

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-i3p9KkbcKGL9nFhtUMEpMQkYwMzQxNUVEWEIxRTNWTdDhPMDVEMS4u>

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/soci_allogin/custom_oauth2/MiData	Configurare redirect URLs Queste informazioni sono generalmente reperibili all'interno dell'applicazione client OAuth.
<ul style="list-style-type: none">- 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.

<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:i etf: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>A tal fine è necessario fornire le seguenti informazioni</p> <ul style="list-style-type: none">- 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
<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>	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

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)

È necessario effettuare le seguenti impostazioni.

<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;">Add group mapping</p>	
---	--

Login Experience

 <p style="text-align: center;">Log in with MiData</p>	
<div style="border: 2px solid #4b0032; 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;">Anmelden</p> <p style="text-align: center;">Passwort vergessen? Keine Bestätigungs-E-Mail bekommen?</p> </div>	