Netsurion™ | EventTracker

Integrate FortiSandbox with EventTracker

EventTracker v8.0 and above

Publication Date: October 8, 2019

Abstract

This guide helps you in configuring **FortiSandbox v3.1.0** and **EventTracker** to receive FortiSandbox events. You will find the detailed procedures required for monitoring FortiSandbox v3.1.0.

Scope

The configurations detailed in this guide are consistent with **EventTracker v8.x** and later, **FortiSandbox v3.1.0.**

Audience

FortiSandbox users, who wish to forward Events to EventTracker and monitor events using EventTracker.

Table of Contents

1.Overview

FortiSandbox Cloud is a cloud-based managed option for businesses looking for a turnkey solution. It delivers the same rapid detection and automated response as the physical FortiSandbox appliance, but is accessed through the cloud, and provides unlimited flexibility to complement entry and mid-range FortiGates.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2.Prerequisites

- Admin privileges for **FortiSandbox v3.1.0** and should be installed.
- If Firewall existed between **EventTracker** and **FortiSandbox** appliance, please allow for port number 514.

3.Integration of FortiSandbox with EventTracker using syslog

FortiSandbox logs we can get by using syslog.

To create a syslog server:

1. Please login into the FortiSandbox admin portal.
2. Go to **Log & Reports > Log Servers**.
3. Select **+** Create New from the toolbar.
4. Enter the following information.
    - **Name**: Enter a name for the syslog server on **FortiSandbox**.
    - **Type**: Select Log Server Type from the drop-down list as **syslog**.
    - **Log Server Address**: Enter **EventTracker IP** address.
    - **Port**: Enter the syslog server port number **514**.
    - **Status**: Select to **enable** sending logs to the EventTracker.
    - **Log Level**: Please select **Alert logs**, **Critical logs**, **error logs**, **warning logs**, and **information logs.**

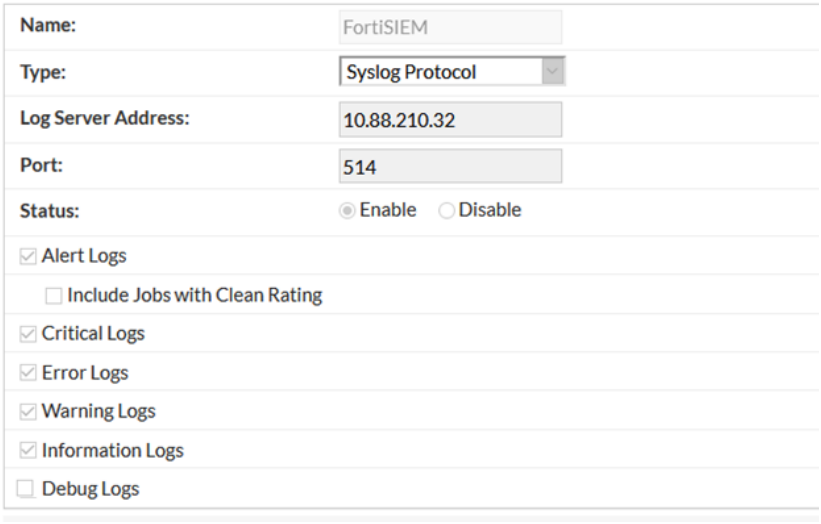

Figure 1

5. Select **OK** to save the entry.

4.EventTracker Knowledge Pack

Once logs are received into EventTracker, Alerts, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Windows.

4.1 Alerts

- **FortiSandbox: Malware detected** – This alert is triggered when a mail attachment has malware files.

4.2 Reports

- **FortiSandbox – Netattack activities** – This report includes the information of virus attack id, malware name, and attachment details.

Sample Report

LogTime	Virus ID	Attack ID	Sorce IP Address and port	Destination IP Address and Port	Host Name	VDOM	Botnet Name
10/03/2019 10:26:56 AM	555739101656	5739161555739101656	209.87.240.248	172.16.32.98	FEVM020000187269	fortisandboxclientsupport.com	WireX
10/03/2019 10:26:56 AM	555739101656	5739161555739101656	209.87.240.248	172.16.32.98	FEVM020000187269	fortisandboxclientsupport.com	Hajime
10/03/2019 10:26:56 AM	555739101656	5739161555739101656	209.87.240.248	172.16.32.98	FSA-FortiDemogate	fortisandboxclientsupport.com	Satori

Figure 2

Log Sample

```
itime=1458669062 date=2016-03-22 time=17:51:02 devid=FEVM020000187269 logid=1220000020 type=netbotnet
subtype=system level=alert virusid=555739101656 attackid=5739161555739101656 srcipport=209.87.240.248
dstipport=172.16.32.98 host=FSA-FortiDemogate attackname=netattack botnetname=PrimeFBA.html
vd=fortisandboxclientsupport.com jstatus=Done
```

- **FortiSandbox – Malware activities** – this report includes the information of attachments has malware attachments, attachment detail.

Sample Report

LogTime	Client Device Name	Destination IP Address	Destination Port Number	File Name	Malware Name	Protocol	Source IP Address	Source Port Number	source User NAme	URL	Virtual Machine OS Name
10/03/2019 10:26:56 AM	FEVM020000187269	209.87.240.248	8613	PrimeFBA.html	W32/ndsa.AVHJ!#tr	tcp	100.26.78.91	2485	maxx	http://xspdj.hyper-s-t-a-r.com/OzmQDtO/AmVAoDV/uOImQAtSHpVotUHtOBqWko1EuXZ2t	WIN7X64VM
10/03/2019 10:26:56 AM	FEVM020000187269	209.87.240.248	8613	Suncorp-payment-4444.zip	W32/Yakes.AVHJ!tr	tcp	100.26.78.91	2485	maxx	http://xspdj.hyper-s-t-a-r.com/OzmQDtO/AmVAoDV/uOImQAtSHpVotUHtOBqWko1EuXZ2t	WIN7X64VM

Figure 3

Log Sample

```
itime=1458669062 date=2016-03-22 time=17:51:02 devid=FEVM020000187269 logid=1215000015 type=Malware
subtype=malware level=alert tzone=UTC clientdev=Demo-FortimailGateway clientvd=fortisolutionsdemo.com
fname=Suncorp-payment-4444.zip jobid=4635327890062625818 md5=d28caf19b453bb1dbeb1714afe74a82b
mname=W32/Yakes.AVHJ!tr proto=tcp risk=W32/Yakes.AVHJ!tr
sha256=ecd65be815acdf0a9690056cd6dca90edcdce23439cfaef92785f2313a7c41f8 scanstart=Sep 25 2019 16:04:36-
07:00 scaned=Sep 25 2019 16:04:37-07:00 srcip=100.26.78.91 srcport=2485 dstip=209.87.240.248 dstport=8613
stype=system suser=maxx
url=http://9.au.download.windowsupdate.com/d/msdownload/update/software/defu/2019/09/am_delta_patch_1.303.479.0_21611cdcdbac339101eefb102b899b29a53a7e6c.exe vd=fortisolutionsdemo.com vmos=WIN7X64VM
jstatus=success
```

- **FortiSandbox – System activities** – This report includes the information of user name, source IP address, destination IP address, access from, sender address, and receiver address.

Sample Report

LogTime	User Name	Blacklist Name	Source IP	Source Port	Email Receiver	Email Sender Address	Destination Port	Destination IP
10/03/2019 10:26:56 AM	admin	Fortiunsafelist	172.98.87.22	6785	jerry@fsb.com	maxx@fsb.com	9877	248.90.67.98
10/03/2019 10:26:56 AM	admin	Fortiunsafelist	172.98.87.22	6785	jerry@fsb.com	maxx@fsb.com	9877	248.90.67.98
10/03/2019 10:26:56 AM	admin	Fortiunsafelist	172.98.87.22	6785	jerry@fsb.com	maxx@fsb.com	9877	248.90.67.98

Figure 4

Log Sample

```
date=2016-03-22 time=17:51:02 tz=PST, PDT user=admin ui=webui action=finished status=activated error=
reason=system activities letype= admin=david blacklist=Fortiunsafelist emailsndr=maxx@fsb.com
emailrcvr=jerry@fsb.com cloneidx= jobcount=17 device=FEVM020000187269 dbid= email=user@fortisandbox.com
etime=Sep 25 2019 16:04:37-07:00 rptfmt= harole= hostname=FEVM020000187269 index= ip= jobtype=
snmpoid=877393c8884b0383ab officekt=text os=WIN7 filepath=.\Demo\Fortisandbox\client pid=9875647380028
pidstatus=done port=8779 quarantine=WEB?!arkLI rpttype= retcode= serial=73664846253899272978 rom=client
sha1=f61045626e5f4f74108fb6b15dde284fe0249370 subject=Pleasecheckthisout.... sharename=FortiSandboxclient
sid=120093745859352 sizebin=14MB sizeconf=824567Bytes snmpaction=allow stime=Sep 25 2019 16:04:37-07:00
susr=jerry urlcat=http://dtat.fortisafe.client.com/?access=acef23.aspx version=3.8 vmname=WIN7CLIENTCON
vmkey=bc89-00ea-9983-cb0f whitelist=fortisafe cip=172.98.87.22 cport=6785 sip=248.90.67.98 sport=9877
service=http ftype=exe rsrc=9.8 fcuid=FCDVEDJSKIKLSJ10034 unauthuser=jack unauthusersource=command line
xforwarded=FortiSandboxconnectivity trueclient=172.67.98.100 session_id=2910828474993
```

4.3 Dashboards

- **FortiSandbox – Top 10 infected attachments Detected** – This dashboard will show attachment names which is infected by malware or virus.

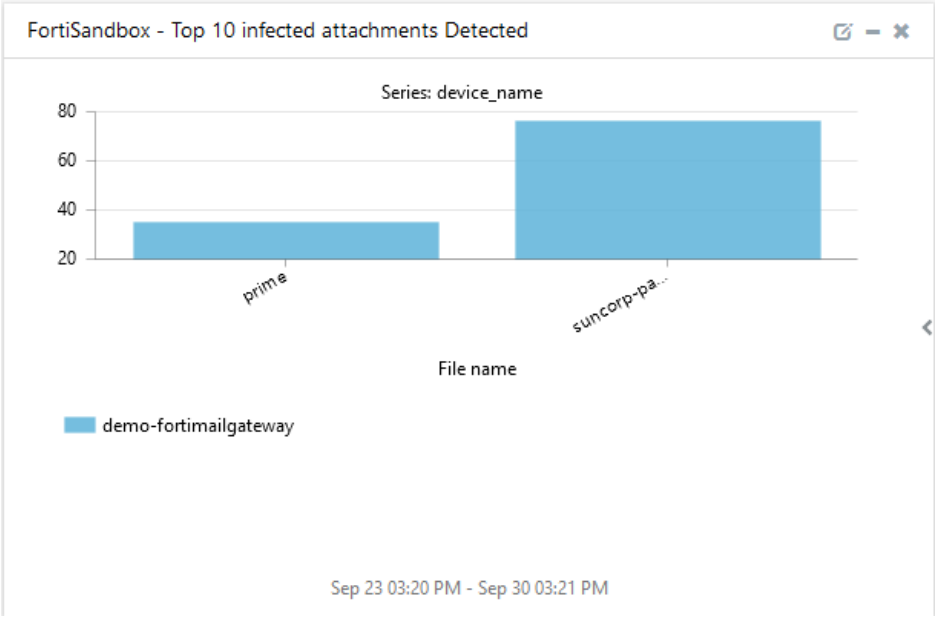

Figure 5

- **FortiSandbox – Mail recipients by sender** – This dashboard will show sender address and receiver address from system activities.

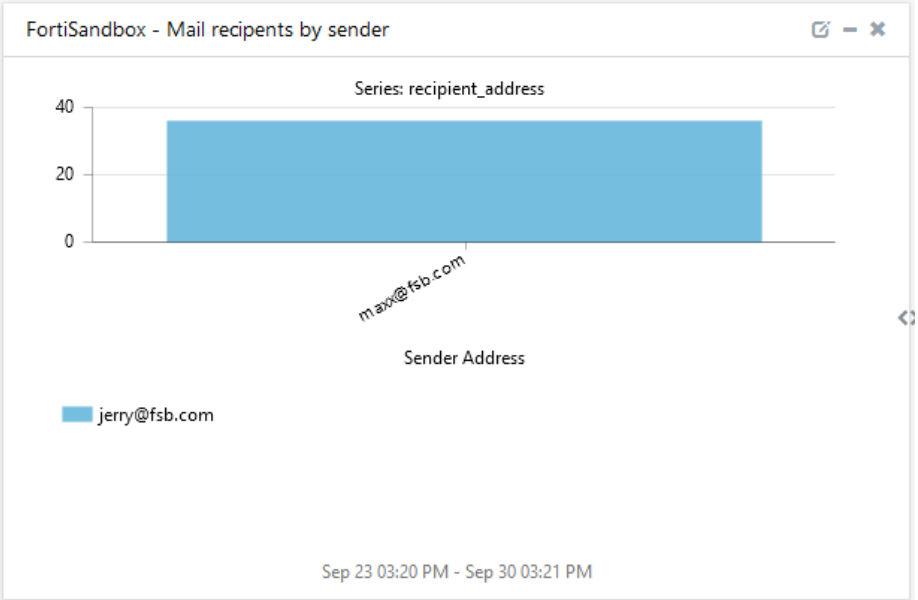

Figure 6

- **FortiSandbox – Top 10 malware attacked on devices –** This dashboard will show which devices have infected malware attachments and attachment names.

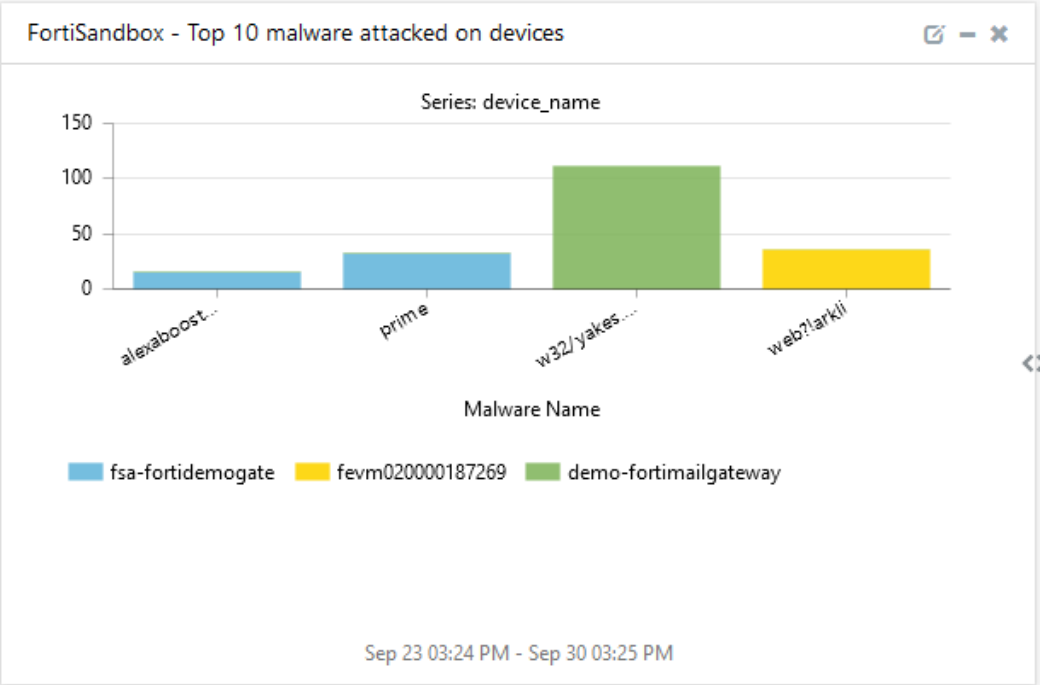

Figure 7

- **FortiSandbox – Top 10 devices infected** – This dashboard will show IP address and device names infected by the virus.

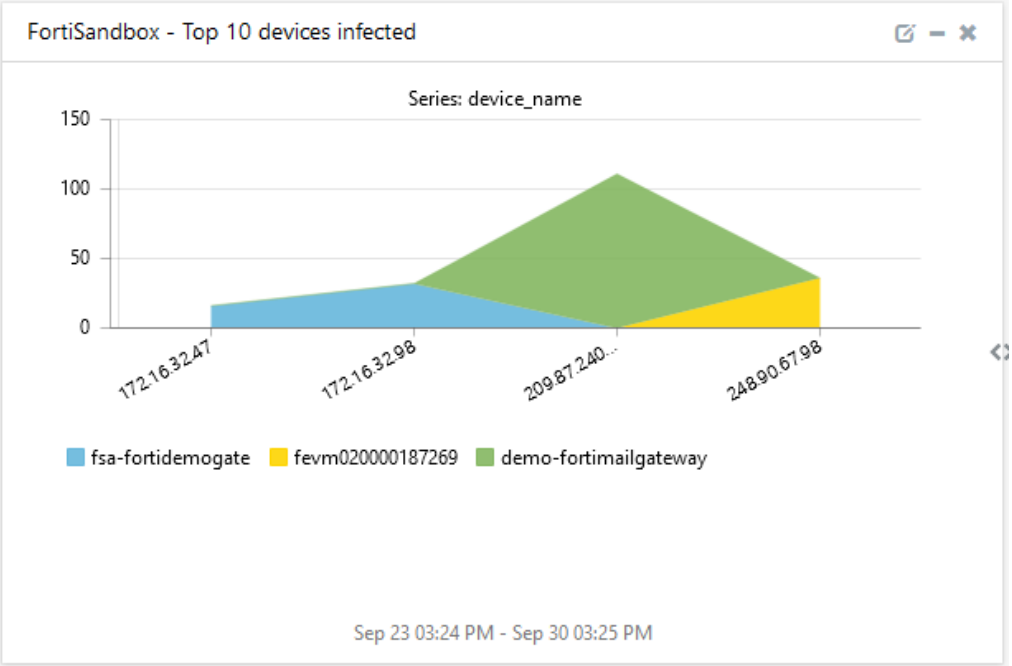

Figure 8

5.Import knowledge pack into EventTracker

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**.

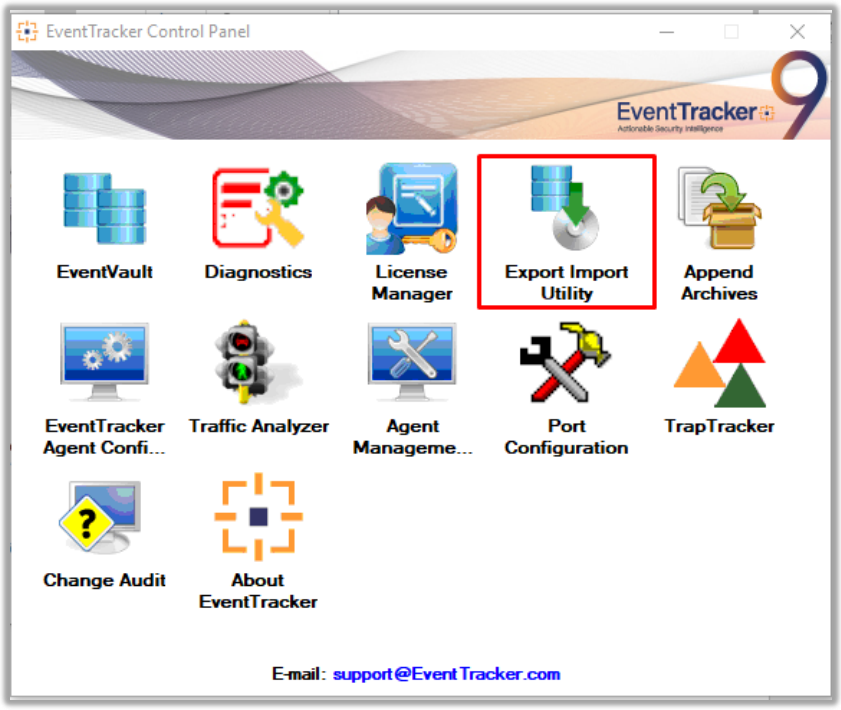

Figure 9

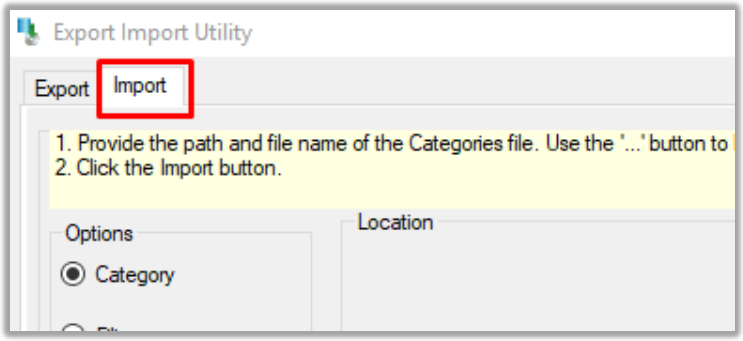

Figure 10

3. Click the **Import** tab.

5.1 Categories

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

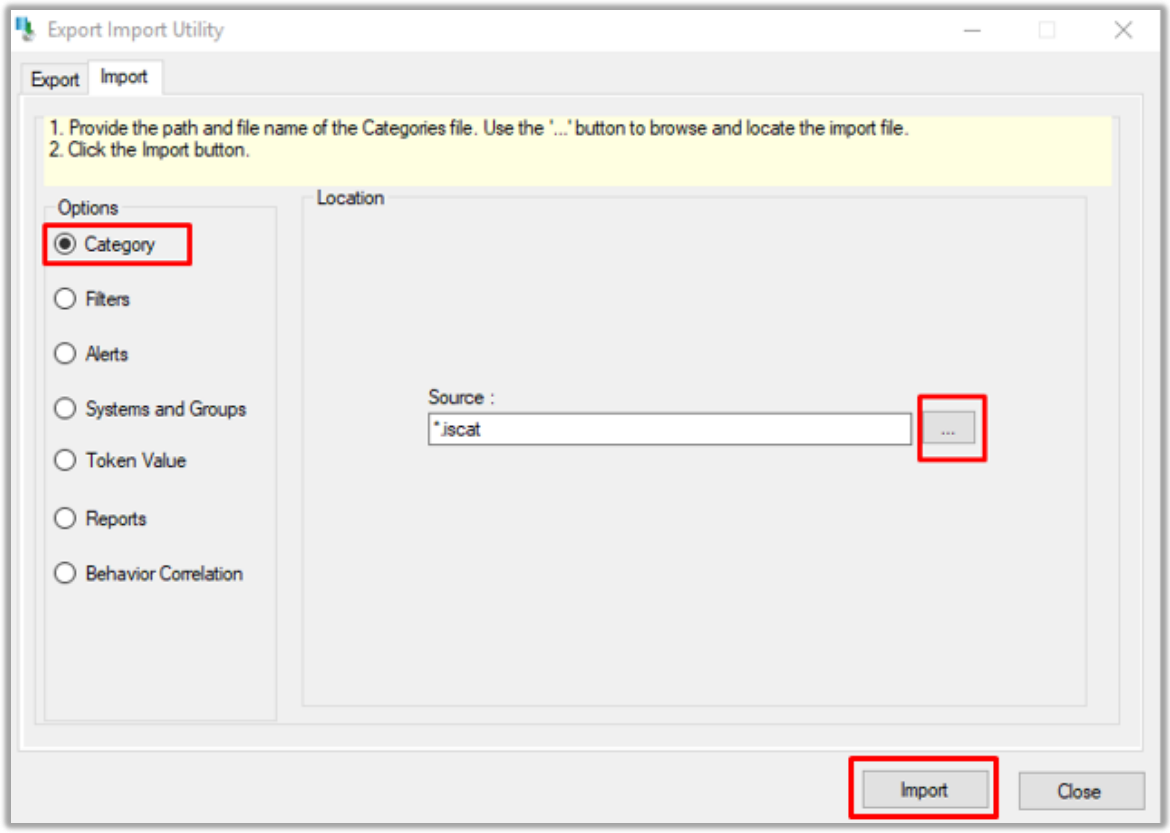

Figure 11

EventTracker displays a success message:

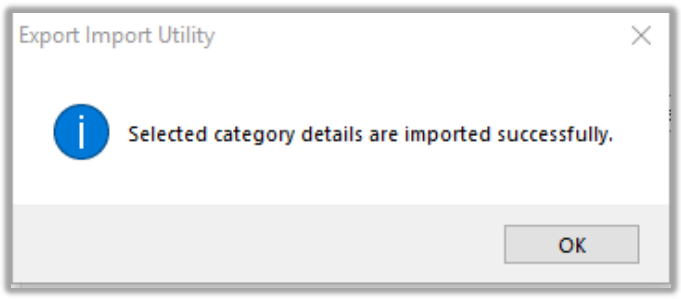

Figure 12

5.2 Alerts

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

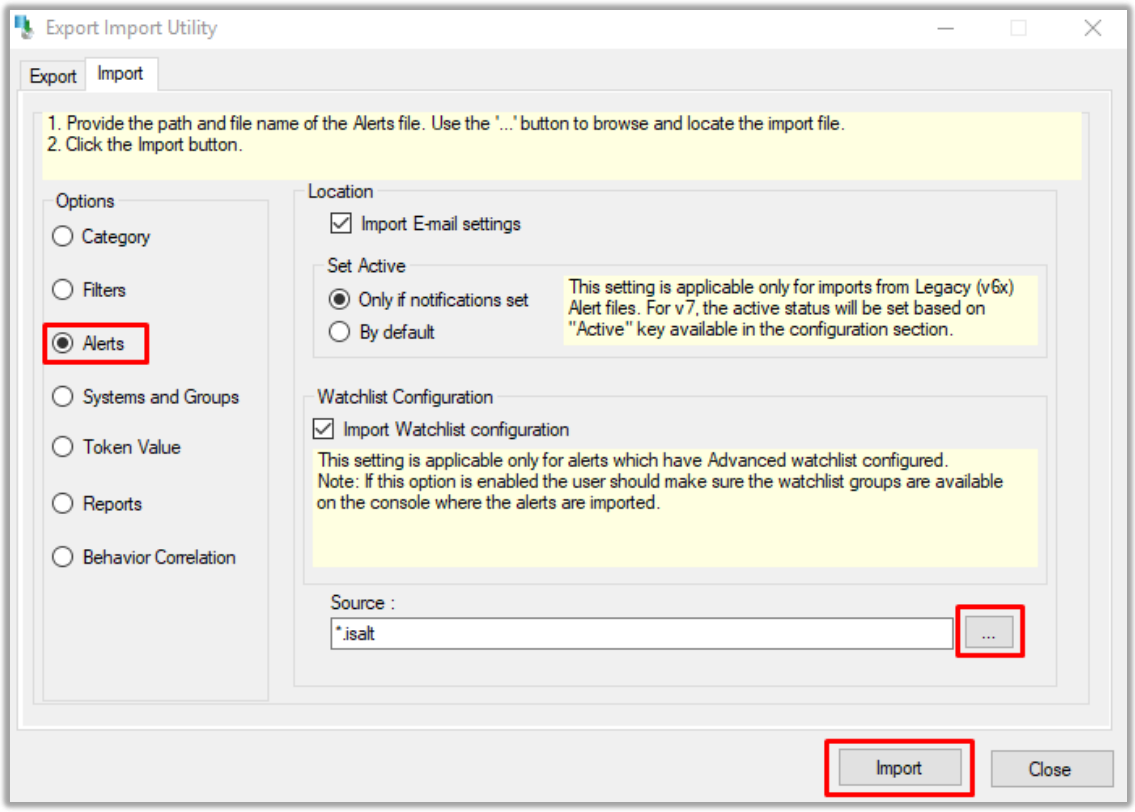

Figure 13

EventTracker displays a success message:

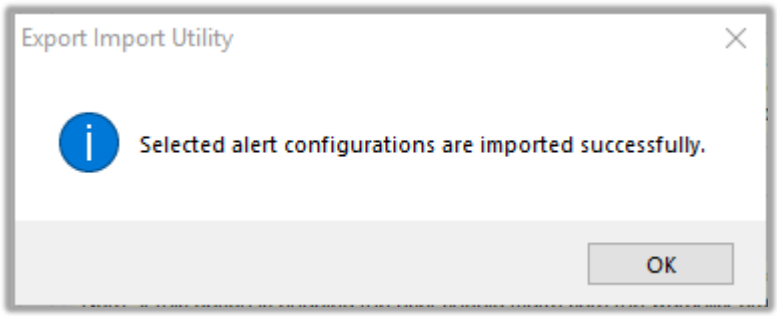

Figure 14

5.3 Token Templates

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

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

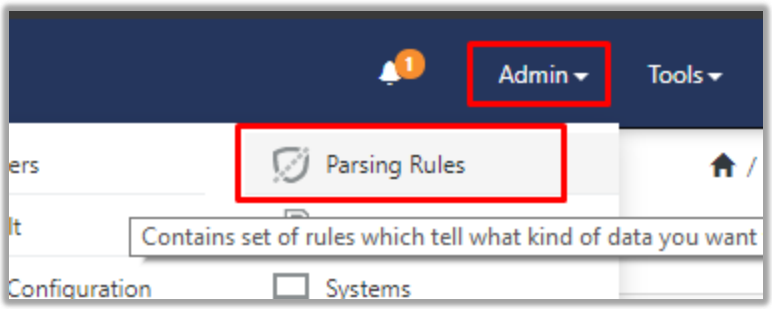

Figure 15

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

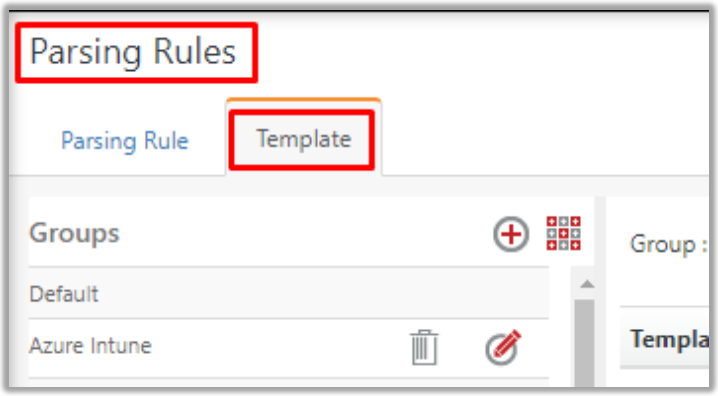

Figure 16

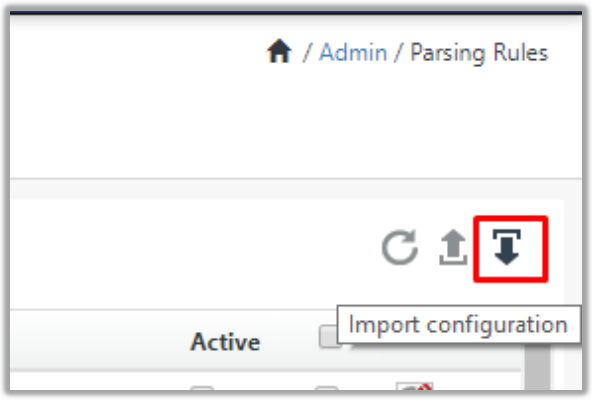

Figure 17

3. Now, click the "**Browse**" button and navigate to the knowledge packs folder (type **C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) where **".ettd", e.g. "Templates_FortiSandbox.ettd"** file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates and click "**Import**" button:

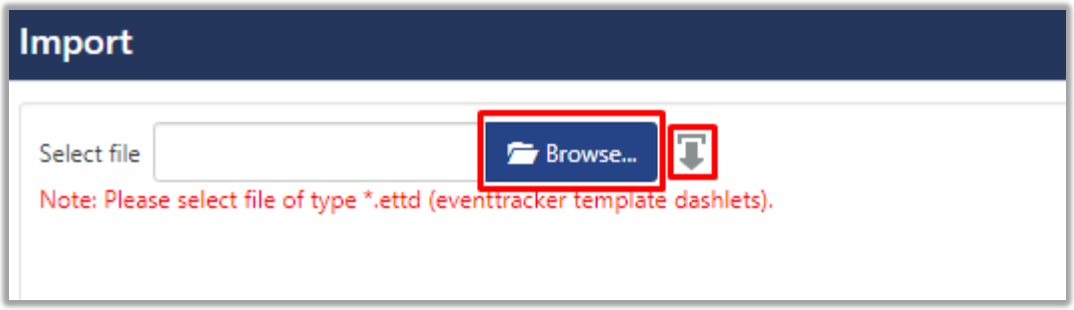

Figure 18

5.4 Flex Reports

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

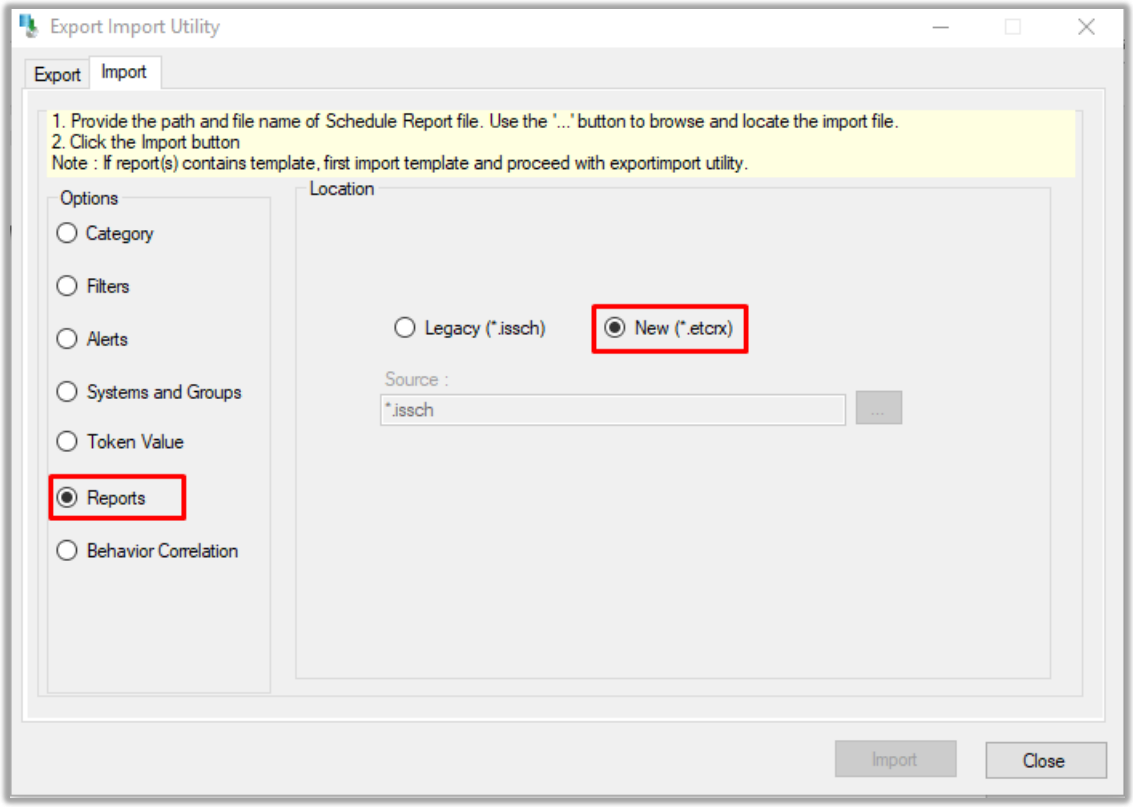

Figure 19

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

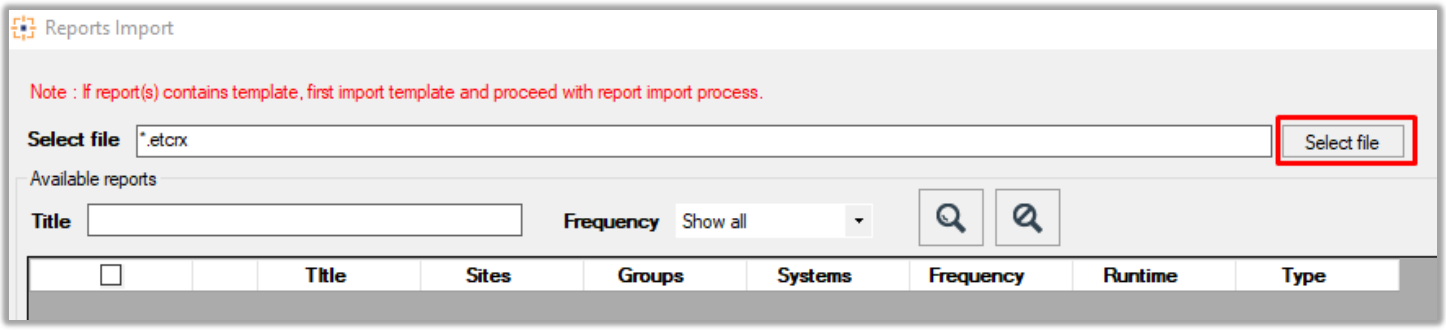

Figure 20

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

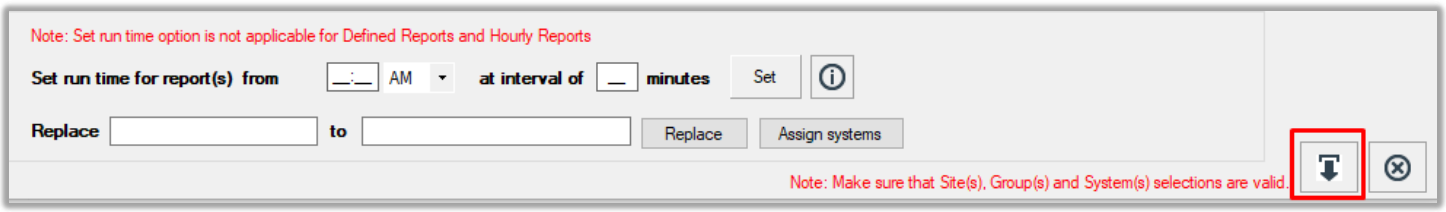

Figure 21

EventTracker displays a success message:

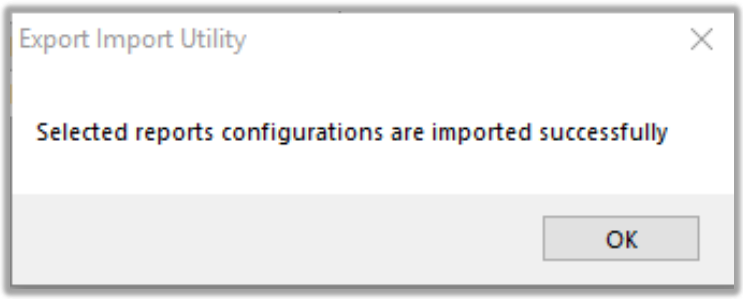

Figure 22

5.5 Knowledge Objects

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

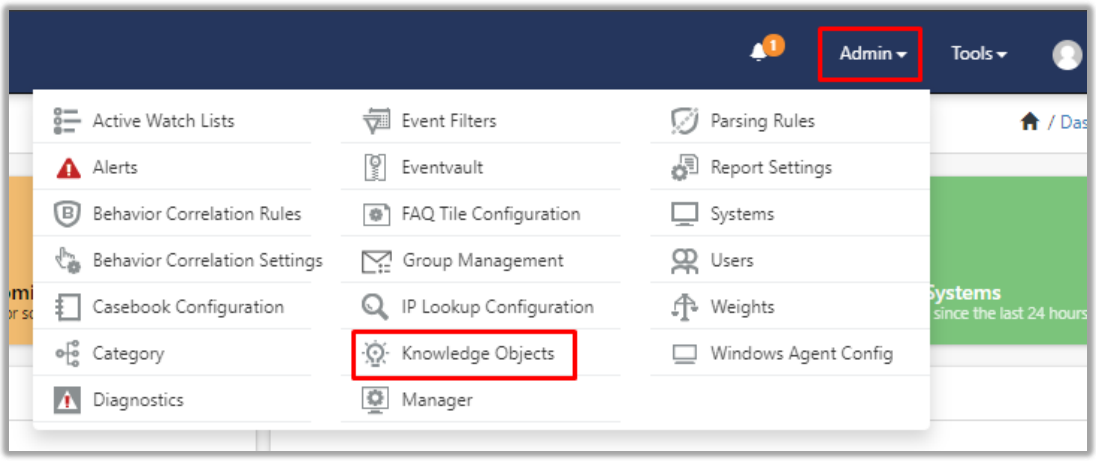

Figure 23

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

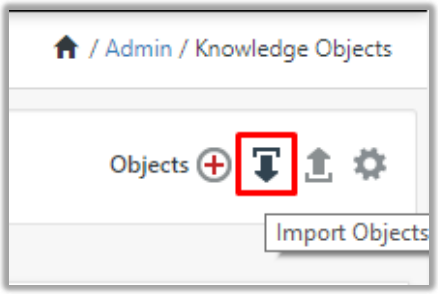

Figure 24

3. A pop-up box will appear, click "**Browse**" in that and navigate to knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g. "KO_FortiSandbox.etko"** and then click "**Upload**" button.

Figure 25

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

Figure 26

5.6 Dashboards

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

Figure 27

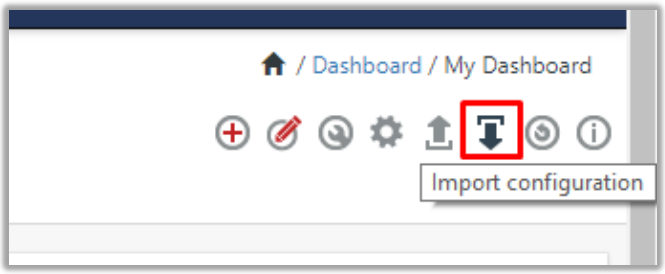

Figure 28

4. Select the **browse** button and navigate to the knowledge pack folder (type **"C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs"** in the navigation bar) where "**.etwd**", **e.g.** "**Dashboard_FortiSandbox.etwd**" is saved and click on "**Upload**" button.

5. Wait while EventTracker populates all the available dashboards. Now, choose "**Select All**" and click on **"Import"** Button.

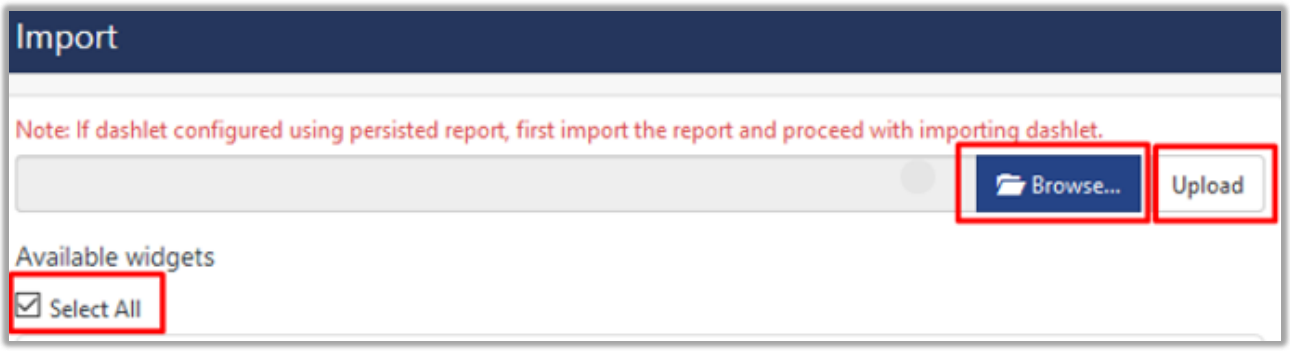

Figure 29

Figure 30

6.Verify knowledge pack in EventTracker

6.1 Categories

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

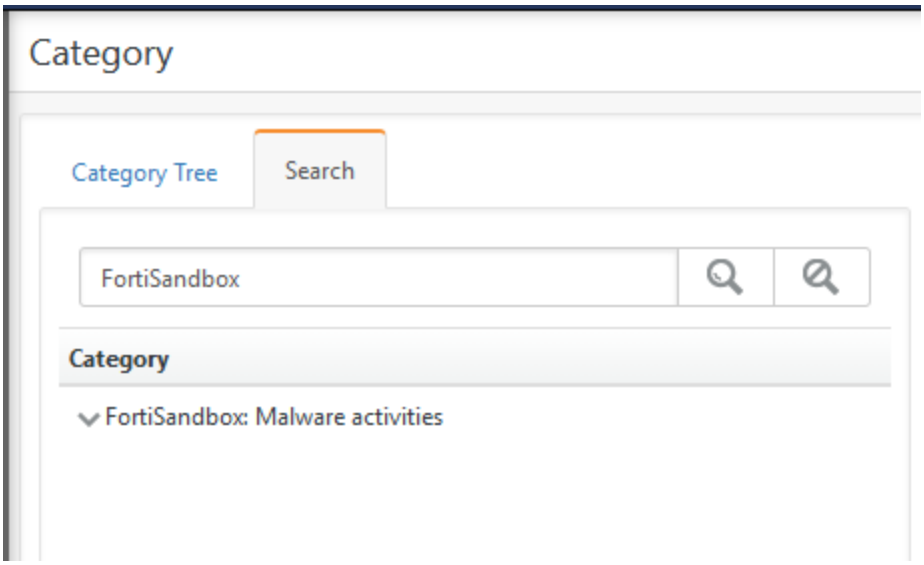

Figure 31

6.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box enter **"FortiSandbox"** and then click the **Search** button.
   EventTracker displays an alert related to the Oracle database**:**

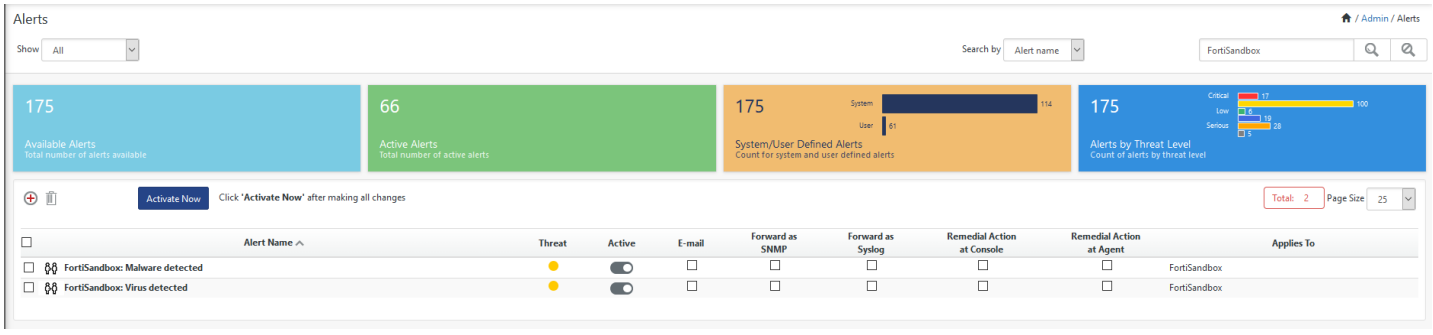

Figure 32

6.3 Token Templates

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

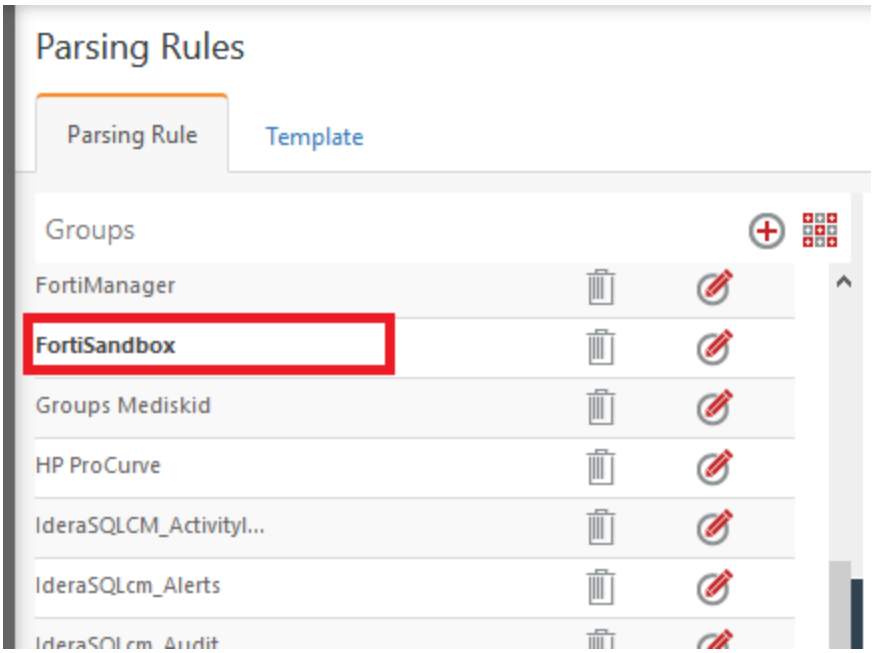

Figure 33

6.4 Flex Reports

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

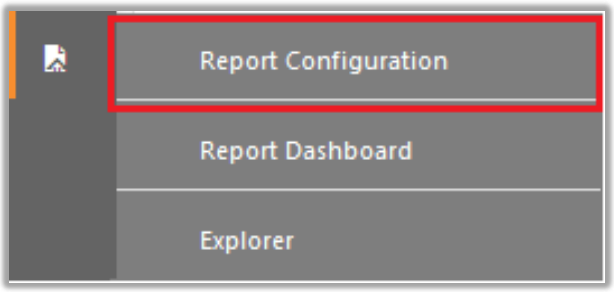

Figure 34

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

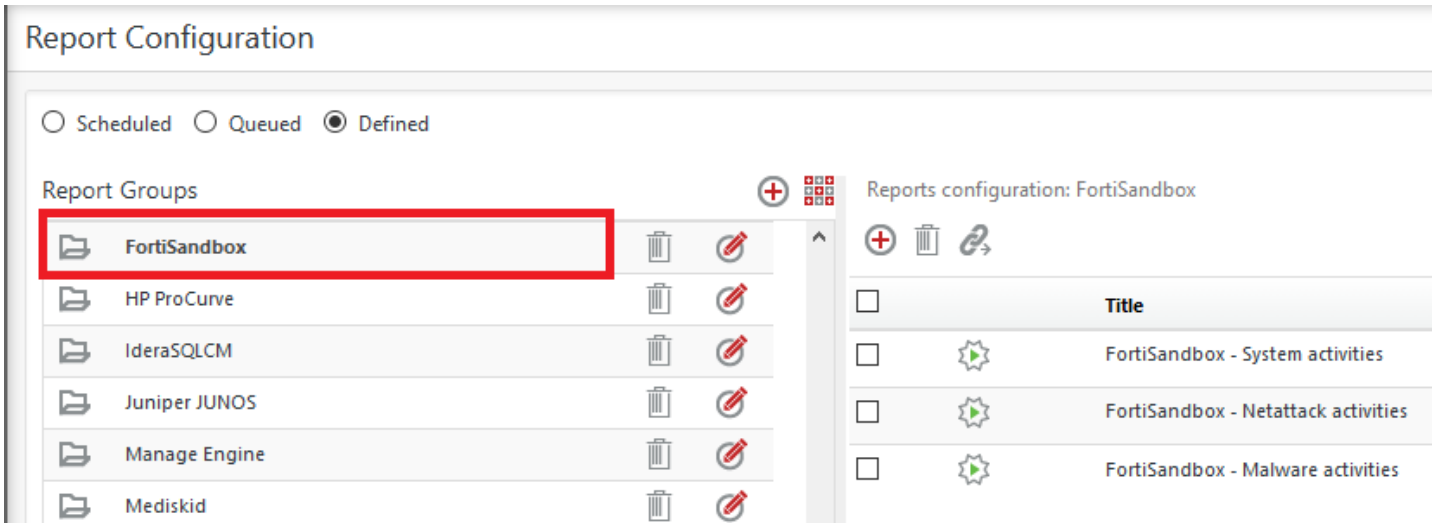

Figure 35

6.5 Knowledge Objects

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

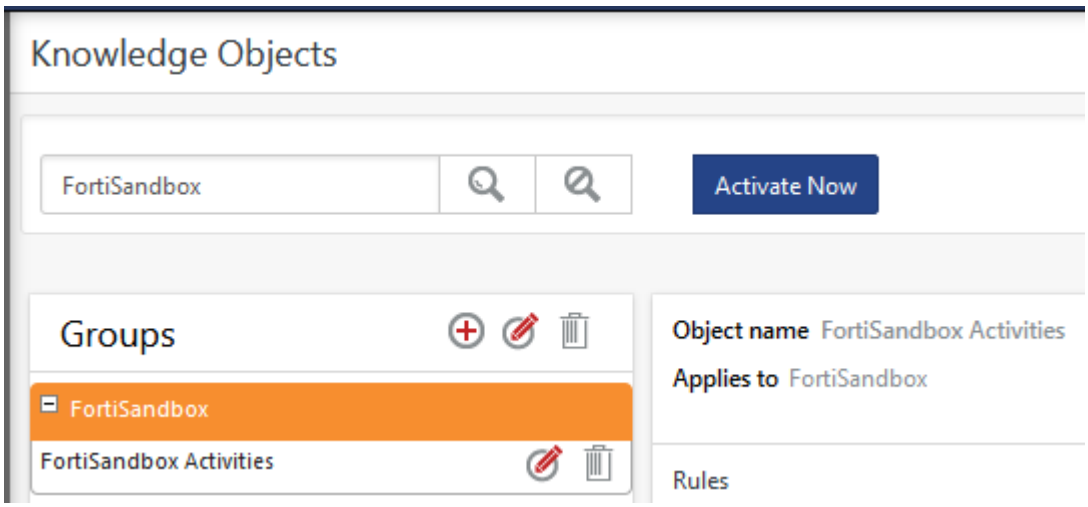

Figure 36

6.6 Dashboards

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

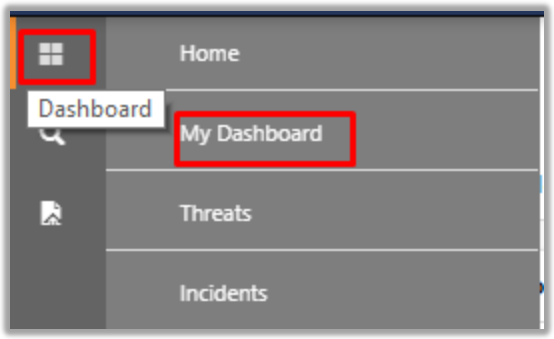

Figure 37

2. In "**FortiSandbox"** dashboard you should be now able to see something like this:

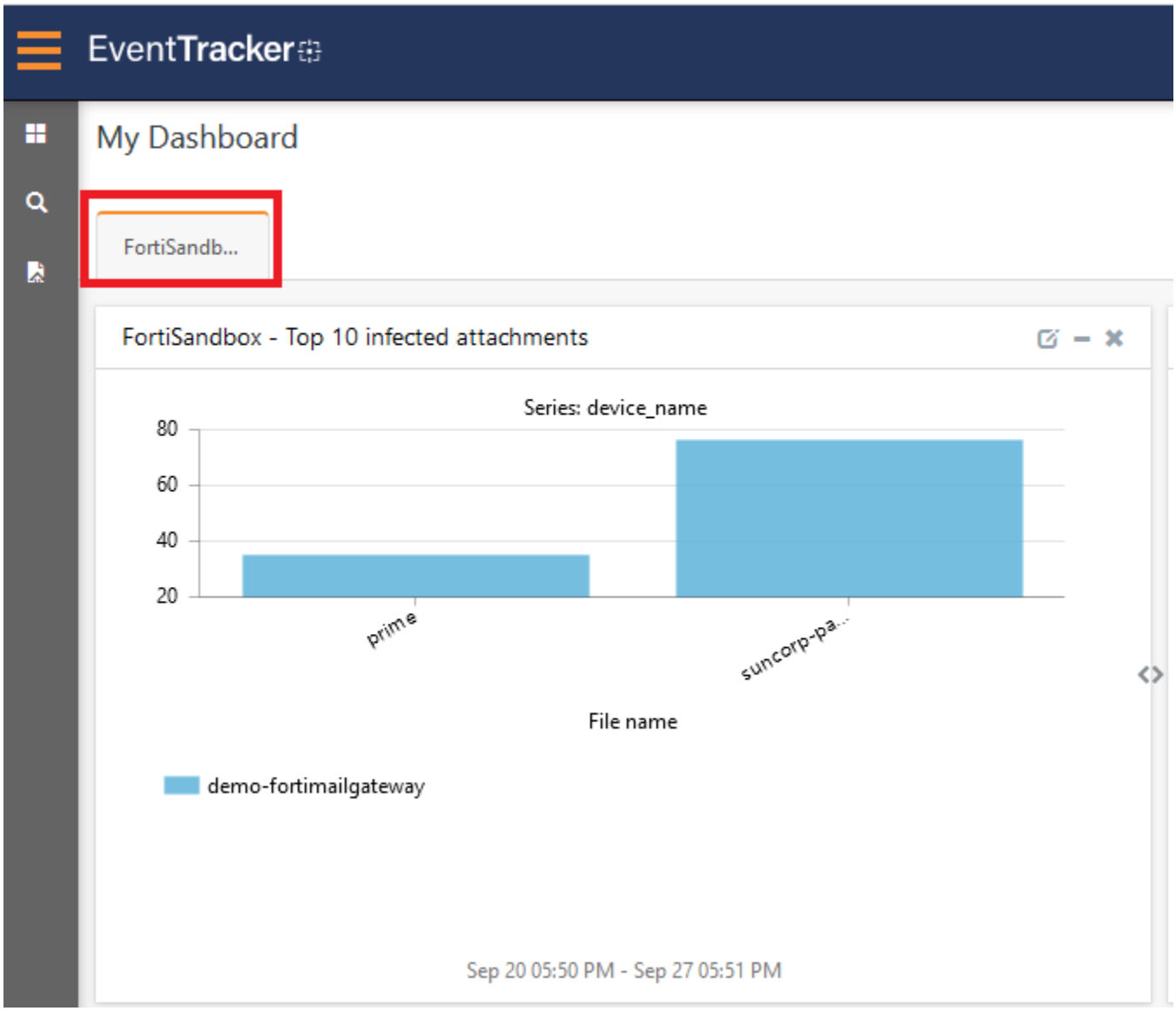

Figure 38