NG SIEM Microsoft Entra ID

Overview

This guide walks you through connecting Microsoft Entra ID to Elastic so that your identity logs flow automatically into Elasticsearch. Once set up, you'll be able to search, visualize, and alert on Sign-in logs, Audit logs, and Identity Protection logs directly in Kibana.

The integration uses Azure Event Hub as the bridge — Entra ID pushes logs into Event Hub, and the Elastic Agent reads from it in real time. A Storage Account is used behind the scenes to checkpoint progress, so Elastic always picks up exactly where it left off.

Prerequisite

Before you begin, ensure the following are in place:

- Active Azure subscription with a Microsoft Entra ID tenant
- An Elastic deployment (Cloud or self-managed 8.x) with Kibana accessible
- Microsoft Entra ID Free or P1 license for Sign-in and Audit logs
- Microsoft Entra ID P2 license if you want Identity Protection logs (UserRiskEvents, RiskyUsers)
- Azure permissions to create Event Hubs and Storage Accounts

Part 1 — Set Up Azure Resources

In this part you will create the Event Hub and Storage Account in Azure. These are the two Azure-side components that Elastic connects to.

Step 1.1 Create an Event Hub Namespace and Hub

The Event Hub is the channel that Entra ID will push logs into.

- In the Azure Portal (portal.azure.com), search for Event Hubs in the top search bar and click Create.
- Choose your Subscription and Resource Group (or create a new one).
- Set a Namespace Name — for example: entra-elastic-hub. This is the parent container.
- Choose a Region close to your Elastic deployment and set Pricing tier to Standard or above.
- Click Review + Create, then Create. Wait for the deployment to complete.
- Once deployed, open the namespace and click + Event Hub in the top toolbar.
- Name the hub — for example: entra-logs — and click Create.

Step 1.2 Create a Consumer Group

A consumer group is a named reader slot on the Event Hub. Elastic needs its own so it does not conflict with any other tools reading from the same hub.

- Inside your Event Hub (entra-logs), click Consumer Groups in the left sidebar.
- Click + Consumer Group.
- Name it elastic-consumer and click Save.
- Write this name down — you will paste it into Elastic in Part 3.

Step 1.3 Copy the Connection String

The connection string is how Elastic authenticates to your Event Hub Namespace.

- Navigate back to the Event Hub Namespace (the parent, not the individual hub).
- In the left sidebar, click Shared Access Policies.
- Click RootManageSharedAccessKey.
- Copy the Connection string–primary key. It starts with Endpoint=sb://

Step 1.4 Create a Storage Account

Elastic uses a Storage Account to checkpoint which events it has already read. This prevents duplicate ingestion if the agent restarts.

- In the Azure Portal, search for Storage Accounts and click Create.
- Choose the same Subscription and Resource Group as your Event Hub.
- Enter a Storage Account Name — for example: entraelascheckpoint. Names must be lowercase, 3–24 characters, no hyphens.
- Choose the same Region as your Event Hub and leave all other defaults.
- Click Review + Create, then Create.
- Once deployed, open the storage account and click Access Keys in the left sidebar.
- Click Show next to key1 and copy both the Storage account name and the Key value.

> **Keep your Storage Account Key secure. Anyone with this key has full access to the storage account. You can rotate it later from the Access Keys page without breaking the integration — just update the key in Elastic too.**

Part 2 — Configure Entra ID Diagnostic Settings

Now you will tell Entra ID which log categories to send and point them at the Event Hub you just created.

- In the Azure Portal, go to Microsoft Entra ID from the left sidebar or top search.
- Under Monitoring in the left sidebar, click Diagnostic settings.
- Click + Add diagnostic setting at the top.
- Give it a descriptive name such as: Stream to Elastic via Event Hub.

- Under Logs, check the categories you want to stream:

SignInLogs	Free	All interactive user sign-ins, MFA results, Conditional Access outcomes
AuditLogs	Free	Directory changes — user creation, group changes, role assignments
NonInteractiveUserSignInLogs	Free	Service and application sign-ins without user interaction
UserRiskEvents	P2 only	Identity Protection risky sign-in detections
RiskyUsers	P2 only	Users flagged as at-risk by Identity Protection

- Under Destination details, check Stream to an event hub.
- Set Event Hub Namespace to your namespace (entra-elastic-hub).
- Set Event Hub name to your hub (entra-logs).
- Leave Event Hub policy name as the default (RootManageSharedAccessKey).
- Click Save at the top of the page.

> **Changes to Diagnostic Settings take effect immediately, but it can take 5–15 minutes before the first events begin appearing in the Event Hub — and then another minute or two before Elastic picks them up. This is normal.**

Elastic Fleet Configuration

With Azure fully configured, the final step is to install the Microsoft Entra ID integration in Kibana and enter the four connection details you collected.

> To enable log collection from the Microsoft Entra ID, provide the following information to **CyTech Support**:

- Consumer Group
- Connection String
- Storage Account
- Storage Account Key

Conclusion

With the integration configured, Microsoft Entra ID logs are now streaming continuously into Elasticsearch via Azure Event Hub. Sign-in, Audit, and Identity Protection events will be indexed automatically and available for search, visualization, and alerting in Kibana.

To maintain the integration, ensure the Elastic Agent remains healthy in Fleet and rotate the Storage Account Key and Event Hub connection string in both Azure and the Elastic integration settings as part of your regular credential rotation cycle.

Revision #2
Created 5 March 2026 07:23:05
Updated 10 March 2026 07:45:40