Netsurion | EventTracker®

Integration Guide for Fastly CDN/WAF

EventTracker v9.x and later

Publication Date: February 06, 2020

Abstract

This guide provides instructions to configure/ retrieve **Fastly CDN/WAF** events by "Syslog" logging for access events collection and REST API for Fastly internal/ operational event collection. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **Fastly CDN/WAF**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Fastly CDN/WAF.**

Audience

Administrators who are assigned the task to monitor **Fastly CDN/WAF** events using EventTracker.

Table of Contents

1. Overview

Fastly is a **Content Delivery Network (CDN) and Web Application Firewall (WAF). Fastly CDN** makes content available through

- Users/organizations websites.
- Internet-accessible (hosted) application programming interfaces (APIs).

Fastly's CDN/WAF Service then makes the transmission of that content (which we sometimes refer to as "content objects") more efficient by automatically storing copies at intermediate locations on a temporary basis.

Fastly WAF protects your applications from malicious attacks designed to compromise web servers. It protects against injection attacks, cross site scripting, HTTP protocols violations, and more. The Fastly WAF provides rules that detect and block potential attacks. The rules are collected into a policy and deployed within your Fastly service at the edge.

EventTracker, when integrated with Fastly CDN/WAF, collects log from Fastly CDN/WAF and creates a detailed reports, alerts, dashboards and saved searches. These attributes of EventTracker help users to view the most critical and important information on a single platform.

Flex reports will contain detailed overview of activities like, Fastly user login/ logout, Fastly login failed, user management events, Fastly service management events, devices, Fastly access events by success and failure, blocked URL and IP and its reason.

Alerts are provided as soon as any critical event triggered by Fastly CDN/WAF. With alerts users will be able to get real time events such as, login failed, service or service version deletion in their email services. From visual representation/ overview of top activities being performed in Fastly CDN/WAF to unauthorized user access (failed) can be viewed on EventTracker ‘dashboard’. For e.g. “Fastly CDN/WAF - Access events by user agent” dashlet displays the user-agents trying to access any specific domain/ URL. “Fastly CDN/WAF - User login fail (Audit events by region)” dashlet displays the Login failure occurring in Fastly account in a world map by country. Dashlets associated with WAF activity will display information such as, PHP Injections attacks, SQL injection attacks, Application attack Session fixation, Application attack RCE (Remote code execution), etc.

2. Prerequisites

- EventTracker manager v9.x is required.
- EventTracker knowledge packs are required.
- Syslog port of the EventTracker console should be open with public IP address.
- API token of a user must be with at least Engineer permissions.

Note: To enable Fastly WAF logging, contact Fastly WAF support.

3. Integrating Fastly CDN/WAF with EventTracker

Although there are various methods to export the Fastly logs, EventTracker recommends using syslog.

Note - The syslog method will require a public IP address to be assigned to syslog port of the EventTracker console.

3.1 Collecting API Key

To configure EventTracker to receive logs from Fastly, we need API key with at-least engineer permissions. To do so, follow the below steps to collect the API key:

1. Go to your "**Fastly**" home page and click on user account:

Figure 1

2. On the left panel, click "**Personal API token**" and then click "**Create Token**"

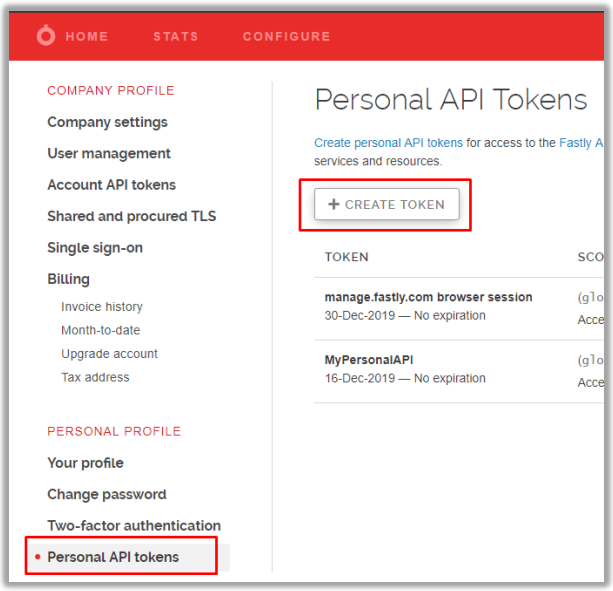


Figure 2

3. Enter the given required fields:
   - **Password** – Enter the password of your Fastly account.
   - **Name** – Give a name to the API. E.g. EventTrackerAPI.
   - **Apply to** – Set it to "**All services**".
   - **Set a scope –** Set it to "**Global API access(**global**)**".
   - **Set a token expiration –** Set it to "**Never expire**".
4. Click "**create"** to generate a new key.

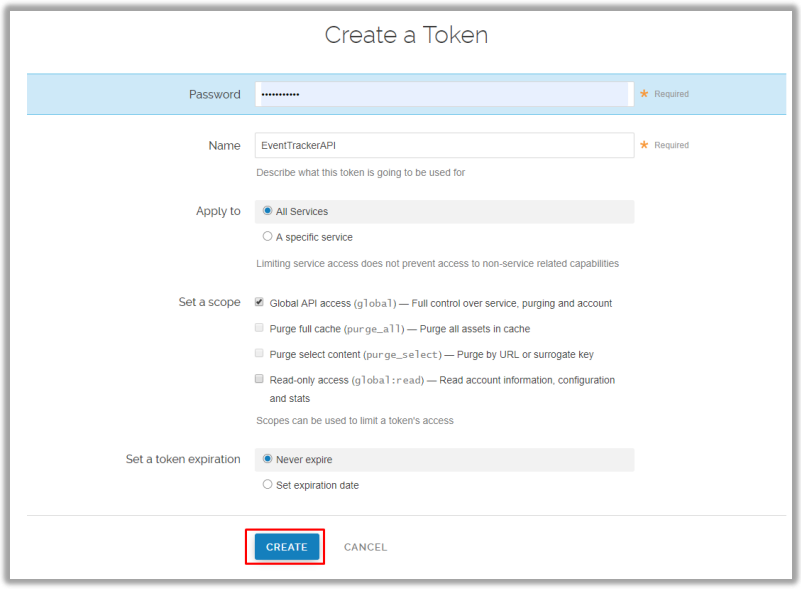


Figure 3

5. A pop-up screen will be triggered for new token creation. Note down the API Key and click "**Okay**"

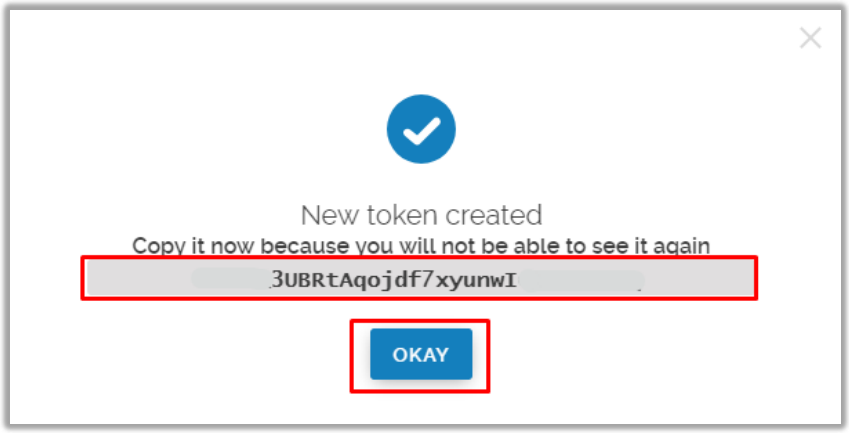


Figure 4

3.2 Forwarding logs from "Fastly audit and syslog"

1. Contact the EventTracker support team and get the "**FASTLY_CDN_Integrator**" executable file.
2. Once the executable application is received, right click on the file and select "**Run as Administrator**".
3. Upon Running the Integrator, fill-in the given fields.

Follow the below procedures to configure Fastly CDN/WAF for EventTracker:

1. Right click the "**EventTracker (Fastly_CDN)**" executable file and "Run as administrator".
2. Enter the **Fastly API key** and click "**Validate**"

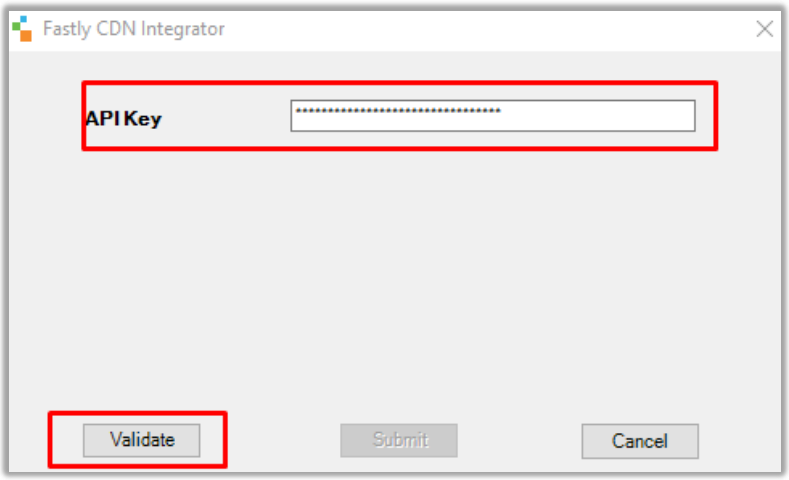


Figure 5

3. Once credentials have been successfully verified, a pop-up message will be triggered for successful validation. Else, pop-up will be triggered for validation failure.
4. Next,
   - Select the service/s "**Active Service Name/ Version**" that needs to be monitored.
   - In "**Syslog IP Address**" field enter the EventTracker Public Ip address.
   - In "**Syslog Port**" enter the EventTracker syslog port. E.g. "**514**".

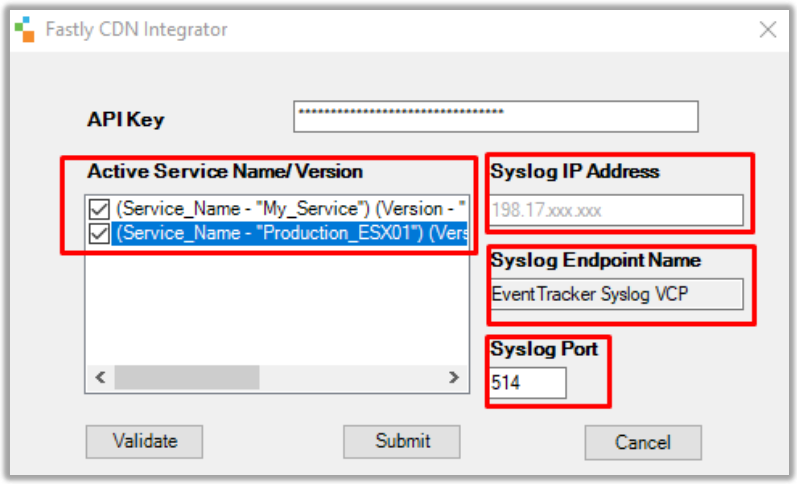


Figure 6

5. Click "**Submit**". When successfully configured, a pop-up message will be triggered for successful integration.

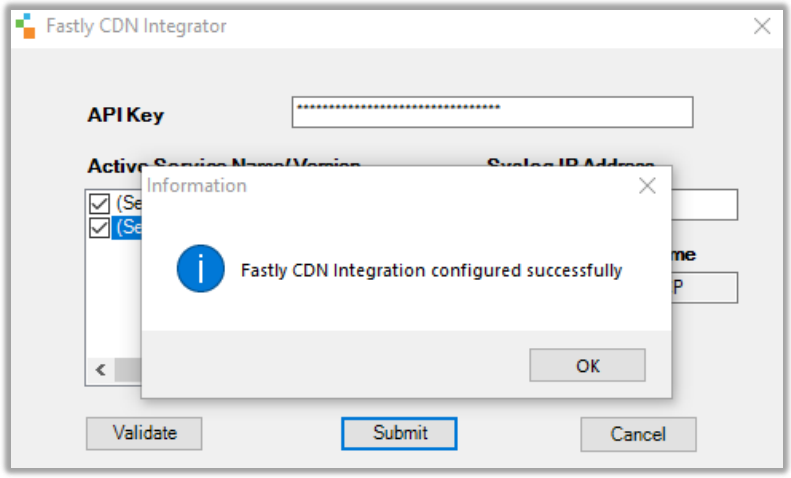


Figure 7

4. EventTracker Knowledge Packs

4.1 Categories

- **Fastly CDN/WAF - Access events**
- **Fastly CDN/WAF - User Login success (Audit events)**
- **Fastly CDN/WAF - User Login Fail (Audit events)**
- **Fastly CDN/WAF - Domain access errors (Access events)**
- **Fastly CDN/WAF - WAF: High severity URLs**

- **Fastly CDN/WAF - Blocked events**

4.2 Alerts

- **Fastly CDN/WAF: User login failed (Audit events)**
- **Fastly CDN/WAF: Service version has been deactivated (Audit events)**
- **Fastly CDN/WAF: Service has been deleted (Audit events)**
- **Fastly CDN/WAF: Service has received domain access error (Access events)**
- **Fastly CDN/WAF: High severity URL**
- **Fastly CDN/WAF: HTTP violation attack**
- **Fastly CDN/WAF: Local file inclusion (LFI) attack**
- **Fastly CDN/WAF: PHP injection attack**
- **Fastly CDN/WAF: Remote code execution (RCE) Attack**
- **Fastly CDN/WAF: Remote file inclusion (RFI) attack**
- **Fastly CDN/WAF: SQL injection threats**
- **Fastly WAF: URL blocked**

4.3 Flex Reports

- **Fastly CDN/WAF - Error events (Access events)**

LogTime	Computer	Fastly syslog IP	Client IP Address	Origin Host	Request Type	Origin-Host Status code	Device Type	Response	Fastly POP
12/18/2019 06:05:00 AM	199.27.77.34-SYSLOG	199.27.xxxx.xxx	193.171.xxx.xxx	envsecure.org	GET	503	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36	No healthy IP available for the backend	MXP
12/18/2019 06:05:00 AM	199.27.77.21-SYSLOG	199.27.xxx.xxx	193.171.xxx.xxx	envsecure.org	GET	503	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36	No healthy IP available for the backend	MXP
12/18/2019 05:35:55 PM	FASTLY-SYSLOG@NTPLDTBLR48	199.27.xxx.xxx	193.171.xxx.xxx	envsecure.org	GET	503	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36	No healthy IP available for the backend	MXP

Figure 8

- **Fastly CDN/WAF - Success events (Access events)**

LogTime	Computer	Fastly syslog IP	Fastly POP	Client IP Address	Origin Host	Device Type	Request Type	Origin-Host Status code	Number of hits	Response	Country Name	Syslog server Region
12/18/2019 02:30:00 AM	199.27.xxx.xxx-SYSLOG	199.27.xxx.xxx	AMS	182.74.xxx.xxx	www.connect-ag.in	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36	GET	302	1	Found	India	EU-Central
12/18/2019 02:30:00 AM	199.27.xxx.xxx-SYSLOG	199.27.xxx.xxx	AMS	182.74.xxx.xxx	www.connect-ag.in	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36	GET	302	1	Found	India	EU-Central

Figure 9

- **Fastly CDN/WAF - Login failure (Audit events)**

LogTime	Computer	Ip	Event Type	Description	User Id	Admin
12/17/2019 11:43:15 AM	FASTLY-INTERNAL@NTPLDxxxxxx	182.74.xxx.xxx	user.login_failure	Failed login attempt for Gary Poulter	1C3J8EO0tRzPwSPbxxxxxx	False
12/17/2019 11:47:05 AM	FASTLY-INTERNAL@NTPLDxxxxxx	182.74.xxx.xxx	user.login_failure	Failed login attempt for Maverick	1dMKtMqm5tqltzPnxxxxxx	False
12/17/2019 11:54:52 AM	FASTLY-INTERNAL@NTPLDxxxxxx	182.74.xxx.xxx	user.login_failure	Failed login attempt for Brenden	2KgFP87oaHUfMovJxxxxxx	False

Figure 10

- **Fastly CDN/WAF - Login success (Audit events)**

LogTime	Computer	Ip	Event Type	Description	User Id	Admin
12/17/2019 11:08:51 AM	FASTLY-INTERNAL@NTPLDxxxxx	182.74.xxx.xxx	token.create	API Token (manage.fastly.com browser session) has been created	1C3J8EO0tRzPwSPbxxxxxx	False
12/17/2019 11:47:23 AM	FASTLY-INTERNAL@NTPLDxxxxx	182.74.xxx.xxx	token.create	API Token (manage.fastly.com browser session) has been created	1dMKtMqm5tqltzPn1xxxxxx	False
12/17/2019 12:00:02 PM	FASTLY-INTERNAL@NTPLDxxxxx	182.74.xxx.xxx	token.create	API Token (manage.fastly.com browser session) has been created	2KgFP87oaHUfMovxxxxxx	False

Figure 11

- **Fastly CDN/WAF - User management (Audit events)**

LogTime	Computer	Ip	Event Type	Description	Name	Login	Role	User Id	Sudo Expiry	Admin
12/17/2019 11:42:08 AM	FASTLY-INTERNAL@NTPLDTxxxxxx	182.74.xxx.xxx	user.create	User '2KgFP87oaHUfMovxxxxxx' (peter.g@abc.com <peter.g@abc.com>) created	peter.g@abc.com	Mary.M@abc.com	user	1C3J8EO0tRzPwSPxxxxx		False
12/17/2019 04:19:21 PM	FASTLY-INTERNAL@NTPLDT	182.74.xxx.xxx	user.sudo	User '1dMKtMqm5tqltzPn1xxxxx' (Gary <Gary.p@abc.com>) sudoed	Gary	Gary.p@abc.com	user	1dMKtMqm5tqltzPn1xxxxx	2019-12-17 10:54:21 +0000	False
12/17/2019 11:43:09 AM	FASTLY-INTERNAL@NTPLDTxxxxxx	182.74.xxx.xxx	user.password_update	User Mary.M@abc.com password was updated						False

Figure 12

- **Fastly CDN/WAF - OWASP Threats**

LogTime	EventId	Computer	EventDescription	Address	WAF anamoly score	WAF block	WAF fixation score	WAF HTTP score	WAF LFI score	WAF message	WAF PHP score	WAF RCE score	WAF RFI score	WAF Severity	WAF sql score	WAF XSS score
1/30/2020 9:38:46 AM	3230	FASTLY-SYSLOG3@NTPLxxxxx	Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220	157.45.xxx.xxx	18	1	2	1	1	SQL Injection Attack Detected via libinjection	3	2	2	3	3	4
01/30/2020 09:38:46 AM	3230	FASTLY-SYSLOG3@NTPLxxxxx	Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220	182.74.xxx.xxx	18	0	2	1	1	Detects MSSQL code execution and information gathering	3	2	2	3	3	4
01/30/2020 09:38:46 AM	3230	FASTLY-	Dec 19 09:46:08 199.27.72.20 2019-12-	157.45.xx.xxx	18	0	2	1	1	Detects basic SQL	3	2	2	3	12	4

Figure 13

- **Fastly CDN/WAF - WAF States**

EventId	Computer	EventDescription	Client IP Address	TLS Client servername	WAF block	WAF message	WAF rule Id
3230	FASTLY-SYSLOG3@NTPLxxxxxxx	Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_ip" = "157.45.xx.xxx", "timestamp" = "Thu, 19 Dec 2019 15:46:07 GMT", "request" = "GET", "url" = "/",	157.45.xx.xxx	envsecure.org.global.prod.fastly.net	1	SQL Injection Attack Detected via libinjection	942100
3230	FASTLY-SYSLOG3@NTPLxxxxxxx	Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_ip" = "182.74.xxx.xxx", "timestamp" = "Thu, 19 Dec 2019 15:46:07 GMT", "request" = "GET", "url" = "/",	182.74.xxx.xxx	www.connect-ag.in.global.prod.fastly.net	0	Detects MSSQL code execution and information gathering attempts	942190
3230		Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_ip" = "157.45.xx.xxx", "timestamp" = "Thu, 19 Dec	157.45.xx.xxx	www.connect-ag.in.global.prod.fastly.net	0	Detects basic SQL authentication bypass attempts 1/3	942180

Figure 14

- **Fastly CDN/WAF - High severity URL's**

LogTime	EventId	Computer	EventDescription	Client IP Address	TLS Client servername	WAF block	WAF message	WAF rule Id	WAF Severity
01/30/2020 09:38:46 AM	3230	FASTLY-SYSLOG3@NTPLxxxxxxx	Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_ip" = "182.74.234.198", "timestamp" = "Thu, 19 Dec 2019 15:46:07 GMT", "request" = "GET", "url" = "/", "origin_host" = "www.connect-ag.in",	182.74.xx.xxx	www.connect-ag.in.global.prod.fastly.net	0	Possible payload execution and remote command execution	944120	3
01/30/2020 09:38:46 AM	3230	FASTLY-SYSLOG3@NTPLxxxxxxx	Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_ip" = "157.45.52.255", "timestamp" = "Thu, 19 Dec 2019 15:46:07 GMT", "request" = "GET", "url" = "/", "origin_host" = "www.connect-ag.in"	157.45.xx.xxx	envsecure.org.global.prod.fastly.net	0	XSS using obfuscated Javascript	941210	3
01/30/2020 09:38:46 AM	3230		Dec 19 09:46:08 199.27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_ip" = "182.74.234.198", "timestamp" = "Thu, 19	182.74.xxx.xxx	www.connect-ag.in.global.prod.fastly.net	1	URL Encoding Abuse Attack Attempt	920220	3

Figure 15

- **Fastly CDN/WAF – Blocked URL's**

LogTime	EventId	Computer	EventDescription	Client IP Address	Origin Host	TLS Client servername	WAF block
01/30/2020 09:20:47 AM	3230	FASTLY-SYSLOG3@NTPLXXXXXXX	Dec 18 02:30:57 199.27.77.23 2019-12-18T08:30:56Z cache-ams21029 EventTrackerSyslogEndpoint[399201]: "client_ip" = "182.74.234.198", "timestamp" = "Wed, 18 Dec 2019 08:30:56 GMT", "request" = "GET", "url" = "/", "origin_host" = "www.connect-ag.in",	182.74.xxx.xxx	www.connect-ag.in	www.connect-ag.in.global.prod.fastly.net	1
01/30/2020 09:20:47 AM	3230	FASTLY-SYSLOG3@NTPLXXXXXXX	Jan 16 03:37:55 199.27.77.21 2020-01-16T09:37:54Z cache-ams21042 EventTrackerSyslogVCP[284910]: "client_ip" = "182.74.234.198", "timestamp" = "Thu, 16 Jan 2020 09:37:53 GMT", "request" = "GET", "url" = "/", "origin_host" = "www.connect-ag.in", "tls_client_servername" = "www.connect-	182.74.xxx.xxx	www.connect-ag.in	www.connect-ag.in.global.prod.fastly.net	1
01/30/2020 09:20:47 AM	3230		Dec 24 00:00:40 199.27.77.44 2019-12-24T06:00:39Z cache-ams21050 EventTrackerSyslogEndpoint[70092]: "client_ip" = "182.74.234.198", "timestamp" = "Tue, 24	182.74.xxx.xxx	www.connect-ag.in	www.connect-ag.in.global.prod.fastly.net	1

Figure 16

4.4 Dashboards

- **Fastly CDN/WAF - Access events by user agent**

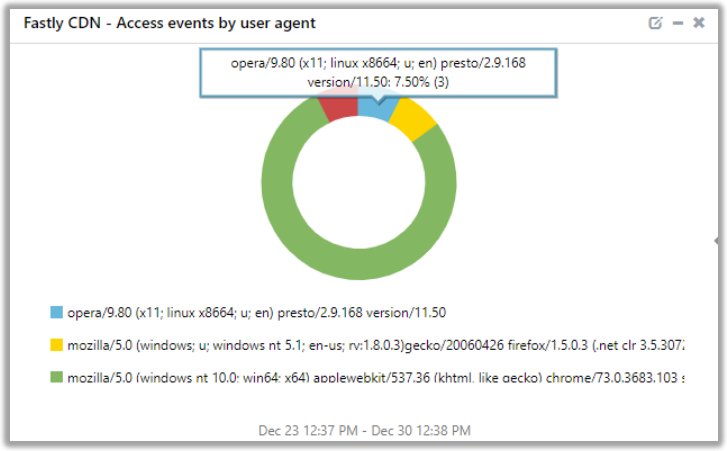


Figure 17

- **Fastly CDN/WAF - Access log by Fastly POP**

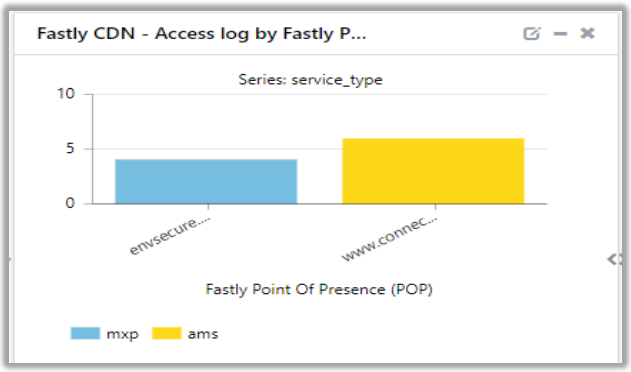


Figure 18

- **Fastly CDN/WAF - Access log by response code**

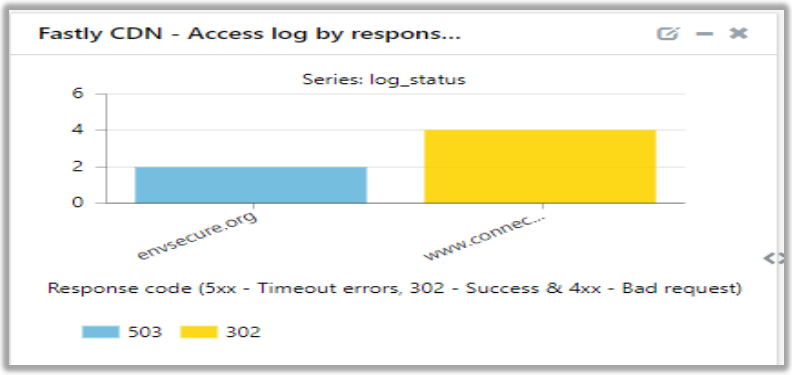


Figure 19

- **Fastly CDN/WAF - Access log by source IP**

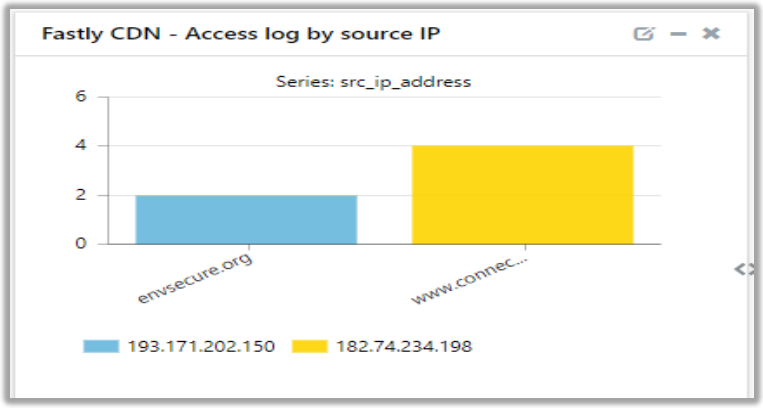


Figure 20

- **Fastly CDN/WAF - Access log by Country (Map)**

Figure 21

- **Fastly CDN/WAF - Access log by Country**

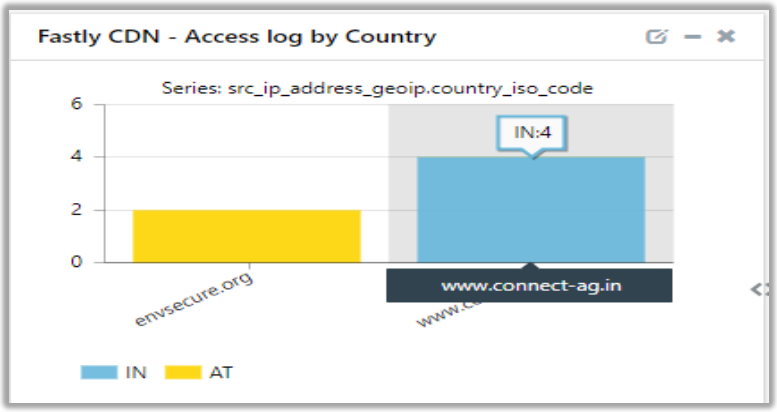


Figure 22

- **Fastly CDN/WAF - User login fail (Audit events by region)**

Figure 23

- **Fastly CDN/WAF - Audit Activities**

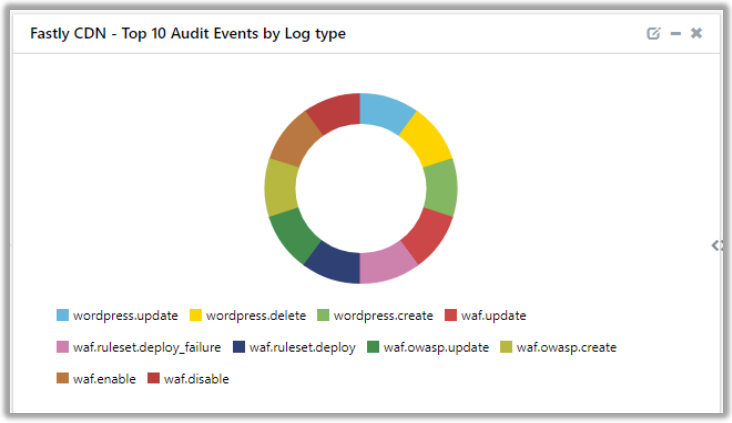


Figure 24

- **Fastly CDN/WAF - User login success (Audit events by IP address)**

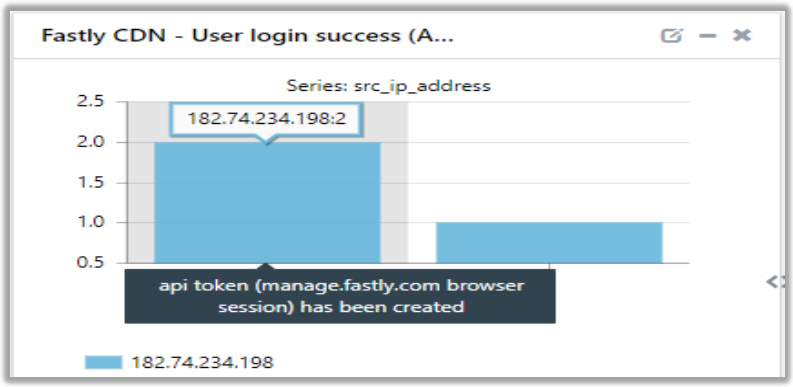


Figure 25

- **Fastly CDN/WAF - User login fail (Audit events by User ID/Email)**

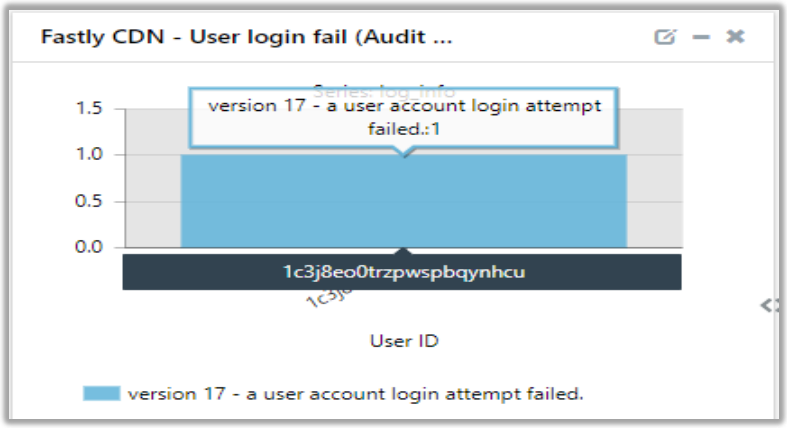


Figure 26

- **Fastly CDN/WAF - service version changes (Audit events)**

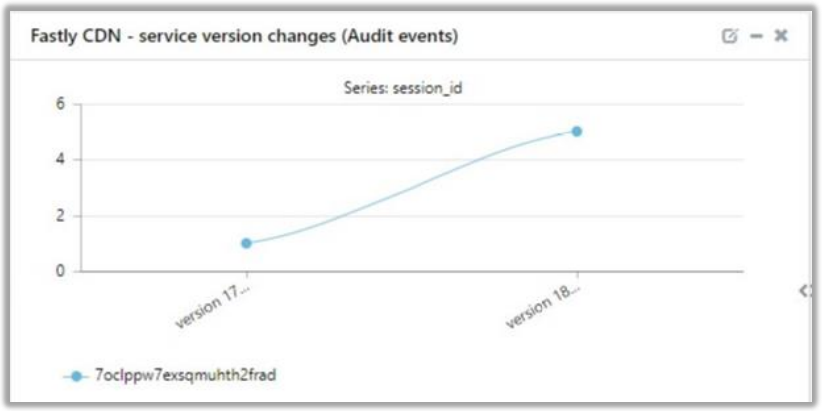


Figure 27

- **Fastly CDN/WAF - High severity URLs**

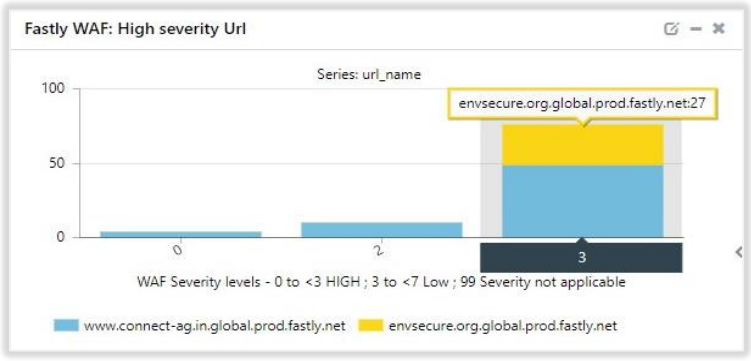


Figure 28

- **Fastly CDN/WAF – Blocked Requests**

Figure 29

- **Fastly CDN/WAF – Rule Matched by Generic Condition**

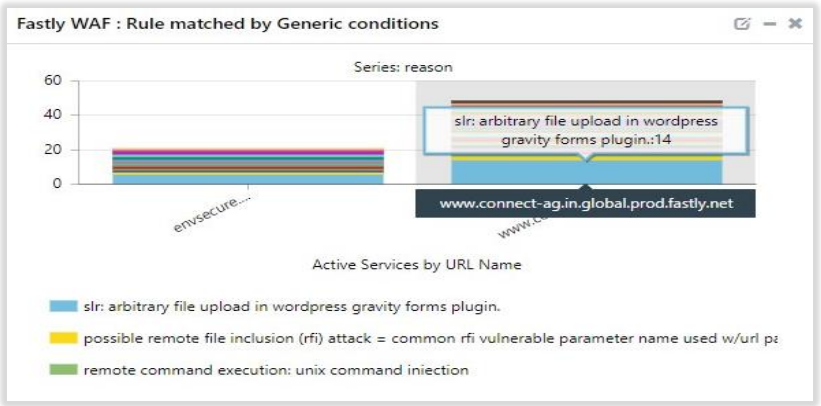


Figure 30

- **Fastly CDN/WAF - SQL Injections**

Figure 31

- **Fastly CDN/WAF - PHP Injections**

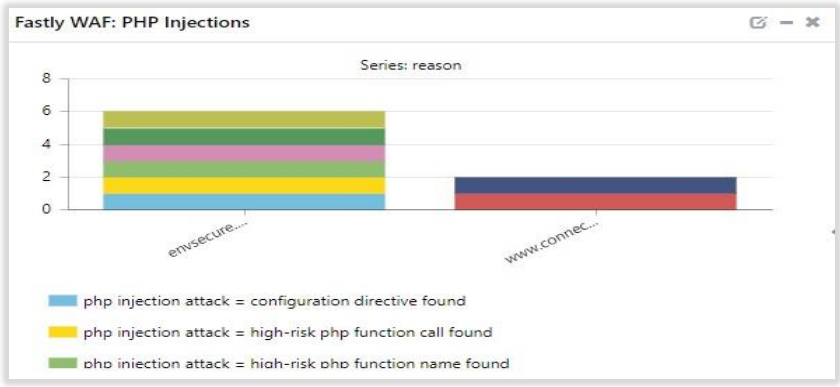


Figure 32

- **Fastly CDN/WAF – Application attack XSS**

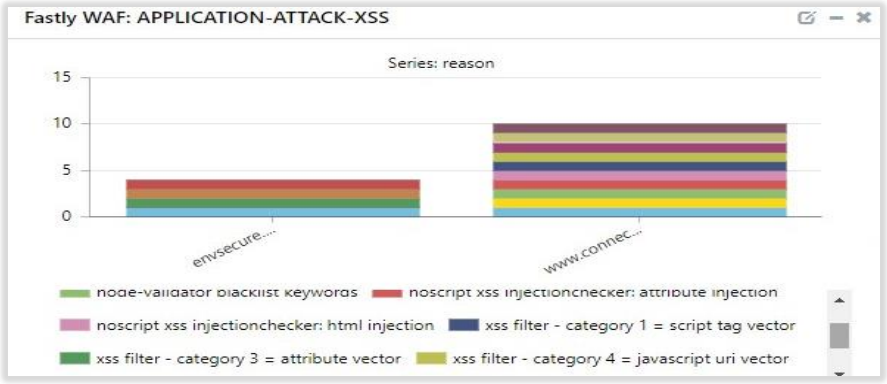


Figure 33

- **Fastly CDN/WAF – Application attack Session fixation**

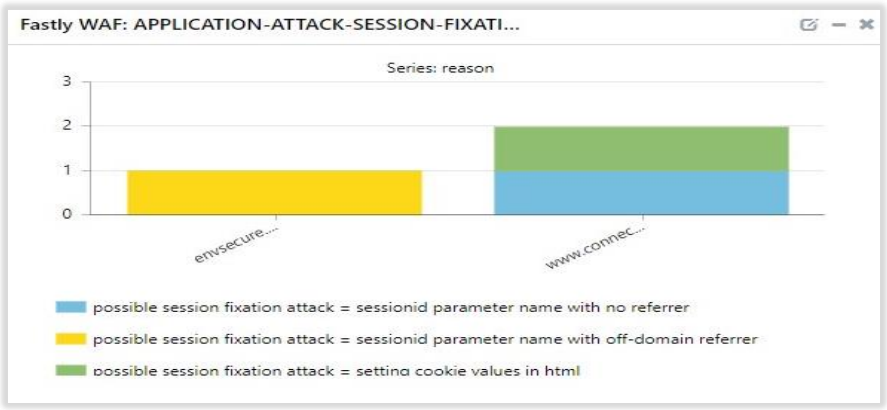


Figure 34

- **Fastly CDN/WAF – Application attack RCE (Remote code execution)**

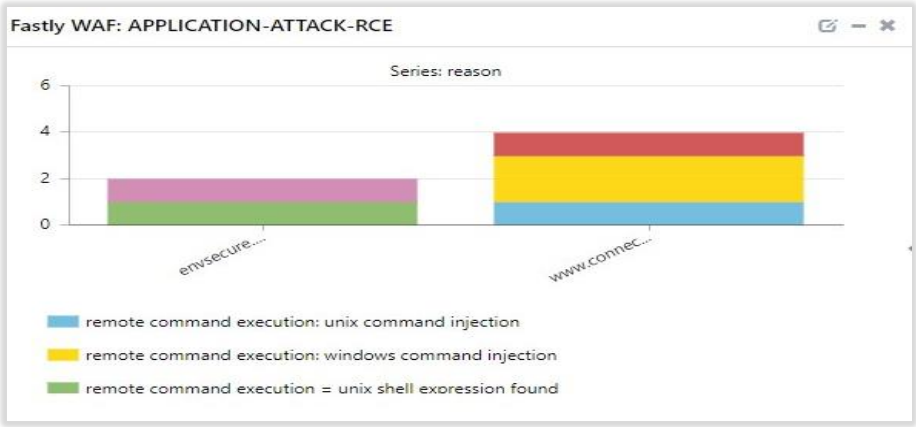


Figure 35

- **Fastly CDN/WAF – Application attack RFI (Remote file inclusion)**

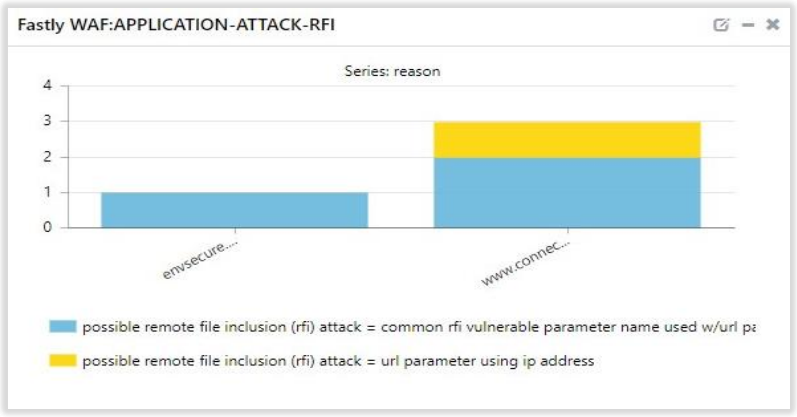


Figure 36

- **Fastly CDN/WAF – Application attack LFI (Local file inclusion)**

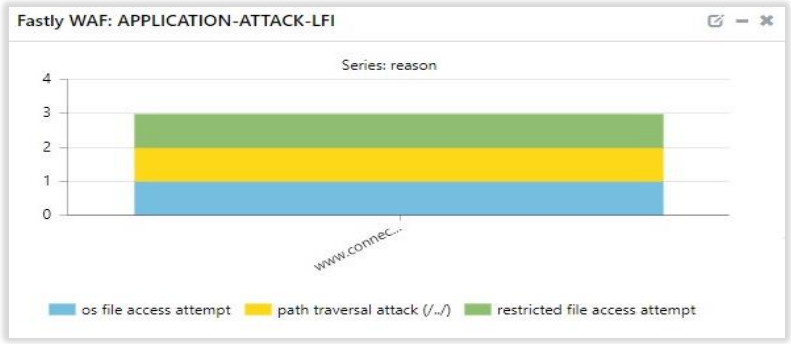


Figure 37

- **Fastly CDN/WAF – Protocol attack**

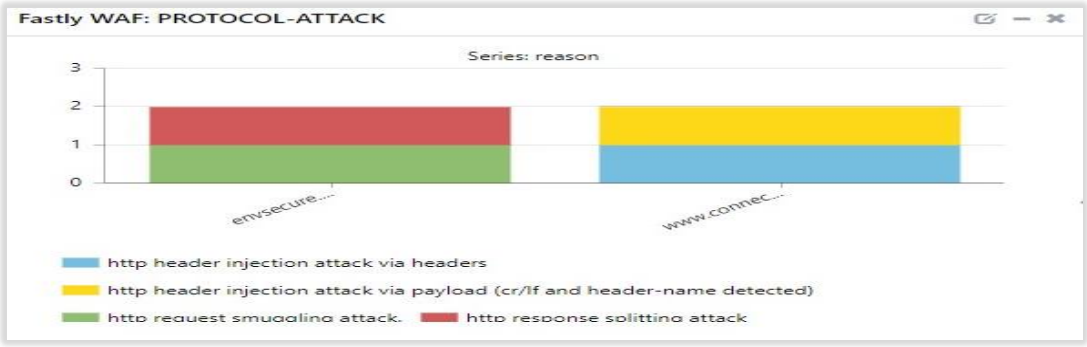


Figure 38

- **Fastly CDN/WAF – Protocol enforcement**

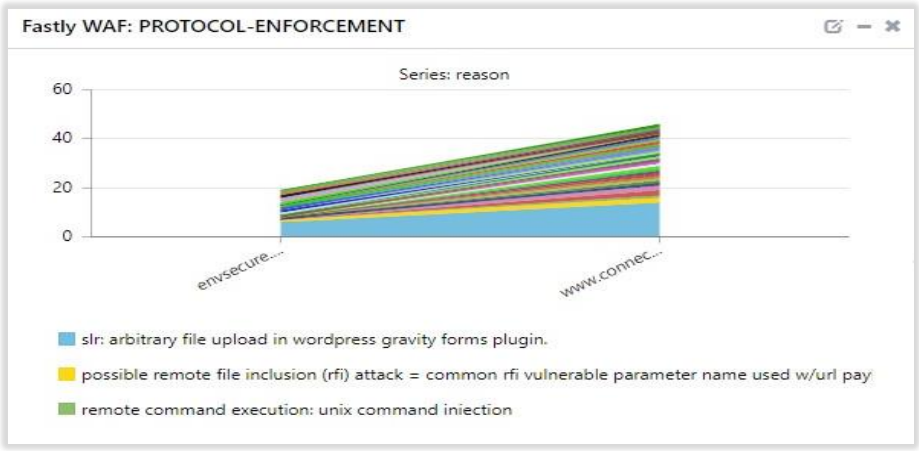


Figure 39

- **Fastly CDN/WAF – Application attack session JAVA**

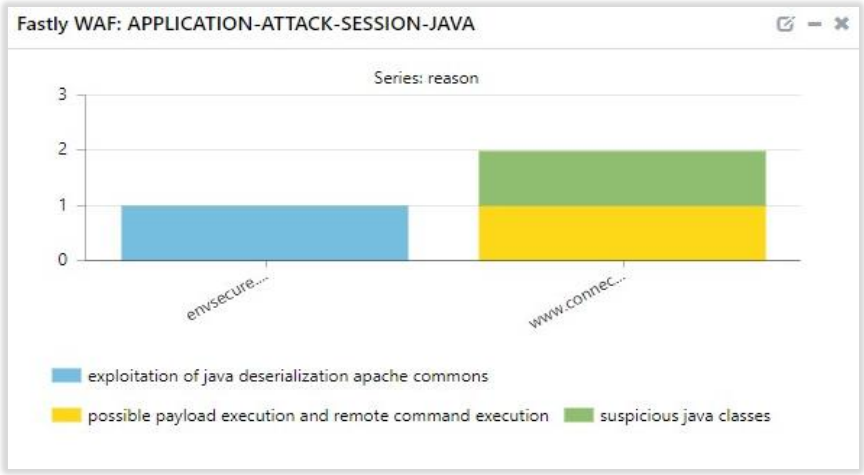
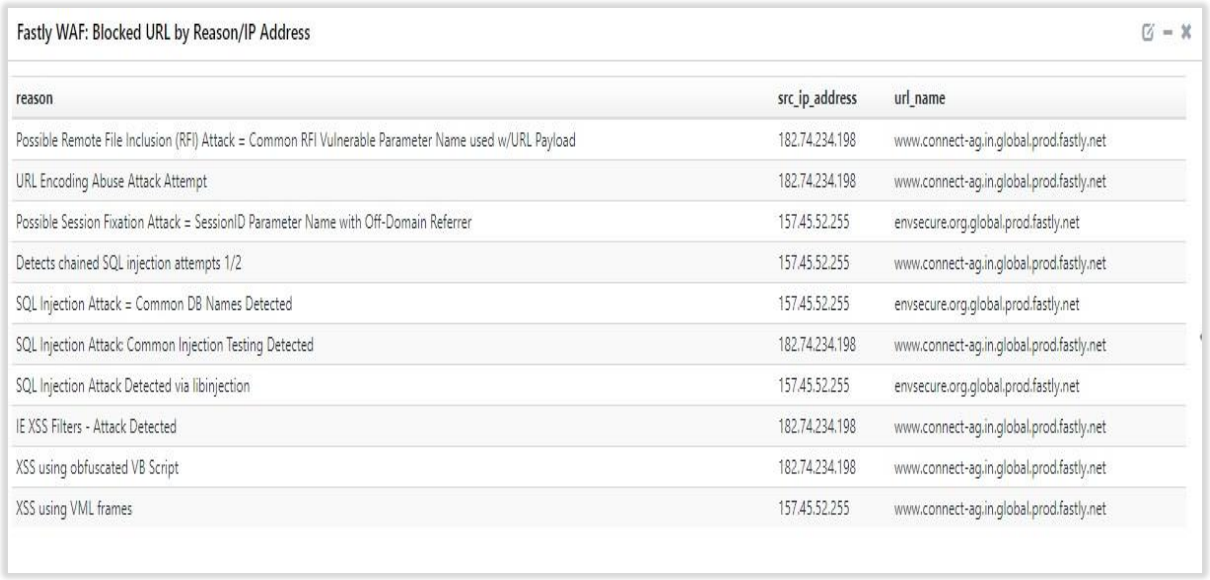


Figure 40

- **Fastly CDN/WAF – Blocked URL by reason/IP address**



Fastly WAF: Blocked URL by Reason/IP Address

reason	src_ip_address	url_name
Possible Remote File Inclusion (RFI) Attack = Common RFI Vulnerable Parameter Name used w/URL Payload	182.74.234.198	www.connect-ag.in.global.prod.fastly.net
URL Encoding Abuse Attack Attempt	182.74.234.198	www.connect-ag.in.global.prod.fastly.net
Possible Session Fixation Attack = SessionID Parameter Name with Off-Domain Referrer	157.45.52.255	envsecure.org.global.prod.fastly.net
Detects chained SQL injection attempts 1/2	157.45.52.255	www.connect-ag.in.global.prod.fastly.net
SQL Injection Attack = Common DB Names Detected	157.45.52.255	envsecure.org.global.prod.fastly.net
SQL Injection Attack: Common Injection Testing Detected	182.74.234.198	www.connect-ag.in.global.prod.fastly.net
SQL Injection Attack Detected via libinjection	157.45.52.255	envsecure.org.global.prod.fastly.net
IE XSS Filters - Attack Detected	182.74.234.198	www.connect-ag.in.global.prod.fastly.net
XSS using obfuscated VB Script	182.74.234.198	www.connect-ag.in.global.prod.fastly.net
XSS using VML frames	157.45.52.255	www.connect-ag.in.global.prod.fastly.net

Figure 41

5. Importing knowledge pack into EventTracker

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

1. Press "⊞ + R".
2. Now, type **"%et_install_path%\Knowledge Packs**" and press "**Enter**".
   (**Note** – If, not able to locate the file path as mentioned above, please contact EventTracker support to get the assistance).

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.

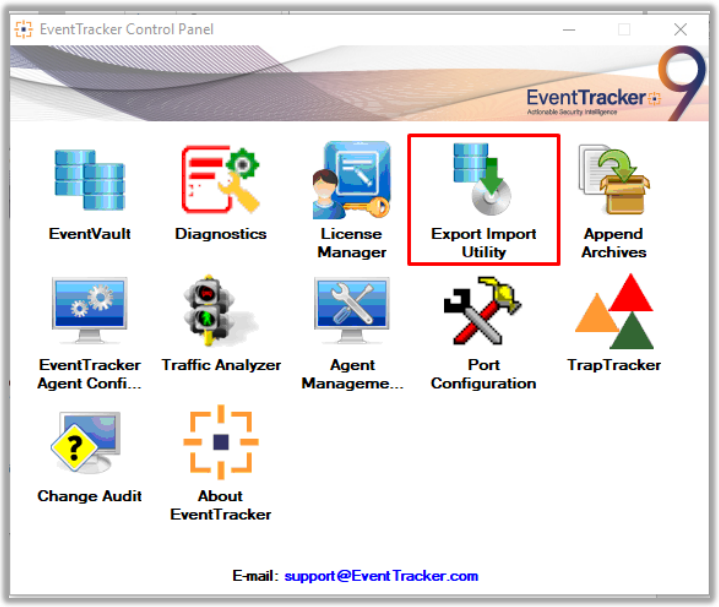


Figure 42

3. Click the **Import** tab.

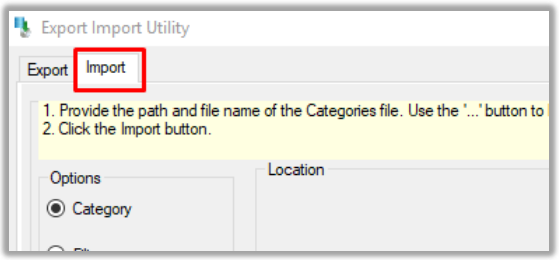


Figure 43

5.1 Categories

1. Once you have opened "**Export Import Utility**" via "**EventTracker Control Panel**", click the **Category** option, and then click Browse ... .
2. Navigate to the knowledge pack folder and select the file with extension **".iscat"**, and then click "**Import**".

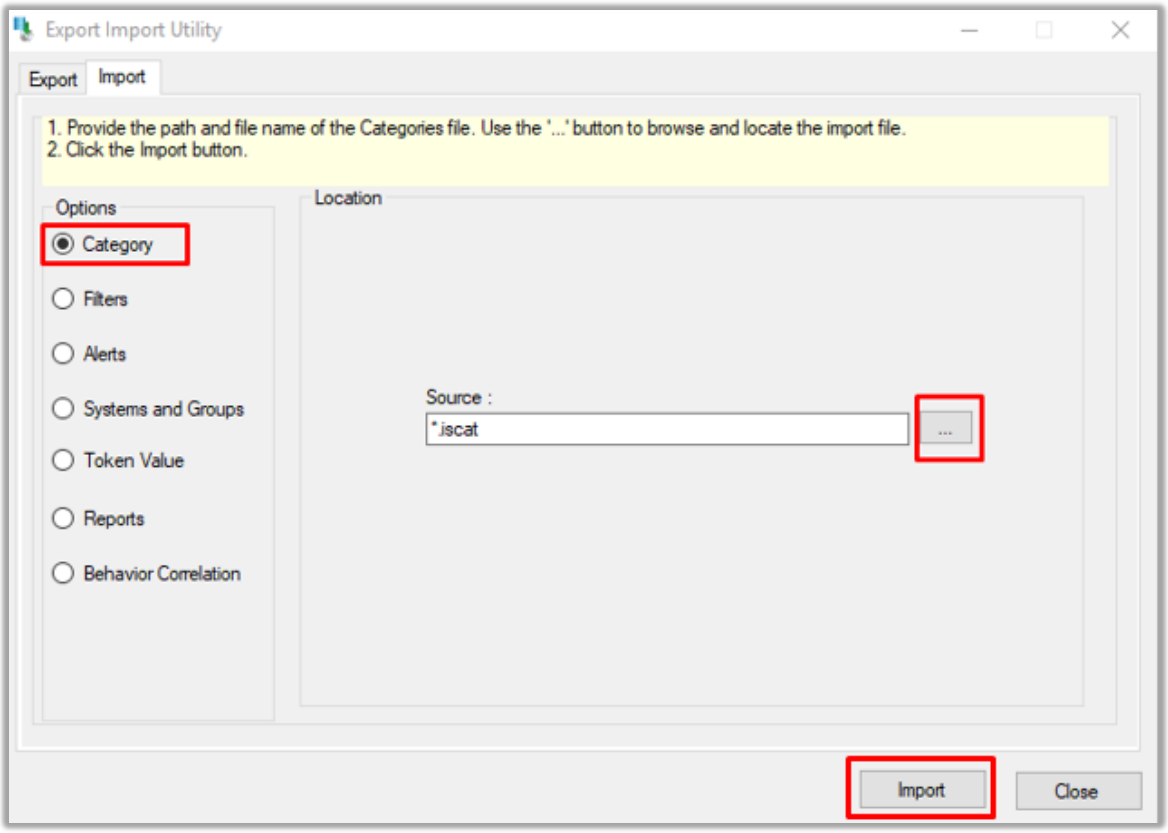


Figure 44

EventTracker displays a success message:

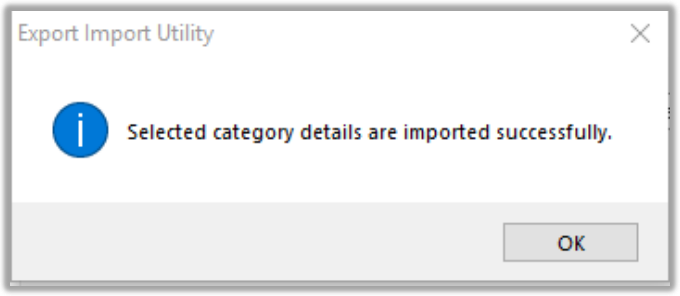


Figure 45

5.2 Alerts

1. Once you have opened "**Export Import Utility**" via "**EventTracker Control Panel**", click **Alert** option, and then click browse. ...
2. Navigate to the knowledge pack folder and select the file with extension **".isalt**", and then click "**Import**" button.

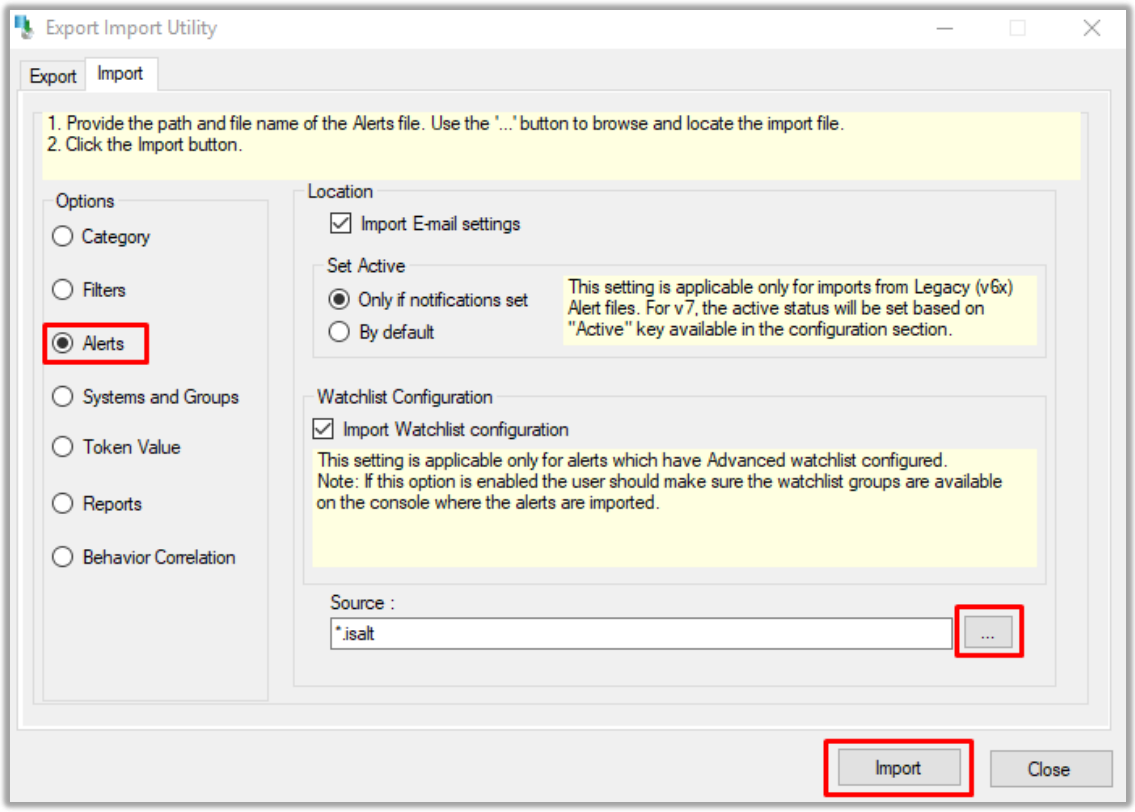


Figure 46

EventTracker displays a success message:

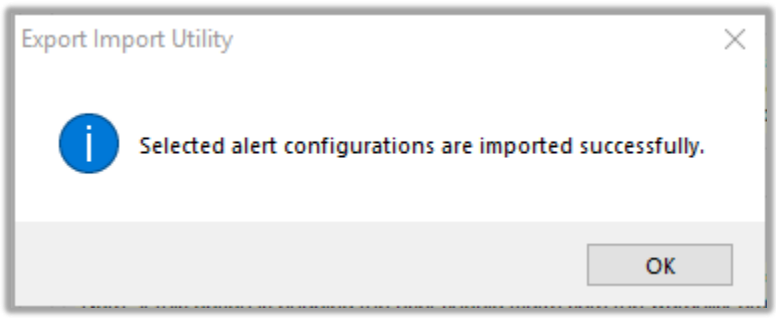


Figure 47

5.3 Parsing Rules

1. Once you have opened "**Export Import Utility**" via "**EventTracker Control Panel**", click the **"Token Value"** option, and then click browse ... button.

2. Navigate to the knowledge pack folder and select the file with extension **".istoken"** and then click "**Import**".

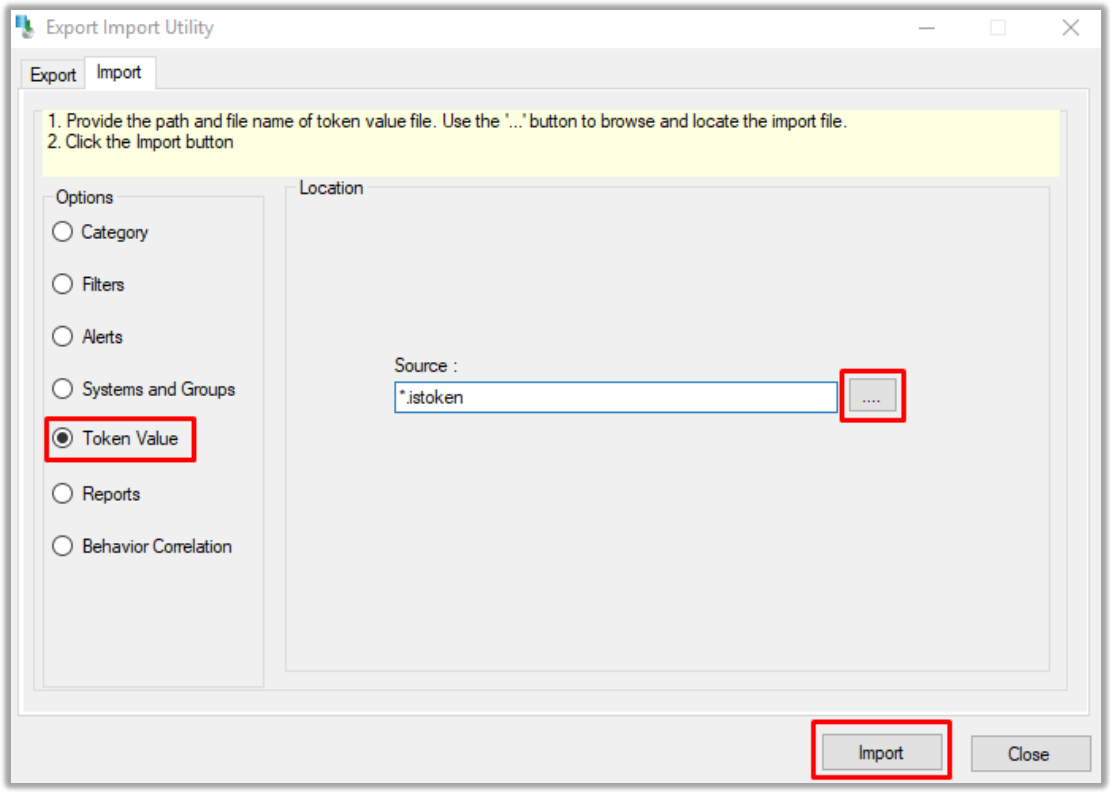


Figure 48

5.4 Token Template

For importing "**Token Template**", navigate to **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.

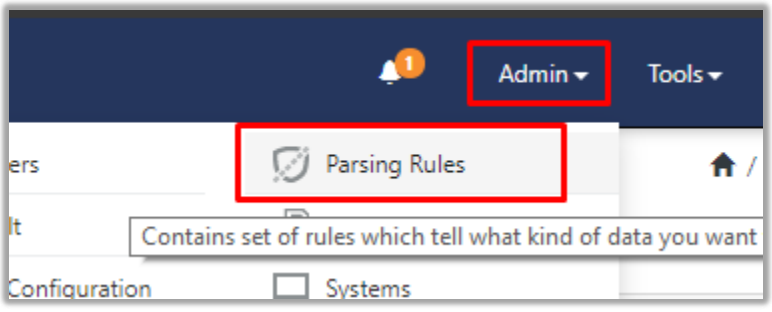


Figure 49

2. Next, click the "**Template**" tab and then click "**Import Configuration**".

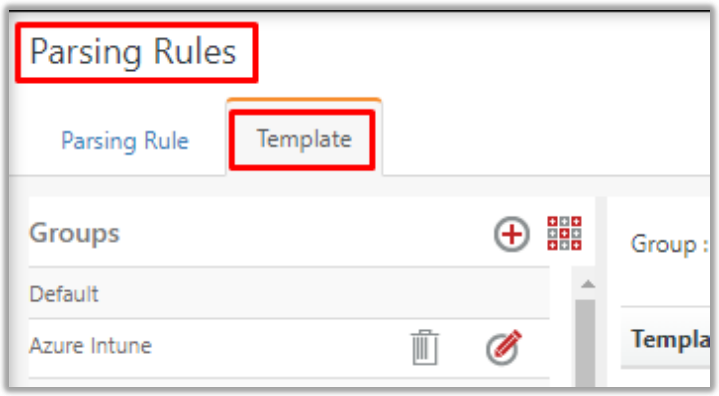


Figure 50

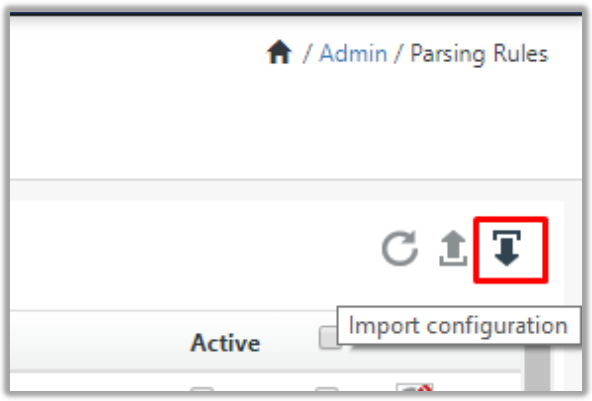


Figure 51

3. Now, click "**Browse**" and navigate to the knowledge packs folder (type **"%et_install_path%\Knowledge Packs**" in navigation bar) where **".ettd"** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click "**Import**".

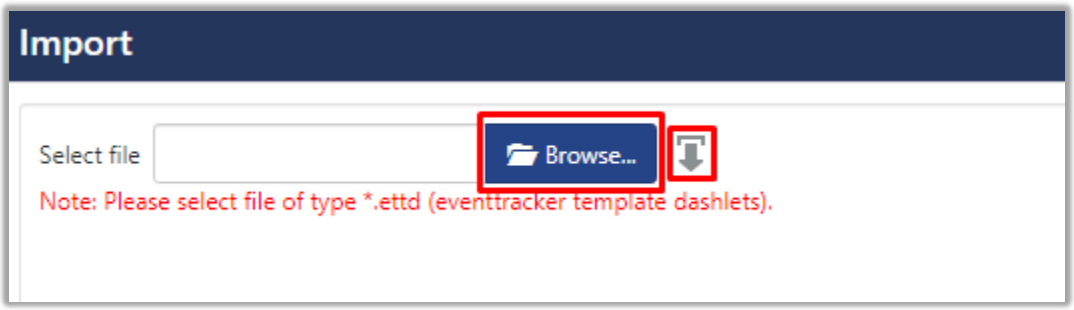


Figure 52

5.5 Flex Reports

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

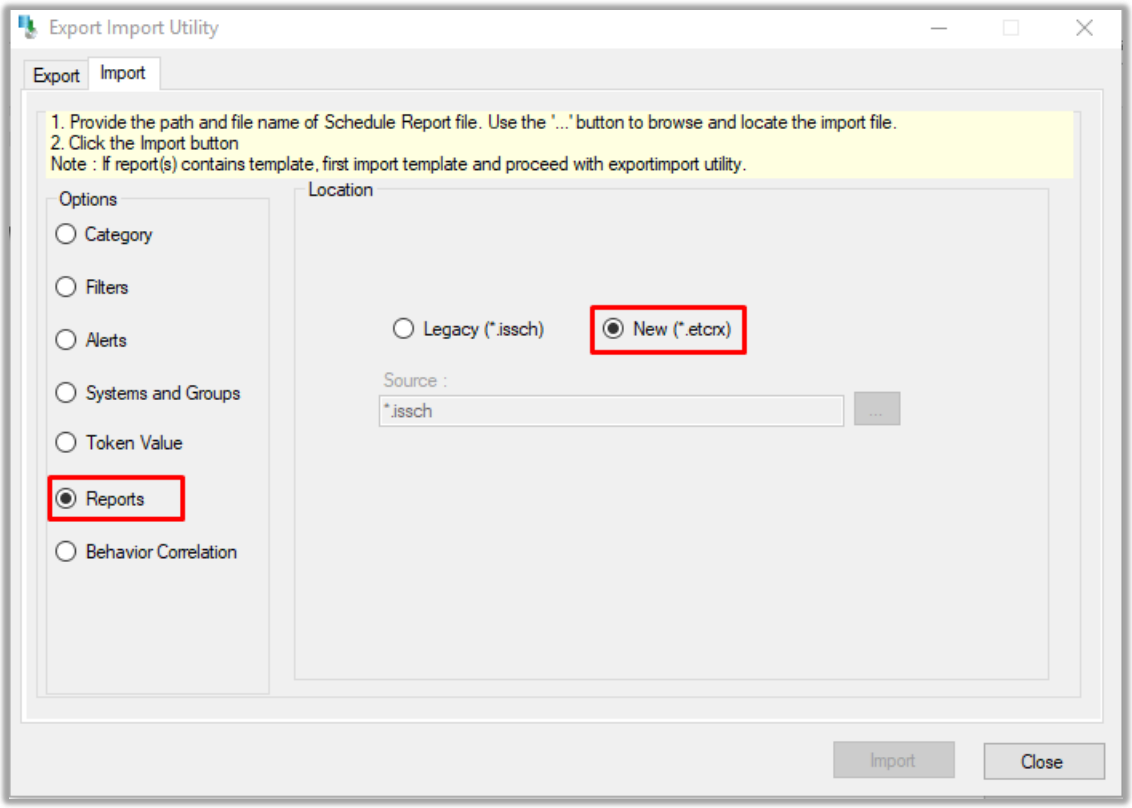


Figure 53

2. Once you have selected "**New (*.etcrx)**", a new pop-up window will appear. Click "**Select File**" and navigate to knowledge pack folder and select file with extension **".etcrx".**

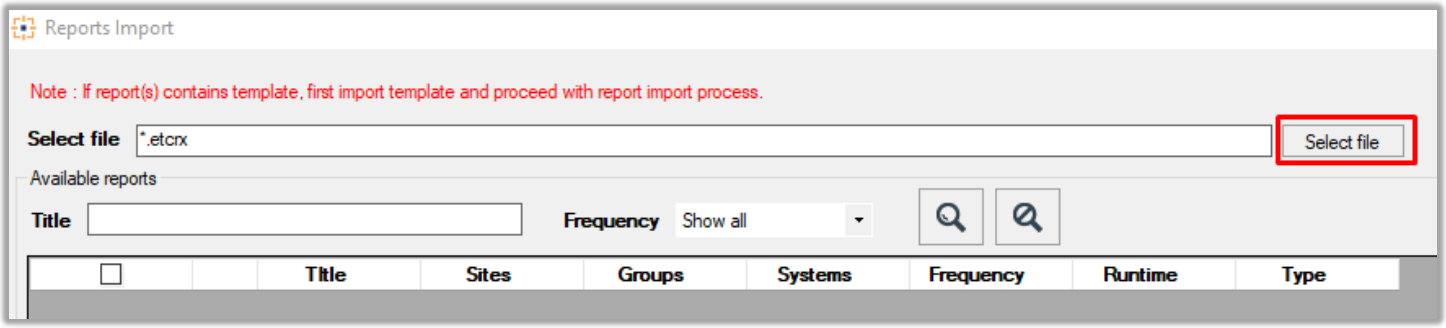


Figure 54

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

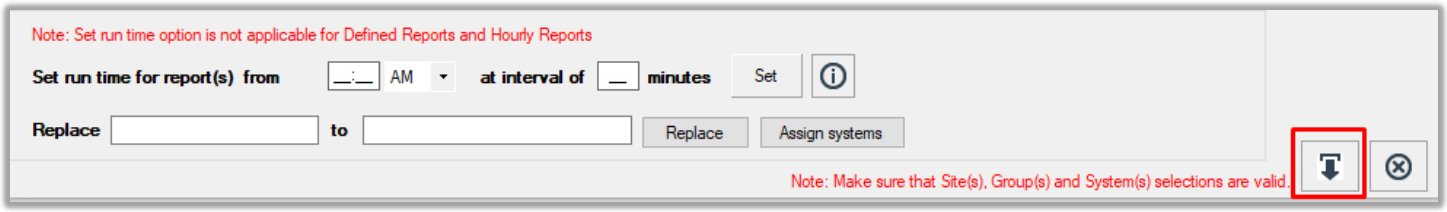


Figure 55

EventTracker displays a success message

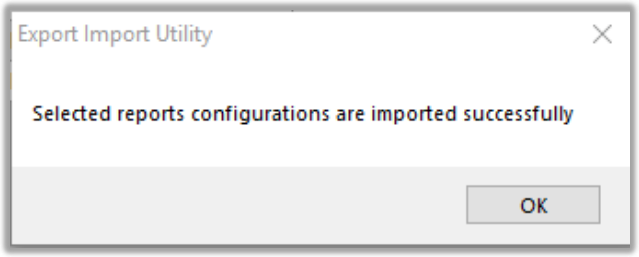


Figure 56

5.6 Knowledge Objects

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

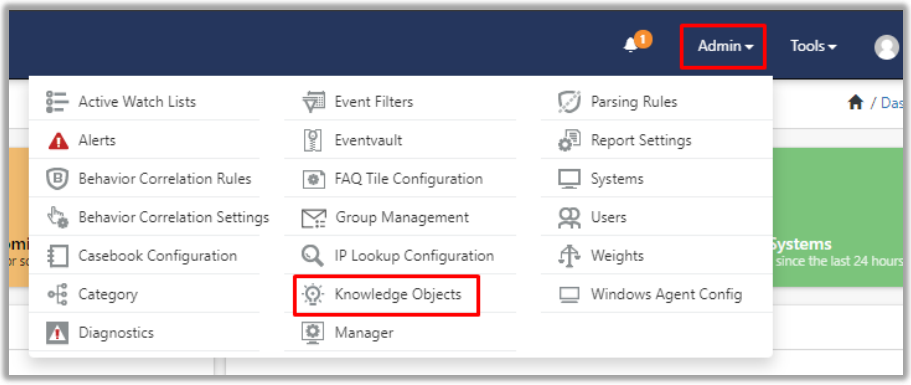


Figure 57

2. Next, click the **"import object"** icon.

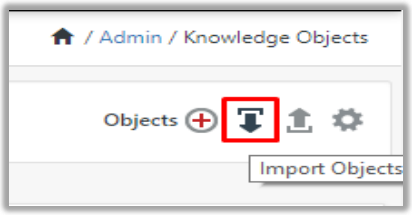


Figure 58

3. A pop-up box will appear, click "**Browse**" in that and navigate to knowledge packs folder (type **"%et_install_path%\Knowledge Packs**" in navigation bar) with the extension **".etko"** and then click "**Upload**".

Figure 59

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

Figure 60

5.7 Dashboards

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

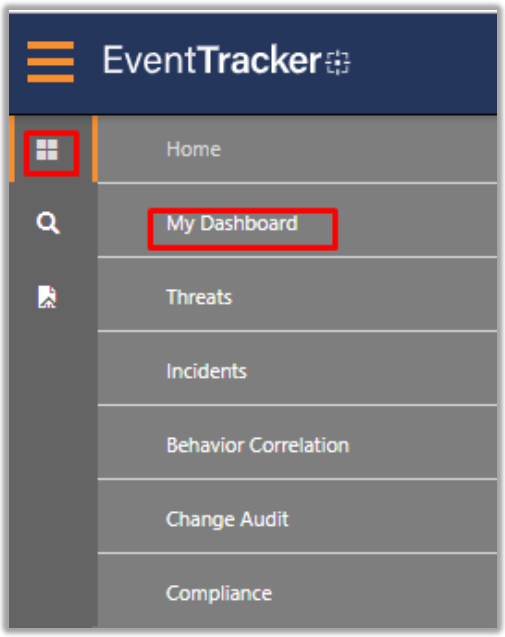


Figure 61

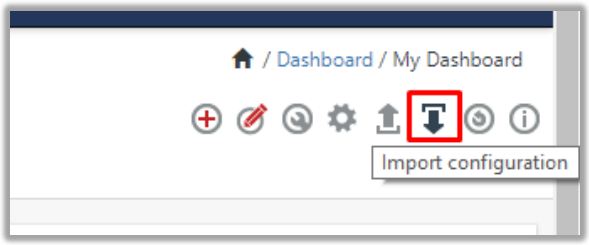


Figure 62

4. Select **Browse** and navigate to knowledge pack folder (type **"%et_install_path%\Knowledge Packs**" in navigation bar) where "**.etwd**" is saved and click "**Upload**".
5. Wait while EventTracker populates all the available dashboards. Now, choose "**Select All**" and click **"Import"**.

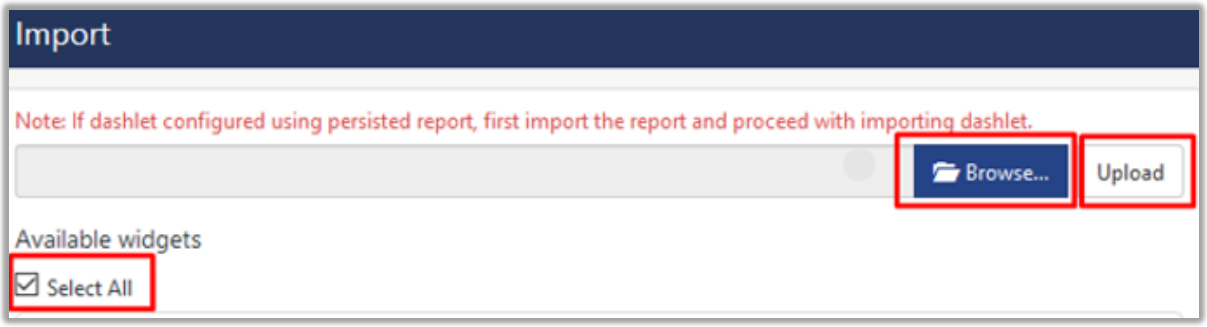


Figure 63

Figure 64

6. In **My Dashboard** page select ⊕ to add dashboard.

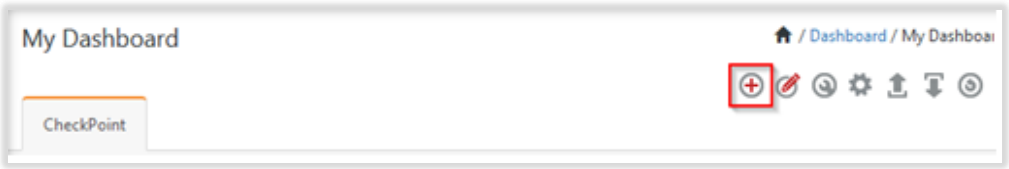


Figure 65

7. Choose appropriate name for **Title** and **Description**. Click **Save**.

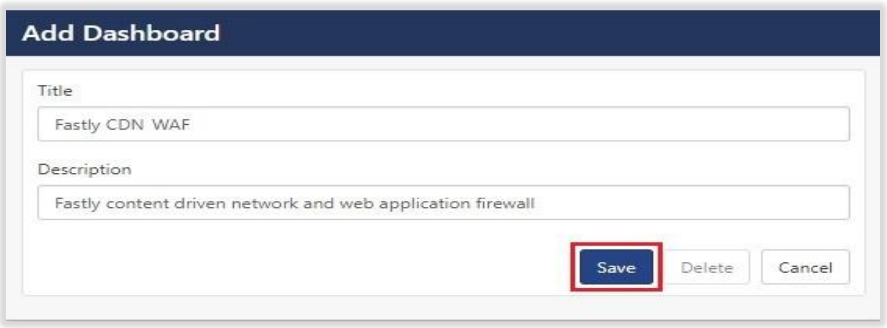


Figure 66

8. In **My Dashboard** page select ◎ to add dashlets.

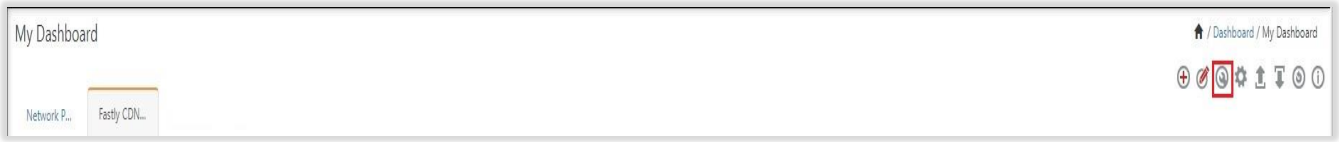


Figure 67

9. Select imported dashlets and click **Add**.

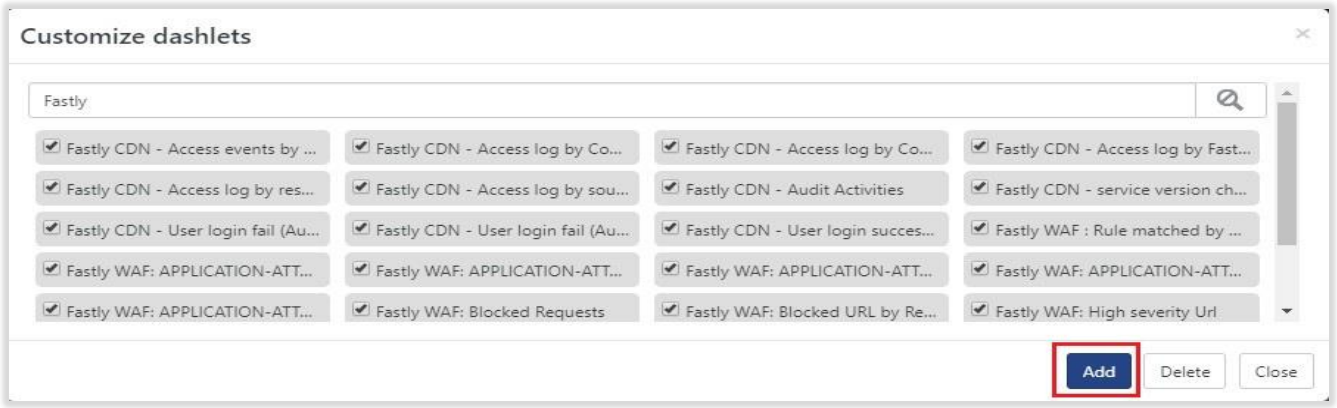


Figure 68

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to **EventTracker manager web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand "**Fastly CDN/WAF**" group folder to view the imported categories.

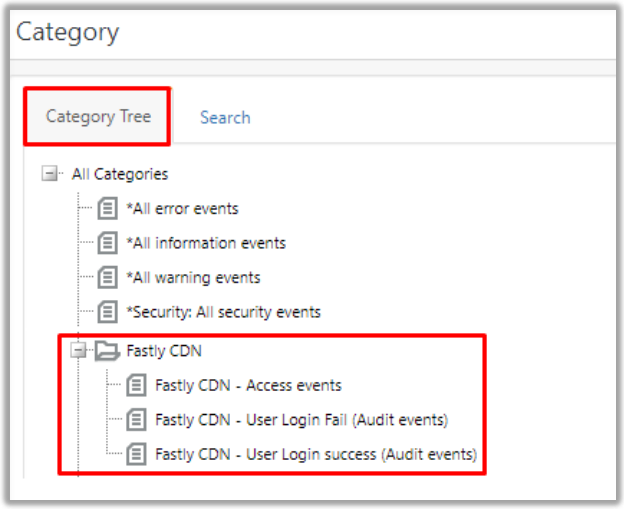


Figure 69

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. "Fastly"** and then click **Search**.

   EventTracker displays an alert related to **"Fastly CDN/WAF":**

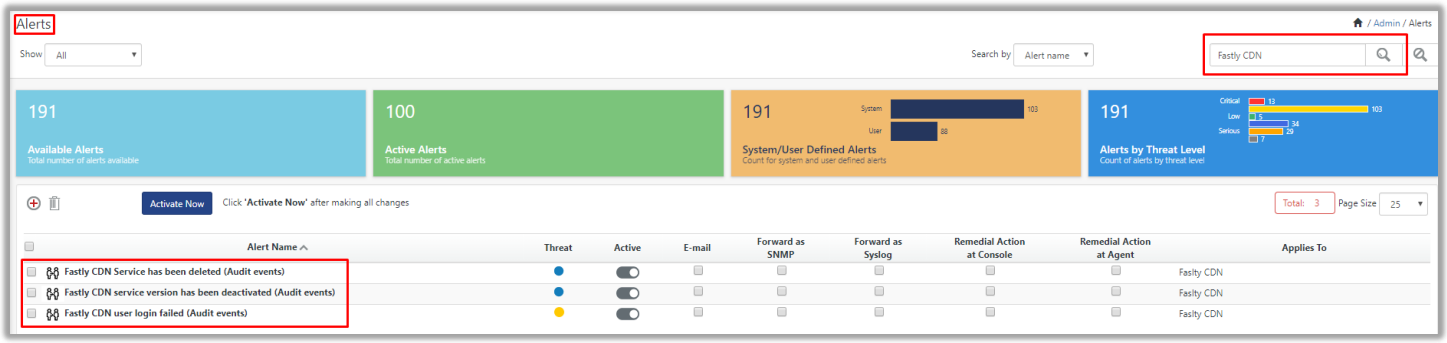


Figure 70

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 **"Fastly CDN/WAF"** group folder to view the imported Token Values.

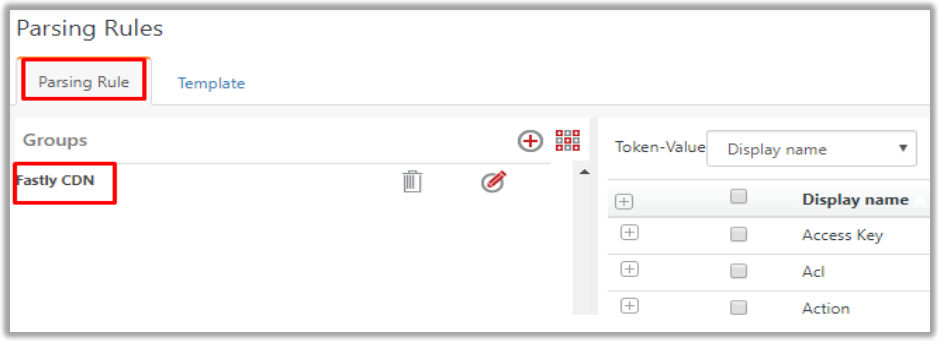


Figure 71

6.4 Token Template

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing Rules.**
2. In the **Template** tab, click on the "**Fastly CDN/WAF**" group folder to view the imported templates.

Figure 72

6.5 Flex Reports

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

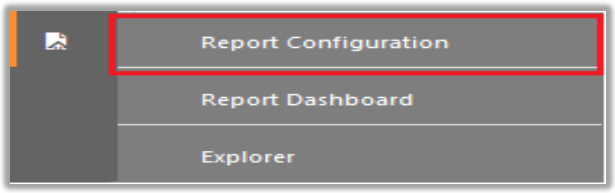


Figure 73

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the "**FASTLY CDN/WAF"** group folder to view the imported reports.

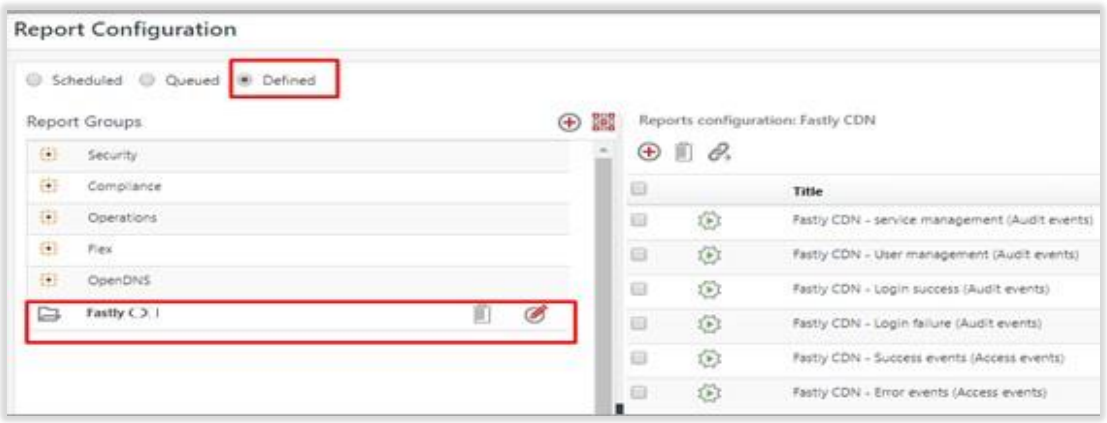


Figure 74

6.6 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 "**Fastly CDN/WAF**" group folder to view the imported Knowledge objects.

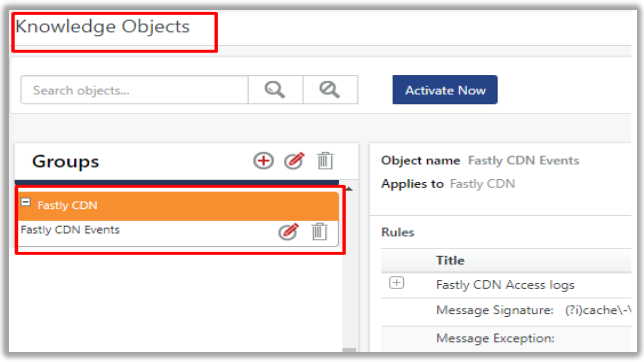


Figure 75

6.7 Dashboards

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

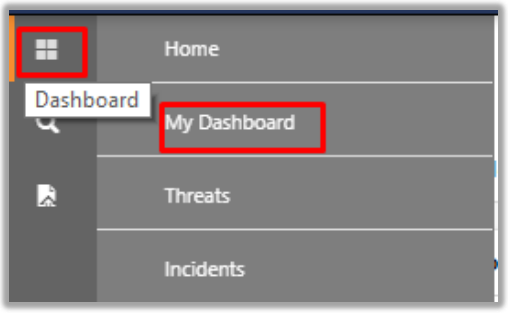


Figure 76

2. "**Fastly CDN/WAF**" dashboard opens.

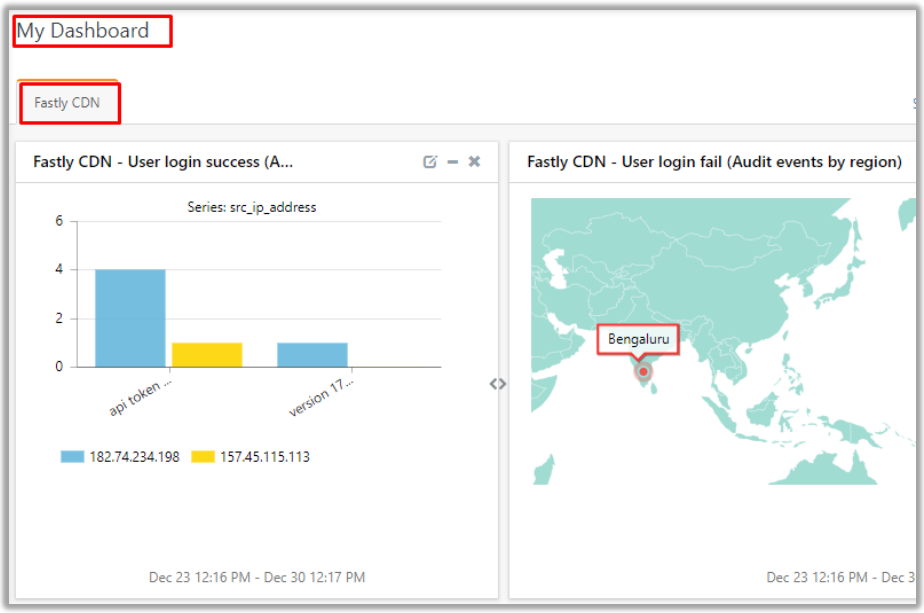

My Dashboard
Fastly CDN
Fastly CDN - User login success (A...
Series: src_ip_address
6
4
2
0
api token ...
version 17...
182.74.234.198
157.45.115.113
Dec 23 12:16 PM - Dec 30 12:17 PM
Fastly CDN - User login fail (Audit events by region)
Bengaluru
Dec 23 12:16 PM - Dec 3

Figure 77