Integration Guide

Integrating Azure App Service with EventTracker

Publication Date:

March 31, 2022

Abstract

This guide provides instructions to retrieve the **Azure App Service** 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, 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 App Service.**

Audience

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

Table of Contents

1. Overview

Azure App Service helps to create apps faster with a one-of-a-kind cloud service to create enterprise-ready web and mobile apps quickly and easily for any platform or device and deploy them on a scalable and reliable cloud infrastructure.

EventTracker helps to monitor events from the Azure App Service. Its dashboard and reports will help you track, login activities of site content in the Azure App Service, IP access restriction with web traffic allowed or denied activities, and web traffic with user agent and status code which helps to detect potential directories brute force and invalid access.

2. Prerequisites

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

3. Configuring Azure App Service to Forward Logs to EventTracker

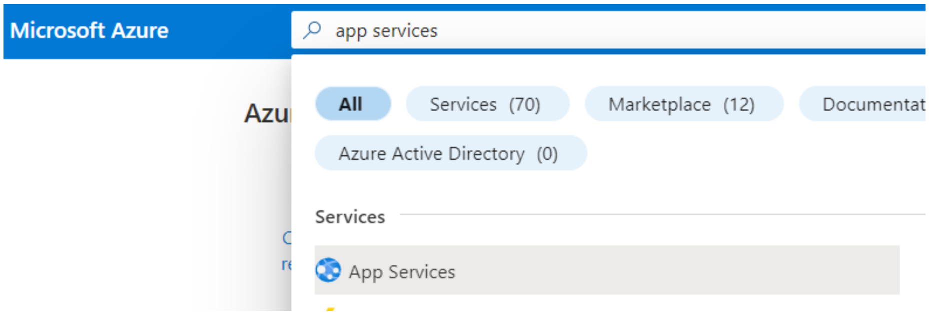
Azure App Service can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

3.1 Forwarding Event Hub data to EventTracker

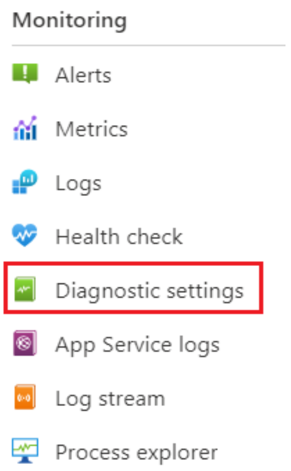
Refer to the Configuration of the Azure function app to forward logs to EventTracker.

3.2 Configuring Azure App Service to stream events to Event Hub

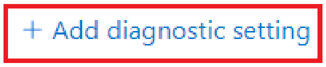
1. Login to portal.azure.com using the Admin account and create an event hub namespace, if not created.
2. Search and select **App Services** from **All services**.

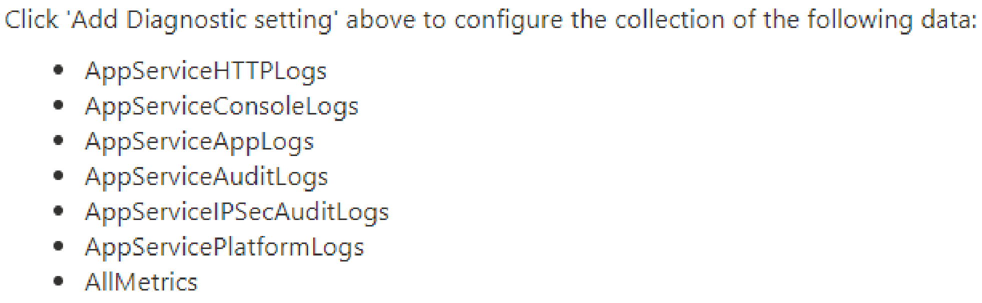


3. From the left panel under **Monitoring**, select **Diagnostics settings**.



4. Click on **Add diagnostics settings**.

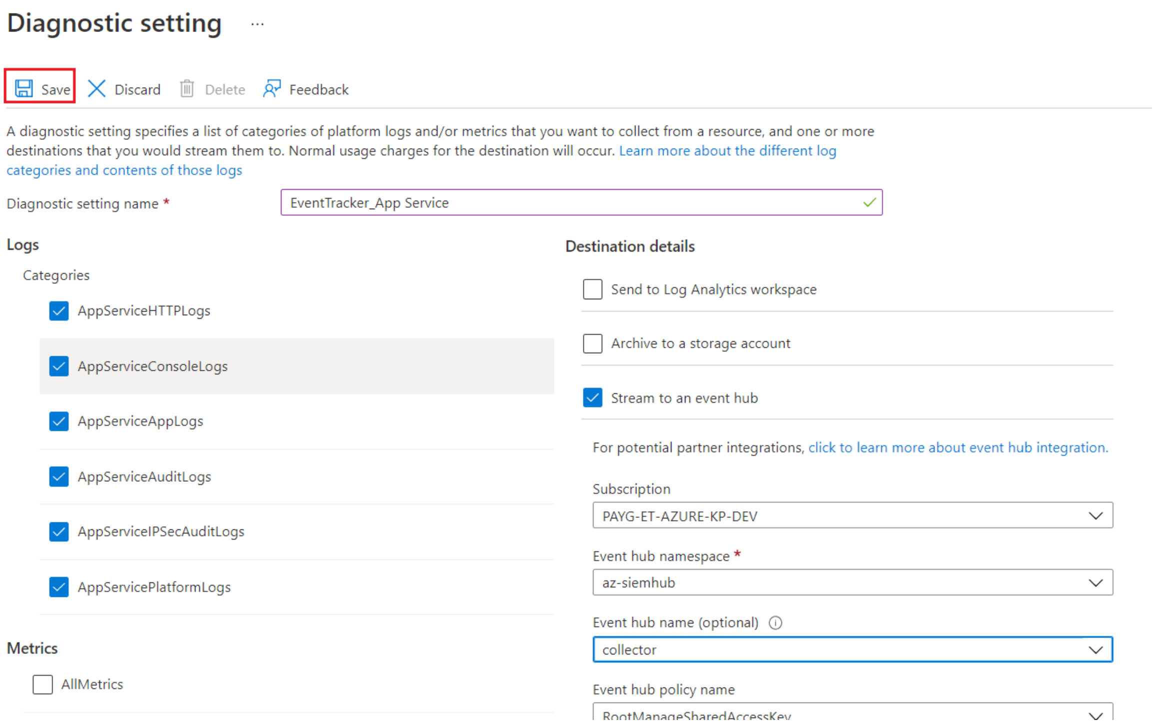




Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AppServiceHTTPLogs
- AppServiceConsoleLogs
- AppServiceAppLogs
- AppServiceAuditLogs
- AppServiceIPSecAuditLogs
- AppServicePlatformLogs
- AllMetrics

5. Provide the inputs.
   Diagnostics settings name, such as **EventTracker_App Service**.
   Select all **log** type, i.e., AppServiceHTTPLogs
   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 Event Hub created under the Event Hub namespace.
   - **Event Hub policy name:** Select the Event Hub policy.
6. Click **Save.**



Diagnostic setting ···

Save | Discard | Delete | Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * EventTracker_App Service

Logs

Categories

- ☑ AppServiceHTTPLogs
- ☑ AppServiceConsoleLogs
- ☑ AppServiceAppLogs
- ☑ AppServiceAuditLogs
- ☑ AppServiceIPSecAuditLogs
- ☑ AppServicePlatformLogs

Metrics

- □ AllMetrics

Destination details

- □ Send to Log Analytics workspace
- □ Archive to a storage account
- ☑ Stream to an event hub

For potential partner integrations, click to learn more about event hub integration.

Subscription: PAYG-ET-AZURE-KP-DEV

Event hub namespace *: az-siemhub

Event hub name (optional): collector

Event hub policy name: RootManageSharedAccessKey

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 Azure App Service.

4.1 Alerts

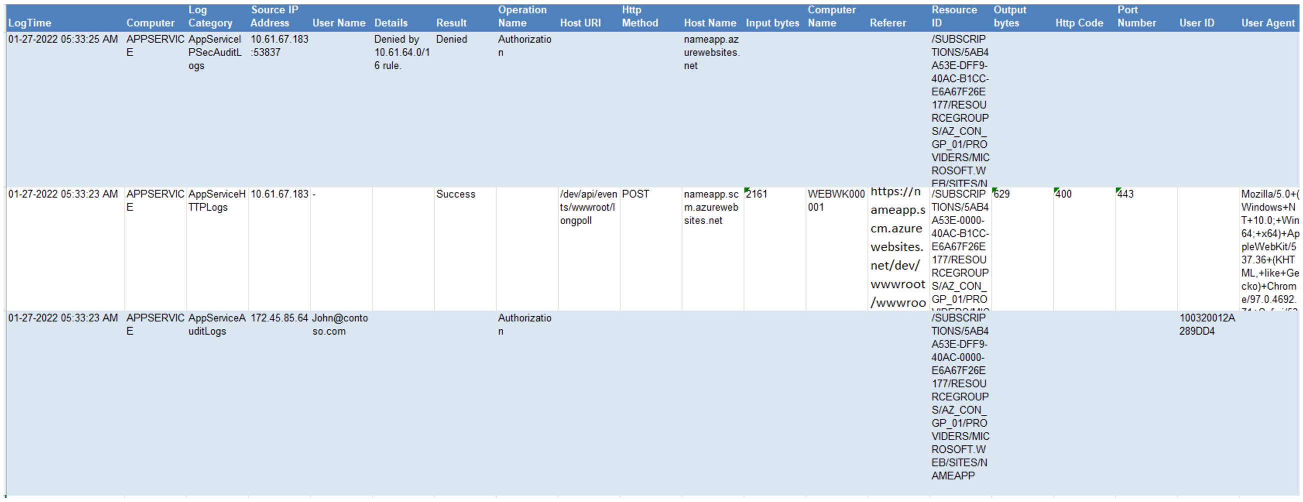
- **Azure App Service: Access denied by IP access restriction:** This alert indicates that an IP address is blocked by the access restriction rule in the Azure App Service.
- **Azure App Service: Illegal web call detected:** This alert indicates that an illegal web call is detected in the Azure App Service.
- **Azure App Service: Potential directories brute force detected:** This alert indicates that a potential directories brute force is detected in the Azure App Service.

4.2 Categories

- **Azure App Service – App service activities:** This category of the saved search will allow the users to parse the events that are specific to the app service activities on the Azure App Service.

4.3 Reports

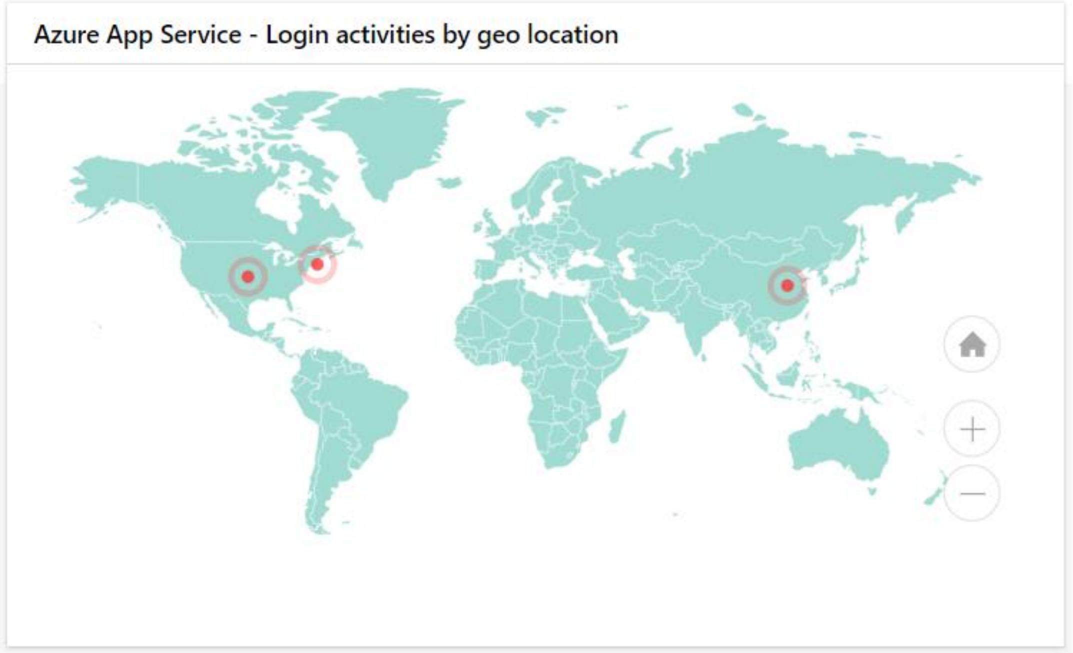
- **Azure App Service – App service activities:** This report provides a detailed summary of app service activities in the Azure App Service. It contains a source IP address, username, user agent, status code, port number, input bytes, output bytes, and more.



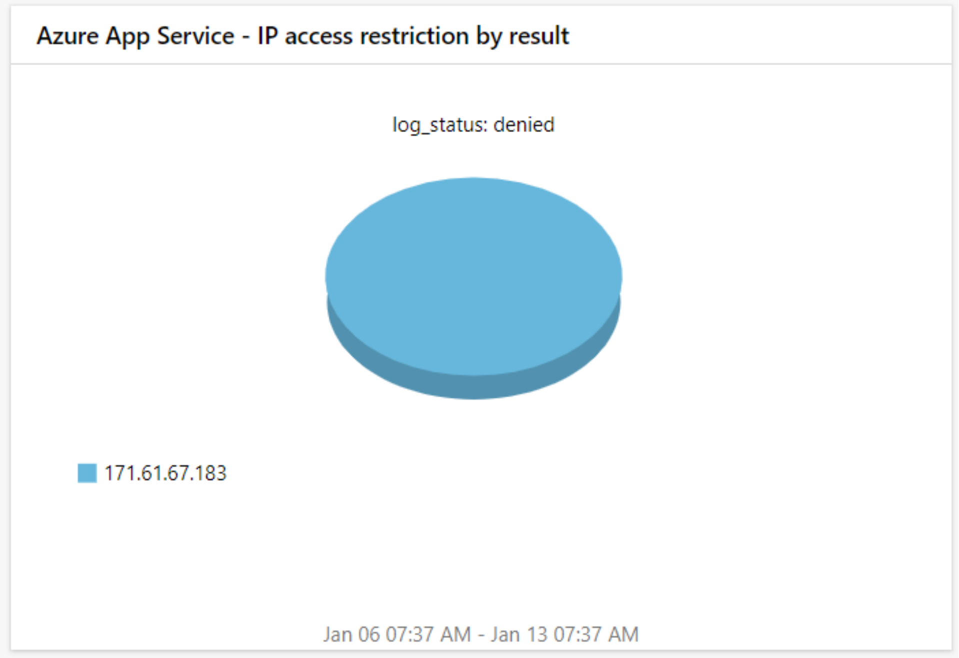
LogTime	Computer	Log Category	Source IP Address	User Name	Details	Result	Operation Name	Host URI	Http Method	Host Name	Input bytes	Computer Name	Referer	Resource ID	Output bytes	Http Code	Port Number	User ID	User Agent
01-27-2022 05:33:25 AM	APPSERVICE	AppServiceIPSecAuditLogs	10.61.67.183:53837		Denied by 10.61.64.0/16 rule.	Denied	Authorization			nameapp.azurewebsites.net				/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ_CON_GP_01/PROVIDERS/MICROSOFT.WEB/SITES/N					
01-27-2022 05:33:23 AM	APPSERVICE	AppServiceHTTPLogs	10.61.67.183	-		Success		/dev/api/events/wwwroot/longpoll	POST	nameapp.scm.azurewebsites.net	2161	WEBWK000001	https://nameapp.scm.azurewebsites.net/dev/wwwroot/wwwroo	/SUBSCRIPTIONS/5AB4A53E-0000-40AC-B1CC-E6A67F26E177/RESOURCEGROUPS/AZ_CON_GP_01/PRO	629	400	443		Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/97.0.4692.
01-27-2022 05:33:23 AM	APPSERVICE	AppServiceAuditLogs	172.45.85.64	John@contoso.com			Authorization							/SUBSCRIPTIONS/5AB4A53E-DFF9-40AC-0000-E6A67F26E177/RESOURCEGROUPS/AZ_CON_GP_01/PROVIDERS/MICROSOFT.WEB/SITES/NAMEAPP				100320012A289DD4	

4.4 Dashboards

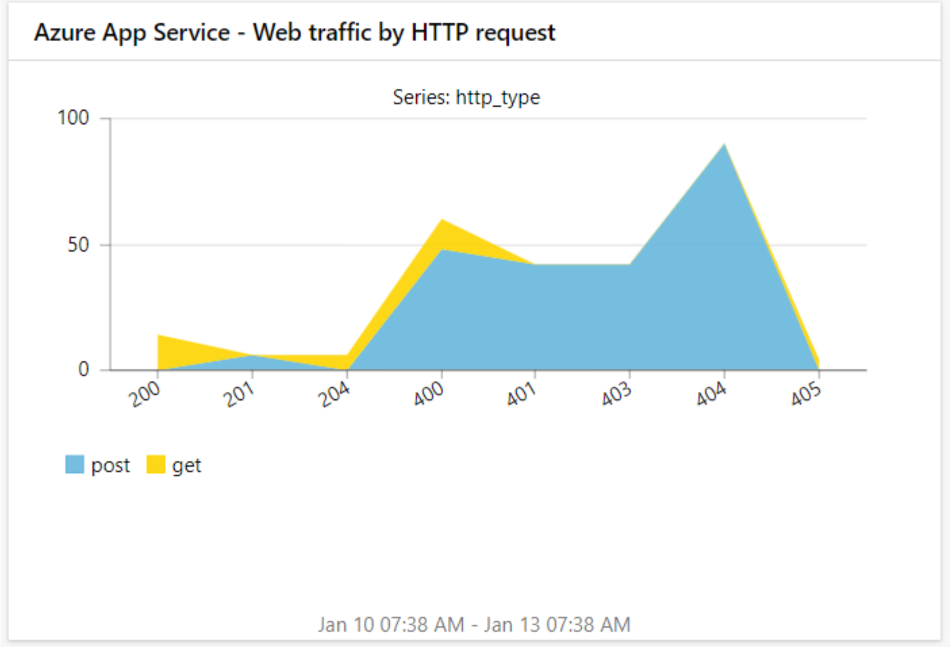
- **Azure App Service - Login activities by geo location**



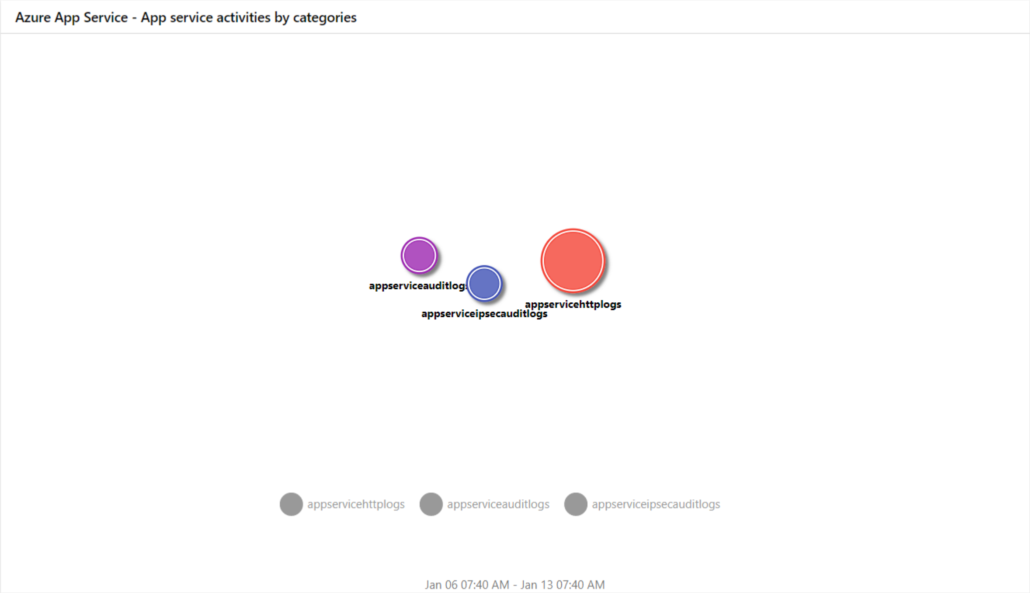
- **Azure App Service - IP access restriction by result**



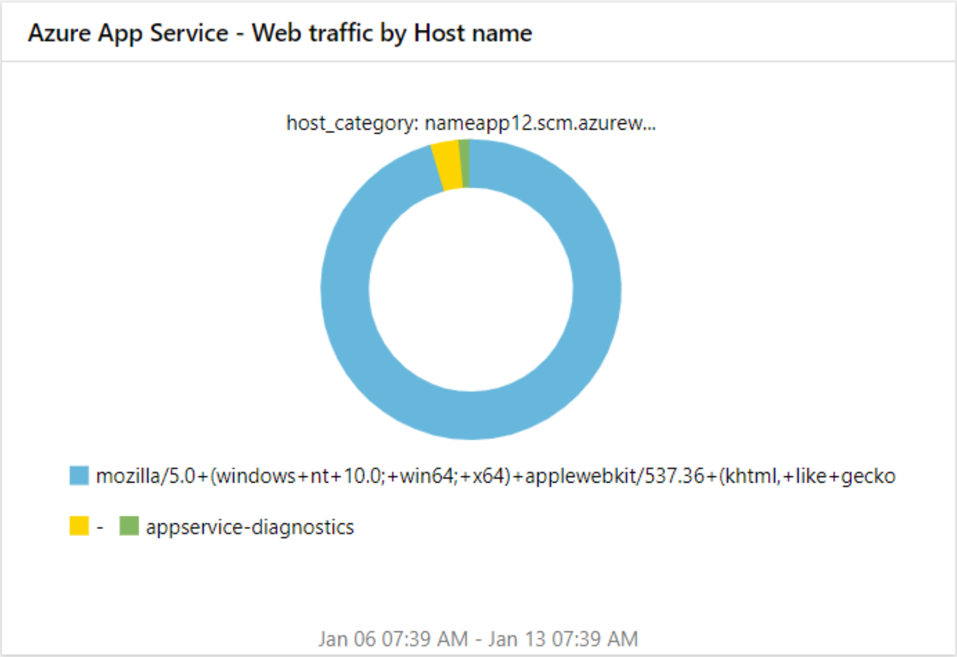
- **Azure App Service - Web traffic by HTTP request**



- **Azure App Service - App service activities by categories**



- **Azure App Service - Web traffic by Host name**

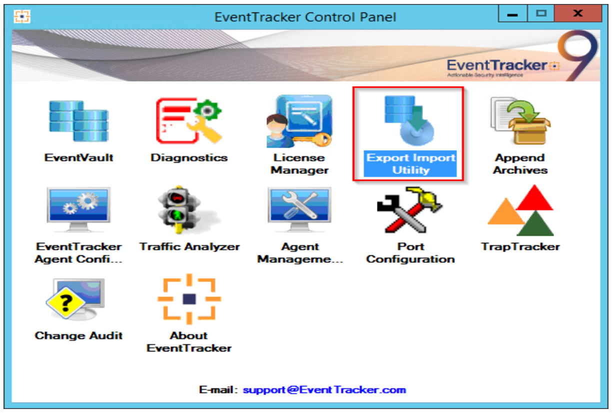


5. Importing Azure App Service Knowledge Packs into EventTracker

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**.

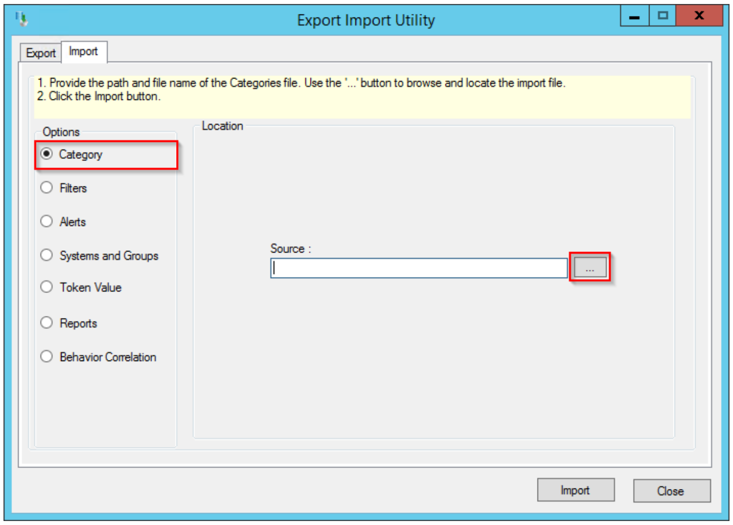


E-mail: support@EventTracker.com

3. Click the **Import** tab.

5.1 Categories

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

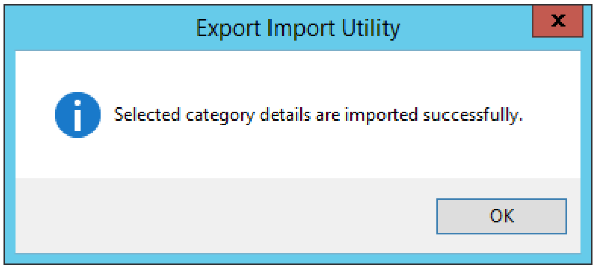


1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

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

   EventTracker displays a success message.

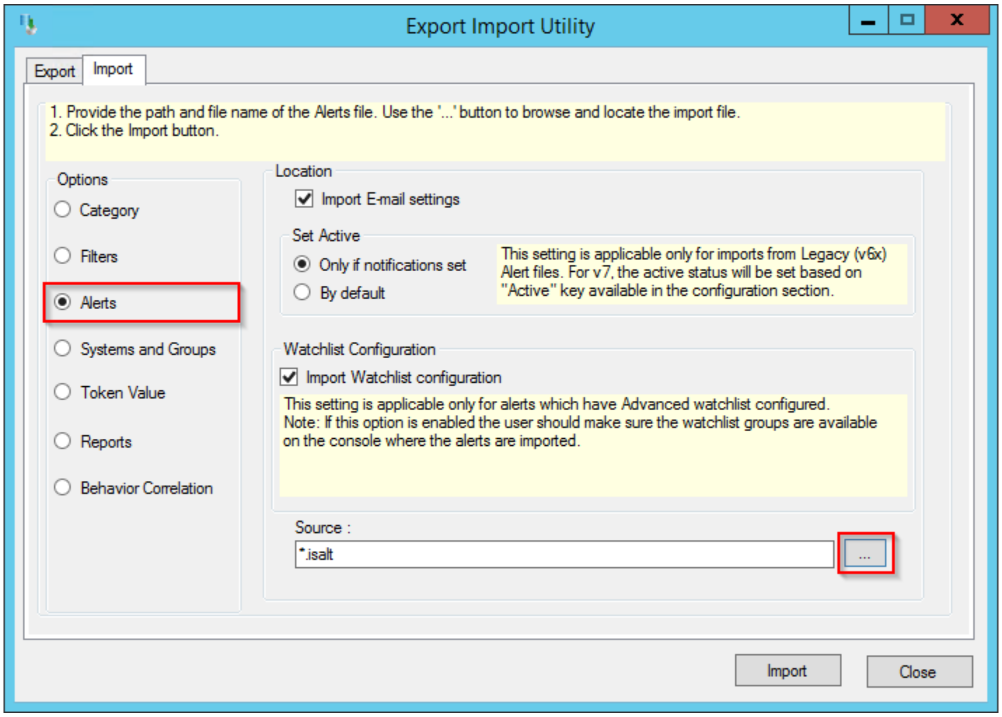


Selected category details are imported successfully.

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

5.2 Alerts

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



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options
○ Category
○ Filters
● Alerts
○ Systems and Groups
○ Token Value
○ Reports
○ Behavior Correlation

Location
☑ Import E-mail settings

Set Active
● Only if notifications set
○ By default

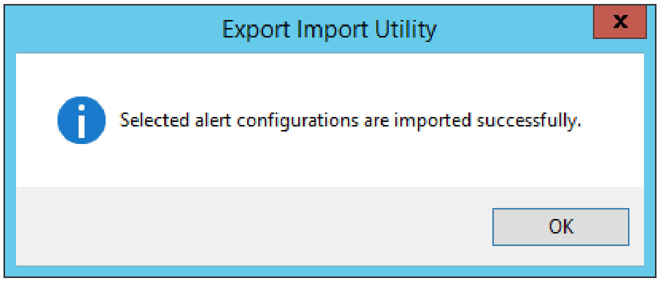
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Watchlist Configuration
☑ Import Watchlist configuration

This setting is applicable only for alerts which have Advanced watchlist configured.
Note: If this option is enabled the user should make sure the watchlist groups are available on the console where the alerts are imported.

Source : *.isalt ...

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

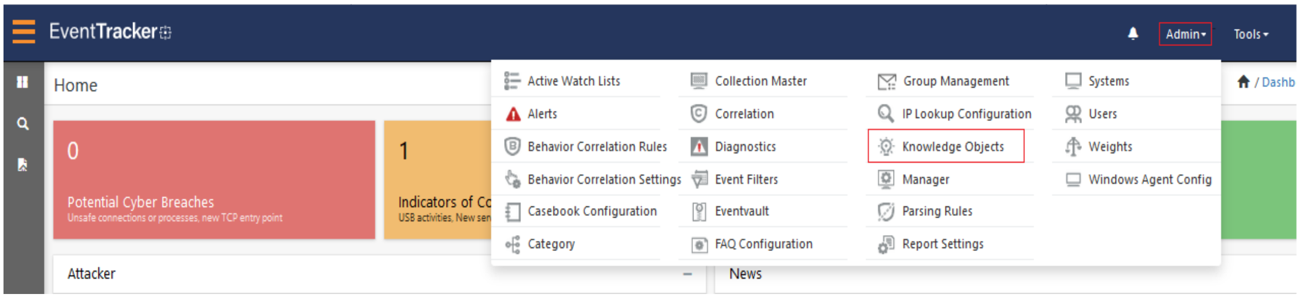


Selected alert configurations are imported successfully.

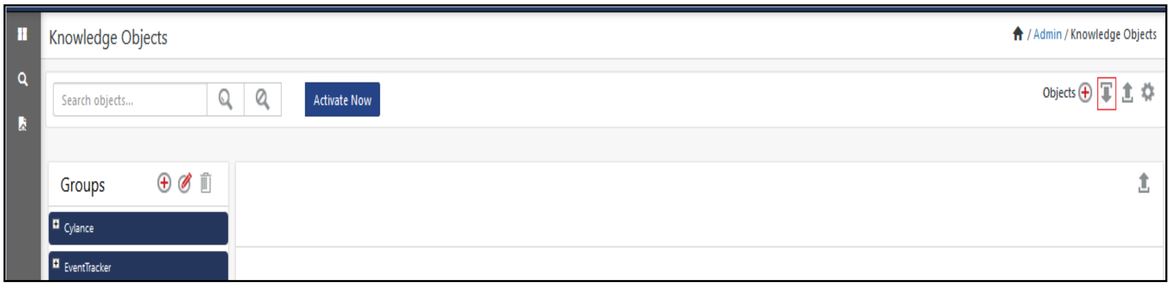
4. Click **OK**, and then click **Close**.

5.3 Knowledge Objects (KO)

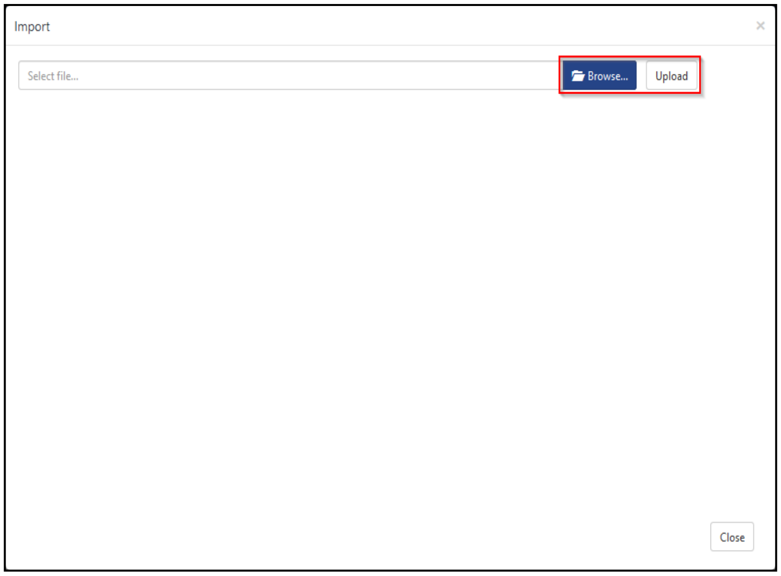
1. Click **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.



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

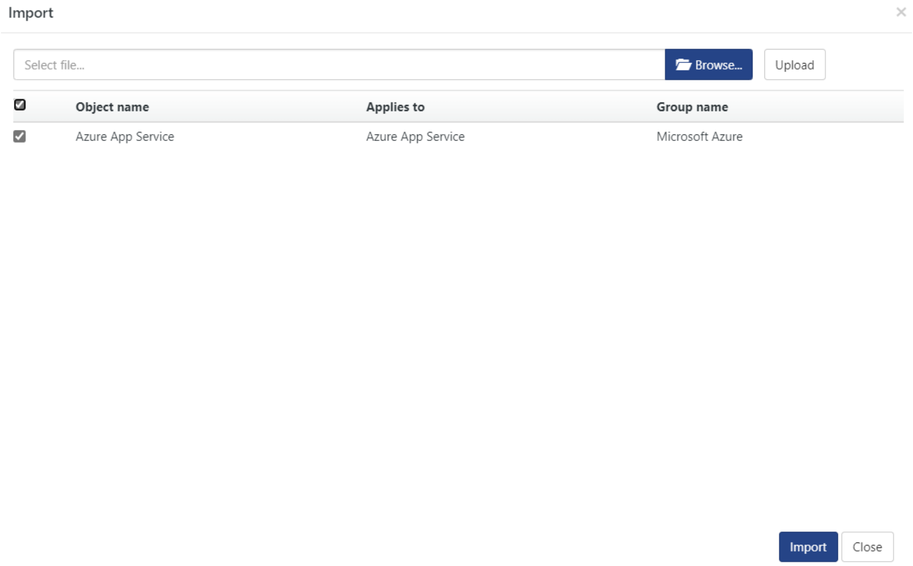


3. Click **Browse**.



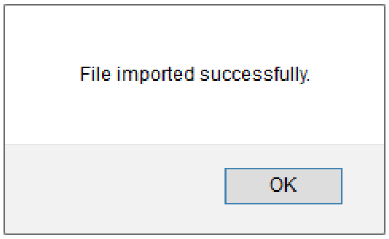
4. Locate the file named **KO_ Azure App Service.etko**.

5. Select the check box and then click the ⤓ **Import** option.



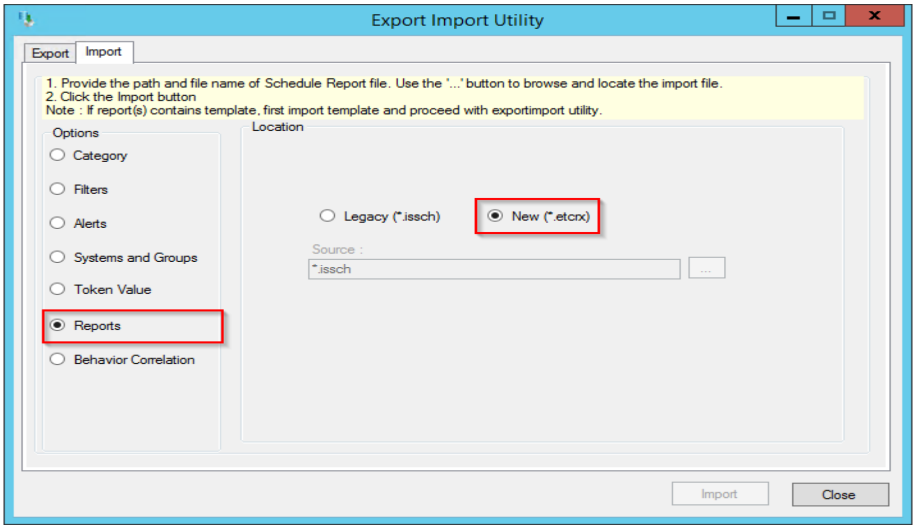
☑	Object name	Applies to	Group name
☑	Azure App Service	Azure App Service	Microsoft Azure

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


File imported successfully.

5.4 Reports

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



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Options

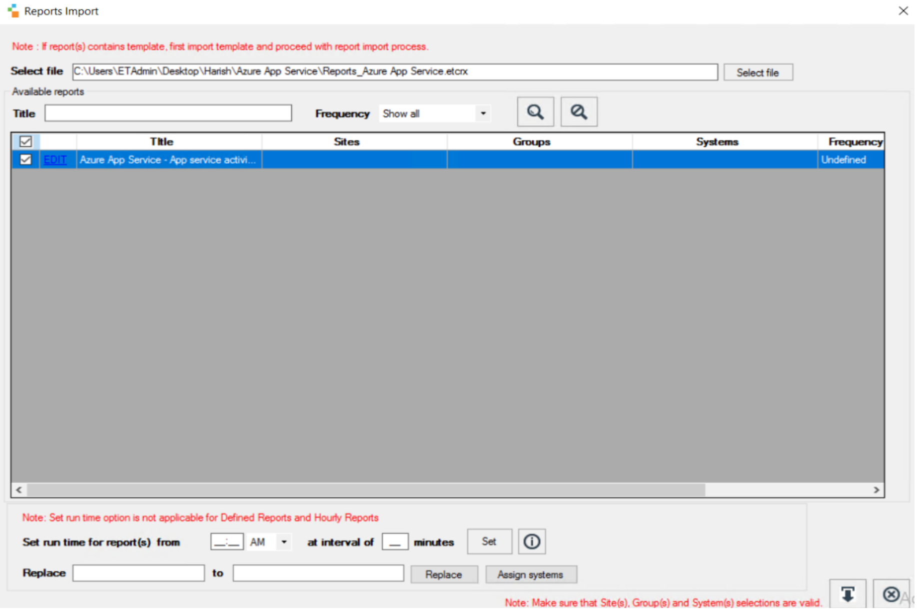
- ○ Category
- ○ Filters
- ○ Alerts
- ○ Systems and Groups
- ○ Token Value
- ● Reports
- ○ Behavior Correlation

Location

○ Legacy (*.issch) ● New (*.etcrx)

Source : *.issch

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



Note : If report(s) contains template, first import template and proceed with report import process.

Select file C:\Users\ETAdmin\Desktop\Harish\Azure App Service\Reports_Azure App Service.etcrx

Title

Frequency Show all

☑		Title	Sites	Groups	Systems	Frequency
☑	EDIT	Azure App Service - App service activi...				Undefined

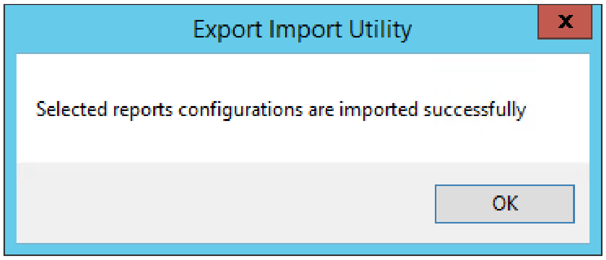
Note: Set run time option is not applicable for Defined Reports and Hourly Reports

Set run time for report(s) from __:__ AM at interval of __ minutes

Replace to

Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

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

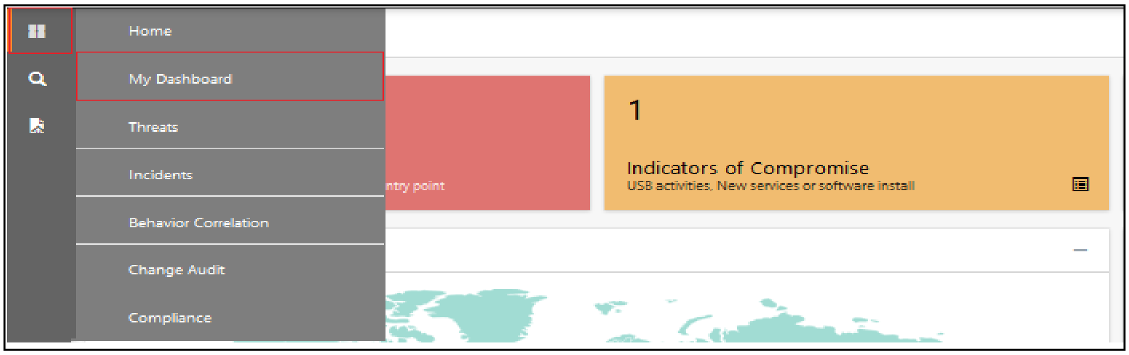


Selected reports configurations are imported successfully

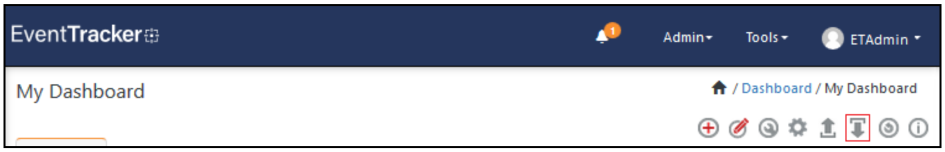
5.5 Dashboards

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

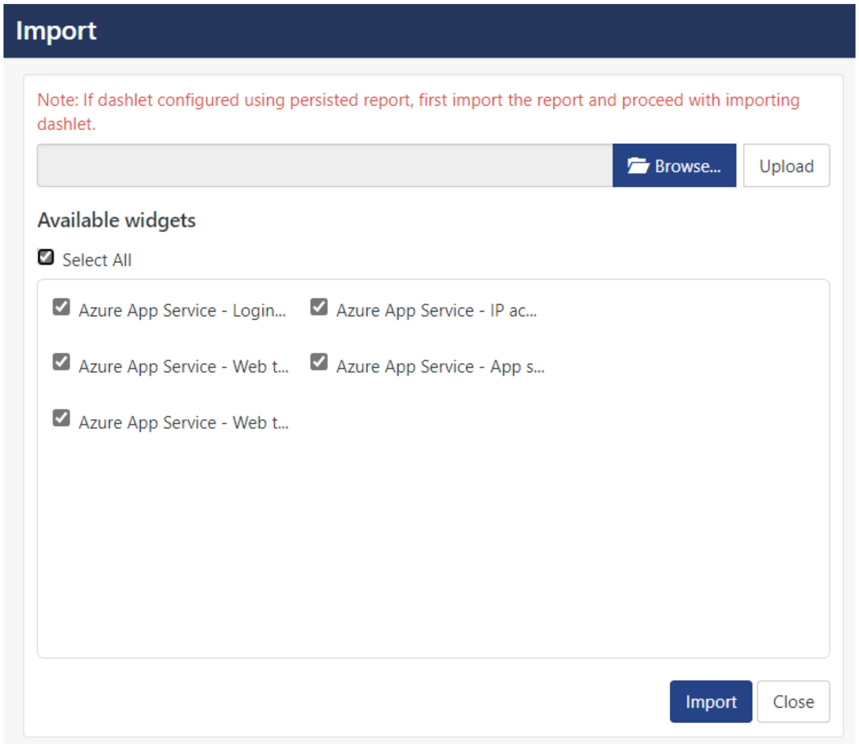
1. Open **EventTracker** in a browser and log on.



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



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



Import

Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.

Browse... Upload

Available widgets

☑ Select All

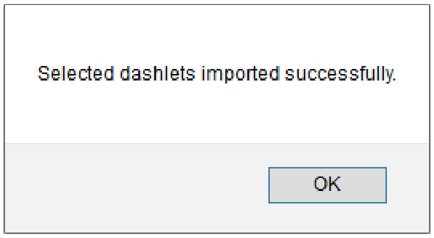
☑ Azure App Service - Login... ☑ Azure App Service - IP ac...

☑ Azure App Service - Web t... ☑ Azure App Service - App s...

☑ Azure App Service - Web t...

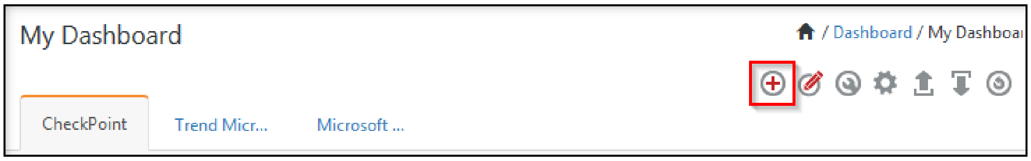
Import Close

6. Import is now completed successfully.

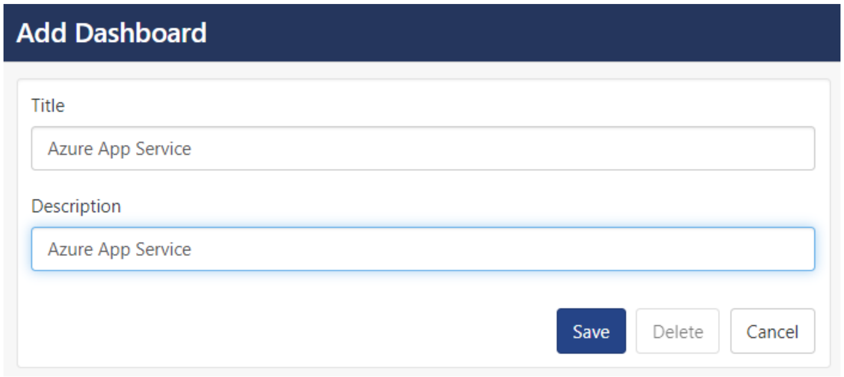


Selected dashlets imported successfully.

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



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

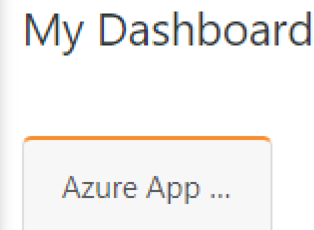


Add Dashboard

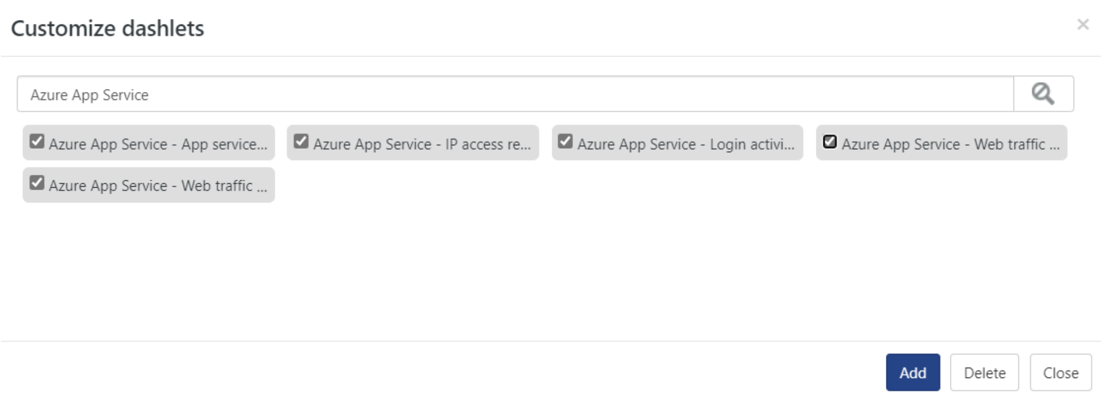
Title: Azure App Service

Description: Azure App Service

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



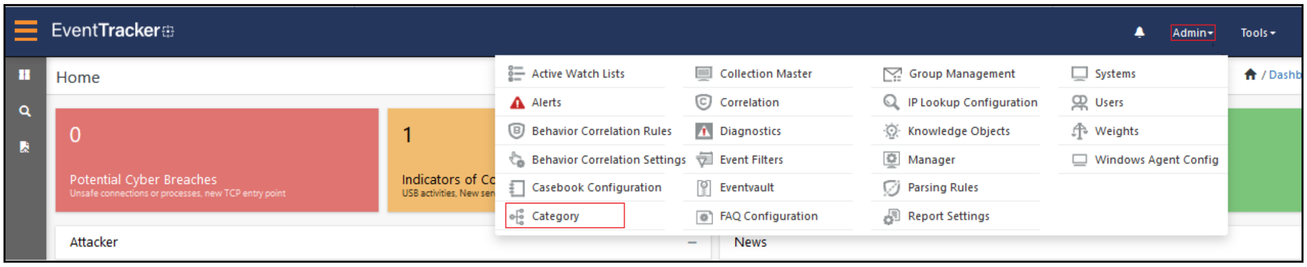
10. Select the imported dashlets and click **Add**.


Customize dashlets
×
Azure App Service
☑ Azure App Service - App service...
☑ Azure App Service - IP access re...
☑ Azure App Service - Login activi...
☑ Azure App Service - Web traffic ...
☑ Azure App Service - Web traffic ...
Add
Delete
Close

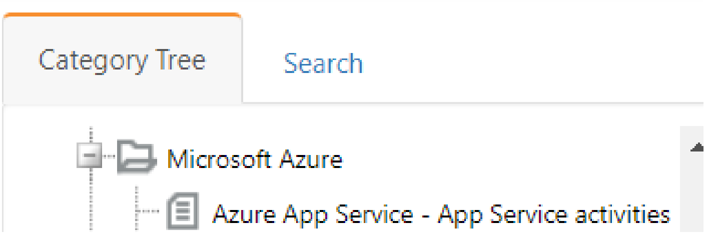
6. Verifying Azure App Service Knowledge Packs in EventTracker

6.1 Categories

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

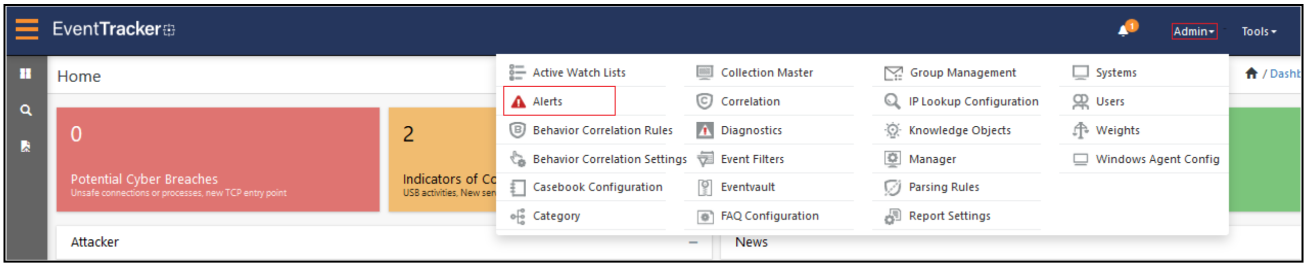


3. In the **Category Tree**, scroll down and expand the **Microsoft Azure** group folder to view the imported category.

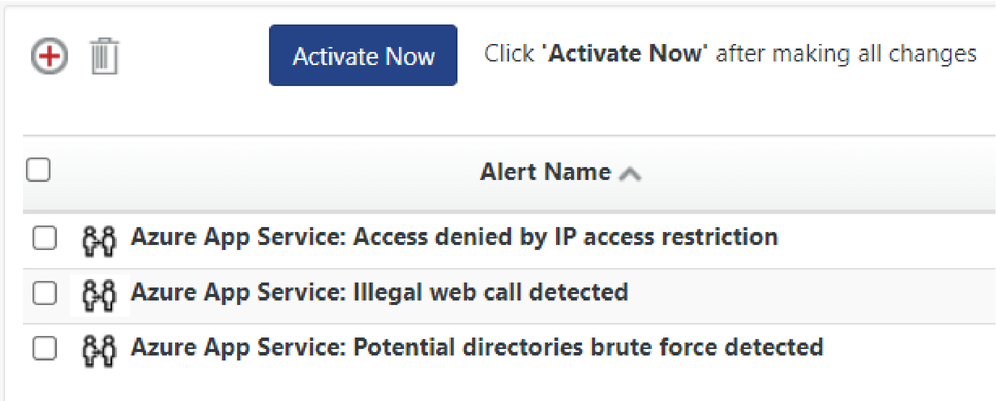


6.2 Alerts

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



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

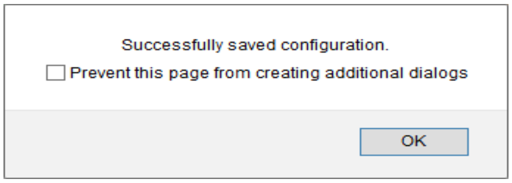


Click '**Activate Now**' after making all changes

□	Alert Name
□	Azure App Service: Access denied by IP access restriction
□	Azure App Service: Illegal web call detected
□	Azure App Service: Potential directories brute force detected

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

   EventTracker displays a message box.



Successfully saved configuration.

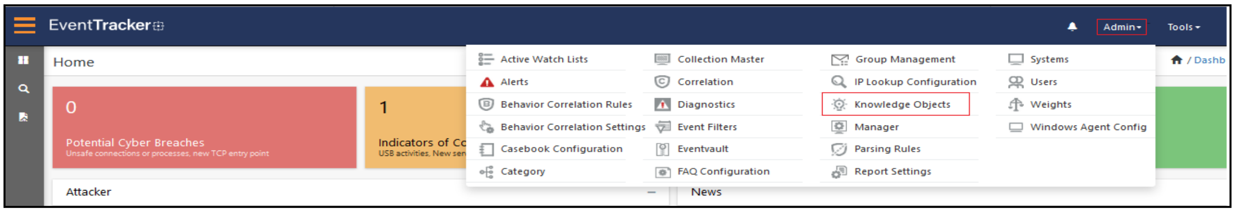
□ Prevent this page from creating additional dialogs

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

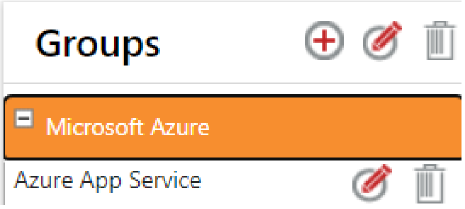
NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Objects

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



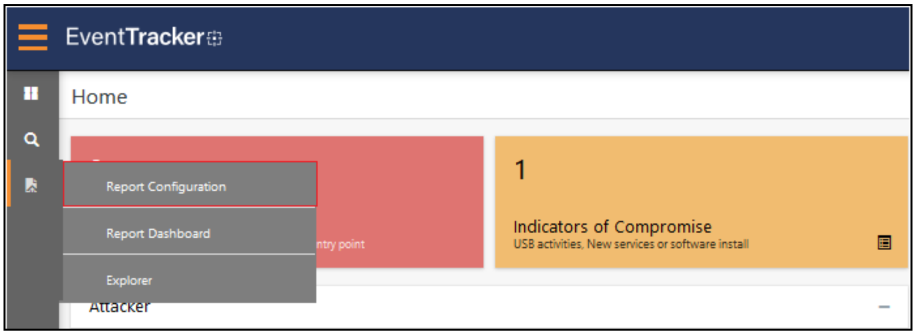
2. In the Knowledge Object tree, expand the **Microsoft Azure group** folder to view the imported Knowledge Objects.



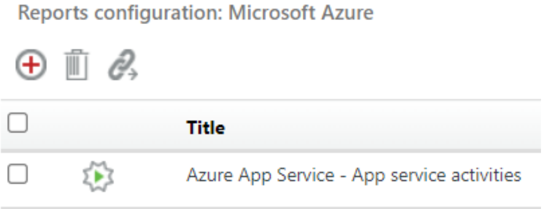
3. Click **Activate Now** to apply the imported Knowledge Objects.

6.4 Reports

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



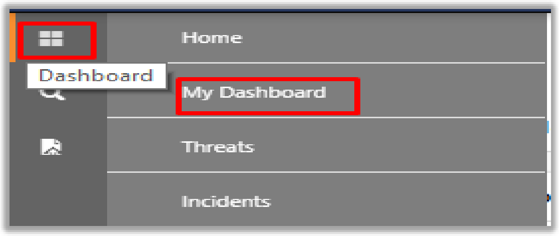
2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Microsoft Azure** group folder to view the imported reports.


Reports configuration: Microsoft Azure

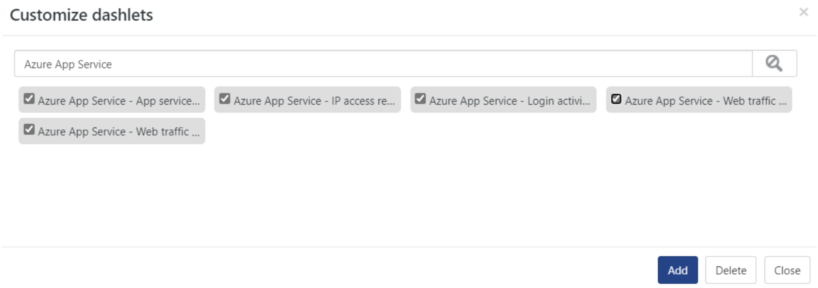
		Title
□		Azure App Service - App service activities

6.5 Dashboards

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



2. Click **Search** for the **Azure App Service.** You will see the following screen.



Customize dashlets

Azure App Service

☑ Azure App Service - App service...

☑ Azure App Service - IP access re...

☑ Azure App Service - Login activi...

☑ Azure App Service - Web traffic ...

☑ Azure App Service - Web traffic ...

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