

## INTEGRATIONS • FOR IT ADMINS

# Send Clouddraw events to your SIEM

Stream Clouddraw audit events, alerts and app-firewall decisions to Splunk, Microsoft Sentinel, Datadog, Amazon S3, syslog over TLS or your own HTTPS endpoint.

Last updated 7 October 2026

## Overview: what Clouddraw sends

Clouddraw can stream its events to the tools your security team already uses. You add a **destination**, choose which streams it gets, and Clouddraw sends new events as they happen. You can have up to **10 destinations** per workspace, of any mix of types.

## What is sent

There are two streams. A new destination gets both unless you pick only one.

| Stream                       | What it contains                                                                                                                                                                                                          | kind in the record |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Audit</b>                 | Every entry in your workspace audit log: admin changes, sign-in and access settings, people and device actions, ended sessions, recordings viewed or deleted, destination changes, and so on.                             | audit              |
| <b>Alerts</b>                | Every notification the console shows (for example connector offline, certificate expiring, security alerts), and a <i>Resolved</i> record when the condition clears.                                                      | alert              |
| <b>Alerts (app firewall)</b> | <b>Every</b> app-firewall decision: a program that was blocked, or would have been blocked in report-only mode. Sent even when the app-firewall alert switch is off, and without the one-per-hour limit the console uses. | app_firewall       |

### NOTE

Individual connections and session traffic are **not** streamed. Admin actions on sessions, such as *End session* or playing a recording, are in the audit stream. A new destination starts from **now**. Older audit entries are not sent.

## Record format

Every record has the same fields, whatever the destination:

```
{
  "at": "2026-10-07T09:12:44.311Z",
  "tenant": "<your workspace id>",
  "kind": "audit | alert | app_firewall",
  "action": "e.g. siem.create, app_firewall.blocked, resolved",
  "severity": "info | warning | critical",
  "message": "short human-readable text",
  "data": { ... details of the event ... }
}
```

- **Audit records** always have severity `info`. The message is `<who>: <action>`. `data` holds the audit entry's fields, the `actor`, and the entry's chain `hash` and sequence number, so your SOC can check that nothing is missing. Fields whose names look like secrets (token, secret, password, API key and similar) are replaced with `[redacted]`.
- **App-firewall records** have severity `warning` (blocked) or `info` (would have been blocked). `data` holds the device, person, connection, program path, publisher, reason and whether the block was enforced.
- Each destination type wraps the record in the format the provider expects. The provider sections below show how.

## Delivery and retries

- Events are sent in batches of up to 100, usually within a few seconds.
- **Audit stream: nothing is lost.** Cloudraw keeps a position for each destination. If the destination fails, Cloudraw holds the entries and retries (after 5 s, 30 s, 2 min, 10 min, then every 30 min) until it works. Entries arrive in order. After a failure a batch can arrive twice, so de-duplicate on the `hash` in `data`.
- If a destination keeps failing for **15 minutes**, Cloudraw raises a security alert: *"Log shipping to your <type> destination is failing since ... Audit entries are held and will be delivered when it recovers."* The alert clears itself when delivery works again.
- **Alerts stream: best effort.** A failed batch is retried with the same back-off, up to 6 attempts, and then dropped. Up to 2,000 alert records wait per destination. Beyond that the oldest are dropped. The destination's delivery status shows how many were delivered and dropped.
- Cloudraw always checks the TLS certificate and never follows redirects. Only ports **443, 8088, 8443 and 6514** are allowed. The destination must be reachable on a **public** address: private, loopback and link-local addresses, internal host names (`localhost`, `*.local`, `*.internal`, `*.localdomain`) and `cloudraw.com` hosts are refused. This is checked again every time Cloudraw connects.

## Add a destination

- 1 Prepare the provider side**  
Follow the section for your provider below. Keep the values you collect at hand.
- 2 Open SIEM streaming**  
In the Cloudraw admin console go to **Settings** → **Integrations** → **SIEM streaming** and click **Add destination**.
- 3 Pick the type and fill in the fields**  
Use the field table in your provider's section. Choose the streams: **Audit**, **Alerts**, or both.
- 4 Save**  
Cloudraw checks the values right away and tells you what is wrong. After saving, secret fields show only `.....`. They are stored encrypted and never shown again.
- 5 Send a test event**  
Click **Test** (see below).

You need the *Owner* or *Security admin* role to add, test or delete destinations. *Auditors* can see them.

### IMPORTANT

A destination cannot be edited. To change a value or rotate a secret, add a new destination with the new values, test it, then delete the old one. Do it in that order: a new destination starts from *now*, so deleting first would leave a gap in your audit trail.

## Test a destination

**Test** sends one real record right away, with no retry, and shows the provider's answer. The record looks like this:

```
kind: alert · action: siem.test · severity: info · message: "Cloudraw test event – the destination is reachable"
```

If it works, the destination status changes to **streaming**. If not, it changes to **error** and the error text is shown. You can run 10 tests per destination per hour.

# Splunk (HTTP Event Collector)

Clouddraw sends to the Splunk HTTP Event Collector (HEC). Works with Splunk Enterprise and Splunk Cloud Platform.

## In Splunk

- 1

Create an index (recommended)

Go to **Settings** → **Indexes** → **New Index**. Name it, for example, `ccloudraw`, and save.
- 2

Turn on HEC

Go to **Settings** → **Data inputs** → **HTTP Event Collector**. On Splunk Enterprise click **Global Settings**, set **All Tokens** to **Enabled**, keep **Enable SSL** on, and note the port (default `8088`).
- 3

Create the token

Click **New Token**. Name: `Ccloudraw`. Leave **Enable indexer acknowledgement** off. Click **Next**.
- 4

Input settings

Source type: **Automatic** (Clouddraw sets it). Under **Allowed Indexes** add your `ccloudraw` index and make it the **Default Index**. Click **Review**, then **Submit**.
- 5

Copy the token value

It is a GUID. You need it in Clouddraw.

Your HEC URL is the event endpoint:

Splunk Enterprise: `https://splunk.example.com:8088/services/collector/event`  
Splunk Cloud: `https://http-inputs-<your-stack>.splunkcloud.com/services/collector/event`

WARNING

Splunk Enterprise ships HEC with a self-signed certificate. Clouddraw rejects it. Give HEC a certificate from a public CA that matches the host name (or put HEC behind a load balancer that has one). Splunk Cloud already has a valid certificate.

## Clouddraw field → value

| Clouddraw field  | Value                                                                                                                                                                                 | Required |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <code>url</code> | The full HEC event URL, ending in <code>/services/collector/event</code> . Must be <code>https://</code> , on port 443, 8088, 8443 or 6514, with no user name or password in the URL. | Yes      |

| Clouddraw field         | Value                                                                                                                                                              | Required |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <code>hec_token</code>  | The HEC token value. Sent as <code>Authorization: Splunk &lt;token&gt;</code> .                                                                                    | Yes      |
| <code>index</code>      | Index name, up to 80 characters. Leave empty to use the token's default index. If you set it, the token must allow that index.                                     | No       |
| <code>sourcetype</code> | Up to 80 characters. Leave empty and Clouddraw uses <code>clouddraw:audit</code> , <code>clouddraw:alert</code> or <code>clouddraw:app_firewall</code> per record. | No       |

Each record becomes one HEC event with `host` and `source` set to `clouddraw`, `time` set from the record, and the full record as `event`.

## Test it

Click **Test** in Clouddraw, then search in Splunk:

```
index=clouddraw source=clouddraw event.action="siem.test"
```

## Troubleshooting

| Message or symptom                                                                                                             | Cause and fix                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>HTTP 403</code>                                                                                                          | Wrong or disabled token. Check the token value and that it is enabled.                                                                                                                             |
| <code>HTTP 400</code>                                                                                                          | Often indexer acknowledgement is on for the token (Clouddraw does not send a channel ID), or <code>index</code> is not in the token's allowed indexes. Turn acknowledgement off, or fix the index. |
| <code>HTTP 404</code>                                                                                                          | The URL path is wrong. Use <code>/services/collector/event</code> .                                                                                                                                |
| <code>...: SELF_SIGNED_CERT_IN_CHAIN, DEPTH_ZERO_SELF_SIGNED_CERT</code><br>or<br><code>UNABLE_TO_VERIFY_LEAF_SIGNATURE</code> | HEC uses a self-signed or private certificate. Use a public CA certificate (see the warning above).                                                                                                |
|                                                                                                                                |                                                                                                                                                                                                    |

| Message or symptom                                                               | Cause and fix                                                  |
|----------------------------------------------------------------------------------|----------------------------------------------------------------|
| <code>url: port 8089 not allowed<br/>(allowed: 443, 8088, 8443,<br/>6514)</code> | 8089 is the Splunk management port, not HEC. Use the HEC port. |

# Microsoft Sentinel

Clouddraw sends to Microsoft Sentinel through the **Azure Monitor Logs Ingestion API** into a custom table in the Log Analytics workspace that Sentinel uses. (The older HTTP Data Collector API is retired and is not used.) This takes about 20 minutes.

## In Microsoft Entra and Azure

### 1 Register an app

In the [Microsoft Entra admin center](https://entra.microsoft.com) (<https://entra.microsoft.com>) go to **Identity** → **Applications** → **App registrations** → **New registration**. Name: `Clouddraw log ingestion`. Single tenant. No redirect URI. Click **Register**. On **Overview** copy the **Application (client) ID** and the **Directory (tenant) ID**.

### 2 Create a client secret

Go to **Certificates & secrets** → **Client secrets** → **New client secret**, click **Add** and copy the secret's **Value** (not the Secret ID). No API permissions are needed.

### 3 Create a Data Collection Endpoint

In the [Azure portal](https://portal.azure.com) (<https://portal.azure.com>) go to **Monitor** → **Settings** → **Data Collection Endpoints** → **Create**. Use the **same region** as your Log Analytics workspace. When it is created, open it and copy the **Logs Ingestion URL** from **Overview**. It looks like `https://<name>-abcd.westeurope-1.ingest.monitor.azure.com`.

### 4 Save a sample file

Save this as `clouddraw-sample.json` on your computer. Azure uses it to build the table columns:

```
[{"TimeGenerated":"2026-10-07T09:00:00.000Z","Tenant":"example","Kind":"audit","Action":"siem.test","Severity":"info","Message":"sample","Data":{"actor":"admin@example.com"}}]
```

### 5 Create the custom table and DCR

Go to **Log Analytics workspaces** → *your workspace* → **Settings** → **Tables** → **Create** → **New custom log (DCR-based)**.

- **Table name:** for example `Clouddraw`. Azure adds `_CL`, so the table is `Clouddraw_CL`.
- **Data collection rule:** **Create a new data collection rule**, for example `clouddraw-dcr`.
- **Data collection endpoint:** the one from step 3.

Click **Next**, upload `clouddraw-sample.json`, keep the default transformation (`source`), click **Next**, then **Create**.

## 6 Copy the DCR immutable ID and stream name

Go to **Monitor** → **Settings** → **Data Collection Rules** → **clouddraw-dcr** and click **JSON View**. Copy `immutableId` (starts with `dcr-`). Under `streamDeclarations` copy the stream name, for example `Custom-Clouddraw_CL`.

## 7 Give the app permission to send

In the same DCR open **Access control (IAM)** → **Add** → **Add role assignment**. Choose the role **Monitoring Metrics Publisher**. Under **Members** choose **User, group, or service principal**, select `Clouddraw log ingestion`, then **Review + assign**. The role can take up to 30 minutes to work.

### NOTE

Clouddraw sends these columns: `TimeGenerated`, `Tenant`, `Kind`, `Action`, `Severity`, `Message` and `Data` (dynamic). The sample file above creates exactly these.

## Clouddraw field → value

| Clouddraw field               | Value                                                                                                                                                                                               | Required |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <code>tenant_id</code>        | Directory (tenant) ID. Must be a GUID.                                                                                                                                                              | Yes      |
| <code>client_id</code>        | Application (client) ID. Must be a GUID.                                                                                                                                                            | Yes      |
| <code>client_secret</code>    | The client secret <b>Value</b> .                                                                                                                                                                    | Yes      |
| <code>endpoint</code>         | The DCE <b>Logs Ingestion</b> URL. Must be <code>https://</code> and the host must end in <code>.ingest.monitor.azure.com</code> . Clouddraw only ever sends the access token to that kind of host. | Yes      |
| <code>dcr_immutable_id</code> | The DCR <code>immutableId</code> : <code>dcr-</code> followed by 32 hex characters.                                                                                                                 | Yes      |
| <code>stream_name</code>      | <code>Custom-</code> followed by letters, digits or <code>_</code> , for example <code>Custom-Clouddraw_CL</code> .                                                                                 | Yes      |

### IMPORTANT

Note when the client secret expires. When it does, delivery stops (audit entries are held). Rotate it by adding a new Clouddraw destination with the new secret, testing it, and then deleting the old destination.

## Test it

Click **Test** in Cloudraw. The first records can take 5 to 10 minutes to appear. Then run this in **Microsoft Sentinel** → **Logs**:

```
Cloudraw_CL | where Action == "siem.test" | sort by TimeGenerated desc
```

## Troubleshooting

| Message or symptom                                                                             | Cause and fix                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>entra token: invalid_client</code>                                                       | Wrong or expired client secret, or you pasted the Secret ID. Create a new secret and use its Value.                                                                             |
| <code>entra token: unauthorized_client</code> or <code>entra token: invalid_request</code>     | The client ID or tenant ID is wrong, or the app is in a different tenant. Copy both again from the app's Overview page.                                                         |
| <code>HTTP 403 - ...</code>                                                                    | The app does not have <b>Monitoring Metrics Publisher</b> on the DCR, or the role is not active yet. Check the role assignment and wait up to 30 minutes.                       |
| <code>HTTP 404 - ...</code> or <code>HTTP 400 - ...</code>                                     | Wrong <code>dcr_immutable_id</code> or <code>stream_name</code> , or the DCE and DCR are in different regions. Check the DCR's JSON View. Azure's own message follows the dash. |
| <code>endpoint must be an Azure Monitor ingestion endpoint (*.ingest.monitor.azure.com)</code> | You pasted a different URL (for example the workspace or DCR resource URL). Use the DCE <b>Logs Ingestion</b> URL.                                                              |
| <code>dcr_immutable_id</code> looks like <code>dcr-&lt;32 hex&gt;</code>                       | You pasted the DCR name or resource ID. Use <code>immutableId</code> from JSON View.                                                                                            |
| <code>stream_name</code> must be <code>Custom-&lt;TableName&gt;</code>                         | The stream name must start with <code>Custom-</code> . Copy it from <code>streamDeclarations</code> .                                                                           |
| <code>tenant_id</code> and <code>client_id</code> must be GUIDs                                | Paste the IDs, not the names.                                                                                                                                                   |
| Test is OK but the table stays empty                                                           | Ingestion can take up to 10 minutes on a new table. Check that the table name in your query matches the table you created.                                                      |

# Datadog

Cloudraw sends to the Datadog Logs intake API (v2).

## In Datadog

### 1 Create an API key

Go to **Organization Settings** → **API Keys** → **New Key**. Name it `Cloudraw` and copy the key. Use an **API key**, not an Application key.

### 2 Find your site

Look at the address bar when you are signed in to Datadog. `app.datadoghq.com` means site `datadoghq.com`. `app.datadoghq.eu` means `datadoghq.eu`. `us3.datadoghq.com`, `us5.datadoghq.com`, `ap1.datadoghq.com` and `ap2.datadoghq.com` are their own sites. US1-FED is `ddog-gov.com`.

## Cloudraw field → value

| Cloudraw field       | Value                                                                                                                                                                                                                                                                 | Required |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <code>key</code>     | The Datadog API key. Sent as the <code>DD-API-KEY</code> header.                                                                                                                                                                                                      | Yes      |
| <code>site</code>    | One of <code>datadoghq.com</code> , <code>us3.datadoghq.com</code> , <code>us5.datadoghq.com</code> , <code>datadoghq.eu</code> , <code>ap1.datadoghq.com</code> , <code>ap2.datadoghq.com</code> , <code>ddog-gov.com</code> . Default: <code>datadoghq.com</code> . | No       |
| <code>service</code> | Value of the <code>service</code> attribute, up to 60 characters. Default: <code>cloudraw</code> .                                                                                                                                                                    | No       |

Each record becomes one log with `ddsource:cloudraw`, `hostname:cloudraw`, `status` set to the severity, tags `tenant:<id>` and `kind:<kind>`, the message, and the full record under the `cloudraw` attribute.

## Test it

Click **Test** in Cloudraw, then open **Logs** → **Explorer** and search:

```
source:cloudraw @cloudraw.action:siem.test
```

## Troubleshooting

| Message or symptom                                                     | Cause and fix                                                                                                                              |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <code>HTTP 403 – ...</code>                                            | Wrong API key, an Application key instead of an API key, or the key belongs to a different site. Check the key and the <code>site</code> . |
| <code>site must be one of datadoghq.com, us3.datadoghq.com, ...</code> | Type only the site, for example <code>datadoghq.eu</code> , without <code>https://</code> or <code>app.</code> .                           |
| Test is OK but nothing in Logs                                         | Check the time range, and that no exclusion filter on your log index drops <code>source:cloudraw</code> .                                  |

# Amazon S3

Cloudraw writes each batch as one NDJSON file (one JSON record per line) to your S3 bucket. Use this for long-term archive, or to feed a SIEM that reads from S3.

## In AWS

### 1 Create the bucket

In the [S3 console](https://console.aws.amazon.com/s3/) (<https://console.aws.amazon.com/s3/>) click **Create bucket**. The name may only use lowercase letters, digits and dashes. **No dots**. Note the **AWS Region**. Keep **Block all public access** on.

### 2 Create an IAM policy

In the [IAM console](https://console.aws.amazon.com/iam/) (<https://console.aws.amazon.com/iam/>) go to **Policies** → **Create policy** → **JSON** and paste this, with your bucket name and prefix:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::<your-bucket>/<your-prefix>/cloudraw/*"
  }]
}
```

Without a prefix, use `arn:aws:s3:::<your-bucket>/cloudraw/*`. Name the policy `cloudraw-log-export`.

### 3 Create an IAM user

Go to **Users** → **Create user**. Name: `cloudraw-log-export`. No console access. Choose **Attach policies directly** and select `cloudraw-log-export`.

### 4 Create an access key

Open the user, go to **Security credentials** → **Create access key**, choose **Third-party service**, and copy the **Access key** and **Secret access key**.

#### NOTE

Cloudraw signs requests with a long-term access key (Signature Version 4). Temporary credentials and IAM roles are not supported. If your bucket uses SSE-KMS with your own key, also allow `kms:GenerateDataKey` on that key for this user.

## Clouddraw field → value

| Clouddraw field                | Value                                                                                                                                                                                                        | Required |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <code>bucket</code>            | Bucket name: 3 to 63 lowercase letters, digits and dashes, no dots.                                                                                                                                          | Yes      |
| <code>region</code>            | The bucket's region code, for example <code>eu-central-1</code> .                                                                                                                                            | Yes      |
| <code>access_key_id</code>     | The IAM access key ID.                                                                                                                                                                                       | Yes      |
| <code>secret_access_key</code> | The IAM secret access key.                                                                                                                                                                                   | Yes      |
| <code>prefix</code>            | Folder inside the bucket, up to 200 characters. Letters, digits, <code>/</code> , <code>_</code> , <code>.</code> , <code>-</code> only, no <code>..</code> . Leave empty to write at the top of the bucket. | No       |

Files are named like this (time in UTC):

```
<prefix>/clouddraw/<workspace id>/YYYY/MM/DD/HHMMSS-<random>.ndjson
```

## Test it

Click **Test** in Clouddraw. A new `.ndjson` file with one line appears under today's date folder.

## Troubleshooting

| Message or symptom                             | Cause and fix                                                                                                                                                                                                                                |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>HTTP 403</code>                          | Wrong access key or secret, or the policy does not allow <code>s3:PutObject</code> on the path Clouddraw writes to. Check that the resource ARN includes <code>clouddraw/*</code> after your prefix. With SSE-KMS, check the KMS permission. |
| <code>HTTP 301</code> or <code>HTTP 400</code> | The <code>region</code> is not the bucket's region. Check the bucket's <b>Properties</b> tab.                                                                                                                                                |
| <code>HTTP 404</code>                          | The bucket name is wrong or the bucket does not exist.                                                                                                                                                                                       |
|                                                |                                                                                                                                                                                                                                              |

| Message or symptom                                                  | Cause and fix                                                                  |
|---------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <code>bucket: lowercase letters, digits and dashes (no dots)</code> | Buckets with dots in the name are not supported. Create a bucket without dots. |
| <code>region like eu-central-1</code>                               | Type the region code, not the name ("Europe (Frankfurt)").                     |
| <code>prefix: letters, digits, / _ . - only</code>                  | Remove spaces and other characters from the prefix.                            |

# Syslog over TLS

Clouddraw sends RFC 5424 syslog messages over TLS (RFC 5425) to your syslog server or SIEM collector, for example rsyslog, syslog-ng, QRadar or ArcSight. TLS is always on. Plain TCP and UDP are not supported.

## On your syslog server

1

### Open a TLS listener

Set up a TCP listener with TLS, normally on port **6514**. Clouddraw uses octet-counting framing (RFC 5425), which rsyslog and syslog-ng accept on TLS inputs.

2

### Install a server certificate

The certificate must match the host name Clouddraw connects to. If you connect by IPv4 address, the certificate needs that address in its Subject Alternative Names. It can come from a public CA, or from your own private CA (see `ca_pem`).

3

### Make it reachable

The listener must have a public IP address that Clouddraw can reach. Allow it in your firewall.

#### NOTE

Clouddraw does not present a client certificate. If your listener requires mutual TLS, turn that off for Clouddraw's connection and limit access by firewall instead.

## Clouddraw field → value

| Clouddraw field     | Value                                                                                                                                                                                                                                                                                        | Required |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <code>host</code>   | DNS name or IPv4 address of the listener. IPv6 addresses are not accepted here. Private, loopback and internal names are refused.                                                                                                                                                            | Yes      |
| <code>port</code>   | Default <code>6514</code> . Must be one of 443, 8088, 8443 or 6514.                                                                                                                                                                                                                          | No       |
| <code>ca_pem</code> | Only if your server certificate comes from a private CA. Paste the CA certificate in PEM format ( <code>-----BEGIN CERTIFICATE-----</code> ... ). It must be a CA certificate (basicConstraints <code>CA:TRUE</code> ). When set, Clouddraw trusts <b>only</b> this CA for this destination. | No       |

Each record is one message. Facility is **authpriv** (10). Severity is critical (2), warning (4) or info (6). The header is `clouddraw orchestrator` as host name and app name, the message ID is the record's

`kind` , and the message body is the full record as JSON:

```
<86>1 2026-10-07T09:12:44.311Z cloudraw orchestrator - alert -  
{ "at": "...", "kind": "alert", "action": "siem.test", ... }
```

## Test it

Click **Test** in Cloudraw and look for a message with message ID `alert` and `"action": "siem.test"`. A successful test means Cloudraw finished the TLS handshake and wrote the message. Syslog has no reply, so check that the message actually arrived.

## Troubleshooting

| Message or symptom                                                                                                                     | Cause and fix                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;host&gt;:6514: ECONNREFUSED</code> , <code>...: timeout</code> OR <code>...: deadline exceeded</code>                        | The listener is not running, or a firewall blocks Cloudraw. Check the port and firewall.                                                                                                        |
| <code>...: UNABLE_TO_VERIFY_LEAF_SIGNATURE</code> , <code>SELF_SIGNED_CERT_IN_CHAIN</code> OR <code>DEPTH_ZERO_SELF_SIGNED_CERT</code> | Cloudraw does not trust the server certificate. Paste your private CA in <code>ca_pem</code> , or use a public CA certificate. A self-signed server certificate that is not a CA does not work. |
| <code>...: ERR_TLS_CERT_ALTNAME_INVALID</code>                                                                                         | The certificate does not match the host name or IP address in <code>host</code> .                                                                                                               |
| <code>...: CERT_HAS_EXPIRED</code>                                                                                                     | Renew the server certificate.                                                                                                                                                                   |
| <code>... resolves to a non-public address</code>                                                                                      | The host name resolves to a private address. Use a name that resolves to the listener's public address.                                                                                         |
| <code>port 514 not allowed (allowed: 443, 8088, 8443, 6514)</code>                                                                     | Plain syslog ports are not supported. Use a TLS listener on 6514.                                                                                                                               |
| <code>ca_pem must be a PEM certificate</code> / <code>ca_pem must be a CA certificate (basicConstraints CA:TRUE)</code>                | Paste the CA certificate (not the server certificate or a private key), including the BEGIN and END lines.                                                                                      |
| <code>host must be a DNS name or IPv4 address</code>                                                                                   | Remove <code>https://</code> , ports or spaces from <code>host</code> .                                                                                                                         |

# Generic HTTPS endpoint

Use this for any collector that accepts JSON over HTTPS, for example a log pipeline (Vector, Fluent Bit, Logstash HTTP input, Cribl) or your own service.

## On your endpoint

### 1 Accept a JSON POST

Clouddraw sends `POST` with `Content-Type: application/json` and this body, with up to 100 records per request:

```
{ "source": "clouddraw", "events": [ { "at": "...", "tenant": "...", "kind": "...",  
  "action": "...", "severity": "...", "message": "...", "data": { ... } } ] }
```

### 2 Check the token (recommended)

If you set a token, Clouddraw sends `Authorization: Bearer <token>`. Reject requests without it.

### 3 Answer quickly with 2xx

Any 2xx status means delivered. Anything else, including a redirect, counts as a failure and is retried. Answer within 8 seconds.

### 4 Use a valid certificate

The endpoint needs a certificate from a public CA on port 443, 8088, 8443 or 6514.

#### TIP

This destination is not signed. If you need each request signed with a shared secret, use Clouddraw **Webhooks** instead, which send an HMAC signature header.

## Clouddraw field → value

| Clouddraw field    | Value                                                                                                                | Required |
|--------------------|----------------------------------------------------------------------------------------------------------------------|----------|
| <code>url</code>   | Full <code>https://</code> URL. Port 443, 8088, 8443 or 6514. No user name or password in the URL. Public host only. | Yes      |
| <code>token</code> | Sent as <code>Authorization: Bearer &lt;token&gt;</code> . Leave empty to send no Authorization header.              | No       |

## Test it

Click **Test** in Cloudraw. Your endpoint gets one request with one record whose `action` is `siem.test`. Cloudraw shows the HTTP status your endpoint returned.

## Troubleshooting

| Message or symptom                                                                 | Cause and fix                                                                              |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <code>HTTP 401</code> or <code>HTTP 403</code>                                     | Your endpoint rejected the token. Check the token value.                                   |
| <code>HTTP 301</code> , <code>HTTP 302</code> or <code>HTTP 308</code>             | Your endpoint redirects. Cloudraw does not follow redirects. Use the final URL.            |
| <code>url: https:// required</code>                                                | Plain HTTP is not supported.                                                               |
| <code>url: credentials in the URL are not allowed – use the token fields</code>    | Remove <code>user:password@</code> from the URL and put the secret in <code>token</code> . |
| <code>&lt;host&gt;: timeout</code> OR <code>&lt;host&gt;: deadline exceeded</code> | Your endpoint took too long. Answer first, then process.                                   |

## Troubleshooting (all destinations)

| Message or symptom                                                                                                                | Cause and fix                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;field&gt; is required</code>                                                                                            | A required field is empty. See the field table for your provider.                                                                                                                                        |
| <code>url: port 9000 not allowed (allowed: 443, 8088, 8443, 6514)</code>                                                          | Only these ports are allowed. Publish your collector on one of them.                                                                                                                                     |
| <code>url: private, loopback and link-local addresses are not allowed</code> OR <code>... resolves to a non-public address</code> | The destination is on a private network. Cloudraw only sends to public addresses. Publish the collector on a public address (for example through a reverse proxy) and restrict it by firewall and token. |
| <code>url: internal host names are not allowed</code>                                                                             | Names like <code>localhost</code> , <code>*.local</code> , <code>*.internal</code> , <code>*.localdomain</code> and <code>cloudraw.com</code> hosts are refused. Use a public DNS name.                  |
| <code>...: ENOTFOUND</code>                                                                                                       | The host name does not resolve in public DNS.                                                                                                                                                            |

| Message or symptom                                                                                               | Cause and fix                                                                                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>at most 10 destinations per tenant</code>                                                                  | Delete a destination you no longer use.                                                                                                                                                                            |
| <code>too many test events this hour</code>                                                                      | 10 tests per destination per hour. Wait and try again.                                                                                                                                                             |
| <code>Secrets cannot be stored safely right now (encryption key missing on this server). Retry later; ...</code> | A temporary problem on the Cloudraw side. Try again later. If it persists, contact support.                                                                                                                        |
| Security alert: <i>"Log shipping to your ... destination is failing since ..."</i>                               | Delivery has failed for 15 minutes. Audit entries are held, not lost. Open the destination to see the last error, fix it on the provider side, and click <b>Test</b> . The alert clears when delivery works again. |
| Some alert records are missing after a long outage                                                               | The alerts stream drops a batch after 6 failed attempts, and keeps at most 2,000 waiting records. The destination's delivery status shows how many were dropped. The audit stream is never dropped.                |
| The same audit record arrived twice                                                                              | Delivery is at-least-once. De-duplicate on <code>data.hash</code> .                                                                                                                                                |