

# Integrate Cloudflare

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.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

## Netsurion. EventTracker

1

## Table of Contents

0	verview	. 3
Pi	rerequisites	. 3
In 3.1	tegrating Cloudflare with EventTracker Collecting Cloudflare API Keys	. 3 . 3
3.2	Forwarding Logs to EventTracker	. 4
Ev 4.1	ventTracker Knowledge Packs Saved Searches	. 6 . 6
4.2	Alerts	. 6
4.3	Reports	. 6
4.4	Dashboards	. 9
In 5.1	nporting knowledge pack into EventTracker Saved Searches	14 15
5.2	Alerts	16
5.3	Parsing Rules	17
5.4	Reports	18
5.5	Knowledge Objects	20
5.6	Dashboards	21
V 6.1	erifying knowledge pack in EventTracker Saved Searches	23 23
6.2	Alerts	23
6.3	Parsing Rules	24
6.4	Reports	24
6.5	Knowledge Objects	25
6.6	Dashboards	26
	O Pi 3.1 3.2 4.1 4.2 4.3 4.4 5.1 5.2 5.3 5.4 5.5 5.6 V 6.1 6.2 6.3 6.4 6.5 6.6	Overview.         Prerequisites.         Integrating Cloudflare with EventTracker         3.1       Collecting Cloudflare API Keys         3.2       Forwarding Logs to EventTracker         EventTracker Knowledge Packs         4.1       Saved Searches         4.2       Alerts         4.3       Reports.         4.4       Dashboards         Importing knowledge pack into EventTracker         5.1       Saved Searches         5.2       Alerts         5.3       Parsing Rules.         5.4       Reports.         5.5       Knowledge pack in EventTracker         5.6       Dashboards         Verifying knowledge pack in EventTracker         6.1       Saved Searches         6.2       Alerts         6.3       Parsing Rules         6.4       Reports.         6.5       Knowledge Objects         6.6       Dashboards

Netsurion. EventTracker\*

## 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.

API Keys Keys used to access Cloudflare APIs.	
Global API Key	Change View
Origin CA Key	Change View
	Help <b>•</b>



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)





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







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

Cloudflare Integrator	- 🗆	$\times$
Client Email	ak i@connect-ag.in	
Client Secret		
Validate	Submit Cancel	

Figure 4

5. A pop-up window appears with message.





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

5

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/

## 4. EventTracker Knowledge Packs

### 4.1 Saved Searches

Saved searches are designed to quickly parse/filter logs and allows user to view only specific events related to:

- **Cloudflare Audit activities** This category of saved search displays the Cloudflare audit events, i.e., activities occurring in Cloudflare UI, such as, view API key, join organization, etc.
- **Cloudflare Firewall activities** This category of saved search displays the Cloudflare firewall events for all the available zones in a Cloudflare account, i.e., drop incoming traffic, challenge incoming traffic to discard any bot activities, etc.
- **Cloudflare** Login and Logout activities This category of saved search displays the Cloudflare audit events, i.e., activities occurring in Cloudflare UI, such as, login and logout.

### 4.2 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as,

• **Cloudflare: A web traffic has been dropped by WAF** – When Cloudflare firewall/WAF drops or discards an incoming traffic, customers are alerted about such event occurrence.

### 4.3 Reports

Reports are a detailed overview of any event occurring in Cloudflare, represented in column-value format.

• **Cloudflare** - **Audit activities** – This report contains a detailed overview of audit activities occurring in Cloudflare UI, such as API key, join organization, etc. The information includes log datetime, source email address, source IP address (IPv4 or IPv6), log type, etc.

Netsurion. EventTracker®

LogTime	Log Type	Source Email Address	Object ID	Source IP Address	Log Status
11/02/2020 08:54:28 PM	API_key_view	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	2409:4c34:2e85:e863:3cf4:4aa:3be5:9ba4	true
11/02/2020 08:54:28 PM	token_create	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	2409:4c34:2e85:e863:31cc:eede:6279:ace6	true
11/02/2020 08:54:29 PM	filter_create	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	2409:4c34:2e85:e863:31cc:eede:6279:ace6	true
11/02/2020 08:54:29 PM	firewallrulesapi_create	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	2409:4c34:2e85:e863:31cc:eede:6279:ace6	true

#### Figure 6

 Cloudflare - Firewall activities - This report contains a detailed overview of firewall activities occurring in Cloudflare zones such as drop incoming traffic, challenge incoming traffic to discard any bot activities. The information includes log datetime, action type, client ASN (autonomous system number), client IP address, user agent, etc.

LogTime	Action Type	Client ASN	Country	Client IP Address	User Agent	Request Path	Event source
11/09/2020 04:41:31 PM	drop	207566	RU	91.241.19.84	Mozilla/5.0 (Windows NT 10.0; Win64; x64)		country
					AppleWebKit/537.36 (KHTML, like Gecko)		
					Chrome/78.0.3904.108 Safari/537.36		
11/09/2020 07:53:01 PM	log	58224	IR	2.183.175.37	Mozilla/5.0 (Windows NT 10.0; Win64; x64)	/api/v2	waf
					AppleWebKit/537.36 (KHTML, like Gecko)		
					Chrome/74.0.3729.169 Safari/537.36		
11/09/2020 09:06:29 PM	drop	5089	GB	203.0.113.69	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)	/%3Cscript%3Ealert()%3C/script%3E	waf
					AppleWebKit/537.36 (KHTML, like Gecko)		
					Chrome/80.0.3987.163 Safari/537.36		
11/09/2020 09:12:48 PM	drop	198375	FR	185.81.157.12	Python-urllib/2.7		bic

#### Figure 7

• Cloudflare - Login and Logout activities - This report contains a detailed overview of login and logout activities occurring in Cloudflare UI. The information includes log datetime, source email address, source IP address (IPv4 or IPv6), log type, etc.

LogTime	Log Type	Source Email Address	Object ID	Source IP Address	Log Status
11/03/2020 04:48:59 PM	login	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	2409:4234:812:9dfb:d993:a371:38ad:f5b2	true
11/03/2020 04:48:59 PM	logout	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	157.42.47.91	true
11/03/2020 04:48:59 PM	login	akash.gunjan@connect-ag.in	c6c69fd778d70e406e6fa229467866c6	157.42.47.91	true

Figure 8



7

#### Logs Considered:

. "action": "drop", "clientASNDescription": "HOSTWAY-AS", "clientAsn": "207566", "clientCountryName": "RU", "clientIP": "91.241.19.84", "clientIPClass": "unknown", "clientRefererQuery": "?XDEBUG SESSION START=phpstorm", "clientRequestQuery": "?XDEBUG\_SESSION\_START=phpstorm", "datetime": "2020-11-09T06:22:17Z", "edgeColoName": "DME", "edgeResponseStatus": 403, "kind": "firewall", "matchIndex": 0, "originResponseStatus": 0, "originatorRayName": "00" "rayName": "5ef5703de9ab0c48", "ruleId": "country", "sampleInterval": 1, "source": "country", "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36"

Figure 9

```
"action": {
"result": true,
"type": "firewallrulesapi_create"
},
"actor": {
"email": "akash.gunjan@connect-ag.in",
"ip": "2409:4064:2e85:e863:31cc:eede:6279:ace2",
"type": "user"
},
"id": "f9e55f1a-****-456c-a8b5-095be7c0****",
"interface": "UI",
"metadata": {
"cf-ray": "5e5b3f3fc72d31fa-FRA",
"zone name": "connect-ag.in"
},
"newValue": "",
"newValueJson": {
"action": "block",
"description": "Block PK traffic",
"filter id": "b03dbf2f8bef4235932c53110949d36d",
"id": "e6f3e92c632d4394b7e6683234dc6f47",
```

Figure 10

### 4.4 Dashboards



• Cloudflare - Firewall Events



• Cloudflare - Audit Events





Netsurion. EventTracker



• Cloudflare - Firewall Event counts by Zone





#### • Cloudflare - Firewall Events Timeline



Netsurion. EventTracker

#### • Cloudflare - Audit Events Timeline



Figure 15



#### Cloudflare - UI Login activities by Source IP





• Cloudflare - Dropped Traffic by Country code



• Cloudflare - Dropped Traffic by ASN



Figure 18



• Cloudflare - Dropped Traffic by user agents



#### • Cloudflare - Dropped Traffic by source IP





• Cloudflare - Edge Colo ID by source IP



Figure 21

## 5. Importing knowledge pack into EventTracker

#### **Getting Knowledge Packs**

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

- 1. Press " 🕷 + R".
- Type "%et\_install\_path%\Knowledge Packs" and press Enter.
   Note: If not able to locate the above file path, please contact <u>EventTracker support</u> to get the assistance.

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Parsing Rules
- Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.



Figure 22

💺 Export Import Utility							
Export	Import						
1. Pr 2. Cli	ovide the p ck the Imp	path and file nam port button.	e of the Categories file. Use the '' button to				
Opt	ons		Location				
۱	Category						

Figure 23

3. Click the Import tab.

### 5.1 Saved Searches

- 1. After opening **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click the browse \_\_\_\_\_ button.
- 2. Navigate to the knowledge pack folder and select the file with extension ".iscat", e.g. Categories\_Cloudflare.iscat and click on the Import button.

Netsurion. EventTracker

Export Import Utility				_		$\times$
Export Import						
1. Provide the path and file na 2. Click the Import button.	ame of the Catego	ies file. Use the '' button to browse	and locate the import file.			
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location	Source : *iscat				
			Imp	ort	Clos	e

Figure 24

EventTracker displays a success message:





### 5.2 Alerts

- 1. After opening **Export Import Utility** via **EventTracker Control Panel**, click **Alert** option and click the browse ... button.
- 2. Navigate to the knowledge pack folder and select the file with extension ".isalt", e.g. Alerts\_ Cloudflare.isalt and click on the Import button.

Export Import Utility			_		$\times$
Export Import					
1. Provide the path and file nam 2. Click the Import button.	e of the Alerts file. Use the '' butt	on to browse and locate the import file.			
Options	Location				
Category	Import E-mail settings				
Filters     Alerts	Set Active     Only if notifications set     By default	This setting is applicable only for imports from Alert files. For v7, the active status will be set "Active" key available in the configuration se	Legacy ( based on ection.	v6x)	
<ul> <li>Systems and Groups</li> </ul>	Watchlist Configuration				
◯ Token Value	This setting is applicable only f	on or alerts which have Advanced watchlist config be user should make sure the watchlist groups :	jured. are availat	ble	
○ Reports	on the console where the alert	s are imported.			
O Behavior Correlation					
	Source : *.isalt				
		Impo	ort	Clos	e

Figure 26

EventTracker displays a success message:



Figure 27

### 5.3 Parsing Rules

1. After opening **Export Import Utility** via **EventTracker Control Panel**, click the **Token Value** option, and click the browse button.

2. Navigate to the knowledge pack folder and select the file with extension **".istoken"**, e.g. Parsing Rules\_ Cloudflare.istoken and click on the Import button.

Export Import Utility	-	_	
Export Import			
1. Provide the path and file na 2. Click the Import button	me of token value file. Use the '' button to browse and locate the import file.		
Options	Location		
Category			
◯ Filters			
○ Alerts			
O Systems and Groups	Source : *.istoken		
Token Value			
◯ Reports			
O Behavior Correlation			
		_	
	Import		Close

#### Figure 28

### 5.4 Reports

1. In EventTracker control panel, select **Export/ Import utility** and select the **Import tab**. Click **Reports** option and choose **New (\*.etcrx)**.

Netsurion. EventTracker

🌯 Export Import Utility		_		$\times$
Export Import				
1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains temp	e of Schedule Report file. Use the '' button to browse and locate the import file. late, first import template and proceed with exportimport utility.			
Options	Location			
Category				
◯ Filters				
⊖ Alerts	C Legacy (*.issch)			
O Systems and Groups	Source : *.issch			
O Token Value				
Reports				
O Behavior Correlation				
	Impo	irt	Clos	e

Figure 29

2. After selecting **New (\*.etcrx)**, a new pop-up window appears. Click **Select File** button and navigate to knowledge pack folder and select file with extension **".etcrx"**, e.g. **Reports\_ Cloudflare.etcrx**.

🔁 Reports Im	Reports Import								
Note : If report	(s) contains tem	plate, first import temr	late and proceed	with report import proces	8				
Select file	Select file *.etcrx Select file								
Available repo	rts								
Title     Frequency     Show all     Image: Comparison of the state of the sta									
		Title	Sites	Groups	Systems	Frequency	Runtime	Туре	



Wait while reports are being populated in below tables. Now, select all the relevant reports and click Import button.

Note: Set run time option is not applicable for Defined Reports and Hourly Reports						
Set run time for report(s) from	AM • at interval of _ minutes	Set 🕕				
Replace	to Replace	Assign systems				
		Note: Make sure that Site(s), Group(s) and System(s) selections are v	alid.	$\otimes$		



EventTracker displays a success message.



Figure 32

### 5.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager web interface.

		🔎 🛛 Admin 🗸	Tools 🕶 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	📌 / Da
Alerts	Sector Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
mi r sc Casebook Configuration	Q IP Lookup Configuration	r Weights	Systems since the last 24 hours
● Category	·☆ Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		



2. Click the **import object** icon.



#### Figure 34

3. A pop-up box appears, click Browse and navigate to knowledge packs folder (type "%et\_install\_path%\Knowledge Packs" in navigation bar) with the extension ".etko", e.g. KO\_ Cloudflare.etko and click Upload button.

Import	
KO_ <product name="">.etko</product>	🖆 Browse Upload

#### Figure 35

4. Wait while EventTracker populates all the relevant knowledge objects. After the objects are displayed, select the required ones, and click on **Import** button.





### 5.6 Dashboards

- 1. Login to EventTracker manager web interface.
- 2. Navigate to **Dashboard**  $\rightarrow$  **My Dashboard**.
- 3. In "My Dashboard", click Import.

≡	Event <b>Tracker</b>								
	Home								
٩	My Dashboard								
	Threats								
	Incidents								
	Behavior Correlation								
	Change Audit								
	Compliance								

Figure 37

↑ Dashboard / My Dashboard
🕀 🧭 🕲 🌣 1 耳 🕲 🛈



- Click the Browse button and navigate to knowledge pack folder (type "%et\_install\_path%\Knowledge Packs" in navigation bar) where ".etwd", e.g. Dashboards\_ Cloudflare.etwd is saved and click on Upload button.
- 5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click **Import**.

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	
🗁 Browse	Upload
Available widgets	
Select All	



Netsurion. EventTracker





## 6. Verifying knowledge pack in EventTracker

### 6.1 Saved Searches

- 1. Login to EventTracker manager web interface.
- 2. Click Admin dropdown and click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand **Cloudflare** group folder to view the imported categories.



Figure 41

### 6.2 Alerts

1. In the EventTracker manager web interface, click the Admin dropdown, and then click Alerts.



2. In search box enter "<search criteria> e.g. Cloudflare and click the Search button. EventTracker displays an alert related to Cloudflare.

P	Alerts										Admin / Alerts
l	Show All ~							Search by Alert	name 🗸	cloudflare	ଦ୍ ଦ୍
h										Critical 🗖 o	
I	196	54				196	System	157	196	Low 5	110
	Available Alerts Total number of alerts available	Active Alerts Total number of active alerts				System/User D Count for system a	efined Alerts nd user defined alerts	23	Alerts by T Count of alerts	hreat Level s by threat level	
ľ	Activate Now Click 'Activate Now' af	ter making all changes								Total: 1	age Size 25 🗸
l	Alert Name A		Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies	То
L	🗌 දිදි Cloudflare: A web traffic has been dropped by WAF		•							Cloudflare	



### 6.3 Parsing Rules

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing Rule.
- 2. In the Parsing Rule tab, click on the Cloudflare group folder to view the imported Token Values.

Parsing Rule	25						
Parsing Rule	Template						
Groups			<b>(</b>		Token-Value	Display	name 🗸
		<u>ل</u>		L	+		Display name
cioudilare			•		+		Action Type
					+		Client ASN

Figure 43

### 6.4 Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.







- 2. In Reports Configuration pane, select the Defined option.
- 3. Click on the **Cloudflare** group folder to view the imported reports.

Repor	t Configuration					
⊖ Scł	neduled 🔿 Queued 🔘 Defined					
Repor	t Groups	Ð		Repo	orts config	uration: Cloudflare
S.,	Security		^	÷	Ü 2,	
1.5	Compliance					Title
S.,	Operations				£ <b>\$</b> \$	Cloudflare - Login and Logout activities
<u> </u>	Flex				£\$3	Cloudflare - Firewall activities
B	Cloudflare	Ø				Cloudflare - Audit activities

Figure 45

### 6.5 Knowledge Objects

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
- 2. In the **Knowledge Object** tree, expand the **Cloudflare** group folder to view the imported Knowledge objects.

Knowledge Objects	
Search objects	Activate Now
Groups 🕀 🧭 🗓	Object name Cloudflare Events
Cloudflare	Applies to Cloudflare
Cloudflare Events 🧭 🗓	Rules

Figure 46

### 6.6 Dashboards

1. In the EventTracker web interface, Click on Home Button and select **My Dashboard**.





2. Select **Customize daslets** Subtron and type **Cloudflare** in the search bar.





Netsurion. EventTracker\*

Custor	nize dashlets			×
Cloudf	lare			Q
	udflare - Audit Events	Cloudflare - Audit Events Timeli	Cloudflare - Dropped Traffic by	Cloudflare - Dropped Traffic by
	udflare - Dropped Traffic by	Cloudflare - Dropped Traffic by	Cloudflare - Edge Colo ID by so	Cloudflare - Firewall Event coun
	udflare - Firewall Events	Cloudflare - Firewall Events Tim	Cloudflare - UI Login activities	
				Add Delete Close

Figure 49