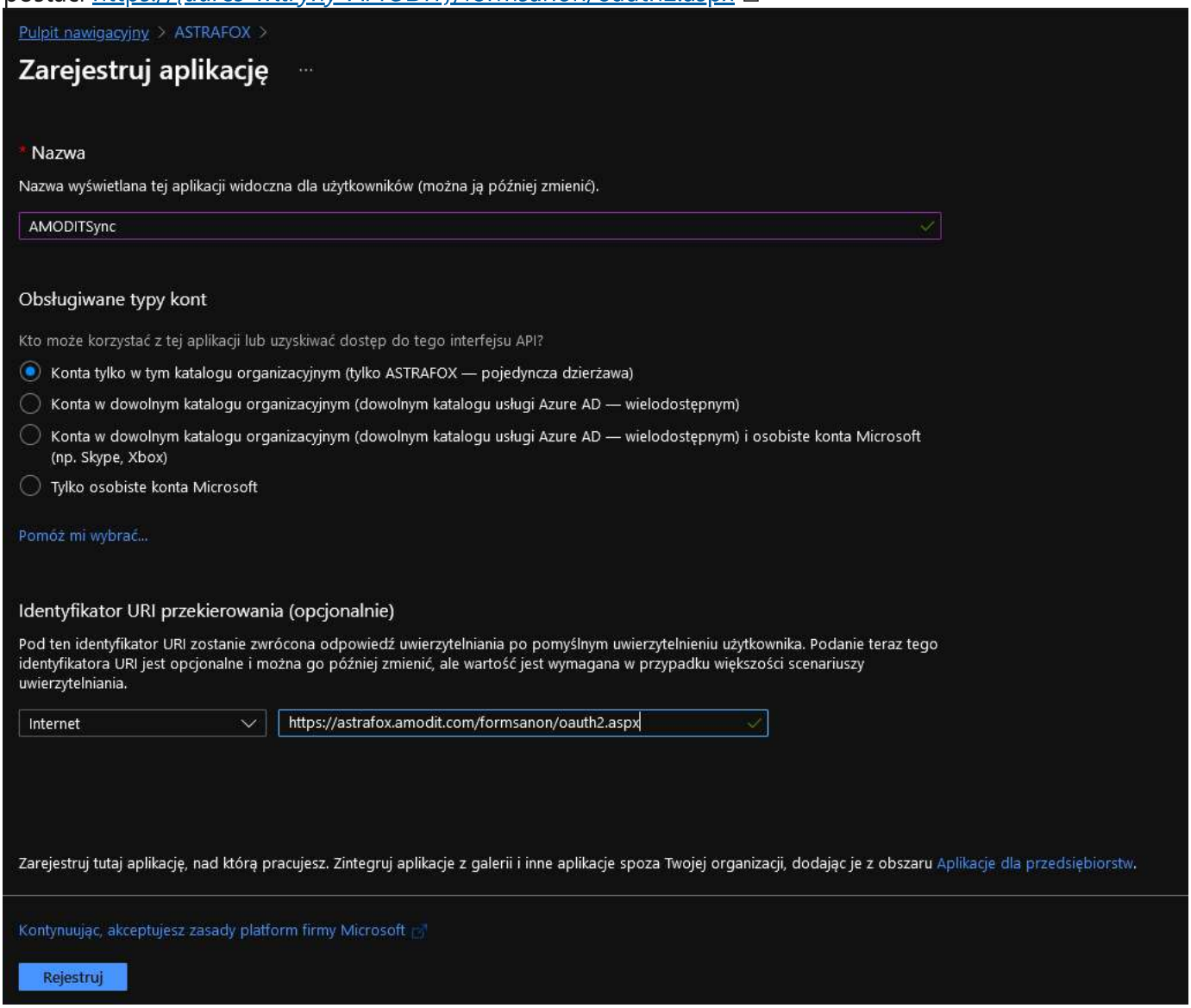
AzureAD i logowanie OpenId z Azure

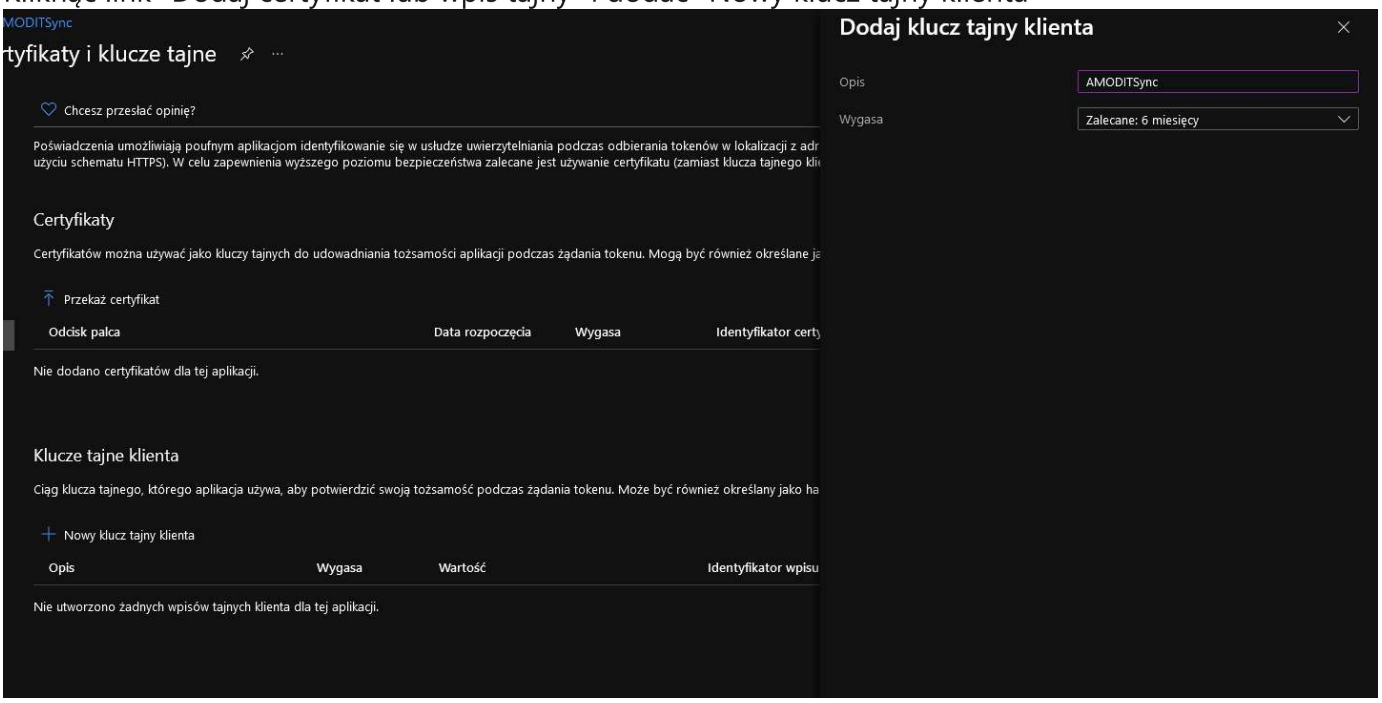
Last updated by | Łukasz Bott | 6 mar 2023 at 10:32 CET

Konfiguracja aplikacji Azure AD

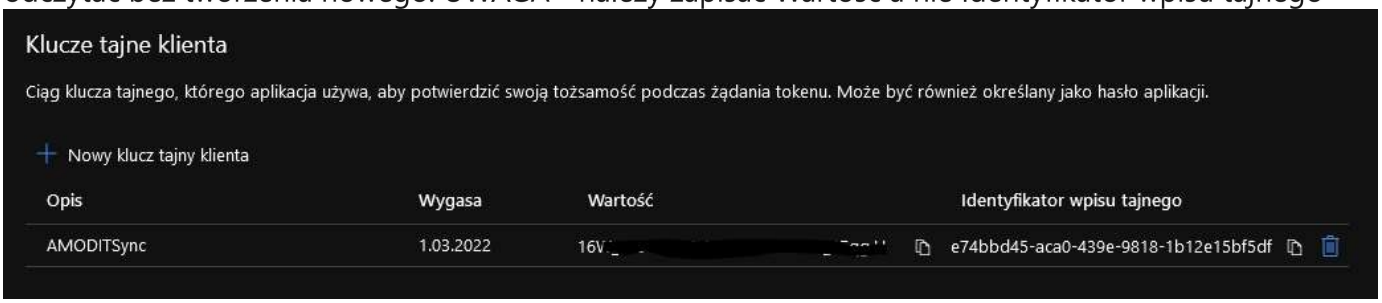
1. Należy wejść na stronę https://go.microsoft.com/fwlink/?linkid=2083908 (https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade)
2. Dodać nową rejestrację aplikacji o nazwie np. AMODITSync. Wpisać adres strony przekierowania w postaci https://*{adres_witryny_AMODIT}*/formsanon/oauth2.aspx



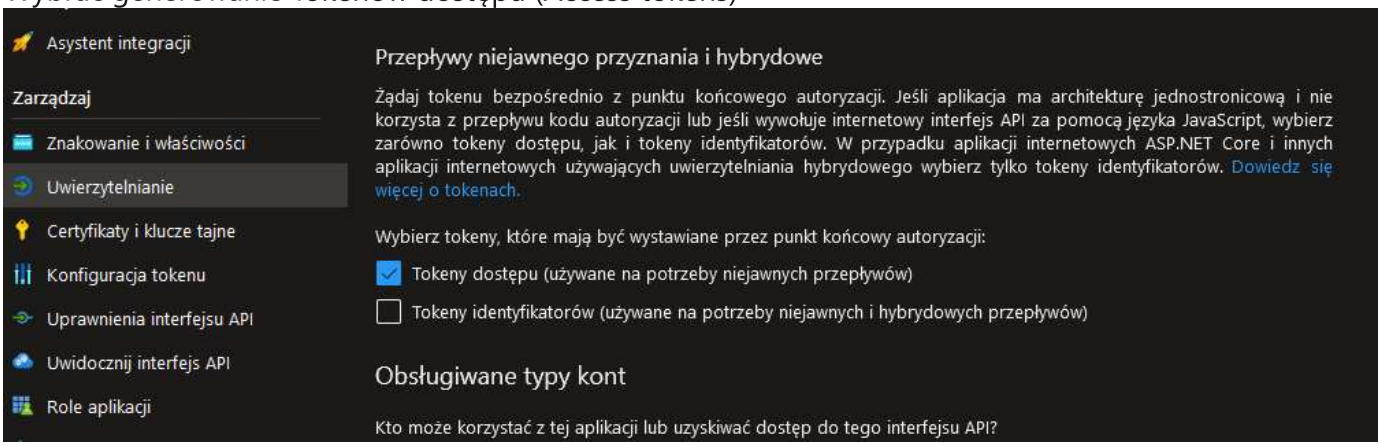
3. Kliknąć link "Dodaj certyfikat lub wpis tajny" i dodać "Nowy klucz tajny klienta"



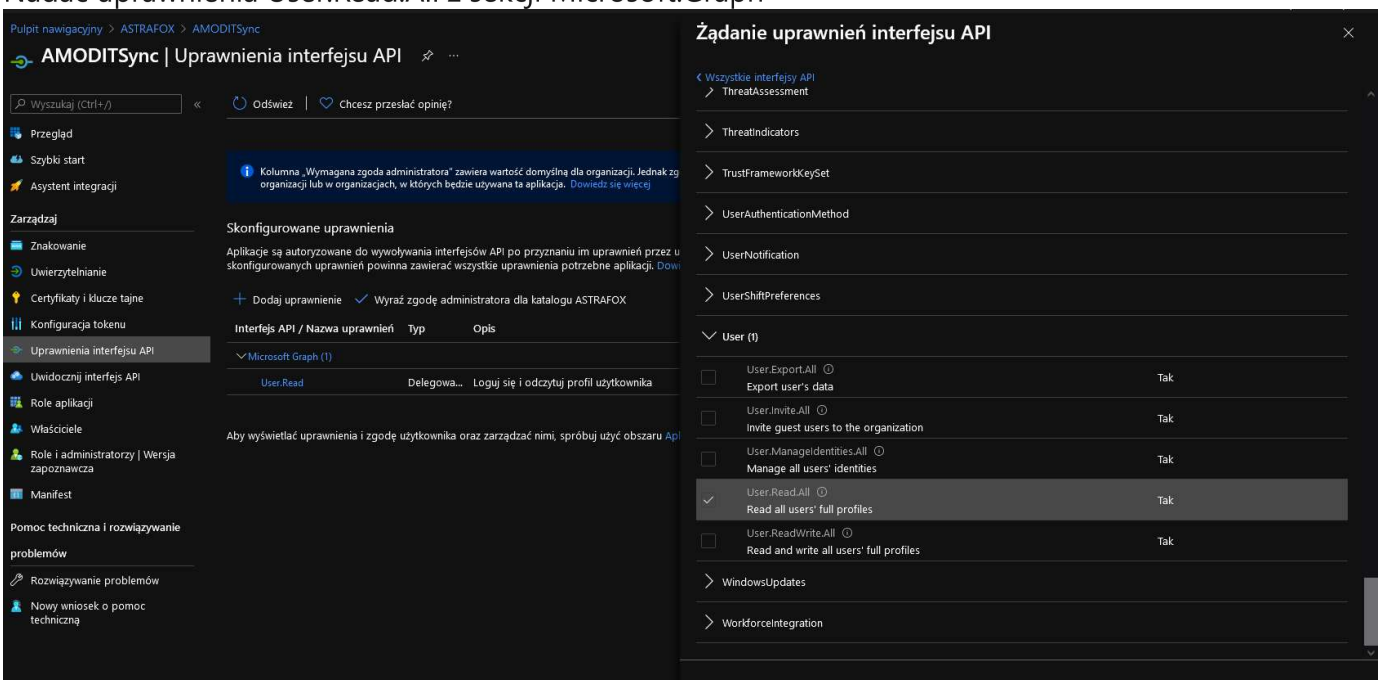
4. Po utworzeniu klucza tajnego należy zapisać jego wartość ponieważ potem nie będzie można go odczytać bez tworzenia nowego. UWAGA - należy zapisać Wartość a nie Identyfikator wpisu tajnego



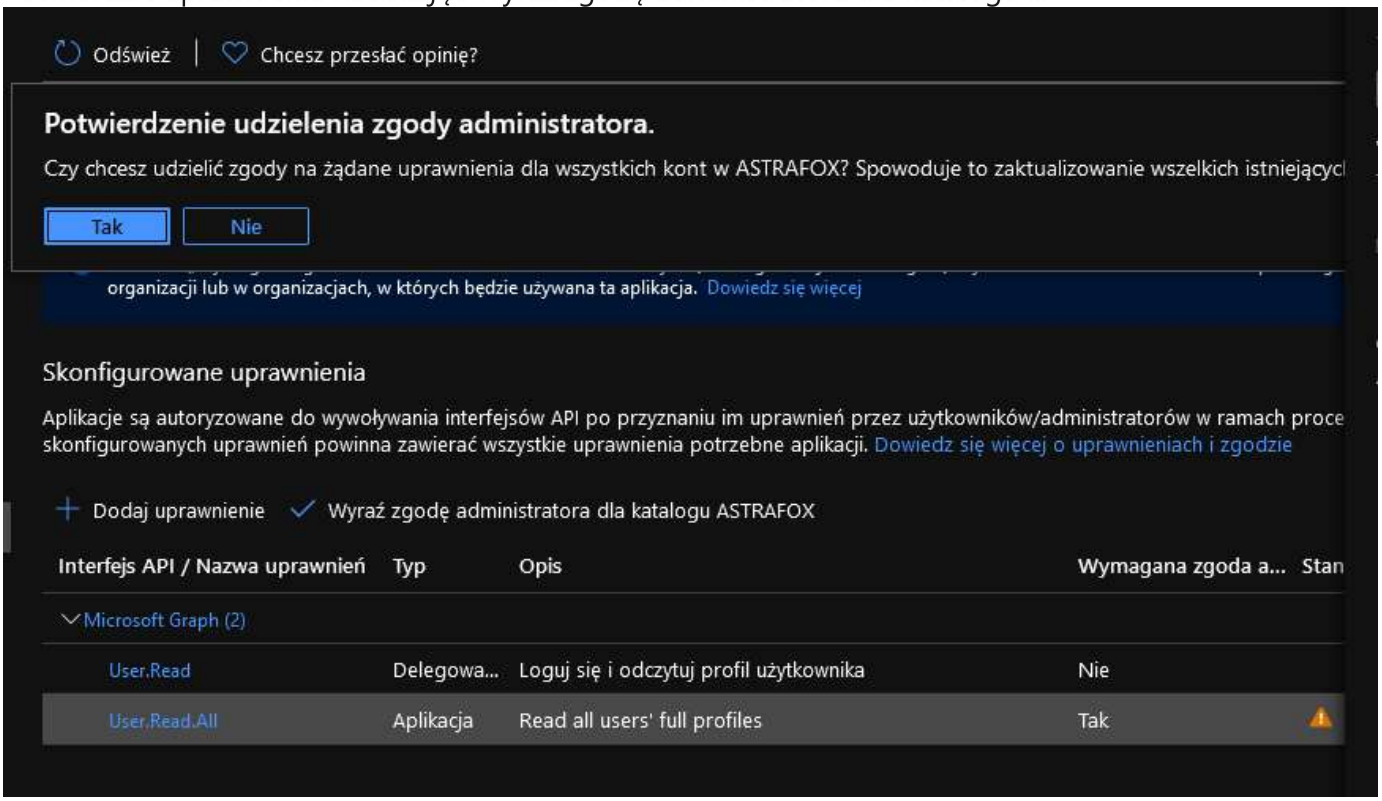
5. Wybrać generowanie Tokenów dostępu (Access tokens)



6. Nadać uprawnienia User.Read.All z sekcji Microsoft.Graph



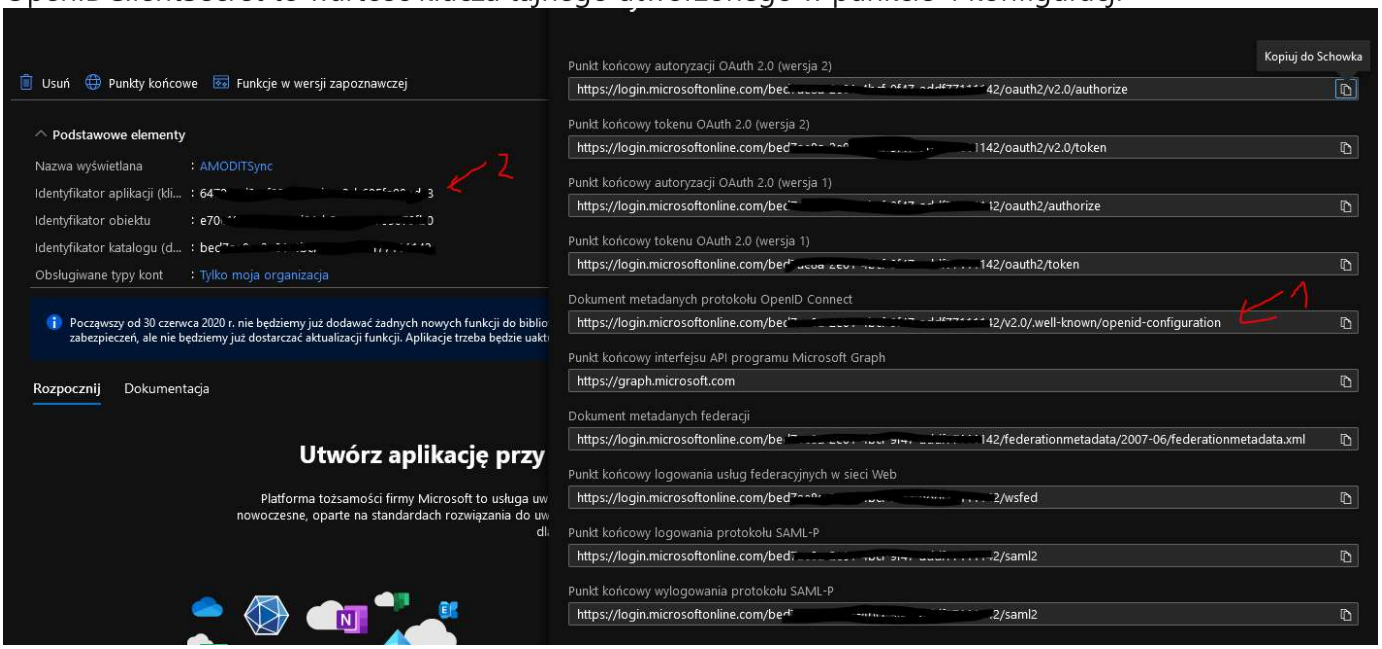
7. Potwierdzić uprawnienia naciskając Wyraź zgodę administratora dla katalogu ...



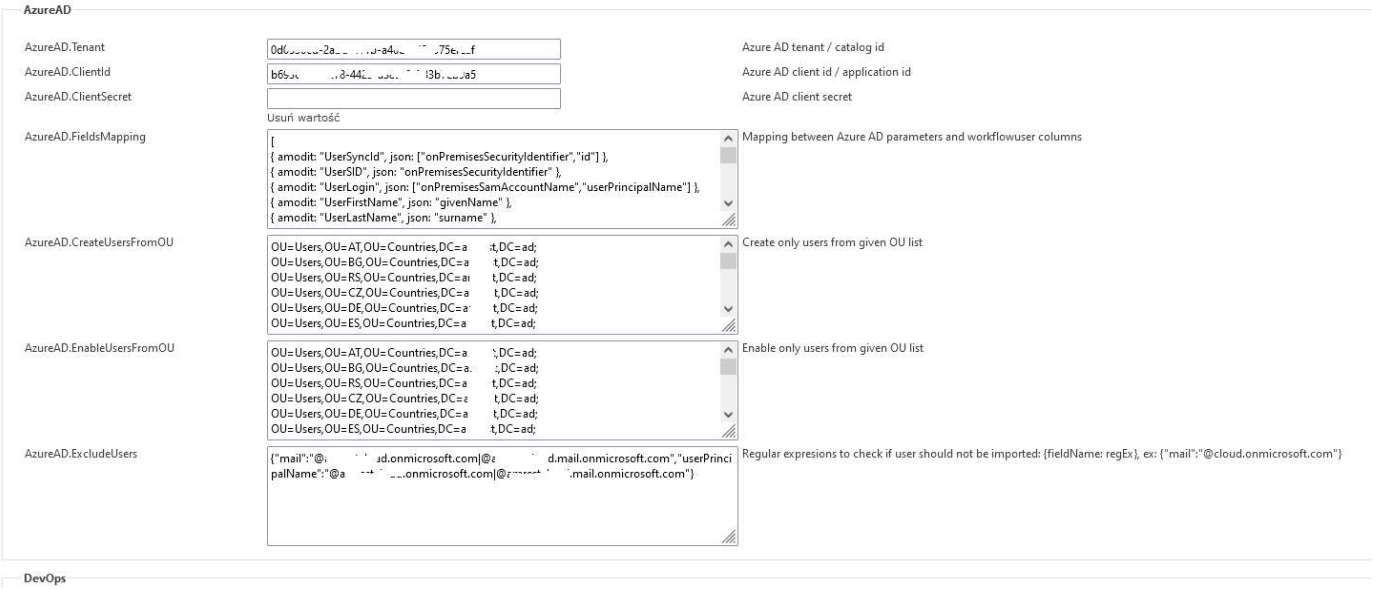
Konfiguracja AMODIT

1. Otworzyć Ustawienia systemowe i skonfigurować logowanie OpenID *(Ustawienia systemowe -> Ogólne -> OpenID)*:

- Wartość OpenIDConfigurationURL odczytać z zakładki Punkty końcowe z pola Dokument metadanych protokołu OpenID Connect (1)
- OpenIDClientId odczytać z pola Identyfikator aplikacji (2)
- OpenIDRedirectURL to adres przekierowania wpisany przy rejestracji aplikacji w punkcie 2 konfiguracji
- OpenIDButtonText to tekst, który pojawi się na przycisku logowania
- OpenIDScope wpisać User.Read
- OpenIDClientSecret to wartość klucza tajnego utworzonego w punkcie 4 konfiguracji



2. Skonfigurować synchronizację z AzureAD w zakładce Rozszerzenia AMODIT w AzureAD *(Ustawienia systemowe -> Rozszerzenia AMODIT -> AzureAD)*:



- AzureAD.Tenant - identyfikator katalogu z parametrów aplikacji
- AzureAD.ClientId - identyfikator aplikacji
- AzureAD.ClientSecret - klucz tajny
- AzureAD.FieldsMapping - mapowanie atrybutów Azure AD na kolumny w tabeli workflowuser
- AzureAD.CreateUsersFromOU - tworzenie kont użytkowników tylko ze wskazanych jednostek organizacyjnych
- AzureAD.EnableUsersFromOU - aktywowanie kont użytkowników tylko ze wskazanych jednostek organizacyjnych
- AzureAD.ExcludeUsers - wyrażenia regularne, umożliwiające ustawienie filtrów wykluczających konta użytkowników z importu z Azure AD.