

Integration Guide

Integrate Azure Application Gateway with EventTracker

Publication Date:

September 02, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Azure Application Gateway. 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 ETS-Azure-LogForwarder version 1.0 and above.

Audience

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

Table of Contents

| | | |
|----------|--|-----------|
| 1 | Overview | 4 |
| 2 | Prerequisite | 4 |
| 3 | EventTracker Knowledge Packs | 4 |
| 3.1 | Category | 4 |
| 3.2 | Alerts..... | 4 |
| 3.3 | Reports | 5 |
| 3.4 | Dashboard | 5 |
| 4 | Importing Azure Application Gateway Knowledge Packs into EventTracker | 7 |
| 4.1 | Category | 8 |
| 4.2 | Alerts..... | 9 |
| 4.3 | Token Template..... | 10 |
| 4.4 | Reports | 11 |
| 4.5 | Knowledge Objects (KO)..... | 13 |
| 4.6 | Dashboard | 15 |
| 5 | Verifying Azure Application Gateway Knowledge Packs in EventTracker..... | 17 |
| 5.1 | Category | 17 |
| 5.2 | Alerts..... | 17 |
| 5.3 | Token Template..... | 19 |
| 5.4 | Reports | 19 |
| 5.5 | Knowledge Objects (KO)..... | 20 |
| 5.6 | Dashboard | 20 |

1 Overview

Azure Application Gateway is a web traffic load balancer that enables managing traffic to web applications. The Azure Application Gateway supports features like SSL/TLS termination, Autoscaling, Zone redundancy, Static VIP, Web Application Firewall, Ingress Controller for AKS, URL-based routing, Multiple-site hosting, Redirection, Session affinity, and more.

Netsurion facilitates monitoring events retrieved from the Azure Application Gateway. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, benefit in tracking application vulnerabilities, brute force attacks, scripting attacks, SQL injection attacks, and others.

2 Prerequisite

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

Note

Refer to [How-To Guide](#) to configure Azure Application Gateway 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 Category

Azure Application Gateway - Access events: This category of the saved search allows you to parse events that are specific to the Access activities of the Azure Application Gateway.

Azure Application Gateway - Firewall events: This category of the saved search allows you to parse events that are specific to the Firewall activities of the Azure Application Gateway.

3.2 Alerts

Azure Application Gateway: Application vulnerabilities detected: This alert is triggered when a vulnerabilities like remote file inclusion, remote code execution, HTTP protocol violations/anomalies and request smuggling are detected.

Azure Application Gateway: Brute force detected: This alert is triggered when brute force is detected.

Azure Application Gateway: Cross-site scripting attack: This alert is triggered when potentially malicious content is detected in the requests through gateway which may be linked to XSS or PHP scripting.

Azure Application Gateway: SQL injection detected: This alert is triggered when SQL injection is detected.

3.3 Reports

Azure Application Gateway - Access error summary: This report provides a detailed summary of access events in Azure Application Gateway. The report includes the client IP, requested URL, response latency, return code, bytes in and out, and more.

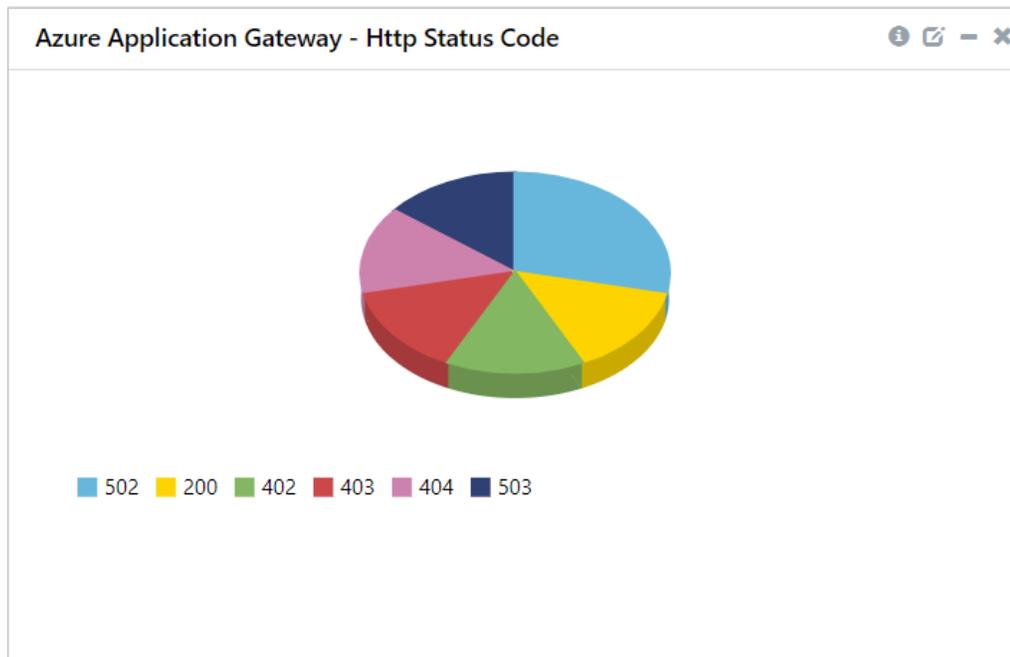
| LogTime | Client IP | Host | User Agent | InstanceID | Http Method | Http Version | Client Port | Http Status |
|------------------------|---------------|----------|--------------------------------------|-------------------------|-------------|--------------|-------------|-------------|
| 06-22-2022 05:05:33 AM | 10.207.204.44 | vgw098 | Mozilla/5.0 (Windows NT 6.1; WOW64) | appgw_2 | PUT | HTTPV1.1 | 51886 | 404 |
| 06-22-2022 05:05:34 AM | 10.2.2.13 | appgw009 | NetSystemsResearch studies the avail | 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; WOW64) | appgw_4 | PUT | HTTPV1.1 | 51886 | 404 |
| 06-22-2022 05:05:34 AM | 10.2.56.36 | appgw009 | NetSystemsResearch studies the avail | appgw_3 | DELETE | HTTP/1.1 | 37408 | 200 |
| 06-22-2022 05:05:35 AM | 10.20.2.139 | vgw098 | Mozilla/5.0 (Windows NT 6.1; WOW64) | appgw_13 | PUT | HTTPV1.1 | 51886 | 404 |
| 06-22-2022 05:05:35 AM | 10.55.53.144 | appgw009 | Mozilla/5.0+(Windows+NT+10.0.+Win | ApplicationGatewayRole_ | DELETE | HTTP/1.1 | 37408 | 200 |
| 06-22-2022 05:05:35 AM | 10.20.2.139 | vgw098 | NetSystemsResearch studies the avail | appgw_25 | POST | HTTPV1.1 | 60929 | 402 |
| 06-22-2022 05:05:35 AM | 10.55.53.144 | appgw009 | NetSystemsResearch studies the avail | appgw_1 | GET | HTTPV1.1 | 60929 | 502 |

Azure Application Gateway - Firewall report: This report provides a detailed summary of the requests that are logged through either detection or prevention mode of an application gateway that is configured with the web application firewall. The report includes the client IP, requested URL, response latency, return code, prevention/detection method, 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 | 0a830da0e1da0d5f6b268de0bce3152 | 10.14.248.32 | 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 | 10.14.248.32 | 60929 | vm000003 | / | AzureApplicationGateway-CACHE-HIT | 942150 | OWASP_CRS | 3.0 | SQL Injection Attack: SQL Tautology Detected |
| 06-22-2022 05:05:35 AM | c6d4051cd01960334279f645b2a6be1b | 10.55.53.144 | 60929 | vm000004 | / | AzureApplicationGateway-CACHE-HIT | 920350 | OWASP | 3.0 | SQL Injection Attack: SQL Tautology Detected |
| 06-22-2022 05:05:35 AM | AcAcAcAcAKH@AcAcAcAcAyAt | 10.14.248.32 | 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 | 10.55.53.144 | 59338 | vm000004 | / | AzureApplicationGateway-CACHE-HIT | 920350 | OWASP | 3.0 | SQL Injection Attack: SQL Tautology Detected |
| 06-22-2022 05:05:36 AM | 0a830da0e1da0d5f6b268de0bce3152 | 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 | vm000004 | / | 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 | vm000003 | / | AzureApplicationGateway-CACHE-HIT | 920350 | OWASP | 3.0 | Host header is a numeric IP address |

3.4 Dashboard

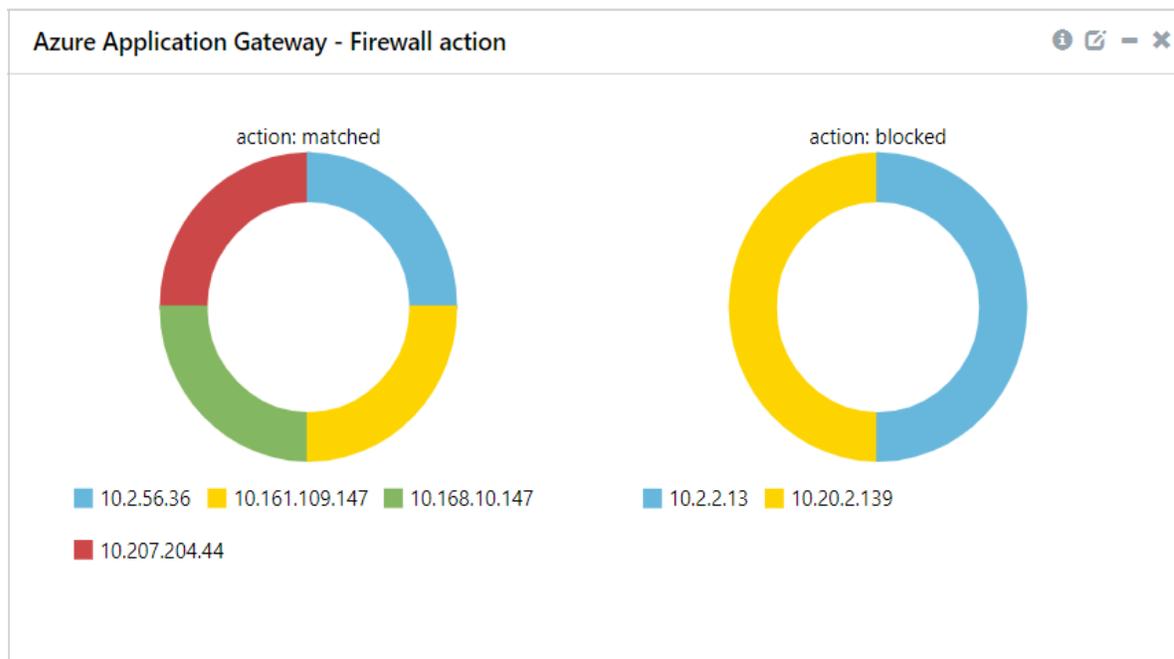
Azure Application Gateway - Http Status Code: This dashlet displays the http status code of the request accessing the Application Gateway.



Azure Application Gateway - Client IP by geolocation: This dashlet displays the geolocation of the client IPs that are connected to the Application Gateway.



Azure Application Gateway - Firewall action: This dashlet displays the actions taken by firewall rules for the connected hosts.

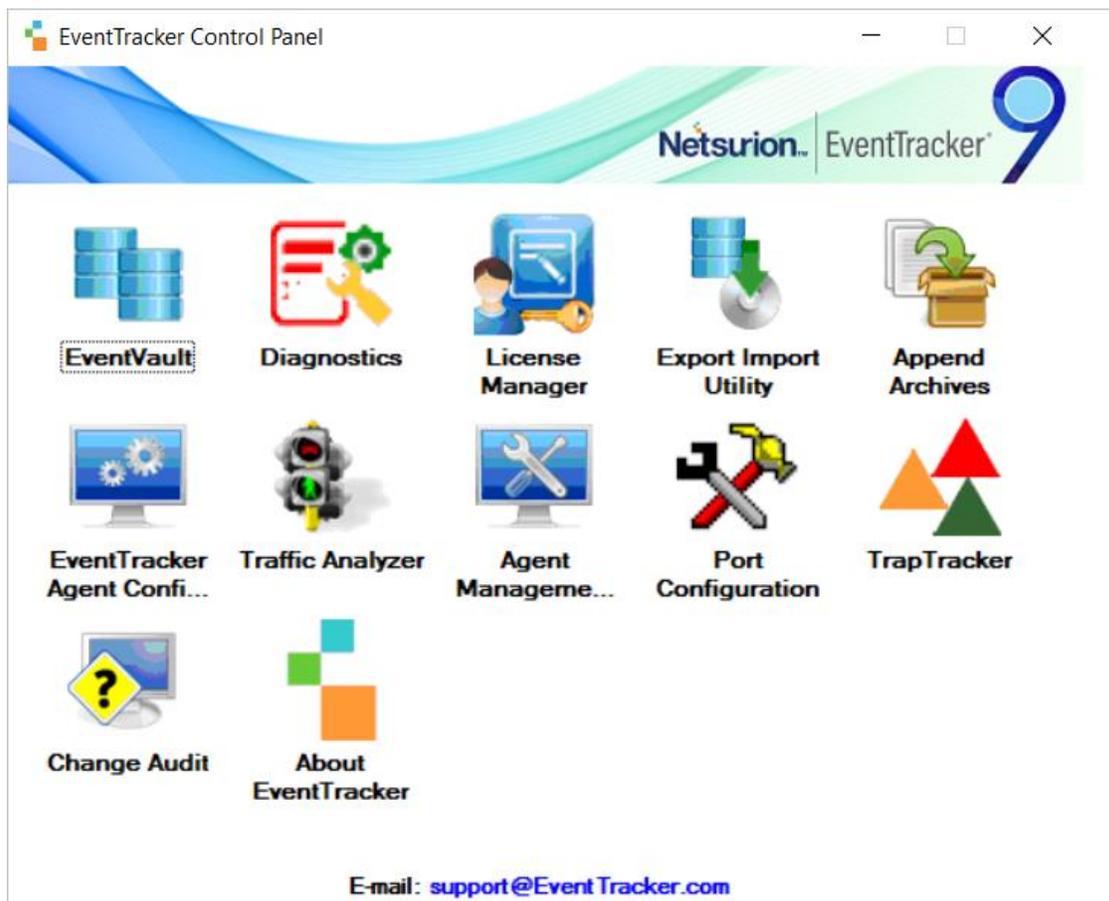


4 Importing Azure Application Gateway Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

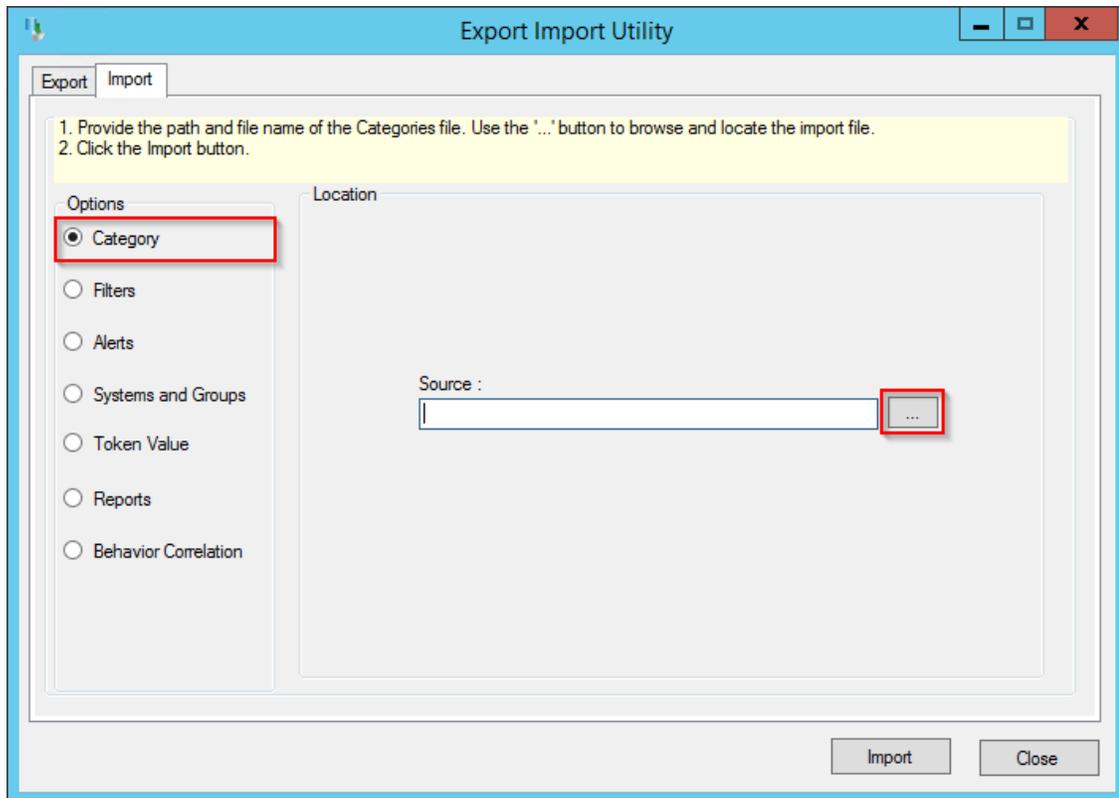
- Categories
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards

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

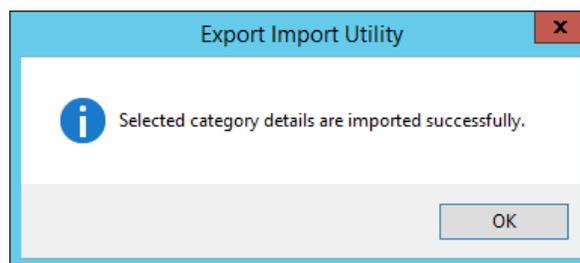


4.1 Category

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



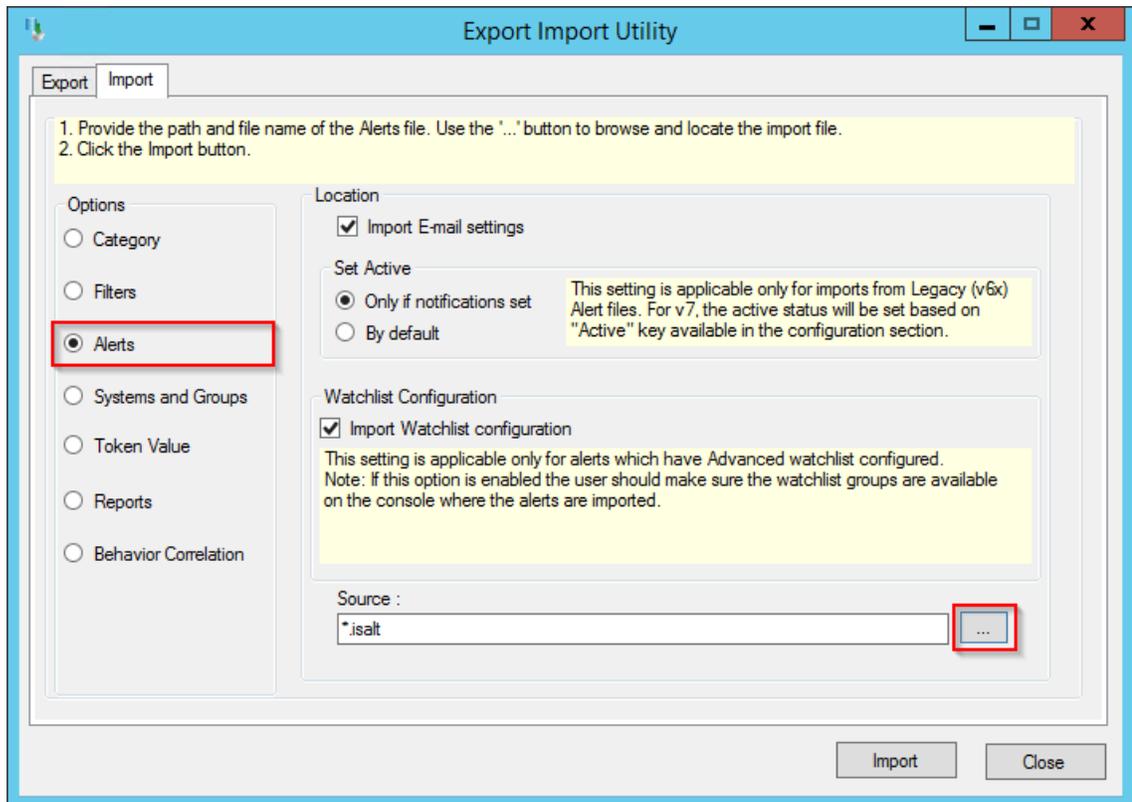
2. In the **Browse** window, locate the **Categories_Azure Application Gateway.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



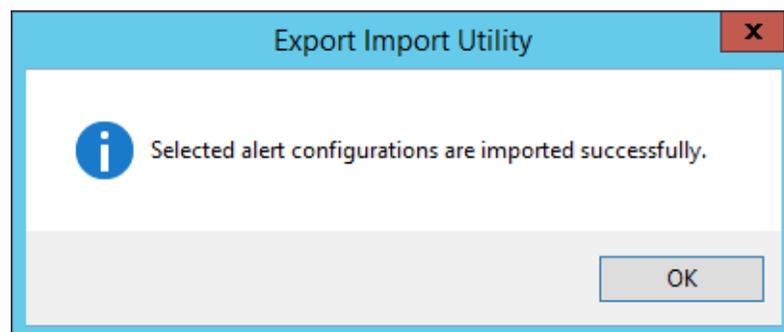
5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

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



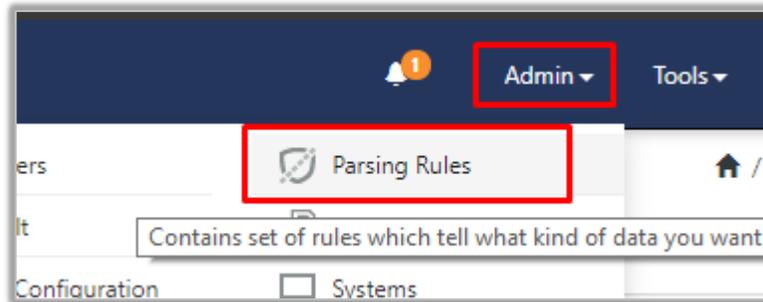
2. In the **Browse** window, locate the **Alerts_ Azure Application Gateway.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Alerts**.



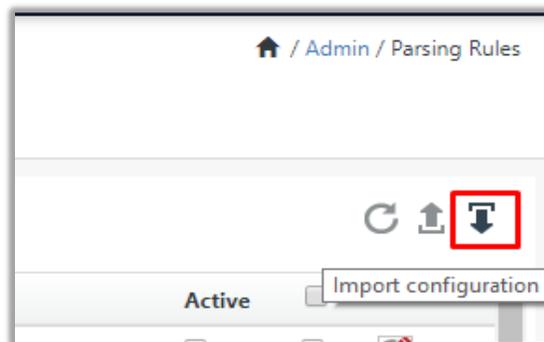
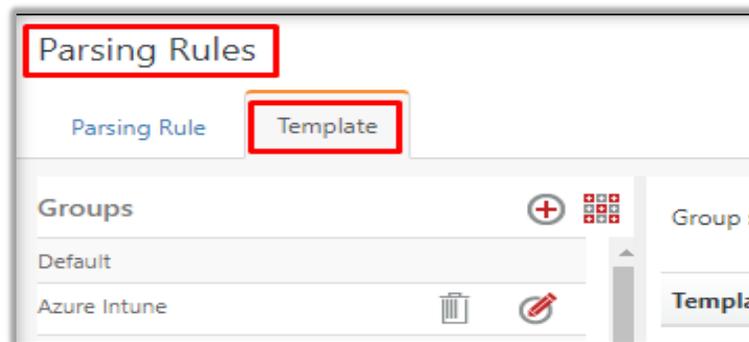
5. Click **OK** or the **Close** button to complete the process.

4.3 Token Template

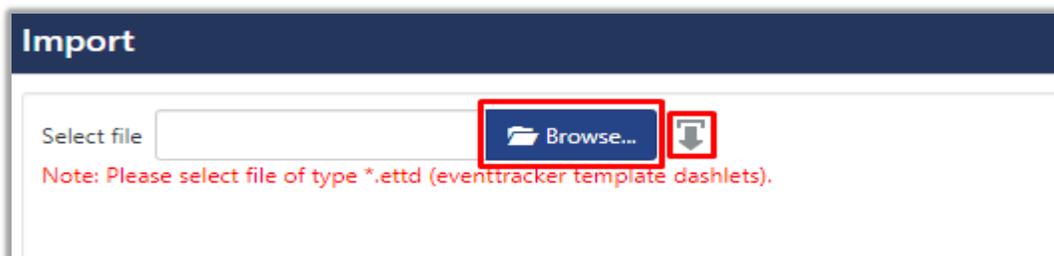
1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Parsing Rules**.



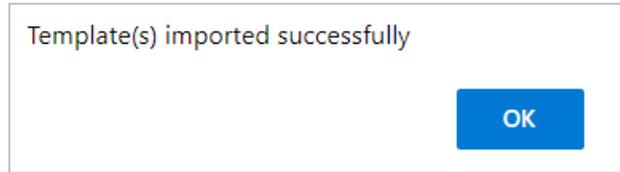
2. In the **Parsing Rules** interface, click the **Template** tab and then click **Import Configuration**.



3. In the **Import** window, click **Browse** to search and locate for the file name with **“.ettd”** extension (example, **Templates_Azure Application Gateway.ettd**).

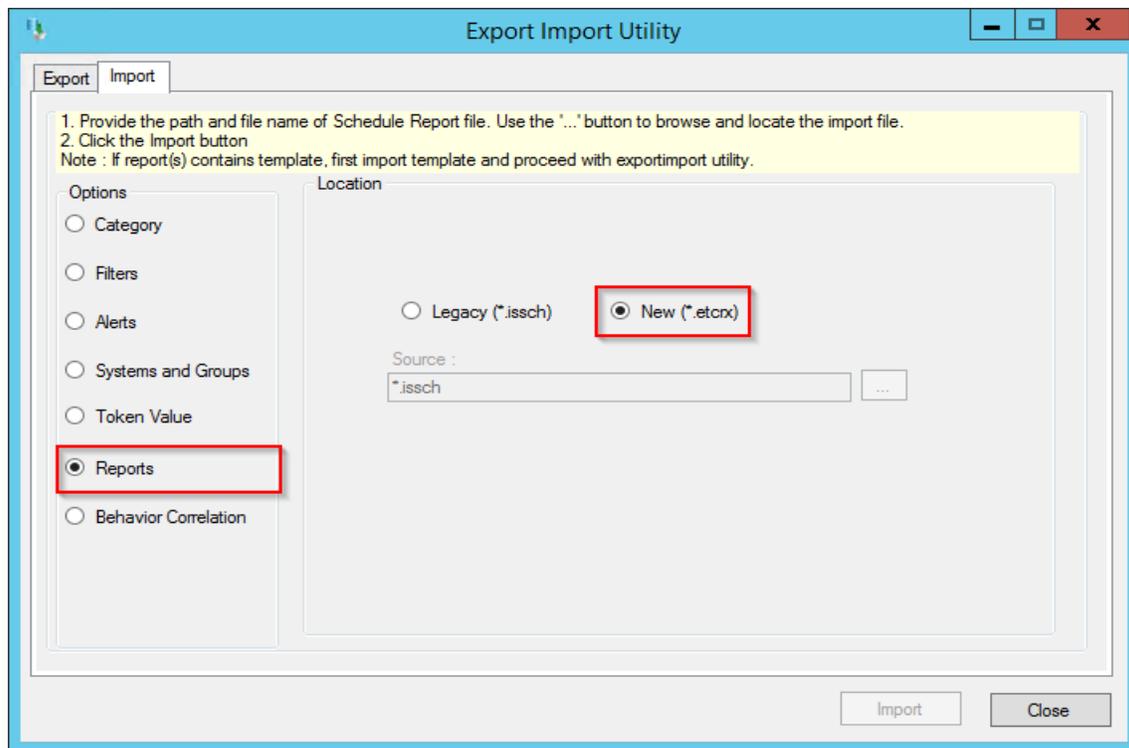


4. It takes few seconds to load the templates and once you see the list of templates, click the appropriate templates, and click **Import**.
5. EventTracker displays a success message on successfully importing the selected file in **Template**.

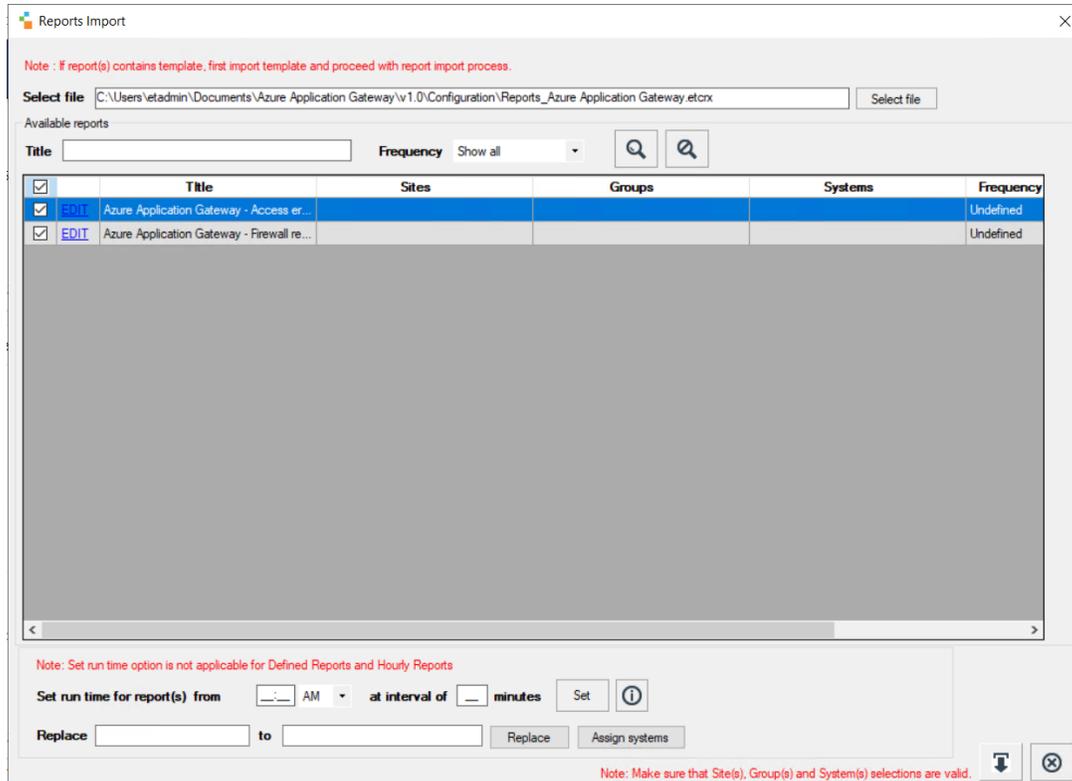


4.4 Reports

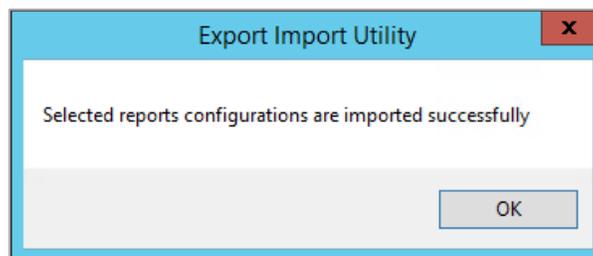
1. In the **Import** tab, click **Reports** and then click **New (*.etcrx)**.



- In the **Reports Import** window, click **Select file** to locate **Reports_Azure Application Gateway.etcrx** file.
- Select the check box of all the files and click the **Import** button to import the selected files



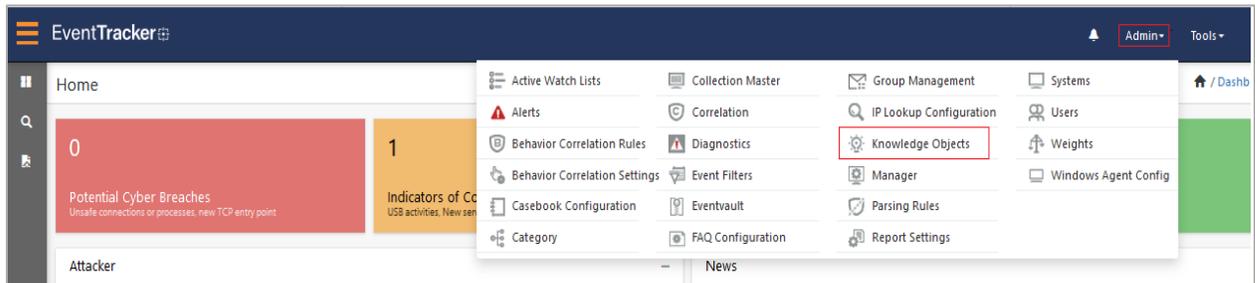
- EventTracker displays a success message on successful importing of the selected file in **Reports**.



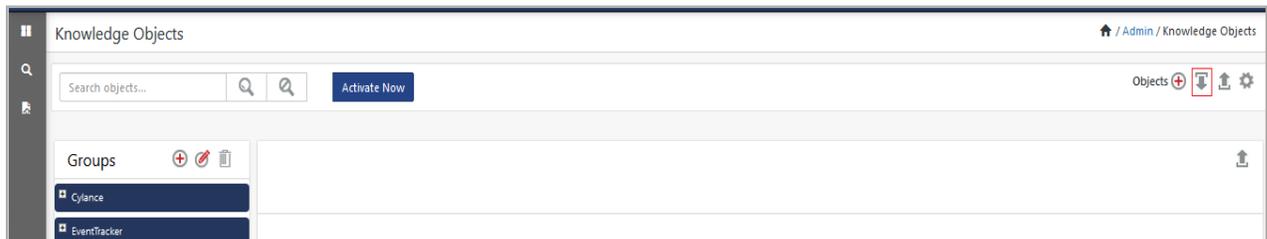
- Click **OK** or the **Close** button to complete the process.

4.5 Knowledge Objects (KO)

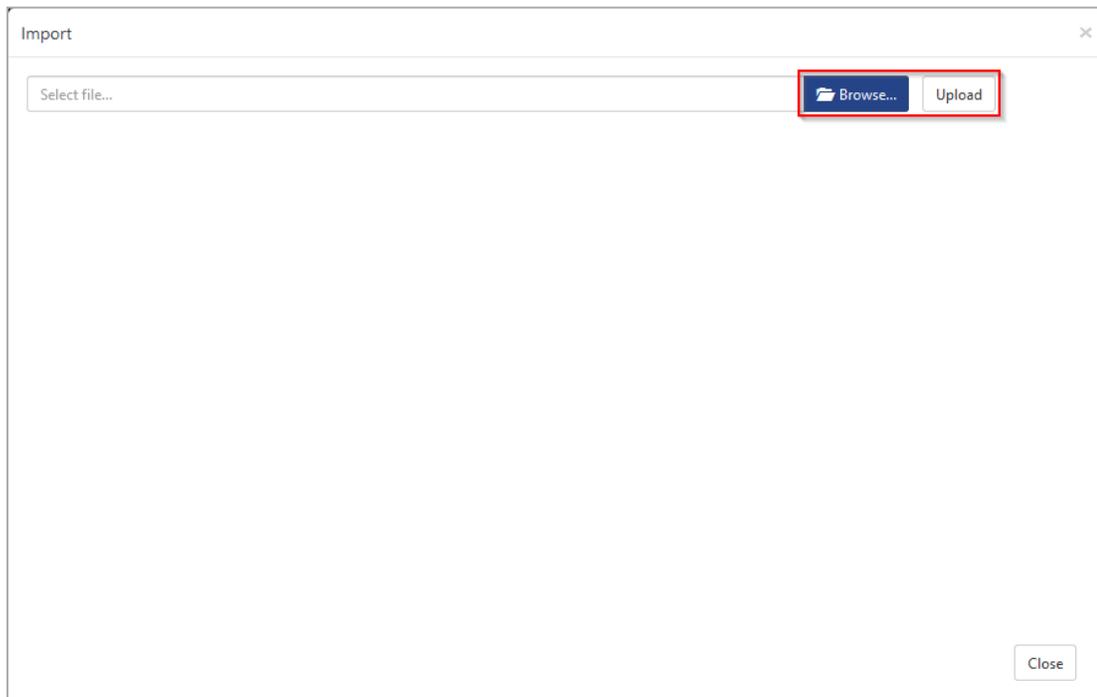
1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.



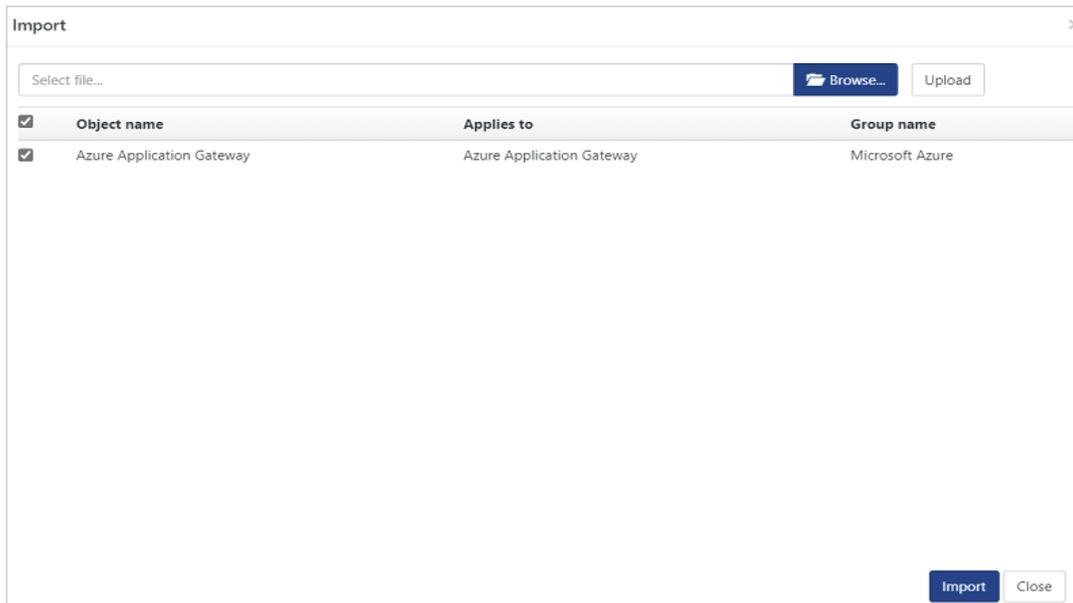
2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.



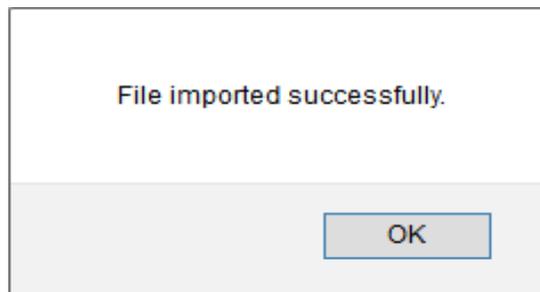
3. In the **Import** window, click **Browse** and locate the **KO_ Azure Application Gateway.etko** file.



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



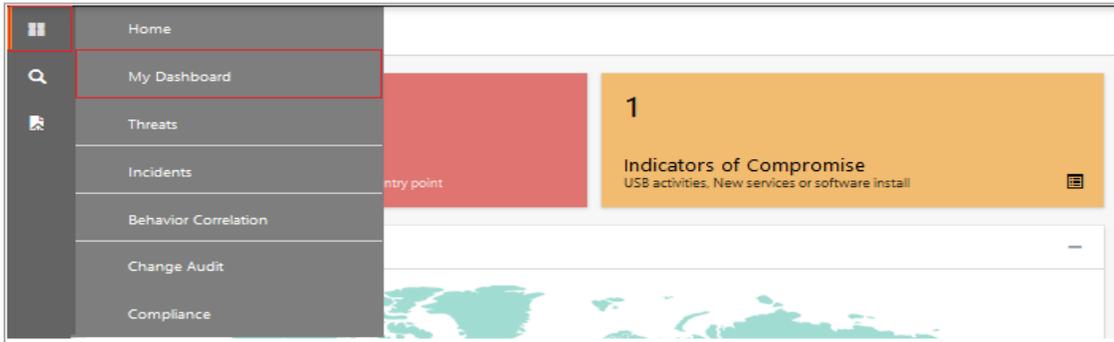
5. EventTracker displays a successful message on successfully importing the selected file in **Knowledge Objects**.



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

4.6 Dashboard

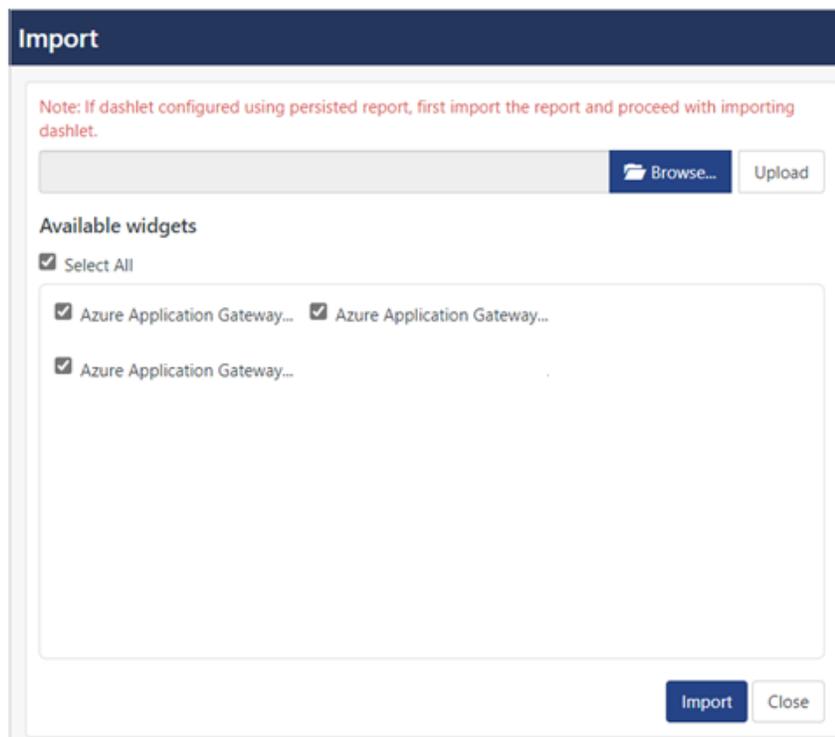
1. Log in to the **EventTracker** web interface and go to **Dashboard > My Dashboard**.



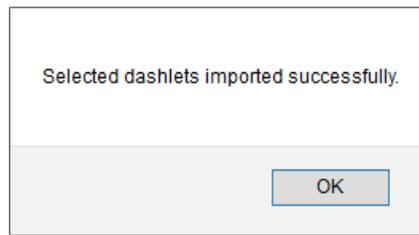
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.



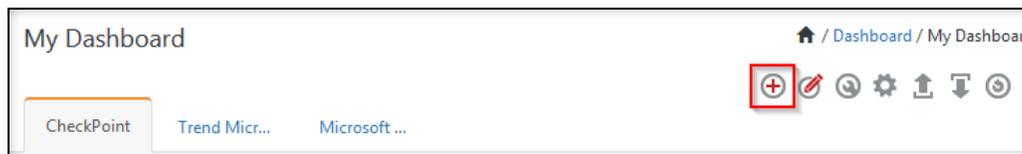
3. In the **Import** window, click **Browse** to locate the **Dashboards_Azure Application Gateway.etwd** file and then click **Upload**.
4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.



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



- Then, in the **My Dashboard** interface click the **Add**  button to add dashboard.



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

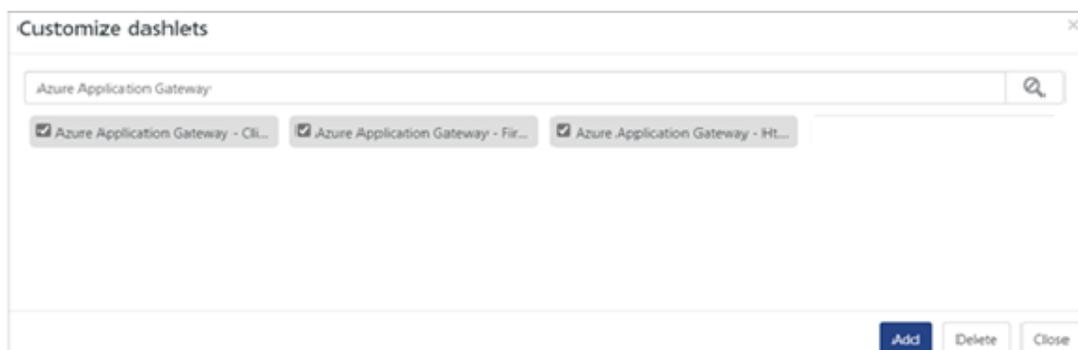
Edit Dashboard

Title

Description

- From the newly created dashboard interface (for example, **Azure Application Gateway**), click the **Configuration**  button to add the Azure Application Gateway dashlets.

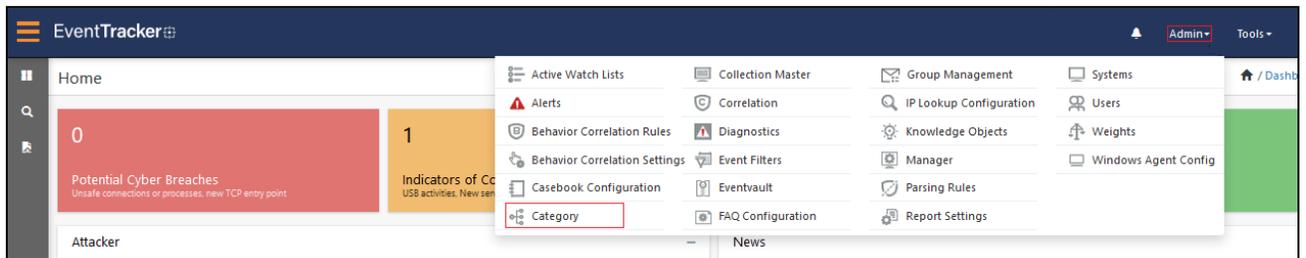
- Search and select the newly imported dashlets and click **Add**.



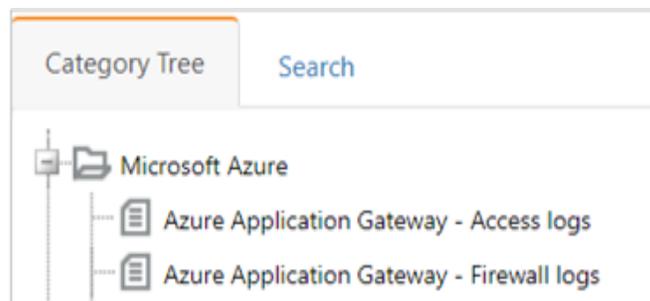
5 Verifying Azure Application Gateway Knowledge Packs in EventTracker

5.1 Category

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

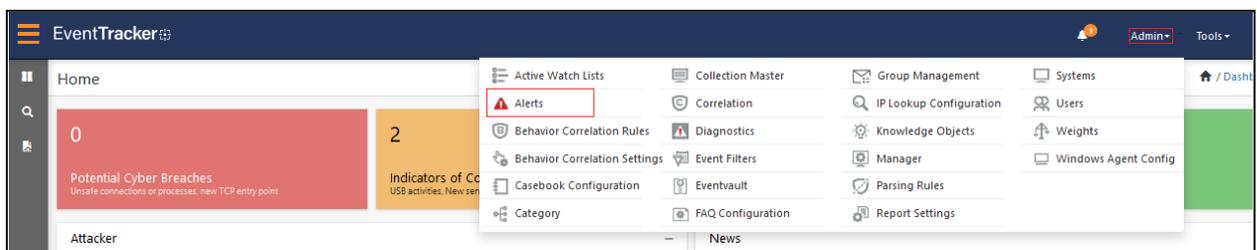


2. In the **Category** interface, under the **Category Tree** tab, click the **Microsoft Azure** group folder to expand and see the imported categories.



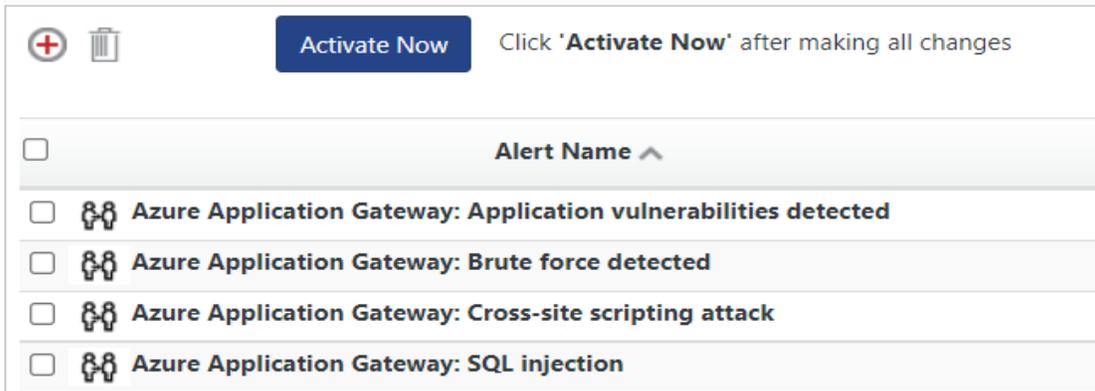
5.2 Alerts

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



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

- The **Alerts** interface will display all the imported **Azure Application Gateway** alerts.



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



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

Note

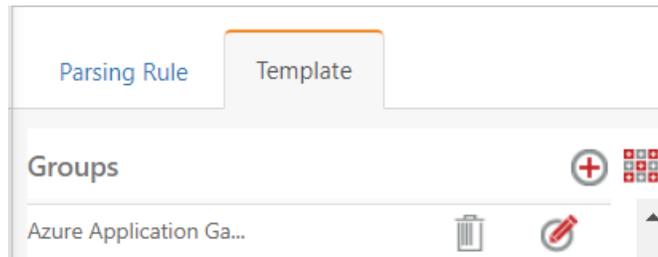
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

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

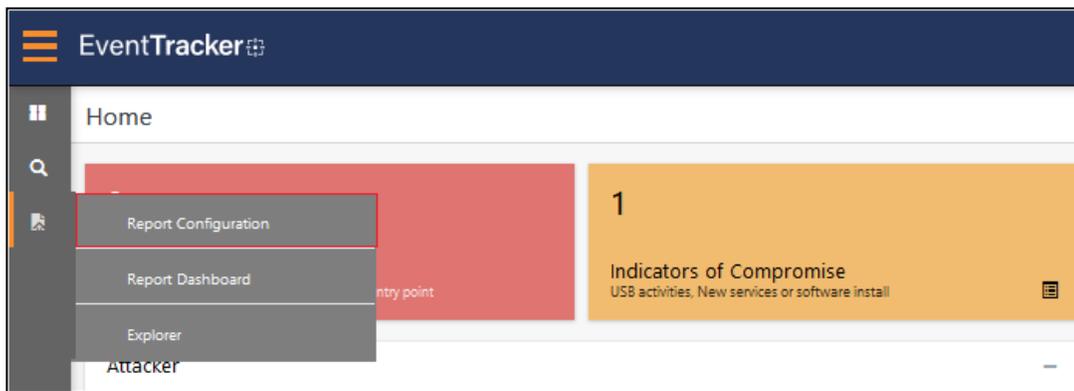
5.3 Token Template

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 Application Gateway** group folder to view the imported Token template.

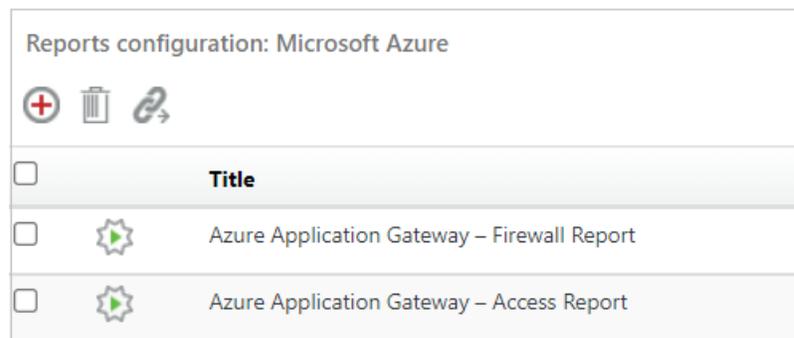


5.4 Reports

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

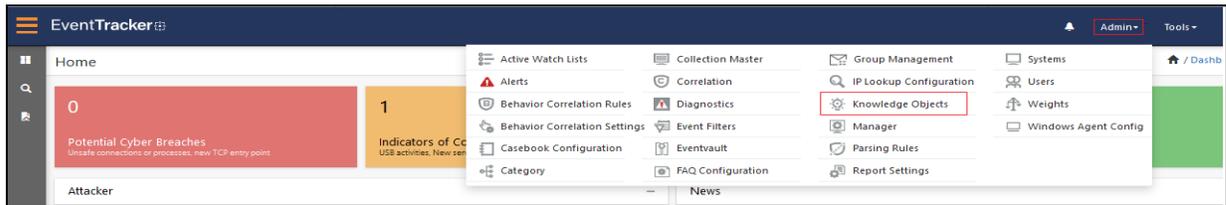


2. In the **Reports Configuration** interface, select the **Defined** option.
3. In the search field, type **Microsoft Azure** and click **Search** to search for the Azure Application Gateway files.
4. EventTracker displays the reports for Azure Application Gateway.

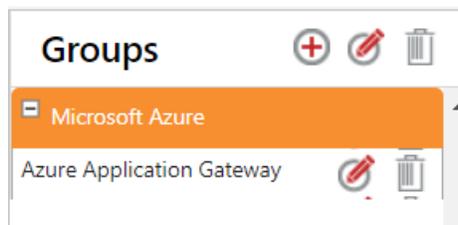


5.5 Knowledge Objects (KO)

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.

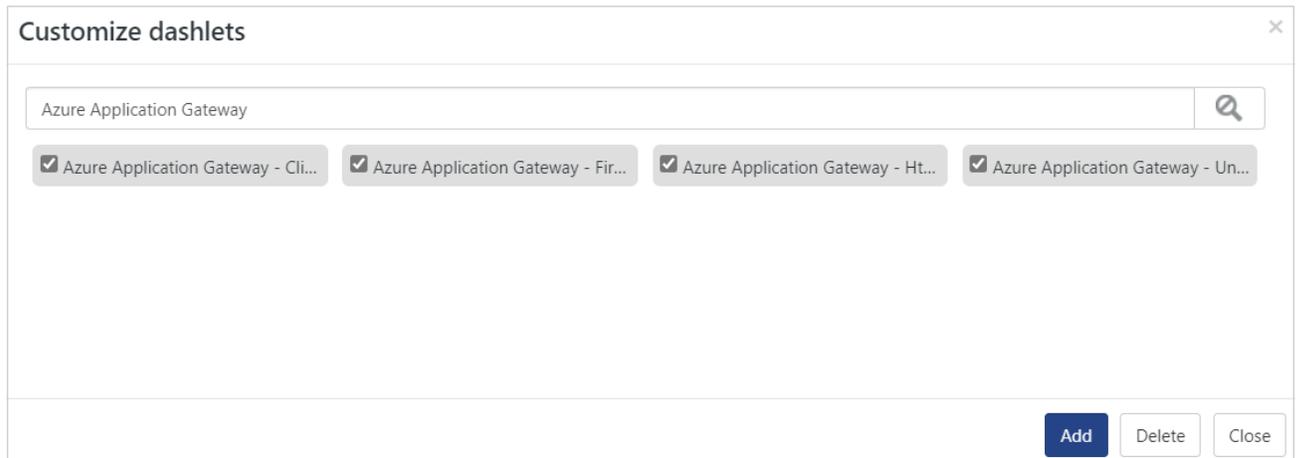
5.6 Dashboard

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



2. In the **Customize dashlets** interface, search for **Azure Application Gateway** in the search field.

3. The following Azure Application Gateway 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](https://www.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>