Netsurion™ | EventTracker

Integrate Microsoft Azure

EventTracker v.9x and above

Publication Date: April 12, 2019

Abstract

This guide provides instructions to configure Azure to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Azure Activity, Azure Intune and Keyvault.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 9.x and later, and Microsoft Azure.

Audience

IT Admins, Azure administrators and EventTracker users who wish to forward logs to EventTracker Manager and monitor events using EventTracker Enterprise.

Table of Contents

Overview

EventTracker Knowledge pack for Microsoft Azure captures important and critical activities in Azure. Monitoring these activities is critical from a security aspect and is required for compliance and operational reasons. The dashboards, reports will help you in getting deeper insights to analyze various security use cases like azure resource and service activities and changes.

EventTracker helps you to monitor day to day activities of Azure resource activities, Intune and Keyvault audit activities.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **PowerShell 5.0** should be installed on EventTracker Manager.
- App should be registered in Azure AD with **Azure Management API** and **Microsoft graph API** permission. Instructions are mentioned here.
- Please enable following URL, if there is any web filter or firewall in between:
    - https://graph.microsoft.com
    - https://login.windows.net
    - https://manage.office.com

Configure Azure to forward logs to EventTracker

1. To create "**Microsoft graph** and **Azure Management API"** enabled app in Azure AD, please follow the steps mentioned here.
2. After successful creation of user and application, run the Azure Integrator.

EventTracker Integrator for Azure

You need to follow these steps, if you want to create application.

1. Please contact EventTracker Support for Azure Integration package.
2. Run executable file "**Azure Integrator.exe"**.

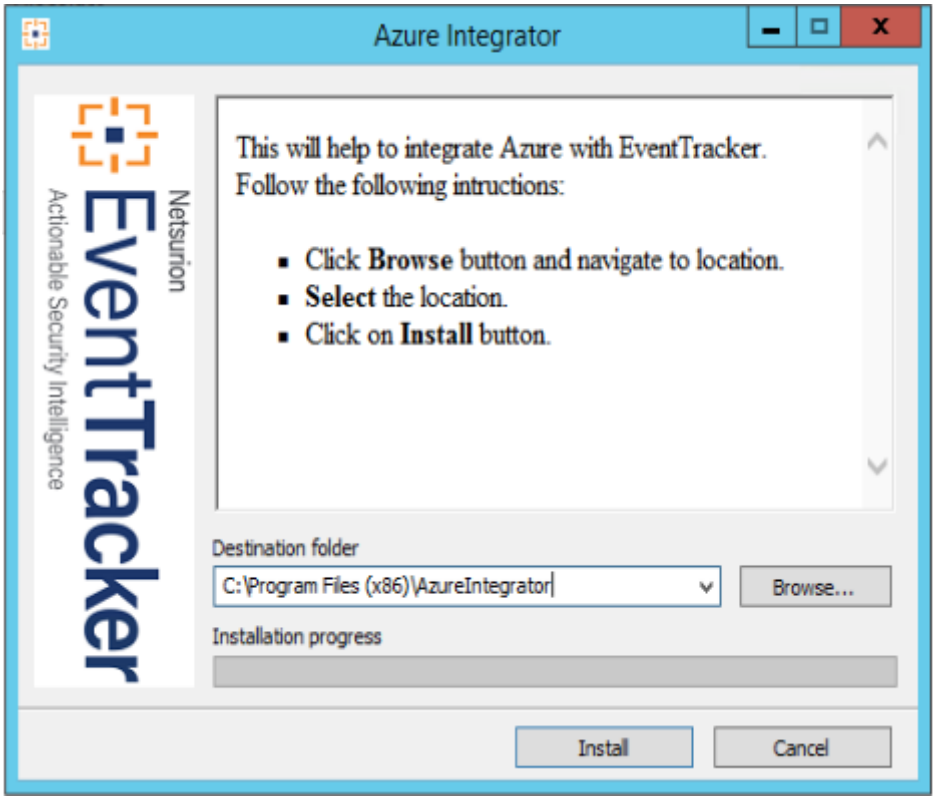

Figure 1

After launching integrator, it will check for PowerShell compatibility. If it is found compatible, integrator will allow you to configure Azure. Otherwise, update PowerShell on the EventTracker Manager machine.

3. Please follow the Register Application section and permission sections for application creation respectively. Fill the details in the Application.

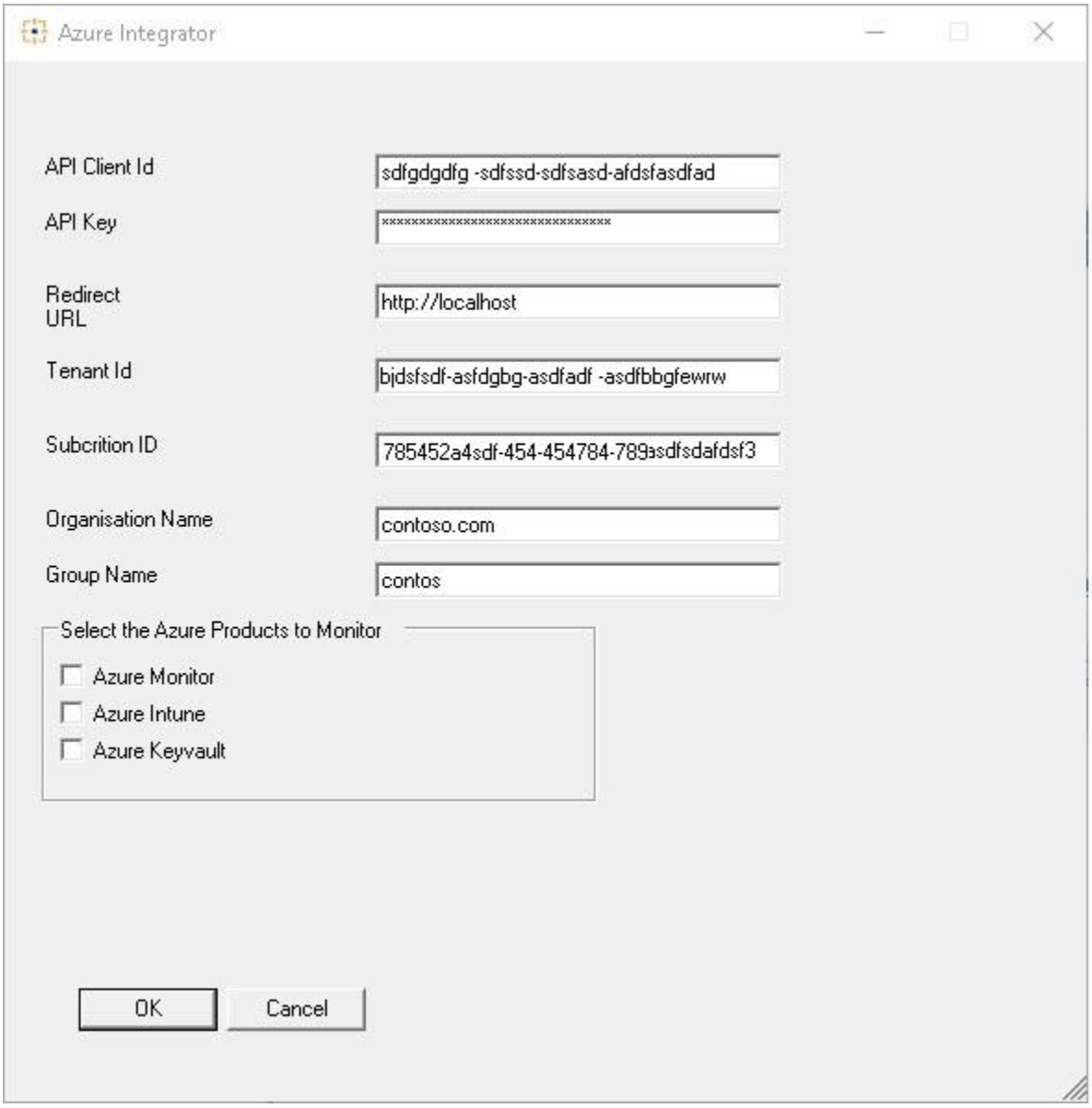

Figure 2

4. Fill the details of the app registered in Azure AD with Microsoft graph and Azure Management API permission. If user doesn't have app registered in Azure AD, please follow the instructions mentioned here.
5. Provide the tenant ID for the enterprise. Please follow the instruction mentioned here, if tenant ID is not known.
6. Once you have filled the appropriate fields in the forms, it will enable the **Select Azure Product** checkboxes.
7. Select the Check box which is required to monitor.
8. If Azure Intune has been selected, it will pop up the browser window to authorize the client. Login with Azure administrator account to authorize the application.

9. If the browser window is not popped-up, it will pop up a form with URL. Click "**Copy URL to Clipboard**" button.

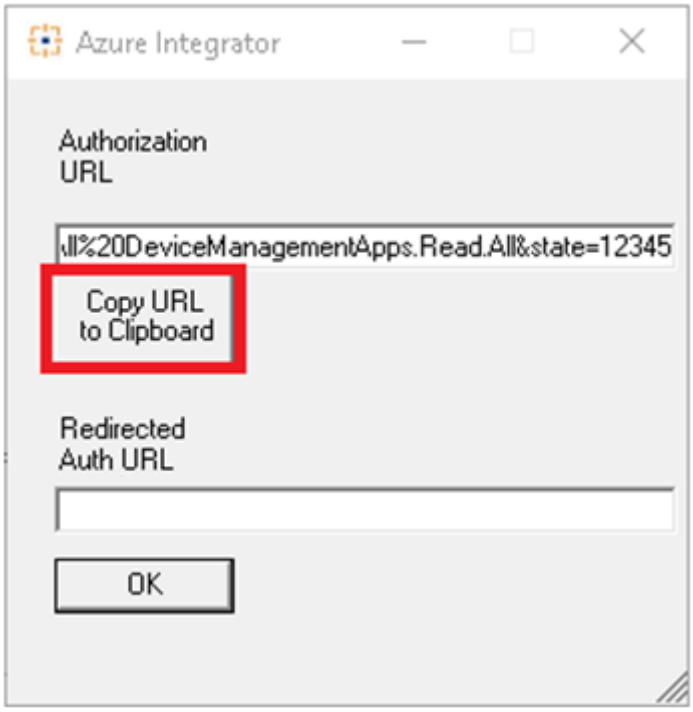

Figure 3

10. Once the link is copied, paste it in your web browser and login with azure administrator credentials.
11. If the application is authorized, the page will redirect to your localhost or redirect to the URL, which you are given.
12. Copy the redirected URL from the browser and paste it in **Redirected Auth URL** text box and click OK to proceed further.
13. If Azure Keyvault Auditing is enabled, please provide the azure Keyvault auditing storage account and storage account resource group.

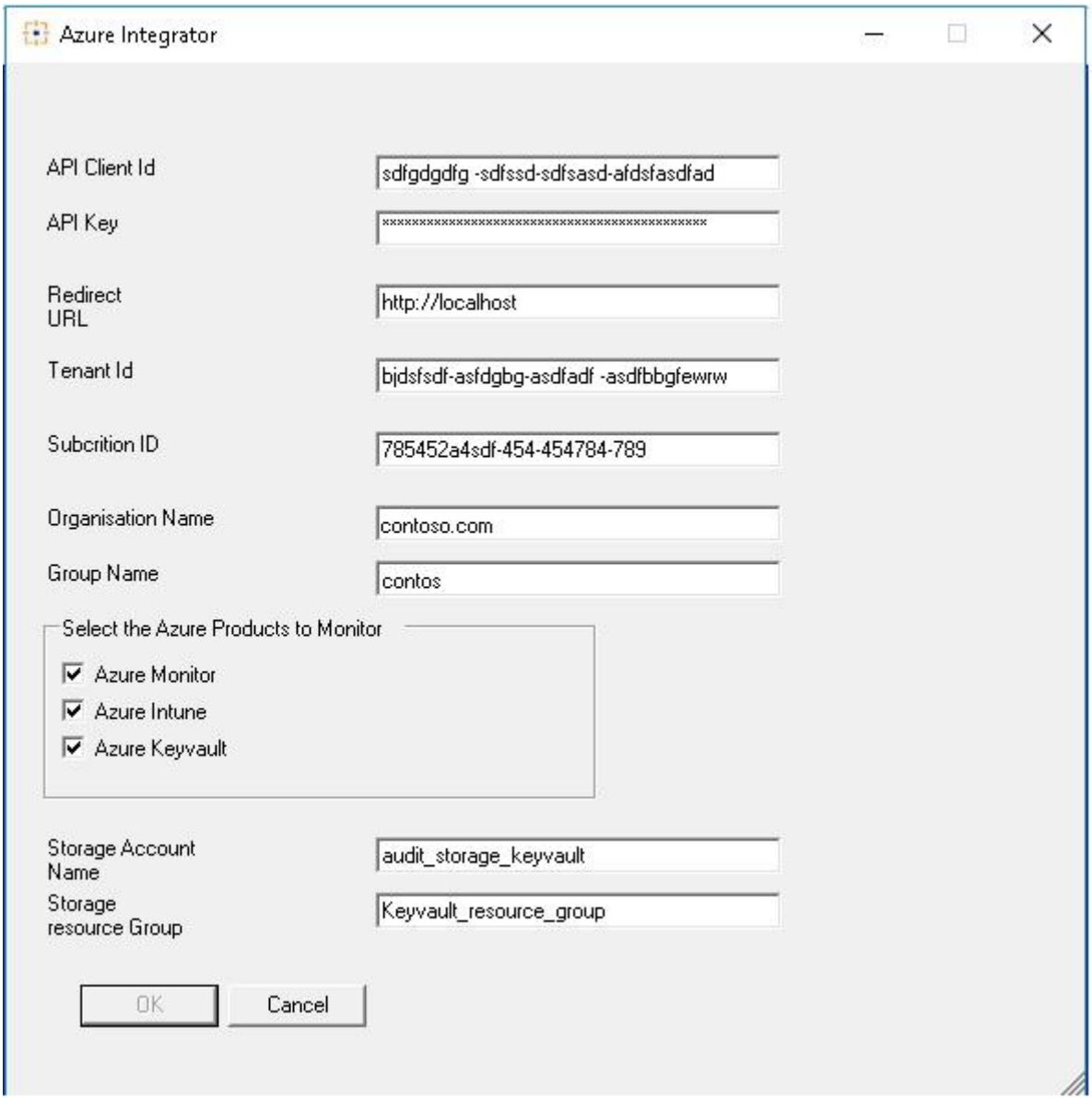

Figure 4

14. Once you provide all the details in Integrator “OK” button will be enabled.
15. Click on **OK** button to complete the Integration.

Register Application with your Azure Active Directory Tenant

If Application has not been registered in Azure AD, please follow the below procedure. This procedure should be carried out by a user having **Global Administrator** rights in Azure.

1. Sign in to the Azure portal.
2. If your account gives you access to more than one, click your account in the top right corner, and set your portal session to the desired Azure AD tenant.
3. In the left-hand navigation pane, click the **Azure Active Directory** service, click **App registrations**, and click **New application registration**.

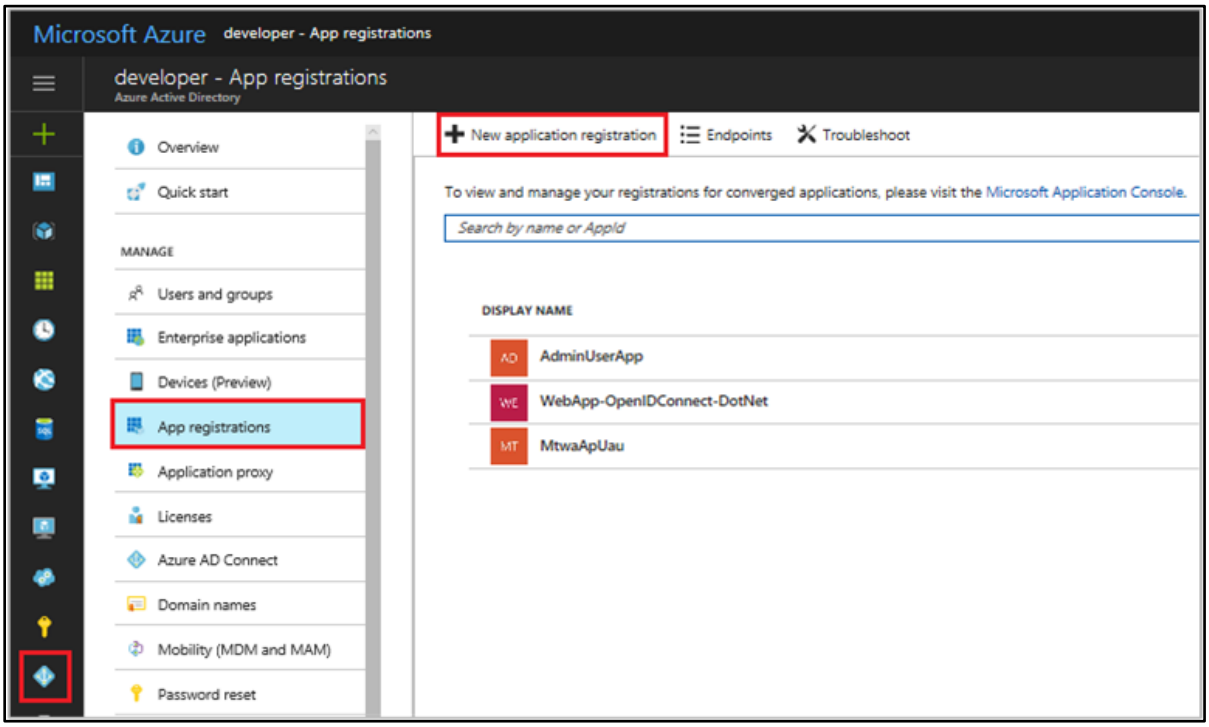

Figure 5

4. When the **Create** page appears, enter your application's registration information:
   - **Name:** Enter an appropriate application name
   - **Application type:** Select **Web app / API**
   - **Sign-On URL:** Enter **http://localhost**

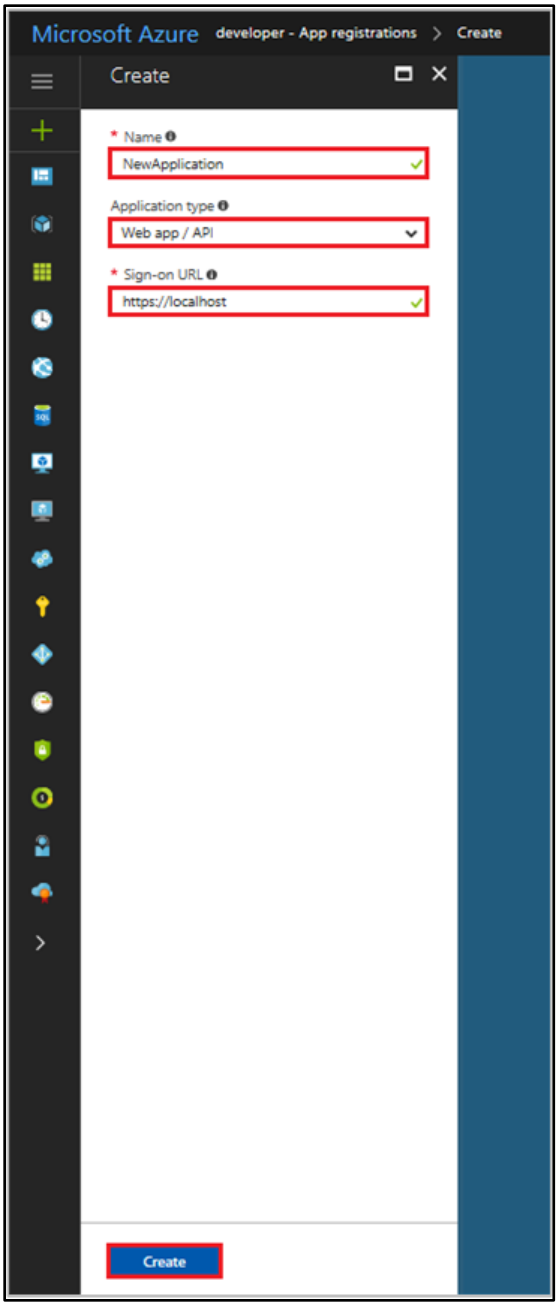

Figure 6

5. When finished, click **Create**. Azure AD assigns a unique Application ID to your application, and you are taken to your application's main registration page. Please note down the **Application ID**.
6. To add permission(s) to access resource APIs from your client,
    - Click the **Required Permissions** section on the **Settings** page.
    - Click the **Add** button.
    - Click **Select an API** to select the type of resources you want to pick from and then select **Microsoft Graph.**

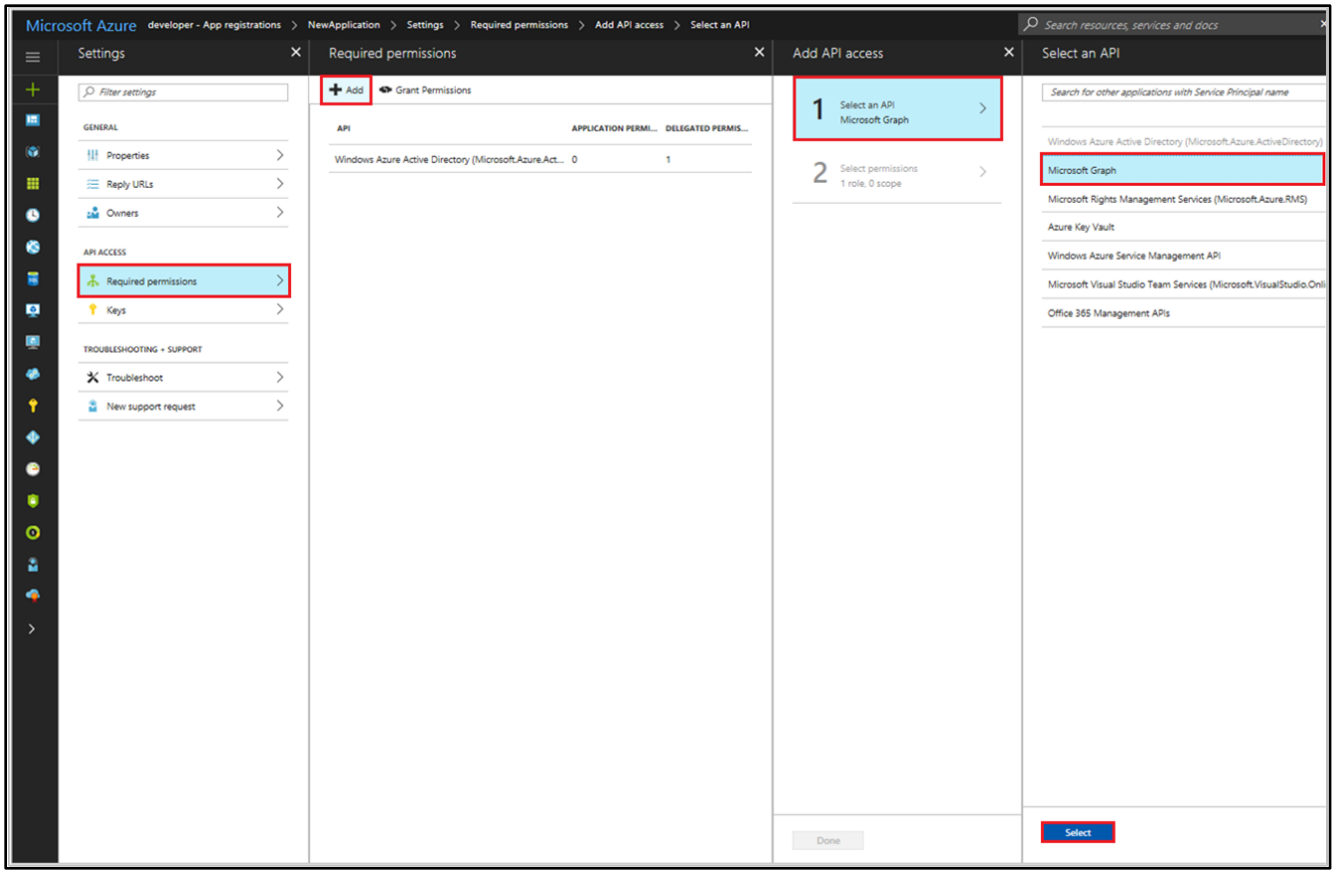

Figure 7

7. After selecting **Microsoft Graph,** add following application permissions:
    - Read all identity risky user information
    - Read all usage reports.
    - Read your organization security events.

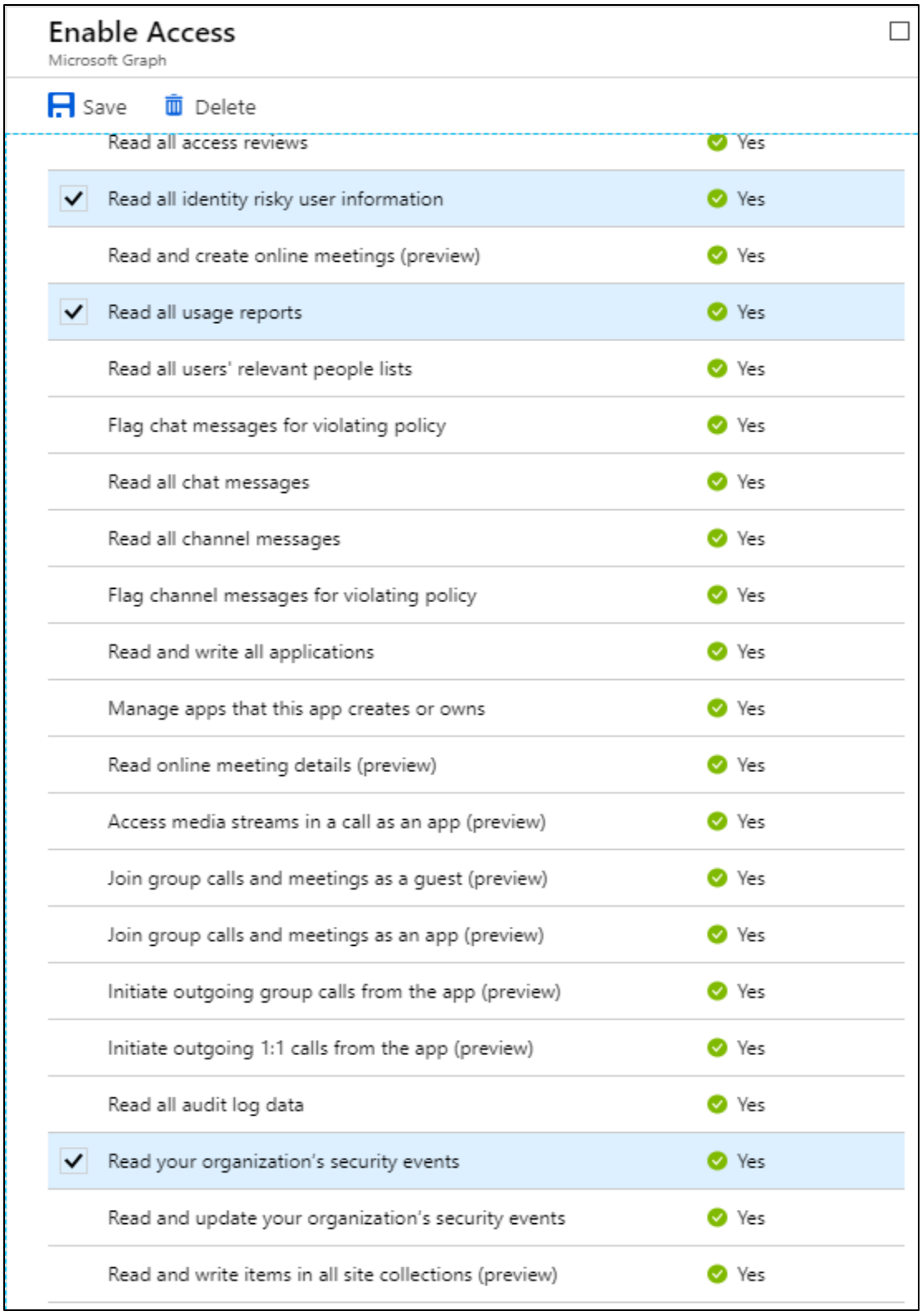
Enable Access
Microsoft Graph
Save
Delete
Read all access reviews
Yes
Read all identity risky user information
Yes
Read and create online meetings (preview)
Yes
Read all usage reports
Yes
Read all users' relevant people lists
Yes
Flag chat messages for violating policy
Yes
Read all chat messages
Yes
Read all channel messages
Yes
Flag channel messages for violating policy
Yes
Read and write all applications
Yes
Manage apps that this app creates or owns
Yes
Read online meeting details (preview)
Yes
Access media streams in a call as an app (preview)
Yes
Join group calls and meetings as a guest (preview)
Yes
Join group calls and meetings as an app (preview)
Yes
Initiate outgoing group calls from the app (preview)
Yes
Initiate outgoing 1:1 calls from the app (preview)
Yes
Read all audit log data
Yes
Read your organization's security events
Yes
Read and update your organization's security events
Yes
Read and write items in all site collections (preview)
Yes

Figure 8

8. Click **Grant permissions** after selecting **Required permissions.** For granting permissions, user(s) with **"Global Administrator"** privileges are required.

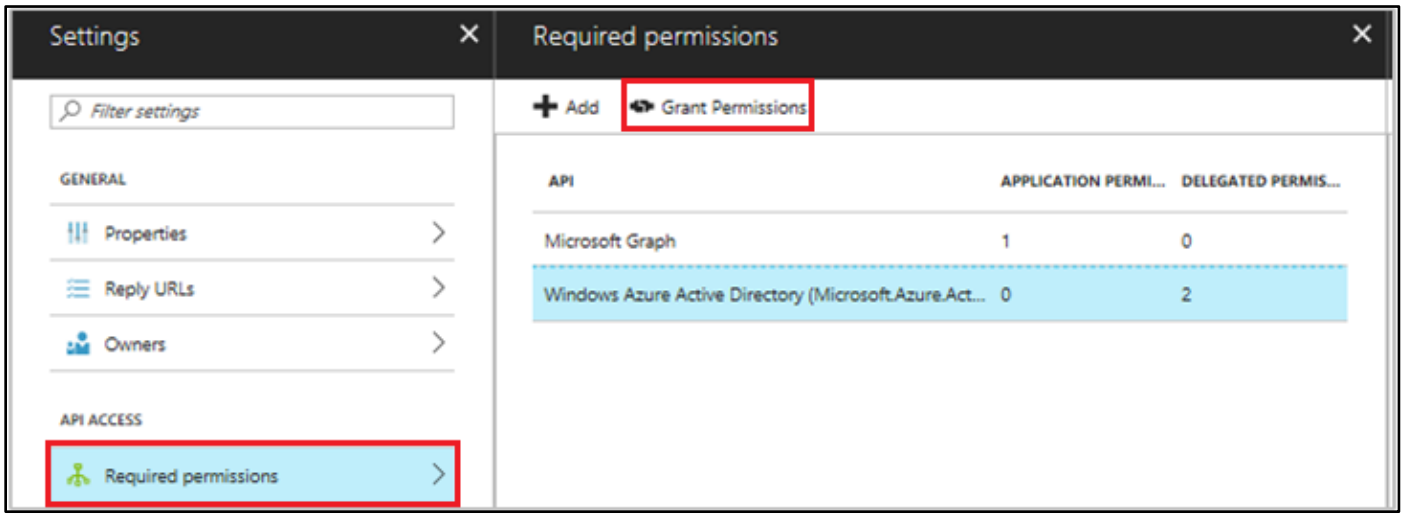

Figure 9

9. You are taken to the application's main registration page, which opens the **Settings** page for the application. To add a secret key for your web application's credentials:
   - Click the **Keys** section on the **Settings** page.
   - Add a description for your key.
   - Select **Never** from **expires** drop-down.
   - Click **Save**. The right-most column will contain the key value, after you save the configuration. Make note of value generated. This will be used in the integrator as **client secret.**

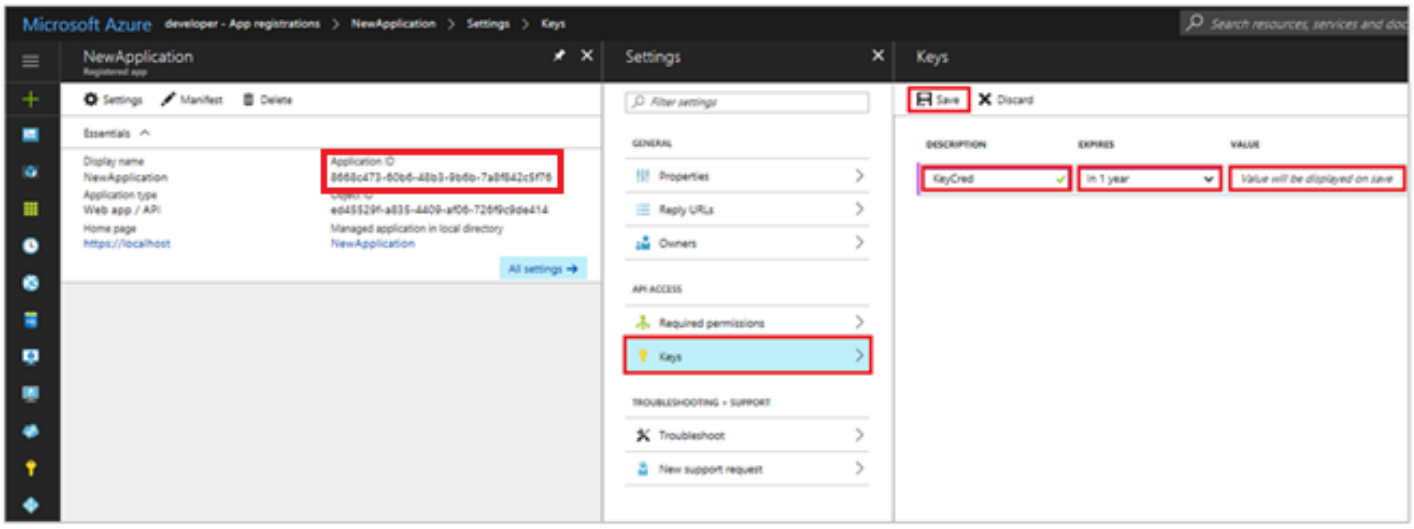

Figure 10

10. Please note down the **Application ID** after completing app configuration.

Grant the Azure AD Application Reader Access to the Subscription

1. After creating the Azure application (which is similar to a service account), the application needs to be granted Security reader access to the subscription(s) via a service principal object.
2. Select **Subscriptions** -> **Your subscription** -> **Access control (IAM)** -> **Add** -> select the **Security Reader role** -> type the name of your application registration from the previous step -> select the application when it appears in the results -> click the **Save** button.

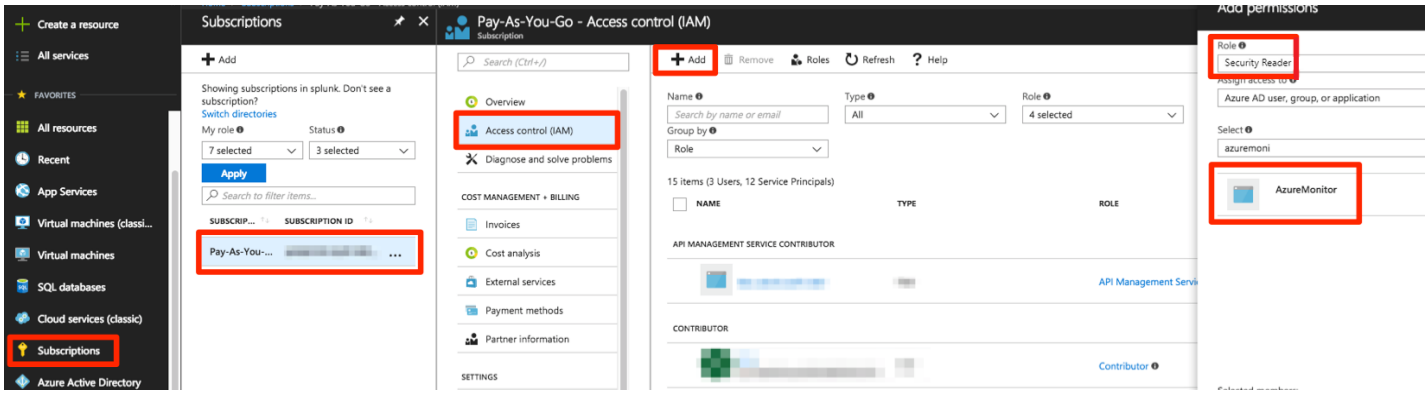

Figure 11

To Enable Auditing for Keyvault in the Azure portal

Before you can enable this, you need a storage account. You can use your existing storage account or create a new storage account in resource group to store the logs.

1. Sign in to the Azure portal.
2. In the Microsoft Azure portal, click **Keyvault**.
3. Navigate to the **Diagnostic logs** under the **MONITORING.**

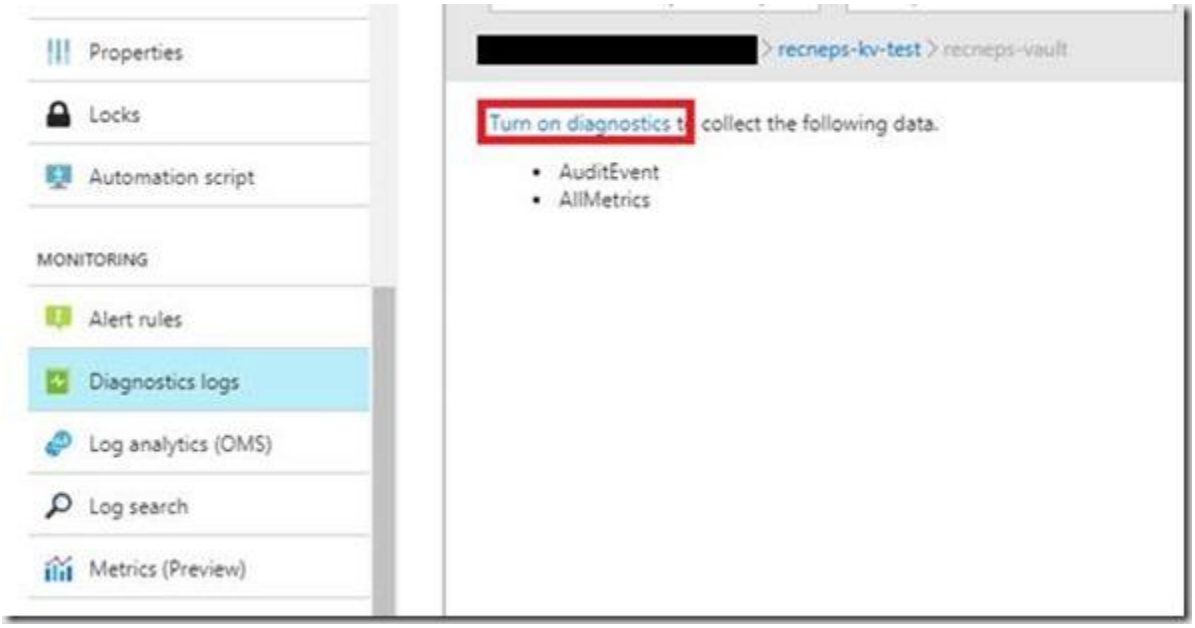

Figure 12

4. Click **"Turn on diagnostics"**
5. Enter the **Name** for the setting. **Example (Keyvault_logger)**

6. Select "**Archive to Storage Account**" and pick the storage account you have just created.

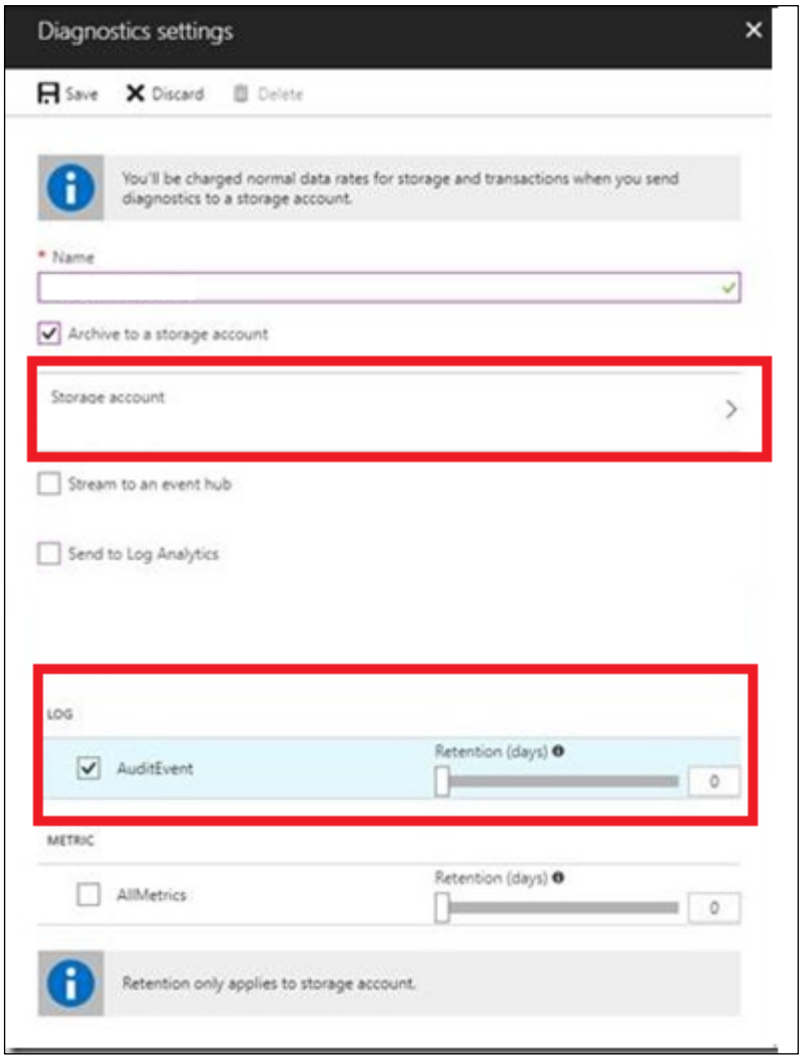

Figure 13

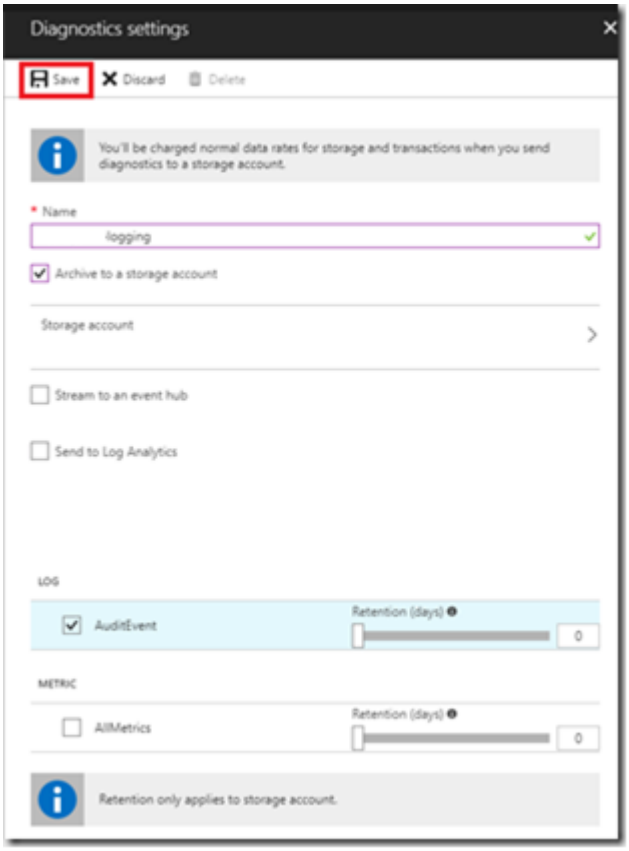

Figure 14

7. Select the **AuditEvent** log and Retention days as required.
8. Click **Save**.

   If you are enabling Azure Keyvault you have to enable addition role to the storage account for accessing Keyvault log.
9. Follow these steps to assign the **Reader** role so that a user can access blobs from the Azure portal. In this example, the assignment is scoped to the storage account:
10. In the Azure portal, navigate to your storage account.
11. Select **Access control (IAM)** to display the access control settings for the storage account. Select the **Role assignments** tab to see the list of role assignments.
12. In the **Add role assignment** window, select the **Reader** role.
13. From the **Assign access to** field, select **Azure AD Application** which we created.
14. Save the role assignment.
15. Repeat the same procedure to assign **Storage Blob Data Reader** to the application.

To find your Azure tenant ID in the Azure AD portal

1. Sign in to the **Azure portal**.

2. In the Microsoft Azure portal, click **Azure Active Directory**.
3. Under **Manage**, click **Properties**. Make note of the value in **Directory ID** box. This will be used as **Tenant ID** in the integrator.

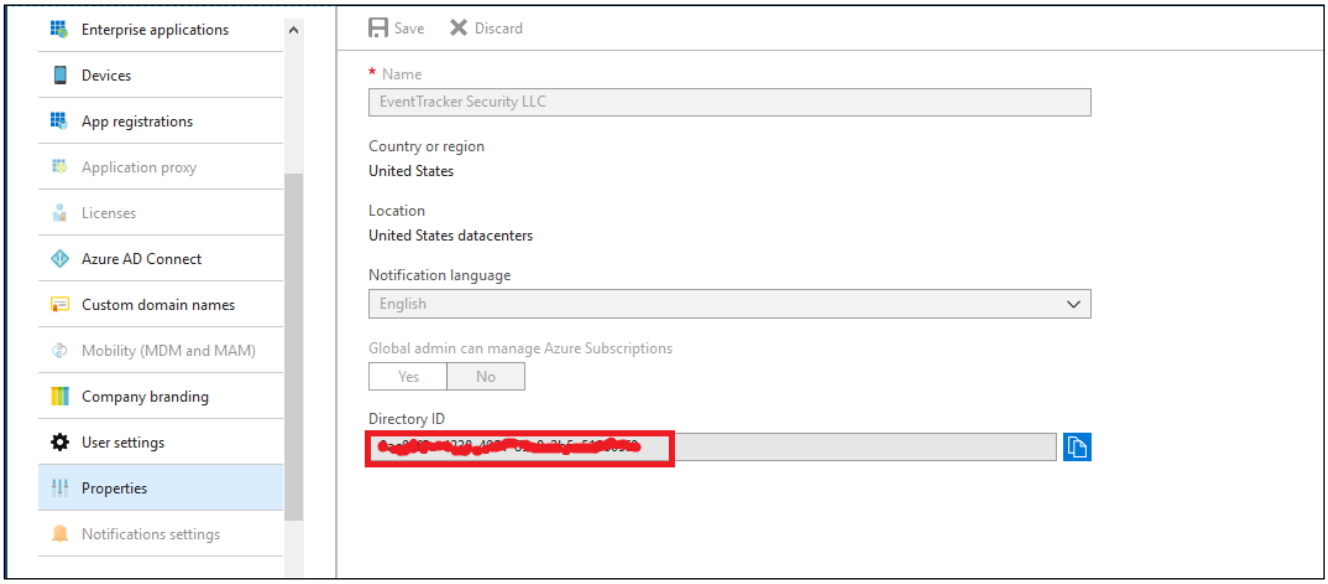

Figure 15

Verify Azure Integration

After providing details in Azure Integrator, please follow the steps to verify the Azure integration.

1. Check if the following task is created in Task Scheduler.

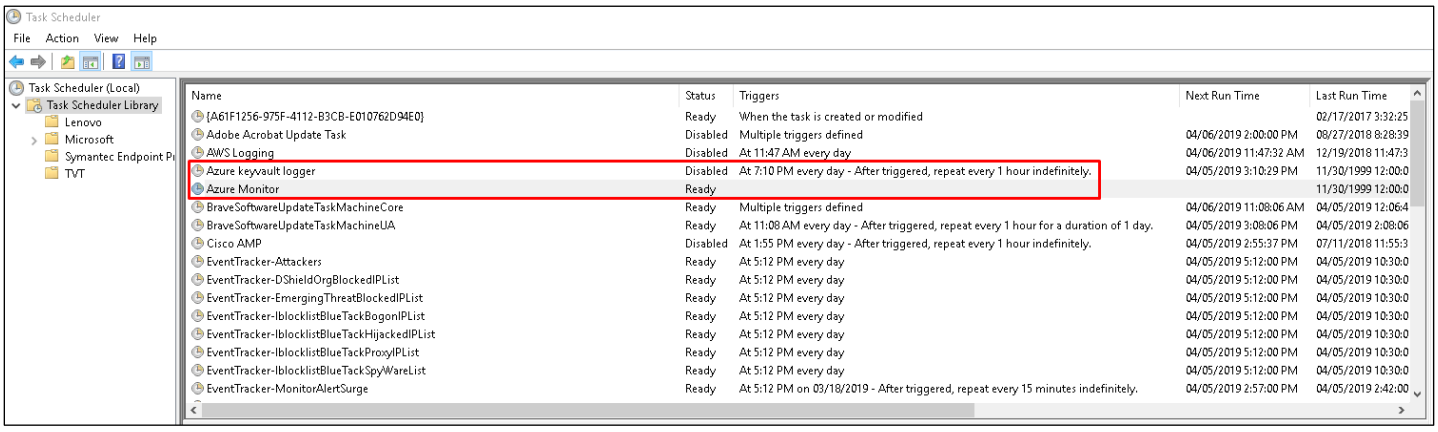

Figure 16

EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; Reports, Knowledge Objects and Dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support Azure monitoring:

Reports

- **Azure – Intune Audit Events:** This report will provide you information related to Azure Intune Audit Events.

  Sample Report:

LogTime	Computer	Activity Date Time	Activity Type	Activity Result	Application Display Name	Category	Activity Operation Type	Log Type	Component Name	User Name	User Type
04/08/2019 06:52:20 PM	AZUREINTUEN_009	2019-03-07T15:50:34.3091045Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:20 PM	AZUREINTUEN_009	2019-03-07T15:51:18.2210346Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:21 PM	AZUREINTUEN_009	2019-03-07T14:47:55.828692Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:21 PM	AZUREINTUEN_009	2019-03-07T14:50:48.0748327Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:21 PM	AZUREINTUEN_009	2019-03-07T14:50:48.0748327Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:22 PM	AZUREINTUEN_009	2019-03-06T22:08:16.3036989Z	SyncWindowsAutopilotDevices WindowsAutopilotSettings	Success	Microsoft Intune portal extension	Enrollment	Action	Syncing Windows Autopilot Devices	Enrollment	netadmin@contoso.local	ItPro
04/08/2019 06:52:22 PM	AZUREINTUEN_009	2019-03-07T14:47:55.828692Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:23 PM	AZUREINTUEN_009	2019-03-06T16:32:15.1599439Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:23 PM	AZUREINTUEN_009	2019-03-06T16:32:15.1599439Z	Create MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Create	Create MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:23 PM	AZUREINTUEN_009	2019-03-06T22:08:16.3036989Z	SyncWindowsAutopilotDevices WindowsAutopilotSettings	Success	Microsoft Intune portal extension	Enrollment	Action	Syncing Windows Autopilot Devices	Enrollment	netadmin@contoso.local	ItPro
04/08/2019 06:52:24 PM	AZUREINTUEN_009	2019-03-06T16:29:50.0340179Z	Delete MobileApp	Success	Microsoft Intune portal extension	Application	Delete	Delete application.	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:25 PM	AZUREINTUEN_009	2019-03-06T16:29:50.0340179Z	Delete MobileApp	Success	Microsoft Intune portal extension	Application	Delete	Delete application.	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:25 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:26 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:26 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:27 PM	AZUREINTUEN_009	2019-03-06T16:29:42.6480499Z	Delete MobileAppAssignment	Success	Microsoft Intune portal extension	Application	Delete	Delete MobileAppAssignment	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:27 PM	AZUREINTUEN_009	2019-03-05T22:36:46.2275035Z	Patch MobileApp	Success	Microsoft Intune portal extension	Application	Patch	Modify application.	MobileApp	netadmin@contoso.local	ItPro
04/08/2019 06:52:27 PM	AZUREINTUEN_009	2019-03-05T22:36:46.2275035Z	Patch MobileApp	Success	Microsoft Intune portal extension	Application	Patch	Modify application.	MobileApp	netadmin@contoso.local	ItPro

Figure 17

Sample Log

Figure 18

- **Azure – Key vault Audit Events:** This report will provide you information related to Azure Keyvault Audit Events.

Sample Log:

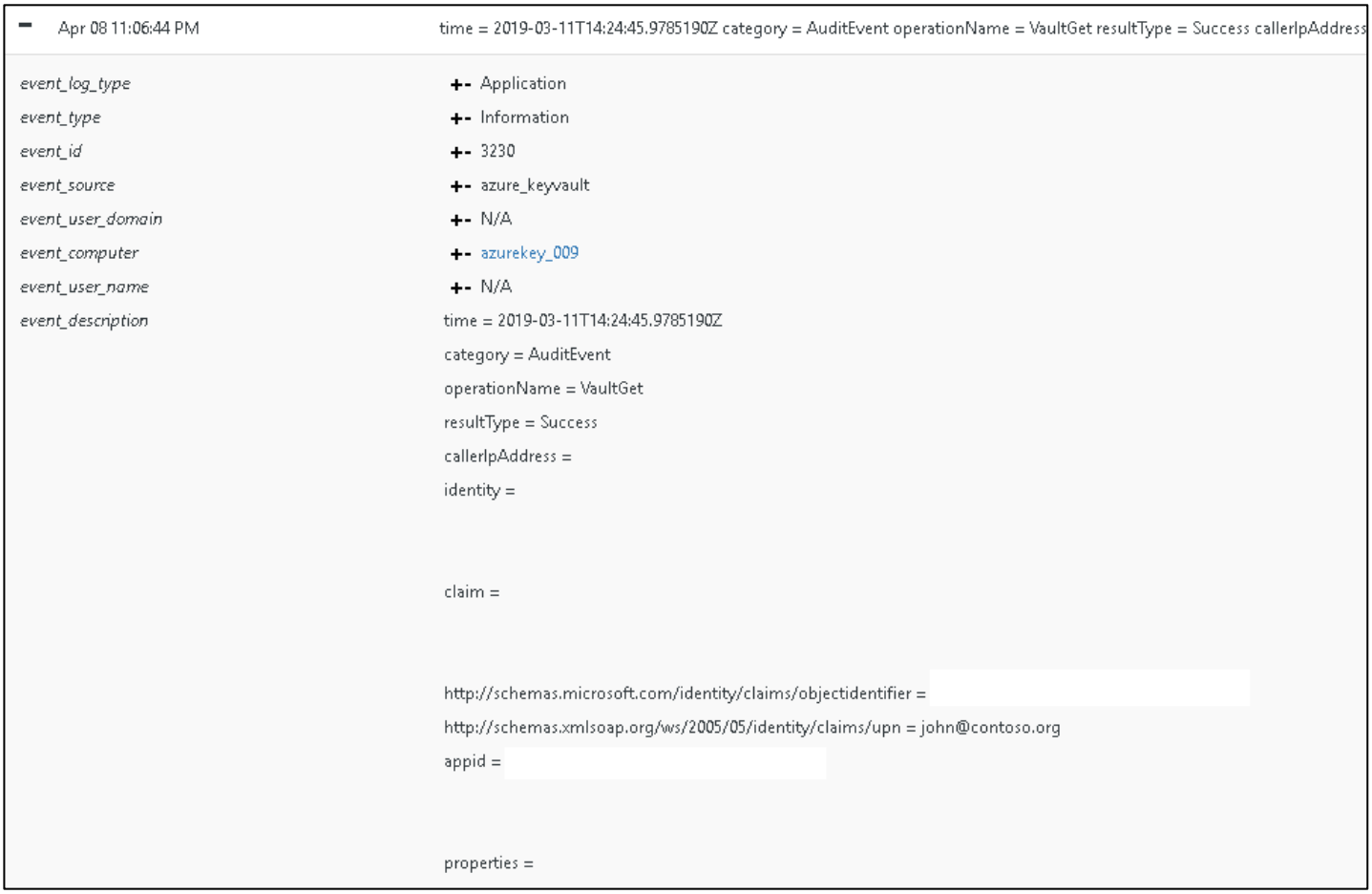

Figure 19

Sample Dashboards

1. **Azure – Azure Intune Audit Activities by Category**

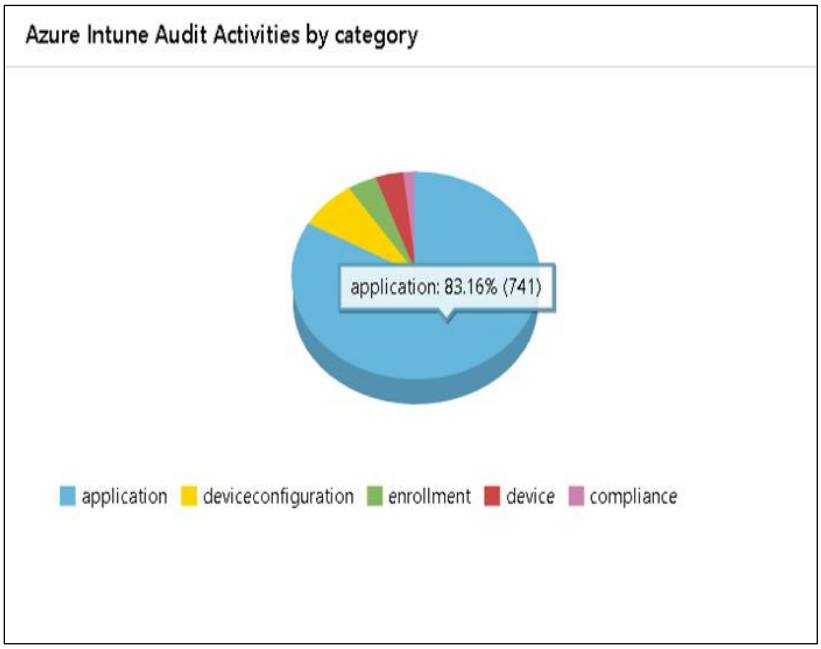

Figure 20

2. **Azure Intune Audit Activities by Type**

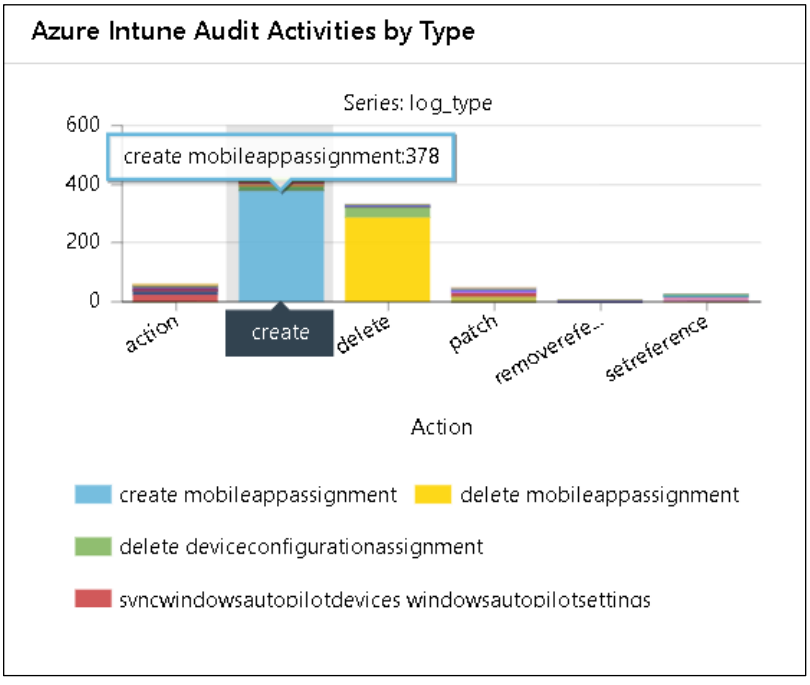

Figure 21

3. Azure Intune Audit Activities by User

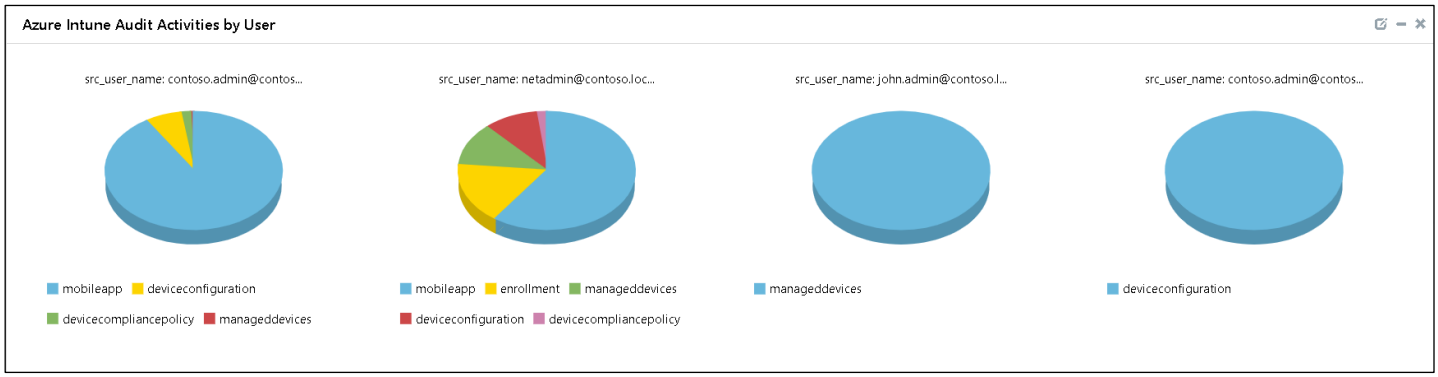

Figure 22

4. Azure Intune Audit Activities by Status

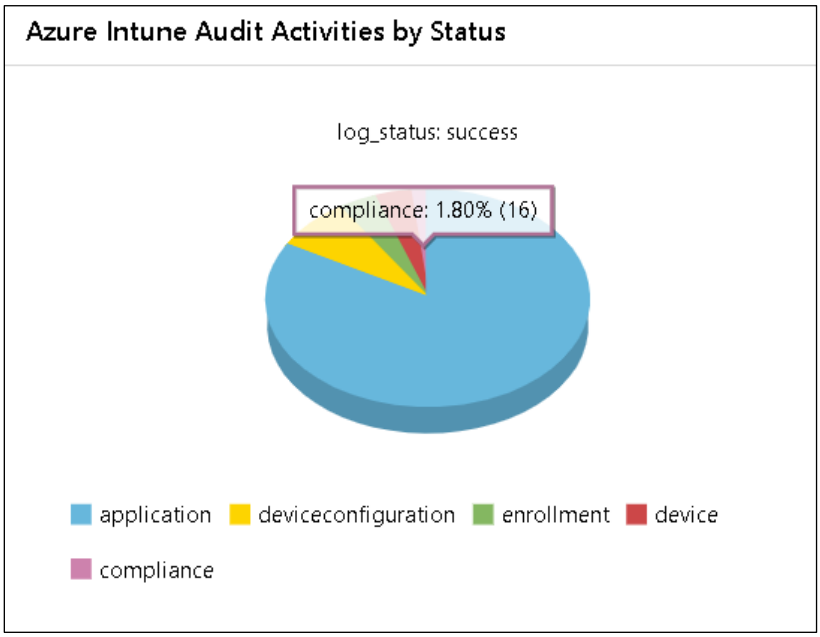

Figure 23

5. **Azure Intune Audit Activities by Component**

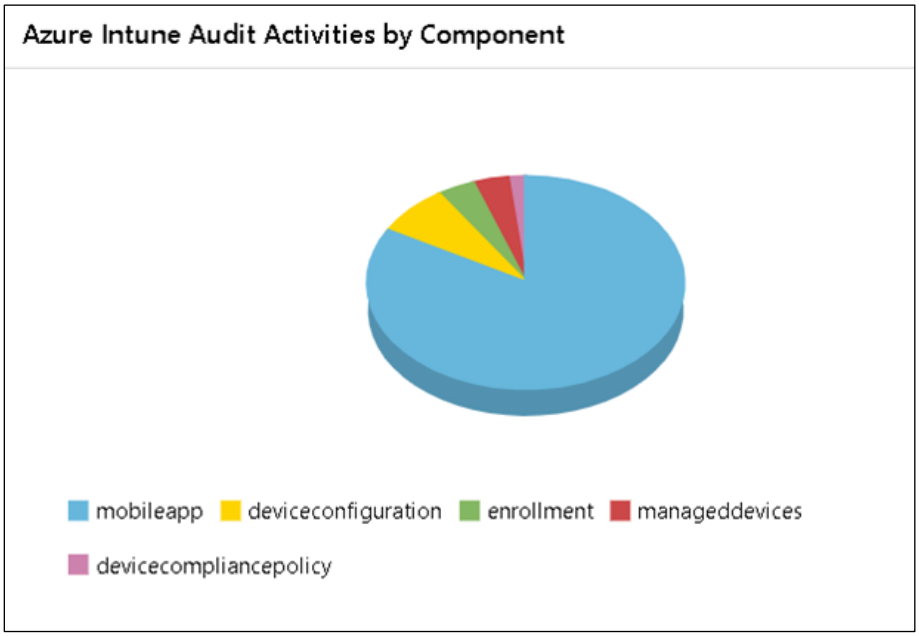

Figure 24

6. **Azure Keyvault Audit Activities by Type**

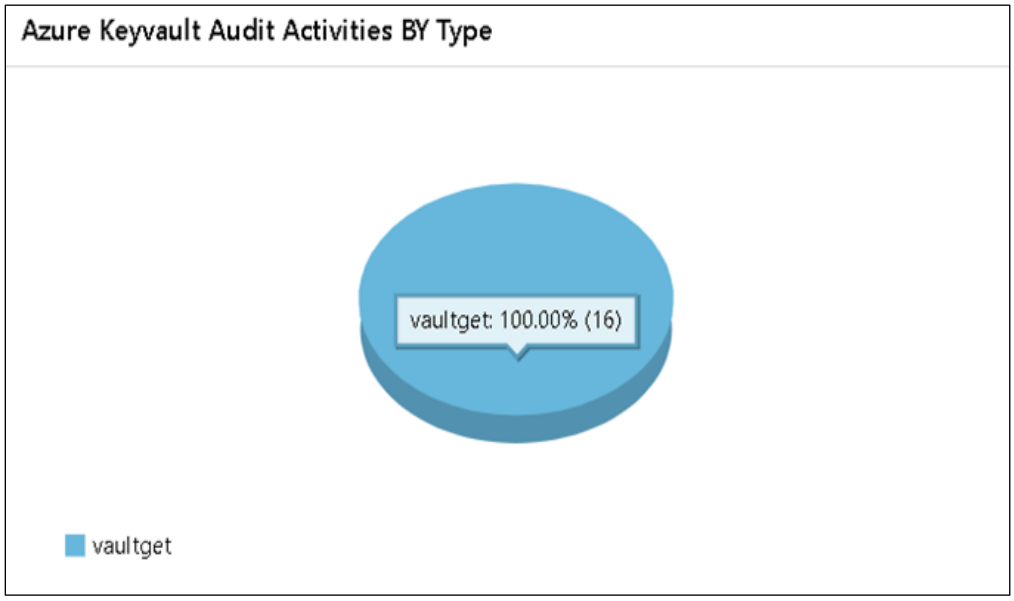

Figure 25

7. **Azure Keyvault Audit Activities By user**

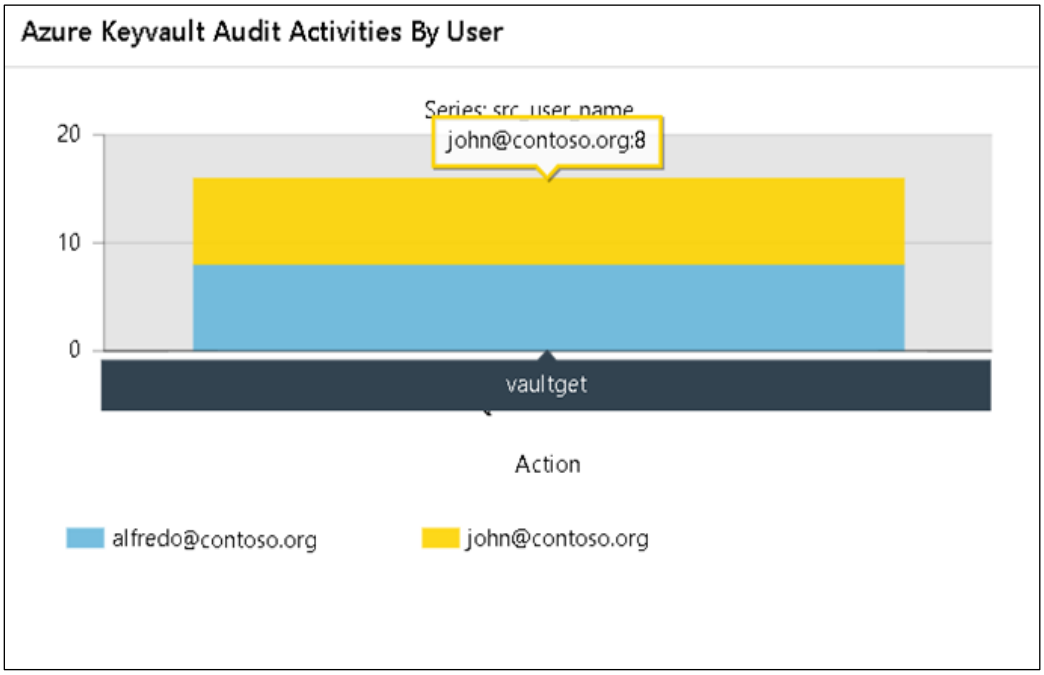

Figure 26

8. **Azure Keyvault Audit Activities By Geo Location**

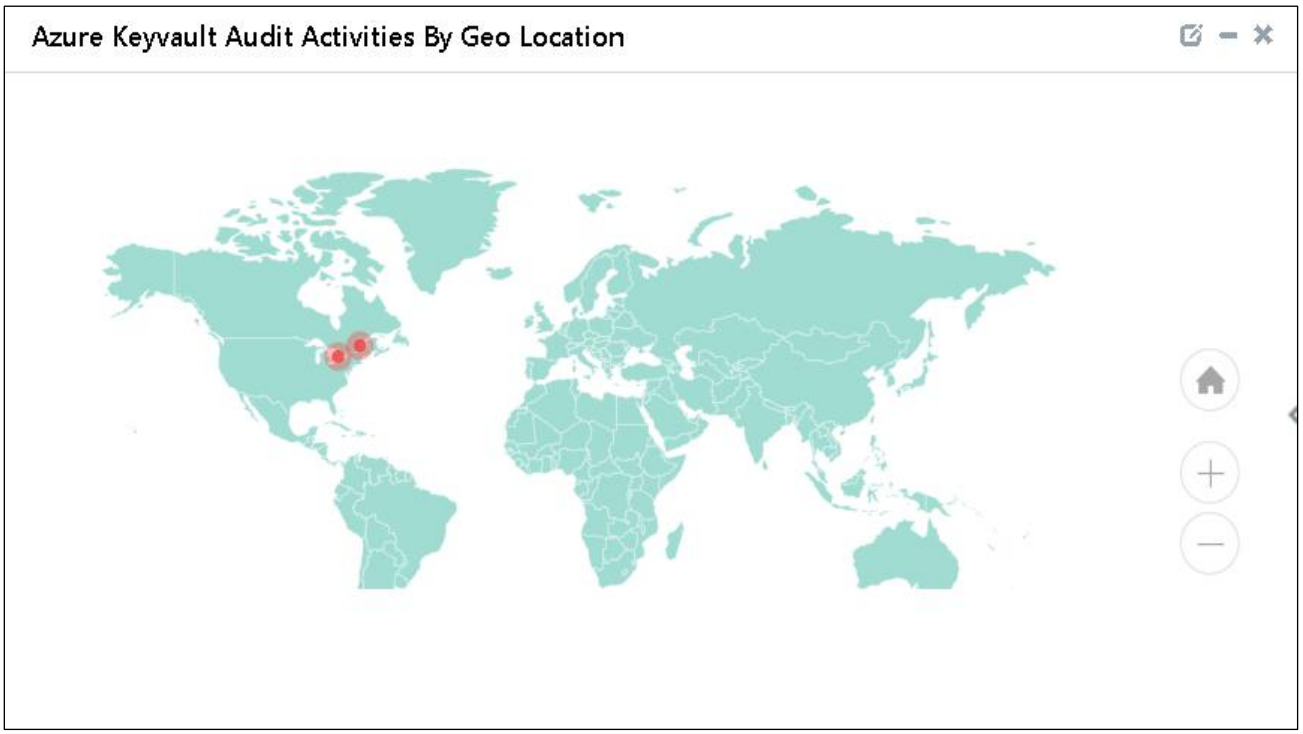

Figure 27

9. **Azure Keyvault Audit Activities by Status**

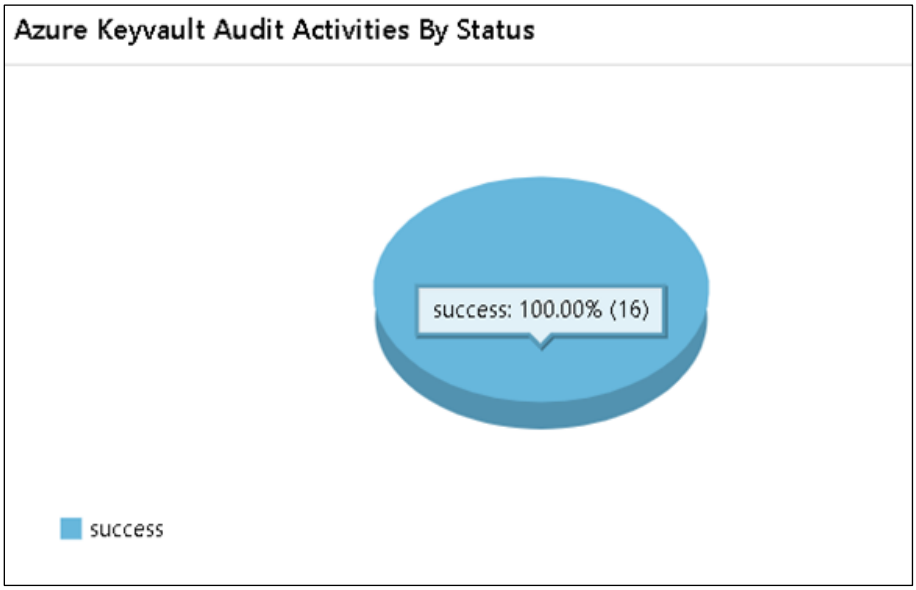

Figure 28

Import Knowledge Pack into EventTracker

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

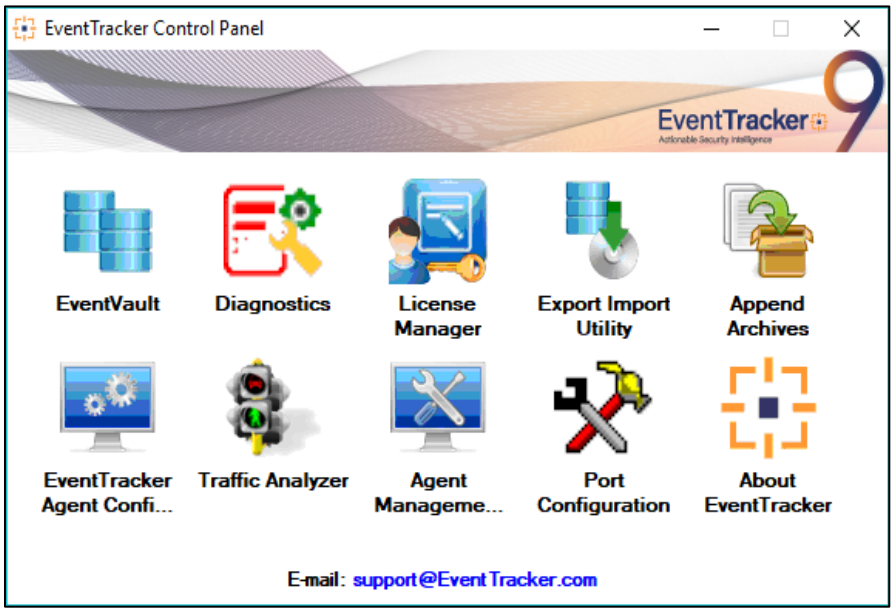

Figure 29

3. Import **Tokens/Flex Reports** as given below.

Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the file named **KO_Azure.etko**.

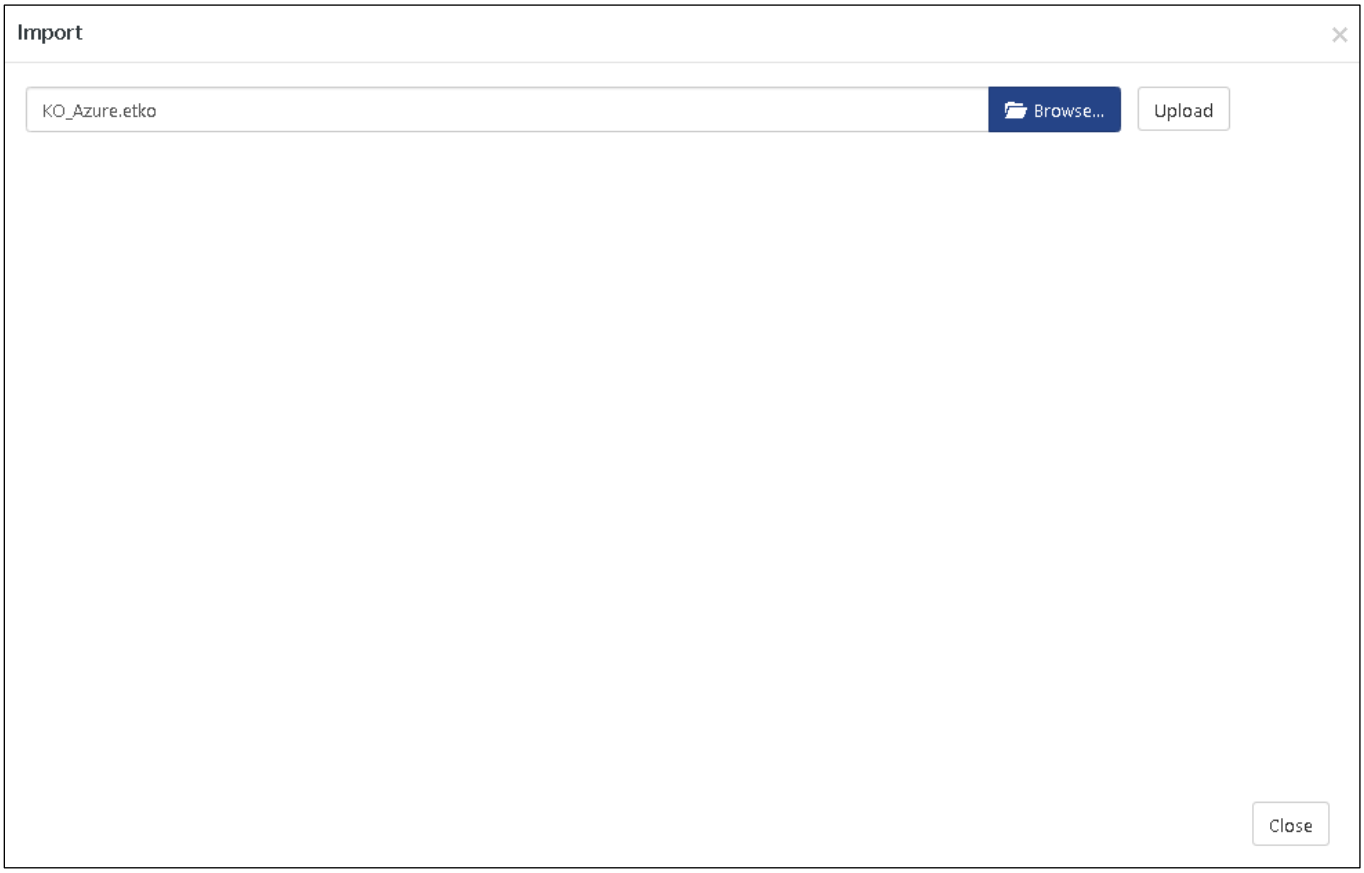

Figure 30

3. Now select all the check box and then click on ‘**Import**’ option.
4. Knowledge objects are now imported successfully.

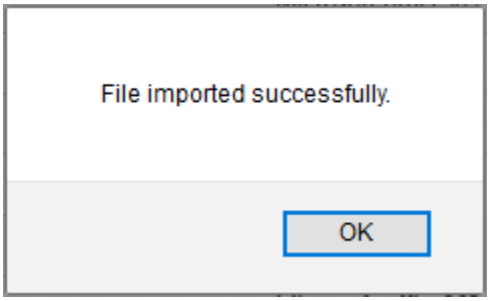

Figure 31

Flex Reports

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

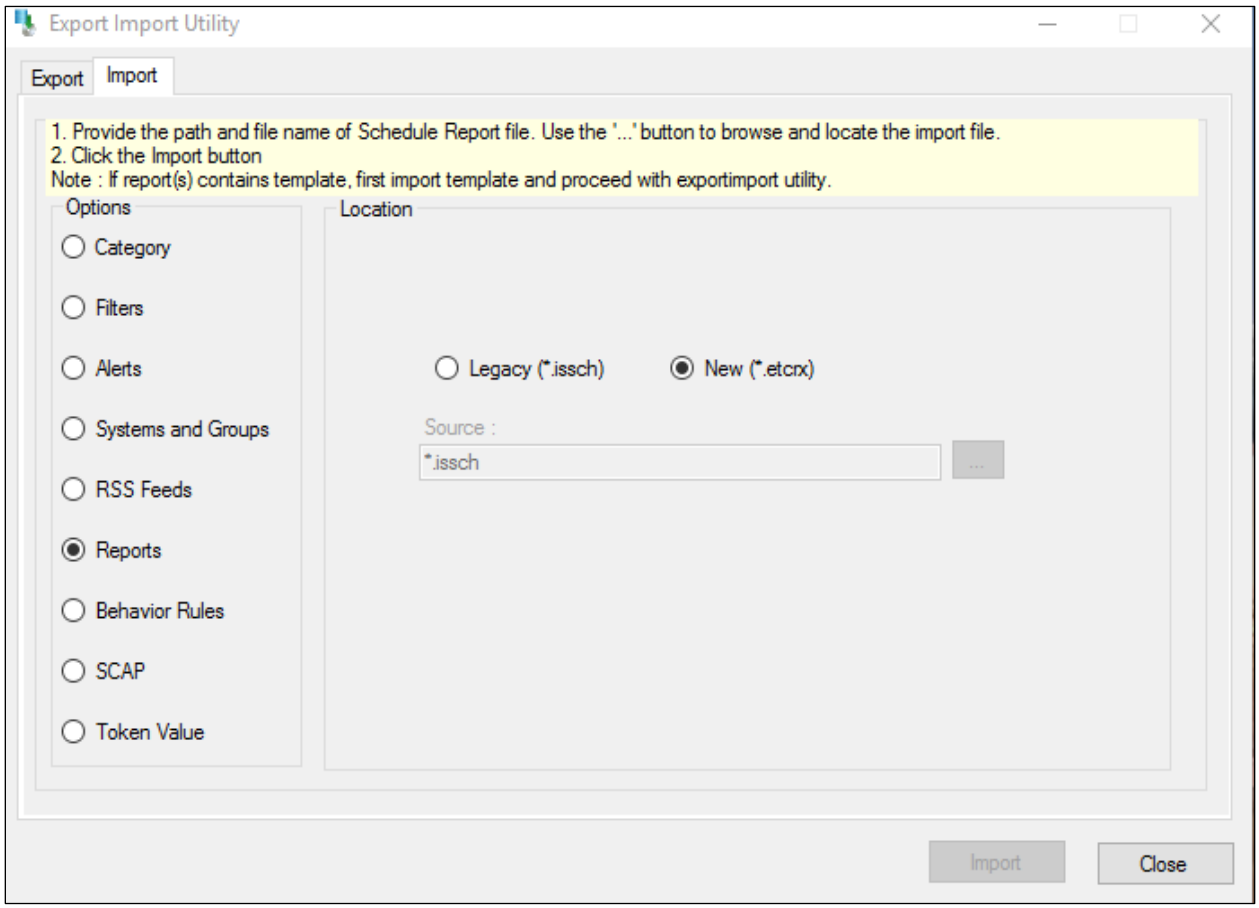

Figure 32

2. Locate the file named **Flex Reports_Azure.etcrx** and select all the check box.

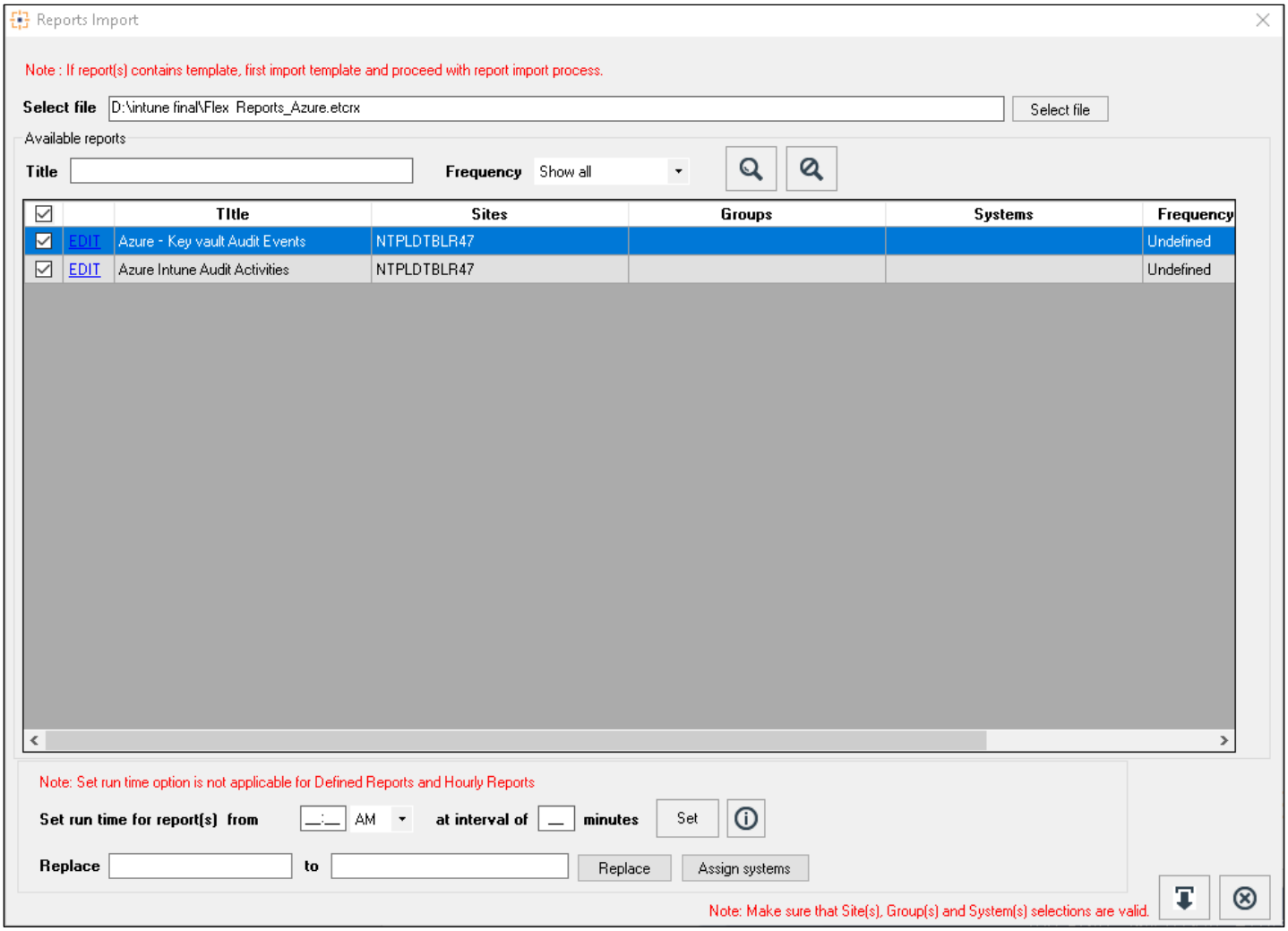

Figure 33

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

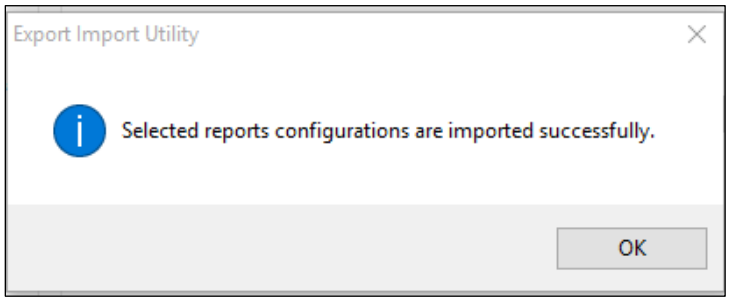

Figure 34

Dashlets

In EventTracker 9.0, we have added a new feature which will help to import/export the dashlet. Following is the procedure to do that:

1. Login into **EventTracker Enterprise Web** console.

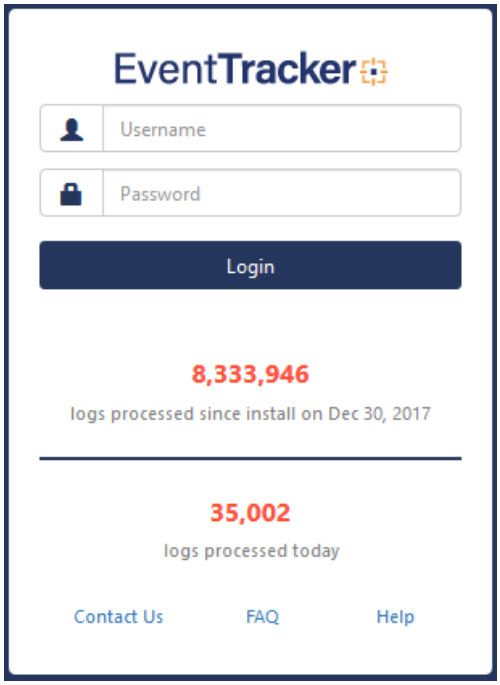

Figure 35

2. Go to **My Dashboard** option.

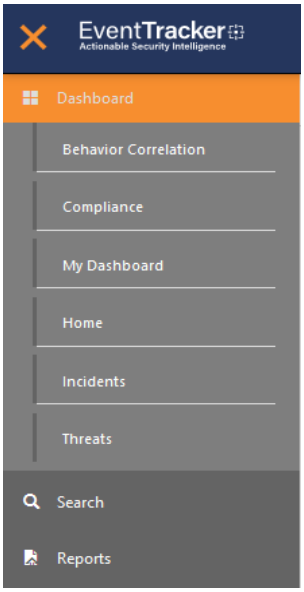

Figure 36

3. Click on import button and select **.etwd** File.

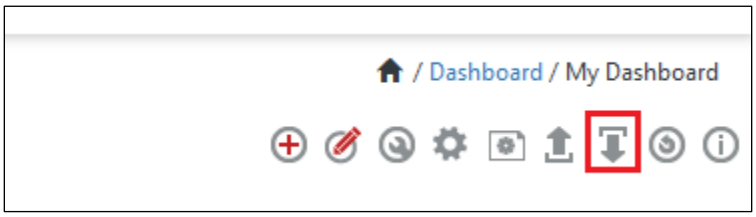

Figure 37

4. Browse to the file path.

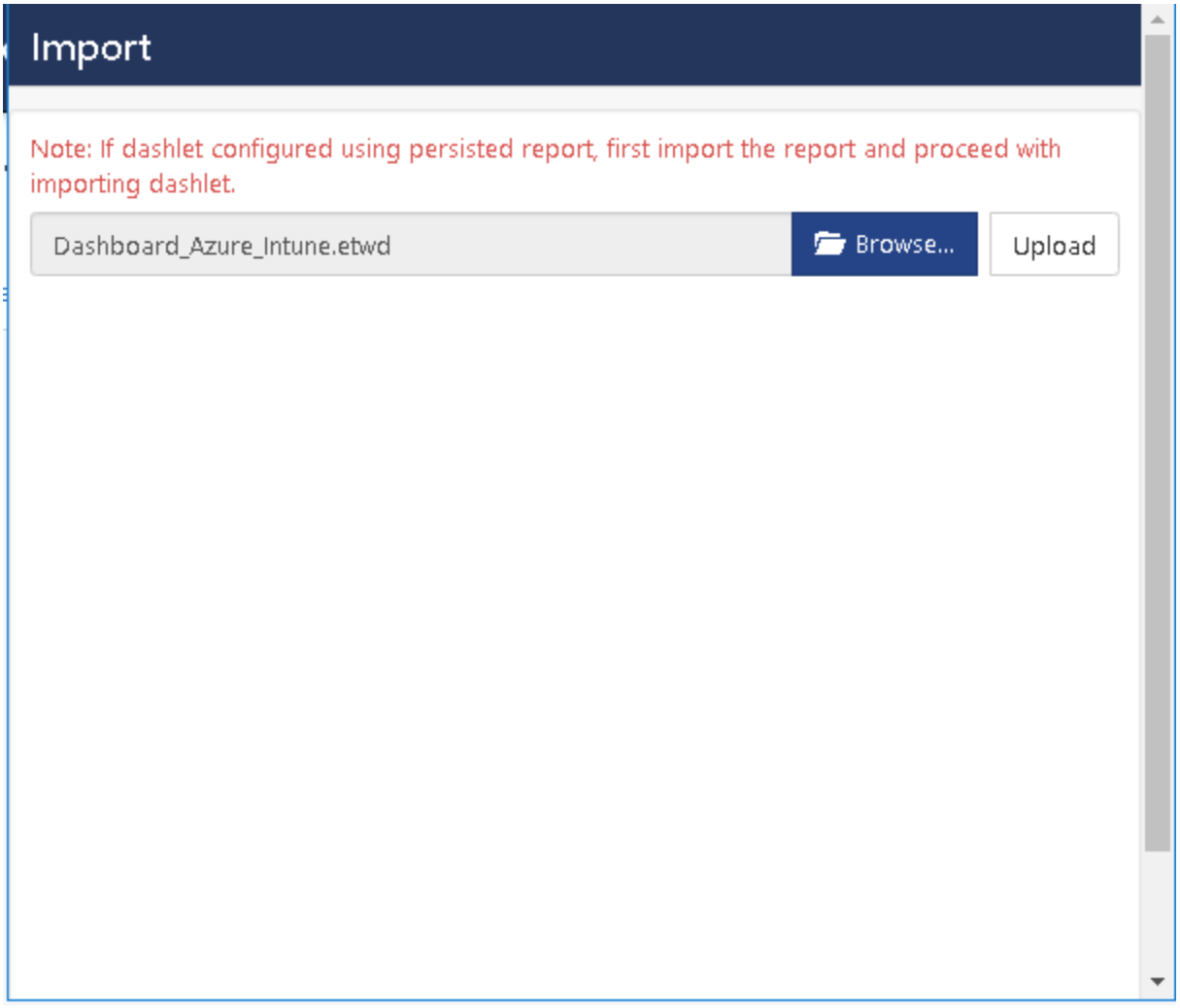

Figure 38

5. Click **Upload** and select the Dashboards which you want to import.

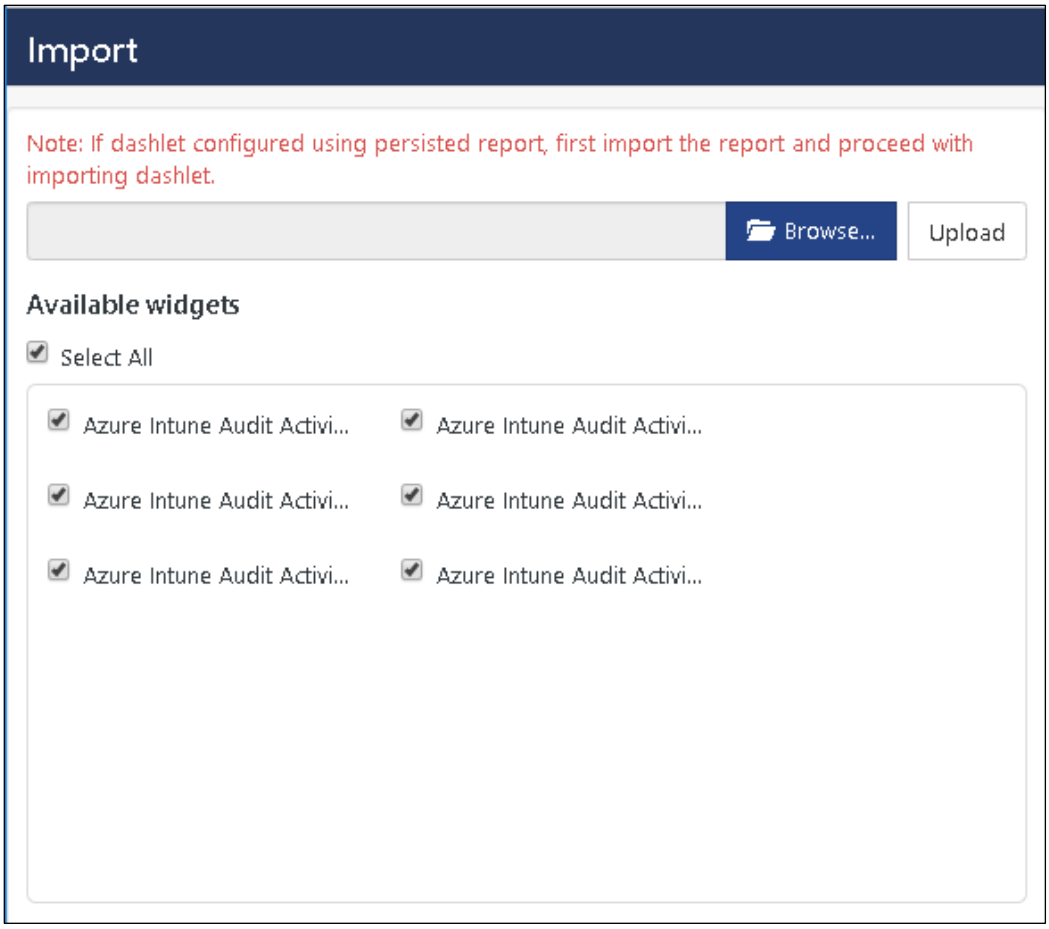

Figure 39

6. Click on **Import** button. It will upload all the selected dashboards.
7. Repeat the same procedure to import **Dashboard_Keyvault.etwd** for Keyvault Dashboards.

Verify Knowledge Pack in EventTracker

Knowledge Object

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Knowledge Object**.
3. In **Knowledge Object Group Tree** to view imported knowledge object, scroll down and click **Azure** group folder.

Knowledge Object are displayed in the pane.

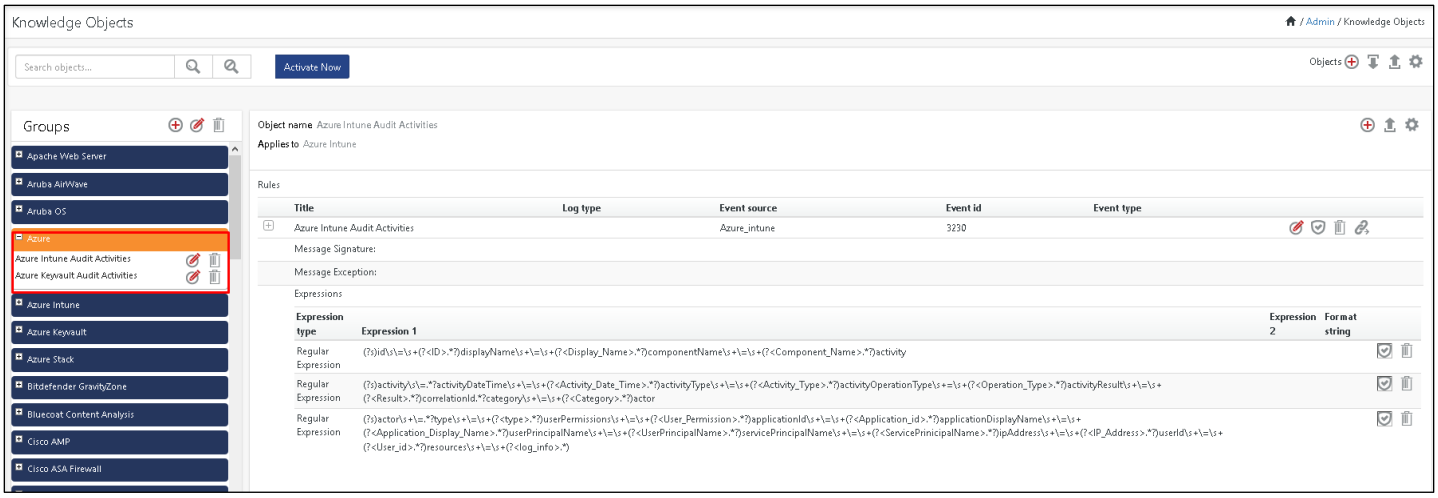

Figure 40

Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Azure** group folder.

   Reports are displayed in the Reports configuration pane.

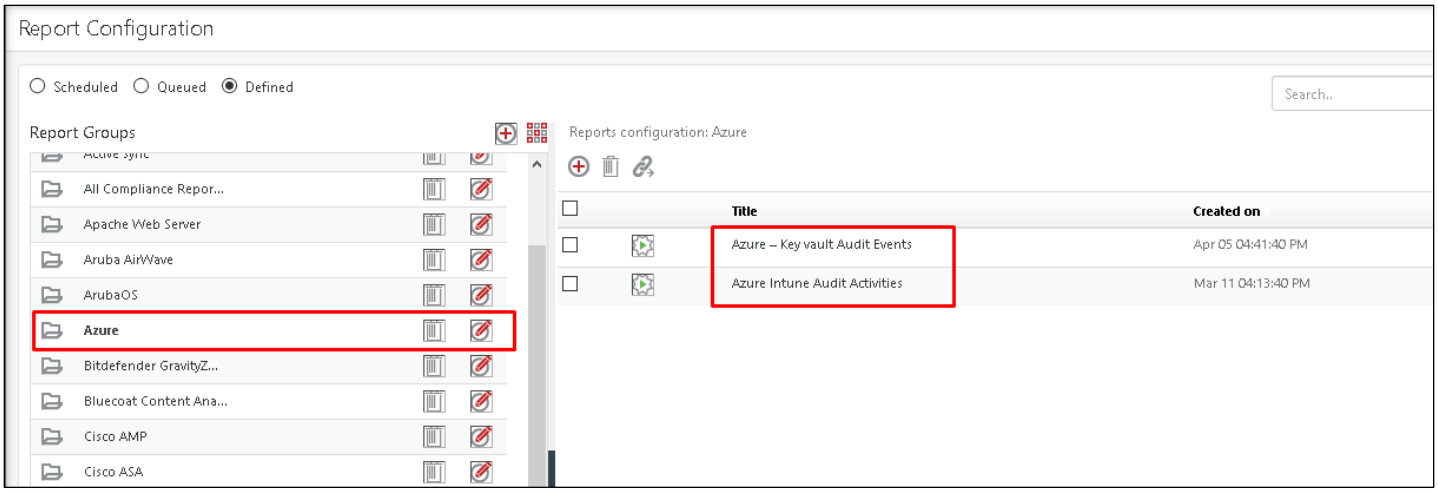

Figure 41

Dashlets

1. Logon to **EventTracker Enterprise**.

2. Click the **Dashboard** menu, and then **My Dashboard.**

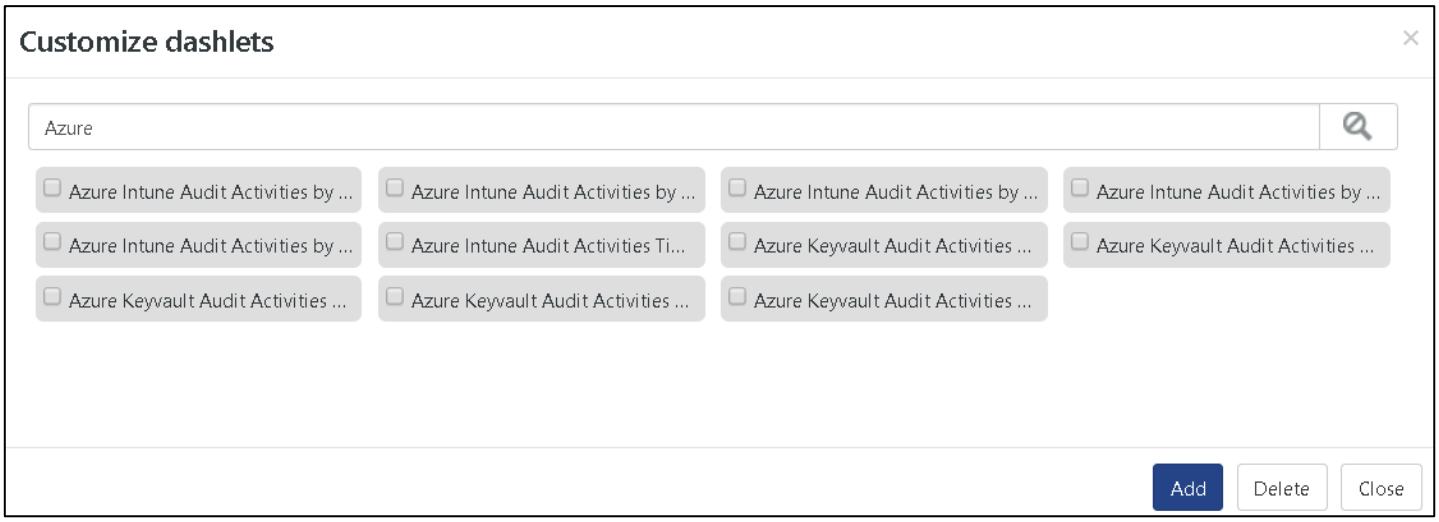

Figure 42

3. Then click on **Customize Dashlet** button and search for **"Azure".**
4. Click on **Add**, for adding the dashlets to the **My Dashboard.**