Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating SQL Server on Azure with EventTracker

Publication Date:

March 29, 2022

Abstract

This guide provides instructions to retrieve the **SQL Server on Azure** events via the Azure Event Hub and then configure the **Azure function app** to forward the logs to EventTracker. After EventTracker receives the logs from the Event Hub, then the reports, dashboard, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **the SQL Server on Azure.**

Audience

The Administrators who are assigned the task to monitor the **SQL Server on Azure** events using EventTracker.

Table of Contents

1. Overview

SQL Server on Azure gets a high-performing, unified SQL platform built on the industry-leading SQL Server engine with limitless scalability and intelligent performance and security. Migrate without the need to redesign your apps, improve the performance of the existing apps, and build highly scalable cloud services by switching to Azure—the best cloud destination for your mission-critical SQL Server workloads. EventTracker helps to monitor events from the SQL Server on Azure. Its dashboard and reports will help you track, SQL server activity with the performed statement, actions performed with session Id for a better understanding of database action flow which potentially leads to data loss and manipulation of organization decisions, functions.

2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.

3. Configuring SQL Server on Azure to Forward Logs to EventTracker

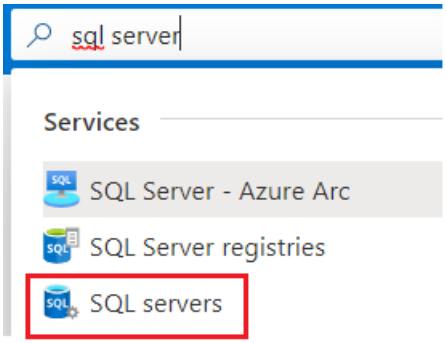
SQL Server on Azure can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

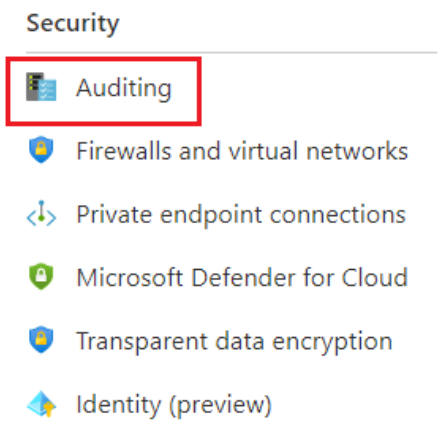
Refer to the configuration of the Azure function app to forward the logs to EventTracker.

3.2 Configuring SQL Server on Azure to stream events to Event Hubs

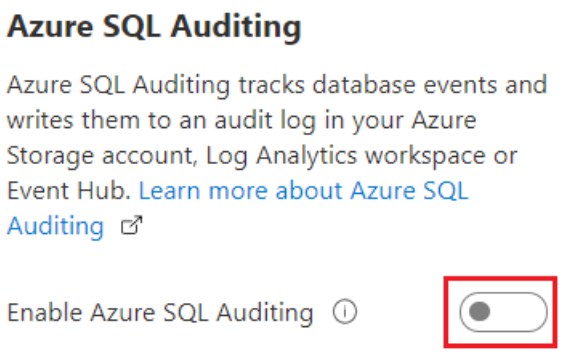
1. Login to portal.azure.com using the Admin account and create an event hub namespace, if not created.
2. Search and select **SQL Server** from **All services**.



3. From the left panel under **Security** select **Auditing**.



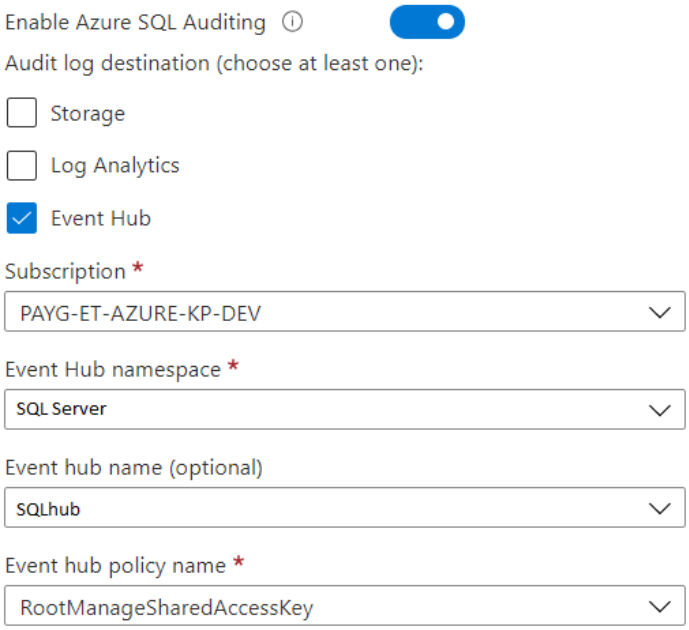
4. **Enable** Azure SQL Auditing.



5. Provide the inputs.

   In the **Audit log Destination** section, check **Event Hubs** and then choose the following options.

   - **Subscription:** Select the desired Azure subscription.
   - **Event Hub namespace:** Select the Event Hubs namespace.
   - **Event Hub name:** Select Event Hub created under the Event Hubs namespace.
   - **Event Hub policy name:** Select the Event Hub policy.



6. Click **OK/Save.**

4. EventTracker Knowledge Packs

After the logs are received by the EventTracker Manager, then the Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs (KPs) are available in EventTracker to support the SQL Server on Azure.

4.1 Alerts

- **Azure SQL Server: Database level activity -** This alert is triggered when the user tries to create, alter, backup, delete, and perform more actions at the database level on the SQL Server.
- **Azure SQL Server: Permission granted or revoked or denied-** This alert is triggered when the user tries permission actions such as a grant, revoke, and deny performed on the SQL Server.
- **Azure SQL Server: Role created or deleted or modified-** This alert is triggered when the user performs create, modify, and delete actions for the role on the SQL Server.
- **Azure SQL Server: Schema created or deleted or modified-** This alert is triggered when the user performs create, modify, and delete actions for the schema on the SQL Server.
- **Azure SQL Server: Stored procedure created or deleted or modified-** This alert is triggered when the user performs create, modify, and delete actions for the store procedure on the SQL Server.
- **Azure -SQL Server: Table/view created or deleted or modified-** This alert is triggered when the user performs create, modify, and delete actions for the table/view on the SQL Server.
- **Azure SQL Server: Trigger created or deleted or modified-** This alert is triggered when the user performs create, modify, and delete actions for trigger on the SQL Server.
- **Azure SQL Server: User-created or deleted or modified or password changed-** This alert is triggered when the user performs password change, create, modify, and delete actions for the user on the SQL Server.

4.2 Categories

- **Azure SQL Server - Server activities-** This category of the saved search will allow users to parse the events specific to the server activities on the SQL Server.

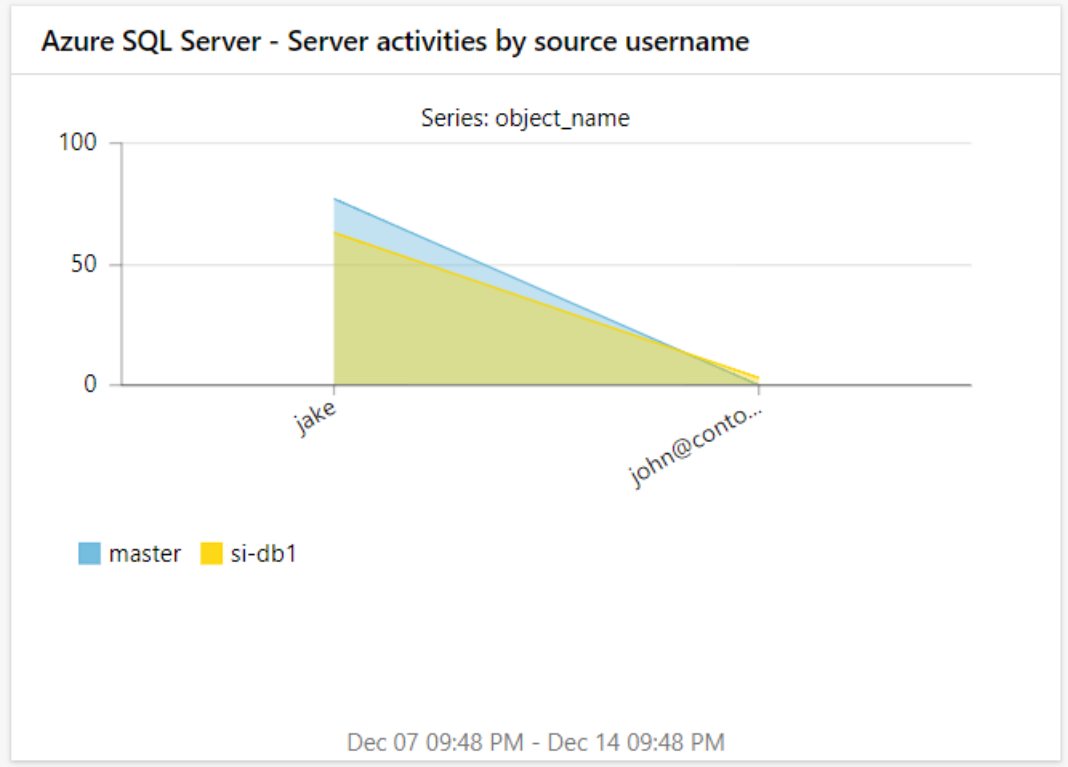
4.3 Reports

- **Azure SQL Server - Server activities:** This report provides a detailed summary of actions performed on the SQL Server. It contains a source IP address, username, database name, server name, statement, session ID, hostname, and more.

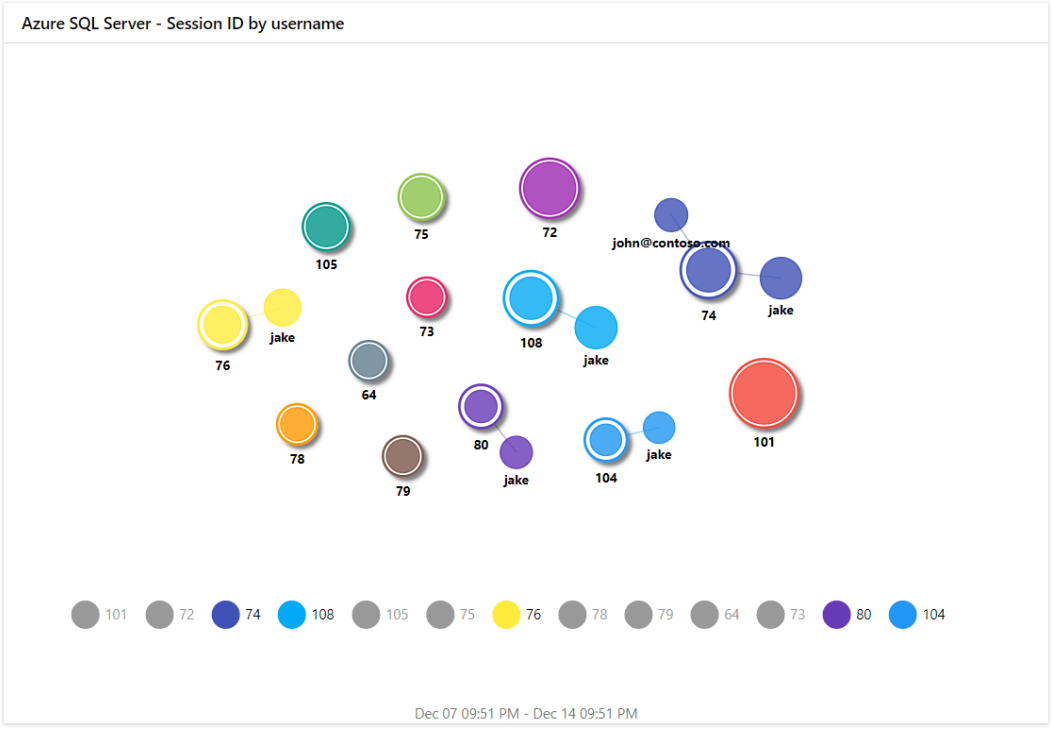
LogTime	Computer	Succeeded	User name	Source IP Address	Databasename	Server name	Object Name	Statement	Action ID	Session ID	Session user name	Resource group
12-11-2021 04:59:49 AM	SQL SERVER-TEST	true	jake@contoso.com	10.62.119.63	DB-Worker	si-ss	DB-Worker	create user Sam with password="*******";	BCM	10	jake@contoso.com	az_con_gp_01
12-11-2021 04:59:49 AM	SQL SERVER-TEST	true	franz@contoso.com	10.12.119.63	DB-Function	si-ss	DB-Function	SELECT @@SPID;	BCM	11	franz@contoso.com	az_con_gp_01
12-11-2021 04:59:49 AM	SQL SERVER-TEST	false	jaffer	10.2.19.63	DB-Function	si-ss	DB-Function	GRANT CONTROL ON USER::john TO Franz;	BCM	15	jaffer	az_con_gp_01

4.4 Dashboards

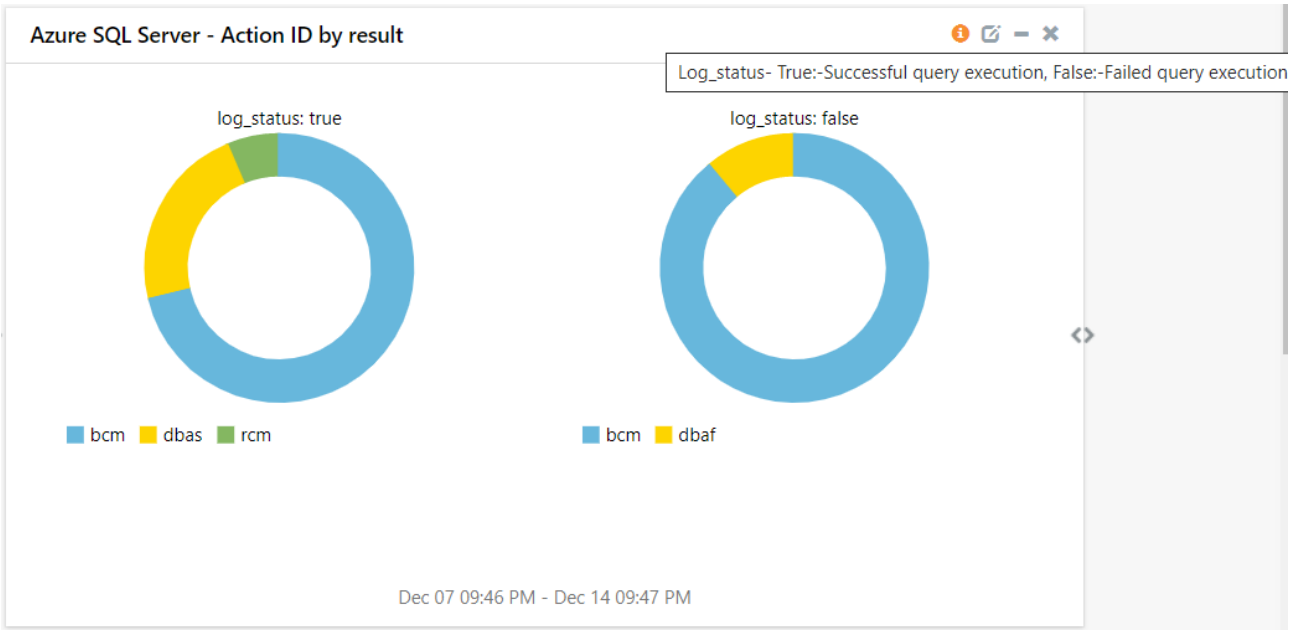
- **Azure SQL Server - Server activities by source username**



- **Azure SQL Server - Session ID by username**



- **Azure SQL Server - Action ID by result**



5. Importing Azure SQL Server Knowledge Packs into EventTracker

NOTE: Import the Knowledge Pack items in the following sequence:

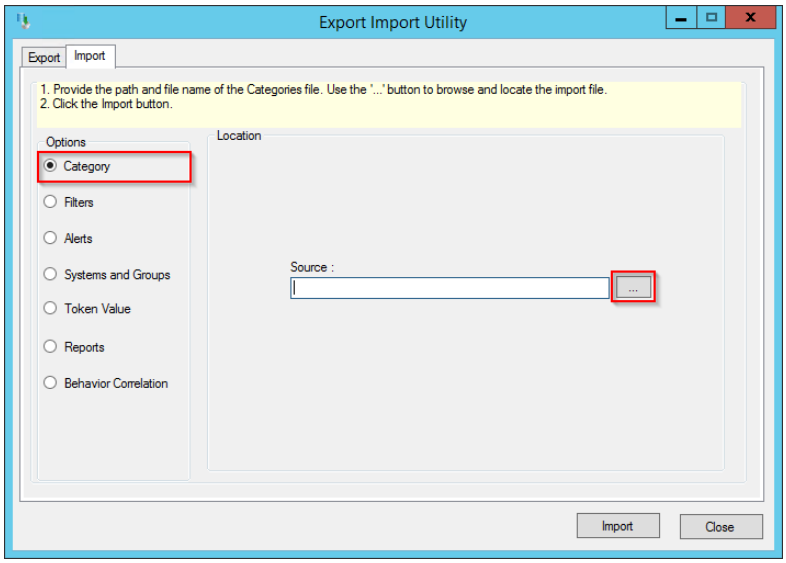
- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards

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

3. Click the **Import** tab.

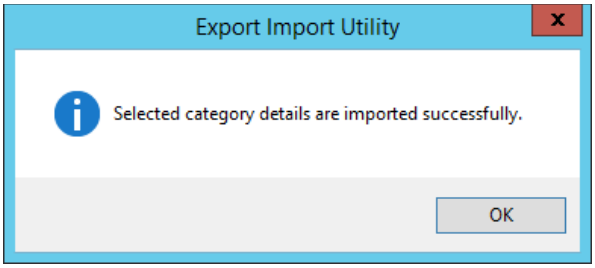
5.1 Categories

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



2. Locate the **Categories_Azure SQL Server.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

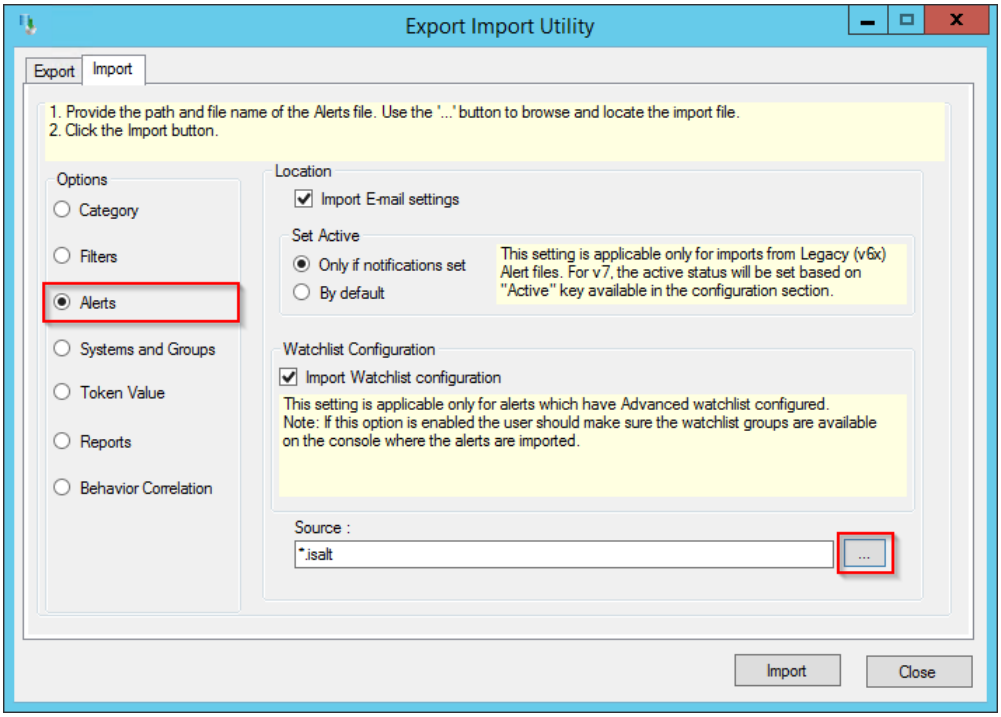
EventTracker displays a success message.



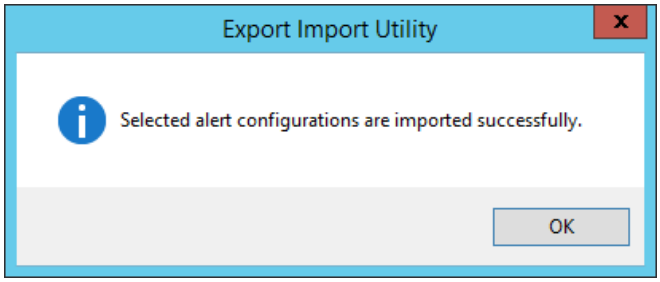
4. Click **OK,** and then click the **Close** button.

5.2 Alerts

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



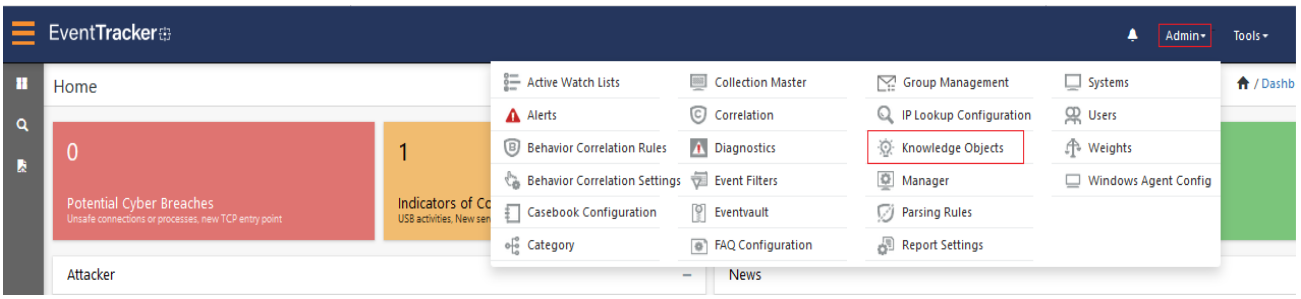
2. Locate the **Alerts_Azure SQL Server.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.
   EventTracker displays a success message.



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

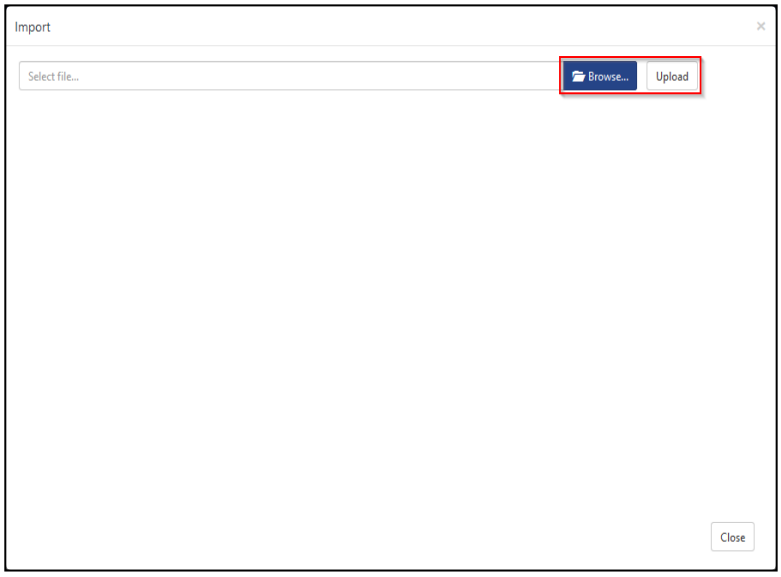
5.3 Knowledge Objects (KO)

1. Click **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.

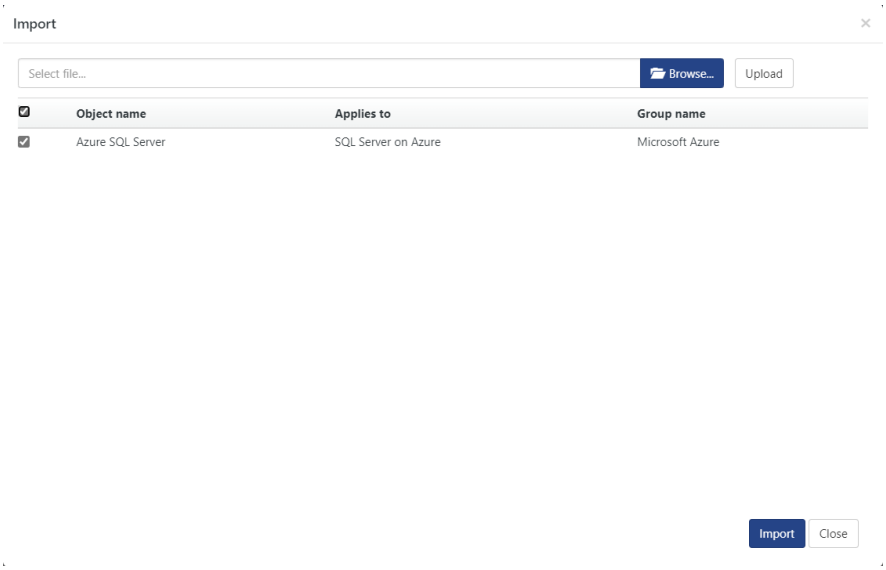


2. Click the **Import** button as highlighted in the below image.

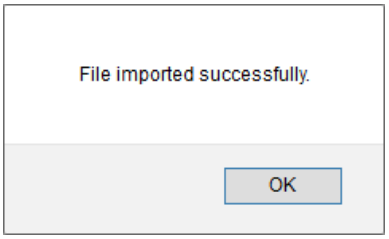
3. Click **Browse**.



4. Locate the file named **KO_Azure SQL Server.etko**.
5. Select the check box and then click the **Import** option.

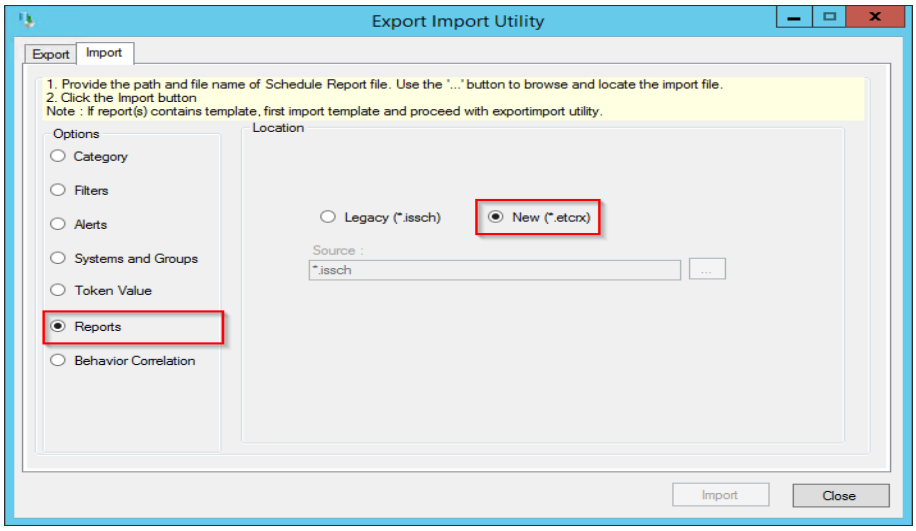


6. The Knowledge Objects (KO) are now imported successfully.

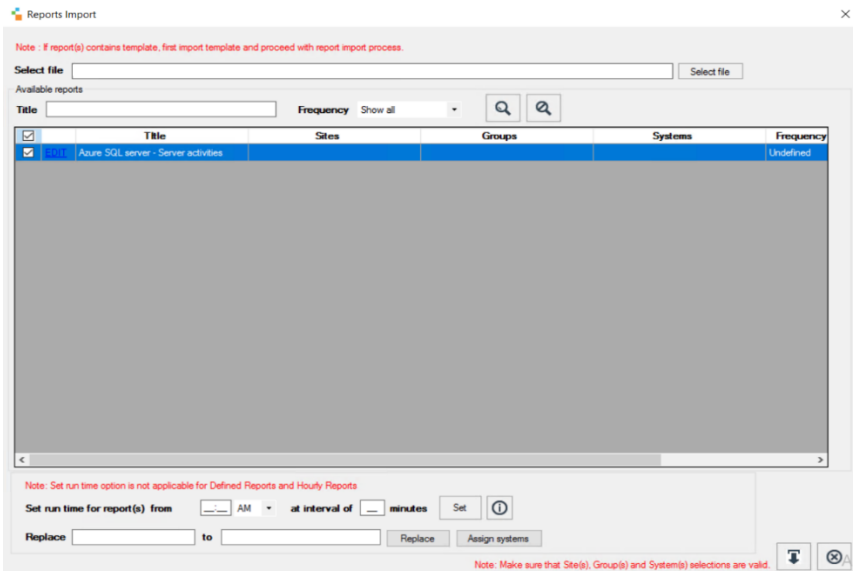


5.4 Reports

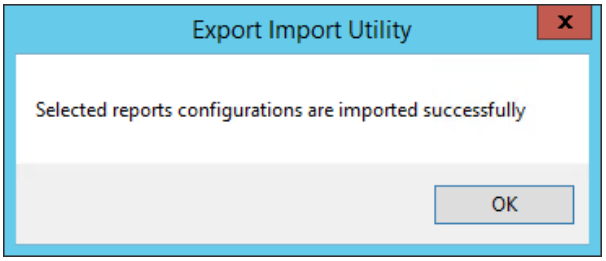
1. Click the **Reports** option and select the **New (*.etcrx)** option.



2. Locate the file named **Reports_ Azure SQL Server.etcrx** and select all the check boxes.



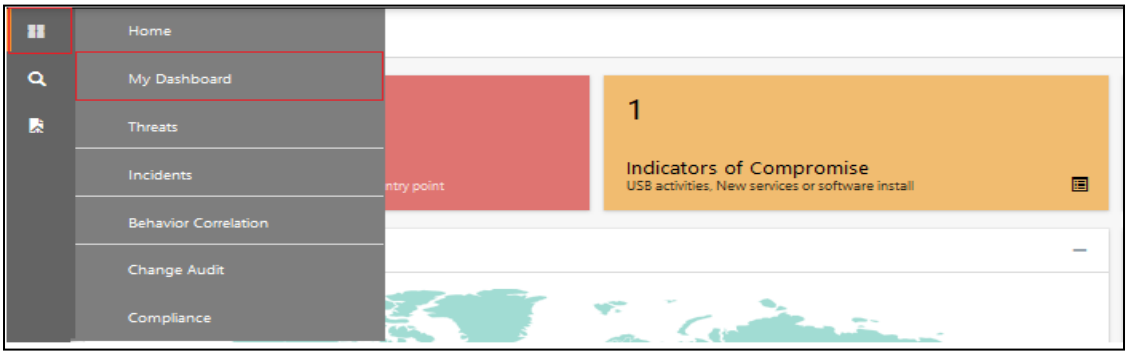
3. Click the **Import** button to import the report. EventTracker displays a success message.



5.5 Dashboards

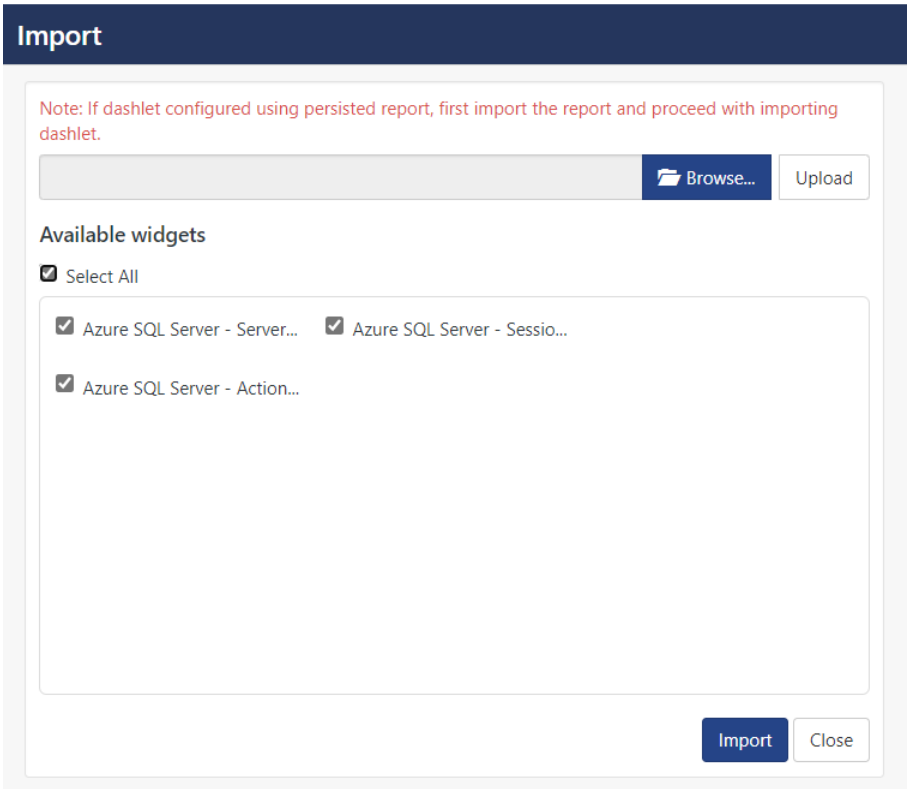
NOTE: Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in a browser and log on.

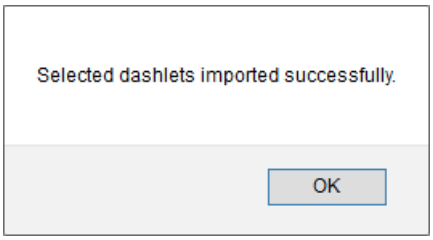


2. Navigate to the **My Dashboard** option.
3. Click the **Import** button as shown below.

4. Import the dashboard file **Dashboards_Azure SQL Server.etwd** and select the **Select All** checkbox**.**
5. Click **Import** as shown below.

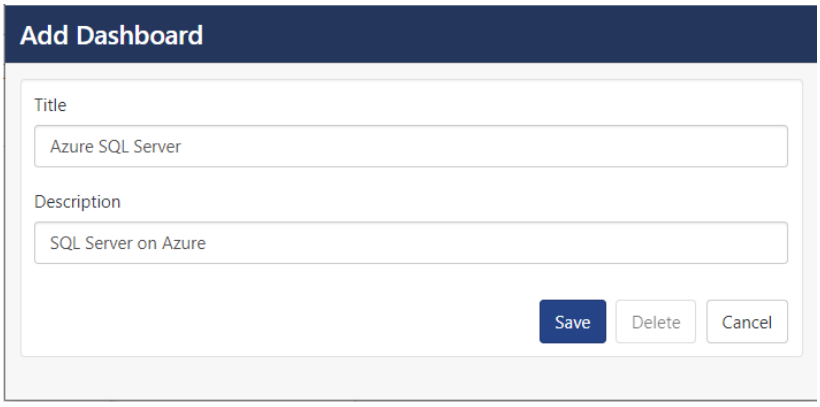


6. Import is now completed successfully.

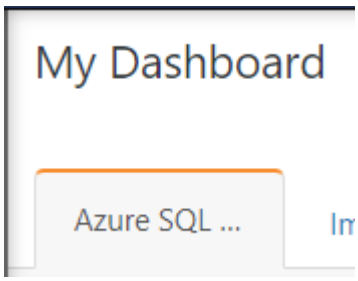


7. In the **My Dashboard** page select ⊕ to add dashboard.

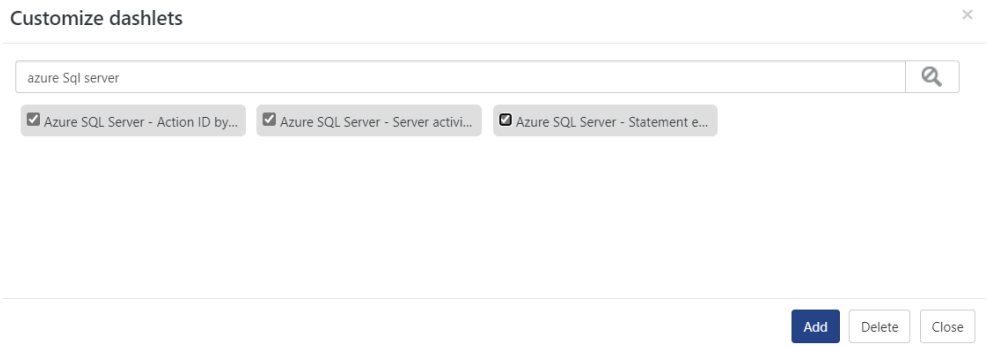
8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.



9. On the **My Dashboard** page select to add dashlets.



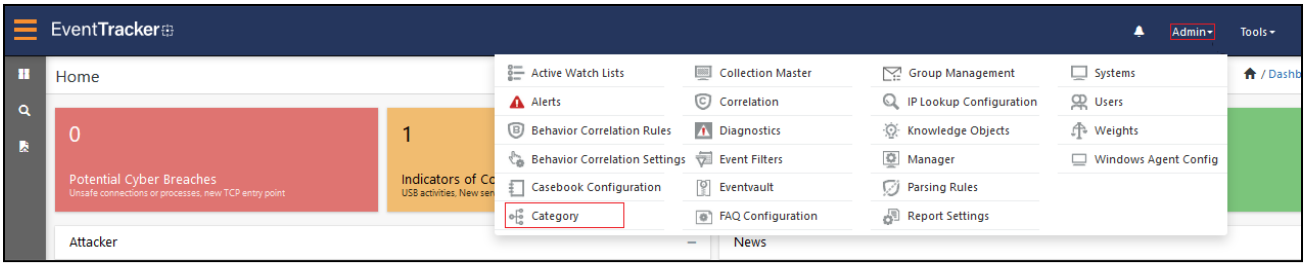
10. Select the imported dashlets and click **Add**.



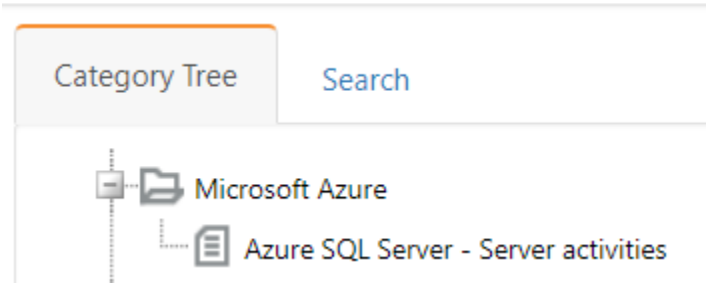
6. Verifying Azure SQL Server Knowledge Packs in EventTracker

6.1 Categories

1. Log onto **EventTracker**.
2. Click the **Admin** dropdown, and then click **Category**.

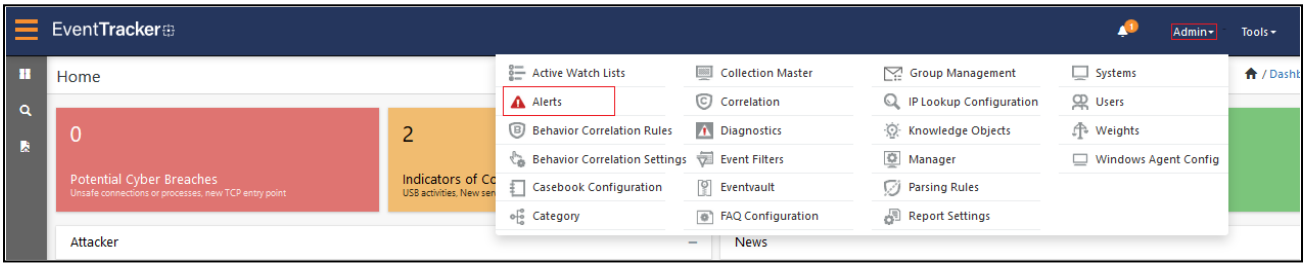


3. In the **Category Tree**, scroll down and expand the **Microsoft Azure** group folder to view the imported category.

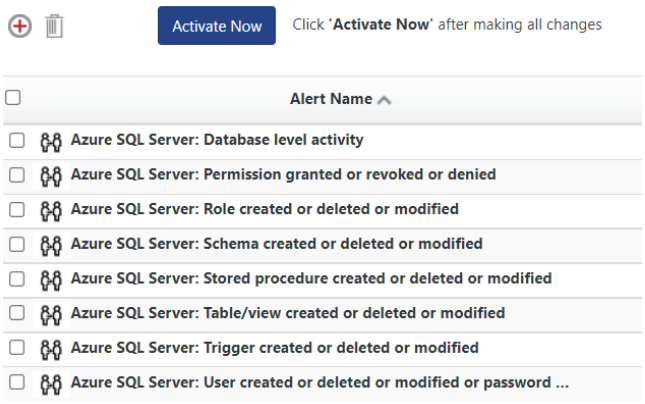


6.2 Alerts

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

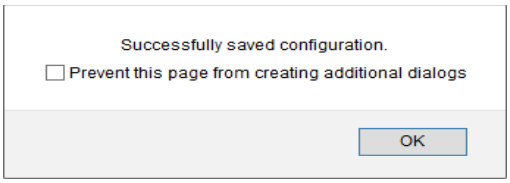


3. In the **Search** box, type **Azure SQL Server**, and then click the **Go** button.
   The Alert Management page will display the imported alert.



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

   EventTracker displays a message box.

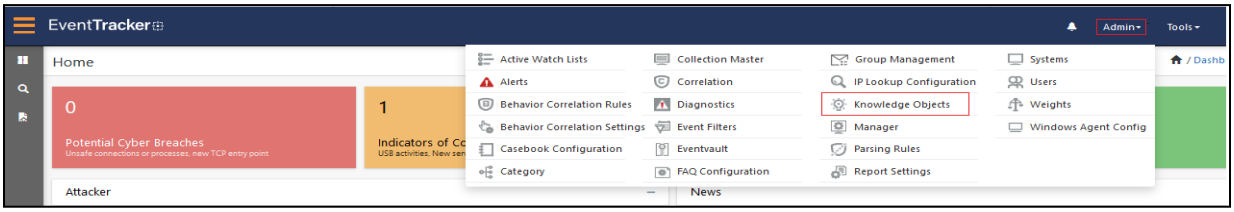


5. Click **OK**, and then click the **Activate Now** button.

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

6.3 Knowledge Objects

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

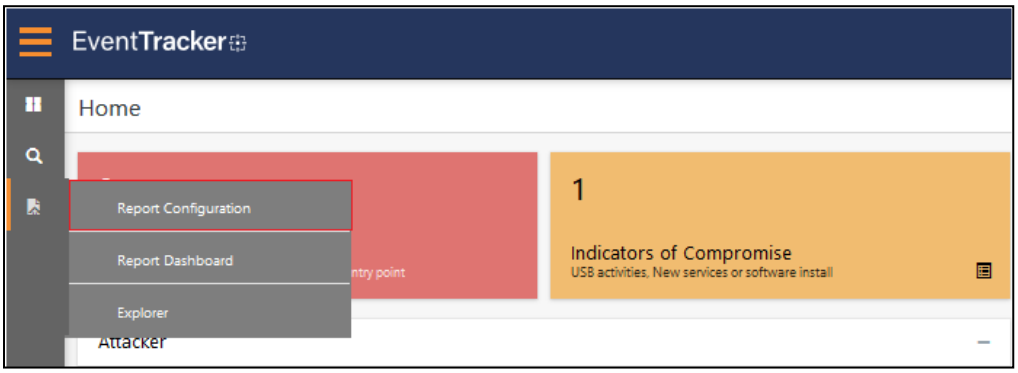


2. In the Knowledge Objects tree, expand the **Microsoft Azure group** folder to view the imported Knowledge Objects.

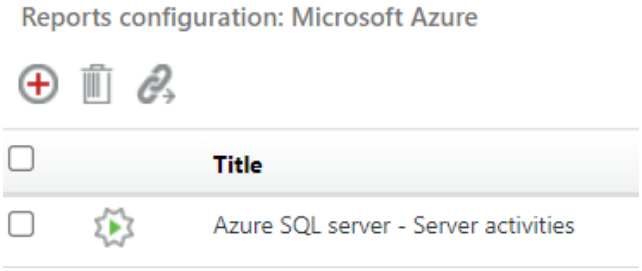
3. Click **Activate Now** to apply the imported Knowledge Objects.

6.4 Reports

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

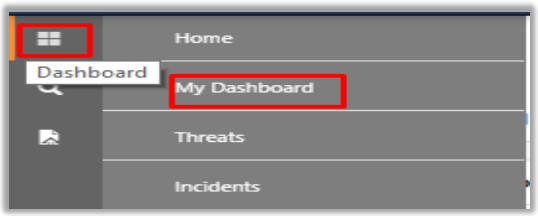


2. In the **Report Configuration** pane, select the **Defined** option.
3. Click the **Microsoft Azure** group folder to view the imported reports.

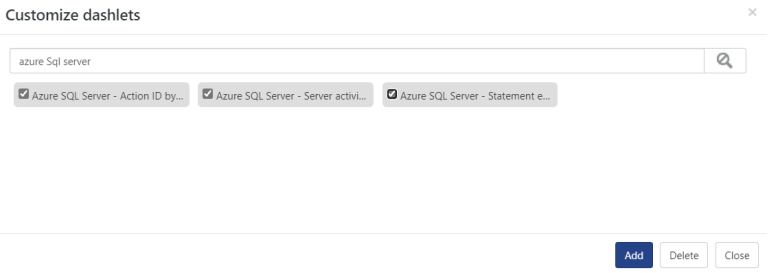


6.5 Dashboards

1. In the EventTracker web interface, click the **Home** Button and select **My Dashboard**.



2. Click **Search** for the **Azure SQL Server.** You will see the following screen.



About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

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