

# 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"/>

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

The screenshot shows the 'Rollen-Attribute' configuration page for the 'LDAP-Gruppe' role type. It features a lock icon and a help icon. There are four input fields for different roles:

- Student:** cn=student,ou=users,dc=beispielschule,dc=de
- Lehrer:** cn=teacher,ou=users,dc=beispielschule,dc=de
- Admin:** admin
- keine Schul-Cloud:** no-sc

### 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 shows the 'Rollen-Attribute' configuration page for the 'Nutzer-Attribut' role type. It features a lock icon and a help icon. There are four input fields for different roles:

- Student:** student
- Lehrer:** teacher
- Admin:** admin
- keine Schul-Cloud:** no-sc

A callout box highlights the 'Rolle' field, which contains 'objectGUID', and the 'description' field, which contains 'description'.

### Klassenzuweisung

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

The screenshot shows the 'Klassen (optional)' configuration page. It features a checked checkbox for 'Klassen (optional)', a lock icon, and a help icon. There are three input fields:

- Klassen-Pfad:** (empty)
- Anzeige-Name:** name
- Domain-Name:** dn

Below these fields is a section for 'Nutzer der Klasse mit vollem Pfad' with the value 'member'.