Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating Azure Storage with EventTracker

Publication Date:

March 30, 2022

Abstract

This guide provides instructions to retrieve the **Azure Storage** 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, 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 **Azure Storage.**

Audience

The Administrators who are assigned the task to monitor the **Azure Storage** events using EventTracker.

Table of Contents

1. Overview

Azure Storage platform is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers highly available, massively scalable, durable, and secure storage for a variety of data objects in the cloud.

EventTracker helps to monitor events from Azure Storage. Its dashboard and reports will help you track, user actions in Azure Storage, geo-location to modify and delete actions performed, and identity access to the storage with status code, which will help to identify manipulations, and malicious activities which may lead to potential data destruction.

2. Prerequisites

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

3. Configuring Azure Storage to Forward Logs to EventTracker

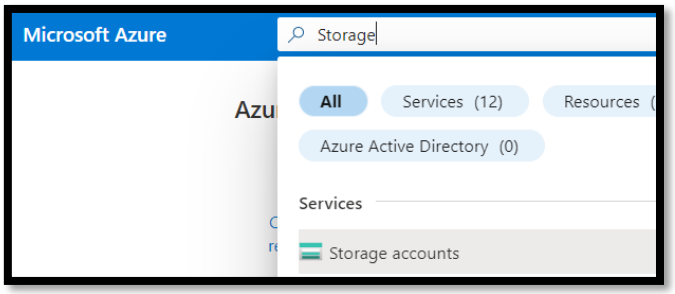
Azure Storage can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

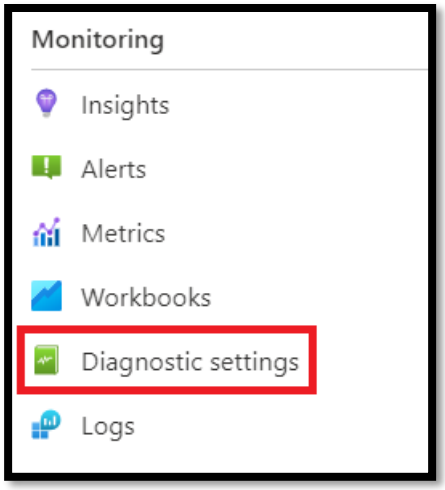
Refer to the Configuration of the Azure function app to forward the logs to EventTracker.

3.2 Configuring Azure Storage to stream events to Event Hub

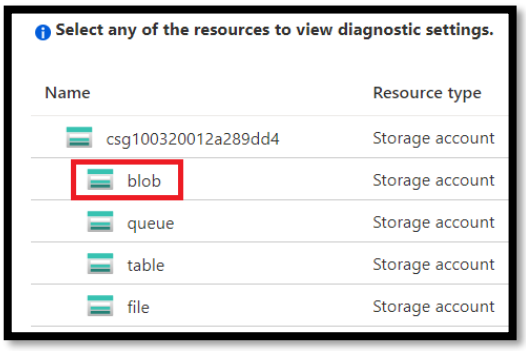
1. Login to portal.azure.com using the Admin account and create an event hub namespace, if not created.
2. Search and select **Storage** from **All services**.



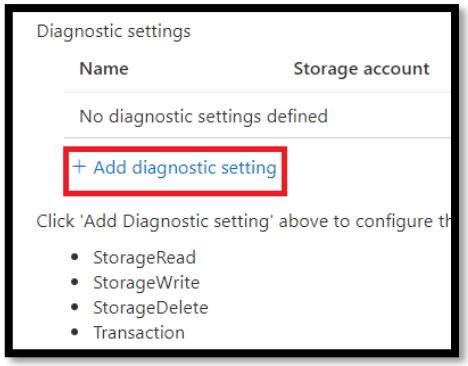
3. Open the storage account which is needed to be monitored.
4. From the left panel under **Monitoring**, select **Diagnostics settings**:



5. Click **Blob.**



6. Click **Add diagnostics settings**.

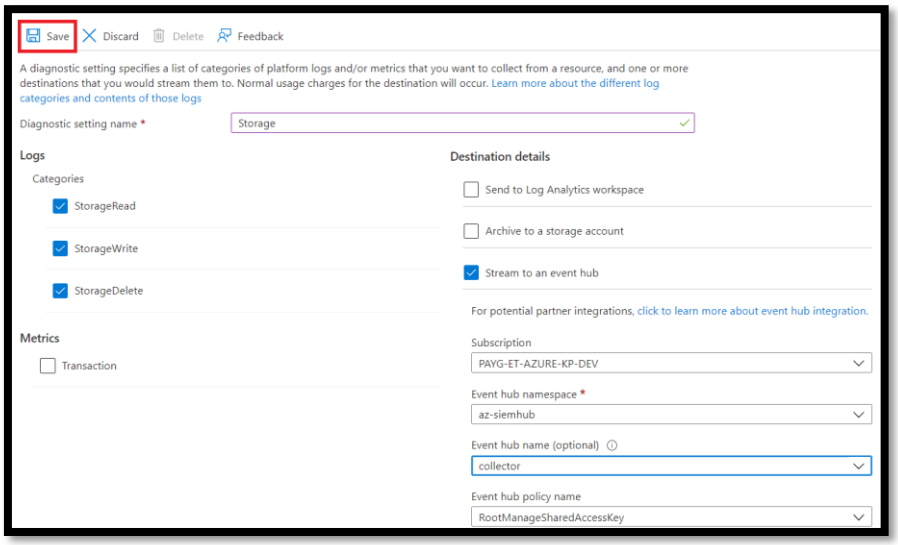


7. Provide the inputs.

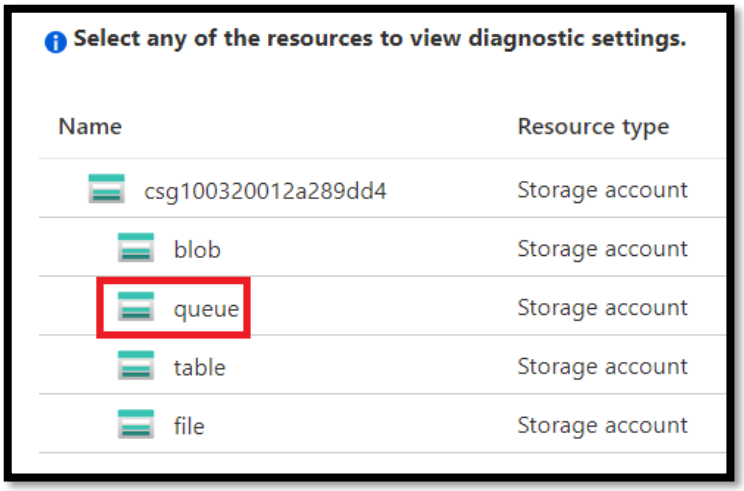
   Diagnostics settings name, such as **Storage**.
   Select **log** type, Storage Read, Storage Write, and Storage Delete
   In the **Destination details** section, select **stream to an Event Hub** and then choose the following options.

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

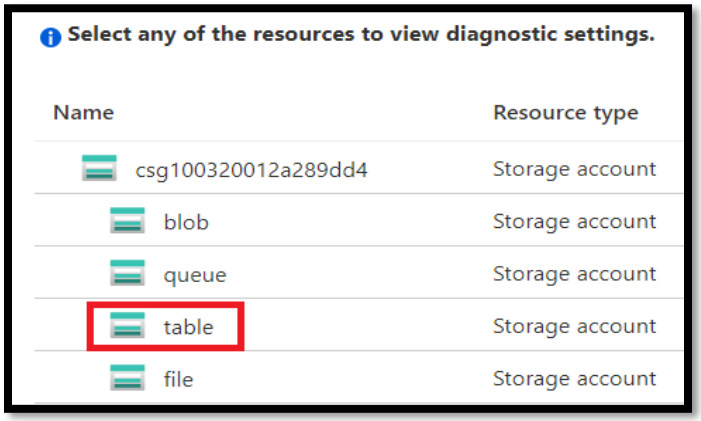
8. Click **Save.**



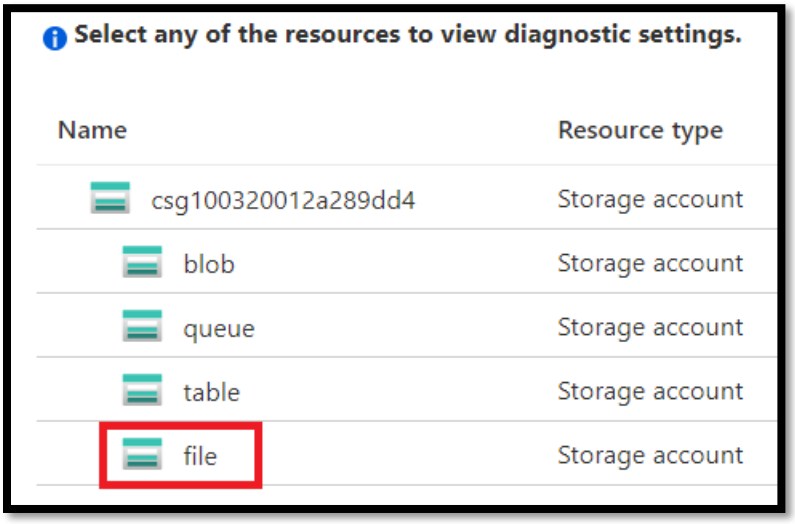
9. Click **Queue** and repeat steps 6, 7, and 8.



10. Click **Table** and repeat steps 6, 7, and 8.



11. Click **file** and repeat steps 6, 7, and 8.



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 Azure Storage.

4.1 Alerts

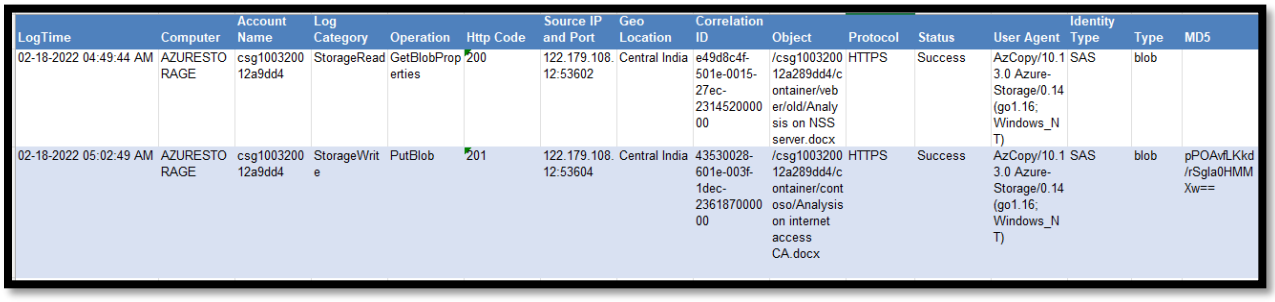
- **Azure Storage: Modify or delete action performed:** This alert indicates that a modify or delete action is detected in Azure Storage.

4.2 Categories

- **Azure Storage – Storage activities:** This category of the saved search will allow users to parse events that are specific to the Storage activities in Azure Storage.

4.3 Reports

- **Azure Storage – Storage activities:** This report provides a detailed summary of Storage activities in Azure Storage. It contains a source IP address, account name, user agent, status code, port number, protocol, operation, and more.

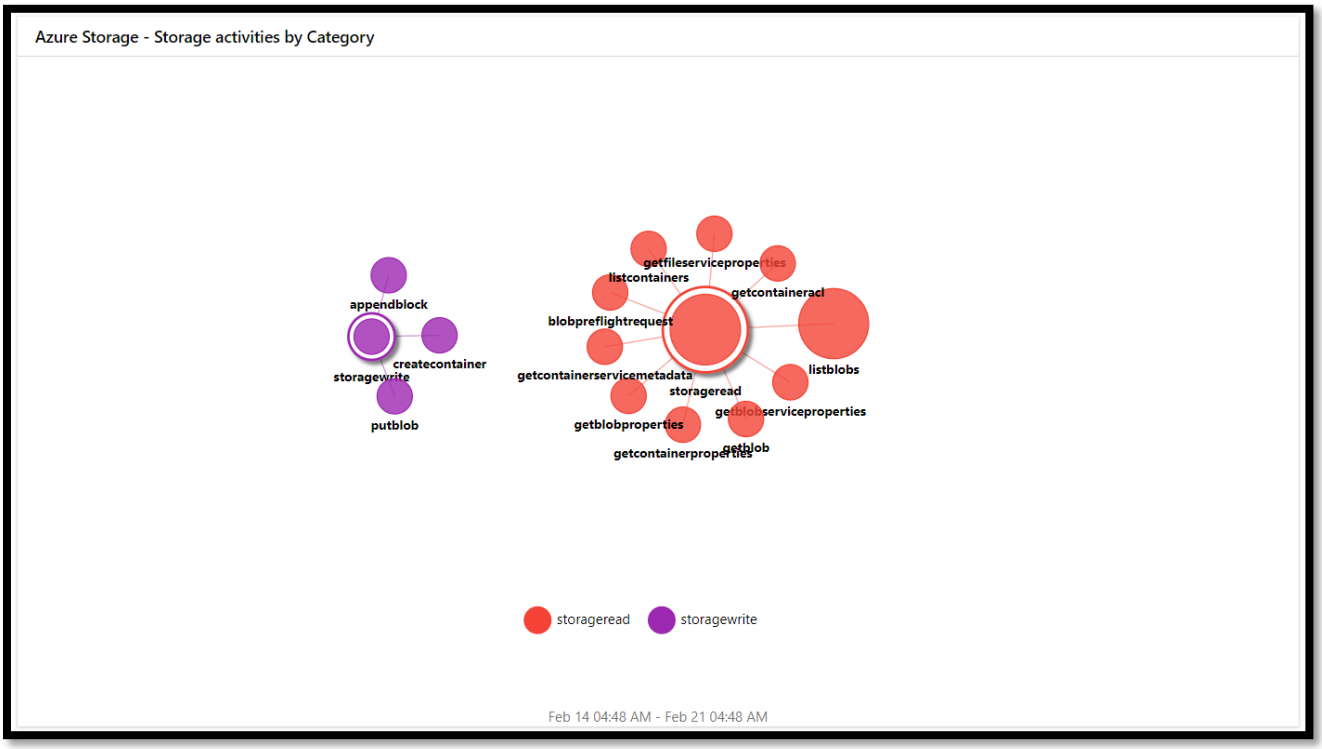


LogTime	Computer	Account Name	Log Category	Operation	Http Code	Source IP and Port	Geo Location	Correlation ID	Object	Protocol	Status	User Agent	Identity Type	Type	MD5
02-18-2022 04:49:44 AM	AZURESTORAGE	csg100320012a9dd4	StorageRead	GetBlobProperties	200	122.179.108.12:53602	Central India	e49d8c4f-501e-0015-27ec-231452000000	/csg100320012a289dd4/container/veber/old/Analysis on NSS server.docx	HTTPS	Success	AzCopy/10.13.0 Azure-Storage/0.14 (go1.16; Windows_NT)	SAS	blob	
02-18-2022 05:02:49 AM	AZURESTORAGE	csg100320012a9dd4	StorageWrite	PutBlob	201	122.179.108.12:53604	Central India	43530028-601e-003f-1dec-236187000000	/csg100320012a289dd4/container/contoso/Analysis on internet access CA.docx	HTTPS	Success	AzCopy/10.13.0 Azure-Storage/0.14 (go1.16; Windows_NT)	SAS	blob	pPOAvfLKkd/rSgla0HMMXw==

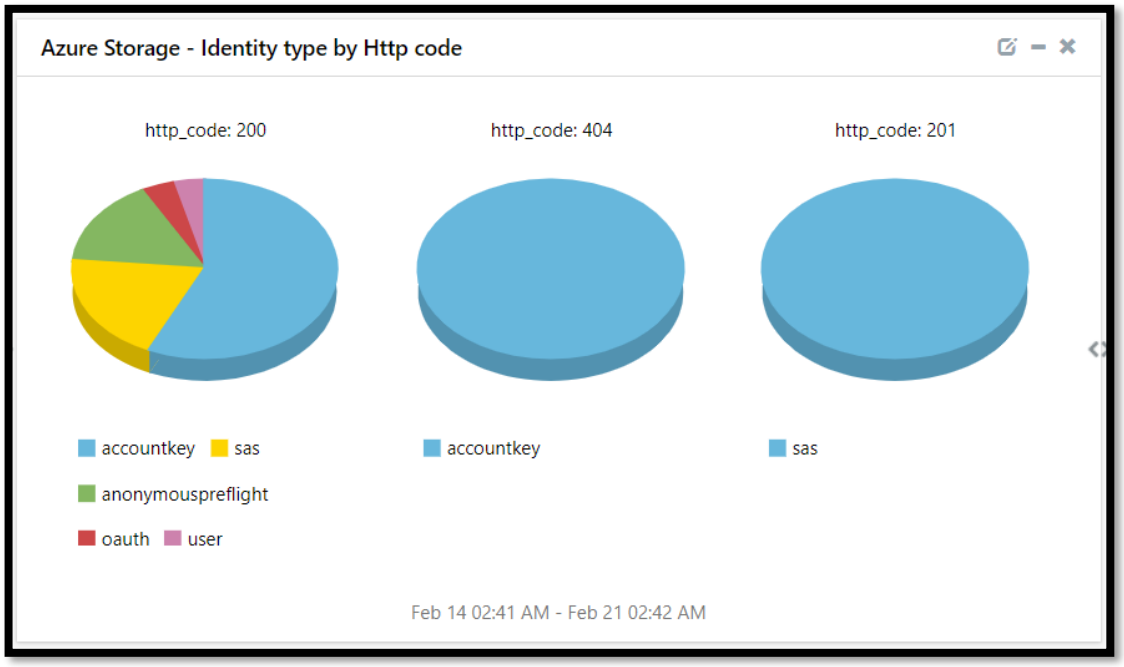
4.4 Dashboards

- **Azure Storage - Modify and delete action by Geo location**

- **Azure Storage - Storage activities by Category**



- **Azure Storage - Identity type by Http code**



5. Importing Azure Storage Knowledge Packs into EventTracker

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

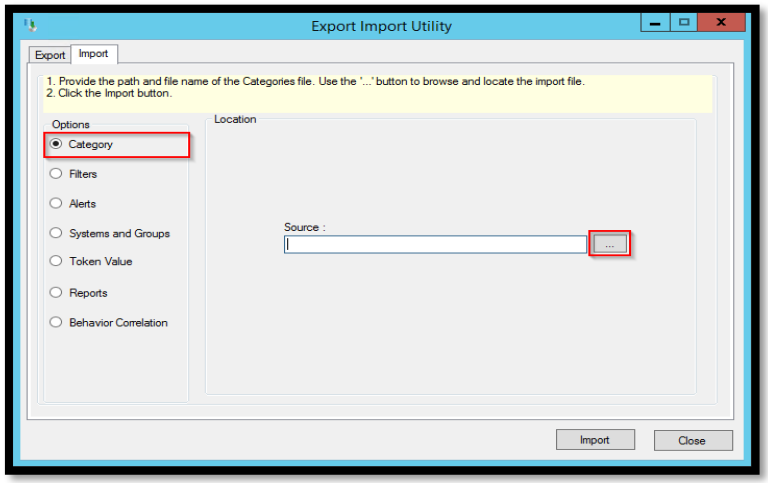
- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards

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

3. Click the **Import** tab.

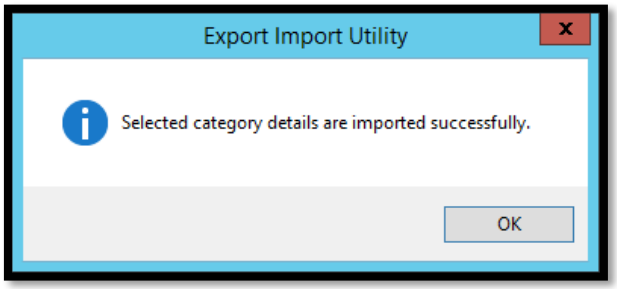
5.1 Categories

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



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

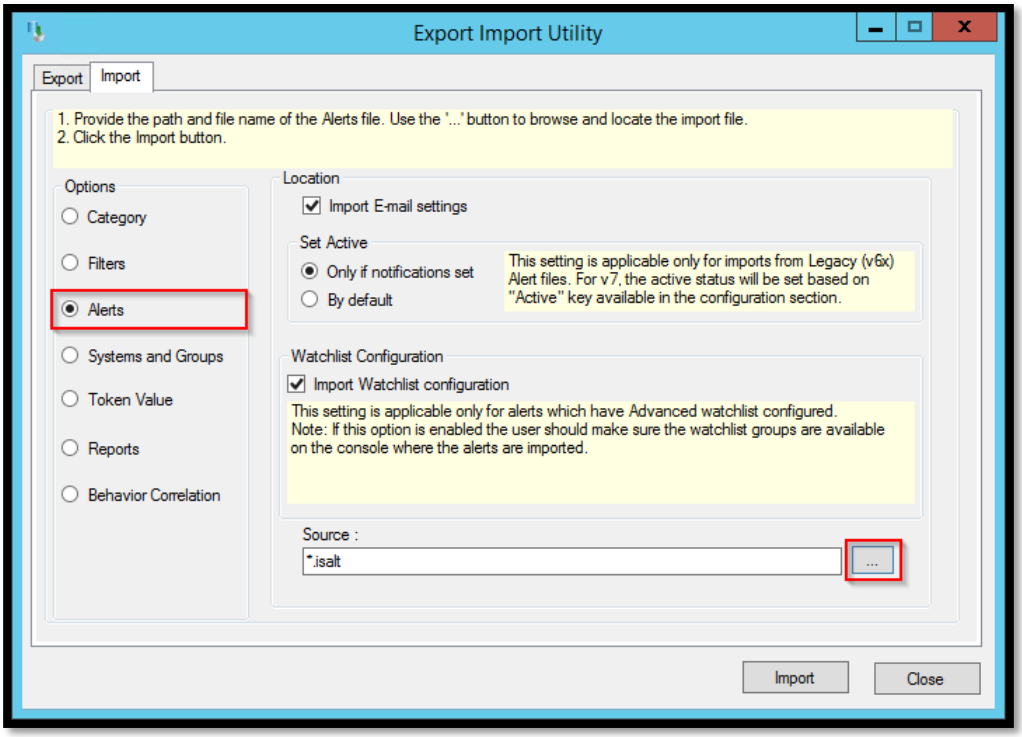
EventTracker displays a success message.



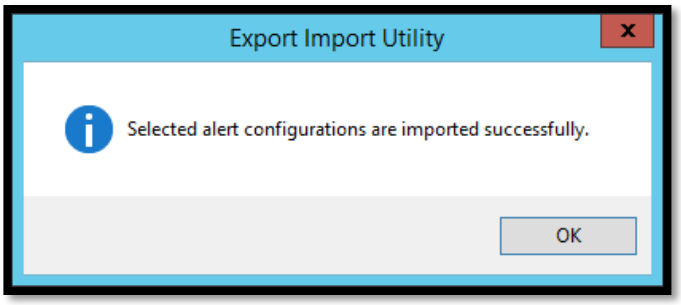
4. Click **OK,** and then click the **Close** button.

5.2 Alerts

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



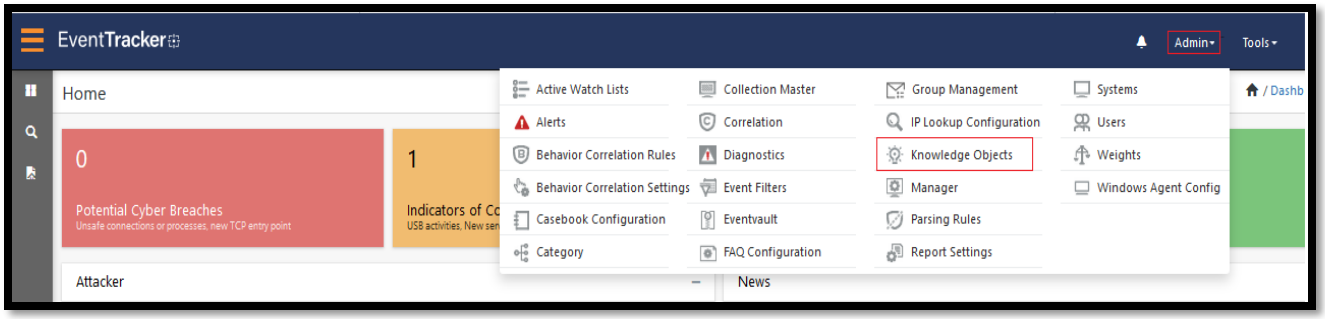
2. Locate the **Alerts_ Azure Storage.isalt** file, and then click the **Open** button.
3. To import the alerts, click the **Import** button.
   EventTracker displays a success message.



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

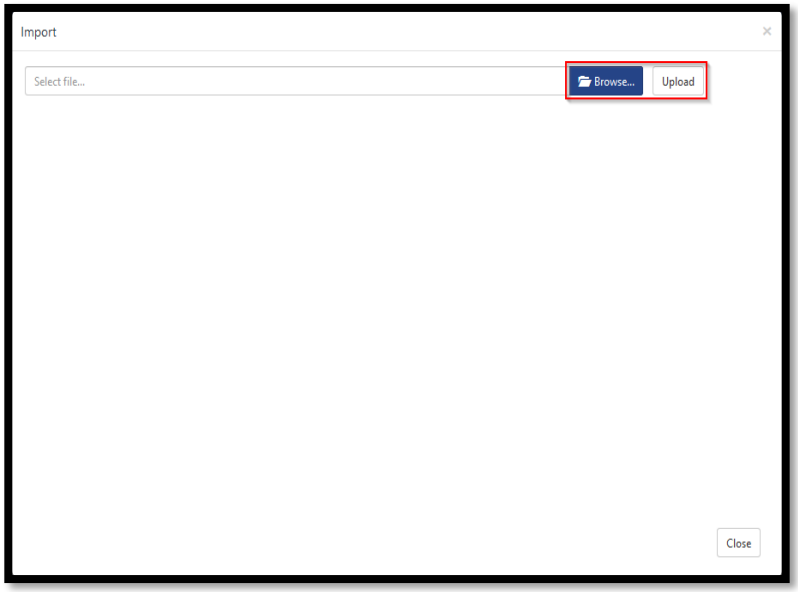
5.3 Knowledge Objects (KO)

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

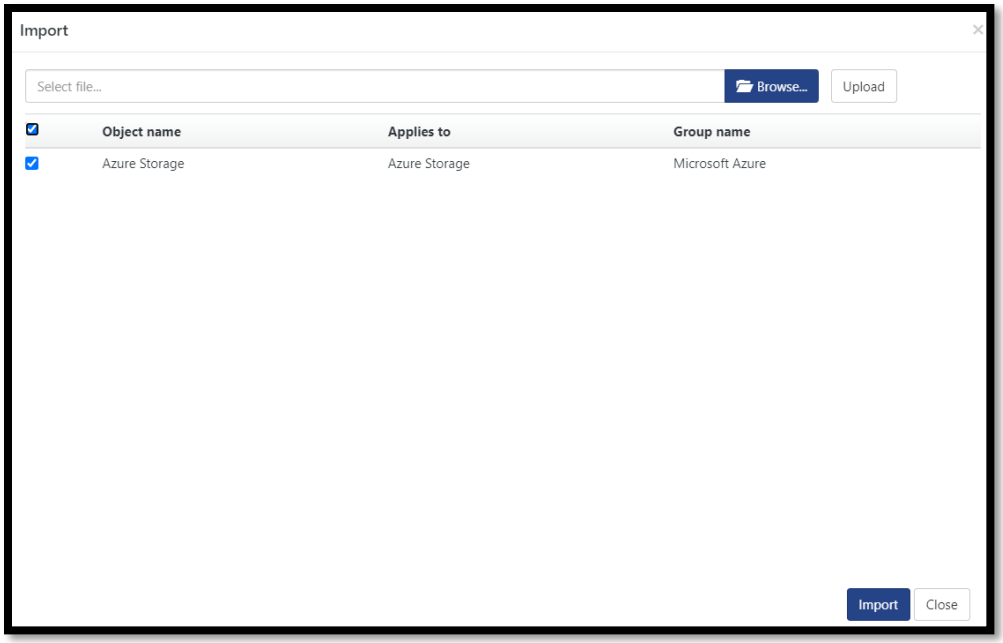


2. Click the **Import** button as highlighted in the below image.

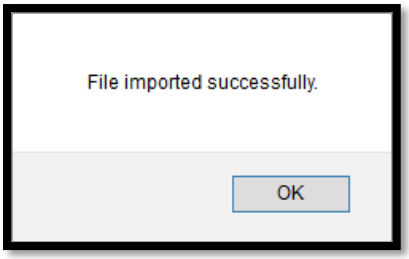
3. Click **Browse**.



4. Locate the file named **KO_ Azure Storage.etko**.
5. Select the check box and then click the **Import** option.

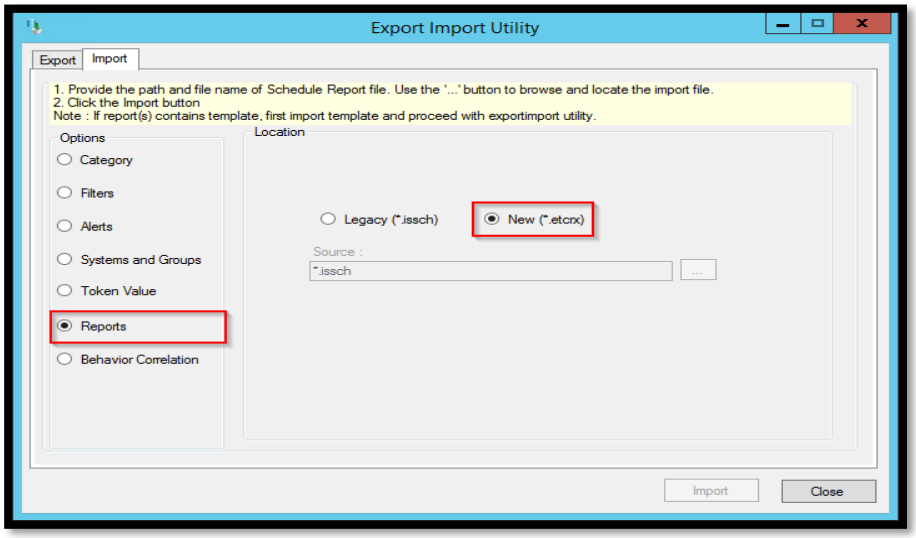


6. The Knowledge Objects (KO) are now imported successfully.

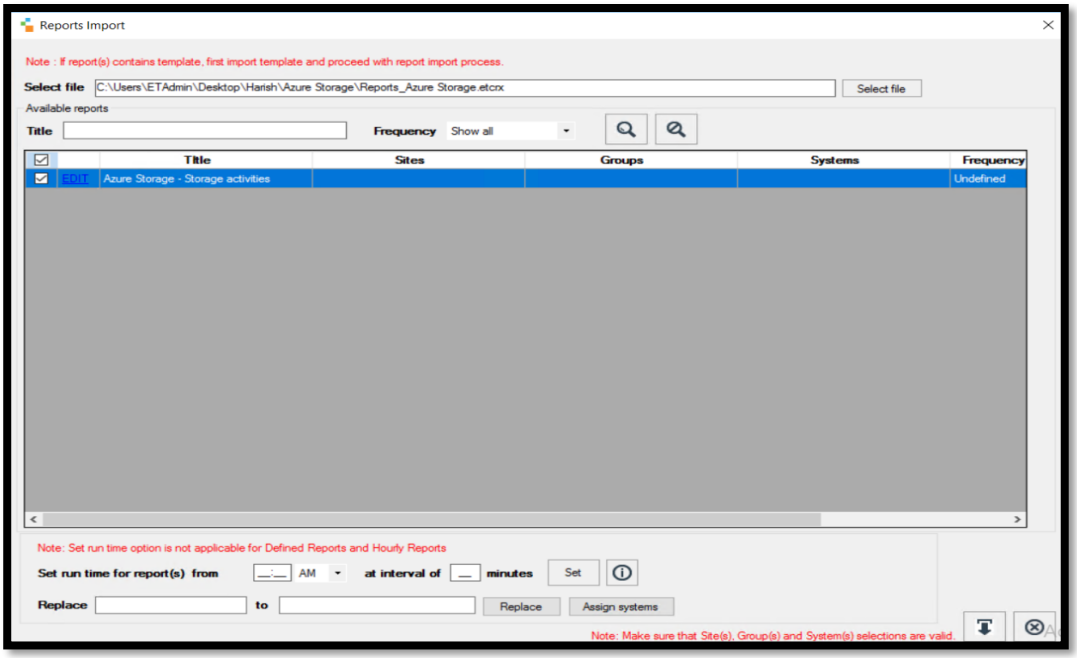


5.4 Reports

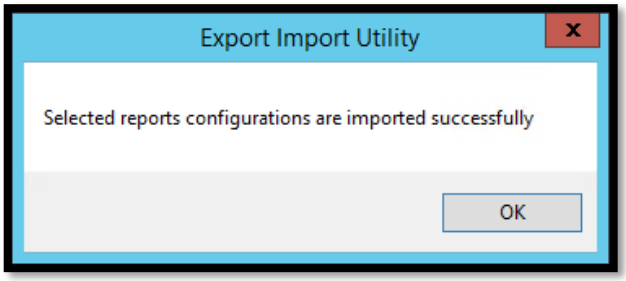
1. Click the **Reports** option and select the **New (*.etcrx)** option.



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



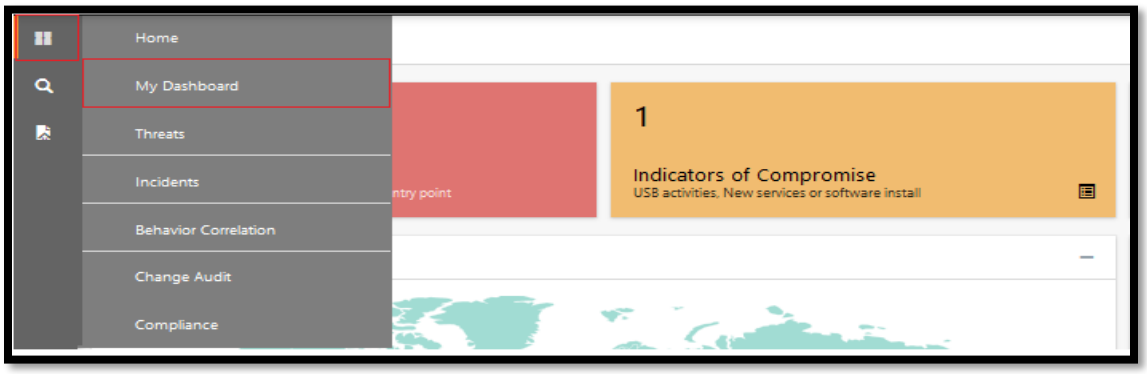
3. Click the **Import** button to import the report. EventTracker displays a success message.



5.5 Dashboards

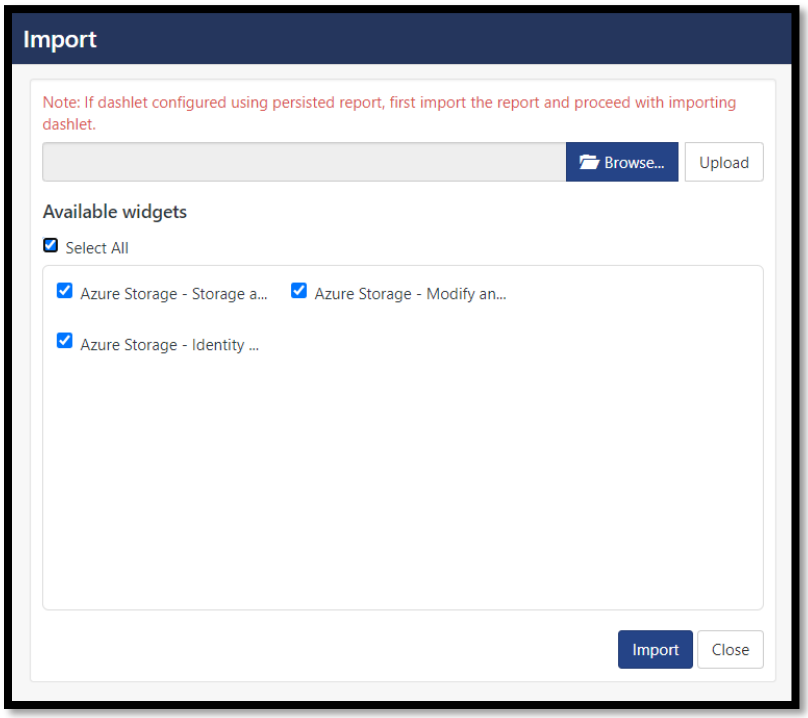
NOTE**:** Below steps given are specific to EventTracker 9 and later.

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

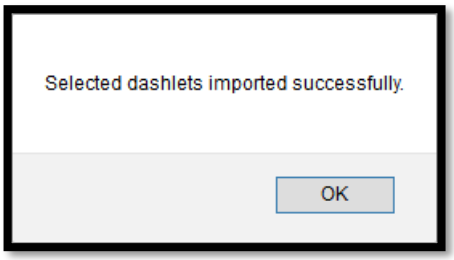


2. Navigate to the **My Dashboard** option.
3. Click the **Import** button as shown below.

4. Import the dashboard file **Dashboards_ Azure Storage.etwd** and select the **Select All** checkbox.
5. Click **Import** as shown below.

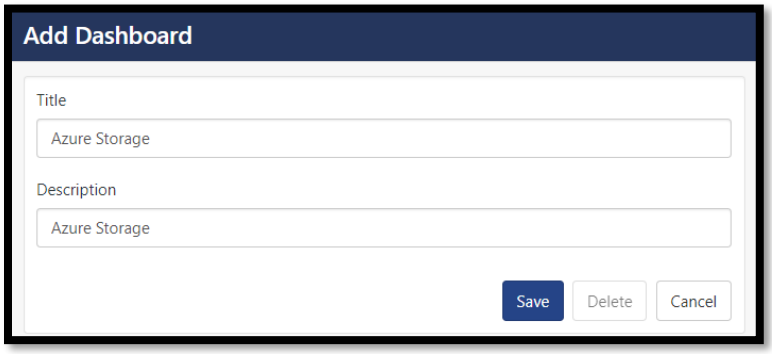


6. Import is now completed successfully.

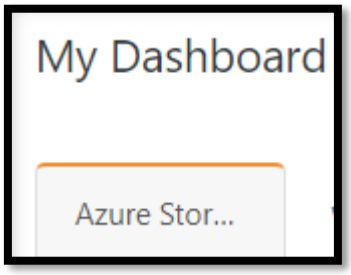


7. In the **My Dashboard** page select ⊕ to add dashboard.

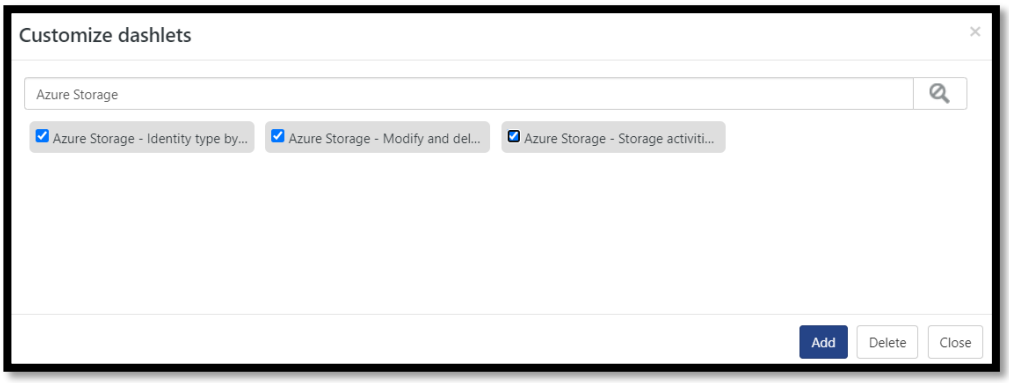
8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.



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



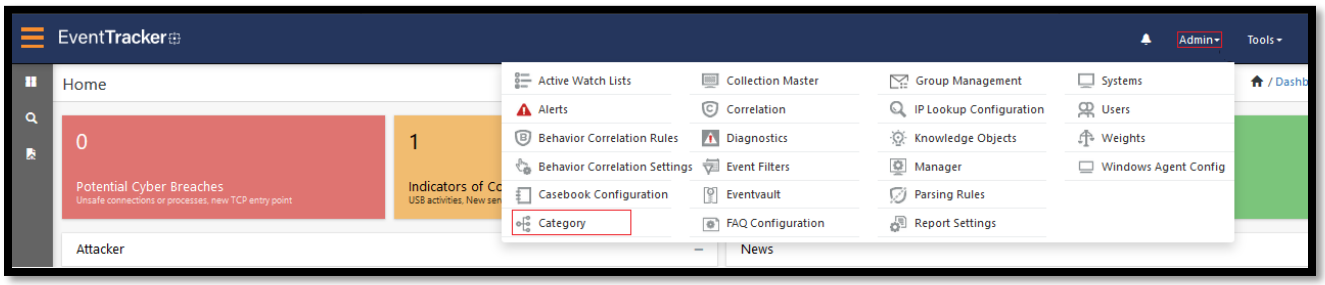
10. Select the imported dashlets and click **Add**.



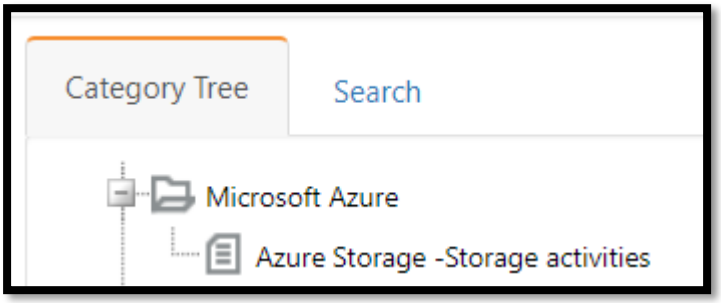
6. Verifying Azure Storage Knowledge Packs in EventTracker

6.1 Categories

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

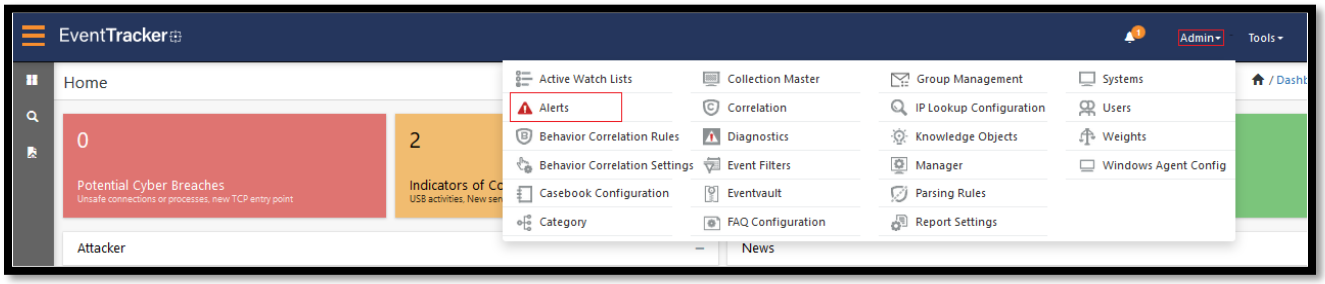


3. In the **Category Tree**, scroll down and expand the **Microsoft Azure** group folder to view the imported category.

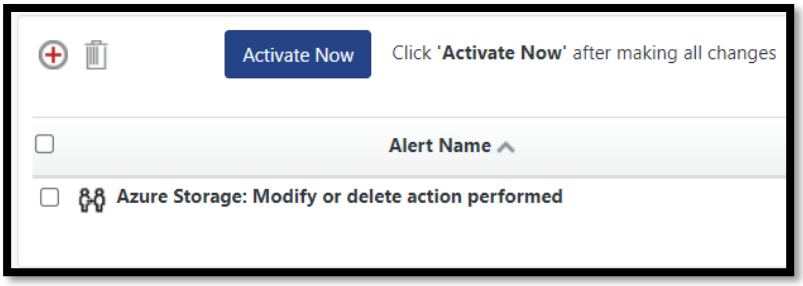


6.2 Alerts

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

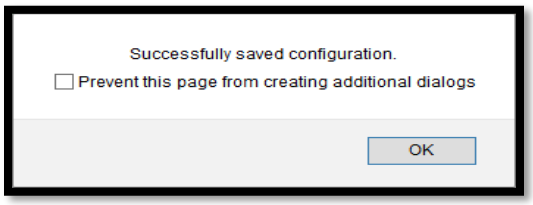


3. In the **Search** box, type **Azure Storage**, and then click the **Go** button.
   The Alert Management page will display the imported alert.



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

   EventTracker displays a message box.

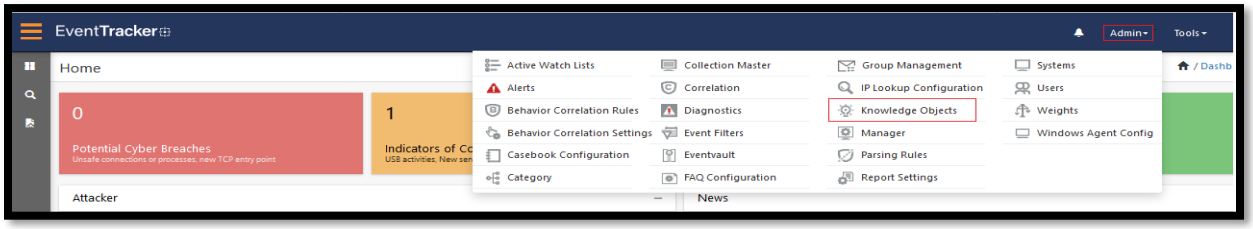


5. Click **OK**, and then click the **Activate Now** button.

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.**



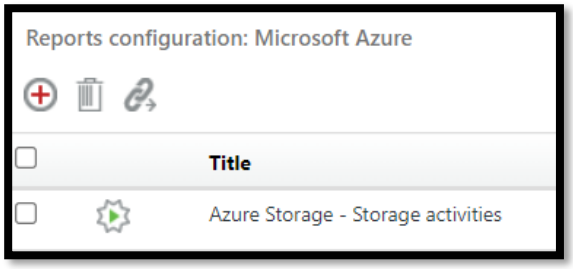
2. In the Knowledge Object tree, expand the **Microsoft Azure group** folder to view the imported Knowledge Objects.

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

6.4 Reports

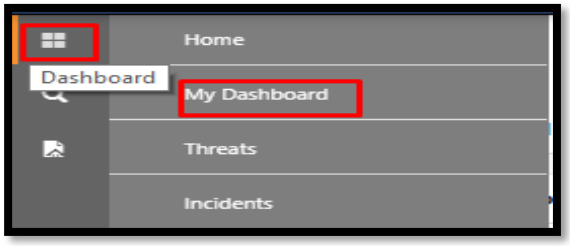
1. In the **EventTracker** web interface, click the **Reports** menu, and then select **Report Configuration**.

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

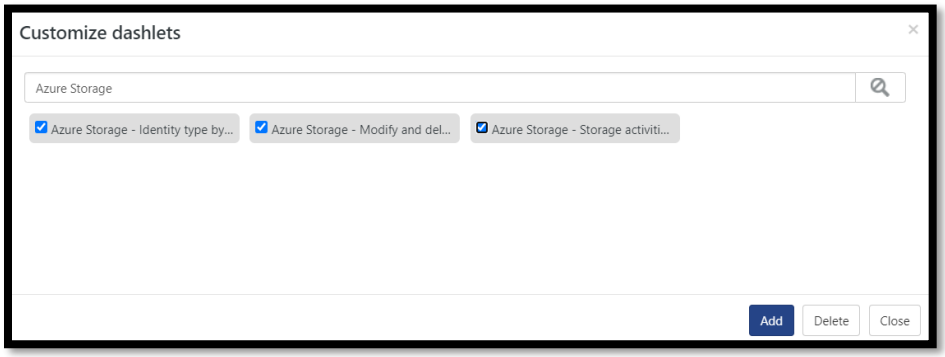


6.5 Dashboards

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



2. Click **Search** for the **Azure Storage.** 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