Netsurion | EventTracker®

Integration Guide for FireEye Network Security and Forensics (NX)

EventTracker v9.x and later

Publication Date: April 30, 2020

Abstract

This guide provides instructions to retrieve the **FireEye Network Security and Forensics (NX)** events by syslog. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **FireEye Network Security and Forensics (NX)**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **FireEye Network Security and Forensics (NX).**

Audience

Administrators who are assigned the task to monitor **FireEye Network Security and Forensics (NX)** 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 FireEye Network Security and Forensics (NX) 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. Overview

The FireEye Network Security and Forensics (NX) is an effective cyber threat protection solution. It helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic.

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

Reports contain a detailed overview of events such as, malware object, indicating the presence of a file attachment with a malicious executable payload.

It will also show web infection indicating an outbound connection to a website initiated by a web browser that was determined to be malicious.

Alerts are provided as soon as any critical event is triggered by the FireEye NX. With alerts, users will be able to get notifications about real time occurrences of events such as, suspicious file hash detection, or suspicious web URL detection, and any such activities.

Dashboards will display a graphical overview of all the malwares detected by FireEye NX, or Command and Control server connection, etc. These services will include information such as suspicious source IP address, source port, destination IP address, destination port, anomaly type, malware name, etc.

2. Prerequisites

- VCP (virtual collection point) syslog port should be opened.
- Port 514 should be allowed in Firewall (if applicable).

3. Integrating FireEye NX with EventTracker

FireEye NX can be integrated with EventTracker using syslog forwarding.

3.1 Configuring a Syslog Forwarding

Follow the below steps to configure syslog.

1. Login to FireEye NX Web UI with an admin account.
2. Navigate to **Settings > Notifications**.
3. Click **rsyslog and** Check the "**Event type**" check box.
4. Make sure Rsyslog settings are:

Default format: CEF

Default delivery: Per event

Default send as: Alert

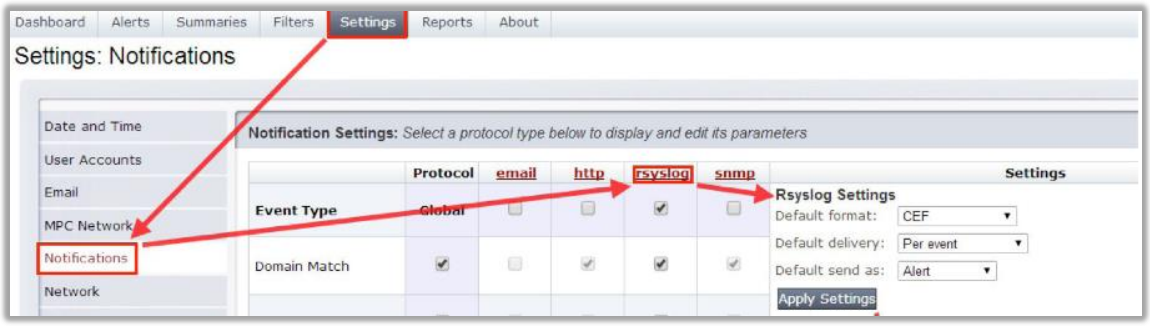

Figure 1

5. Next to the "**Add Rsyslog Server**" button, type "EventTracker". And, click on "**Add Rsyslog Server**" button.
6. Enter the EventTracker server IP address in the "IP Address" field. (Public IP, if hosted in cloud)
7. Check off the Enabled check box.
8. Select Per Event in the "Delivery" drop-down list.
9. Select All Events from the "Notifications" drop-down list.
10. Select CEF as the "Format" drop-down list.
11. Select UDP from the "Protocol" drop-down list. (Default port is 514)
12. Now, click **Update**. And click the "Test-Fire" button to send the test events to EventTracker server.

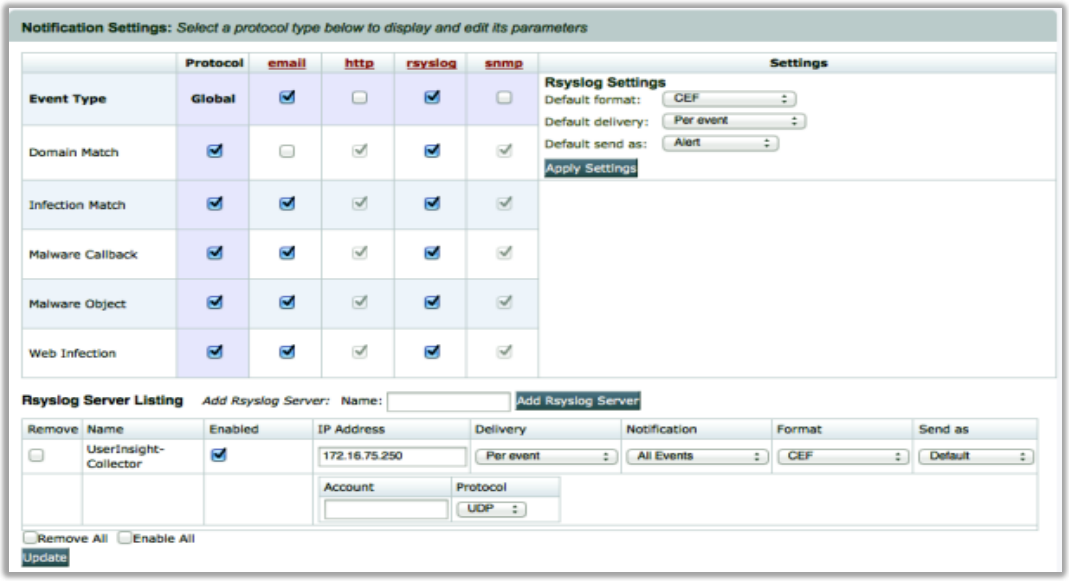

Figure 2

4. EventTracker Knowledge Packs

4.1 Saved Searches

Saved searches are designed to quickly parse logs and allow user to see only specific events related to:

- **FireEye: Suspicious Domain Match –** This category of saved search allows user to filter and view the events specific to website domain that has been identified as the source of malicious behavior.
- **FireEye: Initial Web Infection Identification –** this category of saved search allows user to filter and view events specific to the process of identifying a URL pointing to the initial web infection.
- **FireEye: Command and Control Connections –** This category of saved search allows user to filter and view events specific to situation where there is an established connection between the infected endpoint and a command and control (CnC) server.
- **FireEye: Suspicious File Attachments –** This category of saved search allows user to filter and view events that indicates presence of a file attachment with a malicious executable payload.
- **FireEye: Outbound Connections established with Malicious Website –** This category of saved search allows user to filter and view events that indicates a web browser initiated an outbound connection to a website that was ultimately determined to be malicious.

4.2 Alerts

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

- **FireEye NX: A command and Control connection has been blocked –** This alert is triggered when the FireEye MVX engine detects an established command and control server connection with an endpoint in the network.
- **FireEye NX: A website with malicious contents has been discovered –** This alert is triggered when the FireEye detects a user visited website is infected with malicious contents.
- **FireEye NX: File attachment with a malicious executable payload detected –** This alert is triggered when the FireEye detects a presence of a file attachment with a malicious executable payload.

4.3 Reports

- **FireEye NX – Malicious File detected –** This report for FireEye includes events that indicates the presence of a file attachment with a malicious executable payload. The report contains the file hash of the malicious payload along with relevant information such as source and destination IP.

LogTime	Computer	Source IP	Source Port	Destination IP	Destination Port	File Hash	Malware
04/22/2020 06:00:20 PM	NTPLDTBLR48-SYSLOG	169.250.0.4	10	127.0.0.20	20	dfcc0ebba834870c2860296cdc96c644	FireEye-TestEvent-SIG
04/23/2020 01:01:16 PM	NTPLDTBLR48-SYSLOG	169.250.0.4	10	127.0.0.20	20	dfcc0ebba834870c2860296cdc96c644	FireEye-TestEvent-SIG

Figure 3

- **FireEye NX - Outbound connections with malicious websites –** This report for FireEye includes events that indicates that a web browser initiated an outbound connection to a website that was ultimately determined to be malicious. This report contains the infected website URL, along with relevant information such as, source and destination IP.

Computer	Source IP	Source Port	URL	Anomaly Type	Destination IP	Destination Port
NTPLDTBLR48-SYSLOG	169.250.0.1	10	compl_0_2- someurl.x1y2z3.com	anomaly-tag datatheft keylogger	127.0.0.20	20
NTPLDTBLR48-SYSLOG	169.250.0.1	10	compl_0_2- someurl.x1y2z3.com	anomaly-tag datatheft keylogger	127.0.0.20	20

Figure 4

- **FireEye NX - Successful Command and Control Activities –** This report for FireEye includes events that indicates there is an established connection between the infected endpoint and a command and control (CnC) server. This report contains the information on Command and control server IP address and to which system it has connected, i.e. source IP.

LogTime	Computer	Source IP	Source Port	CnC_Host	Protocol	Destination IP	Destination Port
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	192.168.25.2	28941	172.65.203.203	tcp	172.65.203.203	80
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	192.168.26.142	0	3.3.3.3	tcp	2.2.2.2	80

Figure 5

- **FireEye NX - Suspicious Domain match Activities –** This report for FireEye includes events that indicates the website domain has been identified as the source of malicious behavior.

LogTime	Computer	Source IP	Source Port	Protocol	CnC_Host	Malware	Destination IP	Destination Port
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	169.250.0.1	10	tcp	FireEye-TestEvent.example.com	FireEye-TestEvent-SIG-DM	127.0.0.20	20
04/23/2020 05:31:53 PM	NTPLDTBLR48-SYSLOG	169.250.0.1	10	tcp	FireEye-TestEvent.example.com	FireEye-TestEvent-SIG-DM	127.0.0.20	20

Figure 6

- **FireEye NX - URL pointing to the initial web infection –** This report for FireEye includes events indicates to the process of identifying a URL pointing to the initial web infection.

LogTime	Computer	Source IP	Source Port	Protocol	Malware	Destination IP	Destination Port
04/23/2020 05:36:47 PM	NTPLDTBLR48-SYSLOG	192.168.10.23	123	tcp	nam	192.0.2.2	123
04/24/2020 04:47:39 PM	NTPLDTBLR48-SYSLOG	192.168.10.24	123	tcp	nam	192.0.2.2	123

Figure 7

4.4 Dashboards

- **FireEye - Command and Control connection By Action type**

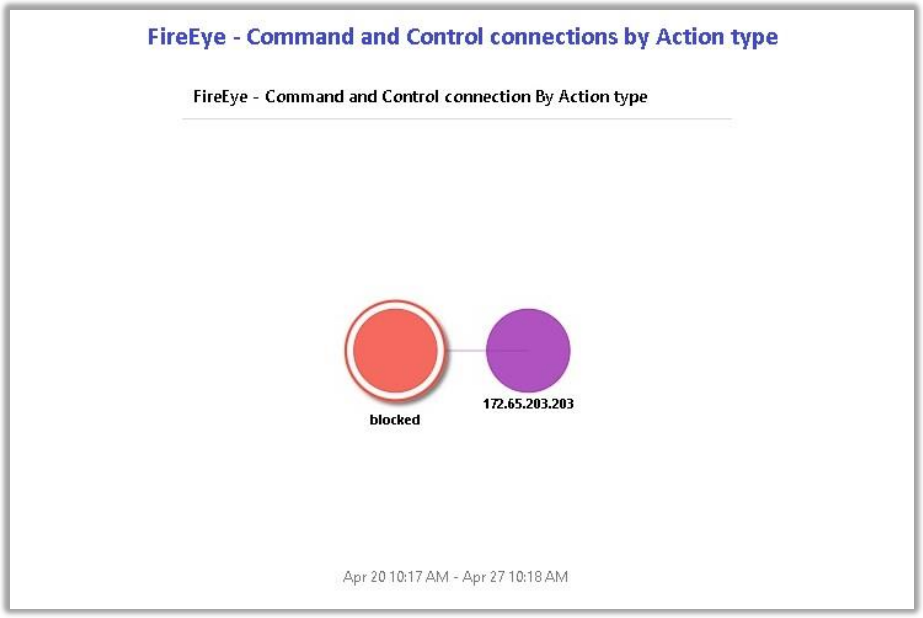

Figure 8

- **FireEye - Command and Control connection By client application**

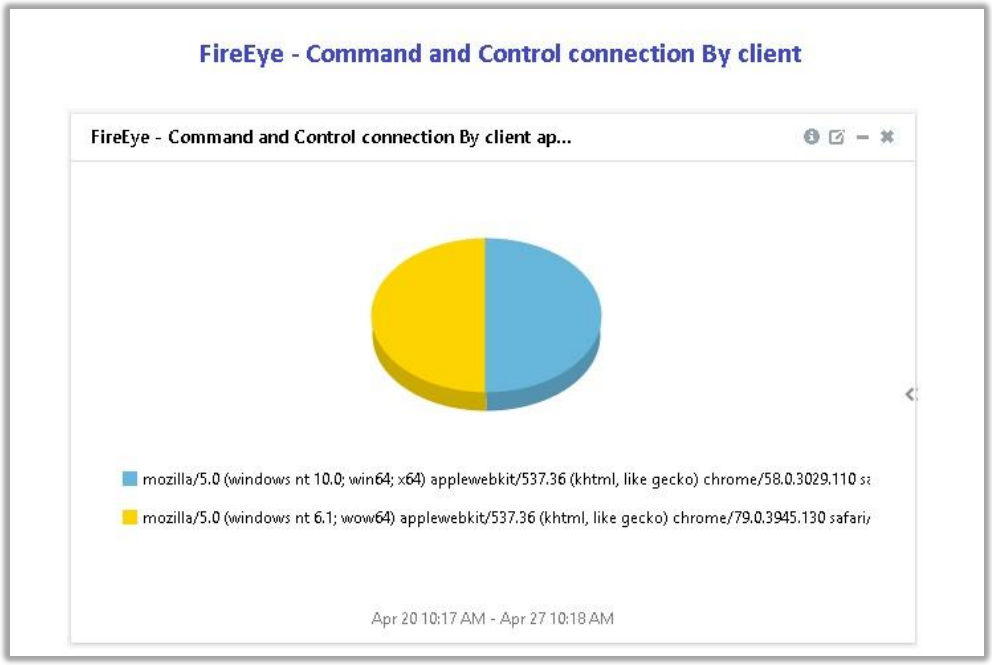

Figure 9

- **FireEye - Suspicious File Hashes**

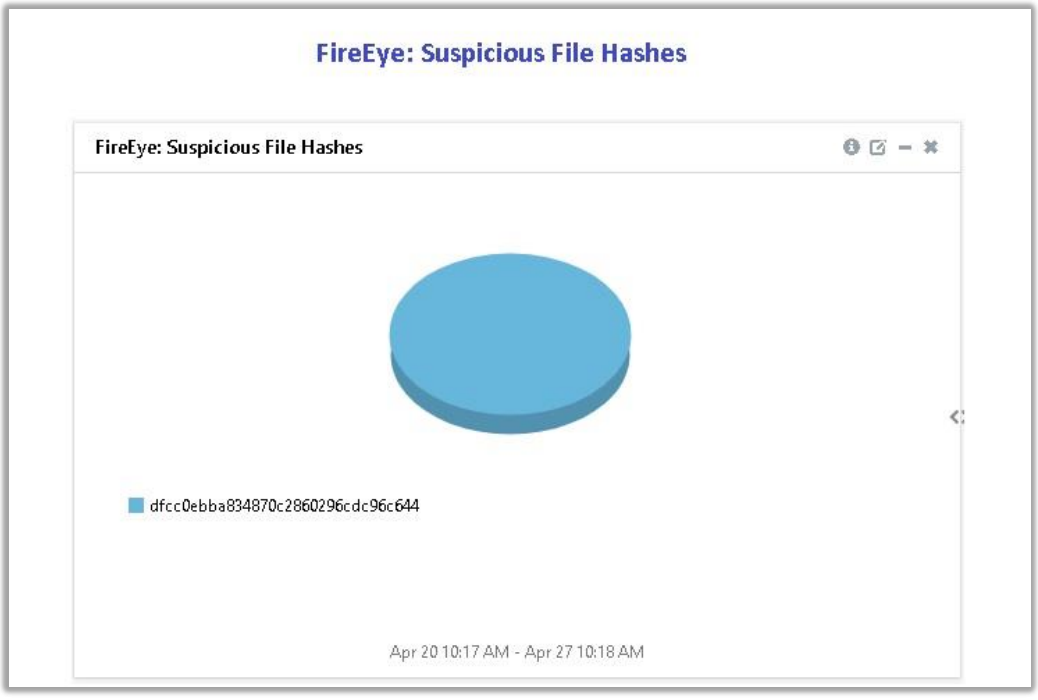

Figure 10

- **FireEye - Suspicious URLs**

Figure 11

- **FireEye - Security event types**

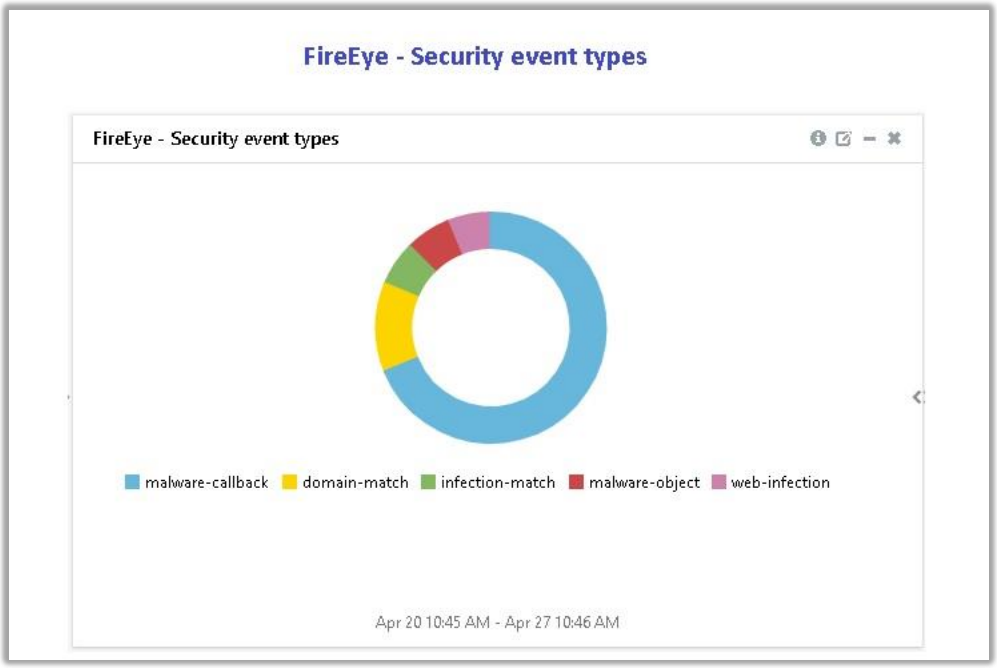

Figure 12

- **FireEye - Malwares by anomaly type**

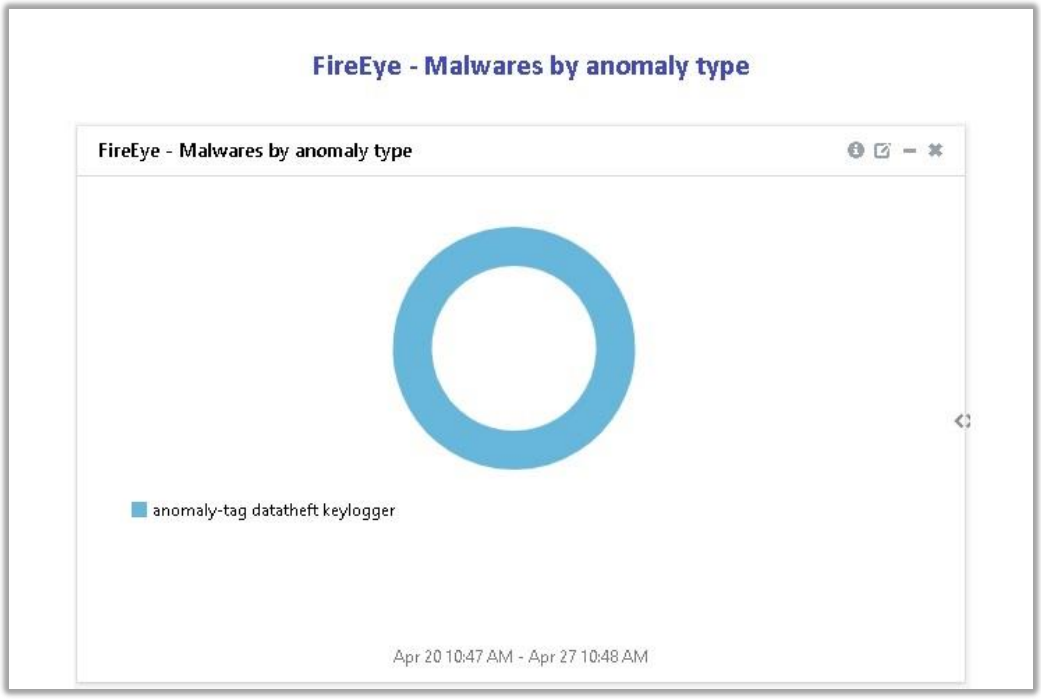

Figure 13

- **FireEye - Malwares types and signature discovered**

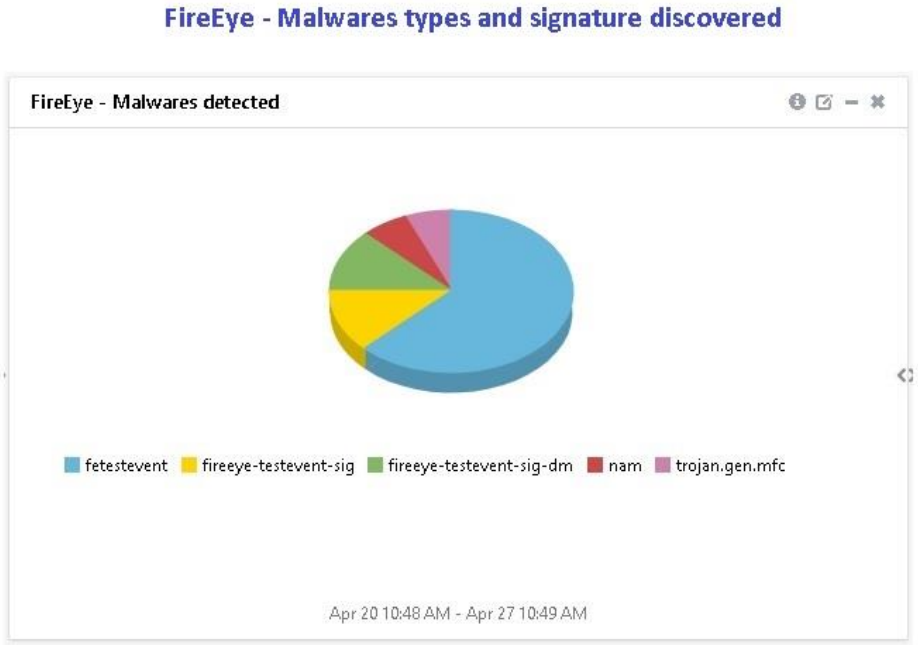

Figure 14

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 15

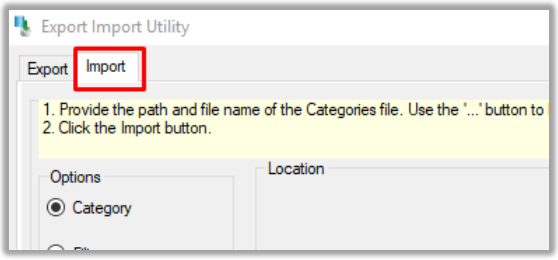

Figure 16

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_FireEye NX.iscat"** and then click "**Import**":

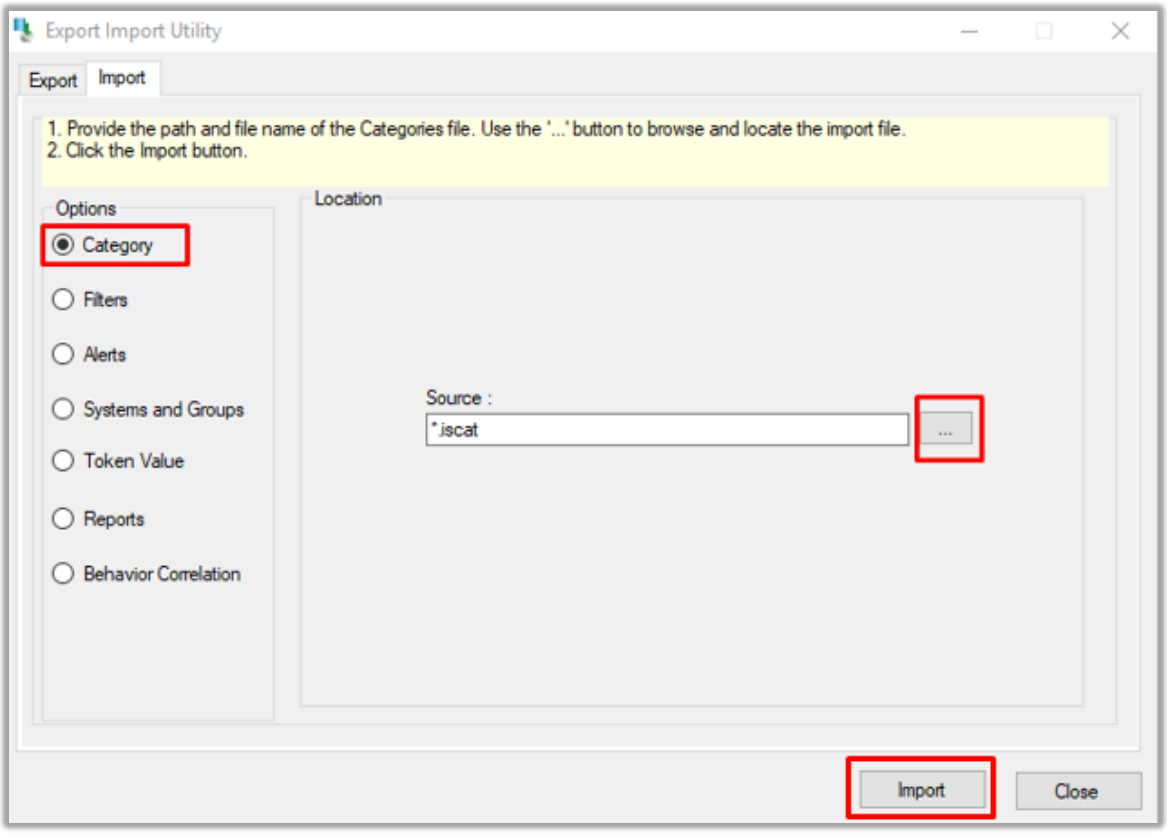

Figure 17

EventTracker displays a success message:

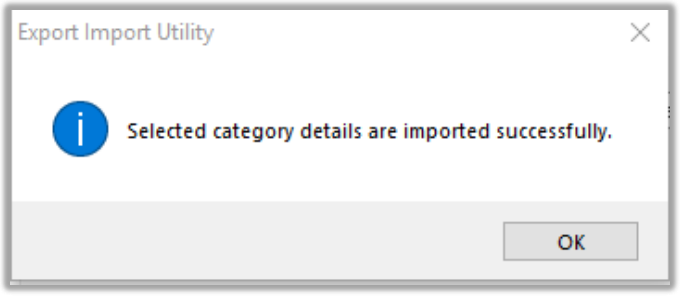

Figure 18

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_ FireEye NX.isalt**" and then click "**Import**".

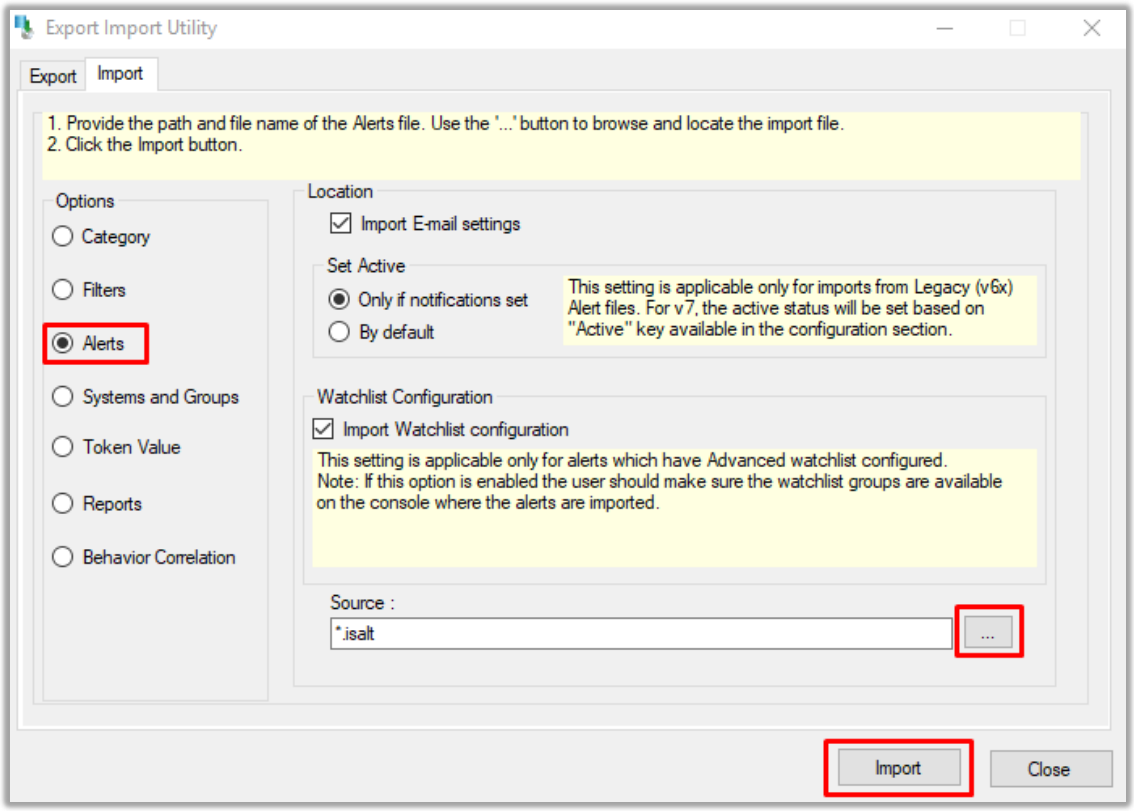

Figure 19

EventTracker displays a success message:

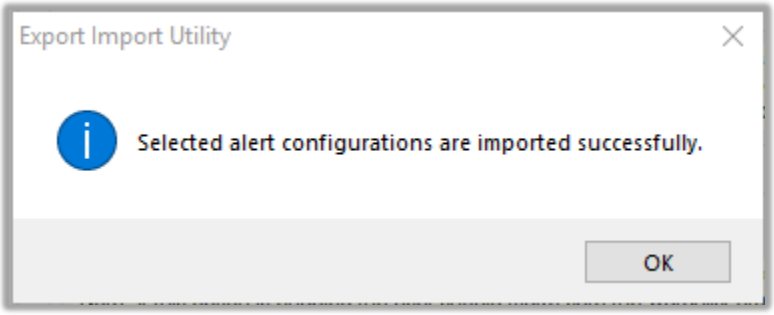

Figure 20

5.3 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.

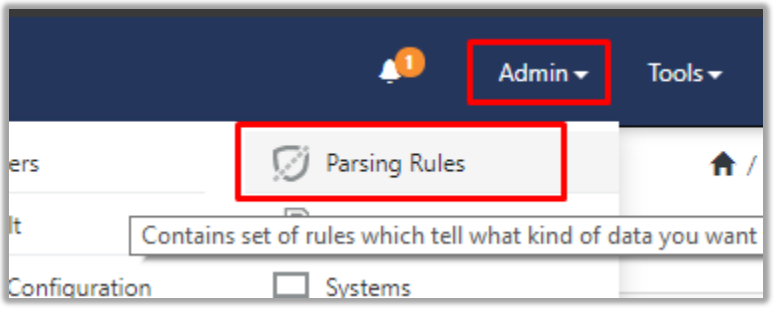

Figure 21

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

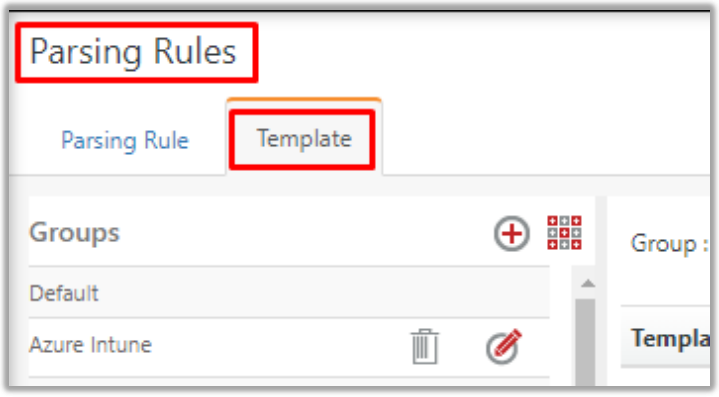

Figure 22

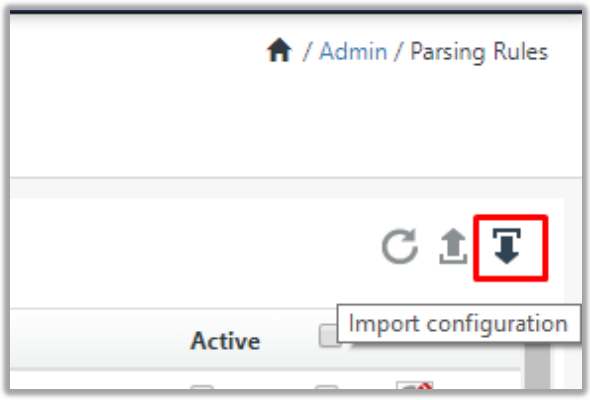

Figure 23

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_FireEye NX.ettd"** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click "**Import**":

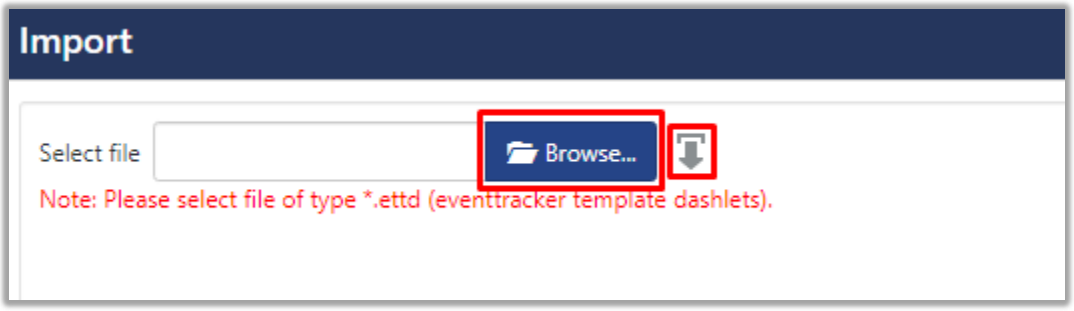

Figure 24

5.4 Reports

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

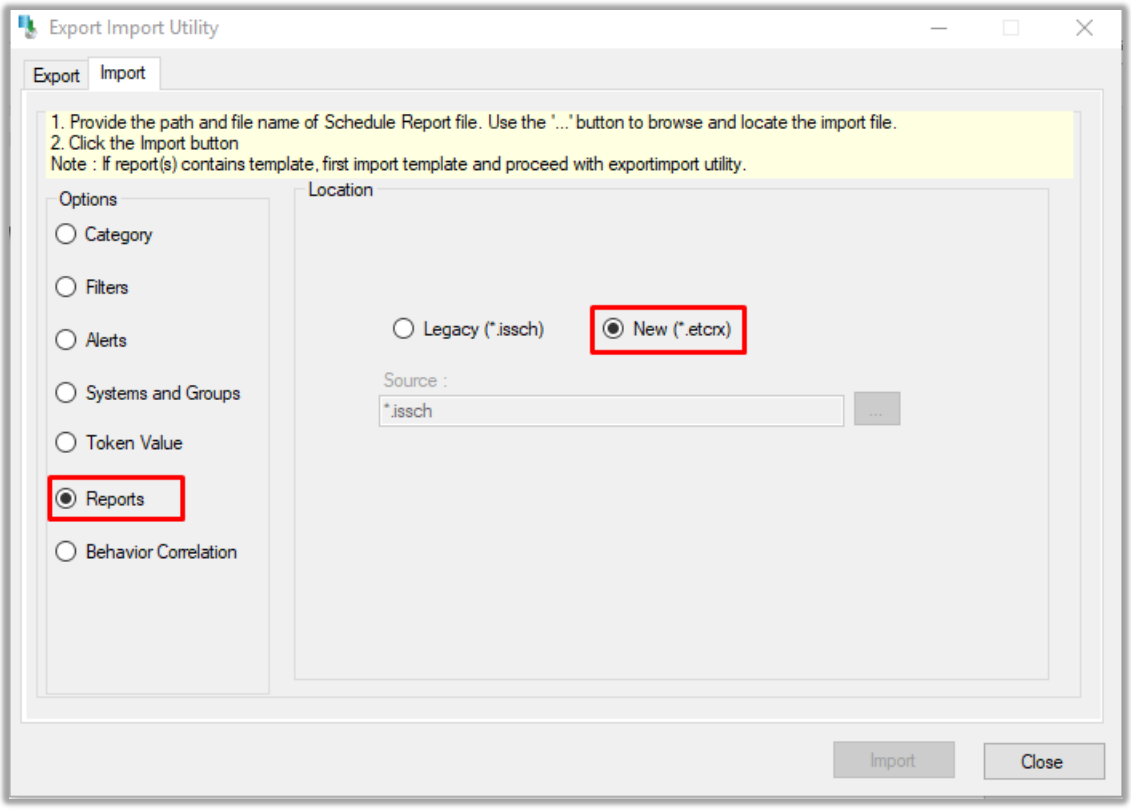

Figure 25

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_ FireEye NX.etcrx".**

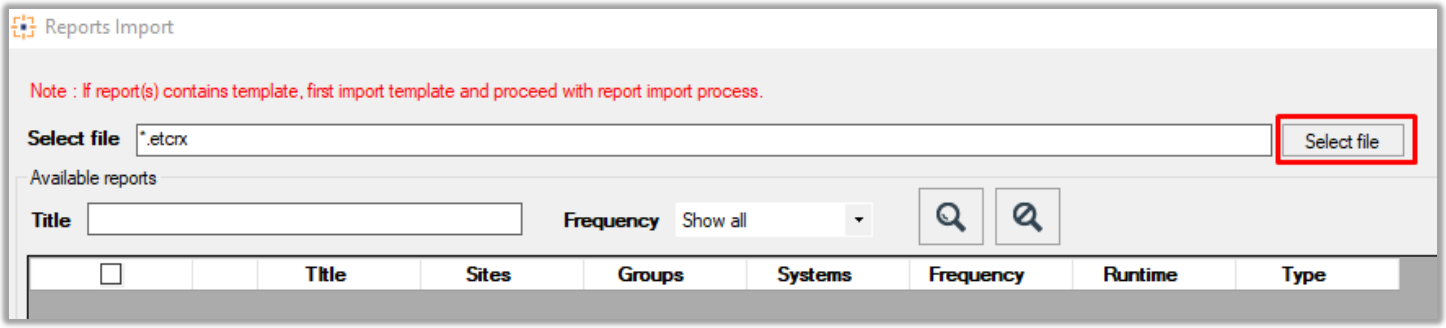

Figure 26

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

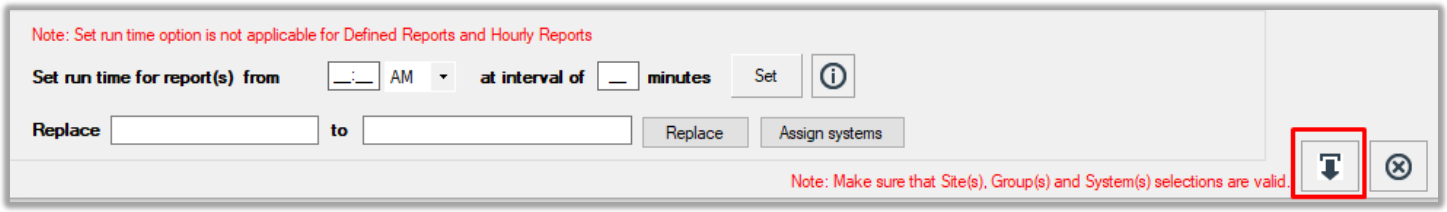

Figure 27

EventTracker displays a success message:

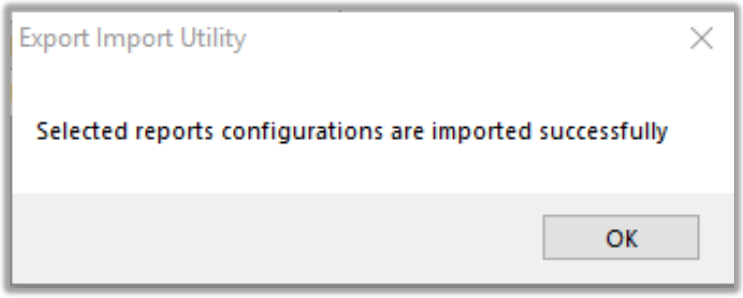

Figure 28

5.5 Knowledge Objects

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

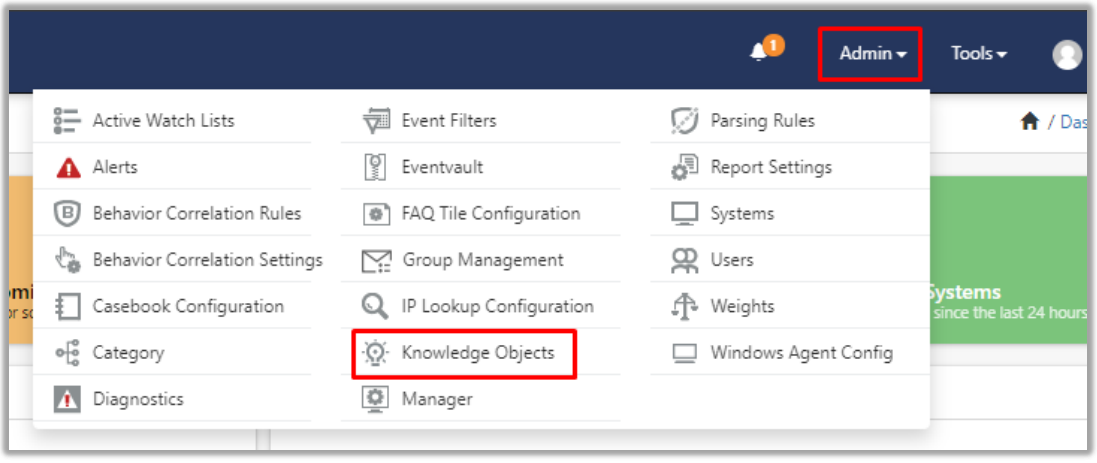

Figure 29

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

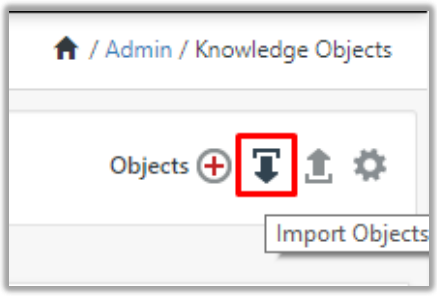

Figure 30

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_ FireEye NX.etko"** and then click "**Upload**".

Figure 31

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

Figure 32

5.6 Dashboards

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

Figure 33

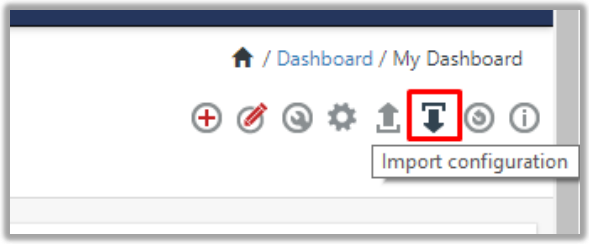

Figure 34

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

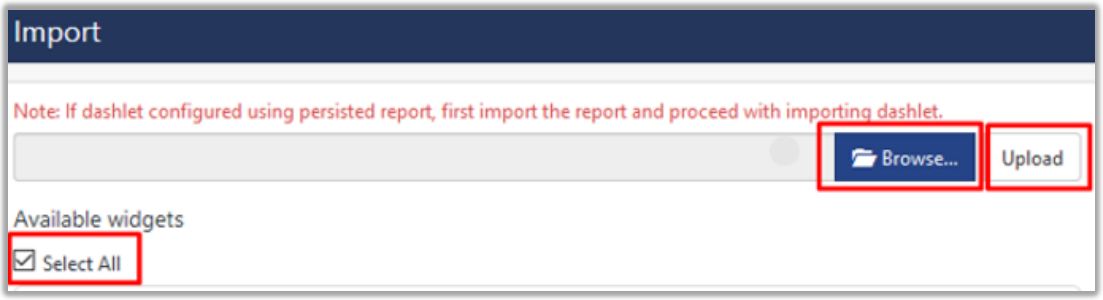

Figure 35

Figure 36

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 "**FireEye NX**" group folder to view the imported categories:

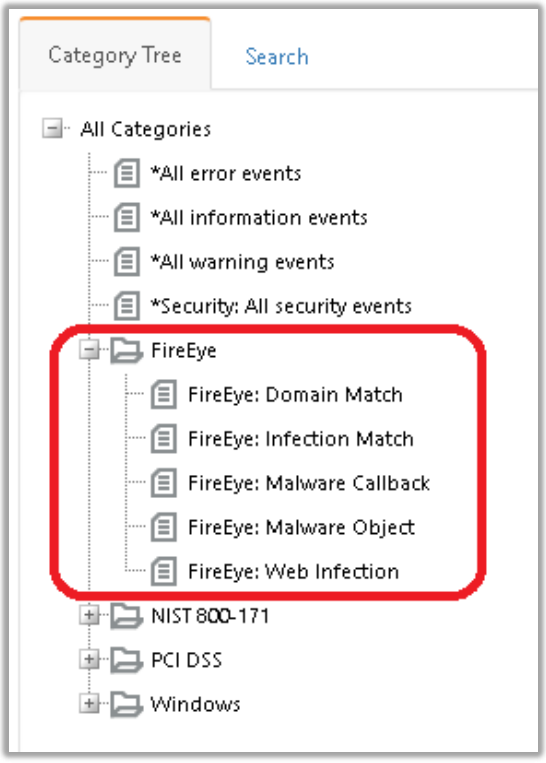

Figure 37

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

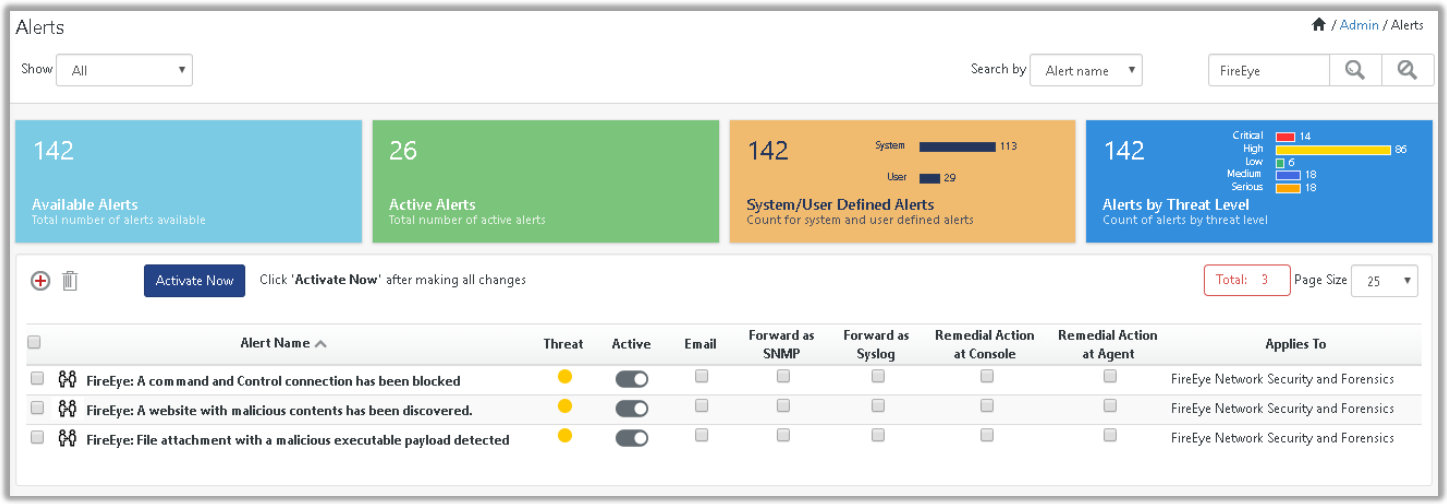

Figure 38

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 **"<product name/ report group name>"** e.g. "**FireEye NX**" group folder to view the imported Templates.

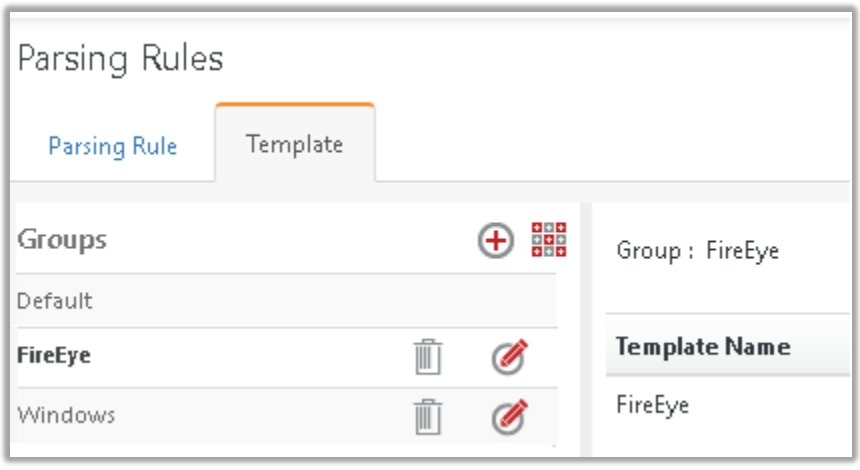

Figure 39

6.4 Reports

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

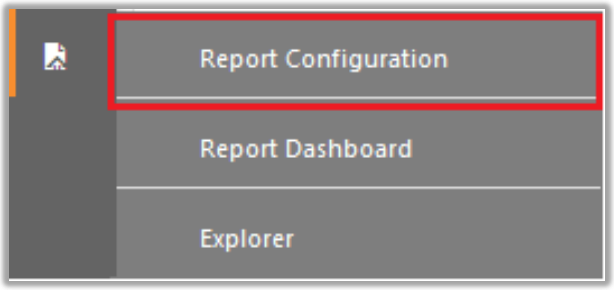

Figure 40

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

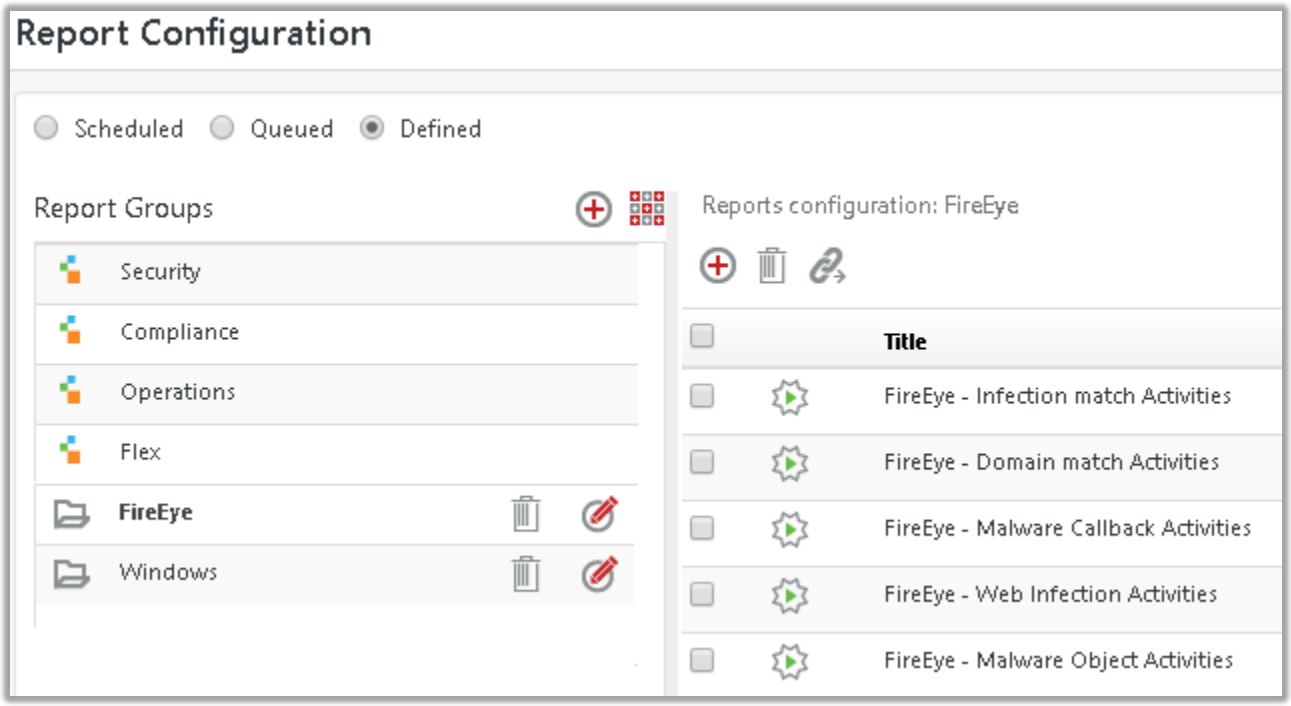

Figure 41

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

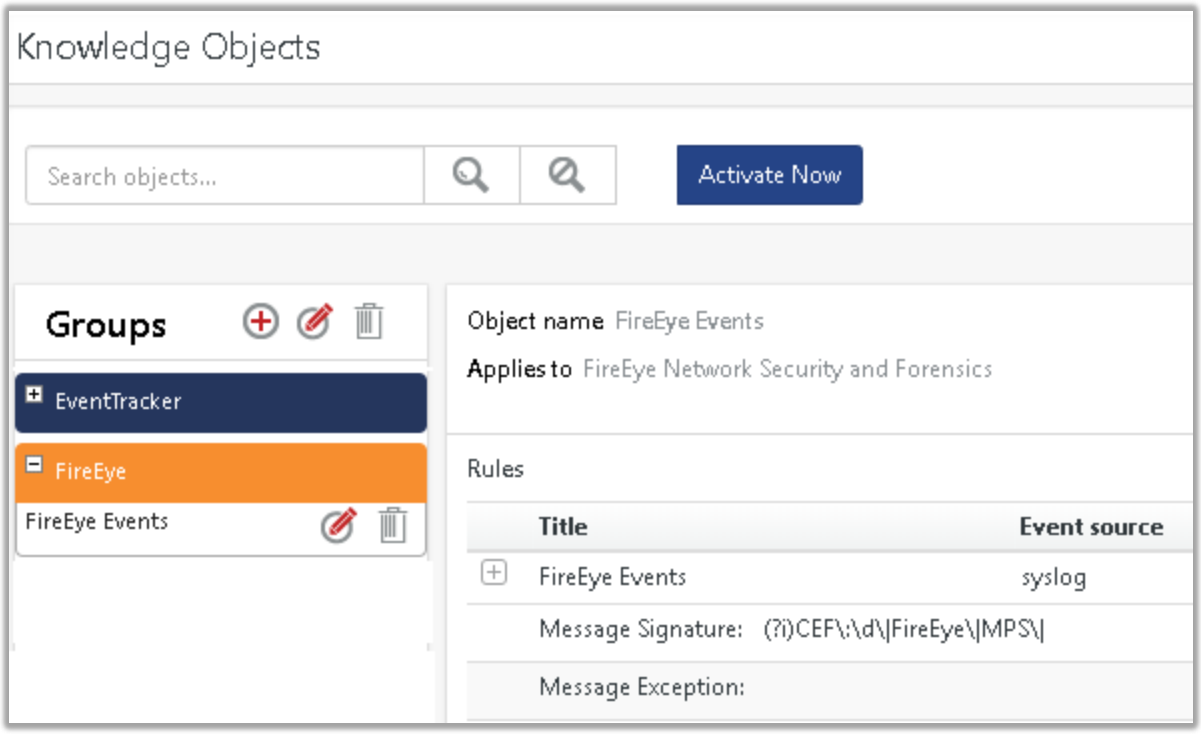

Figure 42

6.6 Dashboards

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

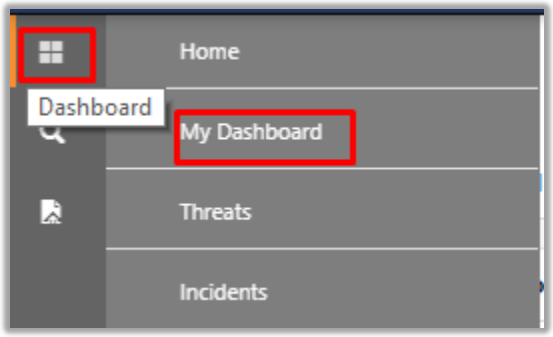

Figure 43

2. Select "**Customize daslets**" And type "**FireEye**" in the search bar.

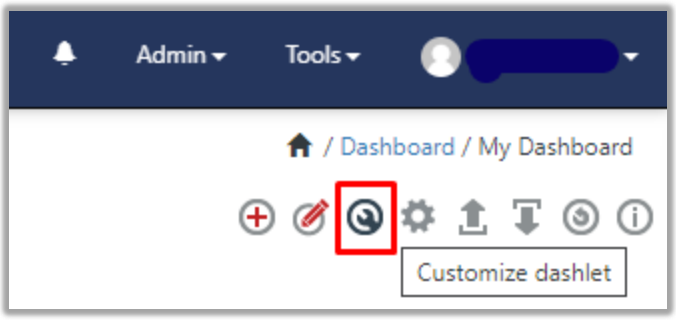

Figure 44

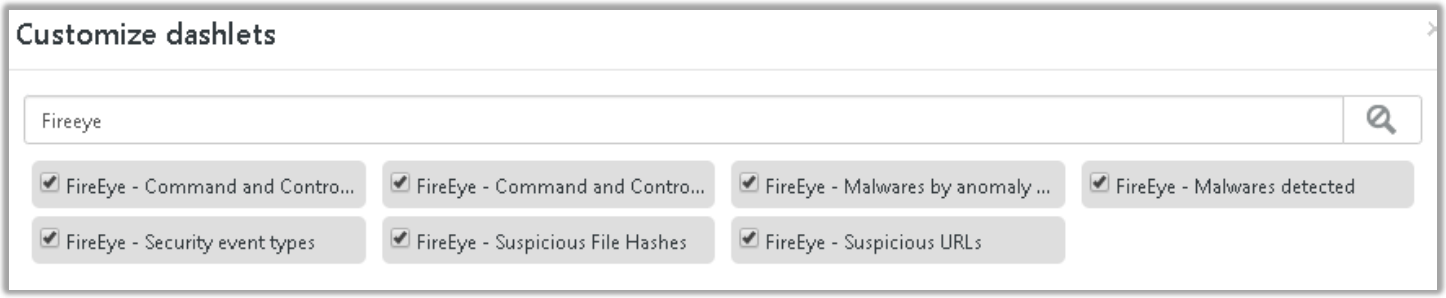

Figure 45