

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 [↗](#)

[Pulpit nawigacyjny](#) > [ASTRAFOX](#) >

Zarejestruj aplikację

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

 [↗](#)

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.

[↕](#) [↗](#)

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"

MODITSync

Certyfikaty i klucze tajne

Chcesz przesłać opinię?

Poświadczenia umożliwiają poufny aplikacjom identyfikowanie się w usłudze uwierzytelniania podczas odbierania tokenów w lokalizacji z adresem URL. W celu zapewnienia wyższego poziomu bezpieczeństwa zalecane jest używanie certyfikatu (zamiast klucza tajnego klienta).

Certyfikaty

Certyfikatów można używać jako kluczy tajnych do udowodnienia tożsamości aplikacji podczas żądania tokenu. Mogą być również określane jako klucze tajne.

Przełącz certyfikat

Odskok palca	Data rozpoczęcia	Wygasa	Identyfikator certyfikatu
Nie dodano certyfikatów dla tej aplikacji.			

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
Nie utworzono żadnych wpisów tajnych klienta dla tej aplikacji.			

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	16V...	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

Żądanie uprawnień interfejsu API

Wszystkie interfejsy API

- ThreatAssessment
 - ThreatIndicators
 - TrustFrameworkKeySet
 - UserAuthenticationMethod
 - UserNotification
 - UserShiftPreferences
- User (1)
 - User.Export.All (O) Export user's data Tak
 - User.Invite.All (O) Invite guest users to the organization Tak
 - User.ManageIdentities.All (O) Manage all users' identities Tak
 - User.Read.All (O) Read all users' full profiles Tak
 - User.ReadWrite.All (O) Read and write all users' full profiles Tak
- WindowsUpdates
- WorkforceIntegration

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

Potwierdzenie udzielenia zgody administratora.

Czy chcesz udzielić zgody na żądane uprawnienia dla wszystkich kont w ASTRAFOX? Spowoduje to zaktualizowanie wszelkich istniejących uprawnień dla katalogu ASTRAFOX w organizacji lub w organizacjach, w których będzie używana ta aplikacja. [Dowiedz się więcej](#)

Skonfigurowane uprawnienia

Aplikacje są autoryzowane do wywoływania interfejsów API po przyznaniu im uprawnień przez użytkowników/administratorów w ramach procesów skonfigurowanych uprawnień powinna zawierać wszystkie uprawnienia potrzebne aplikacji. [Dowiedz się więcej o uprawnieniach i zgodzie](#)

[+](#) Dodaj uprawnienie Wyraź zgodę administratora dla katalogu ASTRAFOX

Interfejs API / Nazwa uprawnień	Typ	Opis	Wymagana zgoda a...	Stan
Microsoft Graph (2)				
User.Read	Delegowa...	Loguj się i odczytuj profil użytkownika	Nie	
User.Read.All	Aplikacja	Read all users' full profiles	Tak	

Konfiguracja AMODIT

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

OpenID		
OpenIDConfigurationURL	<input type="text" value="https://login.microsoftonline.com/"/>	URL of OpenId configuration file
OpenIDClientid	<input type="text" value="dbf"/>	Clientid for OpenId provider
OpenIDRedirectURL	<input type="text" value="http://astrafox.amodit.com/formsanon/oauth2.aspx"/>	URL of OpenId redirect page
OpenIDButtonText	<input type="text" value="Azure"/>	Text on OpenId login button
OpenIDScope	<input type="text" value="User.Read"/>	Scopes to retrieve from OpenId
OpenIDClientSecret	<input type="text" value="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

The screenshot shows the 'Punkty końcowe' (Endpoints) configuration page in the Azure portal. On the left, under 'Podstawowe elementy', the 'Identyfikator aplikacji (kli...)' field is highlighted with a red arrow and the number '2'. The main area displays a list of endpoints, with the 'Dokument metadanych protokołu OpenID Connect' endpoint also highlighted with a red arrow. The endpoints listed include OAuth 2.0 authorization and token endpoints, OpenID Connect metadata, Microsoft Graph API, and SAML endpoints.

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

AzureAD		
AzureAD.Tenant	<input type="text" value="0d6c0c0c-2a..."/>	Azure AD tenant / catalog id
AzureAD.Clientid	<input type="text" value="b69a..."/>	Azure AD client id / application id
AzureAD.ClientSecret	<input type="text" value="Usun wartość"/>	Azure AD client secret
AzureAD.FieldsMapping	<pre>{ "amodit": "UserSynclid", "json": ["onPremisesSecurityIdentifier", "id"], "amodit": "UserSID", "json": ["onPremisesSecurityIdentifier"], "amodit": "UserLogin", "json": ["onPremisesSamAccountName", "userPrincipalName"], "amodit": "UserFirstName", "json": ["givenName"], "amodit": "UserLastName", "json": ["surname"] }</pre>	Mapping between Azure AD parameters and workflowuser columns
AzureAD.CreateUsersFromOU	<input type="text" value="OU=Users,OU=AT,OU=Countries,DC=a..."/>	Create only users from given OU list
AzureAD.EnableUsersFromOU	<input type="text" value="OU=Users,OU=AT,OU=Countries,DC=a..."/>	Enable only users from given OU list
AzureAD.ExcludeUsers	<input type="text" value="(&mail=@...;!(mail=@cloud.onmicrosoft.com))"/>	Regular expressions to check if user should not be 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.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.