select your account.
2. On the **Home** page, select the active domain.
3. Go to Overview **Menu > Analytics > Logs**.

Note: If the curl command that you executed during Step 2 was successful, the Logpush job that you created is now displayed on the **Logpush** page.

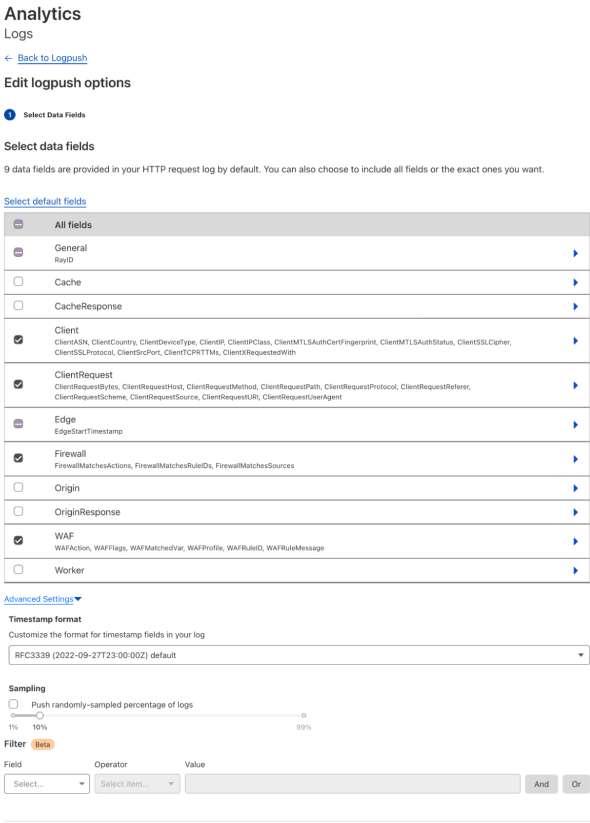
4. Ensure the status of the Logpush job is **Pushing**.





5. Click **Edit**.

6. Ensure the following traffic filters are enabled:



7. Click **Save changes** to apply changes.

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:

Vendor = Cloudflare | Product = One

🔍

Cloudflare Area 1

Set up Cloudflare Area 1 data ingestion through the Cloudflare Area 1 UI.

Requirements

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

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

Vendor requirements: Your environment must include a functioning deployment of Cloudflare Area 1.

Configuration summary

[Step 1: Configure and activate the Cloudflare data connector \[/documentation/page/zb514465/cloudflare#i35be9df\]](#)

[Step 2: Configure alert webhook \[/documentation/page/zb514465/cloudflare#ee3f246f\]](#)


[Step 3: Verify successful data ingestion \[/documentation/page/zb514465/cloudflare#la618172\]](#)

Step 1: Configure and activate the Cloudflare data connector

1. Go to [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).
2. Click the **Cloudflare** tile.
3. Enter a name and optional description to identify the connector.
4. Accept the Terms and Conditions then click **Save**.
5. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate an API key and API URL, navigate to [Data connectors > Data connectors > My connectors \[/data-connectors/connectors\]](#), click on the three dot menu for the data connector, and click **Generate API key**.
6. Copy and safely store the API key and URL for later use when configuring an alert webhook.

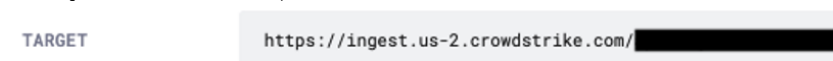
Step 2: Configure alert webhook

These steps are performed in the administration interface for your instance of Cloudflare Area 1. For more detailed info, see the Cloudflare product documentation.


1. In the Cloudflare dashboard, on the **Accounts** page, select your account.
2. Click **Area 1**.
3. Click **Launch dashboard**.
4. Click **Allow**.
5. Click the **Settings** gear icon .
6. In the **Domains & Routing** section, click **Alert Webhooks**.
7. Click + **New Webhook**.
8. Select **SIEM**.
9. From the drop down list, select **Other**.
10. In the **Auth Code** field, enter Bearer <the API key that you saved earlier>.



11. In the **Target** field, enter the **API URL** that you saved earlier.



12. For each **Style** field, select **Expanded**.



13. To save the configuration, click + **Publish Webhook**.

Step 3: 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:



Cloudflare Zero Trust

Set up Cloudflare Zero Trust data ingestion through the Cloudflare Zero Trust UI.

Requirements

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

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

Vendor requirements:

- Your environment must include a functioning deployment of Cloudflare Zero Trust.
- Access to the Cloudflare dashboard to retrieve account information.
 - **Auth_email:** The email address used to sign in to Cloudflare.
 - **Auth_token:** The API Token page.
 - **Zone ID:** The Overview page.
 - **Domain:** Your customer domain.

Other requirements:

- A host machine with internet activity to execute curl commands.

Configuration summary

[Step 1: Configure and activate the Cloudflare data connector \[/documentation/page/zb514465/cloudflare#se29ee66\]](#)

[Step 2: Retrieve the Cloudflare API key \[/documentation/page/zb514465/cloudflare#u9fb1f4e\]](#)

[Step 3: Configure log forwarding \[/documentation/page/zb514465/cloudflare#v6ec6d6c\]](#)

[Step 4: Confirm and enable new Logpush job \[/documentation/page/zb514465/cloudflare#r278f8e1\]](#)

[Step 5: Verify successful data ingestion \[/documentation/page/zb514465/cloudflare#ec30883f\]](#)

Step 1: Configure and activate the Cloudflare data connector

1. Go to [Data connectors > Data connectors > Data connections \[/data-connectors\]](#).
2. Click the **Cloudflare Data Connector** tile.
3. Enter a name and optional description to identify the connector.
4. Accept the Terms and Conditions then click **Save**.
5. A banner message appears in the Falcon console when your API key and API URL are ready to be generated. To generate an API key and API URL, navigate to [Data connectors > Data connectors > My connectors \[/data-connectors/connectors\]](#), click on the three dot menu for the data connector, and click Generate API key.
6. Copy and safely store both to use when configuring log forwarding.

Step 2: Retrieve the Cloudflare API key

These steps are performed in the administration interface for your instance of Cloudflare Zero Trust. For more detailed info, see the Cloudflare product documentation.

1. In the Cloudflare dashboard, on the **Accounts** page, select your account.
2. On the **Home** page, select the active domain.
3. On the **Overview** page, in the **API** section, save the **Account ID** to enter in a later step.
4. Go to **My Profile > API Tokens**.
5. Under the **API Keys** section, click **View** for Global API Key.
6. Enter your Cloudflare account password and click **View** to retrieve the API key.
7. Save the **API Key** to enter when configuring log forwarding.

Important: The **Account ID** and **API Key** pose a security risk if compromised. We recommend deleting them after you enter them in a later step.

Step 3: Configure log forwarding

Important: It is possible to choose which data to send to the Falcon console. However, CrowdStrike does not assist customers in choosing and configuring which data to send. Perform custom configuration with care, and validate your settings and values before finalizing configurations in Falcon.

1. Copy the command and replace these values with your own information before executing the curl command:

```
curl -s https://api.cloudflare.com/client/v4/accounts/Enter_Account_ID/logpush/jobs -X POST -d '{
  "name": "xdr.Enter.dataset.name",
```

```

"logpull_options": "fields=RayID,EdgeStartTimestamp&timestamps=rfc3339",
"destination_conf":
"Enter_API_url?
header_Authorization=Bearer%20Enter_the_CrowdStrike_API_key&tags=host:Enter_your_domain,dataset:Enter_
dataset_name",
"max_upload_bytes": 5000000,
"max_upload_records": 1000,
"dataset": "Enter_dataset_name",
"ownership_challenge": "00000000000000000000",
"enabled": false
}' \
-H "X-Auth-Email: user@domain.com" \
-H "X-Auth-Key: Enter_the_Cloudflare_API_Key"

```

- a. Enter_Account_ID
- b. Enter.dataset.name
- c. Enter_API_url
- d. Enter_the_CrowdStrike_API_key
- e. Enter_your_domain
- f. Enter_dataset_name
- g. Enter_dataset_name
- h. user@domain.com
- i. Enter_the_Cloudflare_API_Key.

2. To ingest additional data sets, replace these fields with the listed data sets and repeat the curl request:

a. In **"name": "xdr.Enter.dataset.name"**, replace **Enter.dataset.name** with the following:

- i. access.requests
- ii. audit.logs
- iii. casb.findings
- iv. device.posture.results
- v. dns.firewall.logs
- vi. gateway.dns
- vii. gateway.http
- viii. gateway.network
- ix. magic.ids.detections
- x. network.analytics.logs
- xi. sinkhole.http.logs
- xii. workers.trace.events
- xiii. Zero.trust.network.session

b. In **dataset:Enter_dataset_name** and **"dataset": "Enter_dataset_name"**, replace **Enter_dataset_name** with the following:

- i. access_requests
- ii. audit_logs
- iii. casb_findings
- iv. device_posture_results
- v. dns_firewall_logs
- vi. gateway_dns
- vii. gateway_http
- viii. gateway_network
- ix. magic_ids_detections
- x. network_analytics_logs
- xi. sinkhole_http_logs
- xii. workers_trace_events
- xiii. zero_trust_network_sessions

Step 4: Confirm and enable new Logpush job

These steps are performed in the administration interface for your instance of Cloudflare Zero Trust. For more detailed info, see the Cloudflare product documentation.

1. In the Cloudflare dashboard, on the **Accounts** page, select your account.

2. Go to **Zero Trust > Logs > Logpush**.

Note: If the curl commands that you executed during Step 2 were successful, the Logpush jobs that you created are now displayed on the **Logpush** page.

3. Ensure the status is **Pushing** for each Logpush job.

Cloudflare

Support

Logpush

← CrowdStrike Integr...

Zero Trust overview

Analytics

Gateway

Access

CASB

DLP

DEX

My Team

Logs

Admin

Access

Gateway

Logpush

Posture

Logs / Logpush

Logpush

Deliver your data sets to your preferred cloud service provider. [Learn more](#)

Your logs Showing 11-16 of 16

Manage your existing logpush configurations or create a new one.


+

Connect a service

Search

Job name	Data set	Service	Path	Status	Enabled
xdr.casb	CASB Findings		ingest.us-2.cro...	PUSHING	✓
xdr.device	Device Posture		ingest.us-2.cro...	PUSHING	✓
xdr.gateway.dns	DNS requests		ingest.us-2.cro...	PUSHING	✓
xdr.gateway.http	HTTP requests		ingest.us-2.cro...	PUSHING	✓
xdr.gateway.network	Network sessions		ingest.us-2.cro...	PUSHING	✓
xdr.zero.sessions	Session Logs		ingest.us-2.cro...	PUSHING	✓

4. For each Logpush job, complete the following steps:

- a. Click the vertical ellipses icon , and then select **Edit**.
- b. In the Data fields section, select **Job name** to include all of the data fields in your event log.

Cloudflare

Logpush

← CrowdStrike Integr...

Zero Trust overview

Analytics

Gateway

Access

CASB

DLP

DEX

My Team

Logs

Admin

Access

Gateway

Logpush

Posture

Settings

← Back to Logpush

Edit xdr.zero.sessions

Job name

Job name cannot be changed after connecting a service.

xdr.zero.sessions

Data set

Data set cannot be changed after connecting a service.

Session Logs

Data fields

Choose which fields to include in your event log.

<input checked="" type="checkbox"/> Job name	Description
<input checked="" type="checkbox"/> Account ID	Cloudflare account ID.
<input checked="" type="checkbox"/> Bytes received	The number of bytes sent from the origin to the client during the network session.
<input checked="" type="checkbox"/> Bytes sent	The number of bytes sent from the client to the origin during the network session.
<input checked="" type="checkbox"/> Client TCP handshake duration (ms)	Duration of handshaking the TCP connection between the client and Cloudflare in milliseconds.
<input checked="" type="checkbox"/> Client TLS cipher	TLS cipher suite used in the connection between the client and Cloudflare.
<input checked="" type="checkbox"/> Client TLS handshake duration (ms)	Duration of handshaking the TLS connection between the client and Cloudflare in milliseconds.
<input checked="" type="checkbox"/> Client TLS version	TLS protocol version used in the connection between the client and Cloudflare.
<input checked="" type="checkbox"/> Connection close reason	The reason for closing the connection, only applicable for TCP. Possible values are clientClosed originClosed timeout clientTcpError clientTlsError originTcpError originTlsError.

c. Click **Save**.

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:

#Vendor=cloudflare | #event.module=zerotrust

Data reference

Next-Gen SIEM events

Next-Gen SIEM events that can be generated by this data connector:

- [Network:Connection:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#i0veu97\]](#)
- [Intrusion_detection:Info:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#k7xn9jc3\]](#)
- [Email:Info:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#f5vqjx4f\]](#)
- [Vulnerability:Info:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#j7b1c38\]](#)
- [Configuration:Change:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#t8jh2vk\]](#)
- [Web:Access:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#p9vhn5jb\]](#)
- [Web:Error:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#z3is1lw0\]](#)
- [Session:Info:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#x0113sk8\]](#)
- [Authentication:Info:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#d6asy112\]](#)
- [Network:Protocol:\(failure.success.unknown\) \[/documentation/page/q1f14b54/next-gen-siem-data#h6gvlrpt\]](#)

For more information about Next-Gen SIEM events, see [Next-Gen SIEM Data Reference \[/documentation/page/q1f14b54/next-gen-siem-data\]](#) .