Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configure Azure Active Directory to forward logs to EventTracker

Publication Date:

August 09, 2022

Abstract

This guide provides instructions to configure and retrieve the Azure Active Directory events via the Azure Event Hub and then forward the logs to EventTracker.

Scope

The configuration details in this guide are consistent with Azure Active Directory and EventTracker version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the Azure Active Directory events using EventTracker.

Table of Contents

1 Overview

Azure Active Directory (Azure AD), an aspect of Microsoft Entra, is an enterprise identity service that offers single sign-on, multifactor authentication, and conditional access to help protect against cybersecurity threats. Azure AD uses strong authentication and risk-based adaptive access policies to help protect access to resources and data.

Netsurion facilitates monitoring events from the Azure Active Directory. The dashboard, categories, alerts, and reports interface in Netsurion's threat protection platform, EventTracker, benefits in tracking azure active directory activities and changes to detect any suspicious activities performed on the Azure Active Directory.

2 Prerequisites

- An Azure AD premium license and a user who is a global administrator.
- An existing or new Azure Resource group.
- EventTracker Manager details (Manager Hostname, Port, Manager public IP address, and Organization name).

3 Configuring Azure Active Directory to forward logs to EventTracker

Integrate Azure Active Directory with EventTracker by streaming the logs to the Azure Event Hub and from Azure Event Hub to EventTracker using function app.

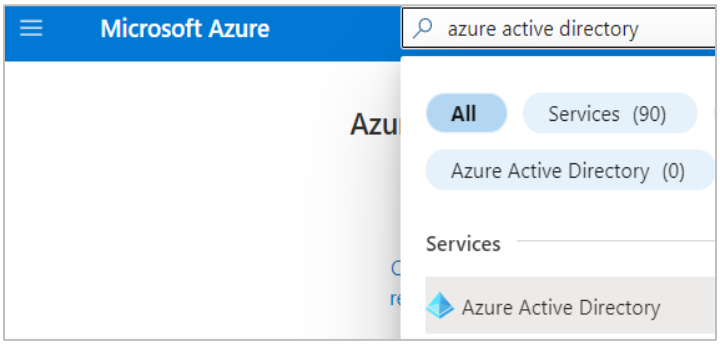
3.1 Create Event Hub and Function App

Refer to the configuration of Azure Active Directory to create the Event Hub and Function App.

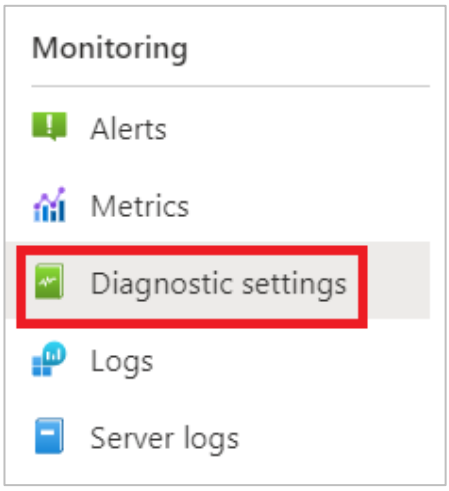
3.2 Configuring Azure Active Directory to stream events to Event Hub

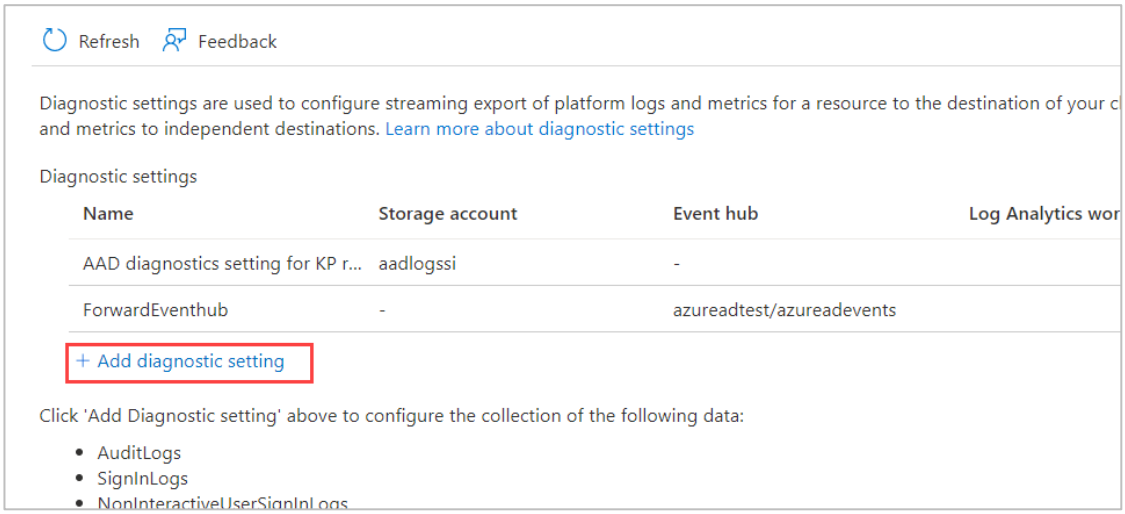
To configure Microsoft Azure Active Directory to stream events to Event Hub, as an Administrator,

1. Log in to Microsoft Azure account and create an event hub namespace.
2. In the **Microsoft Azure** console, click **All** services, then search and click **Azure Active Directory**.



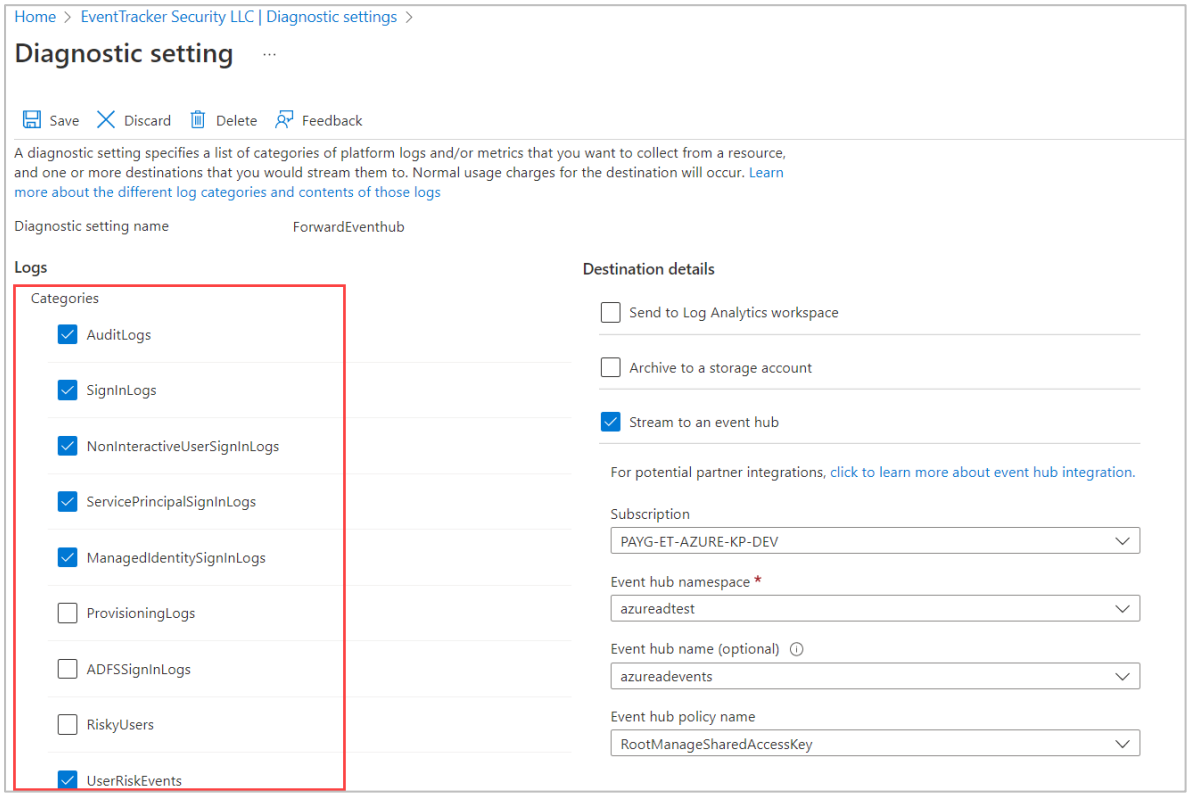
3. From the left panel, go to **Monitoring** > **Diagnostics settings** and click **Add diagnostics setting**.





4. In the **Diagnostic setting** interface, specify the following details.
   - Provide the **Diagnostics settings name**, such as **EventTracker_Active Directory**.

- From the left of the interface, in the **Logs** > **Category groups** section, select the following logs from the **Categories** section.



AuditLogs -Provides the details about the changes applied to your tenant such as users and group management or updates applied to your tenant's resources.

SignInLogs - Provides the details of the sign-ins where a user provides an authentication factor, such as a password, a response through an MFA app, a biometric factor, or a QR code.

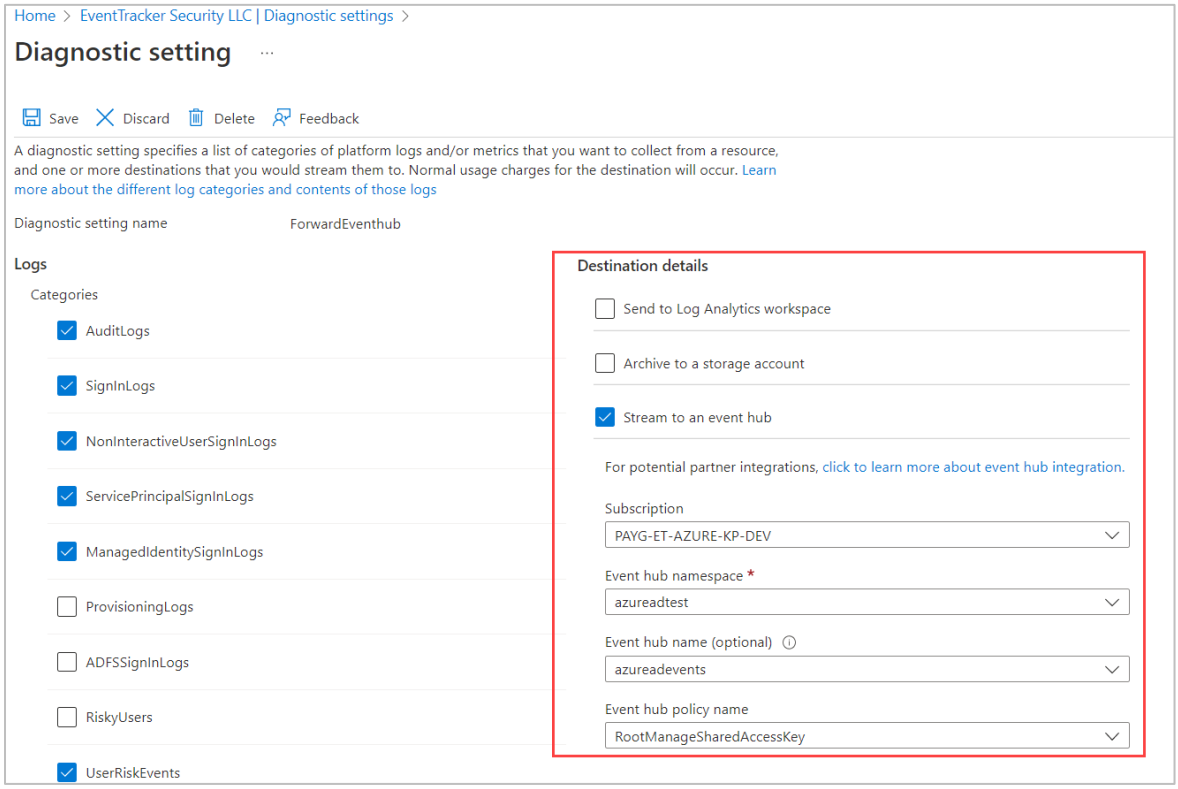
NonInteractiveLogs - Provides the details of the sign-ins performed by a client on behalf of a user. These sign-ins do not require any interaction or authentication factor from the user. For example, authentication and authorization using refresh and access tokens that does not require for a user to provide credentials.

ServicePrincipalSignInLogs - Provides the details of the sign-ins by apps and service principals that do not involve any user. In these sign-ins, the app or service provides a credential automatically to authenticate or access resources.

ManagedIdentitySignInLogs - Provides the details of the sign-ins by Azure resources that have secrets managed by Azure.

UserRiskEvents - Indicates the type of activity associated with the detected risk. Possible values are **signin**, **user**, **unknownFutureValue**.

- From 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 all the details, click **Save.**

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

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