Autenticazione OAuth di un NextCloud

Cos'è OAuth?

Hitobito è un provider OAuth 2.0, il che significa che un'applicazione esterna può autenticare gli utenti tramite hitobito (tipicamente sotto forma di funzione "login tramite hitobito", simile a Google e Facebook ecc.).

Cos'è NextCloud?

Nextcloud è un software gratuito per l'archiviazione di dati (ad esempio file, calendari, contatti, ecc.) su un server. L'utente può accedere ai dati sia tramite interfaccia web che con applicazioni client (smartphone e desktop). Nel far questo server e client possono sincronizzarsi

Richiedere un OAuth API Key

Tramite il seguente formulario si può richiedere sul Midata produttivo(https://db.scout.ch/) un'applicazione OAuth:
https://forms.office.com/Pages/ResponsePage.aspx?id=iq6Fcs2Xq0m9ordFTZ0Fa8gnQG-i3p9KkbcKGL9nFhtUMEpMQkYwMzQxNUVEWEIxRTNWTDhPMDVEMS4u

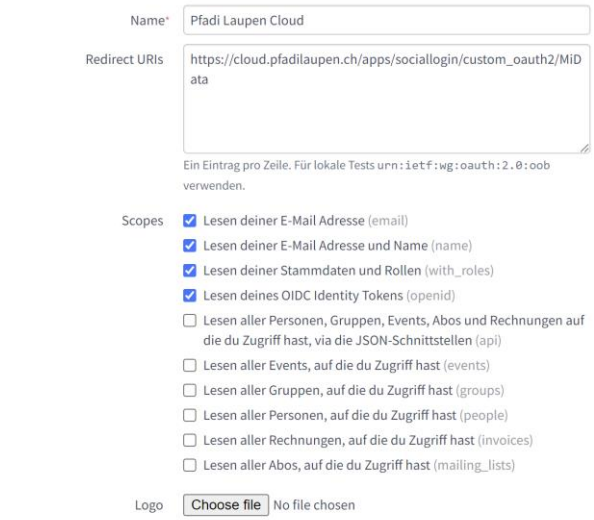
Sulla pagina test di Midata (https://pbs.puzzle.ch/) può venir creata autonomamente un'applicazione OAuth.

Cloud degli Pfadi Laupen	Nome dell'applicazione OAuth
https://cloud.pfadilaupen.ch/apps/sociallogin/custom_oauth2/MiData	Configurare redirect URLs Queste informazioni sono generalmente reperibili all'interno dell'applicazione client OAuth.
- email - nome - with_roles - openid	Definire gli scopes basandosi su https://github.com/hitobito/hitobito/blob/master/doc/development/08_oauth.md
https://pfadilaupen.ch/wp-content/themes/twentytwelve/image/head.png	Indicare la URL del logo
Sì	La mia applicazione salva i dati che provengono da MiData in un database o in un altro formato
Sì	Confermo che la mia applicazione salva i dati di MiData solo laddove è strettamente necessario ed è impossibile fare altrimenti. Inoltre, i dati così raccolti vengono conservati solo per il tempo necessario e possono essere cancellati su richiesta dell'interessato.
Sì	Confermo che i dati ottenuti tramite MiData non sono pubblici né accessibili tramite connessioni non crittografate.
Sì	Confermo che non trasmetterò a terzi nessun dato proveniente da MiData
Sì	La mia applicazione è stata testata sul sistema di integrazione MiData e lì si comporta come previsto.

Sì	Con la presente confermo che la mia applicazione invia a MiData solo il numero minimo di richieste necessarie e non causa errori
10 a settimana	Quanti accessi OAuth ti aspetti almeno dalla tua applicazione (a settimana/mese)
50 a settimana	Quanti accessi OAuth ti aspetti al massimo dalla tua applicazione (a settimana/mese)
No	Posso fornire al team MiData e al proprietario del prodotto MiData l'accesso a un sistema di test dell'applicazione. Per favore comunicare l'accesso in modo bilaterale (p.es. tramite https://onetimesecret.com)
Istanza Nextcloud, gestita da Hetzner	Fornisci l'URL del codice sorgente
James Levell, jimmy.levell@outlook.com, 079 575 22 77	Informazioni di contatto del richiedente
Persone	Quale delle seguenti categorie si adatta (meglio) alla tua applicazione?
Semplificazione dell'autenticazione del Next Cloud degli Pfadi Laupen, integrazione effettuata su ambiente di test: https://pbs.puzzle.ch/de/oauth/applications/47	Altre spiegazioni, commenti

Configurazione dell’app Oauth in Midata

Creare una nuova applicazione OAuth in Midata.

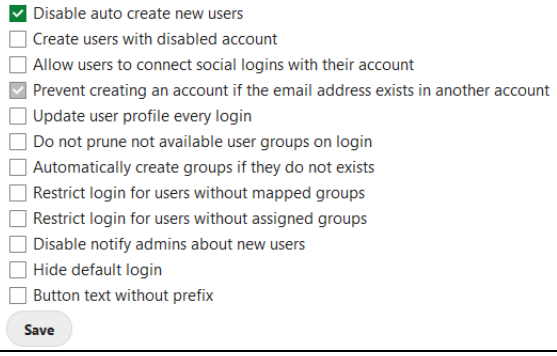


A tal fine è necessario fornire le seguenti informazioni

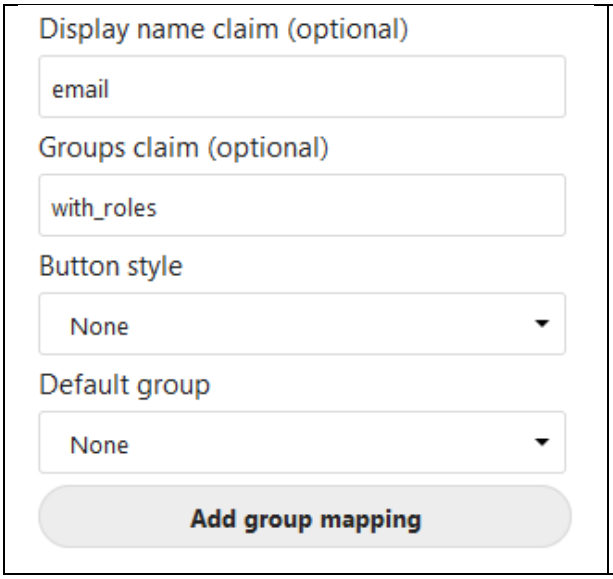
- Nome dell’applicazione
- Redirect URIs
- Scopes

Istallazione e configurazione del plugin NextCloud

Una volta creata l'applicazione OAuth, Midata può essere connessa come client OAuth all'interno di NextCloud. Ciò richiede l'installazione e la configurazione di un plugin aggiuntivo.

https://apps.nextcloud.com/apps/sociallogin	Scaricare e installare plug-in aggiuntivi in NextCloud
	Effettua le seguenti impostazioni nel plugin SocialLogin. Ciò che è importante qui è disattivare la creazione automatica degli account. In questo modo si garantisce che non tutta il MSS possa accedere al cloud e che gli utenti debbano prima essere creati nel cloud.

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)	È necessario effettuare le seguenti impostazioni.



Login Experience