Integration Guide

Integrate Azure Data Factory with EventTracker

Publication Date:

September 26, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Azure Data Factory. The Knowledge Pack contains alerts, reports, dashboards, categories, and knowledge objects.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or later and Azure Data Factory.

Audience

This guide is for the administrators responsible for configuring the Knowledge Packs in EventTracker.

Table of Contents

1 Overview

Azure Data Factory is a cloud-based data integration service used to create data-driven workflows in the cloud for orchestrating and automating data movement and transformation. It also helps to monitor and manage workflows using both programmatic and UI mechanisms.

Netsurion facilitates monitoring events retrieved from the Azure Data Factory. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, benefit in tracking possible attacks, suspicious activities, or any other threat noticed.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Azure Data Factory to forward logs to EventTracker.

> **Note**
>
> Refer to How-To guide to configure Azure Data Factory to forward logs to EventTracker.

3 EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, configure the Knowledge Packs into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker.

3.1 Alerts

Azure Data Factory: Potential exfiltration detected: This alert is triggered when data transfer contains a large payload.

Azure Data Factory: Service interruption detected: This alert is triggered when a network is disrupted or if there is a DNS failure.

Azure Data Factory: Unauthorized access attempt: This alert is triggered when multiple attempts made to establish connection with data factory without proper credentials.

3.2 Category

Azure Data Factory - Activities summary: This category of the saved search allows you to parse events that are specific to the pipeline activities for Azure Data Factory.

Azure Data Factory - SSIS integration runtime summary: This category of the saved search allows you to parse events that are specific to the SQL server integration service activities for Azure Data Factory.

3.3 Reports

Azure Data Factory - Activities summary: This report provides a detailed summary of pipeline activities in Azure Data Factory. The report includes the activity type, data source, destination, error type, error message, and more.

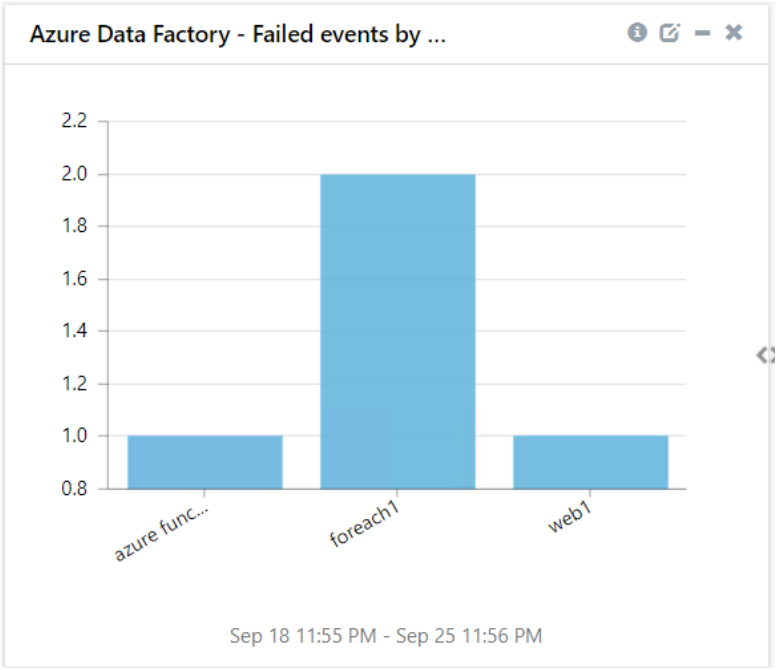
LogTime	Client IP	Host	User Agent	InstanceID	Http Method	Http Version	Client Port	Http Status
06-22-2022 05:05:33 AM	10.207.204.44	vgw098	Mozilla\/5.0 (Windows NT 6.1; WOW6	appgw_2	PUT	HTTP\/1.1	51886	404
06-22-2022 05:05:34 AM	10.2.2.13	appgw009	NetSystemsResearch studies the avai	appgw_5	DELETE	HTTP/1.1	37408	200
06-22-2022 05:05:34 AM	10.20.2.139	vgw098	Mozilla\/5.0 (Windows NT 6.1; WOW6	appgw_4	PUT	HTTP\/1.1	51886	404
06-22-2022 05:05:34 AM	10.2.56.36	appgw009	NetSystemsResearch studies the avai	appgw_3	DELETE	HTTP/1.1	37408	200
06-22-2022 05:05:35 AM	192.168.155.102	vgw098	Mozilla\/5.0 (Windows NT 6.1; WOW6	appgw_13	PUT	HTTP\/1.1	51886	404
06-22-2022 05:05:35 AM	10.55.53.144	10.55.53.144	Mozilla/5.0+(Windows+NT+10.0;+Win	ApplicationGatewayRole_	DELETE	HTTP/1.1	37408	200
06-22-2022 05:05:35 AM	192.168.162.27		NetSystemsResearch studies the avai	appgw_25	POST	HTTP\/1.1	60929	402
06-22-2022 05:05:35 AM	192.168.161.37	appgw009	NetSystemsResearch studies the avai	appgw_1	GET	HTTP\/1.1	60929	502

Azure Data Factory – SSIS integration runtime summary: This report provides a detailed summary of SQL server integration services runtime activities in Azure Data Factory. The report includes the source component, destination component, package name, package path. and more.

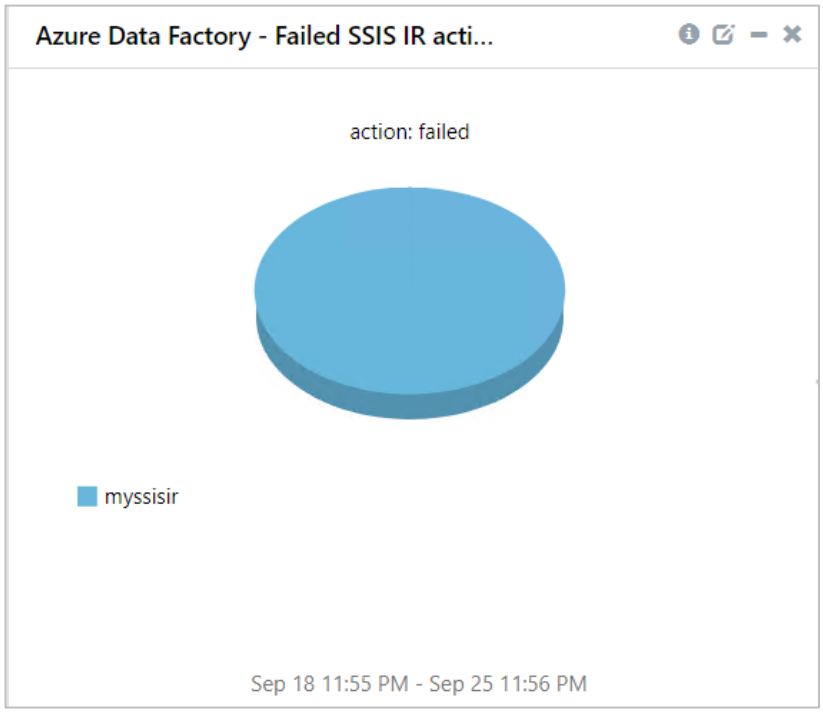
LogTime	TransactionId	Client IP	Client Port	Hostname	Requested URI	Requested Query	RuleID	Rule Type	Rule Version	Message
06-22-2022 05:05:35 AM	0a830da0e1da0d5f6b268deb0bce3152	192.168.155.102	51886	vm000003	\/	AzureApplicationGateway-CACHE-HIT	942150	OWASP_CRS	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:35 AM	16861477007022634343	10.55.53.144	37408	vm000004	/\	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:35 AM	c6d4051cd01960334279f645b2a6be1b	192.168.162.27	60929	vm000003	\/	AzureApplicationGateway-CACHE-HIT	942150	OWASP_CRS	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:35 AM	c6d4051cd01960334279f645b2a6be1b	192.168.161.37	60929	vm000004	\/	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:35 AM	AcAcAcAcAKH@AcAcAcAcAyAt	31.58.237.148	17270	vm000003	/	AzureApplicationGateway-CACHE-HIT	942150	OWASP_CRS	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:36 AM	AcAcAcAcAKH@AcAcAcAcAyAt	192.168.248.32	59338	vm000004	/	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	SQL Injection Attack: SQL Tautology Detected
06-22-2022 05:05:36 AM	0a830da0e1da0d5f6b268deb0bce3152	10.14.248.32	59338	vm0002	/	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3	Host header is a numeric IP address
06-22-2022 05:05:37 AM	16861477007022634343	10.168.10.147	"0"	127.0.0.1	/	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	Host header is a numeric IP address
06-22-2022 05:05:37 AM	16861477007022634343	10.161.109.147	"0"	127.0.0.1	/	AzureApplicationGateway-CACHE-HIT	920350	OWASP	3.0	Host header is a numeric IP address

3.4 Dashboard

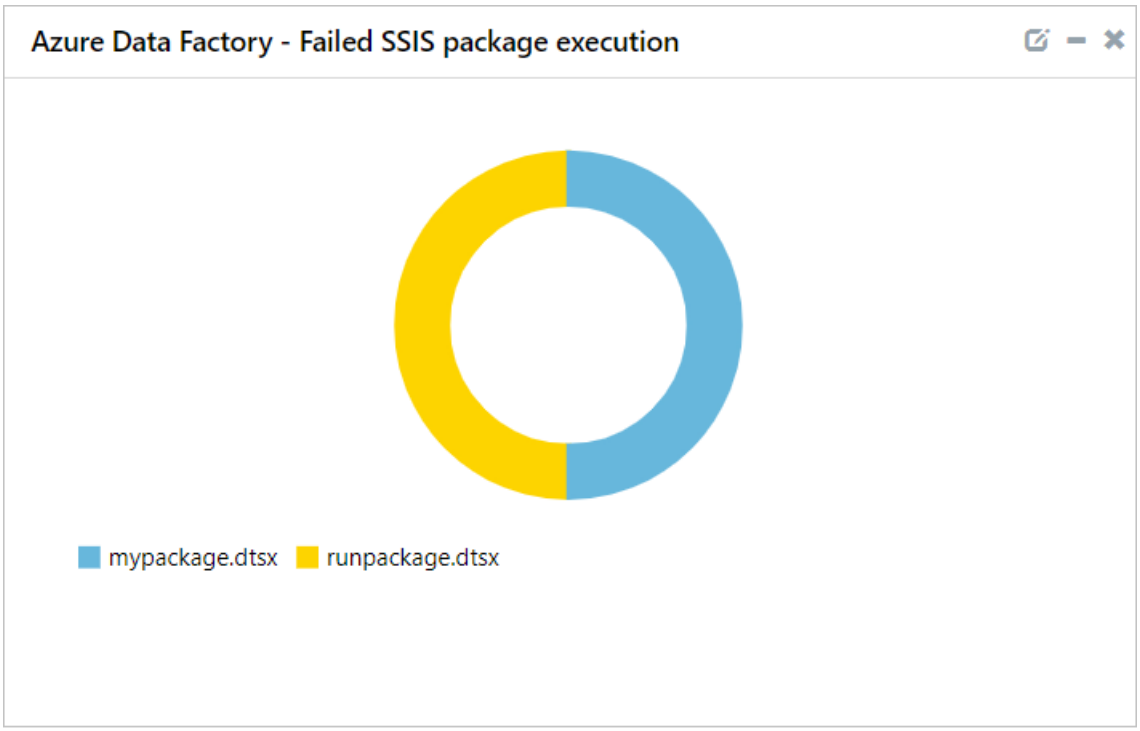
Azure Data Factory - Failed events by activities: This dashlet displays the failed activities of the request made to access the data factory.



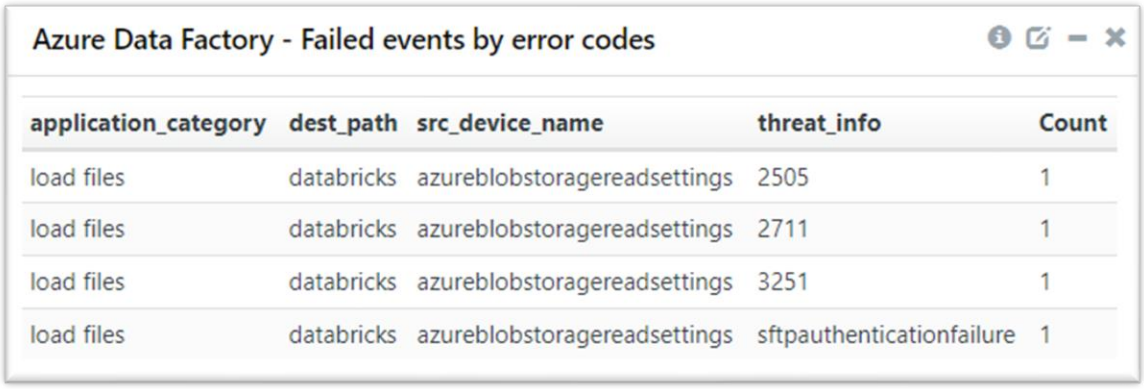
Azure Data Factory - Failed SSIS IR activities: This dashlet displays the failed activities made to data factory.



Azure Data Factory - Failed SSIS package execution: This dashlet displays the failed package execution in SQL server integration services.



Azure Data Factory - Failed events by error codes: This dashlet displays the error codes of the failed events along with data source and destination.



Azure Data Factory - Failed events by error codes

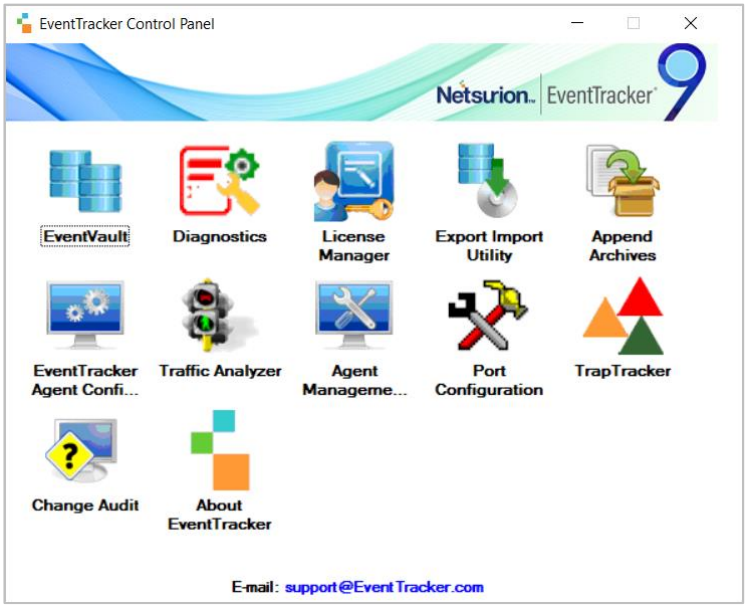
application_category	dest_path	src_device_name	threat_info	Count
load files	databricks	azureblobstoragereadsettings	2505	1
load files	databricks	azureblobstoragereadsettings	2711	1
load files	databricks	azureblobstoragereadsettings	3251	1
load files	databricks	azureblobstoragereadsettings	sftpauthenticationfailure	1

4 Importing Azure Data Factory Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

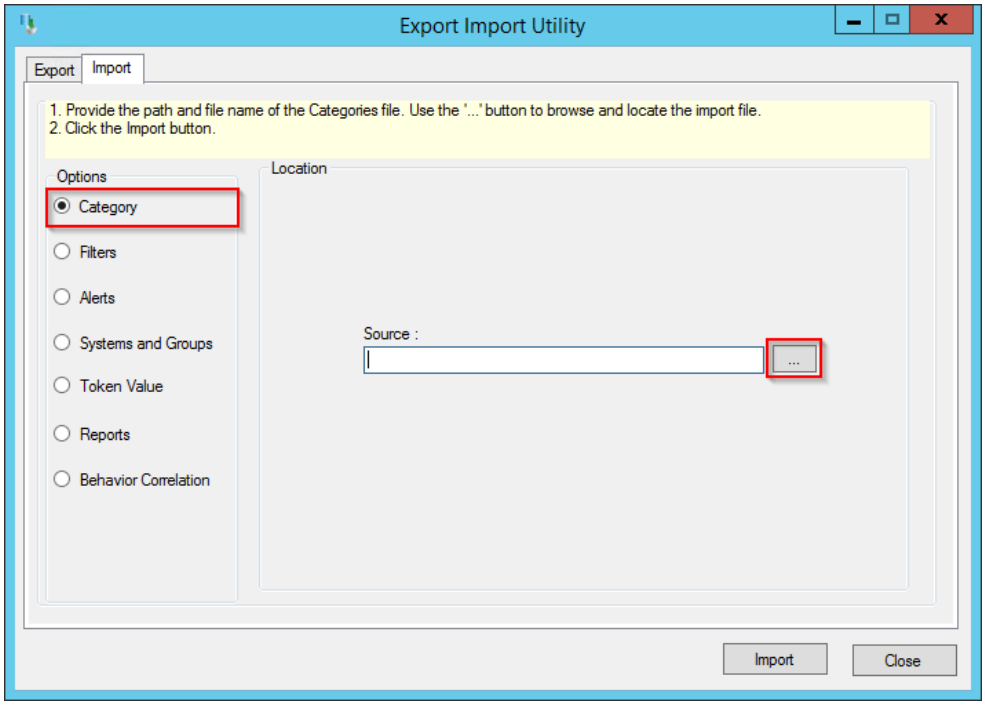
- Categories
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards

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

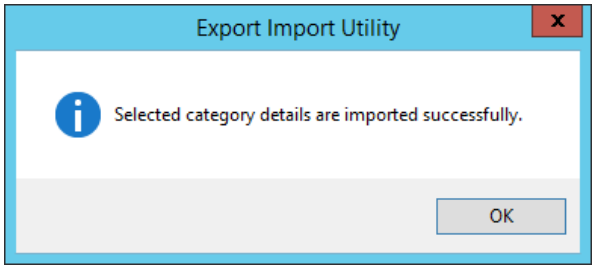


4.1 Category

1. In the **Import** tab, click **Category**, and then click the **Browse** button to locate the file.



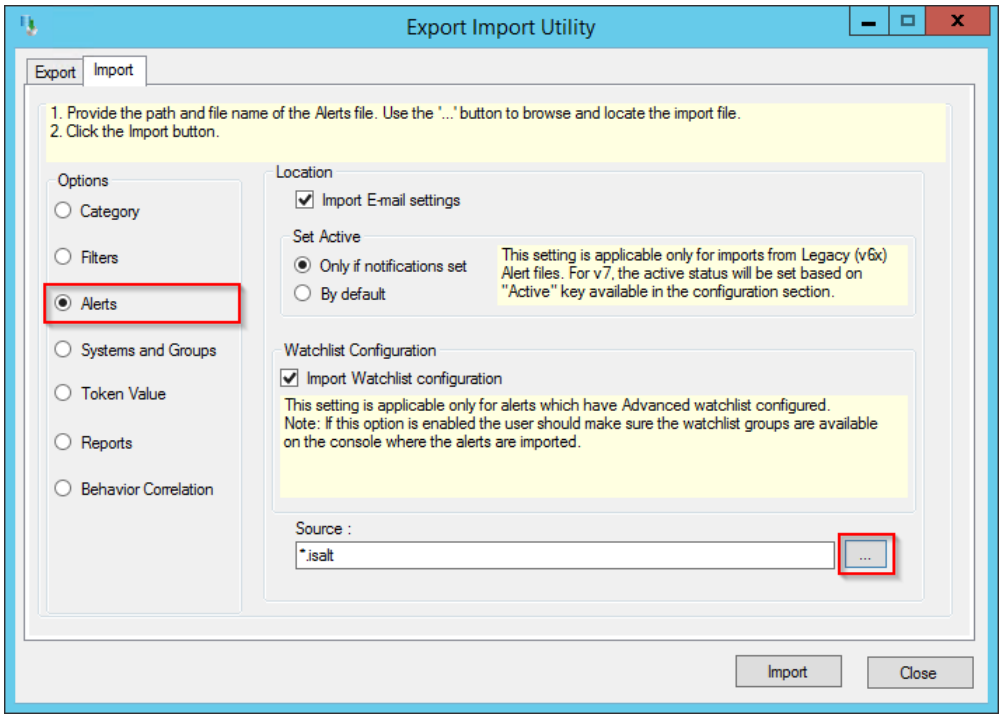
2. In the **Browse** window, locate the **Categories_Azure Data Factory.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



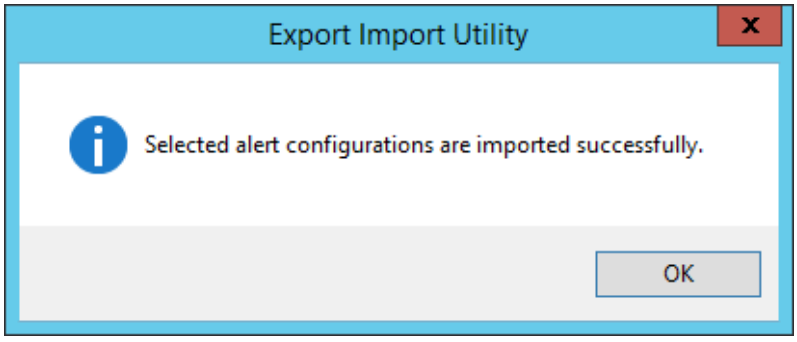
5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

1. In the **Import** tab, click **Alerts**, and then click the **Browse** button to locate the file.



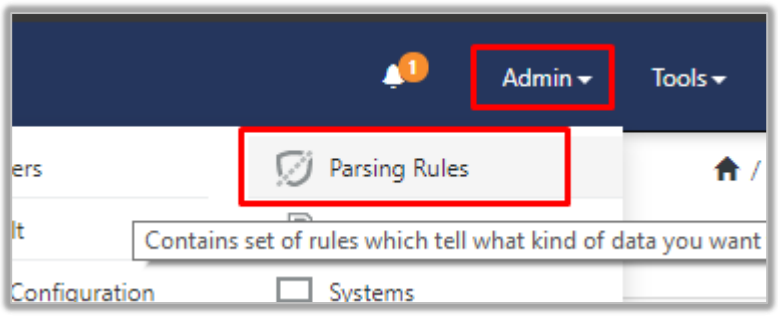
2. In the **Browse** window, locate the **Alerts_ Azure Data Factory.isalt** file, and then click **Open** button.
3. To import the alerts, click the **Import** button.
4. EventTracker displays a success message on successfully importing the selected file in **Alerts**.



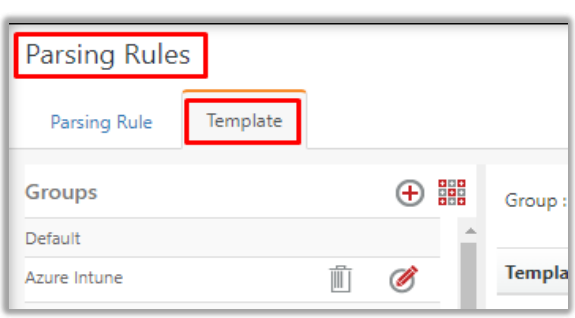
5. Click **OK** or the **Close** button to complete the process.

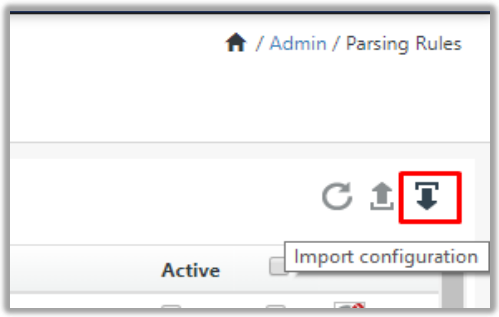
4.3 Token Template

1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Parsing Rules**.



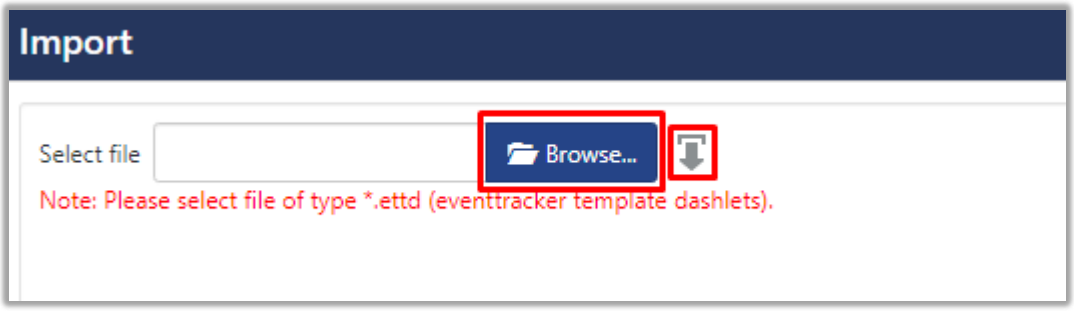
2. In the **Parsing Rules** interface, click the **Template** tab and then click **Import Configuration**.



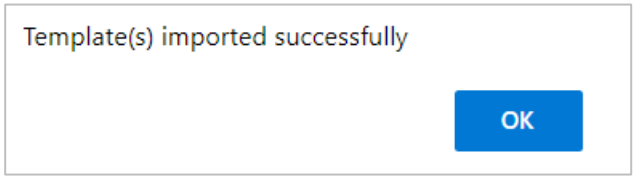


3. In the **Import** window, click **Browse** to search and locate for the file name with **".ettd"** extension (example, **Templates_Azure Data Factory.ettd**).

4. It takes few seconds to load the templates and once you see the list of templates, click the appropriate templates, and click **Import**.

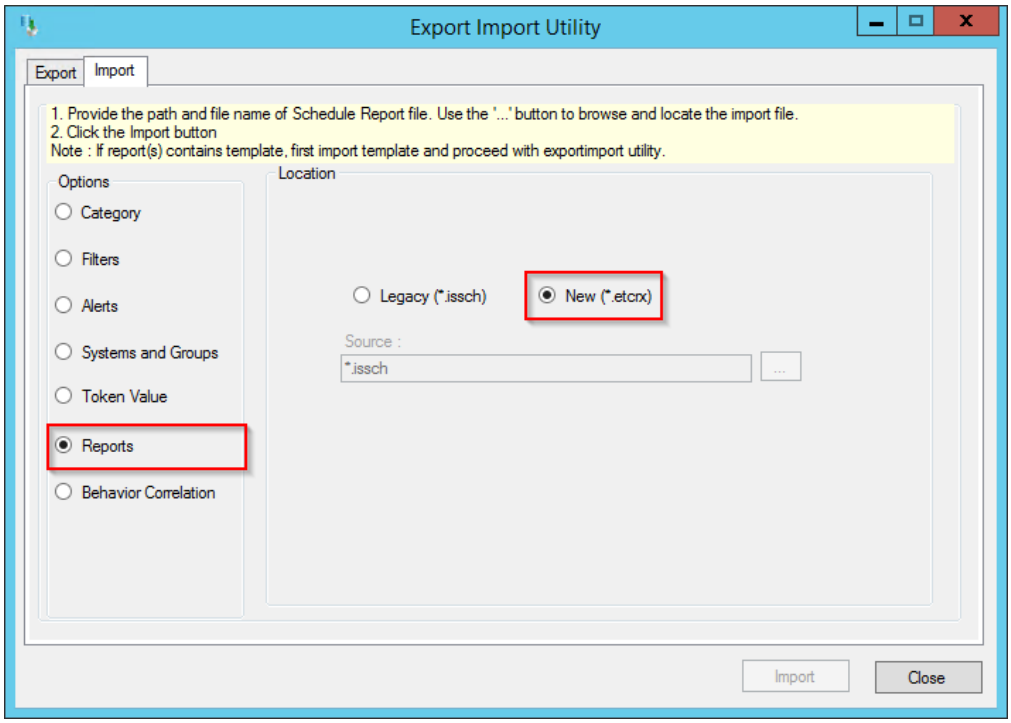


5. EventTracker displays a success message on successfully importing the selected file in **Template**.

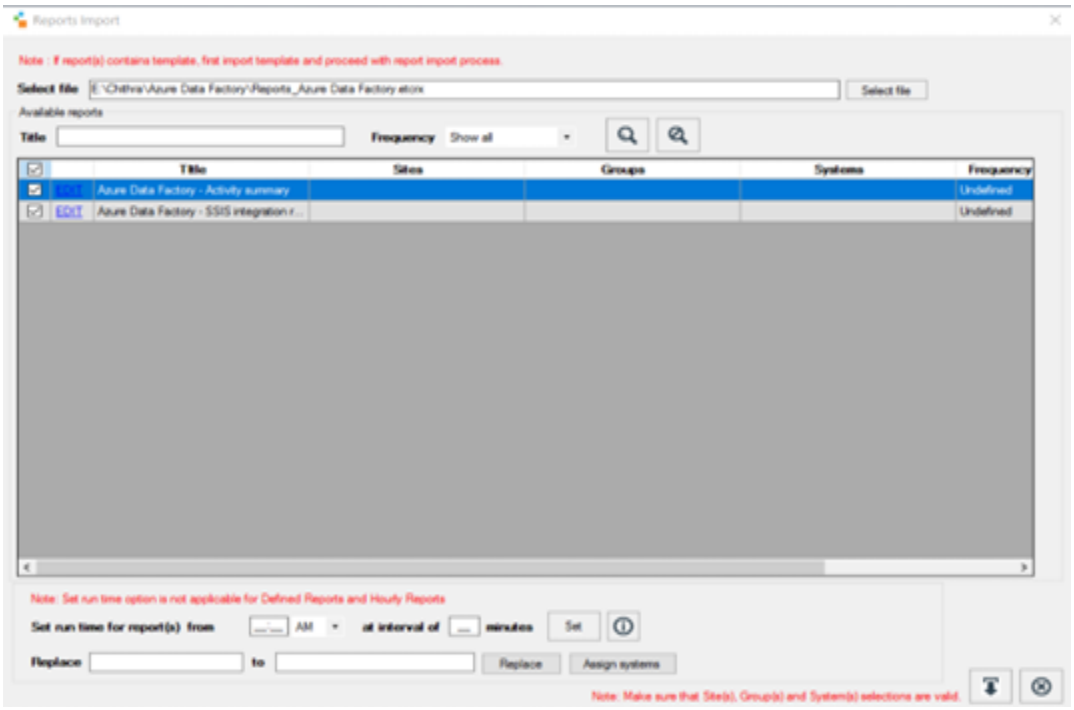


4.4 Reports

1. In the **Import** tab, click **Reports** and then click **New (*.etcrx)**.

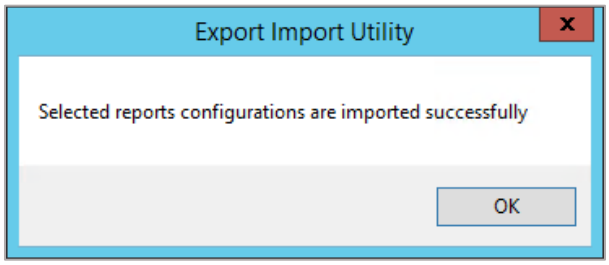


2. In the **Reports Import** window, click **Select file** to locate **Reports_Azure Data Factory.etcrx** file.



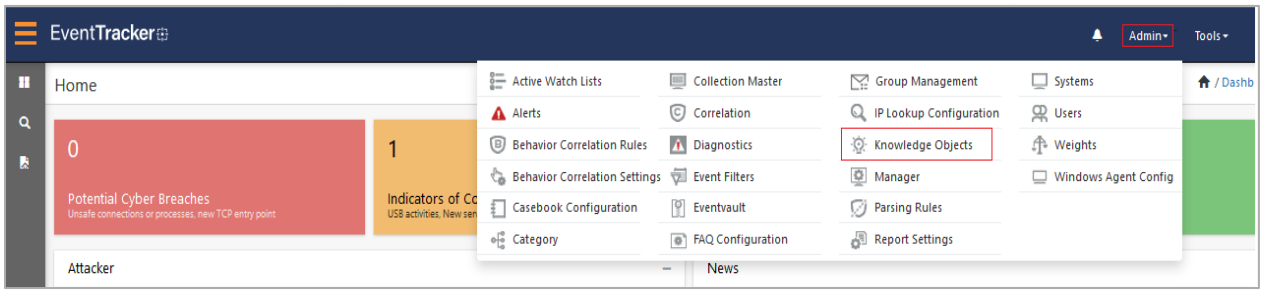
3. Select the check box of all the files and click the **Import** button to import the selected files.

4. EventTracker displays a success message on successful importing of the selected file in **Reports**.

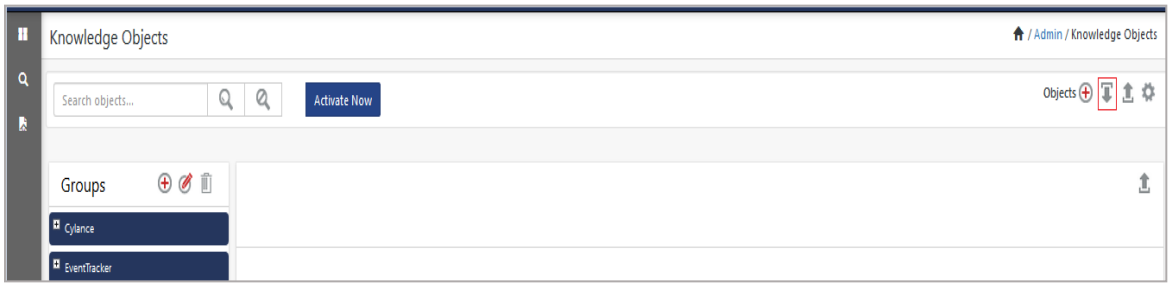


4.5 Knowledge Objects (KO)

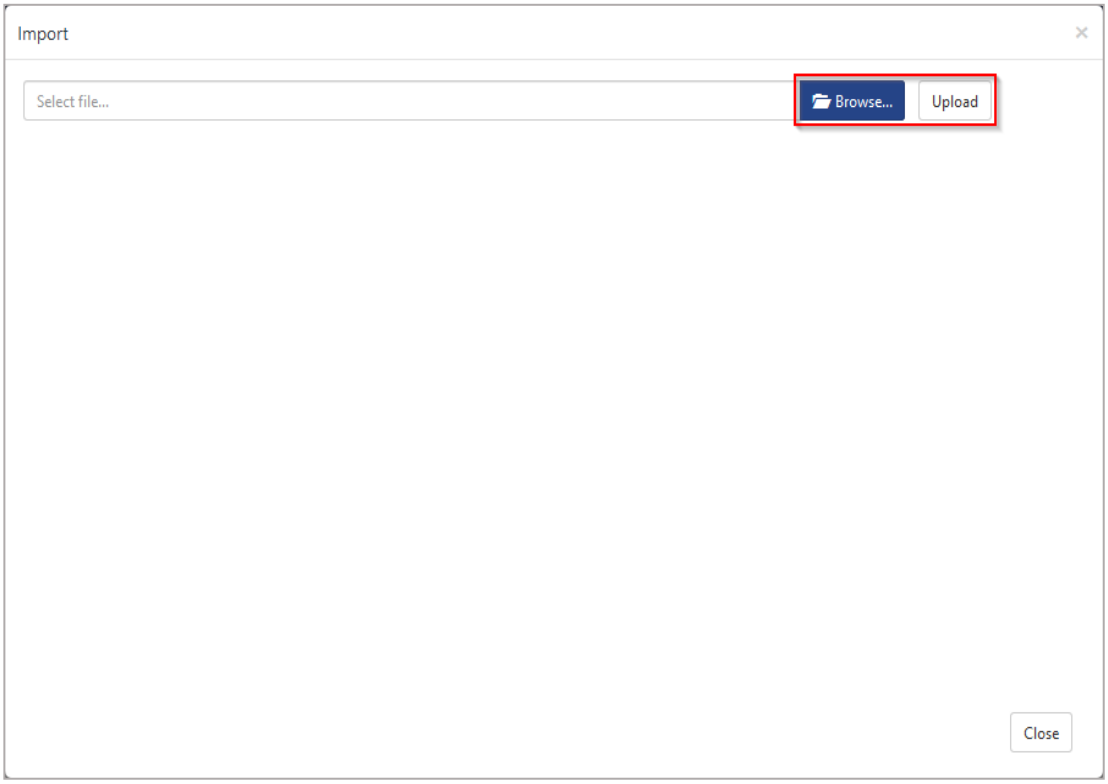
1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.



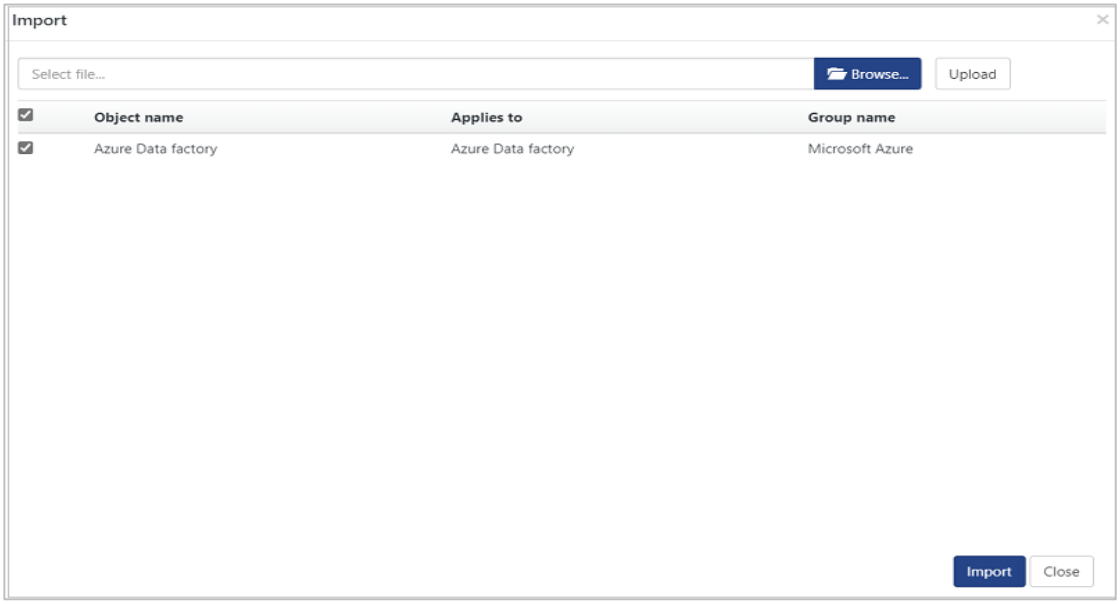
2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.



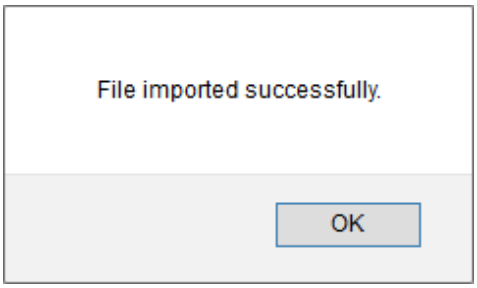
3. In the **Import** window, click **Browse** and locate the **KO_ Azure Data Factory.etko** file.



4. Select the check box next to the browsed KO file and then click the **Import** button.



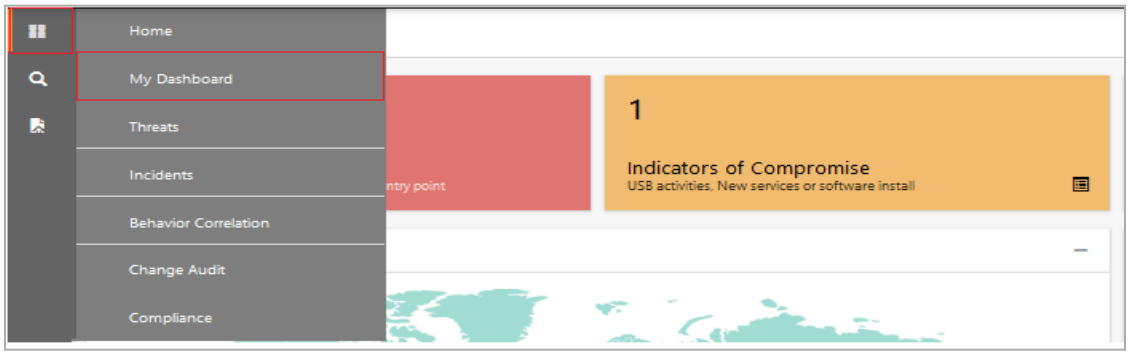
5. EventTracker displays a successful message on successfully importing the selected file in **Knowledge Objects**.



6. Click **OK** or the **Close** button to complete the process.

4.6 Dashboard

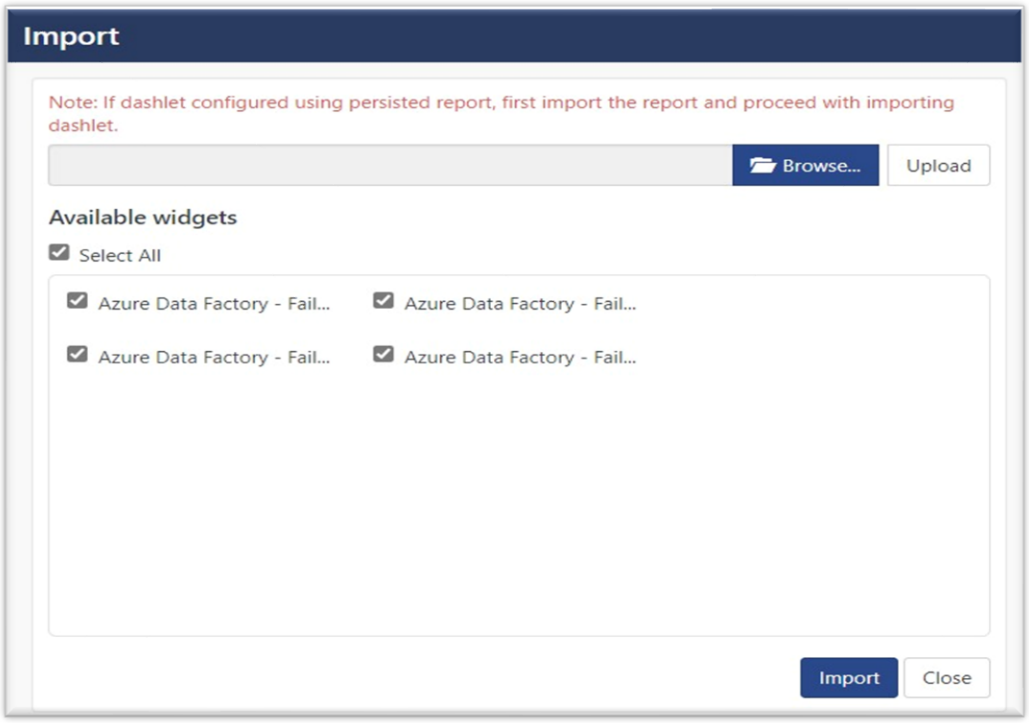
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



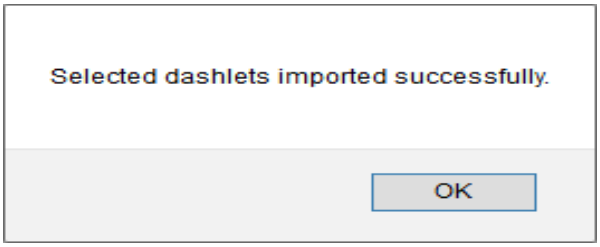
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_ Azure Data Factory.etwd** file and then click **Upload.**

4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

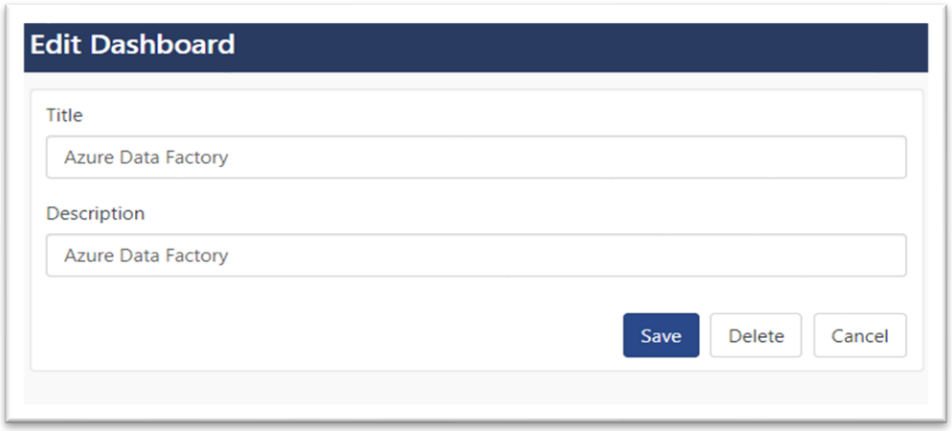


5. The EventTracker displays the success message on successful import of the dashlet files.

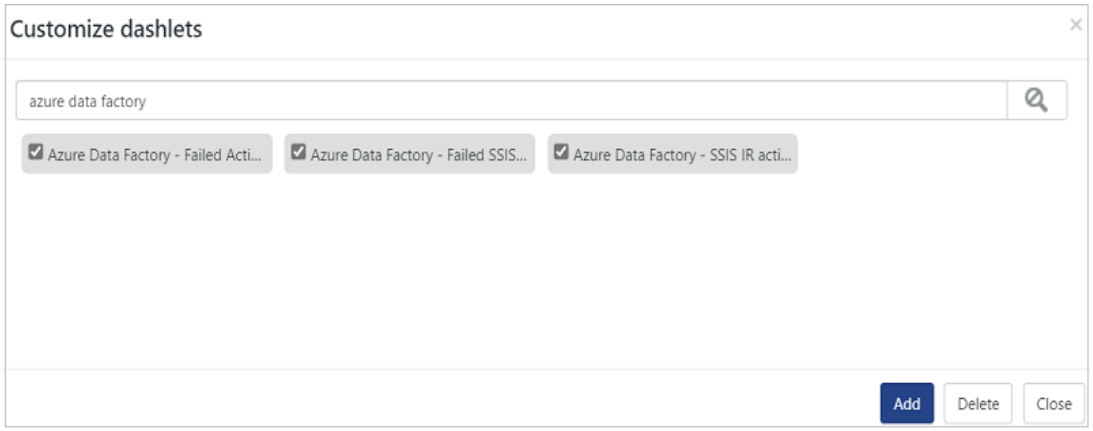


6. Then, in the **My Dashboard** interface click on the Add ⊕ button to add dashboard.

7. In the **Add Dashboard** interface, specify the **Title** and **Description** and click **Save**.



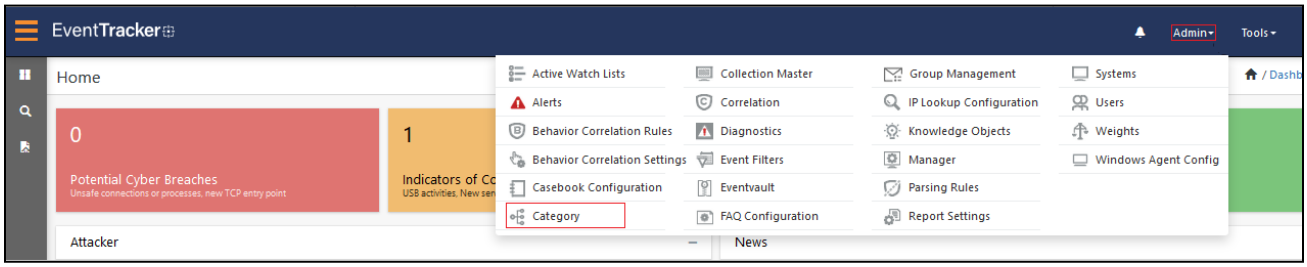
8. From the newly created dashboard interface (for example, **Azure Data Factory**), click the **Configuration** button to add the Azure Data Factory dashlets.
9. Search and select the newly imported dashlets and click **Add**.



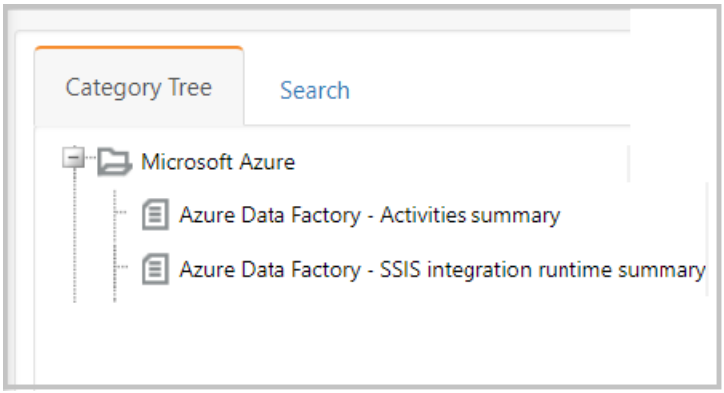
5 Verifying Azure Data Factory Knowledge Packs in EventTracker

5.1 Category

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Category**.

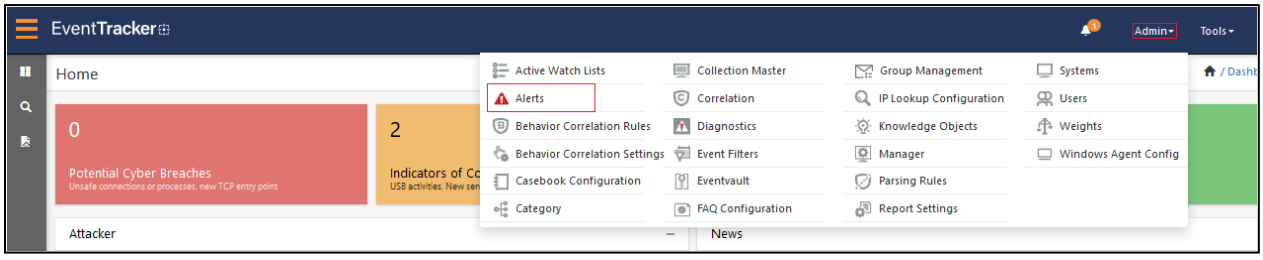


2. In the **Category** interface, under the **Category Tree** tab, click the **Microsoft Azure** group folder to expand and see the imported categories.



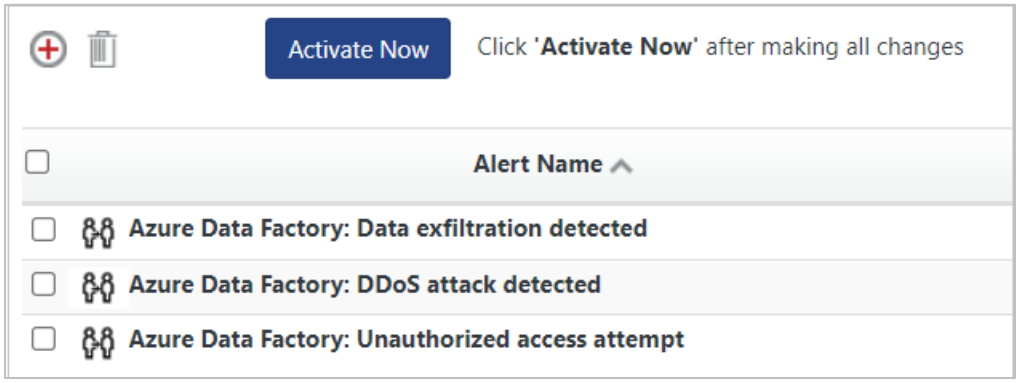
5.2 Alerts

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Alerts**.

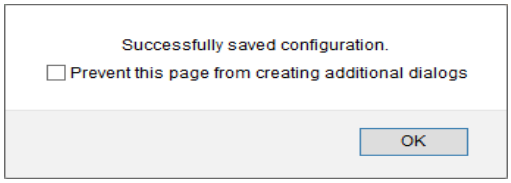


2. In the **Alerts** interface, type **Azure Data Factory** in the **Search** field and click the **Search** button.

3. The **Alerts** interface will display all the imported **Azure Data Factory** alerts.



4. To activate the imported alert, toggle the **Active** button, which is available next to the respective alert name.
5. EventTracker displays a success message on successfully configuring the alerts.



6. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

Note

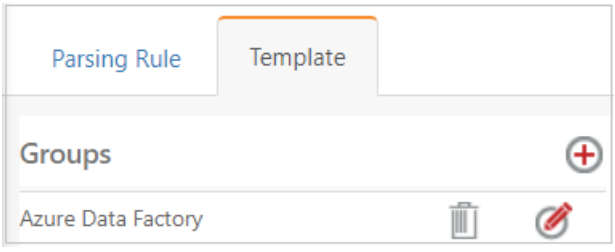
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

In the **Alert Configuration** interface, specify the appropriate **System** for better performance.

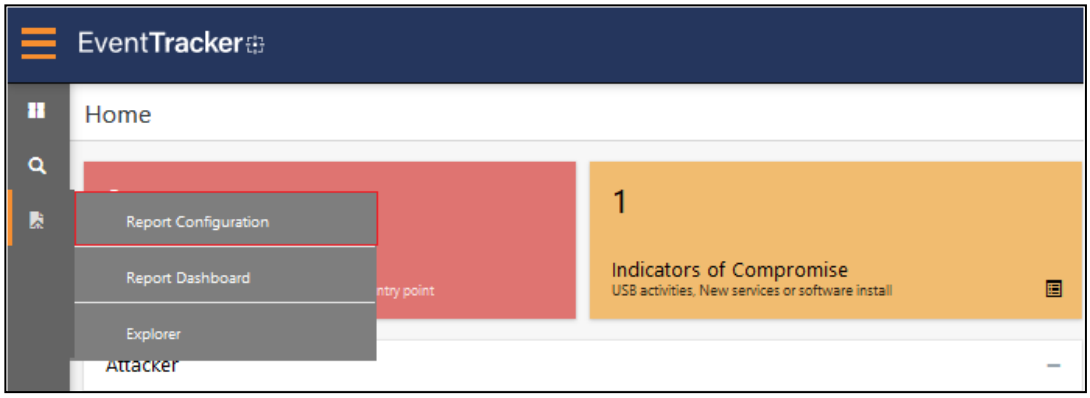
5.3 Token Template

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Parsing Rules.**
2. Go to the **Template** tab and click the **Azure Data Factory** group folder to view the imported Token template.

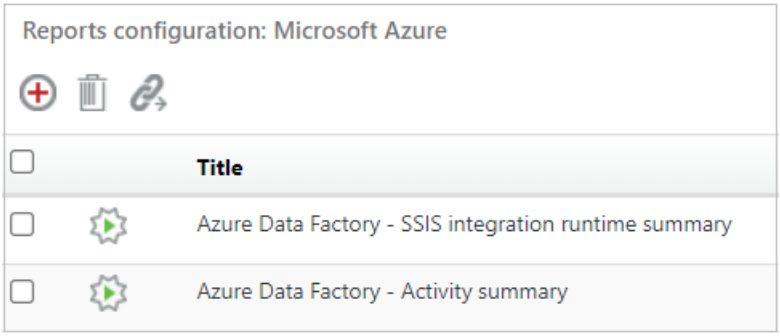


5.4 Reports

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

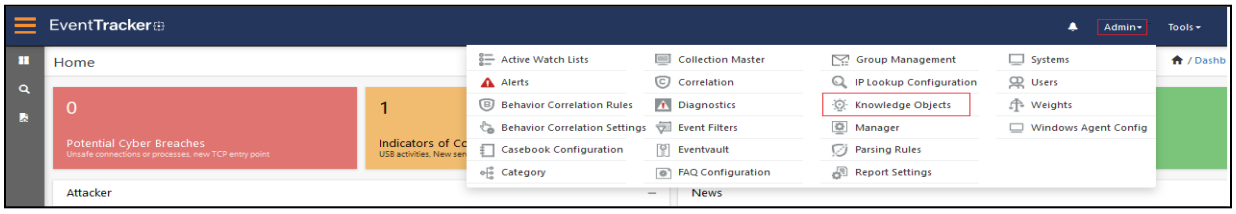


2. In the **Reports Configuration** interface, select the **Defined** option.
3. In the search field, type **Microsoft Azure** and click **Search** to search for the Azure Data Factory files.
4. EventTracker displays the reports for Azure Data Factory.

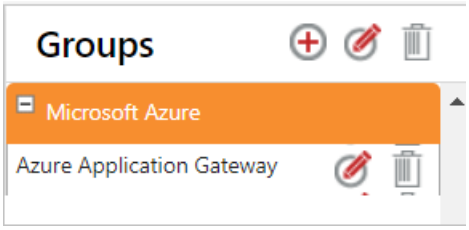


5.5 Knowledge Objects (KO)

1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Knowledge Objects.**



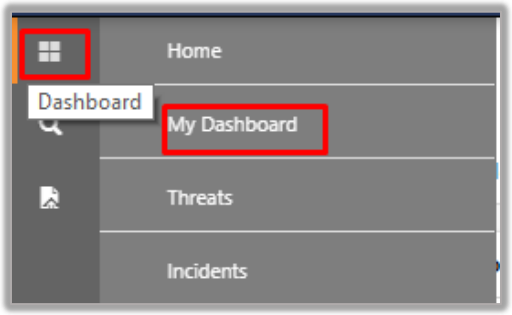
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Microsoft Azure** group to expand and view the imported Knowledge objects.



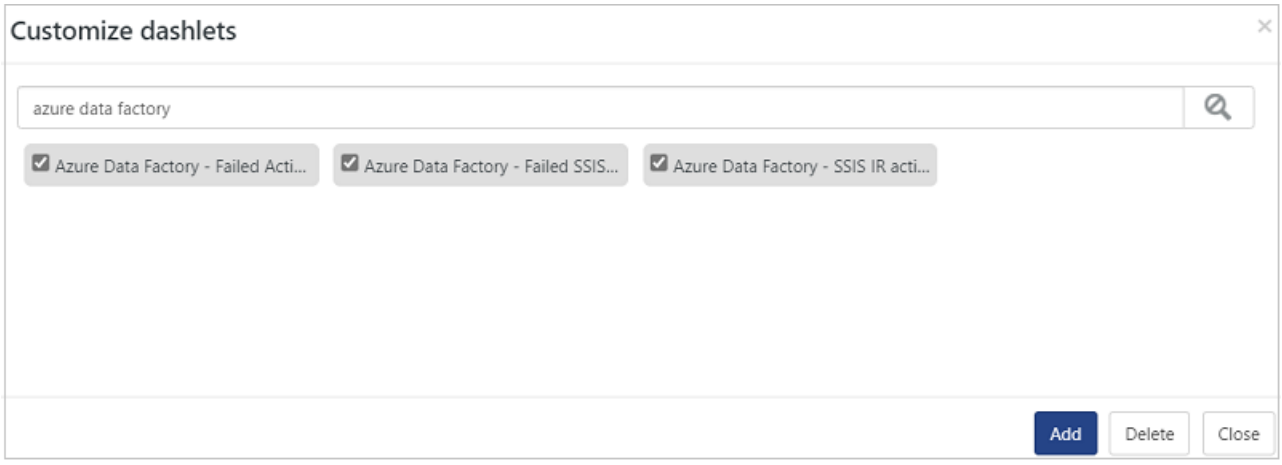
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.6 Dashboard

1. In the **EventTracker** console, go to **Home** > **My Dashboard**, and click the **Customize dashlets**.



2. In the **Customize dashlets** interface, search for **Azure Data Factory** in the search field.
3. The following Azure Data Factory dashlet files will get displayed



About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSPs SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support