Netsurion | EventTracker®

Integrate Barracuda Essentials with EventTracker

EventTracker v9.0 and above

Publication Date: January 22, 2020

Abstract

This guide will facilitate a **Barracuda Essentials** users to send logs to **EventTracker.**

Scope

The configurations detailed in this guide are consistent with **EventTracker 9.x or later and Barracuda Essentials.**

Audience

Administrators who want to monitor the **Barracuda Essentials** using **EventTracker**.

Table of Contents

1. Introduction

Barracuda Essentials provides critical multi-layer security, archiving, and backup for Office 365, Microsoft Exchange, and G Suite.

The Barracuda Essentials service basically consists of:

- **Barracuda Email Security**
- **Barracuda Cloud Archiving Service**
- **Barracuda Cloud Backup**

Barracuda Essentials event is integrated with EventTracker via syslog. It helps to monitor both inbound and outbound emails against the latest spams, viruses, worms, and phishing.

Reports provide a detailed information about the email traffic allowed and email traffic blocked.

Reports provide insight into the security statistics like suspicious email such as spam links and suspicious attachments. One can analyze suspicious emails using the dashboards, we can view the top sender and recipient. Dashboards show emails with spam links, suspicious attachments along with action taken like blocked, quarantined and deferred with reason. Alerts are generated if emails have spam links, malicious attachments, and those that are getting blocked.

1.1 Pre-requisites

- The host machine should have installed the **EventTracker agent**.
- Administrator privilege for **Barracuda Essentials web interface**.
- Please use a new port that should support TCP+TLS certificate enabled in EventTracker for receiving Barracuda Essentials syslog messages.
- EventTracker manager IP address and TCP+TLS certificate enabled port should be publically reachable.

Note: Please enable EventTracker bad syslog receiving to receive Barracuda Essentials syslog messages.

1.2 Integrating Barracuda Essentials events to EventTracker via syslog

1. Log into Barracuda Essentials web console (In Barracuda Cloud Control, in the left panel, click Barracuda Email Security Service) and navigate to the **Account Management** tab.

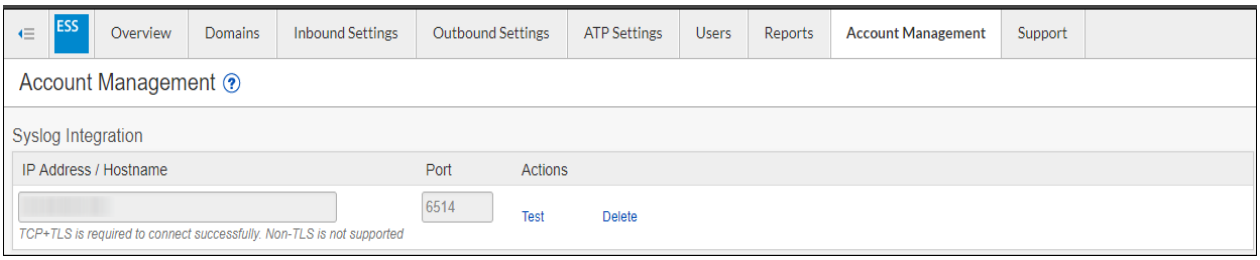

Figure 1

2. Open any firewall ports needed for communicating with EventTracker.
3. Enter the **IP Address/Hostname** and **Port** for EventTracker Manager syslog VCP port.
    - **IP Address/Hostname**: Enter EventTracker Public IP address.
    - **Port**: Enter the TCP+TLS certificate enabled port number.
4. Click **Test** to ensure that the Barracuda Essentials can connect with EventTracker.

Note: If the test works, your message log data begins transferring to EventTracker.

2. EventTracker Knowledge Pack

Once Barracuda Essential's events are received in EventTracker, alerts, and reports is configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support the Barracuda Essentials monitoring.

2.1 Saved Searches

Barracuda Essentials: Not allowed traffic – This saved search will give email blocked traffic, deferred traffic, and quarantined traffic logs.

Barracuda Essentials: Allowed traffic – This saved search will give allowed email traffic.

Barracuda Essentials: Rejected traffic – This saved search will give rejected email traffic.

2.2 Alerts

Barracuda Essentials: Suspicious emails blocked – This alert will trigger whenever emails have spam links, threat attachments and blocked by Barracuda Essentials.

2.3 Report

Barracuda Essentials: Email traffic blocked: This report provides information related to email traffic blocked, deferred, and quarantined by Barracuda Essentials email security service.

Log Considered

645 <6> 2019-12-26T10:38:52Z ip-100-69-12-62.us-east-2.compute.internal ESS101777[1]: {"message_id":"1577356724-893443-25789-521440-1","src_ip":"205.233.73.32","hdr_from":"eicar@aleph-tec.com","account_id":"ESS101777","domain_id":"205534","ptr_record":"batch.outbound.your-site.com","attachments":[{"name":"SecretNumber.gif"},{"name":"eicarpasswdocr.zip"}],"recipients":[{"action":"blocked","reason":"atd_subscribed","reason_extra":"eicarpasswdocr.zip","delivered":"not_delivered","delivery_detail":"","email":"info@connect-ag.in"}],"hdr_to":"serous \u003cinfo@connect-ag.in\u003e","recipient_count":1,"dst_domain":"connect-ag.in","size":4129,"subject":"EICAR anti-virus test file:","env_from":"eicar@aleph-tec.com","timestamp":"2019-12-26T10:38:46+0000"}

Sample Report

LogTime	Action	Source IP Address	Sender Mail ID	Recipient Mail ID	Email Delivery Status	Domain Name	Reason	Reason Detailed	Attachment Names
01/14/2020 12:04:56 PM	deferred	182.74.234.198	pavankumar258589@gmail.com	info@connect-agcnet.in	not_delivered	connect-agcnet.in	sender_rset		
01/14/2020 12:04:57 PM	quarantined	100.69.30.7	noreply@barracuda.com	akash@connect-agcnet.in	rejected	connect-agcnet.in	dest_invalid_recipient		
01/14/2020 12:04:57 PM	blocked	205.233.73.32	eicar@aleph-tec.com	info@connect-agcnet.in	not_delivered	connect-agcnet.in	atd_subscribed	eicarpasswdocr.zip	{"name":"SecretNumber.gif"},{"name":"eicarpasswdocr.zip"}

Figure 2

Barracuda Essentials – Email traffic allowed: This report provides information related to inbound and outbound email traffic allowed by Barracuda Essentials email security service.

Log Considered

772 <6> 2019-12-26T10:19:09Z ip-100-69-22-95.us-east-2.compute.internal ESS101777[1]: {"message_id":"1577355532-893278-20131-541688-1","src_ip":"93.99.104.21","hdr_from":"MAILER-DAEMON@localhost (Mail Delivery System)","account_id":"ESS101777","domain_id":"205534","ptr_record":"emkei.cz","attachments":null,"recipients":[{"action":"allowed","reason":"recipient","reason_extra":"default_scan_policy:exempt","delivered":"delivered","delivery_detail":"smtp.secureserver.net:25:250 2.0.0 kQEHil5TWH1uq – kQEHil5TWH1uqkQEIitWFp mail accepted for delivery","email":"info@connect-ag.in"}],"hdr_to":"info@connect-ag.in","recipient_count":1,"dst_domain":"connect-ag.in","size":3566,"subject":"Undelivered Mail Returned to Sender","env_from":"","timestamp":"2019-12-26T10:18:54+0000"}

Sample Report

LogTime	Source IP Address	Sender Mail ID	Email Subject	Recipient Mail ID	Domain Name	Reason	Reason Detailed	Attachment Names
12/30/2019 03:57:07 PM	209.85.210.196	tirupathipavan11@gmail.com	Quarantine check	info@connect-ag.in	connect-ag.in	recipient	default_scan_policy:exempt	null
12/30/2019 03:57:07 PM	100.69.30.7	eicar@aleph-tec.com	EICAR anti-virus test file:	info@connect-ag.in	connect-ag.in	ui_delivered		null
12/30/2019 03:57:07 PM	93.99.104.21		Undelivered Mail Returned to Sender	info@connect-ag.in	connect-ag.in	recipient	default_scan_policy:exempt	null

Figure 3

2.4 Dashboards

Barracuda Essentials – Top sender detail – This dashboard shows the sender details by Barracuda Email security service.

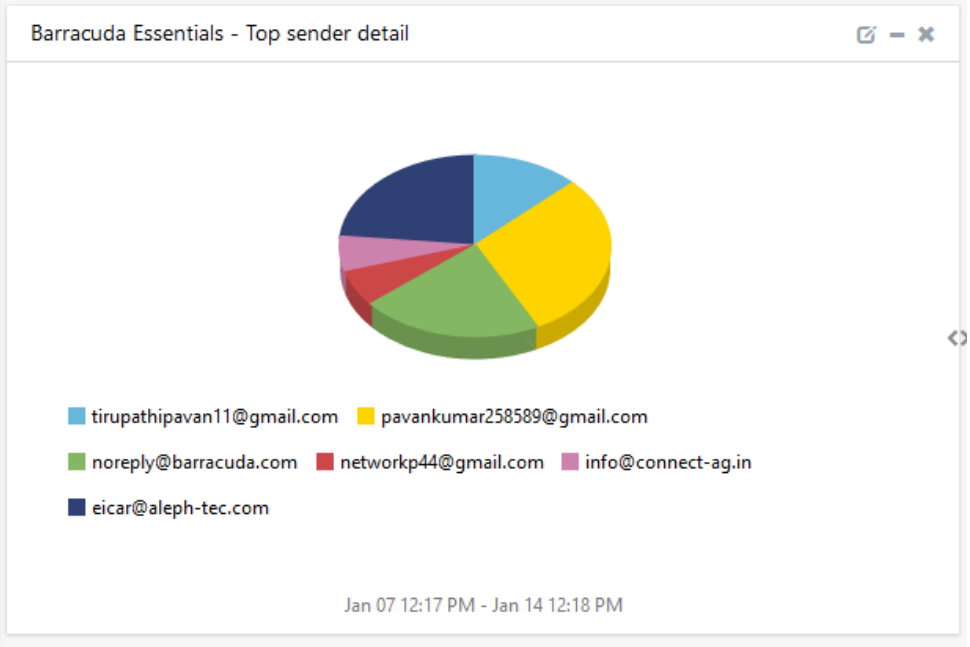

Figure 4

Barracuda Essentials – Top recipient detail- This dashboard shows the recipient details.

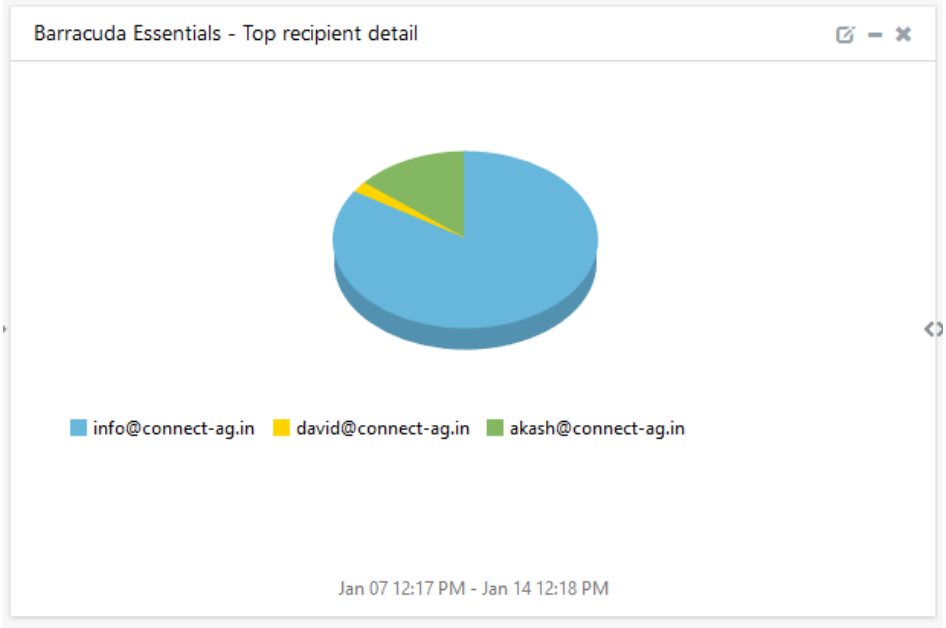

Figure 5

Barracuda Essentials – Geolocation by sender IP address – This dashboard will show sender geolocation.

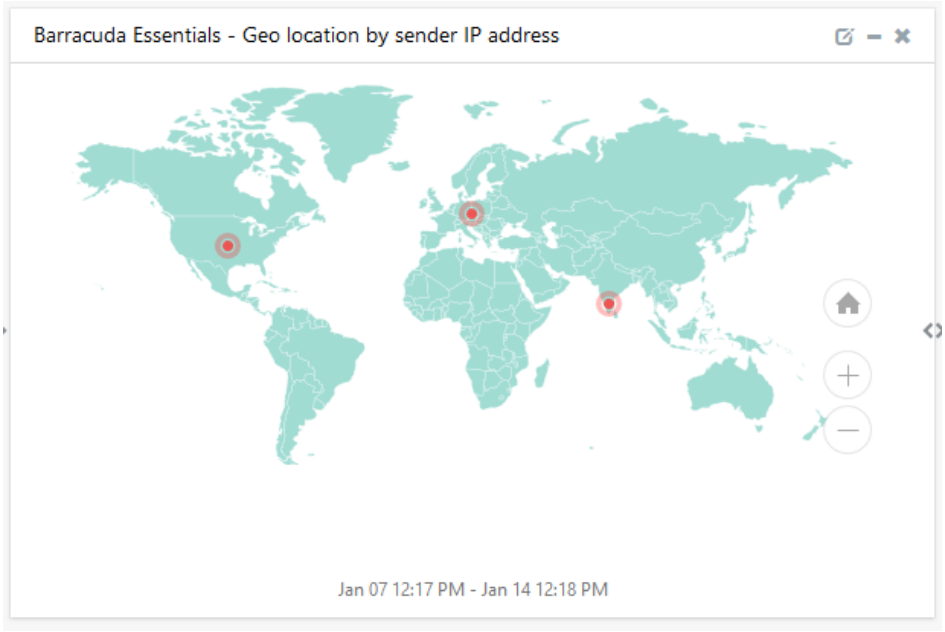

Figure 6

Barracuda Essentials – Emails blocked by reason – This dashboard will show emails blocked by reasons.

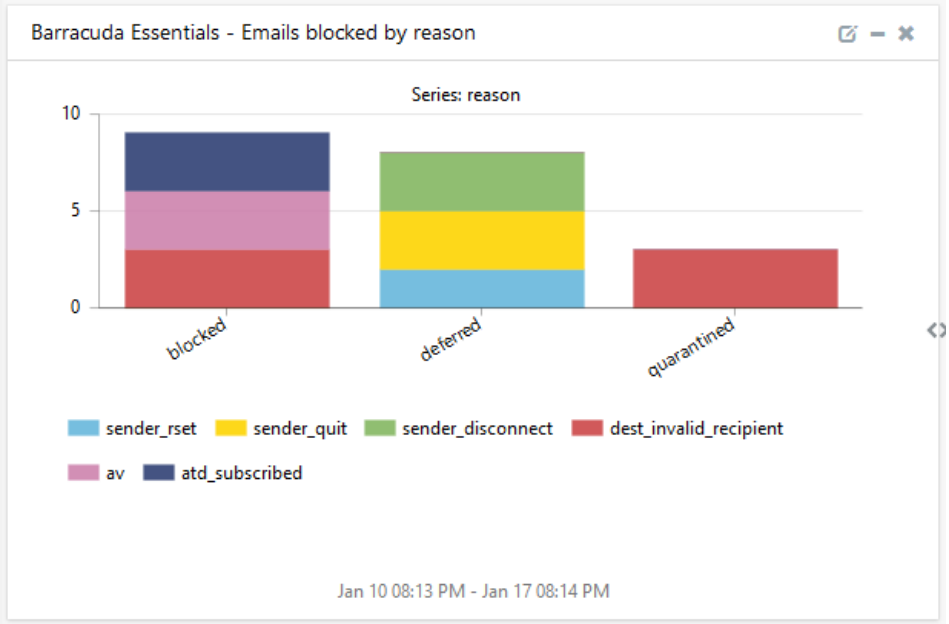

Figure 7

3. Importing 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**.

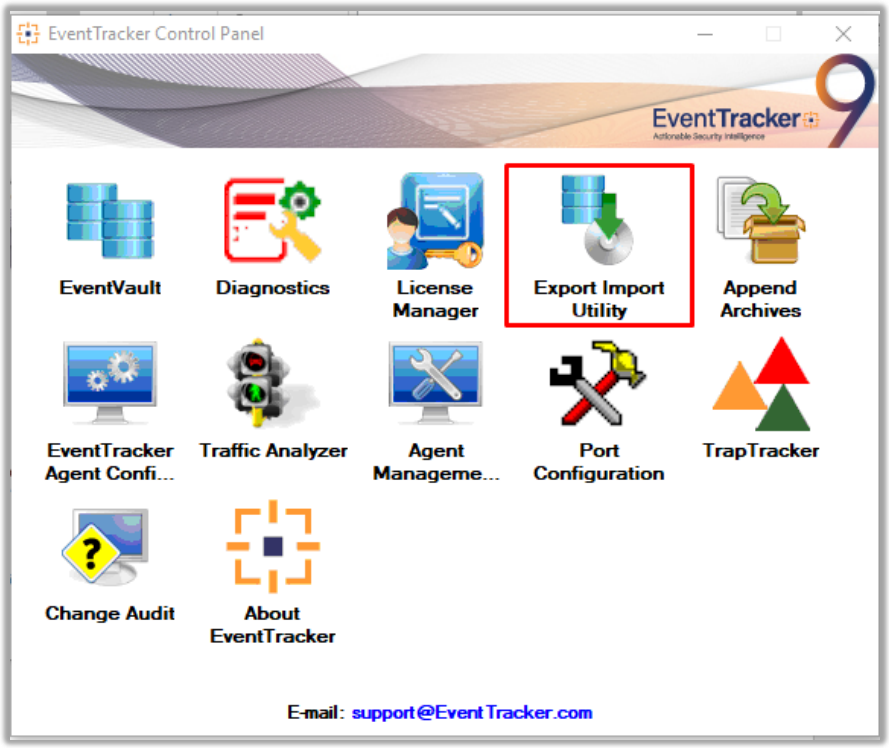

Figure 8

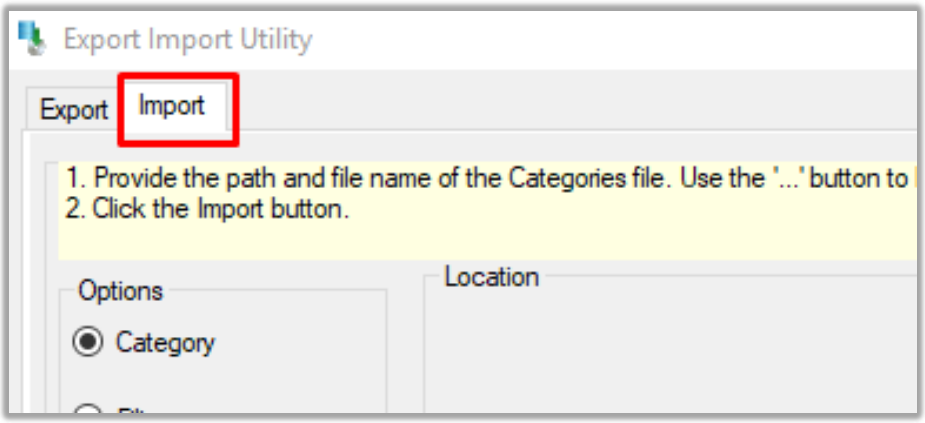

Figure 9

3. Click the **Import** tab.

3.1 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_Barracuda Essentials. iscat"** and then click on the "**Import**" button:

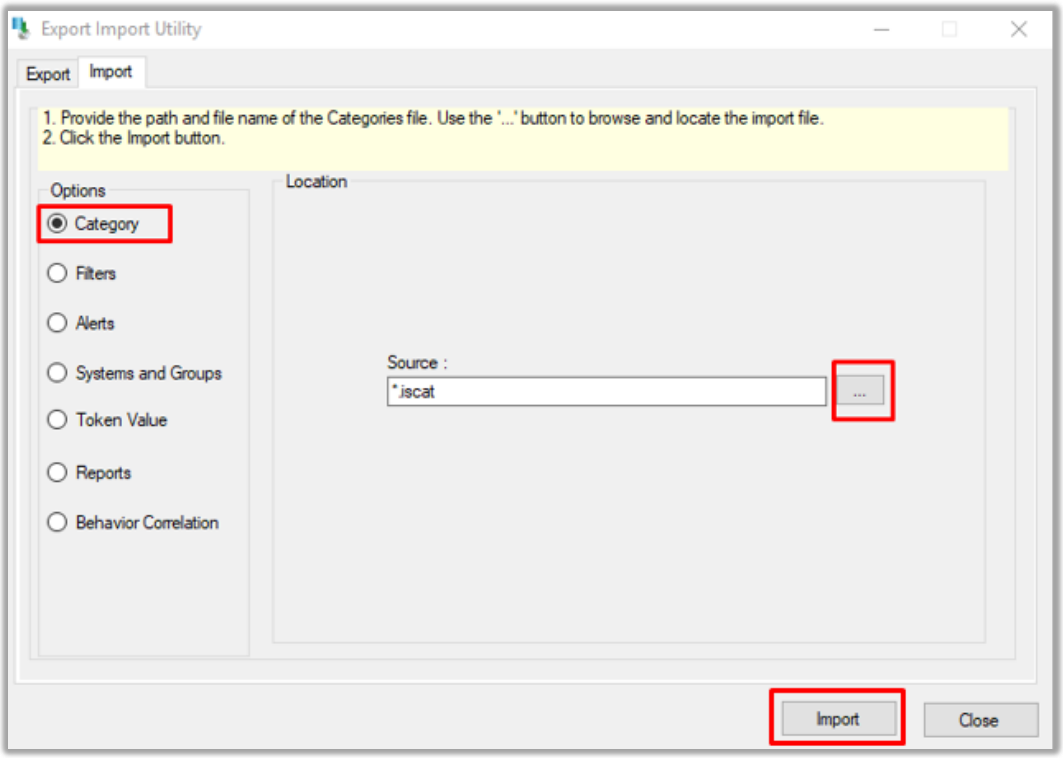

Figure 10

EventTracker displays a success message:

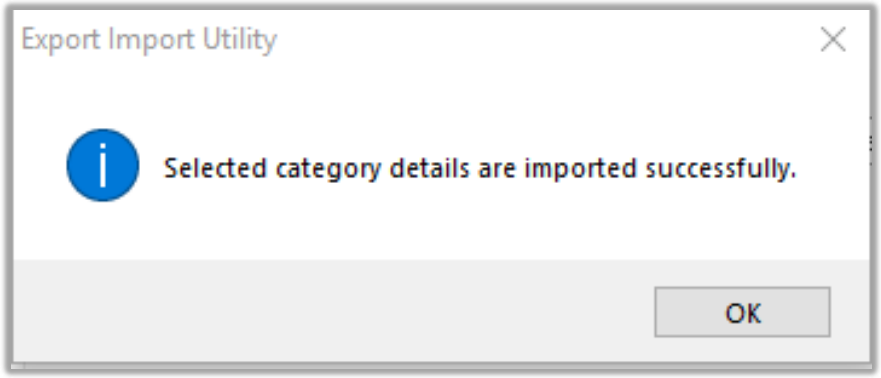

Figure 11

3.2 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_ Barracuda Essentials.isalt**" and then click on the "**Import**" button:

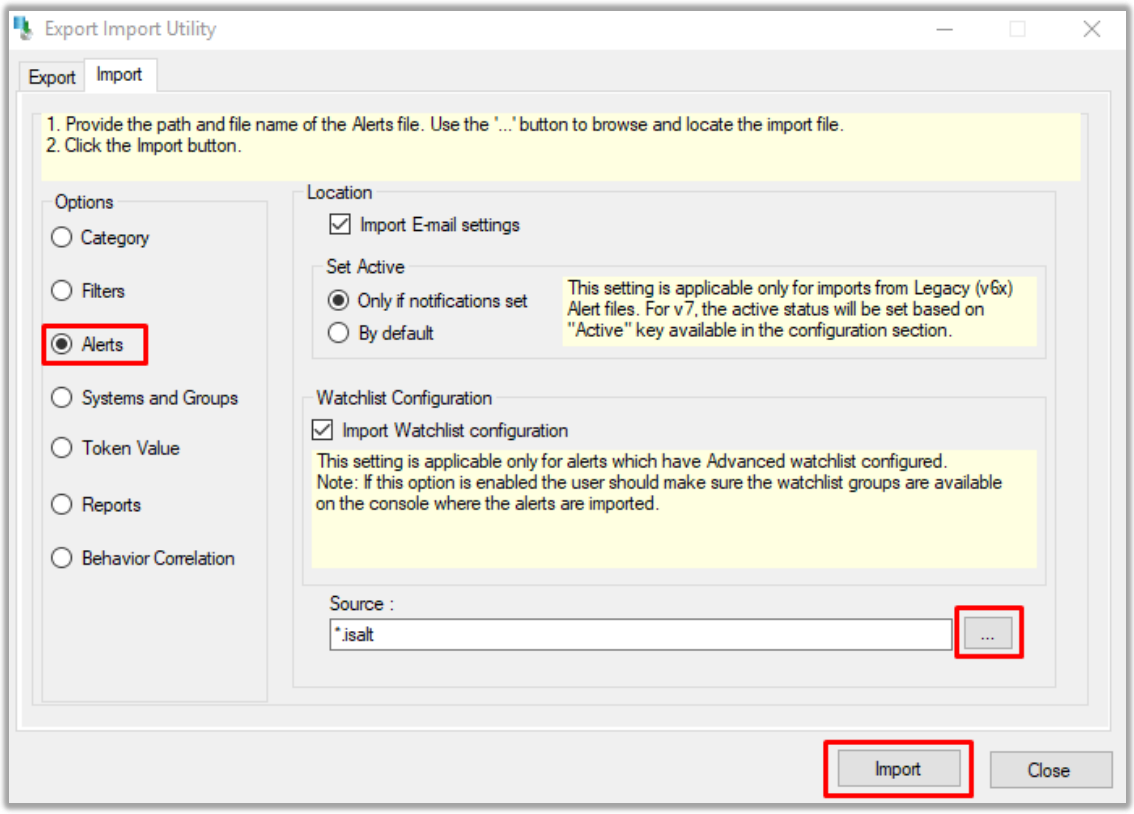

Figure 12

EventTracker displays a success message:

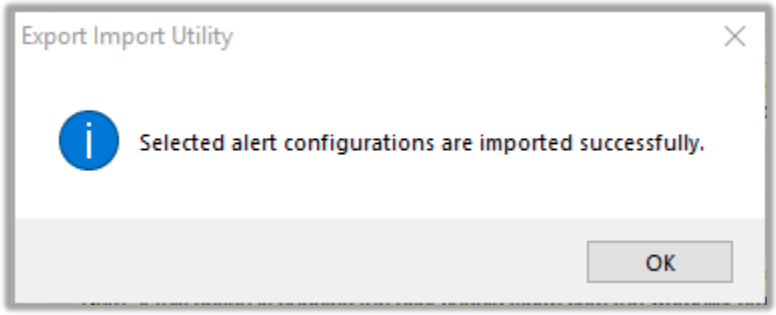

Figure 13

3.3 Parsing Rule

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

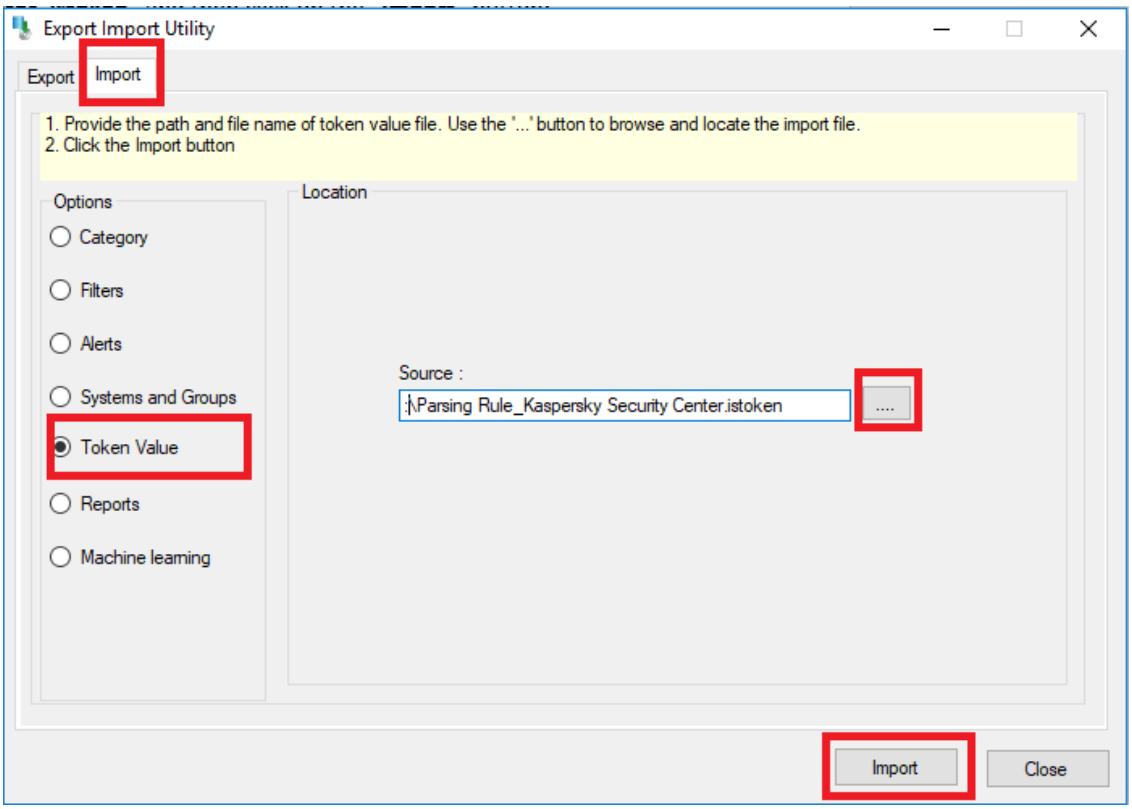

Figure 14

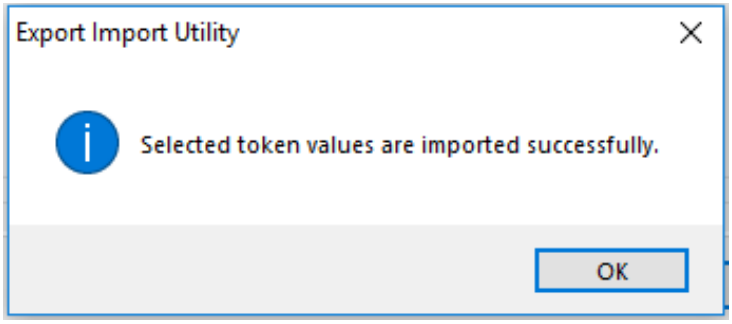

Figure 15

3.4 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)**":

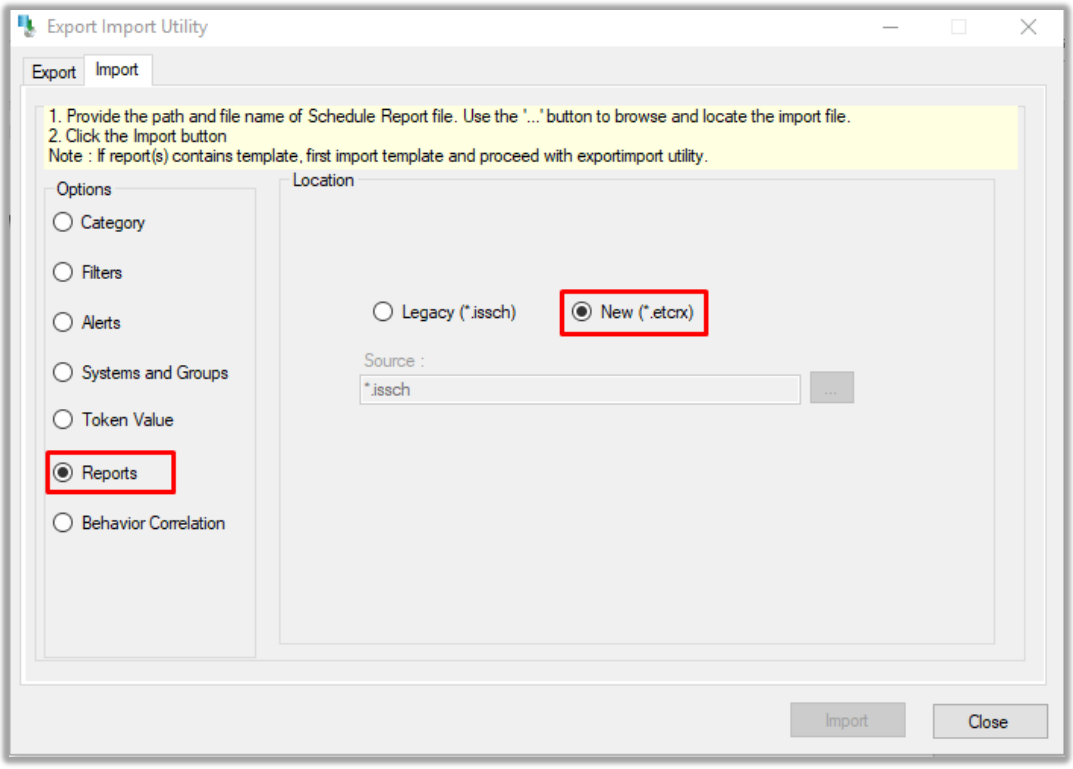

Figure 16

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_Barracuda Essentials.etcrx".**

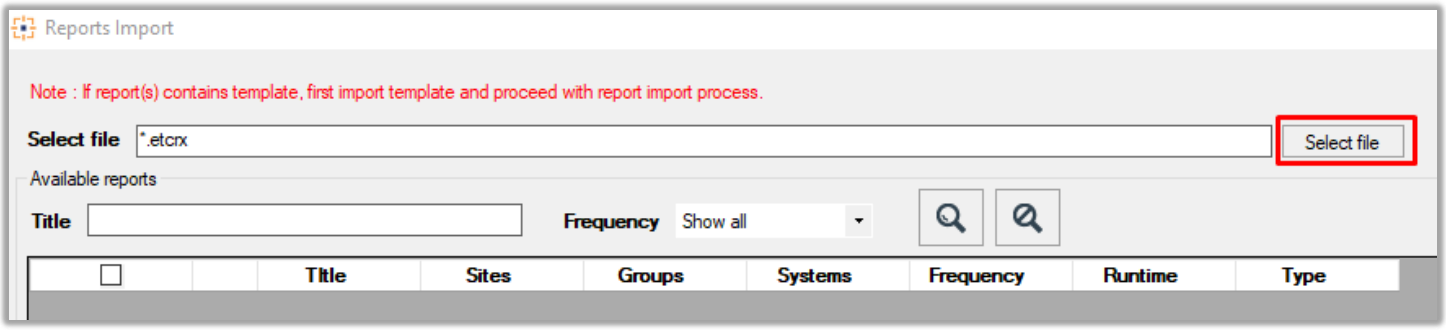

Figure 17

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

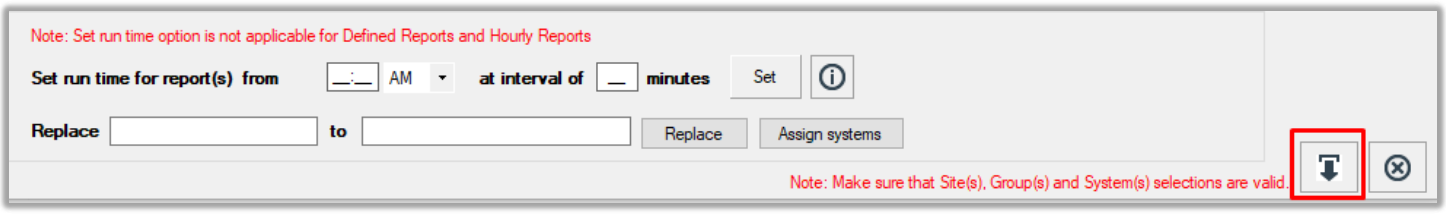

Figure 18

EventTracker displays a success message:

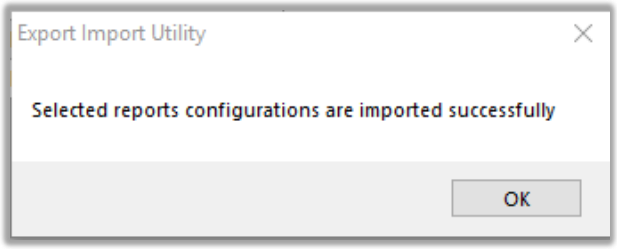

Figure 19

3.5 Knowledge Objects

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

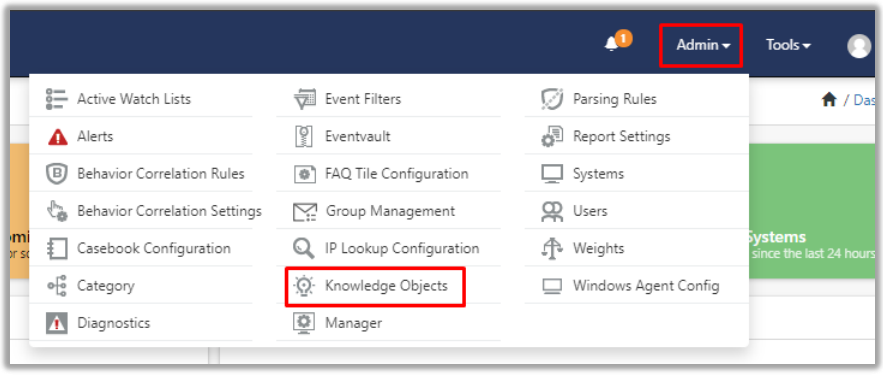

Figure 20

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

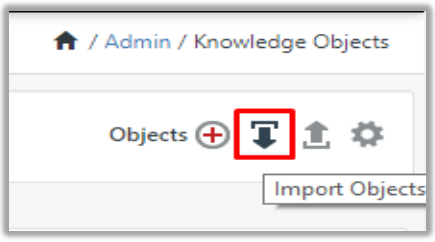

Figure 21

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

Figure 22

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 23

3.6 Dashboards

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

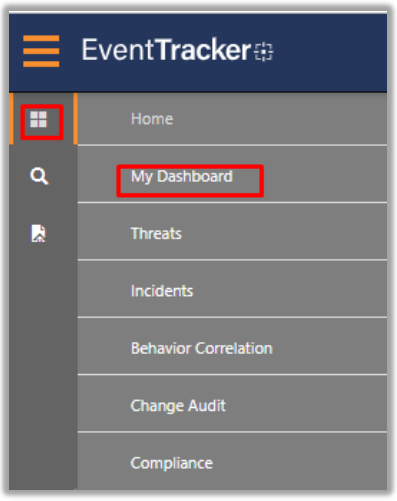

Figure 24

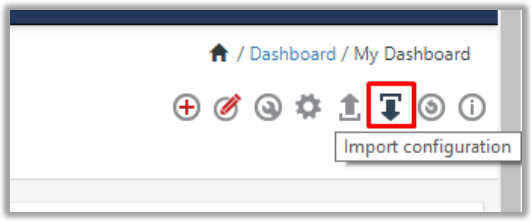

Figure 25

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_Barracuda Essentials.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.

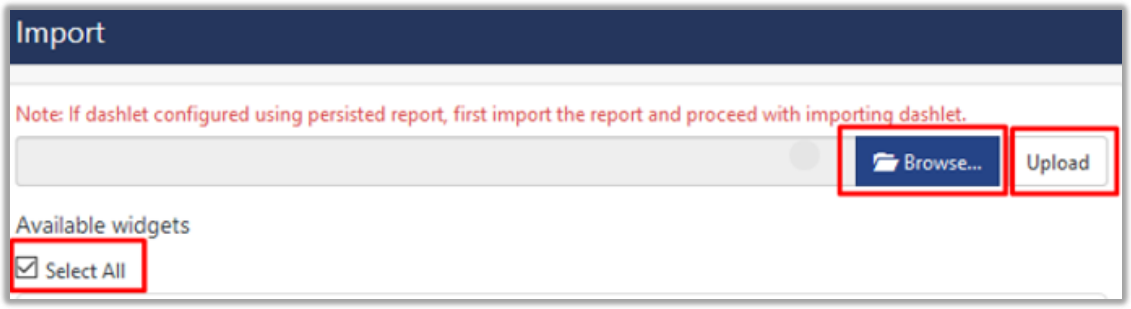

Figure 26

Figure 27

4. Verifying knowledge pack in EventTracker

4.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, please click on "**Search**" and search with the **"Barracuda Essentials".** You will see the below results:

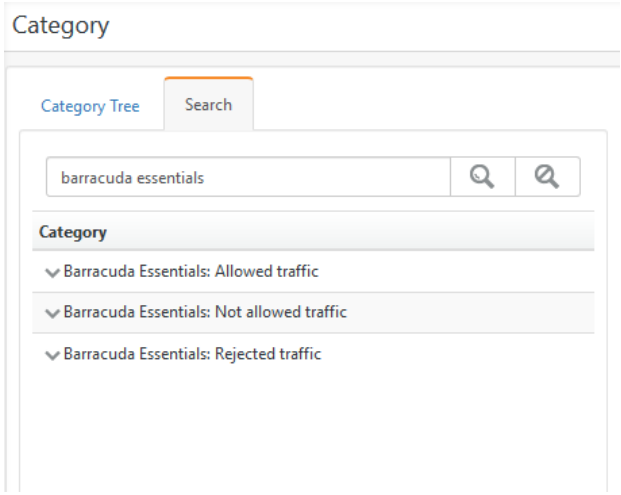

Figure 28

4.2 Alerts

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

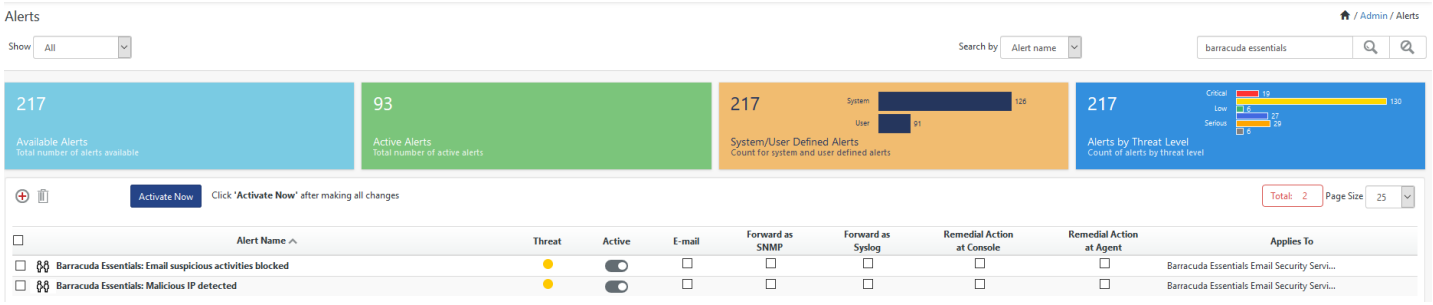

Figure 29

4.3 Parsing Rules

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

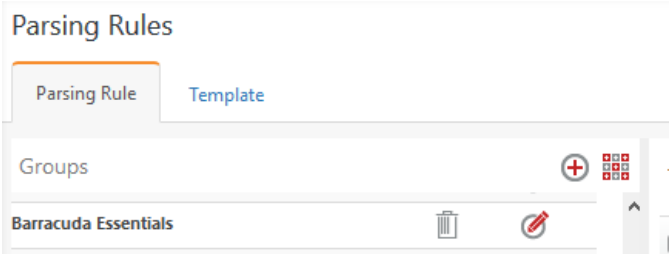

Figure 30

4.4 Flex Reports

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

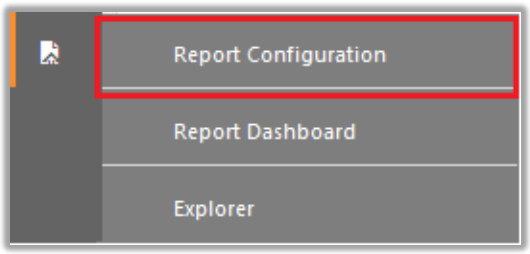

Figure 31

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

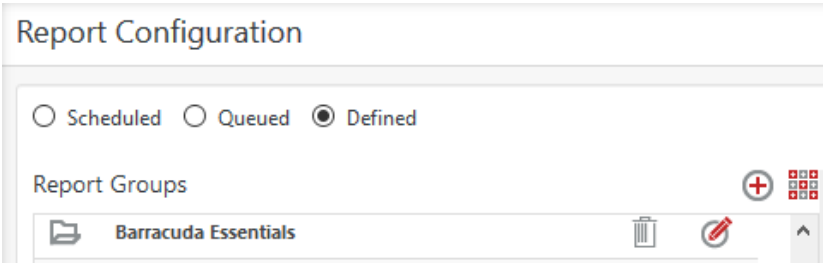

Figure 32

4.5 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 **"Barracuda Essentials"** group folder to view the imported Knowledge objects.

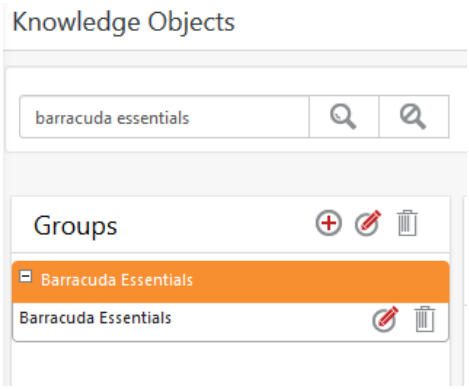

Figure 33

4.6 Dashboards

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

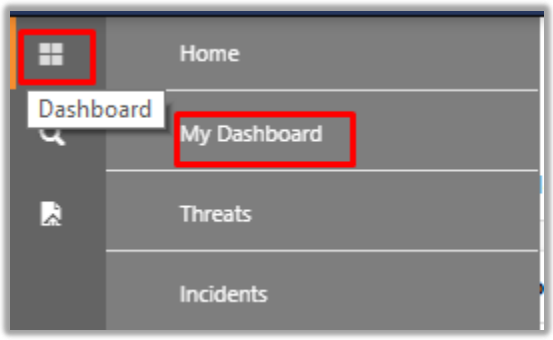

Figure 34

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

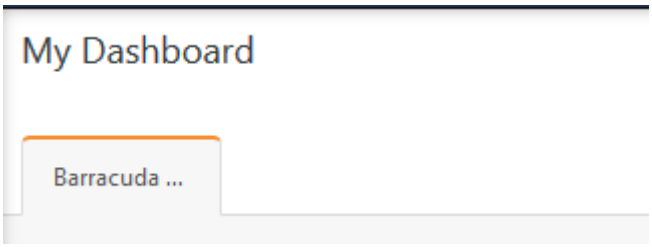

Figure 35