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

Pulpit nawigacyjny > ASTRAFOX >
Zarejestruj aplikację 🖤
* Nazwa
Nazwa wyświetlana tej aplikacji widoczna dla użytkowników (można ją później zmienić).
AMODITSvnc
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 V https://astrafox.amodit.com/formsanon/oauth2.aspx V
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 wpis tajny" i dodać "Nowy klucz tajny klienta"

Opis MADDITSync Poświadczenia umożliwiają poufnym aplikacjom identyfikowanie się w usłudze uwierzytelniania podczas odbierania tokenów w lokalizacji z adr Wygasa Załecane: 6 miesięcy Poświadczenia umożliwiają poufnym aplikacjom identyfikowanie się w usłudze uwierzytelniania podczas odbierania tokenów w lokalizacji z adr Wygasa Załecane: 6 miesięcy Certyfikaty Certyfikaty Certyfikaty Kłucze tajnek kliuczy tajnych do udowadniania tożsamości aplikacji podczas żądania tokenu. Mogą być również odreślane ja Kłucze tertyfikat Certyfikaty Medoino certyfikatow można używać jako kluczy tajnych do udowadniania tożsamości aplikacji podczas żądania tokenu. Mogą być również odreślane ja Kłucze tajne klienta Kłucze tajne klienta Ciąz klucza tajnego, którego aplikacja używa, aby potwierdzić śwoją tożsamość podczas żądania tokenu. Może być również określany jako ha Hentyfikator remie Opis Wygasa Watość Identyfikator remie Opis Wygasa Watość Identyfikator remie	DITSync fikatv i klucze taine	<u>,</u> , ,				Dodaj klucz t	ajny klienta
Checsz przesłać opinię? Poświadczenia umożliwiąją poufnym apilkacjom identyfikowanie się w usłudze uwierzytelniania podczas odbierania tokenów w lokalizacji z adr trzyciu schematu HTTPS). W celu zapewnienia wyższego poziomu bezpieczeństwa zalecane jest używanie certyfikatu (zamiast klucza tajnego kli Certyfikaty Certyfikaty Certyfikaty Przekaż certyfikat Odcisk palca Odcisk palca Odcisk palca Odcisk palca Odcisk palca Klucze tajne klienta Ciąg klucza tajnego, którego apilkacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jało hu Muże tajnek klienta Ciąg klucza tajnego, którego apilkacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jało hu Opis Mygasa Martość Martość Martość Identyfikator wpisu						Opis	AMODITSync
Posku za na p	💛 Chcesz przesłać opinię?					Wygasa	Zalecane: 6 missiery
Certyfikatý certyfikatów można używać jako kluczy tajnych do udowadniania tożsamości aplikacji podczas żądania tokenu. Mogą być również określane je r Przekaż certyfikat odcisk palca Data rozpoczęcia Wygasa Identyfikator certy Klucze tajne klienta Ciąg klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako ha opis Wygasa Wartość Identyfikator wpisu	Poświadczenia umożliwiają pouf użyciu schematu HTTPS). W celu	nym aplikacjom identyfikowanie się v zapewnienia wyższego poziomu be	w usłudze uwierzytelniania zpieczeństwa zalecane jes	podczas odbierani t używanie certyfikat	a tokenów w lokalizacji z adr u (zamiast klucza tajnego kli		zanzemen z miestęsy
certyfikatów można używać jako kluczy tajnych do udowadniania tożsamości aplikacji podczas żądania tokenu. Mogą być również określane je	Certyfikaty						
Przekaż certyfikat Odcisk palca Data rozpoczęcia Wygasa Identyfikator certy 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 ha Powy klucz tajny klienta Opis Wygasa Martość	Certyfikatów można używać jako	kluczy tajnych do udowadniania toż	samości aplikacji podczas	i żądania tokenu. M	ogą być również określane ja		
Oddisk palca Data rozpoczęda Wygasa Identyfikator certy Nie dodano certyfikatów dla tej aplikacji. Klucze tajne klienta Klucze tajne klienta Klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako ha + Nowy klucz tajny klienta Opis Wygasa Wartość	↑ Przekaż certyfikat						
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 ha + Nowy klucz tajny klienta Opis Wygasa Watość Identyfikator wpisu	Odcisk palca		Data rozpoczęcia	Wygasa	Identyfikator certy		
Klucze tajne klienta Ciąg klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako ha + Nowy klucz tajny klienta Opis Wygasa Wartość Identyfikator wpisu	Nie dodano certyfikatów dla tej	aplikacji.					
Ciąg klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako ha + Nowy klucz tajny klienta Opis Wygasa Wartość Identyfikator wpisu	Klucze tajne klienta						
+ Nowy klucz tajny klienta Opis Wygasa Wartość Identyfikator wpisu	Ciąg klucza tajnego, którego apl	ikacja używa, aby potwierdzić swoją	tożsamość podczas żąda	inia tokenu. Może bj	vć również określany jako ha		
Opis Wygasa Wartość Identyfikator wpisu	+ Nowy klucz tajny klienta						
	Opis	Wygasa	Wartość		Identyfikator wpisu		

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	v potwierdzić swoją to	rżsamość podczas żądania tokenu. Może być rów	mież 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)

Ħ	Asystent integracji	Przepływy niejawnego przyznania i hybrydowe
Za	rządzaj	Żądaj tokenu bezpośrednio z punktu końcowego autoryzacji. Jeśli aplikacja ma architekturę jednostronicową i nie
	Znakowanie i właściwości	zarówno tokeny dostępu, jak i tokeny identyfikatorów. W przypadku aplikacji internetowych ASP.NET Core i innych
Э	Uwierzytelnianie	aplikacji internetowych używających uwierzytelniania hybrydowego wybierz tylko tokeny identyfikatorów. Dowiedz się więcej o tokenach.
Ŷ	Certyfikaty i klucze tajne	Wybierz tokeny, które mają być wystawiane przez punkt końcowy autoryzacji:
ili	Konfiguracja tokenu	🔽 Tokeny dostępu (używane na potrzeby niejawnych przepływów)
.	Uprawnienia interfejsu API	🗌 Tokeny identyfikatorów (używane na potrzeby niejawnych i hybrydowych przepływów)
	Uwidocznij interfejs API	Obsługiwane typy kont
	Role aplikacji	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.

		Żądanie uprawnień interfejsu API	
	wnienia interfejsu API 👒 \cdots		
	🖒 Odśwież 📔 🛇 Chcesz przesłać opinię?	Kuzystke interfejsy API AnneatAssessment AnneatAssessmen	
矏 Przegląd		> Threatindicators	
🖴 Szybki start 💉 Asystent integracji	(i) Kolumna "Wymagana zgoda administratora" zawiera wartość domyślną dla organizacji. Jednak zg organizacji lub w organizacjach, w których będzie używana ta aplikacja. Dowiedz się więcej	> TrustFrameworkKeySet	
Zarządzaj	Skonfigurowane uprawnienia	> UserAuthenticationMethod	
 Znakowanie Uwierzytelnianie 	Aplikacji są autoryzowane do wywoływania interfejsów API po przyznaniu im uprawnień przez u skonfigurowanych uprawnień powinna zawierać wszystkie uprawnienia potrzebne aplikacji. Dowi	UserNotification	
Y Certyfikaty i klucze tajne	🕂 Dodaj uprawnienie 🗸 Wyraź zgodę administratora dla katalogu ASTRAFOX	> UserShiftPreferences	
Konfiguracja tokenu	Interfejs API / Nazwa uprawnień Typ Opis		
Oprawnienia interfejsu API			
lwidocznij interfejs API	User.Read Delegowa Loguj się i odczytuj profil użytkownika	User.Export.All O Tak Tak	
u Role aplikacji		User.Invite All O	
Właściciele	Aby wyświetlać uprawnienia i zgodę użytkownika oraz zarządzać nimi, spróbuj użyć obszaru Apl	Invite guest users to the organization	
Role i administratorzy Wersja zapoznawcza		User.Manageldentities.All O Tak Manage all users' identities	
Manifest		User.Read.All O Read all users' full profiles Tak	
Pomoc techniczna i rozwiązywanie		User.ReadWrite.All O Bead and write all users' full profiles Tak	
Ø Rozvizzywanie problemów		Windows Indator	
		/ Windowsopoates	
techniczną		> WorldorceIntegration	

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

💍 Odśwież 📔 🛇 Chcesz przesłać opinię?					
Potwierdzenie udzielenia z	gody adm	ninistratora.			
Czy chcesz udzielić zgody na żądane	e uprawnienia	a dla wszystkich kont w ASTRAFOX? Spowoduje to zaktuali	zowanie wszelkich istniej	ącyc	
Tak Nie					
organizacji lub w organizacjach, v	v których będzi	e używana ta aplikacja. Dowiedz się więcej		_	
Skonfigurowane uprawnienia Aplikacje są autoryzowane do wywoływania interfejsów API po przyznaniu im uprawnień przez użytkowników/administratorów w ramach proce 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 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/bg/12-02-04-04-04-04-04-04-04-04-04-04-04-04-04-
OpenIDClientId	dbfeyry
OpenIDRedirectURL	http://astrafox.amodit.com/formsanon/oauth2.aspx
OpenIDButtonText	Azure
OpenIDScope	User.Read
OpenIDClientSecret	
	Usuń wartość

URL of OpenId configuration file ClinetId for OpenId provider URL of OpenId redirect page Text on OpenId login button Scopes to retrieve from OpenId 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

	Punkt końcowy autoryzacji OAuth 2.0 (wersja 2)	Kopiuj do Schowka
📋 Usuń 🜐 Punkty końcowe 🔤 Funkcje w wersji zapoznawczej	https://login.microsoftonline.com/bec.usuu 2000 46 of an additionary additionary 42/oauth2/v2.0/authorize	D
A Rodstaugurg domontu	Punkt końcowy tokenu OAuth 2.0 (wersja 2)	
	https://login.microsoftonline.com/bed700a0	ß
Nazwa wyświetlana : AMODITSync	Bunk haf anna ait anna a' O tath 2.0 fannia th	
Identyfikator aplikacji (kli 🗄 6470 👘 🖅 👘 👘 👘 👘 🕹 soci-oc 🚽 3 🧏	Punkt koncowy autoryzacji OAuth 2.0 (wersja 1)	
Identyfikator objektu : e70.1	https://login.microsoftonline.com/bec	<u> </u>
Identyfikator katalogu (d., . ; bed 2 - 0 - 0 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	Punkt końcowy tokenu OAuth 2.0 (wersja 1)	
	https://login.microsoftonline.com/bed ^t ucca_zev rated the https://login.microsoftonline.com/bedtucca_zev ra	ĥ
obsugiwane typy kont in tyrko moja organizacja	Dokument metadanych protokołu OpeniD Connect	
Począwszy od 30 czerwca 2020 r. nie będziemy już dodawać żadnych nowych funkcji do biblio	https://login.microsoftonline.com/bec 🗂 ն 💷 👘 bei star - 🖓 🖓 🖓 https://login.microsoftonline.com/bec 🦷 🕻	
zabezpieczeń, ale nie będziemy już dostarczać aktualizacji funkcji. Aplikacje trzeba będzie uakti	Punkt końcowy interfejsu API programu Microsoft Graph	
Rozpocznii Dokumentacia	https://graph.microsoft.com	ũ
	Dokument metadanych federacji	
Uterséen an Rive at a more	https://login.microsoftonline.com/be/11112.cov/loci/9142/clili111142/federationmetadata/2007-06/federationmet	adata.xml 🗈
Utworz aplikację przy	Punkt końcowy logowania usług federacyjnych w sieci Web	
Platforma tożsamości firmy Microsoft to usługa uw	https://login.microsoftonline.com/bed7oo0	D
nowoczesne, oparte na standardach rozwiązania do uw dli	Punkt końcowy logowania protokołu SAML-P	
	https://login.microsoftonline.com/bedTTvor_siter_addi	D
	Punkt końcowy wyłogowania protokołu SAML-P	
	https://login.microsoftonline.com/bed	ß

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		Azure AD tenant / catalog id
AzureAD.ClientId		Azure AD client id / application id
AzureAD.ClientSecret		Azure AD client secret
AzureAD.FieldsMapping	Usuń wartość [{ amodit: "UserSyncid", json: "id"}, { amodit: "UserSyncid", json: "serPrincipalName"}, { amodit: "UserFirstName", json: "givenName" }, { amodit: "UserLastName", json: "surname" }, }	Mapping between Azure AD parameters and workflowuser columns
AzureAD.CreateUsersFrom	"groups":["AMODIT Rozwój", "AMODIT Wdrożenia"] }	Create only users from given list
AzureAD.ExcludeUsers	("userRrincipalName":"#EXT#", "accountEnabled":"false")	Regular expresions 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: "UserLocation", json: "mobilePhone" },
{ amodit: "UserIsBlocked", json: "accountEnabled", op: "!"},
{ amodit: "UserEmployeeId", json: "employeeId" },
{ amodit: "UserManager", json: "manager", expand: true}
```

 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

O

D

częstotliwość według uzna	nia			
AzureADSynchronizationJ	Inne	AMODITAzureAD.Jc	day 🗸	1

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 synchronizacj	ji		
Lista członków gru	py będzie synchroni	zowana z grupą w Ac	tive Directory
Nazwy grup /	AD Azure	AMODIT Rozwój	
Rozdzielone przec AMODIT. Zamiast i być rozdzielone śr AMODIT.	inkiem nazwy grup nazw grup można uż ednikiem. Jeżeli pol	AD, które będą synch tyć pełnych ścieżek d le jest puste to brana	ironizawane z tą grupą o grup AD, jednak muszą jest nazwa grupy