

## Integrate FortiWeb

EventTracker v8.x and above

# Abstract

This guide provides instructions to configure a **FortiWeb** to send its syslog to EventTracker Enterprise.

# Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and **FortiWeb version 5.0- 6.0**.

# Audience

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

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

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

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

*EventTracker 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 EventTracker, 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.*

*© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

Abstract .....	1
Scope .....	1
Audience .....	1
Overview .....	3
Prerequisites .....	3
Integration of FortiWeb with EventTracker Manager .....	3
EventTracker Knowledge Pack .....	6
Category .....	7
Alerts .....	7
Knowledge Object .....	7
Flex Reports .....	7
Import FortiWeb knowledge pack into EventTracker .....	11
Category .....	12
Alerts .....	13
Token Templates .....	14
Knowledge Object .....	15
Flex Report .....	17
Dashboard .....	19
Verify FortiWeb knowledge pack in EventTracker .....	20
Category .....	20
Alerts .....	21
Token Template .....	22
Knowledge Object .....	23
Flex Report .....	24
Dashboard .....	25

## Overview

**FortiWeb's** AI-enhanced and multi-layered approach protects your web apps from the OWASP Top 10 and more. Its Web Application Security Service from FortiGuard Labs ensures that you're protected from the latest application vulnerabilities, bots, and suspicious URLs, and with dual machine learning detection, engines your applications and make sure they are safe from sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, cookie poisoning, malicious sources, and DoS attacks.

EventTracker helps to monitor events from **FortiWeb**. It's knowledge object and flex reports will help you to analyse web attacks such as **Sql injection, Cross site scripting, Directory traversal** etc.

## Prerequisites

- **EventTracker v8.x** or **above** should be installed.
- **FortiWeb** version **5.0-6.0** should be configured.
- Create a **rule** in **EventTracker Manager Workstation** firewall for inbound and outbound to allow **UDP** port **514**.

## Integration of FortiWeb with EventTracker Manager

- To store log messages remotely on a syslog server, you first need to create the syslog connection settings.
- Syslog settings can be referenced by a trigger, which in turn can be selected as the trigger action in a protection profile and used to send log messages to one or more syslog servers whenever a policy violation occurs.
- You can use each syslog policy to configure connections to up to 3 syslog servers.

To configure Syslog policies,

- Before you can log to syslog, you must enable it for the log type that you want to use as a trigger.
  1. Go to **Log&Report > Log Policy > Syslog Policy**.
  2. Click **Create New**.

Figure 1

3. If the policy is new, in **Policy Name**, type the name of the policy as it will be referenced in the configuration.
4. Click **Create New**.

Figure 2

5. In **IP Address**, enter the **EventTracker Manager IP Address**.
  6. In **Port**, enter **514 (UDP)**.
  7. Click **OK**.
- You can enable or disable logging for each log type, as well as configure system alert thresholds, and which policy violations should cause the appliance to retain the TCP/IP packet payload (HTTP headers and a portion of the HTTP body, if any) that can be viewed with its corresponding log message.

To enable logging,

1. Go to **Log&Report > Log Config > Other Log Settings**

Configure these settings:

### Other Log Settings

Enable Attack Log	<input checked="" type="checkbox"/>
Enable Traffic Log	<input type="checkbox"/>
Enable Traffic Packet Log	<input type="checkbox"/>
Enable Event Log	<input checked="" type="checkbox"/>
Ignore SSL Errors	<input checked="" type="checkbox"/>

---

#### Retain Packet Payload For

Parameter Rule Violation	<input checked="" type="checkbox"/>
Hidden Fields Violation	<input checked="" type="checkbox"/>
HTTP Protocol Constraints	<input checked="" type="checkbox"/>
Signature Detection	<input checked="" type="checkbox"/>
Custom Signature Detection	<input checked="" type="checkbox"/>
Anti Virus Detection	<input checked="" type="checkbox"/>
Custom Access Violation	<input type="checkbox"/>
Illegal XML Format	<input checked="" type="checkbox"/>
IP Reputation Violation	<input checked="" type="checkbox"/>
Illegal File Type	<input checked="" type="checkbox"/>
Cookie Security	<input checked="" type="checkbox"/>
Padding Oracle Attack	<input type="checkbox"/>
FortiSandbox Detection	<input checked="" type="checkbox"/>
Illegal JSON Format	<input type="checkbox"/>
Illegal File Size	<input type="checkbox"/>
Trojan Detection	<input checked="" type="checkbox"/>
CSRF Detection	<input type="checkbox"/>
User Tracking Detection	<input checked="" type="checkbox"/>
Account Lockout	<input checked="" type="checkbox"/>
Credential Stuffing Detection	<input checked="" type="checkbox"/>

---

#### System Alert Thresholds

CPU Utilization	<input type="text" value="60"/>	(60-99)
Memory Utilization	<input type="text" value="60"/>	(60-99)
Log Disk Utilization	<input type="text" value="60"/>	(60-99)
Trigger Policy	<input type="text" value="[Please Select...]"/>	

Figure 3

2. Click **Apply**.

To configure log settings,

1. Go to **Log&Report > Log Config > Global Log Settings**

Configure these settings:

Global Log Settings

Disk

Log Level: Information

When log disk is full: Overwrite oldest logs

Syslog

Syslog Policy: Please Select...

Log Level: Information

Facility: reserved for local use 7

Alert Mail

Email Policy: Please Select...

FortiAnalyzer

Log Level: Information

FortiAnalyzer Policy: Please Select...

SIEM

Log Level: Information

SIEM Policy: Please Select...

Apply

Figure 4

2. Click **Apply**.

## EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support FortiWeb Business.

## Category

- **FortiWeb- Admin activities-** This category provides information related to all the admin activities that are done.
- **FortiWeb- Admin login and logout-** This category provides information related to all the admin login and logout activities.
- **FortiWeb- Admin login failures-** This category provides information related to all the admin login failures.
- **FortiWeb- System activities-** This category provides information related to all the system activities that are done.
- **FortiWeb- Attack detection-** This category provides information related to all the attacks and threats that are detected by FortiWeb.
- **FortiWeb- Traffic details-** This category provides information related to all the web traffic flow that is observed by the FortiWeb.

## Alerts

- **FortiWeb: Admin login failures:** This alert is generated when any admin login failure has happened.
- **FortiWeb: Attack detection:** This alert is generated when any attack or threat is detected.

## Knowledge Object

- **FortiWeb Admin activities** - This knowledge object will help us to analyze all the logs related to admin activities.
- **FortiWeb Admin logons** - This knowledge object will help us to analyze all the logs related to admin logons.
- **FortiWeb Attack detection** - This knowledge object will help us to analyze all the logs related to attack and threat detection.
- **FortiWeb System activities** - This knowledge object will help us to analyze all the logs related to system activities.
- **FortiWeb Traffic details** - This knowledge object will help us to analyze all the logs related to web traffic flow.

## Flex Reports

- **FortiWeb- Attack detection-** This report gives the information about all the attacks and threats that are detected by FortiWeb.



LogTime	Computer	User Name	Source IP Address	Source Port	Destination IP Address	Destination Port	Priority	Attack Type	Action	Message	Signature Subclass	Policy Name	Status	Http Method	URL Accessed	Service Name	User Agent	Source Country
08/09/2018 05:34:17 PM	Contoso-11	Unknown	10.0.8.103	8142	172.20.120.4	443	alert	Information Disclosure	Alert_Deny	HTTP Header triggered signature ID 080200001 of Signatures policy et2-20181025012904	HTTP Header Leakage	Threat IDR	Disabled	Post	/EventTracker/Home.aspx	https/tls1.2	Mozilla/4.0 (compatible; MSE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C;	US
08/09/2018 05:34:17 PM	Contoso-11	Unknown	172.20.120.4	53817	10.20.8.22	443	alert	SQL Injection (Syntax Based Detection)	Alert	Parameter(searchValue_0) triggered signature ID 120030003 of Signatures policy V9DemoLrned-20181026161142	As-is Based SQL Injection	Threat IDR	Disabled	Post	/EventTracker/LogSearch/AdvancedSearch.aspx	https/tls1.2	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0	US
08/09/2018 05:34:17 PM	Contoso-11	casey	113.193.182.226	62049	1.244.106.253	443	alert	Directory Traversal	Alert_Deny	Parameter(hdnJsonFile) triggered signature ID 050180003 of Signatures policy et2-20181025012904	Directory Traversal	Threat IDR	Disabled	Post	/EventTracker/LogSearch/AdvancedSearch.aspx	https/tls1.2	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0	US

Figure 5

Logs Considered

```

- Nov 13 03:03:54 PM Oct 29 08:35:42 1.244.68.100 date=2018-10-29 time=08:35:42 log_id=20000004 msg_id=000000129486 device_id=FVVM020000175209 vd="root" timezone="(GMT-6:00)Central Time(US&Canada)" type=attack pri=alert main...

event_category      +- 0
event_computer      +- Fortiweb
event_datetime      +- 11/13/2018 3:03:54 PM
event_datetime_utc  +- 1542101634
event_description    Oct 29 08:35:42 1.244.68.100 date=2018-10-29 time=08:35:42 log_id=20000004 msg_id=000000129486 device_id=FVVM020000175209 vd="root" timezone="(GMT-6:00)Central Time(US&Canada)" type=attack pri=alert main...
n_type="Start Pages" sub_type="N/A" trigger_policy="" severity_level=Low proto=tcp service=https/tls1.2 action=Alert policy="ETPVMDFHMDR06" src=184.58.134.126 src_port=22381 dst=1.244.106.180 dst_port=443 http
_method=get http_url="/EventTracker/Account/Logout.aspx" http_host="mdr6.eventtracker.com" http_agent="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.353
8.77 Safari/537.36" http_session_id=364f64d5408f8ebw4e6dhyt8thxkn388f msg="Start Page Violation" signature_subclass="N/A" signature_id="N/A" srccountry="United States" content_switch_name="none" server_p
ool_name="ETPVMDFHMDR06-10.255.0.33/32" false_positive_mitigation="none" user_name="Unknown" monitor_status="Disabled" http_refers="https://mdr6.eventtracker.com/EventTracker/Admin/Role/Roles.aspx" htt
p_ver
event_id            +- 30
event_log_type      +- Application
event_source        +- syslog
event_type          +- Information
event_user_domain   +- N/A
event_user_name     +- N/A
    
```

Figure 6

- **FortiWeb- Admin login and logout**– This report gives the information about all the admin login and logout activities.

LogTime	Computer	User Name	Action	Status	Message	Policy Name
08/09/2018 05:34:17 PM	Contoso-11	admin	login	success	User admin logged in successfully from telnet (10.200.0.1)	admincheck
08/09/2018 05:34:17 PM	Contoso-11	admin	logout	success	User admin logs out from GUI(172.20.120.47)	admincheck

Figure 7

## Logs Considered

```

- Nov 13 04:02:05 PM      date=2014-04-10 time=13:31:37 log_id=10000016 msg_id=000044294845 device_id=FV1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice...

event_category          +- 0
event_computer          +- Fortiweb
event_datetime          +- 11/13/2018 4:02:05 PM
event_datetime_utc      +- 1542105125
event_description       date=2014-04-10 time=13:31:37 log_id=10000016 msg_id=000044294845 device_id=FV1KD3A13800002 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=notice...
                        e trigger_policy="check1" user=admin ui=telnet action=login status=success msg="User admin logged in successfully from telnet (10.200.0.1)"

event_id                +- 30
event_log_type          +- Application
event_source            +- syslog
event_type              +- Information
event_user_domain       +- N/A
event_user_name         +- N/A

```

Figure 8

- **FortiWeb- Admin login failures** -This report gives information about all the admin login failures.

LogTime	Computer	User Name	Action	Status	Message	Policy Name
08/09/2018 05:34:17 PM	Contoso-11	admin	login	failed	User a login failed from GUI	admincheck

Figure 9

## Logs Considered

```

- Nov 13 04:02:05 PM      date=2014-04-10 time=18:11:53 log_id=10000017 msg_id=000000195892 device_id=FV1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert tr...

event_category          +- 0
event_computer          +- Fortiweb
event_datetime          +- 11/13/2018 4:02:05 PM
event_datetime_utc      +- 1542105125
event_description       date=2014-04-10 time=18:11:53 log_id=10000017 msg_id=000000195892 device_id=FV1KD3A13800012 vd="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtype="system" pri=alert t...
                        rigger_policy="check1" user=a ui=GUI action=login status=failed msg="User a login failed from GUI(172.22.6.240)"

event_id                +- 30
event_log_type          +- Application
event_source            +- syslog
event_type              +- Information
event_user_domain       +- N/A
event_user_name         +- N/A

```

Figure 10

- **FortiWeb- System activities** -This report gives information about all the system activities that are performed.

LogTime	Computer	User Name	Priority	Action	Status	Message	Policy Name
08/09/2018 05:34:17 PM	Contoso-11	admin	critical	reboot	failed	User admin rebooted the device from GUI (172.20.120.47)	systemcheck
08/09/2018 05:34:17 PM	Contoso-11	admin	critical	shutdown	success	User admin shut down the device from GUI(172.22.6.241)	systemcheck
08/09/2018 05:34:17 PM	Contoso-11	admin	notice	del	success	User admin has deleted disk log elog(2014-04-09-23:34:02).log from GUI(172.22.6.240)	systemcheck
08/09/2018 05:34:17 PM	Contoso-11	admin	critical	downgrade	success	User admin downgraded the image from GUI (10.200.0.1)	systemcheck
08/09/2018 05:34:17 PM	Contoso-11	admin	critical	update	success	User admin manually update virus signature from GUI (10.200.10.80) success	systemcheck

Figure 11

Logs Considered

```

event_category      +- 0
event_computer      +- Fortiweb
event_datetime      +- 11/13/2018 4:02:05 PM
event_datetime_utc  +- 1542105125
event_description    date=2014-04-10 time=15:22:38 log_id=10000020 msg_id=000000548987 device_id=FVVM040000018474 vds="root" timezone="(GMT+8:00)Beijing,ChongQing,HongKong,Urumgi" type=event subtypes="system" pri=critical trigger_policy="check1" user=admin ui=GUI action=downgrade status=success msg="User admin downgraded the image from GUI (10.200.0.1)"
event_id            +- 30
event_log_type      +- Application
event_source        +- syslog
event_type          +- Information
event_user_domain   +- N/A
event_user_name     +- N/A
    
```

Figure 12

- **FortiWeb- Traffic details**-This report gives information about all the web traffic flow that is observed by FortiWeb.

LogTime	Computer	Source IP Address	Source Port	Destination IP Address	Destination Port	Priority	Status	Message	Reason	Policy Name	Bytes In	Bytes Out	Http Method	URL Accessed	Service Name	User Agent	Status Code	Source Country
08/09/2018 05:34:17 PM	Contoso-11	10.0.8.103	8142	172.20.120.4	80	notice	success	HTTP GET request from 10.0.8.103:8142 to 10.20.8.22:80	none	Auto-policy	7575	2338	GET	http://www.fortinet.com/products/web-application-firewall/fortiweb.html	http	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C;	200	US
08/09/2018 05:34:17 PM	Contoso-11	172.20.120.4	53817	10.20.8.22	80	notice	success	HTTPS GET request from 172.20.120.47:53817 to 172.20.120.47:80	none	Auto-policy	5756	3836	GET	/index	http	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0	200	US

Figure 13

**Logs Considered:**

Nov 13 04:02:05 PM	date=2014-04-11 time=09:26:22 log_id=30000000 msg_id=00000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto...
event_category	+-- 0
event_computer	+-- Fortiweb
event_datetime	+-- 11/13/2018 4:02:05 PM
event_datetime_utc	+-- 1542105125
event_description	date=2014-04-11 time=09:26:22 log_id=30000000 msg_id=00000000156 device_id=FVVM00UNLICENSED vd="root" timezone="(GMT-5:00)Eastern Time(US & Canada)" type=traffic subtype="http" pri=notification proto... o=tcp service=https status=success reason="none" policy="policy1" src=172.20.120.47 src_port=53817 dst=172.20.120.47 dst_port=80 http_request_time=18 http_response_time=1 http_request_bytes=464 http_response_bytes=3060 http_method=get http_url="/index" http_host="172.20.120.48" http_agent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0" http_retcode=200 msg="HTTPS GET request from 172.20.120.47:53817 to 172.20.120.47:80 " srccountry="United States" content_switch_name="testa" server_pool_name="AutoServerFarm"
event_id	+-- 30
event_log_type	+-- Application
event_source	+-- syslog
event_type	+-- Information
event_user_domain	+-- N/A
event_user_name	+-- N/A

Figure 14

## Import FortiWeb knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Templates
- Knowledge Objects
- Flex Reports
- Dashboards

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

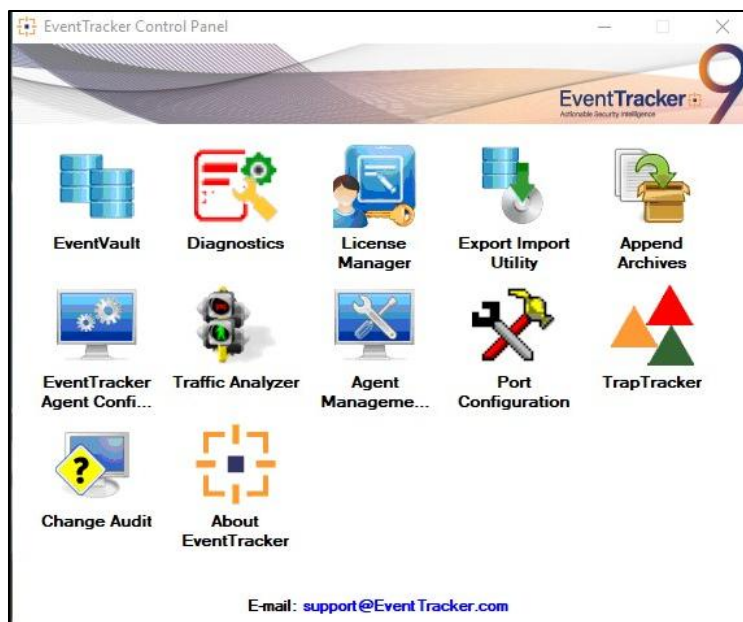



Figure 15

3. Click the **Import** tab.

## Category

1. Click **Category** option, and then click the browse  button.

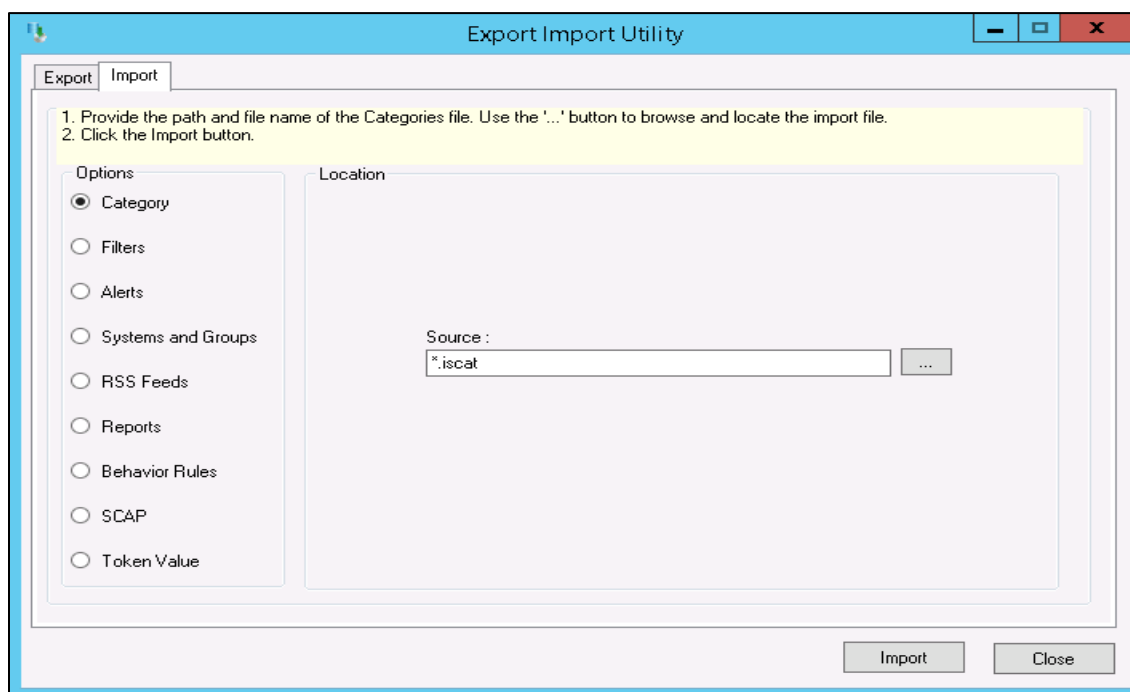


Figure 16

2. Locate **Category\_FortiWeb.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

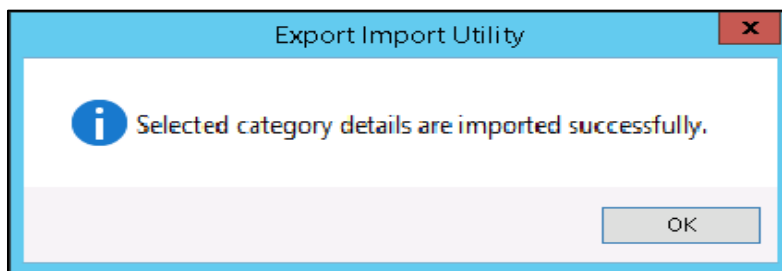



Figure 17

4. Click **OK**, and then click the **Close** button.

## Alerts

1. Click **Alert** option, and then click the **browse**  button.

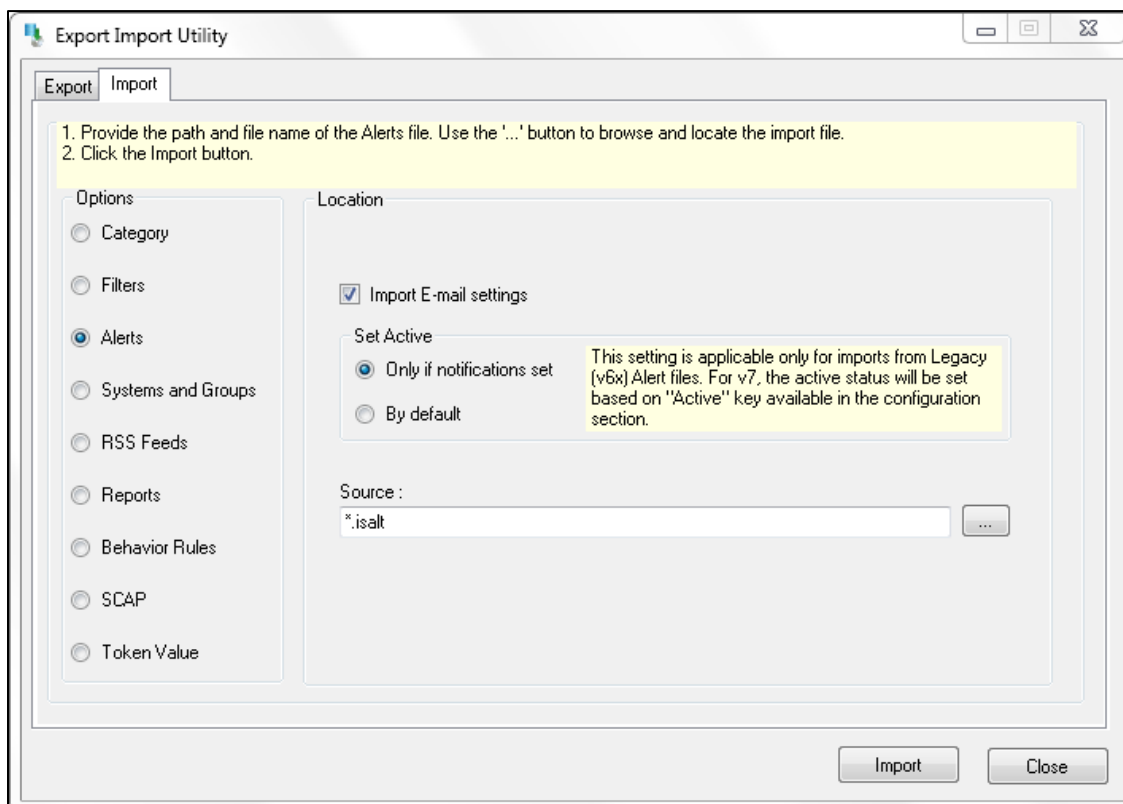


Figure 18

2. Locate **Alerts\_FortiWeb.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.  
EventTracker displays success message.

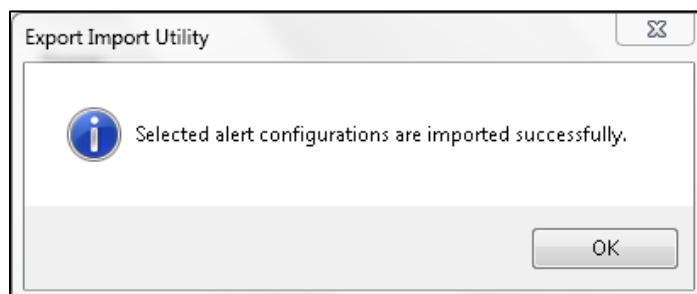


Figure 19

4. Click the **OK** button, and then click the **Close** button.

## Token Templates

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

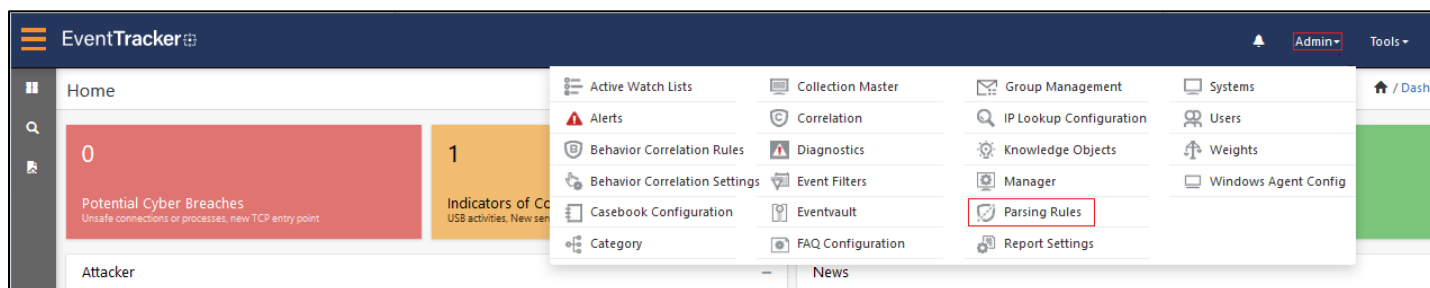



Figure 20

2. Move to **Template** and click on import configuration  icon on the top right corner.
3. In the popup window browse the file named **Template\_FortiWeb.ett**.

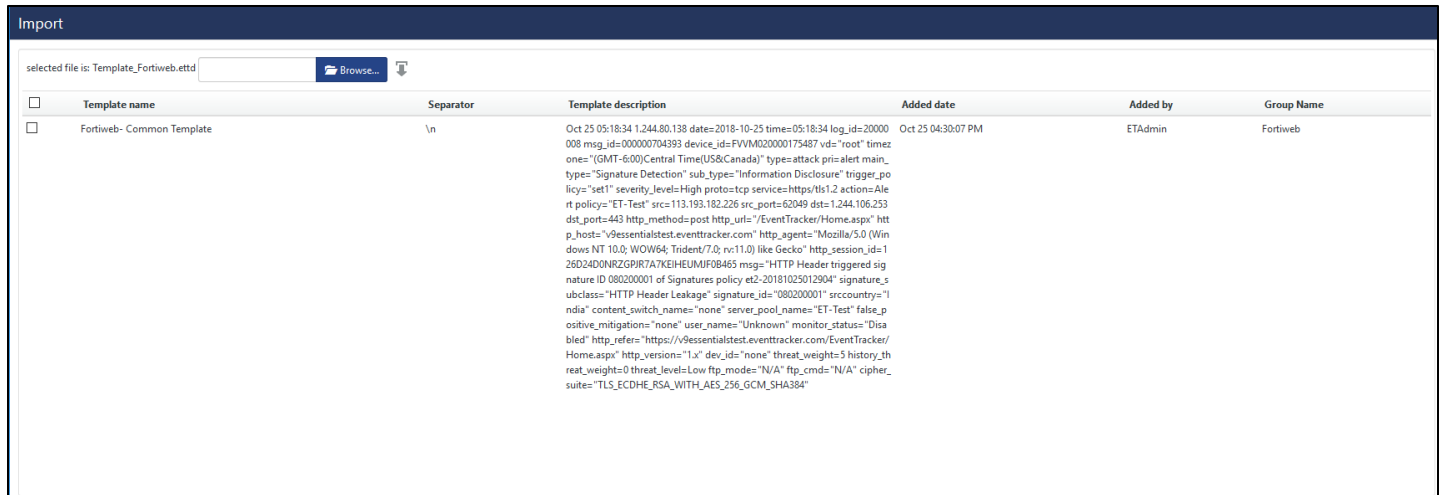



Figure 21

- Now select all the check box and then click on  Import option.

## Knowledge Object

- Click **Knowledge objects** under Admin option in the EventTracker manager page.

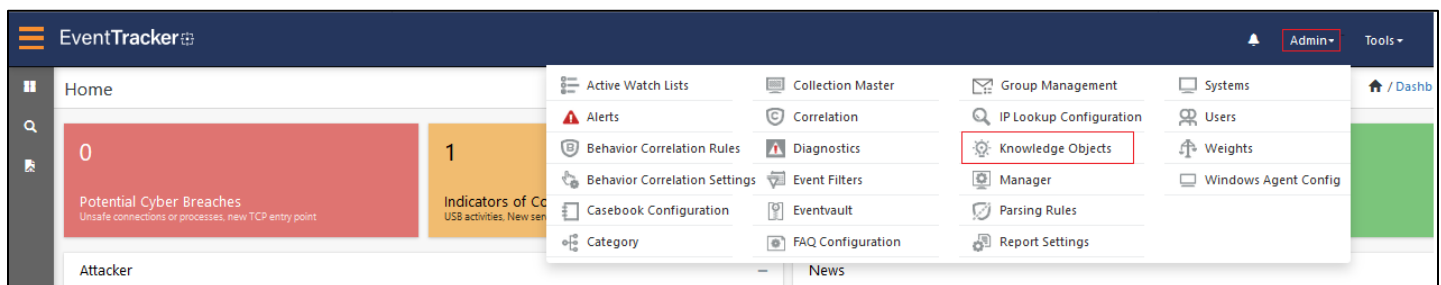


Figure 22

- Click on **Import** button as highlighted in the below image:

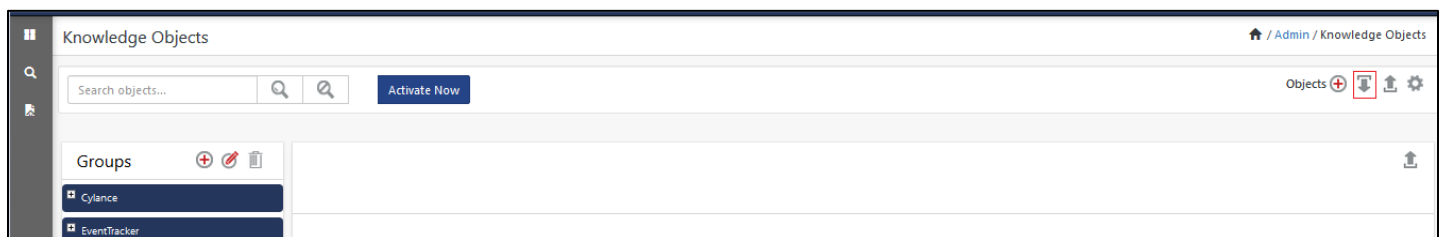


Figure 23

- Click on **Browse**.



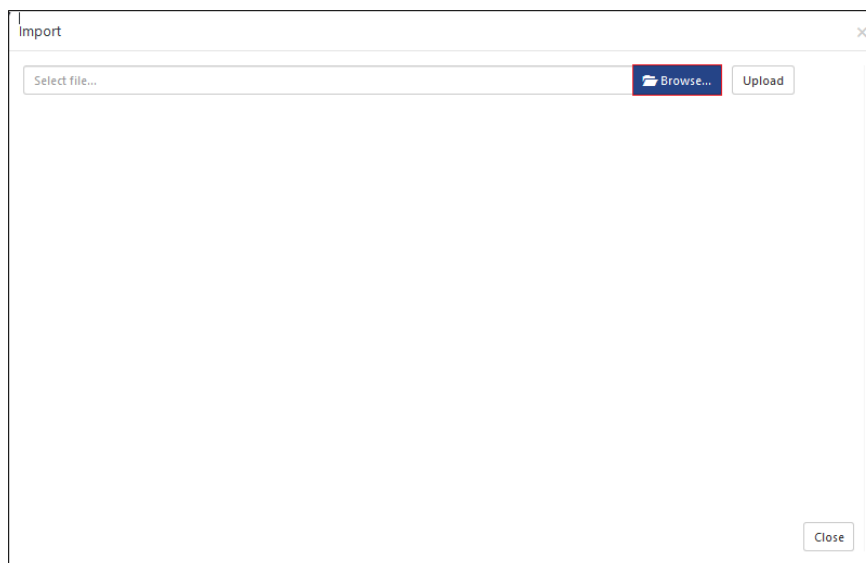



Figure 24

4. Locate the file named **KO\_FortiWeb.etko**.
5. Now select all the check box and then click on  **'Import'** option.

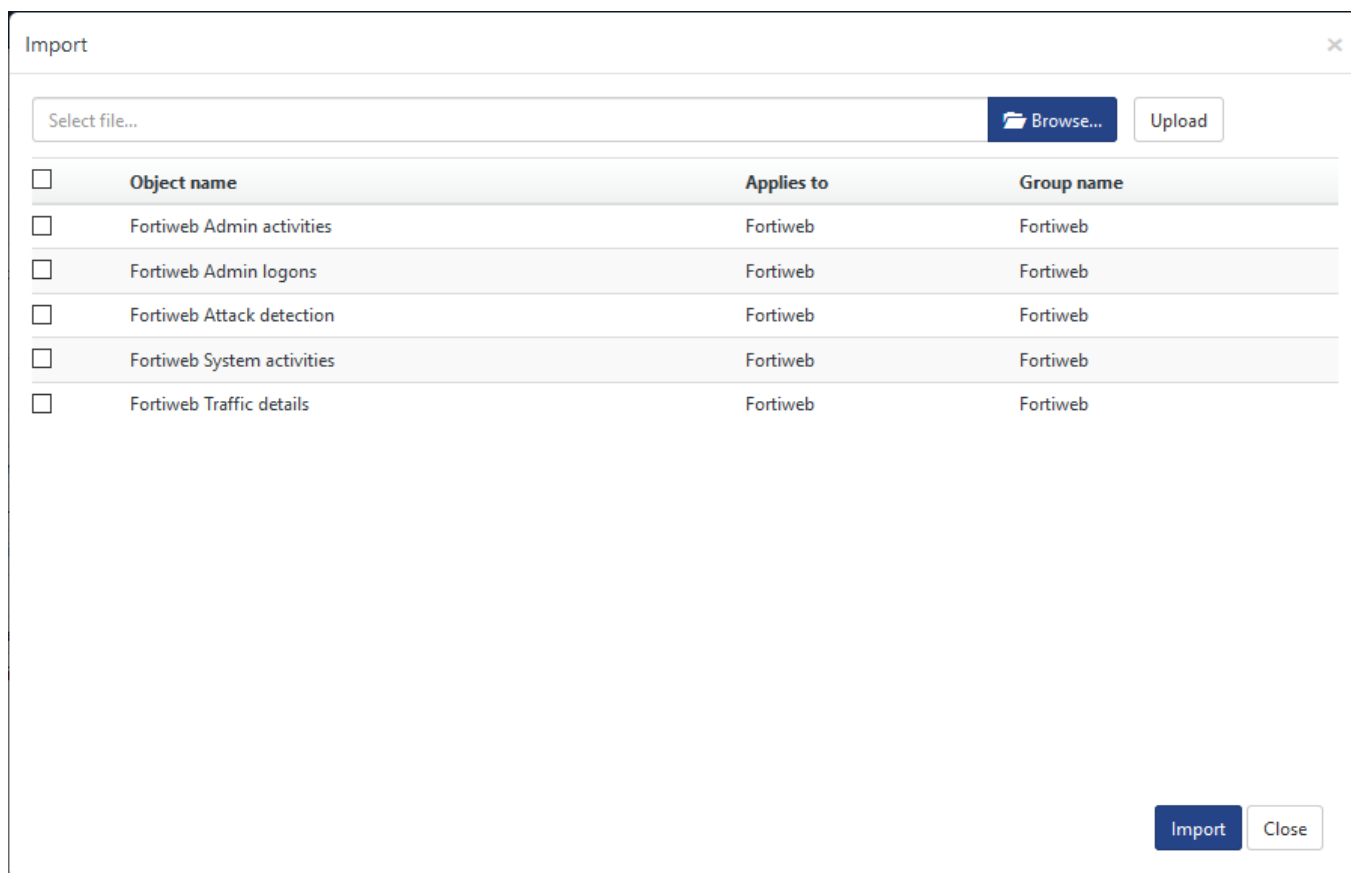


Figure 25

- Knowledge objects are now imported successfully.

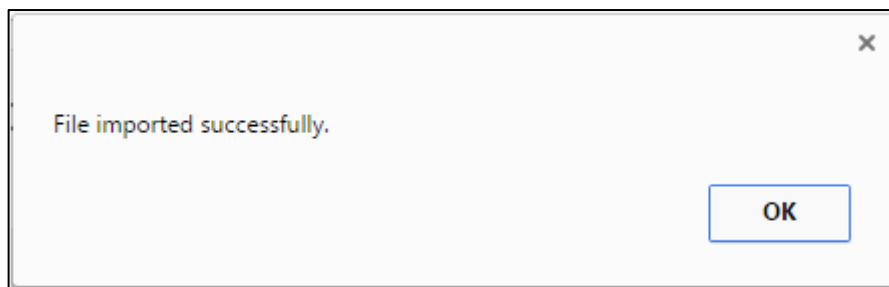


Figure 26

## Flex Report

On **EventTracker Control Panel**,

- Click **Reports** option and select **New (\*.etcrx)** option.

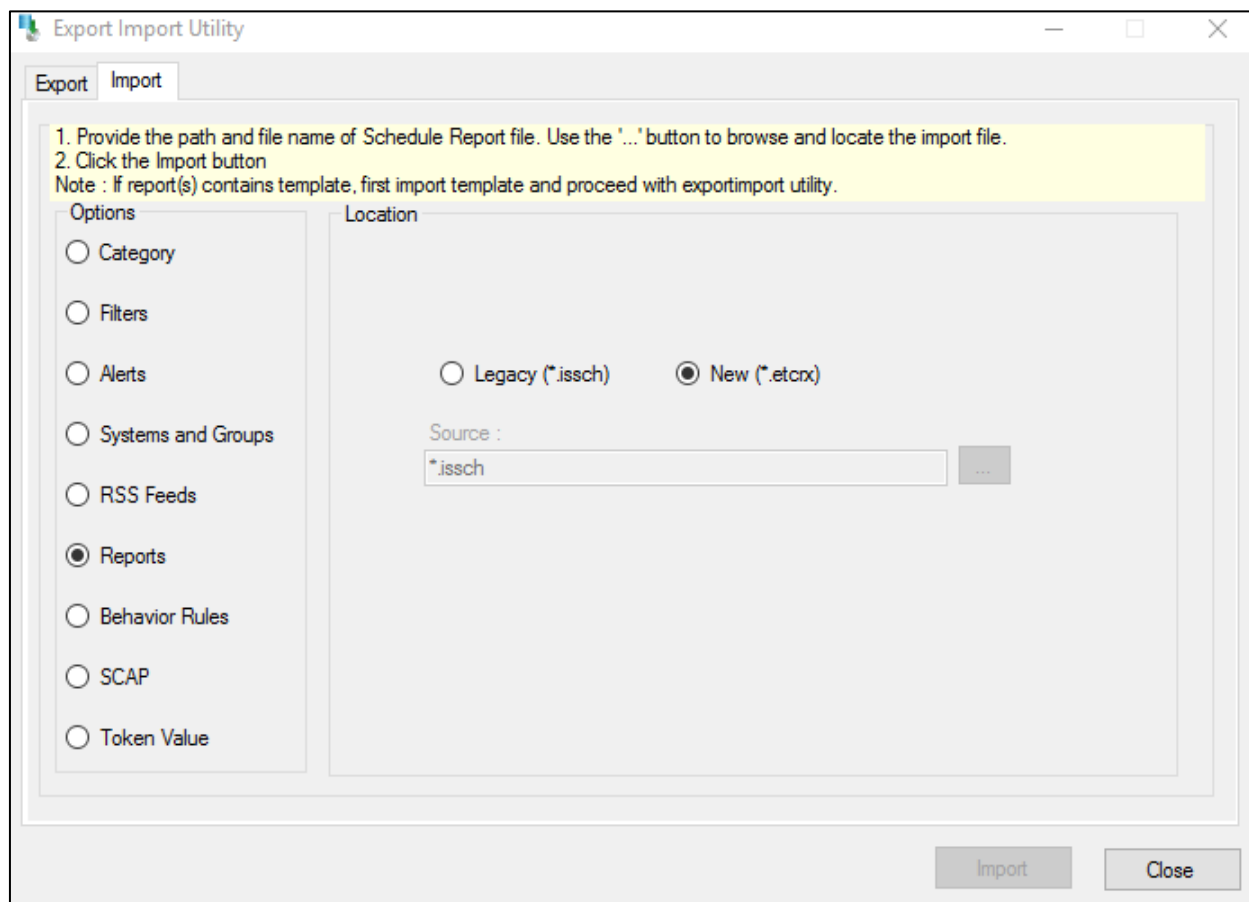


Figure 27

- Locate the file named **Reports\_FortiWeb.etcrx** and select all the check box.

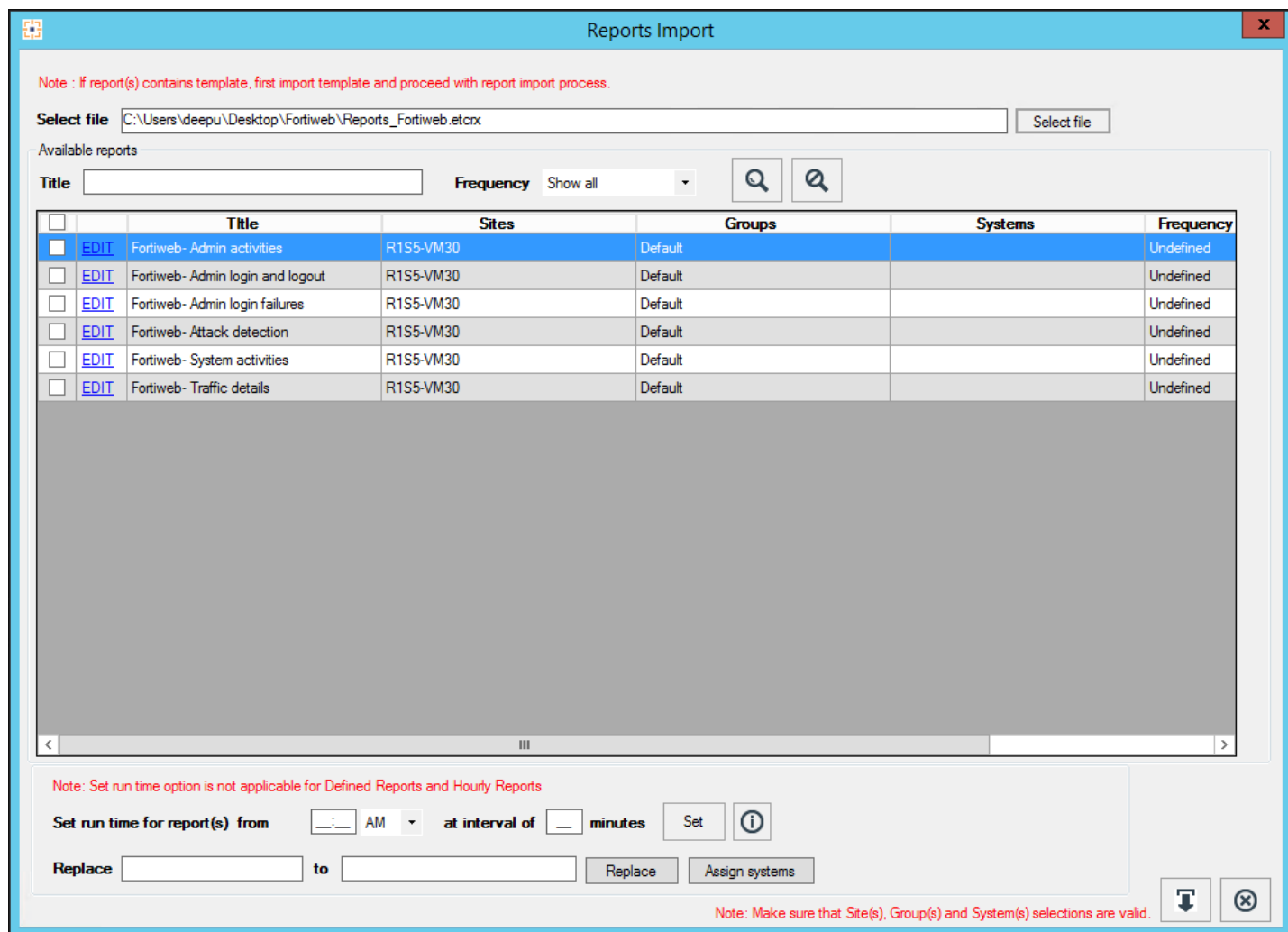


Figure 28

- Click the **Import** button to import the reports. EventTracker displays success message.

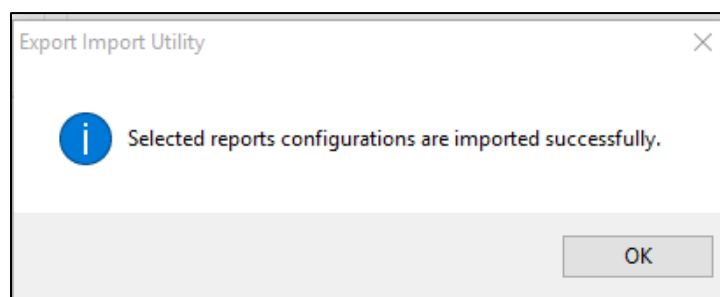


Figure 29

## Dashboard

**NOTE-** Below steps given are specific to EventTracker 9 and later.

- Open **EventTracker Enterprise** in browser and logon.

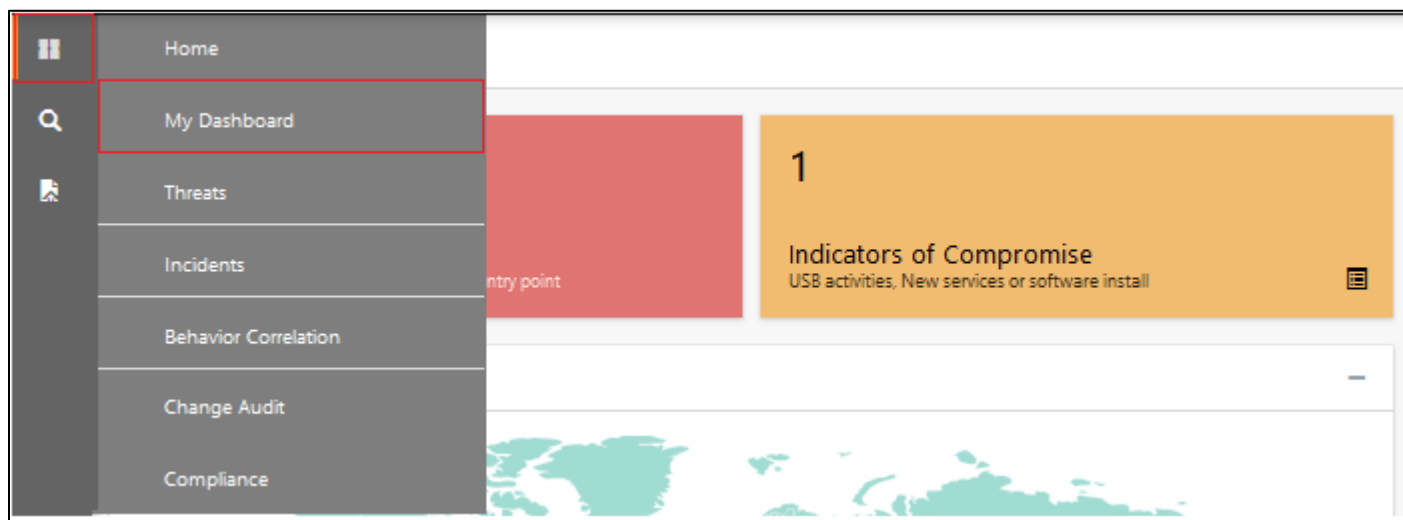


Figure 30

- Navigate to **My Dashboard** option as shown above.
- Click on the **Import** button as show below:



Figure 31

- Import dashboard file **Dashboard\_FortiWeb.etwd** and select the dashboards that you require and click on **Import** as shown below:

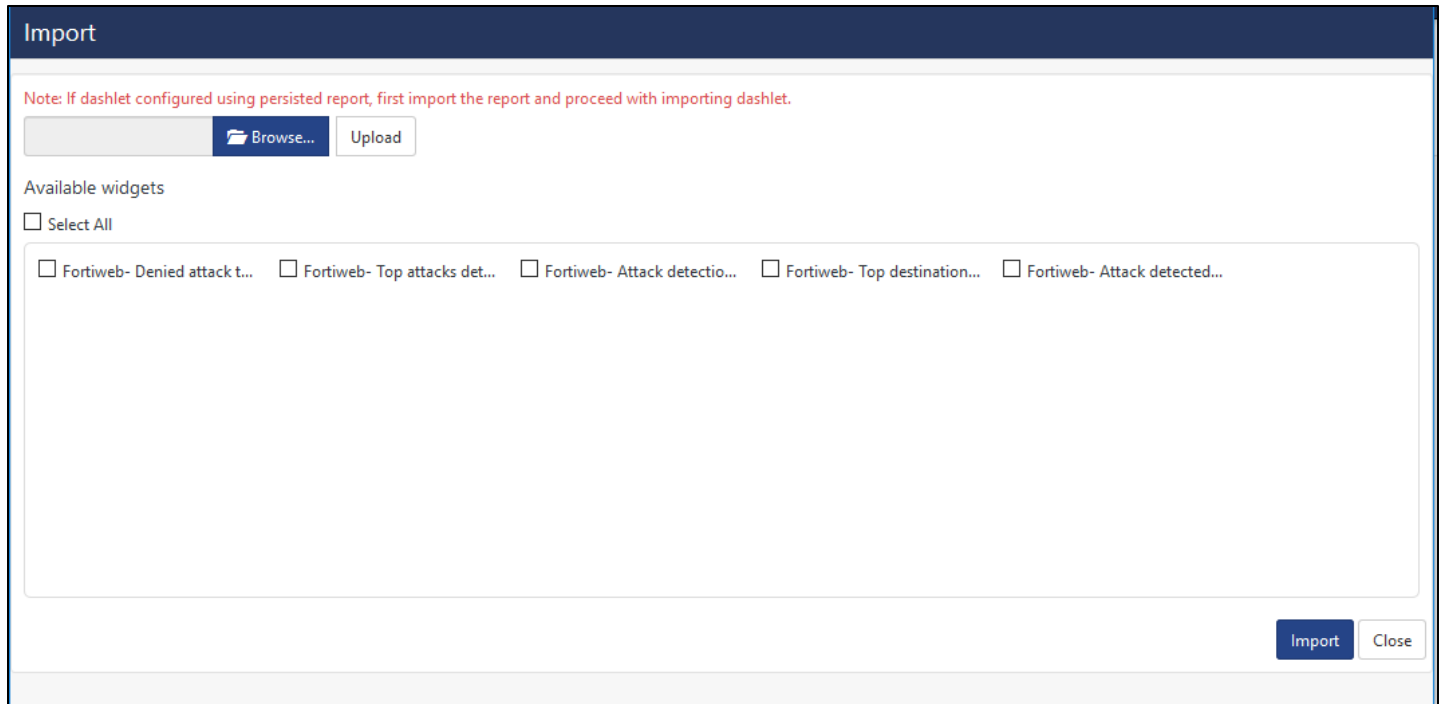


Figure 32

- Import is now completed successfully.

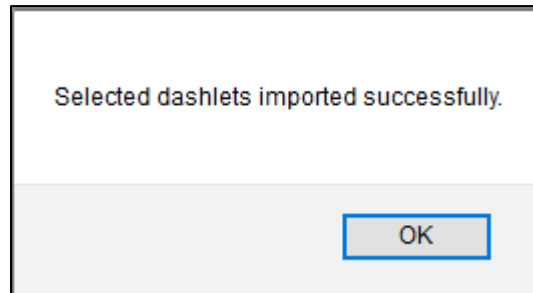


Figure 33

## Verify FortiWeb knowledge pack in EventTracker

### Category

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.

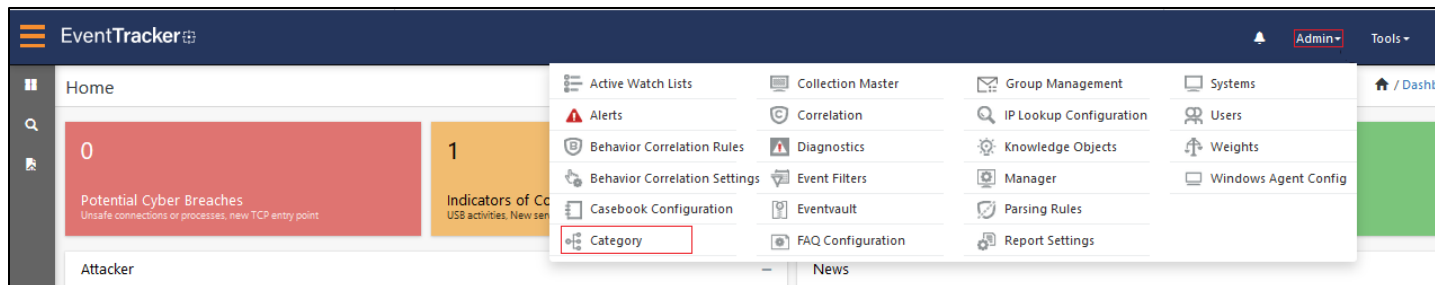


Figure 34

3. In **Category Tree** to view imported categories, scroll down and expand FortiWeb group folder to view the imported categories.

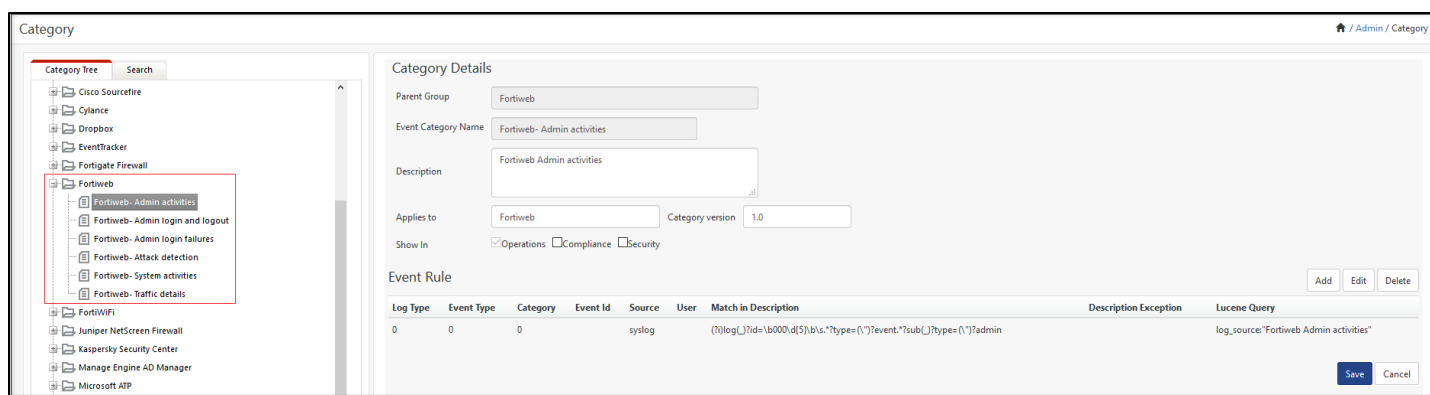


Figure 35

## Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.

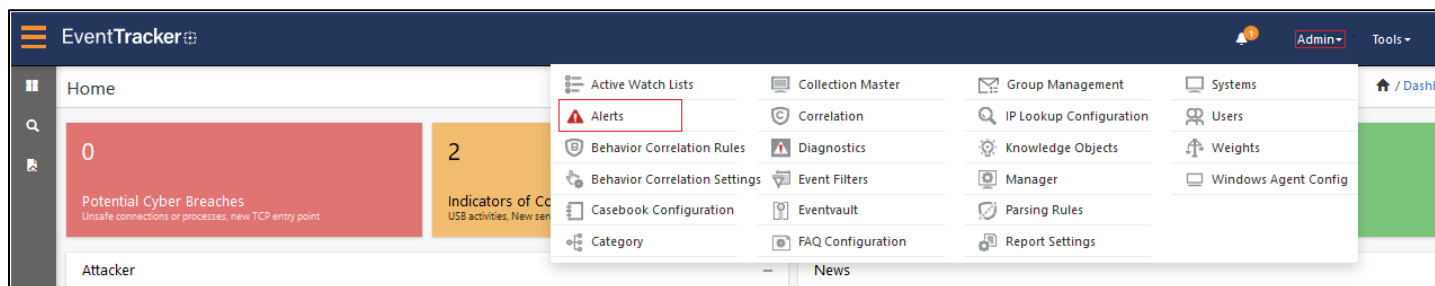


Figure 36

3. In the **Search** box, type '**Fortiweb**', and then click the **Go** button. Alert Management page will display all the imported alerts.

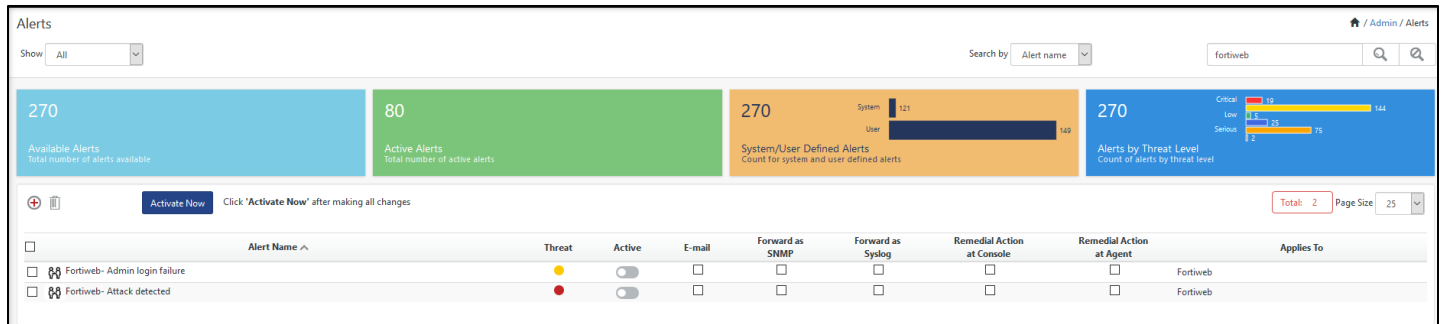


Figure 37

- To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

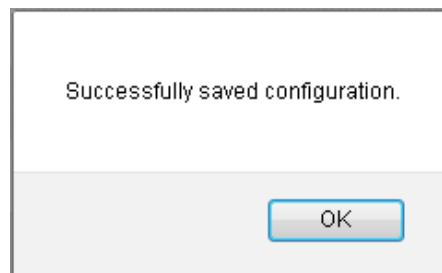


Figure 38

- Click **OK**, and then click the **Activate Now** button.

**NOTE:** Please specify appropriate **systems** in **alert configuration** for better performance.

## Token Template

- In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

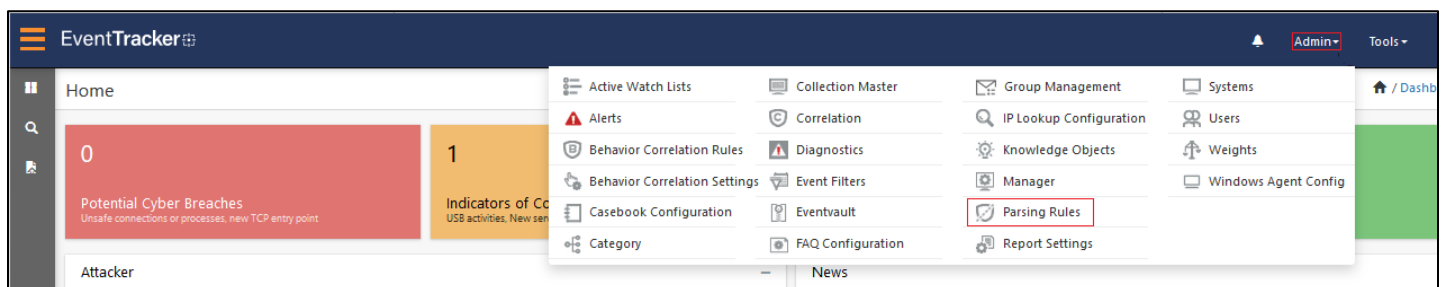


Figure 39

- On **Template** tab, click on the **FortiWeb** group folder to view the imported Templates.

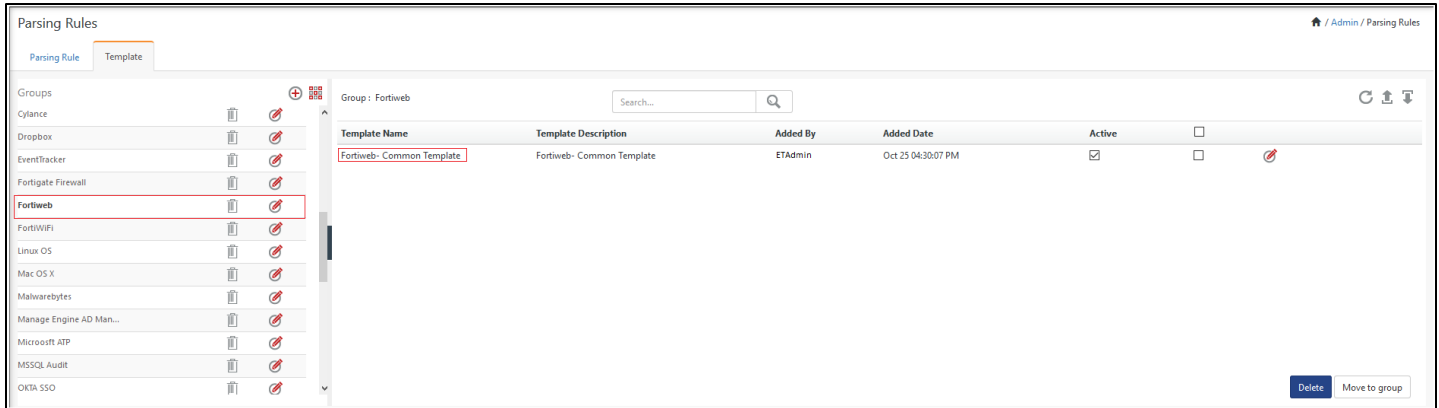


Figure 40

## Knowledge Object

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.

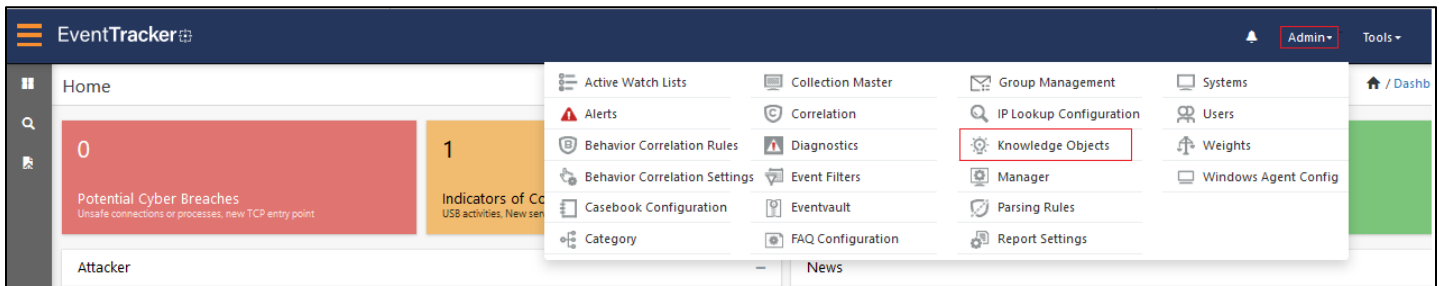


Figure 41

2. In the Knowledge Object tree, expand **FortiWeb** group folder to view the imported Knowledge objects.

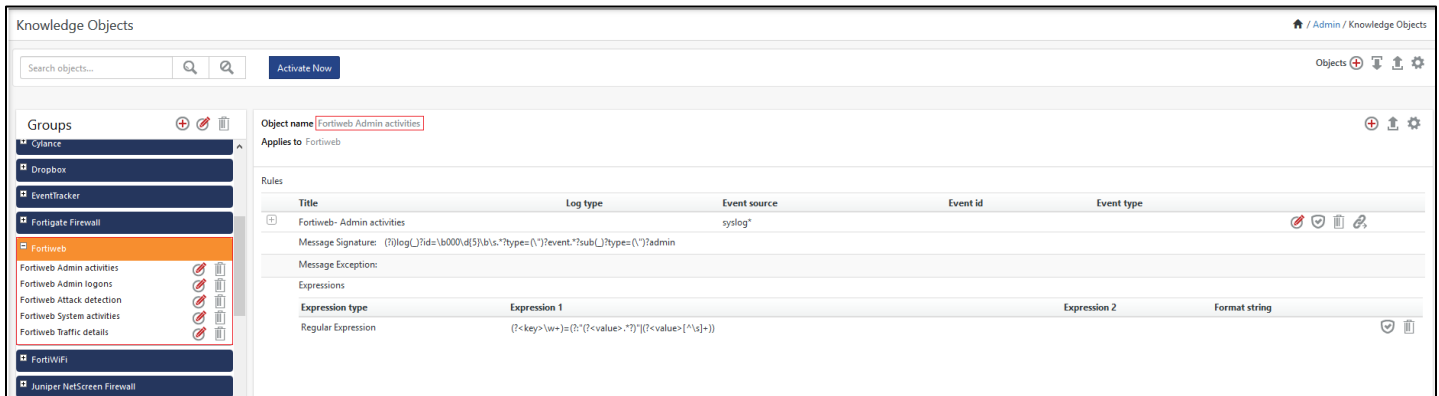


Figure 42



## Flex Report

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

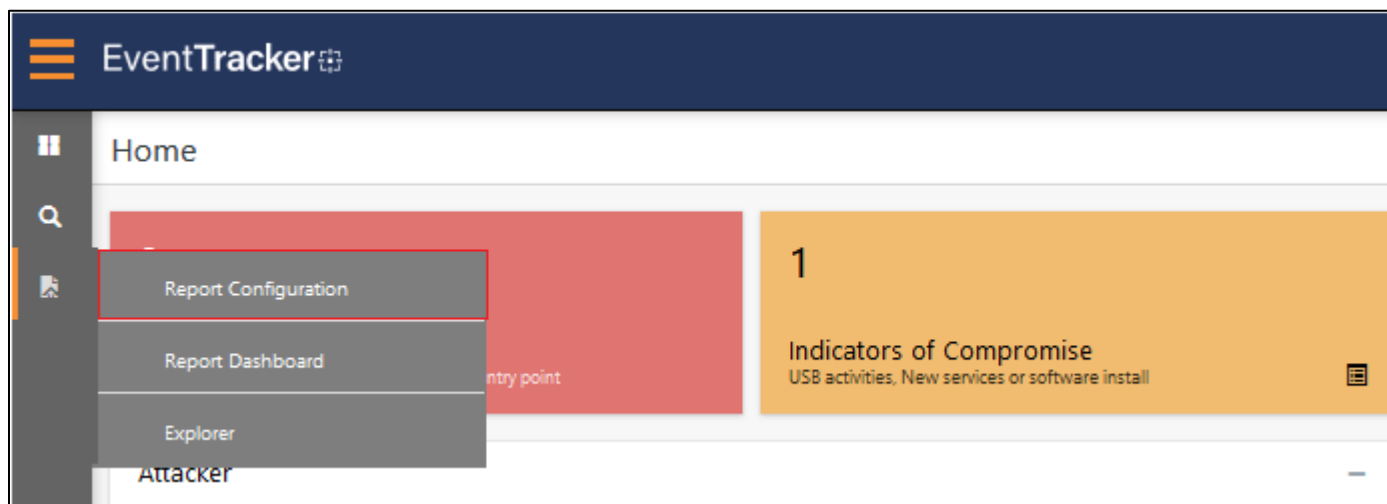


Figure 43

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

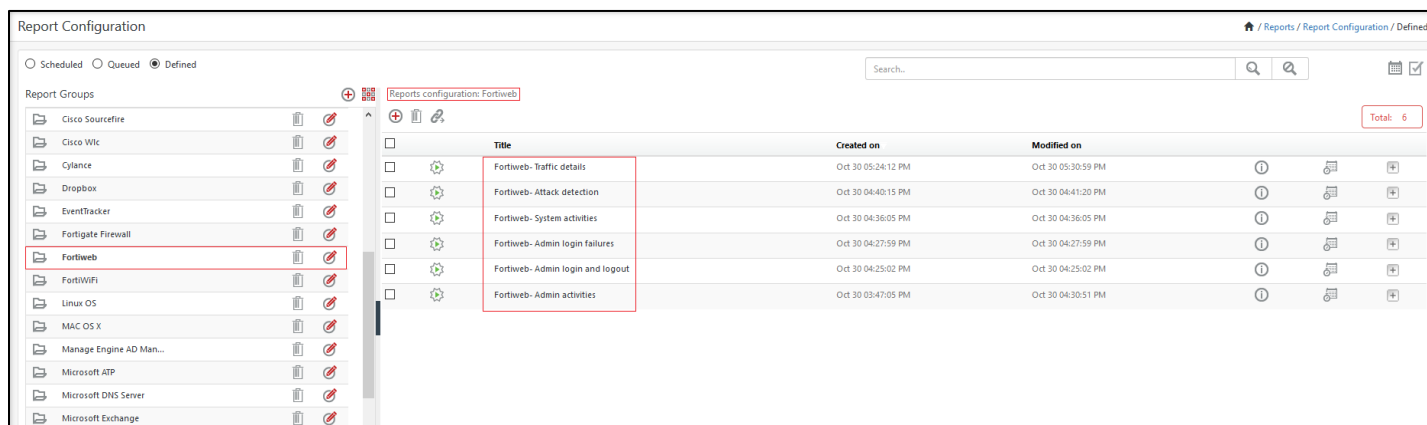


Figure 44

## Dashboard

- **WIDGET TITLE:** FortiWeb- Denied attack trend

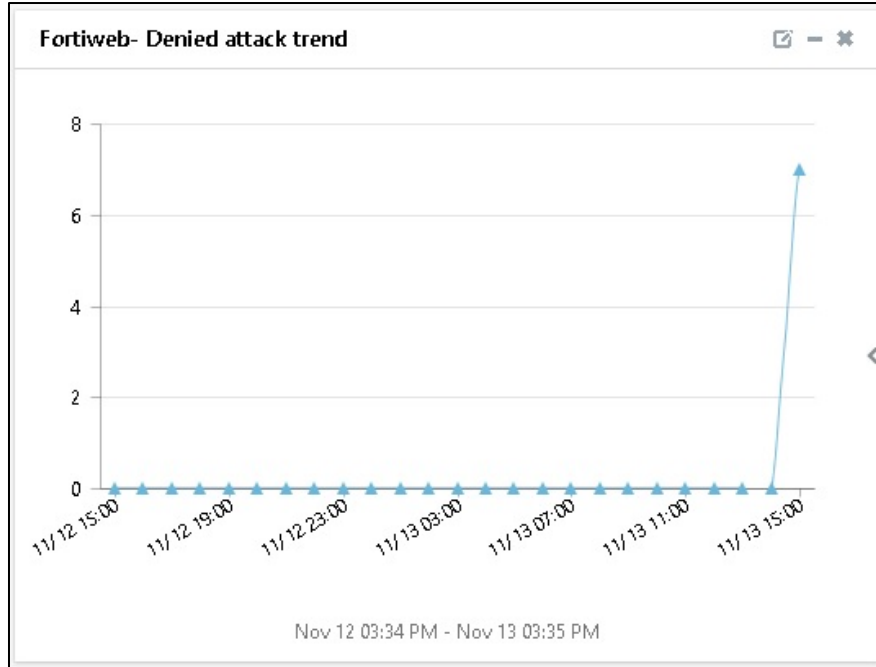


Figure 45

- **WIDGET TITLE:** FortiWeb- Attack detected by Source IP Address

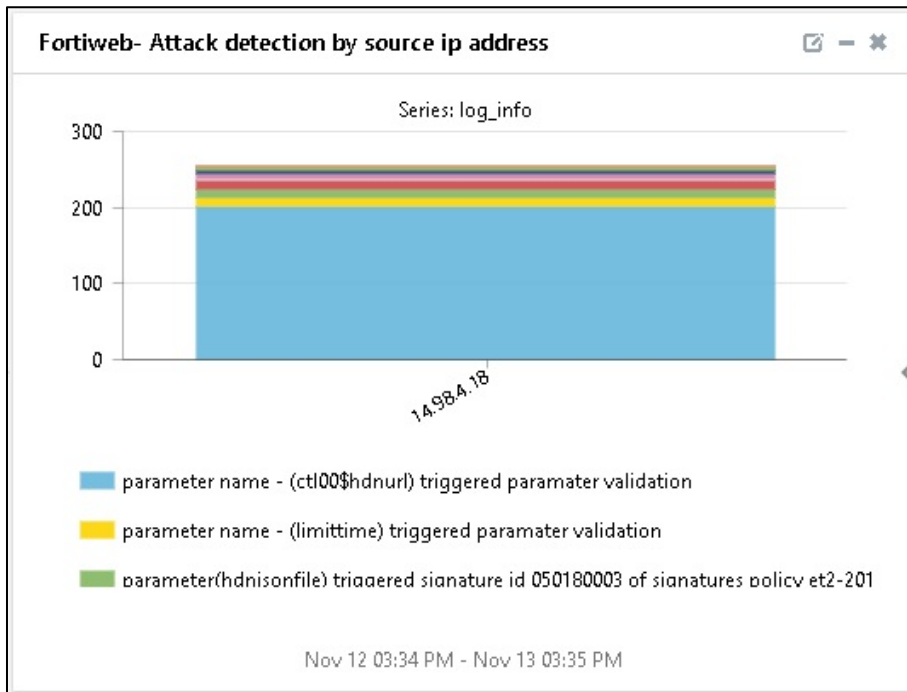


Figure 46

- **WIDGET TITLE:** FortiWeb- Top attacks detected

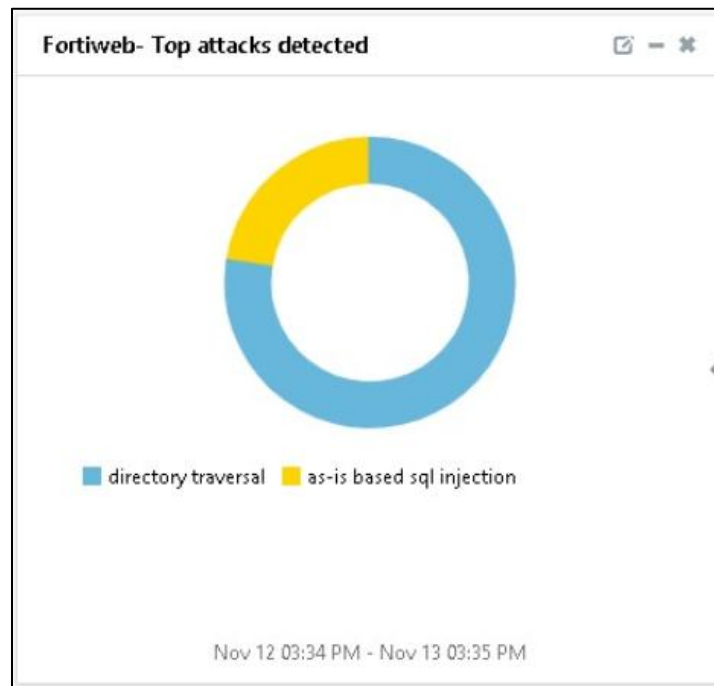


Figure 47

- **WIDGET TITLE:** FortiWeb- Attack detection by destination IP address

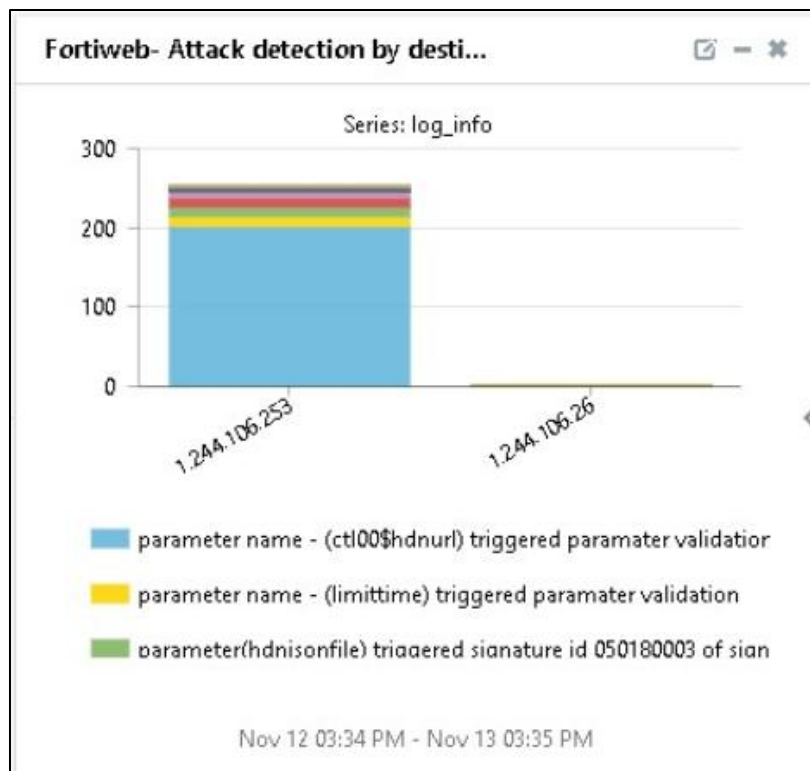


Figure 48

- **WIDGET TITLE:** FortiWeb- Attack detected by geolocation



Figure 49