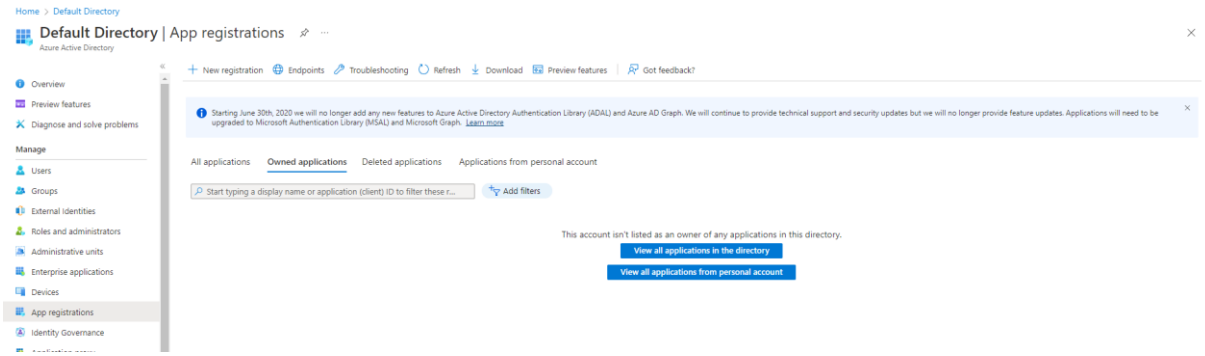
Konfiguracja Microsoft OAuth w Wizlink®

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.

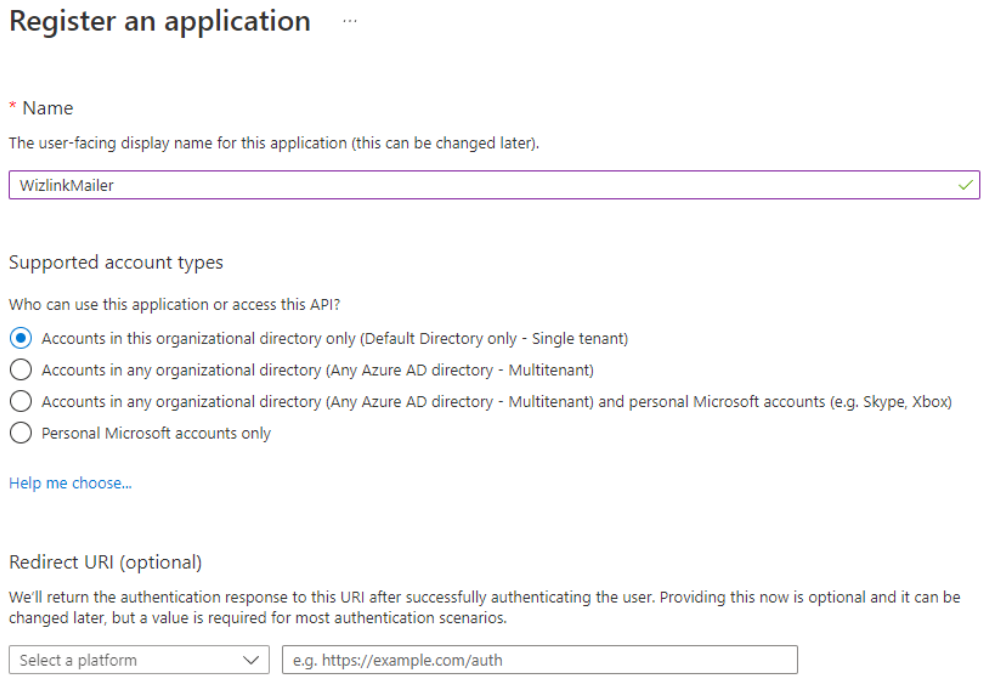
1. Utworzenie aplikacji w AAD.

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:



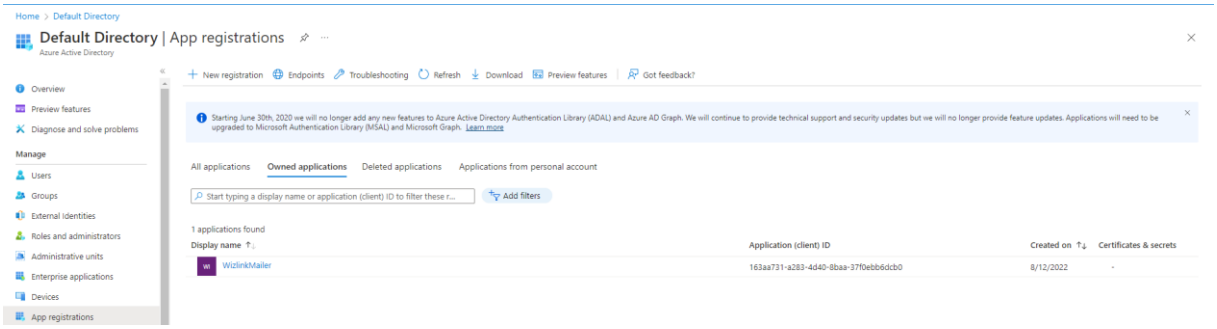
Z tego ekranu należy wybrać opcję „New Registration”.

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

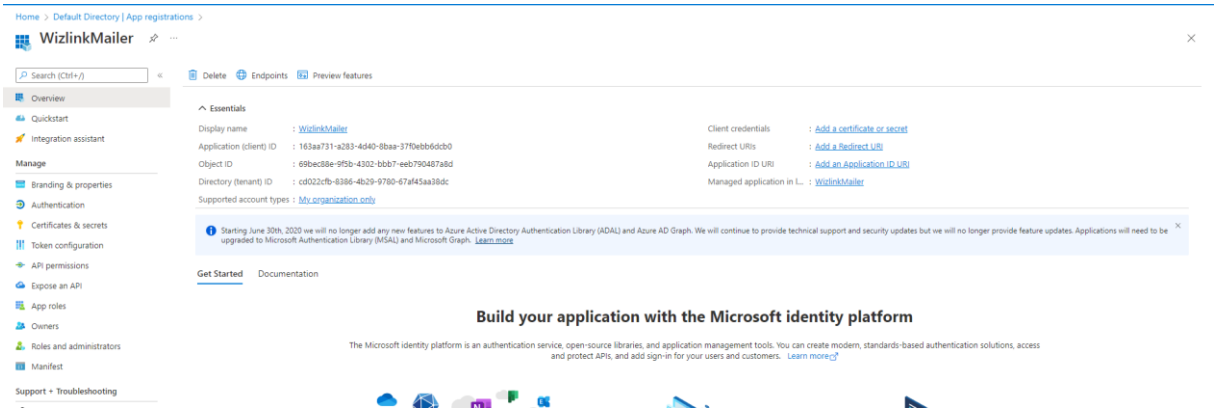


Następnie należy nacisnąć przycisk register.

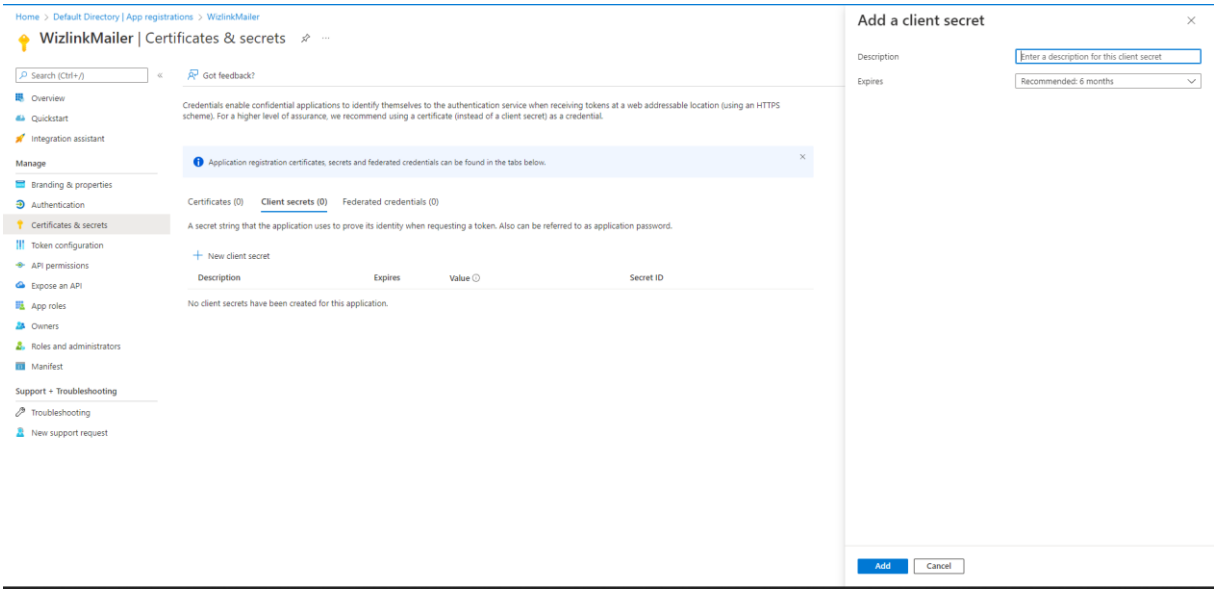
Jeżeli portal powróci na stronę główną, trzeba ponownie przejść do strony rejestracji aplikacji - a więc znowu wybrać opcję „Azure Active Directory" i po niej „App Registrations". Tym razem powinna się tam znajdować nowa aplikacja utworzona w poprzednim kroku:



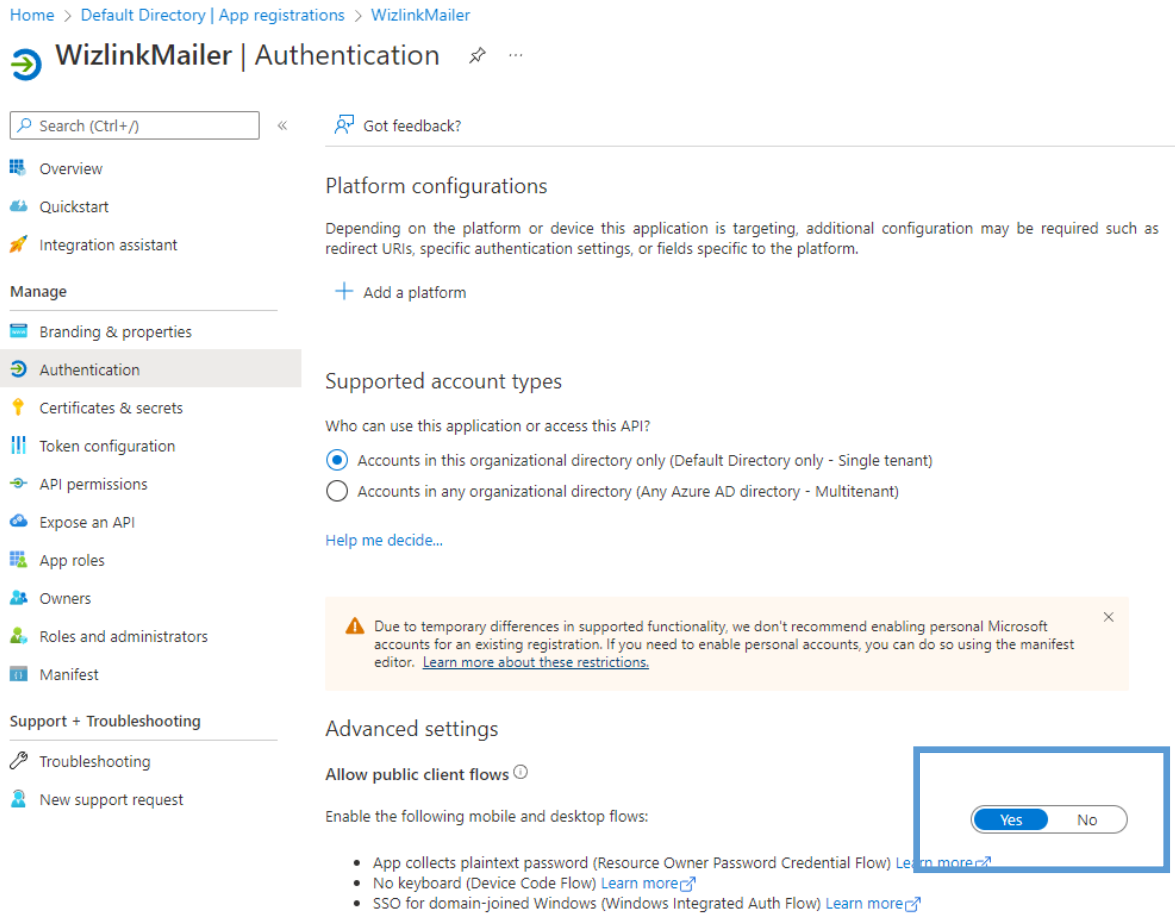
Klikając na jej nazwę następuje przeniesienie do zarządzania aplikacją:



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

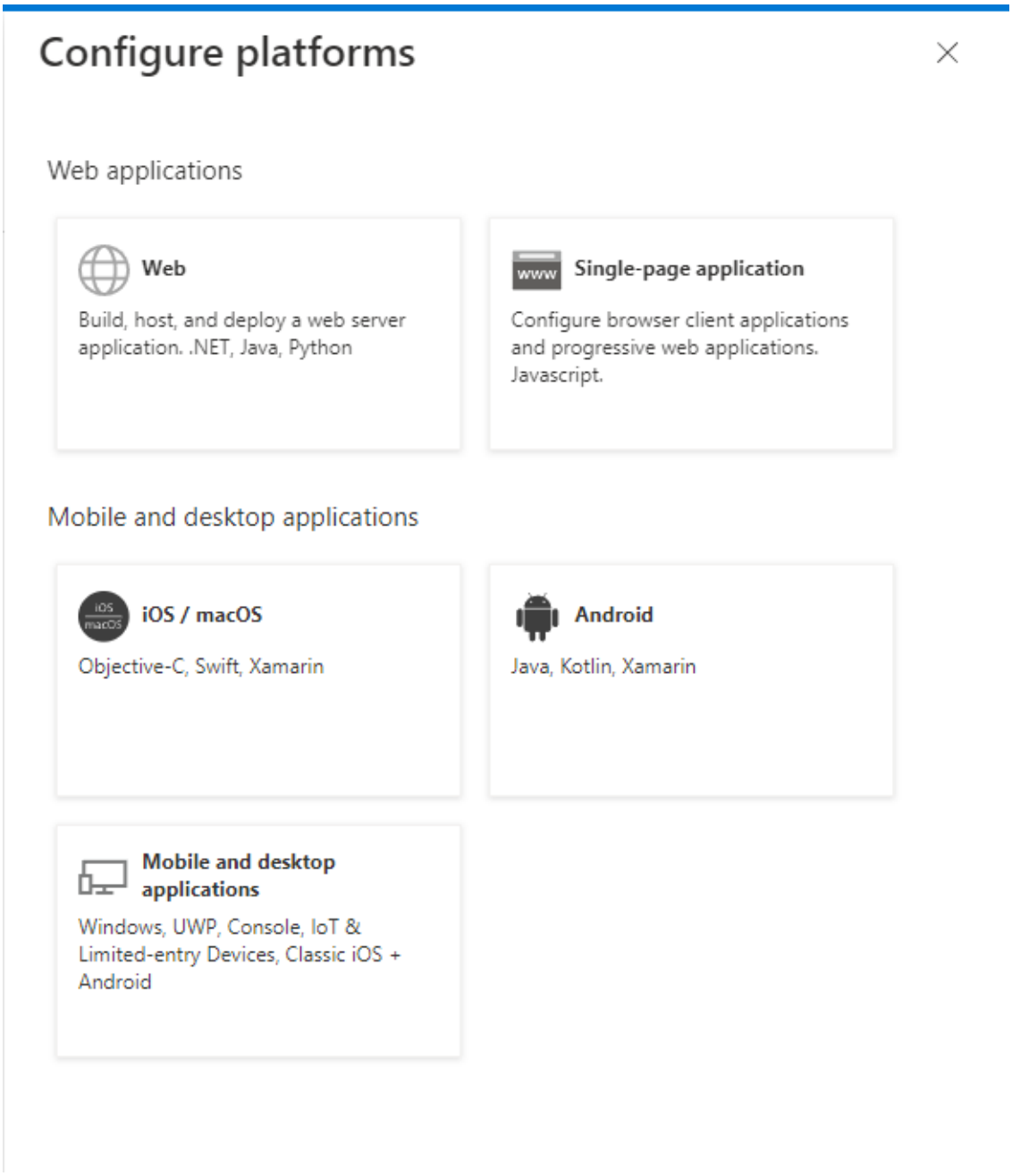


Po naciśnięciu przycisku „New client secret", po prawej stronie pojawi się okno. Formularz w tym oknie należy wypełnić, podając opis i czas, przez który ww. token będzie ważny. **Po upływie wybranego czasu, ten krok będzie trzeba powtórzyć.** Po uzupełnieniu wszystkich pól, należy podane dane zatwierdzić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

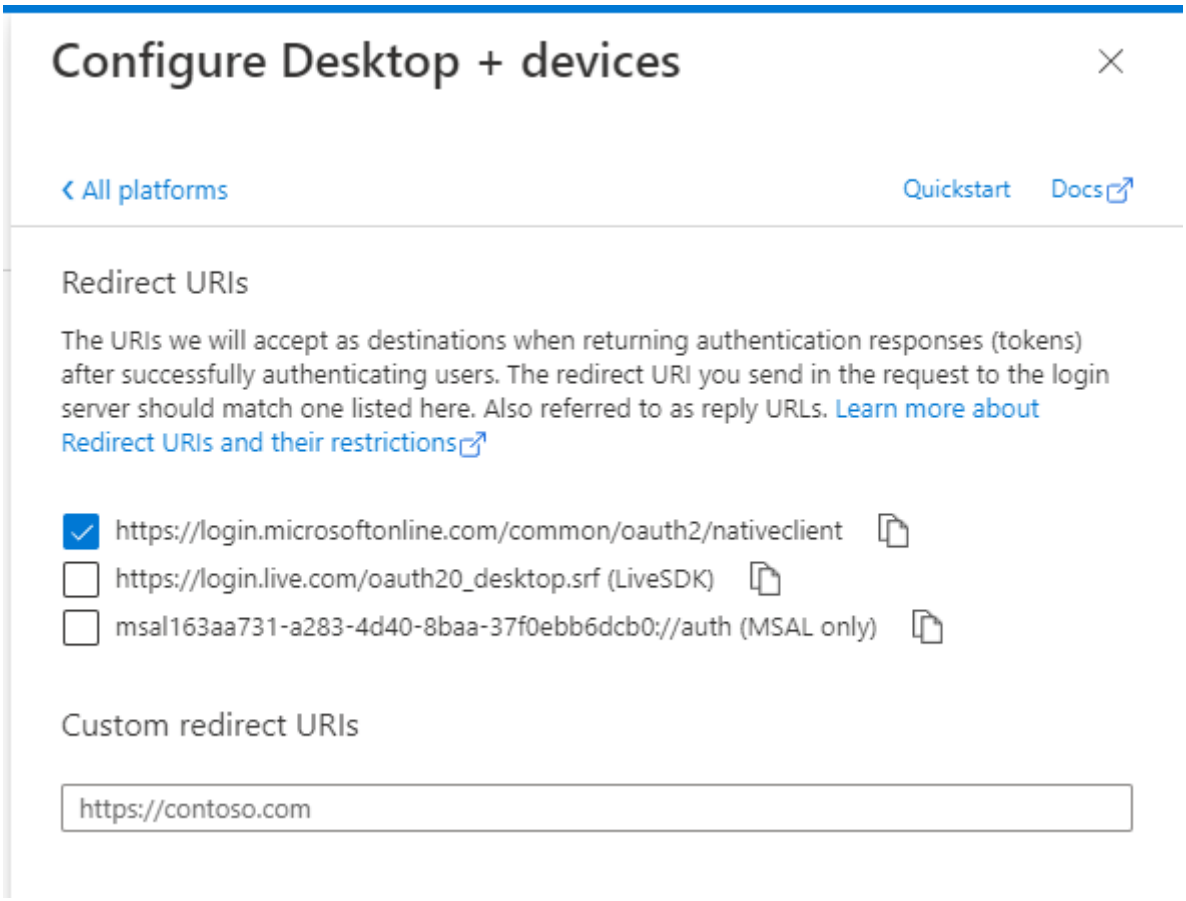


Jeżeli ta opcja jest wyłączona, należy ją włączyć przestawiając na „yes".

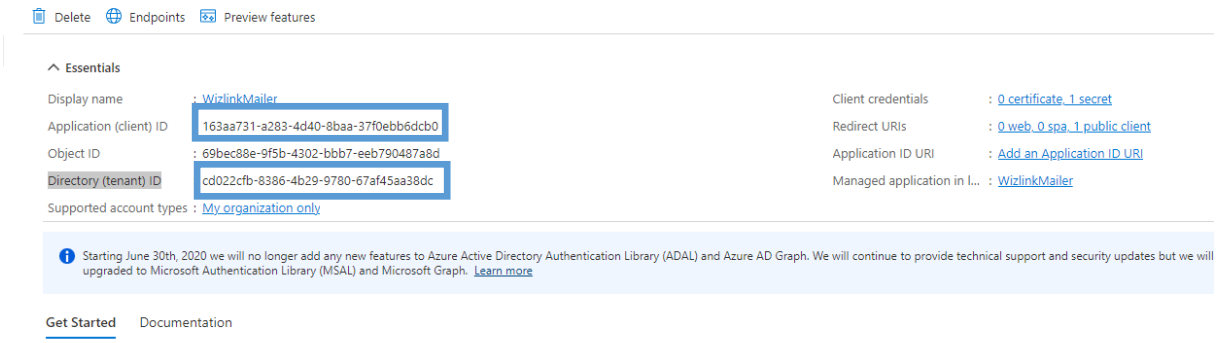
Oprócz tego należy dodać platformę, na której będzie działać aplikacja. W sekcji „Platform configurations", trzeba kliknąć przycisk „Add a platform", co spowoduje wyświetlenie dodatkowego okienka, z którego należy wybrać opcję „Mobile and desktop applications":



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

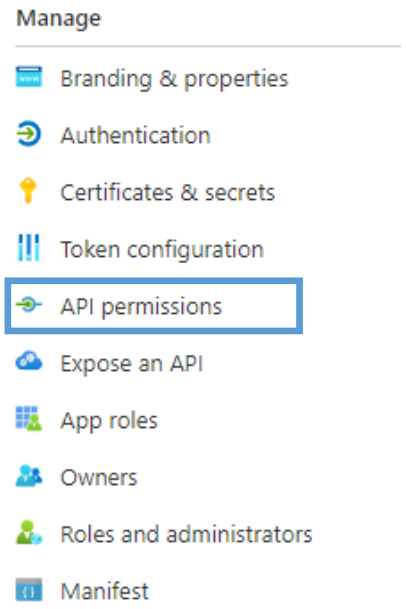


Następnie po przejściu do zakładki overview należy skopiować wartości znajdujące się w „Application (client) ID" i „Directory (tenant) ID". Te wartości będzie trzeba podać w aktywności w Wizlink.

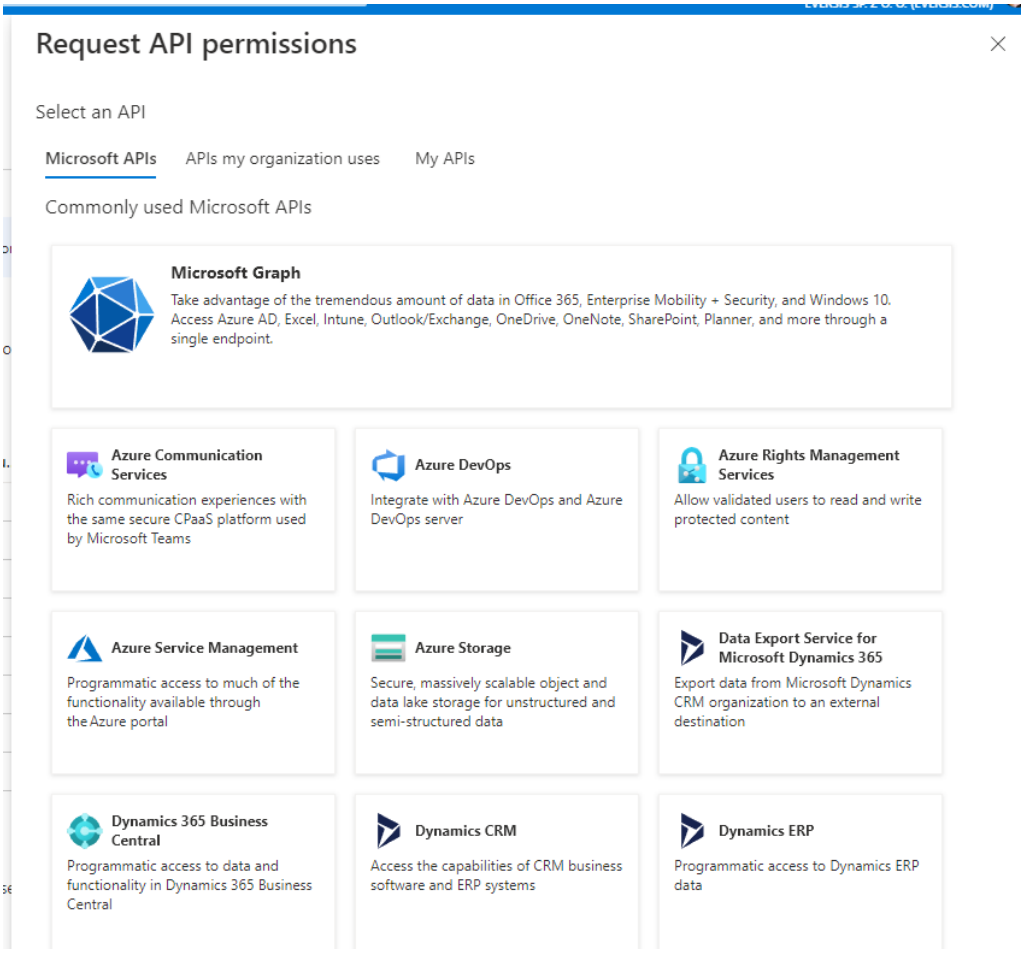


2. Nadanie uprawnień aplikacji

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

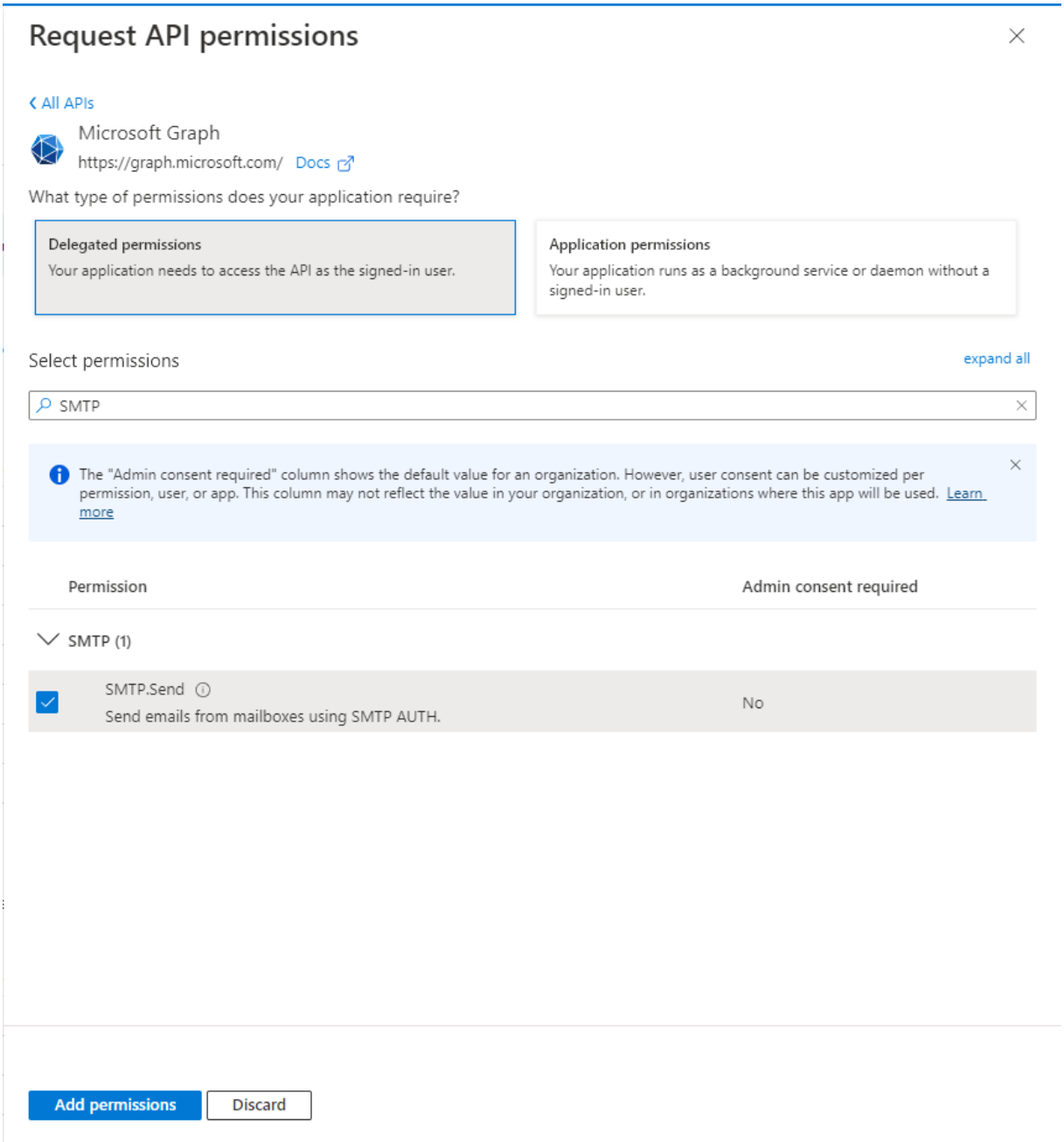


Na otwartej stronie należy nacisnąć przycisk „Add a permission", a z otwartego po prawej stronie panelu wybrać „Microsoft Graph":

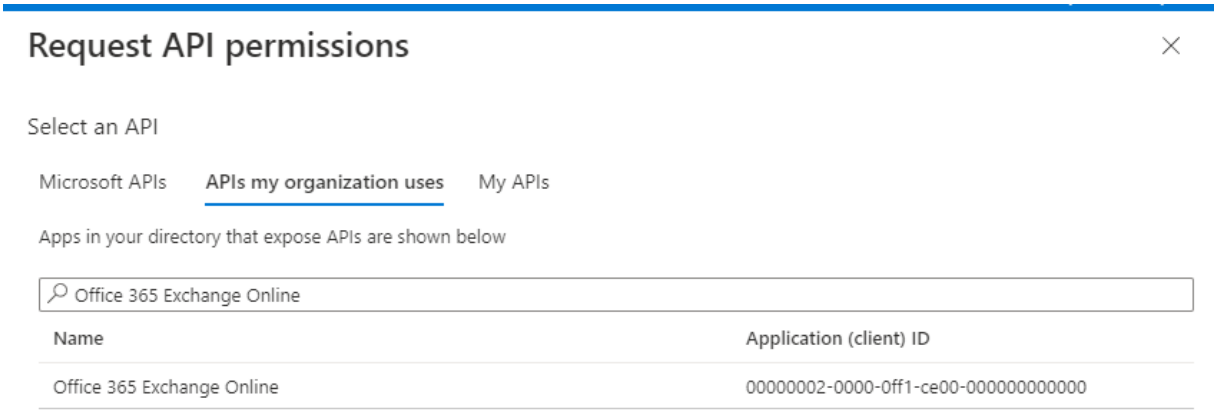


W zakładce Delegated permissions trzeba dodać następujące dostępy kolejno je wyszukując:

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



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:



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

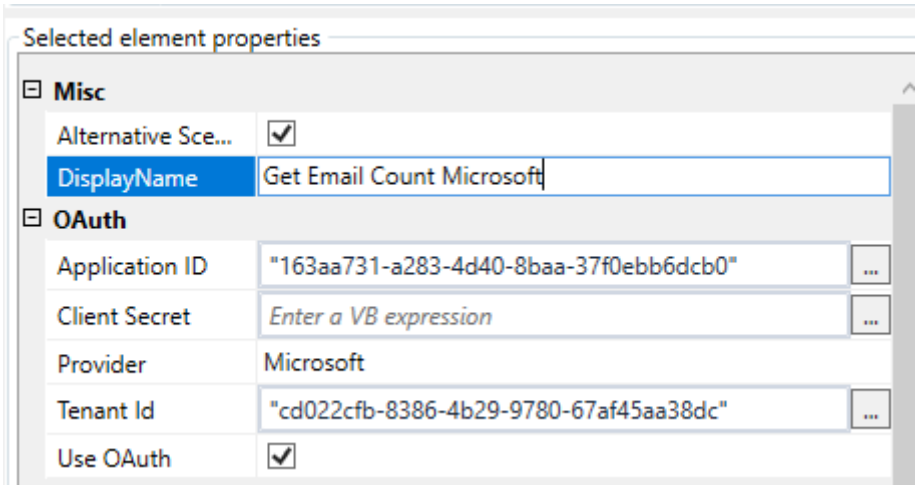
- IMAP.AccessAsApp
- POP.AccessAsApp

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.

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:



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.