Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Microsoft Intune to Forward Logs to EventTracker

Publication Date:

June 02, 2022

Abstract

This guide provides instructions to retrieve the Microsoft Intune events via the Azure Event Hub and then configure the Azure function app to forward the logs to EventTracker.

Scope

The configuration details in this guide are consistent with Microsoft Intune and EventTracker version 9.3 or later.

Audience

This guide is for the Administrators responsible for configuring the Microsoft Intune to forward logs to EventTracker.

Table of Contents

1 Overview

Microsoft Intune is a cloud-based service that aims to provide unified endpoint management. It focuses on controlling both organization and personally owned mobile devices and mobile applications to protect corporate data. This service also configures specific policies to manage applications.

EventTracker facilitates monitoring events from the Microsoft Intune. Its dashboard and reports interface benefits you to track user activities, configurational changes, and device data to detect compliance, managed, and registered devices in Microsoft Intune. In this way, you will be able to recognize the device's criticality and take the necessary measure.

2 Prerequisite

- An Azure Subscription and a user who is a global administrator.
- Azure Resource group.
- EventTracker Manager details (Manager Hostname, Port, Manager public IP address, and Organization name).

3 Configuring Microsoft Intune with Event Hub and Function App

Microsoft Intune is integrated with EventTracker by streaming the logs to the Azure Event Hub, and then to EventTracker from Azure Event Hub.

3.1 Create an Event Hub and Function App

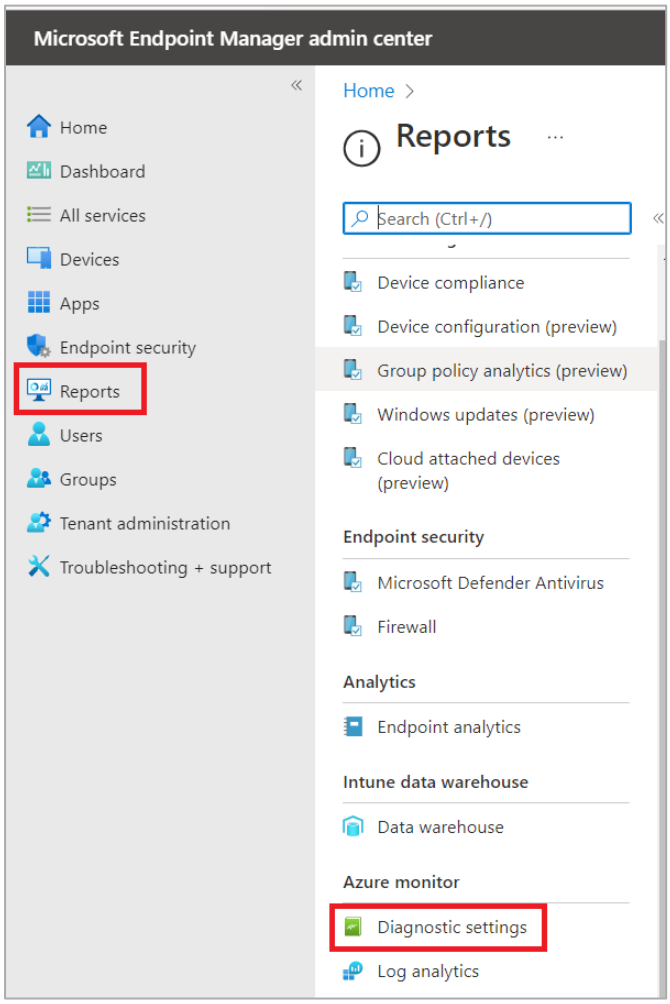
Refer to the configuration of the Azure function app to create an Event Hub and Function App.

3.2 Configuring Microsoft Intune to stream events to Event Hub

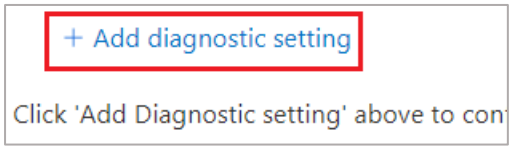
To configure Microsoft Intune to stream events to Event Hub, as an Administrator,

1. Log in to the Microsoft Endpoint Manager admin center and create an Event Hub namespace.

2. In the **Microsoft Endpoint Manager admin center** interface, from the left panel, click **Reports** and then click **Diagnostics settings** under **Azure monitor.**



3. Then, click **Add diagnostic setting** to add the settings.

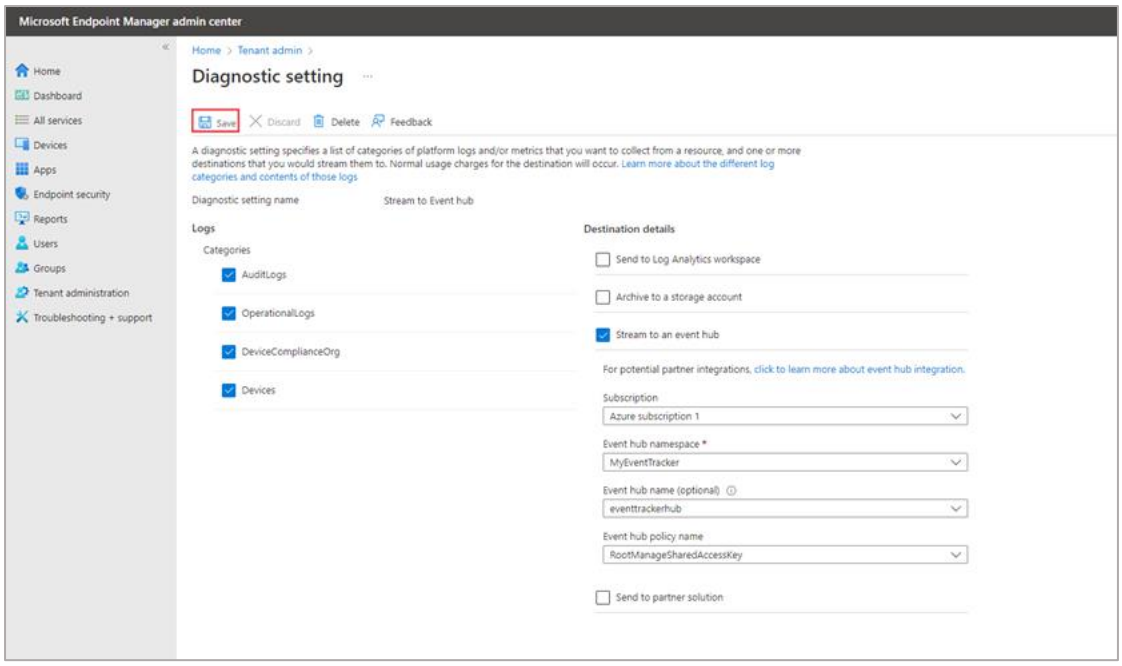


4. In the **Diagnostic setting** interface, specify the following details.

- Provide the **Diagnostics settings name**, such as **EventTracker_App Service**.
- On the left of the interface, in the **Logs** > **Categories** section, select all the listed **Logs** check boxes.
- On the right of the interface, in the **Destination details** section, select **Stream to an event hub** and then choose the following.
  - **Subscription:** Choose the appropriate Azure subscription from the drop-down list.

- **Event Hub namespace:** Choose the Event Hub namespace from the drop-down list.
- **Event Hub name:** Choose the Event Hub created under Event Hub namespace from the drop-down list.
- **Event Hub policy name:** Choose the Event Hub policy from the drop-down list.

5. After providing the necessary details, click **Save** to save the diagnostic setting**.**



About Netsurion

Flexibility and security within the IT environment are two of the most key 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