Integrate KnowBe4 with EventTracker

EventTracker v9.0 and above

Publication Date: November 21, 2019

Abstract

This guide helps you in configuring **KnowBe4** and **EventTracker** to receive KnowBe4 events. You will find the detailed procedures required for monitoring KnowBe4.

Scope

The configurations detailed in this guide are consistent with **EventTracker v9.x** and later, **KnowBe4.**

Audience

KnowBe4 users, who wish to forward Events to EventTracker and monitor 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 laws 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.

Table of Contents

1.Overview

KnowBe4 is a platform for security awareness training and simulated phishing attacks. It helps you manage the ongoing problem of social engineering, spear phishing, and ransomware attacks.

KnowBe4 can be integrated with EventTracker using API. EventTracker can fetch all the phishing campaign done by knowbe4 and provide the report which helps us to understand the user risk score. Its dashboard will help us to view the risk score for each user and provide information about the phishing campaign done by knowbe4.

2.Prerequisites

- Admin privileges for **KnowBe4** web console.

Note: Reporting APIs are available only to customers at Platinum and Diamond subscription levels.

3. Configuring KnowBe4 to forward logs to EventTracker

3.1 Collecting API key

1. Please login to your KnowBe4 web console with admin privileges.
2. Navigate to **Account Settings**.

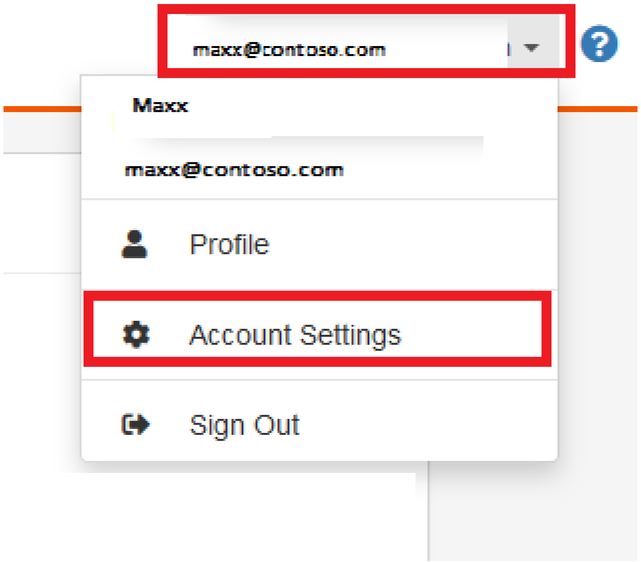
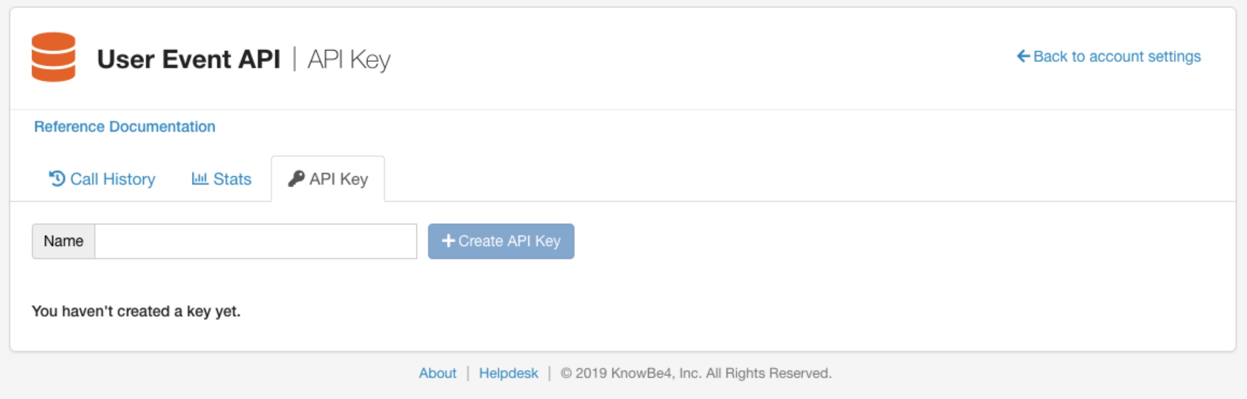


Figure 1

3. Search for **User Event API > API Key** section.

- **Name**: Please enter the name as **EventTracker API**.
- Click the **+Create API Key** button.



You haven't created a key yet.

Figure 2

4. Please download/copy the EventTracker API key.

3.2 Forwarding logs to EventTracker

1. Contact the EventTracker Support team and get the "KnowBe4 Integrator" executable file.
2. Once the executable application is received, right-click on the file and select "Run as Administrator".

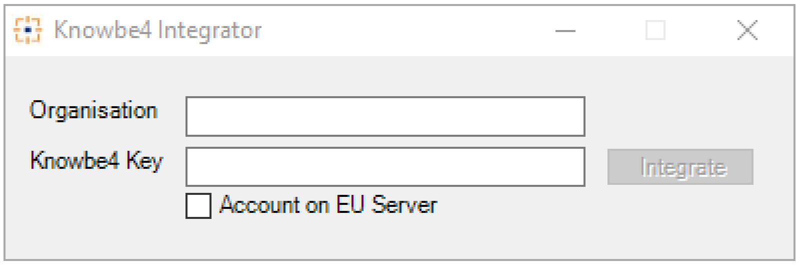
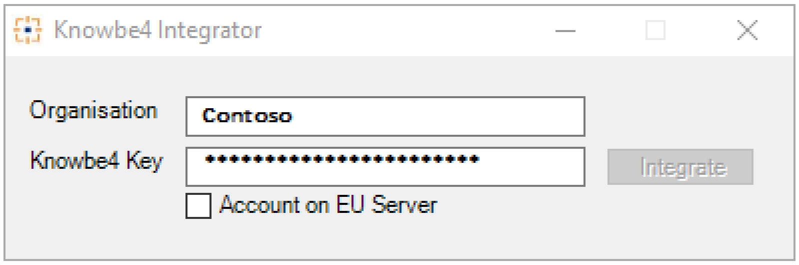


Figure 3

3. Please enter the **organization** name, the **Knowbe4 API key** and by default **Account on US server** selected or select **Account on EU server** if server existed in EU and click on the Integrate button.



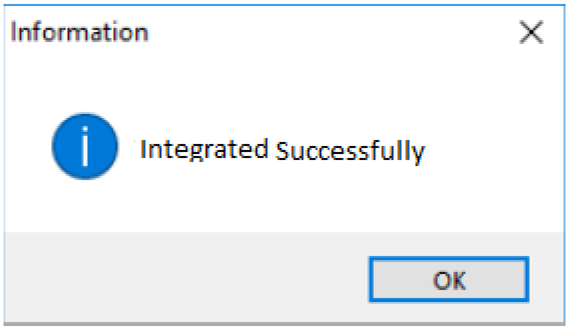
Organisation: Contoso

Knowbe4 Key: ************************

□ Account on EU Server

Figure 4

4. Click on the "**OK**" button to complete the integration process.



Information

Integrated Successfully

Figure 5

4. EventTracker Knowledge Pack

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

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

4.1 Saved Searches

KnowBe4 – User account detail– This category shows the user complete detail logs like user names, user organization related information and risk scores, etc.

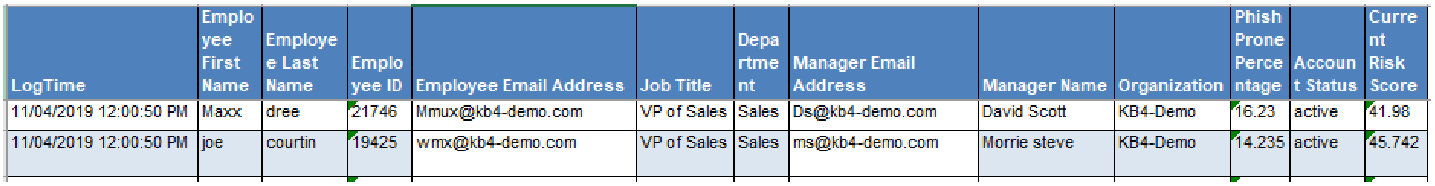
KnowBe4 – User phishing campaign detail – This category shows the knowbe4 user logs like user training status, user count, training type and organization user phish prone percentage.

KnowBe4 – User phishing security statistics – This category shows the user phishing statistics logs.

4.2 Reports

KnowBe4 – User account detail – This report provides information about the user account who is using knowbe4. This report provides details of users like first name, last name, email id, and risk score.

Sample Report

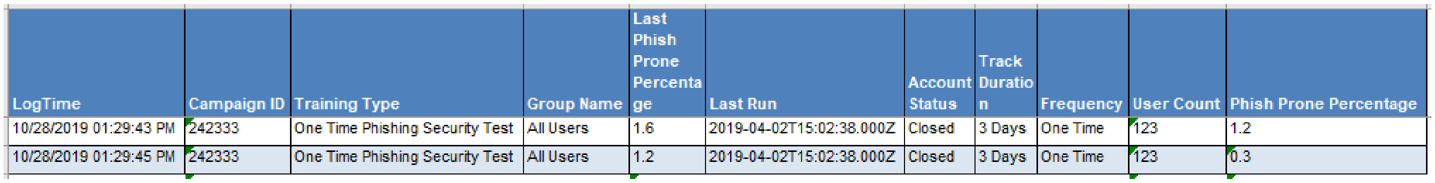


LogTime	Employee First Name	Employee Last Name	Employee ID	Employee Email Address	Job Title	Department	Manager Email Address	Manager Name	Organization	Phish Prone Percentage	Account Status	Current Risk Score
11/04/2019 12:00:50 PM	Maxx	dree	21746	Mmux@kb4-demo.com	VP of Sales	Sales	Ds@kb4-demo.com	David Scott	KB4-Demo	16.23	active	41.98
11/04/2019 12:00:50 PM	joe	courtin	19425	wmx@kb4-demo.com	VP of Sales	Sales	ms@kb4-demo.com	Morrie steve	KB4-Demo	14.235	active	45.742

Figure 6

KnowBe4 – User phishing campaign detail – This report provides information about phishing campaign which is scheduled in knowbe4. This report will contain campaign name, schedule time and end time.

Sample Report

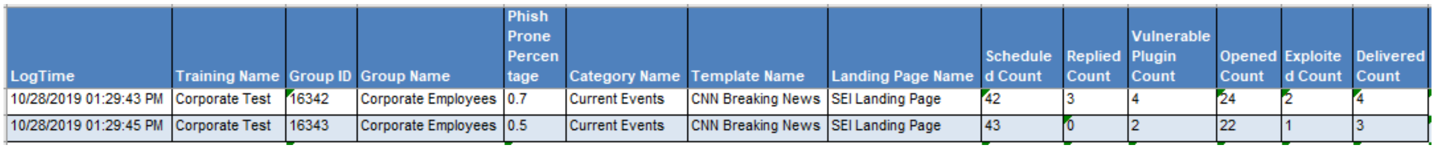


LogTime	Campaign ID	Training Type	Group Name	Last Phish Prone Percentage	Last Run	Account Status	Track Duration	Frequency	User Count	Phish Prone Percentage
10/28/2019 01:29:43 PM	242333	One Time Phishing Security Test	All Users	1.6	2019-04-02T15:02:38.000Z	Closed	3 Days	One Time	123	1.2
10/28/2019 01:29:45 PM	242333	One Time Phishing Security Test	All Users	1.2	2019-04-02T15:02:38.000Z	Closed	3 Days	One Time	123	0.3

Figure 7

KnowBe4 – User phishing security statistics – This report provides the risk statistics of the user who have attended the phishing campaign. This report contains information about the user, it's risk score and phishing campaign user attended.

Sample Report

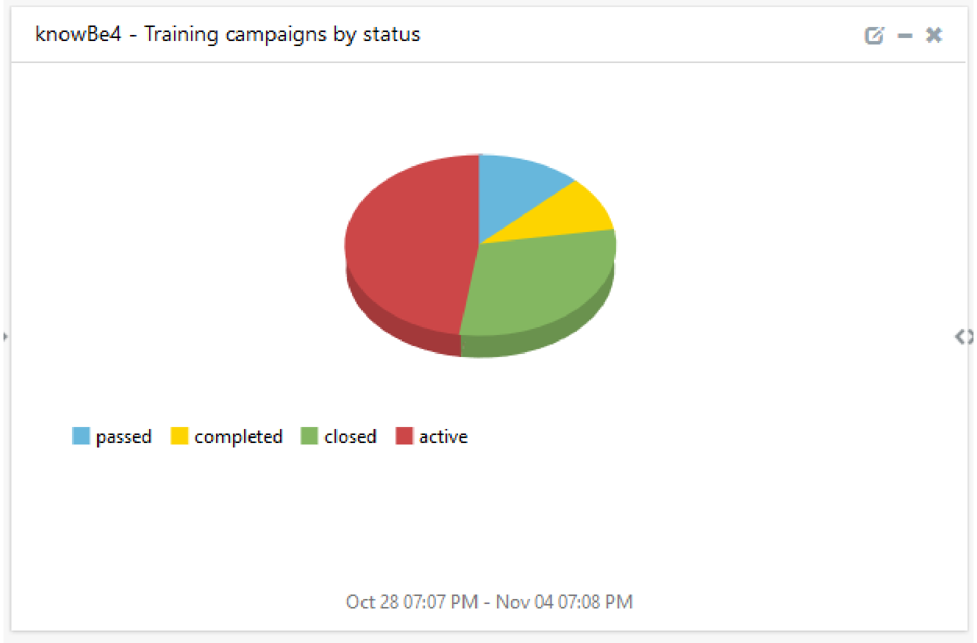


LogTime	Training Name	Group ID	Group Name	Phish Prone Percentage	Category Name	Template Name	Landing Page Name	Scheduled Count	Replied Count	Vulnerable Plugin Count	Opened Count	Exploited Count	Delivered Count
10/28/2019 01:29:43 PM	Corporate Test	16342	Corporate Employees	0.7	Current Events	CNN Breaking News	SEI Landing Page	42	3	4	24	2	4
10/28/2019 01:29:45 PM	Corporate Test	16343	Corporate Employees	0.5	Current Events	CNN Breaking News	SEI Landing Page	43	0	2	22	1	3

Figure 8

4.3 Dashboards

KnowBe4 – Training campaigns by status – This dashboard will show user training campaign status like active, passed, completed, and closed.



knowBe4 - Training campaigns by status
passed
completed
closed
active
Oct 28 07:07 PM - Nov 04 07:08 PM

Figure 9

KnowBe4 – User vulnerability by phish prone percentage – This dashboard will show user phishing security training like user names and phish prone percentage.

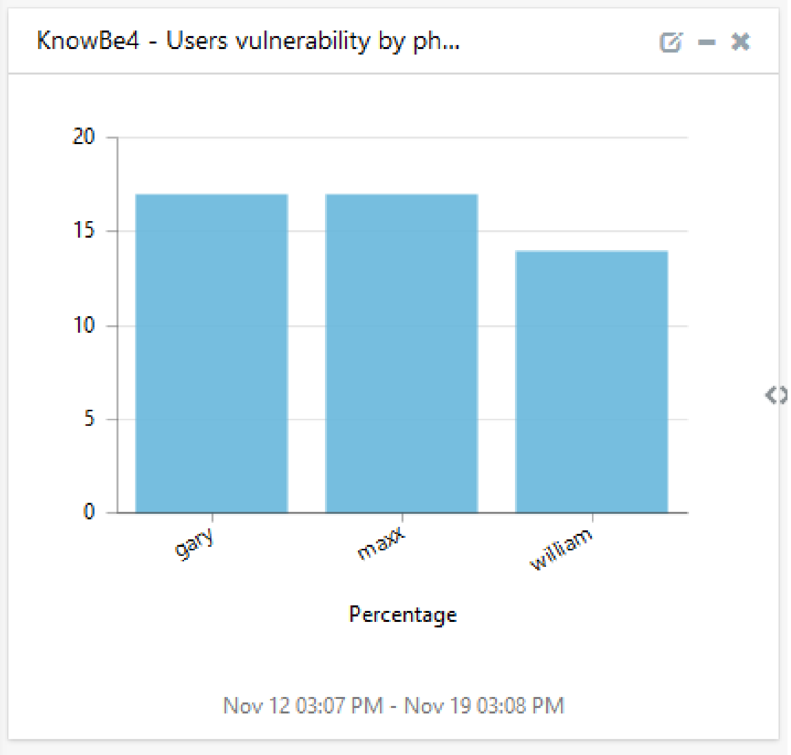

KnowBe4 - Users vulnerability by ph...
20
15
10
5
0
gary
maxx
william
Percentage
Nov 12 03:07 PM - Nov 19 03:08 PM

Figure 10

KnowBe4 – Risk score by users – This dashboard will show about user names and user risk scores.

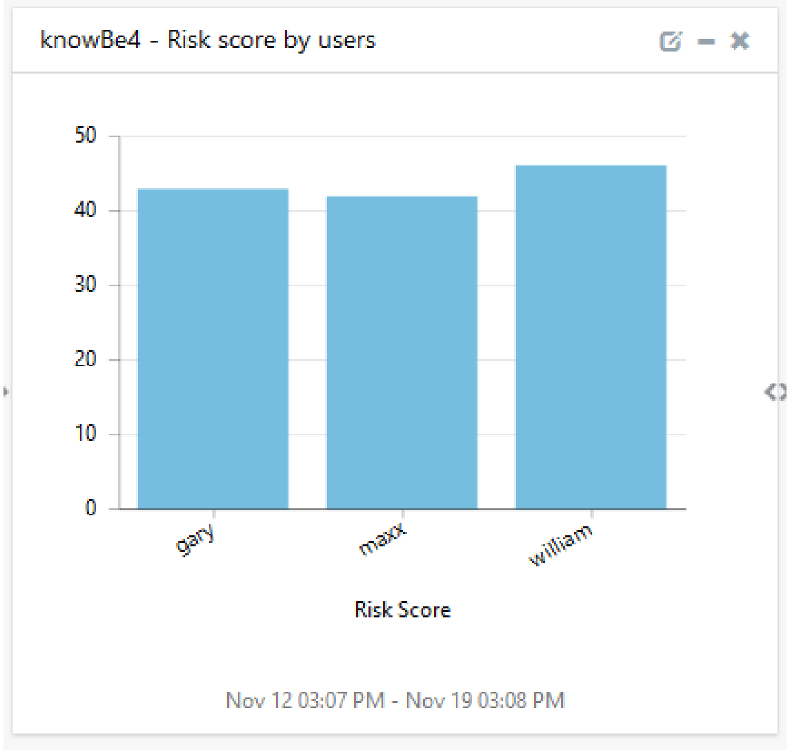

knowBe4 - Risk score by users
50
40
30
20
10
0
gary
maxx
william
Risk Score
Nov 12 03:07 PM - Nov 19 03:08 PM

Figure 11

5. 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**.

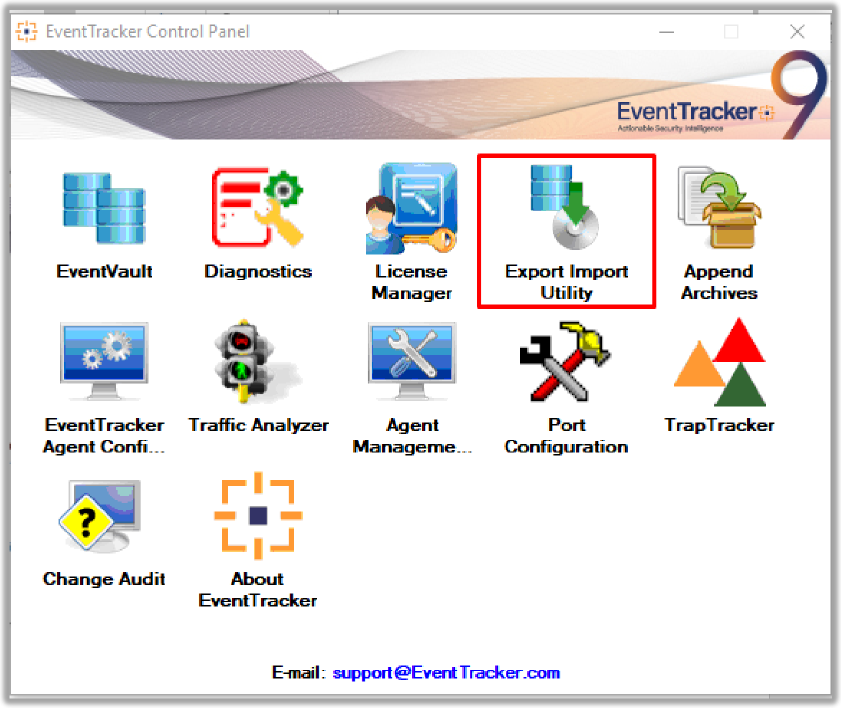
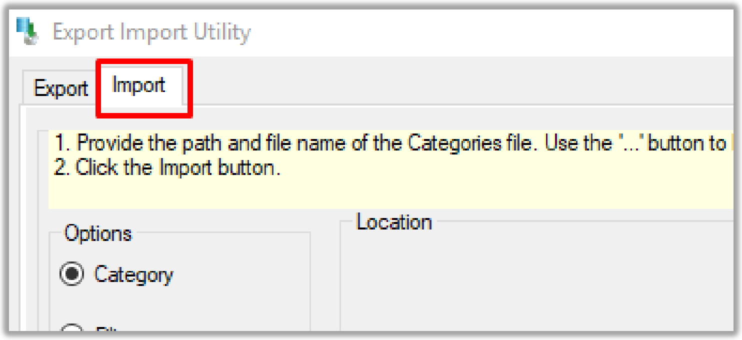


Figure 12



1. Provide the path and file name of the Categories file. Use the '...' button to
2. Click the Import button.

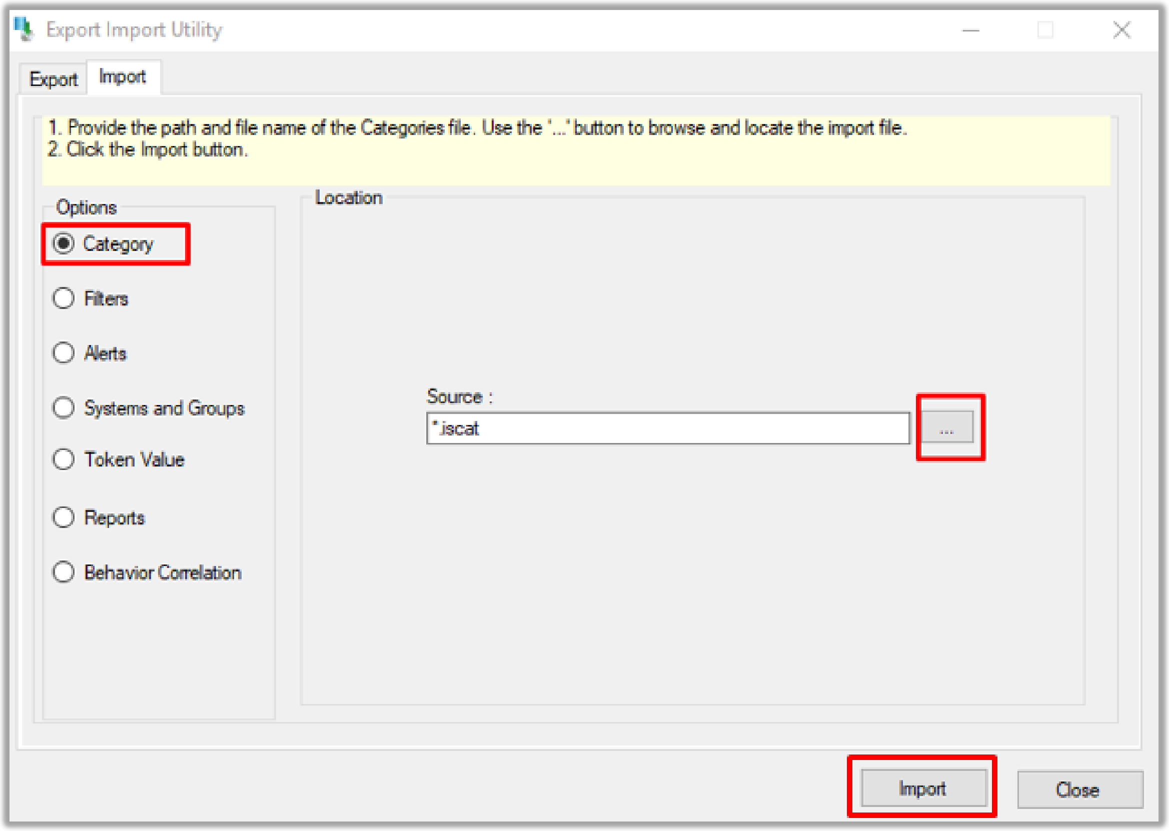
● Category

Figure 13

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 extension **“.iscat”, like “Categories_KnowBe4.iscat”** and then click on the “**Import**” button:



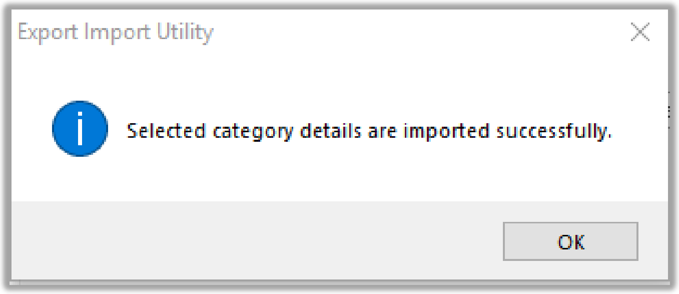
1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Source : *.iscat

Figure 14

EventTracker displays a success message:

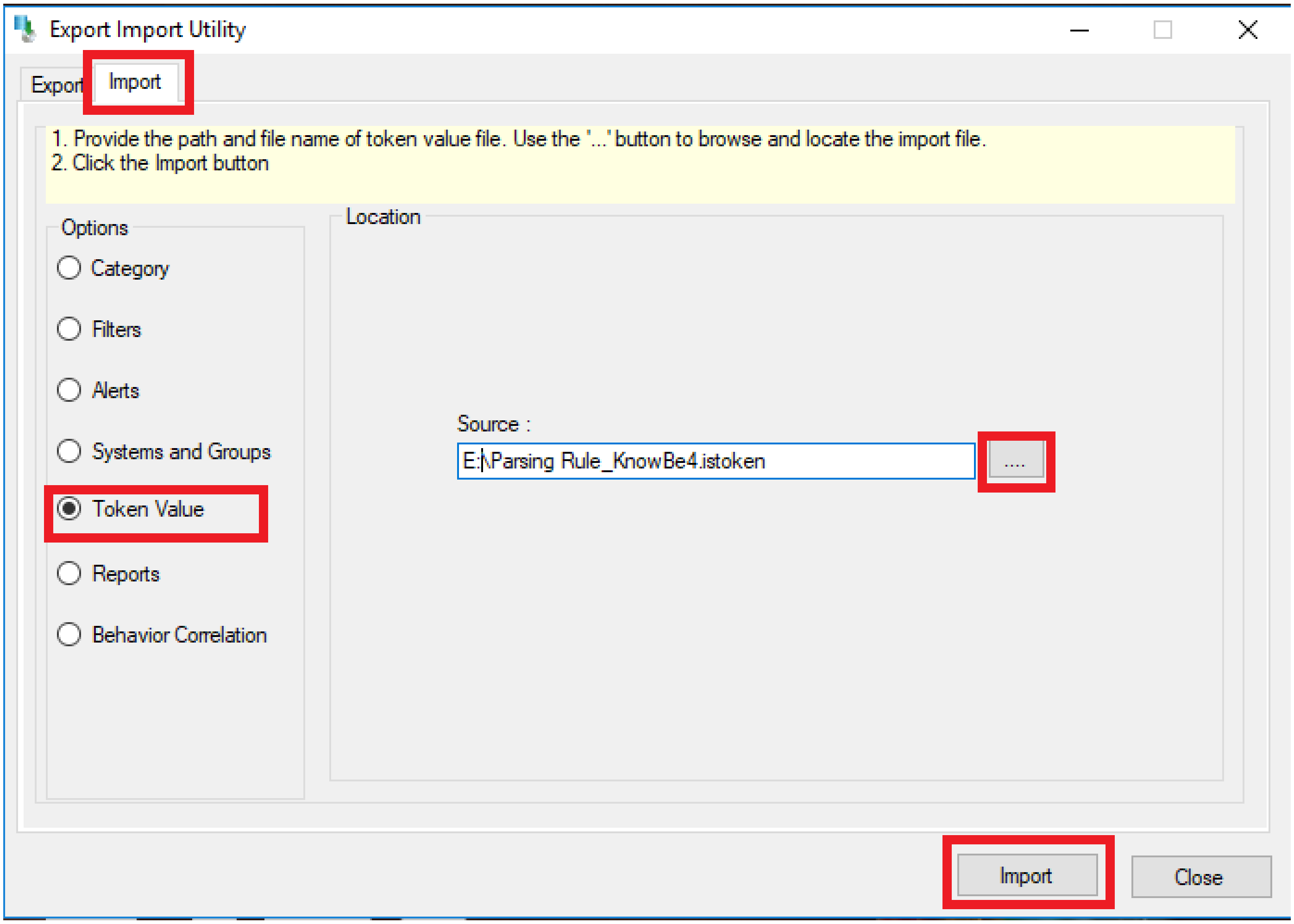

Export Import Utility

Selected category details are imported successfully.

Figure 15

5.2 Parsing Rule

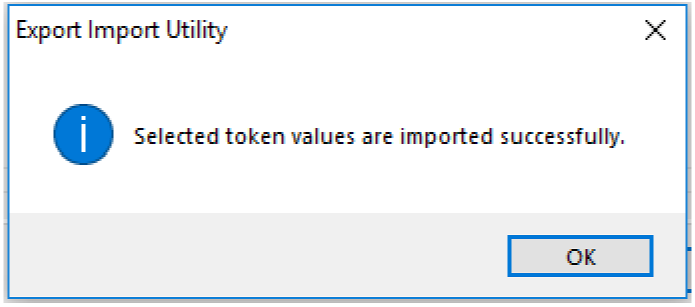
1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click the **Token Value** option, and then click the browse … button.
2. Navigate to the knowledge pack folder and select the file with the extension **“.iscat”, like “Parsing Rule_KnowBe4.iscat”** and then click on the “**Import**” button:



1. Provide the path and file name of token value file. Use the '...' button to browse and locate the import file.
2. Click the Import button

Source : E:\Parsing Rule_KnowBe4.istoken

Figure 16

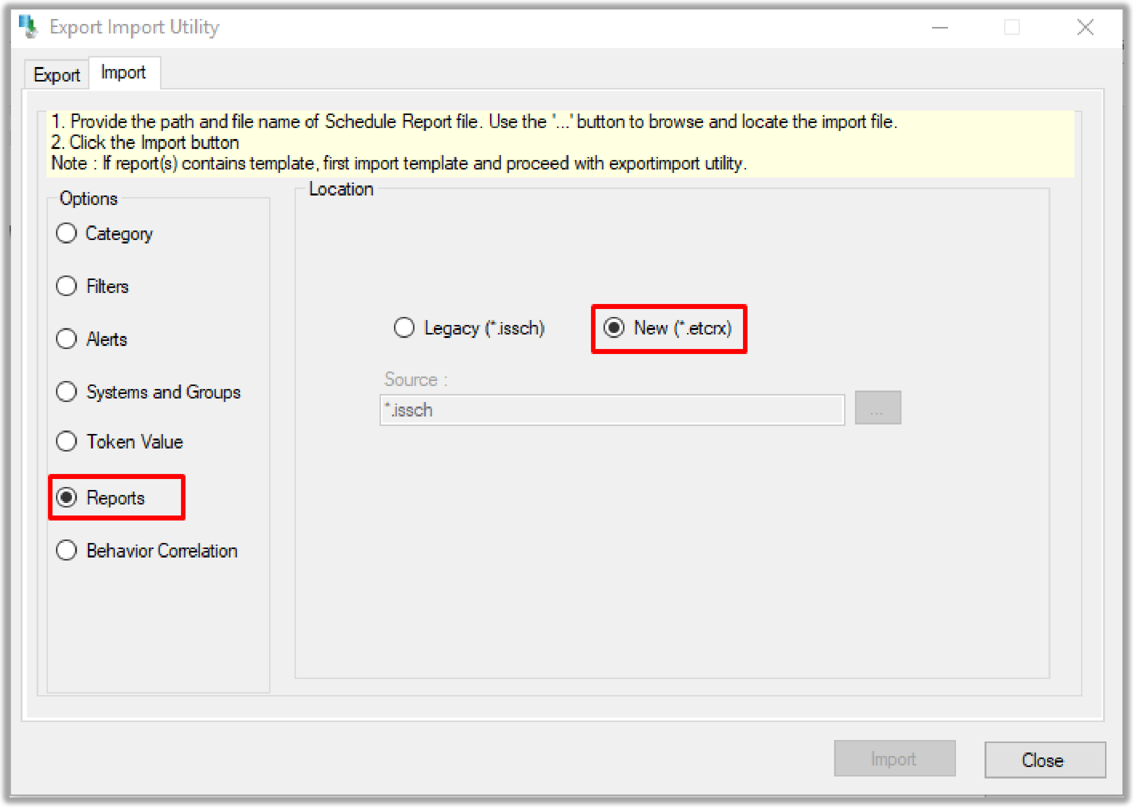


Selected token values are imported successfully.

Figure 17

5.3 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)**”:



Export Import Utility

Export | Import

1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options
- ○ Category
- ○ Filters
- ○ Alerts
- ○ Systems and Groups
- ○ Token Value
- ● Reports
- ○ Behavior Correlation

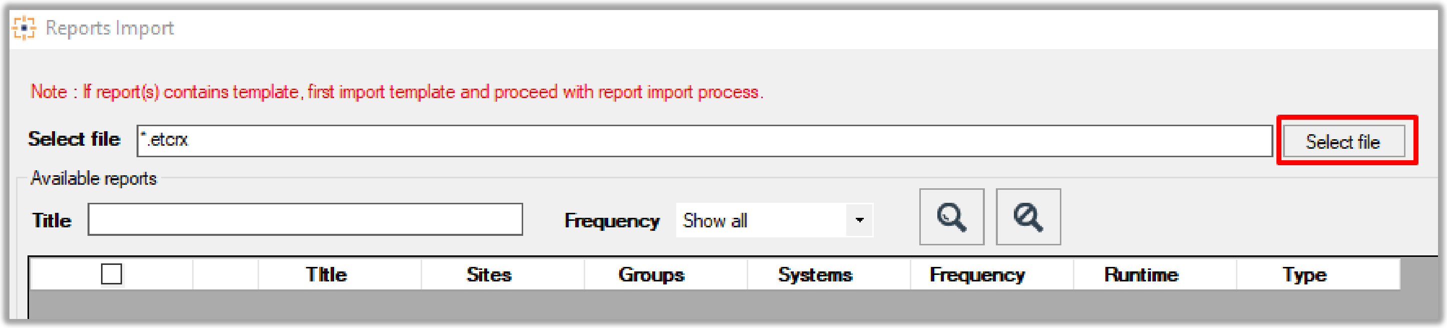
Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

Figure 18

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_KnowBe4.etcrx”.**



Reports Import

Note : If report(s) contains template, first import template and proceed with report import process.

Select file: *.etcrx

Available reports

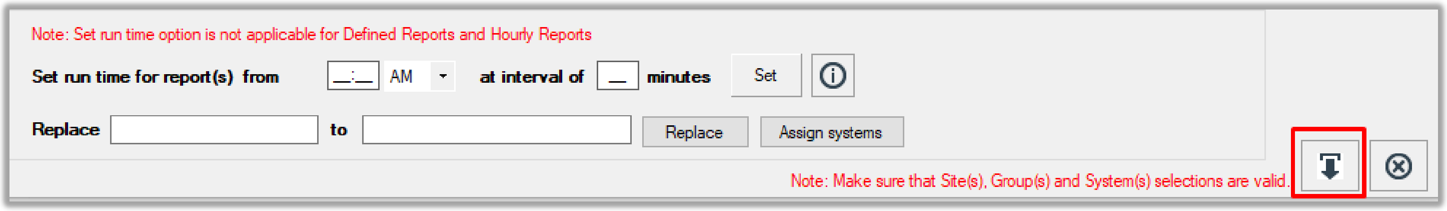
Title:

Frequency: Show all

□		Title	Sites	Groups	Systems	Frequency	Runtime	Type

Figure 19

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



Note: Set run time option is not applicable for Defined Reports and Hourly Reports

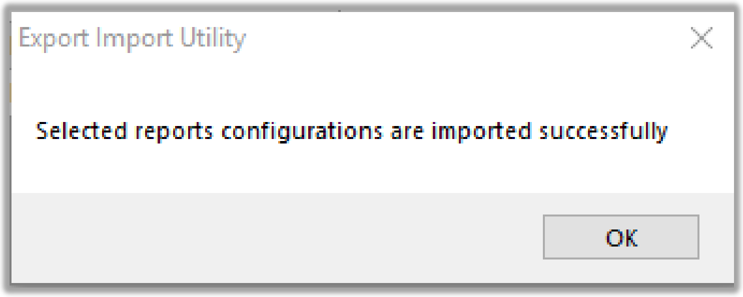
Set run time for report(s) from __:__ AM at interval of __ minutes

Replace to

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 20

EventTracker displays a success message:



Export Import Utility

Selected reports configurations are imported successfully

Figure 21

5.4 Knowledge Objects

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

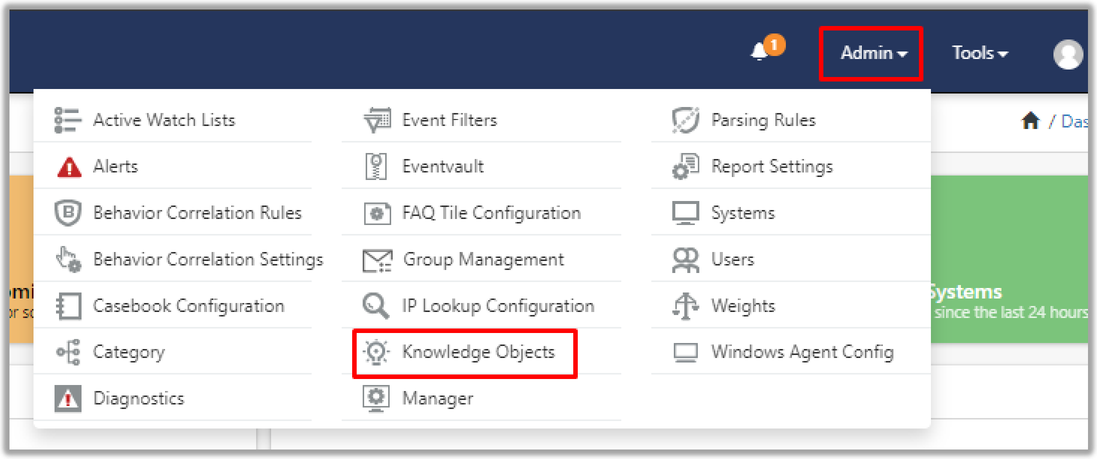


Figure 22

2. Next, click the **“import object”** icon:

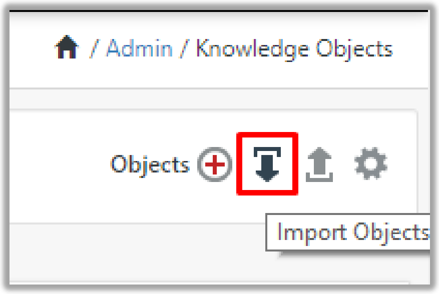


Figure 23

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_KnowBe4.etko”** and then click “**Upload**” button.

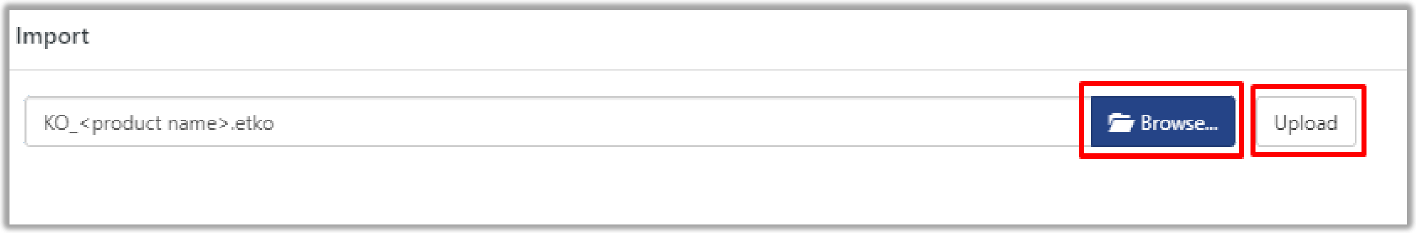


Figure 24

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:

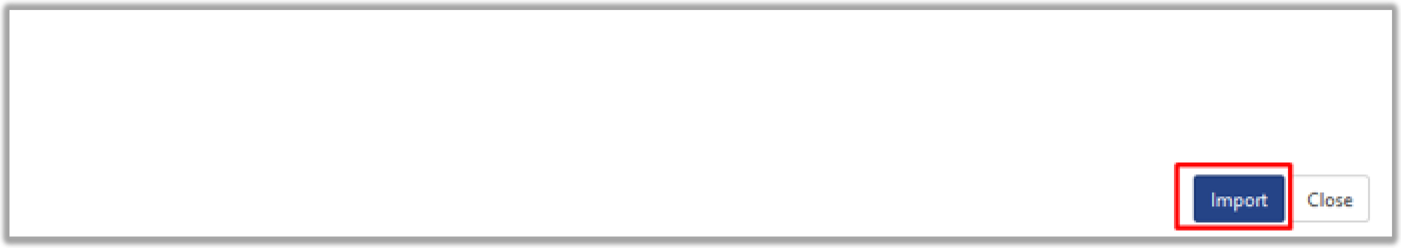


Figure 25

5.5 Dashboards

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

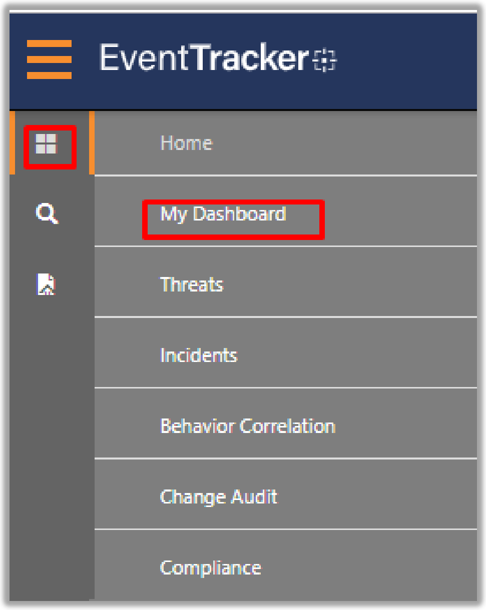


Figure 26

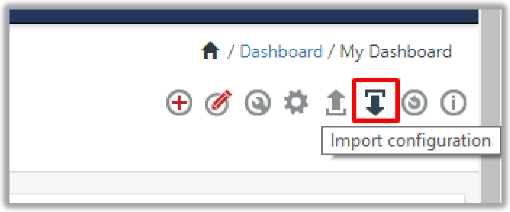
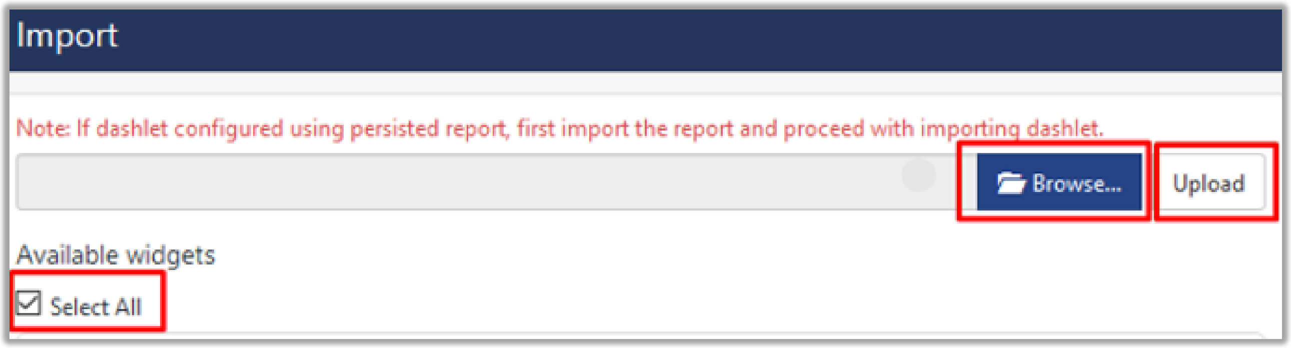


Figure 27

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_KnowBe4.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.



Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Figure 28

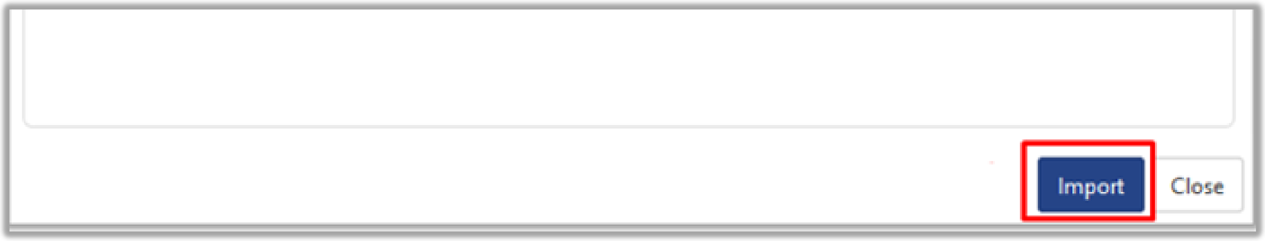
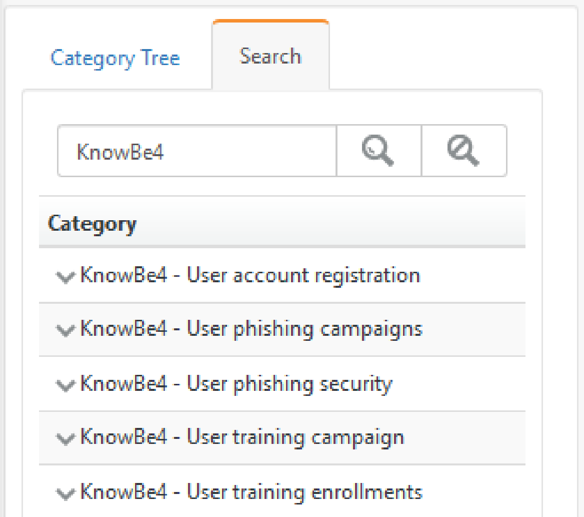


Figure 29

6. Verifying 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 **“KnowBe4”** group folder to view the imported categories:



KnowBe4 - User account registration
KnowBe4 - User phishing campaigns
KnowBe4 - User phishing security
KnowBe4 - User training campaign
KnowBe4 - User training enrollments

Figure 30

6.2 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 **"KnowBe4"** group folder to view the imported Token Values.

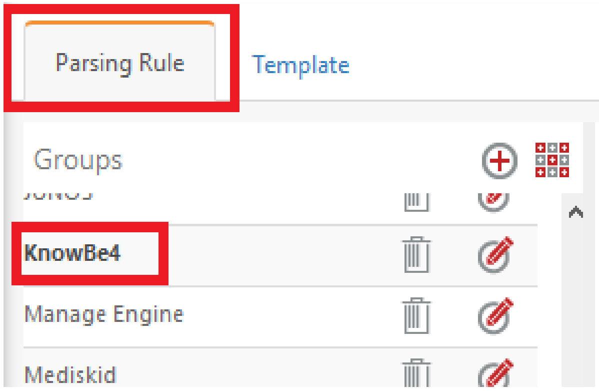


Figure 31

6.3 Flex Reports

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

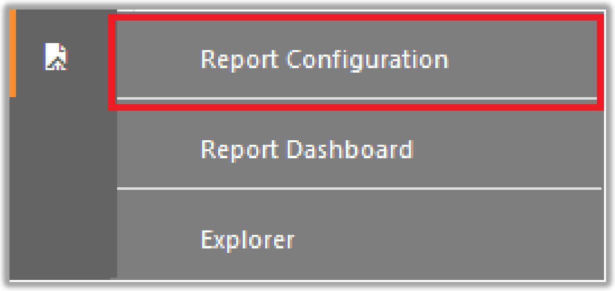
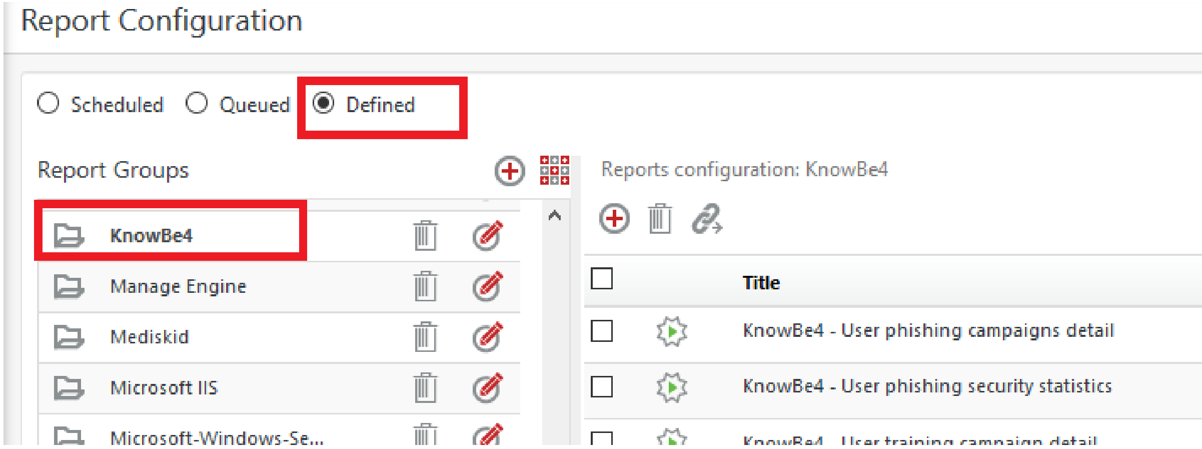


Figure 32

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the **"KnowBe4"** group folder to view the imported reports.


Report Configuration

○ Scheduled ○ Queued ● Defined

Report Groups

- KnowBe4
- Manage Engine
- Mediskid
- Microsoft IIS
- Microsoft-Windows-Se...

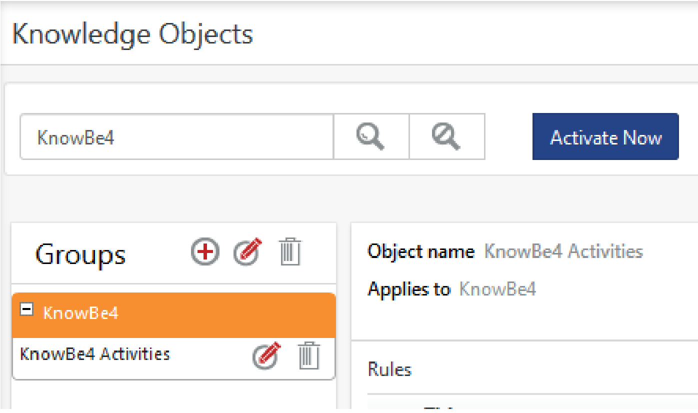
Reports configuration: KnowBe4

□		Title
□		KnowBe4 - User phishing campaigns detail
□		KnowBe4 - User phishing security statistics
□		KnowBe4 - User training campaign detail

Figure 33

6.4 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 **"KnowBe4"** group folder to view the imported Knowledge objects.


Knowledge Objects

KnowBe4

⊟ KnowBe4
KnowBe4 Activities

Object name KnowBe4 Activities
Applies to KnowBe4

Rules

Figure 34

6.5 Dashboards

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

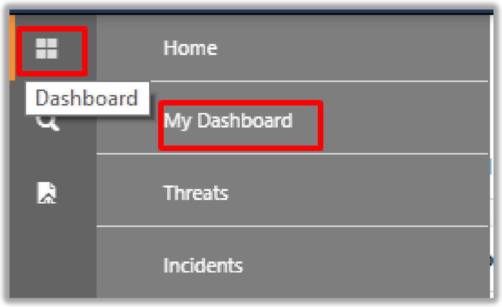


Figure 35

2. In “**KnowBe4”** dashboard you should be now able to see something like this:

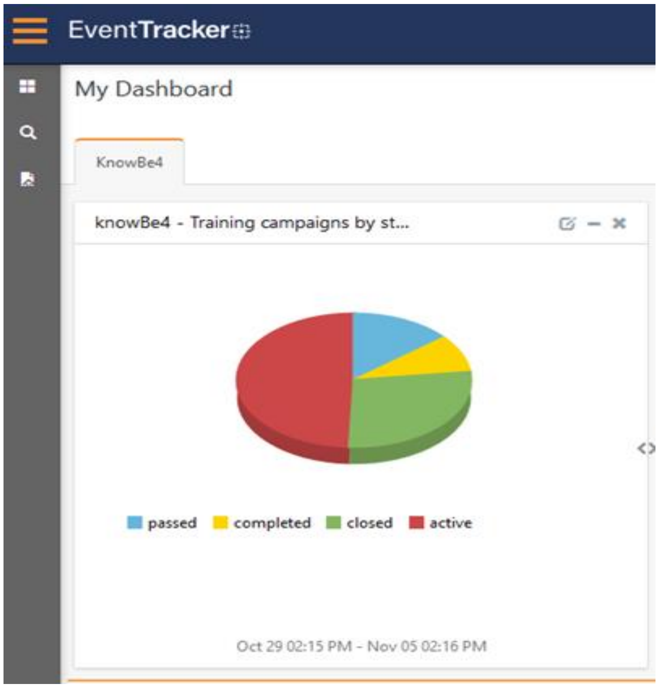

EventTracker
My Dashboard
KnowBe4
knowBe4 - Training campaigns by st...
passed
completed
closed
active
Oct 29 02:15 PM - Nov 05 02:16 PM

Figure 36