

# Anleitung

## WP Hitobito Auth Plugin

In der folgenden Anleitung wird erklärt, wie ihr dieses Plugin installiert, einrichtet und benutzt. Beispielhaft wird die Hitobito-Instanz der PBS (Pfadibewegung Schweiz), die [MiData](#) verwendet.

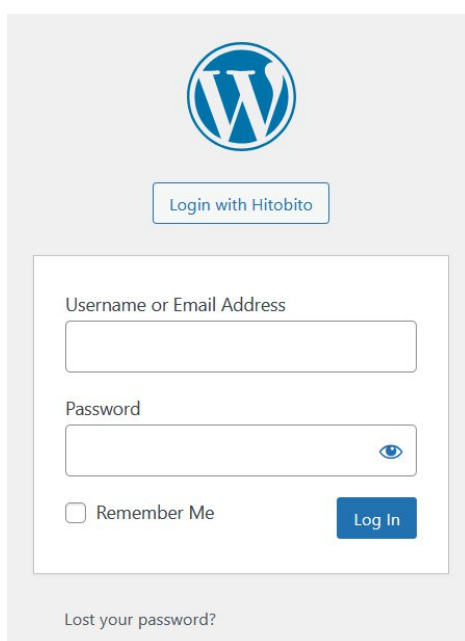
### Was macht dieses Plugin?

Mit diesem Plugin kannst du für deine Wordpress Webseite einen Login-Button zur Anmeldung via einer Hitobito Instanz hinzugefügt werden. Damit ist es möglich, sich auf der Wordpress Webseite mit den Login-Daten der Hitobito (MiData) einzuloggen.

### Ersteller

Das Plugin wurde von den beiden Pfadern, Schlumpf und Vivo an einem Hackathon entwickelt und wird regelmässig geprüft und aktuell gehalten.

Wenn du einen Bug findest, bitte Melde diesen direkt auf dem [GitHub Repository](#) des Plugins als Issue. Wir werden uns zeitnah darum kümmern.



The image shows a screenshot of a WordPress login page. At the top center is the WordPress logo. Below it is a button labeled "Login with Hitobito". Underneath is a white login form with the following elements: a text input field for "Username or Email Address", a text input field for "Password" with an eye icon for toggling visibility, a checkbox labeled "Remember Me", and a blue "Log In" button. At the bottom of the form area, there is a link that says "Lost your password?".

## Konfiguration der OAuth App in der Hitobito/MiData

Damit man die Authentifizierungs-Schnittstelle (OAuth) von Hitobito/MiData verwenden kann, muss die Applikation, hier eine Wordpress Webseite, registriert werden.

In der Testumgebung könnt ihr dies mit dem Admin-Account selber machen. Im Produktivsystem muss dazu ein OAuth-Antrag an den Power-User gemacht werden.

### Das Testsystem

Es wird empfohlen, das Plugin und deren Integration zuerst mit dem Testsystem zu testen.

Weitere Infos zum Testsystem der MiData: <https://docu.scout.ch/de/faq/#testung>

### Das Produktivsystem

Das Produktivsystem ist die eigentliche Mitgliederdatenbank, die von deinem Verband offiziell genutzt wird. Bei der Pfadi (PBS) ist das die MiData. Weitere Infos zum OAuth-Antrag für die MiData: <https://docu.scout.ch/de/documentation/article-15>

Für andere Hitobito-Instanzen gelten dazu andere Formalitäten. Nimm Kontakt mit dem Admin (Power-User) der Hitobito-Instanz auf.

### Konfiguration im Testsystem

Eine neue OAuth-Applikation in MiData erstellen:

<https://pbs.puzzle.ch/de/oauth/applications>

OAuth Applikation	
<input type="button" value="Speichern"/> <input type="button" value="Abbrechen"/>	
Name*	<input type="text" value="Pfadi Laupen Test Website"/>
Redirect URIs	<input type="text" value="http://localhost/wordpress/wp-admin/admin-ajax.php?action=openid-connect-authorize"/>
	<small>Ein Eintrag pro Zeile. Für lokale Tests <code>urn:ietf:wg:oauth:2.0:oob</code> verwenden.</small>
Weitere Audiences	<input type="text"/>
	<small>Zusätzliche Einträge für den <code>aud</code> Key im JWT Access Token.</small>
Scopes	<input checked="" type="checkbox"/> Lesen deiner E-Mail Adresse (email) <input checked="" type="checkbox"/> Lesen deiner E-Mail Adresse und Name (name) <input type="checkbox"/> Lesen deiner Stammdaten und Rollen (with_roles) <input checked="" type="checkbox"/> Lesen deiner OIDC Identity Tokens (openid) <input type="checkbox"/> Lesen aller Personen, Gruppen, Events, Abos und Rechnungen auf die du Zugriff hast, via die JSON-Schnittstellen (api) <input type="checkbox"/> Lesen aller Events, auf die du Zugriff hast (events) <input type="checkbox"/> Lesen aller Gruppen, auf die du Zugriff hast (groups) <input type="checkbox"/> Lesen aller Personen, auf die du Zugriff hast (people) <input type="checkbox"/> Lesen aller Rechnungen, auf die du Zugriff hast (invoices) <input type="checkbox"/> Lesen aller Abos, auf die du Zugriff hast (mailing_lists)
Einwilligung überspringen	<input type="checkbox"/> Applikation ist verbandsintern und vertrauenswürdig, Consent Screen überspringen
Logo	<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/>

**Name**  
Eindeutiger Name deiner Webseite

**Redirect URIs**  
Oauth Endpoint deiner Webseite. Diese wird dir in den Plugin-Einstellungen in deinem Wordpress angezeigt.

**Scopes**  
email, name und openid werden gebraucht.

# Konfiguration des Wordpress Plugins

Download: <https://github.com/scout-ch/wp-hitobito-auth/releases>

1. Herunterladen des Plugins
2. Upload den inhalt des zip nach /wp-content/plugins/ directory
3. Aktiviere das Plugin
4. Öffne Einstellungen > Hitobito Auth konfiguriere das Plugin

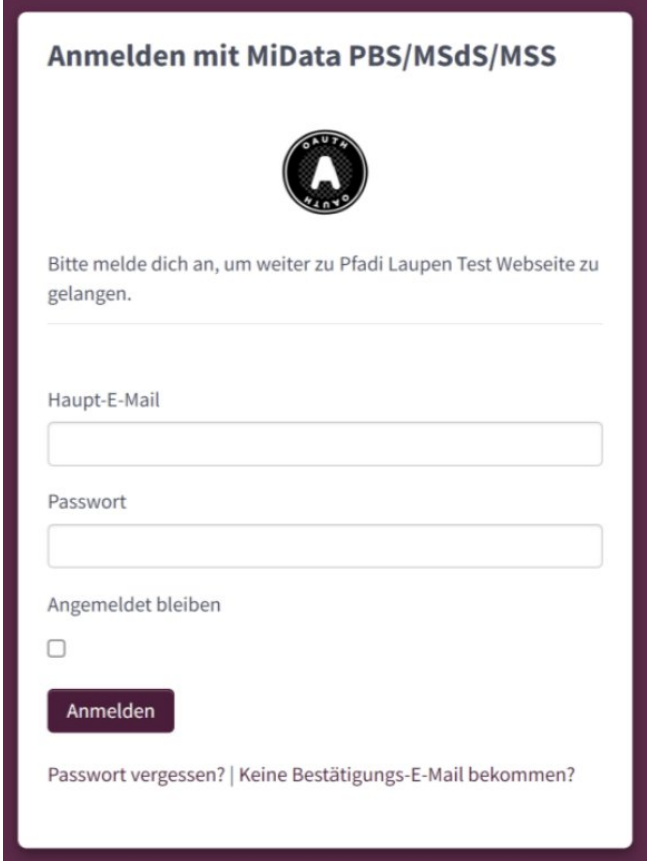
<p><b>Hitobito Auth</b></p> <p><b>Client Settings</b></p> <p>Enter your OpenID Connect identity provider settings.</p> <p><b>Client ID</b></p> <input type="text" value="cwG030MZY4N59uGiOnU1_9NZ1SV3aHs5g3eSh79CTvk"/> <p>The ID this client will be recognized as when connecting the to Identity provider server. Example: <code>my-wordpress-client-id</code></p> <p><b>Client Secret Key</b></p> <input type="text" value="iPcwjC_OzyhwrNxNjP2yO-mcojYdwmF6QEB7K_2h1UY"/> <p>Arbitrary secret key the server expects from this client. Can be anything, but should be very unique.</p> <p><b>Hitobito URL</b></p> <input type="text" value="TEST MiData [pbs.puzzle.ch]"/> <p>For testing please use: <code>XXX.puzzle.ch/</code> and for production please use e.g. <code>db.scout.ch</code></p> <p><b>WordPress User Settings</b></p> <p>Modify the interaction between your Hitobito and WordPress the users.</p> <p><b>Create user if does not exist</b></p> <input type="checkbox"/> <p>If the user identity is not linked to an existing WordPress user, it is created. If this setting is not enabled, and if the user authenticates with an account which is not linked to an existing WordPress user, then the authentication will fail.</p> <p><b>Log Settings</b></p> <p>Log information about login attempts through OpenID Connect Generic.</p> <p><b>Enable Logging</b></p> <input type="checkbox"/> <p>Very simple log messages for debugging purposes.</p> <p><b>Log Limit</b></p> <input type="text" value="1000"/> <p>Number of items to keep in the log. These logs are stored as an option in the database, so space is limited.</p> <p><input type="button" value="Save Changes"/></p>	<p><b>Client ID</b> Entspricht der <b>Client ID</b> der registrierten Oauth Applikation in der MiData</p> <p><b>Client Secret Key</b> Entspricht dem <b>Client secret</b> der registrierten Oauth Applikation in der MiData</p> <p>Registrierten Oauth Applikation:</p> <pre>Name Pfadi Laupen Test Webseite Client ID W6pl3xDI-OjDOWpn293TjKC5SphKivsl1m5WL5UPFTE Client secret 23CWPOFX3aJsDuAHhNrxWTPtF5_utHedHwdK9XL4dFo Redirect URIs https://test.kpsychologovi.cz/wp-admin/admin-ajax.php?action=openid-connect-authorize</pre> <p><b>Hitobito URL</b> Wähle die Hitobito Instanz, wo du die Oauth Applikation registriert hast. (Test oder Produktivsystem)</p> <p><b>Create user if not exists</b> Soll das Plugin automatisch neue Benutzer erstellen, wenn sich jemand neues über die MiData anmeldet?</p> <p>Wenn diese Option nicht aktiviert ist, musst du selber Wordpress Benutzer erstellen. Diese müssen zwingend den Schema entsprechen:</p> <p>Benutzername: hussein_kohlmann</p> <p>E-mail: hussein_kohlmann@hitobito.example.com</p>
--	--

## Login Experience

Nachdem die Oauth Applikation in der MiData registriert und das Plugin konfiguriert und aktiviert ist, bekommst du auf dem Anmelde Bildschirm einen neuen Button:

Login mit Hitobito

Nach dem klick auf den Button, wird man auf die Anmelde-Seite der MiData weitergeleitet. Hier muss man sich mithilfe eines MiData Accounts anmelden.



The screenshot shows a login form titled "Anmelden mit MiData PBS/MSdS/MSS". At the top center is a circular logo with a white 'A' on a black background, surrounded by the text "OAUTH" and "MiData". Below the logo, the text reads "Bitte melde dich an, um weiter zu Pfadi Laupen Test Webseite zu gelangen." There are two input fields: "Haupt-E-Mail" and "Passwort". Below the password field is a checkbox labeled "Angemeldet bleiben" which is currently unchecked. A dark purple button labeled "Anmelden" is positioned below the checkbox. At the bottom of the form, there is a link: "Passwort vergessen? | Keine Bestätigungs-E-Mail bekommen?".

Nach erfolgreichem Login wird man wieder zurück zu Wordpress geleitet und falls erfolgreich direkt in den Admin-Bereich.