



Administracja systemów komputerowych

Sample Web application with federated
authentication and identity management

Adam Samsonowicz
Kacper Kwapisz

1. Cel projektu

Celem projektu jest pokazanie integracji prostej aplikacji webowej z zewnętrznym serwerem do autentykacji.

2. Opis działania aplikacji

Aplikacja ma na celu wyświetlenia informacji o profilu użytkownika(ROLE_USER) oraz wylistowania wszystkich zarejestrowanych użytkowników dla administratora(ROLE_ADMIN).

User Profile

- [Home](#)
- [Users](#)
-
- User:

Details

UserId	User details	Email	First Name	Last Name
fa61d1b6-4747-425f-a4cc-38663cbfc829	Default details for default profile	pies@gmail.com	Admin	Systemowy

Rys1. Wyświetlony profil użytkownika

User Profile

- [Home](#)
- [Users](#)
-
- User:

Users

First Name	Last Name	Email
Adam	Samsonowicz	adamsam1412@gmail.com
AdamTest	Samsonowicz	eeeeeeeeee2@gmail.com
Admin	Systemowy	pies@gmail.com

Rys2. Lista użytkowników dostępna dla administratora

←

→

↻

localhost:8082/users

User Profile

• [Home](#)

• [Users](#)

• [logout](#)

User:

You are not permitted to view this content, please go back to your profile.

[My Profile](#)

Rys3. Użytkownik bez roli administratora nie ma prawa do wyświetlenia listy użytkowników

3.Konfiguracja serwera do autentykacji

AdminSys

General

Login

Keys

Email

Themes

Localization

Cache

Tokens

Client Registration

Security Defenses

* Name

AdminSys

Display name

HTML Display name

Frontend URL ⓘ

Enabled ⓘ

ON

User-Managed Access ⓘ

OFF

Endpoints ⓘ

OpenID Endpoint Configuration














SAML 2.0 Identity Provider Metadata

Save

Cancel

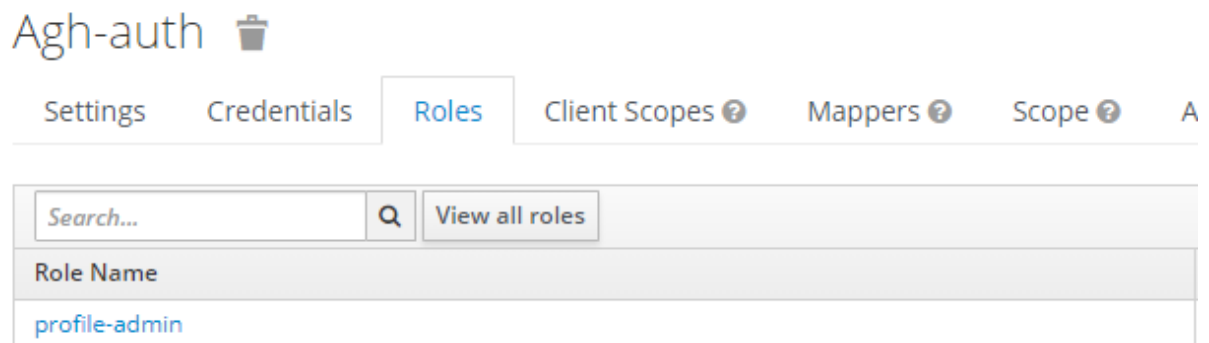
Rys4. Realm na cele projektu

Agh-auth

[Settings](#)[Credentials](#)[Roles](#)[Client Scopes !\[\]\(e78f798d4ea5c530c9db49e7d26e6b95_img.jpg\)](#)[Mappers !\[\]\(23d9fc146e83b5c3013cfa32c784f8d5_img.jpg\)](#)[Scope !\[\]\(c694a3ff3b077d76910920a6a1593ab4_img.jpg\)](#)[Authoriza](#)Client ID Name Description Enabled ☒ ONAlways Display in Console ☐ OFFConsent Required ☐ OFFLogin Theme Client Protocol Access Type Standard Flow Enabled ☒ ONImplicit Flow Enabled ☐ OFFDirect Access Grants Enabled ☐ OFFService Accounts Enabled ☒ ONAuthorization Enabled ☒ ONRoot URL * Valid Redirect URIs Base URL Admin URL Web Origins Backchannel Logout URL Backchannel Logout Session Required ☒ ONBackchannel Logout Revoke Offline Sessions ☐ OFF

Rys5. Client dla aplikacji webowych

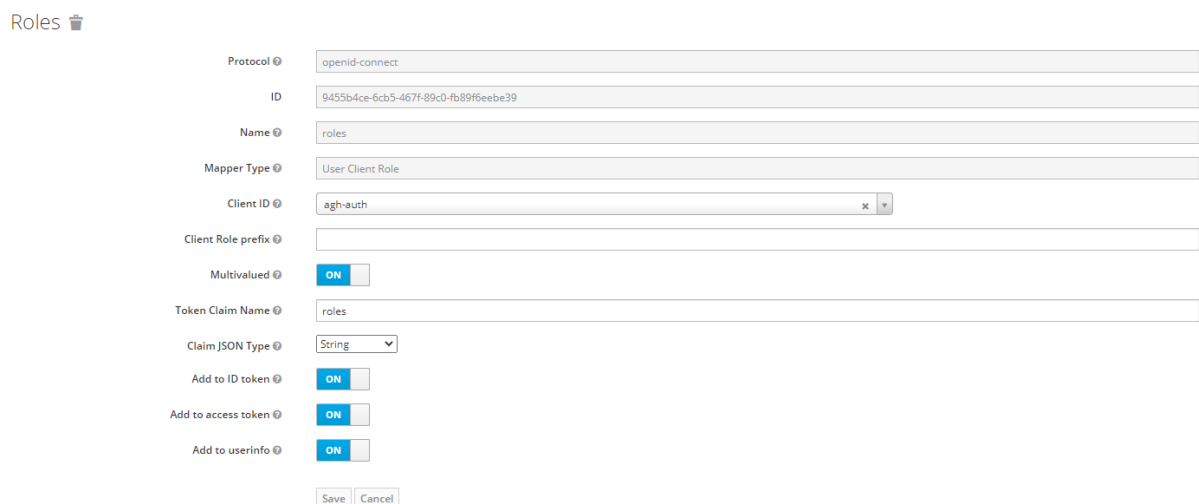
Klient korzysta z protokołu openid-connect



The screenshot shows the 'Agh-auth' application interface. At the top, there is a navigation bar with tabs: 'Settings', 'Credentials', 'Roles' (selected), 'Client Scopes', 'Mappers', 'Scope', and 'A'. Below the navigation bar, there is a search bar with the text 'Search...' and a magnifying glass icon, followed by a 'View all roles' button. Below this, there is a table with the header 'Role Name'. The table contains one entry: 'profile-admin'.

Rys6. Role klienta

Rola profile-admin jest kolejno mapowana na poziomie aplikacji w celu przydzielenia dostępu dla administratora.



The screenshot shows the 'Roles' configuration page. The page has a title 'Roles' with a trash icon. Below the title, there are several configuration fields: 'Protocol' (openid-connect), 'ID' (9455b4ce-6cb5-467f-89c0-fb89f6eebe39), 'Name' (roles), 'Mapper Type' (User Client Role), 'Client ID' (agh-auth), 'Client Role prefix' (empty), 'Multivalued' (ON), 'Token Claim Name' (roles), 'Claim JSON Type' (String), 'Add to ID token' (ON), 'Add to access token' (ON), and 'Add to userinfo' (ON). At the bottom, there are 'Save' and 'Cancel' buttons.

Rys7. Role mapping

Role mapping służy do doklejenia claim'u 'roles' do tokena.

Adamsam1412@gmail.com 

Details Attributes Credentials **Role Mappings** Groups Consents Sessions Identity Provider Links

Realm Roles	<div>Available Roles ⓘ</div> <div></div> <div>Add selected ></div>	<div>Assigned Roles ⓘ</div> <div>offline_access uma_authorization</div> <div><< Remove selected</div>
Client Roles	<div>agh-auth</div> <div>Available Roles ⓘ</div> <div>profile-admin uma_protection</div> <div>Add selected ></div>	<div>Assigned Roles ⓘ</div> <div></div> <div><< Remove selected</div>

Rys8. Role mapping zwykłego usera

Zwykły user nie ma roli profile-admin.

Sysadmin 

Details Attributes Credentials **Role Mappings** Groups Consents Sessions Identity Provider Links

Realm Roles	<div>Available Roles ⓘ</div> <div></div> <div>Add selected ></div>	<div>Assigned Roles ⓘ</div> <div>offline_access uma_authorization</div> <div><< Remove selected</div>
Client Roles	<div>agh-auth</div> <div>Available Roles ⓘ</div> <div>uma_protection</div> <div>Add selected ></div>	<div>Assigned Roles ⓘ</div> <div>profile-admin</div> <div><< Remove selected</div>

Rys9. Role mappings administratora

Administrator ma role profile-admin.

Konfiguracja pomiędzy Okta a KeyCloak

oktaoidc

Settings Mappers

Redirect URI ⓘ	http://localhost:8081/auth/realms/AdminSys/broker/oktaoidc/endpoint
* Alias ⓘ	oktaoidc

Rys10. Redirect URI w keycloak

LOGIN

Sign-in redirect URIs ?	http://localhost:8081/auth/realms/AdminSys/broker/oktaoidc/endpoint
Sign-out redirect URIs ?	http://localhost:8080
Login initiated by	App Only
Initiate login URI ?	http://localhost:8080/authorization-code/callback

Rys11. Redirect URI w serwisie okta

▼ OpenID Connect Config ?

* Authorization URL ?	<input type="text" value="https://dev-56649284.okta.com/oauth2/default/v1/authorize"/>
Pass login_hint ?	<input type="checkbox"/> OFF
Pass current locale ?	<input type="checkbox"/> OFF
* Token URL ?	<input type="text" value="https://dev-56649284.okta.com/oauth2/default/v1/token"/>
Logout URL ?	<input type="text" value="https://dev-56649284.okta.com/oauth2/default/v1/logout"/>
Backchannel Logout ?	<input type="checkbox"/> OFF
Disable User Info ?	<input type="checkbox"/> OFF
User Info URL ?	<input type="text"/>
* Client Authentication ?	<input type="text" value="Client secret as jwt"/>
* Client ID ?	<input type="text" value="0oaqjqz6y9ubrHtK15d6"/>
* Client Secret ?	<input type="password" value="....."/>

Rys12. OpenID Connect konfiguracja w keycloak

Konfigurację można wykonać na podstawie informacji z utworzonej aplikacji w okta.

Client Credentials

[Edit](#)

Client ID

Ooaqjqz6y9ubrHtK15d6



Public identifier for the client that is required for all OAuth flows.

Client secret

.....



Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.

Rys13. ClientID oraz Client secret aplikacji okta.

```
{
  "issuer": "https://dev-56649284.okta.com/oauth2/default",
  "authorization_endpoint": "https://dev-56649284.okta.com/oauth2/default/v1/authorize",
  "token_endpoint": "https://dev-56649284.okta.com/oauth2/default/v1/token",
  "userinfo_endpoint": "https://dev-56649284.okta.com/oauth2/default/v1/userinfo",
  "registration_endpoint": "https://dev-56649284.okta.com/oauth2/v1/clients/0oaqjqz6y9ubrHtK15d6",
  "jwks_uri": "https://dev-56649284.okta.com/oauth2/default/v1/keys",
}
```

Rys14. Pomocny endpoint do konfiguracji zapewniany przez okta.

2FA realizowany przy pomocy Google Authenticator, są również inne opcje do wyboru.









Multifactor

Factor Types

Factor Enrollment


Okta Verify	<h3>Google Authenticator</h3> <p>After configuring this factor, users signing in to Okta see that extra verification is required. If Google Authenticator is selected they will be instructed to download the Google Authenticator App. Once installed, the user will be prompted to enter the generated six digit number to gain access.</p> <div>Active ▾</div>
SMS Authentication	
✔ Google Authenticator	
FIDO2 (WebAuthn)	
Symantec VIP	
On-Prem MFA	
RSA SecurID	
Email Authentication	

Rys15. Multifactor konfiguracja w okta.


Priority	Rule name	Status	Actions
1  	2FA RUIE	Active	 
CONDITIONS		ACTIONS	
 User assigned this app		 Require multifactor every sign on	
 Anywhere			
 Any client			

Rys16. SignOn Policy na poziomie aplikacji w okna.

Dla celów prezentacji wybraliśmy wymaganie 2FA przy każdym logowaniu.

 ACCESS

When all the conditions above are met, sign on to this application is: Allowed ▾

☐ Prompt for re-authentication 

☒ Prompt for factor · [Multifactor Settings](#)

☒ Every sign on

☐ Once per session

☐ Once a day


☐ Once a week

☐ Once a month

☐ Once per six months

☐ Only once


Rys17. Wszystkie możliwości zarządzania 2FA

 PEOPLE

Who does this rule apply to?

☒ Users assigned this app

☐ The following groups and users:


 LOCATION

If the user is located:

☒ Anywhere

☐ In Zone

☐ Not in Zone

 CLIENT

Note: The user-agent from the access request

If the user's platform is any of these:

Mobile

☒ iOS

☒ Android

☒ Other mobile (e.g. BlackBerry)

Desktop

☒ Windows

☒ macOS

☒ Other desktop (e.g. Linux)

Rys18. Bardziej specyficzne konfiguracje 2FA

Administrator może dostosować konfigurację logowania dla celów bezpieczeństwa. Przykładowo jeżeli użytkownicy firmy korzystają tylko z systemu Windows nie ma potrzeby dawania możliwości logowania się z innych systemów operacyjnych.