Netsurion™ | EventTracker

Integrate Kaspersky Security Center

EventTracker v9.0 and above

Publication Date: September 30, 2019

Abstract

This guide will facilitate a **Kaspersky Security Center** user to send logs to **EventTracker.**

Scope

The configurations detailed in this guide are consistent with EventTracker 9.x or later and Kaspersky Security Center 10.

Audience

Administrators who want to monitor the Kaspersky Security Center using EventTracker.

Table of Contents

1.Introduction

Kaspersky Lab offers consumer security products, such as anti-virus, anti-malware and firewall applications, in addition to security systems designed for small businesses, corporations and large enterprises. Corporate solutions include protection for workstations, file servers, mail servers, payment gateways, banking servers, mobile devices, and internet gateways managed through a centralized administration kit. These applications are also available in bundled security suites scaled to fit the requirements of organizations of varying sizes.

1.1. Pre-requisites

- **EventTracker 9.x or later** should be installed.
- **EventTracker Agent** to be installed on Kaspersky Security Center administrative server.
- **Advance licensed Kaspersky** is required to forward the syslog.

1.2. Enabling Kaspersky Event Logs and Sending logs to EventTracker

1. Open Kaspersky Security Center 10 and go to **Administration Server.**

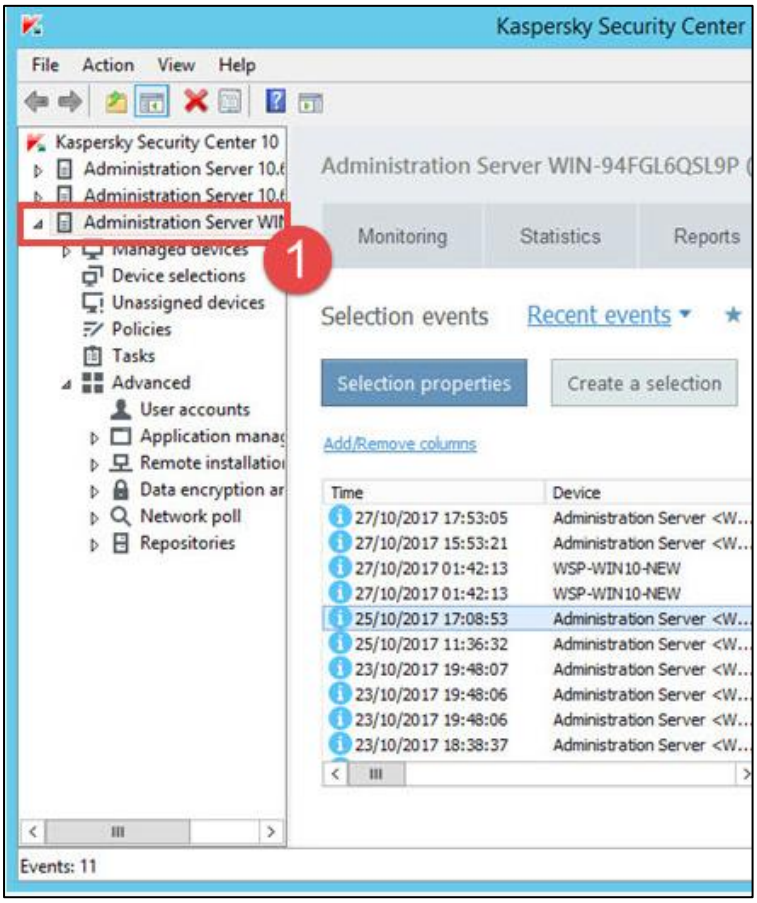

Figure 1

2. In Admin **Administration Server**, select **Events** in the right frame.
3. Click on **Configure notifications and event export.**

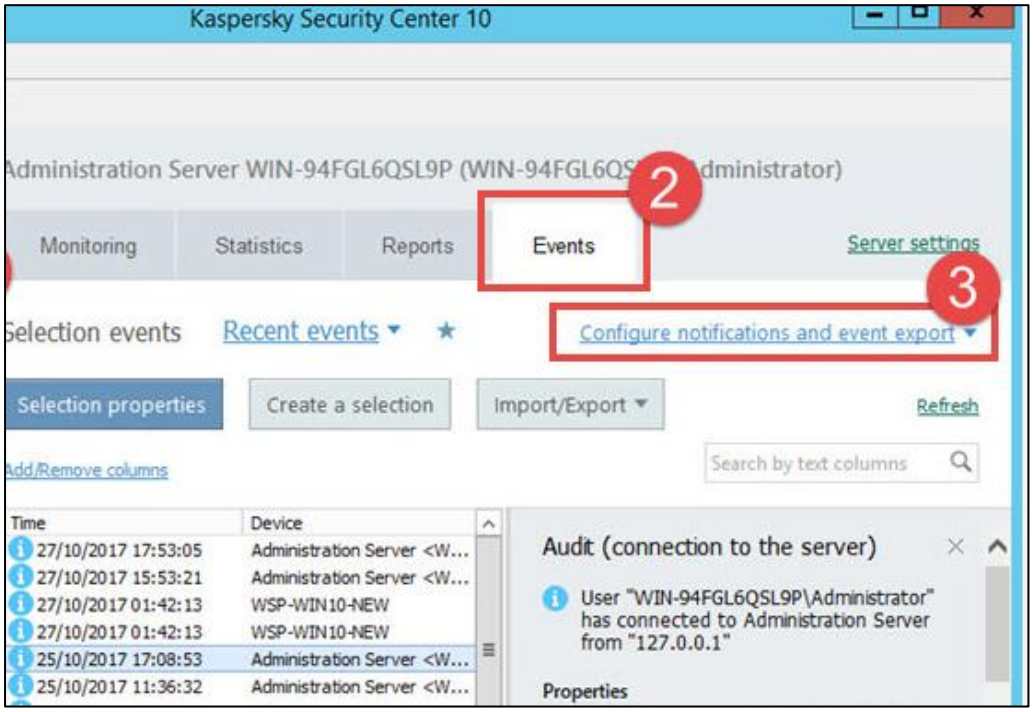

Figure 2

4. Select **Configure export to the SIEM system**.

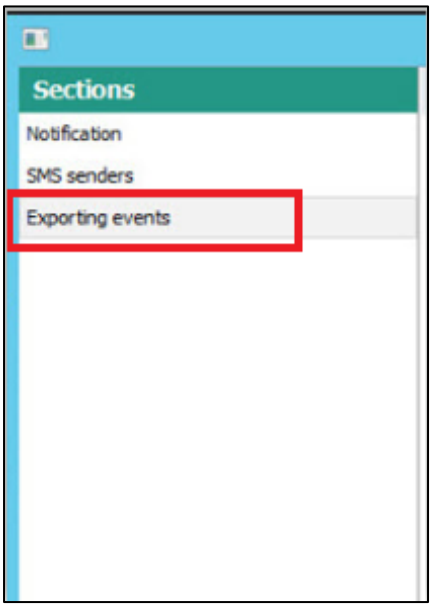

Figure 3

5. Select the check box **Automatically export events to the SIEM system database**.

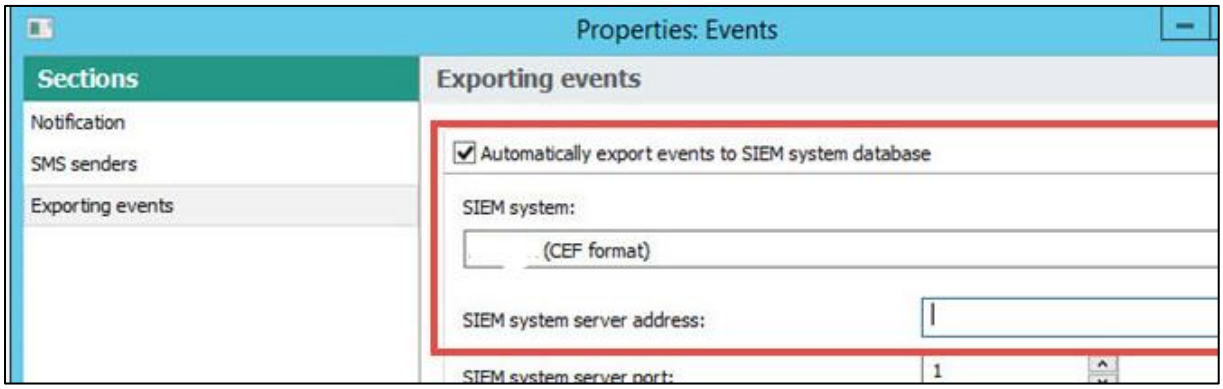

Figure 4

6. Choose the **SIEM** system. Specify the EventTracker Manager address.
7. Click **OK**.

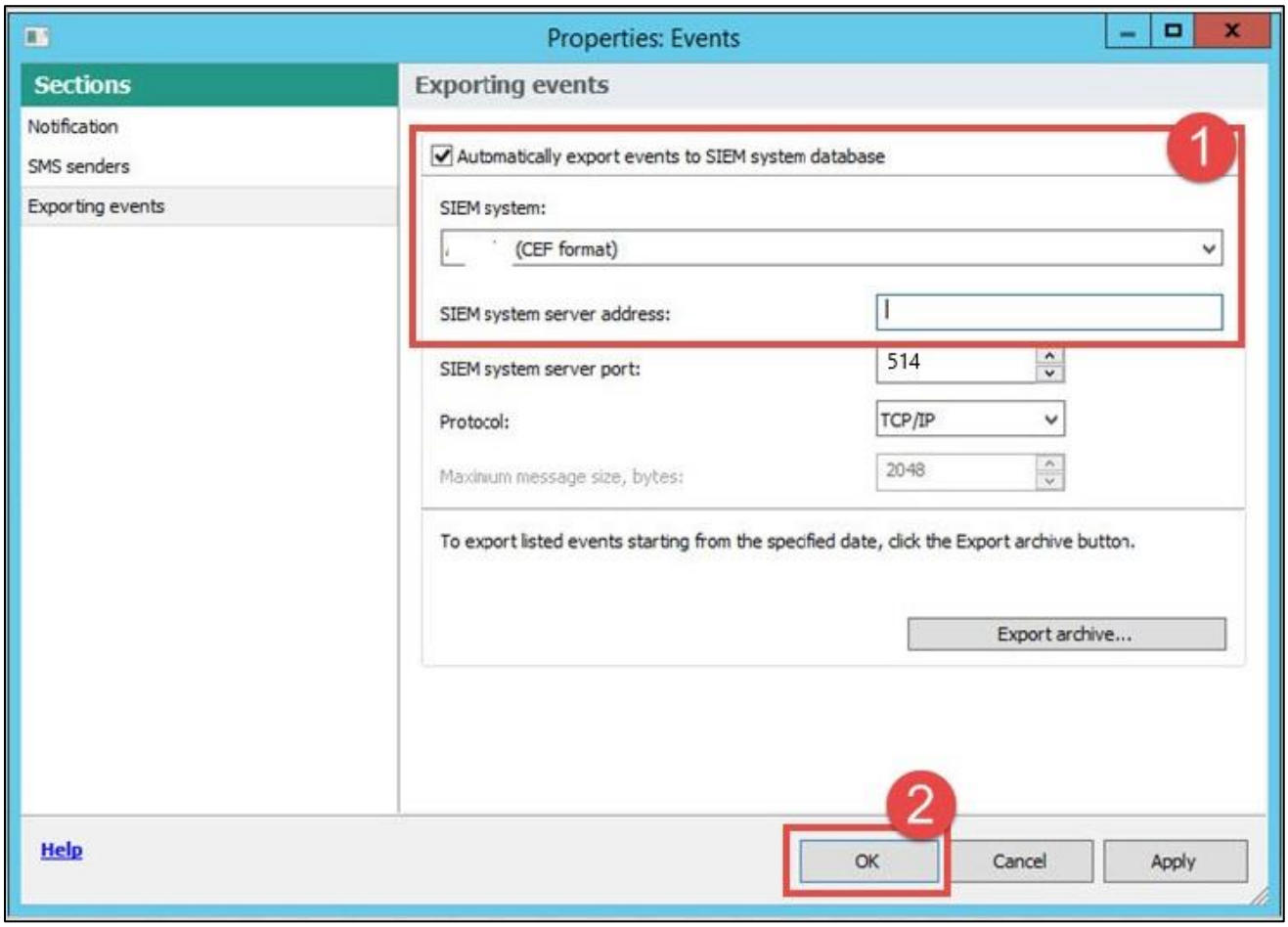

Figure 5

2.EventTracker Knowledge Pack

Once Kaspersky Security Center events are enabled and Kaspersky Security Center events are received in EventTracker, Alerts, and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support the Kaspersky Security Center monitoring.

2.1. Categories

- **Kaspersky Security Center: Report management:** This category provides information related to report management when a report is added, deleted or modified on Kaspersky Security Center.

- **Kaspersky Security Center: Task management**: This category provides information related to task management when a task is added, deleted or modified on Kaspersky Security Center.

- **Kaspersky Security Center: Policy management:** This category provides information related to policy management when a policy is added, deleted or modified on Kaspersky Security Center.

- **Kaspersky Security Center: Group task management:** This category provides information related to group task management when a group task is added, deleted or modified on Kaspersky Security Center.

- **Kaspersky Security Center: Administrative group management**: This category provides information related to administrative group management when an administrative group is added, deleted or modified on Kaspersky Security Center.

- **Kaspersky Security Center: Malicious object scan status:** This category provides information related to the malicious object which has been detected and untreated on Kaspersky Security Center.

- **Kaspersky Security Center: Application privilege management:** This category provides information related to applications that have been added to the trusted group on Kaspersky Security Center.

- **Kaspersky Security Center: Application settings change:** This category provides information related to applications where their settings are changed on Kaspersky Security Center.

- **Kaspersky Security Center: Blocked files**: This category provides information related to files which are being blocked by Kaspersky Security Center.

- **Kaspersky Security Center: Device Control:** This category provides information related to devices which have been blocked when inserted into the Kaspersky Security Center system.
- **Kaspersky Security Center: Malware detected:** This category provides information related to malwares which have been detected in the system of Kaspersky Security Center.
- **Kaspersky Security Center: Object quarantine:** This category provides information related to malware objects which are added into the quarantine list in Kaspersky Security Center.
- **Kaspersky Security Center: Task management:** This category provides information related to task management of Kaspersky Security Center.
- **Kaspersky Security Center: Vulnerability detected:** This category provides information related to a vulnerability which has been detected in Kaspersky Security Center.

2.2. Alerts

- **Kaspersky Security Center: Attack Detected:** This alert is generated when an Alert is detected in the Kaspersky Security Center.
- **Kaspersky Security Center: Suspicious Object Found:** This alert is generated when a malicious/Suspicious object is detected in Kaspersky Security Center.
- **Kaspersky Security Center: Virus Found:** This Alert is generated when one of the files or web Viruses is detected in the Kaspersky Security Center.

2.3. Report

- **Kaspersky Security Center- Suspicious Object Found:** This report provides information related to malware detected in the web for which the user tries to access an unidentified object.

Logs considered

Jan 14 05:04:28 ccc-app9 CEF:0|KasperskyLab|SecurityCenter|10.3.407|GNRL_EV_SUSPICIOUS_OBJECT_FOUND|Probably infected object detected|4|msg=Result: Detected: not-a-virus:WebToolbar.Win32.Asparnet.gen\r\nUser: CCCNTR\\CCC5055$ (Initiator)\r\nObject: C:\\Program Files (x86)\\askpartnernetwork\\toolbar\\updater\\tbnotifier.exe\r\n rt=1547463838 dhost=CCC5055 dst=192.168.6.242 cs2=KES cs2Label=ProductName cs3=10.2.4.0 cs3Label=ProductVersion filePath=C:\Program Files (x86)\AskPartnerNetwork\Toolbar\Updater\TBNotifier.exe cs1=not-a-virus:WebToolbar.Win32.Asparnet.gen cs1Label=VirusName duser=CCCNTR\CCC5055$

Sample Report

EventSource	EventDescription	Destination Host	Destination IP	Product Name	Product Version
syslog	Jan 13 12:53:54 ccc-app9 CEF:0|KasperskyLab|SecurityCenter|10.3.407|KLPRCI_TaskState|Completed|1|rt=1547405610 dhost=CCC5352 dst=192.168.10.190 cs2=KES cs2Label=ProductName cs3=10.2.4.0 cs3Label=ProductVersion cs5=Database Update cs5Label=TaskName cs4=324 cs4Label=TaskId cn2=4 cn2Label=TaskNewState cn1=1	CCC5352	192.168.10.190	KES	10.2.4.0
syslog	Jan 13 12:54:24 ccc-app9 CEF:0|KasperskyLab|SecurityCenter|10.3.407|KLPRCI_TaskState|Completed|1|rt=1547405643 dhost=CCC5358 dst=192.168.11.243 cs2=KES cs2Label=ProductName cs3=10.2.4.0 cs3Label=ProductVersion cs5=Database Update cs5Label=TaskName cs4=324 cs4Label=TaskId cn2=4 cn2Label=TaskNewState cn1=1	CCC5358	192.168.11.243	KES	10.2.4.0

- **Kaspersky Security Center-Task Status Updated:** This report provides information related to task management where the task is started or stopped.

Logs considered

Jan 14 05:07:58 ccc-app9 CEF:0|KasperskyLab|SecurityCenter|10.3.407|KLPRCI_TaskState|Completed|1|rt=1547464052 dhost=CCC-RD-HOST11 dst=192.168.0.101 cs2=WSEE cs2Label=ProductName cs3=10.0.0.0 cs3Label=ProductVersion cs5=Server Database Update cs5Label=TaskName cs4=204 cs4Label=TaskId cn2=4 cn2Label=TaskNewState cn1=1 cn1Label=TaskOldState

Sample Report

EventId	EventUser	Computer	EventSource	EventDescription
123458	N/A	KASPERSKY	Syslog	Jan 14 04:57:58 ccc-app9 CEF:0|KasperskyLab|SecurityCenter|10.3.407|GNRL_EV_SUSPICIOUS_OBJECT_FOUND|Probably infected object detected|4|msg=Result: Detected: not-a-virus:WebToolbar.Win32.Asparnet.gen User: CCCNTR\CCC5055$ (Initiator) Object: C:\Program Files (x86)\askpartnernetwork\toolbar\updater\tbnotifier.exe rt=1547463462 dhost=CCC5055 dst=192.168.6.242 cs2=KES cs2Label=ProductName cs3=10.2.4.0 cs3Label=ProductVersion filePath=C:\Program Files (x86)\AskPartnerNetwork\Toolbar\Updater\TBNotifier.exe cs1=not-a-virus:WebToolbar.Win32.Asparnet.gen cs1Label=VirusName duser=CCCNTR\CCC5055$

3.Importing Kaspersky Security Center knowledge pack into EventTracker

1. Launch the **EventTracker Control Panel**.
2. Double click **Export Import Utility**, and then click the **Import** tab.

   Import **Token Templates/Category/Alert/Tokens/ Flex Reports** as given below.

   Note: Importing should be in the same order as mentioned above.

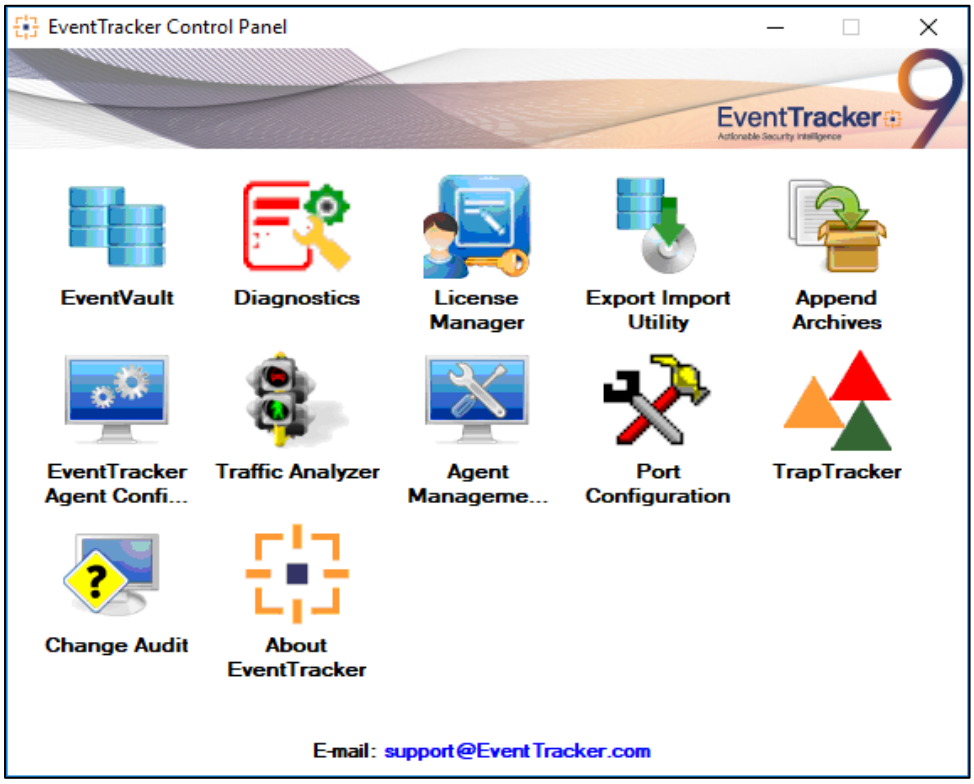

Figure 6

3.1. Category

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

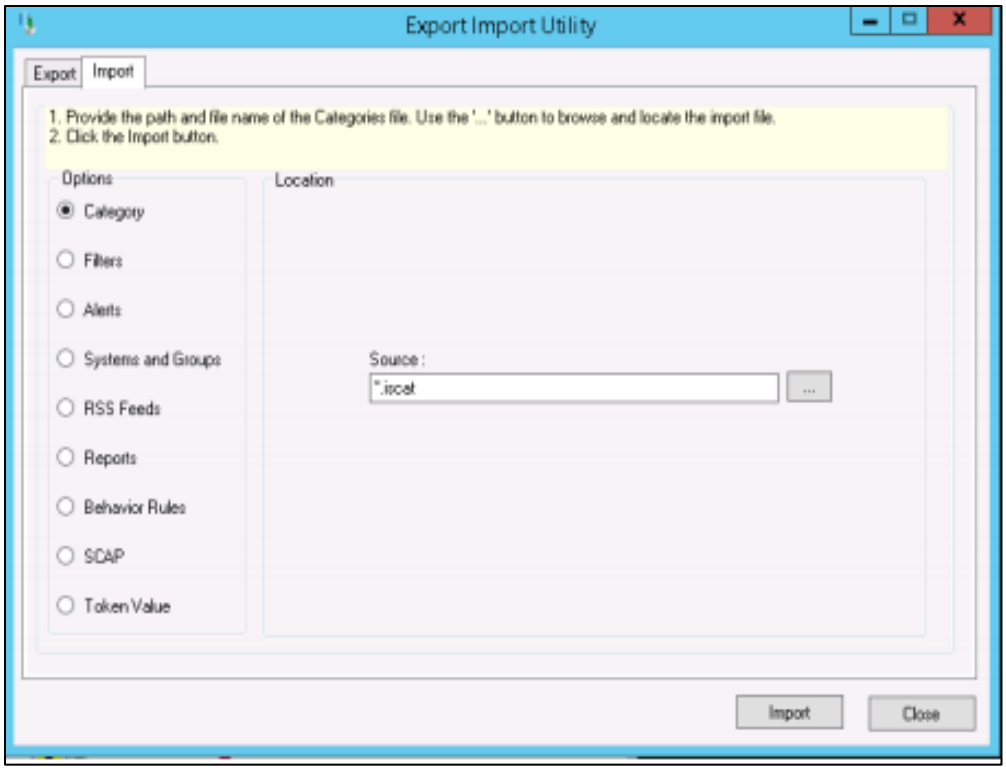

Figure 7

2. Locate **All Kaspersky Security Center group of Categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays a success message.

Figure 8

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

3.2. Alerts

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

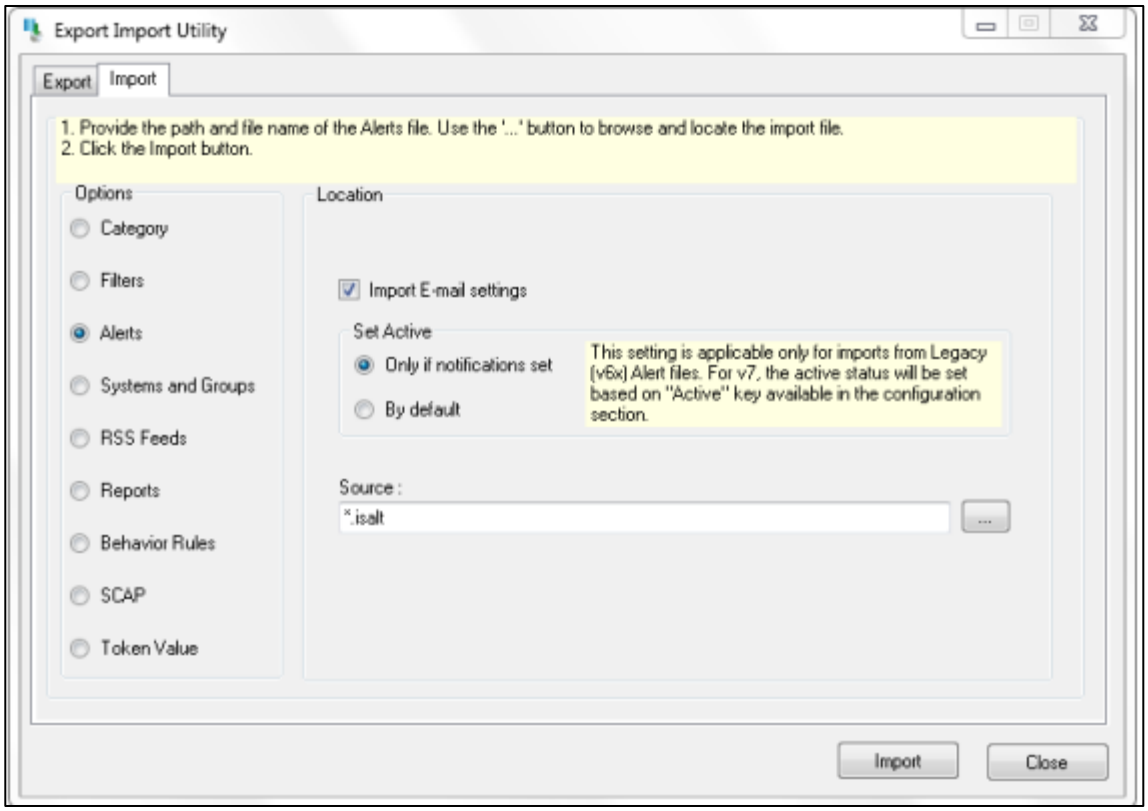

Figure 9

2. Locate **All Kaspersky Security Center group of Alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays a success message.

Figure 10

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

3.3. Flex Reports

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

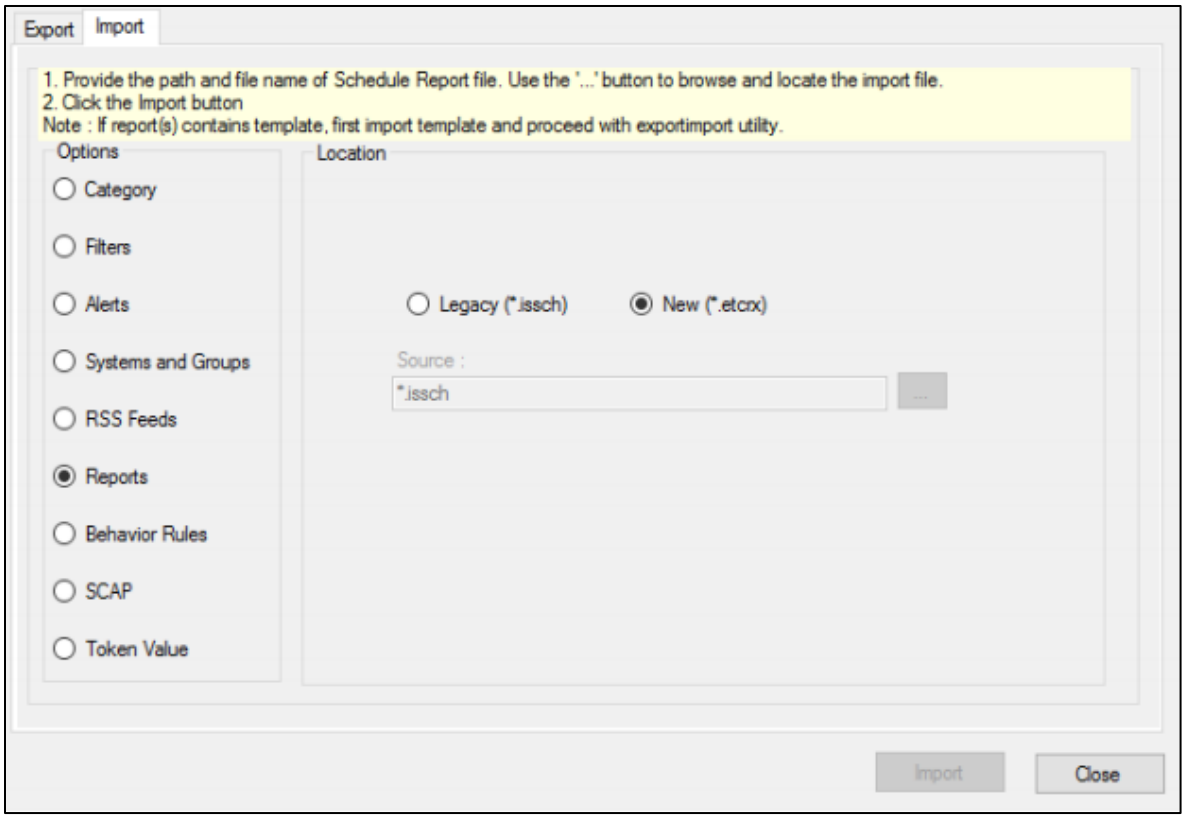

Figure 11

2. Locate **All Kaspersky Security Center group of Flex Report.issch** file, and then click the **Open** button.
3. To import reports, click the **Import** button.

   EventTracker displays a success message.

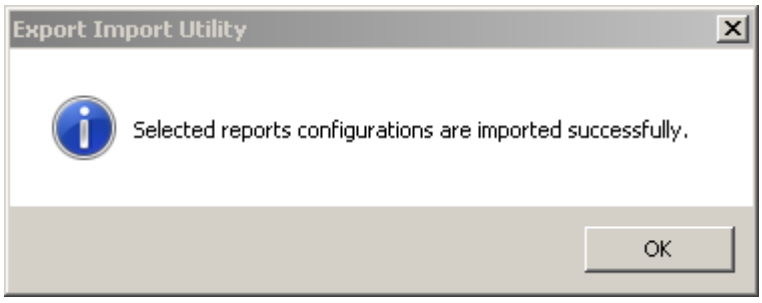

Figure 12

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

3.4. Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select the **Template** tab, and then click on ‘**Import**’ option.

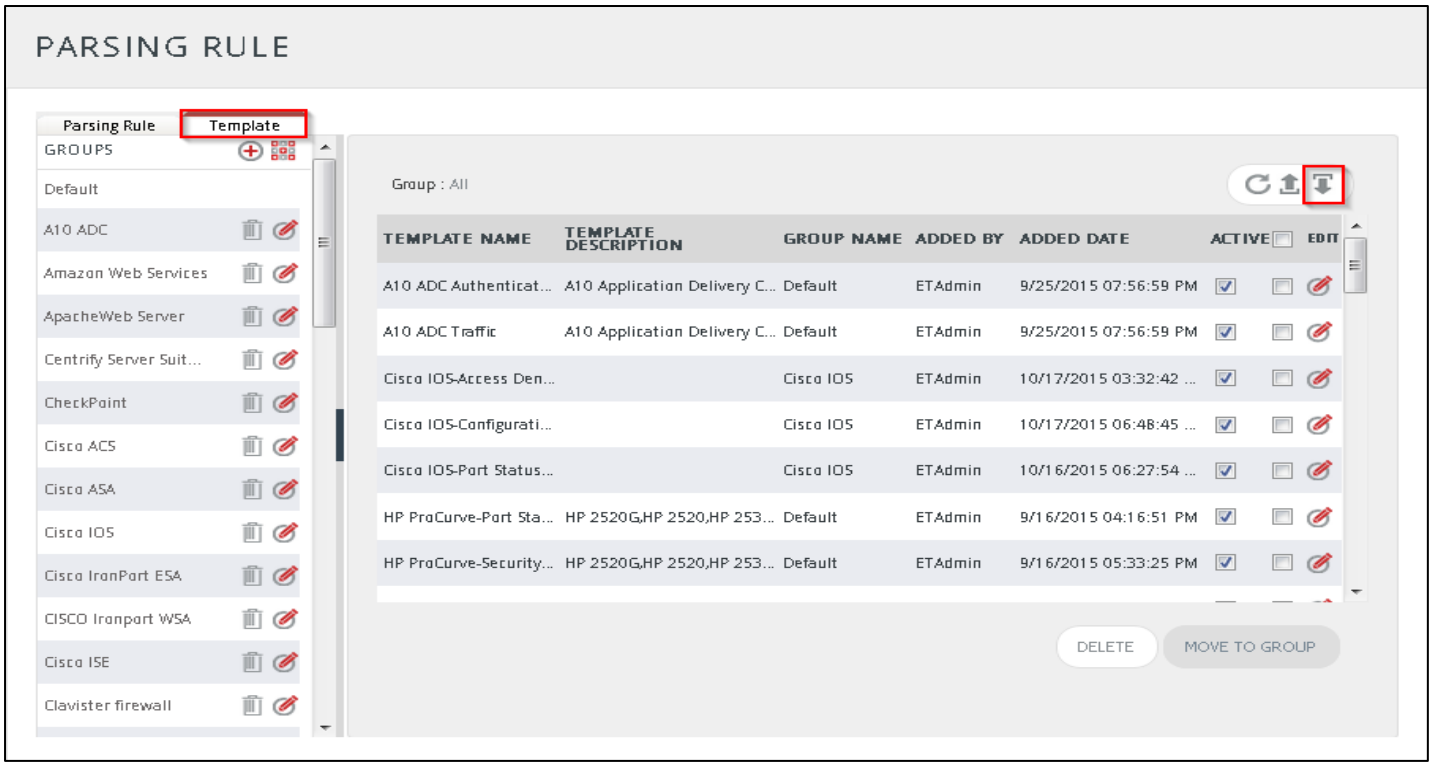

Figure 13

3. Click on the **Browse** button.

Figure 14

4. Locate **All Kaspersky Security Center group of template.ettd** file, and then click the **Open** button.

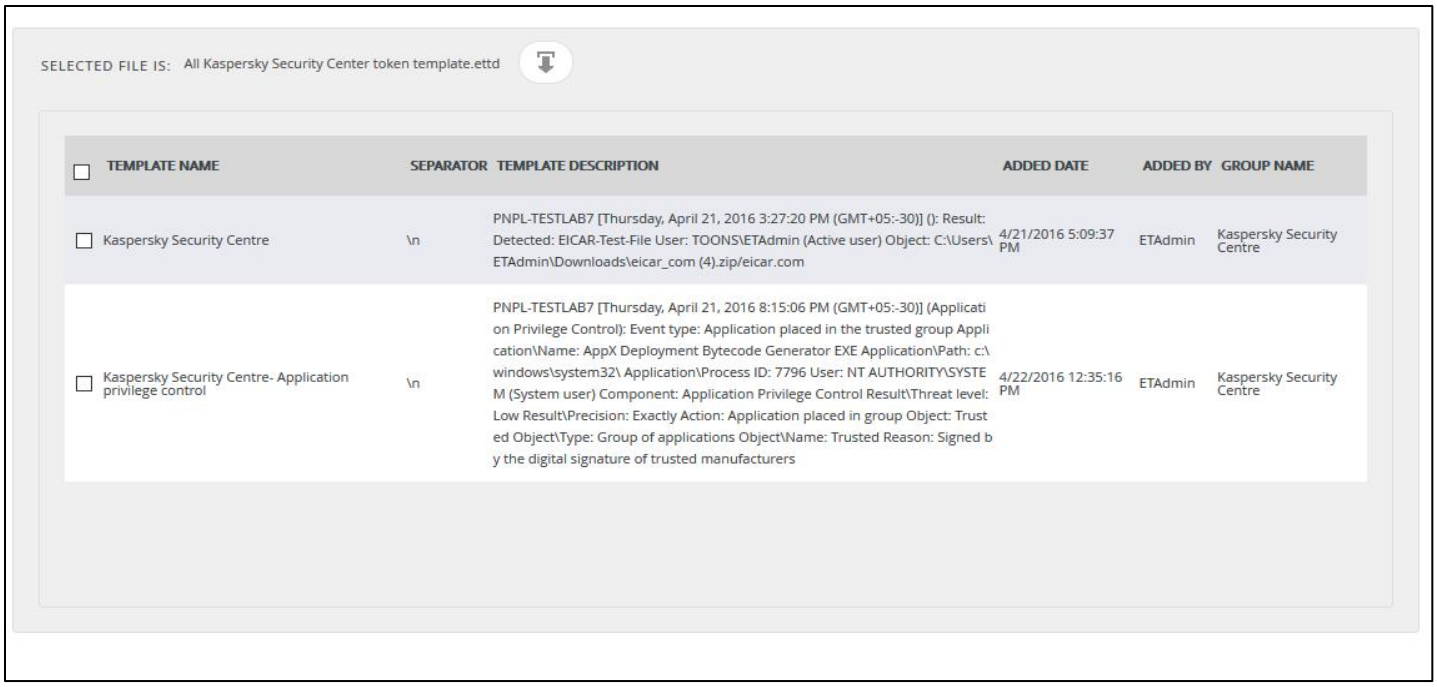

Figure 15

5. Now select the check box and then click on ‘**Import**’ option. EventTracker displays a success message.

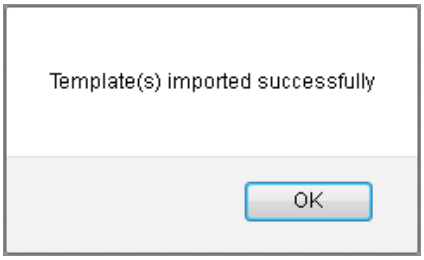

Figure 16

6. Click on the **OK** button.

4.Verifying Kaspersky Security Center knowledge pack in EventTracker

4.1. Categories

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand the **Kaspersky Security Center** group folder to view the imported categories.

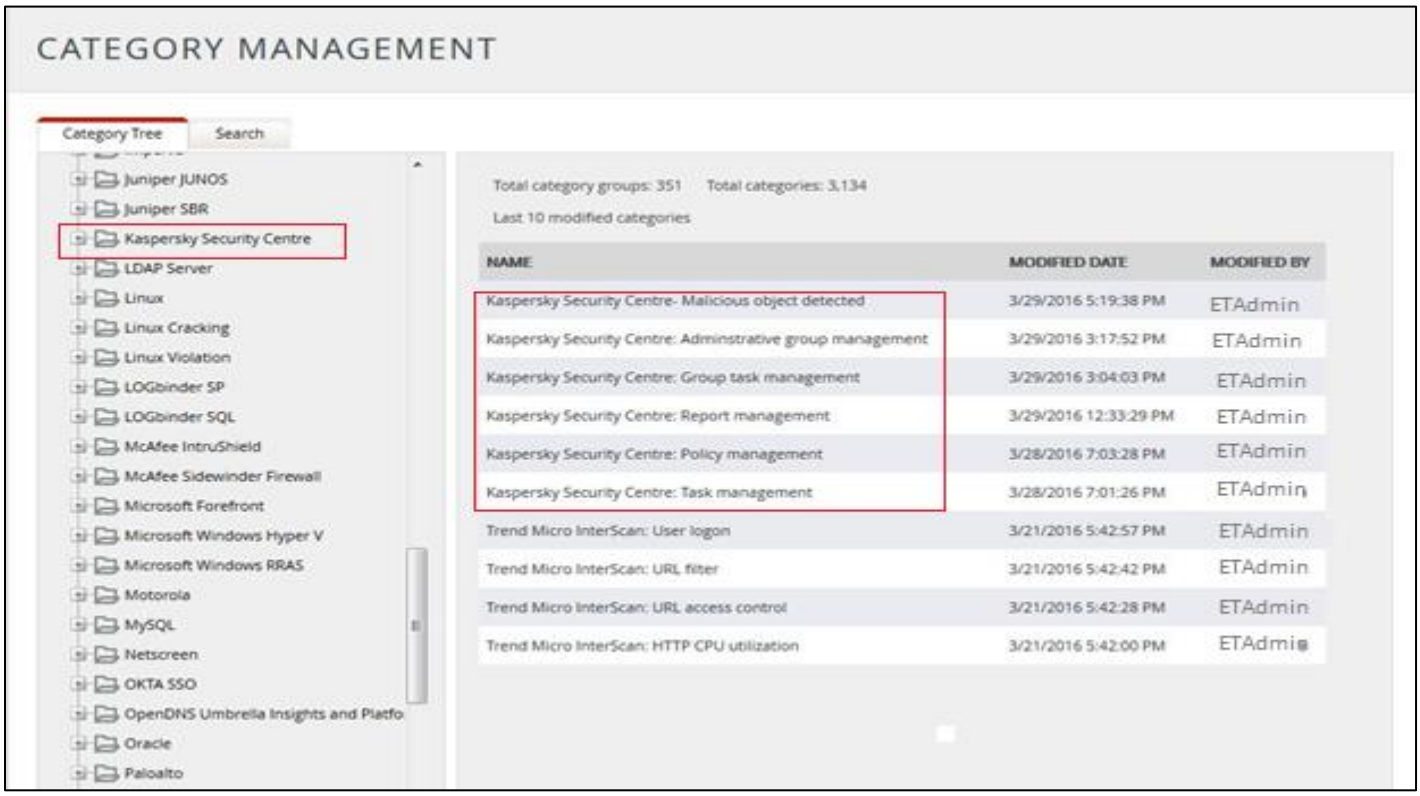

Figure 17

4.2. Alerts

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** field, type '**Kaspersky Security Center**', and then click the **Go** button.

Alert Management page will display all the imported Kaspersky Security Center alerts.

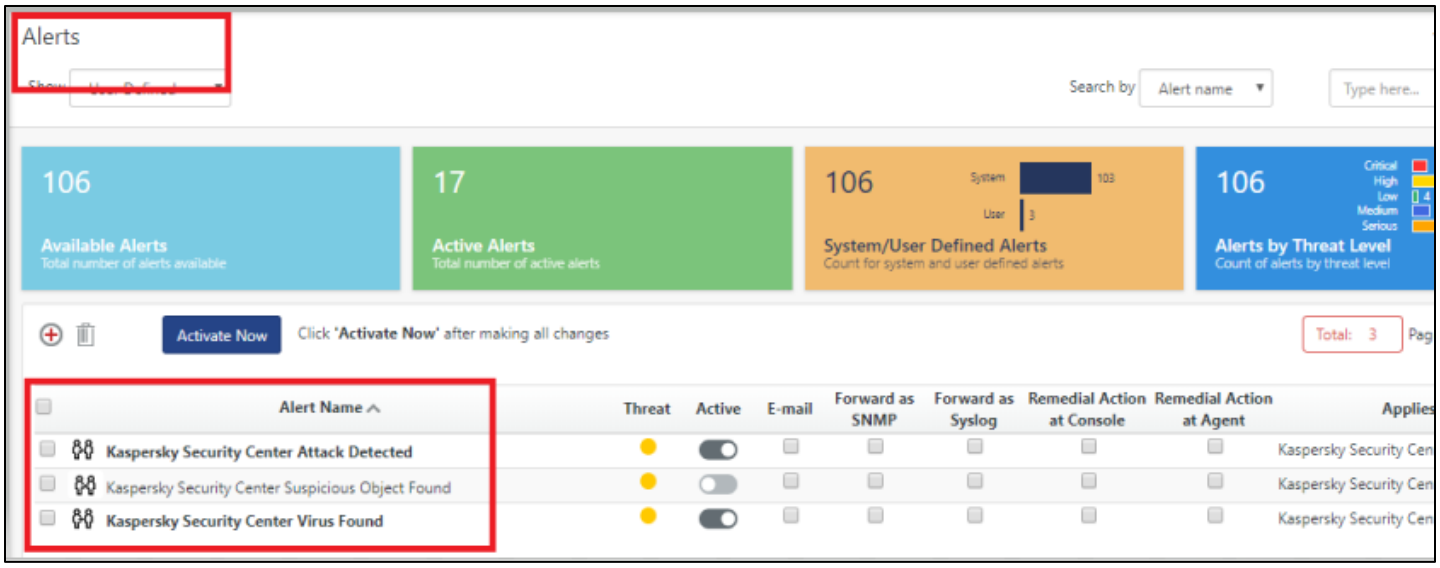

Figure 18

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

EventTracker displays a message box.

Figure 19

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

NOTE:

You can select alert notification such as Email, and Message, etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

4.3. Reports

1. Logon to **EventTracker**.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select the **Defined** option.

EventTracker displays the **Defined** page.

4. In search box enter '**Kaspersky Security Center**', and then click the **Search** button.

   EventTracker displays Flex reports of Kaspersky Security Center.

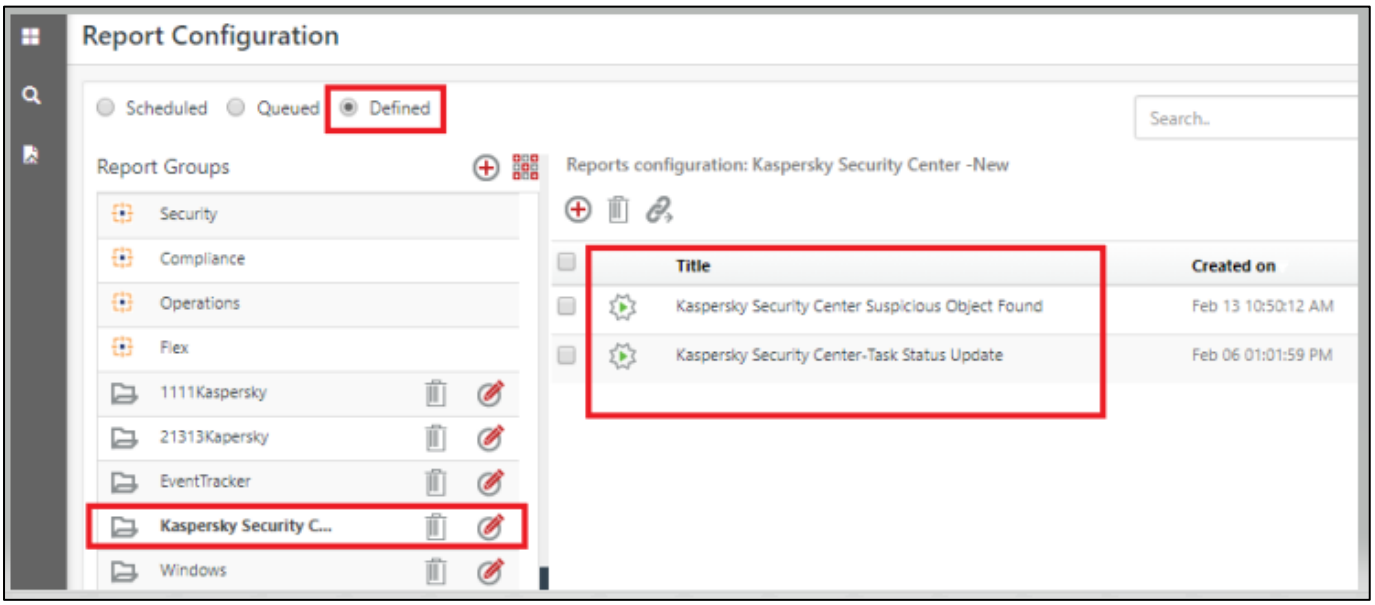

Figure 20

4.4. Token Template

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Parsing Rules**.

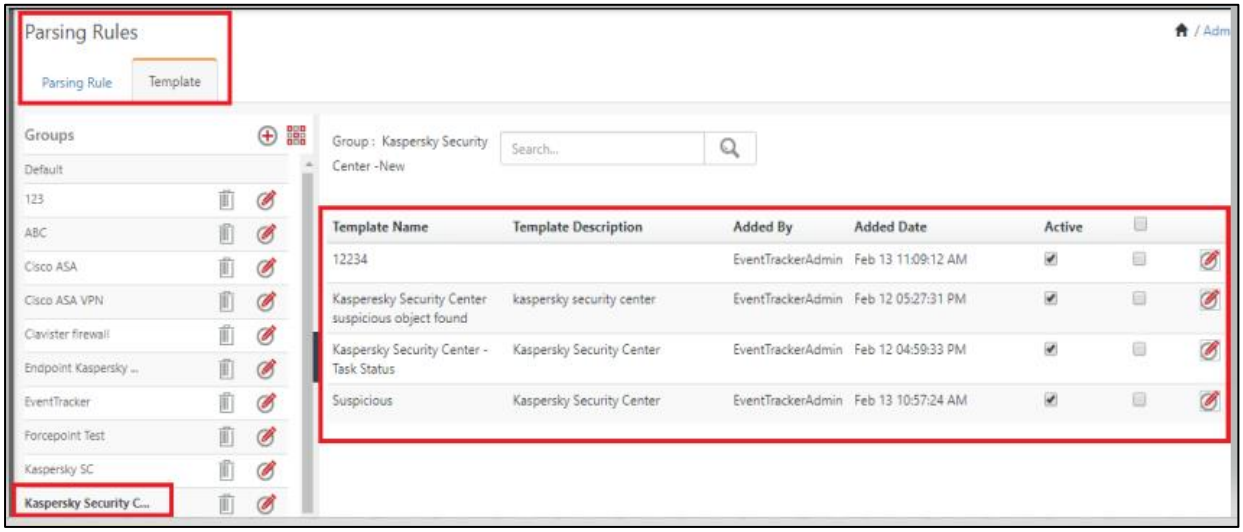

Figure 21

5.Sample Dashboards

- **Kaspersky Security Center-** Suspicious object Found by Host

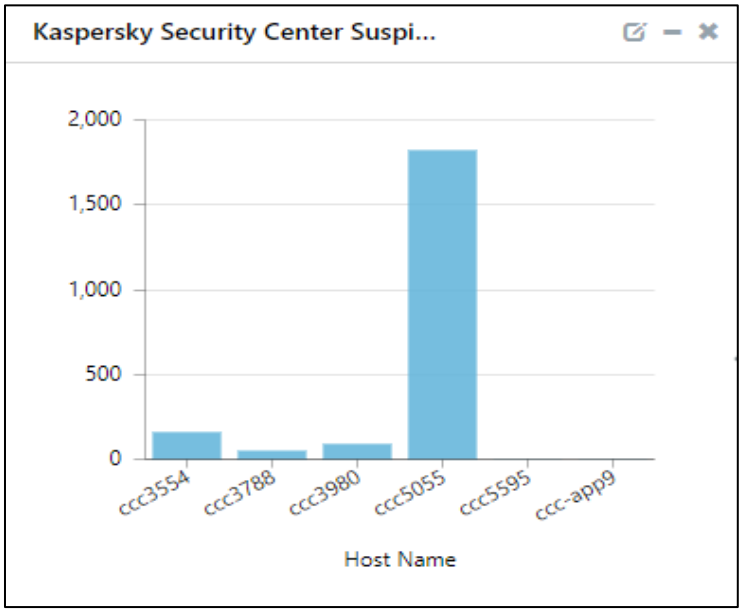

Figure 22

- **Kaspersky Security Center-** Suspicious object Found on IP Address

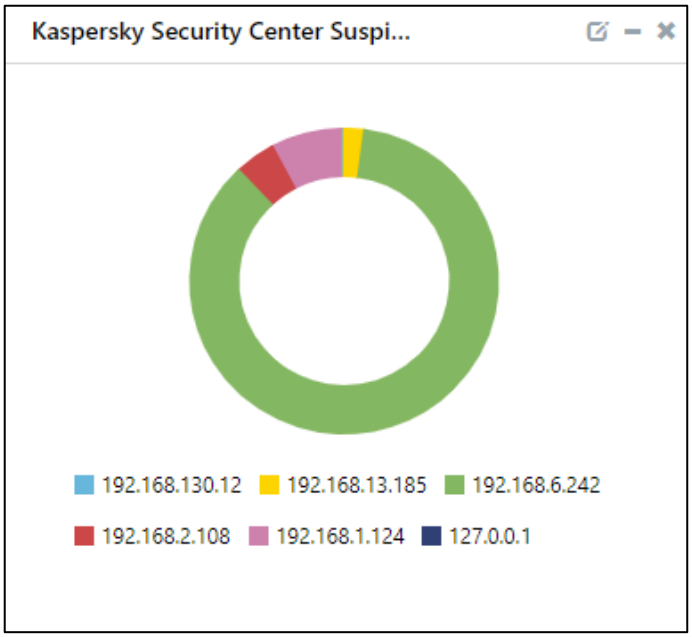

Figure 23

- **Kaspersky Security Center-** Suspicious object Found by Threat

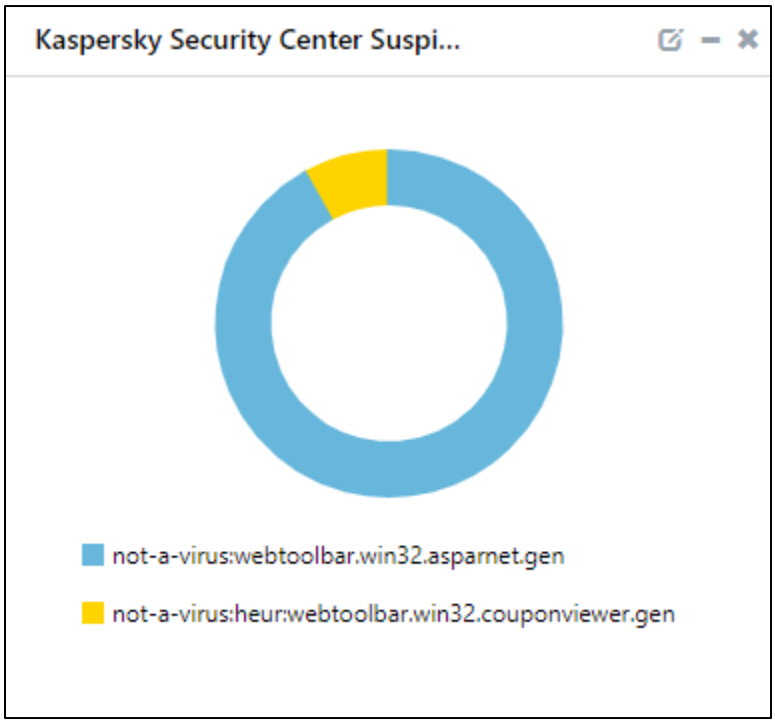

Figure 24

- **Kaspersky Security Center-** Suspicious object Found by user

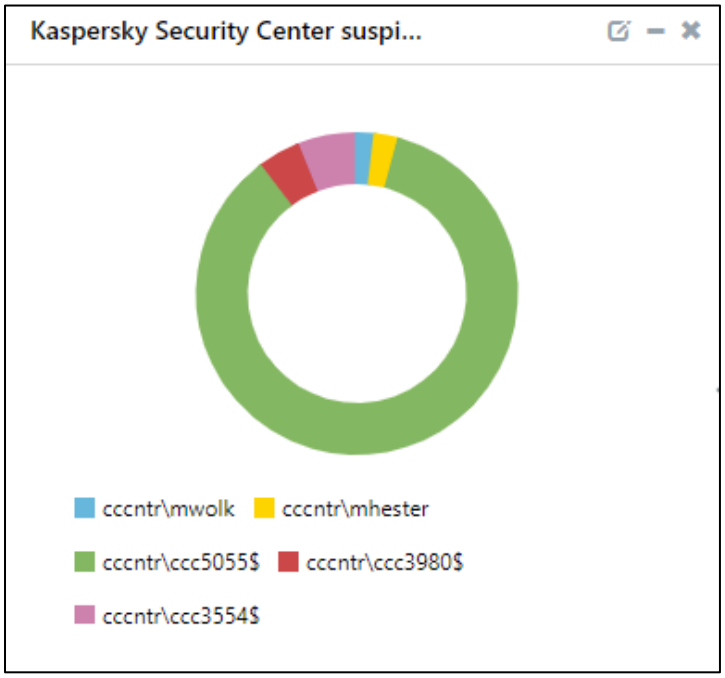

Figure 25

- **Kaspersky Security Center-** Suspicious object Found by Task Status

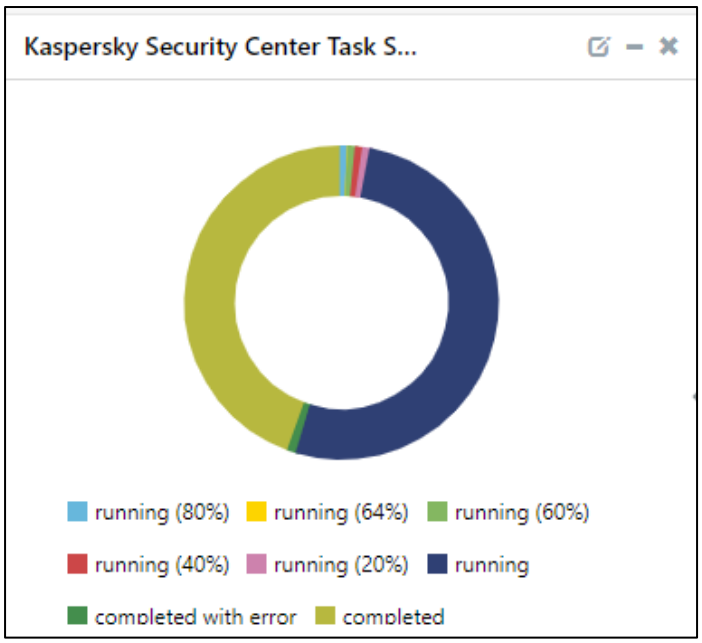

Figure 26

- **Kaspersky Security Center-** Suspicious object Found by System

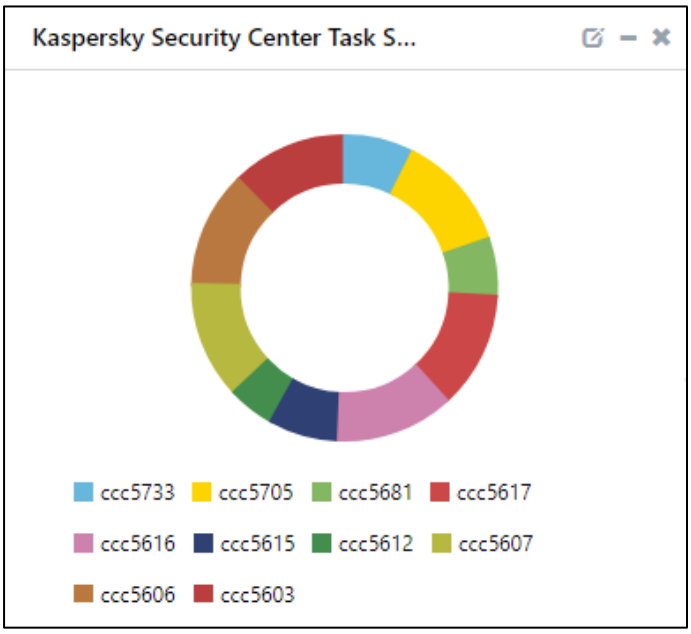

Figure 27