Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrate Azure Active Directory with EventTracker

Publication Date:

August 09, 2022

Abstract

This guide provides instructions to configure the Knowledge Packs in EventTracker to receive the logs from Azure Active Directory. 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 Active Directory.

Audience

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

Table of Contents

1 Overview

Azure Active Directory (Azure AD), an aspect of Microsoft Entra, is an enterprise identity service that offers single sign-on, multifactor authentication, and conditional access to help protect against cybersecurity threats. Azure AD uses strong authentication and risk-based adaptive access policies to help protect access to resources and data.

Netsurion facilitates monitoring events from the Azure Active Directory. The dashboard, categories, alerts, and reports interface in Netsurion's threat protection platform, EventTracker, benefits in tracking azure active directory activities and changes to detect any suspicious activities performed on the Azure Active Directory.

2 Prerequisite

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

Note

Refer to How-To guide to configure Azure Active Directory 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 Active Directory – Audit operations: This category of the saved search will allow the users to parse the events that are specific to the audit level operations such as updating and deleting of the users in the Azure Active Directory.

Azure Active Directory – Sign in activities: This category of the saved search will allow the users to parse the events that are specific to the sign in operations in the Azure Active Directory.

3.2 Alerts

Azure Active Directory - Sign in failure: This alert indicates that an attempt was made to sign in without proper credentials.

Azure Active Directory - Sign in blocked: This alert indicates that an attempt was made to sign in from a malicious IP or is not trusted by the Azure Active Directory devices.

Azure Active Directory - User risk detection: This alert indicates that the user attempted a risky event in the Azure Active Directory.

Azure Active Directory – Audit operations failure: This alert provides the details of the failed attempts made to any update operations in the Azure Active Directory.

3.3 Reports

Azure Active Directory – Audit Operations: This report provides a detailed summary of the audit and performance activities in Azure Active Directory. It includes Tenant ID, User Mail ID, Activity Type and their Result, Activity Time, Caller IP.

LogTime	Activity Time	Caller IP	Activity Type	Result	Tenant ID	User Mail ID
07-15-2022 11:18:18 AM	2022-07-15T11:18:17.5894027+00:00	127.0.0.1	Update device	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	
07-15-2022 12:25:53 PM	2022-07-15T12:25:52.9164149+00:00	127.0.0.1	Update device	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	
07-15-2022 10:16:37 PM	2022-07-15T22:16:37.0842489+00:00		Change user password	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	abcdef@eventtracker.onmicrosoft.com
07-15-2022 10:16:37 PM	2022-07-15T22:16:37.0842489+00:00		Update StsRefreshTokenValidFrom Timestamp	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	abcef@eventtracker.onmicrosoft.com
07-15-2022 10:36:27 PM	2022-07-15T22:36:27.351443+00:00		Update user	success	0ac05f5c-4238-4951-89a8-2b5e518805f0	nsdfgh@eventtracker.com

Azure Active Directory – Sign in Failures: This report provides a detailed summary of the sign in failure activities in Azure Active Directory. It includes Source IP, Tenant ID, User Mail ID, Authentication Type, etc.

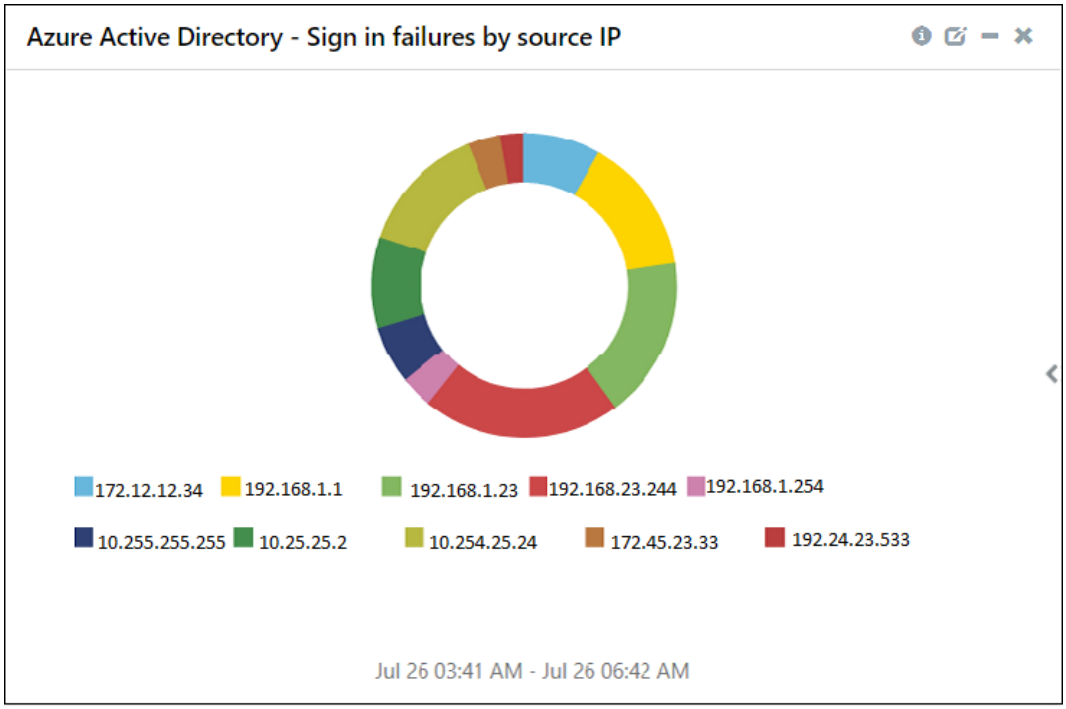
LogTime	Source IP	Operating System	Tenant ID	User Name	User Mail ID	System Name	Authentication Type	Failure Reason	Trusted By	Sign In Category
07-13-2022 11:26:25 AM	211.12.12.112	Windows 10	0ac05f5c-4238-4951-89a8-2bdsfdg530	contoso	contoso@eventtracker.com	NTETSYSNAME1	singleFactorAuthentication	Other	Azure AD registered	NonInteractiveUserSignInLogs
07-13-2022 11:26:26 AM	127.0.0.1	Windows 10	034rf5c-4238-4951-89a8-2b5e518805f0	john	john@eventtracker.com	SYSNAME2	singleFactorAuthentication	Other	Azure AD registered	NonInteractiveUserSignInLogs
07-13-2022 11:26:29 AM	234.12.12.45	Windows 10	0ac05f5c-4238-4951-89a8-2b5e518805f0	smith	smith@eventtracker.com	SYSNAME3	singleFactorAuthentication	Other	Azure AD registered	NonInteractiveUserSignInLogs
07-13-2022 11:26:30 AM	234.45.23.323	Windows 10	0ac05f5c-4238-4951-89a8-2b5e5dsff4f0	samanta	samanta@eventtracker.com	SYSNAME4	singleFactorAuthentication	Other	Azure AD registered	NonInteractiveUserSignInLogs
07-13-2022 11:26:30 AM	211.12.12.123	Windows 10	0ac05f5c-4238-4951-89a8-2bdst5g05f0	nayana tara	nayana@eventtracker.com	SYSNAME5	singleFactorAuthentication	Other	Azure AD registered	NonInteractiveUserSignInLogs

Azure Active Directory – Sign in Success: This report provides a detailed summary of the sign-in success activities in the Azure Active Directory. It includes Source IP, Tenant ID, User Mail ID, Authentication Type, etc.

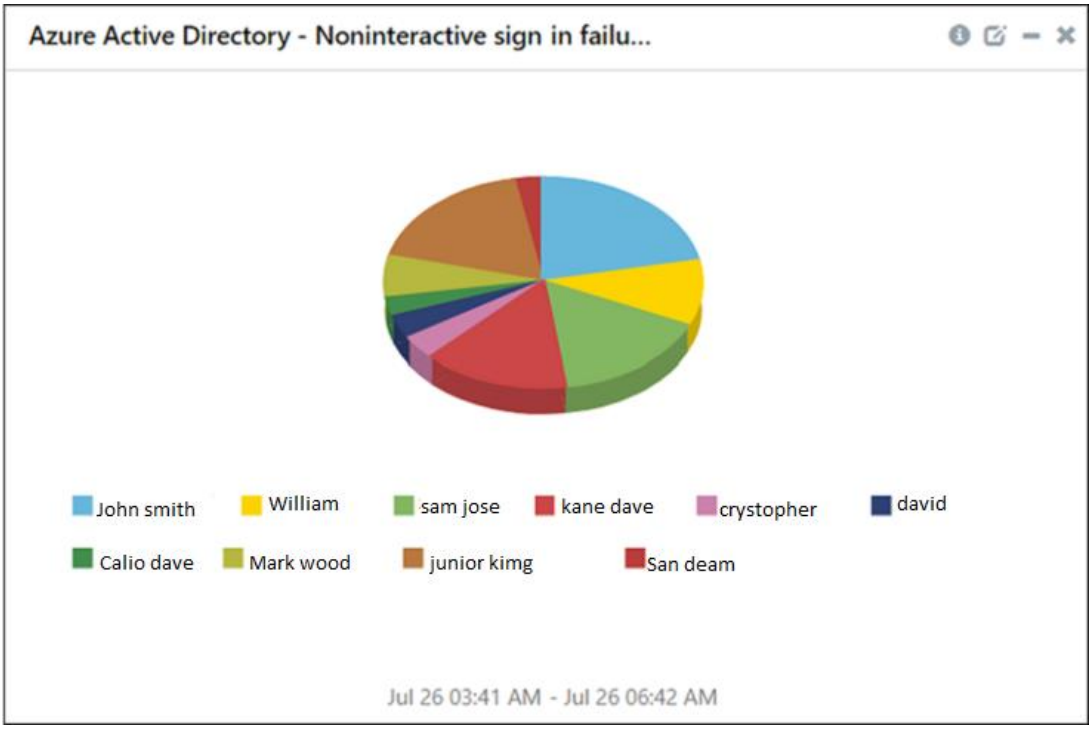
LogTime	Authentication Type	Application	Source IP	Operating System	Activity Type	Tenant ID	Trusted By
08-05-2022 11:42:44 AM	multiFactorAuthentication	Rich Client 4.42.1.0	172.12.21.21	Windows10	Sign-in activity	0ac05f5c-4238-4951-89a8-2b5f0	Azure AD registered
08-05-2022 11:43:50 AM	singleFactorAuthentication	Edge 18.19044	172.12.21.22	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8-2b5f1	Azure AD registered
08-05-2022 11:43:51 AM	multiFactorAuthentication	Edge 18.19044	172.12.21.23	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8-2b5f2	Azure AD registered
08-05-2022 11:43:51 AM	multiFactorAuthentication	Edge 18.19044	172.12.21.24	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8-2b5f3	Azure AD registered
08-05-2022 11:43:52 AM	multiFactorAuthentication	Edge 18.19044	172.12.21.25	Windows 10	Sign-in activity	0ac05f5c-4238-4951-89a8-2b5f4	Azure AD registered

3.4 Dashboard

Azure Active Directory - Sign in failures by source IP

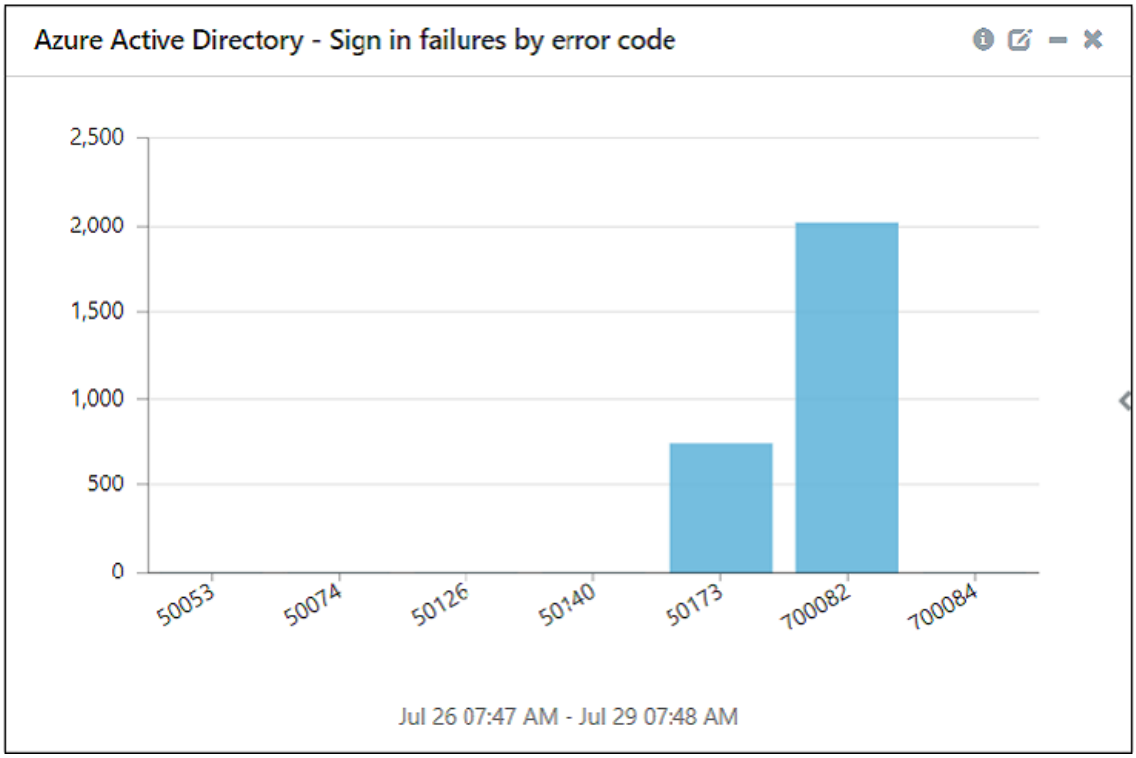


Azure Active Directory - Noninteractive sign in failures by user

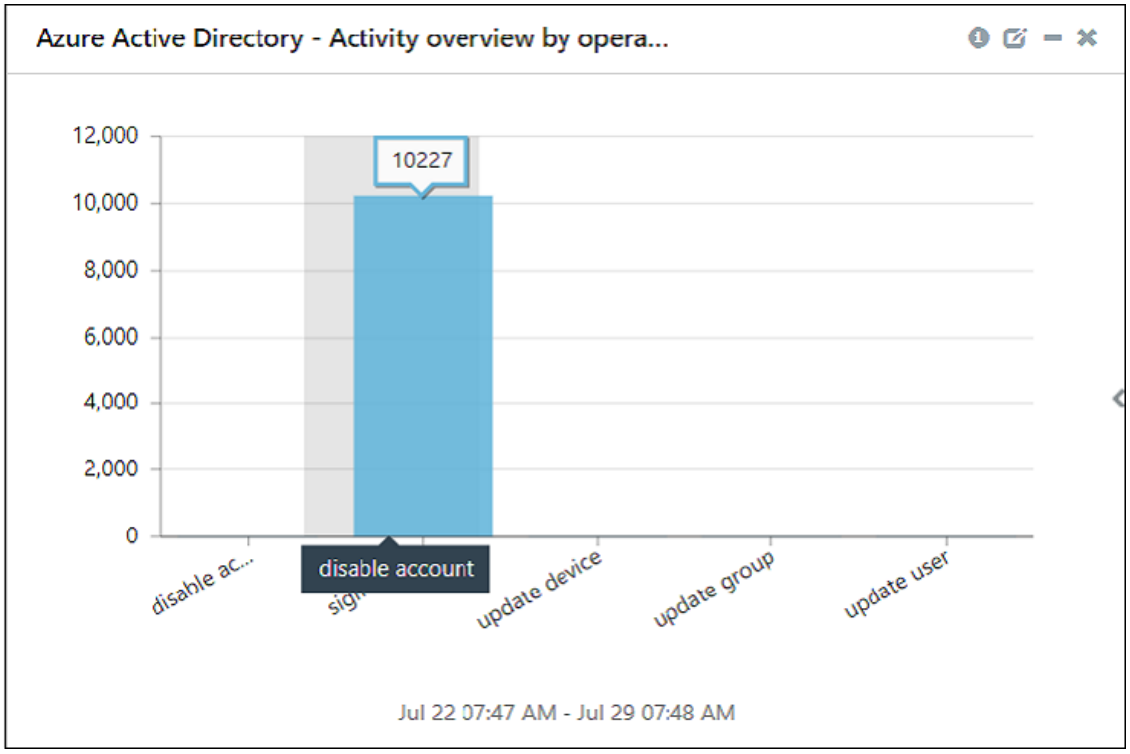


Azure Active Directory - Sign in by geolocation

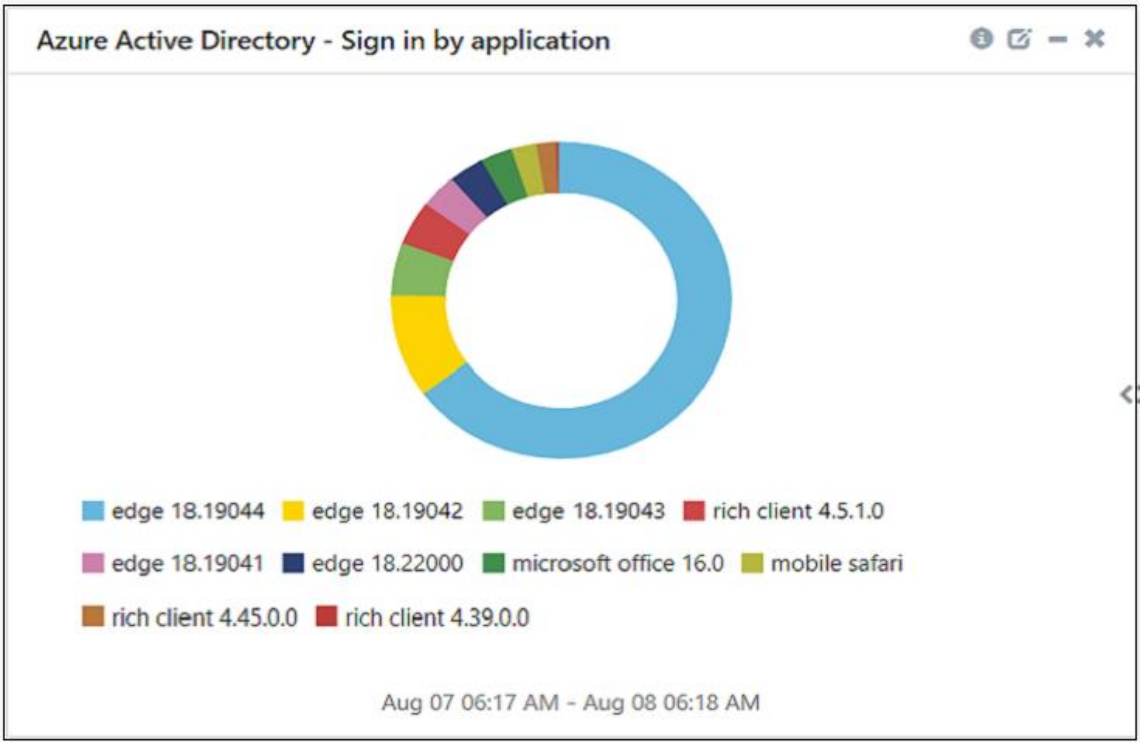
Azure Active Directory - Sign in failures by error codes



Azure Active Directory - Activity overview by operations



Azure Active Directory – Sign in by application

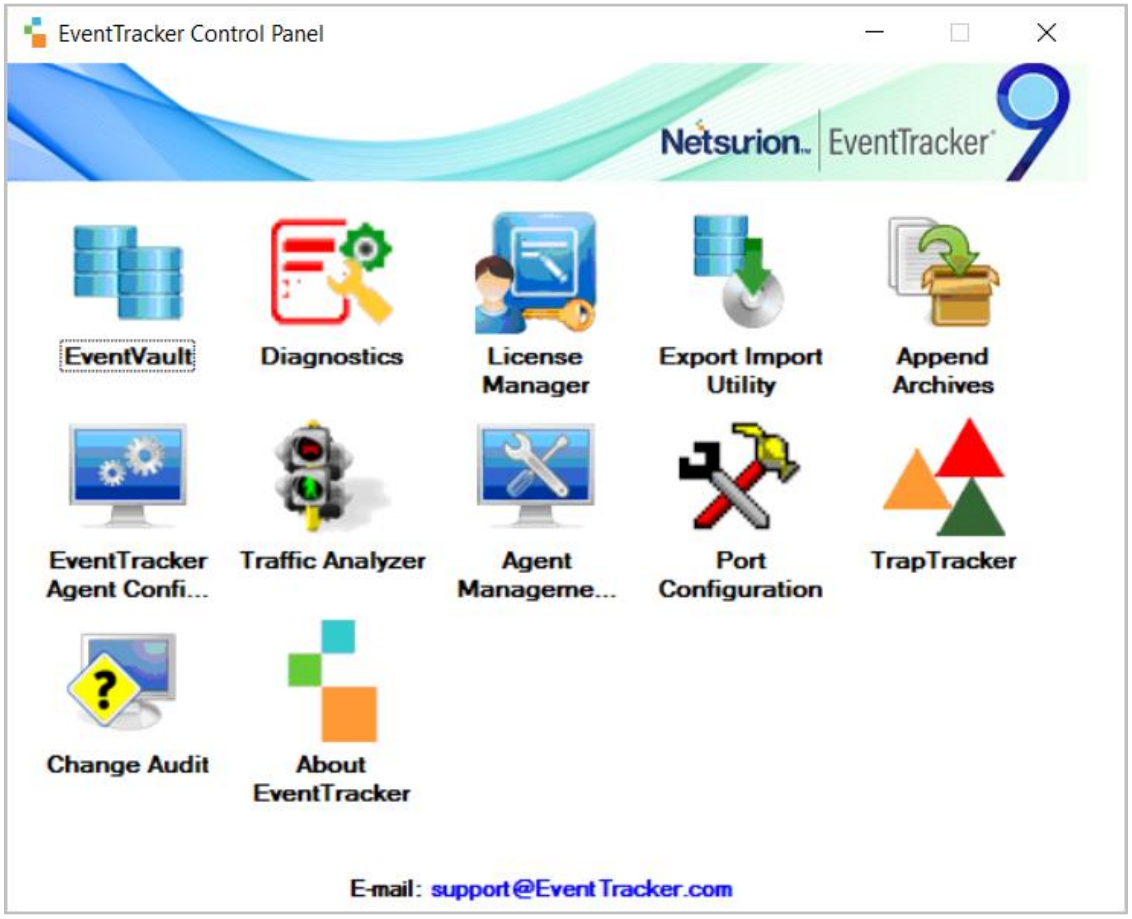


4 Importing Azure Active Directory Knowledge Packs into EventTracker

Import the Knowledge Pack items in the following sequence.

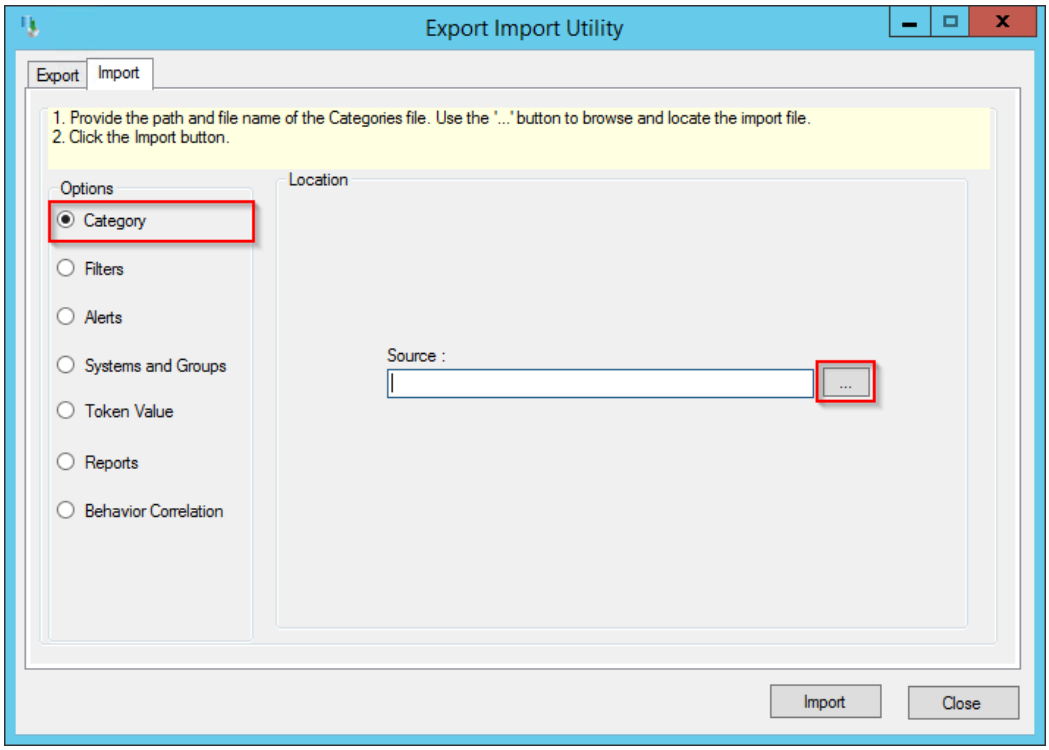
- Category
- Alerts
- Reports
- Knowledge Objects
- Dashboards

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

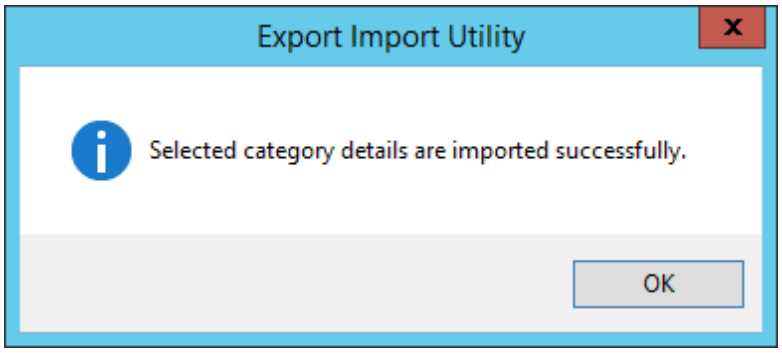


4.1 Category

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



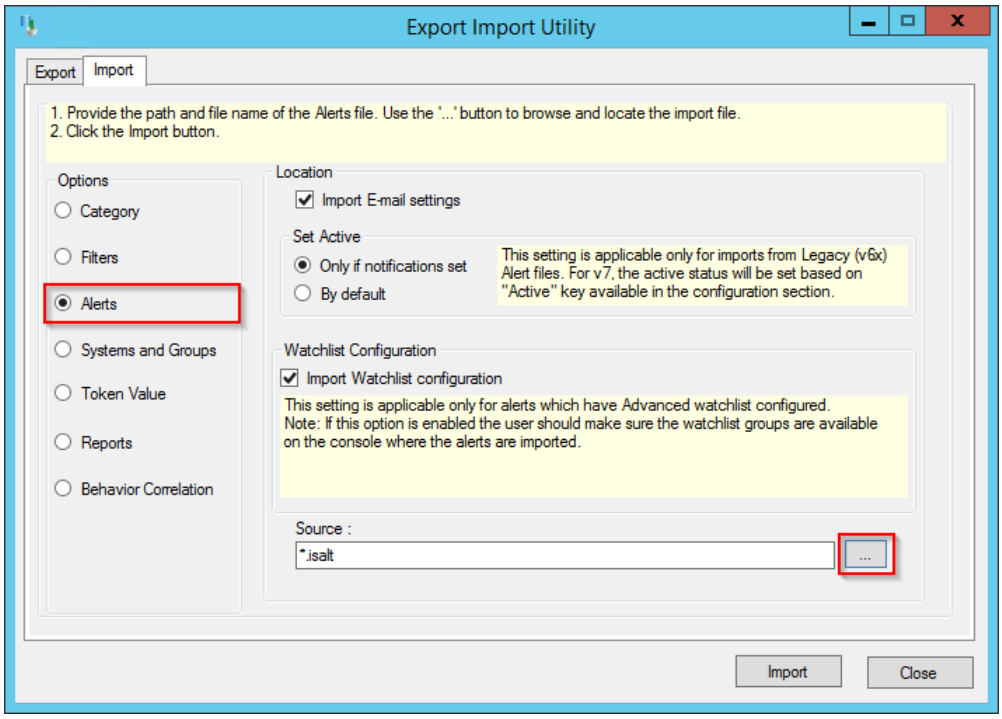
2. In the **Browse** window, locate the **Categories_Azure Active Directory.iscat** file and click **Open**.
3. To import the category, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Category**.



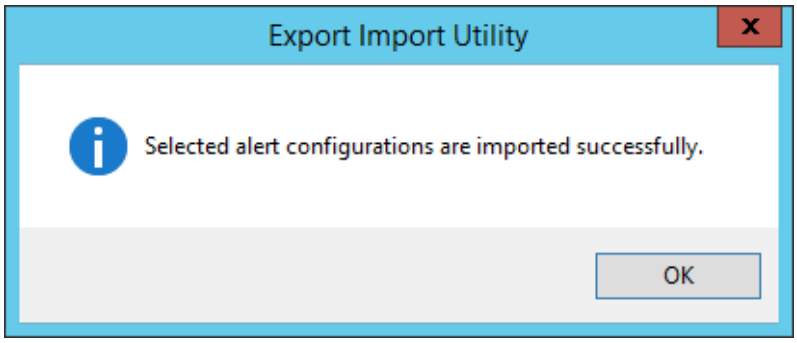
5. Click **OK** or the **Close** button to complete the process.

4.2 Alerts

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



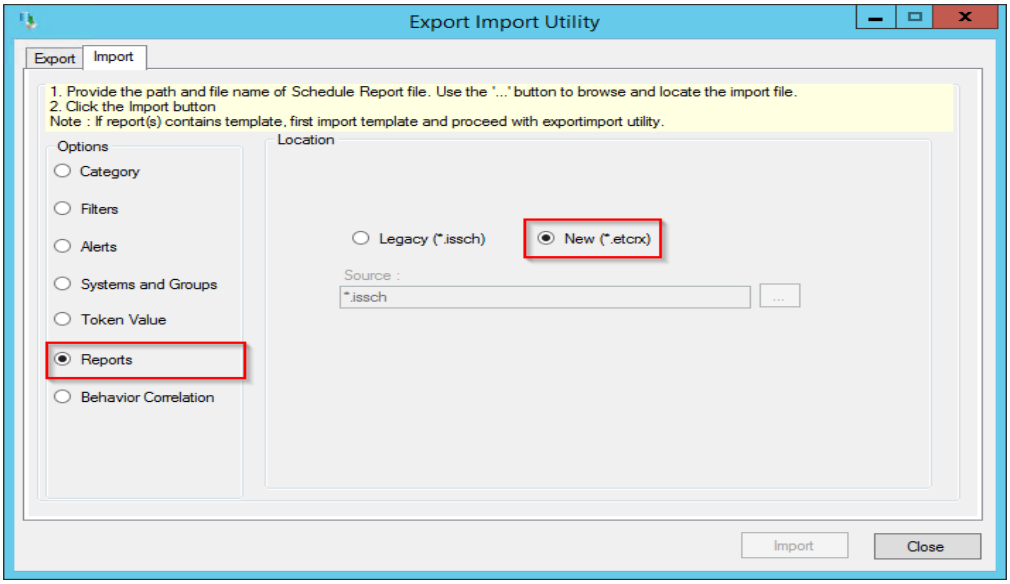
2. In the **Browse** window, locate the **Alerts_ Azure Active Directory.isalt** file, and then click **Open**.
3. To import the alerts, click **Import**.
4. EventTracker displays a success message on successfully importing the selected file in **Alerts**.



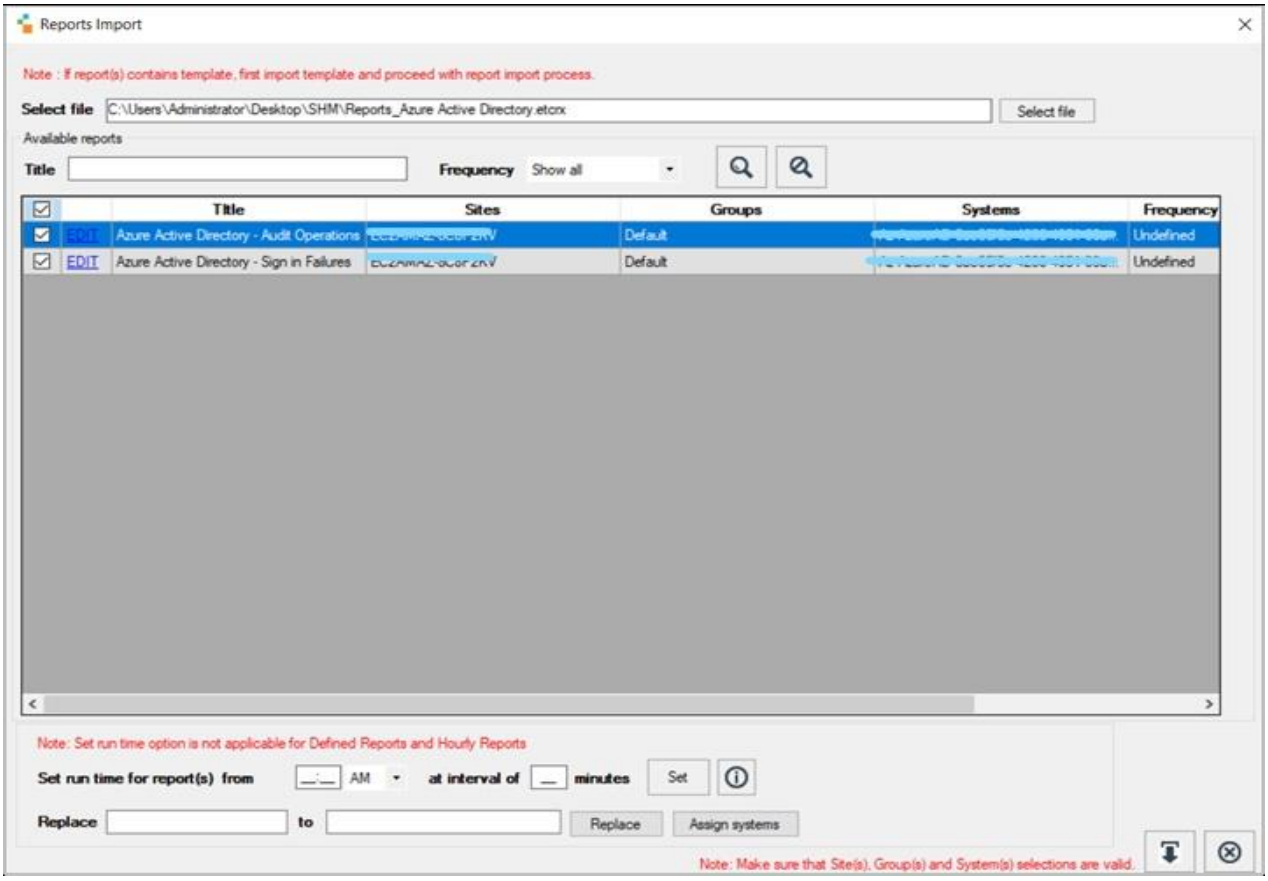
5. Click **OK** or the **Close** button to complete the process.

4.3 Reports

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

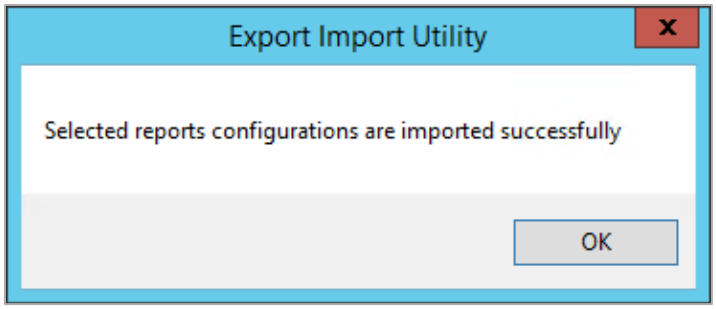


2. In the **Reports Import** window, click **Select file** to locate the **Reports_ Azure Active Directory.etcrx** file.



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

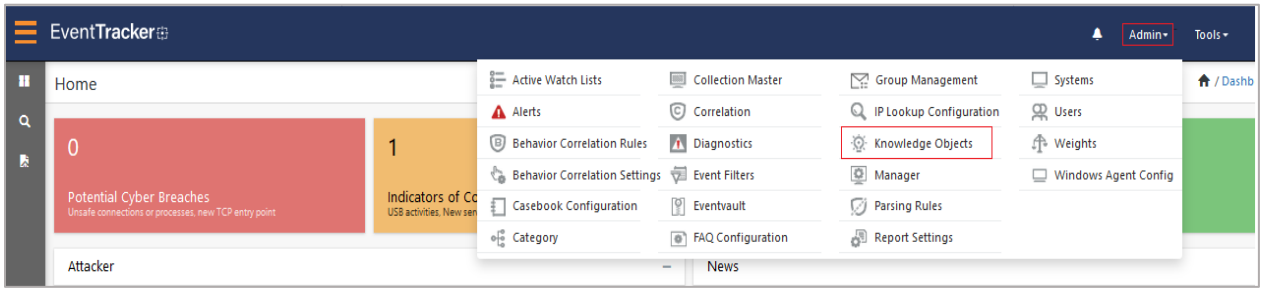
4. EventTracker displays a success message on successful importing of the selected file in **Reports**.



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

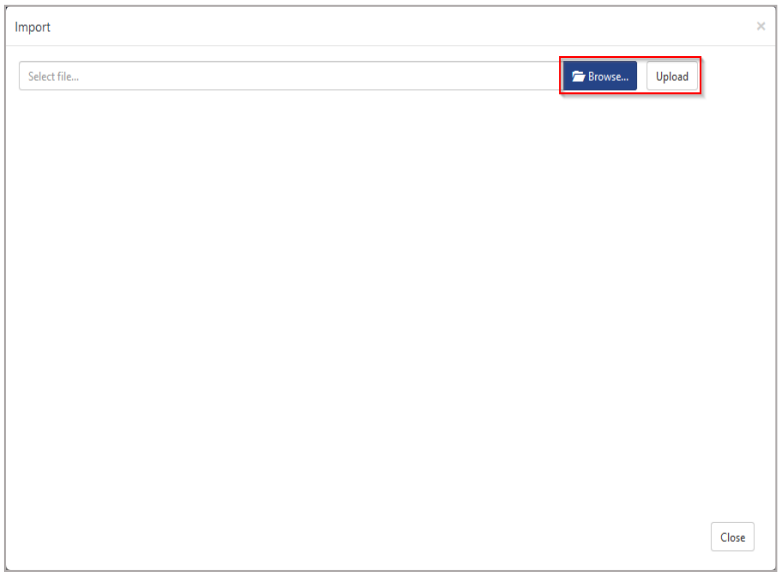
4.4 Knowledge Objects (KO)

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

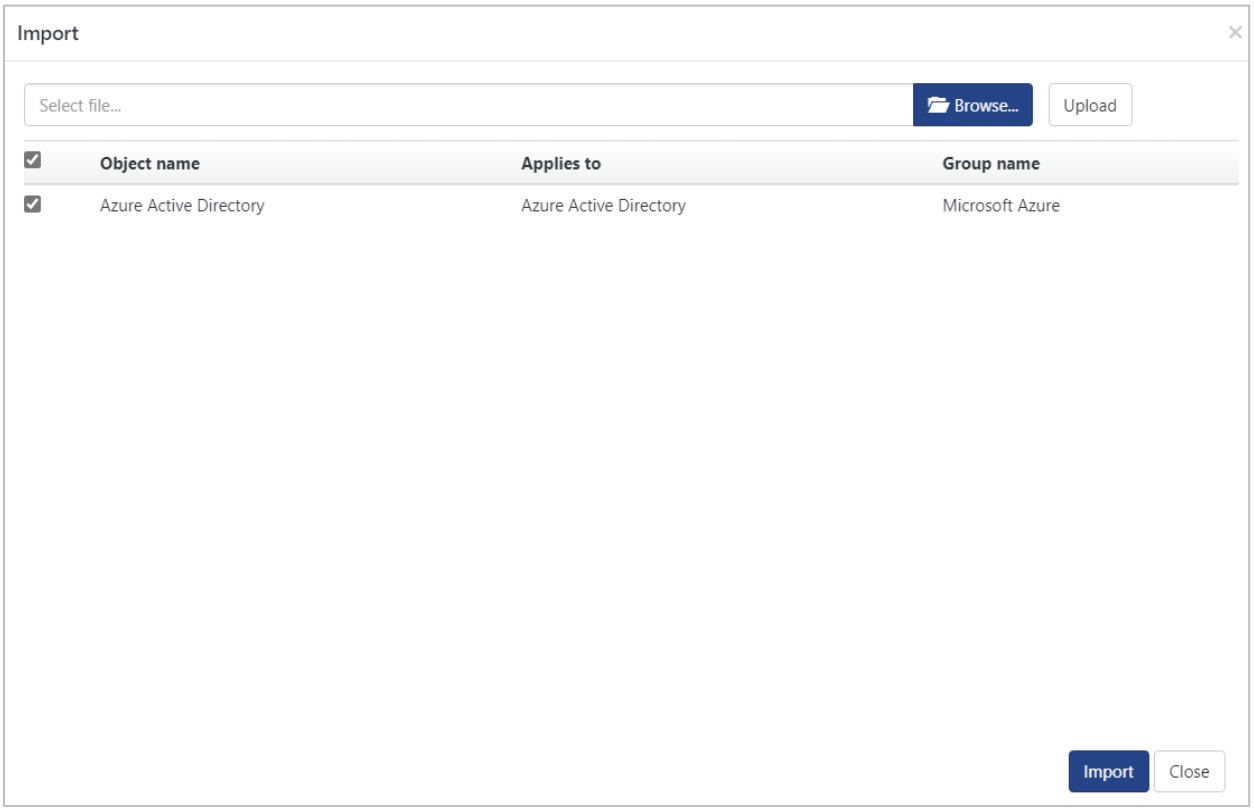


2. In the **Knowledge Objects** interface, click the **Import** button to import the KO files.

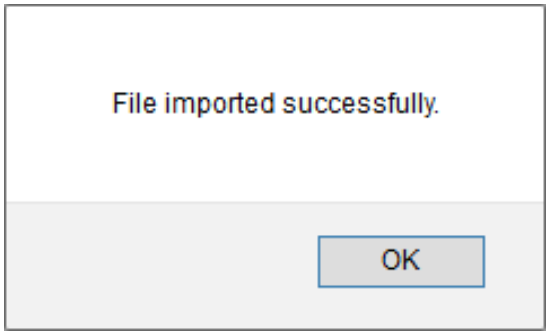
3. In the **Import** window, click **Browse** and locate the **KO_ Azure Active Directory.etko** file.



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



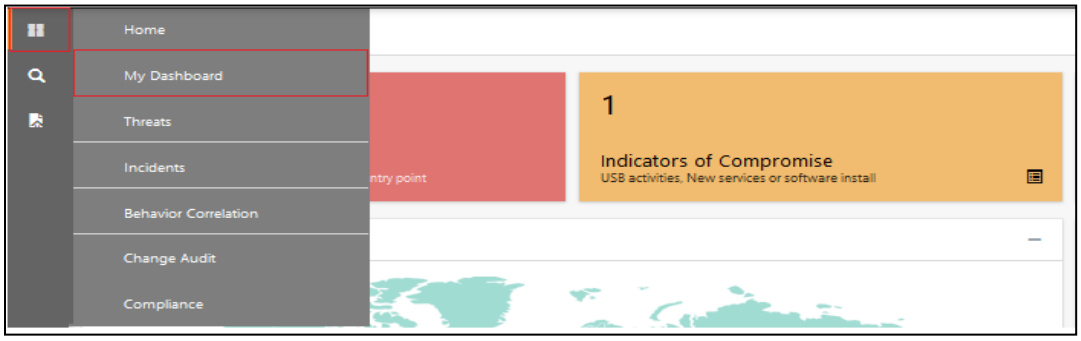
5. EventTracker displays a successful message on successfully importing the selected file in **Knowledge Objects**.



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

4.5 Dashboard

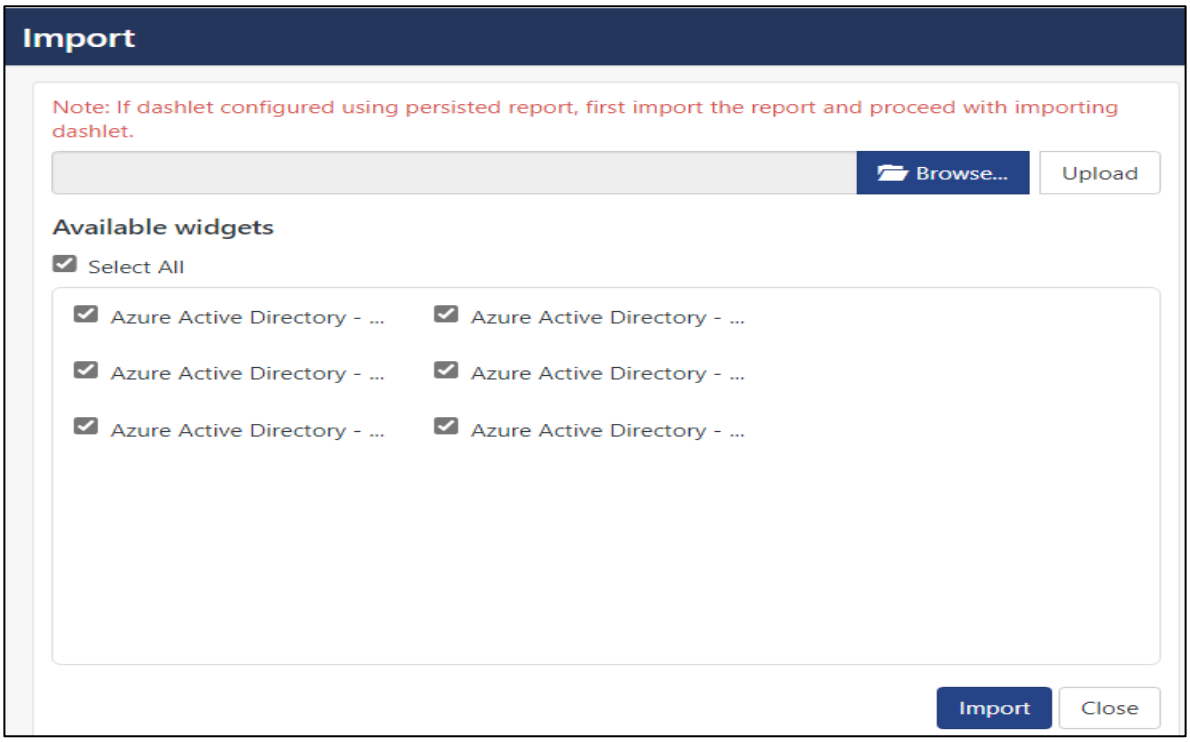
1. Log in to the **EventTracker** web interface and go to **Dashboard** > **My Dashboard**.



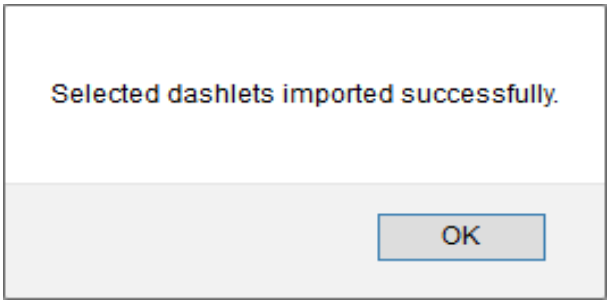
2. In the **My Dashboard** interface, click the **Import** button to import the dashlet files.

3. In the **Import** window, click **Browse** to locate the **Dashboards_ Azure Active Directory.etwd** file and then click **Upload.**

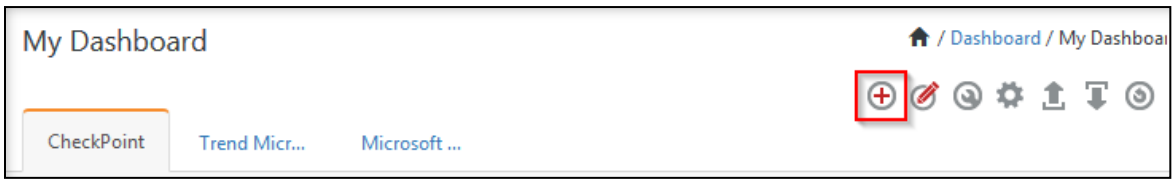
4. Click the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.



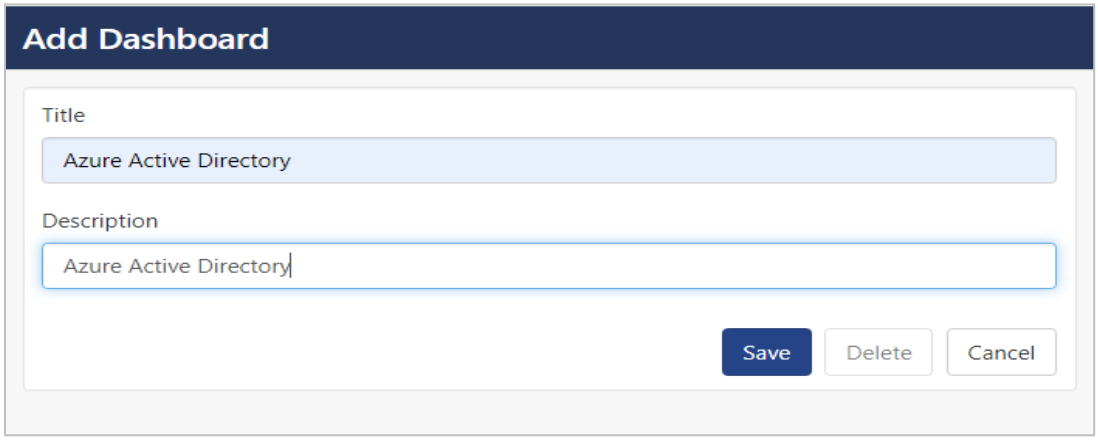
5. The EventTracker displays the success message on successfully importing the dashlet files.



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

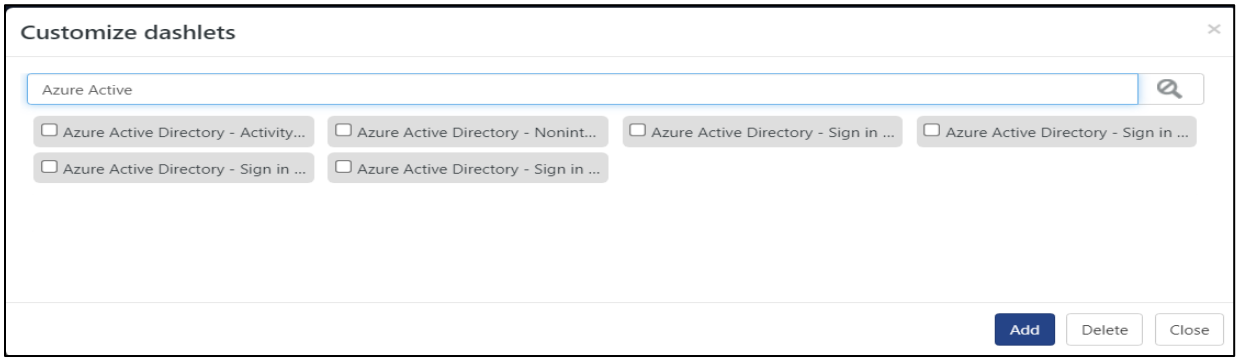


7. In the **Add Dashboard** interface, specify the **Title** and **Description** and click **Save**.



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

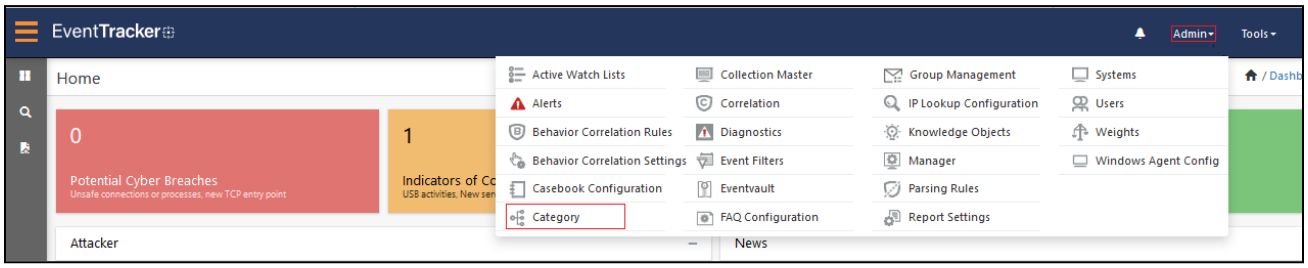
9. Search and select the newly imported dashlets and click **Add**.



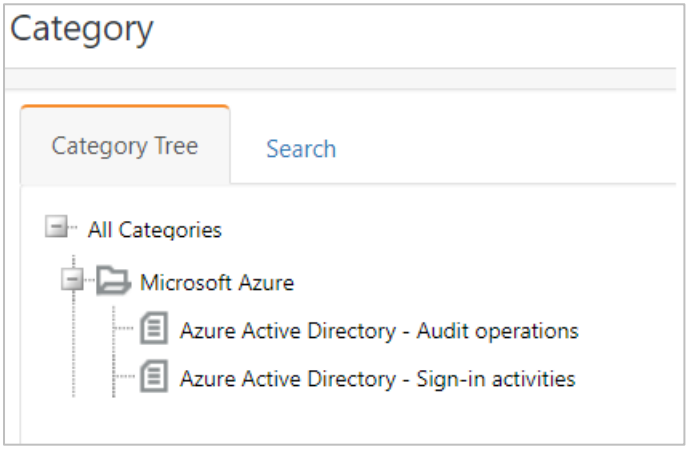
5 Verifying Azure Active Directory Knowledge Packs in EventTracker

5.1 Category

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

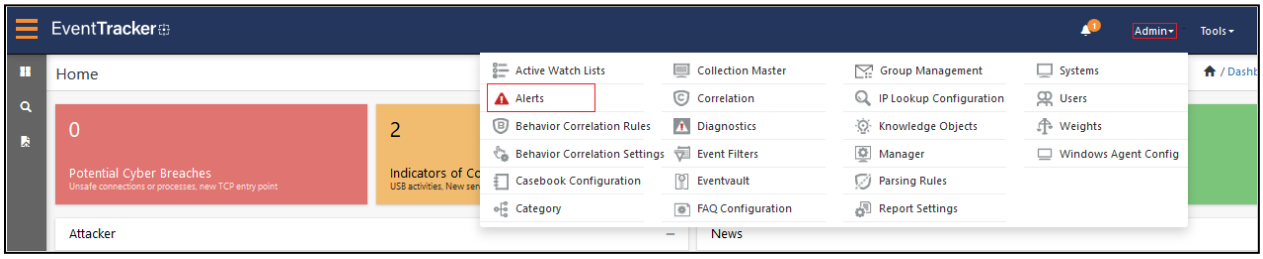


2. In the **Category** interface, under the **Category Tree** tab, click the **Microsoft Azure** group folder to expand and see the imported categories.



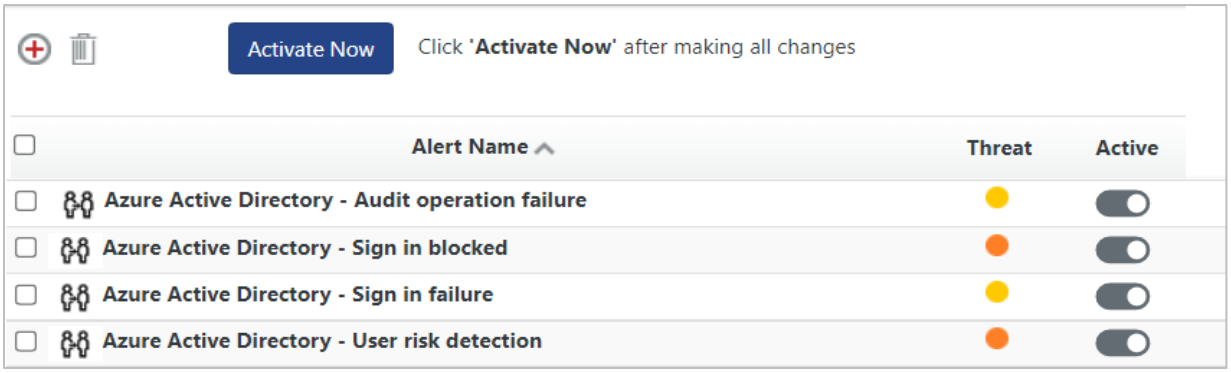
5.2 Alerts

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



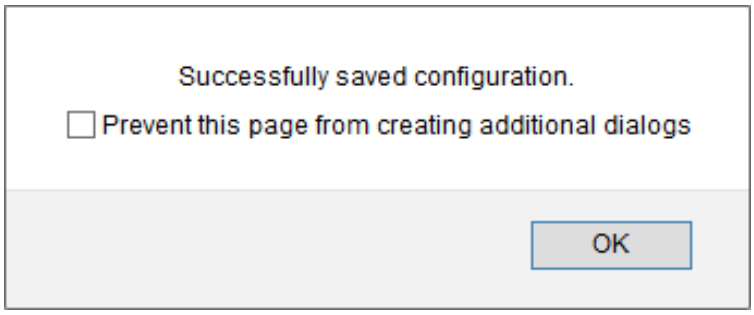
2. In the **Alerts** interface, type **Azure Active Directory** in the search field, and click the **Search** button.

3. The **Alerts** interface will display all the imported **Azure Active Directory** 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

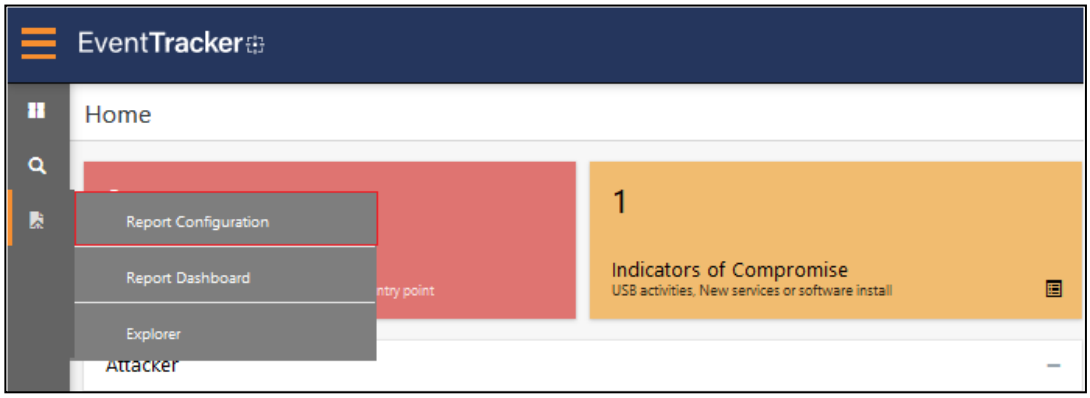
You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

Note

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

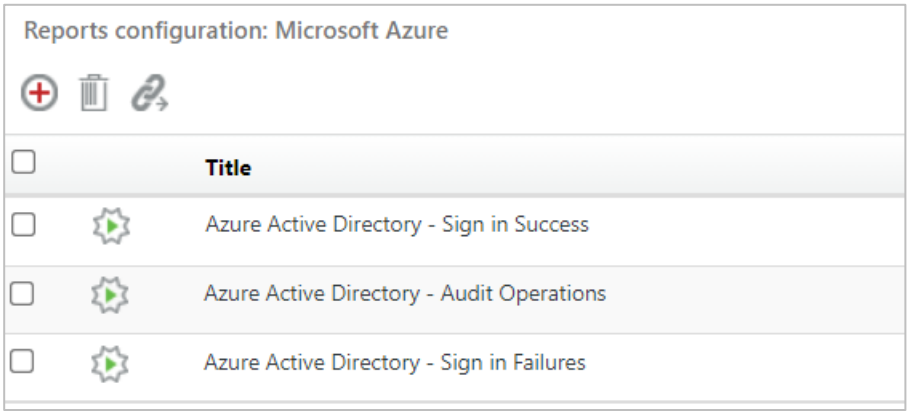
5.3 Reports

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



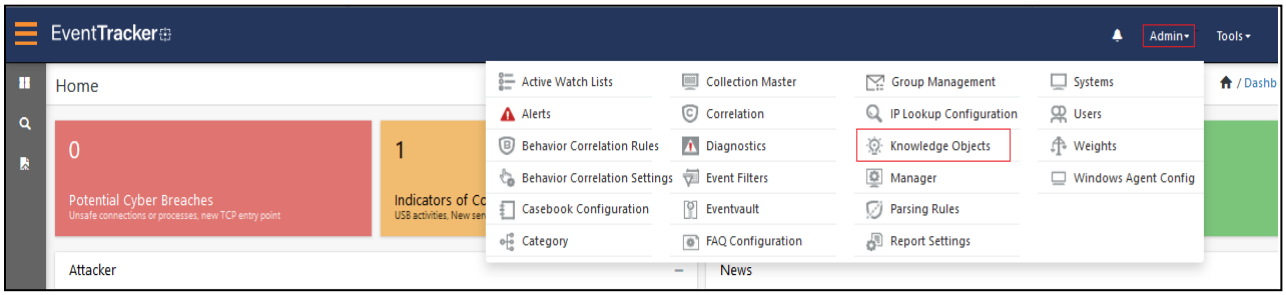
2. In the **Reports Configuration** interface, click **Defined**.
3. In the search field, type **Microsoft Azure** and click **Search** to search for the Azure Active Directory files.

4. EventTracker displays the reports for Azure Active Directory.

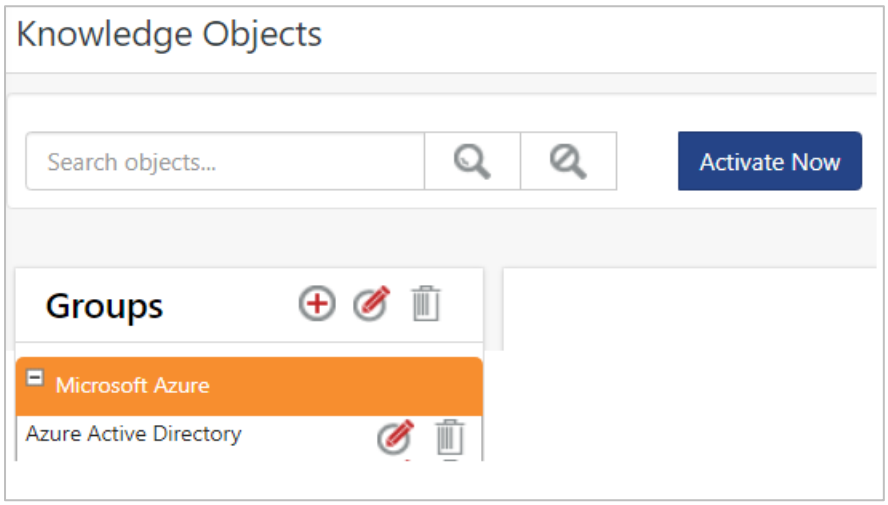


5.4 Knowledge Objects (KO)

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



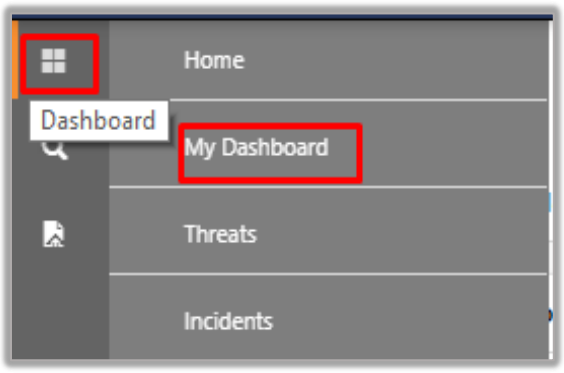
2. In the **Knowledge Object** interface, under **Groups** tree, click the **Microsoft Azure** group to expand and view the imported Knowledge objects.



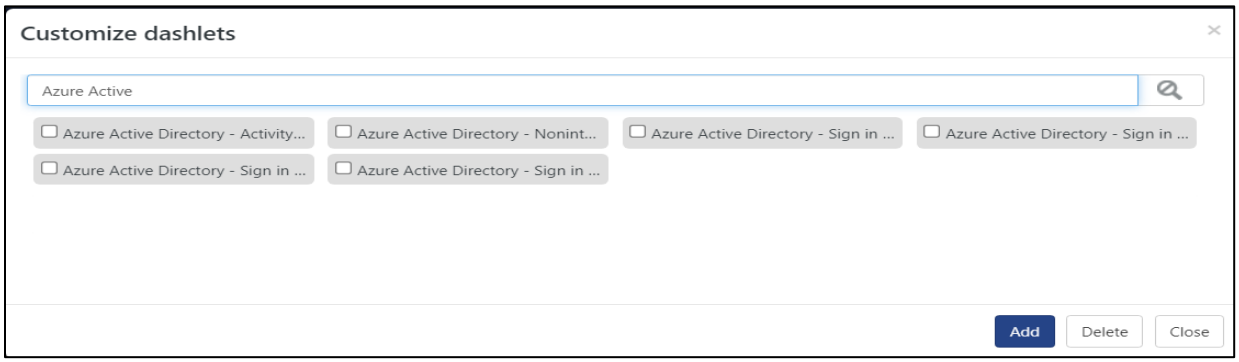
3. Click **Activate Now** to apply the imported Knowledge Objects.

5.5 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 Active Directory** in the search field.
3. The following Azure Active Directory 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