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

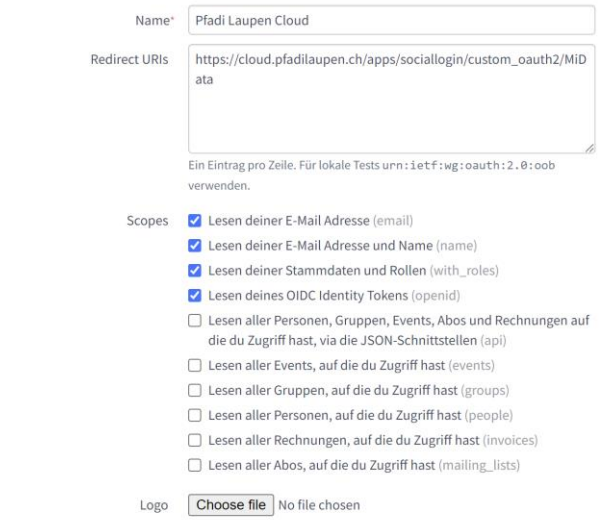
Auf der Testseite der Midata (https://pbs.puzzle.ch/) kann die OAuth Applikation selbständig erstellt werden.

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.
- 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.

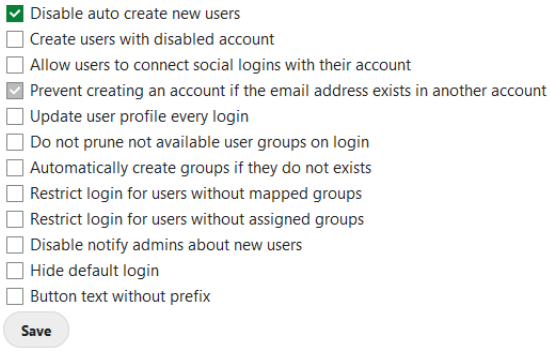


Folgende Informationen müssen dafür angeben werden

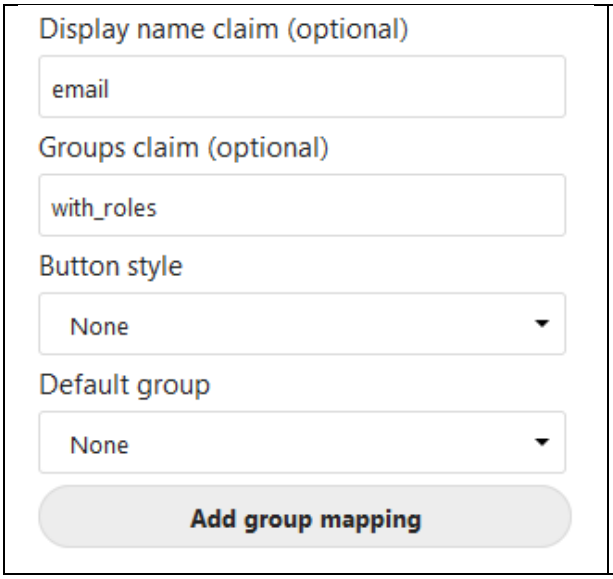
- Name der Applikation
- Redirect URIs
- Scopes

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
	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 MiData Title MiData API Base URL https://pbs.puzzle.ch/oauth Authorize url (can be relative to base URL) https://pbs.puzzle.ch/oauth/authorize Token url (can be relative to base URL) https://pbs.puzzle.ch/oauth/token Profile url (can be relative to base URL) https://pbs.puzzle.ch/de/oauth/profile Logout URL (optional) Client Id kSfBVrjLNzbYvebApEFseFo8AiH0A0PJF86AB-Ju1 Client Secret •••••••••••••••••••••••••••••••••••• Scope (optional) email name openid with_roles Profile Fields (optional, comma-separated) Display name claim (optional)	Folgende Einstellungen müssen vorgenommen werden.



Login Experience