OAuth (Open Authorization) de NextCloud

Qu'est-ce que OAuth ?

Hitobito est un fournisseur OAuth 2.0, ce qui signifie qu'une application externe peut authentifier les utilisateur·trice·s via hitobito (généralement sous la forme d'une fonction "Login via hitobito", similaire à celle de Google et Facebook, etc.).

Qu'est-ce que NextCloud?

Nextcloud est un logiciel gratuit permettant de stocker des données (par ex. fichiers, calendriers, contacts, etc.) sur un serveur. L'utilisateur·trice peut accéder aux données aussi bien via une interface web que via des applications client (smartphone et bureau). Le serveur et les applications client peuvent se synchroniser.

Demander un accès OAuth API

Le formulaire suivant permet de mettre en place une application OAuth sur Midata en production (https://db.scout.ch/) :
https://forms.office.com/Pages/ResponsePage.aspx?id=iq6Fcs2Xq0m9ordFTZ0Fa8gnQG-i3p9KkbcKGL9nFhtUMEpMQkYwMzQxNUVEWEIxRTNWTDhPMDVEMS4u

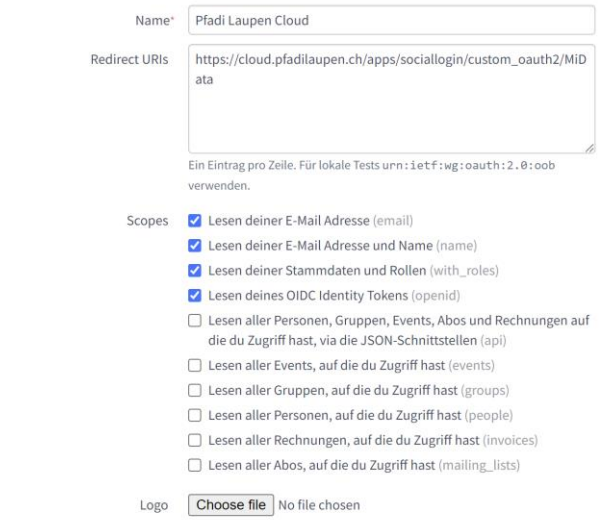
Sur la page de test de Midata (https://pbs.puzzle.ch/), l'application OAuth peut être créée de manière autonome..

Pfadi Laupen Cloud	Nom de l'application OAuth
https://cloud.pfadilaupen.ch/apps/sociallogin/custom_oauth2/MiData	Configurer les URL de redirection. Cette information se trouve généralement dans l'application client OAuth.
- email - name - with_roles - openid	Définir des scopes openid basés sur https://github.com/hitobito/hitobito/blob/master/doc/development/08_oauth.md
https://pfadilaupen.ch/wp-content/themes/twentytwelve/image/head.png	Indiquer l'URL du logo
Oui	Mon application enregistre les données issues de MiData dans une base de données ou sous une autre forme.
Oui	Je confirme que mon application ne stocke des données issues de MiData que si cela n'est pas possible autrement. De plus, les données ainsi collectées ne sont conservées que le temps nécessaire et peuvent être supprimées sur demande par la personne concernée.
Oui	Je confirme que les données récupérées via MiData ne sont pas accessibles au public ou par des connexions non cryptées.

Oui	Je confirme que je ne transmettrai aucune donnée provenant de MiData à des tiers.
Oui	Mon application a été testée sur le système d'intégration de MiData et s'y comporte comme prévu.
Oui	Je confirme par la présente que mon application n'envoie que le minimum nécessaire de requêtes à MiData et ne provoquera pas de pannes.
10 par semaine	Combien d'accès OAuth attends-tu au minimum de ton application (par semaine / par mois) ?
50 par semaine	Combien d'accès OAuth attends-tu au maximum de ton application (par semaine / mois) ?
Non	Je peux donner à l'équipe MiData et au/à la Product Owner MiData l'accès à un système de test de l'application. Veuillez communiquer l'accès de manière bilatérale (par ex. via https://onetimesecret.com).
Instance Nextcloud exploitée par Hetzner	Veuillez indiquer l'URL du code source.
Max Muster, max.muster@muster.ch, 076 111 11 11	Informations de contact de la personne qui fait la demande
Personnes	Laquelle des catégories suivantes correspond (le mieux) à ton application ?
Simplification de l'authentification Next Cloud de Pfadi Laupen, Intégration réalisée sur un environnement de test : https://pbs.puzzle.ch/de/oauth/applications/47	Autres explications, commentaires

Konfiguration der OAuth App in Midata

Eine neue OAuth-Applikation in Midata anlegen.

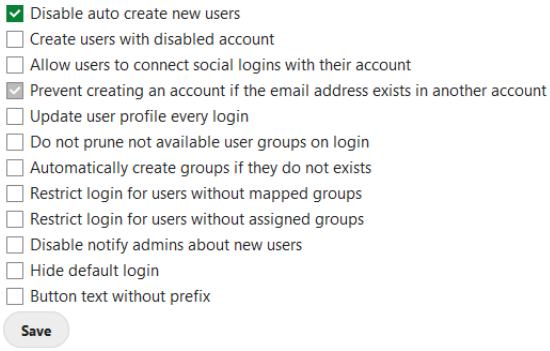


Folgende Informationen müssen dafür angeben werden

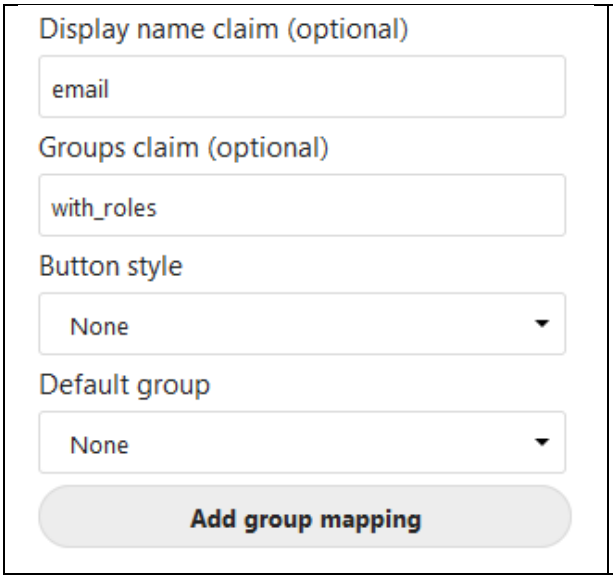
- Name der Applikation
- Redirect URIs
- Scopes

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