

Anleitung: LDAP-Anbindung

Hier ein paar Informationen für alle, die Nutzerauthentifizierung über ein individuelles LDAP nutzen wollen.

Die Dokumentation des HPI dazu befindet sich hier (QR-Code):

<https://docs.schul-cloud.org/pages/viewpage.action?pageId=55902270>



Vorbereitung

- Der LDAP der Schule muss von außen über eine LDAPS-Verbindung erreichbar sein. -> ggf. müssen in einer Firewall folgende IP-Adressen freigegeben werden: 141.89.221.180 (HPI) und z.B. 78.46.103.254 (NBC).
- Der LDAP muss sich mit einem Zertifikat ausweisen, dass von einer der anerkannten CA ausgestellt wurde. **Let's Encrypt**-Zertifikate funktionieren auch.
- Es muss ein Search-User zum Auslesen und Synchronisieren des Verzeichnisses angelegt werden, der möglichst nur Leserechte haben sollte.

Für die Konfiguration erforderliche Angaben zum LDAP-Verzeichnis

- Root-Pfad und Pfad(e) zu den Nutzern
- Die in der Eingabemaske benannten Nutzer-Attribute müssen bekannt und vorhanden sein. Attributnamen sind wählbar
- Die E-Mail muss für jeden User systemweit über die gesamte NBC einmalig sein, ebenso die UUID.

Alias	<input type="text" value="NBC-Testschule I"/>
Typ	<input type="text" value="Allgemein"/>
URL (ldaps ist verpflichtend)	<input type="text" value="ldaps://"/>
root-Pfad	<input type="text"/>
search-Nutzer	<input type="text" value="nds@mailinator.com"/>
search-Nutzer Passwort	<input type="password" value="....."/>
Nutzer-Pfad	<input type="text"/>
Rollen-Typ	<input type="text" value="LDAP-Gruppe"/>

Nutzer-Attribute	
Vorname	Nachname
<input type="text" value="givenName"/>	<input type="text" value="sn"/>
Domainname (Pfad im LDAP)	uid
<input type="text" value="dn"/>	<input type="text" value="cn"/>
uuid	E-Mail
<input type="text" value="objectGUID"/>	<input type="text" value="mail"/>

Es werden nur Nutzer mit Rollen synchronisiert. Die Rollenzuweisung ist **(a)** entweder durch eine Gruppenzugehörigkeit mit „memberOf“-Attribut oder **(b)** alternativ über ein frei definiertes Attribut, dass die Rolle direkt beschreibt, möglich. Die Auswahl geschieht über „Rollen-Typ“.

Fall (a), Rollenzuweisung durch Gruppenzugehörigkeit

Bei Rollen-Typ „LDAP-Gruppe“ auswählen und die LDAP-Gruppen für Schüler, Lehrer und Admin als vollen Pfad inkl. Root-DN angeben.

Die Gruppen-/Rollenzugehörigkeit der User muss durch das User-Attribut „memberOf“ gegeben sein.

Rollen-Attribute



Student

Lehrer

Admin

keine Schul-Cloud

Fall (b), Rollenzuweisung durch ein Attribut

Bei Rollen-Typ „Nutzer-Attribut“ auswählen und bei „Rolle“ den Namen des Attributs eingeben.

Die Werte des Attributs für die jeweiligen Rollentypen (Schüler, Lehrer, Admin) müssen dann bei Rollen-Attribute eingetragen werden.


The screenshot displays the 'Rollen-Attribute' configuration page. It features a grid of four role types, each with a text input field for the LDAP path. A blue box highlights the 'keine Schul-Cloud' field. A zoomed-in view of the 'keine Schul-Cloud' field shows a dropdown menu with 'objectGUID' selected and 'Rolle' and 'description' as options.


Rollen-Typ	LDAP-Gruppe (Vollständiger Pfad)
Student	cn=student,ou=users,dc=beispielschule,dc=de
Lehrer	cn=teacher,ou=users,dc=beispielschule,dc=de
Admin	cn=admin,ou=users,dc=beispielschule,dc=de
keine Schul-Cloud	cn=no-sc,ou=users,dc=beispielschule,dc=de


Klassenzuweisung

Für Klassen- und Gruppenzuweisungen kann optional ein Pfad zu den Klassen-Gruppen angegeben werden. Alle Gruppen unter diesem Pfad werden als Klassen abgebildet.

Klassen (optional)

Klassen-Pfad 

Klassen-Attribute 



Anzeige-Name Domain-Name

Nutzer der Klasse mit vollem Pfad