Integration Guide

Integrate Azure Database for MySQL with EventTracker

Publication Date:

July 13, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Azure Database for MySQL. 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 Database for MySQL.

Audience

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

Table of Contents

1 Overview

Azure Database for MySQL is a relational database service in the Microsoft Azure cloud that uses the MySQL Community Edition database engine. It benefits you to stay focused on rapid app development and rev your time to market rather than managing virtual machines and infrastructure.

Netsurion facilitates monitoring events from the Azure Database for MySQL. The dashboard, categories, alerts, and reports interface in Netsurion's threat protection platform, EventTracker, benefits in tracking database activities and changes to detect any suspicious activities performed on the MySQL database.

2 Prerequisite

- EventTracker version 9.3 or later must be installed and configured to receive logs.
- Configure Azure Database for MySQL to forward logs to EventTracker.

Note

Refer to How-To guide to configure Azure Database for MySQL 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 Database for MySQL - Database activities: This category of the saved search will allow the users to parse the events that are specific to the database activities in Azure Database for MySQL.

3.2 Alerts

Azure Database for MySQL: Access denied: This alert indicates that an attempt was made to modify the database without a proper credentials or the user does not have the appropriate privilege to do the modifications.

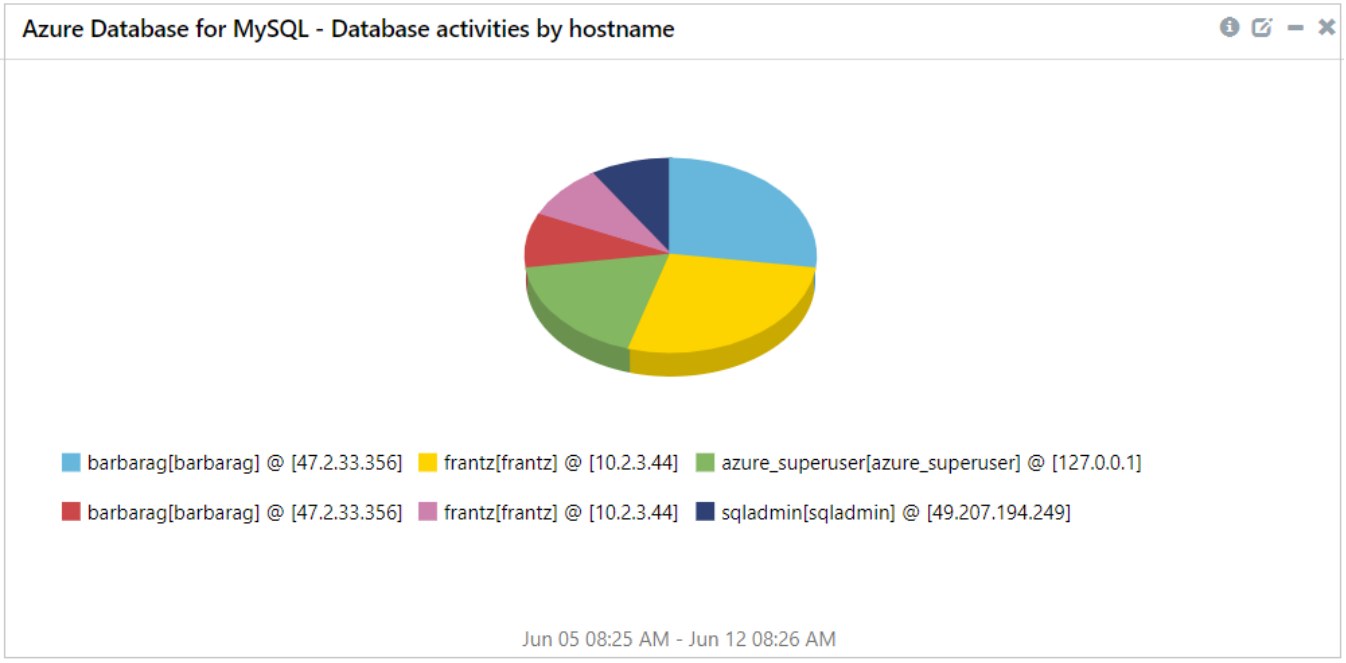
Azure Database for MySQL: Table deleted or updated: This alert indicates that an attempt was made to delete or update the table.

3.3 Reports

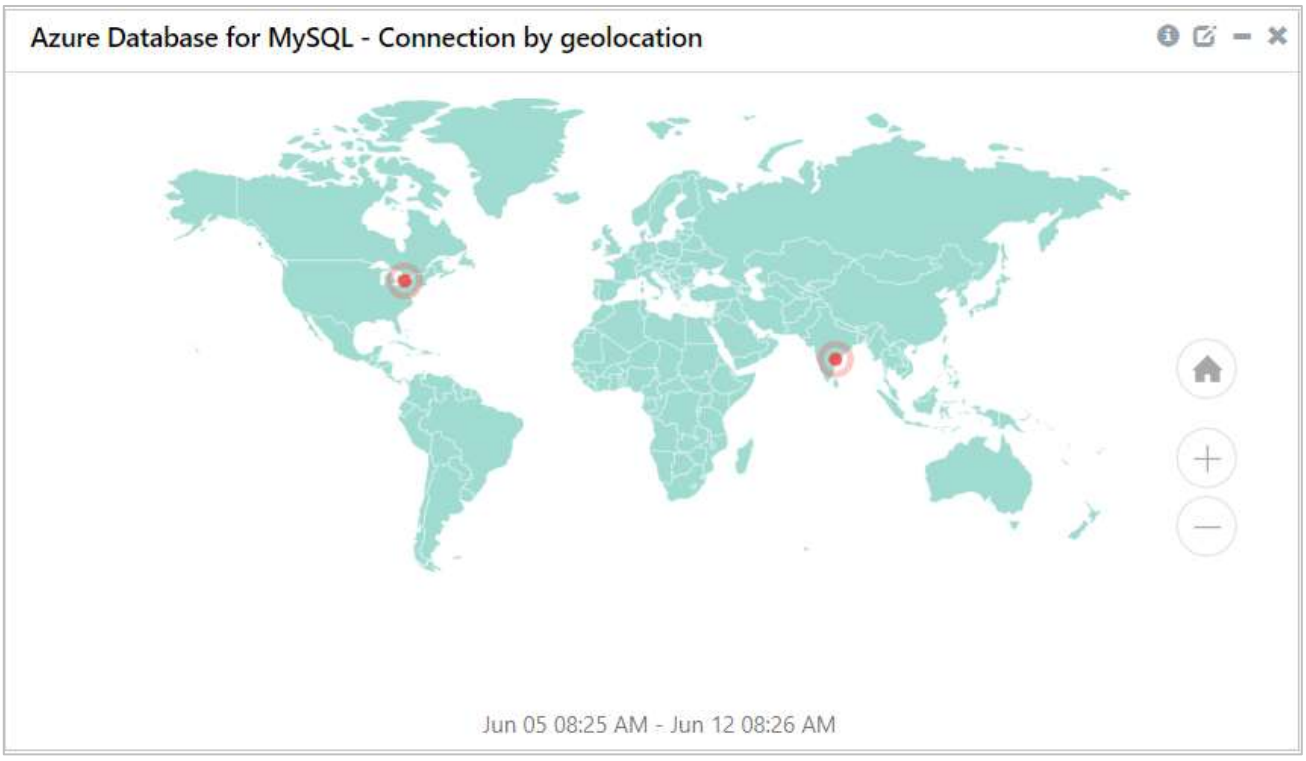
Azure Database for MySQL - Database activities: This report provides a detailed summary of the audit and performance activities in Azure Database for MySQL. It includes source IP address, operation name, operation type, result, correlation ID, and more.

3.4 Dashboard

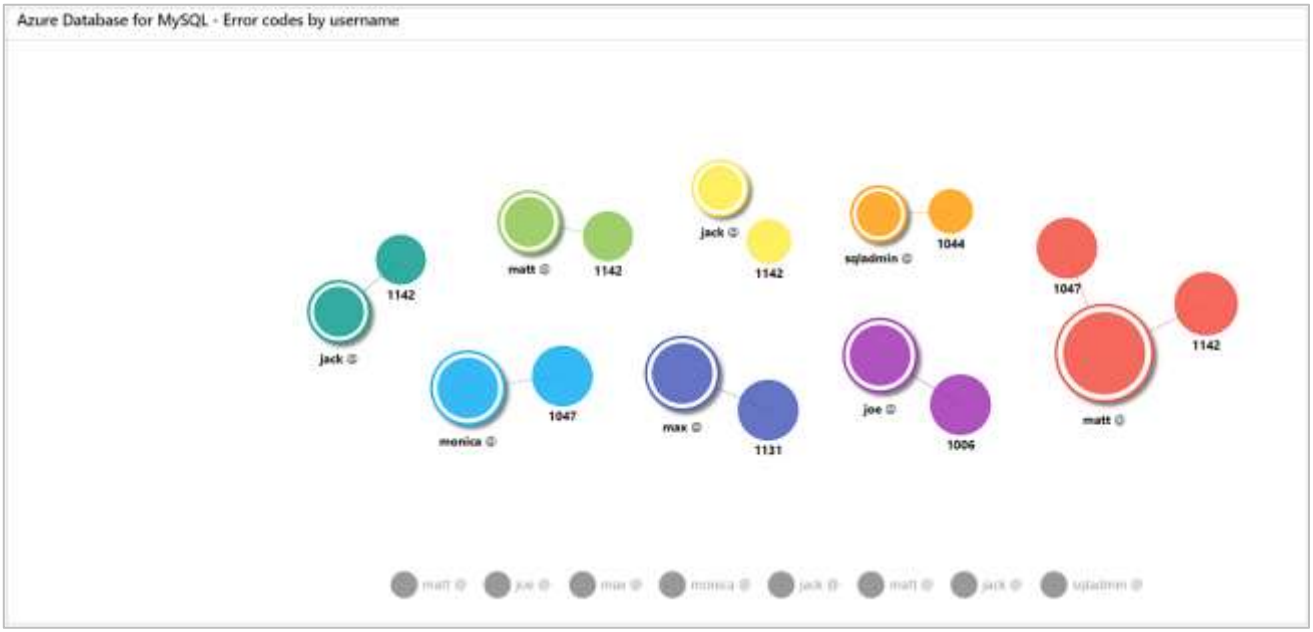
Azure Database for MySQL - Database activities by hostname



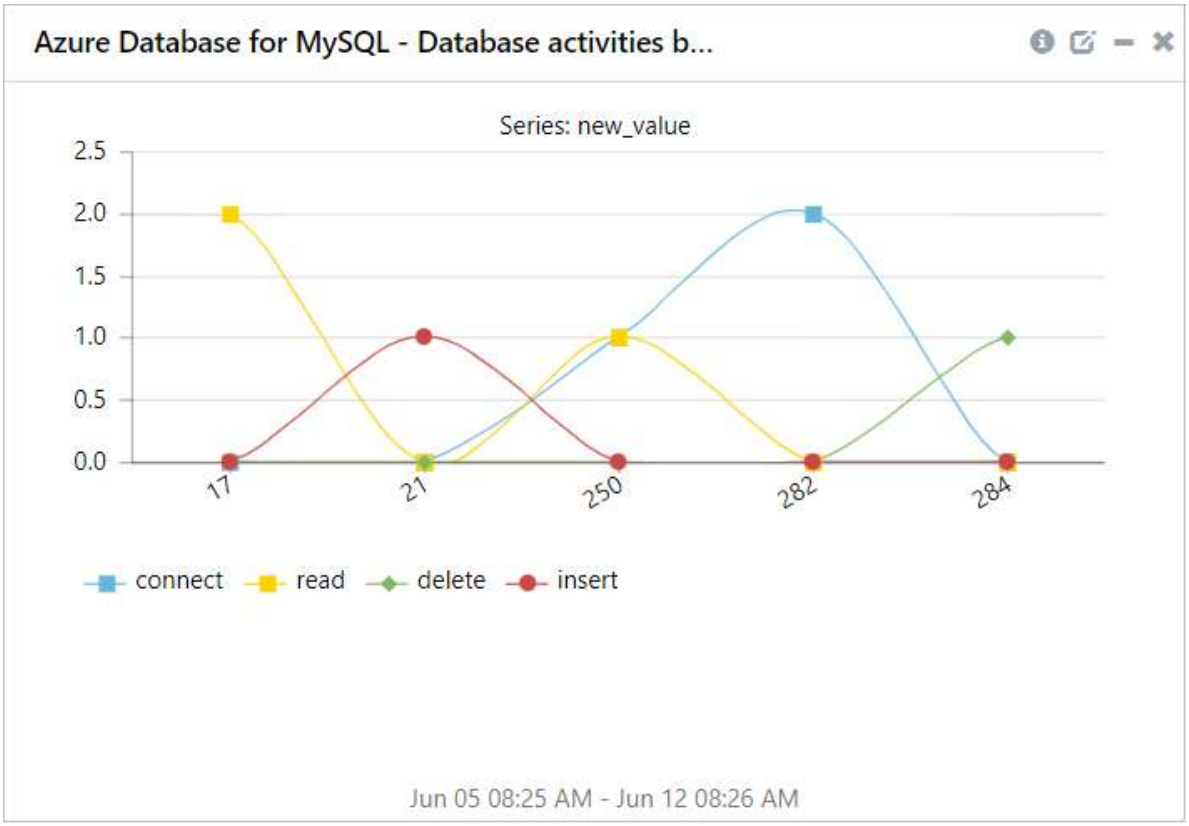
Azure Database for MySQL - Connection by geolocation



Azure Database for MySQL - Error codes by username



Azure Database for MySQL - Database activities by connection id

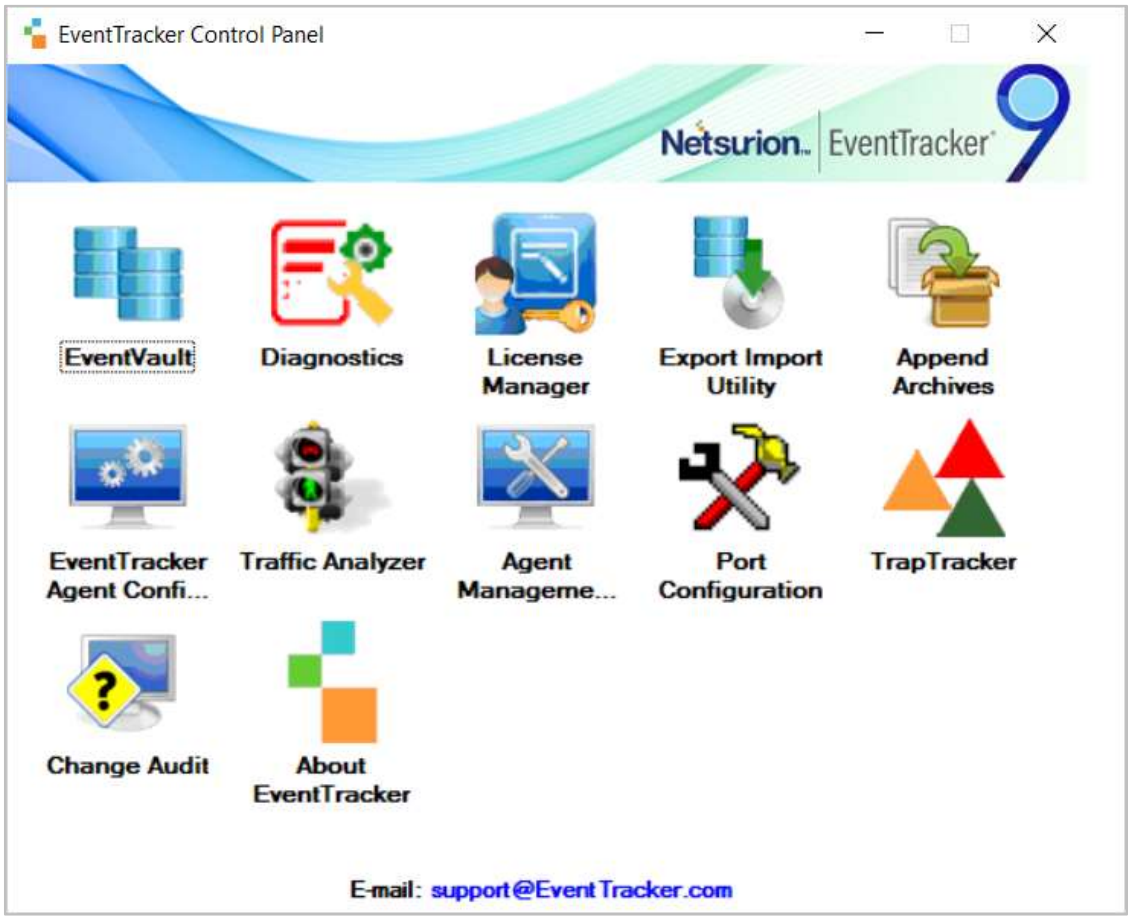


4 Importing Azure Database for MySQL Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

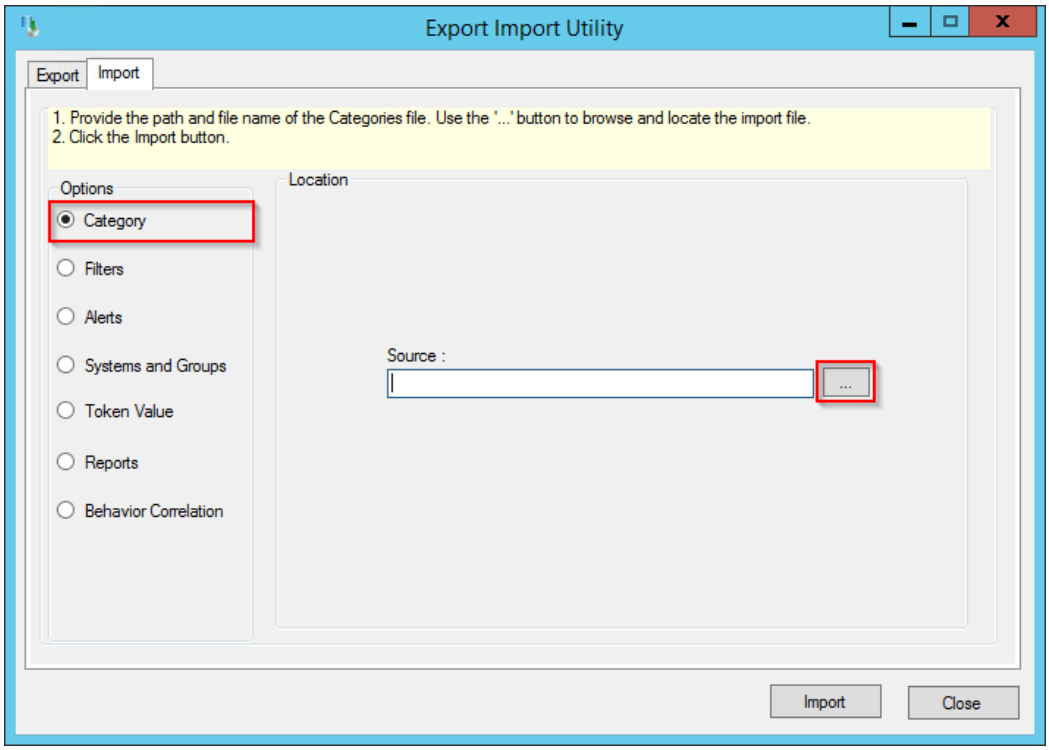
- Category
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards

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

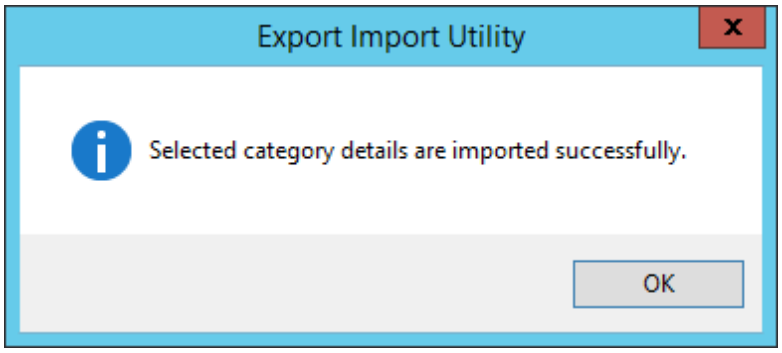


4.1 Category

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



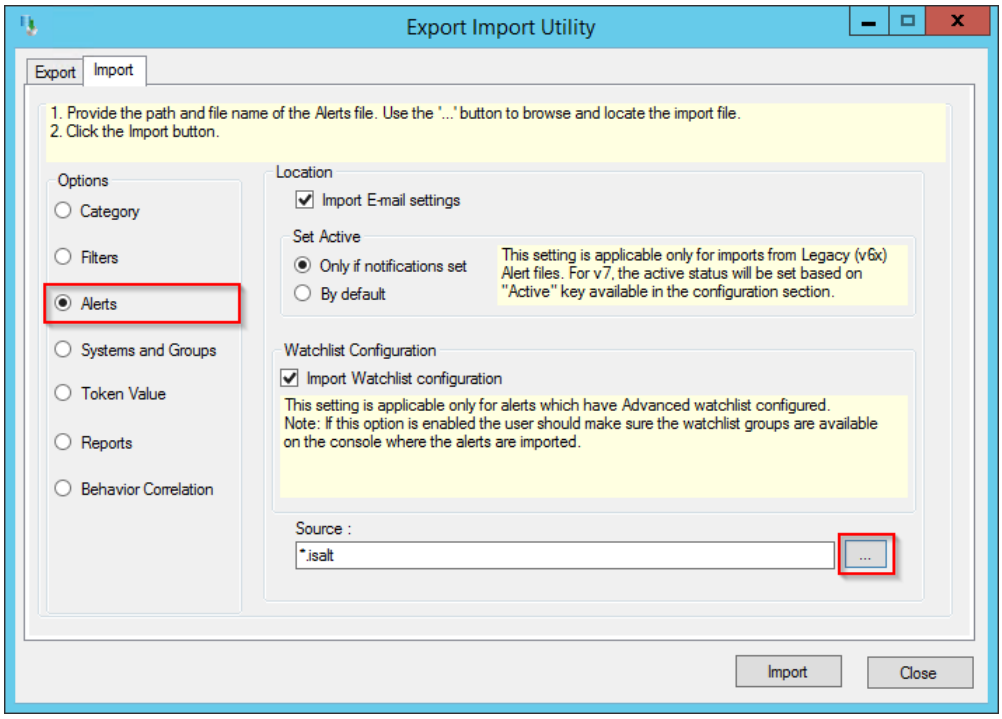
2. In the **Browse** window, locate the **Categories_Azure Database for MySQL.iscat** file and click **Open**.
3. To import the category, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



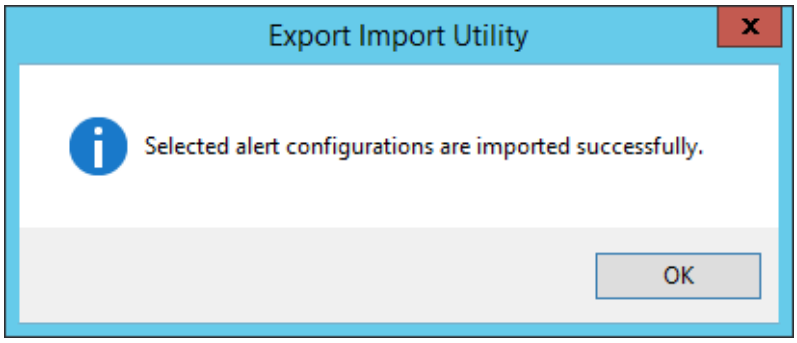
5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

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



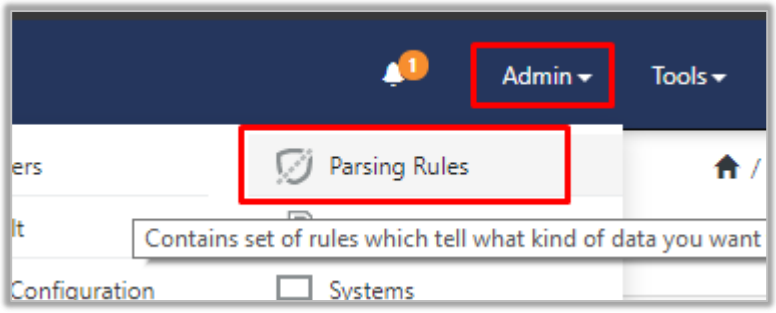
2. In the **Browse** window, locate the **Alerts_ Azure Database for MySQL.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Alerts**.



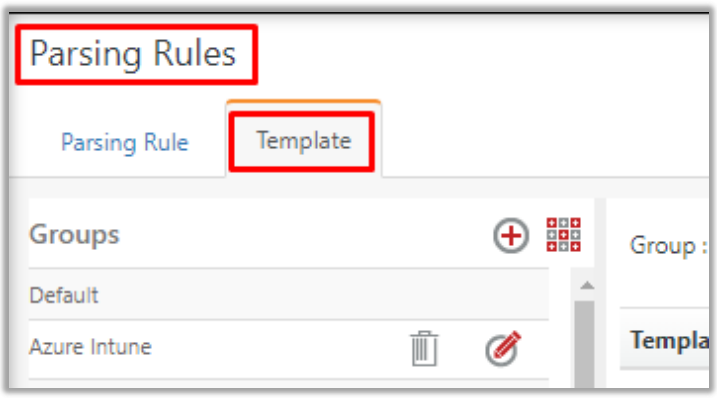
5. Click **OK** or the **Close** button to complete the process.

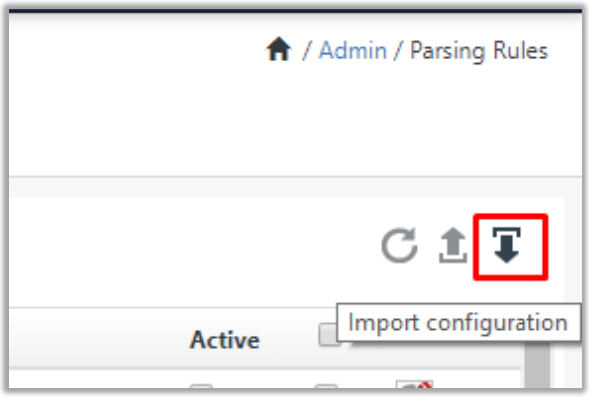
4.3 Token Template

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



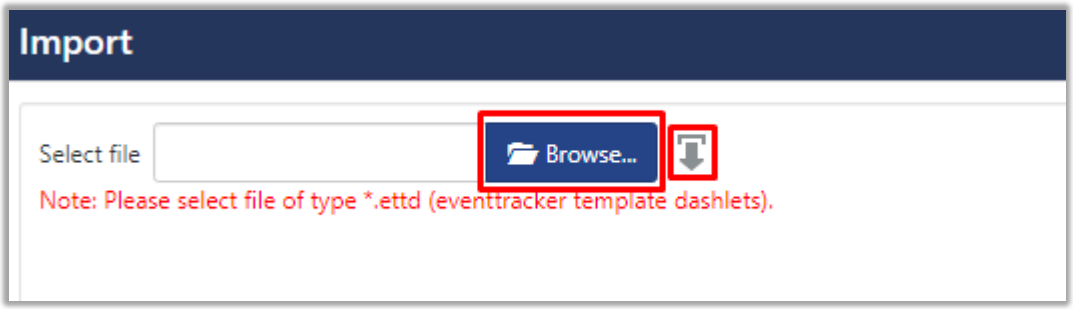
2. In the **Parsing Rules** interface, click the **Template** tab and then click **Import Configuration**.





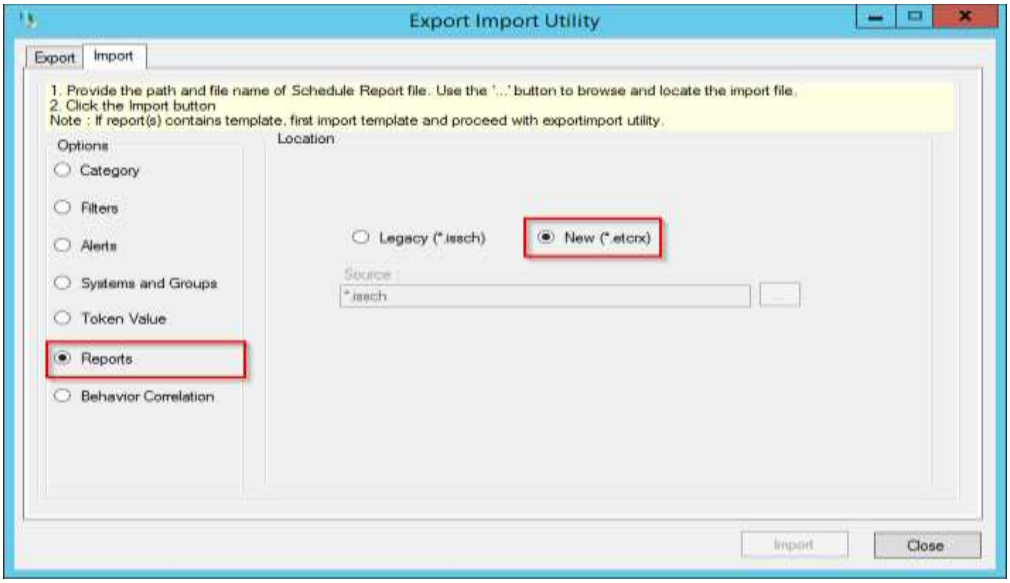
3. In the **Import** window, click **Browse** to search and locate for the file name with **".ettd"** extension (example, **Templates_Azure Database for MySQL.ettd**).

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

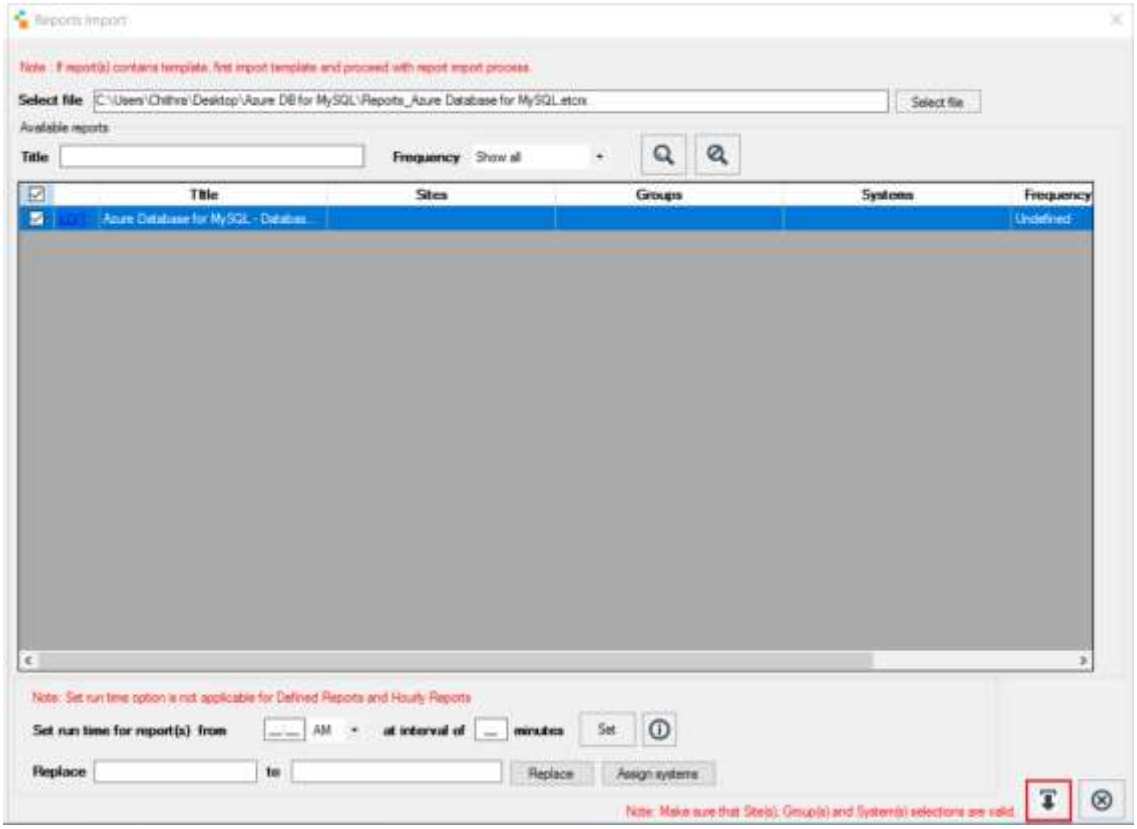


4.4 Reports

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

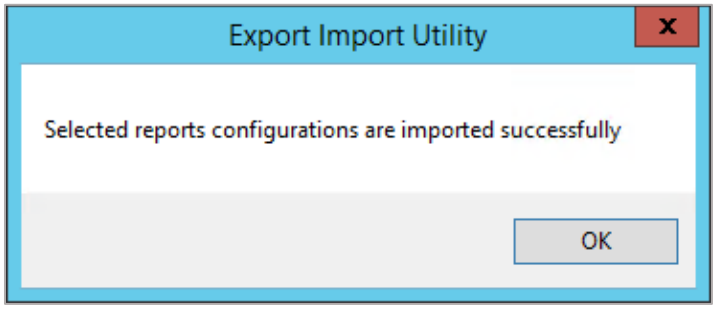


2. In the **Reports Import** window, click **Select file** to locate the **Reports_Azure Database for MySQL.etcrx** file.



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

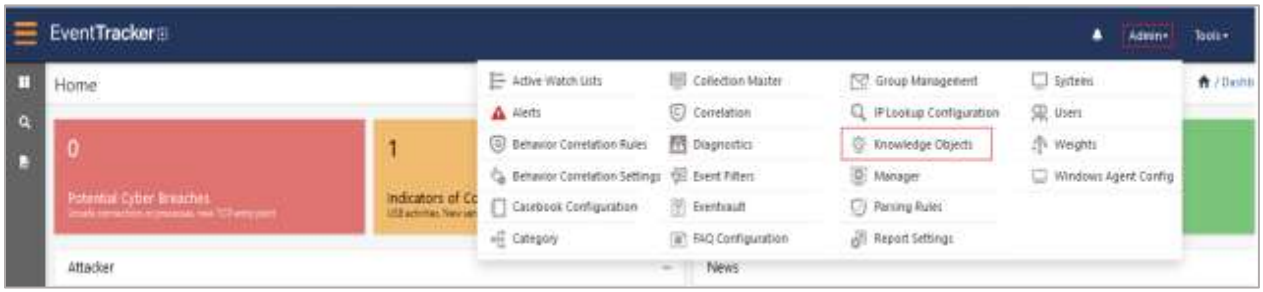
4. EventTracker displays a success message on successful importing of the selected file in **Reports**.



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

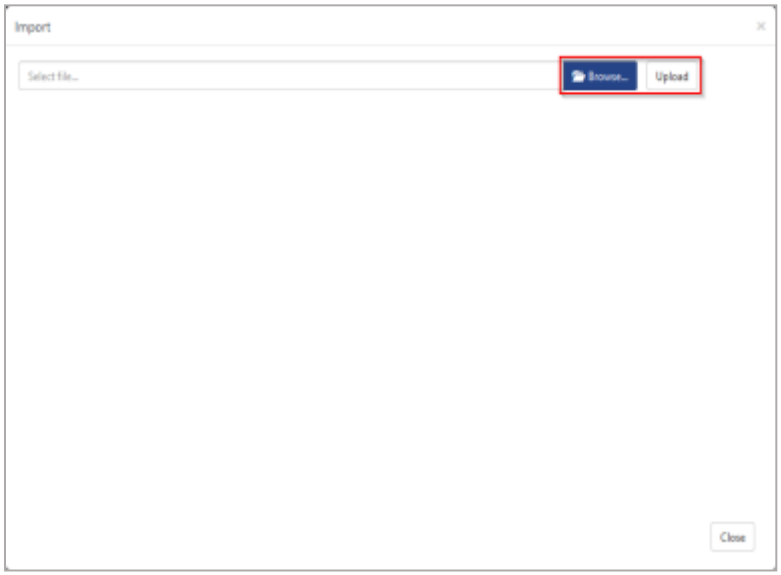
4.5 Knowledge Objects (KO)

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

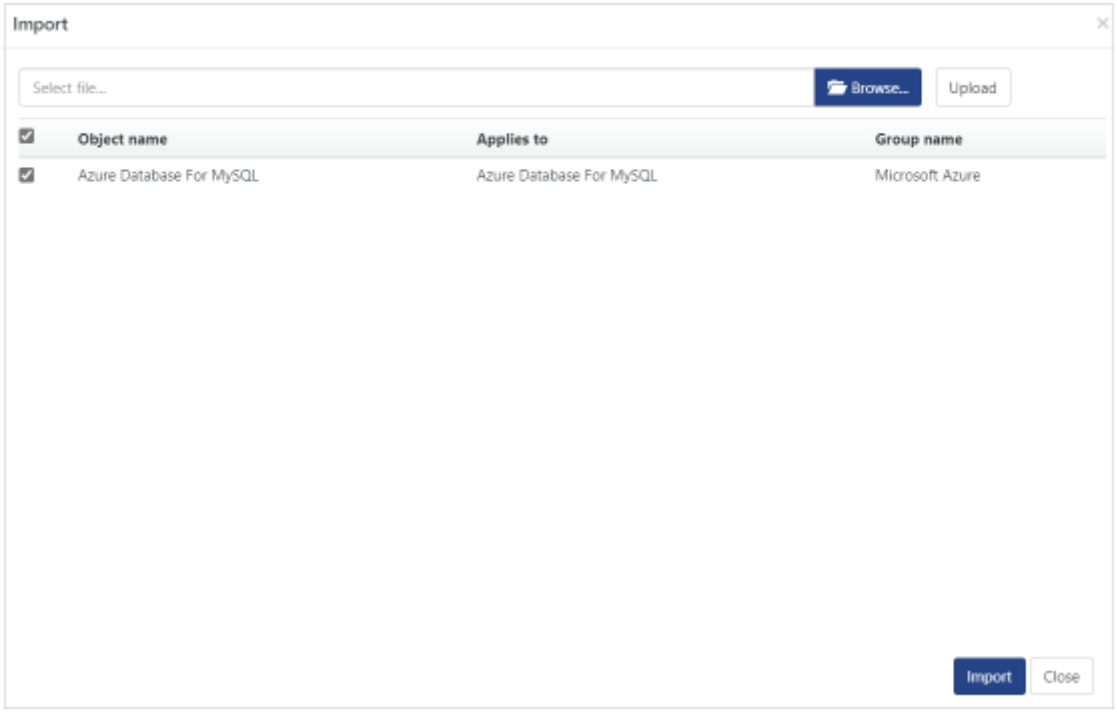


2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.

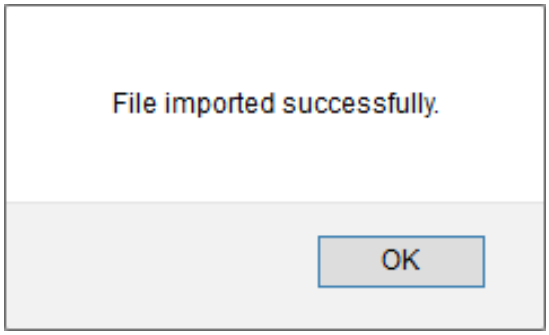
3. In the **Import** window, click **Browse** and locate the **KO_ Azure Database for MySQL.etko** file.



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.

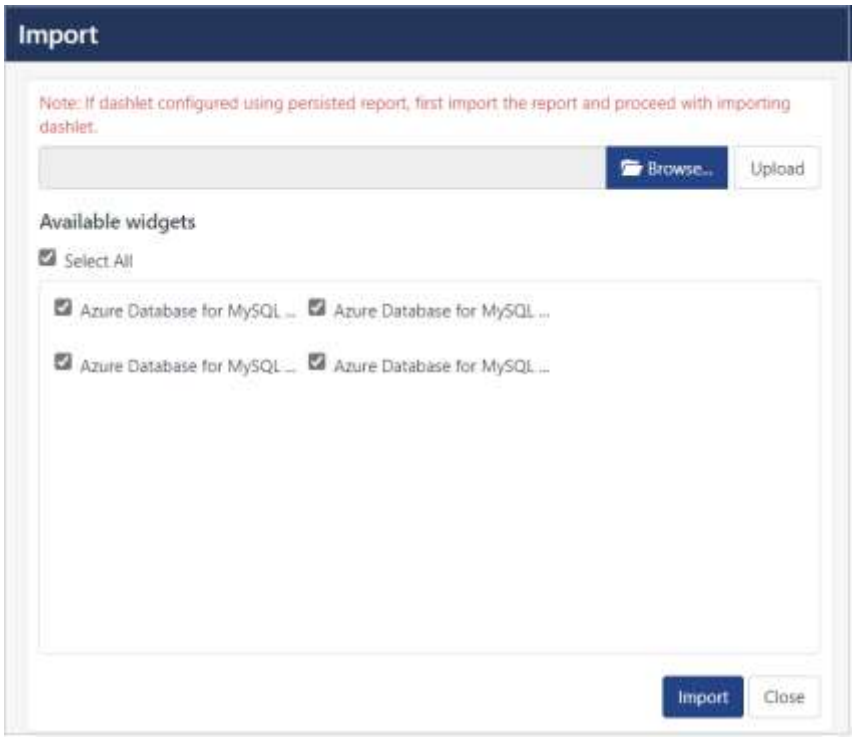
4.6 Dashboard

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

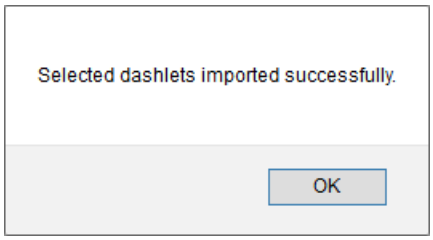
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_ Azure Database for MySQL.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.

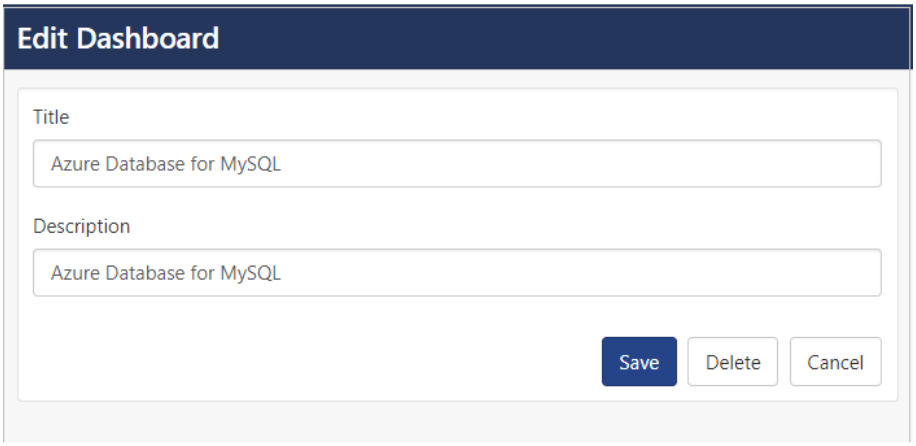


5. The EventTracker displays the success message on successfully importing the dashlet files.



6. Then, in the **My Dashboard** interface, click the **Add** button to add the 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 Database for MySQL**), click the **Configuration** button to add the Azure Database for MySQL dashlets.

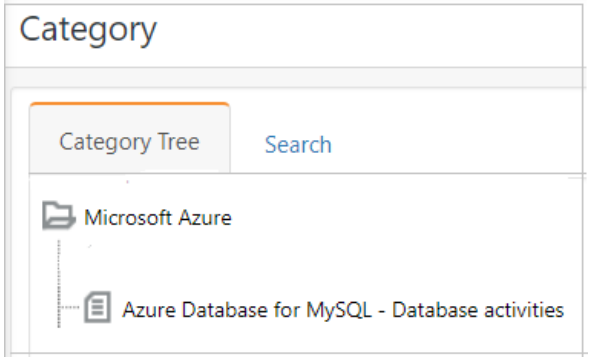
9. Search and select the newly imported dashlets and click **Add**.

5 Verifying Azure Database for MySQL Knowledge Packs in EventTracker

5.1 Category

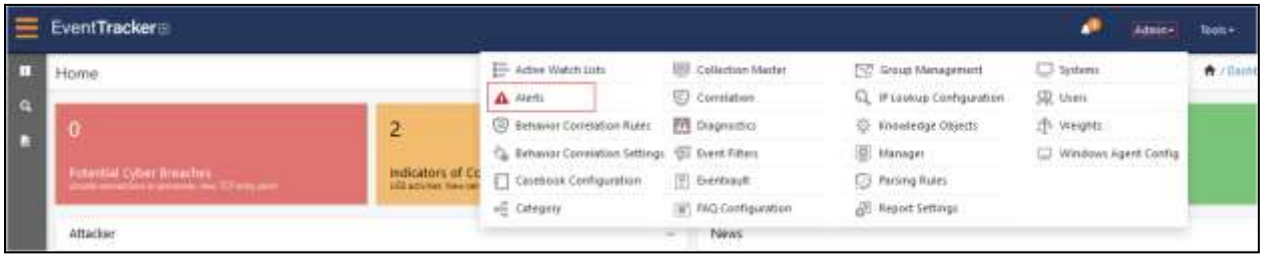
1. In the **EventTracker** web interface, hover over the **Admin** menu and click **Category**.

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



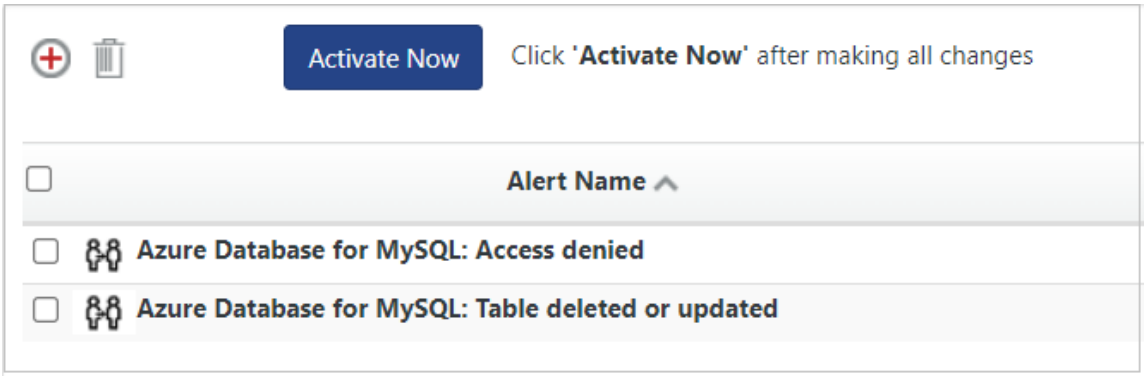
5.2 Alerts

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



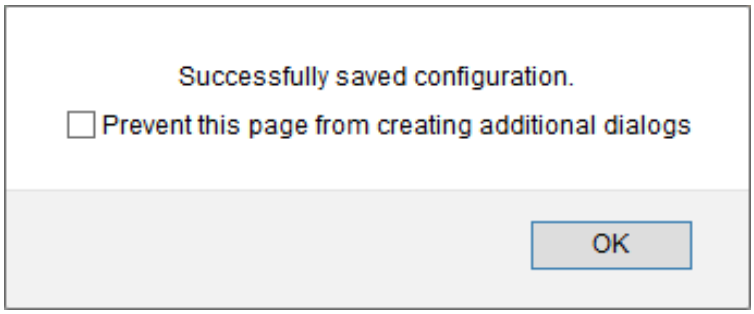
2. In the **Alerts** interface, type **Azure Database for MySQL** in the search field, and click the **Search** button.

3. The **Alerts** interface will display all the imported **Azure Database for MySQL** alerts.



4. To activate the imported alerts, click **Active**, 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

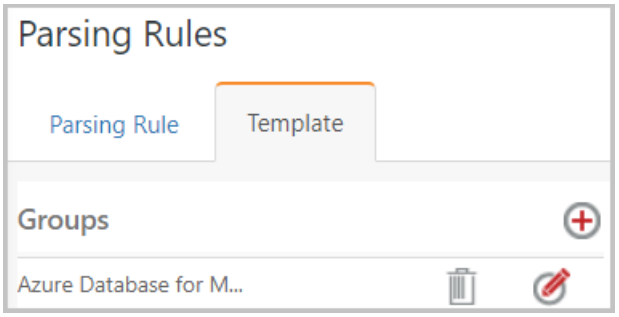
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

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

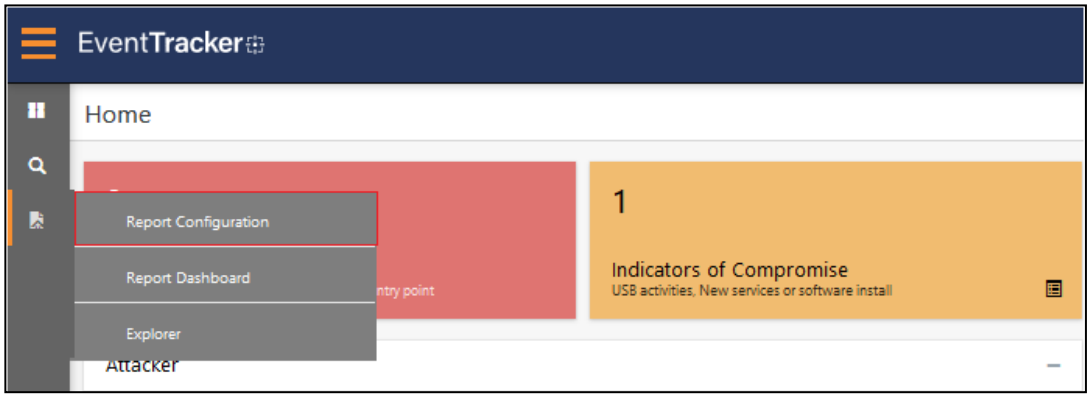
5.3 Token Template

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 Database for MySQL** group folder to view the imported Token template.

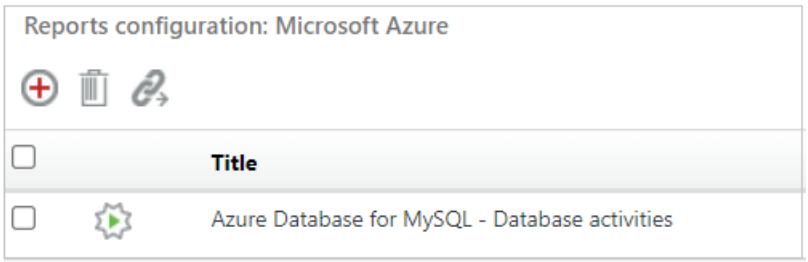


5.4 Reports

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

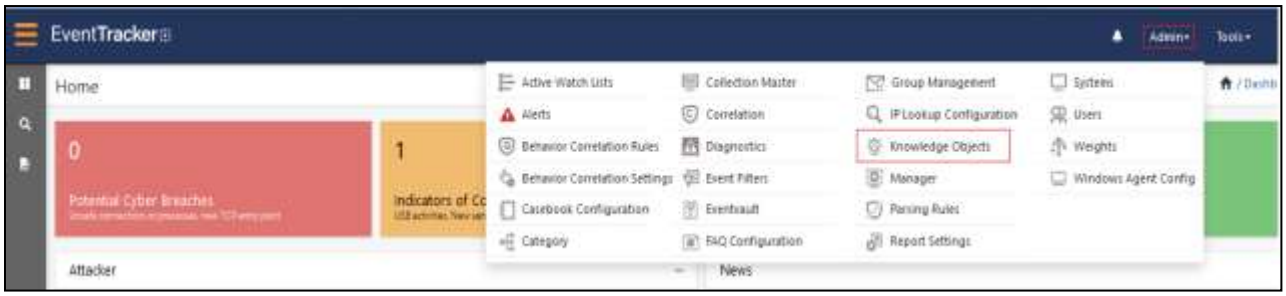


2. In the **Reports Configuration** interface, click **Defined**.
3. In the search field, type **Microsoft Azure** and click **Search** to search for the Azure Database for MySQL files.
4. EventTracker displays the reports for Azure Database for MySQL.

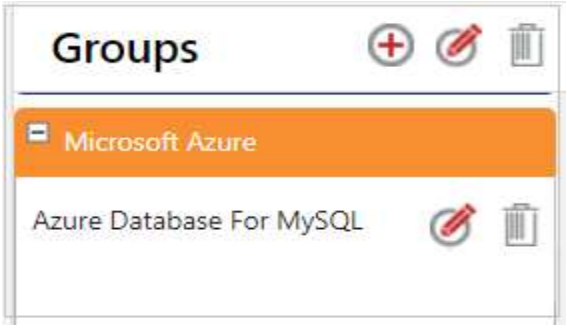


5.5 Knowledge Objects (KO)

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



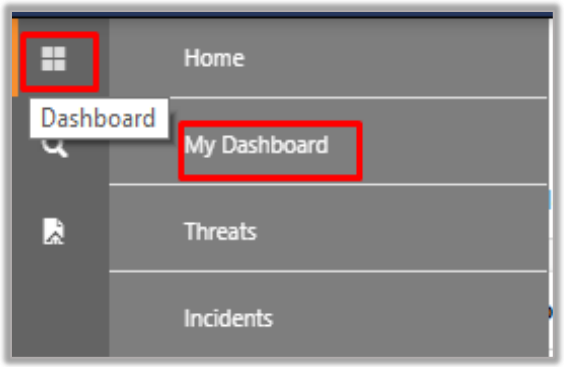
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Microsoft Azure** group to expand and view the imported Knowledge objects.



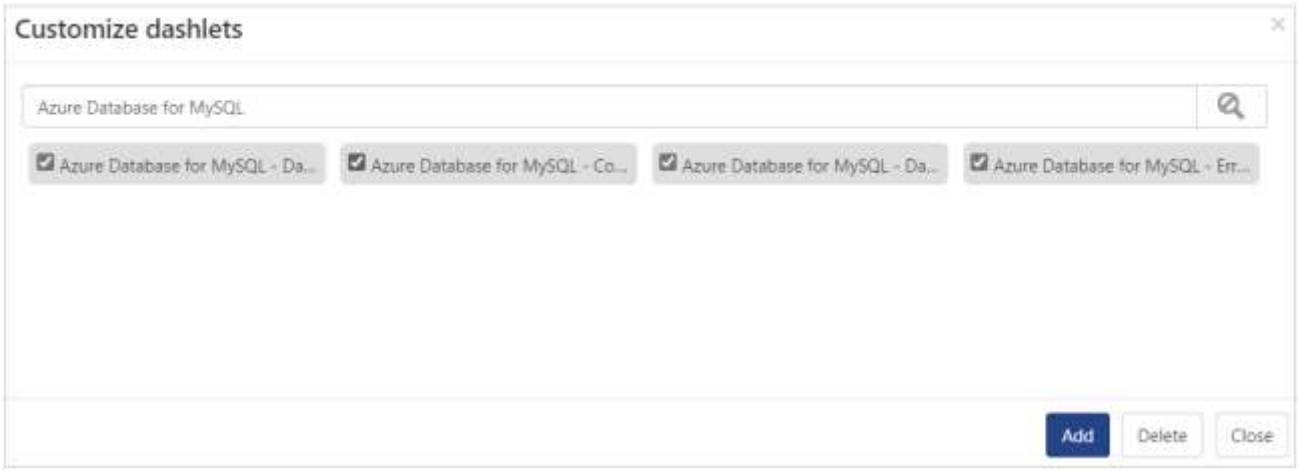
3. Click **Activate Now** to apply the imported Knowledge Objects.

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 Database for MySQL** in the search field.
3. The following Azure Database for MySQL 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