

NG SIEM - Cloudflare Integration

Introduction

Cloudflare logs provide detailed insights into client connections, request paths through the Cloudflare network, and origin server responses. These logs help track activity, identify issues, and support security and performance analysis.

Authentication Options

You can configure log retrieval using the following authentication methods:

1. **Auth Email and Auth Key(Deprecated)**
2. **API Token**

For detailed information on authentication, refer to the [Cloudflare API documentation](#).

1. Configure Using Auth Email and Auth Key

To set up using this method, you need:

- **Auth Email:** The email address associated with your Cloudflare account.
- **Auth Key:** Your global API key, available on the [My Profile](#) page.
- **Zone ID:** The unique identifier of your [Cloudflare zone](#), available in the zone's dashboard.

These credentials must be included in the request headers:

- `X-Auth-Email`: Your account email.
- `X-Auth-Key`: Your global API key.

For more details, refer to Cloudflare's [authentication headers guide](#).

2. Configure Using API Token

To set up using an API token, you need:

- **API Token:** A token with appropriate permissions.
- **Zone ID:** As noted above, can be found in your Cloudflare zone dashboard.

Minimum Required Permissions for the API Token:

- Account.Access: Audit Logs: Read
- Account.Account: Settings: Read

API Tokens are preferred for security as they support fine-grained access control. Create and manage tokens via the [API Tokens dashboard](#).

Manage Account > Account API Tokens > Custom Token > Get Started

Cloudflare Account

Account API Tokens

Create Custom Token

Token name
Give your API token a descriptive name.
test-support

Permissions
Select edit or read permissions to apply to your accounts or websites for this token.

Account	Access: Audit Logs	Read	X
Account	Account Settings	Read	X

+ Add more

Client IP Address Filtering
Select IP addresses or ranges of IP addresses to filter. This filter limits the client IP addresses that can use the API token with Cloudflare. By default, this token will apply to all addresses.

Operator	Value
Select item...	e.g. 192.168.1.88

+ Add more

TTL
Define how long this token will stay active.

Start Date	→	End Date
------------	---	----------

Cancel Continue to summary

Account API Tokens

Manage account owned API tokens. User owned API tokens are found in the 'My Profile' section.

[API tokens documentation](#)

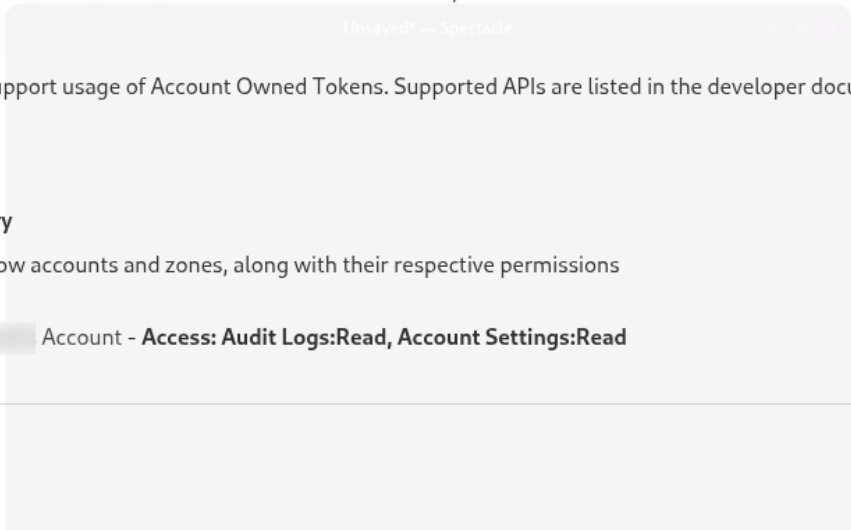
Not all APIs are guaranteed to support usage of Account Owned Tokens. Supported APIs are listed in the developer documentation.

[← Edit token](#)

test-support API token summary

This API token will affect the below accounts and zones, along with their respective permissions

Account - **Access: Audit Logs:Read, Account Settings:Read**



Account API Tokens

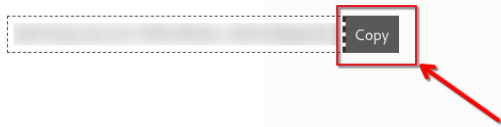
Manage account owned API tokens. User owned API tokens are found in the 'My Profile' section.

[API tokens documentation](#)

Not all APIs are guaranteed to support usage of Account Owned Tokens. Supported APIs are listed in the developer documentation.

test-support API token was successfully created

Copy this token to access the Cloudflare API. For security this will not be shown again. [Learn more](#)



Test this token

To confirm your token is working correctly, copy and paste the below CURL command in a terminal shell to test.

```
curl "https://api.cloudflare.com/client/v4/accounts/e7eb7f1a1476d7b27f134e55b1a346d6/tokens/verify" \
-H "Authorization: Bearer Qk9Yx6Ip1wErvB-V090wRMyLl-il4kXrD8dpAnb3"
```

```
curl -X GET "https://api.cloudflare.com/client/v4/user/tokens/verify" \
-H "Authorization: Bearer <token>" \
-H "Content-Type: application/json"
```

```
(tech01@tech-support)-[~]
$ curl "https://api.cloudflare.com/client/v4/accounts/.../tokens/verify" \
-H "Authorization: Bearer ..."
{"result":{"id":"...", "status":"active"}, "success":true, "errors":[], "messages":[{"code":10000, "message":"This API Token is valid and active", "type":null}]}
```

Audit Logs

Audit logs provide a record of configuration changes within your Cloudflare account, including:

- Logins/logouts

- DNS setting changes
- Modifications to Firewall, Caching, Page Rules, Speed, Network, and Traffic features

These logs are essential for tracking administrative activity and detecting unusual behavior.

To enable log collection from the Cloudflare API token, provide the following information to **CyTech Support**:

- **Account ID**
- **API Token**

If you need further assistance, kindly contact support@cytechint.com for prompt assistance and guidance.

Revision #2

Created 23 September 2025 08:12:26 by Richmond Abella

Updated 3 October 2025 13:54:42 by Richmond Abella