

# Integration Guide for Defender MFA

## EventTracker v9.2 and later

## Abstract

This guide provides instructions to retrieve the **Defender MFA (One Identity)** events via syslog. Once the logs start coming into EventTracker, reports, dashboards, alerts and saved searches can be configured.

## Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Defender MFA 5.9 and above**.

## Audience

Administrators who are assigned the task to monitor **Defender MFA** 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.*

*© 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.....	3
2. Prerequisites.....	3
3. Integrating Defender MFA with EventTracker .....	3
3.1 Part 1 Configuring Syslog Message Forwarding .....	3
3.2 Part 2 Configuring Defender Console event log forwarding .....	5
4. EventTracker Knowledge Packs.....	8
4.1 Saved Searches .....	8
4.2 Alerts.....	9
4.3 Flex Reports .....	9
4.4 Dashboards .....	10
5. Importing knowledge pack into EventTracker .....	14
5.1 Saved Searches .....	15
5.2 Alerts.....	16
5.3 Token Template .....	17
5.4 Flex Reports .....	18
5.5 Knowledge Objects .....	20
5.6 Dashboards .....	21
6. Verifying knowledge pack in EventTracker .....	23
6.1 Saved Searches .....	23
6.2 Alerts.....	24
6.3 Token Template .....	24
6.4 Flex Reports .....	25
6.5 Knowledge Objects .....	26
6.6 Dashboards .....	27

# 1. Overview

One Identity Defender is a two-factor authentication or Multi-Factor Authentication (MFA) program. It uses the current identity store within Microsoft Active Directory to enable two-factor authentication, taking advantage of its inherent scalability and security, and eliminate the costs and time involved to set up and maintain proprietary databases.

Defender MFA integrates with EventTracker SIEM application to give security analytics with deep data context so that organizations can be confident in their data security strategy. Benefits include scheduled reports, integrated defender MFA dashboards and alerts for streamlined investigation.

Reports will allow users to keep records that is easy to read and to format. It is a detailed summary of events generated by Defender MFA. It includes successful or failed user sign-in attempts with user assigned tokens.

Alerts are best way to keep updated with critical events occurring in Defender MFA, such as, failed sign-in attempt with a user token, or when a token or defender password is assigned/unassigned to/from a user.

Dashboard provides a graphical representation of events generated by Defender MFA in the form of pie chart or bar graph, or force direction, and many more. Some of them are, top successful user authentications, user authentication failure reasons, top user authentication failures, etc.

## 2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Defender Security Server (DSS).
- Syslog port (e.g. 514) should be allowed in firewall.
- EventTracker Manager IP address.

## 3. Integrating Defender MFA with EventTracker

### 3.1 Part 1 Configuring Syslog Message Forwarding

User can configure the syslog server address in DSS configuration wizard so that logs are sent to EventTracker.

1. Login to your Defender Security Server (DSS) with administrative account.
2. Navigate to **Start > Programs > Defender Active Directory Edition > Defender Security Server Configuration**.

3. In **Defender Security Server Configuration** wizard, select **"Audit Log"** tab and click on the **"Enable syslog"** checkbox.

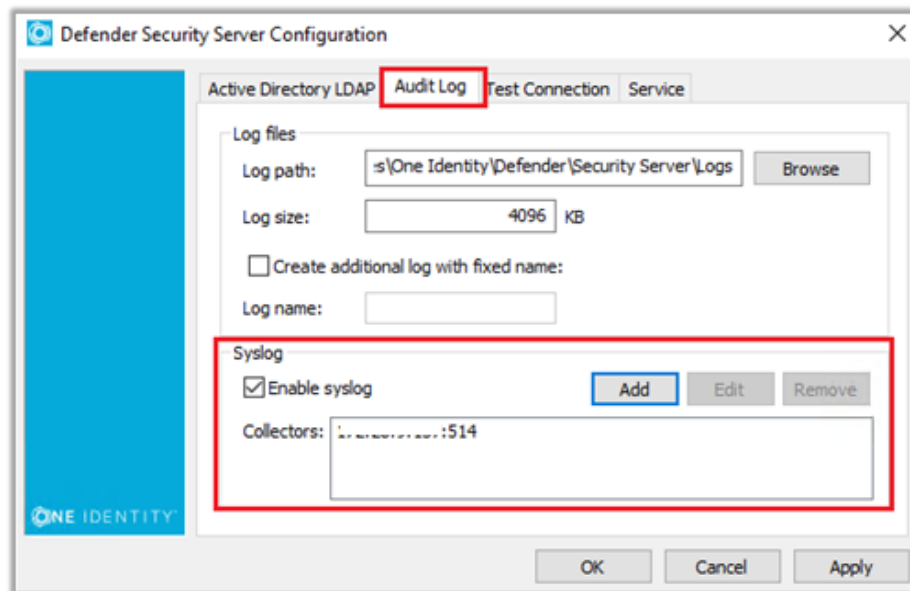


Figure 1

4. Next, click on **"Add"** button to add new syslog server. Enter the syslog server **IP address** and **port** number (default is 514) and click **OK**.

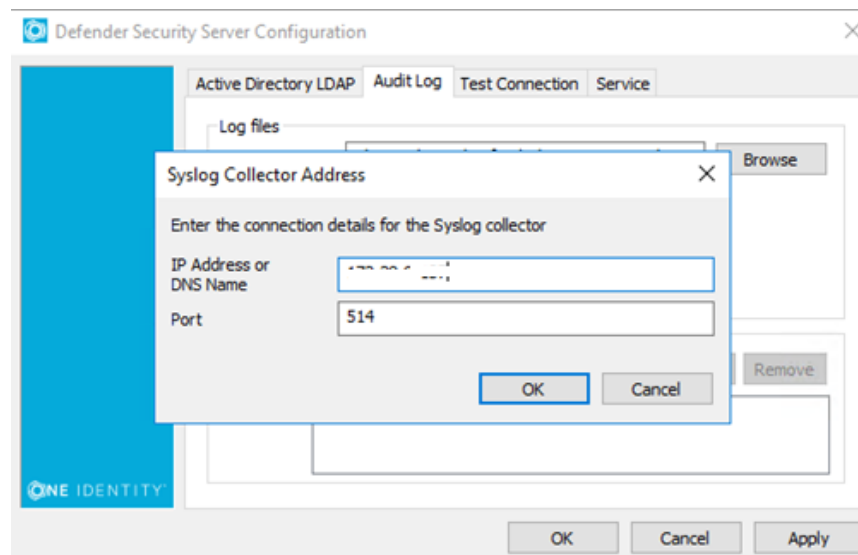


Figure 2

5. Finally click **Apply**, then **OK** to complete integration process.

## 3.2 Part 2 Configuring Defender Console event log forwarding

Defender MFA is also able to record events to the Windows Event Log. These logs are typically associated with token/defender password/ PIN management in Defender AD console. E.g. assigning a token to a user, assigning a Defender password to a user, setting a token PIN, etc.

By default, event logging is turned off in the Defender Console. To allow these events to be logged in windows event viewer and then forwarded to EventTracker, follow the below steps:

1. Set the following value in the registry on each desktop/server that is used to administer Defender tokens (i.e., wherever the Defender Console is installed).

```
x86: HKEY_LOCAL_MACHINE\Software\PassGo Technologies\Defender\Defender AD MMC
x64: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PassGo Technologies\Defender\Defender AD MMC
Value: LoggingEnabled (create the entry if it does not exist)
Type: DWORD
Data: 0 to disable logging, 1 to enable logging
```

Figure 3

2. Next, Configure EventTracker agent to pick up the Defender Console logs. For this, Open EventTracker agent configuration by navigating to path:

“C:\Program Files (x86)\Prism Microsystems\EventTracker\Agent\” or “%et\_install\_path%\Agent” and run “**etacconfig.exe**”. EventTracker Agent Configuration wizard opens, select “**Event Filters**”.

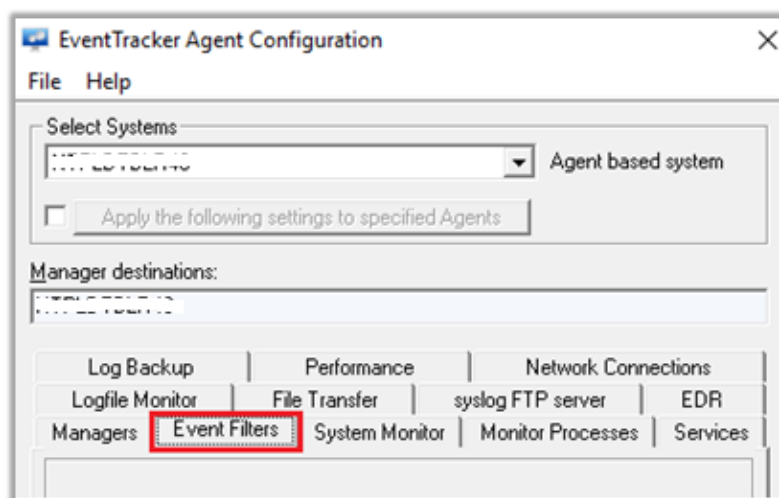


Figure 4

3. In “Event Filters”, select “Filter exception” button:

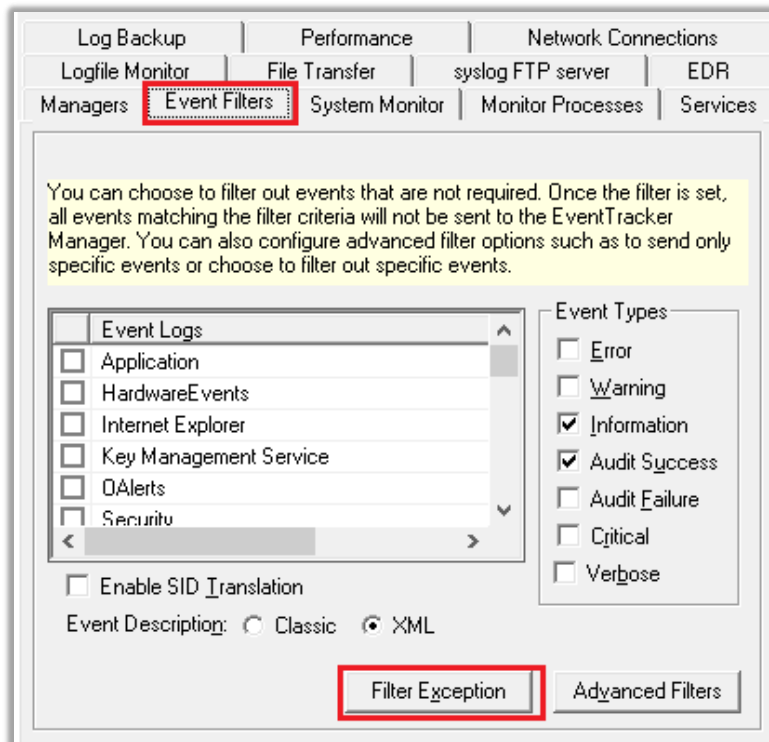


Figure 5

4. In “Filter Exception” wizard, click on “New” button:

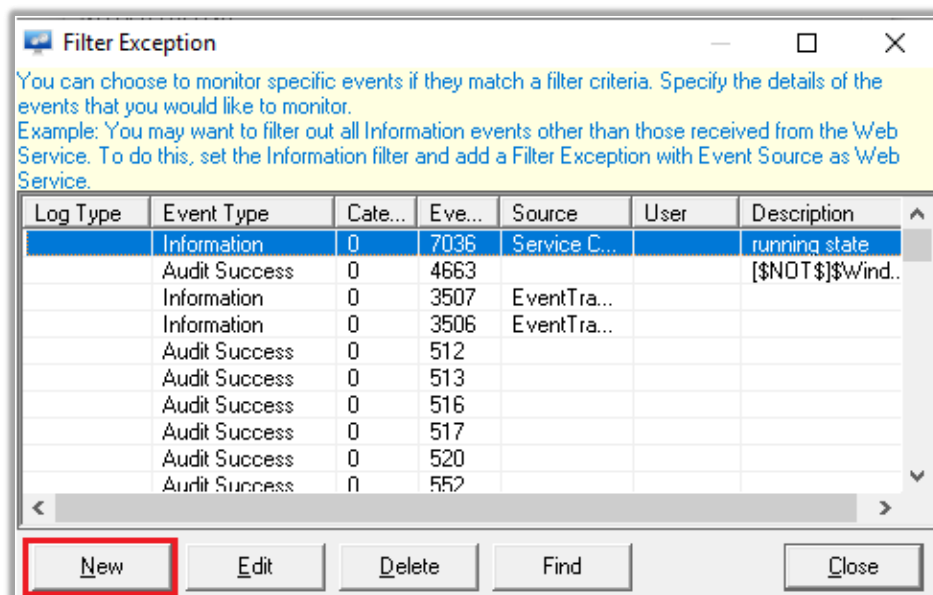


Figure 6

5. In “New Event Details” wizard, specify the values as give in the picture below and click “OK”:

**New Event Details**

Event Details (empty field implies all matches)

Log Type :  
Defender

Event Type :  
Information

Event ID :

Category :

Match in User :

Match in Source :  
Defender Console

Match in Event Descr :

"Match in Event Descr", "Match in User" and "Match in Source" field can take multiple strings separated with && or ||. && stands for AND condition. || stands for OR condition. For negating the result of match operation, prefix the string with "[NOT\$]". If there are multiple strings, then the result of the whole expression is negated. Only one "[NOT\$]" should be used in the string.  
Example:  
The string "[NOT\$]Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description.  
[For more information click here.](#)

OK Cancel

Figure 7

6. Next, click on “Close” button and then click on “Save”:

**Filter Exception**

You can choose to monitor specific events if they match a filter criteria. Specify the details of the events that you would like to monitor.  
Example: You may want to filter out all Information events other than those received from the Web Service. To do this, set the Information filter and add a Filter Exception with Event Source as Web Service.

Log Type	Event Type	Cate...	Eve...	Source	User	Description
	Audit Success	0	611			
	Audit Success	0	610			
	Audit Success	0	551			
	Audit Success	0	540		[NOT...	
	Audit Success	0	538		[NOT...	
	Information	0	104			
	Information	0	1074	USER32		
	Information	0	3230			
	Information	0		Defender...		

New Edit Delete Find Close

Figure 8



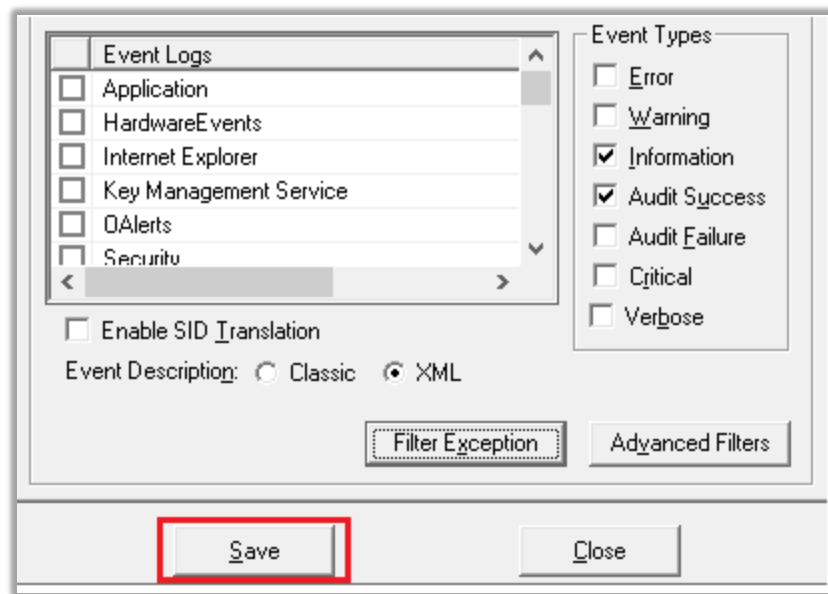


Figure 9

7. Finally, click on “**Close**” button to complete the integration process.

## 4. EventTracker Knowledge Packs

### 4.1 Saved Searches

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

- **Defender MFA - Accepted connections:** This category of saved searches will allow users to quickly parse and display events associated with successfully authenticated token requests from users.
- **Defender MFA - Authentication requests:** This category of saved searches will allow users to quickly parse and display events associated with authentications requests/ attempt made by a user.
- **Defender MFA - Defender Console Activity:** This category of saved searches will allow users to quickly parse and display events associated with events logged One Identity Defender AD console, such as assigning a Defender password to a user, setting a token PIN, etc.
- **Defender MFA - Rejected connections:** This category of saved searches will allow users to quickly parse and display events associated with rejected authentications requests by a user due wrong token code or some other reason.
- **Defender MFA - Token Management:** This category of saved searches will allow users to quickly parse and display events associated with events logged One Identity Defender AD console, such as assigning a token to a user or deleting/removing token from user.

## 4.2 Alerts

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

- **Defender MFA: A defender password has been assigned to a user** - This alert is triggered as soon as EventTracker receives an event that indicate a defender password is assigned to a user.
- **Defender MFA: A defender password has been unassigned from user** - This alert is triggered as soon as EventTracker receives an event indicate that a defender password is unassigned/removed from a user.
- **Defender MFA: A token has been assigned to a user** - This alert is triggered as soon as EventTracker receives an event that indicate a token is assigned to a user.
- **Defender MFA: A token has been unassigned from user** – This alert is triggered as soon as EventTracker receives an event that indicate a token is unassigned from a user.
- **Defender MFA: A user authentication request has been rejected** – This alert is triggered as soon as EventTracker receives an event that indicates a failed authentication attempt using a token.

## 4.3 Flex Reports

Reports are a detailed overview of any event occurring in Defender MFA, represented in column-value format.

- **Defender MFA - Successful user authentications:** This report generates a detailed overview of activities that includes a successful token/defender password authentication by any user. It includes, event datetime, event computer, username, authentication type, and session ID.
- **Defender MFA - Failed user authentications:** This report generates a detailed overview of activities that includes a failed token/defender password authentication by any user. It includes, event datetime, event computer, username, failure reason, request ID, and session ID.
- **Defender MFA - Token Management:** This report generates a detailed overview of activities that includes a successful token/defender password authentication by any user. It includes, event datetime, event computer, username, token ID and token status.

## 4.4 Dashboards

- Defender MFA - Top successful user authentications

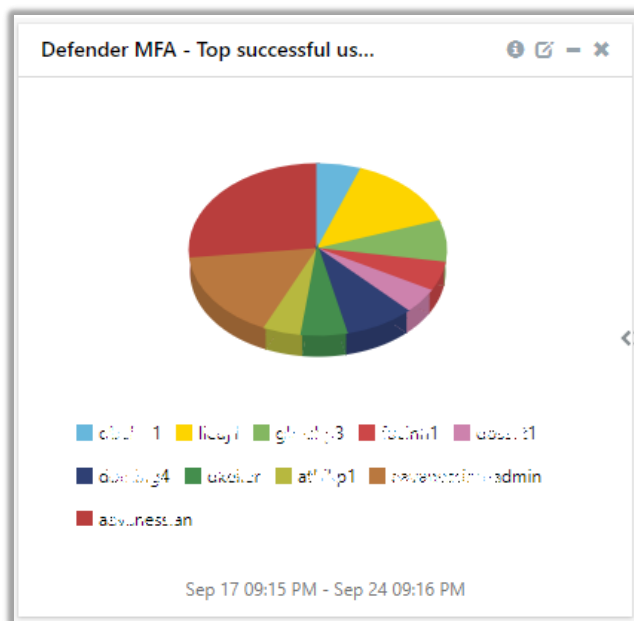


Figure 10

- Defender MFA - Authentication success by login count

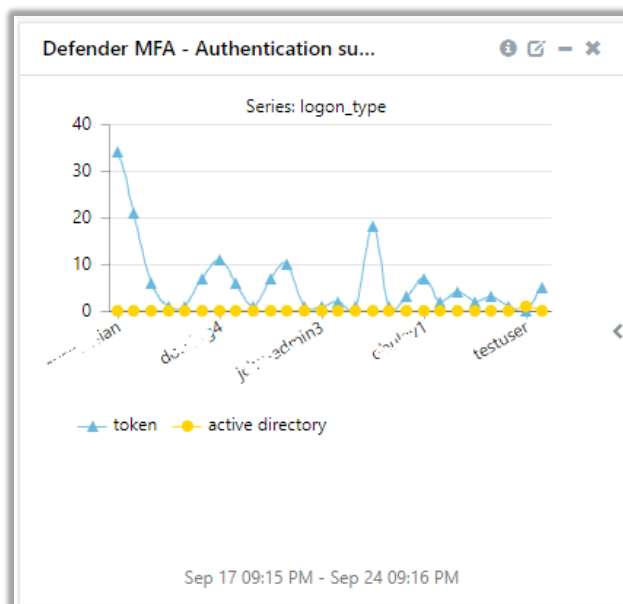


Figure 11

- Defender MFA - Authentication success by logon type

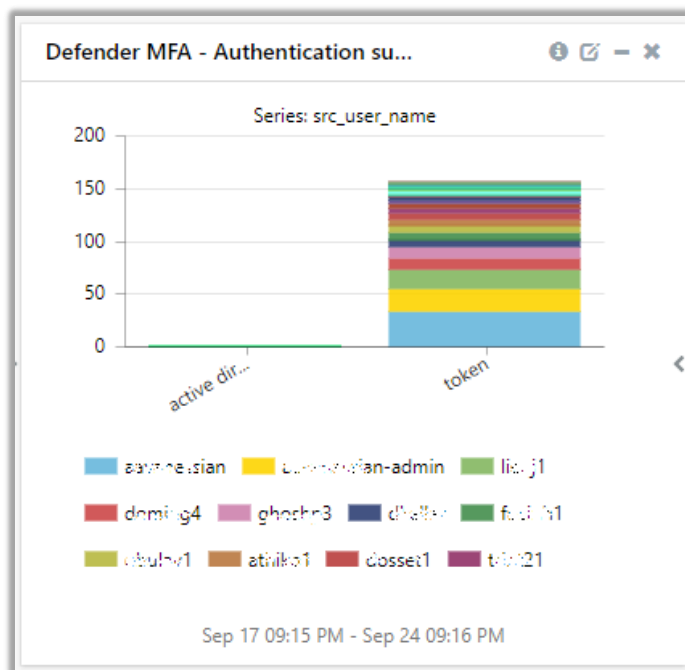


Figure 12

- Defender MFA - Top user authentication fails

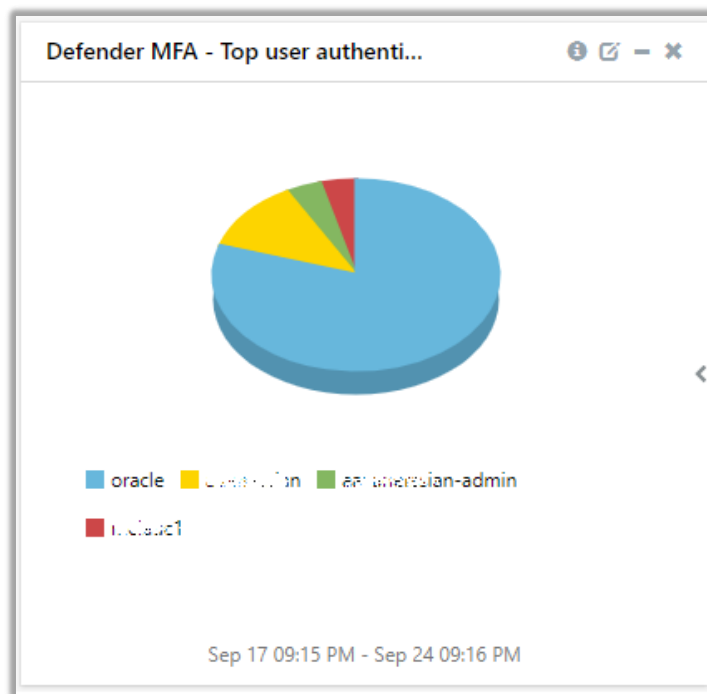


Figure 13

- Defender MFA - User authentication failure reasons

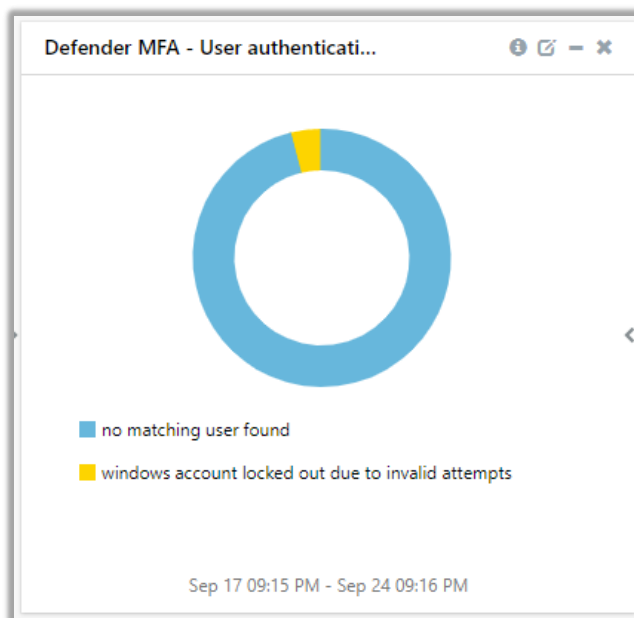


Figure 14

- Defender MFA - Authentication requests by source IP

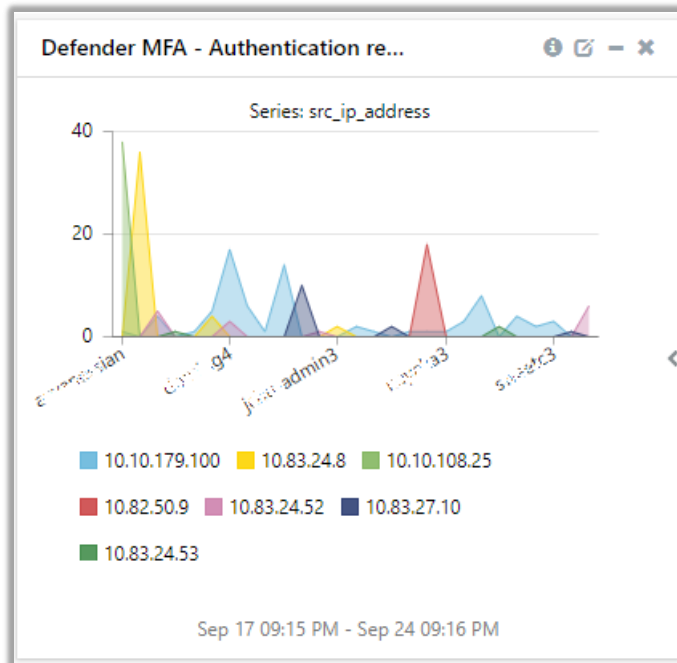


Figure 15

- Defender MFA - Token assigned to user

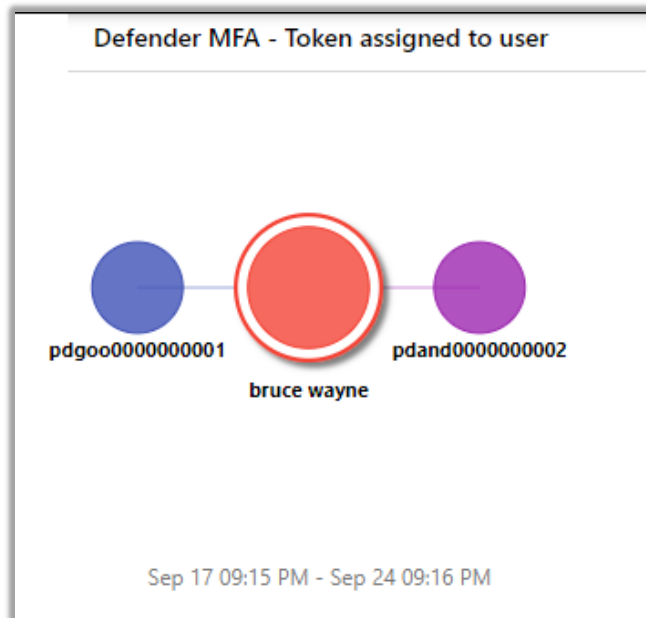


Figure 16

- Defender MFA - Token unassigned from user

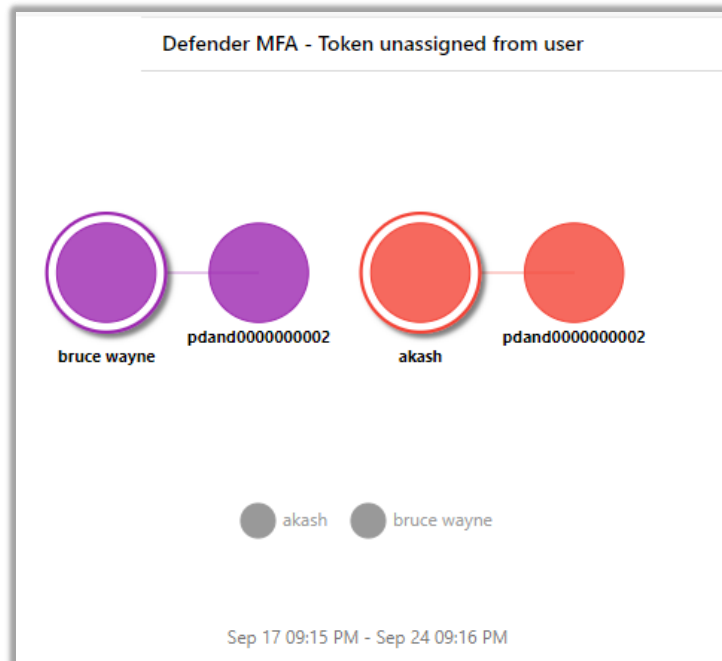


Figure 17

## 5. Importing knowledge pack into EventTracker

### Getting Knowledge Packs

To get the knowledge packs, locate the knowledge pack folder. Follow the below steps:

1. Press “**Windows** + 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
  - Flex Reports
  - Knowledge Objects
  - Dashboards
1. Launch the **EventTracker Control Panel**.
  2. Double click **Export-Import Utility**.

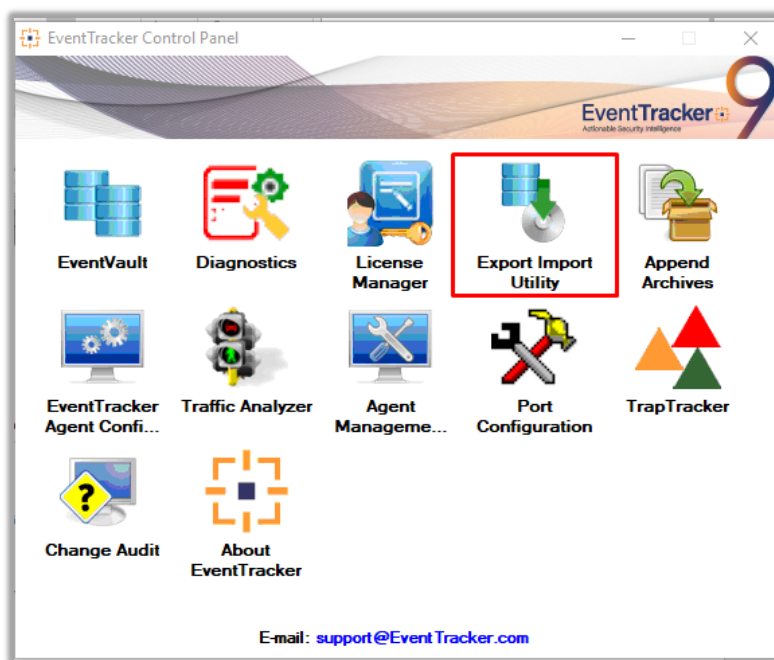


Figure 18

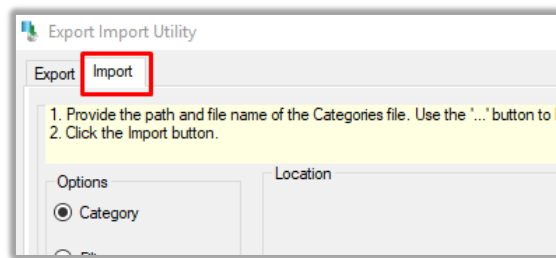


Figure 19

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 the browse  button.
2. Navigate to the knowledge pack folder and select the file with extension “.iscat”, e.g. “**Categories\_Defender MFA.iscat**” and then click on the “**Import**” button:

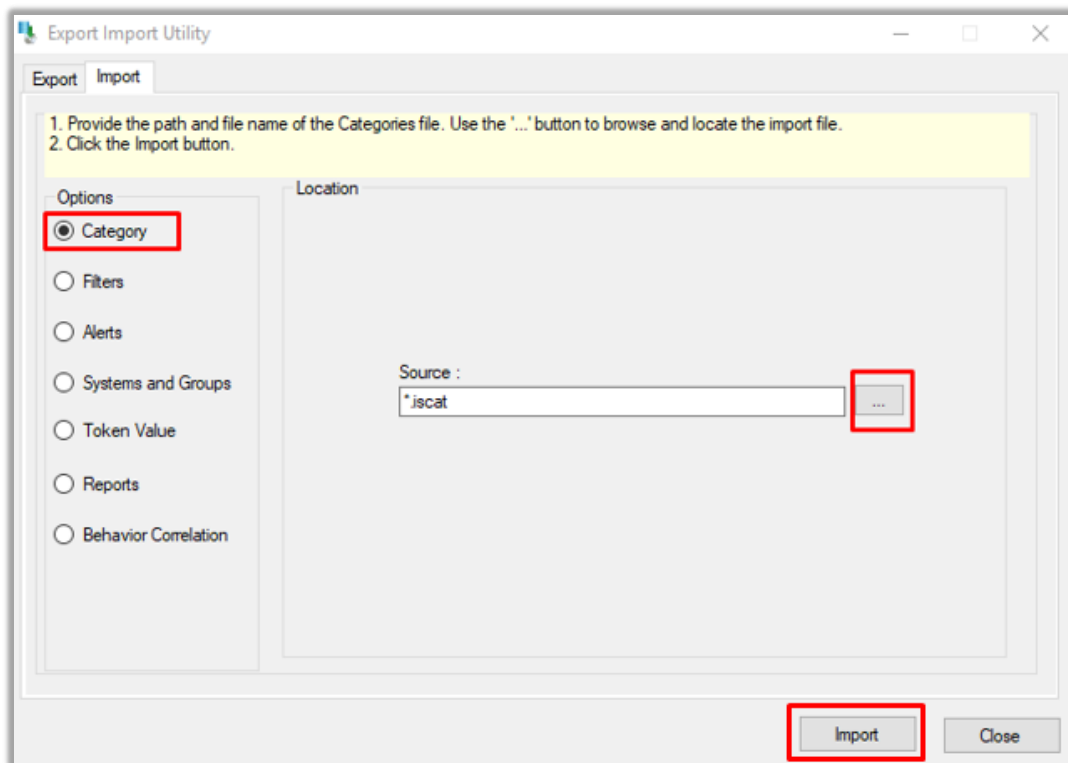


Figure 20



EventTracker displays a success message.

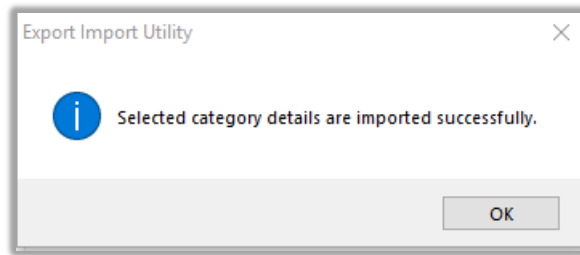



Figure 21

## 5.2 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 extension ".isalt", e.g. "Alerts\_Defender MFA.isalt" and then click on the "Import" button:

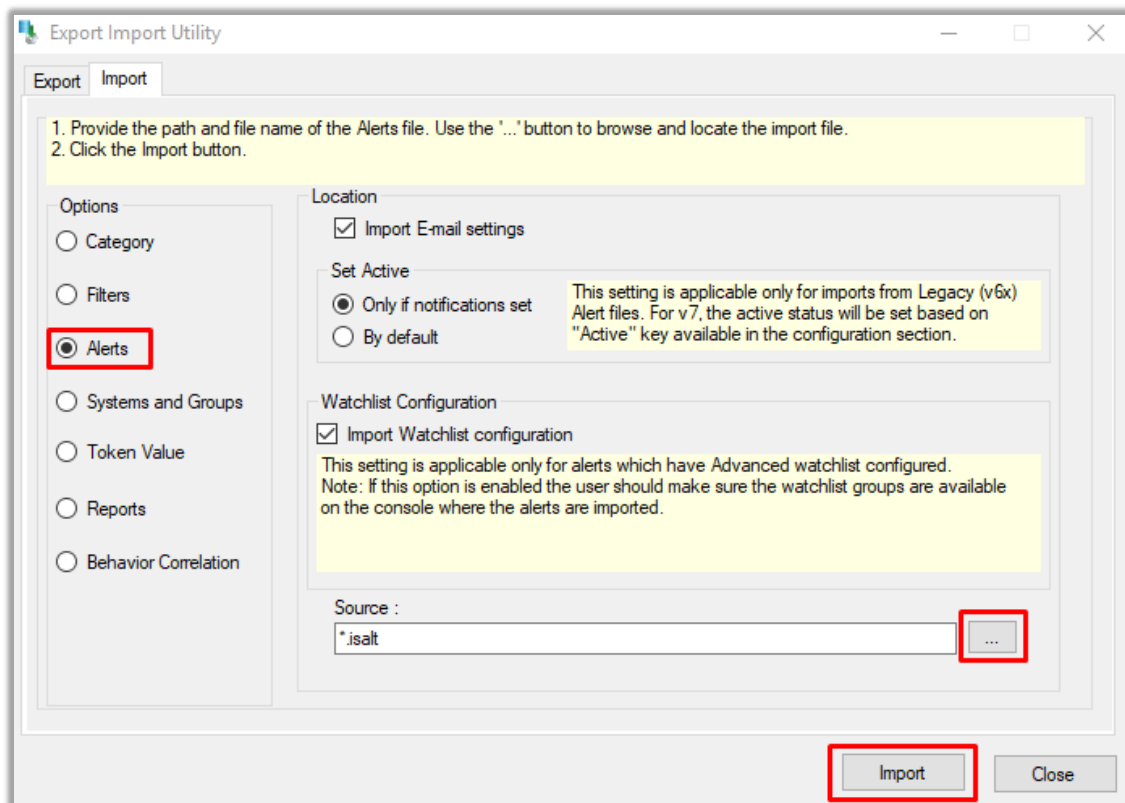


Figure 22

EventTracker displays a success message:

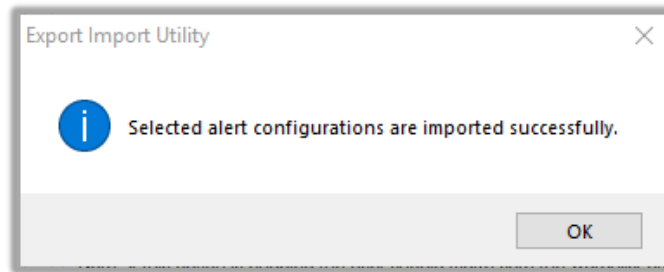


Figure 23

## 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.

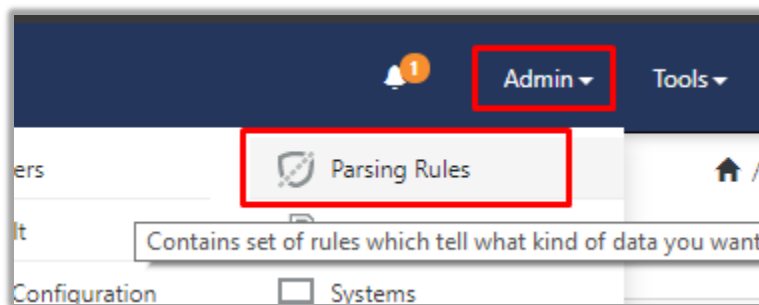


Figure 24

2. Next, click the “**Template**” tab and then click the “**Import Configuration**” button.

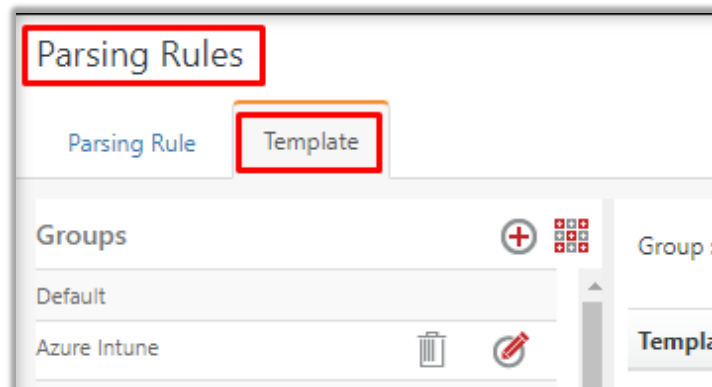


Figure 25

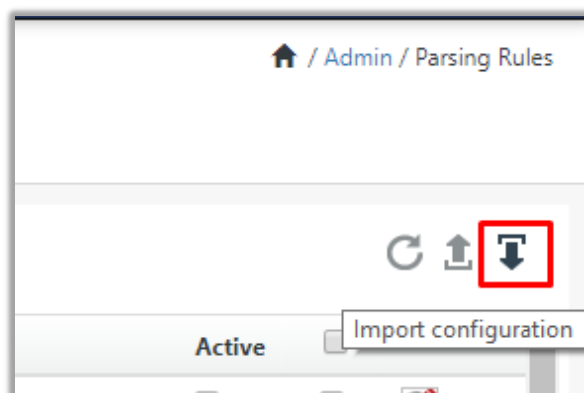


Figure 26

- Now, click **“Browse”** button and navigate to the knowledge packs folder (type **“%et\_install\_path%\Knowledge Packs”** in navigation bar) where **“.ettd”**, e.g. **“Templates\_Defender MFA.ettd”** file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click **“Import”** button:

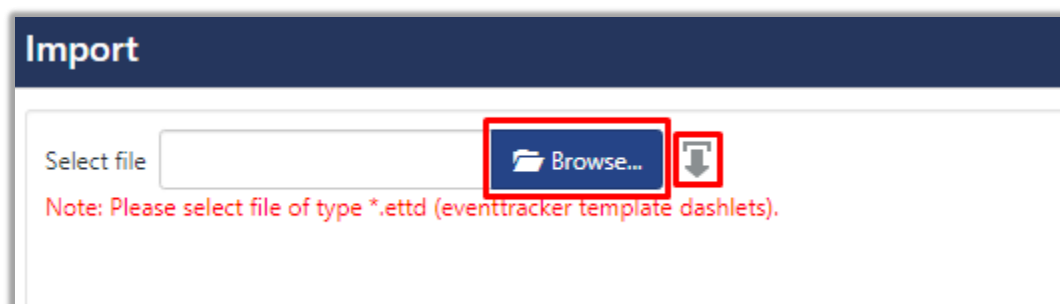


Figure 27

## 5.4 Flex Reports

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

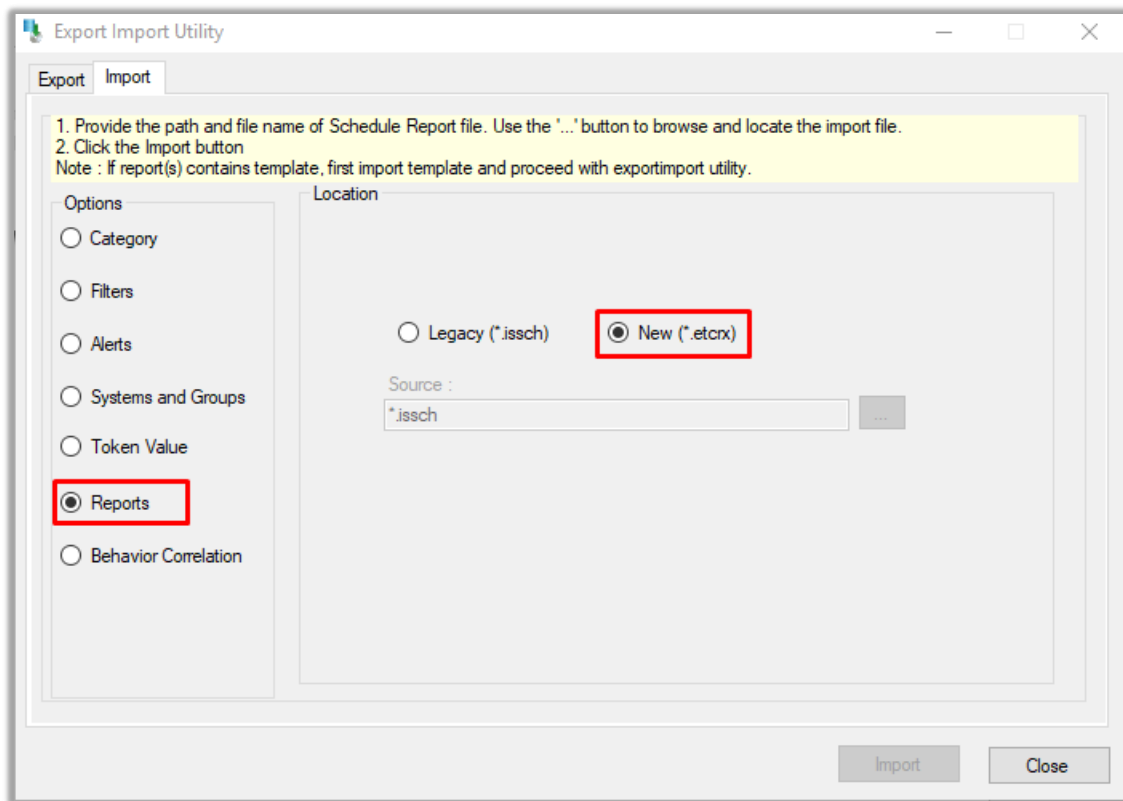


Figure 28

2. Once you have selected “**New (\*.etcrx)**”, a new pop-up window will appear. Click “**Select File**” button and navigate to knowledge pack folder and select file with extension “**.etcrx**”, e.g. “**Reports\_ Defender MFA.etcrx**”.

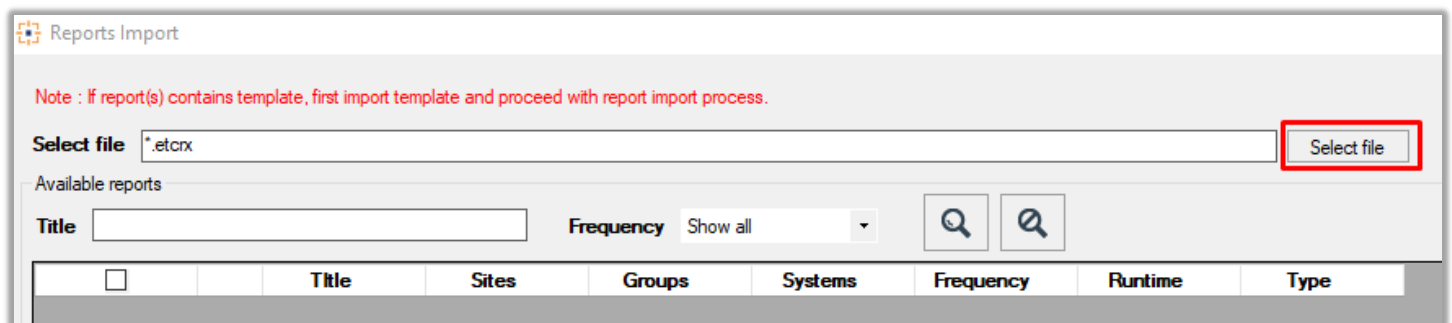



Figure 29

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

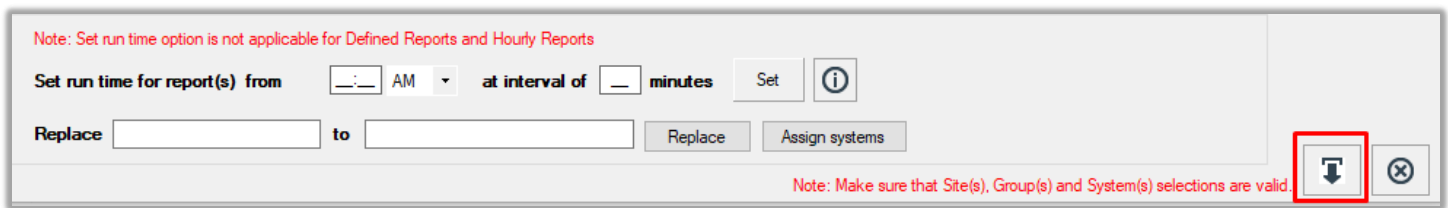


Figure 30

EventTracker displays a success message:

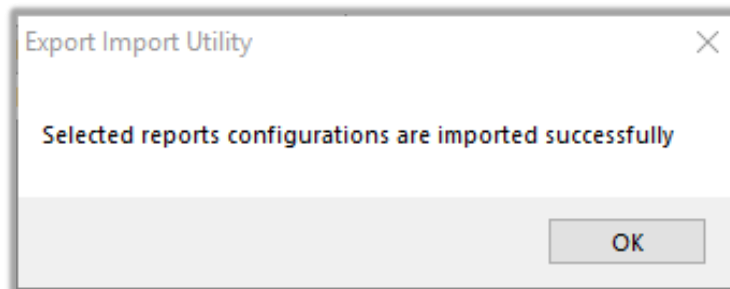


Figure 31

## 5.5 Knowledge Objects

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

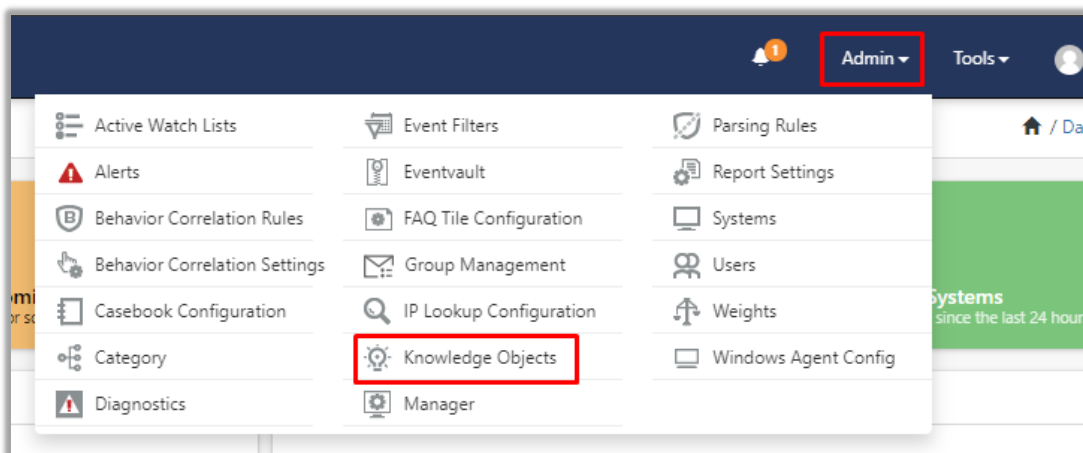


Figure 32

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

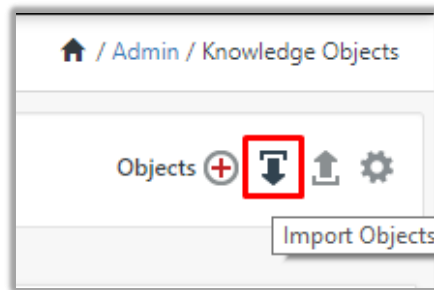


Figure 33

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\_Defender MFA.etko"** and then click **"Upload"** button.

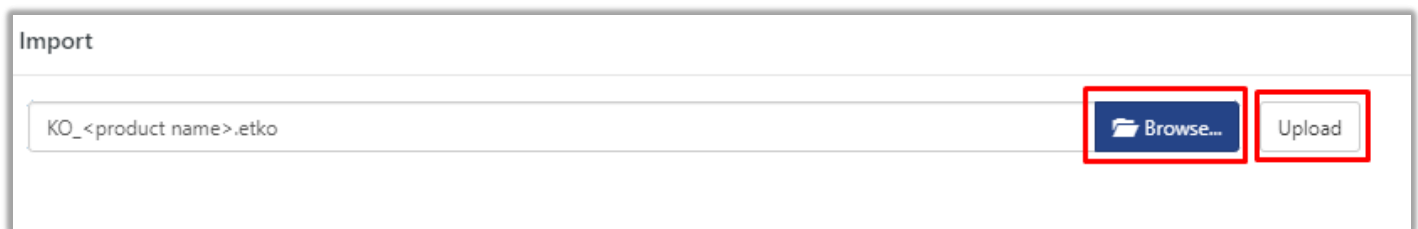


Figure 34

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



Figure 35

## 5.6 Dashboards

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

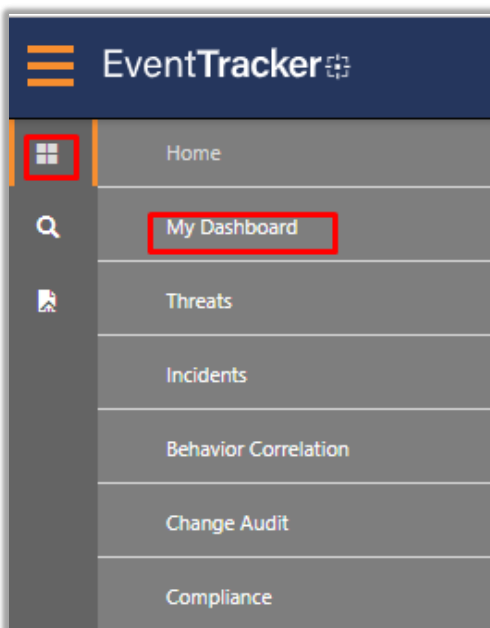


Figure 36

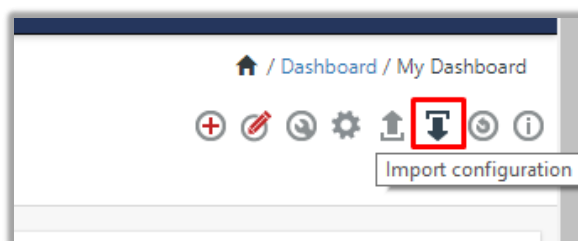


Figure 37

4. Select the **browse** button and navigate to knowledge pack folder (type “%et\_install\_path%\Knowledge Packs” in navigation bar) where “.etwd”, e.g. “Dashboards\_Defender MFA.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.

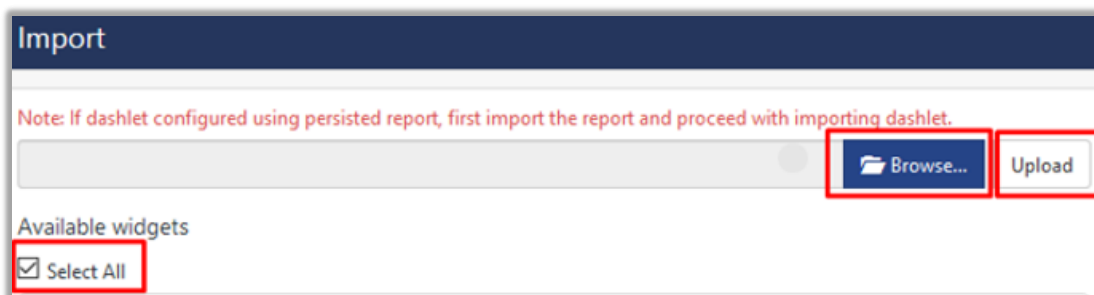


Figure 38

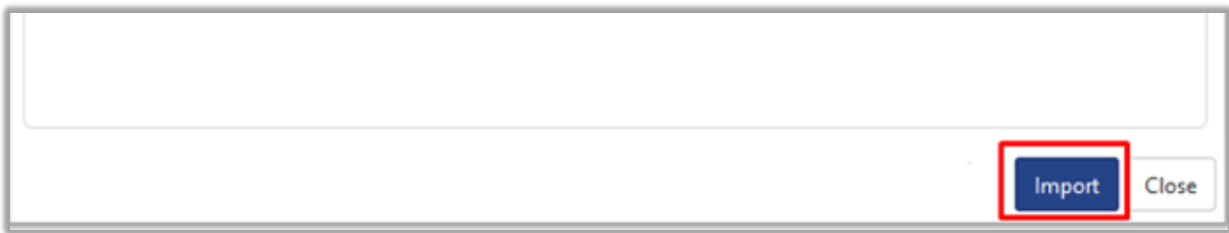


Figure 39

## 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 “**Defender MFA**” group folder to view the imported categories:

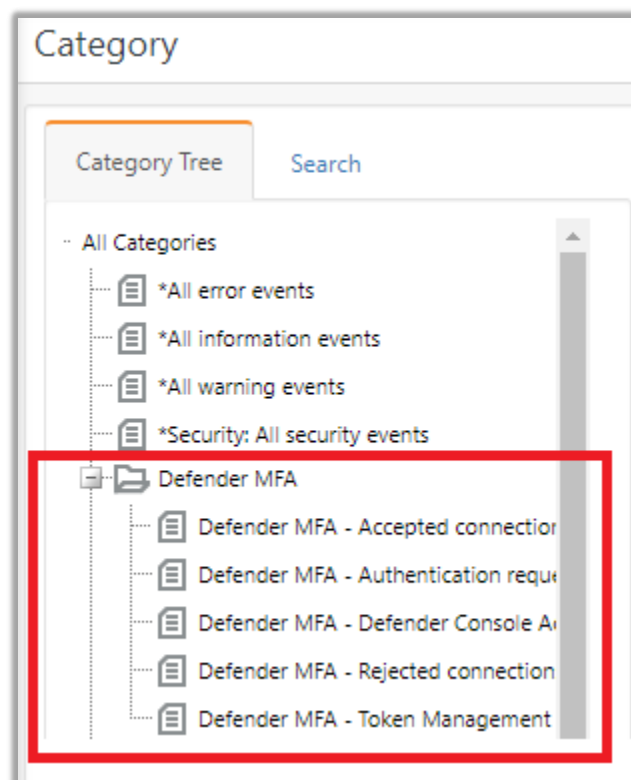


Figure 40



## 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. “**Defender MFA**” and then click the **Search** button.

EventTracker displays an alert related to “**Defender MFA**”:

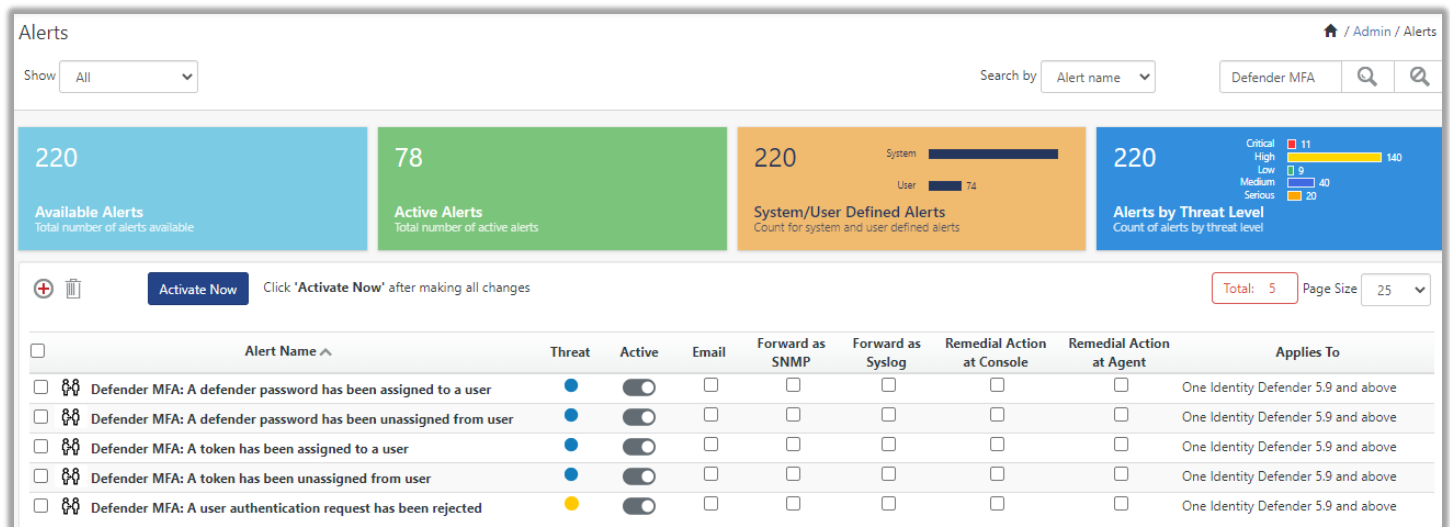


Figure 41

## 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. “**Defender MFA**” group folder to view the imported Templates.

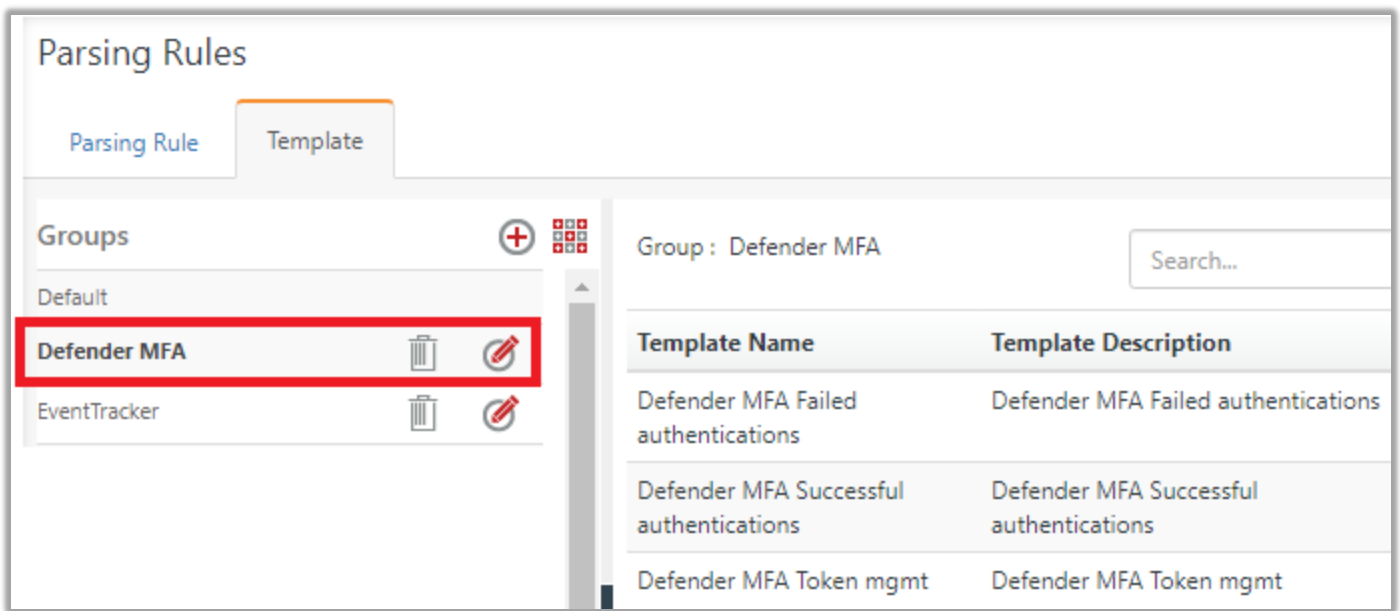


Figure 42

## 6.4 Flex Reports

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

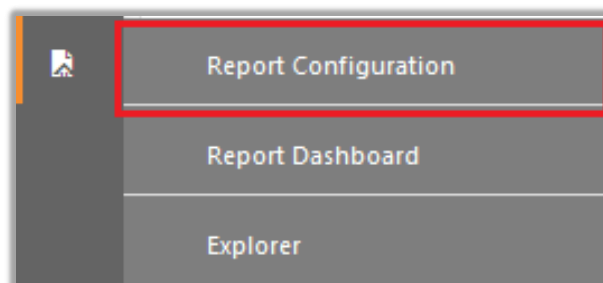


Figure 43

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

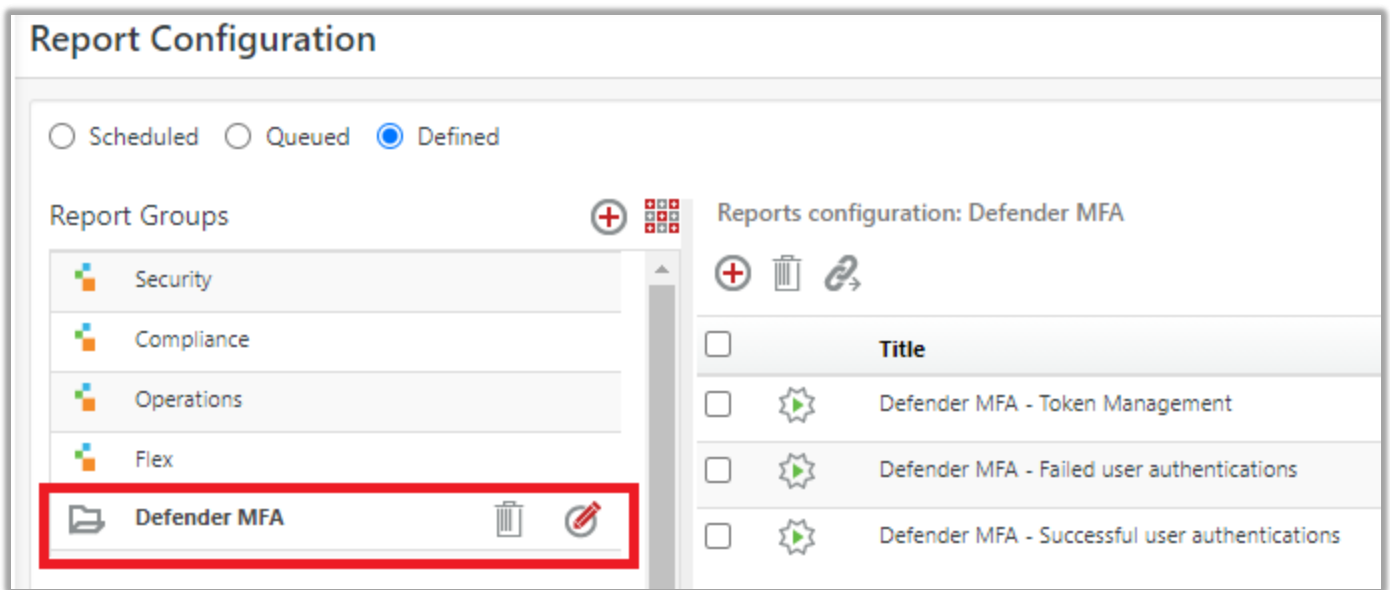


Figure 44

## 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 “**Defender MFA**” group folder to view the imported Knowledge objects.

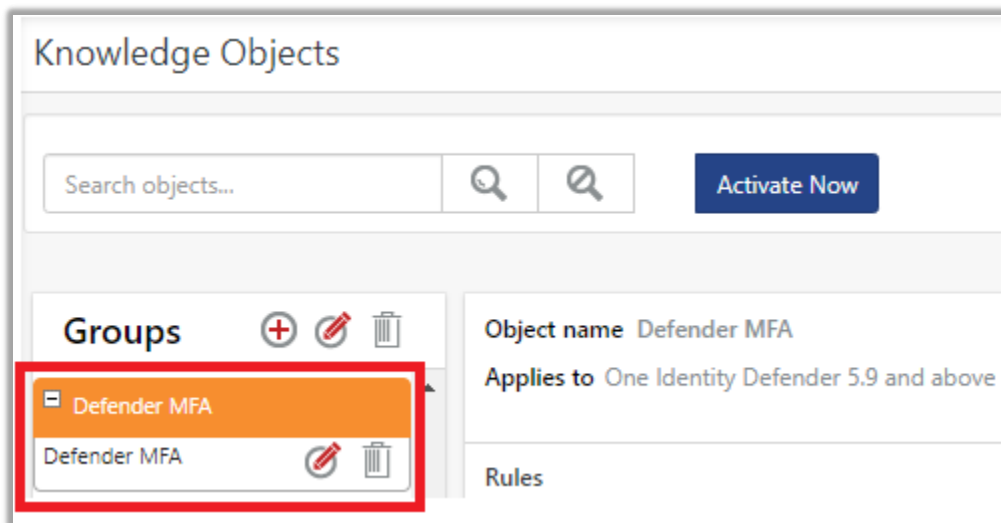



Figure 45

## 6.6 Dashboards

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

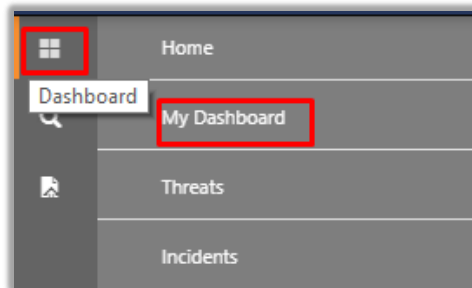



Figure 46

2. Select **"Customize daslets"**  button. And type **"Defender MFA"** in the search bar.

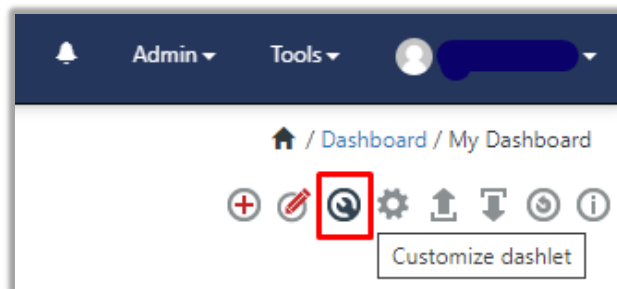


Figure 47

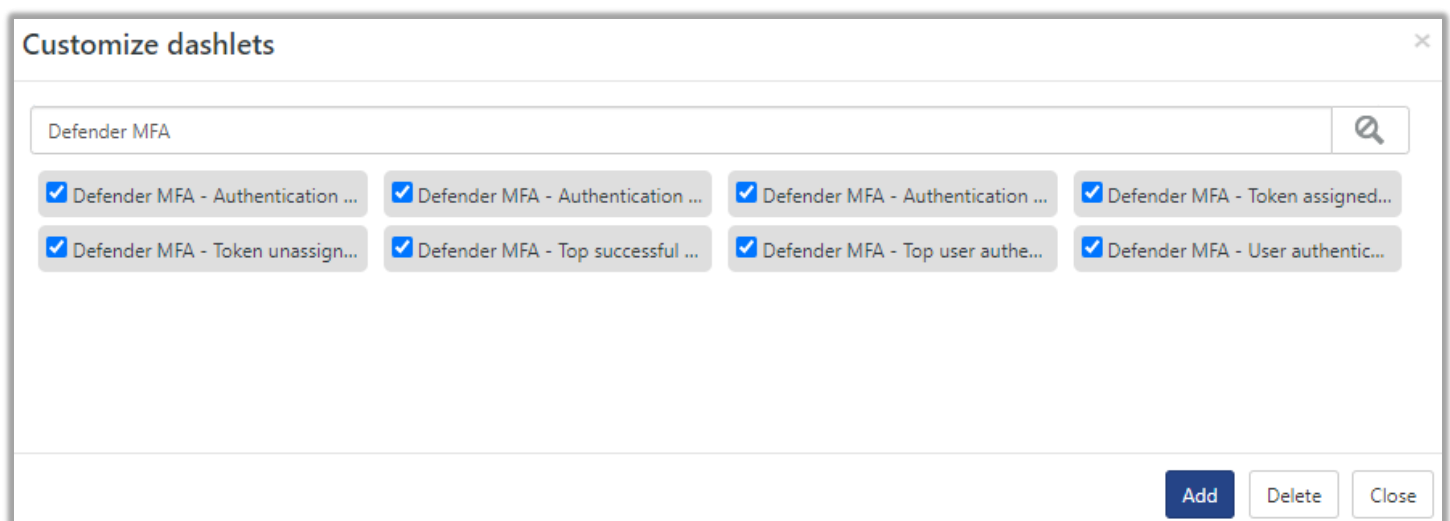


Figure 48