# LDAP / LDAPS Authentifizierung BelWü Moodle

Für ein bei Belwue gehostetes Moodle ist die Authentifizierung per ldaps gegenüber einem Server der paedML Linux in der Schule möglich. Durch die Verwendung von ldaps werden die Passwörter verschlüsselt übertragen, so dass sie nicht abgehört werden können.

Sicherheitshalber sollte man aber immer einen administrativen Zugang zum Moodle vorsehen, der von Hand eingetragen wurde, und bei dem die Authentifizierung von Moodle intern durchgeführt wird. Dies ist sinnvollerweise der bei der Erstinstallation schon eingerichtete Admin Nutzer, der sowieso nur für Notfälle eingesetzt werden sollte.

**Anmerkung:** am Moodle kann man sich dann aber nur anmelden, wenn die eigene paedML auch erreichbar ist!

# 1. Einstellungen im eigenen Netzwerk

Damit das Moodle bei Belwue mit dem LDAP / LDAPS Server der ML kommunizieren kann, muss moodle den Server der paedML4.x erreichen können, deswegen sind folgende Einstellungen erforderlich:

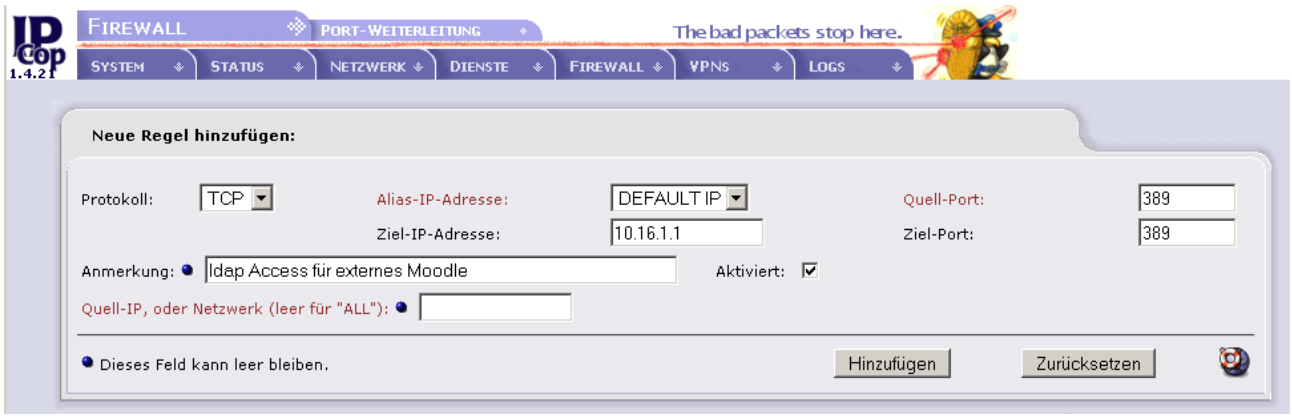
Am Router zum Provider (Belwue):

- Portweiterleitung für die Ports 389 (LDAP) und 636 (LDAPS) im Router von Belwue einrichten lassen bzw. einrichten

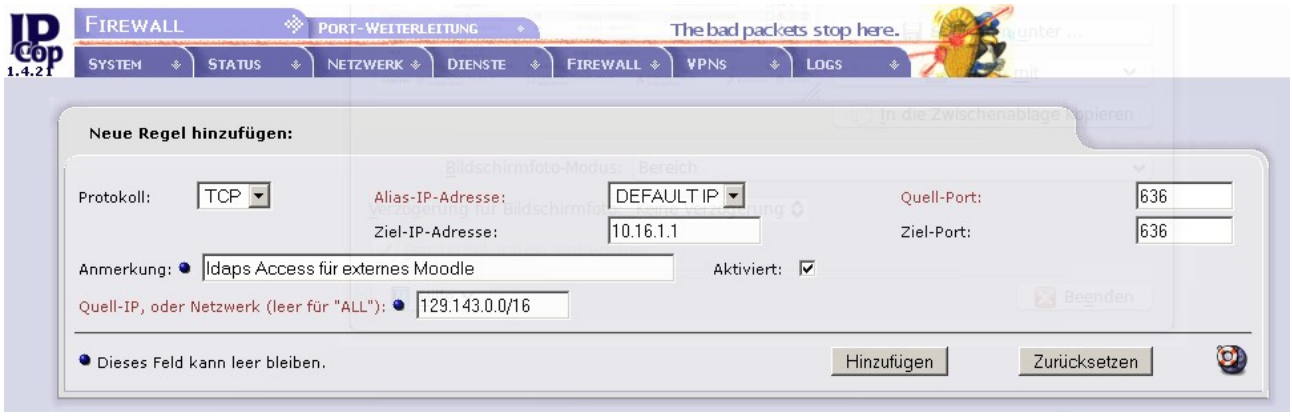
Am IPCOP des Schulnetzes:

- Im Webfrontend des IPCop muss unter „Firewall“ - „Port Weiterleitung“ eine neue Regel erstellt werden, die den Port 389 TCP für LDAP bzw. den Port 636 TCP für LDAPS auf den server (normalerweise 10.16.1.1) weiterleitet. Im Feld Quell-IP, oder Netzwerk sollten Sie wie im Bild für die ldaps Regel zu sehen, den Eintrag 129.143.0.0/16 eintragen.

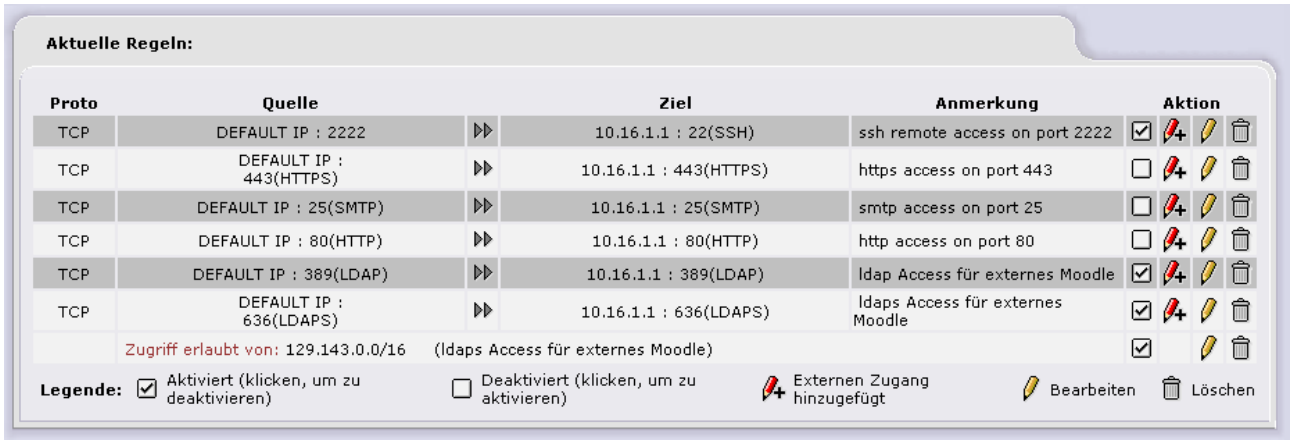
Regel für ldap




Regel für ldaps




Überblick über die exstierenden Regeln




Hinweise

- Es ist darauf zu achten, dass diese Regeln auch aktiviert sind (Häkchen im Kasten am Ende der Zeile).
- Sobald die Authentifizierung per ldaps funktioniert können Sie die Regel für ldap wieder deaktivieren oder sogar löschen.

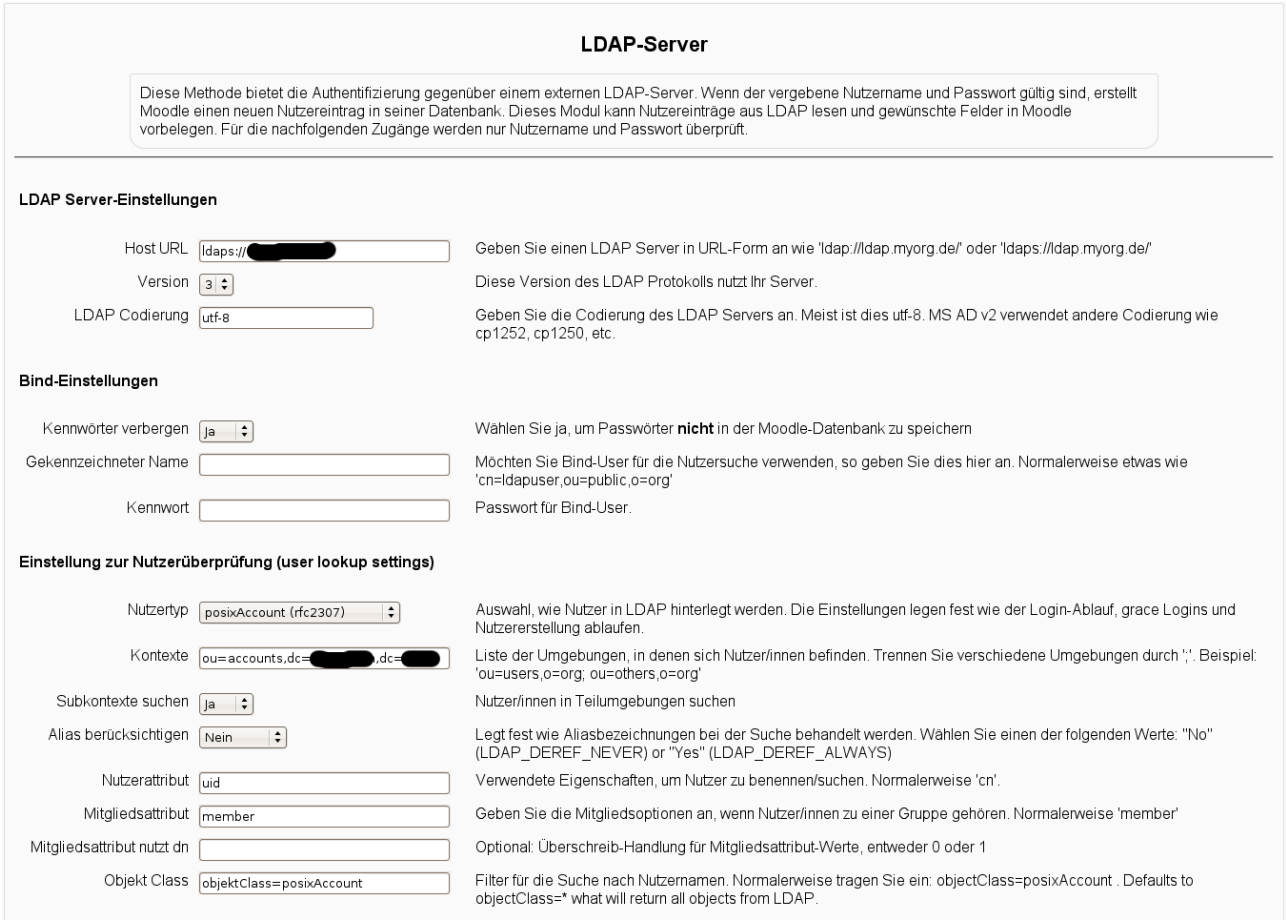
# 2. Umstellen auf LDAP

Folgende Einstellungen sind im Moodle vorzunehmen, um die Benutzerauthentifizierung über den LDAP / LDAPS -Server der paedML Linux einzurichten:

Melden Sie sich als admin (s.o.) an Ihrem Moodle an. Gehen Sie im Block Website-Administration auf Nutzer /innen – Authentifizierung – Übersicht. „Öffen“ Sie dort in der Zeile LDAP Server „das Auge“ und wählen Sie dann Einstellungen.

# 3. LDAP Server Einstellungen

Auf der Konfigurationsseite sind folgende Einstellungen vorzunehmen:




LDAP Server Einstellungen

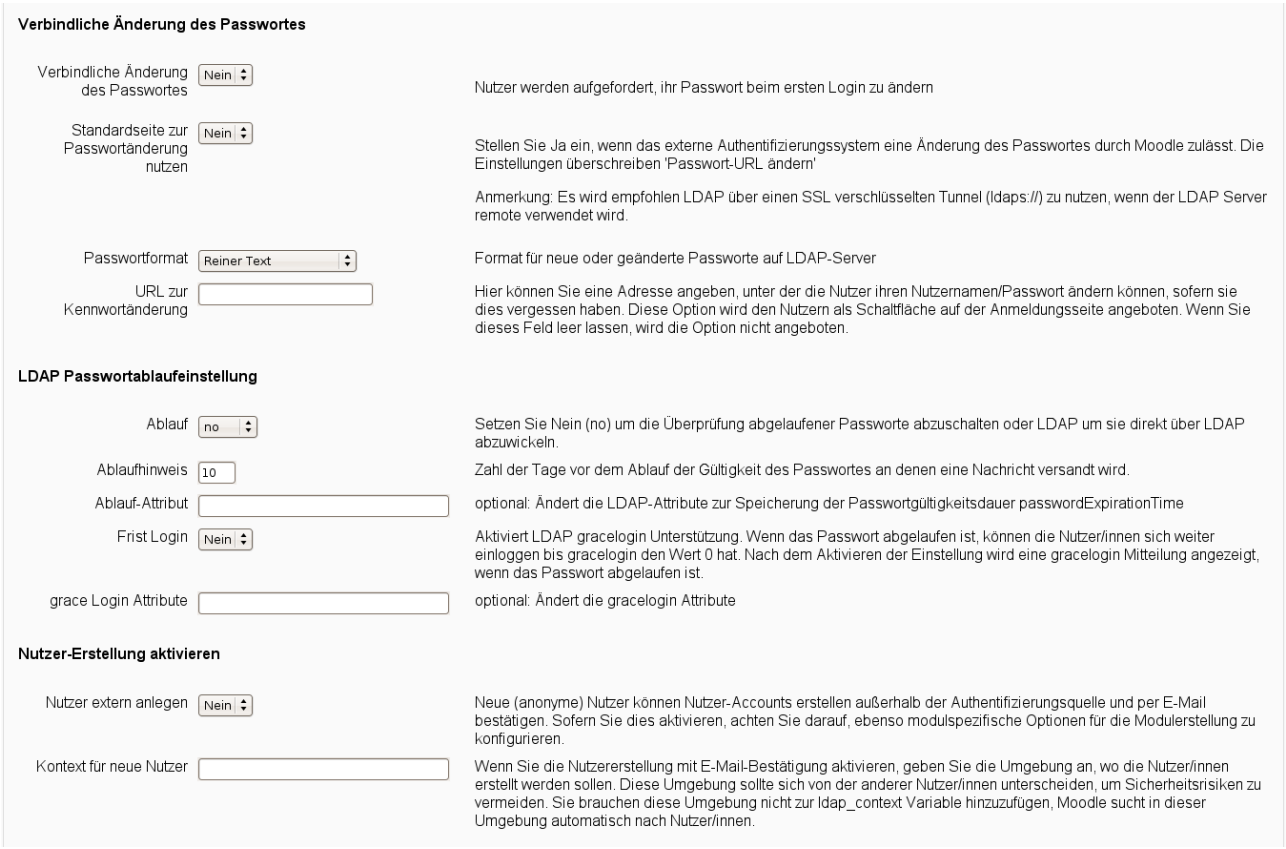
| | |
|---|---|
| Host URL: | *ldaps: //<IPAdresse>*<br>aus Sicherheitsgründen lässt der paedML Linux Server eine einfache Abfrage per ldap nicht mehr zu. Es muss ldaps verwendet werden. |
| Version: | *3* |
| LDAP Codierung: | *utf-8* |

Bind-Einstellungen

| | |
|---|---|
| Kennwörter verbergen (ldap-preventpassindb): | *nein* |
| Gekennzeichneter Name (ldap bind dn) | *Leer lassen* |
| Kennwort (ldap bind_pw): | *Leer lassen* |

Einstellung zur Nutzerüberprüfung (user lookup settings)

| | |
|---|---|
| Nutzertyp (ldap user type): | *posixAccount (rfc2307 )* |
| Kontexte (ldap contexts) | *ou=accounts,* ***dc=linuxmuster, dc=local***<br>(der komplette Pfad muss wie oben eingetragen werden. Die Information für den fettgedruckten Teil muss in der Datei /etc/ldap/ldap.conf am Server nachgeschaut werden. Der Eintrag nach BASE muss komplett übernommen werden. Die Einträge müssen durch Leerzeichen und Komma getrennt werden. |
| Suchkontexte: (ldap_search_sub): | *ja* |
| Alias berücksichtigen: (ldap opt deref ) | *nein* |
| Nutzerattribut: (ldap user attribute) | *uid* |
| Mitgliedsattribut: (ldap-memberattribute) | *member* |
| Mitgliedsattribut nutzt dn | *leer* |
| Objekt Class (ldap objectclass) | *objektClass=posixAccount* |




Verbindliche Änderung des Passwortes

| | |
|---|---|
| Verbindliche Änderung des Passwortes: | *nein* |
| Standardseite zur Passwortänderung nutzen: | *nein* |

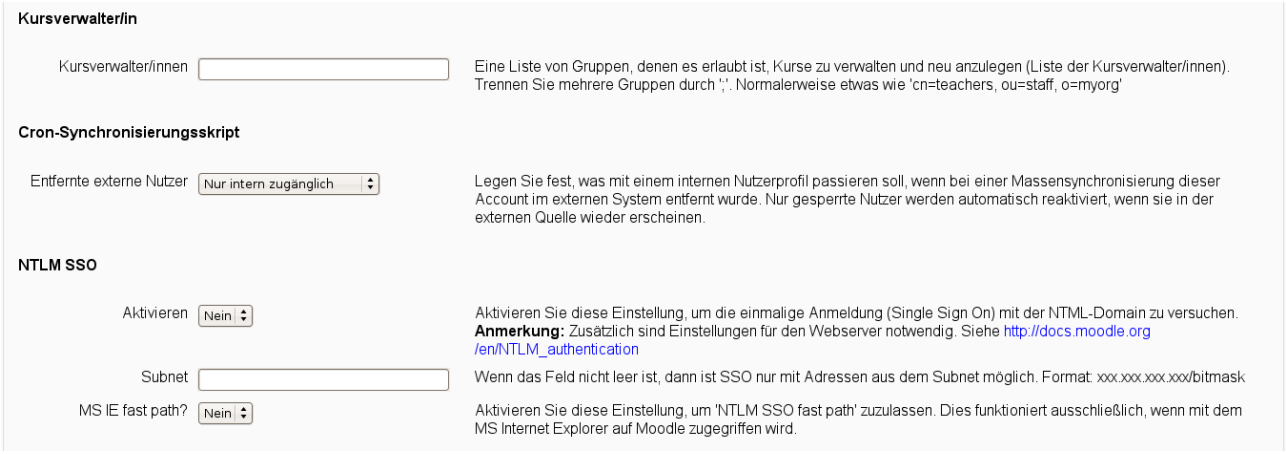
| | |
|---|---|
| Passwortformat: | *Reiner Text* |
| URL zur Kennwortänderung: | *Leer lassen* |

LDAP Passwortablaufeinstellung

| | |
|---|---|
| Ablauf: (ldap expiration) | *no* |
| Ablaufhinweis: (ldap expiration warning) | *10* |
| Ablaufattribut: (ldap expireattr) | *Leer lassen* |
| Frist Login: (ldap_gracelogins) | *nein* |
| grade Login Attribute: (ldap_graceattr) | *Leer lassen* |

Nutzer Einstellung aktivieren

| | |
|---|---|
| Nutzer extern anlegen: | *nein* |
| Kontext für neue Nutzer: (ldap_create_context) | *Leer lassen* |




Kursverwalter/in

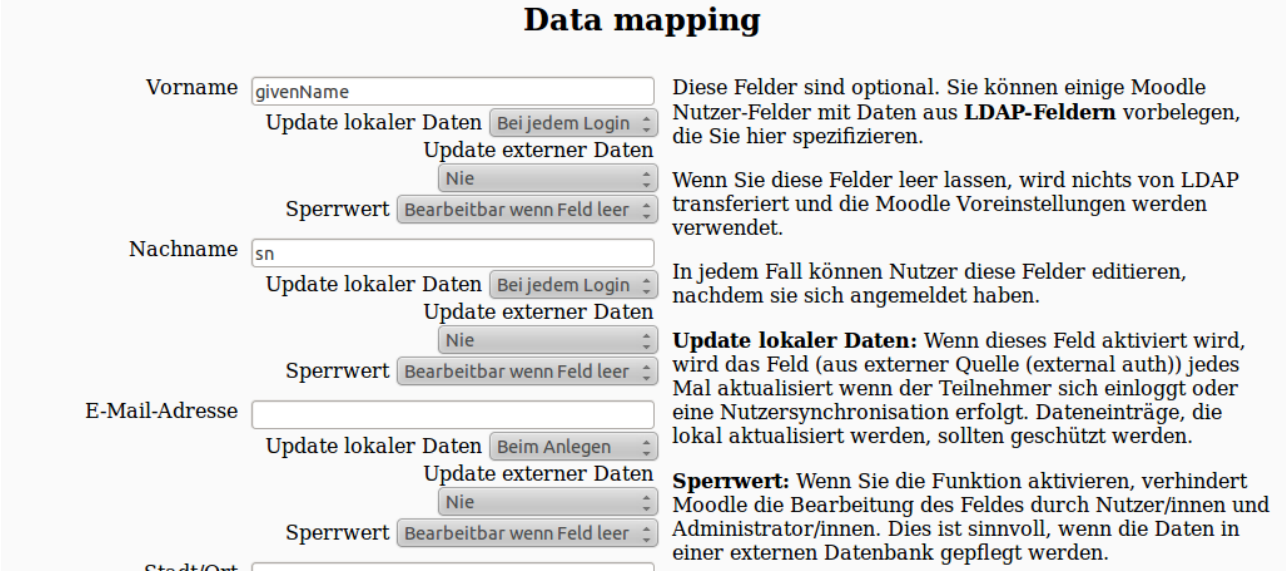
| | |
|---|---|
| Kursverwalter/innen: (ldap_creators): | *Leer lassen* |

Cron-Synchronisierungsskrip

| | |
|---|---|
| Entfernte externe Nutzer | *Nur intern zugänglich* |

NTLM SSO

| | |
|---|---|
| Aktivieren | *nein* |
| Subnet | *Leer lassen* |
| MS IE fast path? | *nein* |




Data mapping

Um Daten der Nutzer per ldaps Abfrage gleich in die Felder des Moodle Profils einzutragen, konfigurieren Sie in *Data mapping* die Felder Vorname und Nachname wie auf dem Bild oben zu sehen. Falls Sie die schulischen e-mail Adressen nutzen wollen, können Sie im Feld *E-Mail-Adresse* den Eintrag *mail* vornehmen. Die restlichen Felder lassen Sie leer.

# 4. Hinweise zur Umstellung auf ldaps

## 4.1. Neu installiertes Moodle

Am einfachsten verläuft die Umstellung auf die ldap/ldaps Authentifizierung, wenn man in einem neu eingerichteten Moodle von Anfang per ldap/ldaps authentifizieren lässt. Bis auf administrative Nutzer, die manuell angelegt werden, authentifizieren sich alle Nutzer des Moodle dann über ldaps gegenüber dem eingetragenen Server.

## 4.2. Laufendes Moodle

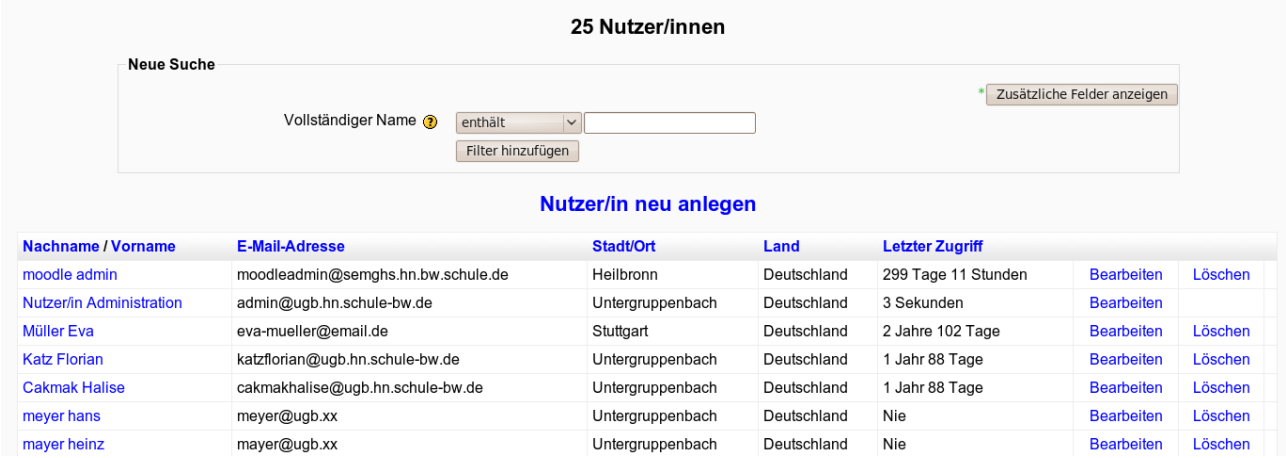
Auf einem laufenden Moodle muss man je nach Situation unterschiedlich vorgehen.

### 4.2.1. Manuelle Änderung

Wenn bisher nur wenige Nutzer manuell aufgenommen wurden, dann kann man diese von Hand auf die neue Authentifizierung umstellen. Voraussetzung dazu ist, dass der manuell vergebene Nutzername mit dem Nutzernamen auf der paedML übereinstimmt.

Vorgehensweise

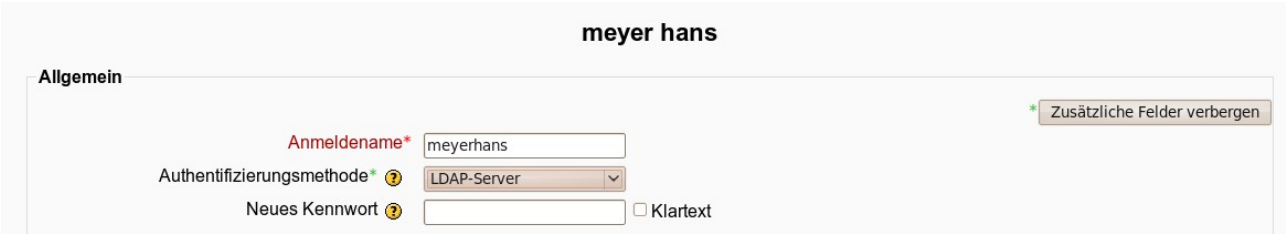
Melden Sie sich als admin an Ihrem Moodle an. Gehen Sie im Administrationsblock zu *Nutzer/innen – Nutzerkonten – Nutzerliste* anzeigen. Wählen Sie die Nutzer nacheinander über *Bearbeiten* aus.




| Nachname / Vorname | E-Mail-Adresse | Stadt/Ort | Land | Letzter Zugriff | | |
|---|---|---|---|---|---|---|
| moodle admin | moodleadmin@semghs.hn.bw.schule.de | Heilbronn | Deutschland | 299 Tage 11 Stunden | Bearbeiten | Löschen |
| Nutzer/in Administration | admin@ugb.hn.schule-bw.de | Untergruppenbach | Deutschland | 3 Sekunden | Bearbeiten | |
| Müller Eva | eva-mueller@email.de | Stuttgart | Deutschland | 2 Jahre 102 Tage | Bearbeiten | Löschen |
| Katz Florian | katzflorian@ugb.hn.schule-bw.de | Untergruppenbach | Deutschland | 1 Jahr 88 Tage | Bearbeiten | Löschen |
| Cakmak Halise | cakmakhalise@ugb.hn.schule-bw.de | Untergruppenbach | Deutschland | 1 Jahr 88 Tage | Bearbeiten | Löschen |
| meyer hans | meyer@ugb.xx | Untergruppenbach | Deutschland | Nie | Bearbeiten | Löschen |
| mayer heinz | mayer@ugb.xx | Untergruppenbach | Deutschland | Nie | Bearbeiten | Löschen |

und aktivieren Sie Zusätzliche Felder anzeigen.


Ändern Sie nun die Authentifizierungsmethode von Manuelle Zugänge auf LDAP-Server.




Führen Sie diesen Vorgang bei allen Nutzern durch.

### 4.2.2. Manuelle angelegte Nutzer löschen

Ist die Anzahl der manuell angelegten Nutzer zu groß, so ist die folgende Vorgehensweise sinnvoll:

- Sichern sie alle Kurse ohne Nutzer
- löschen Sie alle Nutzer per bulk Verwaltung
- löschen Sie alle Kurse
- importieren Sie die Kurse wieder in Ihr Moodle
- stellen Sie sicher, dass sich alle Nutzer wieder an Ihrem Moodle registrieren.