Netsurion | EventTracker®

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.

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)

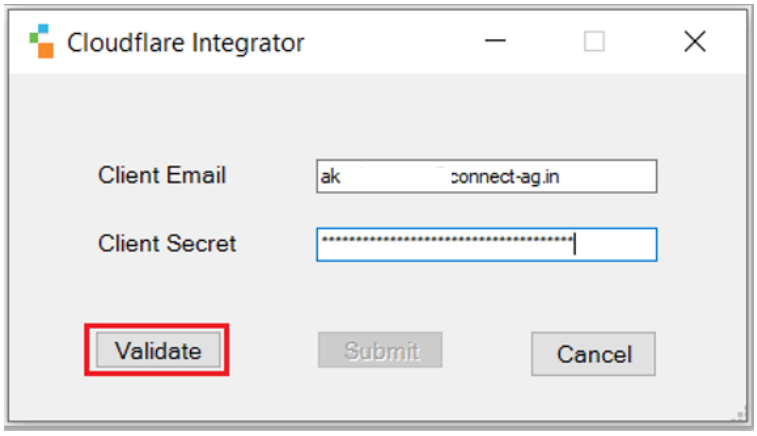

Figure 2

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

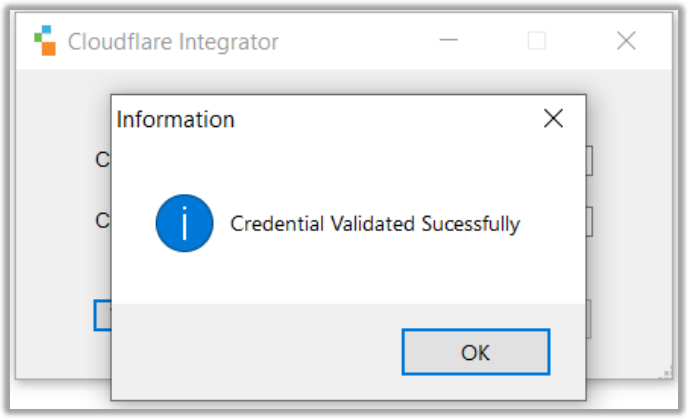

Figure 3

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

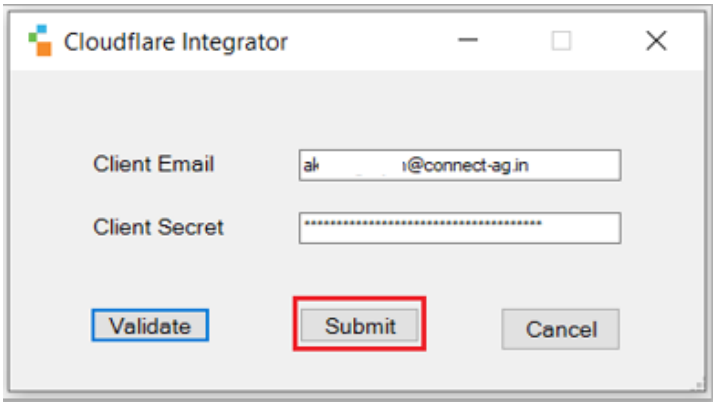

Figure 4

5. A pop-up window appears with message.

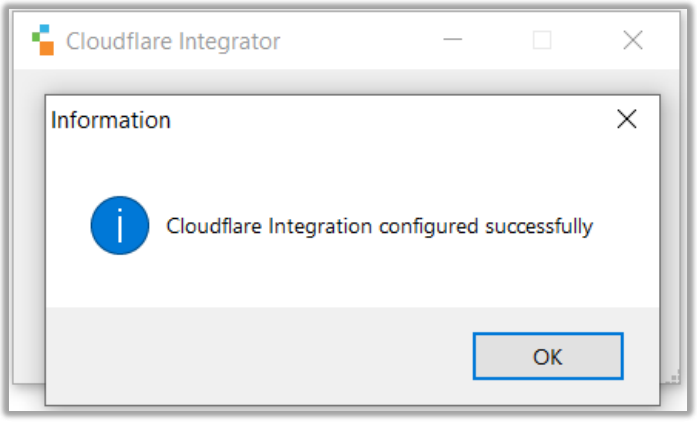

Figure 5

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/

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.

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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safari/537.36		country
11/09/2020 07:53:01 PM	log	58224	IR	2.183.175.37	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36	/api/v2	waf
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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36	/%3Cscript%3Ealert()%3C/script%3E	waf
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

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",
"id": "c472a70**************************",
"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**

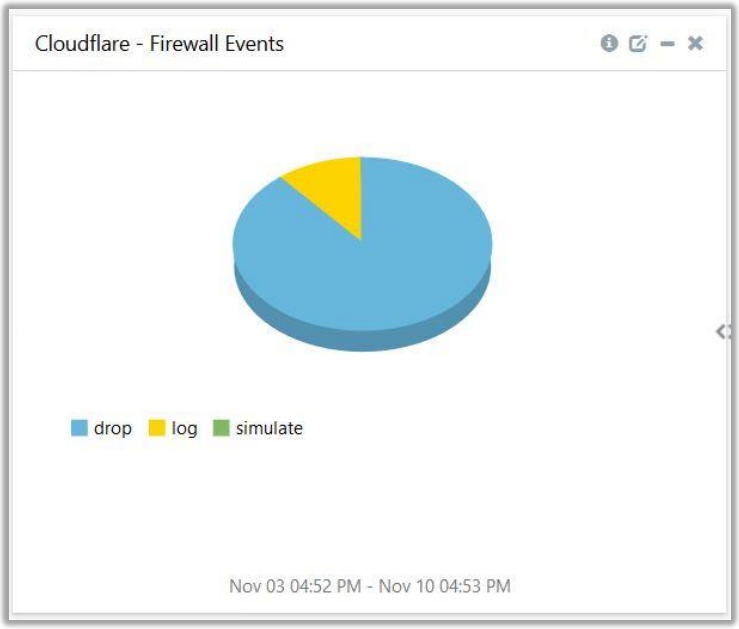

Figure 11

- **Cloudflare - Audit Events**

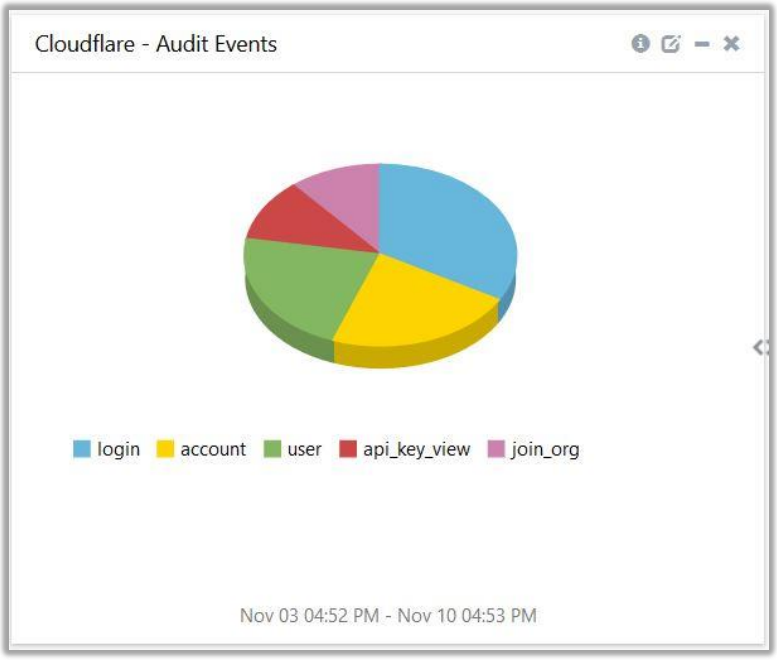

Figure 12

- **Cloudflare - Firewall Event counts by Zone**

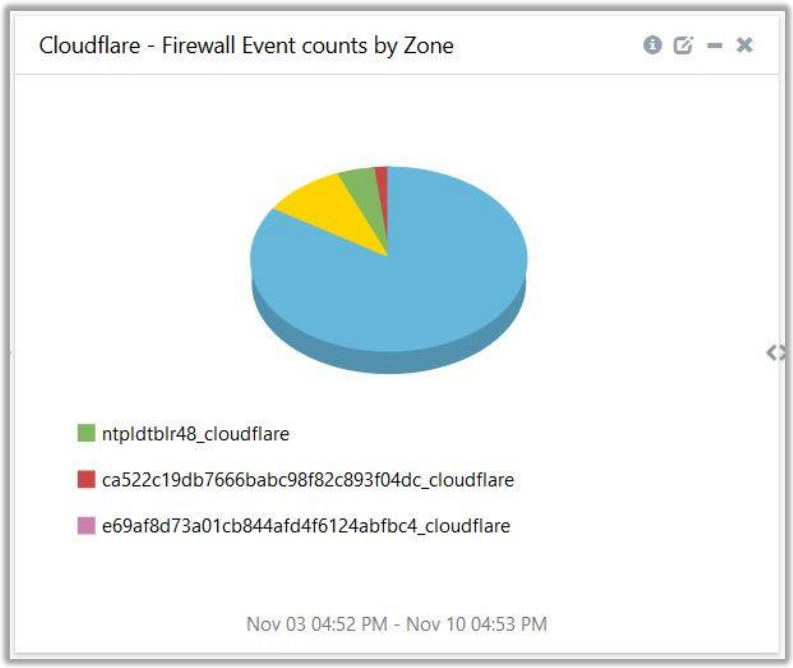

Figure 13

- **Cloudflare - Firewall Events Timeline**

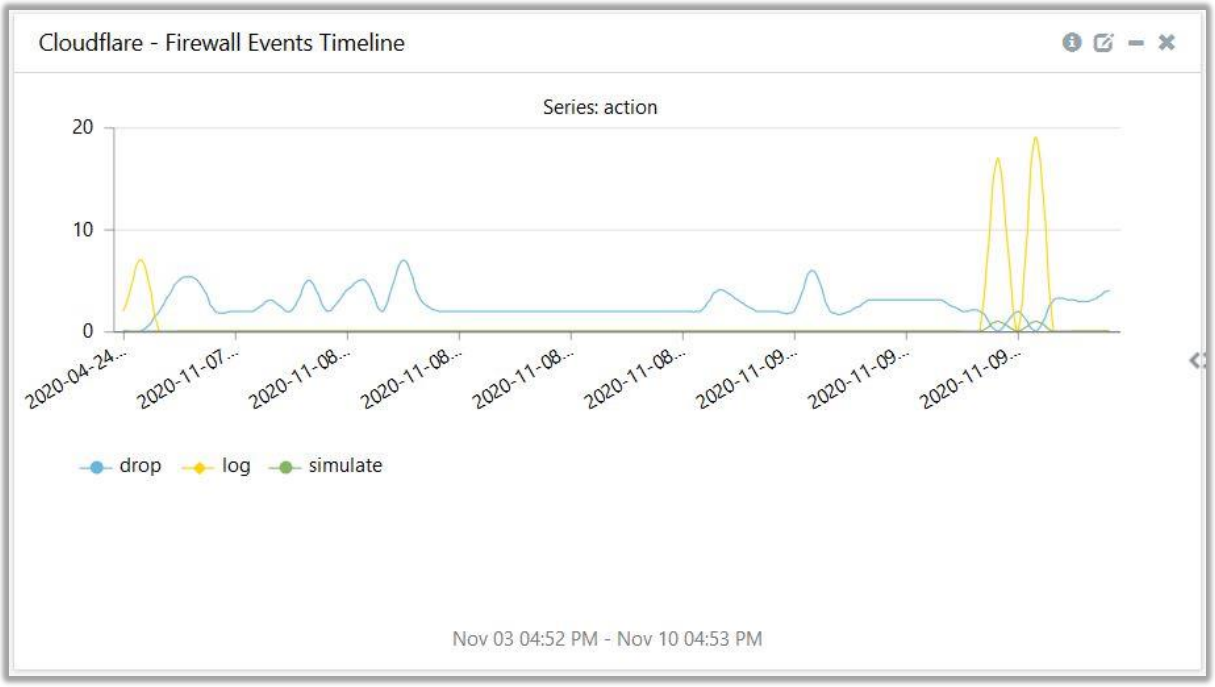

Figure 14

- **Cloudflare - Audit Events Timeline**

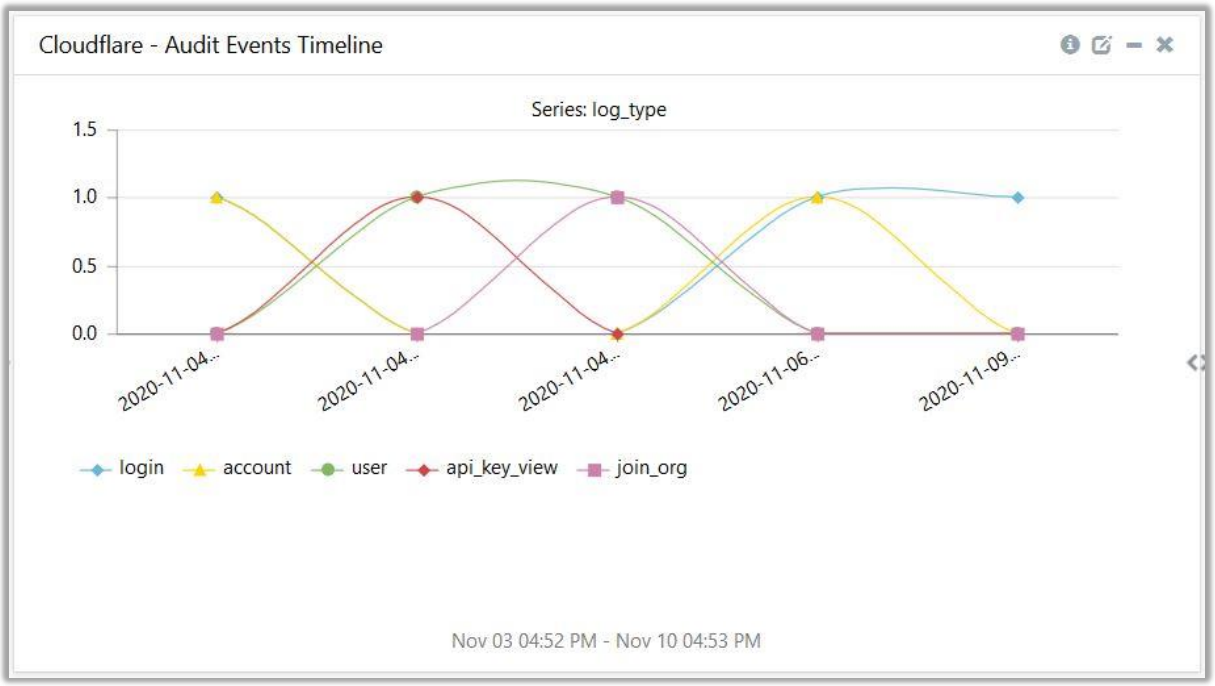

Figure 15

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

Figure 16

- **Cloudflare - Dropped Traffic by Country code**

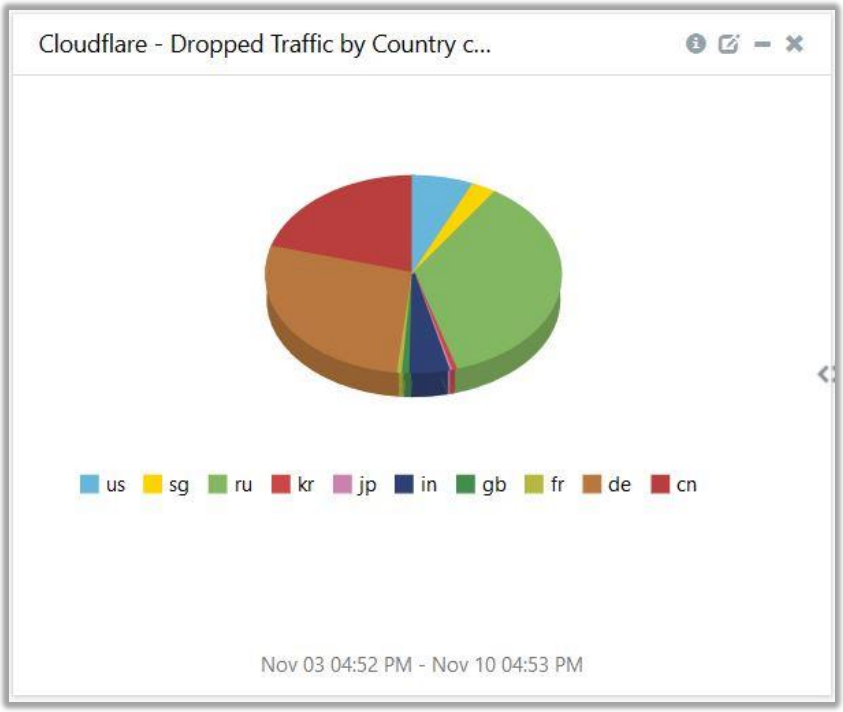

Figure 17

- **Cloudflare - Dropped Traffic by ASN**

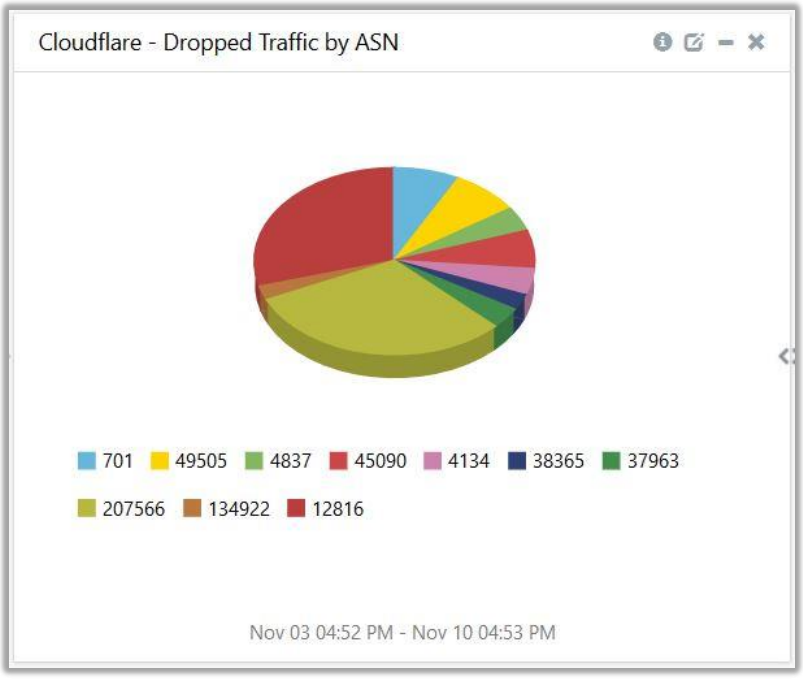

Figure 18

- **Cloudflare - Dropped Traffic by user agents**

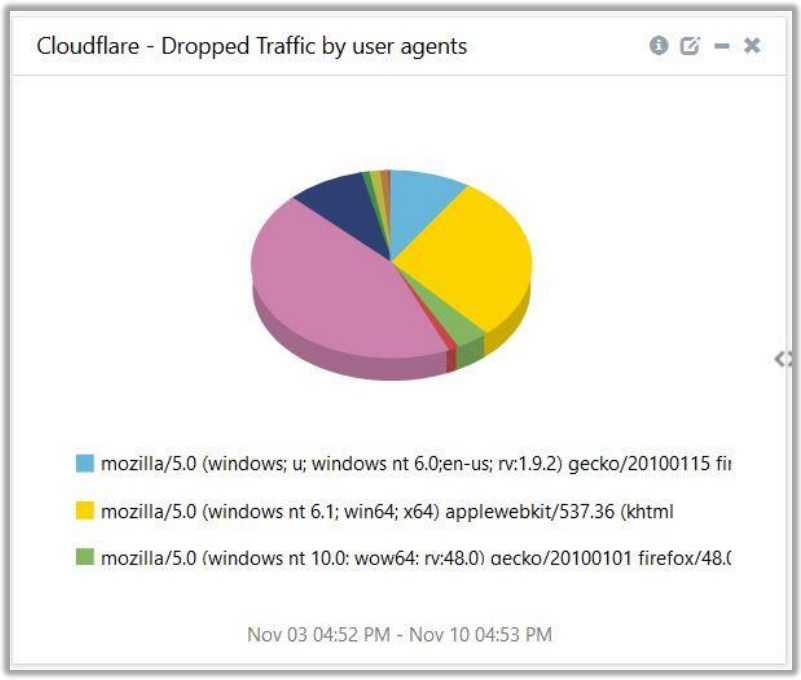

Figure 19

- **Cloudflare - Dropped Traffic by source IP**

Figure 20

- **Cloudflare - Edge Colo ID by source IP**

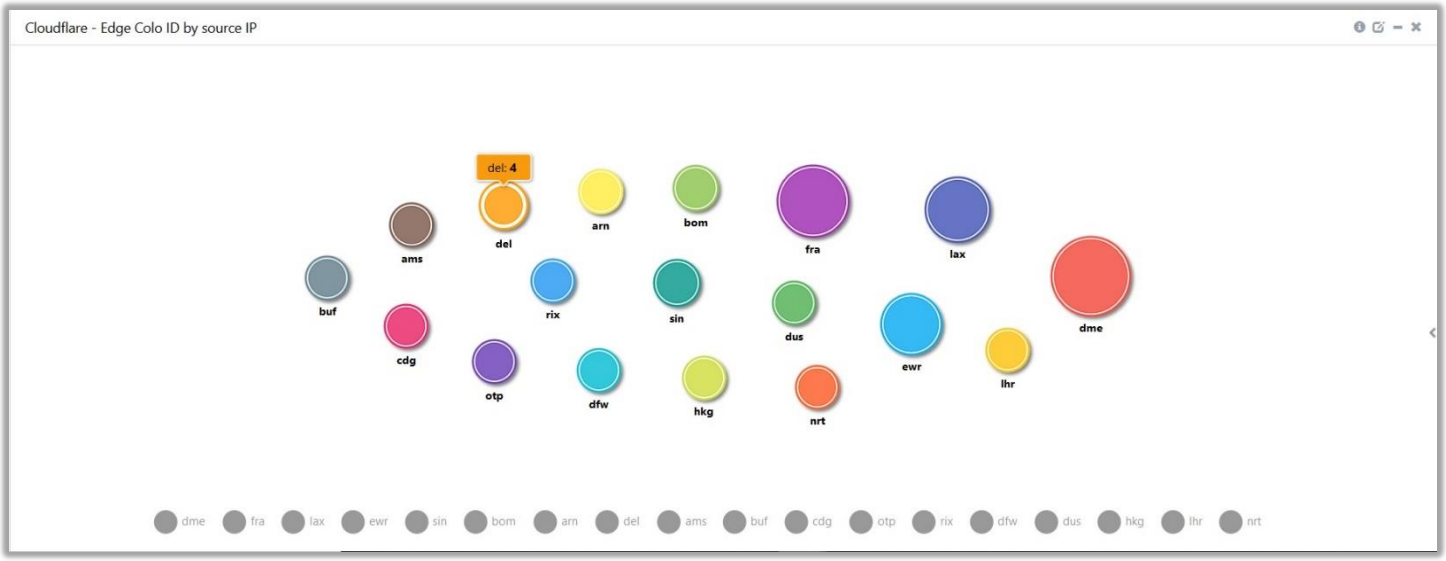

Figure 21

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".
2. Type **"%et_install_path%\Knowledge Packs"** and press **Enter**.
   Note: If not able to locate the above file path, please contact EventTracker support 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**.

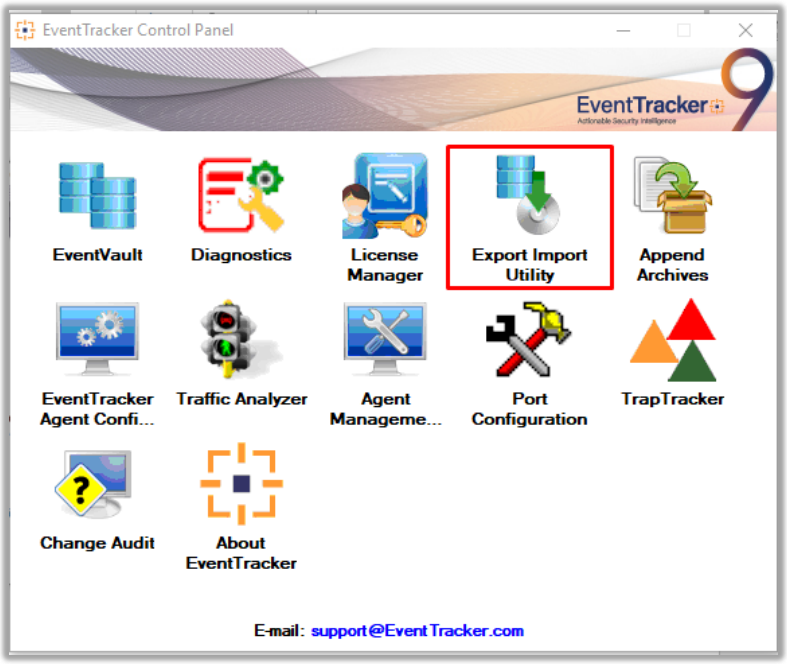

Figure 22

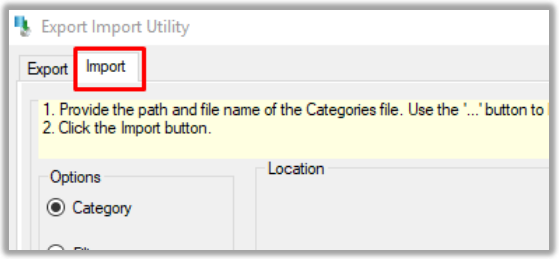

Figure 23

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.

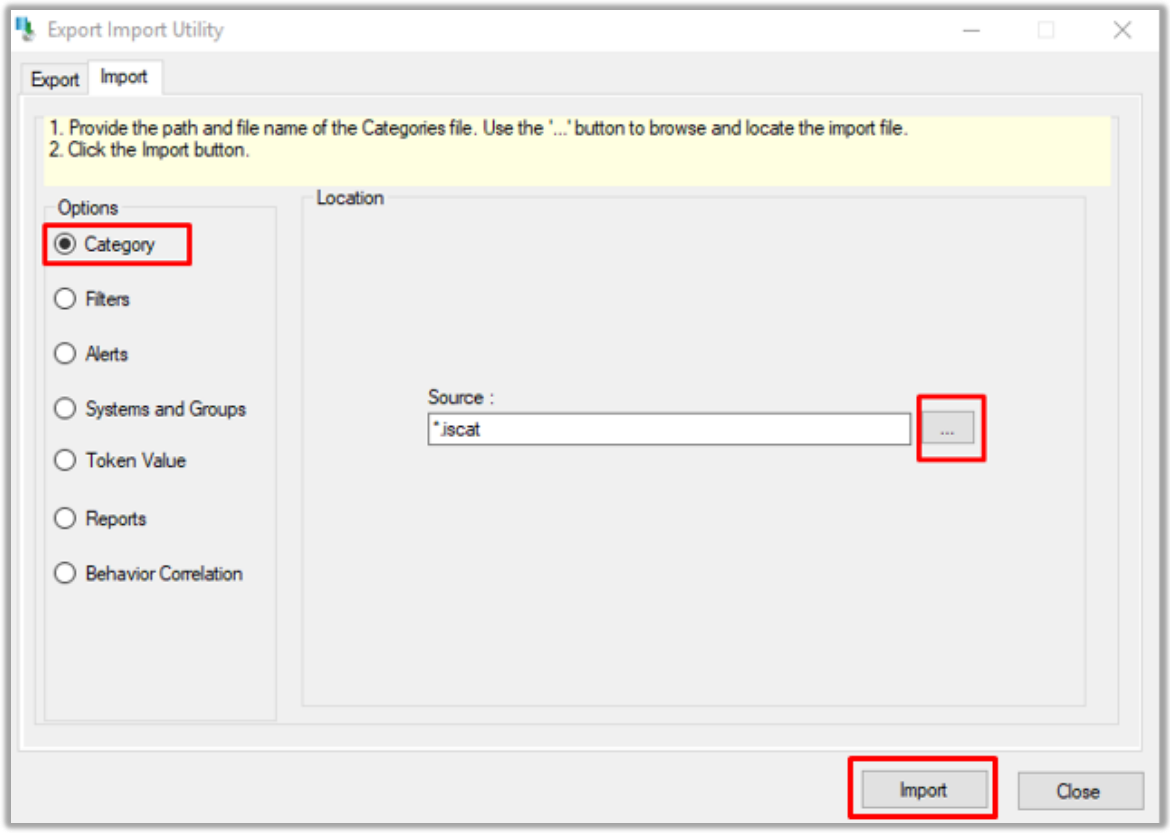

Figure 24

EventTracker displays a success message:

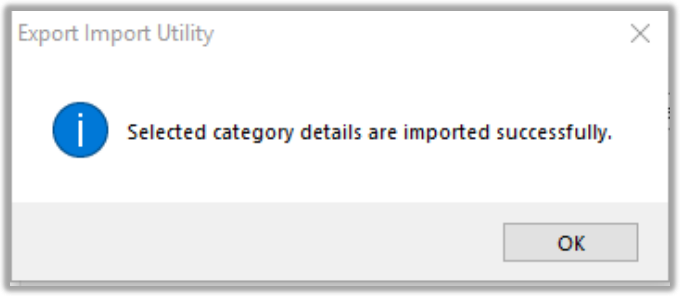

Figure 25

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.

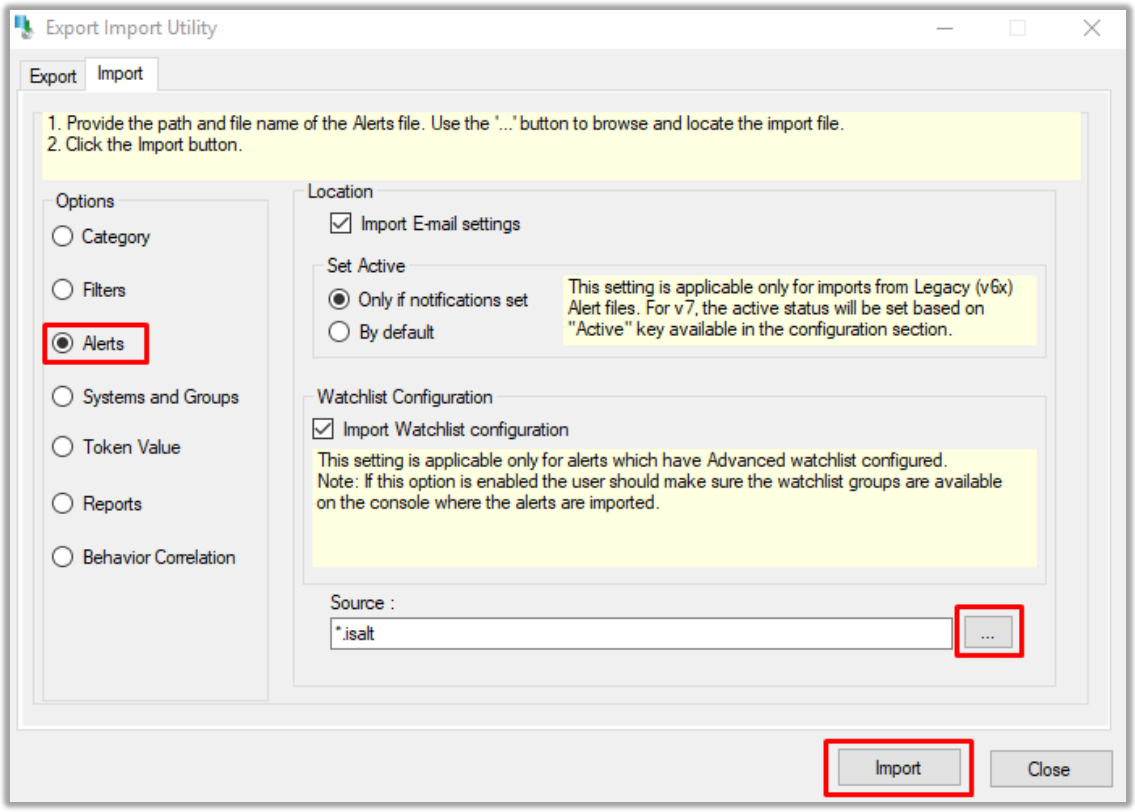

Figure 26

EventTracker displays a success message:

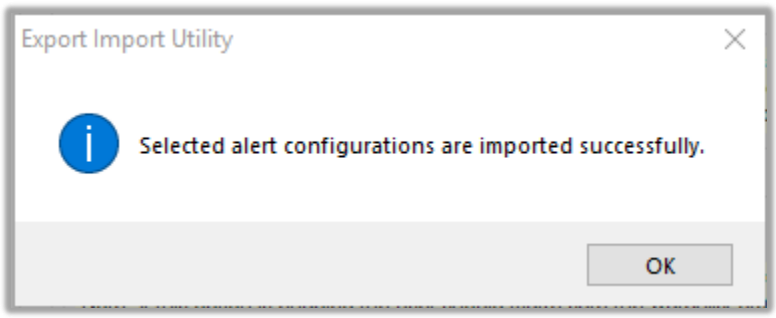

Figure 27

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.

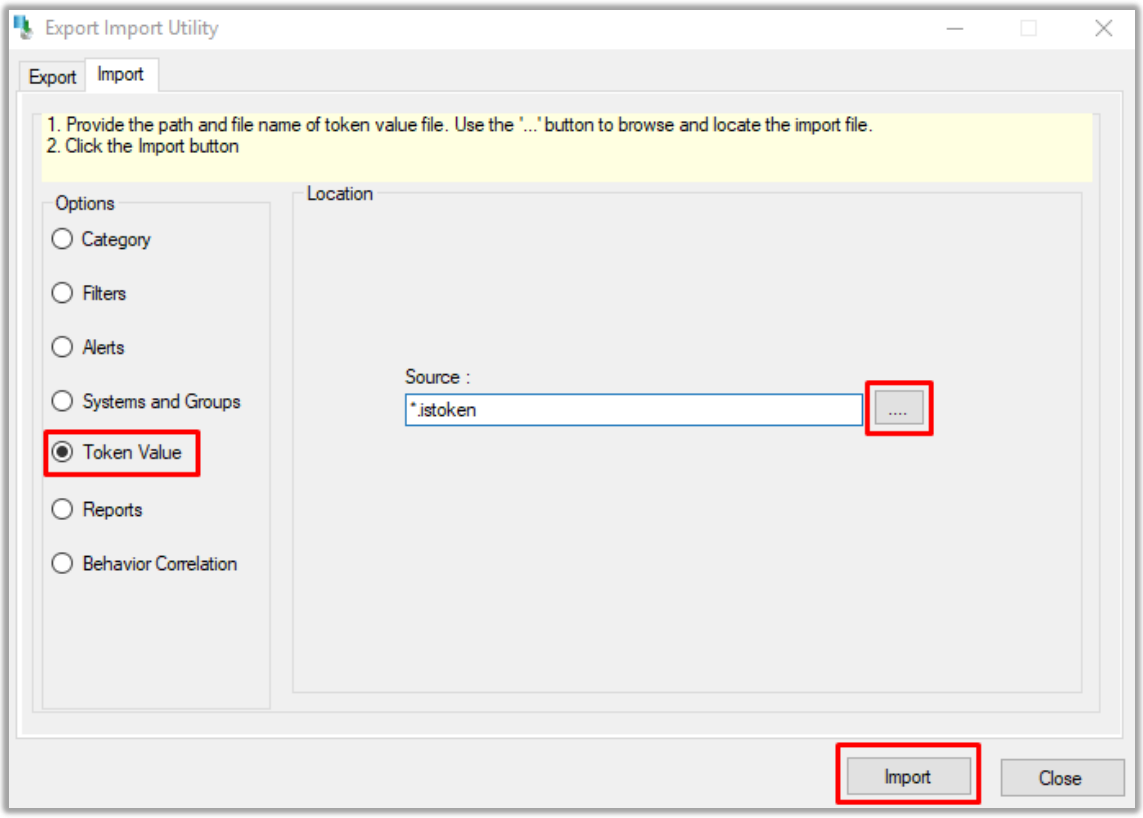

Figure 28

5.4 Reports

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

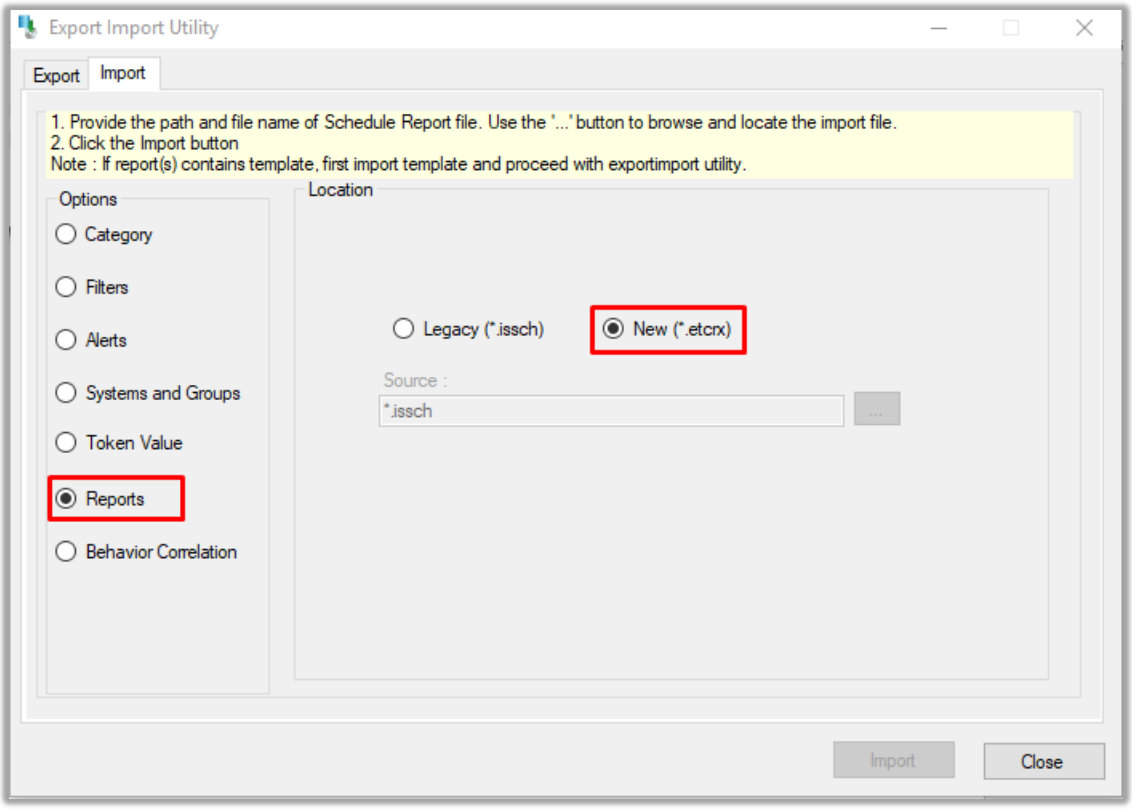

Figure 29

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.**

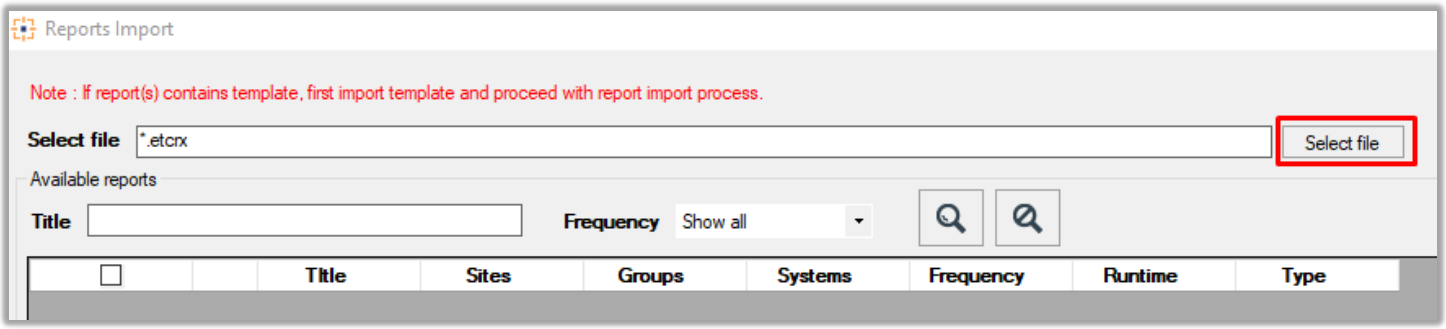

Figure 30

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

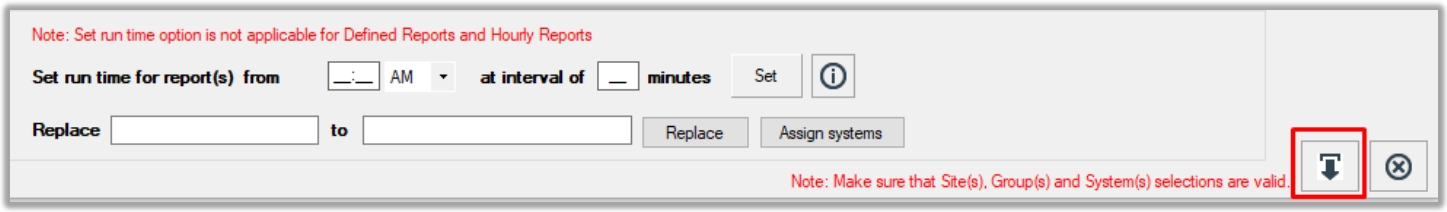

Figure 31

EventTracker displays a success message.

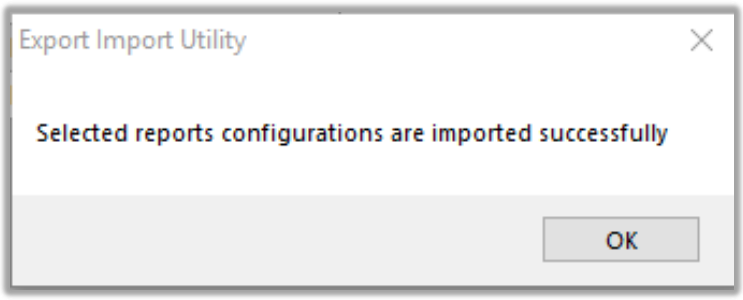

Figure 32

5.5 Knowledge Objects

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

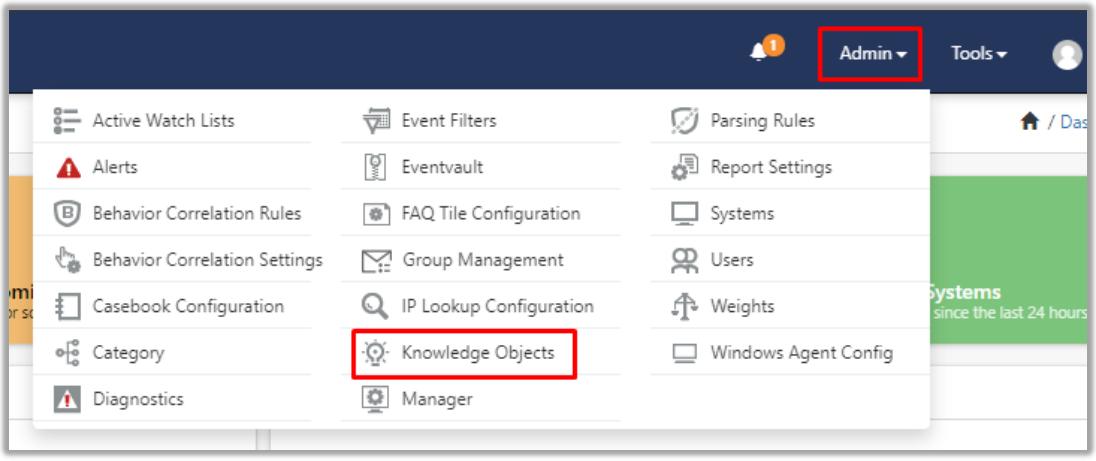

Figure 33

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

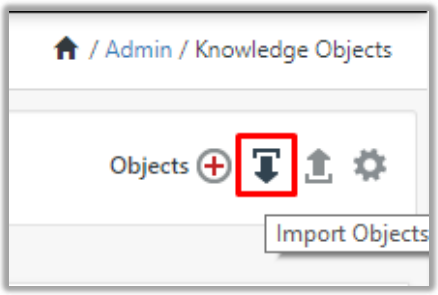

Figure 34

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.

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.

Figure 36

5.6 Dashboards

1. Login to **EventTracker manager web interface**.
2. Navigate to **Dashboard → My Dashboard**.
3. In "My Dashboard", click **Import.**

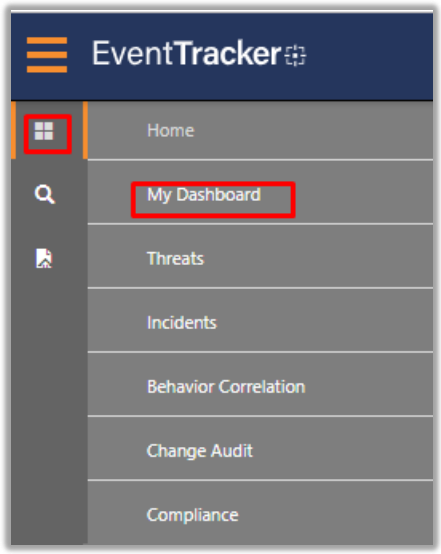

Figure 37

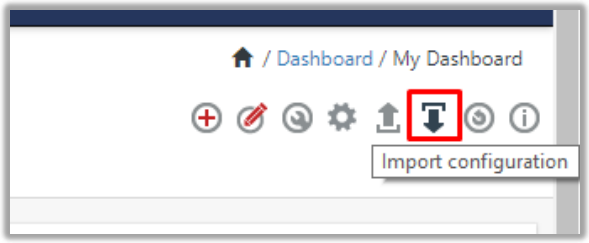

Figure 38

4. 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**.

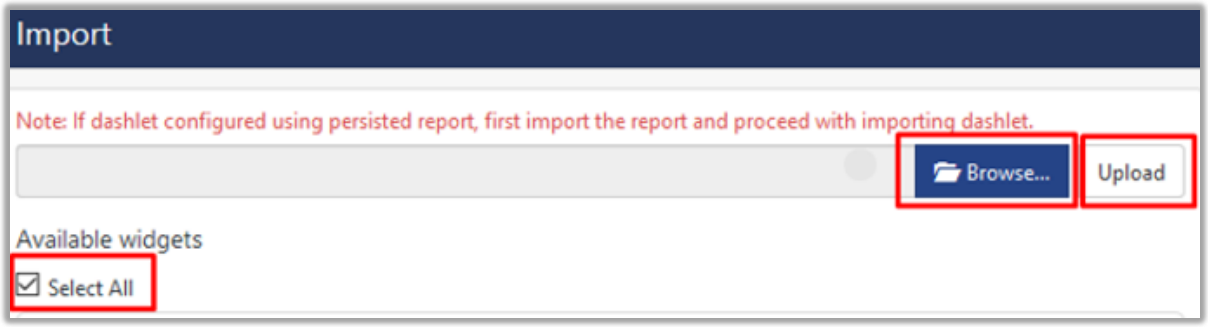

Figure 39

Figure 40

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.

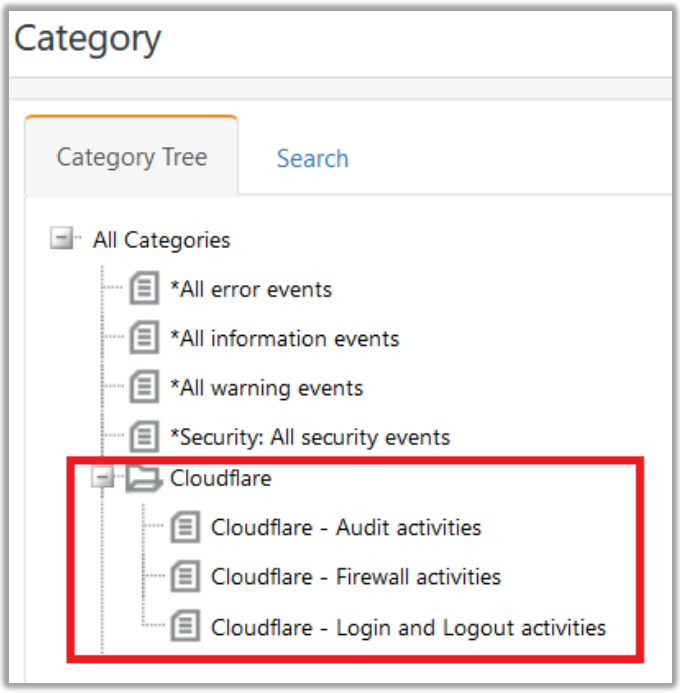

Figure 41

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.**

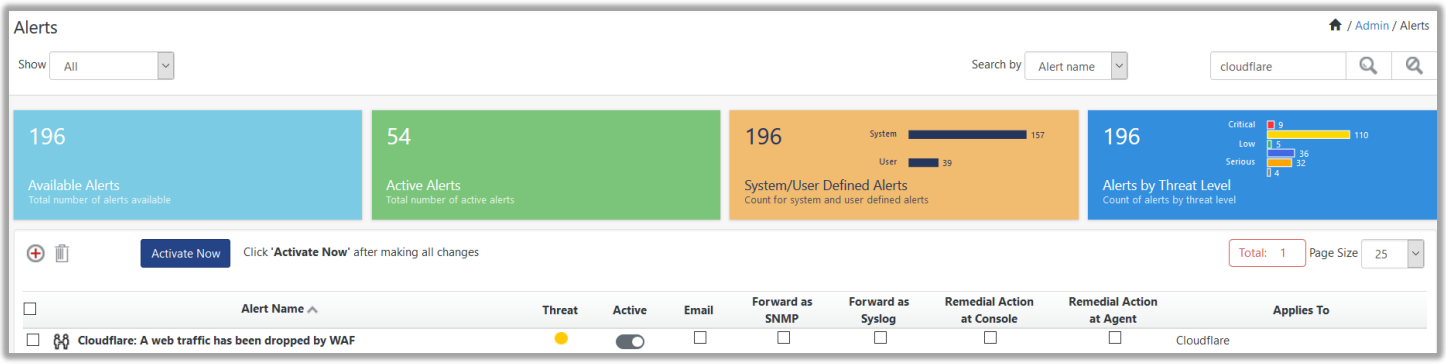

Figure 42

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.

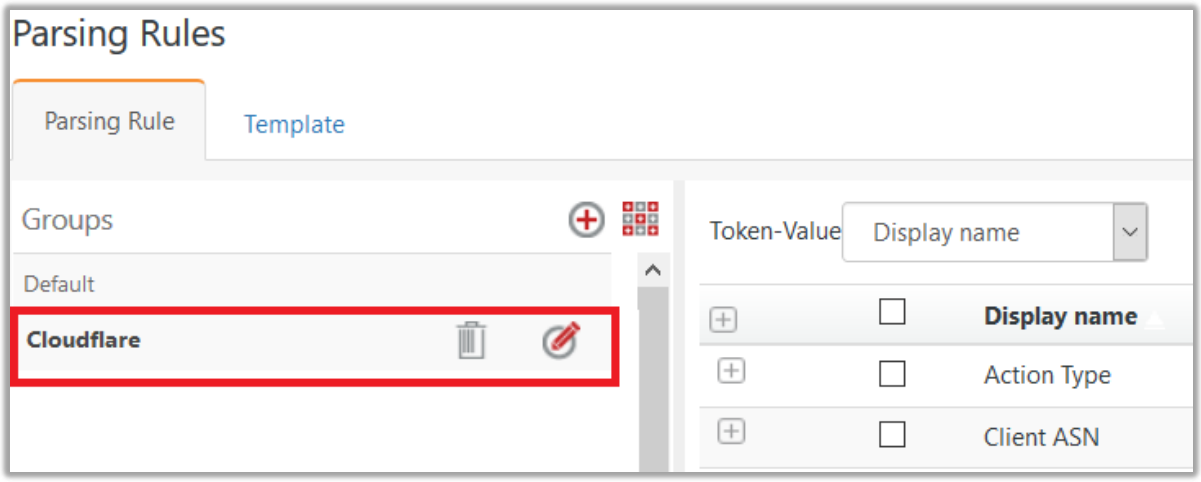

Figure 43

6.4 Reports

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

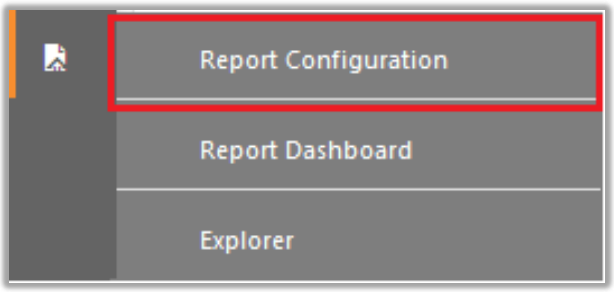

Figure 44

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

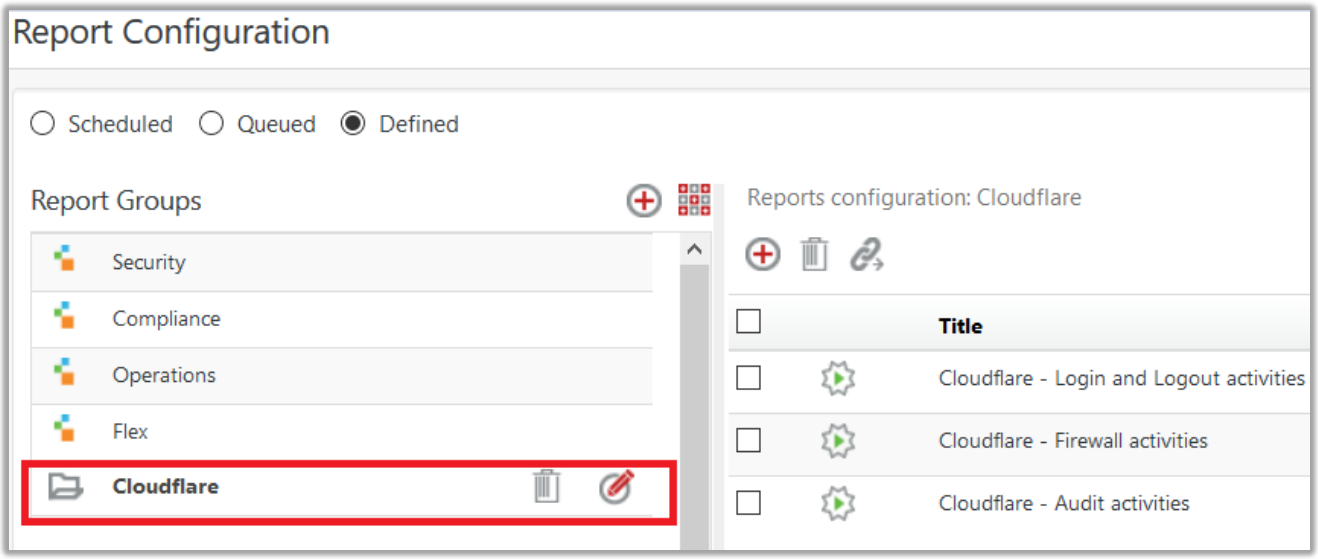

Figure 45

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.

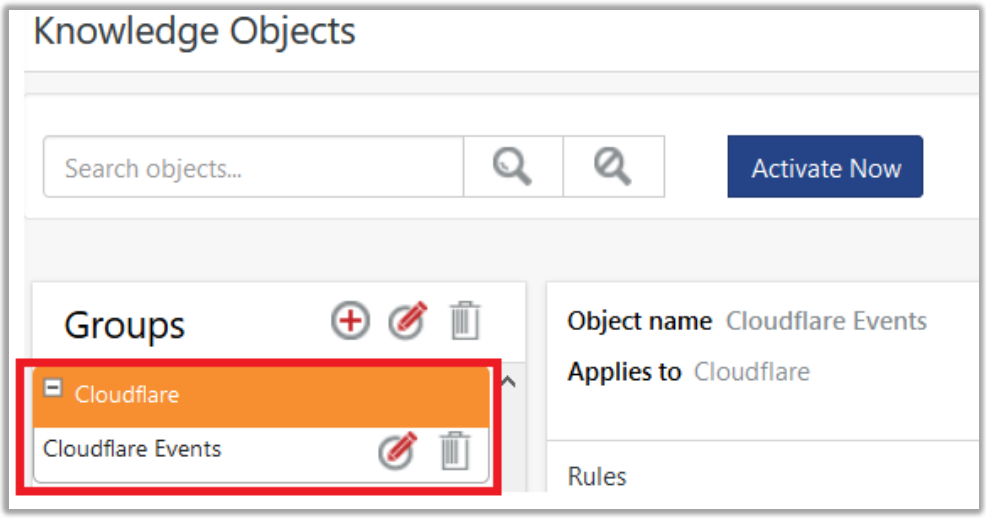

Figure 46

6.6 Dashboards

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

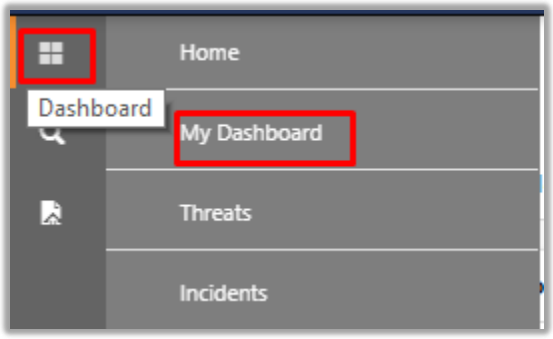

Figure 47

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

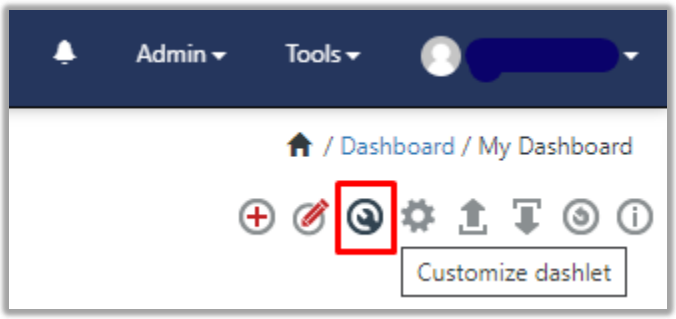

Figure 48

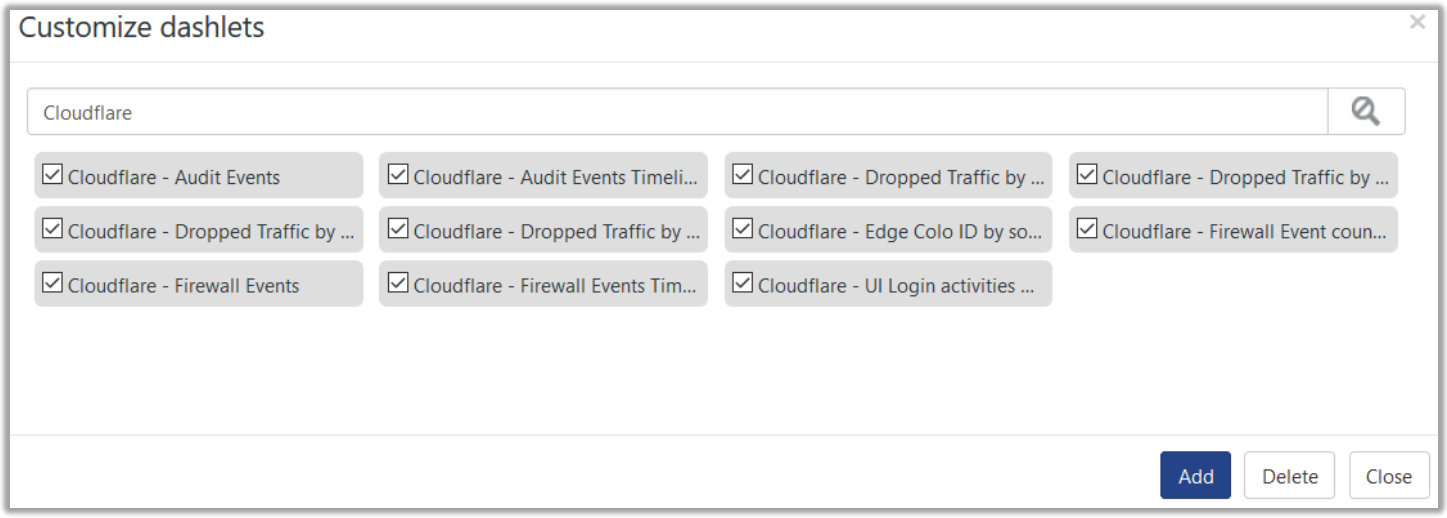
Customize dashlets
Cloudflare
Cloudflare - Audit Events
Cloudflare - Audit Events Timeli...
Cloudflare - Dropped Traffic by ...
Cloudflare - Dropped Traffic by ...
Cloudflare - Dropped Traffic by ...
Cloudflare - Dropped Traffic by ...
Cloudflare - Edge Colo ID by so...
Cloudflare - Firewall Event coun...
Cloudflare - Firewall Events
Cloudflare - Firewall Events Tim...
Cloudflare - UI Login activities ...
Add
Delete
Close

Figure 49