LDAP-Information für Schulen

Damit die Nutzer:innendaten sowie Rollen und Klassenzugehörigkeiten korrekt in die Cloud synchronisiert werden, muss Ihr LDAP bestimmte Informationen mitbringen. Die folgenden Punkte helfen Ihnen, das LDAP auf die Synchronisation mit der Cloud vorzubereiten.

Schuljahreswechsel

Informationen rund um den Schuljahreswechsel an einer LDAP-Schule finden Sie hier.

Bitte beachte, dass Sie die Sommerferien-Transferphase aktiv beenden müssen, damit neue Klassen und Nutzer:innen wieder synchronisiert werden.

ührungsv

rmieren? Hie

Ablauf der Synchronisation

- Die Nutzer:innen werden regelmäßig über den Sychronisierungsprozess angelegt bzw. aktualisiert
- Der Login erfolgt über den LDAP Server - Daher sind Passwortänderungen sofort aktiv

Voraussetzungen (wichtig!)

1. Das **LDAP muss verschlüsselt über ldaps://** erreichbar sein, der Standardport ist 10636 kann aber auch anders gewählt werden
2. In der Firewall muss der **LDAP-Port (z.B. 10636) nach außen freigegeben** sein
3. Wenn die Firewall IPs filtert ist eine **Freischaltung der IPs** notwendig:

	IPv4	IPv6
Ionos 1	185.132.46.51	ipv4 only
Ionos 2	85.215.249.208	ipv4 only
Ionos 3	85.215.249.184	ipv4 only
Ionos 4	85.215.249.82	ipv4 only
Ionos IP Range 1	185.56.148.0**/24**	ipv4 only
Ionos IP Range 2	217.160.200.64**/28**	ipv4 only

4. Es muss ein:e Nutzer:in mit Passwort im LDAP angelegt werden, die:er Lese-Zugriff auf alle Nutzer:innen und Gruppen hat (z.B. cn=schulcloud, ou=ldap,dc=ihreSchulDomain,dc=de). Diese:r Nutzer:in sollte keinesfalls Schreibrechte haben. Die:er Nutzer:in wird später für die Synchronisation benutzt.
    a. **Achtung:** Die Eingabe des Suchnutzer-Pfades erfolgt mit einem **vollen FQDN**, also vollständig inklusive "DC=" Domainangabe.

LDAP-Struktur für Nutzer:innen

LDAP-Verzeichnis, in dem alle Nutzer:innen z.B. (ou=users) enthalten sind:

```
ou=users,dc=ihreSchulDomain,dc=de
```

Achtung: Die Eingabe der "Nutzer-Pfad(e)" erfolgt mit einem **verkürzten FQDN**, welche sich aus der Eingabe und dem "Basis-Pfad" weiter oben in der Konfiguration zusammensetzt.

Der Pfad zu einer:m Nutzer:in ist wie folgt definiert:

`uid=max.mustermann,ou=users,dc=ihreSchulDomain,dc=de`

Ein:e Nutzer:in benötigt folgende LDAP-Attribute:

- uid (eindeutige Login-ID, z.B. max.musterman)
- uuid (eindeutige *nicht änderbare* ID, uid kann sich z.B. bei Heirat verändern)
- mail (E-Mail-Adresse des Nutzers; *darf nicht mehrfach vergeben sein*)
- givenName (Vorname)
- sn (Nachname)
- userPassword (verschlüsseltes Passwort des Nutzers für den Login-Prozess, wird nicht von der SchulCloud sychronisiert)
- objectClass (**Einer der Werte muss *person* sein**)

Sollten die Attribute im LDAP anders heißen, so können sie im Administrationsbereich angepasst werden (siehe Video).

Nutzer:innenrollen:

Nutzer:innenrollen können entweder als Attribut (z.B. "description") oder als Gruppenmitgliedschaft (LDAP-Gruppe via "memberOf") konfiguriert werden.

Achtung: Die Eingabe der Gruppen-Pfade erfolgt jeweils mit einem **vollen FQDN**, also vollständig inklusive "DC=" Domainangabe.

Die Benennung ist variabel einstellbar:

- ROLE_STUDENT (Nutzer ist Schüler)
- ROLE_TEACHER (Nutzer ist Lehrer)
- ROLE_ADMIN (Nutzer ist Admin)

Nutzer:innen vom Sync ausschließen

bitte vergeben sie folgendes Attribut/Gruppenmitgliedschaft:

- ROLE_NO_SC (Nutzer:in möchte nicht an der Schul-Cloud teilnehmen)

LDAP-Struktur für Klassen

Optional lassen sich auch Klassenzugehörigkeiten in die Schul-Cloud synchronisieren. Benötigt wird ein LDAP-Sub-Verzeichnis, in dem nur Klassen enthalten sind (z.B. *ou=classes,dc=ihreSchulDomain,dc=de*).

Achtung: Die Eingabe erfolgt mit einem **verkürzten FQDN**, welche sich aus der Eingabe und dem "Basis-Pfad" weiter oben in der Konfiguration zusammensetzt.

Die Klassen sind dann einfach Gruppen innerhalb dieses Verzeichnisses, bspw: *cn=klasse-1-c,ou=classes,dc=ihreSchulDomain,dc=de*

Eine Klasse benötigt folgende Attribute (Tipp - ObjectClass: groupOfUniqueNames):

- description (Anzeigenamen) (nicht veränderbar und notwendig)
- uniqueMember (Einträge der User als LDAP-Pfade, die zur Klasse gehören)

Besonderheiten bei der Nutzung des iServ-Zentral-LDAPs in der Niedersächsischen Bildungscloud

Die Nutzung Ihres iServ-LDAPs gestaltet sich besonders komfortabel: Ist das entsprechende Paket auf Ihrem Server installiert, wird Ihre Schule in Niedersachsen automatisch mit der Niedersächsischen Bildungscloud synchronisiert, ohne dass Sie das LDAP wie hier beschrieben selbst verknüpfen müssen.

Achtung: Derzeit werden alle Gruppen aus dem iServ als Klasse synchronisiert. Dies lässt sich leider derzeit nicht vermeiden.