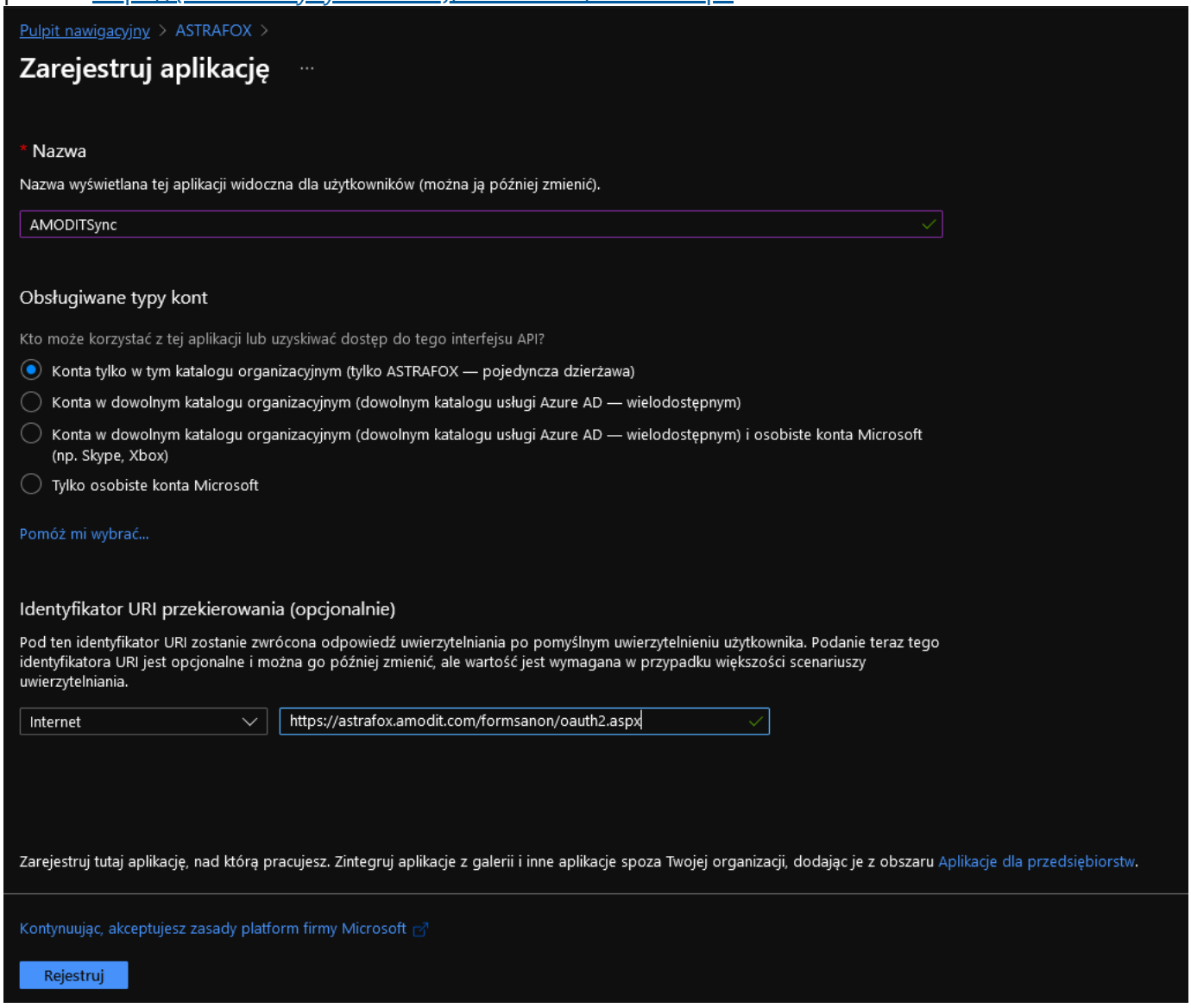
AzureAD i logowanie OpenId z Azure

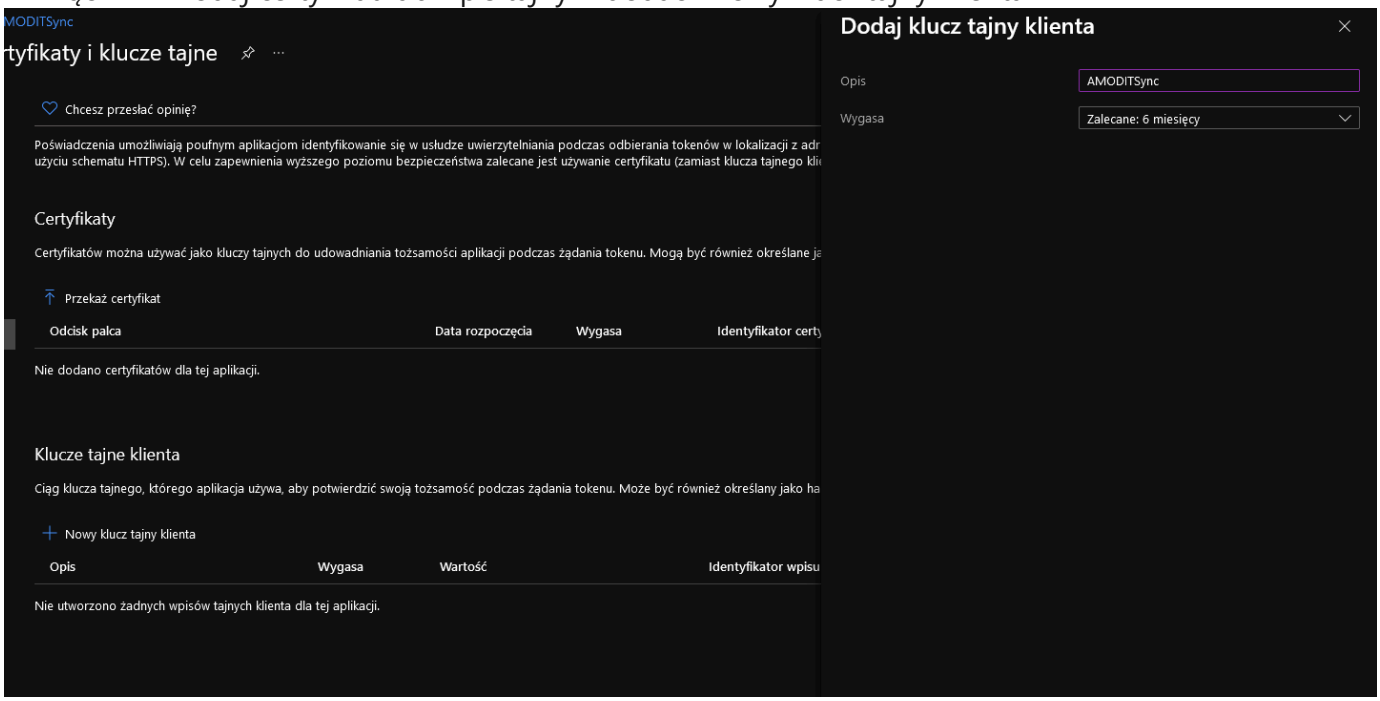
Last updated by | Piotr Buczkowski | 20 cze 2024 at 15:40 CEST

Konfiguracja aplikacji Azure AD

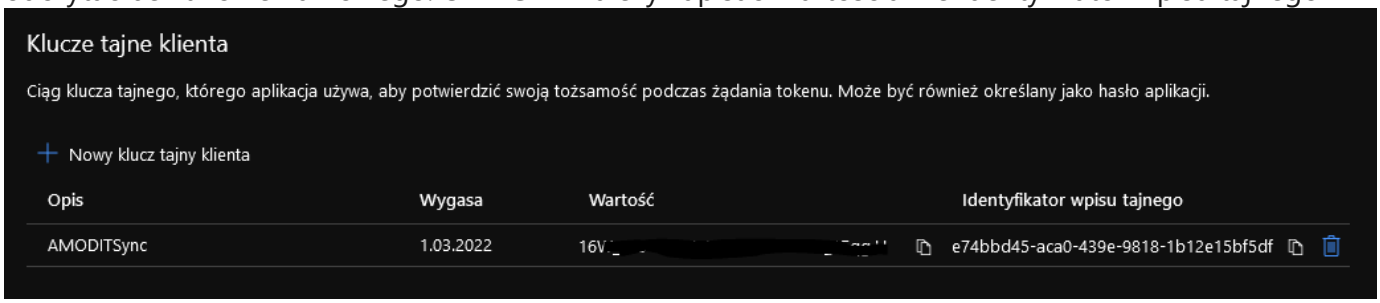
1. Należy wejść na stronę https://go.microsoft.com/fwlink/?linkid=2083908 (https://portal.azure.com/#blade/Microsoft_AAD_RegisteredApps/ApplicationsListBlade)
2. Dodać nową rejestrację aplikacji o nazwie np. AMODITSync. Wpisać adres strony przekierowania w postaci https://*{adres_witryny_AMODIT}*/formsanon/oauth2.aspx



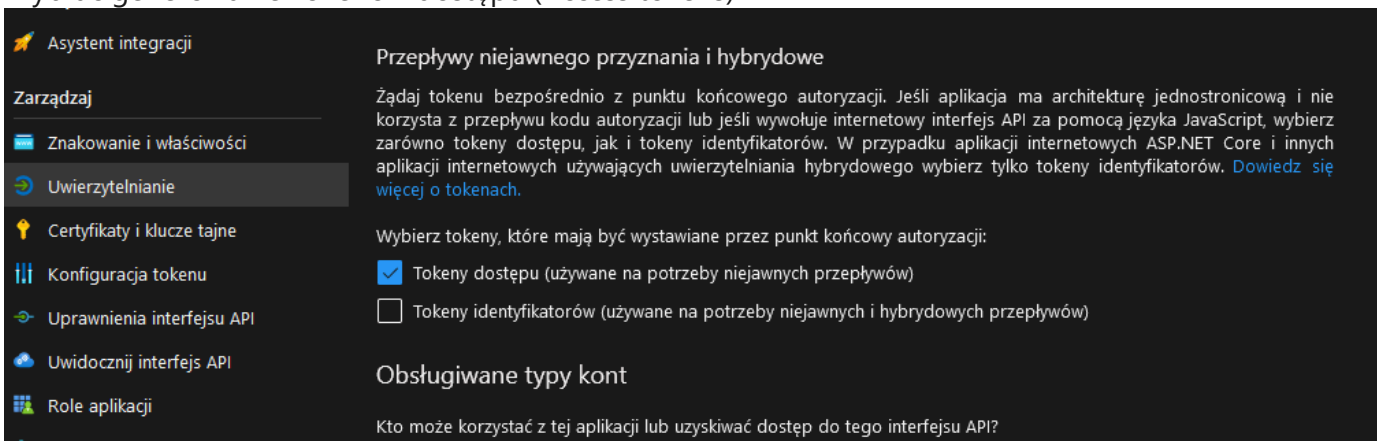
3. Kliknąć link "Dodaj certyfikat lub wpis tajny" i dodać "Nowy klucz tajny klienta"



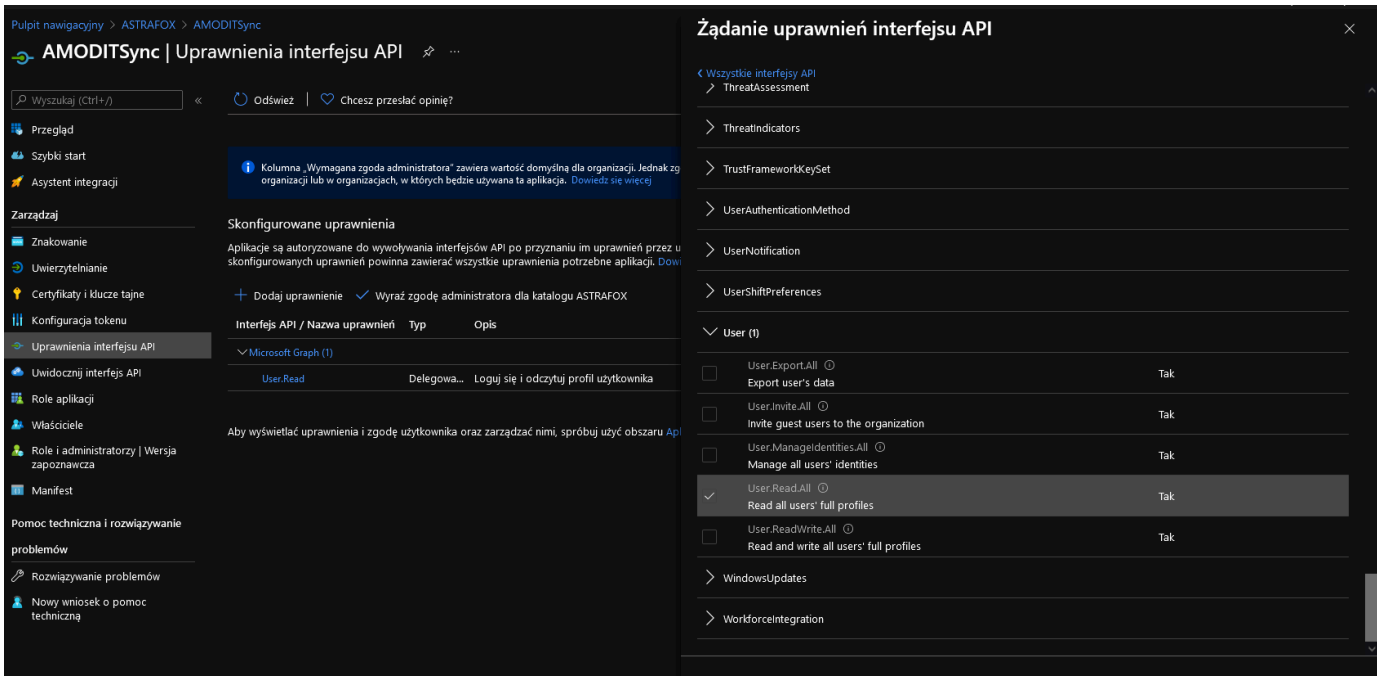
4. Po utworzeniu klucza tajnego należy zapisać jego wartość ponieważ potem nie będzie można go odczytać bez tworzenia nowego. UWAGA - należy zapisać Wartość a nie Identyfikator wpisu tajnego



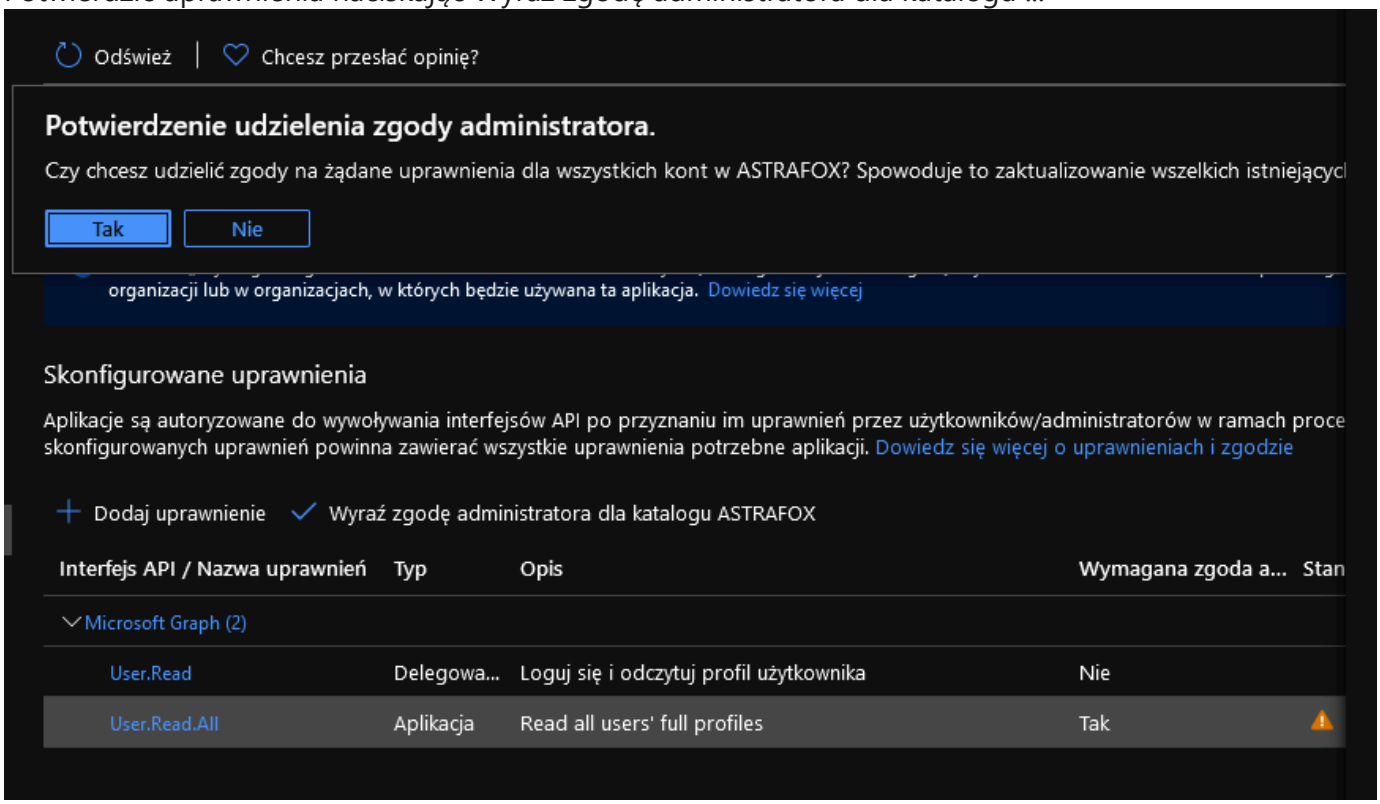
5. Wybrać generowanie Tokenów dostępu (Access tokens)



6. Nadać uprawnienia User.Read.All z sekcji Microsoft.Graph. Jeżeli chcemy ograniczyć synchronizację użytkowników tylko do wybranych grup to należy dodać także uprawnienie Group.Read.All.

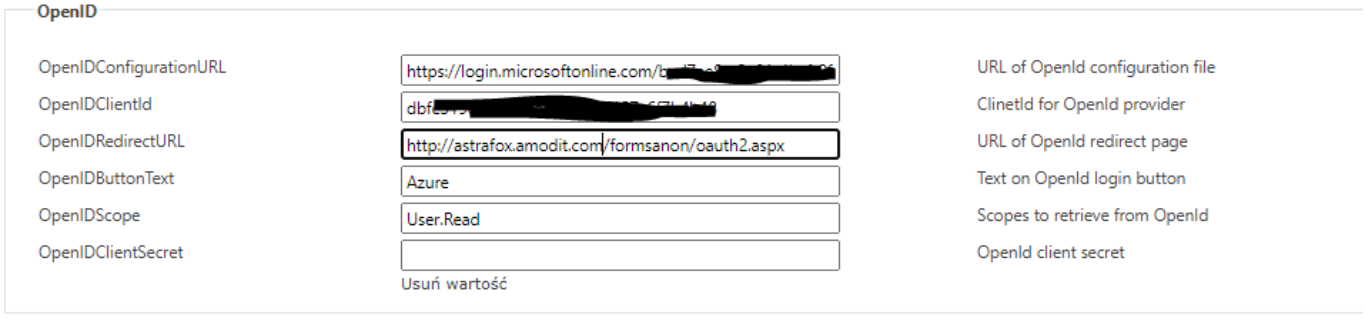


7. Potwierdzić uprawnienia naciskając Wyraź zgodę administratora dla katalogu ...

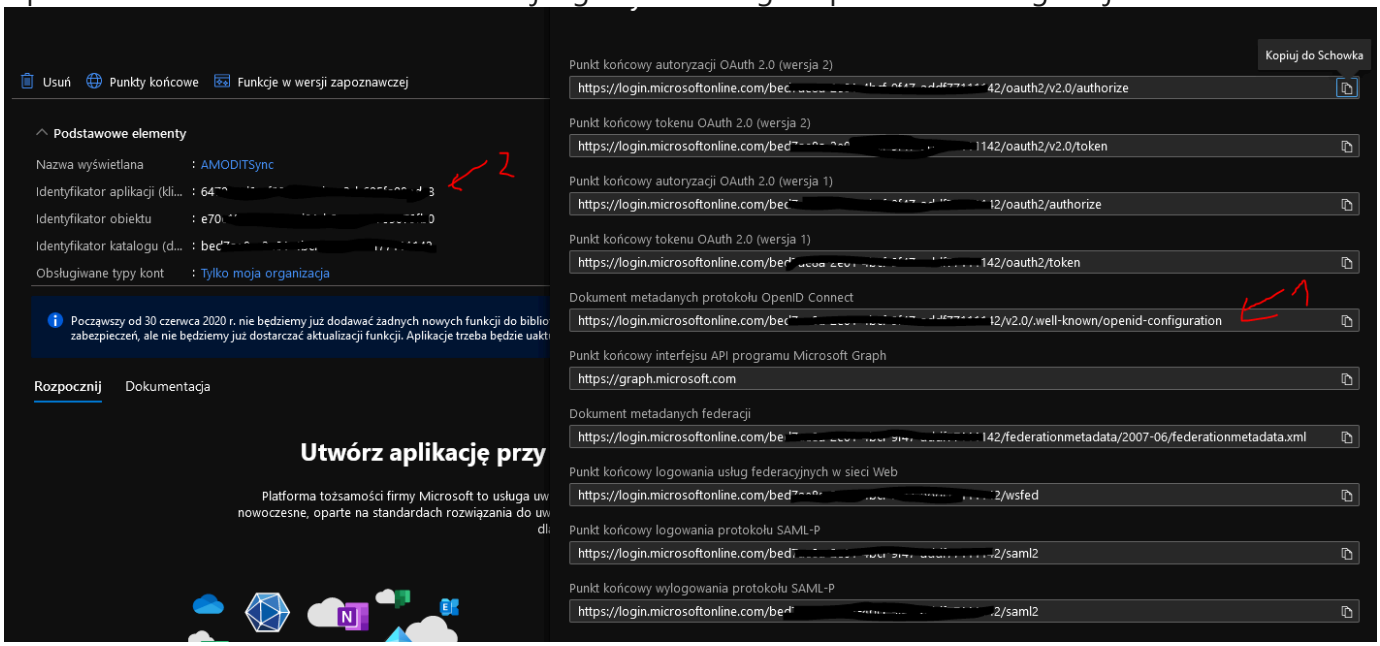


Konfiguracja logowania do AMODIT przy pomocy kont AzureAD

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

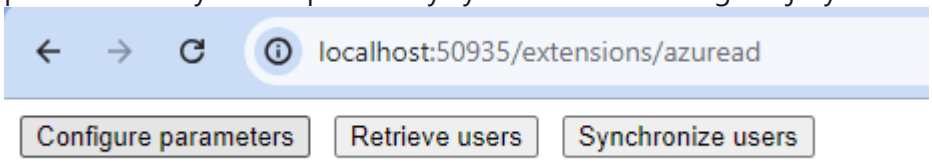


- Wartość OpenIDConfigurationURL odczytać z zakładki Punkty końcowe z pola Dokument metadanych protokołu OpenID Connect (1)
- OpenIDClientId odczytać z pola Identyfikator aplikacji (2)
- OpenIDRedirectURL to adres przekierowania wpisany przy rejestracji aplikacji w punkcie 2 konfiguracji
- OpenIDButtonText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

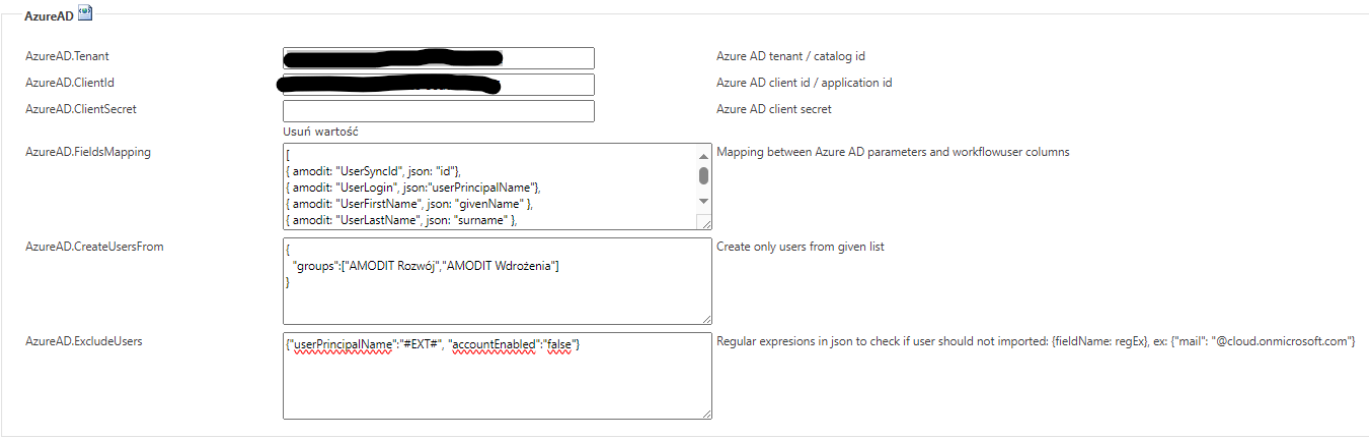


Konfiguracja synchronizacji użytkowników z AzureAD

1. Wejść na stronę https://adres_witryny_AMODIT/extensions/azuread i nacisnąć przycisk Configure parameters aby dodać parametry systemowe do konfiguracji synchronizacji z AzureAD.



2. Skonfigurować parametry synchronizacji w zakładce Rozszerzenia AMODIT w sekcji 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.CreateUsersFrom - tworzenie kont użytkowników tylko ze wskazanych elementów, obecnie obsługiwana jest tylko synchronizacja z grup.
- AzureAD.ExcludeUsers - wyrażenia regularne, umożliwiające ustawienie filtrów wykluczających konta użytkowników z importu z Azure AD.

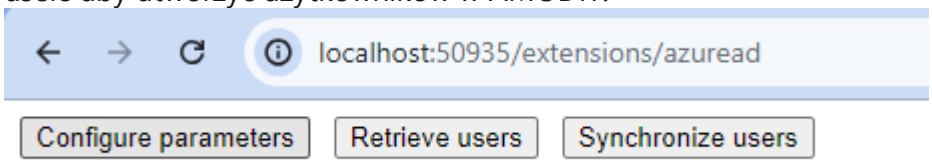
3. Przykładowa wartość parametru AzureAD.FieldsMapping

```
[
{ amodit: "UserSyncId", json: "id" },
{ amodit: "UserLogin", json: "userPrincipalName" },
{ amodit: "UserFirstName", json: "givenName" },
{ amodit: "UserLastName", json: "surname" },
{ amodit: "UserEmail", json: "mail" },
{ amodit: "UserPosition", json: "jobTitle" },
{ amodit: "UserPhoneNumbers", json: "businessPhones" },
{ amodit: "UserMobileNumbers", json: "mobilePhone" },
{ amodit: "UserLocation", json: "officeLocation" },
{ amodit: "UserIsBlocked", json: "accountEnabled", op: "!"},
{ amodit: "UserDepartment", json: "department" },
{ amodit: "UserEmployeeId", json: "employeeId" },
{ amodit: "UserManager", json: "manager", expand: true}
]
```

4. Przykładowa wartość AzureAD.CreateUsersFrom
   Synchronizacja tylko członków grup AMODIT Rozwój i AMODIT Wdrożenia. Należy pamiętać o nadaniu uprawnień Group.Read.All w Azure.

```
{
  "groups":["AMODIT Rozwój","AMODIT Wdrożenia"]
}
```

5. Przykładowa wartość AzureAD.ExcludeUsers
   Wyklucza synchronizację użytkowników z ciągiem #EXT# w userPrincipalName oraz tych nie włączonych.
   `{ "userPrincipalName": "#EXT#", "accountEnabled": "false" }`
   Różnica pomiędzy synchronizowaniem pola accountEnabled do UserIsBlocked a pomijaniem użytkowników z accountEnabled:false jest takie, że w pierwszym przypadku tacy użytkownicy zostaną dodani ale ze statusem blocked a w drugim zostaną pominięci przy synchronizacji. Jeżeli aktywny użytkownik AMODIT zostanie zablokowany w AzureAD to w czasie synchronizacji w obydwu przypadkach zostanie zablokowany w AMODIT.
6. Przetestować działanie synchronizacji użytkowników z AzureAD
   Na stronie https://adres_witryny_AMODIT/extensions/azuread nacisnąć przycisk Retrieve users i sprawdzić czy została pobrana prawidłowa lista użytkowników. Jeżeli tak to można nacisnąć Synchronize users aby utworzyć użytkowników w AMODIT.



7. Skonfigurować job synchronizacji użytkowników z AzureAD
   W ustawieniach systemowych na zakładce Zadania dodać zadanie:
   Nazwa: AzureADSynchronizationJob
   Biblioteka: Inne->AMODITAzureAD
   Klasa: AMODITAzureAD.Job.AzureADSynchronizationJob

częstotliwość według uznania

8. Synchronizacja grupy AMODIT z grupą Azure
   Aby zsynchronizować grupę AMODIT z grupą Azure w ustawieniach grupy AMODIT należy wybrać synchronizację z AD oraz wpisać nazwę grupy Azure poprzedzoną przedrostkiem Azure: