

OAuth Authbindung einer NextCloud

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.).

Was ist NextCloud?

Nextcloud ist eine freie Software für das Speichern von Daten (z. B. Dateien, Kalender, Kontakte etc.) auf einem Server. Auf die Daten kann der Anwender sowohl über eine Weboberfläche als auch mit Client-Applikationen (Smartphone und Desktop) zugreifen. Server und Clients können sich dabei synchronisieren

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>

Auf der Testseite der Midata (<https://pbs.puzzle.ch/>) kann die OAuth Applikation selbständig erstellt werden.

| | |
|---|---|
| Pfadi Laupen Cloud | Name der OAuth Applikation |
| https://cloud.pfadilaupen.ch/apps/sociallogin/custom_oauth2/MiData | Redirect URLs konfigurieren. Diese Information findet man meistens innerhalb der OAuth Client Applikation. |
| <ul style="list-style-type: none">- email- name- with_roles- openid | Scopes basierend auf https://github.com/hitobito/hitobito/blob/master/doc/development/08_oauth.md definieren |
| https://pfadilaupen.ch/wp-content/themes/twentytwelve/image/head.png | URL zum Logo angeben |
| Ja | Meine Applikation speichert Daten, die aus der MiData stammen, in einer Datenbank oder in einer anderen Form ab |
| Ja | Ich bestätige, dass meine Applikation Daten aus der MiData nur wenn nicht anders möglich abspeichert. Weiter werden die so gesammelten Daten nur so lange gespeichert wie nötig und können auf Anfrage durch die betroffene Person gelöscht werden. |
| Ja | Ich bestätige, dass die über die MiData erlangten Daten nicht öffentlich oder durch unverschlüsselte Verbindungen zugänglich sind. |
| Ja | Ich bestätige, dass ich keine Daten, die aus der MiData stammen, an Dritte weitergeben |
| | |

| | |
|---|--|
| Ja | Meine Applikation wurde auf dem MiData-Integrationssystem getestet und verhält sich dort wie vorgesehen. |
| Ja | Ich bestätige hiermit, dass meine Applikation nur so wenig Anfragen wie nötig an die MiData schickt und keine Ausfälle provoziert |
| 10 pro Woche | Wie viele OAuth Zugriffe erwartest du mindestens durch deine Applikation (pro Woche / Monat) |
| 50 pro Woche | Wie viele OAuth Zugriffe erwartest du höchstens durch deine Applikation (pro Woche / Monat) |
| | |
| Nein | Ich kann dem Team MiData und der/dem MiData Product Owner*in Zugriff auf ein Testsystem der Applikation geben. Zugang bitte bilateral mitteilen (z.B. über https://onetimesecret.com) |
| Nextcloud Instanz, welche durch Hetzner betrieben wird | Bitte URL zum Quellcode angeben |
| | |
| Max Muster, max.muster@muster.ch , 076 111 11 11 | Kontaktinformation Antragsteller*in |
| Personen | Welche der folgenden Kategorien passt (am besten) zu deiner Applikation? |
| Vereinfachung der Authentifizierung der Next Cloud der Pfadi Laupen, Integration auf Testumgebung durchgeführt: https://pbs.puzzle.ch/de/oauth/applications/47 | Sonstige Erklärungen, Kommentare |

Konfiguration der OAuth App in Midata

Eine neue OAuth-Applikation in Midata anlegen.

| | |
|--|---|
| <p>Name* <input type="text" value="Pfadi Laupen Cloud"/></p> <p>Redirect URIs <input type="text" value="https://cloud.pfadilaupen.ch/apps/sociallogin/custom_oauth2/Midata"/></p> <p><small>Ein Eintrag pro Zeile. Für lokale Tests urn:iETF:wg:oauth:2.0:oob verwenden.</small></p> <p>Scopes</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Lesen deiner E-Mail Adresse (email)<input checked="" type="checkbox"/> Lesen deiner E-Mail Adresse und Name (name)<input checked="" type="checkbox"/> Lesen deiner Stammdaten und Rollen (with_roles)<input checked="" type="checkbox"/> Lesen deines 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) <p>Logo <input type="button" value="Choose file"/> No file chosen</p> | <p>Folgende Informationen müssen dafür angegeben werden</p> <ul style="list-style-type: none">- Name der Applikation- Redirect URIs- Scopes |
|--|---|

Installation und Konfiguration des NextCloud Plugins

Sobald die OAuth Applikation erstellt wurde, kann Midata als OAuth Client innerhalb der NextCloud angebunden werden. Dafür sind die Installation und Konfiguration eines zusätzlichen Plugins notwendig.

| | |
|--|--|
| https://apps.nextcloud.com/apps/sociallogin | Zusätzliches Plugin innerhalb von NextCloud herunterladen und installieren |
| <ul style="list-style-type: none"><input checked="" type="checkbox"/> Disable auto create new users<input type="checkbox"/> Create users with disabled account<input type="checkbox"/> Allow users to connect social logins with their account<input checked="" type="checkbox"/> Prevent creating an account if the email address exists in another account<input type="checkbox"/> Update user profile every login<input type="checkbox"/> Do not prune not available user groups on login<input type="checkbox"/> Automatically create groups if they do not exists<input type="checkbox"/> Restrict login for users without mapped groups<input type="checkbox"/> Restrict login for users without assigned groups<input type="checkbox"/> Disable notify admins about new users<input type="checkbox"/> Hide default login<input type="checkbox"/> Button text without prefix <p><input type="button" value="Save"/></p> | Folgende Einstellungen innerhalb des SocialLogin Plugins vornehmen. Wichtig ist hier die Deaktivierung der automatischen Erstellung von Accounts. So kann sichergestellt werden, dass sich nicht die gesamte PBS auf der Cloud anmelden kann und User zuerst vorgängig innerhalb der Cloud angelegt werden müssen. |

Custom OAuth2 +

Internal name x

Title

API Base URL

Authorize url (can be relative to base URL)

Token url (can be relative to base URL)

Profile url (can be relative to base URL)

Logout URL (optional)

Client Id

Client Secret

Scope (optional)



Profile Fields (optional, comma-separated)

Display name claim (optional)

Folgende Einstellungen müssen vorgenommen werden.

| | |
|---|--|
| <p>Display name claim (optional)</p> <input type="text" value="email"/> <p>Groups claim (optional)</p> <input type="text" value="with_roles"/> <p>Button style</p> <input type="text" value="None"/> <p>Default group</p> <input type="text" value="None"/> <p style="text-align: center; margin-top: 10px;">Add group mapping</p> | |
|---|--|

Login Experience

| | |
|---|--|
|  <p style="text-align: center;">Log in with MiData</p> | |
| <div style="border: 2px solid #800000; padding: 10px;"> <p>Anmelden mit MiData PBS/MSdS/MSS</p> <div style="text-align: center;">  </div> <p>Bitte melde dich an, um weiter zu Pfadi Laupen Cloud Webseite zu gelangen.</p> <hr/> <p>Haupt-E-Mail</p> <input type="text"/> <p>Passwort</p> <input type="password"/> <p>Angemeldet bleiben</p> <input type="checkbox"/> <p style="text-align: center; margin-top: 5px;">Anmelden</p> <p style="font-size: small; margin-top: 5px;">Passwort vergessen? Keine Bestätigungs-E-Mail bekommen?</p> </div> | |