

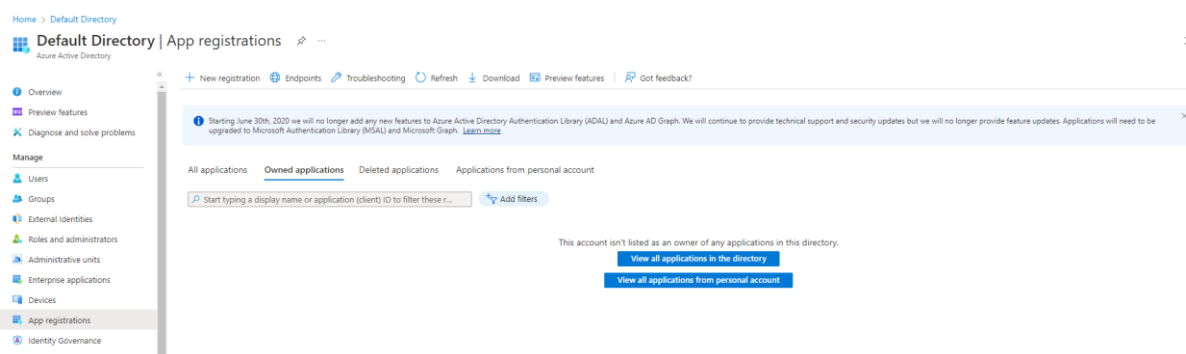
Konfiguracja Microsoft OAuth w Wizlink®

Aby skorzystać z mechanizmów logowania Microsoft OAuth w Wizlink należy zrealizować trzy kolejne kroki:

1. Utworzenie aplikacji wewnętrznej (single tenant) w „Azure Active Directory”.
2. Nadanie uprawnień w panelu administracyjnym.
3. Podanie Application ID oraz Tenant ID w aktywności do obsługi wiadomości email.

1. Utworzenie aplikacji w AAD.

Po zalogowaniu się do <https://portal.azure.com/#home> na konto znajdujące się w tej samej organizacji posiadającej konto mailowe, z którego będzie korzystał robot, należy wybrać opcję „Azure Active Directory” w menu. Następnie trzeba przejść do opcji „App Registrations”, dzięki czemu zostanie wyświetlony następujący ekran:



Z tego ekranu należy wybrać opcję „New Registration”.

Na następnej stronie trzeba podać nazwę aplikacji, a pozostałe opcje zostawić domyślne (w szczególności opcję definiującą, kto będzie z niej korzystać).

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Default Directory only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

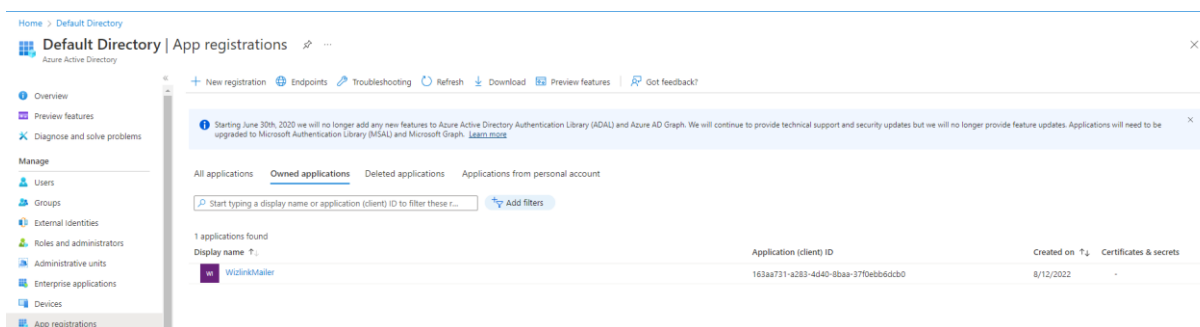
[Help me choose...](#)

Redirect URI (optional)

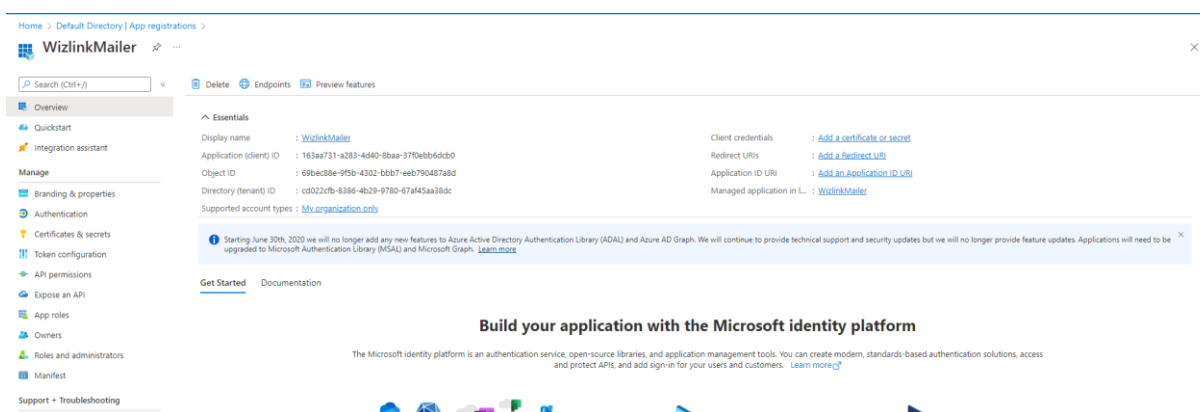
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Następnie należy nacisnąć przycisk register.

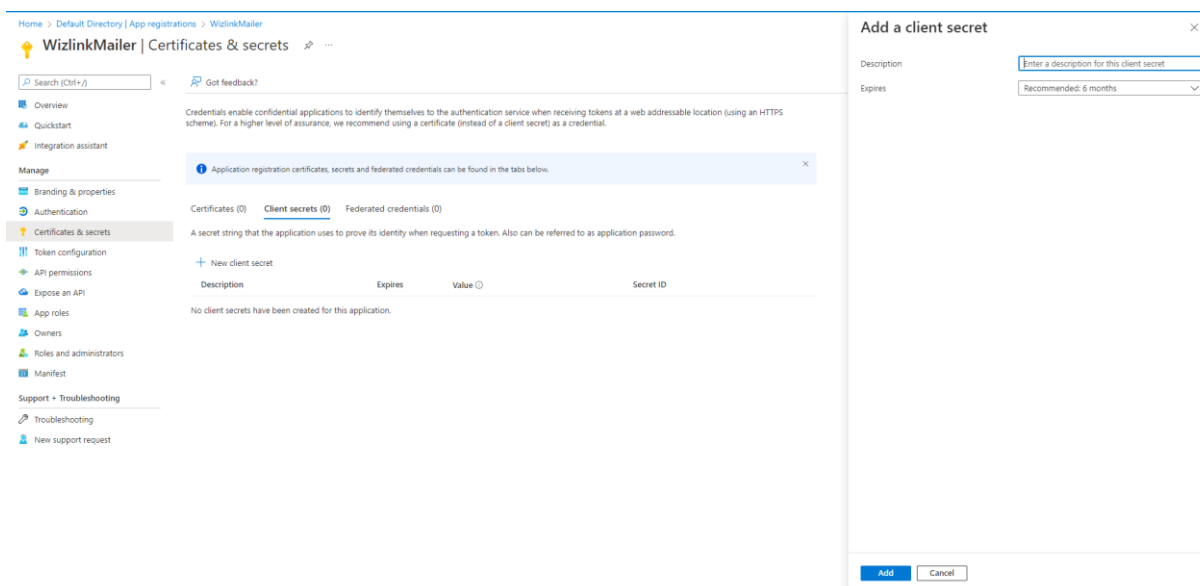
Jeżeli portal powróci na stronę główną, trzeba ponownie przejść do strony rejestracji aplikacji - a więc znowu wybrać opcję „Azure Active Directory” i po niej „App Registrations”. Tym razem powinna się tam znajdować nowa aplikacja utworzona w poprzednim kroku:



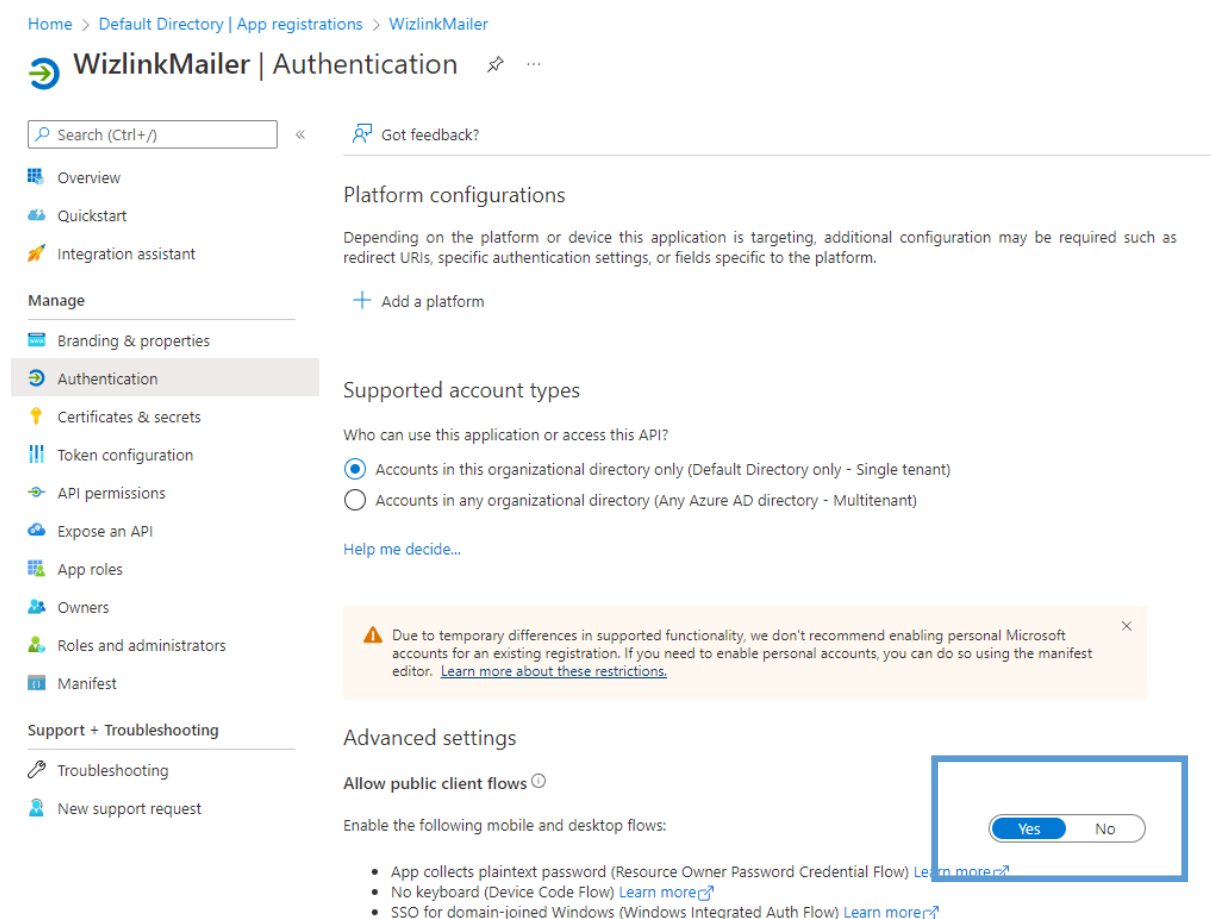
Klikając na jej nazwę następuje przeniesienie do zarządzania aplikacją:



Tu należy skonfigurować kilka elementów. Po pierwsze w zakładce „Certificates & secrets” trzeba utworzyć token, którym aplikacja będzie się uwierzytelniać z resztą Active Directory.



Po naciśnięciu przycisku „New client secret”, po prawej stronie pojawi się okno. Formularz w tym oknie należy wypełnić, podając opis i czas, przez który ww. token będzie ważny. Po upływie wybranego czasu, ten krok będzie trzeba powtórzyć. Po uzupełnieniu wszystkich pól, należy podane dane zatwierdzić przyciskiem „add”. Następnie w zakładce Authentication, w sekcji „Advanced settings” należy się upewnić, że włączona jest opcja „Allow public client flows”.



Jeżeli ta opcja jest wyłączona, należy ją włączyć przestawiając na „yes”.

Oprócz tego należy dodać platformę, na której będzie działać aplikacja. W sekcji „Platform configurations”, trzeba kliknąć przycisk „Add a platform”, co spowoduje wyświetlenie dodatkowego okienka, z którego należy wybrać opcję „Mobile and desktop applications”:

Configure platforms



Web applications



Web

Build, host, and deploy a web server application. .NET, Java, Python



Single-page application

Configure browser client applications and progressive web applications. Javascript.

Mobile and desktop applications



iOS / macOS

Objective-C, Swift, Xamarin



Android

Java, Kotlin, Xamarin



Mobile and desktop applications

Windows, UWP, Console, IoT & Limited-entry Devices, Classic iOS + Android

Następnie należy zaznaczyć kwadrat przy adresie <https://login.microsoftonline.com/common/oauth2/nativeclient> jako „Redirect URI” i zatwierdzić zmiany przyciskiem „Configure”:

Configure Desktop + devices

[All platforms](#)
[Quickstart](#)
[Docs](#)

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

☒ <https://login.microsoftonline.com/common/oauth2/nativeclient>
☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)
 ☐ [msal163aa731-a283-4d40-8baa-37f0ebb6dcb0//auth](https://login.live.com/msal163aa731-a283-4d40-8baa-37f0ebb6dcb0//auth) (MSAL only)

Custom redirect URIs

Następnie po przejściu do zakładki overview należy skopiować wartości znajdujące się w „Application (client) ID” i „Directory (tenant) ID”. Te wartości będzie trzeba podać w aktywności w Wizlink.

[Delete](#)
[Endpoints](#)
[Preview features](#)

Essentials

Display name	: WizlinkMailer	Client credentials	: 0 certificate_1 secret
Application (client) ID	: 163aa731-a283-4d40-8baa-37f0ebb6dcb0	Redirect URIs	: 0 web_0 spa_1 public client
Object ID	: 69bec88e-9f5b-4302-bbb7-eeb790487a8d	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: cd022cfb-8386-4b29-9780-67af45aa38dc	Managed application in I...	: WizlinkMailer

Supported account types : [My organization only](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will upgrade to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#)
[Documentation](#)

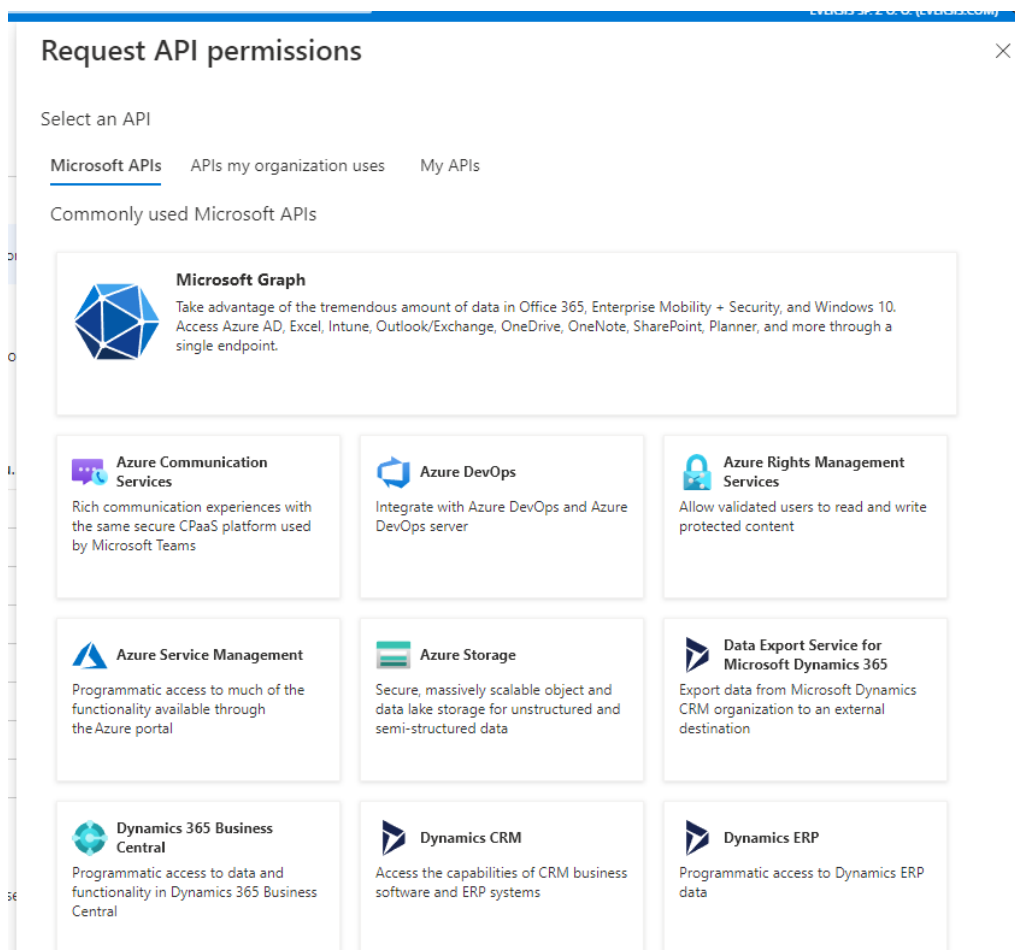
2. Nadanie uprawnień aplikacji

Następnym krokiem jest nadanie uprawnień do interakcji z potrzebnymi elementami Active Directory. W tym celu trzeba przejść do menu „API permissions”:

Manage

-  Branding & properties
-  Authentication
-  Certificates & secrets
-  Token configuration
-  API permissions
-  Expose an API
-  App roles
-  Owners
-  Roles and administrators
-  Manifest

Na otwartej stronie należy nacisnąć przycisk „Add a permission”, a z otwartego po prawej stronie panelu wybrać „Microsoft Graph”:



Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

- Microsoft Graph**
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.
- Azure Communication Services**
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams
- Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server
- Azure Rights Management Services**
Allow validated users to read and write protected content
- Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal
- Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data
- Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination
- Dynamics 365 Business Central**
Programmatic access to data and functionality in Dynamics 365 Business Central
- Dynamics CRM**
Access the capabilities of CRM business software and ERP systems
- Dynamics ERP**
Programmatic access to Dynamics ERP data

W zakładce Delegated permissions trzeba dodać następujące dostępy kolejno je wyszukując:

- email
- offline_access
- SMTP.Send
- User.Read

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](#)

i 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
SMTP (1) ☒ SMTP.Send ⓘ Send emails from mailboxes using SMTP AUTH.	No

Add permissions

Discard

Wybór trzeba zatwierdzić klikając przycisk „Add permissions”. Następnie trzeba ponownie nacisnąć przycisk „Add a permission”, w panelu wybrać zakładkę „APIs my organization uses” i wyszukać tam Office 365 Exchange Online:

Request API permissions



Select an API

Microsoft APIs **APIs my organization uses** My APIs

Apps in your directory that expose APIs are shown below

Office 365 Exchange Online	
Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000

W przeciwieństwie do Microsoft Graph, tym razem należy wybrać „Application premissions” i tam już analogicznie dodać uprawnienia do:

- IMAP.AccessAsApp
- POP.AccessAsApp

Ponownie zatwierdzamy przyciskiem „Add permissions”.

Na zakończenie konfiguracji osoba z uprawnieniami administratora w Azure Active Directory musi wyrazić zgodę na korzystanie z danych uprawnień przyciskiem Grant admin consent. Jeżeli ta opcja jest nieaktywna, należy skontaktować się z właścicielem konta z odpowiednimi prawami.

[+ Add a permission](#) [✓ Grant admin consent](#)

3. Konfiguracja po stronie Wizlink Designer

W aktywnościach związanych z obsługą maili dodana została nowa sekcja odpowiedzialna za OAuth. Zgodnie z konfiguracją z pierwszego punktu, na przykładzie aktywności „Get Email Count”, wypełnione wartości powinny wyglądać tak:

Selected element properties

Misc

Alternative Sce... ☒

DisplayName

OAuth

Application ID

Client Secret

Provider

Tenant Id

Use OAuth ☒

Należy zwrócić uwagę, że w przypadku OAuth Microsoftu, pole Client Secret powinno pozostać puste – jest ono wymagane w przypadku innych usługodawców uwierzytelniania OAuth. Pozostałe pola w aktywności należy skonfigurować tak jak do tej pory.