Microsoft 365 / Azure Email Integration

This guide explains how to connect your Microsoft 365 Outlook email to the Enginy platform. Our integration uses the industry-standard **OAuth 2.0 authentication protocol** to ensure secure access without storing your password.

For Users: What to do if you see "Approval Required"

If you attempt to connect and see a screen stating "Approval required," follow these immediate steps:

1. Enter a brief justification in the text box (e.g., "Required for CRM integration").
2. Click the **Request approval** button.
3. This will send a notification to your administrator so they can review the request

---

For IT Administrators: How to Grant Permissions

To allow users to connect their email accounts, an Azure Administrator must adjust the tenant configuration. Please choose one of the following solutions in the **Microsoft Entra Admin Center** (formerly Azure AD).

Solution A: Grant Tenant-Wide Admin Consent (Recommended)

This method explicitly authorizes the application for your organization.

1. Navigate to the **Microsoft Entra Admin Center** > **Enterprise applications**.
2. Search for and select the **Enginy AI** application.

3. In the left menu, select **API permissions**.
4. If you see warnings such as "Admin consent required," click the button labeled **Grant admin consent for [Organization Name]**.

Solution B: Modify User Consent Settings

If you prefer to allow users to authorize apps themselves:

1. Navigate to **Microsoft Entra Admin Center** > **Applications** > **Enterprise applications** > **Consent and permissions** > **User consent settings**.
2. Ensure that **"Allow user consent for apps from verified publishers"** is selected.

◦ *Note: Genesy AI is a verified publisher*

Troubleshooting: Connection Still Failing?

If the integration fails despite granting consent, check for **Conditional Access Policies** that may be blocking third-party apps.

1. Go to **Microsoft Entra Admin Center** > **Protection** > **Conditional Access** > **Policies**.
2. Check for policies affecting "All cloud apps".
3. Look for blocks related to **legacy authentication**, **non-compliant devices**, or **untrusted locations**.
4. **Action:** Exclude the application from restrictive policies or create an exception

---

Alternative Solution: Connect via Admin Browser

Note: This solution is a workaround if permission propagation is delayed.

If the standard procedure above does not resolve the issue, the Azure Administrator should attempt to connect the email integration directly through the Enginy platform:

1. The **Azure Administrator** opens the browser where they are **already logged in** with their Azure Admin permissions.
2. Log in to the **Enginy platform** on that same browser (using a member account).
3. Navigate to the email integration settings and attempt to connect the email account.
4. Because the browser session already holds valid Azure Admin credentials, this action often bypasses user-level restrictions and forces the initial connection.

Reference: Required Permissions (Scopes)

For your security review, our integration requests the following specific permissions:

- `https://graph.microsoft.com/SMTP.Send`
- `https://graph.microsoft.com/Mail.Send`
- `https://graph.microsoft.com/Mail.ReadWrite`
- `https://graph.microsoft.com/Mail.ReadBasic`
- `https://graph.microsoft.com/Mail.Read`
- `https://graph.microsoft.com/User.Read`
- `offline_access`

References

- Configure how users consent to applications - Microsoft Learn
- Grant tenant-wide admin consent - Microsoft Learn
- Conditional Access: Targeting Resources - Microsoft Learn
- Overview of permissions and consent - Microsoft Learn