Walkthrough: Wordpress-Seite via OAuth an die MiData anbinden

Was ist OAuth?

Hitobito ist ein OAuth 2.0-Anbieter, was bedeutet, dass eine externe Anwendung Benutzer*innen über hitobito authentifizieren kann (normalerweise in Form einer "Login via hitobito"-Funktion, ähnlich wie bei Google und Facebook usw.). In dieser Anleitung lernst du, wie du das MiData-Login für deine Wordpress-Seite verwenden kannst.

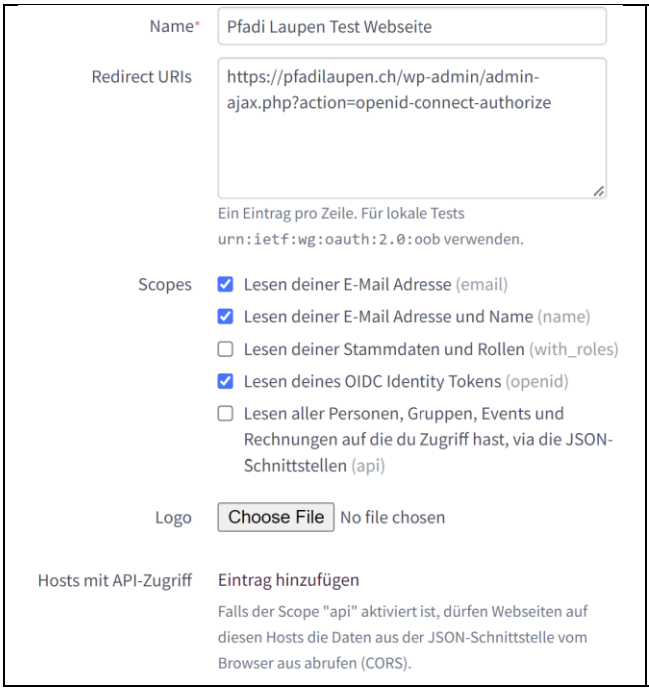
Testsystem verwenden

Immer wenn du an einer Schnittstelle zur MiData arbeitest, solltest du dein Vorhaben zuerst auf dem Testsystem der MiData ausprobieren. So merkst du beispielsweise, wenn deine Applikation einen Fehler auf dem System verursacht oder wenn du ein ganz anderes Plugin einsetzen musst.

Mehr Infos zum Testsystem findest du im F.A.Q.

Konfiguration der OAuth App im MiData

Eine neue OAuth-Applikation in MiData erstellen: https://pbs.puzzle.ch/de/oauth/applications

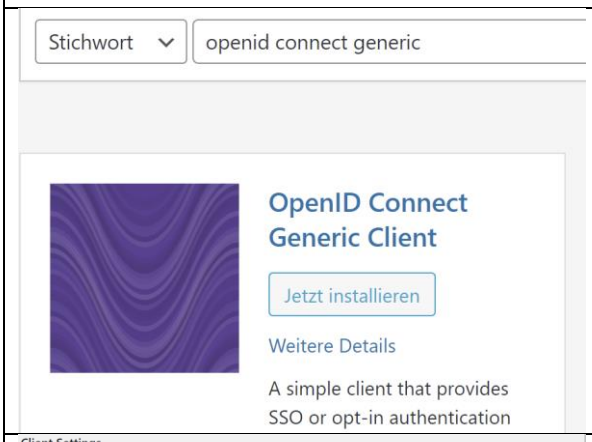


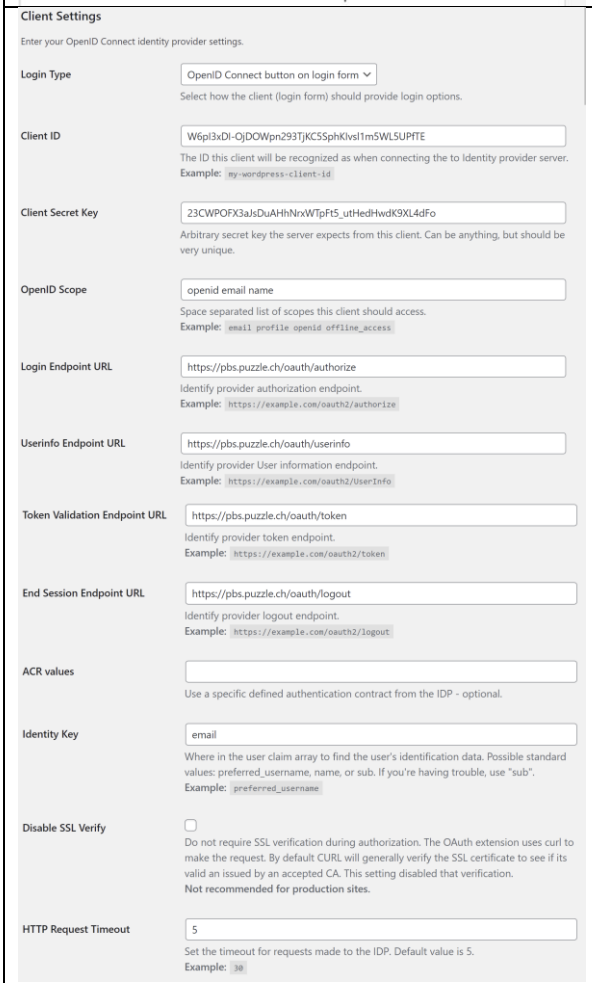
Folgende Informationen müssen dafür angeben werden

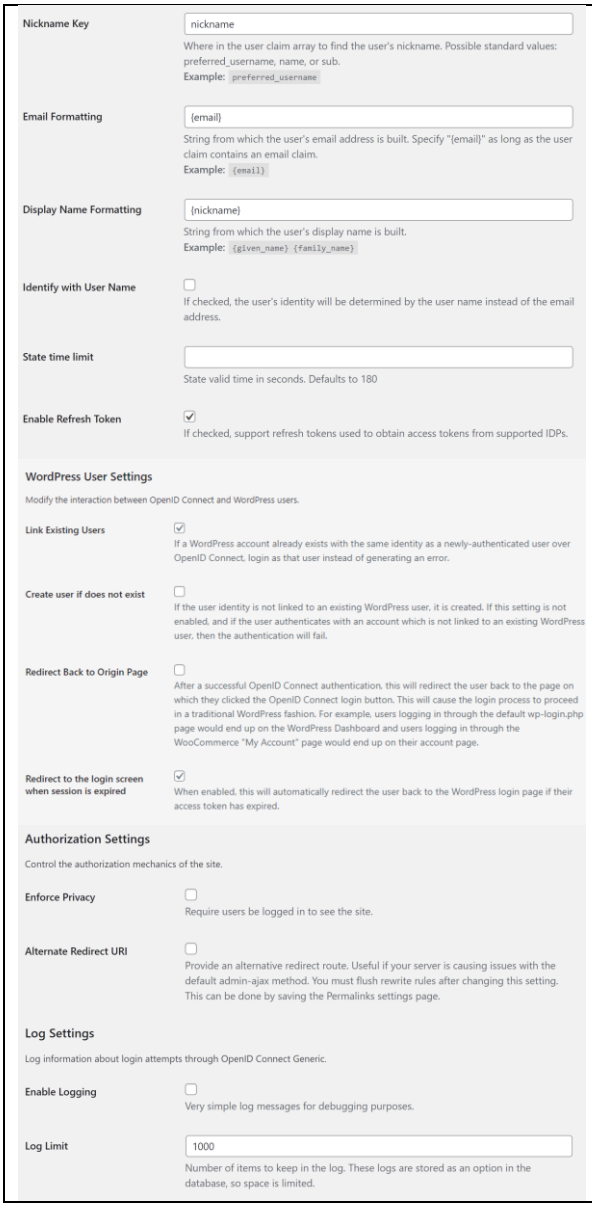
- Name der Applikation
- Redirect URIs
- Scopes

Installation und Konfiguration des Wordpress Plugins

Sobald die OAuth Applikation erstellt wurde, kann Wordpress als OAuth Client angebunden werden. Dafür ist die Installation und Konfiguration eines zusätzlichen Plugins notwendig.

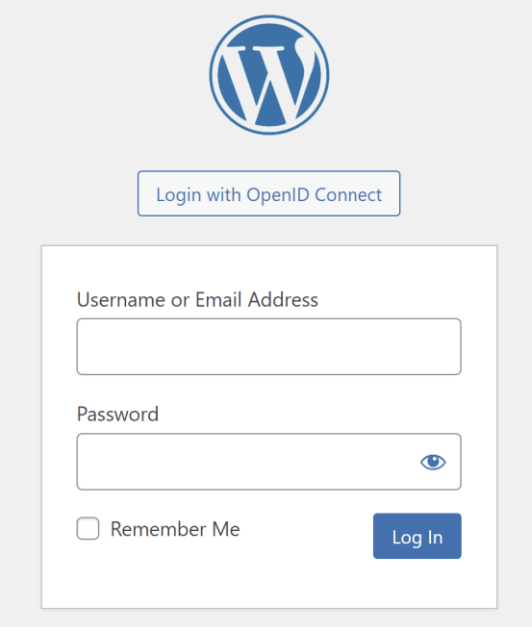
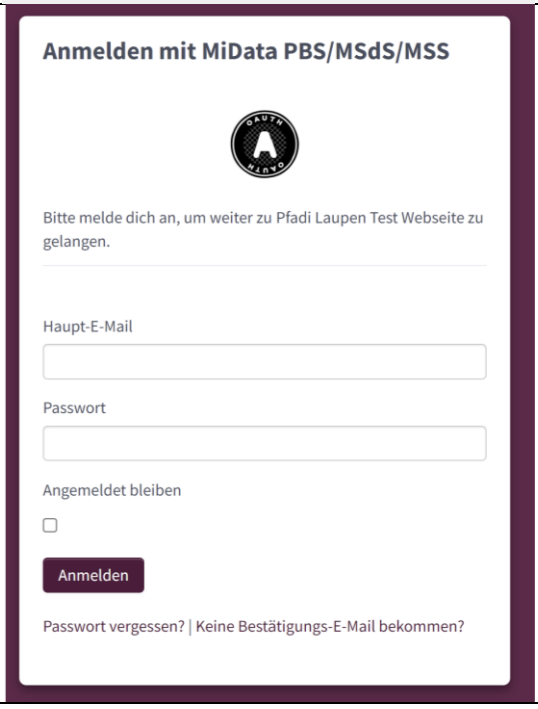
	https://wordpress.org/plugins/daggerhart-openid-connect-generic/
	Das Plugin «OpenID Connect Generic Client» via Wordpress Plugin Manager installieren und aktivieren

	Folgende Plugin Konfiguration vornehmen
	- Login Type: OpenID Connect button on login form
	- Client ID: <Wert aus MiData nehmen>
	- Client Secret Key: <Wert aus MiData nehmen>
	- ClientID Scope: openid email name
	- Login Endpoint URL:
	  o Test: https://pbs.puzzle.ch/oauth/authorize
	  o Produktion: https://db.scout.ch/oauth/authorize
	- Userinfo Endpoint URL:
	  o Test: https://pbs.puzzle.ch/oauth/userinfo
	  o Produktion: https://db.scout.ch/oauth/userinfo
	- Token Validation Endpoint URL:
	  o Test: https://pbs.puzzle.ch/oauth/token
	  o Produktion: https://db.scout.ch/oauth/token
	- End Session Endpoint URL:
	  o Test: https://pbs.puzzle.ch/oauth/logout



- Produktion: https://db.scout.ch/oauth/logout
- Identity Key: email
- HTTP Request Timeout: 5
- Email Formatting: {email}
- Display Name Formatting: {nickname}
- Enable Refresh Token: true
- Link Existing Users: true
- Create user if does not exist: false, somit müssen die User, welche über OAuth authentifiziert werden, vorgängig innerhalb von Wordpress angelegt werden.
- Redirect back to Origin Page: false
- Redirect to the login screen when session expired: true
- Enforce Privacy: false
- Alternate Redirect URI: false
- Enable Logging: false

Login Experience

	Aufruf der Wordpress Login Seite (z.B https://wordpresseite.ch/wp-admin/). Auf ”Login with OpenID Connect” klicken
	Mithilfe eines MiData Accounts sich anmelden

Wechsel aufs produktive System

Sobald du dir sicher bist, dass deine Applikation das macht, was sie soll, kannst du deinen Zugang für die «richtige» MiData beantragen.

OAuth API Key beantragen

Über das nachfolgende Formular kann auf der produktiven MiData (https://db.scout.ch/) eine OAuth Applikation beantragt werden:
https://forms.office.com/Pages/ResponsePage.aspx?id=iq6Fcs2Xq0m9ordFTZ0Fa8gnQG-i3p9KkbcKGL9nFhtUMEpMQkYwMzQxNUVEWEIxRTNWTDhPMDVEMS4u