

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

Pulpit nawigacyjny > ASTRAFOX >

Zarejestruj aplikację ...

* Nazwa

Nazwa wyświetlana tej aplikacji widoczna dla użytkowników (można ją później zmienić).

AMODITSync ✓

Obsługiwane typy kont

Kto może korzystać z tej aplikacji lub uzyskiwać dostęp do tego interfejsu API?

☒ Konta tylko w tym katalogu organizacyjnym (tylko ASTRAFOX — pojedyncza dzierżawa)

☐ Konta w dowolnym katalogu organizacyjnym (dowolnym katalogu usługi Azure AD — wielodostępnym)

☐ Konta w dowolnym katalogu organizacyjnym (dowolnym katalogu usługi Azure AD — wielodostępnym) i osobiste konta Microsoft (np. Skype, Xbox)

☐ Tylko osobiste konta Microsoft

[Pomóż mi wybrać...](#)

Identyfikator URI przekierowania (opcjonalnie)

Pod ten identyfikator URI zostanie zwrócona odpowiedź uwierzytelniania po pomyślnym uwierzytelnieniu użytkownika. Podanie teraz tego identyfikatora URI jest opcjonalne i można go później zmienić, ale wartość jest wymagana w przypadku większości scenariuszy uwierzytelniania.

Internet ▼ <https://astrafox.amodit.com/formsanon/oauth2.aspx> ✓

Zarejestruj tutaj aplikację, nad którą pracujesz. Zintegruj aplikacje z galerii i inne aplikacje spoza Twojej organizacji, dodając je z obszaru [Aplikacje dla przedsiębiorstw](#).

Kontynuując, akceptujesz zasady platform firmy Microsoft [🔗](#)

Rejestruj

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

Dodaj klucz tajny klienta

Opis: AMODITSync

Wygasa: Zalecane: 6 miesięcy

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

Klucze tajne klienta

Ciąg klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako hasło aplikacji.

+ Nowy klucz tajny klienta

Opis	Wygasa	Wartość	Identyfikator wpisu tajnego
AMODITSync	1.03.2022	[Redacted]	e74bbd45-aca0-439e-9818-1b12e15bf5df

5. Wybrać generowanie Tokenów dostępu (Access tokens)

Asystent integracji

Zarządzaj

- Znakowanie i właściwości
- Uwierzytelnianie**
- Certyfikaty i klucze tajne
- Konfiguracja tokenu
- Uprawnienia interfejsu API
- Uwidocznij interfejs API
- Role aplikacji

Przepływy niejawnego przyznania i hybrydowe

Żądaj tokenu bezpośrednio z punktu końcowego autoryzacji. Jeśli aplikacja ma architekturę jednostronicową i nie korzysta z przepływu kodu autoryzacji lub jeśli wywołuje internetowy interfejs API za pomocą języka JavaScript, wybierz zarówno tokeny dostępu, jak i tokeny identyfikatorów. W przypadku aplikacji internetowych ASP.NET Core i innych aplikacji internetowych używających uwierzytelniania hybrydowego wybierz tylko tokeny identyfikatorów. [Dowiedz się więcej o tokenach.](#)

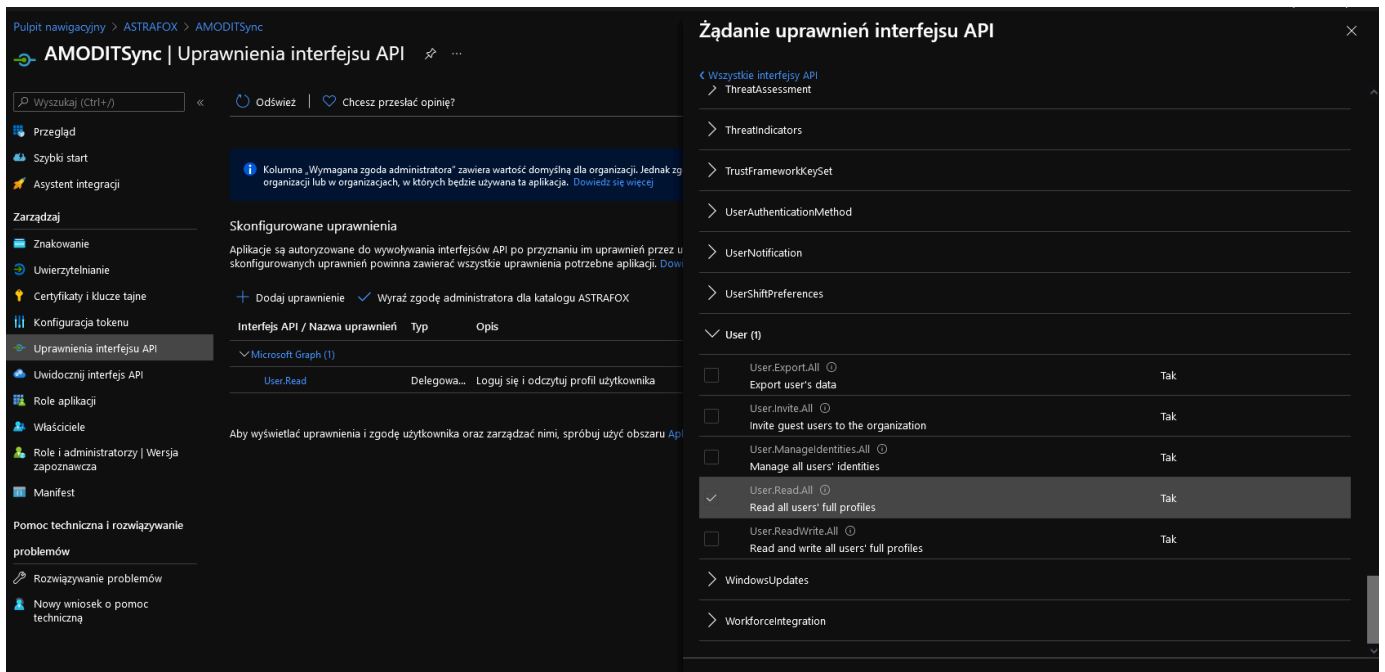
Wybierz tokeny, które mają być wystawiane przez punkt końcowy autoryzacji:

- ☒ Tokeny dostępu (używane na potrzeby niejawnych przepływów)
- ☐ Tokeny identyfikatorów (używane na potrzeby niejawnych i hybrydowych przepływów)

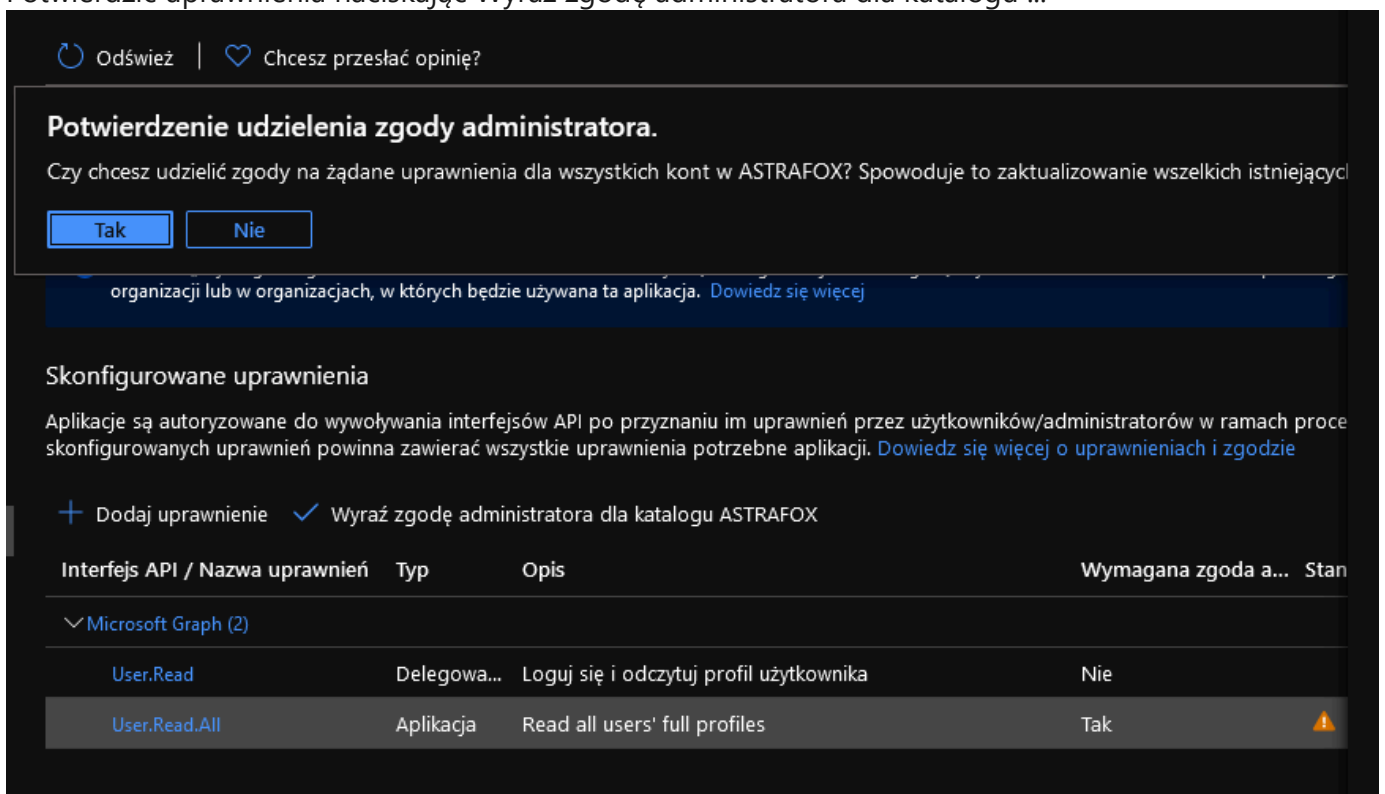
Obsługiwane typy kont

Kto może korzystać z tej aplikacji lub uzyskiwać dostęp do tego interfejsu API?

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 Wyraż zgodę administratora dla katalogu ...

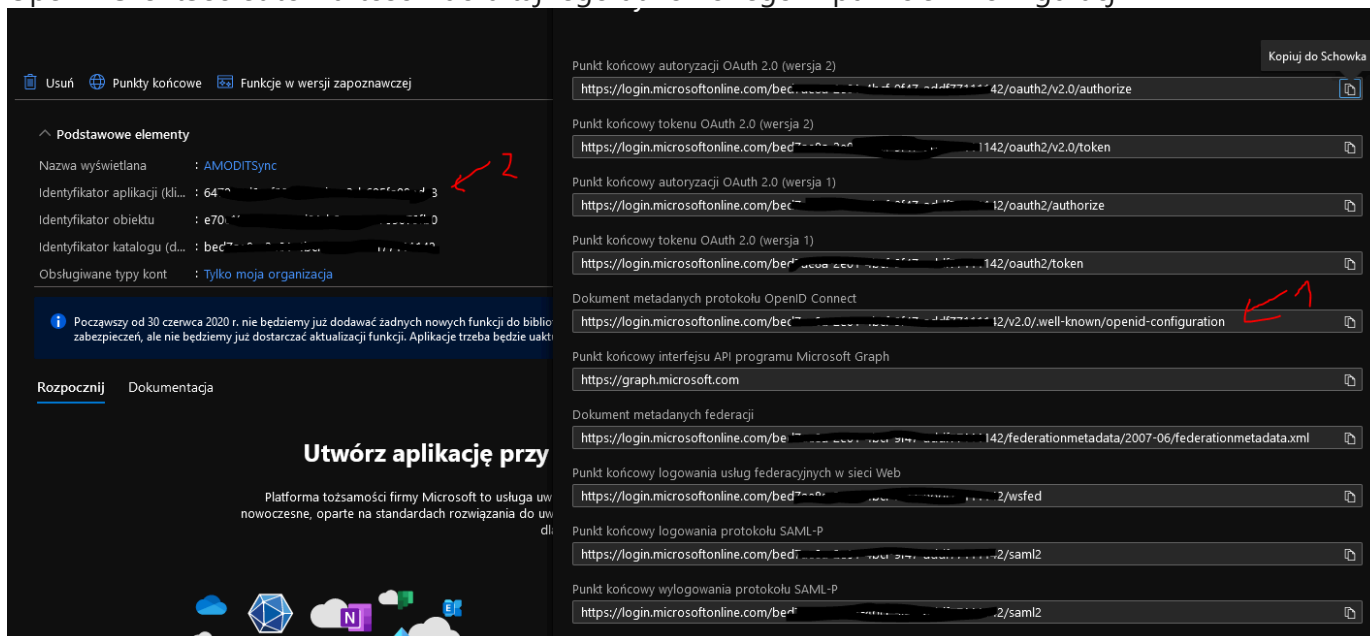


Konfiguracja logowania do AMODIT przy pomocy kont AzureAD

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

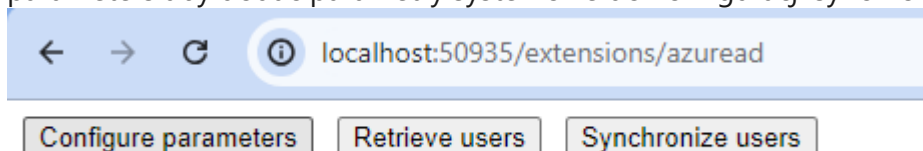
OpenID		
OpenIDConfigurationURL	https://login.microsoftonline.com/b1754394-2101-407d-b11d-8f5b5d1f1224	URL of OpenId configuration file
OpenIDClientid	dbf54394-2101-407d-b11d-8f5b5d1f1224	Clientid for OpenId provider
OpenIDRedirectURL	http://astrafox.amodit.com/formsanon/oauth2.aspx	URL of OpenId redirect page
OpenIDButtonText	Azure	Text on OpenId login button
OpenIDScope	User.Read	Scopes to retrieve from OpenId
OpenIDClientSecret	Usun wartość	OpenId client secret

- 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	
AzureAD.Tenant	REDACTED
AzureAD.ClientId	REDACTED
AzureAD.ClientSecret	REDACTED
AzureAD.FieldsMapping	<pre>[{ amodit: "UserSyncId", json: "id" }, { amodit: "UserLogin", json: "userPrincipalName" }, { amodit: "UserFirstName", json: "givenName" }, { amodit: "UserLastName", json: "surname" },]</pre> Mapping between Azure AD parameters and workflowuser columns
AzureAD.CreateUsersFrom	<pre>{ "groups": ["AMODIT Rozwój", "AMODIT Wdrożenia"] }</pre> Create only users from given list
AzureAD.ExcludeUsers	<pre>("userPrincipalName"!="EXT#"; "accountEnabled":"false")</pre> Regular expressions in json to check if user should not imported: (fieldName: regEx, ex: {"mail": "@cloud.onmicrosoft.com"})

- 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

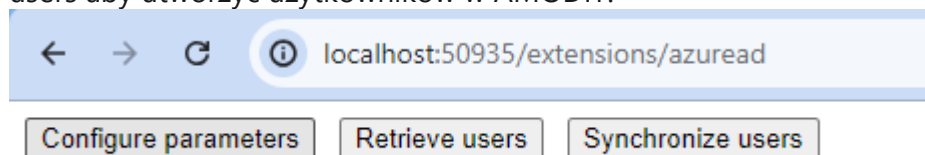
Wyklucza synchronizację użytkowników z ciągiem #EXT# w userPrincipalName oraz tych nie włączonych.

```
{ "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

AzureADSyncronizationJc	Inne	AMODITAzureAD.Jc	day	1
	AMODITAzureAD			

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:

Ustawienia główne	Administratorzy	Synchronizacja
Wykorzystanie grupy	Obszary grupy	

☐ Brak synchronizacji

☒ Lista członków grupy będzie synchronizowana z grupą w Active Directory

Nazwy grup AD

Rozdzielone przecinkiem nazwy grup AD, które będą synchronizowane z tą grupą AMODIT. Zamiast nazw grup można użyć pełnych ścieżek do grup AD, jednak muszą być rozdzielone średnikiem. Jeżeli pole jest puste to brana jest nazwa grupy AMODIT.