NG SIEM Microsoft Exchange Online Message Trace

Overview

Microsoft Exchange Online Message Trace is a powerful diagnostic and security feature within Microsoft 365 that tracks the flow of email messages through your Exchange Online organization. Integrating Message Trace data into Elastic provides security operations teams with centralized visibility into email traffic, anomaly detection, and compliance monitoring.

This guide covers the end-to-end process of collecting, ingesting, parsing, and analyzing Exchange Online Message Trace data within the Elastic Stack, including configuration of the Microsoft 365 integration via Elastic Agent, index templates, field mappings, dashboards, and alerting

Prerequisite

Before configuring the integration, ensure the following prerequisites are met:

Microsoft 365 Requirements

- An active Microsoft 365 or Office 365 subscription (Business Premium, E3, or E5 recommended)
- An Azure Active Directory (Azure AD) tenant with Global Administrator or Security Administrator privileges
- An Azure AD App Registration with appropriate API permissions
- Exchange Online Plan 1 or Plan 2 license for the service account used

Azure App Registration

The Microsoft 365 integration authenticates using OAuth2 client credentials. You must create an App Registration in Azure AD and grant it the correct API permissions.

Creating the App Registration

- Sign in to the Azure portal at portal.azure.com with Global Administrator credentials.
- Navigate to Azure Active Directory > App registrations > New registration.
- Provide a descriptive name such as Elastic-M365-MessageTrace.

- Set the Supported account type to Accounts in this organizational directory only (Single tenant).
- Leave the Redirect URI blank and click Register.
- Note the Application (client) ID and Directory (tenant) ID from the Overview page.

Configuring API Permissions

Navigate to API permissions > Add a permission > Office 365 Management APIs and add the following application permissions:

API	Permission	Type
Office 365 Management APIs	ActivityFeed.Read	Application
Office 365 Management APIs	ActivityFeed.ReadDlp	Application
Microsoft Graph	Reports.Read.All	Application

After adding permissions, click Grant admin consent for [your tenant] to activate them. The status column should show a green checkmark.

Creating a Client Secret

- Navigate to Certificates & secrets > Client secrets > New client secret.
- Set a meaningful description (e.g., Elastic Agent Secret) and an expiry period of 24 months.
- Click Add and immediately copy the secret Value. This value is only shown once.
- Store the secret securely in a secrets management system such as HashiCorp Vault or Elastic Keystore.

Elastic Fleet Configuration

With the Azure application registered, the next step is to configure Elastic Fleet to deploy the Microsoft Exchange Online Message Trace integration.

Collect Microsoft Exchange Online Message Trace logs from Graph API

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

- **Collect Microsoft Exchange Online Message Trace logs from Graph API**
  - **Tenant ID**
  - **Client ID**
  - **Client Secret**

- **Collect Microsoft Exchange Online Message Trace logs via file**

- **Local Domains**
- **Paths**

Conclusion

Integrating Microsoft Exchange Online Message Trace into Elastic is straightforward when using the Graph API collection method. The client is only required to complete the Azure AD App Registration, grant the necessary API permissions, and securely share three credentials — Tenant ID, Client ID, and Client Secret — with the Elastic team.

Once those credentials are entered into the Microsoft 365 integration in Kibana, Elastic Cloud handles the rest. Data will begin flowing into the platform within 5 to 30 minutes, and the built-in dashboards provide immediate visibility into email traffic, delivery status, and suspicious activity.

No backend configuration, file paths, or command-line access is required for this setup. The alternative file-based collection method available in the Elastic UI is not applicable here, as logs are pulled directly from Microsoft's Graph API.

The only ongoing maintenance required is coordinating with the client to renew the Client Secret before it expires, typically every 24 months.

Revision #1
Created 5 March 2026 07:24:13
Updated 12 March 2026 03:39:29