Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate Azure Cache for Redis with EventTracker

Publication Date:

June 21, 2022

Abstract

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

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and Azure Cache for Redis.

Audience

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

Table of Contents

1 Overview

Azure Cache for Redis is a fully managed, in-memory cache service on Microsoft Azure that implements the open-source Redis. Redis enables high-performance and scalable architectures that bring a critical low-latency and high-throughput data storage solution to modern applications. It can process large volumes of application requests by retaining frequently accessed data in the server memory, which can be written to and read from quickly.

Netsurion facilitates monitoring events retrieved from the Azure Cache for Redis. The dashboard, category, alerts, and reports in Netsurion's threat protection platform, EventTracker, will benefit you in tracking users connected to the Cache and their connection count.

2 Prerequisite

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

> **Note**
>
> Refer to the How-To guide to configure Azure Cache for Redis to forward logs to EventTracker.

3 EventTracker Knowledge Packs

Configure the Knowledge Packs into EventTracker once the logs are received by the EventTracker Manager.

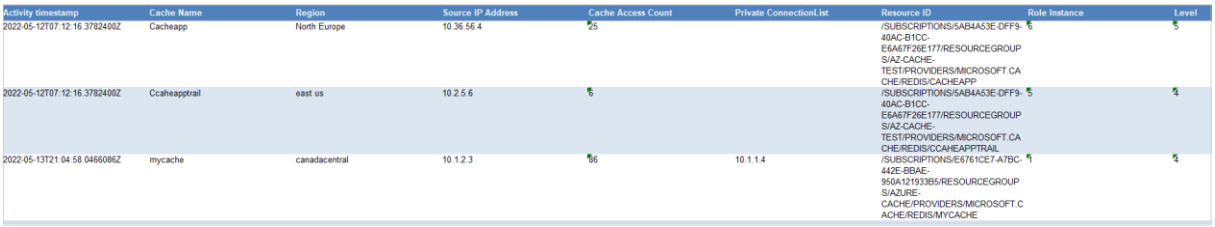
The following Knowledge Packs (KPs) are available in EventTracker.

3.1 Category

Azure Cache for Redis – Cache activities: This category of the saved search allows you to parse events that are specific to the Cache activities on the Azure Cache for Redis.

3.2 Reports

Azure Cache for Redis – Connected clients list: This report provides a detailed summary of connected clients activities in Azure Cache for Redis. The report includes the source IP address, account name, resource ID, connection count, operation, and more.

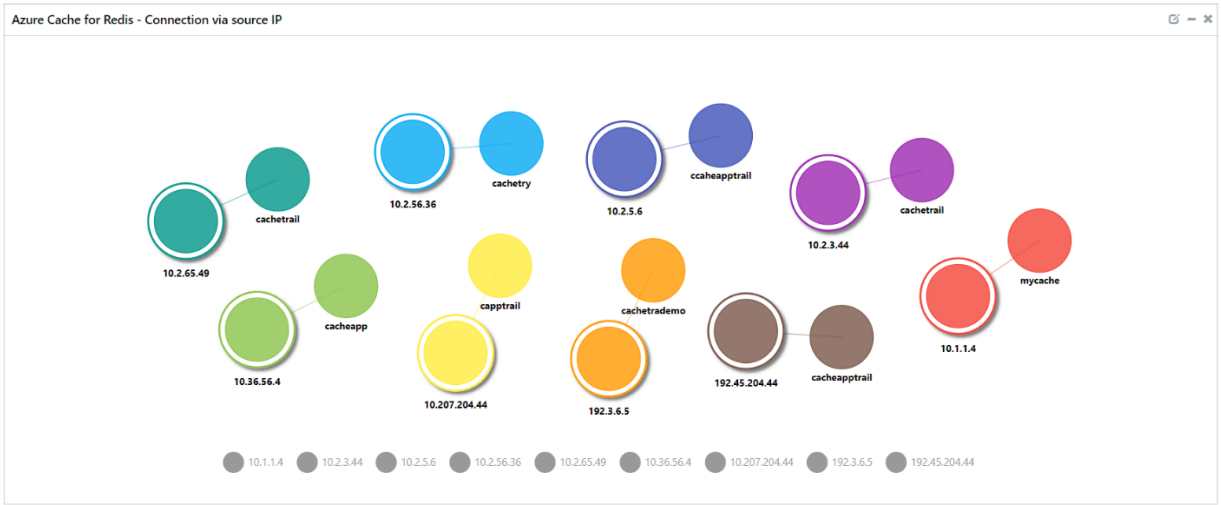


Activity timestamp	Cache Name	Region	Source IP Address	Cache Access Count	Private ConnectionList	Resource ID	Role Instance	Level
2022-05-12T07:12:16.3782400Z	Cacheapp	North Europe	10.36.56.4	25		/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ-CACHE-TEST/PROVIDERS/MICROSOFT.CACHE/REDIS/CACHEAPP		
2022-05-12T07:12:16.3782400Z	Ccaheapptrail	east us	10.2.5.6	6		/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ-CACHE-TEST/PROVIDERS/MICROSOFT.CACHE/REDIS/CCAHEAPPTRAIL		
2022-05-13T21:04:58.0466086Z	mycache	canadacentral	10.1.2.3	6	10.1.1.4	/SUBSCRIPTIONS/E6761CE7-A7BC-442E-BBAE-950A121933B5/RESOURCEGROUPS/AZURE-CACHE/PROVIDERS/MICROSOFT.CACHE/REDIS/MYCACHE		

3.3 Dashboard

Azure Cache for Redis - Connection by geolocation: This dashlet displays the geolocation of the public IPs that are connected to the Cache.

Azure Cache for Redis – Connection via source IP: This dashlet displays the Cache and its connected source IP details.

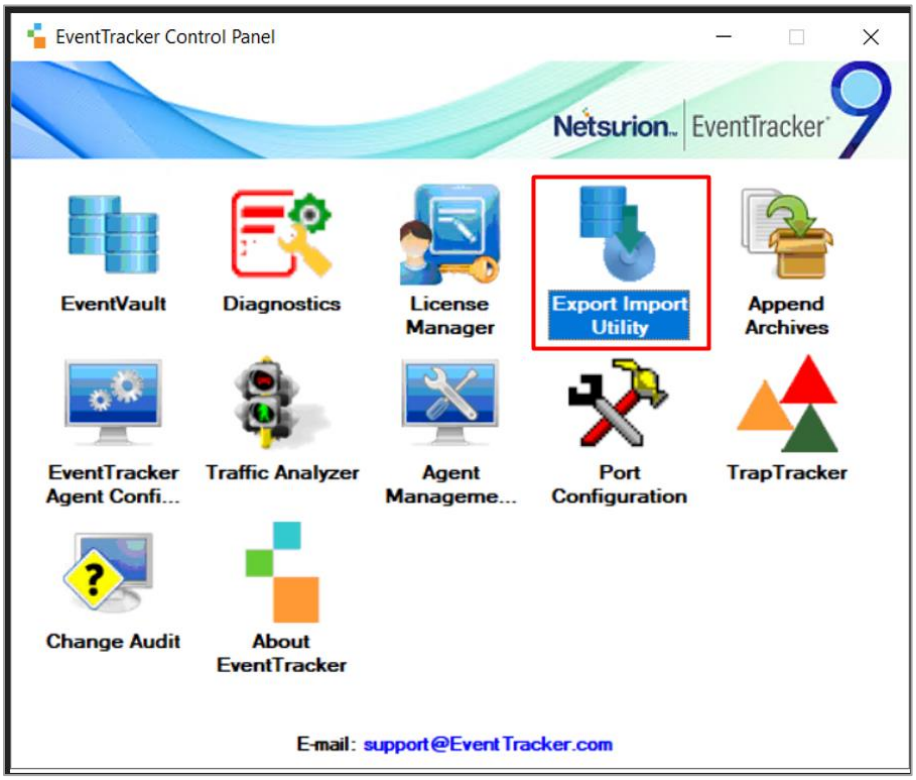


4 Importing Azure Cache for Redis Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

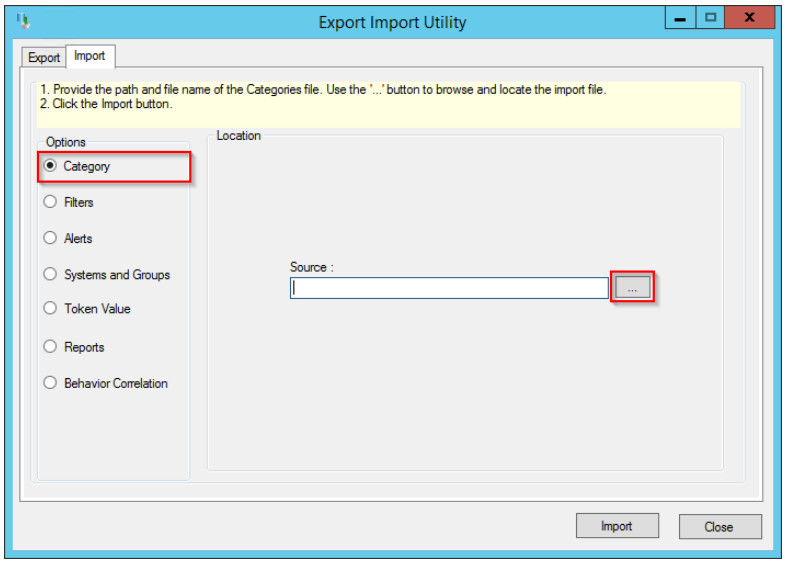
- Category
- Reports
- Knowledge Objects
- Dashboards

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

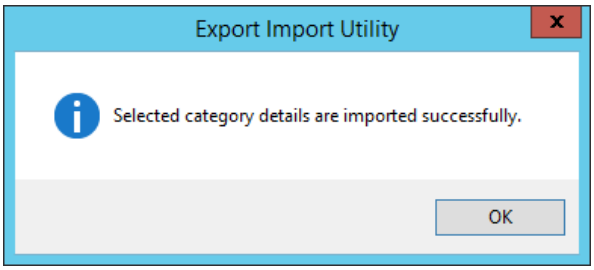


4.1 Category

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



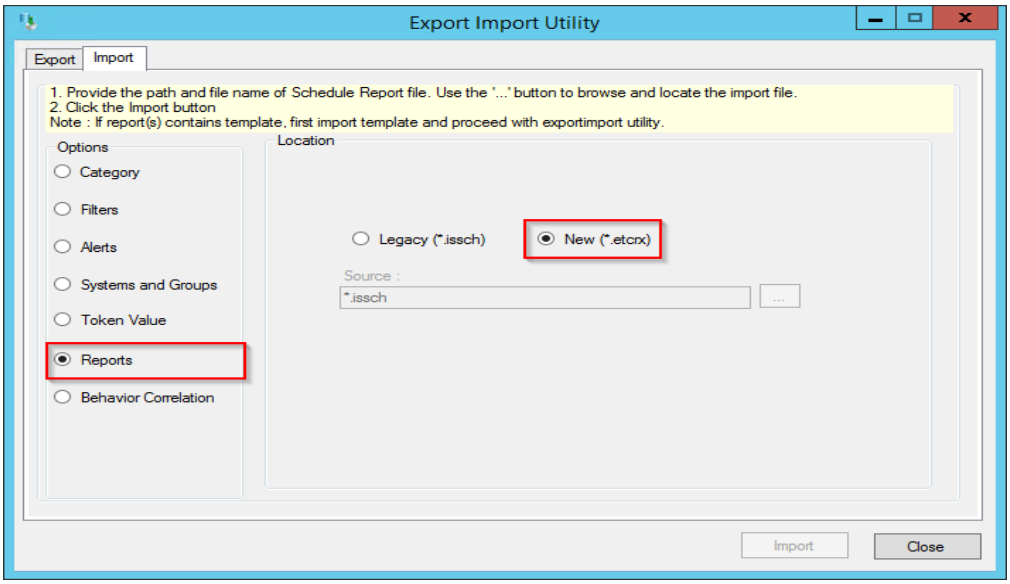
2. In the **Browse** window, locate the **Categories_Azure Cache for Redis.iscat** file and click **Open**.
3. To import the categories, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



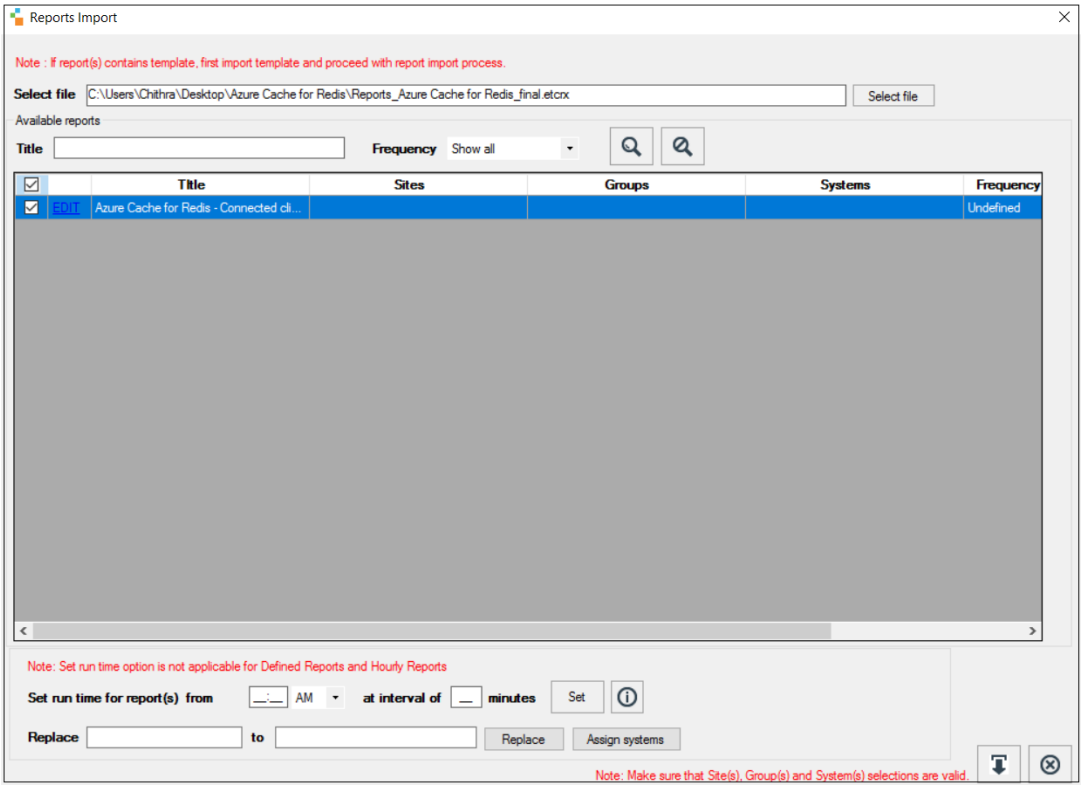
5. Click **OK** or the **Close** button to complete the process.

4.2 Reports

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

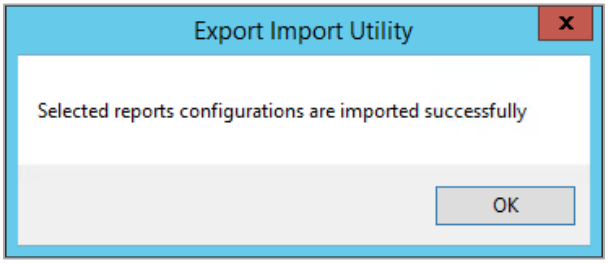


2. In the **Reports Import** window, click **Select file** to locate the **Reports_ Azure Cache for Redis.etcrx** file.



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

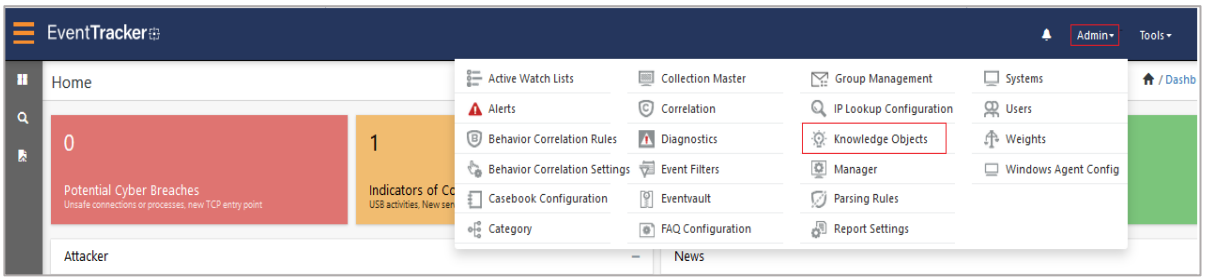
4. EventTracker displays a success message on successful importing of the selected files in **Reports**.



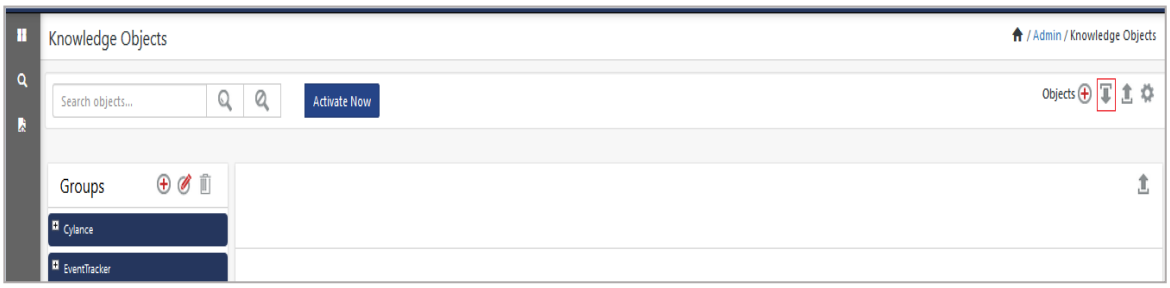
5. Click **OK** or the **Close** button to complete the process.

4.3 Knowledge Objects (KO)

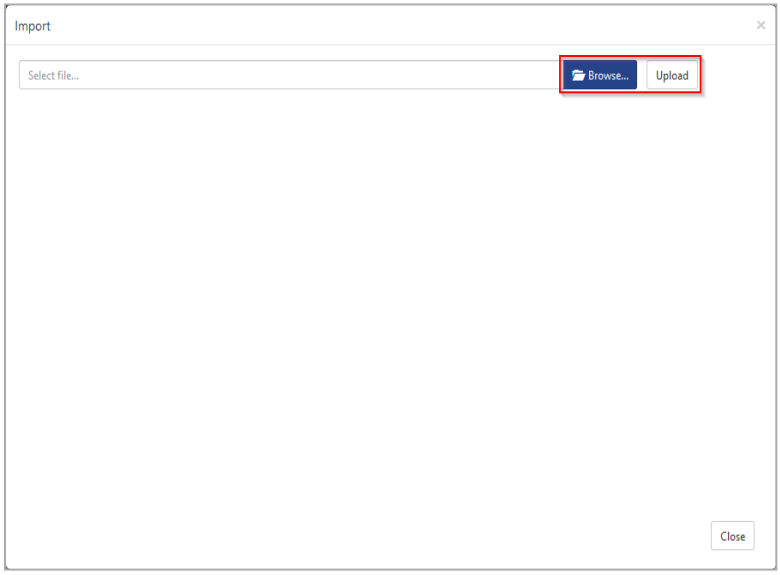
1. In the **EventTracker Manager** console, hover over the **Admin** menu and click **Knowledge Objects**.



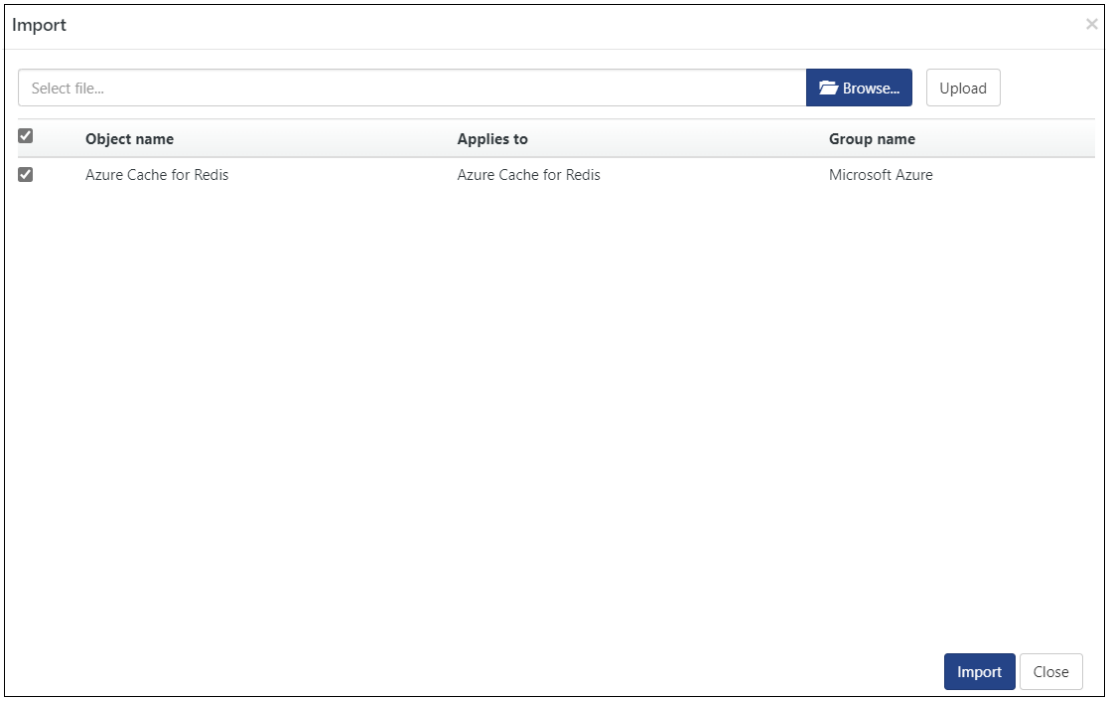
2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.



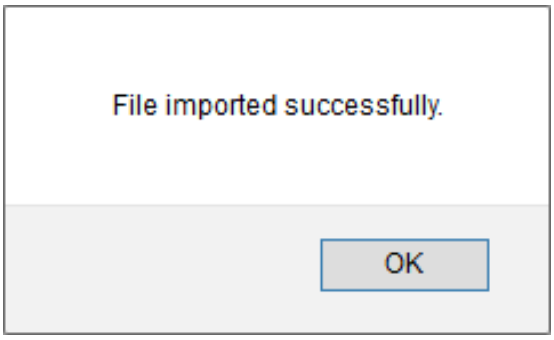
3. In the **Import** window, click **Browse** and locate the **KO_ Azure Cache for Redis.etko** file.



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

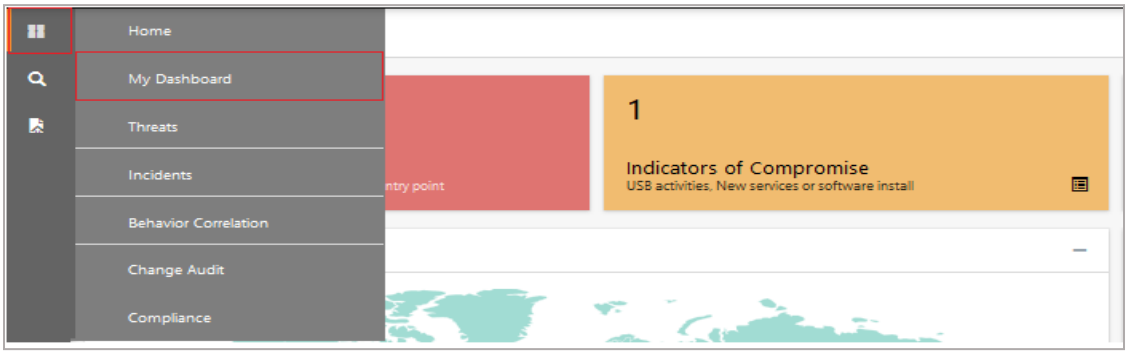


5. EventTracker displays a success message on successfully importing the selected file in **Knowledge Objects**.



4.4 Dashboards

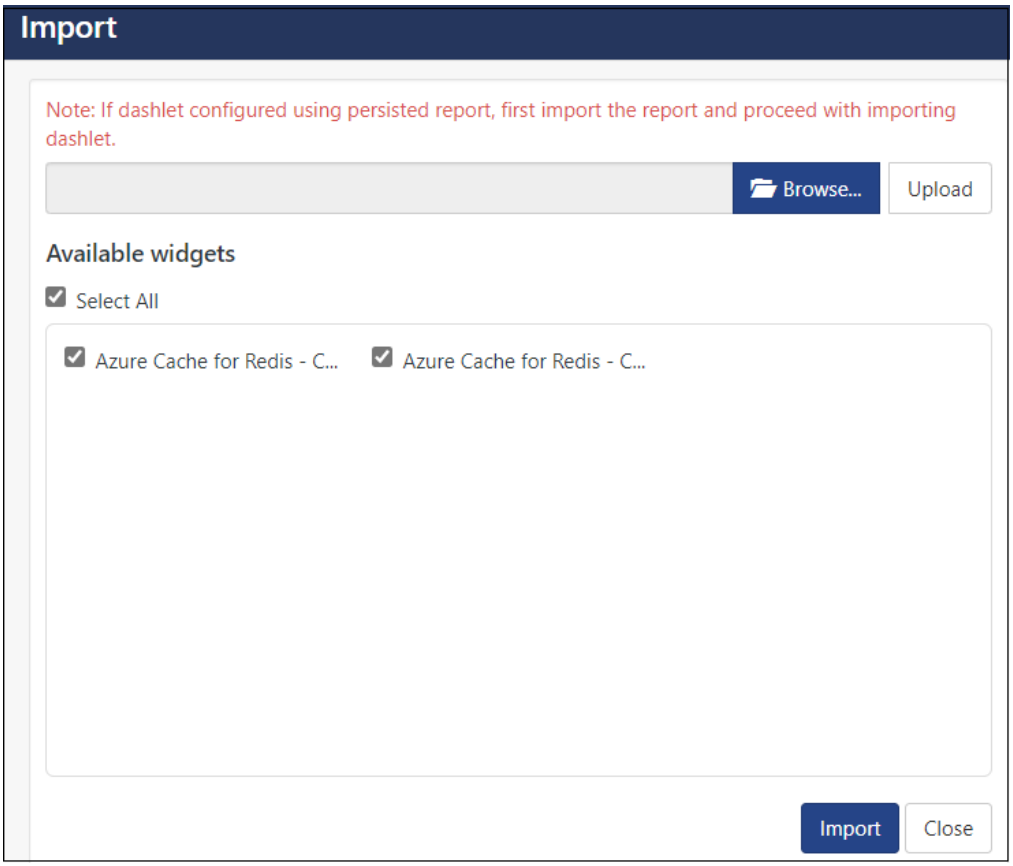
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



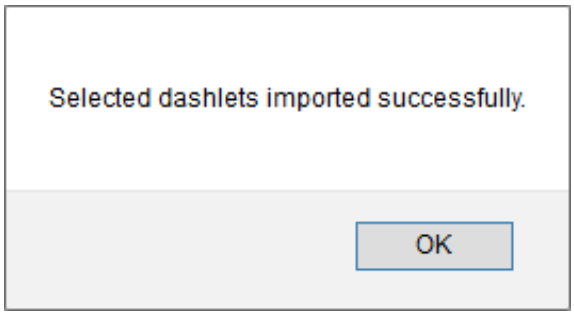
2. In the **My Dashboard** interface, click the **Import** button to import the files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_Azure Cache for Redis Redis.etwd** file and then click **Upload.**

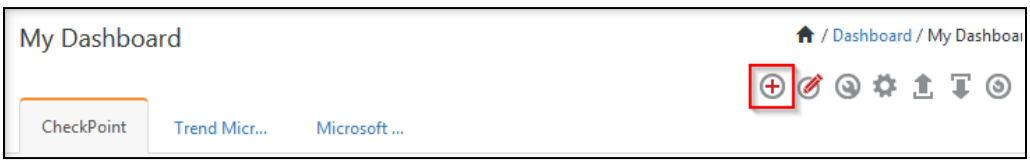
4. Select the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.



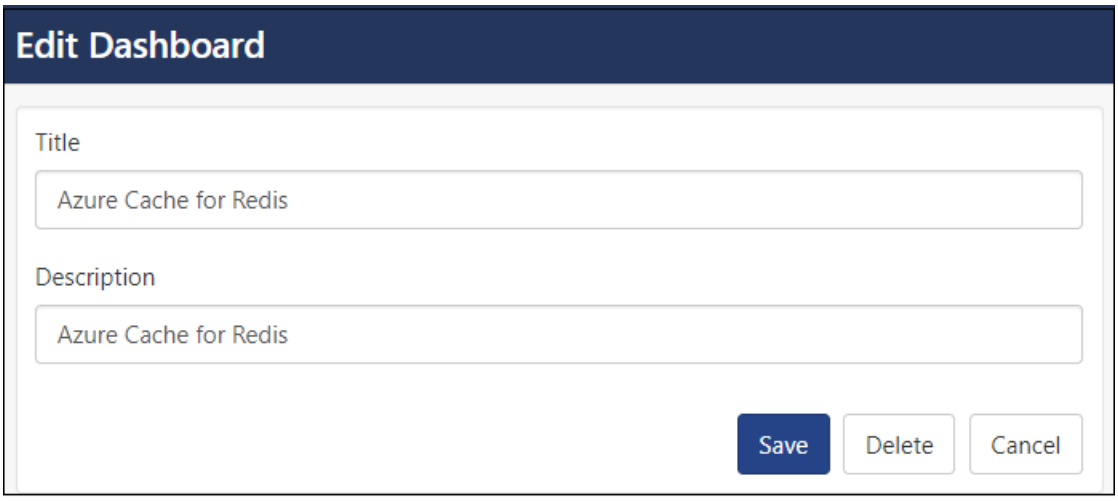
5. The EventTracker displays a success message on successful import of the dashlet files.



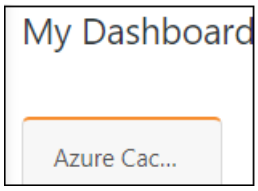
6. Then, in the **My Dashboard** interface, click the **Add** button to add the dashboard.



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



8. From the newly created dashboard interface (for example, **Azure Cache for Redis**), click the **Configuration** button to add the Azure Cache for Redis dashlets.

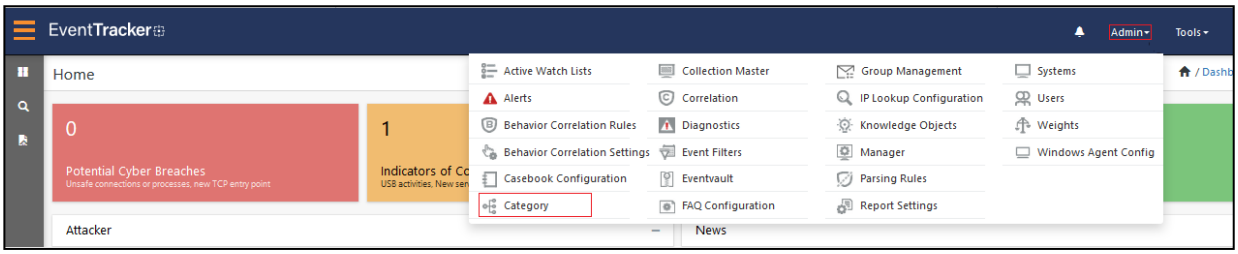


9. Search and select the newly imported dashlets and click **Add**.

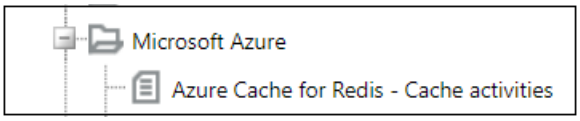
5 Verifying Azure Cache for Redis Knowledge Packs in EventTracker

5.1 Category

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

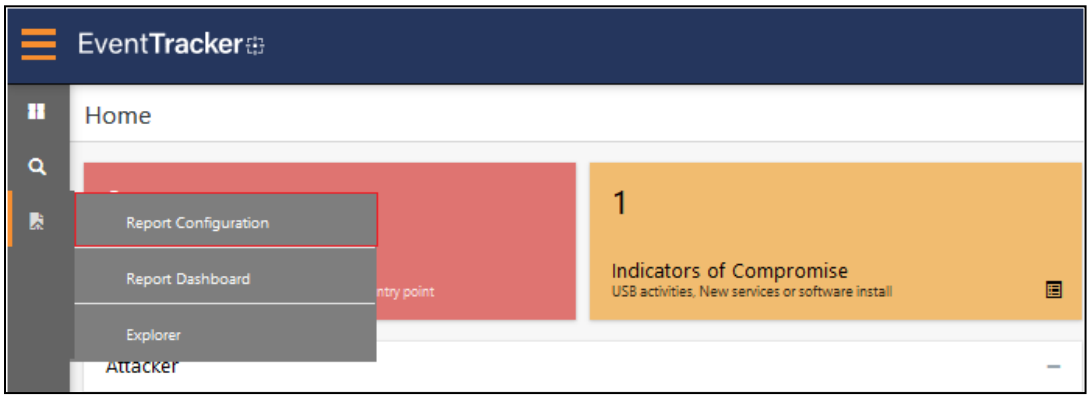


2. In the **Category** interface, under the **Category Tree** tab, click the **Microsoft Azure** group folder to expand and see the imported categories.



5.2 Reports

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



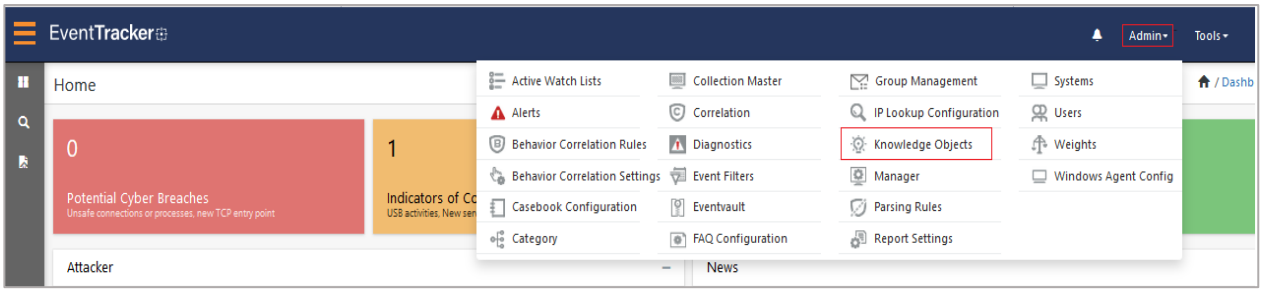
2. In the **Reports Configuration** interface, click **Defined**.

3. In the search field, type **Microsoft Azure** and click **Search** to search for the Azure Cache for Redis files.

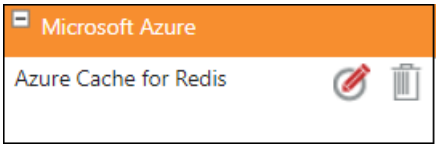
4. EventTracker displays the reports for Azure Cache for Redis.

5.3 Knowledge Objects (KO)

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



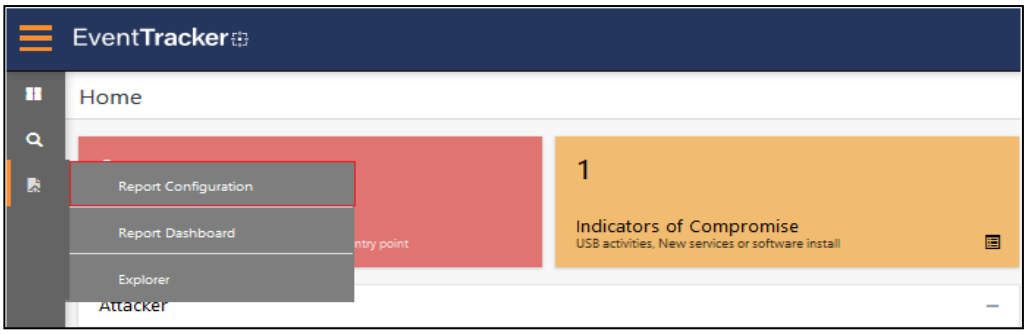
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Microsoft Azure** group to expand and view the imported Knowledge objects.



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

5.4 Dashboards

1. In the **EventTracker** web interface, go to **Home** > **My Dashboard**.



2. The **My Dashboard** interface displays all the dashlets related to **Azure Cache for Redis**.

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 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