

Integrate Azure MFA On-Premise

EventTracker v9.x and above

Abstract

This guide provides instructions to configure Microsoft Azure Multi-Factor Authentication (MFA) to send logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.x or above and **Azure MFA On-Premise**

Audience

Administrators who are assigned the task to monitor Azure MFA On-Premise 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. Integration of Azure MFA On-Premise with EventTracker	3
3.1 Integrating via syslog configuration	3
4. EventTracker Knowledge Pack	5
4.1 Category	5
4.2 Alert	5
4.3 Report	5
4.4 Dashboards	6
5. Importing Azure MFA On-Premise knowledge pack into EventTracker	9
5.1 Category	9
5.2 Alert	10
5.3 Token template	11
5.4 Knowledge Object	13
5.5 Report	15
5.6 Dashboards	16
6. Verifying Azure MFA On-Premise knowledge pack in EventTracker	19
6.1 Category	19
6.2 Alert	20
6.3 Token templates	21
6.4 Knowledge Object	21
6.5 Report	22
6.6 Dashboards	23

1. Overview

Microsoft Azure Multi-Factor Authentication (MFA) prompts the users during the sign-in process for an additional form of identification, such as to enter a code on cellphone or to provide a fingerprint scan.

EventTracker helps to monitor events from **Azure MFA On-Premise**. Its dashboard and reports will help you to detect authentication activities.

EventTracker's built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Prerequisites

- Admin privileges for **Azure MFA** and should be installed.
- **EventTracker agent** should be installed in the system.

3. Integration of Azure MFA On-Premise with EventTracker

3.1 Integrating via syslog configuration

Follow the below steps to configure syslog.

1. Log on to the server running the Multi-Factor Authentication Server with administrative privileges.
2. Open the Multi-Factor Authentication Server Management console by searching for it on the Start Screen.
3. In the left pane, click **Logging-> syslog** tab.

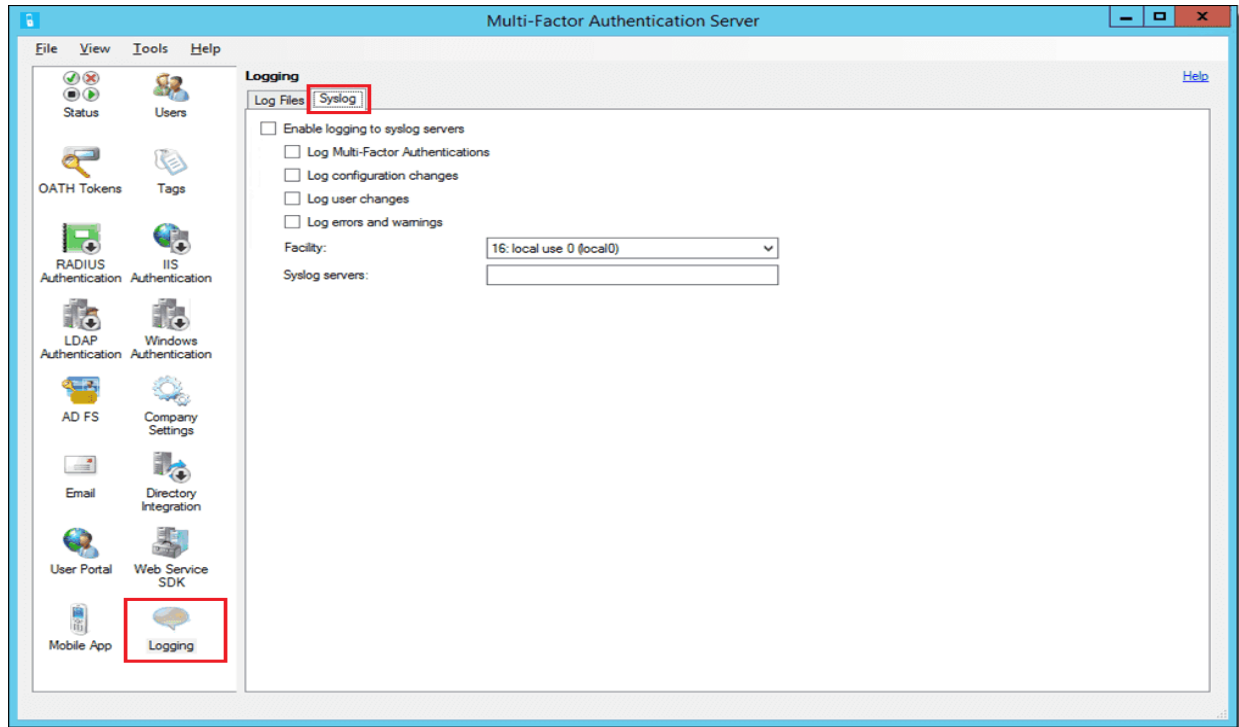


Figure 1

4. Check the “Enable logging to syslog server” box.
5. Enter the EventTracker Manager IP in the syslog server field.

Integration is complete, EventTracker will receive Azure MFA logs.

4. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support Azure MFA.

4.1 Category

- **Azure MFA: Authentication Success** - This category provides information related to successful authentication.
- **Azure MFA: Authentication Failure** – This category provides information related to all authentication failure.

4.2 Alert

- **Azure MFA: Authentication Failure** - This alert is generated when any authentication failure is detected by Azure MFA.

4.3 Report

- **Azure MFA – Authentication Failure** - This report gives information about all the authentication failure detected by Azure MFA. Report contains username, source IP, guide, call status along with other useful information for further analysis.

LogTime	Computer	Call Status	Guid	IP Address	Message	Username	EventDescription
05/07/2020 12:09:16 PM	172.xx.xxx-SYSLOG	FAILED_PHONE_BUSY	080dc30d-9b6d-419f-8378-46d762944486		Auth Already In Progress	ericschm	May 07 12:09:16 172.27.100.13 Apr 30 18:47:20 RAMADFS02 Apr 30 18:47:20 ramads02 pfsvc: info:080dc30d-9b6d-419f-8378-46d762944486
05/07/2020 12:09:16 PM	172.xx.xxx-SYSLOG	FAILED_PHONE_APP_NO_RESPONSE	b345747c-09d3-4b26-94e7-58045fa8f1aa		Mobile App No Response	ericschm	May 07 12:09:16 172.27.100.13 Apr 30 18:49:49 RAMADFS02 Apr 30 18:49:49 ramads02 pfsvc: info:080dc30d-9b6d-419f-8378-46d762944486
05/07/2020 12:09:16 PM	172.xx.xxx-SYSLOG	FAILED_PHONE_APP_NO_RESPONSE	e0fec917-a60a-4743-92dd-9039bd20b93e		Mobile App No Response	ericschm	May 07 12:09:16 172.27.100.13 Apr 30 18:48:26 RAMADFS02 Apr 30 18:48:26 ramads02 pfsvc: info:080dc30d-9b6d-419f-8378-46d762944486

Figure 2

- **Azure MFA – Authentication Success** - This report gives information about all the successful authentication detected by Azure MFA. Report contains username, source IP, guide, call status along with other useful information for further analysis.

LogTime	Computer	Call Status	Guid	IP Address	Message	Username	EventDescription
05/07/2020 12:09:23 PM	172.xx.xxx-SYSLOG	SUCCESS_PHONE_APP_AUTHENTICATED	76bae747-3fb2-4c8e-a312-3dcadfd7c997	172.xx.xx.xx	Mobile App Authenticated	joshmde@connexusenergy.com	May 07 12:09:23 172.xx.xxx Apr 30 06:59:07 RAMMFA01 Apr 30 06:59:07 ramffa01 pfsvc: info:080dc30d-9b6d-419f-8378-46d762944486
05/07/2020 12:09:23 PM	172.xx.xxx-SYSLOG	SUCCESS_PHONE_APP_AUTHENTICATED	2ddadce3-ebc6-4c72-b3e9-6eba18b2c962		Mobile App Authenticated	joshmde	May 07 12:09:23 172.xx.xxx Apr 30 06:59:27 RAMADFS02 Apr 30 06:59:27 ramads02 pfsvc: info:080dc30d-9b6d-419f-8378-46d762944486
05/07/2020 12:09:23 PM	172.xx.xxx-SYSLOG	SUCCESS_PHONE_APP_AUTHENTICATED	2f7d1d88-2ab7-49e4-935f-c143d38ec20c		Mobile App Authenticated	mattclay	May 07 12:09:23 172.xx.xxx Apr 30 07:11:20 RAMADFS02 Apr 30 07:11:20 ramads02 pfsvc: info:080dc30d-9b6d-419f-8378-46d762944486

Figure 3

- **Logs Considered**

action	+ - succeeded
event_category	+ - 0
event_computer	+ - 172.27.100.13-syslog
event_datetime	+ - 5/7/2020 5:16:17 PM
event_datetime_utc	+ - 1588851977
event_description	May 07 17:16:17 172.27.100.13 Apr 29 06:47:28 RAMADFS02 Apr 29 06:47:28 ramadfs02 pfsvc: i pfsvc 7c8195d4-b738-45fa-9b4d-8d16dfa842d1 succeeded for user 'davejohn'. Call status: SUCCESS_PHONE_APP_AUTHENTICATED - "Mobile App Authentic
event_group_name	+ - Default
event_id	+ - 128
event_log_type	+ - Application
event_source	+ - SYSLOG local0
event_type	+ - Error
event_user_domain	+ - N/A
event_user_name	+ - N/A
log_source	+ - Azure MFA
log_type	+ - SUCCESS_PHONE_APP_AUTHENTICATED
object_id	+ - 7c8195d4-b738-45fa-9b4d-8d16dfa842d1
reason	+ - Mobile App Authenticated
source_type	+ - Azure MFA
src_user_name	+ - davejohn
tags	+ - Authentication Success
tags	+ - Authentication Activities

Figure 4

4.4 Dashboards

- **Azure MFA: Authentication Success**

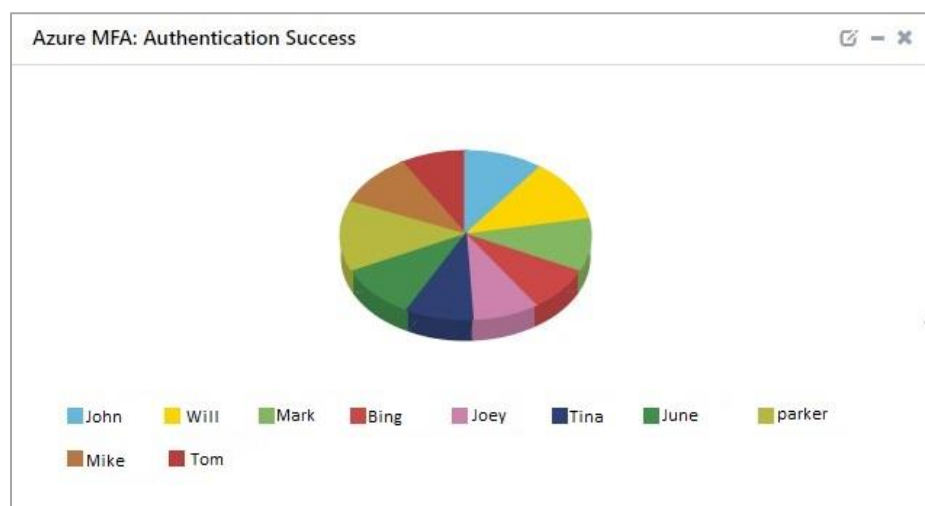


Figure 5

- **Azure MFA: Authentication Failure**

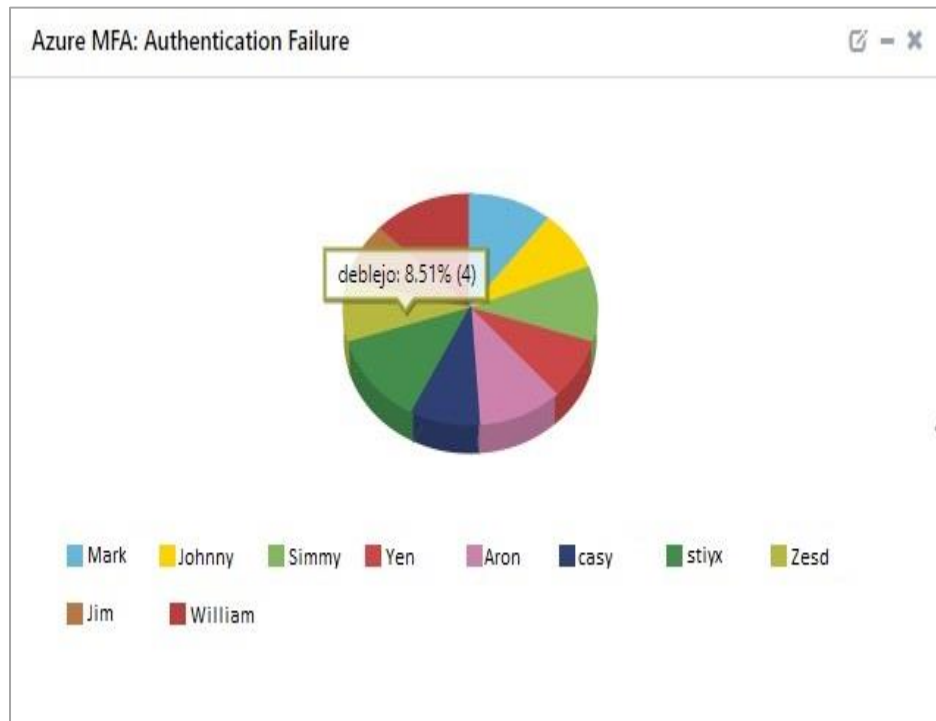


Figure 6

- **Azure MFA: User Location**



Figure 7

- **Azure MFA: Authentication Failed with Method Used**

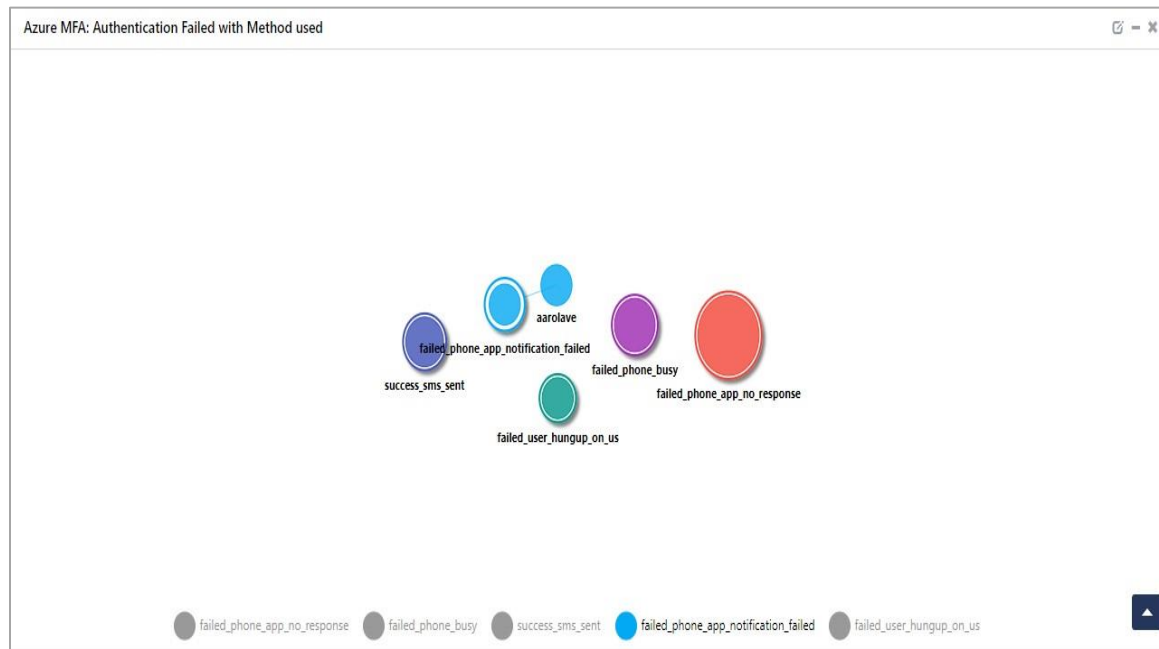


Figure 8

- **Azure MFA: Authentication Request Mode**

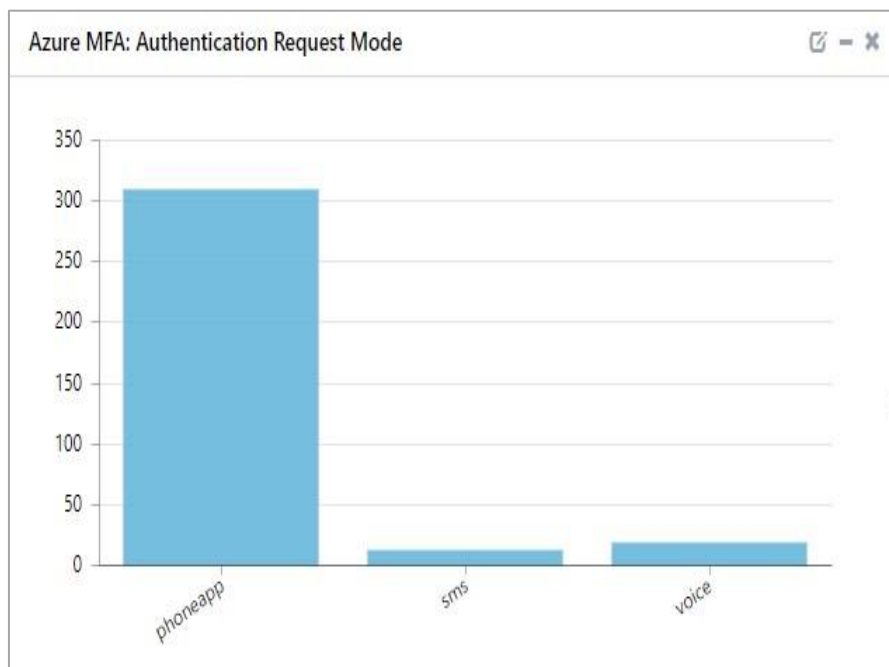


Figure 9

5. Importing Azure MFA On-Premise knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence.

- Category
- Alert
- Token template
- Knowledge Object
- Report
- Dashboard

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

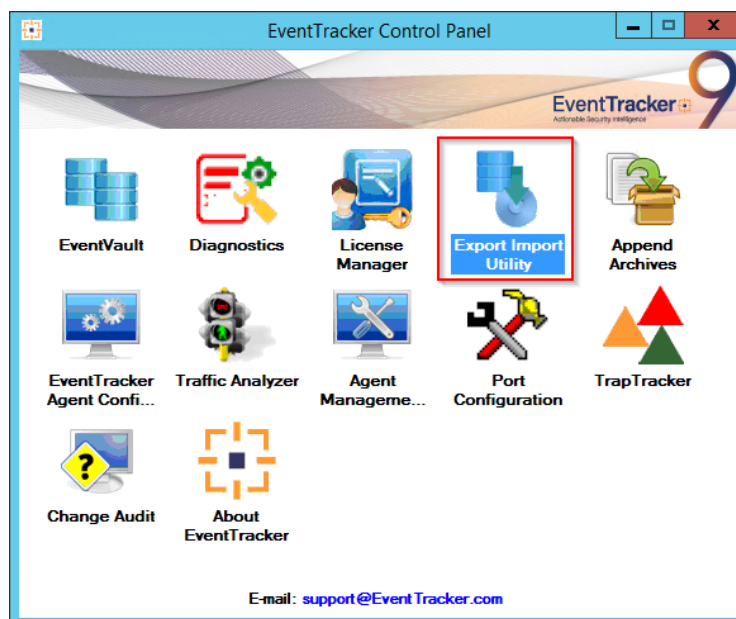


Figure 10

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click **Browse** .

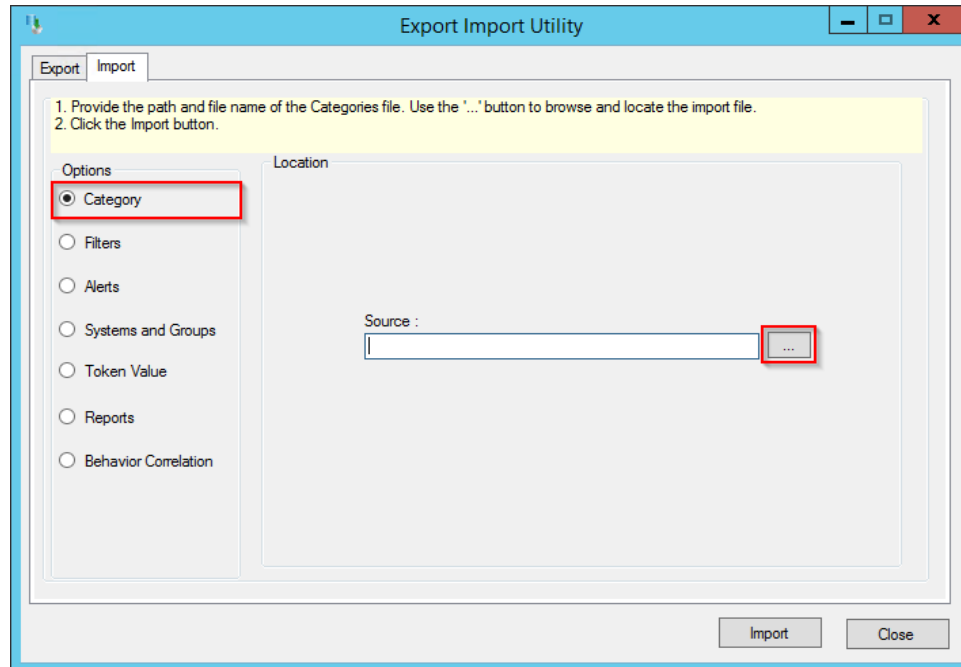


Figure 11

2. Locate **Categories_Azure MFA.iscat** file, and then click **Open**.
3. To import categories, click **Import**.

EventTracker displays success message.

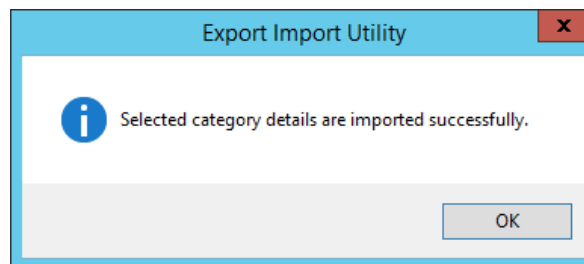



Figure 12

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

5.2 Alert

1. Click **Alert** option, and then click **Browse**  .

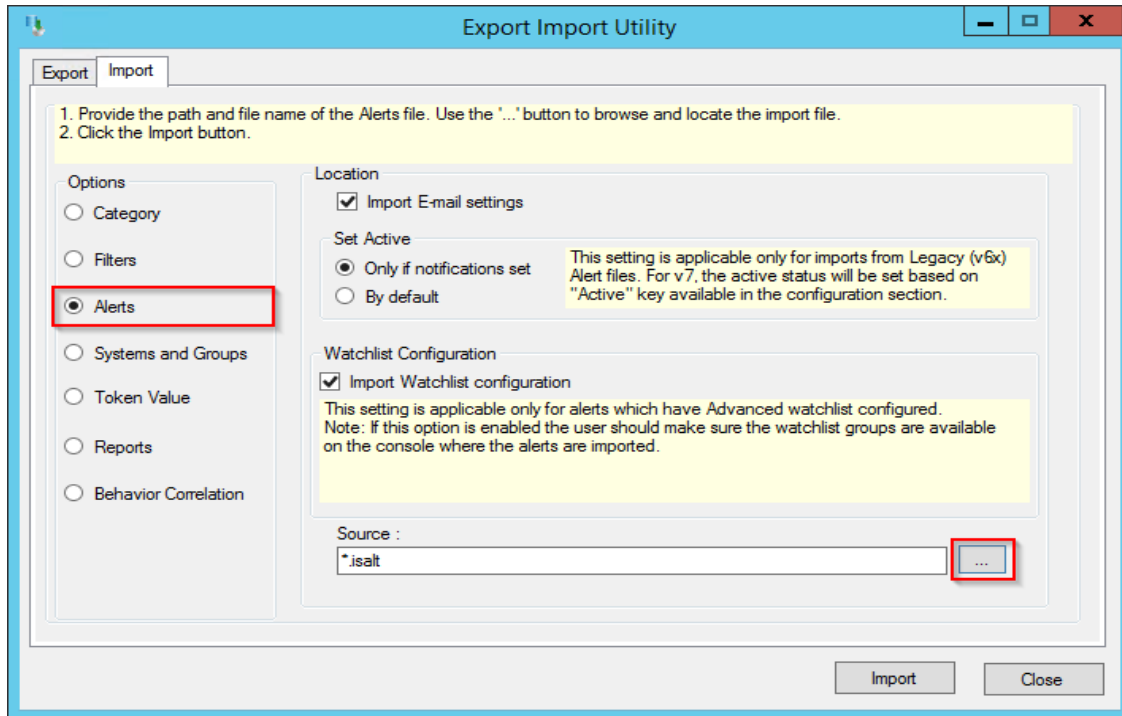


Figure 13

2. Locate **Alerts_Azure MFA.isalt** file, and then click **Open**.
3. To import alerts, click **Import**.
EventTracker displays success message.

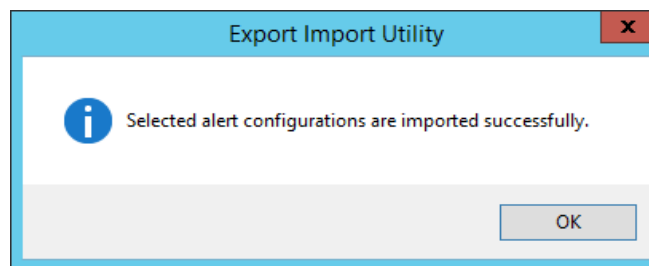


Figure 14

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

5.3 Token template

1. Click **Parsing rule** under **Admin** option in the EventTracker manager page.

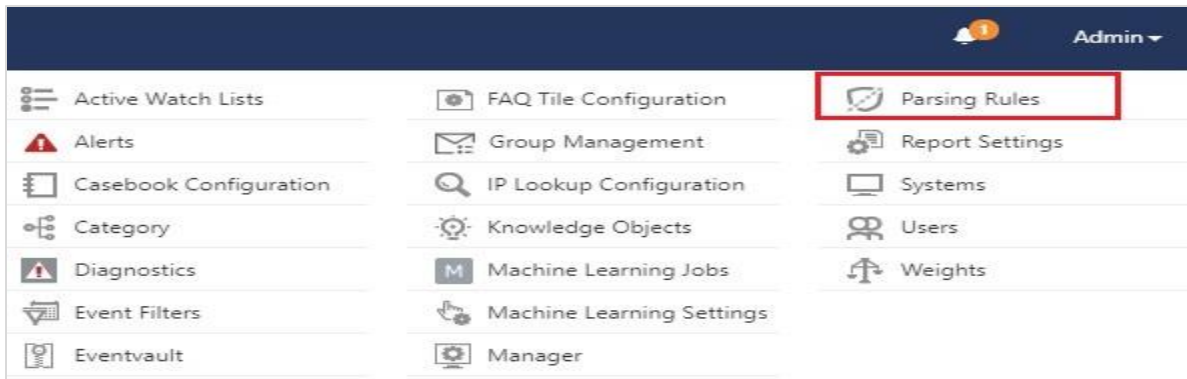


Figure 15

2. Click **Template**.

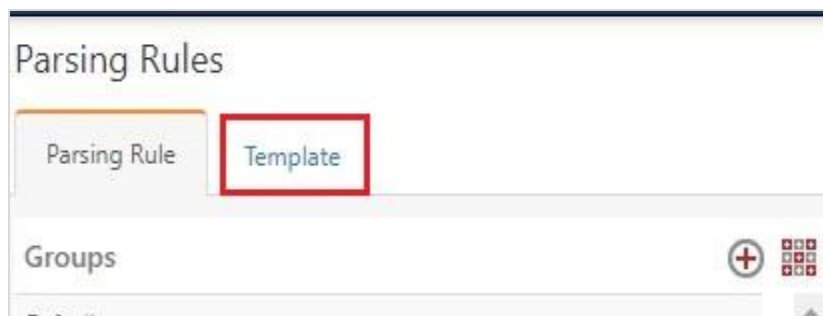


Figure 16

3. To import token template, click **Import**.



Figure 17

4. Locate the **Templates_Azure MFA.ett** type file by clicking **Browse**, enable all the templates and click **import**.

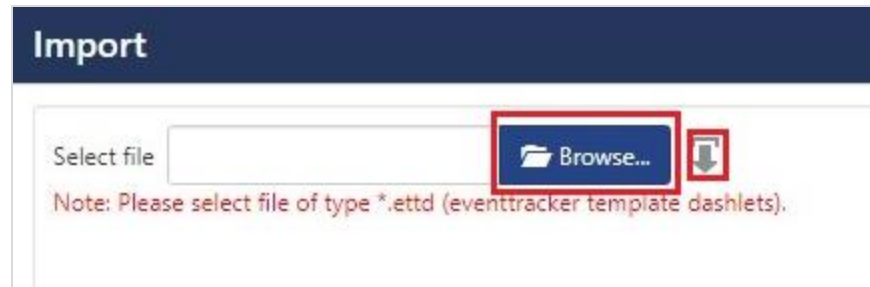


Figure 18

5. Click **OK**.

5.4 Knowledge Object

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

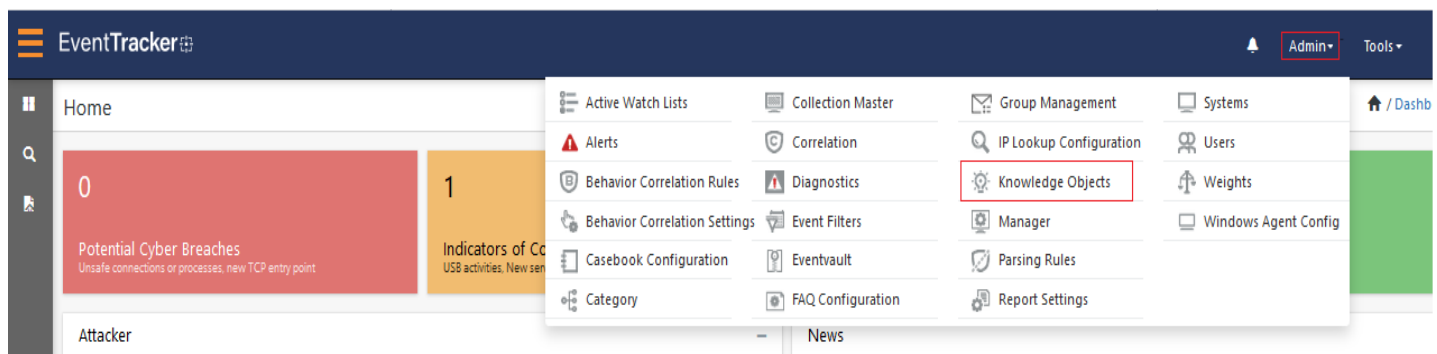


Figure 19

2. Click **Import** as highlighted in the below image:

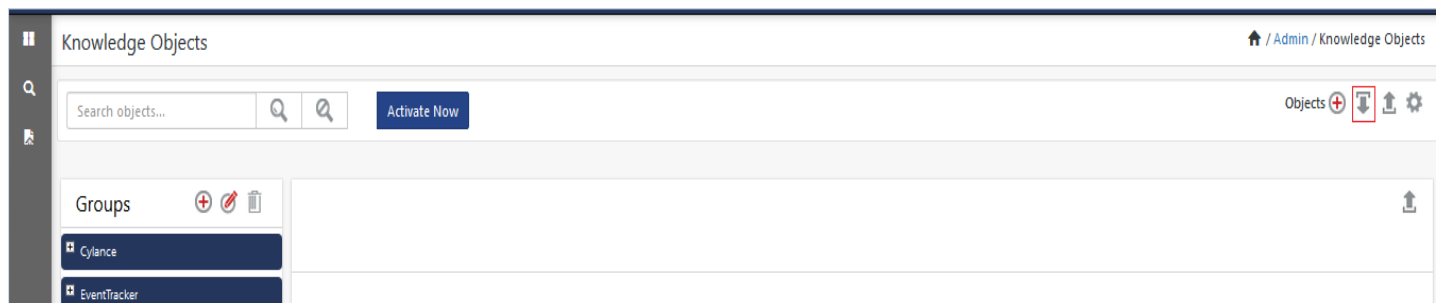


Figure 20

3. Click **Browse**.

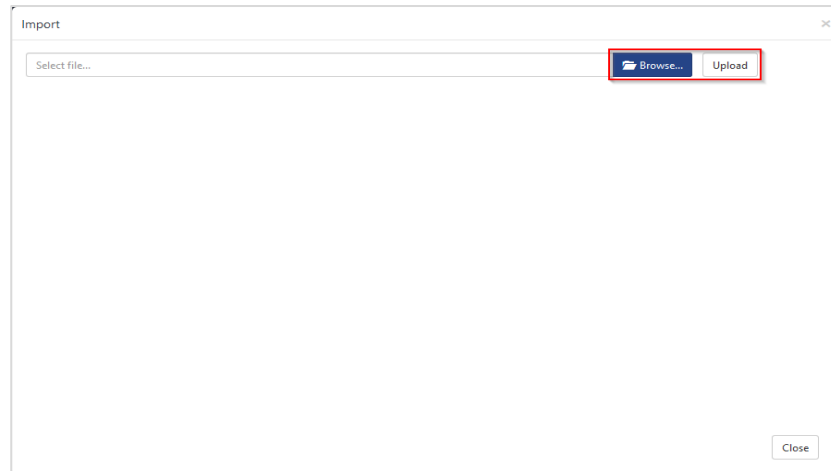



Figure 21

4. Locate the file named **KO_Azure MFA.etko**.
5. Now select the check box and then click  **Import**.

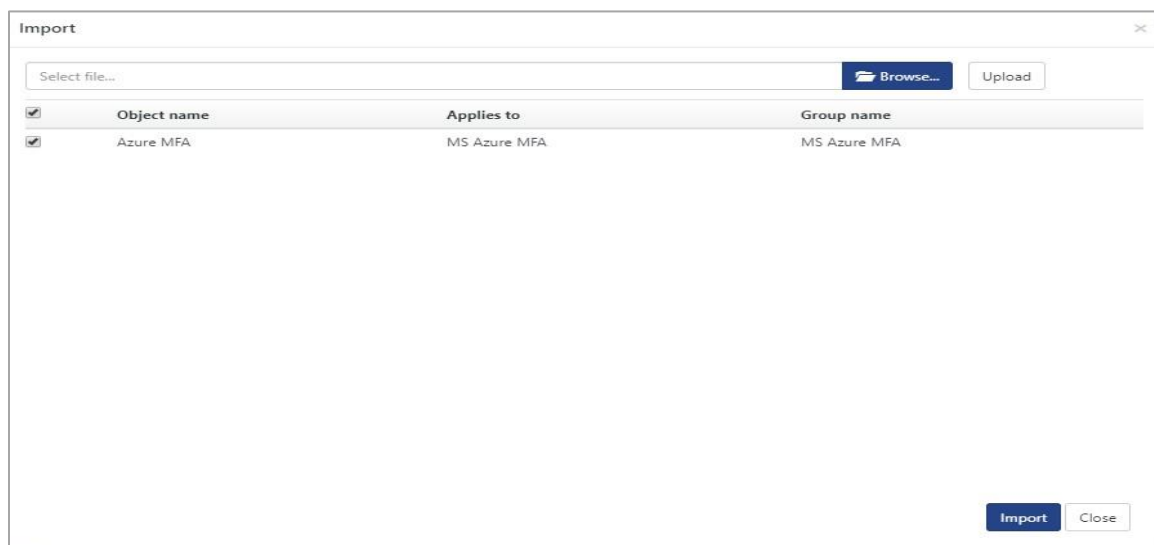


Figure 22

6. Knowledge objects are now imported successfully.

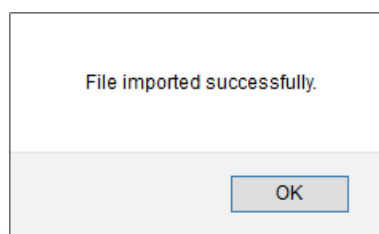


Figure 23

5.5 Report

1. Click **Reports** option and select **New (*.etcrx)** option.

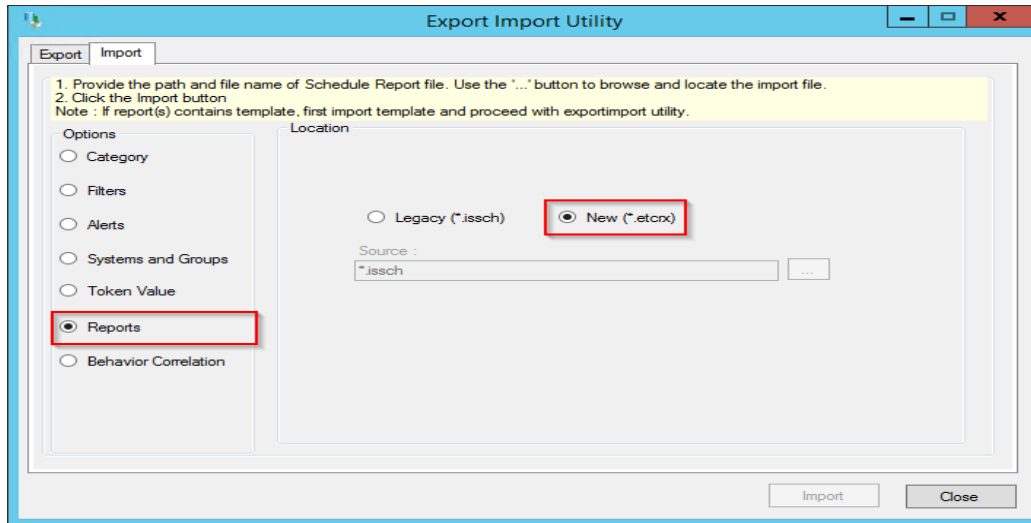


Figure 24

2. Locate the file named **Reports_Azure MFA.etcrx** and select the check box.

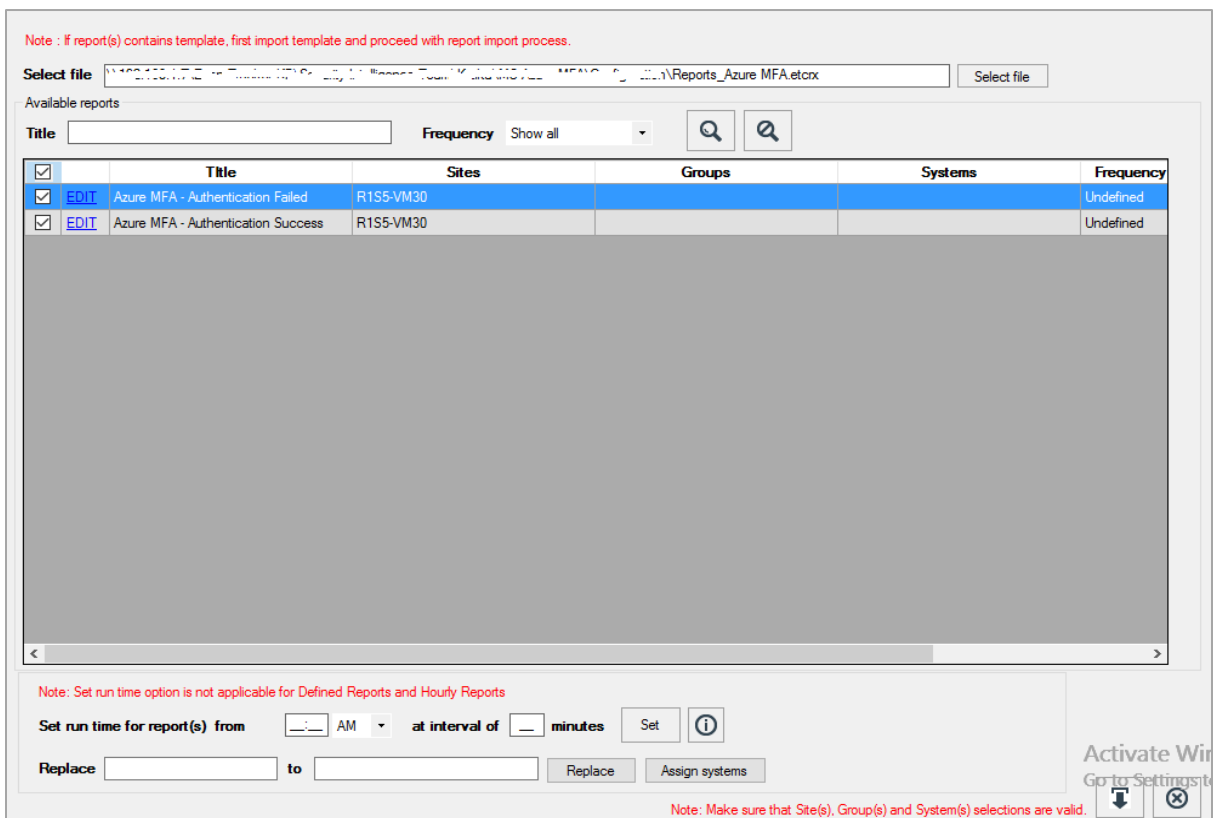



Figure 25

- Click **Import**  to import the report. EventTracker displays success message.

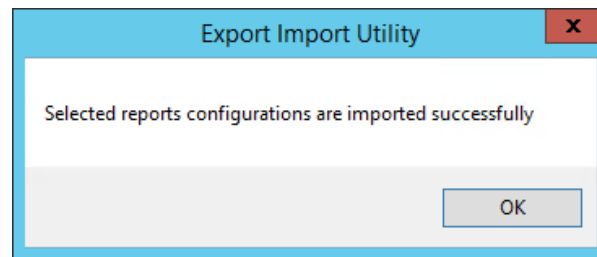


Figure 26

5.6 Dashboards

NOTE- Below steps given are specific to EventTracker 9 and later.

- Open **EventTracker** in browser and login.

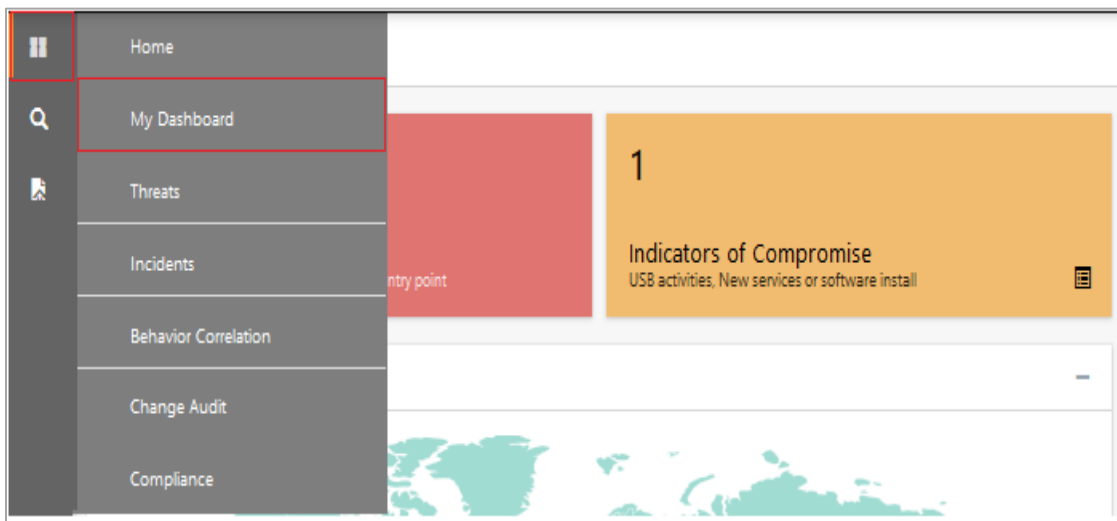


Figure 27


- Navigate to **My Dashboard** option as shown above.
- Click **Import**  as show below:



Figure 28

4. Import dashboard file **Dashboard_Azure MFA.etwd** and select **Select All** checkbox.
5. Click **Import** as shown below.

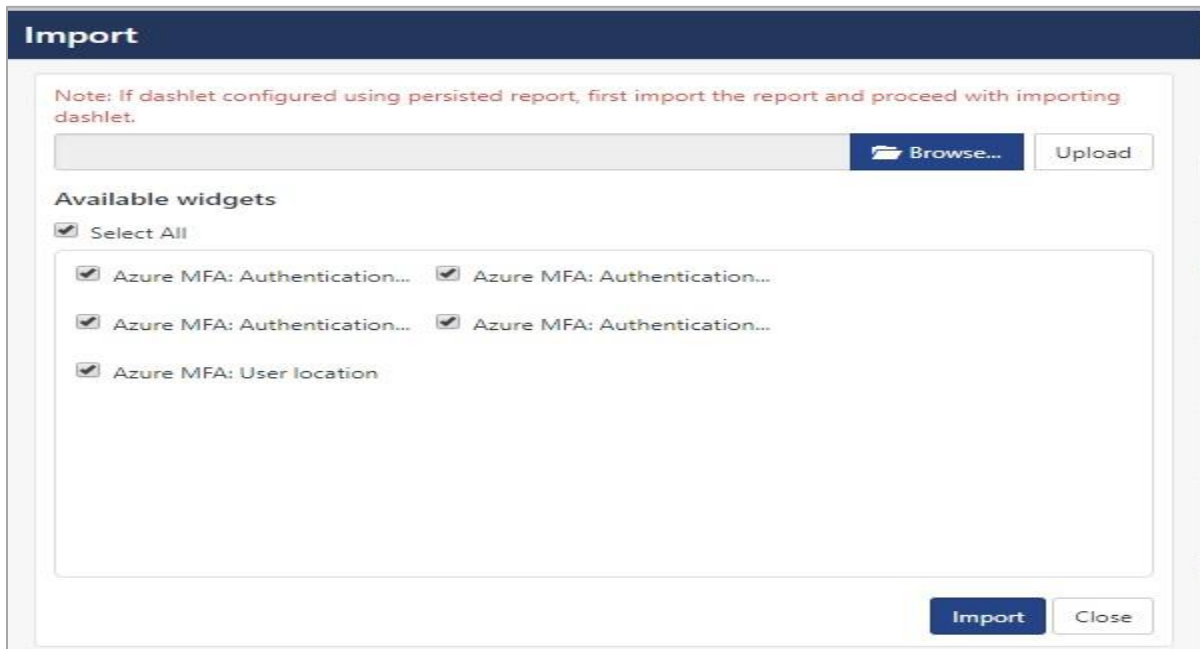


Figure 29

6. Import is now completed successfully.

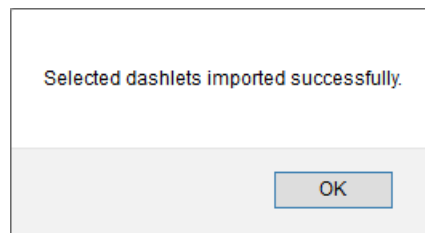



Figure 30

7. In **My Dashboard** page select  to add dashboard.

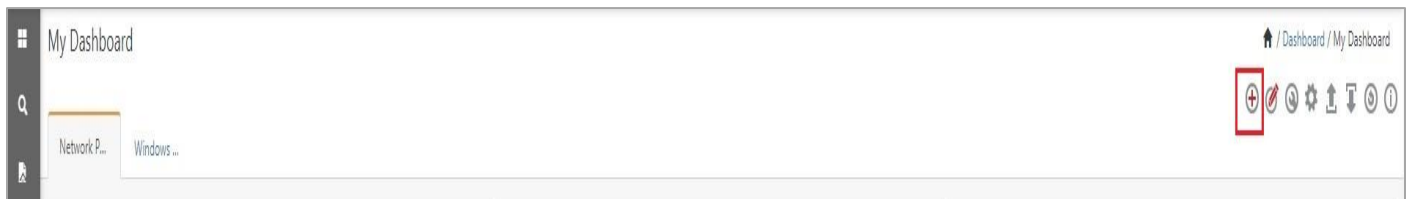




Figure 31

8. Choose appropriate name for **Title** and **Description**. Click **Save**.



The 'Edit Dashboard' dialog box has a dark blue header. It contains two text input fields: 'Title' with the value 'Azure MFA' and 'Description' with the value 'Microsoft Azure MFA'. At the bottom right are three buttons: 'Save' (dark blue), 'Delete' (light blue), and 'Cancel' (light blue).

Figure 32

9. In **My Dashboard** page select  to add dashlets.

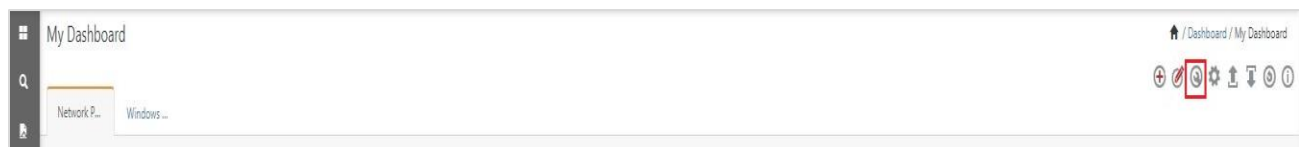
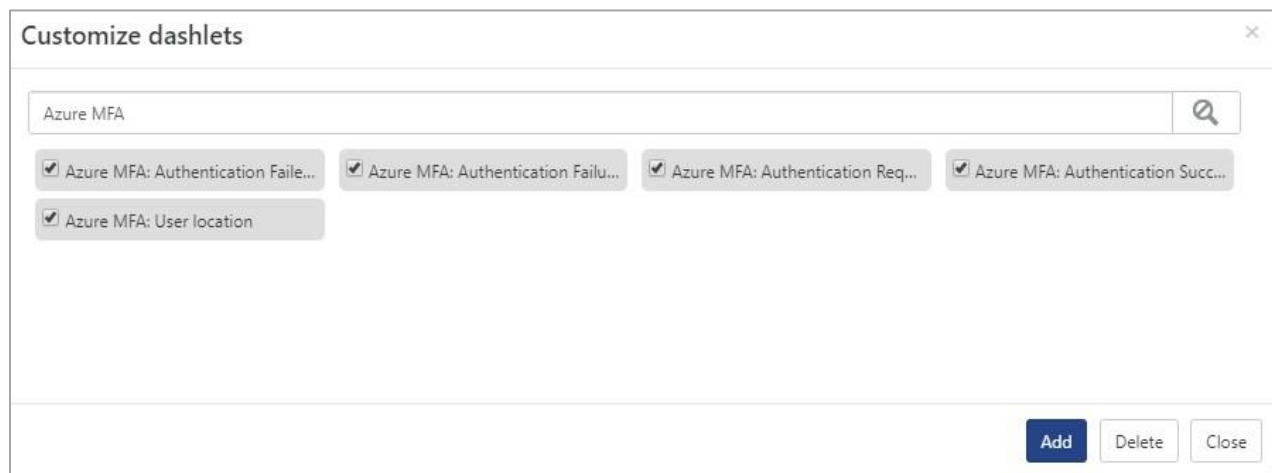


Figure 33

10. Select imported dashlets and click **Add**.



The 'Customize dashlets' dialog box has a search bar at the top containing 'Azure MFA'. Below the search bar are five dashlet tiles, each with a checked checkbox: 'Azure MFA: Authentication Failure...', 'Azure MFA: Authentication Failure...', 'Azure MFA: Authentication Required...', 'Azure MFA: Authentication Successful...', and 'Azure MFA: User location'. At the bottom right are three buttons: 'Add' (dark blue), 'Delete' (light blue), and 'Close' (light blue).

Figure 34

6. Verifying Azure MFA On-Premise knowledge pack in EventTracker

6.1 Category

1. Login to **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.

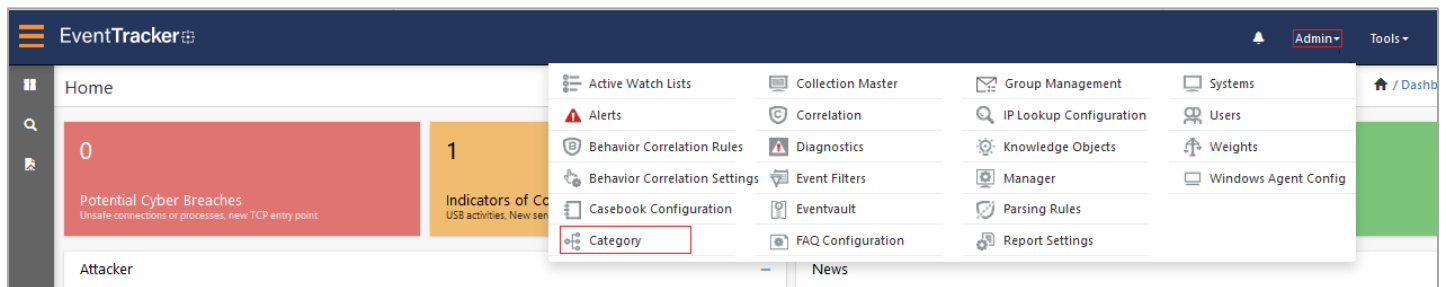


Figure 35

3. In **Category Tree** to view imported category, scroll down and expand **Azure MFA** group folder to view the imported category.

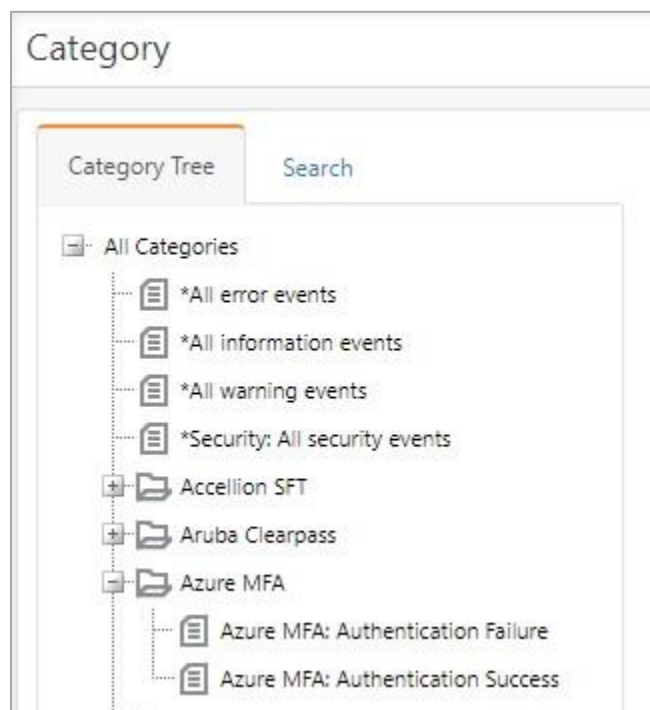


Figure 36

6.2 Alert

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

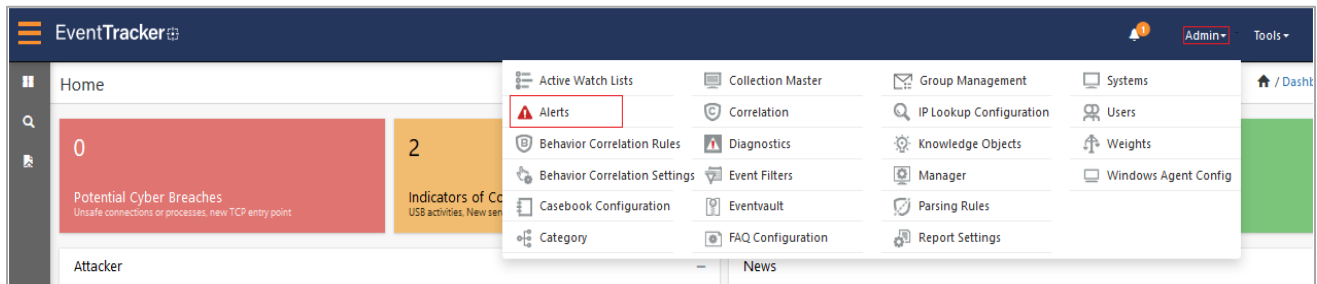


Figure 37

3. In the **Search** box, type '**Azure MFA**', and then click **Go**.
Alert Management page will display the imported alert.



	Alert Name ^	Threat	Active	Email
<input type="checkbox"/>	 Azure MFA: Authentication Failure		<input type="checkbox"/>	<input type="checkbox"/>

Figure 38

4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.

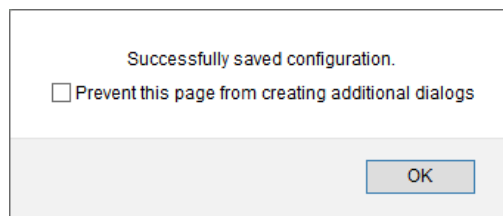


Figure 39

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

NOTE: Specify appropriate **system** in **alert configuration** for better performance.

6.3 Token templates

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

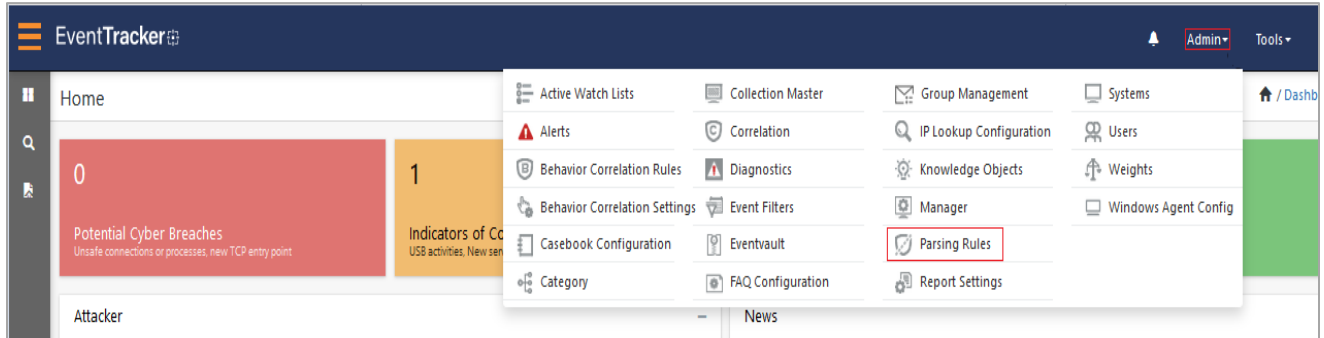


Figure 40

2. On **Template** tab, click on the **Azure MFA** group folder to view the imported token values.

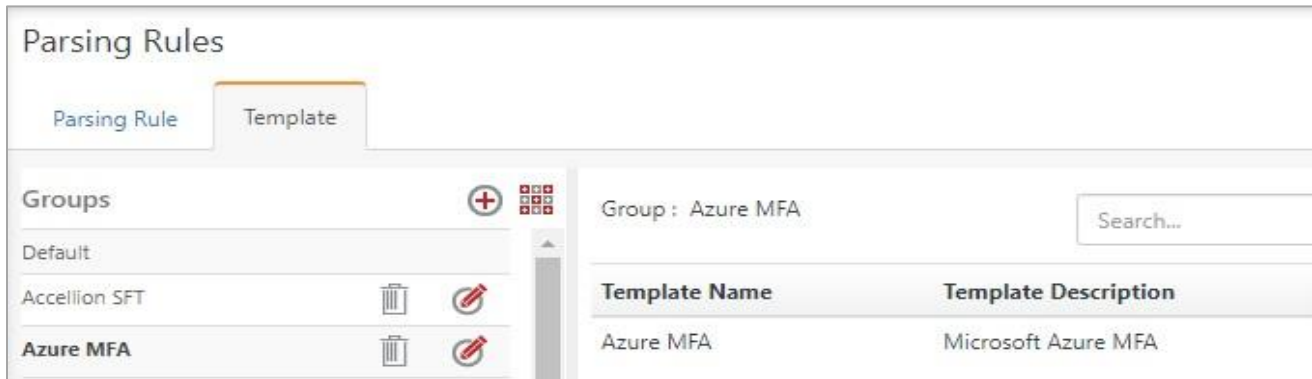


Figure 41

6.4 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects**.

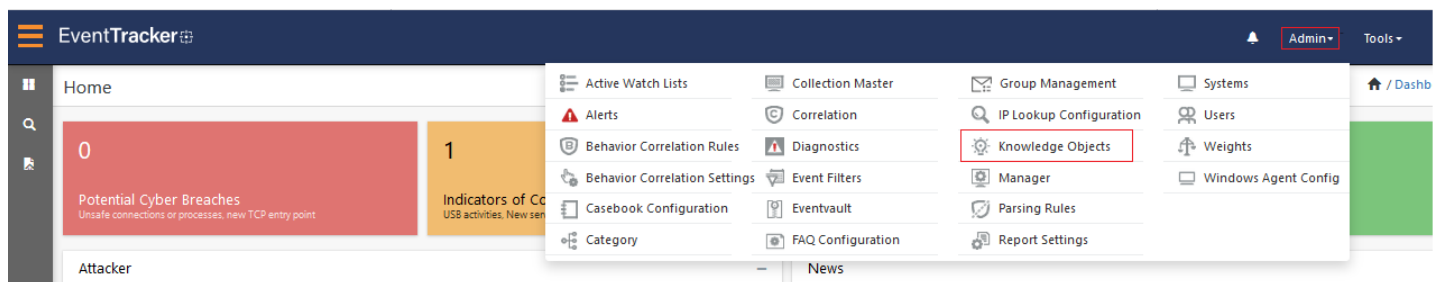


Figure 42

2. In the Knowledge Object tree, expand **Azure MFA** group folder to view the imported knowledge object.

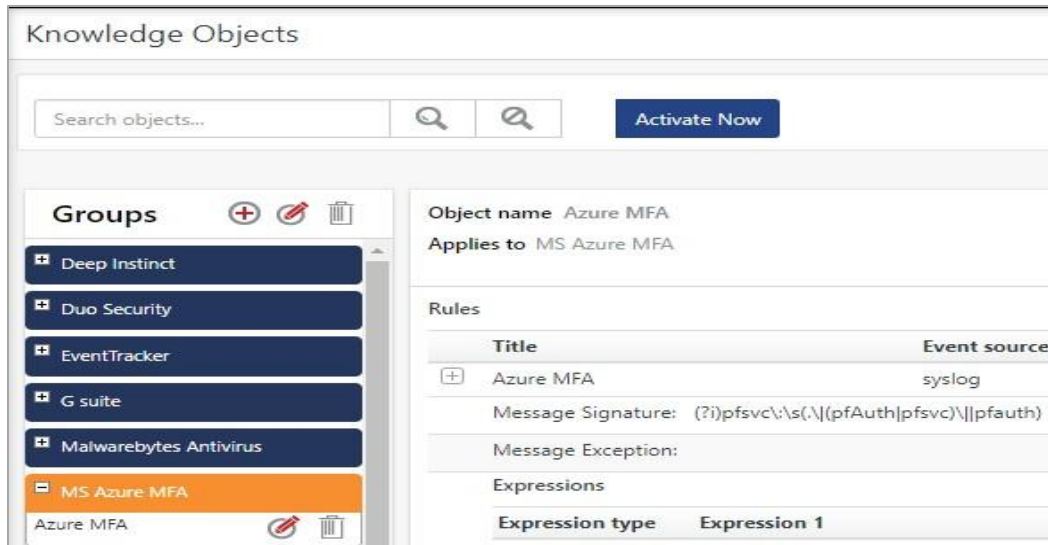


Figure 43

3. Click **Activate Now** to apply imported knowledge objects.

6.5 Report

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

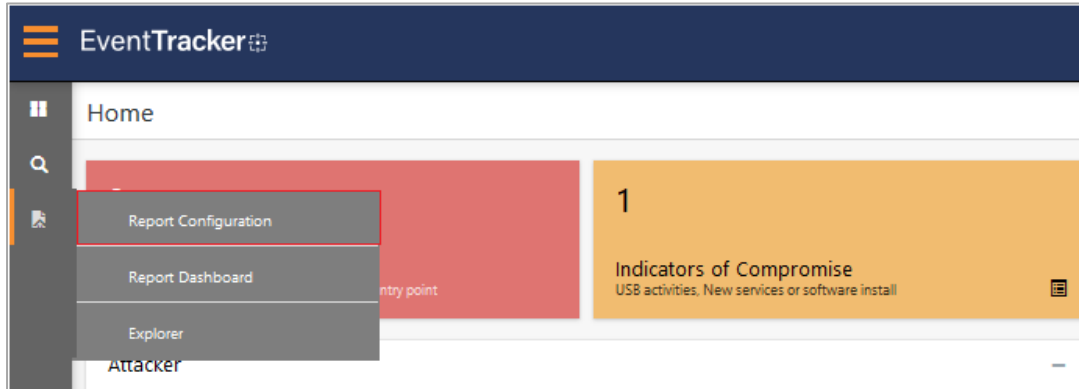


Figure 44

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

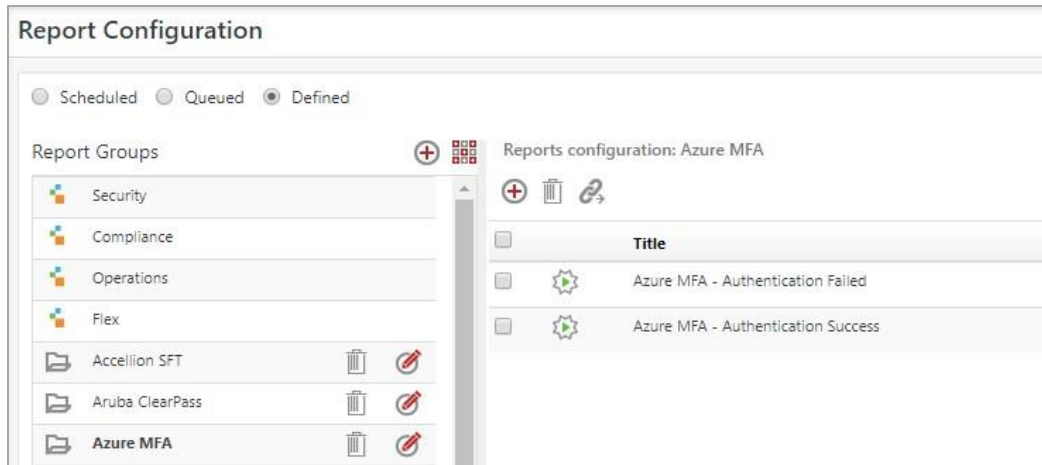


Figure 45

6.6 Dashboards

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

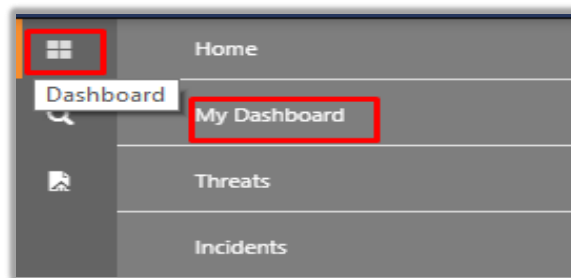


Figure 46

2. In the “**Azure MFA**” dashboard you should be now able to see something like this.

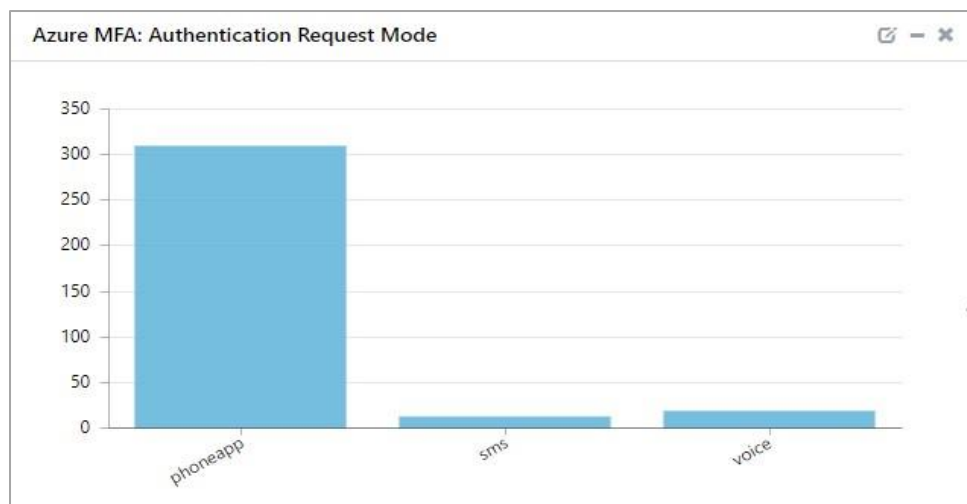


Figure 47