Netsurion | EventTracker®

Integration Guide for NetMotion Mobility

EventTracker v9.x and later

Publication Date: April 16, 2020

Abstract

This guide provides instructions to retrieve the **NetMotion Mobility** events by syslog configuration. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **NetMotion Mobility**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **NetMotion Mobility.**

Audience

Administrators who are assigned the task to monitor **NetMotion Mobility** events using EventTracker.

Table of Contents

1. Overview

NetMotion Mobility is a mobile VPN software, designed specifically for wireless environments. NetMotion Mobility provides IT managers with the security and centralized control to effectively manage a mobile deployment.

EventTracker, when integrated with NetMotion Mobility, collects log from NetMotion Mobility and creates a detailed reports, alerts, dashboards and saved searches. This KP (knowledge Pack) provides detailed information about the User logon failure, in real time. It is helpful to investigate and take responsive actions against Brute-Force Attack.
EventTracker provides a thorough information about policies such as pending policies that must be applied and the policies that have been applied. It also provides information related to Proxy events which contain many important information such as source user, source IP address and session ID. Sessions can be monitored to identify details of user logon and logoff success required for Auditing.
Alerts are provided for critical events such as user logon failure to identify logon attempt. Using the EventTracker's Dashboards we can view and monitor events like user logon events (success, failed), user policy details, user/group management, etc.

2. Prerequisites

- EventTracker manager v9.x is required.
- Enable external logging on your **NetMotion Mobility** appliance.
- Allow Port 514 in the firewall.

3. Integrating NetMotion Mobility with EventTracker

NetMotion Mobility can be integrated with EventTracker using syslog forwarding.

3.1 Configuring a Syslog Server

The NetMotion Mobility server can send NetMotion Mobility events to EventTracker. NetMotion Mobility support for syslog is only implemented on the NetMotion Mobility server; the NetMotion Mobility client cannot log messages to a syslog server.

To log NetMotion Mobility events to EventTracker:

1. Go to **Mobility console > Configure > Server Settings**.
   In the left-hand pane, select the level at which you want to configure logging:
   - To apply the setting to all Mobility servers in a server pool, select **Global Server Settings**.

- To apply the setting to a single server, select the name of the Mobility server you want to configure. Settings applied at the server level take precedence over global settings.

Configure the following settings:

- Select **Syslog - On/Off,** and then select the Turn syslog event logging on check box. This enables a Mobility server to log Mobility events to a syslog server. Any information, warning, or error events that are recorded in the Mobility event log are also sent to syslog. However, the Mobility server does not log debug events to syslog. To record debug events, use the Mobility event log.
- Select **Syslog - Server Host**. In the Host box, enter the **host name** or **IP address** of the **EventTracker**.

2. By default, the syslog protocol uses UDP **port 514**. To configure the Mobility server to use a different port, select Syslog - Server Port in the list of settings. In the Port box, enter the syslog server port.

3. In a syslog message, the facility identifies the type of software component that generated the message. Some facilities are reserved for the operating system, or for types of applications (for example, email). Applications that are not assigned a facility can use a "local use" facility, which is not reserved.

4. EventTracker Knowledge Packs

4.1 Alerts

Alerts are triggered when an event received is identified as critical and requires immediate notification. Such as,

- **NetMotion – Login Failure –** This alert is triggered when the NetMotion Mobility detects a login failure event.

4.2 Saved Searches

- **NetMotion – Login Failed:** This Saved Search provides information related to a login failure event. It includes information such username, hostname and the reason for login failure.
- **NetMotion – Login Logout Events:** This Saved Search provides information related to login and logout events generated by NetMotion Mobility.
- **NetMotion – Policy Activities –** This Saved Search provides information related to Policy activities.
- **NetMotion – Proxy Event:** This Saved Search provides information related to Proxy Activities.
- **NetMotion – Directory Activity –** This Saved Search provides information related to directory activities such as user added or deleted from group etc.

4.3 Reports

- **NetMotion – Login Failed:** This report generates a summary of login failure event. It includes information such username, hostname and the reason for login failure.

LogTime	Computer	Username	Hostname	Reason
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	AD\James	IFS-HP-REMOTE3	The user name or password is incorrect
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	AD\Adam	IFS-HP-REMOTE2	The user name or password is incorrect
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	AD\Leo	UTL18106L	The user name or password is incorrect
04/09/2020 01:01:44 PM	172.27.100.9-SYSLOG	AD\James	IFS-HP-REMOTE3	The user name or password is incorrect

Figure 1

- **NetMotion – Login Logout Events:** This report generates a summary of login and logout events generated by NetMotion Mobility. It includes username, roles of the user group the user belongs to, and the action performed i.e. login or logout.

LogTime	Computer	Username	Role	Group	Action
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\administrator	Super User		logon
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\Adam	Super User		logon
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\Joey	Client Administration	is_admin	logged on
04/09/2020 01:01:43 PM	172.27.100.9-SYSLOG	ad\administrator			logged off
04/09/2020 01:01:44 PM	172.27.100.9-SYSLOG	ad\administrator	Super User		logon
04/09/2020 01:01:44 PM	172.27.100.9-SYSLOG	ad\Leo	Client Administration	is_admin	logged on

Figure 2

- **NetMotion – Policy Activities –** This report contains a summary of Policy activities. It includes the username, device on which the policy was applied and the name of the policy along with the message regarding the status.

LogTime	Computer	Username	Device	Policy	Message
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\Joey	01D602C4C6BE193900505697E7B 2020		Client not subscribed to a policy and is already running without policy, no policy download will be attempted
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\Adam	01D5FC688808EEE000505697E7B 200B	Global_Policy	Policy (Global_Test_Policy), NAC (None) on client is current, it will not be downloaded
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\Mike	01D5FC688808EEE000505697E7B 200B	Admin_Policy	Policy (Global_Test_Policy), NAC (None) on client is current, it will not be downloaded

Figure 3

- **NetMotion – Proxy Event:** This report has a summary of Proxy activities. This includes hostname, session ID, Message, source IP address and the username.

LogTime	Computer	Hostname	IMP Session ID	Message	Reason	Source IP Address	Username
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	UTL18061L	0xebeaf4a	Client PID request			
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG			Client PIDGEN RPC session indication			
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebe9f4a	[605] Client XG RPC session indication		10.30.99.30	AD\Martin
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebe944a	[601] Client XG RPC session termination indication	A server session was terminated because the client has established a new connection from the same device	10.30.99.30	
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebeae4a	[604] Client XG RPC session indication		10.30.99.19	AD\Adam
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0x000000000ebe9e4a	Client PID accept			
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebea34a	\[597\] Client XG RPC session indication		10.30.99.35	AD\Joey
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebea14a	\[596\] Client XG RPC session termination indication	The Mobility Client is shutting down or restarting	10.30.99.35	
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG		0xebebe4a	\[617\] Client XG RPC session indication	User-initiated disconnect	10.30.99.57	AD\Ross

Figure 4

- **NetMotion - Directory Activity –** This report consists summary of Directory activities. It includes username, group on which the action was taken and the status.

LogTime	Computer	Username	Group	Action
04/12/2020 07:39:14 PM	172.27.100.9-SYSLOG	AD\John	New Users	added
04/12/2020 07:39:15 PM	172.27.100.9-SYSLOG	AD\Adam	New Users	added

Figure 5

4.4 Dashboards

- **NetMotion: Login Failure**

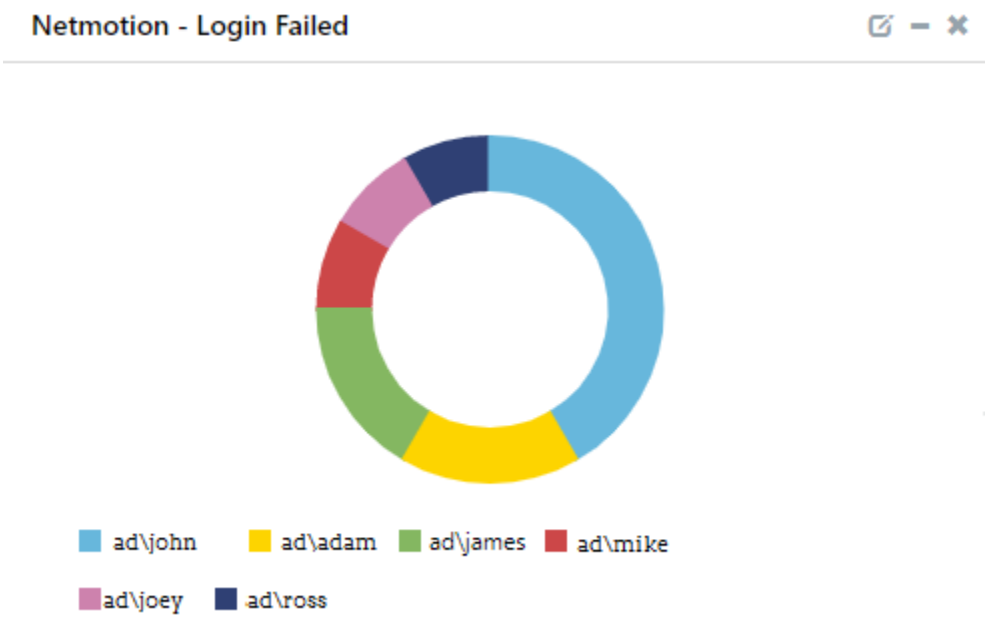

Figure 6

- **NetMotion: Login Logout Activities**

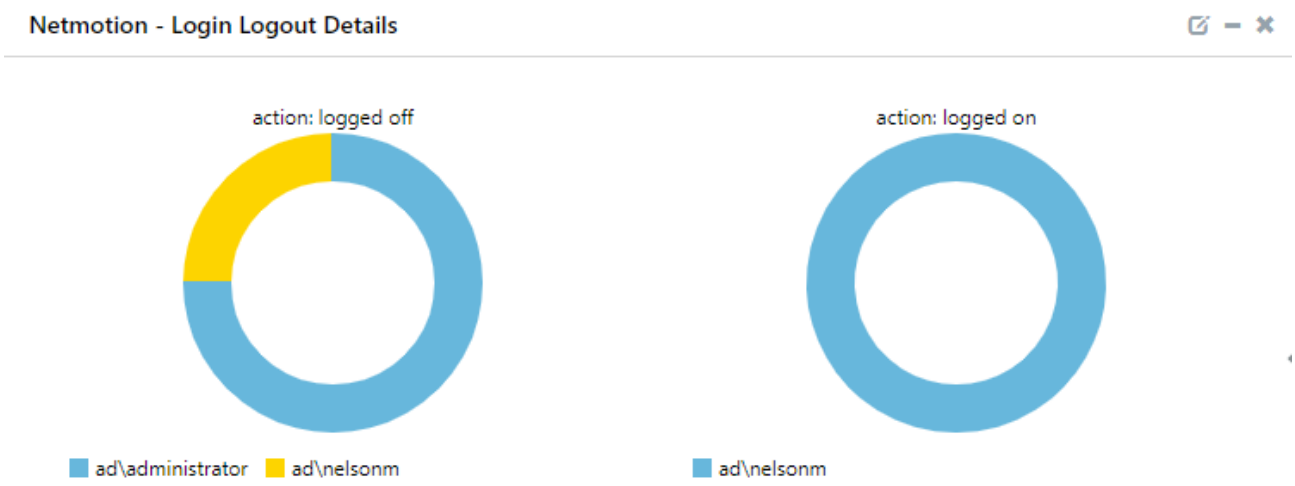

Figure 7

- **NetMotion: Policy Details**

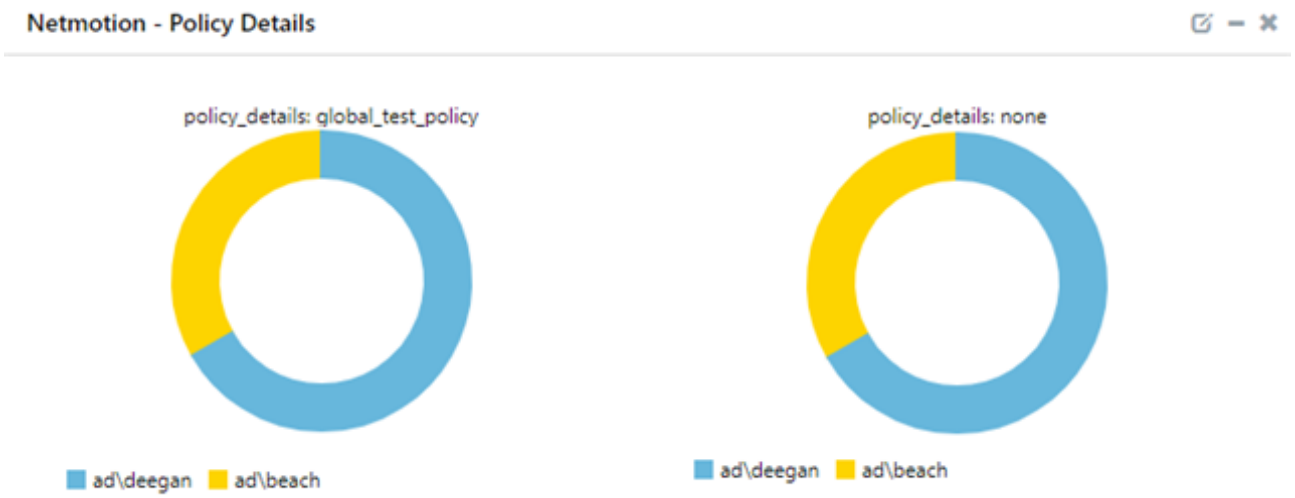

Figure 8

- **NetMotion: IMP Authentication by Geo Location**

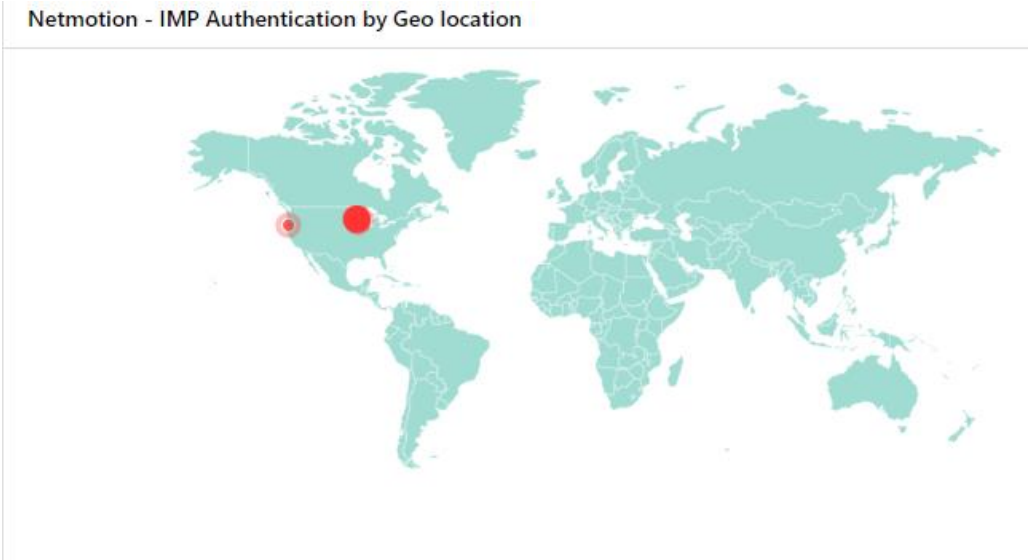

Figure 9

- **NetMotion: User added to group**

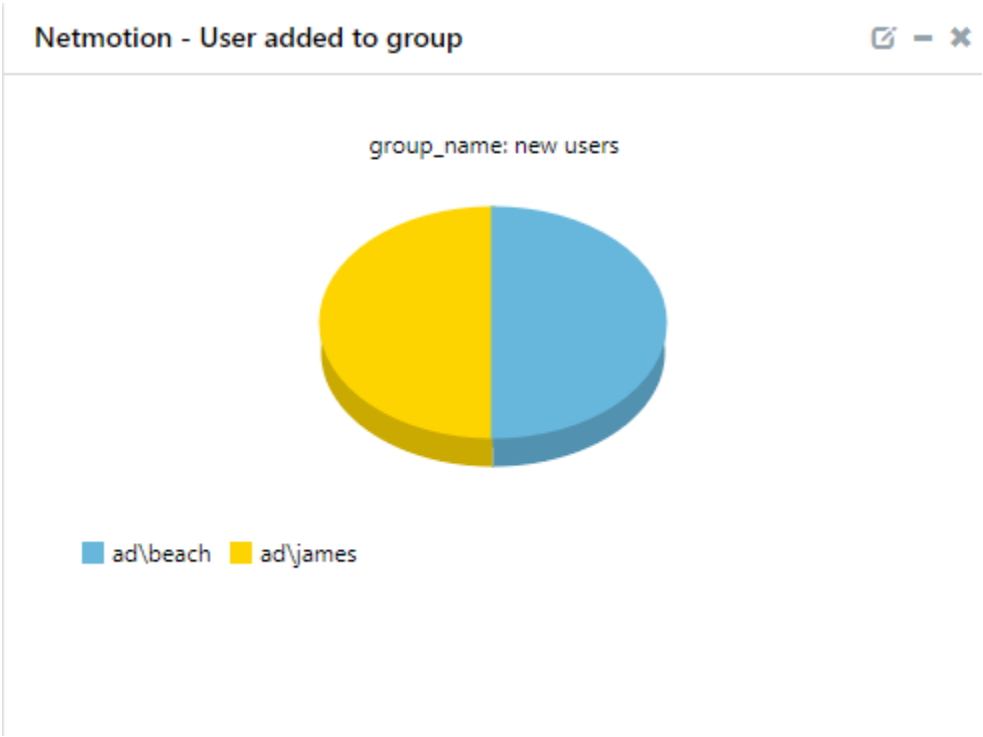

Figure 10

- **NetMotion: Proxy Login Logout Details by Source IP**

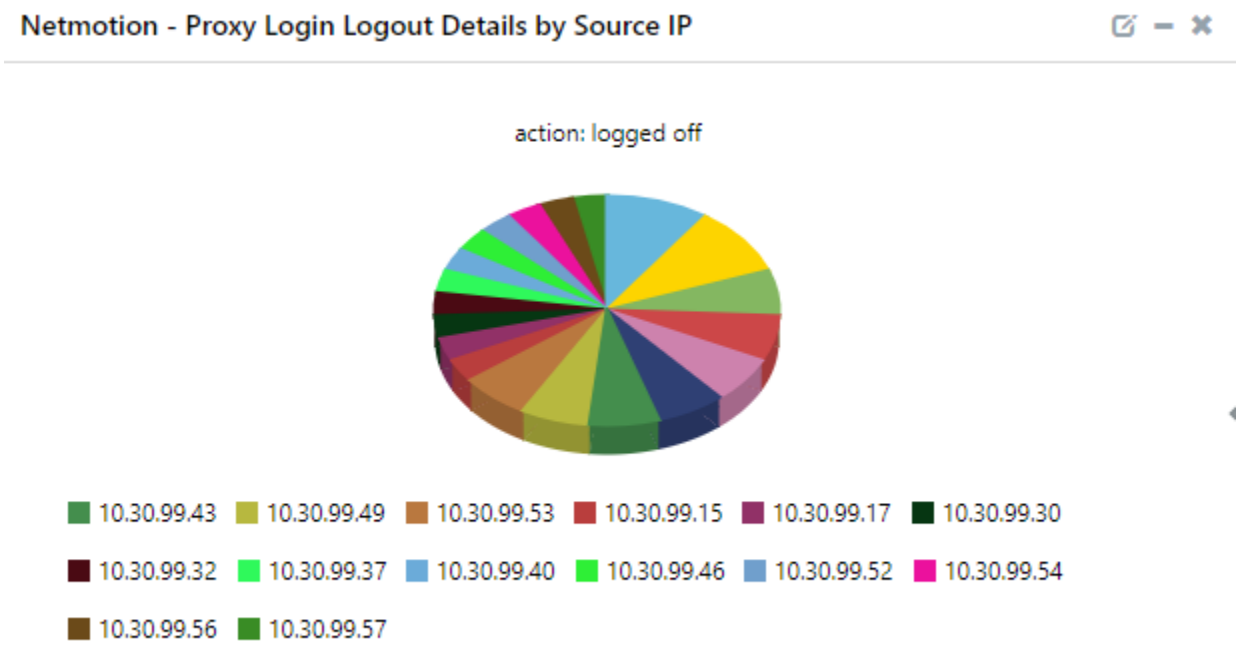

Figure 11

5. Importing knowledge pack into EventTracker

How to get Knowledge Packs

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**.

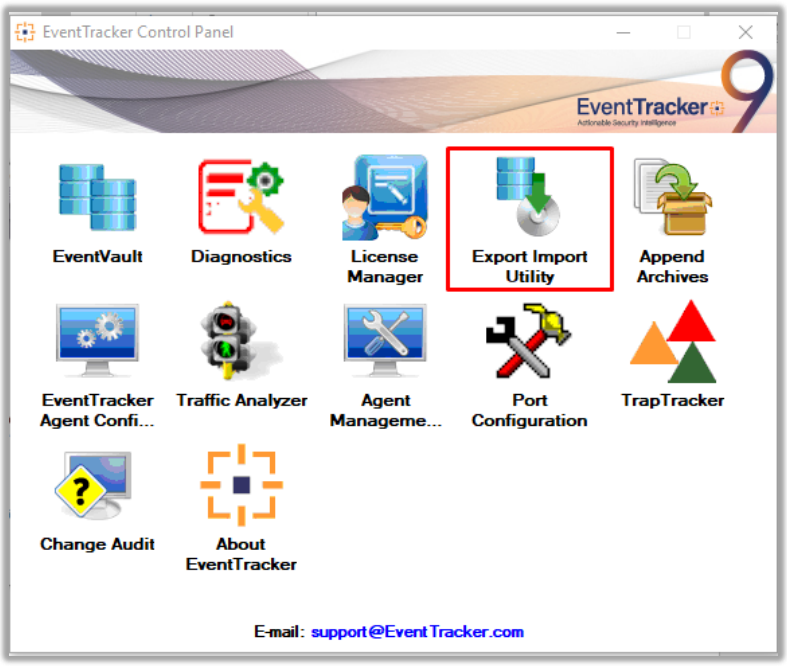

Figure 12

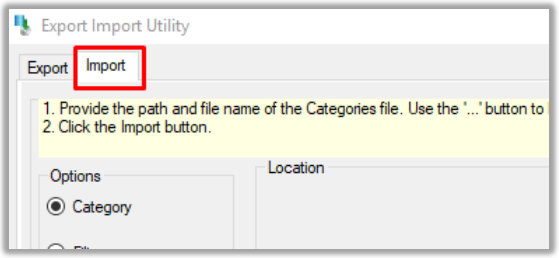

Figure 13

3. Click the **Import** tab.

5.1 Saved Searches

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", e.g. "Categories_NetMotion.iscat"** and then click "**Import**".

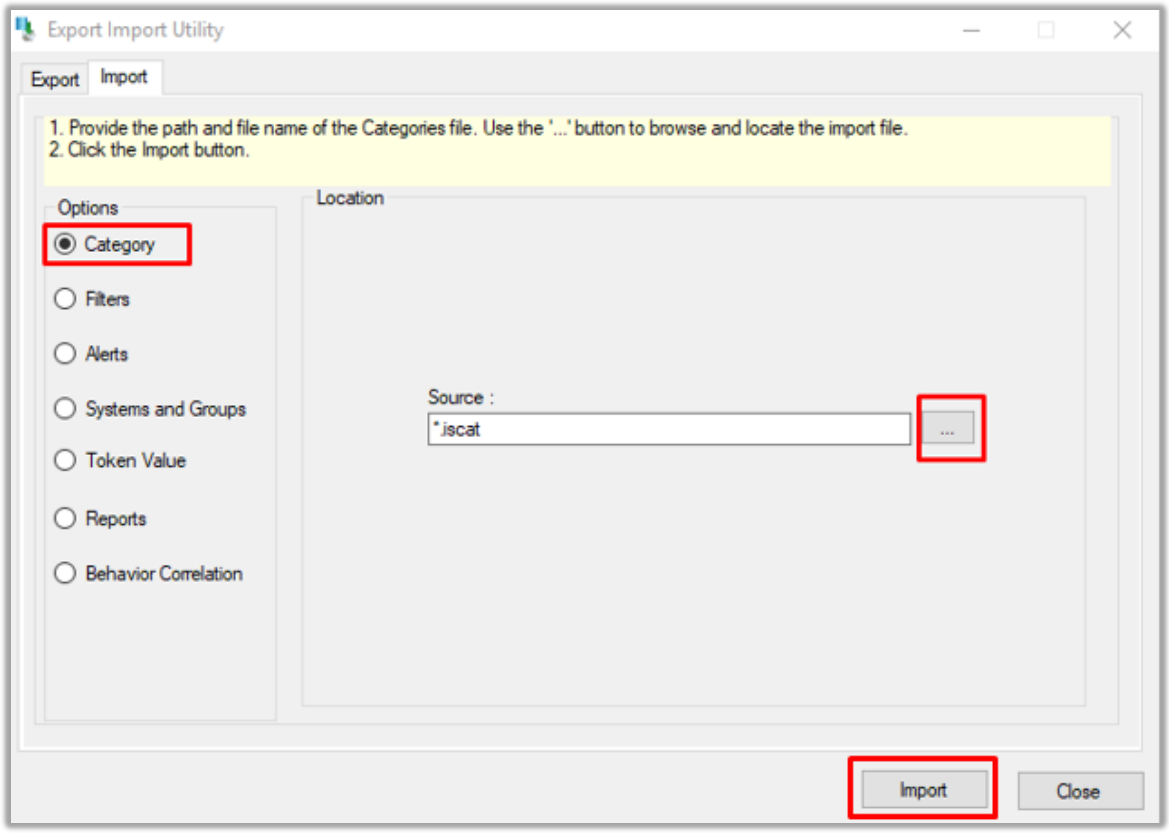

Figure 14

EventTracker displays a success message:

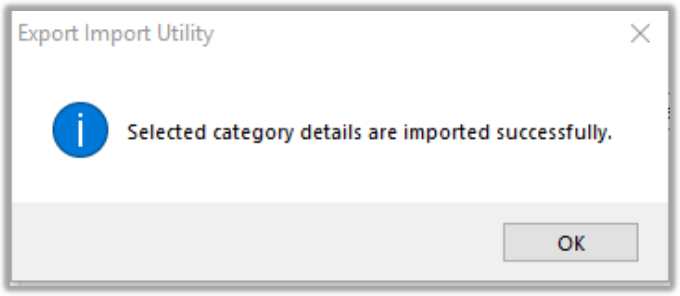

Figure 15

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"**, **e.g.** "**Alerts_ NetMotion.isalt**" and then click "**Import**":

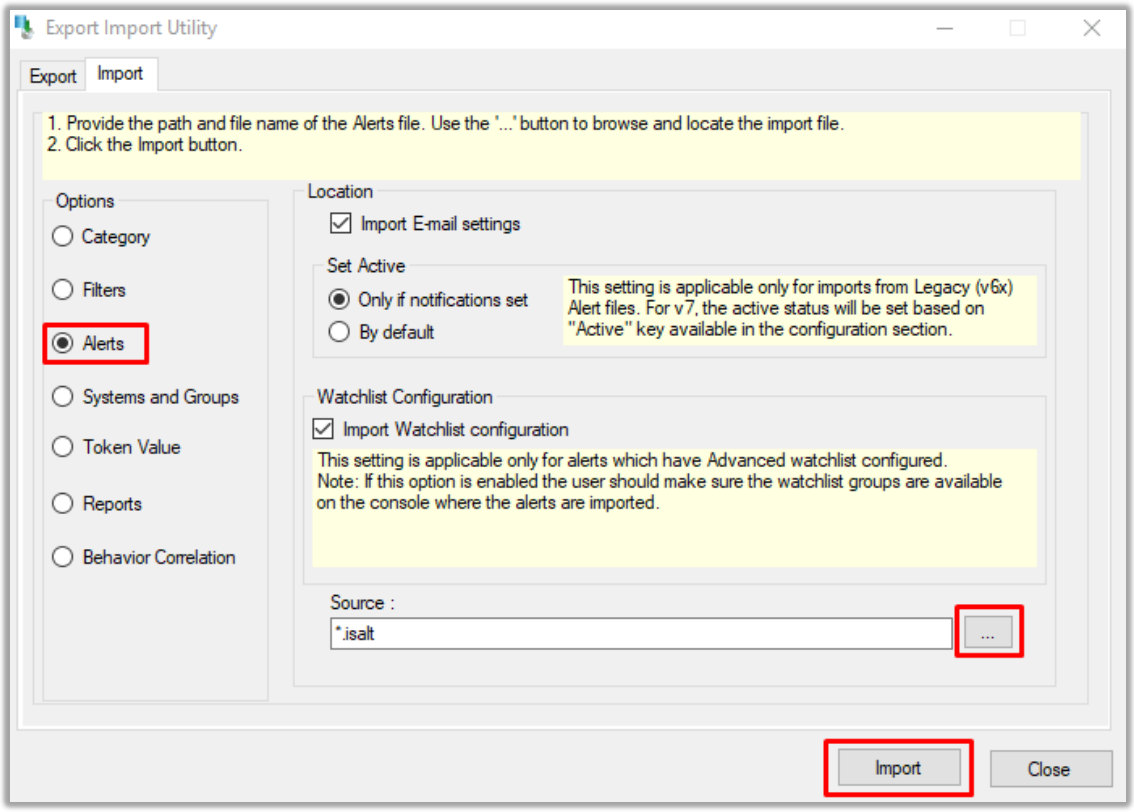

Figure16

EventTracker displays a success message:

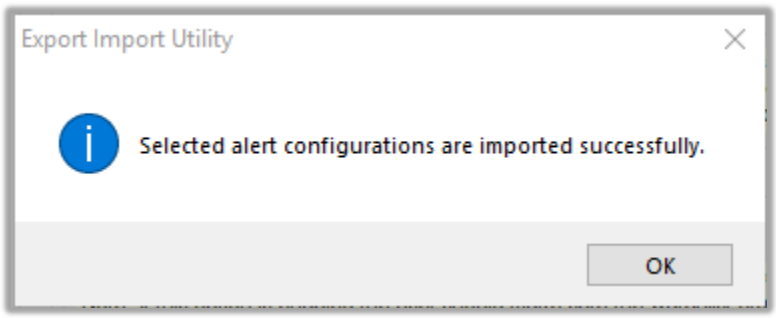

Figure 17

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 ... .
2. Navigate to the knowledge pack folder and select the file with extension **".istoken", e.g. "Parsing Rules_ NetMotion.istoken"** and then click "**Import**":

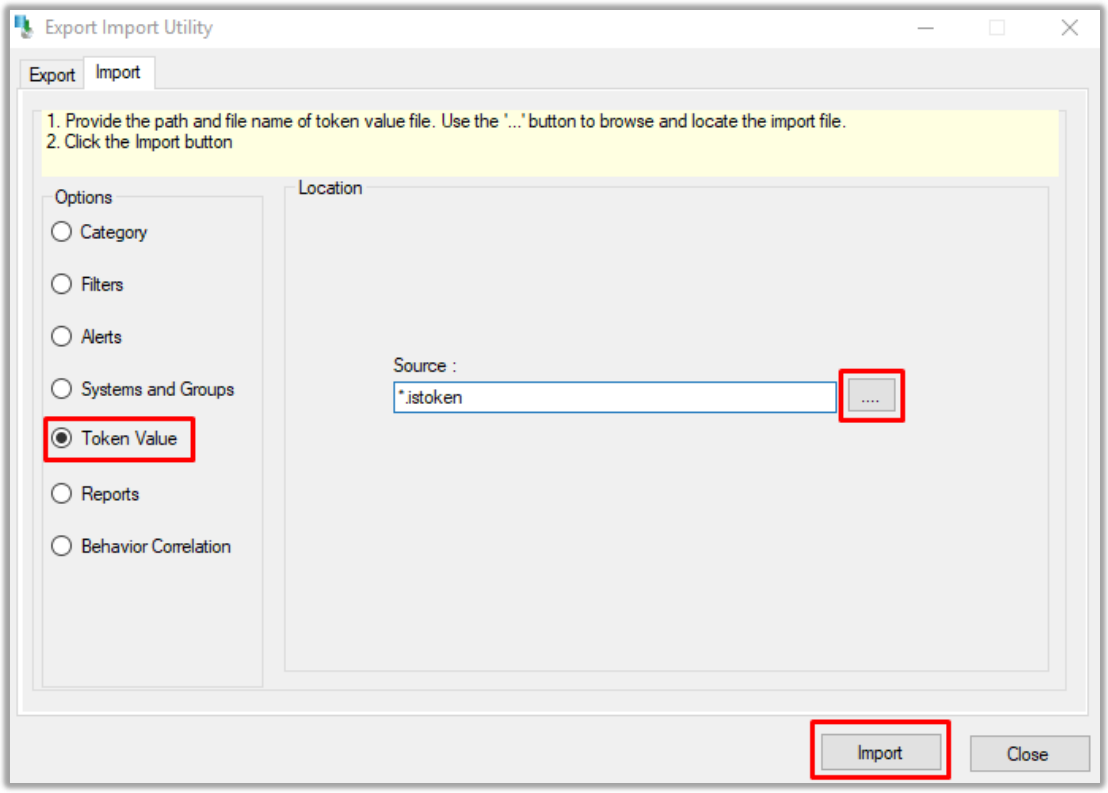

Figure 18

5.4 Token Template

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

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

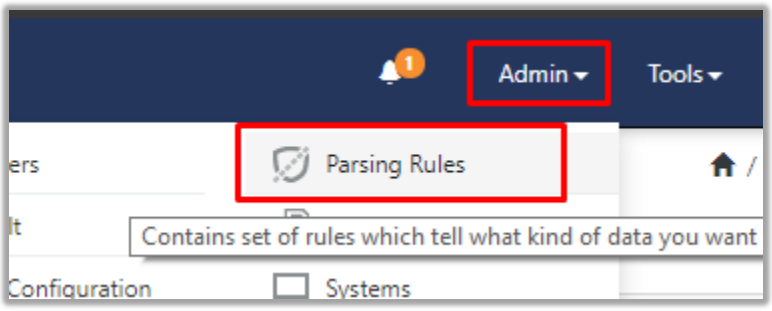

Figure 19

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

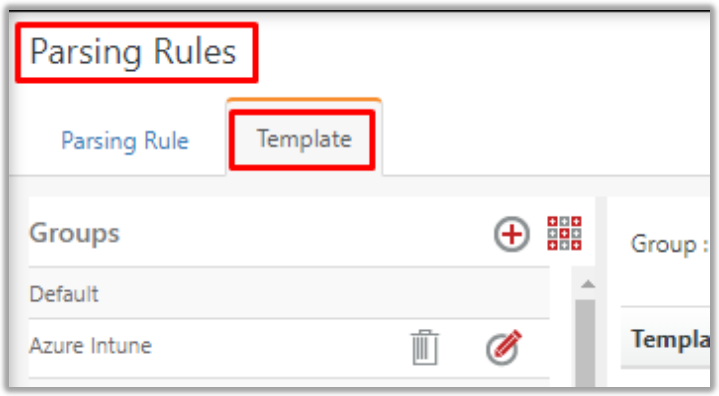

Figure 20

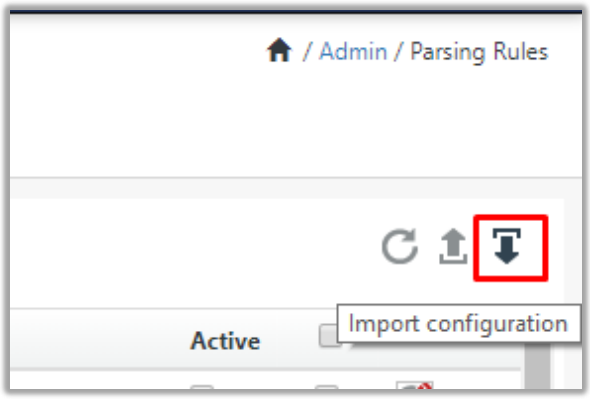

Figure 21

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

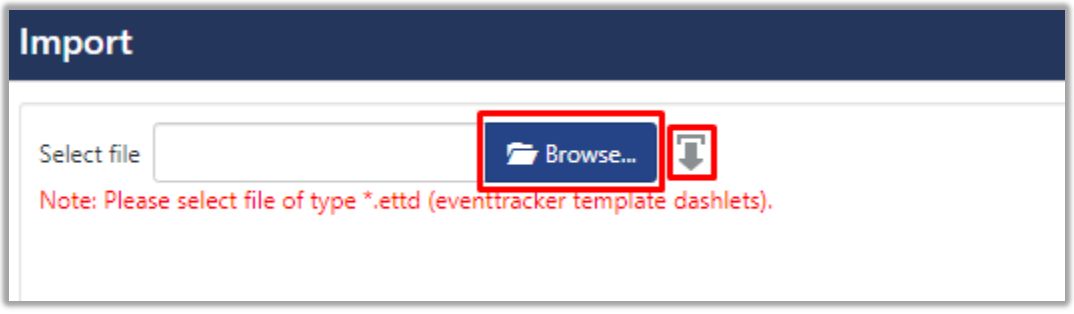

Figure 22

5.5 Reports

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

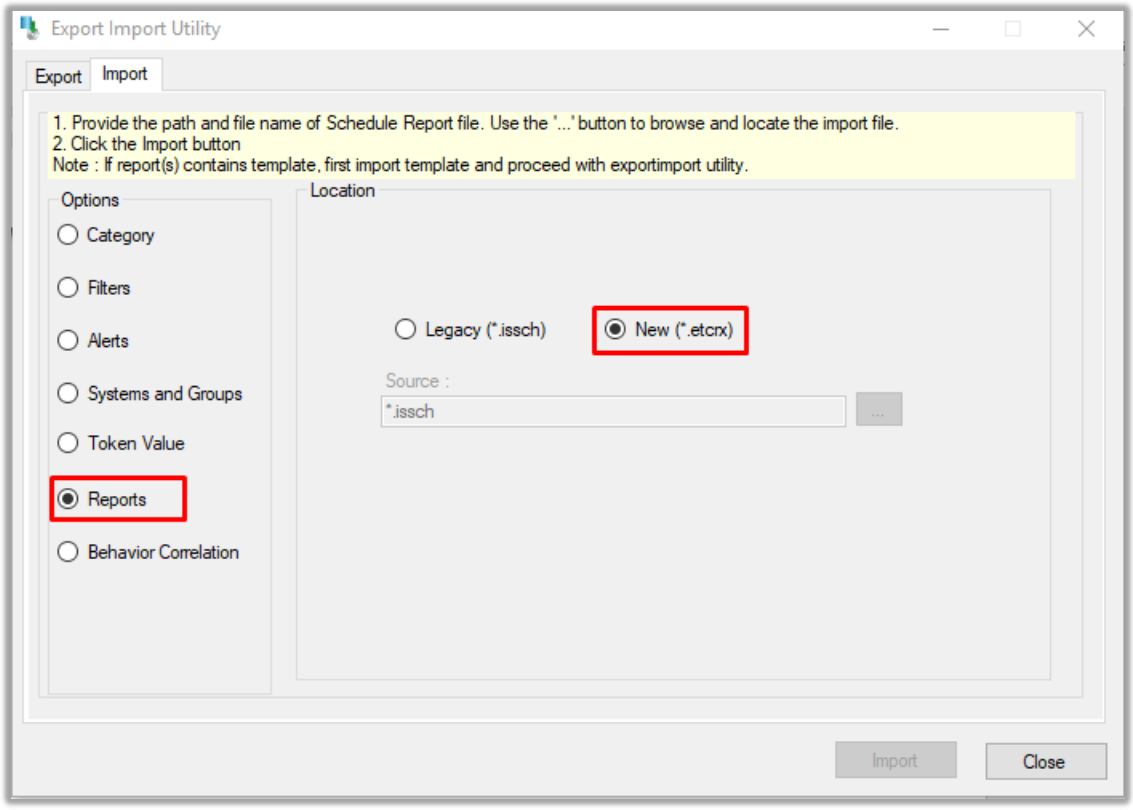

Figure 23

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", e.g. "Reports_ NetMotion.etcrx".**

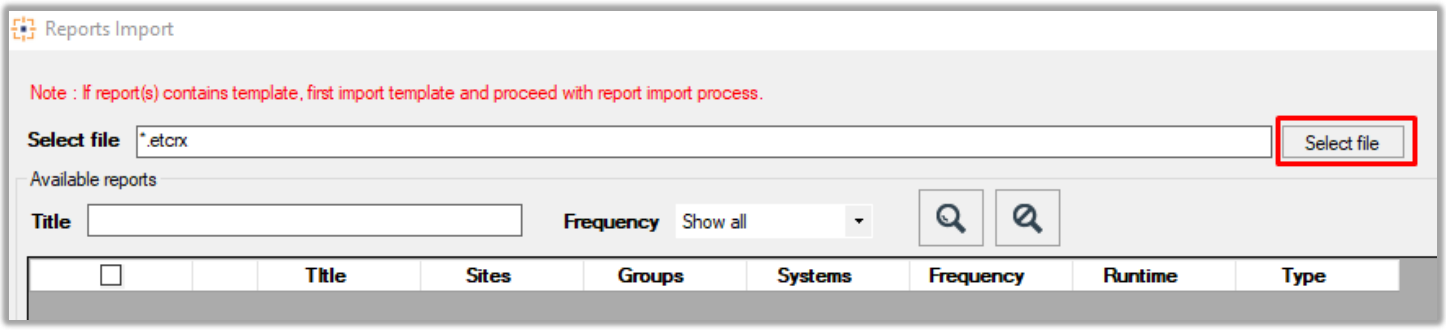

Figure 24

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

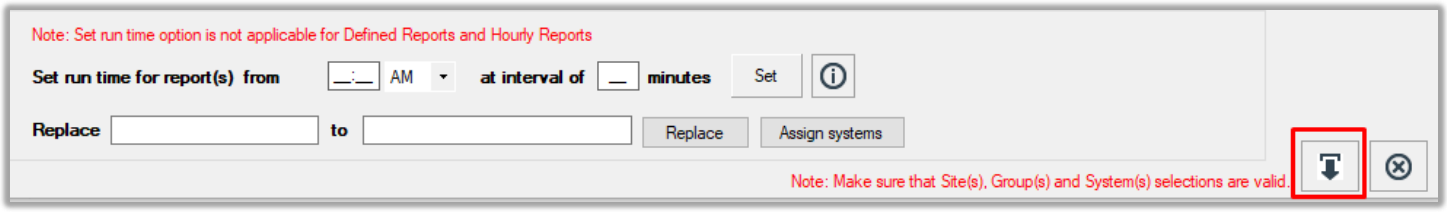

Figure 25

EventTracker displays a success message:

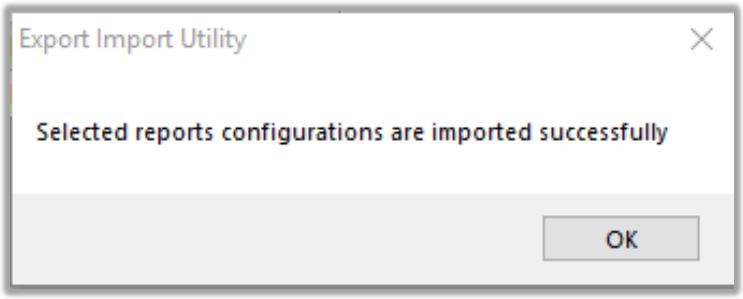

Figure 26

5.6 Knowledge Objects

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

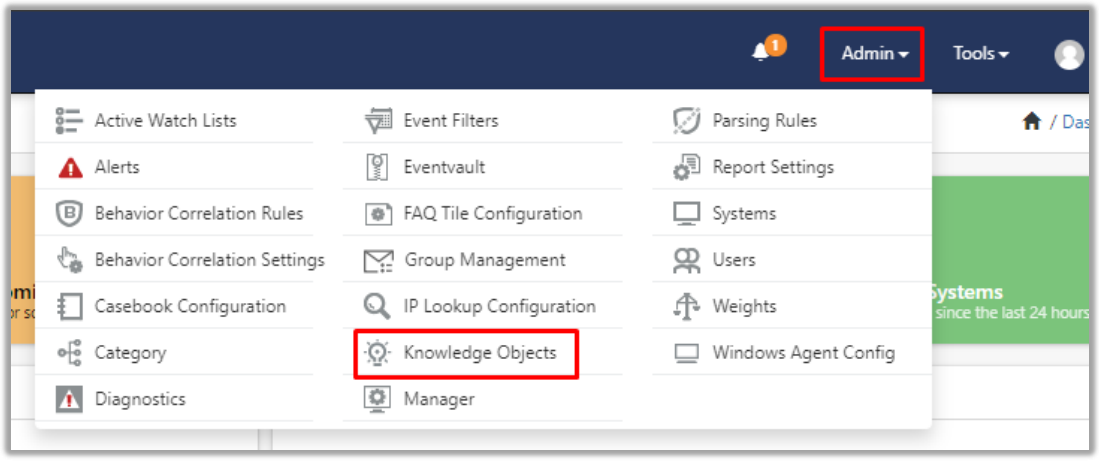

Figure 27

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

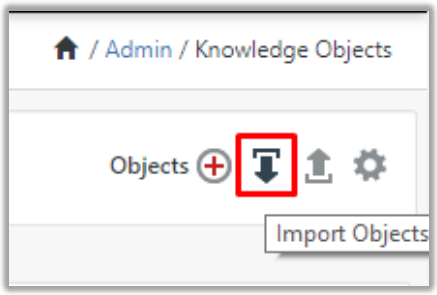

Figure 28

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", e.g. "KO_ NetMotion.etko"** and then click "**Upload**".

Figure 29

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

Figure 30

5.7 Dashboards

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

Figure31

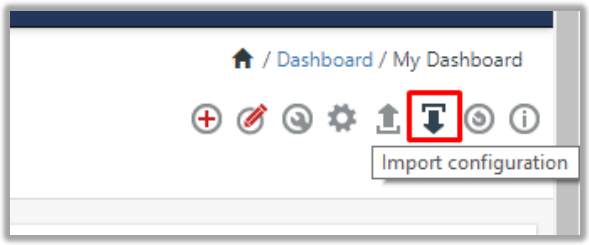

Figure 32

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

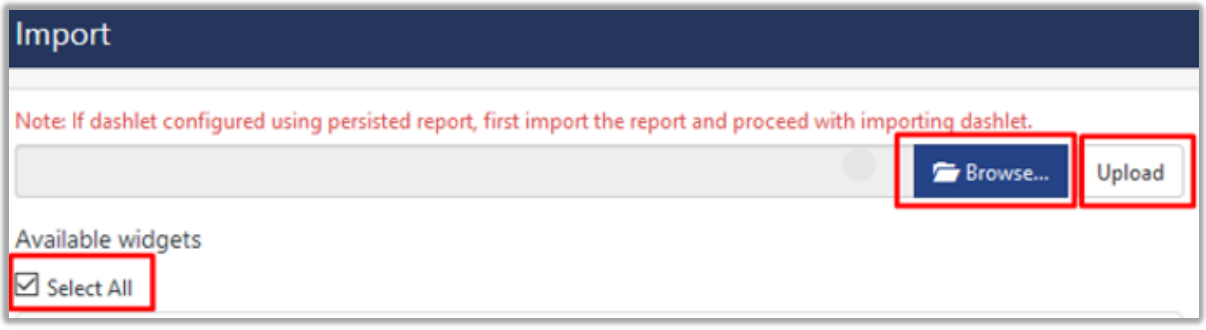

Figure 33

Figure 34

6. Verifying knowledge pack in EventTracker

6.1 Saved Searches

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 "**NetMotion**" group folder to view the imported categories:

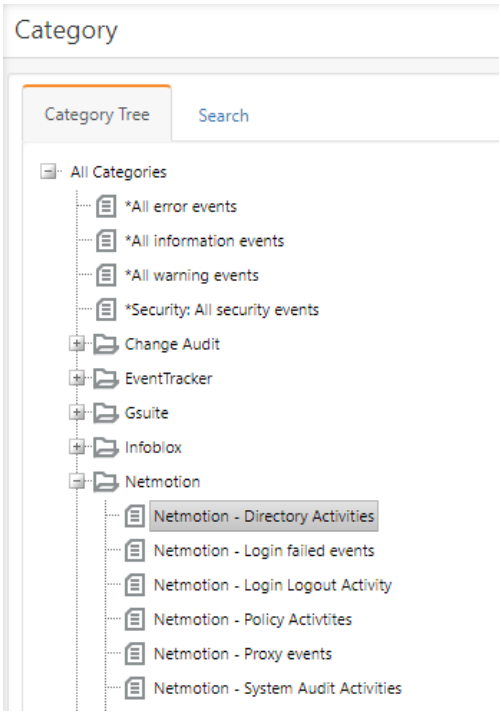

Figure 35

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. "NetMotion"** and then click **Search**.
   EventTracker displays an alert related to **"NetMotion":**

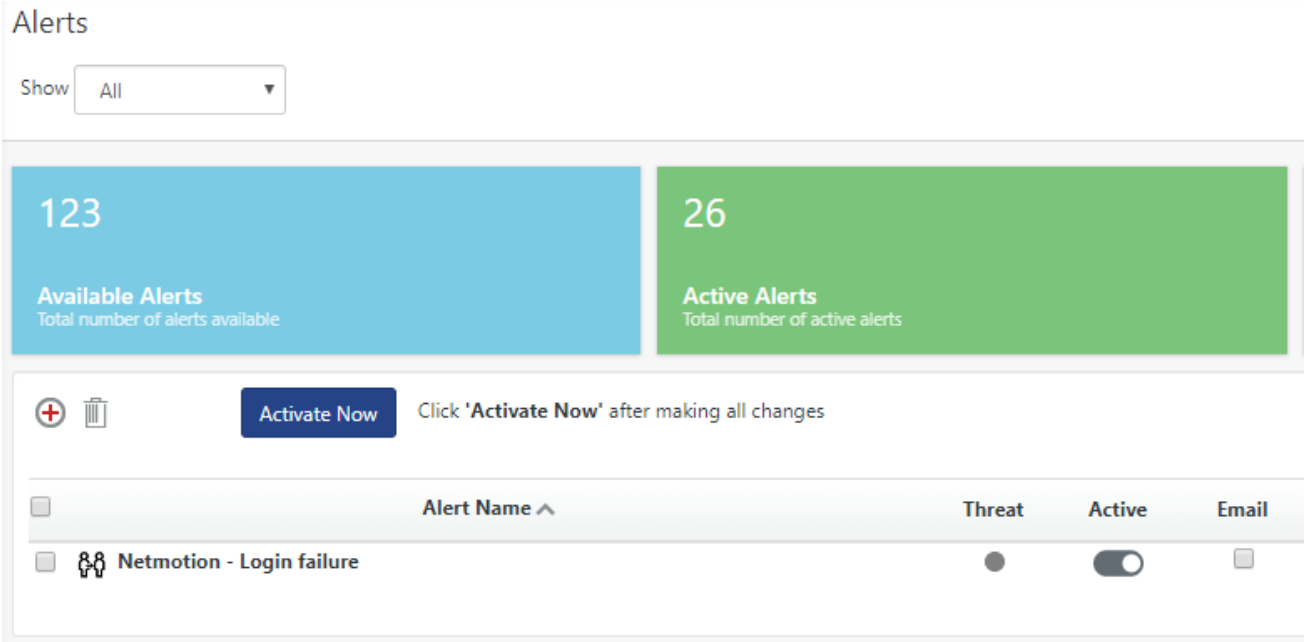

Figure 36

6.3 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 **"NetMotion"** group folder to view the imported Templates.

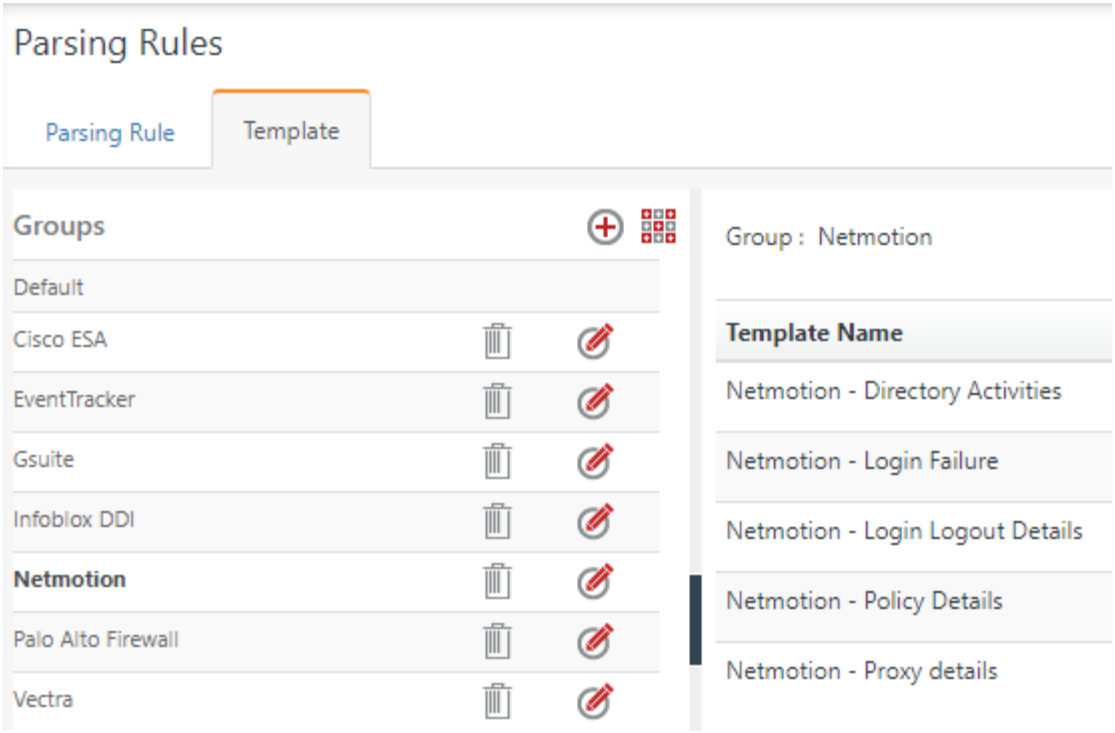

Figure 37

6.4 Reports

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

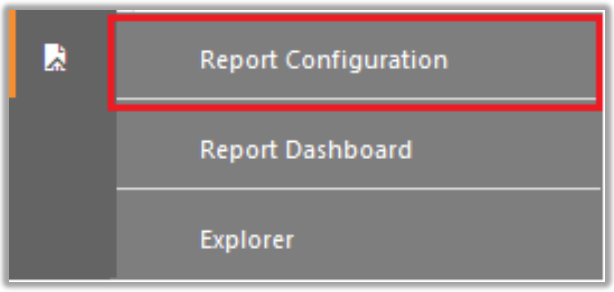

Figure 38

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

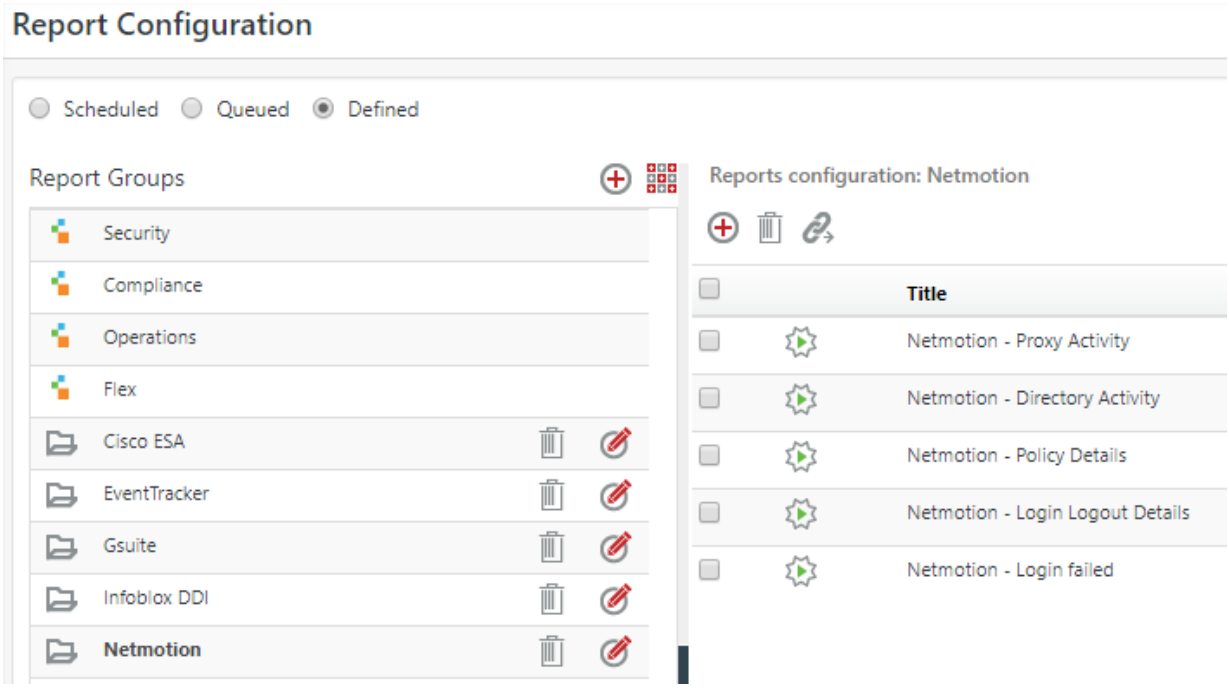

Figure 39

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 "**NetMotion**" group folder to view the imported Knowledge objects.

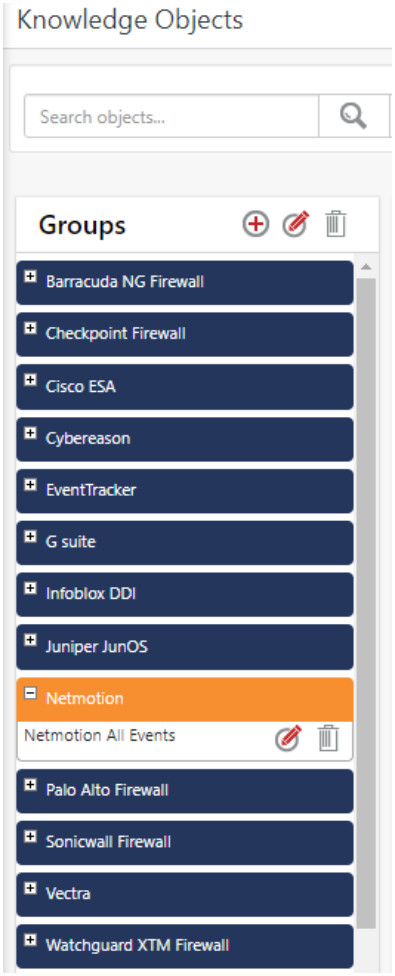

Figure 40

6.6 Dashboards

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

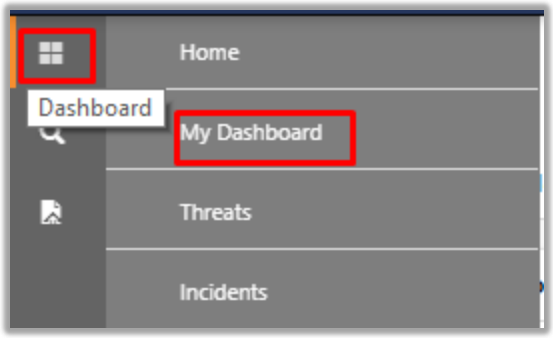

Figure 41

2. Select "**Customize daslets**". and type "**Cisco**" in the search bar.

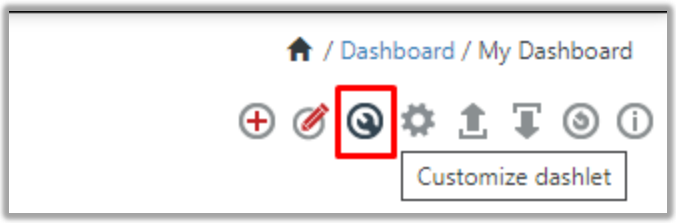

Figure 42

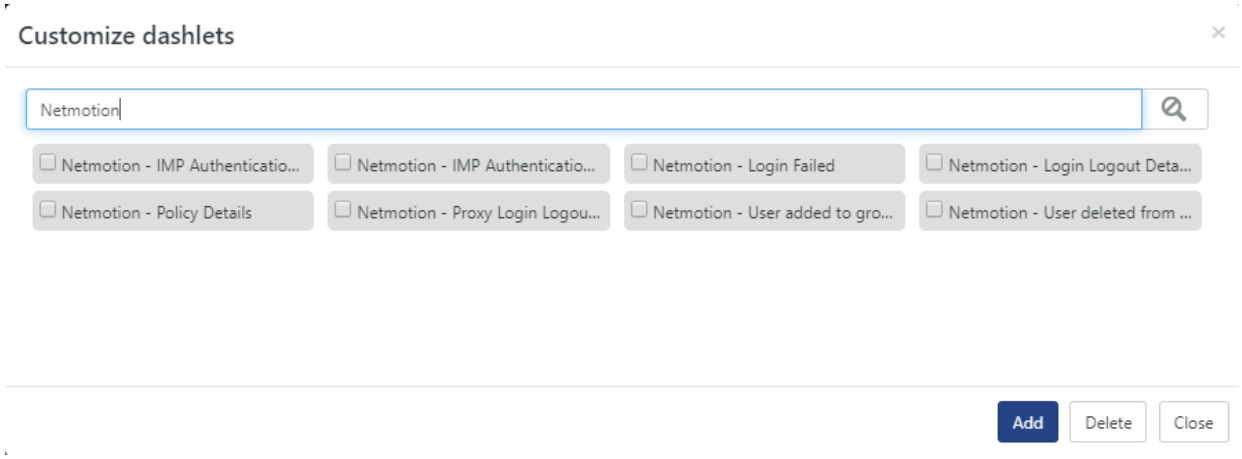

Figure 43