

Configure Email Sending using Microsoft Entra ID

Gathid can be configured to send emails via your Microsoft 365 Platform. Users of the Gathid system will then receive email notifications from an internal company email address.

This guide outlines the standard process of configuring Entra ID to act as an Identity Provider for Single Sign-On for your Gathid instance.

Overview

This feature is currently only available only for Microsoft 365 and requires a Microsoft App Registration. You can use an existing App Registration that has already been configured for SSO and/or the MS Entra ID system connector.

Gathid recommends creating a dedicated App Registration for email sending. Alternatively, follow step one below to create a new App Registration.

Summary

1. [Create a new App Registration in MS Entra ID \(if required\)](#)
 2. [Configure API Permissions in the App Registration](#)
 3. [Obtain credentials from the App Registration](#)
 4. [Set up a sending Email Account](#)
 5. [Provide the credentials to your Gathid representative](#)
-
-

Steps to configure a Mailbox for Gathid

1. Create a new App Registration in MS Entra ID (if required)

1. Sign in to the Microsoft Azure Portal and navigate to the App Registration service.
2. Create a **New registration** and enter a name for this application. eg, Gathid Email


3. Click the **Register** button.

2. Configure API Permissions in the App Registration

1. Navigate to the App Registration that has been created for Gathid.
2. From the left-hand side menu, under **Manage**, click on **API permissions**.
3. **Add a permission** and choose **Microsoft Graph** from the pop-up box. Select **Delegate permission**.
4. Search for **Mail.Send**, select it in the Permissions section. Click on **Add permission**.

Request API permissions ×

[← All APIs](#)


 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions expand all

 The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#) ×

Permission	Admin consent required
▼ Mail (1)	
<input checked="" type="checkbox"/> Mail.Send ⓘ Send mail as a user	No
<input type="checkbox"/> Mail.Send.Shared ⓘ Send mail on behalf of others	No

[Add permissions](#) [Discard](#)

5. Note, your organization may require admin consent for this permission. If so, click on the **Grant admin consent for ...** option

3. Obtain credentials from the App Registration

1. In the **Overview** section of your App Registration find and note down the IDs for:
Application (client) ID
Directory (tenant) ID
These will need to be provided to your Gathid representative.
2. Under **Manage** on the left-hand menu, click on **Certificates & secrets**. Ensure you are on the **Client secrets** tab and create a **New client secret**.

3. Enter a **Description** e.g., Gathid email and select an **Expires** time period. (We suggest 2 years for easier management.) Click **Add**.
4. Copy and securely store this client secret value as it will not be visible again. It will need to be provided to your Gathid representative.

4. Set up a sending Email Account

1. You will need to have a **Microsoft 365 email address** (e.g., gathid@yourdomain.com) for the application to send emails. We recommend using a Shared Mailbox so that your in-house administrator can monitor any responses.

5. Provide the credentials to your Gathid representative

1. Provide the credentials obtained in step 3 to your Gathid representative.
Note: If required, Gathid can provide a PowerShell script that will obtain this information automatically.
 - ✓ **Application (client) ID**
 - ✓ **Directory (tenant) ID**
 - ✓ **Client Secret Value**