

Integration Guide

Integrating Microsoft Defender with EventTracker

Publication Date:

April 4, 2022

Abstract

This guide provides instructions to retrieve the **Microsoft Defender** 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 and later and Microsoft Defender for Endpoint.

Audience

The Administrators who are assigned the task to monitor the **Microsoft Defender** events using EventTracker.

Table of Contents

Table of Contents	3
1. Overview	4
2. Prerequisites.....	4
3. Configuring Event hub to Forward Logs to EventTracker	4
3.1 Creating an Event Hubs namespace and an Event Hub	4
3.2 Configuring Azure Function app to forward data to EventTracker	6
3.3 Cost Management	15
3.4 Verifying Function App.....	15
4. Configuring Microsoft Defender to Forward Logs to Event hub	17
4.1 Configuring Microsoft Defender to stream events to Event Hub	17
5. EventTracker Knowledge Packs	19
5.1 Alerts	19
5.2 Categories	19
5.3 Reports	19
5.4 Dashboards	20
6. Importing Microsoft Defender Knowledge Packs into EventTracker	22
6.1 Categories	22
6.2 Alerts	23
6.3 Knowledge Objects (KO)	24
6.4 Reports	26
6.5 Dashboards	27
7. Verifying Microsoft Defender Knowledge Packs in EventTracker	29
7.1 Categories	29
7.2 Alerts	29
7.3 Knowledge Objects	30
7.4 Reports	31
7.5 Dashboards	31
About Netsurion	33
Contact Us.....	33

1. Overview

Microsoft 365 Defender is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

EventTracker helps to monitor events from the Microsoft Defender for Endpoint. Its dashboard and reports will help you track, alert information, and alert evidence which in turn help to detect file-less attacks, backdoor drops, and virus/malware.

2. Prerequisites

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager public IP address.
- Download Azure integration package from [ETS Microsoft Defender Forwarder.zip](#)

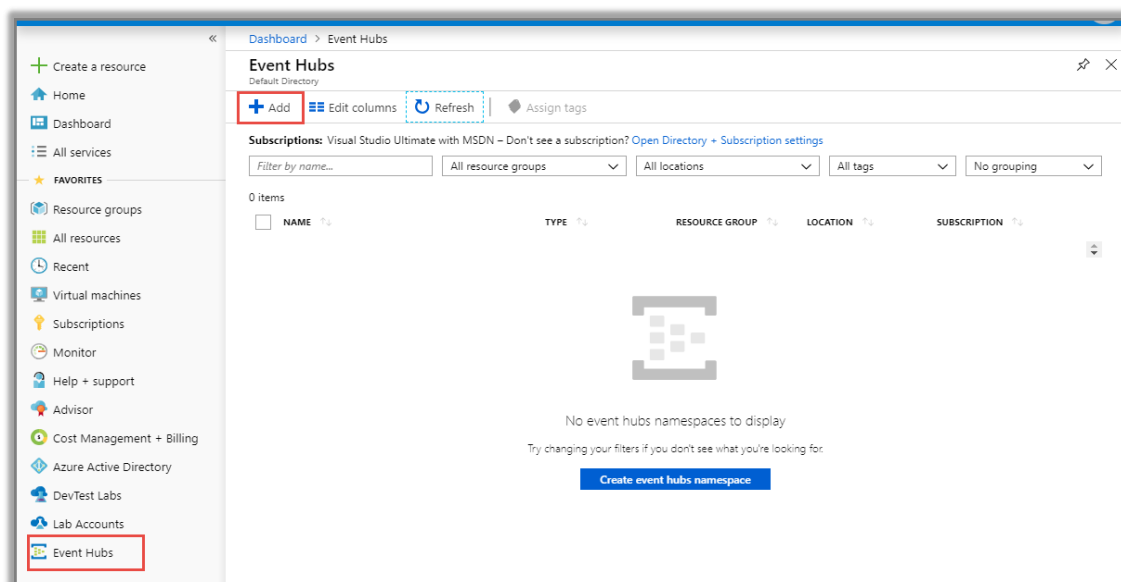
3. Configuring Event hub to Forward Logs to EventTracker

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

3.1 Creating an Event Hubs namespace and an Event Hub

The Event Hubs namespace contains one or more Event Hubs. The configured Azure services create Event Hub in these namespaces to store activities and diagnostics logs.

1. Login to portal.azure.com
2. Navigate to **All services > Event Hubs > Add**.

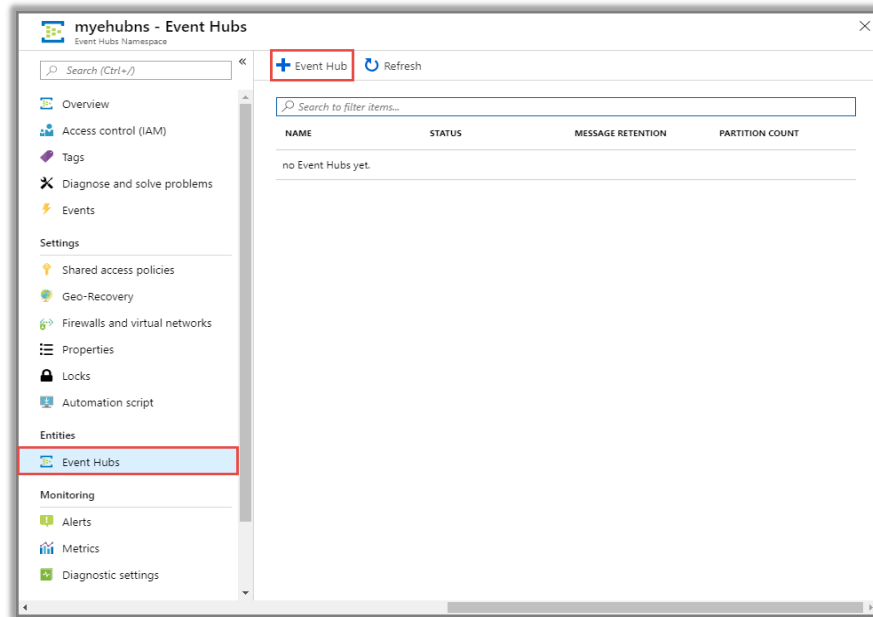


3. Create a namespace. Provide a **Namespace Name**, e.g. **MyEventTrackerHub**, Resource group, and any other settings -> **Review + Create**.

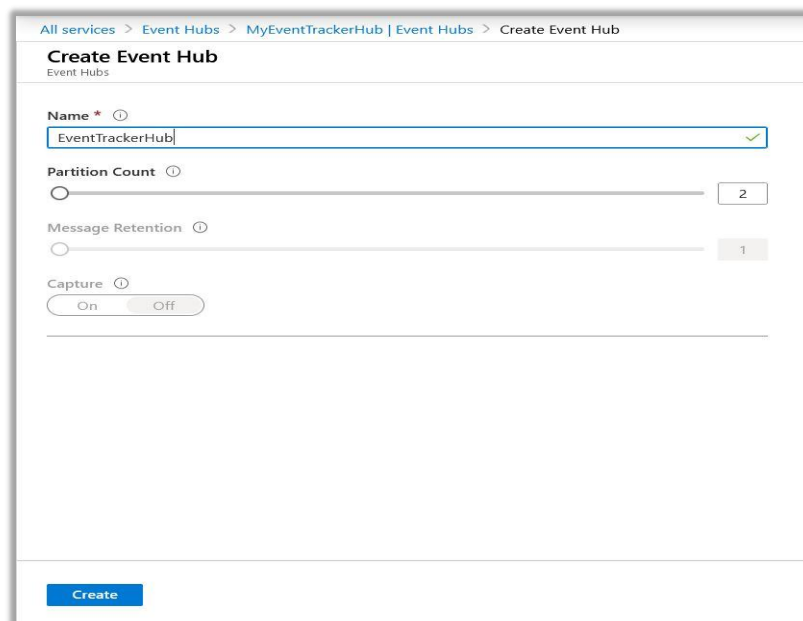
Recommendation: Create and choose Resource group Name with “EventTracker”. It would give a better picture of the billing for the services.

4. On the Event Hubs namespace page, Click **Properties** under **Settings** on the left panel and copy the **Resource ID** value, Which will be used in [further](#) steps (4.1 step 3)

5. On the Event Hubs namespace page, select **Event Hubs** on the left menu. At the top of the window, click **+ Event Hub**.



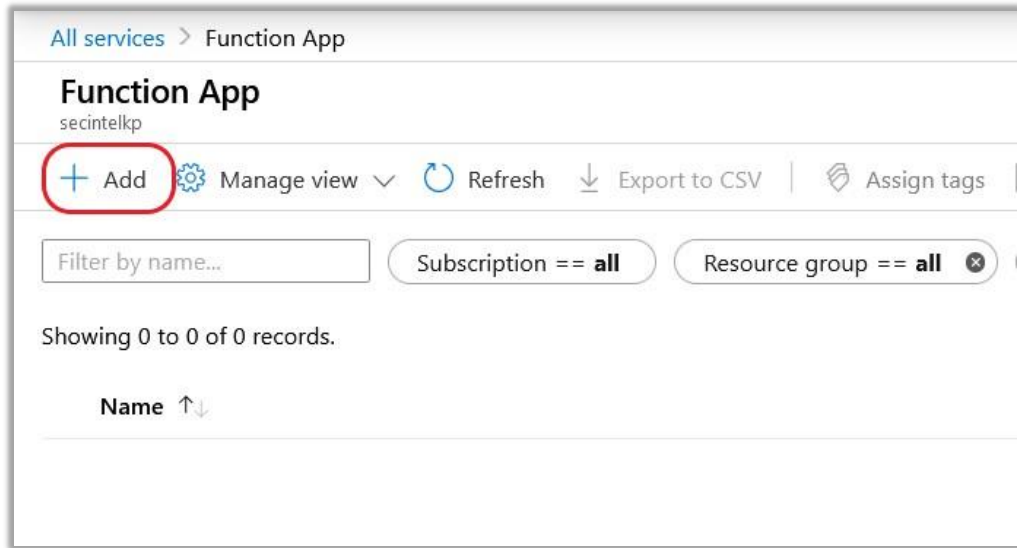
6. Type a name for your Event Hub and provide the EventHub name, partition count based on your environment, **Copy** the Event Hub name which will be used in [further](#) steps (4.1 Step 3), and then click **Create**.



3.2 Configuring Azure Function app to forward data to EventTracker

Azure Functions is a solution for easily running small pieces of code, or **functions**, in the cloud. For more details on the function app overview and cost, refer to the [link](#).

1. Navigate to **All Services > Function App** and click the **+ Add** button.



2. In the configure function app window,
 - In **Project Details**, select the desired subscription and **Resource Group**.
 - In **Instance Details**:
 - Provide a **function app name**, like **FunctionEventTracker**.
 - Select **Code** in **Publish** option.
 - In **Runtime stack**, select **PowerShell Core**.
 - Select the appropriate **region**.

Recommendation: Create and choose Resource group Name with “EventTracker”. It would give a better picture of the billing for the services.

Create Function App ...

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	PAYG-ET-AZURE-KP-DEV
Resource Group *	az_con_gp_01

[Create new](#)

Instance Details

Function App name *	FunctionEventTracker
Publish *	<input checked="" type="radio"/> Code <input type="radio"/> Docker Container
Runtime stack *	PowerShell Core
Version *	7.0
Region *	Central US

.azurewebsites.net

[Review + create](#)

[< Previous](#)

[Next : Hosting >](#)

3. Click **Next: Hosting**.

- Under Storage Section, select your storage account.
- Under the Operating system, select Windows.
- Under Plan, choose a plan of your choice.

[All services](#) > [Function App](#) > Function App

Function App

Basics **Hosting** Monitoring Tags Review + create

Storage

When creating a function app, you must create or link to a general-purpose Azure Storage account that supports Blobs, Queue, and Table storage.

Storage account * [Create new](#)

Operating system

Windows is the only supported Operating System for your selection of runtime stack.

Operating System * ☐ Linux ☒ Windows

Plan

The plan you choose dictates how your app scales, what features are enabled, and how it is priced. [Learn more](#)

Plan type *

[Review + create](#) < Previous Next : Monitoring >

- Click **Review + Create**.
- After the **Function** app is created, navigate to **All services > Function App > FunctionEventTracker** to do further configuration and click on **Advanced tools** under **Development Tools**.

FunctionEventTracker | Functions ...

Function App

<< [+ Create](#) [Refresh](#) [Delete](#)

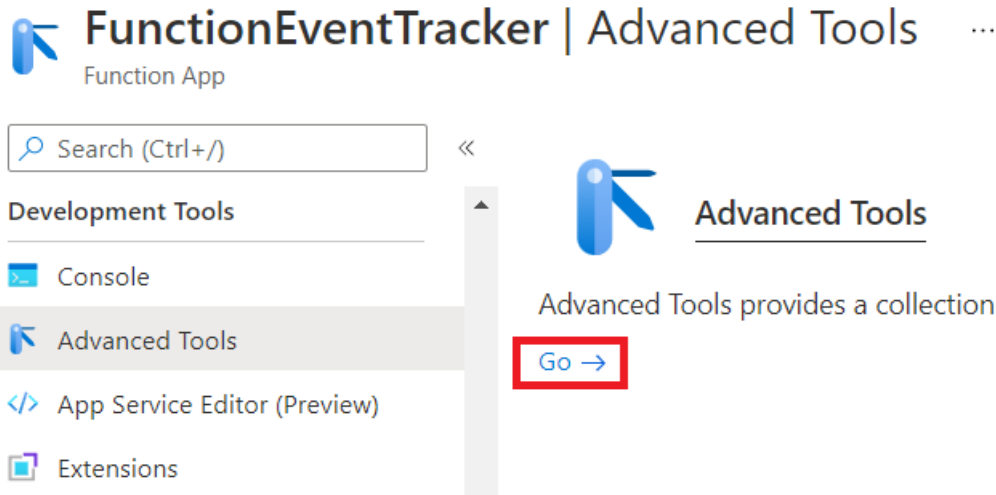
Development Tools

- Console
- Advanced Tools**
- App Service Editor (Preview)
- Extensions

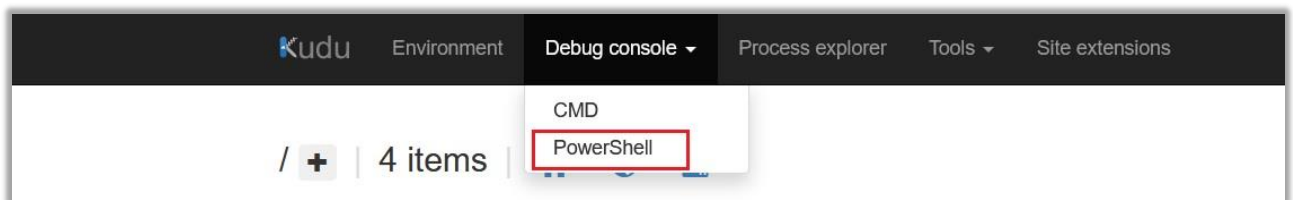
☐ Name ↑↓

☐ EventHubTrigger1

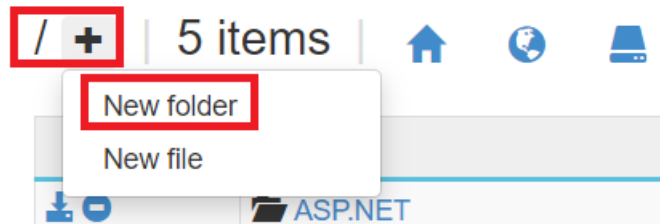
- Click **Go** and provide Azure credentials.



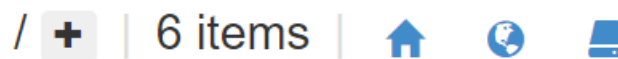
7. A new browser window opens. Select **PowerShell** from **Debug console** menu.



8. Click on **+** and click on **New folder** provide a folder name such as **ETS_Microsoft_Defender_FunctionApp**.



9. Click on folder which was created on last step



Name	
	ETS_Microsoft_Defender_FunctionApp
	ASP.NET

10. Copy the Base path as shown below, which will be used in the future step (step 21)
(Example path: - C:\home\ETS_Microsoft_Defender_FunctionApp)

... / ETS_Microsoft_Defender_FunctionApp +


Name

```
Kudu Remote Execution Console
Type 'exit' then hit 'enter' to get a new powershell process.
Type 'cls' to clear the console




















PS C:\home>
cd "C:\home\ETS_Microsoft_Defender_FunctionApp"
PS C:\home\ETS_Microsoft_Defender_FunctionApp>
```

11. Drag and drop the **Support** folder (as received in the integration package) to create a folder. A new **Support** folder is added.

... / ETS_Microsoft_Defender_FunctionApp +

Name
 Support

12. Navigate to the **Support/** folder and click on the **Edit** button for the **Details.xml** file.

... / Support +	4 items			
Name				
	Data Encryption.dll			
	Details.xml			
	EtsIns.dll			
	EvtTrkList.dll			

13. Here,
 - In line number 9, **mgr_name**, provide the EventTracker Manager hostname.
 - In line no. 10, **mgr_port**, enter the EventTracker Manager port number, e.g., 14505.
 - In line number 11, **mgr_ip**, provide the EventTracker Manager public IP address.
 - In line number 13, **org_name**, provide your organization name and org_name can only contain A-Z, a-z, 0-9, and Under score(_).

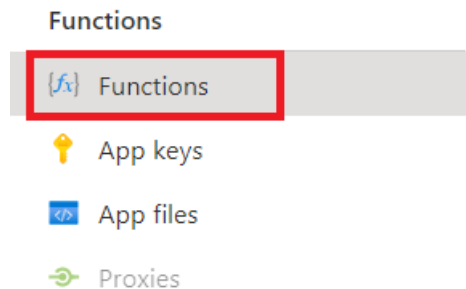
```

1 <Obj version="1.1.0.1"
2   xmlns="http://schemas.microsoft.com/powershell/2004/04">
3   <Obj RefId="0">
4     <TN RefId="0">
5       <T>System.Management.Automation.PSCustomObject</T>
6       <T>System.Object</T>
7     </TN>
8     <MS>
9       <S N="mgr_name">ET.CONTOSO.LOCAL</S> <!-- Replace with EventTracker manager name. e.g., ET.CONTOSO.LOCAL -->
10      <S N="mgr_port">14505</S> <!-- Replace with EventTracker manager port. e.g., 14505 -->
11      <S N="mgr_ip">198.17.23.198</S> <!-- Replace with EventTracker manager public IP address. e.g., 198.17.23.198 -->
12      <S N="sys_ip">127.0.0.1</S>
13      <S N="org_name">EventTracker</S> <!-- Replace with Organization Name. e.g., EventTracker -->
14    </MS>
15  </Obj>
16 </Obj>
17

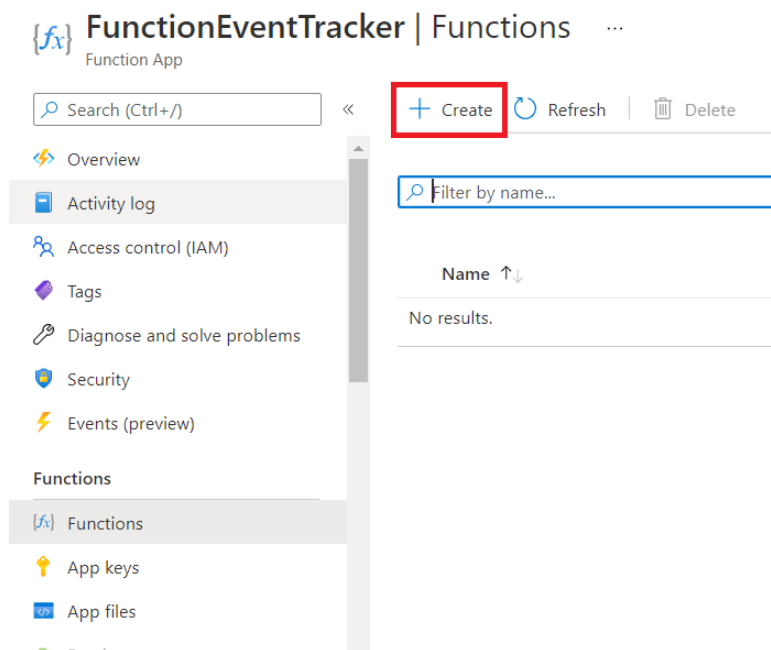
```

14. Click **Save**.

15. Come back to the Function APP tab (navigate to All services > Function App > FunctionEventTracker) to do further configuration and click **Functions** under Functions.



16. Click **Create**.



17. Select the **Develop in portal** option and click the **Azure Event Hub trigger**.

Create function

✕

Select development environment

Instructions will vary based on your development environment. [Learn more](#)

Development environ...

Develop in portal

Select a template

Use a template to create a function. Triggers describe the type of events that invoke your functions. [Learn more](#)

Filter

Azure Service Bus Queue trigger	A function that will be run whenever a message is added to a specified Service Bus queue
Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue
Azure Event Grid trigger	A function that will be run whenever an event grid receives a new event
Durable Functions HTTP starter	A function that will trigger whenever it receives an HTTP request to execute an orchestrator function

Create

Cancel

18. In the Event Hub connection, click **New**.

Create function

✕

Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue
Azure Event Grid trigger	A function that will be run whenever an event grid receives a new event
Durable Functions HTTP starter	A function that will trigger whenever it receives an HTTP request to execute an orchestrator function

Template details

We need more information to create the Azure Event Hub trigger function. [Learn more](#)

New Function *

EventHubTrigger1

Event Hub connection * ⓘ

No existing connections available

New

Event Hub name * ⓘ

samples-workitems

Event Hub consumer group ⓘ

\$Default

Create

Cancel

19. Let Azure populate the available Event Hub namespace and Event Hub. Select the desired ones and click **Ok**.

New Event Hub connection

☒ Event Hub
 ☐ IoT Hub
 ☐ Custom App Setting

Event Hub connection*

Microsoft Defender

Event Hub connection*

Microsoft Defender

Event Hub connection*

RootManageSharedAccessKey (nam...

OK

20. Click **Create**.

Create function

Azure Service Bus Topic trigger	A function that will be run whenever a message is added to the specified Service Bus topic
Azure Blob Storage trigger	A function that will be run whenever a blob is added to a specified container
Azure Event Hub trigger	A function that will be run whenever an event hub receives a new event
Azure Cosmos DB trigger	A function that will be run whenever documents change in a document collection
IoT Hub (Event Hub)	A function that will be run whenever an IoT Hub receives a new event from IoT Hub (Event Hub)
SendGrid	A function that sends a confirmation e-mail when a new item is added to a particular queue
Azure Event Grid trigger	A function that will be run whenever an event grid receives a new event
Durable Functions HTTP starter	A function that will trigger whenever it receives an HTTP request to execute an orchestrator function

Template details

We need more information to create the Azure Event Hub trigger function. [Learn more](#)

New Function*

EventHubTrigger1

Event Hub connection* ⓘ

hubaks_RootManageSharedAccessK... [New](#)

Event Hub name* ⓘ

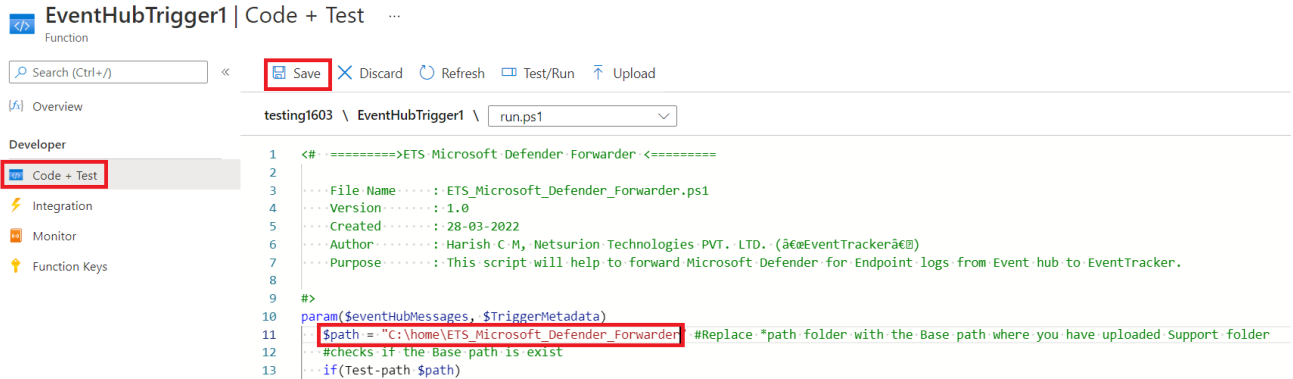
samples-workitems

Event Hub consumer group ⓘ

\$Default

Create **Cancel**

21. Click **Code+Test** and copy the contents of **ETS_Microsoft_Defender_forwarder.ps1** (as received in the integration package) and paste it into the given **run.ps1** window in the Azure function app portal and replace the path which was copied on **step 10** (Example path: - C:\home\ETS_Azure_FunctionApp) and click **Save**.

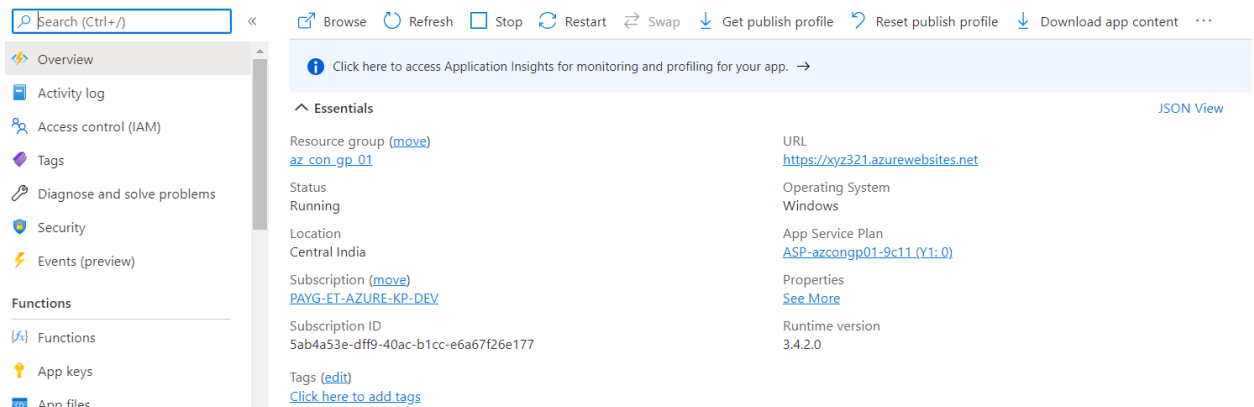


3.3 Cost Management

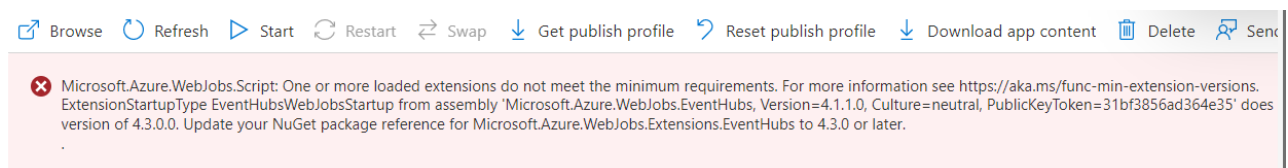
- The below-mentioned services are charged by Microsoft based on usage.
 - Function App
 - Click here [Function-App-price-tier](#) to know more on pricing details.
 - Event Hub
 - Click here [Event-Hub-price-tier](#) to know more on pricing details.

3.4 Verifying Function App

- Once the Function App is deployed, follow the below -mentioned steps to verify the deployment.
 - Login to <https://portal.azure.com/>
 - Search for Function App service.
 - Click on created Function App.
 - On successful deployment the screen would look as shown below.

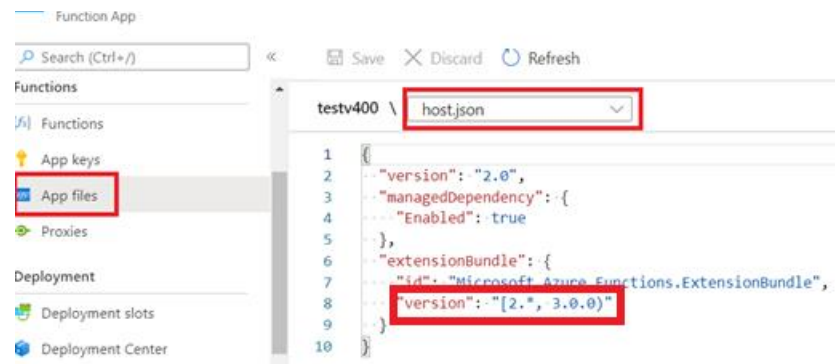


- Sometimes due to the mismatch of the extension package one could see below-mentioned error. Below are the steps provided to remediate the issue.

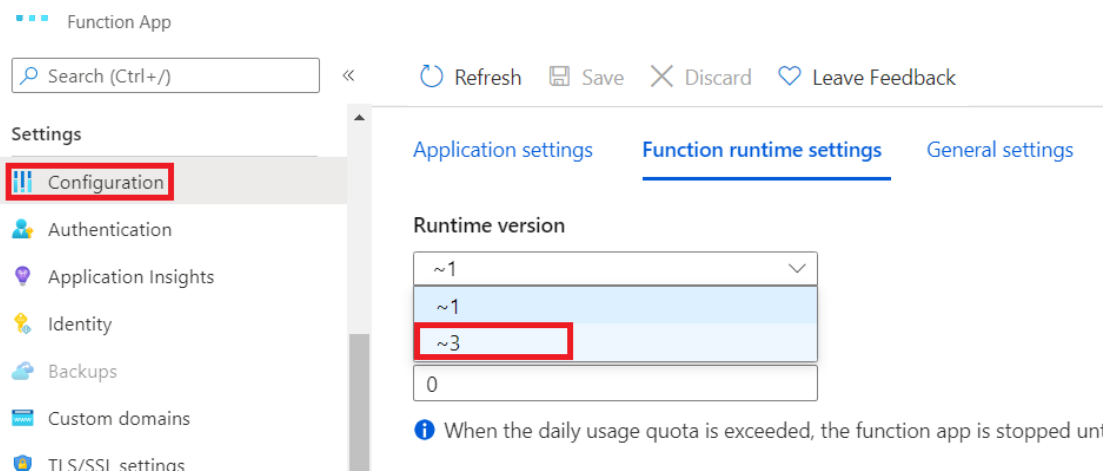


- To check the extension bundle.

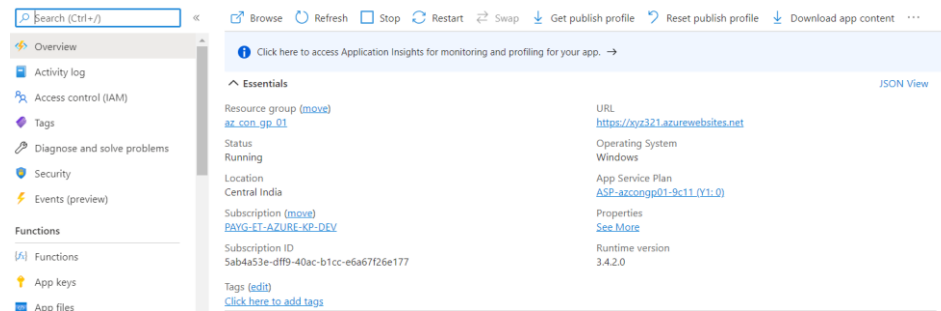
1. Click on **App files** under the Function section in the left pane of the function App home page
2. Choose **host.json** from the dropdown
3. Modify the version details in the JSON file to **"version": "[2.*, 3.0.0)"**
4. Click **Save**.



- To check the Function App run time version.
 1. Click on **Configuration** under Settings in the left pane of the function App home page.
 2. Click on **Function runtime settings**.
 3. Choose Runtime version to **~3** from the dropdown.
 4. Click **Save**.



- Click on the **Overview** in the left pane to go to the **Function App** home page.
Now the home page should not be showing the earlier error message as shown below.



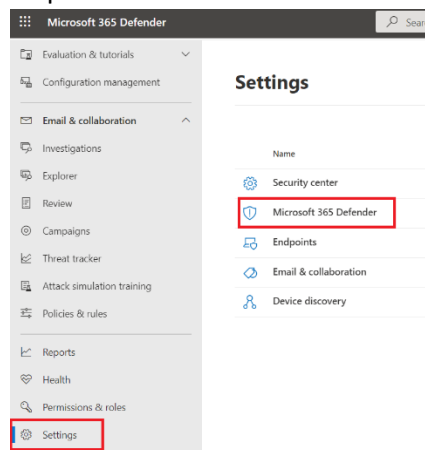
4. Configuring Microsoft Defender to Forward Logs to Event hub

Microsoft Defender for Endpoint can be integrated with EventTracker by streaming the logs to the Azure Event Hub, and from Azure Event Hub to EventTracker.

4.1 Configuring Microsoft Defender to stream events to Event Hub

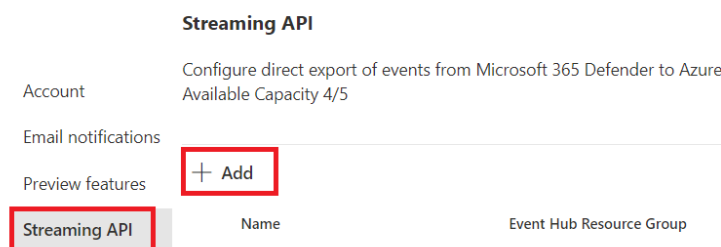
Login to security.microsoft.com using the admin account and [create an event hub namespace](#), if not created.

1. Click on **Settings** on the left panel and click **Microsoft 365 Defender**.



2. Click **Streaming API** and Click on **+Add**.

Settings > Microsoft 365 Defender



3. Configure Stream API.

- Fill Name like **EventTracker**.
- Check the box **Forward event to Azure Storage**.
- **Paste** Event-Hub Resource ID (Copied on 3.1 step 4).
- **Paste** Event-Hub name (Copied on 3.1 step 6).
- Check the box **Alerts** under **Events Types**.
- Click **Submit**.

Add new Streaming API settings

Configure new Streaming API settings, in order to forward Microsoft 365 Defender events to Azure storage and / or event hub. [Read about how to fill this form](#)

Name *

EventTracker

☐ Forward events to Azure Storage

☒ Forward events to Event Hub

Event-Hub Resource ID *

/subscriptions/5ab4a53e-dff9-40ac-b1cc-e6a67f26e177/resourceGroups/az_con_g...

Event-Hub name ⓘ

MicrosoftDefender

Events Types (2/20)

☒ Alerts
☐ Devices
☐ Email

Submit Cancel

4. After successful configuration the following screen display.

Settings > Microsoft 365 Defender

Streaming API

Account Configure direct export of events from Microsoft 365 Defender to Azure
Available Capacity 3/5

Email notifications

Preview features

+ Add

Streaming API

Name

Event Hub Resource Group

EventTracker

az_con_gp_01

5. 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 Microsoft Defender.

5.1 Alerts

- **Microsoft Defender for Endpoint: Critical threat detected:** This alert indicates a critical threat is detected in Microsoft Defender for Endpoint.

5.2 Categories

- **Microsoft Defender for Endpoint – Alerts:** This category of the saved search will allow users to parse events specific to the alert info on the Microsoft Defender for Endpoint.

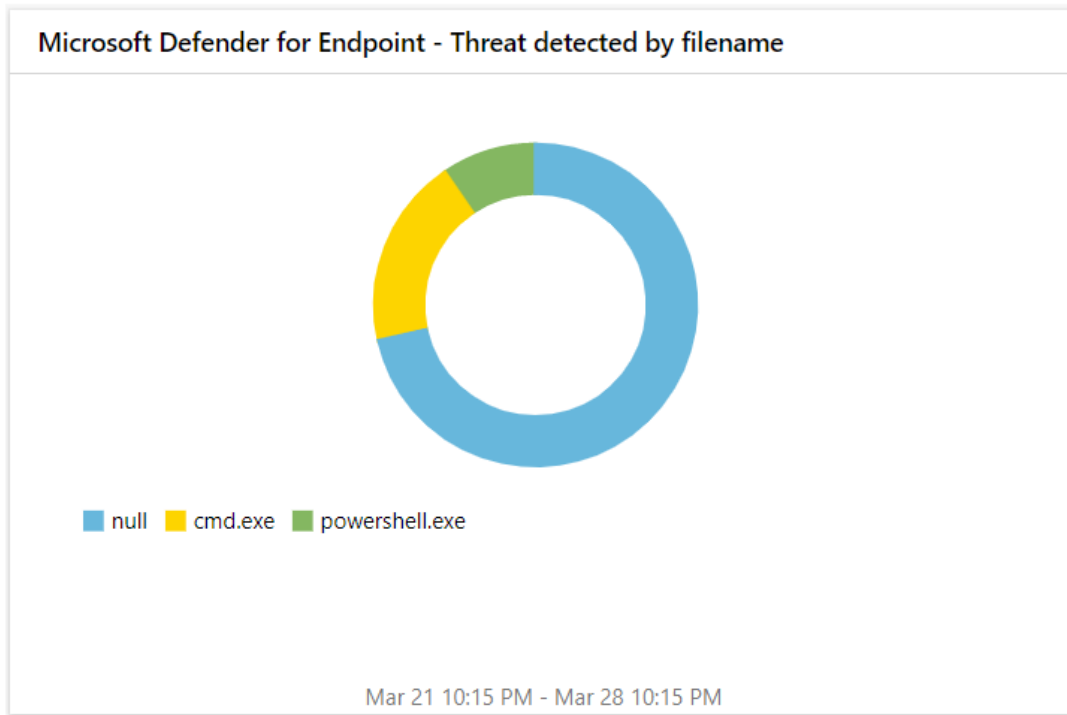
5.3 Reports

- **Microsoft Defender for Endpoint - Alerts detail:** This report provides a detailed summary of defender alerts in Microsoft Defender for Endpoint. It contains a source IP address, remote IP address, alert ID, detection source, attack technique, severity, device name, remote URL, threat family, and more.

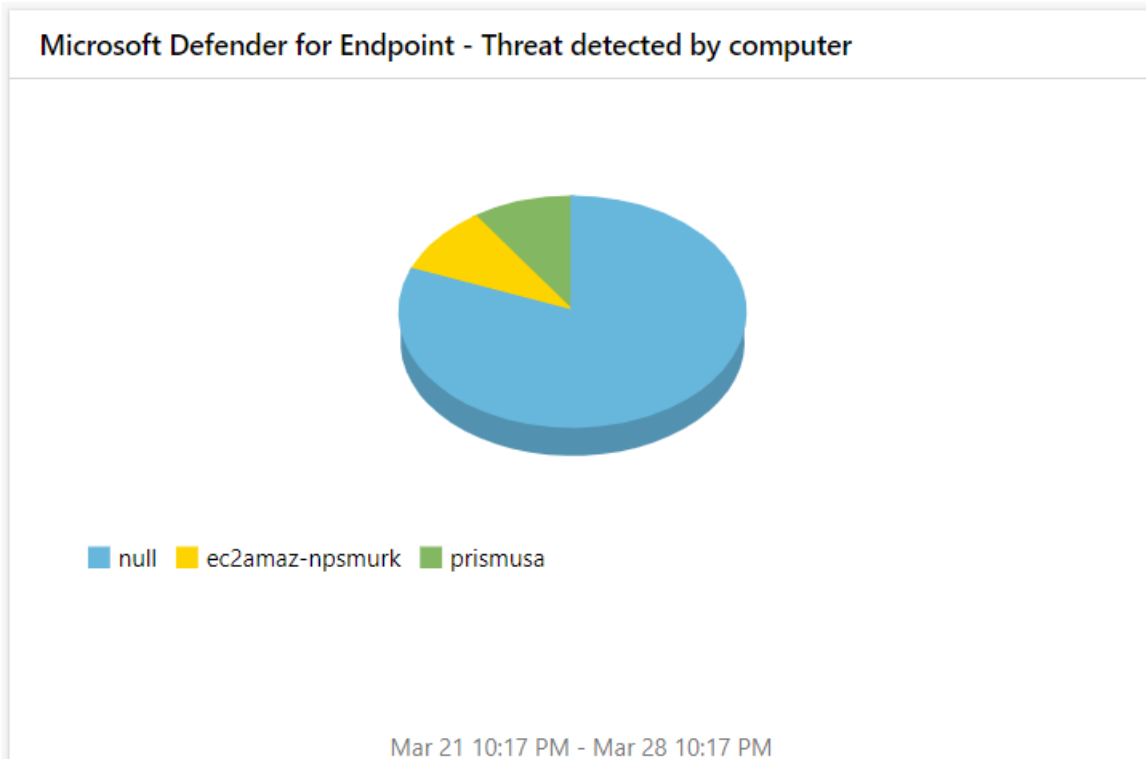
LogTime	Computer	Alert ID	Attack Techniques	Severity	Alert Title	Operation	Detection Source	Alert Category	Evidence Role	SHA256	Tenant ID	Account Domain	Account Name	Account SID	Device Name	File Name	Folder Path	Source IP	Machine Group
03-25-2022 04:48:54 AM	MSDEFEND POINT	da6378361- 659087978 14_- 259418956				Publish		Advanced Hunting- AlertEvide nce	Impacted	da6378361- 1659087978 7814_- 259418956 4	0ac05f5c- 4238-4951- 89a8- 2b5e51880 5f0	"EAMAZ- NPSMUR K",	"Administ rator",	"S-1-5-21- 17456755- 4238-4951- 93- 89a8- 13871087- 2b5e518805f 66- 15992110 62-500",	0ac05f5c- 4238-4951- 89a8- 2b5e518805f 0	"powershell. exe",	"C:\\Window s\\System32 ",	10.12.56.101	MTB-LIFE
03-25-2022 04:48:54 AM	MSDEFEND POINT	da6378361- 659087978 14_- 259418813	["PowerShell (T1059.001)"]	High	Suspicious Powershell commandline	Publish	EDR	Advanced Hunting- AlertInfo			0ac05f5c- 4238-4951- 89a8- 2b5e51880 5f0								null,
03-25-2022 04:48:54 AM	MSDEFEND POINT	da6378361- 659087978 14_- 259418813				Publish		Advanced Hunting- AlertEvide nce	Related	bc866cfc- dda37e24- dc2634dc- 282c7a0e- 6f55209d- a17a8fa1- 05451741- 4c0e7c52 7	0ac05f5c- 4238-4951- 89a8- 2b5e51880 5f0	"SES- NPSMUR K",	"Administ rator",	"S-1-5-21- 17456755- 4238-4951- 93- 89a8- 13871087- 2b5e518805f 66- 15994551 62-500",	0ac05f5c- 4238-4951- 89a8- 2b5e518805f 0	"cmd.exe",	"C:\\Windo ws\\System 32",	10.52.12.3	null,

5.4 Dashboards

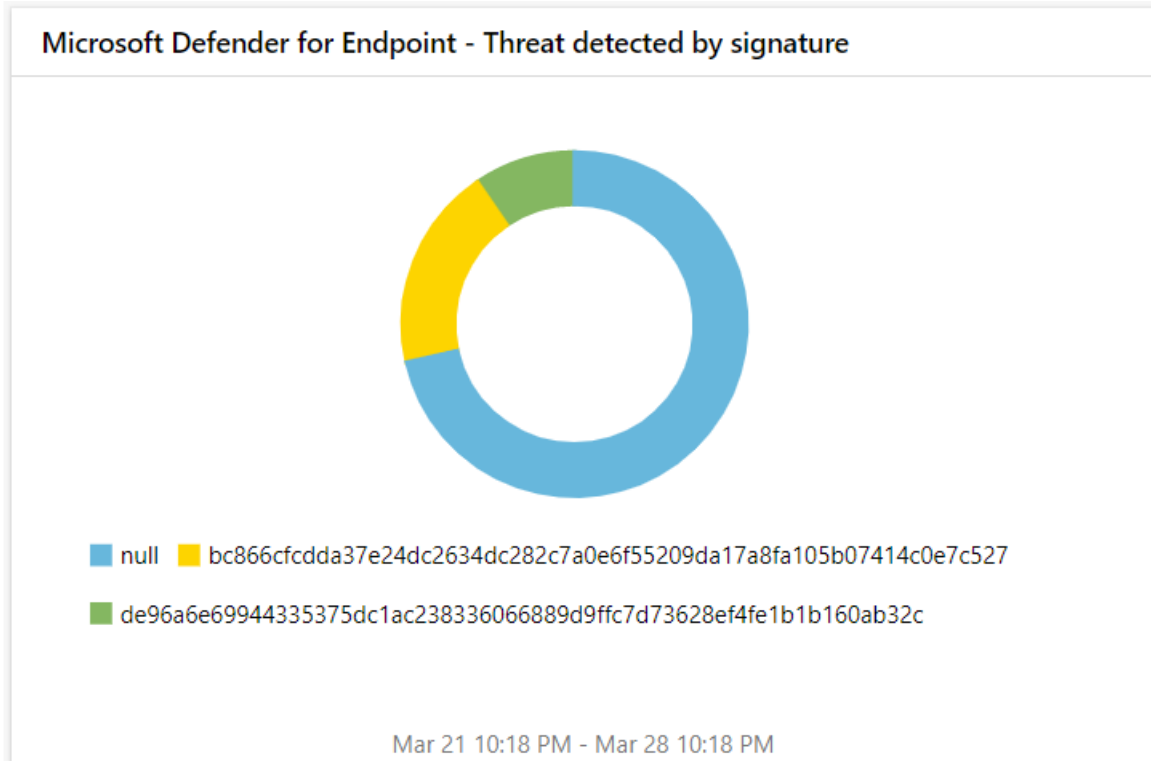
- Microsoft Defender for Endpoint - Threat detected by filename



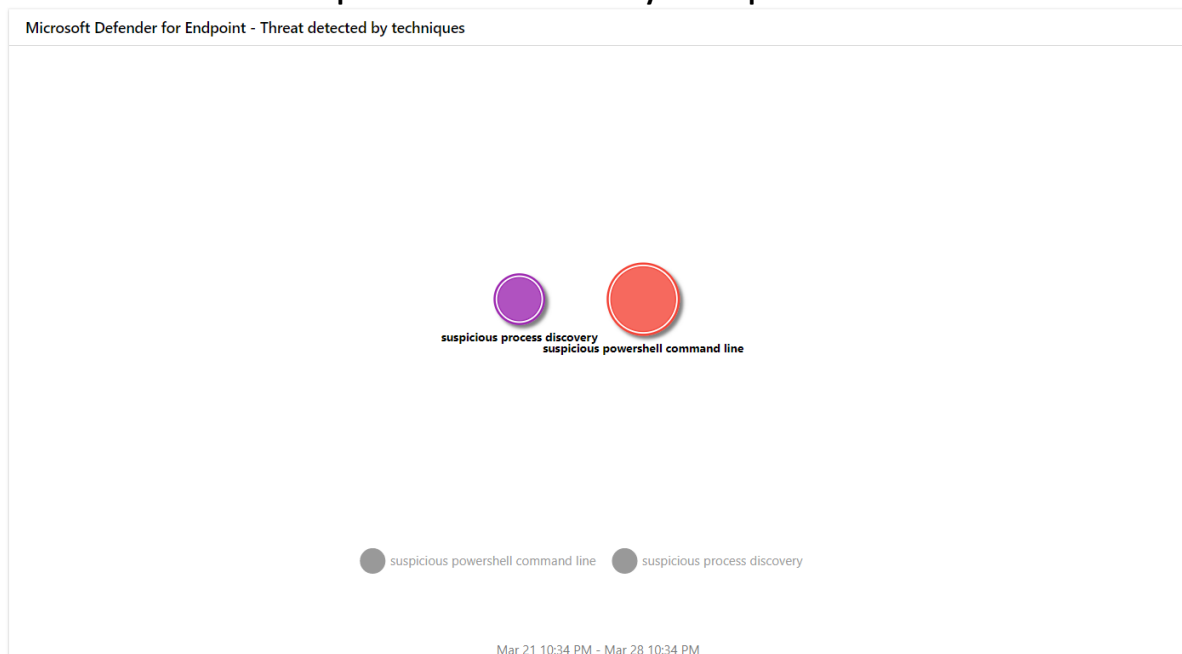
- Microsoft Defender for Endpoint - Threat detected by computer



▪ **Microsoft Defender for Endpoint - Threat detected by signature**



▪ **Microsoft Defender for Endpoint - Threat detected by techniques**

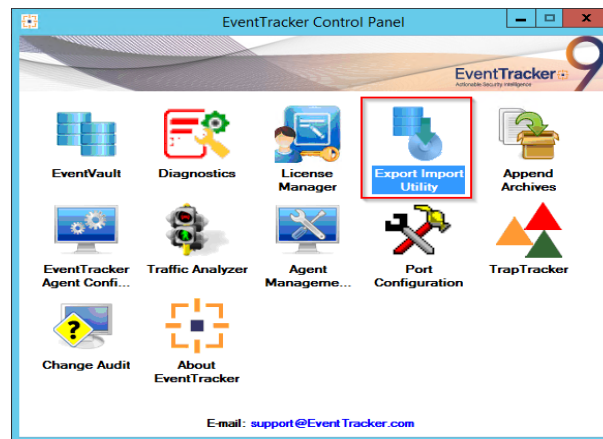


6. Importing Microsoft Defender Knowledge Packs into EventTracker

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

- Categories
- Alerts
- Knowledge Objects
- Reports
- Dashboards

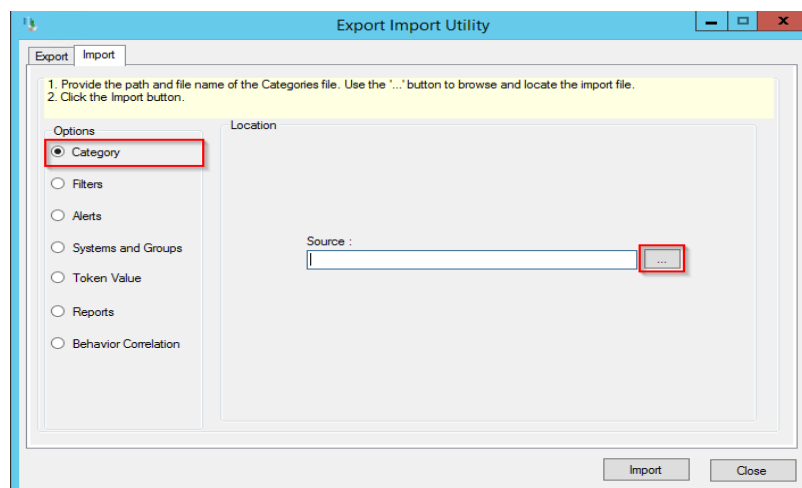
1. Launch the **EventTracker Control Panel**.
2. Double click the **Export-Import Utility**.



3. Click the **Import** tab.

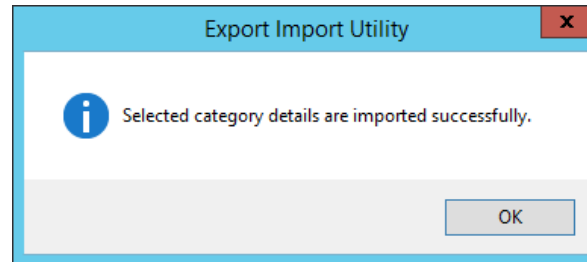
6.1 Categories

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



2. Locate the **Categories_Microsoft Defender for Endpoint.iscat** file, and then click the **Open** button.
3. To import the categories, click the **Import** button.

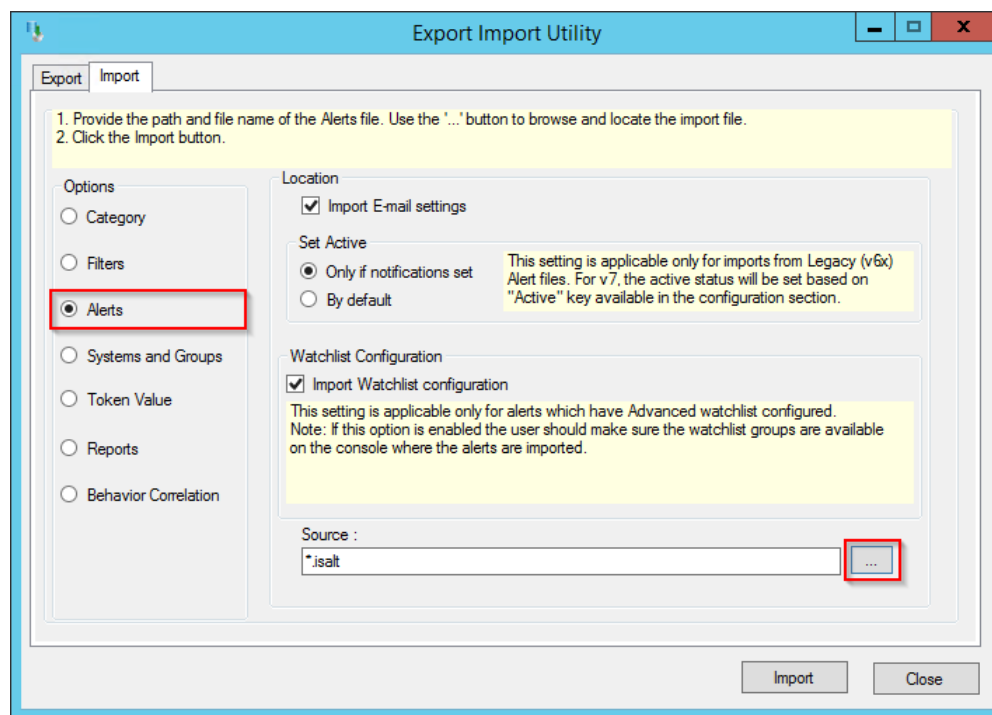
EventTracker displays a success message.



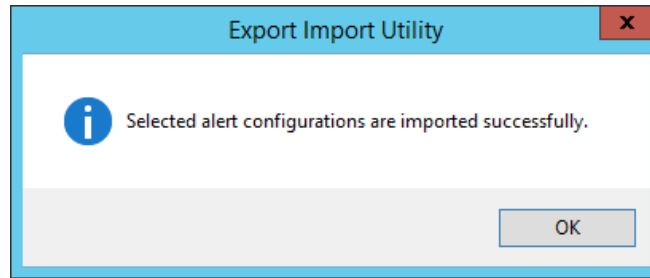
4. Click **OK**, and then click the **Close** button.

6.2 Alerts

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



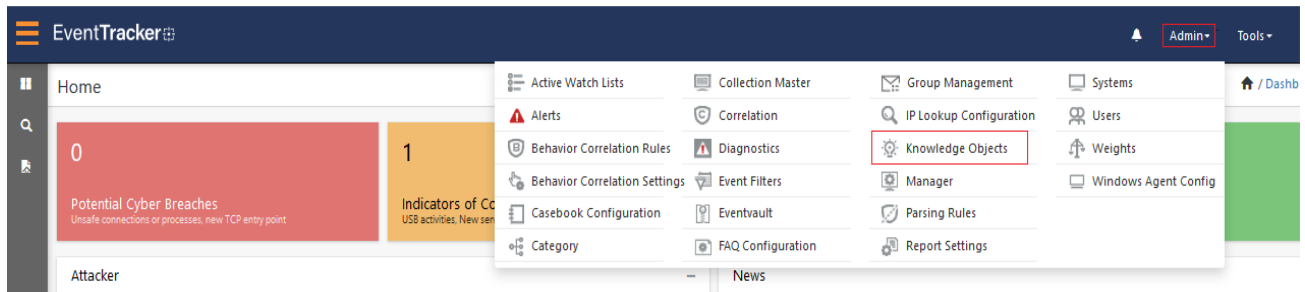
2. Locate the **Alerts_Microsoft Defender for Endpoint.isalt** file, and then click the **Open** button.
 3. To import the alerts, click the **Import** button.
- EventTracker displays a success message.



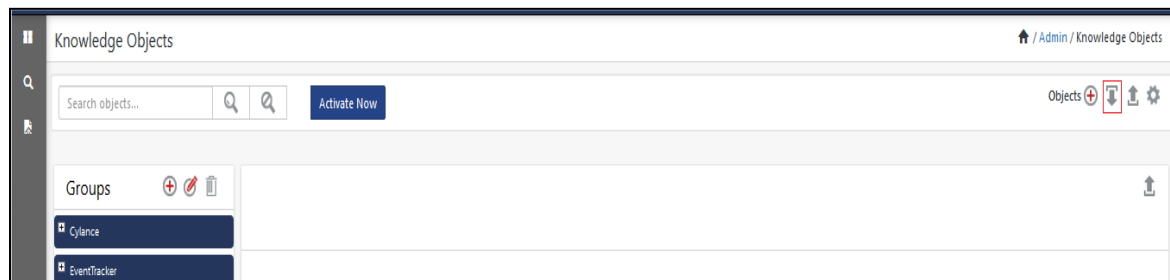
- Click **OK**, and then click **Close**.

6.3 Knowledge Objects (KO)

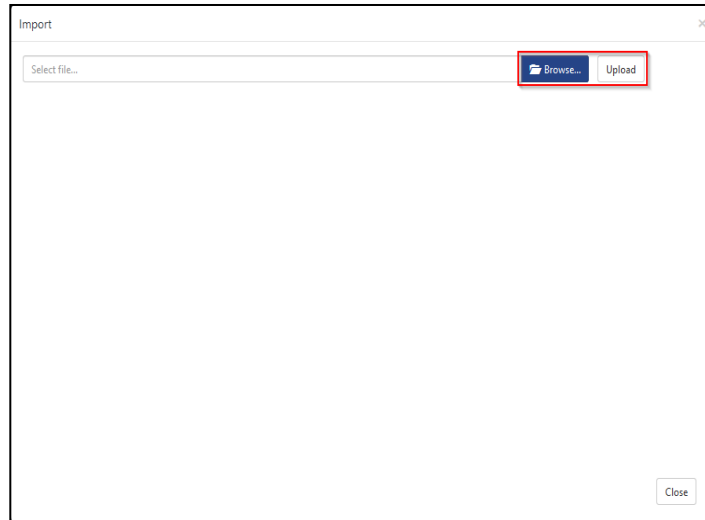
- Click **Knowledge Objects** under the **Admin** option on the EventTracker Manager page.




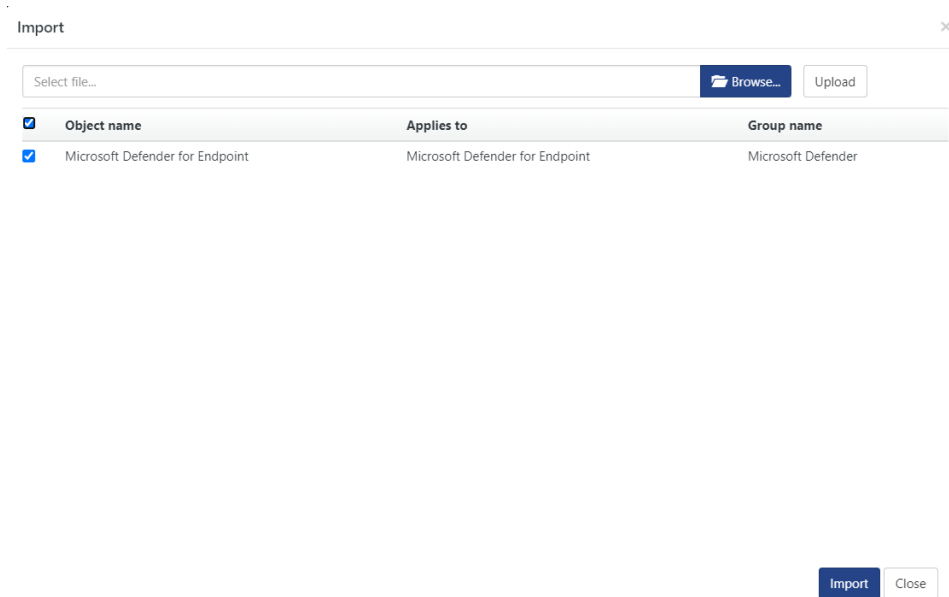
- Click the **Import** button as highlighted in the below image:



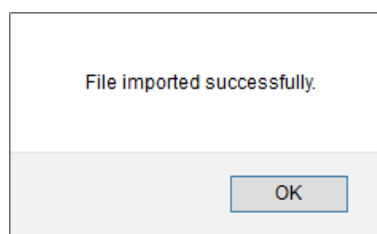
- Click **Browse**.



4. Locate the file named **KO_Microsoft Defender for Endpoint.etko**.
5. Select the check box and then click the  **Import** option.

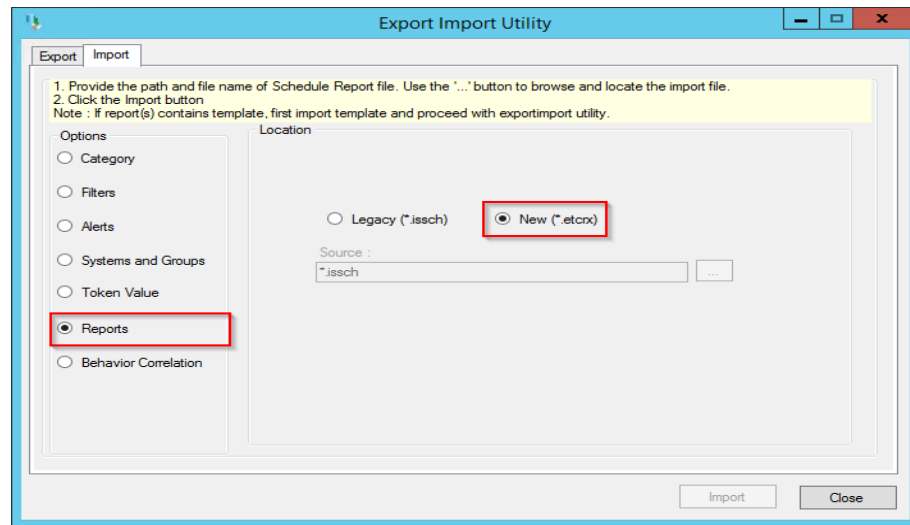


6. The Knowledge Objects (KO) are now imported successfully.

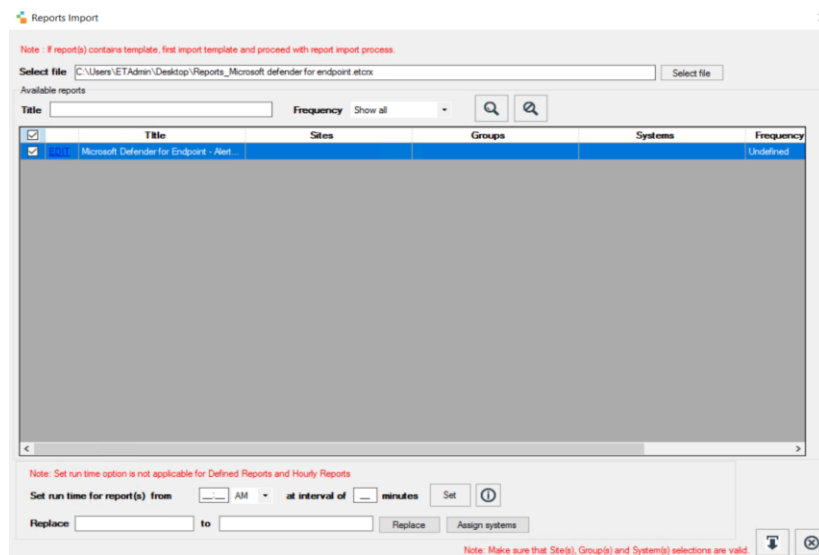


6.4 Reports

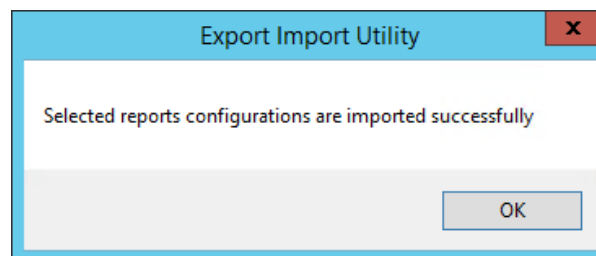
1. Click the **Reports** option and select the **New (*.etcrx)** option.



2. Locate the file named **Reports_Microsoft Defender for Endpoint.etcrx** and select all the check boxes.



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



6.5 Dashboards

NOTE: Below steps given are specific to EventTracker9 and later.

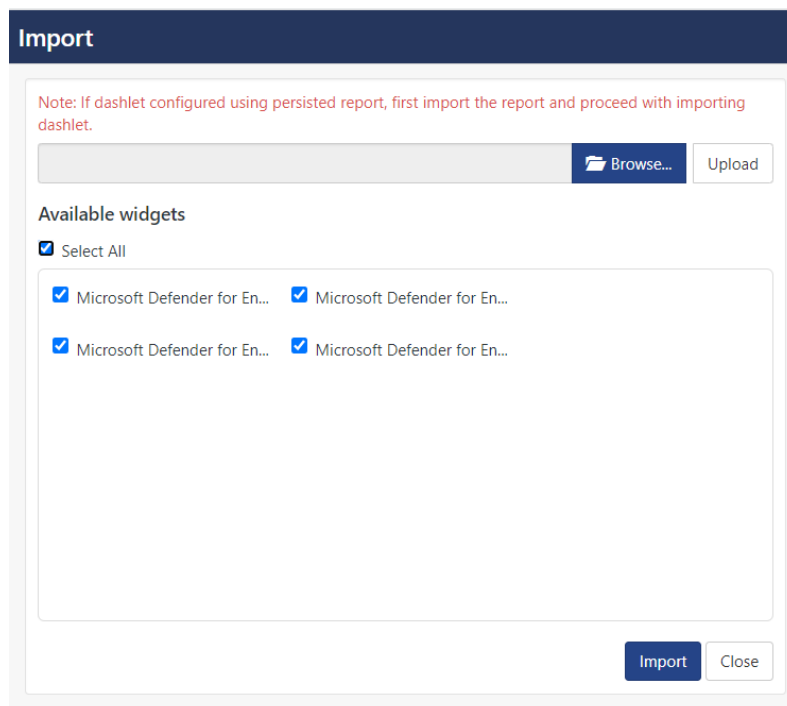
1. Open **EventTracker** in a browser and log on.



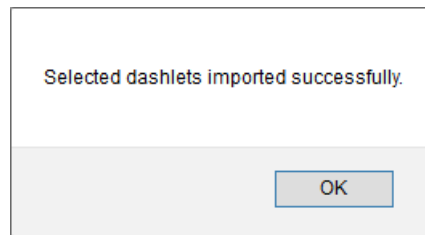
2. Navigate to the **My Dashboard** option.
3. Click the **Import** button as shown below.




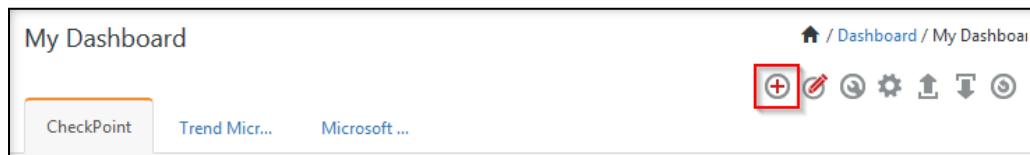
4. Import the dashboard file **Dashboards_ Microsoft Defender for Endpoint.etwd** and select the **Select All** checkbox.
5. Click **Import** as shown below.



6. Import is now completed successfully.



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



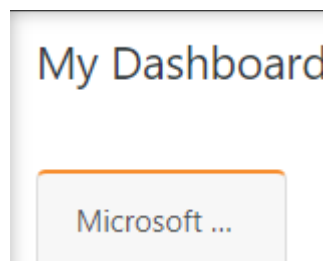
8. Choose the appropriate name for the **Title** and **Description**. Click **Save**.

Add Dashboard

Title

Description

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



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

Customize dashlets

Microsoft Defender

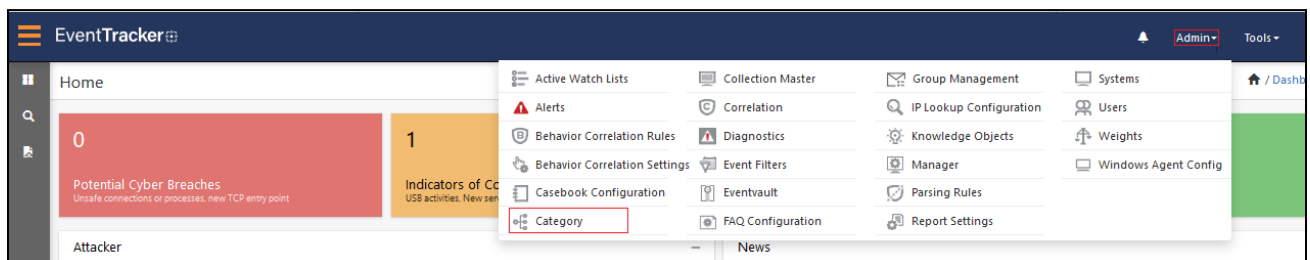
☒ Microsoft Defender For Endpoi... ☒ Microsoft Defender For Endpoi... ☒ Microsoft Defender For Endpoi... ☒ Microsoft Defender For Endpoi...

Add Delete Close

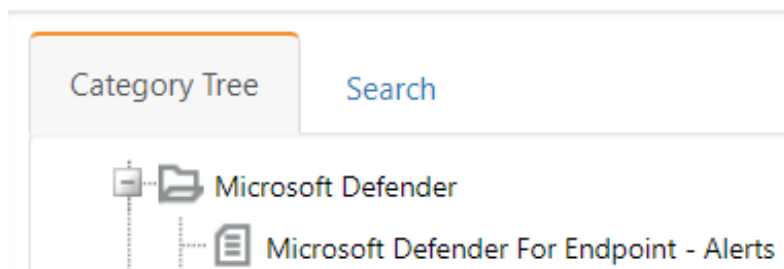
7. Verifying Microsoft Defender Knowledge Packs in EventTracker

7.1 Categories

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

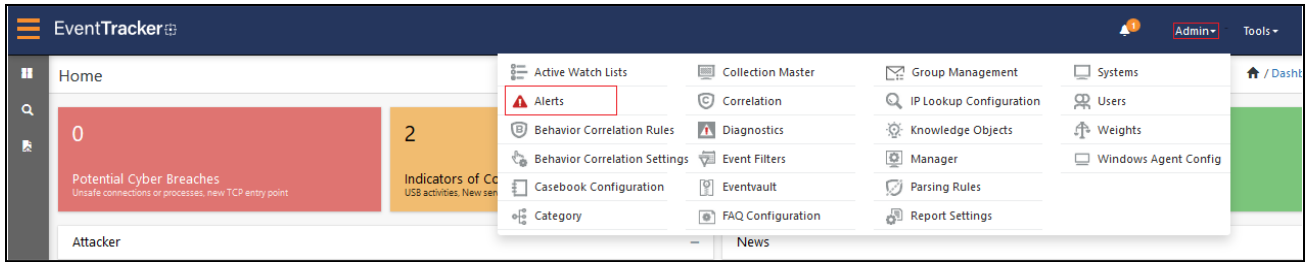


3. In the **Category Tree**, scroll down and expand the **Microsoft Defender** group folder to view the imported category.

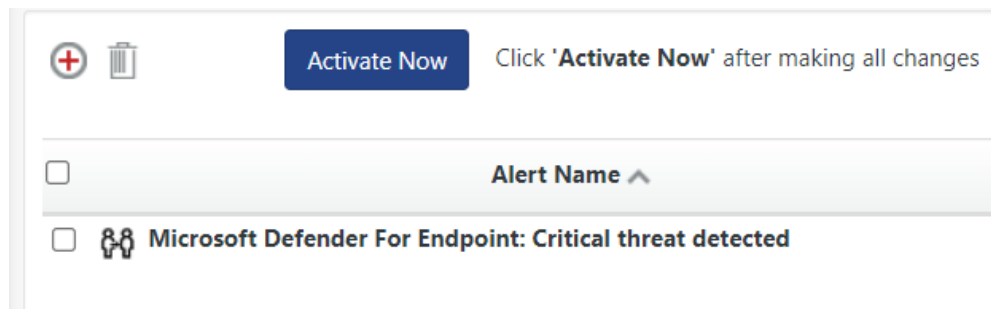


7.2 Alerts

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



3. In the **Search** box, type **Microsoft Defender**, 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.

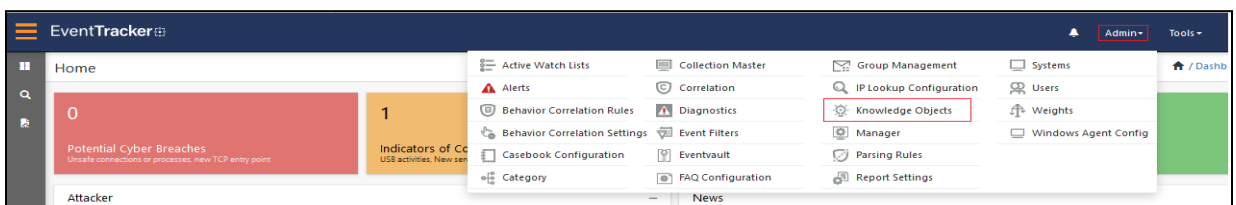


5. Click **OK**, and then click the **Activate Now** button.

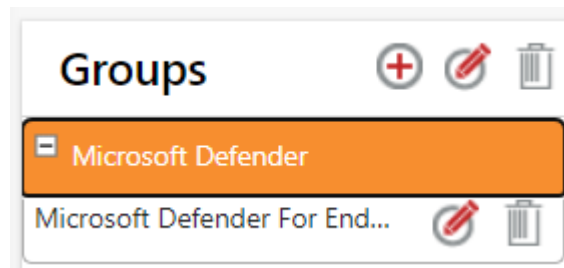
NOTE: Specify the appropriate **system** in **alert configuration** for better performance.

7.3 Knowledge Objects

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



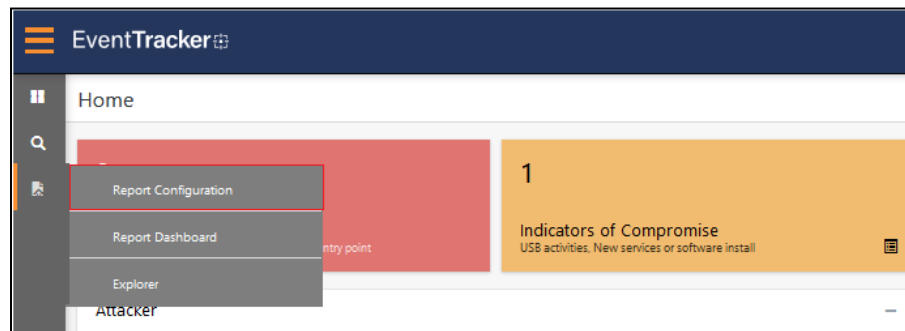
2. In the Knowledge Object tree, expand the **Microsoft Defender** group folder to view the imported Knowledge Objects.



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

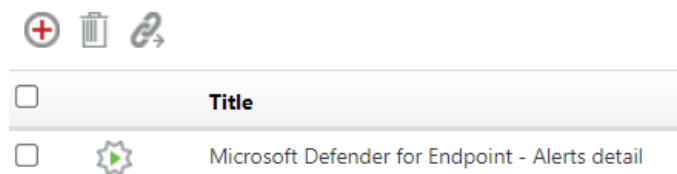
7.4 Reports

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



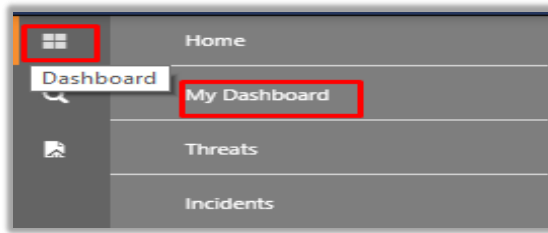
2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click the **Microsoft Defender** group folder to view the imported reports.

Reports configuration: Microsoft Defender

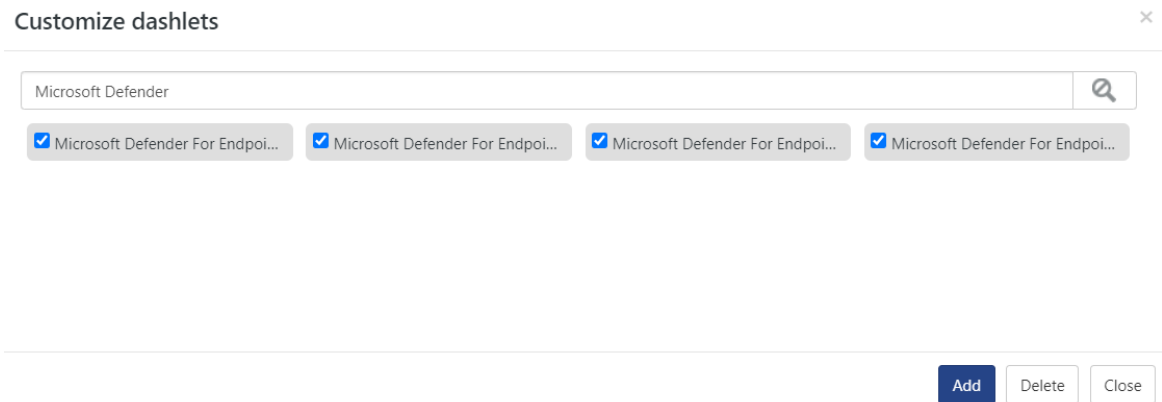


7.5 Dashboards

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



- Click **Search**  for the **Microsoft Defender**. 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](https://www.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>