NG SIEM - Microsoft Entra ID Entity Analytics

Overview

This guide provides step-by-step instructions for integrating Microsoft Entra ID (formerly Azure Active Directory) Entity Analytics with the Elastic Security platform. By completing this integration, your security team will be able to ingest identity-based risk signals from Entra ID directly into Elastic, enabling enriched detection, investigation, and response workflows.

Entity Analytics in Elastic Security correlates user and host risk scores derived from your identity provider with security events, helping analysts prioritize high-risk entities and reduce alert fatigue.

Prerequisite

Before beginning the integration, ensure the following requirements are met:

Microsoft Entra ID Requirements

- An active Microsoft Azure subscription with Entra ID (Azure AD) configured
- Global Administrator or Privileged Role Administrator permissions in Entra ID
- Microsoft Graph API access enabled for your tenant
- Entra ID Identity Protection license (P2) for risk signal data

Azure App Registration

Elastic connects to Entra ID via the Microsoft Graph API using an Azure App Registration with appropriate permissions. Follow these steps to configure the application.

Register a New Application

- Sign in to the Azure Portal at portal.azure.com with administrative credentials.
- Navigate to Microsoft Entra ID > App registrations.
- Click New registration.
- Provide the following details:

Field	Value
Name	Elastic-EntraID-EntityAnalytics

Field	Value
Supported account types	Accounts in this organizational directory only (Single tenant)
Redirect URI	Leave blank (not required for this integration)

- Click Register.

> Note down the Application (client) ID and Directory (tenant) ID — these will be needed when configuring the Elastic integration.

Create a Client Secret

- In your new App Registration, navigate to Certificates & secrets > Client secrets.
- Click New client secret.
- Set a description (e.g., "Elastic Entity Analytics") and choose an expiry period.
- Click Add, then immediately copy the Value. This is shown only once.

Grant API Permissions

The application requires the following Microsoft Graph API permissions:

User.Read.All	Application	Read all user profiles
IdentityRiskEvent.Read.All	Application	Read identity risk events
IdentityRiskyUser.Read.All	Application	Read risky user data
AuditLog.Read.All	Application	Read audit log data
Directory.Read.All	Application	Read directory data

- In the App Registration, go to API permissions > Add a permission.
- Select Microsoft Graph > Application permissions.
- Search for and add each permission listed in the table above.
- Click Grant admin consent for [Your Organization] and confirm.

> **Note**: **Admin consent must be granted by a Global Administrator. If you do not have this role, coordinate with your Azure administrator**

Elastic Fleet Configuration

With the Azure application registered, the next step is to configure Elastic Fleet to deploy the Microsoft Entra ID Entity Analytics integration.

>

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

Tenant ID	Directory (Tenant) ID from App Registration
Client ID	Application (Client) ID from App Registration
Client Secret	Secret value created in Section 3.2
Dataset	azure.entityanalytics (auto-populated)
Sync Interval	Recommended: every 30 minutes (default)
Enable User Sync	Toggle ON
Enable Risk Sync	Toggle ON (requires P2 license)

Conclusion

Integrating Microsoft Entra ID Entity Analytics with Elastic Security gives your team a significant advantage in identifying and responding to identity-based threats. By pulling user risk signals directly from Entra ID into Elastic, you gain a unified view of your security posture without having to switch between platforms.

Once the Elastic Agent is configured with the App Registration credentials, it handles everything automatically — authenticating to Microsoft Graph API, syncing user and risk data on your set interval, and feeding that data into Elastic's Entity Analytics engine. From there, detection rules can alert your team on risky sign-ins, elevated risk levels, and behavioral anomalies in real time.

For Elastic Cloud deployments specifically, the integration works out of the box with no additional network configuration needed. The main things to keep on top of after go-live are tuning your detection rules to fit your environment and rotating the Azure App Registration client secret before it expires to avoid any interruption in data collection.

Revision #2
Created 5 March 2026 07:23:46
Updated 11 March 2026 06:21:19