

# SSO IMPLEMENTATIE

Dit document legt uit hoe je een Single Sign On inlogmethode kunt implementeren voor New Heroes Academy. Wij maken voor Single Sign On gebruik van OpenID.

## BENODIGDE GEGEVENS

Om de SSO-koppeling op te zetten ontvangen we graag de volgende gegevens:

1. Naam identity provider waarvan gebruik wordt gemaakt (bijv. MS Entra)
2. Authority URL (bijv. MS Entra: <https://login.microsoftonline.com/<Tenant-ID>>)
3. Client (Application) Id
4. Client secret

## VOORBEREIDINGEN

Nadat wij bovenstaande punten hebben ontvangen, ontvang je van ons de 3 URL's die nodig zijn voor de SSO-koppeling:

Redirect URL/ Callback URL	<a href="https://klantnaam.newheroes.com/signin-oidc/providernaam">https://klantnaam.newheroes.com/signin-oidc/providernaam</a>
Remote signout	<a href="https://klantnaam.newheroes.com/signout-oidc/providernaam">https://klantnaam.newheroes.com/signout-oidc/providernaam</a>
Sign out callback URL / Front channel logout URL	<a href="https://klantnaam.newheroes.com/signout-callback-oidc/providernaam">https://klantnaam.newheroes.com/signout-callback-oidc/providernaam</a>

## IMPLEMENTATIE MET MICROSOFT

Bij het instellen van de SSO-koppeling met Microsoft Entra kunnen deze stappen gevolgd worden:

1. Ga naar Azure -> Microsoft Entra ID
2. Klik op de '+ Add' knop en kies voor 'App registration'.
3. Kies een naam, bij het kopje 'Redirect URL (optional)' kies voor platform Web uit de dropdown en vul de redirect URL in die is aangeleverd door New Heroes Academy. Bevestig dit met de register knop. (Zie screenshot)

Microsoft Azure | Search resources, services, and

Home > New Heroes | App registrations > Register an application

**Name**  
The user-facing display name for this application (this can be changed later).  
My New Heroes

**Supported account types**  
Who can use this application or access this API?  
 Accounts in this organizational directory only (New Heroes only - Single tenant)  
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)  
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)  
 Personal Microsoft accounts only  
[Help me choose...](#)

**Redirect URI (optional)**  
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.  
 Web | https://klantnaam.newheroes.com/signin-oidc/nh\_onmicrosoft

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

**Register**

- Ga in het linker menu naar Manage -> Certificates & secrets. Klik hier op de '+ New client secret' knop.
- Vul een description en expiration datum in en klik op de Add knop.
- Kopieer de waarde van de client secret. (Zie screenshot)

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
My New Heroes 24-06	12/21/2024	f~m8Q~zZEh1AEjclNpeTbM3CHIsu3rAL...	02a4eafc-8fe0-407f-aa0b-15f40f481afa

- Ga in het linker menu naar Manage -> Authentication. Vink daarna bij 'Implicit grant and hybrid flows' het vakje aan voor 'ID Tokens'. (Zie screenshot)

Home > New Heroes | App registrations > My New Heroes

**My New Heroes | Authentication**

Search | Got feedback?

Overview  
Quickstart  
Integration assistant  
Diagnose and solve problems  
Manage  
Branding & properties  
**Authentication**  
Certificates & secrets  
Token configuration  
API permissions  
Expose an API  
App roles  
Owners  
Roles and administrators  
Manifest  
Support + Troubleshooting

**Front-channel logout URL**  
This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.  
e.g. https://example.com/logout

**Implicit grant and hybrid flows**  
Request a token directly from the authorization endpoint. If the application has a single-page architecture (SPA) and doesn't use the authorization code flow, or if it invokes a web API via JavaScript, select both access tokens and ID tokens. For ASP.NET Core web apps and other web apps that use hybrid authentication, select only ID tokens. [Learn more about tokens.](#)

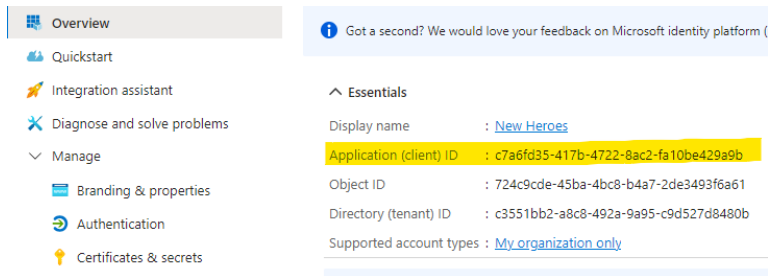
Select the tokens you would like to be issued by the authorization endpoint:  
 Access tokens (used for implicit flows)  
 ID tokens (used for implicit and hybrid flows)

**Supported account types**  
Who can use this application or access this API?  
 Accounts in this organizational directory only (New Heroes only - Single tenant)  
 Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)  
[Help me decide...](#)

**Advanced settings**  
Save Discard

Due to temporary differences in supported functionality, we don't recommend enabling personal Microsoft accounts for an existing registration. If you need to enable personal accounts you can do so using the manifest editor. [Learn more about these restrictions.](#)

- Ga in het linker menu naar overview. Hier is het application (client) ID te vinden. Deel dit samen met de waarde van de client secret met New Heroes Academy.



Overview

Got a second? We would love your feedback on Microsoft identity platform (

Essentials

Display name : [New Heroes](#)

Application (client) ID : **c7a6fd35-417b-4722-8ac2-fa10be429a9b**

Object ID : 724c9cde-45ba-4bc8-b4a7-2de3493f6a61

Directory (tenant) ID : c3551bb2-a8c8-492a-9a95-c9d527d8480b

Supported account types : [My organization only](#)

## ACTIES NA DE KOPPELING

Wanneer dit is goed gegaan hebben we een werkende SSO-koppeling met New Heroes Academy. Wanneer je met de browser naar de URL van je omgeving gaat zal je worden doorgestuurd naar je eigen login pagina. Hierna zal je ingelogd worden doorgestuurd naar de website van New Heroes Academy.

Voorbeeld url: <https://klantnaam.newheroes.com>

## VERVAL DATUM CLIENT SECRET

Bij het instellen van de client secret wordt een vervaldatum ingesteld. Zorg ervoor dat New Heroes Academy tijdig wordt geïnformeerd wanneer deze moet worden bijgewerkt. Het is mogelijk om meerdere secrets tegelijkertijd actief te hebben om zo de continuïteit te waarborgen.

## HULP NODIG?

Neem contact op met onze Customer Support, mail naar [customersupport@newheroes.com](mailto:customersupport@newheroes.com) of bel 0418 682 888.