Netsurion | EventTracker®

How to - Configure Cloudflare to forward logs to EventTracker

EventTracker v9.2 and later

Publication Date: March 10, 2020

Abstract

This guide provides instructions to retrieve the Cloudflare events via REST API. After the logs start coming-in into EventTracker, reports, dashboards, alerts and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and Cloudflare**.**

Audience

Administrators who are assigned the task to monitor Cloudflare events using EventTracker.

Table of Contents

1. Overview

Cloudflare is a next-generation Content Delivery Network (CDN) that provides content-delivery-network, DDoS mitigation, Internet security and distributed domain-name-server services. Cloudflare's services connects website's visitor and Cloudflare user's hosting provider, acting as a reverse proxy for the websites.

Cloudflare integrates with EventTracker SIEM application to provide security analytics with deep data context, organizations can be confident in their data security strategy. Benefits include scheduled reports, Integrated Cloudflare dashboards and alerts for streamlined investigation.

Reports are the best way to view the historical data (depending on the timeline defined). Some of the EventTracker reports provided for Cloudflare are summary of audit activities such as API key view, login and logout, summary of firewall/ WAF related activities occurring in different Cloudflare zones, such as dropping or discarding an incoming traffic.

Dashboards are graphical representations of activities occurring in Cloudflare zones/UI. These dashboards can be a pie chart, a bar diagram, or a map. This allows user to view the key highlights of Cloudflare events. Some of the dashboards include audit events timeline, UI login activities, dropped traffic by country code, etc.

Alerts such as traffic dropped by firewall or WAF are present in the knowledge packs. These alerts can be configured to forward emails to users/admin of Cloudflare if any suspicious events are detected.

2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Cloudflare management UI.

3. Integrating Cloudflare with EventTracker

Depending on authentication request of the new API Tokens or old API Keys, required headers differ.

3.1 Collecting Cloudflare API Keys

To retrieve your API key:

1. Log in to the Cloudflare dashboard.
2. Under the **My Profile** dropdown, click **My Profile**.
3. Click the **API tokens** tab.
4. In the **API keys** section, choose one of two options: **Global API Key** or **Origin CA Key**. Choose the API Key that you would like to view. In this case we need **Global API Key**.

Note - The **Global API Key** is your main API key. The **Origin CA Key** is only used when creating origin certificates using the API.

5. To change your API Key, click **Change**. You will have to complete Captcha before applying the change.

Figure 1

6. Save the **Global API Key**. This key is required for future API authentications.

3.2 Forwarding Logs to EventTracker

Collect the EventTracker Cloudflare Integrator package from EventTracker support.

1. Run the **EventTracker Integrator (Cloudflare).exe** on your EventTracker agent machine.
2. Fill in the Cloudflare account registered email and the Global API key (as retrieved from previous section)

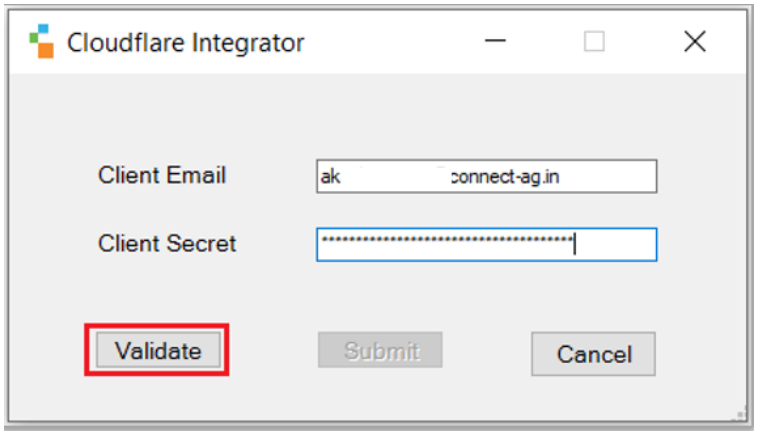

Figure 2

3. Click on the **Validate** button. If successful, a pop-up window appears with the message:

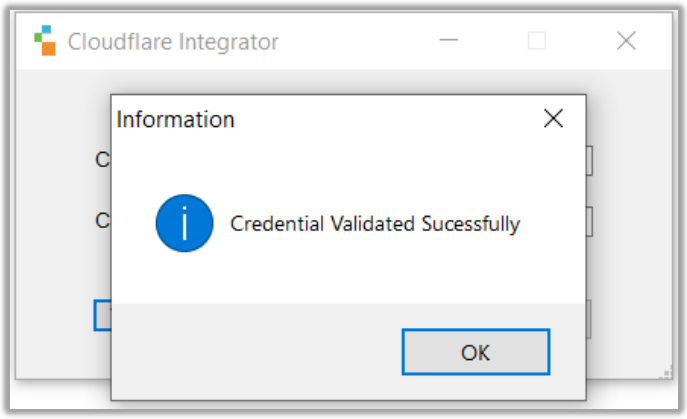

Figure 3

4. Click **OK** and click on the **Submit** button.

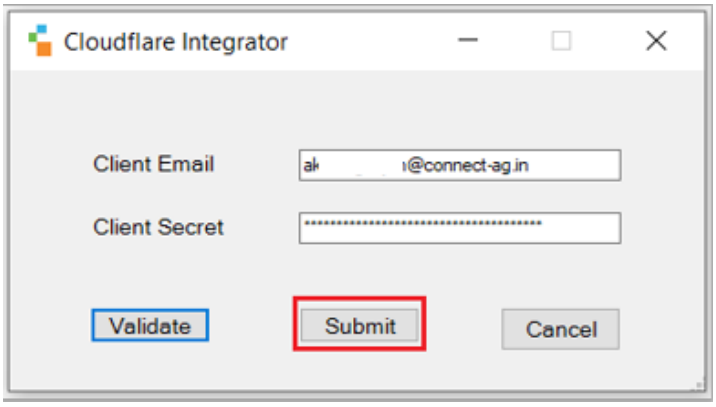

Figure 4

5. A pop-up window appears with message.

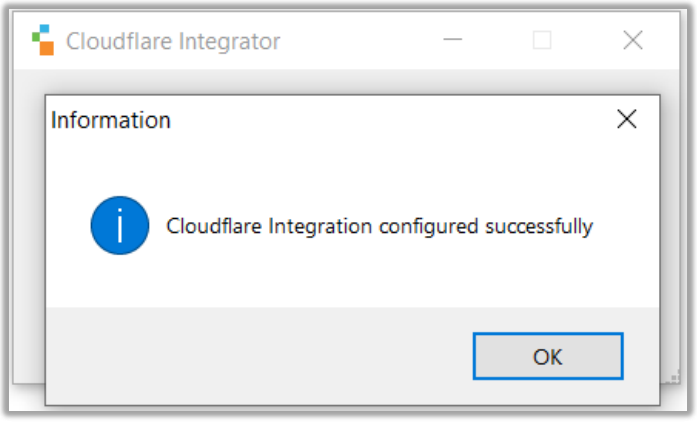

Figure 5

6. Click **OK** to complete the integration process.

Note: We are collecting two types of logs from Cloudflare namely **Audit log** and **Firewall log**.

For **Audit Log**, one system is created and for **Firewall Log**, number of systems created are equals to number of Cloudflare zones. (Zone is the basic resource for working with Cloudflare and is roughly equivalent to a domain name that the user purchases.)

Useful link: https://www.cloudflare.com/learning/dns/glossary/dns-zone/