

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.

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 of FastlyCDN/WAF 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

1.	Ove	erview
2.	Pre	requisites3
3.	Inte 3.1	egrating Fastly CDN/WAF with EventTracker
	3.2	Forwarding logs from "Fastly audit and syslog" 6
4.	Eve 4.1	ntTracker Knowledge Packs
	4.2	Alerts
	4.3	Flex Reports
	4.4	Dashboards
5.	Imp 5.1	oorting knowledge pack into EventTracker
	5.2	Alerts
	5.3	Parsing Rules
	5.4	Token Template
	5.5	Flex Reports
	5.6	Knowledge Objects
	5.7	Dashboards
6.	Ver 6.1	ifying knowledge pack in EventTracker
	6.2	Alerts
	6.3	Parsing Rules
	6.4	Token Template
	6.5	Flex Reports
	6.6	Knowledge Objects
	6.7	Dashboards

Netsurion... EventTracker*

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:





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.

	Create a Token	
Password		* Required
Name	EventTrackerAPI Describe what this token is going to be used for	* Required
Арріу to	All Services Aspecific service Limiting service access does not prevent access to non-service related capabilities	
Set a scope	 Global API access (global) — Full control over service, purging and account Purge full cache (pur ge_all) — Purge all assets in cache Purge select content (pur ge_select) — Purge by URL or surrogate key Read-only access (global:read) — Read account information, configuration and stats Scopes can be used to limit a token's access 	
Set a token expiration	Never expire Set expiration date	
	CREATE	



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







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"

Fastly CDN Integrator		
АРІКеу	•••••	
Validate	Submit	Cancel

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".

APIKey	*****	•••••
Active Service	Name/Version	Syslog IP Address
✓ (Service_Name ✓ (Service_Name)	- "My_Service") (Versio - "Production_ESX01") (n - " 198.17,500,5000 Vers Syslog Endpoint Name Event Tracker Syslog VCP Currles Back
<		> 514



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

Fastly CDN Integrator	>	$\langle $
APIKey	*****	
Active Service N	smal/Varrian Quala a ID Address	- 1
(Se (Se	Fastly CDN Integration configured successfully	
<	ОК	
Validate	Submit Cancel	



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 AI	1 199.27.77.34-SYSLOG	199.27.3000.300	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	МХР
12/18/2019 06:05:00 AI	1 199.27.77.21-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 Pi	FASTLY- SYSLOG@NTPLDTBL R48	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	lp	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	2KgFP87oaHUfMovJxxxxx	False

Figure 10

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

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

Figure 11

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

LogTime	Computer	lp	Event Type	Description	Name	Login	Role	User Id	Sudo Expiry	Admin
12/17/2019 11:42:08 AM	FASTLY-	182.74.xxx.xxx	user.create	User	peter.g@abc.com	Mary.M@abc.com	user	1C3J8EO0tRzPwSPxxxxx		False
	INTERNAL@NTPLDTxxxxxxx			'2KgFP87oaHUfMovxxxx						
				xx' (peter.g@abc.com						
				<peter.g@abc.com>)</peter.g@abc.com>						
				created						
12/17/2019 04:19:21 PM	FASTLY-INTERNAL@NTPLD	182.74.xxx.xxx	user.sudo	User	Gary	Gary.p@abc.com	user	1dMKtMqm5tqltzPn1xxxxx	2019-12-17 10:54:21 +0000	False
				'1dMKtMqm5tqltzPn1xxx						
				xx' (Gary						
				<gary.p@abc.com>)</gary.p@abc.com>						
				sudoed						
12/17/2019 11:43:09 AM	FASTLY-	182.74.xxx.xxx	user.password_	User Mary.M@abc.com						False
	INTERNAL@NTPLDTxxxxxxx		update	password was updated						

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@NTPLx xxxxx	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@NTPLx xxxxx	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	157.45.xx.xxx	18	Ó	2	1	1	Detects basic	3	2	2	3	12	4

Netsurion... EventTracker*

Figure 13

• Fastly CDN/WAF - WAF States

EventId	Computer	EventDescription	Client IP Address	TLS Client servername	WAF block	WAF message	WAF rule ld
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 xxxe", "timestamp" = "Thu, 19 Dec 2019 15:46:07 GMT", "request" = "GET", "ut" = "I",	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", "urt" = "/",	182.74.xxx.xxx	www.connect- ag.in.global.prod.fastly.net	6	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	δ	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[159Z74] "client_jp" = "182.74.234.198", "timestamp" = "Thu, 19 Dec 2019 15:46:07 GHT", "request" = "OET", "url" = "/, "origin_host" = "www.connect-ag.in",	182.74.30x300x	www.connect- ag.in.global.prod.fastly.net	6	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_p" = "157.45.52 255, "timestamp" = "Thu, 19 Dec 2019 15:46:07 GMT", "request" = "GET", "urf" = "/", "finish host" = "www.connect-an in".	157.45.xx.xxx	envsecure.org.global.prod.fastly.n et	6	XSS using obfuscated Javascript	941210	3
01/30/2020 09:38:46 AM	3230	PAGTIN	Dec 19 09:46:08 199:27.72.20 2019-12-19T15:46:07Z cache-bom18220 EventTrackerSyslogEndpoint[159274]: "client_jp" = "182.74.234.198", "timestamp" = "Thu, 19	182.74.xxxxxxxx	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_jp" = "182,74,234.198", "timestamp" = "Wed, 18 Dec 2019 08:30:56 GMT", "request = "GET", "urf" = "/", "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@NTPLXXXXXX	Jan 16 03:37:55 199.27.77.21 2020-01-16T09:37.54Z cache-ams21042 EventTrackerSyslogVCP[264910] "Client" jor ""1827.2324 199", "muestamp" = Thu, 16 Jan 2020.09:37:53 GMT", "request" = "GET", "urf" = "/", "origin_host" = "www.connect-ag.in", "be: client caremana" = "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

Netsurion... EventTracker*

4.4 Dashboards



• Fastly CDN/WAF - Access events by user agent



• Fastly CDN/WAF - Access log by Fastly POP





• Fastly CDN/WAF - Access log by response code





Figure 19



• Fastly CDN/WAF - Access log by source IP



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





• Fastly CDN/WAF - Access log by Country



Netsurion EventTracker*





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



• Fastly CDN/WAF - Audit Activities





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







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





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





Netsurion. EventTracker*

• Fastly CDN/WAF - High severity URLs





• Fastly CDN/WAF – Blocked Requests





• Fastly CDN/WAF – Rule Matched by Generic Condition



Figure 30



• Fastly CDN/WAF - SQL Injections





• Fastly CDN/WAF - PHP Injections





Fastly CDN/WAF – Application attack XSS



Figure 33





• Fastly CDN/WAF – Application attack Session fixation



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





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







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



Figure 37

• Fastly CDN/WAF – Protocol attack





Fastly CDN/WAF – Protocol enforcement







• Fastly CDN/WAF – Application attack session JAVA





• Fastly CDN/WAF – Blocked URL by reason/IP address



Fastly WAF: Blocked URL by Reason/IP Address			© - X
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 D8 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 <u>EventTracker support</u> 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.



문 EventTracker Con	trol Panel		Fv	- X
EventVault	Diagnostics	License	Export Import	Append
C ient Tooker		Manager		Archives
Agent Confi		Agent Manageme	Port Configuration	i rap i racker
Change Audit	About EventTracker E-mail: s	support@EventTra	acker.com	

Figure 42

3. Click the Import tab.

💺 Export Import Utility						
Export Import						
1. Provide the path and file r 2. Click the Import button.	I. Provide the path and file name of the Categories file. Use the '' button to Click the Import button.					
Options	Location					
Category						
0.5%						



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".

🐁 Export Import Utility				_		\times
Export Import						
1. Provide the path an 2. Click the Import butt	d file name of the Catego on.	ries file. Use the '' button t	o browse and locate the im	port file.		
Options Category Filters Alerts Systems and Grou Token Value Reports Behavior Correlation	ps	Source : *iscat				
				Import	Close	•

Figure 44

EventTracker displays a success message:





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.



Export Import Utility		— D >
Export Import		
1. Provide the path and file na 2. Click the Import button.	ame of the Alerts file. Use the '' but	ton to browse and locate the import file.
Options	Location	
Category	Import E-mail settings	
	Set Active	
○ Filters	 Only if notifications set 	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7 the active status will be set based on
Alerts	O By default	"Active" key available in the configuration section.
O Systems and Groups	Watchlist Configuration	
O Talvas Valua	Import Watchlist configurat	ion
	This setting is applicable only f	or alerts which have Advanced watchlist configured.
O Reports	on the console where the alert	s are imported.
O Behavior Correlation		
	Source :	
	*.isalt	
	·	
		Import Close

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".

🐁 Export Import Utility	-		\times
Export Import			
1. Provide the path and file na 2. Click the Import button	ame 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 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.

		" D	Admir	1-	Tools -
ers		🧭 Parsing Rules			† /
lt	Contains	set of rules which tell	what kin	d of c	lata you want
Configurat	tion	Systems			



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

Parsing Rules]			
Parsing Rule	Template			
Groups			(Group :
Default			-	
Azure Intune		Ē	1	Templa
	Figure 5	0		
	† / Ad	lmin / F	arsing Rules	٦

^	/ Admin / Parsing Rules
	C 1 T
Active	Import configuration



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".

Import	
Select file Note: Please s	elect file of type *.ettd (eventtracker template dashlets).



5.5 Flex Reports

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



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



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".

🔁 Reports Import				
Note : If report(s) contains template, first import template	and proceed with report import proces	S.		
Select file *.etcrx				Select file
Available reports				
Title	Frequency Show all	-	2 9	
Title	Sites Groups	Systems Fr	requency	Runtime Type

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

Note: Set run time option is not applicat	le 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 valid.

EventTracker displays a success message

Export Import Utility	×
Selected reports configurations are imported succes	sfully
	OK

Figure 56

5.6 Knowledge Objects

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

		🔎 Admin 🗸	Tools 🕶 🌔
Active Watch Lists	Event Filters	河 Parsing Rules	† / D
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
ni sc 扪 Casebook Configuration	🔍 IP Lookup Configuration	🕀 Weights	Systems since the last 24 ho
● Category	€ ∲ • C Knowledge Objects	Windows Agent Config	
▲ Diagnostics	😰 Manager		

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

Figure 58

 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".

Import	
KO_ <product name="">.etko</product>	General Browse 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**".

Import Close

Figure 60

5.7 Dashboards

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

≡	EventTracker 🕀
	Home
٩	My Dashboard
	Threats
	Incidents
	Behavior Correlation
	Change Audit
	Compliance

Figure 61

↑ Dashboard / My Dashboard
Import configuration

- 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

 Import

Figure 64

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

My Dashboard	🔒 / Dashboard / My Dashboar
CheckPoint	⊕∅9\$\$\$

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

dd Dashboard				
litle				
Fastly CDN WAF				
Description				
Fastly content driven network and web appli	cation firewall			
		Save	Delete	Cancel

8. In **My Dashboard** page select (a) to add dashlets.

N	My Dashboard	🕈 / Dashboard / My Dashboard
	Network P., Fastly CDN	+ • • • • • • • • • • • • • • • • • • •
L		

Figure 67

9. Select imported dashlets and click Add.

astly			Q
✓ Fastly CDN - Access events by	✓ Fastly CDN - Access log by Co	I Fastly CDN - Access log by Co	✓ Fastly CDN - Access log by Fast
Fastly CDN - Access log by res	☑ Fastly CDN - Access log by sou	Sastly CDN - Audit Activities	Fastly CDN - service version ch
Fastly CDN - User login fail (Au	🗹 Fastly CDN - User login fail (Au	☑ Fastly CDN - User login succes	Sastly WAF : Rule matched by
Fastly WAF: APPLICATION-ATT	Sastly WAF: APPLICATION-ATT	Sastly WAF: APPLICATION-ATT	☑ Fastly WAF: APPLICATION-ATT
Fastly WAF: APPLICATION-ATT	✓ Fastly WAF: Blocked Requests	Sastly WAF: Blocked URL by Re	 Fastly WAF: High severity Url

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":

I	Alerts									🔒 / Admin	/ Alerts
l	Show All						Search by Alert name	¥	Fastly CDN	୍	٩
l	191	100			191	System	88	191	Critical 1 Low 5 Serious	3 103 34 29	
l	Available Alerts Total number of alerts available	Active Alerts Total number of active alerts			System/User Defir Count for system and use	ed Alerts er defined alerts		Alerts by Thre Count of alerts by t	at Level hreat level		
l	Î Activate Now Click 'Activate Now' after making all changes									Total: 3 Page Size 25	•
l	Alert Name A	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent		Applies To	
L	ββ Fastly CDN Service has been deleted (Audit events)	•							Fasity CDN		
L	📄 දිරි Fastly CDN service version has been deactivated (Audit events)	•							Fasity CDN		
	📄 δδ Fastly CDN user login failed (Audit events)	•							Fasity CDN		

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.

Parsing Rules					
Parsing Rule Template					
Groups	-5-	()	Token-Value	Display r	name 🔻
Fastly CDN		0	+		Display name
			(\pm)		Access Key
			+		Acl
			+		Action

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.

Parsing Rules	5				
Parsing Rule	Template				
Groups	roups				Group : Fastly CDN
Fastly CDN				0	Template Name
					Fastly CDN

Figure 72

6.5 Flex Reports

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

2	Report Configuration
	Report Dashboard
	Explorer

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

Scheduled Queued Defined				
Report Groups	•	Repo	erts configur	ation: Fastly CDN
(:) Security		- 🕀	1 8.	
Compliance		8		Title
(i) Operations		13	(2)	Fastly CDN - service management (Audit event
(1) Piex		8	Ð	Fastly CDN - User management (Audit events)
(f) OpenDNS			0	Fastly CDN - Login success (Audit events)
Fastly ()	i c		۲	Fastly CDN - Login failure (Audit events)
	2	0	()	Pastly CDN - Success events (Access events)
		0	۲	Fastly CDN + Error events (Access events)

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.

Knowledge Objects		
Search objects	Q Q	Activate Now
Groups	+ Ø 🗊	Object name Fastly CDN Events Applies to Fastly CDN
 Fastly CDN Fastly CDN Events 	Ø	Rules
		Title
		Fastly CDN Access logs Message Signature: (?i)cache\-\
		Message Exception:

6.7 Dashboards

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

2. "Fastly CDN/WAF" dashboard opens.

Figure 77

