

How-To Guide

Configuring Microsoft Defender to Forward Logs to 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 Contents3
- 1. Overview4
- 2. Prerequisites.....4
- 3. Configuring Event hub to Forward Logs to EventTracker4
 - 3.1 Creating an Event Hubs namespace and an Event Hub4
 - 3.2 Configuring Azure Function app to forward data to EventTracker6
 - 3.3 Cost Management15
 - 3.4 Verifying Function App.....15
- 4. Configuring Microsoft Defender to Forward Logs to Event hub17
 - 4.1 Configuring Microsoft Defender to stream events to Event Hub17
- About Netsurion19
- Contact Us.....19

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](#)

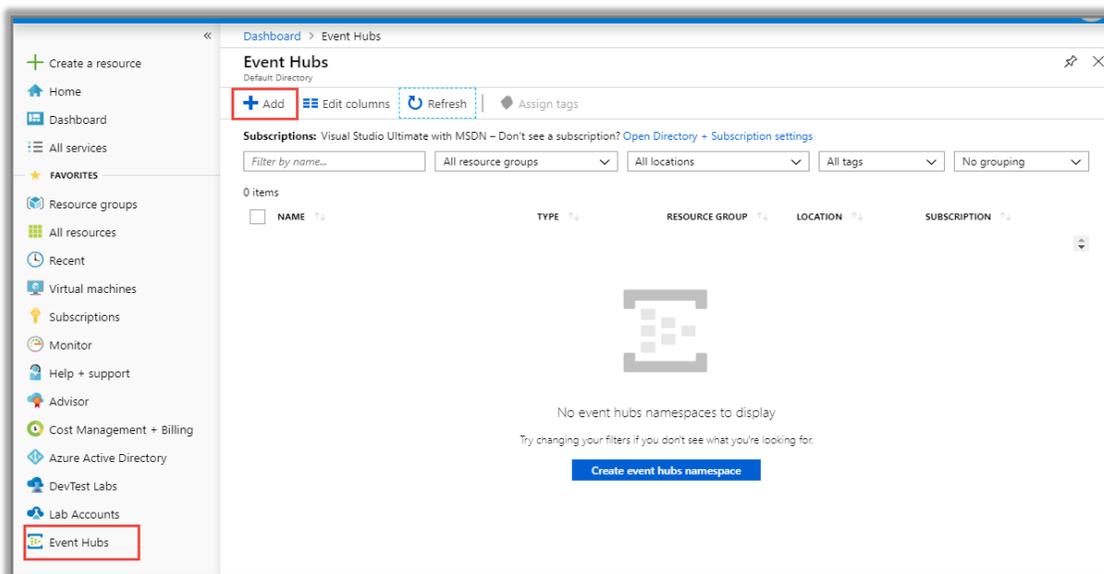
3. Configuring Event hub to Forward Logs to EventTracker

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

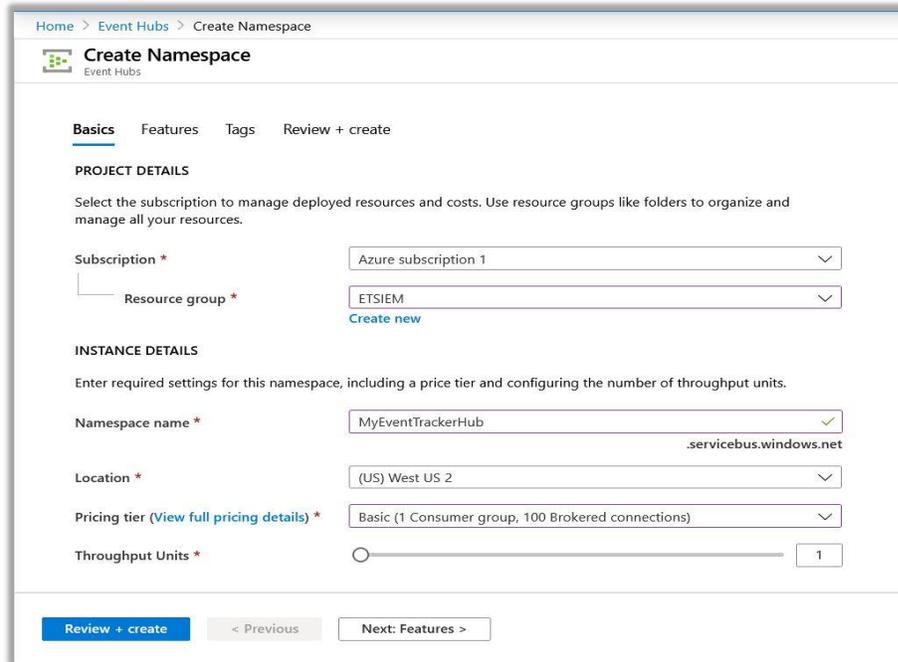
3.1 Creating an Event Hubs namespace and an Event Hub

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.

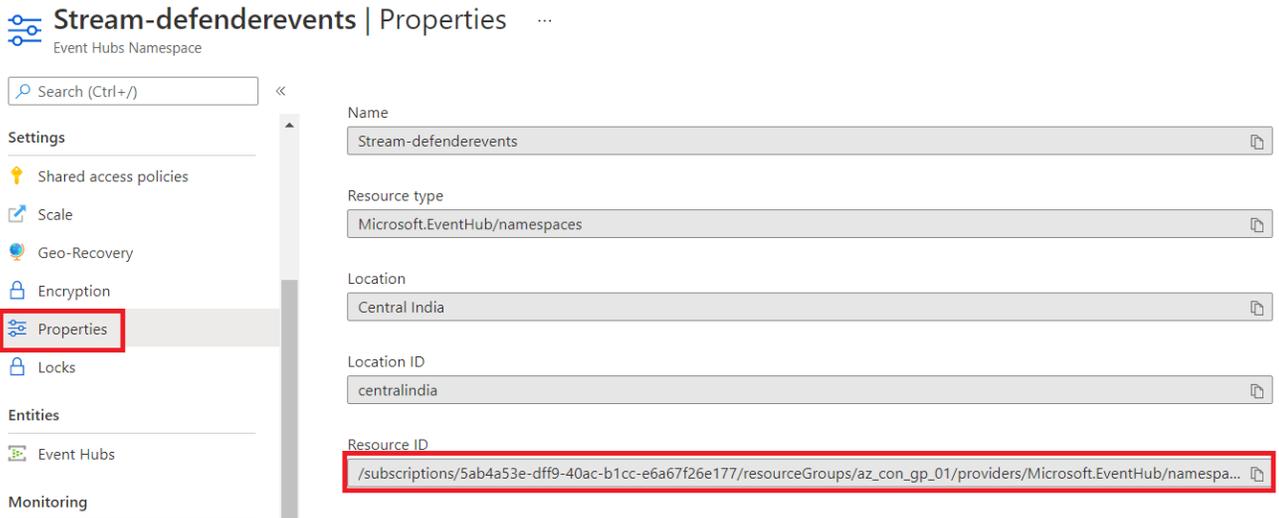
1. Login to portal.azure.com
2. Navigate to **All services > Event Hubs > Add**.



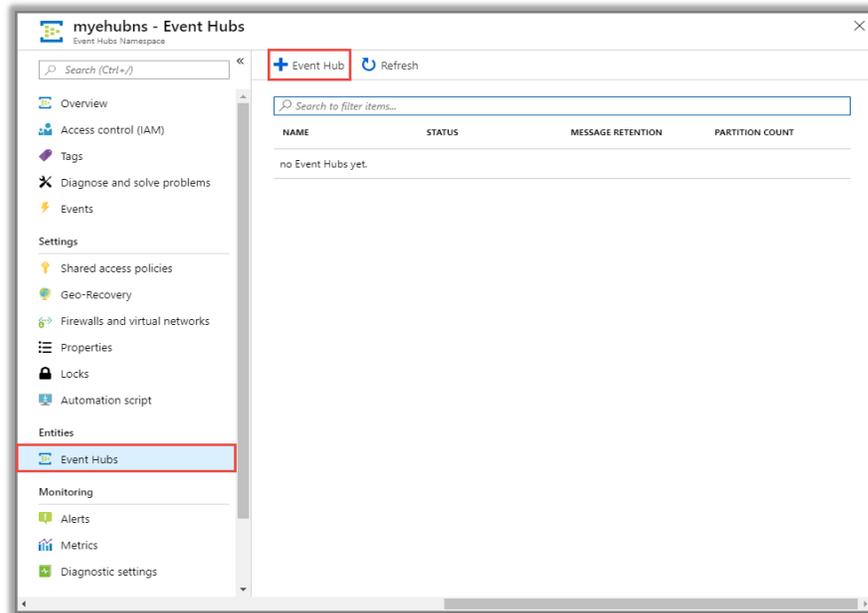
3. Create a namespace. Provide a **Namespace Name**, e.g. **MyEventTrackerHub**, Resource group, and any other settings -> **Review + Create**.
Recommendation: Create and choose Resource group Name with "EventTracker". It would give a better picture of the billing for the services.



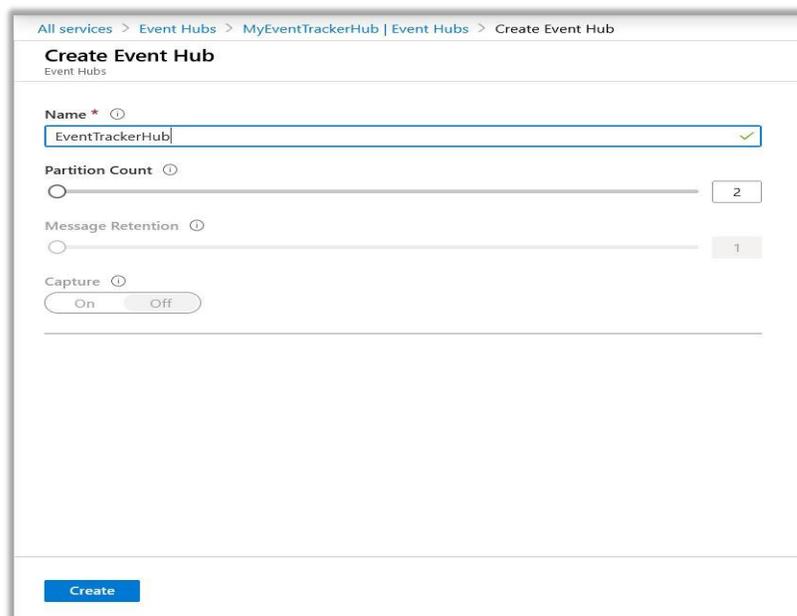
4. On the Event Hubs namespace page, Click **Properties** under **Settings** on the left panel and copy the **Resource ID** value, Which will be used in [further](#) steps (4.1 step 3)



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



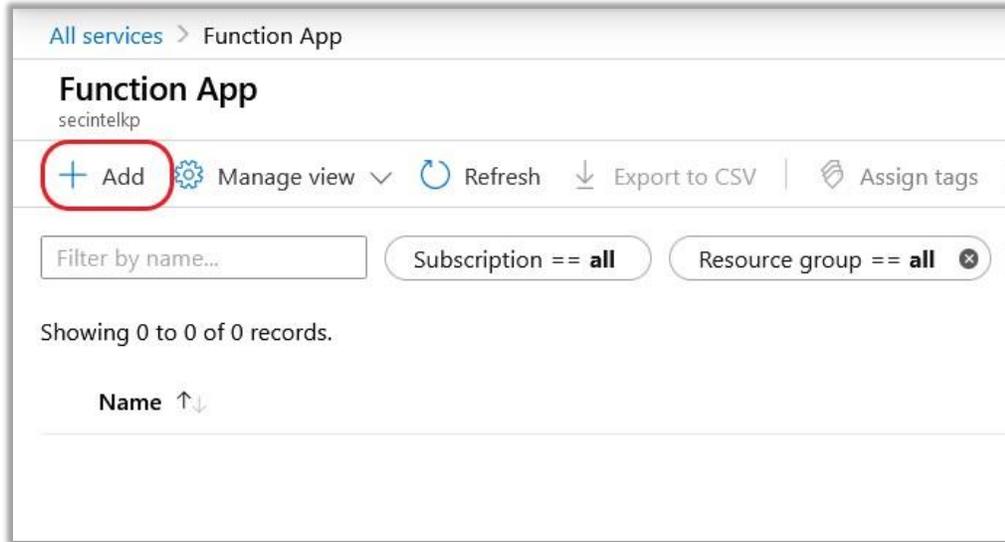
6. Type a name for your Event Hub and provide the EventHub name, partition count based on your environment, **Copy** the Event Hub name which will be used in [further](#) steps (4.1 Step 3), and then click **Create**.



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 * ⓘ

Resource Group * ⓘ [Create new](#)

Instance Details

Function App name * .azurewebsites.net

Publish * Code Docker Container

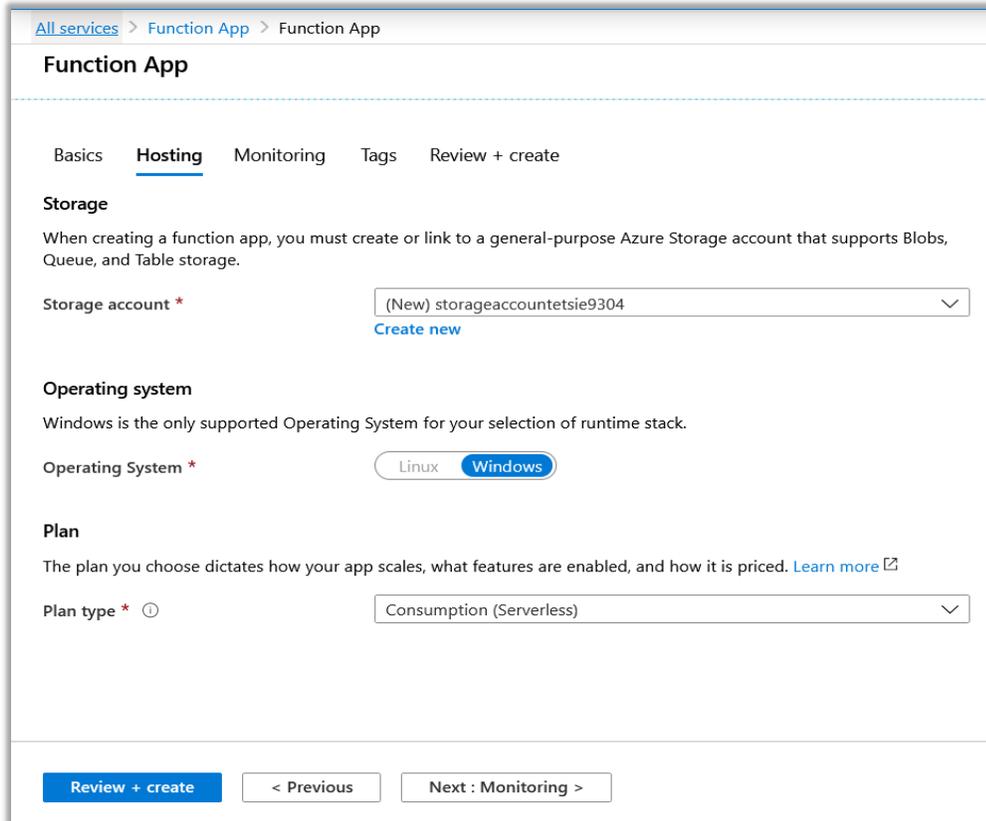
Runtime stack *

Version *

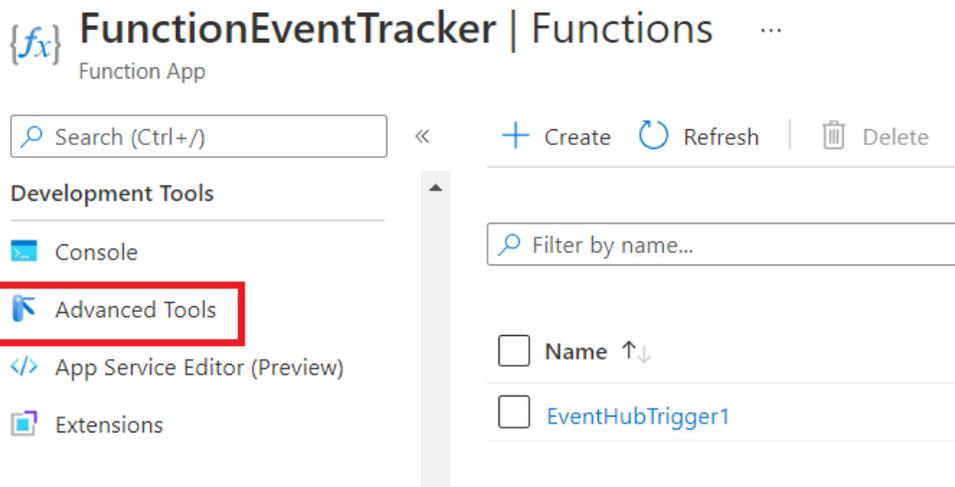
Region *

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

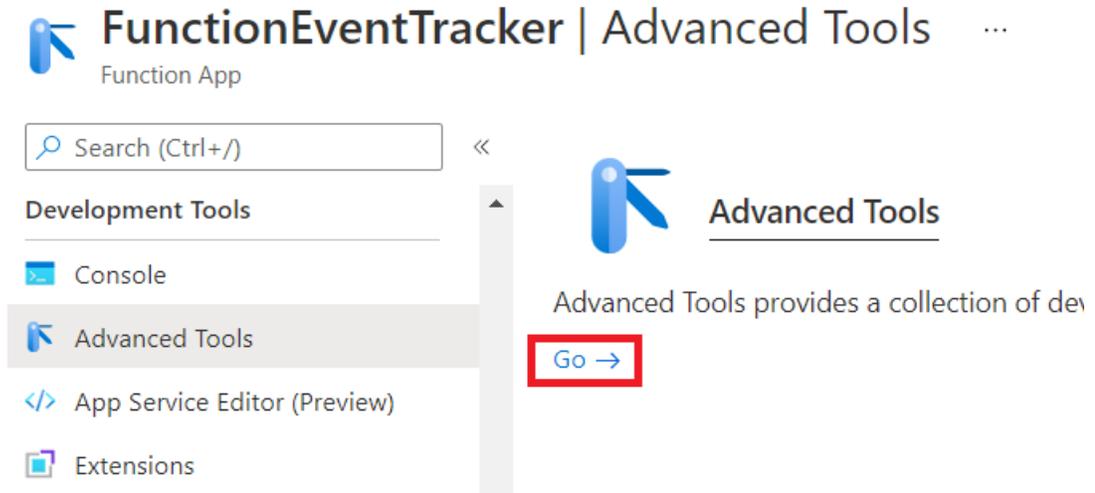
3. Click **Next: Hosting**.
 - Under Storage Section, select your storage account.
 - Under the Operating system, select Windows.
 - Under Plan, choose a plan of your choice.



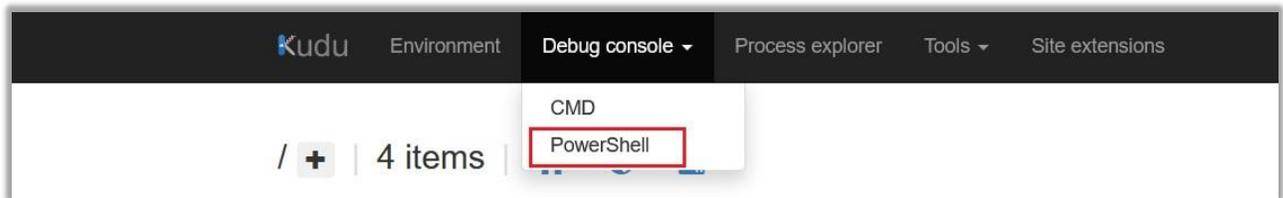
4. Click **Review + Create**.
5. After the **Function** app is created, navigate to All services > Function App > FunctionEventTracker to do further configuration and click on Advanced **tools** under **Development Tools**.



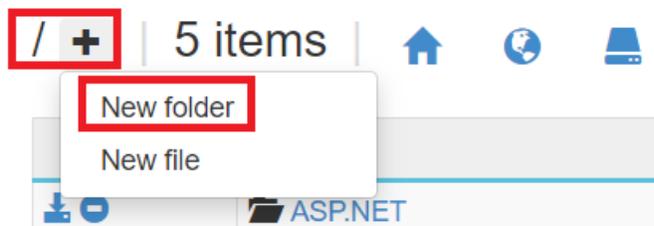
6. Click **Go** and provide Azure credentials.



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**)



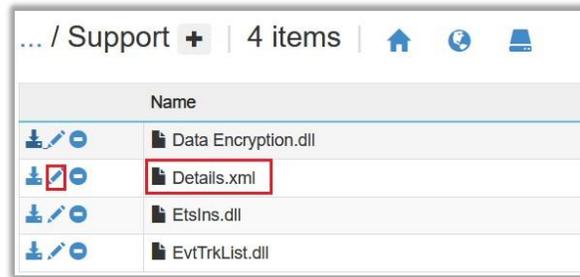
```
Kudu Remote Execution Console
Type 'exit' then hit 'enter' to get a new powershell process.
Type 'cls' to clear the console

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.



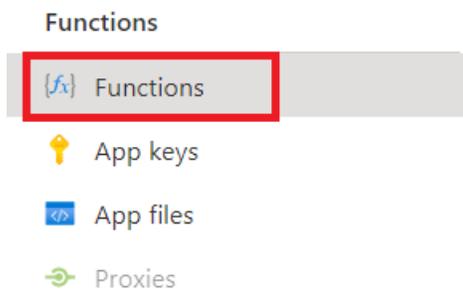
- 12. Navigate to the **Support/** folder and click on the **Edit** button for the **Details.xml** file.



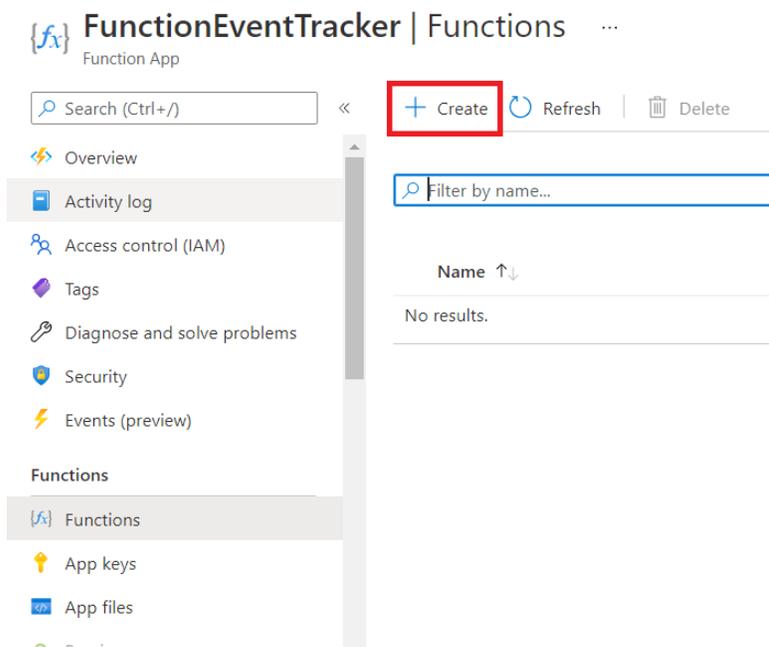
- 13. Here,
 - In line number 9, **mgr_name**, provide the EventTracker Manager hostname.
 - In line no. 10, **mgr_port**, enter the EventTracker Manager port number, e.g., 14505.
 - In line number 11, **mgr_ip**, provide the EventTracker Manager public IP address.
 - In line number 13, **org_name**, 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>
```

- 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*

Event Hub connection*

New

Event Hub name*

Event Hub consumer group

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 (preview)	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 *

Event Hub connection * ⓘ New

Event Hub name * ⓘ

Event Hub consumer group ⓘ

Create

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**.

```

1 <#=====>ETS_Microsoft_Defender_Forwarder <=====>
2
3 File Name : ETS_Microsoft_Defender_Forwarder.ps1
4 Version : 1.0
5 Created : 28-03-2022
6 Author : Harish C M, Netsurion Technologies PVT. LTD. (â€@EventTrackerâ€@)
7 Purpose : This script will help to forward Microsoft Defender for Endpoint logs from Event hub to EventTracker.
8
9 #>
10 param($eventHubMessages, $TriggerMetadata)
11 $path = "C:\home\ETS_Microsoft_Defender_Forwarder" #Replace "path folder with the Base path where you have uploaded Support folder
12 #checks if the Base path is exist
13 if(Test-path $path)
    
```

3.3 Cost Management

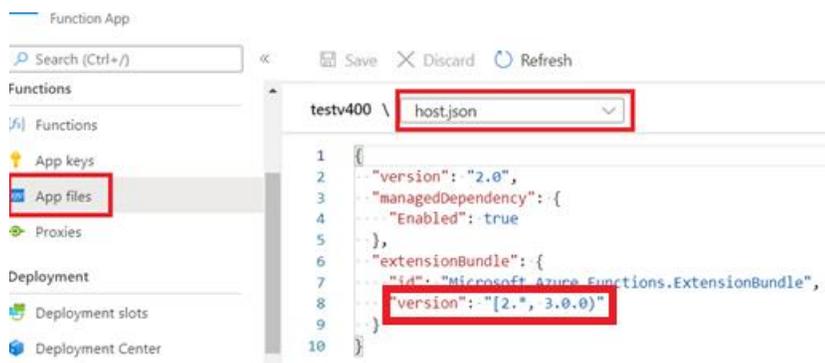
- The below-mentioned services are charged by Microsoft based on usage.
 - Function App
 - Click here [Function-App-price-tier](#) to know more on pricing details.
 - Event Hub
 - Click here [Event-Hub-price-tier](#) to know more on pricing details.

3.4 Verifying Function App

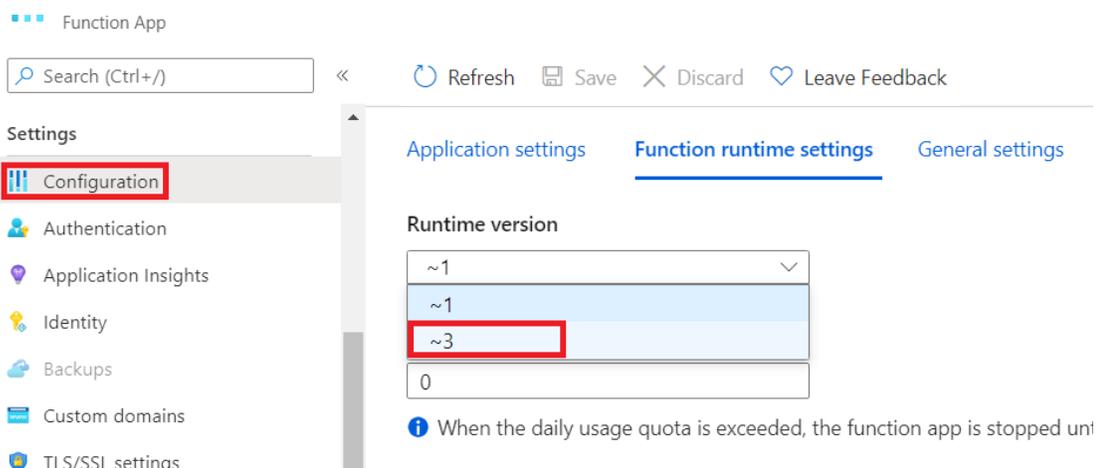
- Once the Function App is deployed, follow the below -mentioned steps to verify the deployment.
 1. Login to <https://portal.azure.com/>
 2. Search for Function App service.
 3. Click on created Function App.
 4. On successful deployment the screen would look as shown below.

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

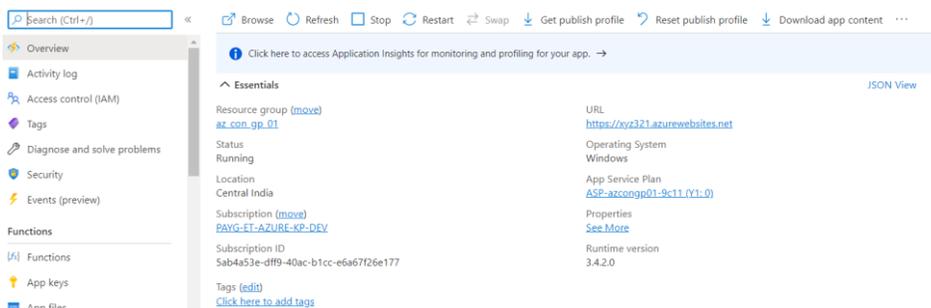
- To check the extension bundle.
 1. Click on **App files** under the Function section in the left pane of the function App home page
 2. Choose **host.json** from the dropdown
 3. Modify the version details in the JSON file to **"version": "[2.*, 3.0.0]"**
 4. Click **Save**.



- 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.



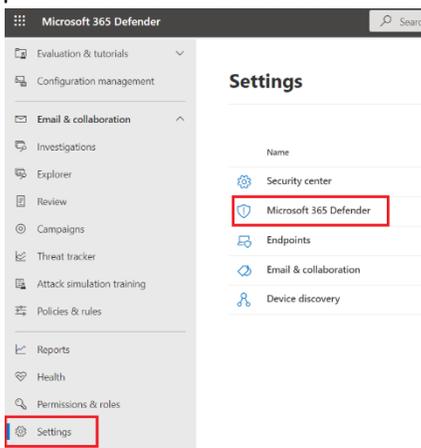
4. Configuring Microsoft Defender to Forward Logs to Event hub

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.

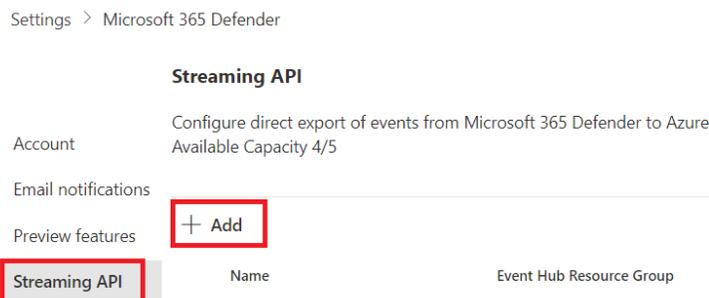
4.1 Configuring Microsoft Defender to stream events to Event Hub

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**.



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

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>