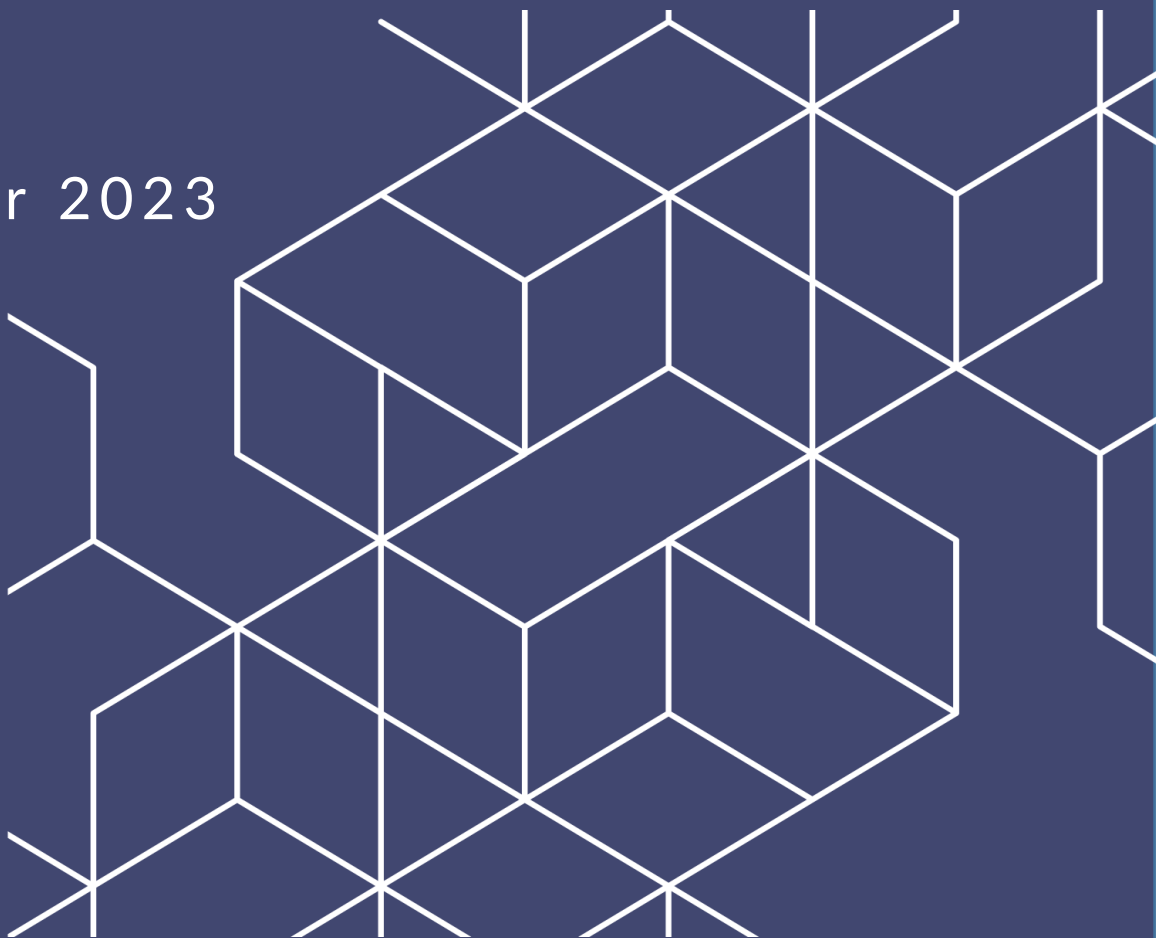
eCASE

OPEXUS

Office 365 OAuth Configuration

v11.2.0

December 2023



eCASE 11.2.0 Office 365 OAuth Configuration

Notice of Rights

Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (AINS, LLC.) on an “As Is” basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

Notice of Trademarks

The publisher’s company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: AINS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

Non-Disclosure Statement

This document’s contents are confidential and proprietary to AINS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from AINS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of AINS, LLC.

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.

Contents

1 About Office 365 OAuth Configuration

1.1 In This Manual

This manual contains steps to configure eCASE to integrate with OAuth for sending emails from a system account. The steps to complete this configuration take place in three parts:

- Register Application: Register your application through the Azure Portal.
- Create Client Secret: Using the Azure Portal, create a Client Secret you will use for OAuth configuration.
- API Permissions: Add appropriate API permissions to permit sending emails.

1.2 Prerequisites

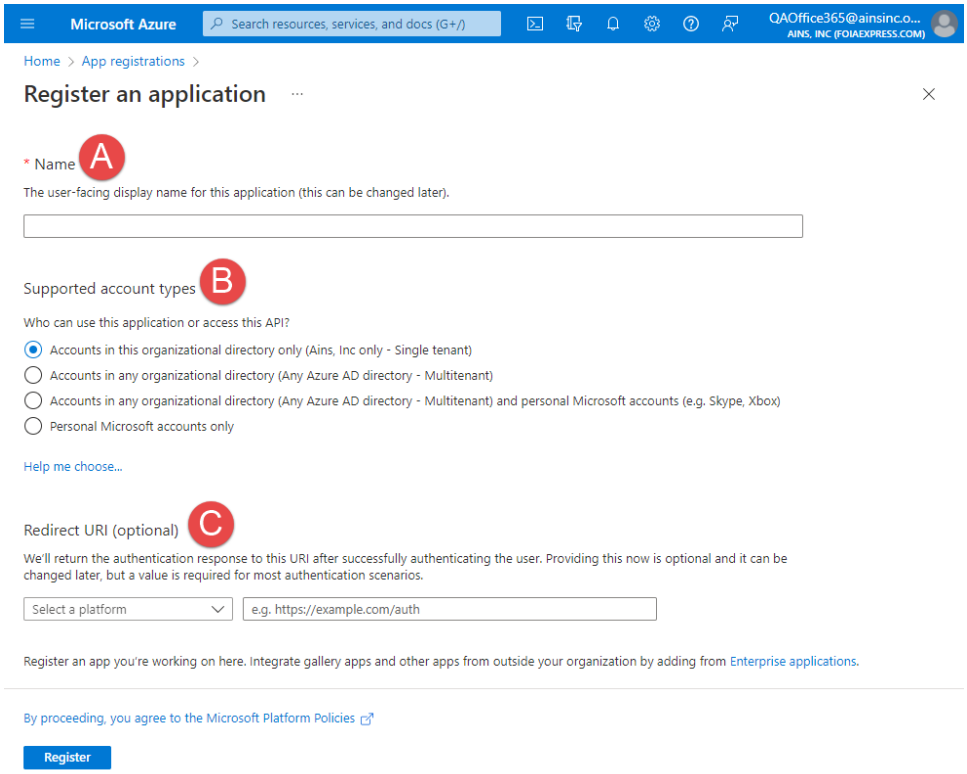
The following are prerequisites for completing OAuth configuration:

- OAuth configuration should be completed by a system administrator with the appropriate knowledge and access to complete all required steps.
- Before beginning the configuration, you must create an Exchange mailbox in Office 365 (ex. noreply@opexustech.com). This email appears as the sender for all system messages from eCASE and is used to complete the configuration.

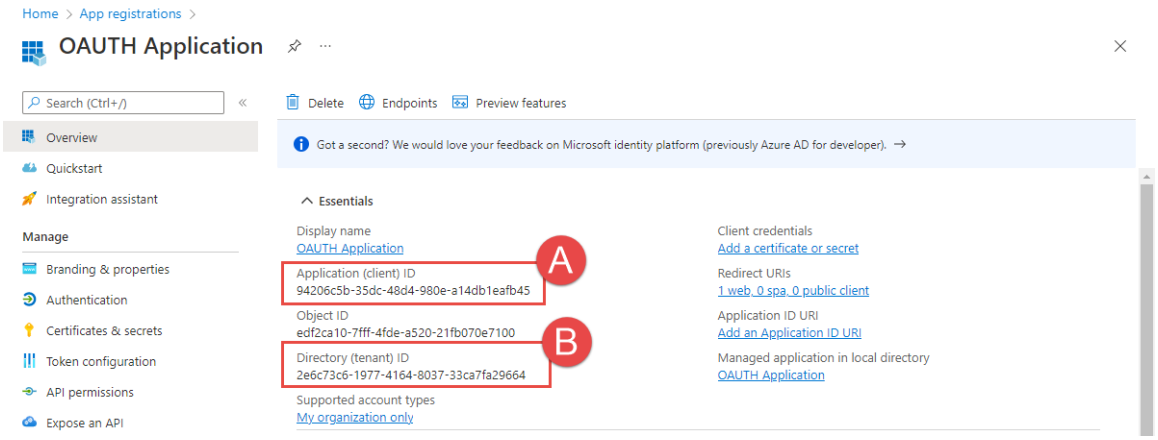
2 Register Application

The first step in OAuth configuration is to register your app. Follow the steps below to register the app in Azure:

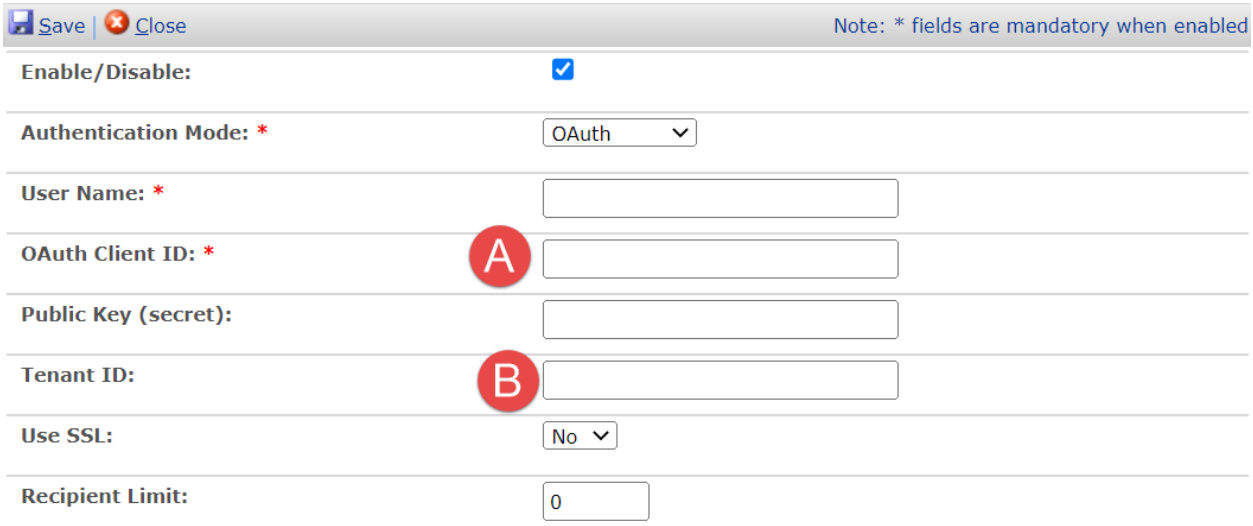
1. Log in to portal.azure.com using the Exchange mailbox created as the eCASE system account.
2. Click **App Registrations > New Registration**. The *Register an application* screen appears:



3. Enter a **(A) Name** for the app in the field provided.
4. Under **(B) Supported account types**, the top option is selected by default. You may need to make a different selection depending on your organization's needs.
5. Under **(C) Redirect URL**, enter "<Application Admin URL>/connectors/SMTP.aspx" where <Application URL> is replaced with your application's admin URL.
6. Click **Register** to register the app.
7. The app is registered. The screen displays the **(A) Application (client) ID and (B) Directory (tenant) ID.** Copy both to your clipboard or otherwise save for later reference:



8. Access eCASE Administration (**eCASE > Settings > Connectors > eMail (SMTP)**). The configuration screen appears as shown below:

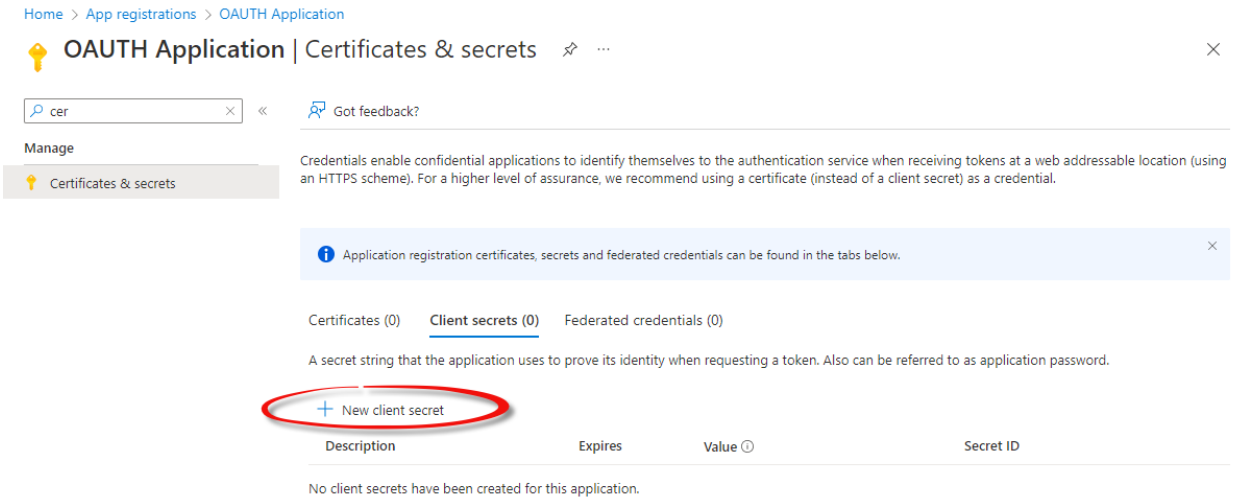


9. Under **(A) OAuth Client ID,** enter the **Application (client) ID** from step 7.
10. Under **(B) Tenant ID**, enter the **Directory (tenant) ID** from step 7.
11. In the *User Name* field, enter the email address being used as the system account for this configuration (ex. noreply@ains.com).
12. Click **Save** to save the changes.

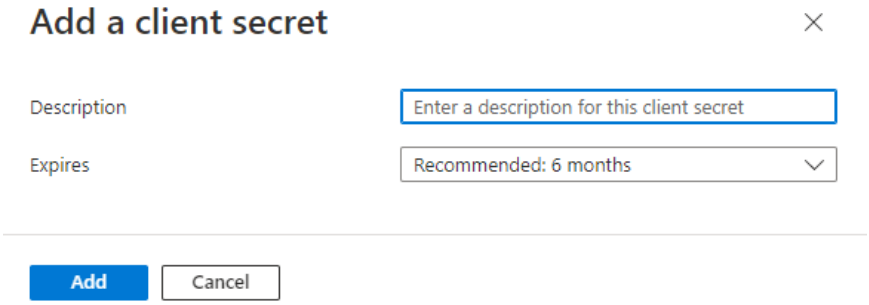
3 Create Client Secret

Next, you'll follow the steps below to create a new Client Secret:

1. Within the Azure Portal, access your application, then access the *Certificates & Secrets* screen.
2. Click **New Client Secret**:



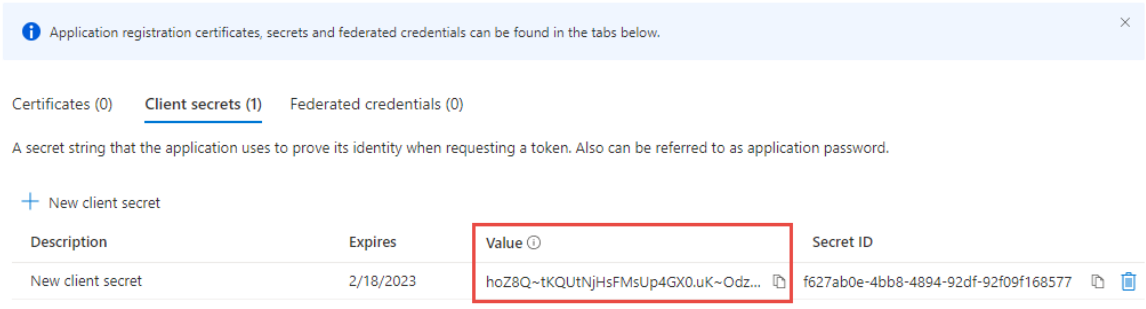
3. The *Add a client secret* screen appears. First enter a *Description* in the field provided. This is an internal description that is visible only to Admin users:



4. Use the *Expires* field to determine an expiration date based on your organization's preference (with a 24-month maximum).

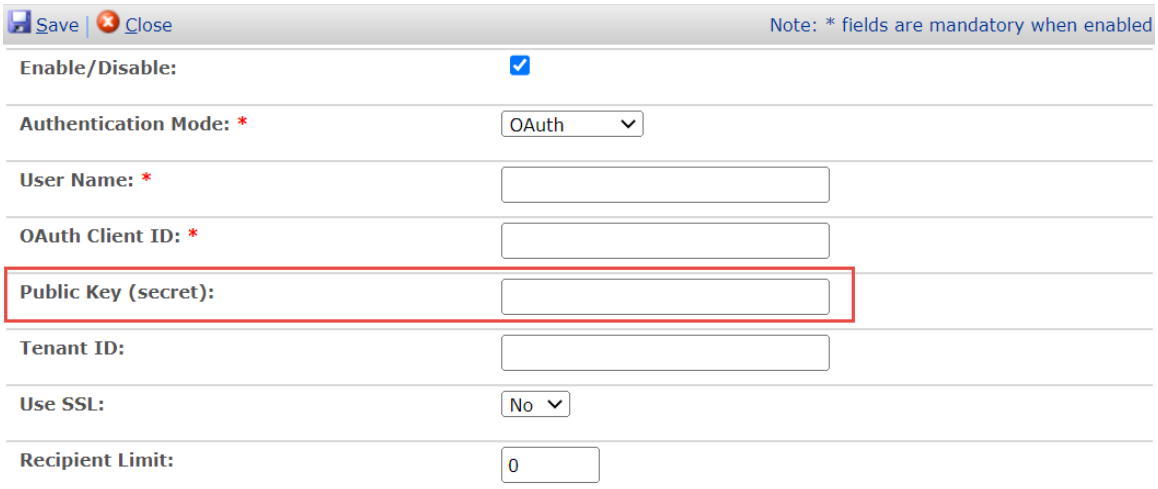
(!!) Note: Take a note of this expiration date, as this Client Secret will need to be renewed prior to the expiration for continuous operation.

5. Click **Add** to generate the Client Secret.
6. The Client Secret is successfully generated, and the secret appears as shown in the example below:



(!!) Note: Save the "Value" as this cannot be retrieved. You will need this to complete the configuration.

7. Copy the *Value* field to your clipboard.
8. Access eCASE Administration (**eCASE > Settings > Connectors > eMail (SMTP)**).
9. Copy the value obtained in step 7 into the Public Key (secret) field:

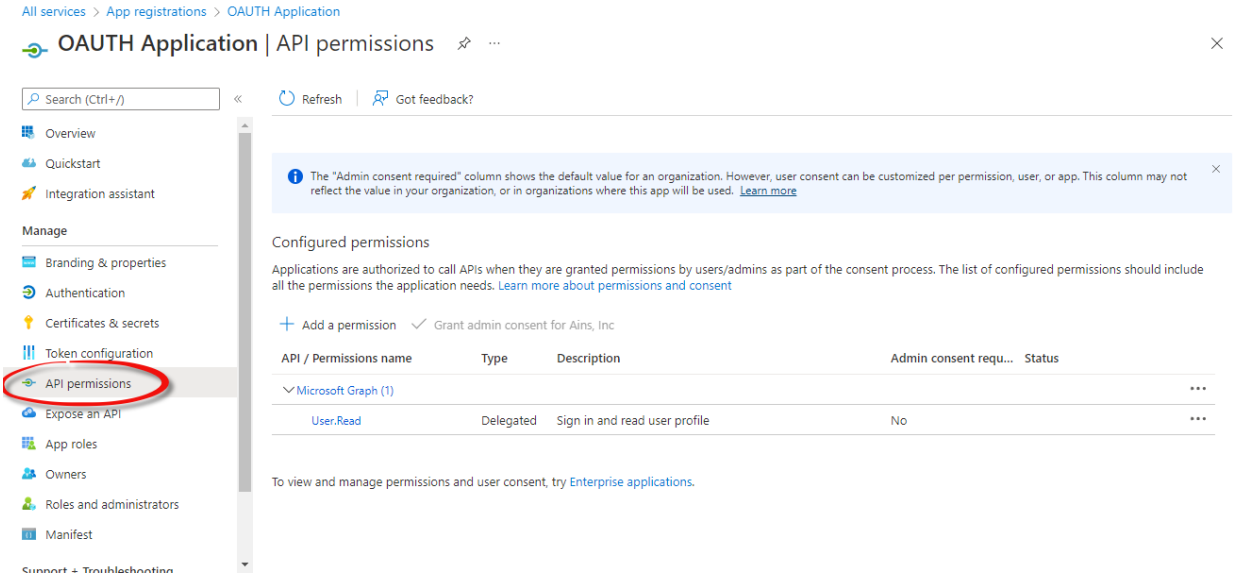


10. Click **Save** to save the changes.

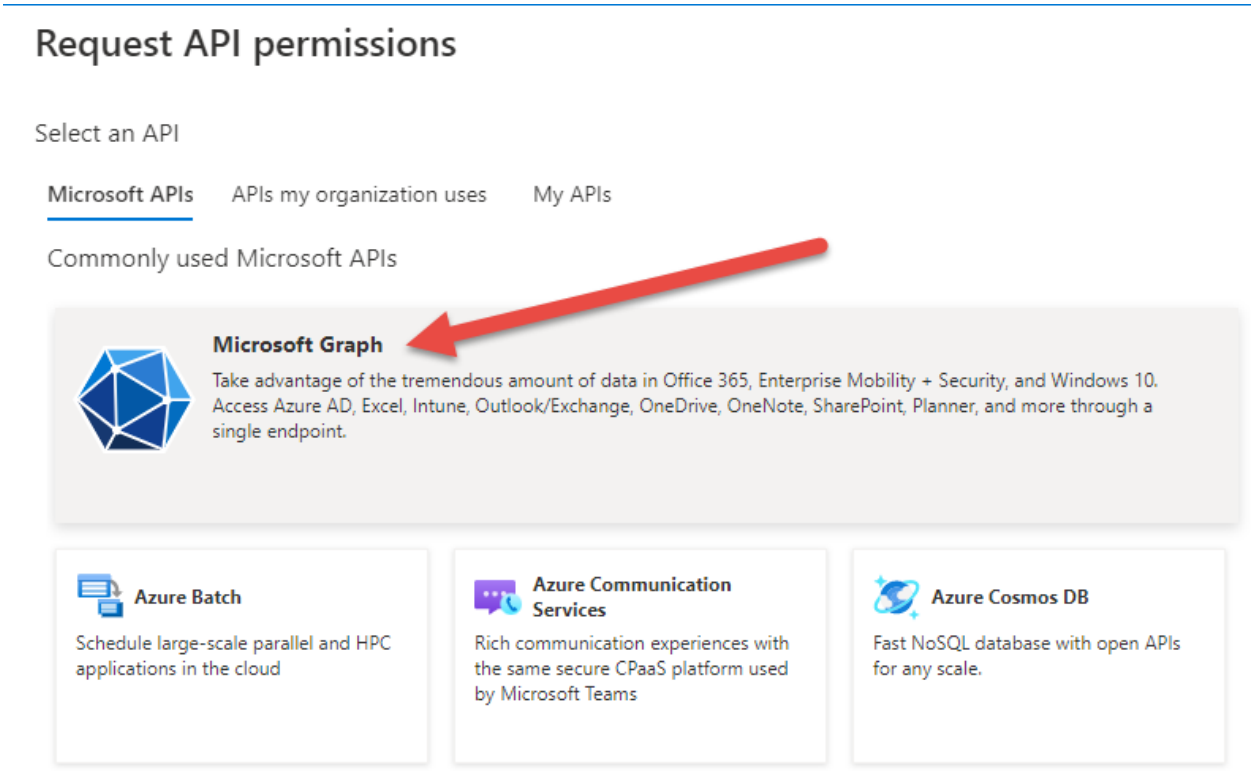
4 API Permissions

The final step to enable OAuth is configuring API permissions:

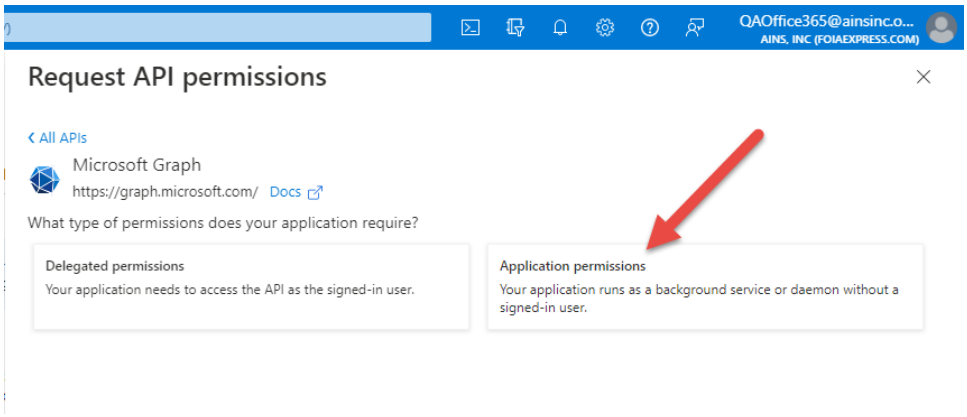
1. Open the Azure Portal and access your application page, then click **API permissions**:



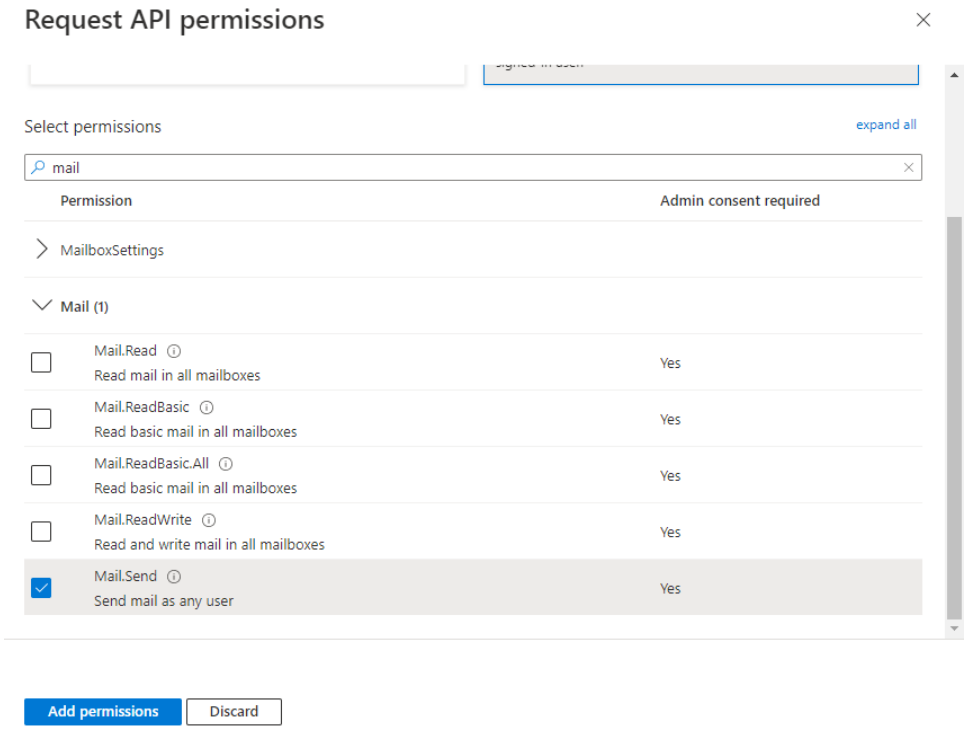
2. From the API Permissions screen click **Add a Permission**.
3. The *Request API Permissions* screen appears. Click **Microsoft Graph**:



4. Next click **Application Permissions**.



5. In the Select Permissions field, type “mail”.
6. Locate and expand the Mail permissions, then select **Mail.Send**:



7. Click **Add Permissions** to apply the selected permission.
8. The Administrator must grant these permissions. The Admin receives a notification to grant the requested permission and, once this permission is granted, the mailbox can send mail from the system account.