Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

# Anleitung

LDAP und LDAPs für externe Dienste wie Moodle und WebUntis anbinden

Stand 04.10.2023

## paedML® Linux / GS

Version: 7.2

paedML L

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG

**Herausgeber**

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

**Autoren**

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Johannes Albani

**Endredaktion**

Kay Höllwarth

**Bildnachweis**

Symbole von “The Noun Project” (www.thenounproject.com)

**Weitere Informationen**

www.support-netz.de
www.lmz-bw.de

**Änderungen und Irrtümer vorbehalten.**

Veröffentlicht: 2023

# Inhaltsverzeichnis

**1 Vorwort ..... 4**

**2 Vorgehen 1: LDAPs mit Zertifikat ..... 5**

*2.1 Installation und Konfiguration von nginx ..... 5*

*2.2 pfSense Firewall Konfiguration ..... 6*

**3 Vorgehen 2: LDAPs ohne öffentliches Zertifikat ..... 10**

*3.1 PfSense NAT Einstellungen ..... 10*

*3.2 Portweiterleitung am Router ..... 11*

**4 Moodle per LDAP anbinden ..... 12**

*4.1 Authentifizierung von Benutzern ..... 12*

4.1.1 Aktive Plugins ..... 12
4.1.2 LDAP-Server-Einstellungen ..... 12
4.1.3 Bind-Einstellungen ..... 13
4.1.4 Nutzersuche (user lookup) ..... 14
4.1.5 Kennwortänderung fordern ..... 15
4.1.6 Einstellungen zum Ablauf von LDAP-Kennwörtern ..... 15
4.1.7 Nutzererstellung aktivieren ..... 16
4.1.8 Zuordnung von Systemrollen ..... 16
4.1.9 Synchronisierung von Nutzerkonten ..... 17
4.1.10 NTLM-SSO ..... 17
4.1.11 Datenzuordnung ..... 18
4.1.12 Abschluss ..... 23

*4.2 Automatisches Einschreiben ..... 24*

4.2.1 Aktive Plugins ..... 24
4.2.2 Einstellung für LDAP-Server und Bind-Einstellungen ..... 24
4.2.3 Rollenabbildung ..... 25

*4.3 Synchronisierung automatisieren ..... 28*

*4.4 Profilfeld-basierende Zuweisung globaler Gruppen ..... 29*

4.4.1 Gruppen anlegen ..... 29
4.4.2 Benutzer zuweisen ..... 29
4.4.3 Geplante Aufgabe prüfen ..... 30

**5 WebUntis ..... 31**

*5.1 Konfiguration ..... 32*

# 1 Vorwort

Der Verzeichnisdienst LDAP verwaltet nicht nur Benutzer, Gruppen und vieles mehr innerhalb des Schulhauses, er kann auch verwendet werden, um viele externe Dienste mit Benutzerdaten zu befüllen. So können sich Schülerinnen und Schüler mit ihren Zugangsdaten für die Computerräume auch z.B. bei Moodle, WebUntis und vielen weiteren Diensten einsetzen, sobald diese konfiguriert wurden.

In diesem Dokument stellen wir für den Verzeichnisdienst zwei Wege vor: LDAPs mit selbst signiertem Zertifikat (Kapitel 3) und LDAPs mit dem Zertifikat der paedML Nextcloud (Kapitel 2). Ersteres ist etwas leichter umsetzbar und setzt keine Nextcloud voraus, letzteres ist jedoch universeller einsetzbar und wird von manchen Diensten wie WebUntis zwingend vorausgesetzt.

In Kapitel 4 wird neben der Benutzerauthentifizierung (Kapitel 4.1) vor allem die Profilfeld-basierende Zuweisung globaler Gruppen (Kapitel 4.4) beschrieben, welche für einige paedML Kunden ein wichtiges Feature auf dem Wunschzettel für die Lösung war.

In Kapitel 5 wird die Erstellung von Accounts in WebUntis beschrieben, welche aufgrund der SchülerID dann direkt mit den Stammdaten in WebUntis verbunden werden können.

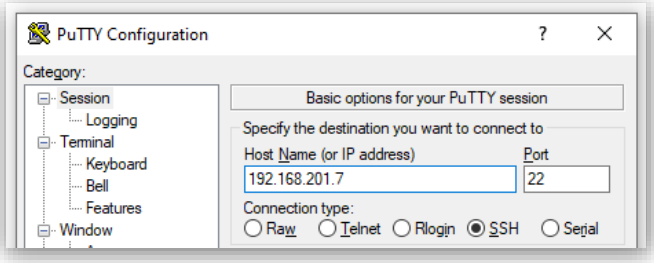
Vergessene Passwörter oder uneinheitliche Benutzernamen sollten damit großteils der Vergangenheit angehören. Und falls doch einmal Login-Probleme bestehen, können Lehrerinnen und Lehrer per Schulkonsole die Kennwörter unkompliziert zurücksetzen.

# 2 Vorgehen 1: LDAPs mit Zertifikat

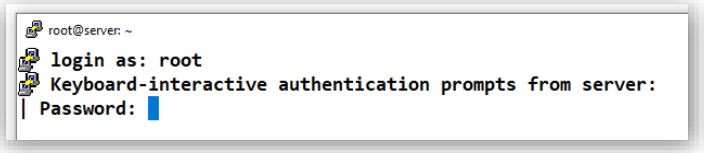
Wir empfehlen Ihnen diese Konfiguration, wenn Sie Dienste per LDAPs mit dem paedML-Server verbinden möchten, die ein öffentliches Zertifikat voraussetzen, z.B. WebUntis. Falls Sie dies nicht benötigen, kann der „einfachere“ Weg mit dem selbst ausgestellten Zertifikat (siehe Kapitel 3) gewählt werden.

## 2.1 Installation und Konfiguration von nginx

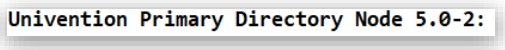
Öffnen Sie Putty und verbinden Sie sich auf die Nextcloud (in der Regel 192.168.201.7).




Und melden sich als root mit dem passenden Kennwort an:




Nach dem Login sollten Sie auch die Server-Version sehen können.

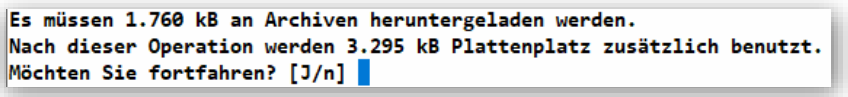



Der folgende Befehl funktioniert erst ab UCS-Version 5.0. Wenn Sie noch eine ältere UCS-Installation haben sollten, führen Sie bitte zunächst das Upgrade durch. Dies ist in der „Upgradeanleitung Nextcloud auf UCS 5“ beschrieben, die sie hier abrufen können: https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-linux/downloads#updates

Starten Sie den Befehl

```
univention-install nginx
```

Und bestätigen Sie die Installation mit „J“:




Nun muss die Datei */etc/nginx/nginx.conf* bearbeitet werden. Dies können Sie entweder über Putty mit einem Editor wie nano, mc oder vi tun, oder Sie verwenden WinSCP und verbinden sich wieder zur 192.168.201.7, melden sich als root an und navigieren zu dem Ordner.

In der Datei müssen die Zeilen

```
include /etc/nginx/conf.d/*.conf;
include /etc/nginx/sites-enabled/*;
```

mit einer vorangestellten Raute (#) auskommentiert werden.

```
#       include /etc/nginx/conf.d/*.conf;
#       include /etc/nginx/sites-enabled/*;
```

Am Ende der Datei fügen Sie nun folgenden Code ein:

```
stream {
      server {
            listen 8636 ssl;
            proxy_pass 10.1.0.1:7636;
            proxy_ssl on;
            ssl_certificate /etc/univention/letsencrypt/signed_chain.crt;
            ssl_certificate_key /etc/univention/letsencrypt/domain.key;
      }
}
```

Zur Erklärung: Der nginx-Server wird nun auf den Port 8636 hören. Anfragen auf diesem Port werden mit dem SSL-Zertifikat der Nextcloud signiert und die Anfrage auf dem LDAPs Port des paedML-Servers weitergeleitet.

Starten Sie per Putty den nginx Service neu.

```
service nginx restart
```

Die interne Firewall des Nextcloud-Servers muss nun Anfragen auf dem Port 8636 annehmen, führen Sie dazu per Putty die folgenden Befehle aus:

```
ucr set security/packetfilter/lmz-nginx/tcp/8636/all='ACCEPT'
ucr set security/packetfilter/lmz-nginx/tcp/8636/en='LDAPS'
```

und starten Sie die Firewall neu

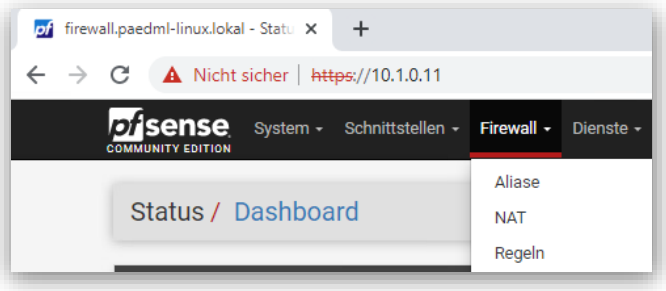
```
[ -x "/etc/init.d/univention-firewall" ] && invoke-rc.d univention-firewall
restart
```

Die Arbeiten auf der Nextcloud sind damit erledigt.

## 2.2 pfSense Firewall Konfiguration

Nun müssen externe Anfragen von der pfSense Firewall auf dem Port 636 auf den Port 8636 der Nextcloud weitergeleitet werden.

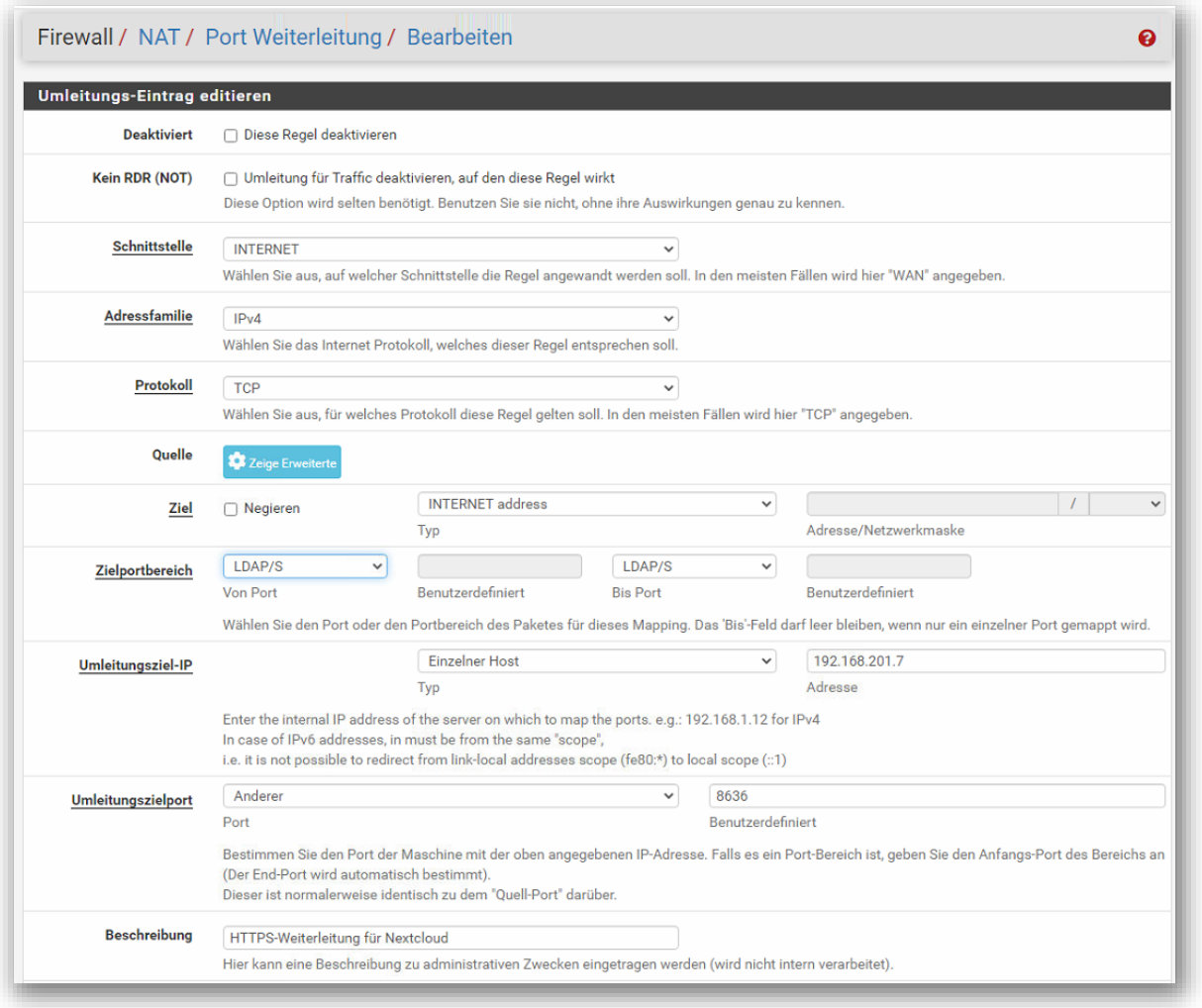
Öffnen Sie die Adresse der Firewall 10.1.0.11 in einem Browser und melden sich als Administrator an. Dort klicken Sie auf Firewall – NAT



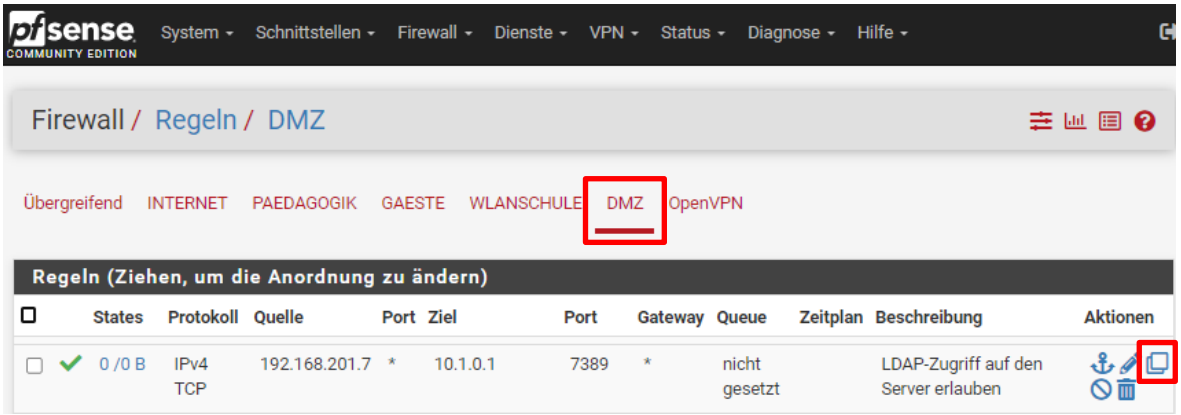

Mit einem Klick auf Hinzufügen ( Hinzufügen ) erstellen Sie eine neue Weiterleitungs-Regel. In dieser wählen Sie beim Zielportbereich LDAP/S aus, Umleitungsziel-IP auf die Nextcloud 192.168.201.7 und der

Umleitungszielport auf Anderer 8636. Als Beschreibung geben Sie z.B. „LDAPs-Weiterleitung zur Nextcloud“ ein.

Klicken Sie ganz unten auf der Seite auf Speichern.

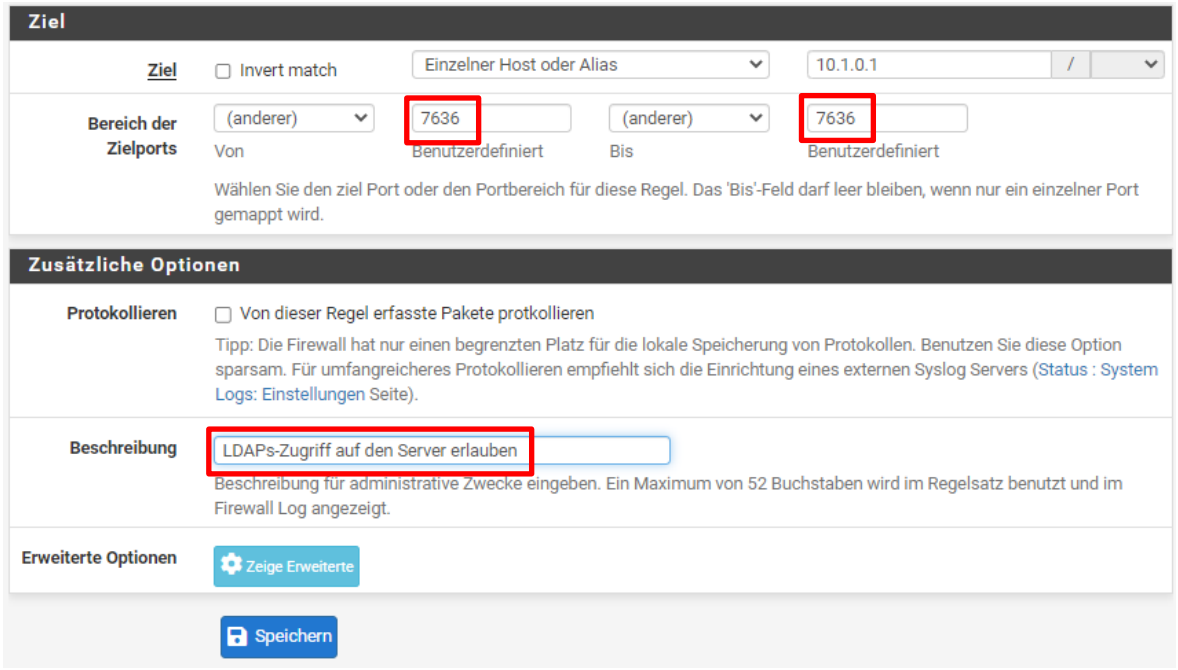



Nun muss noch die Kommunikation zwischen Nextcloud und dem paedML Server über den LDAPs Port 7636 erlaubt werden.

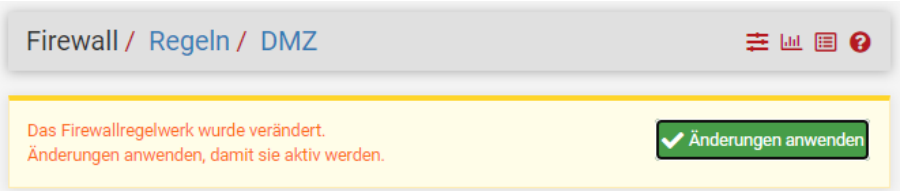



Öffnen Sie Firewall – Regeln und Wählen Sie DMZ.

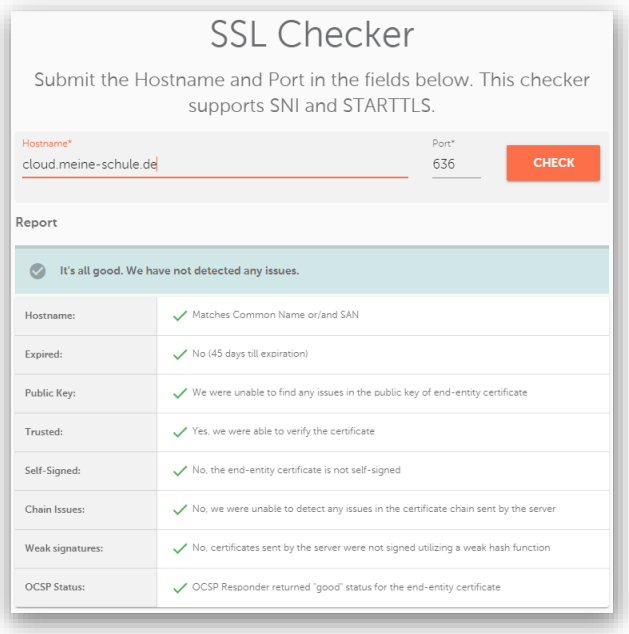
Es besteht bereits eine Regel mit dem Ziel 10.1.0.1 und dem Port 7389, kopieren Sie diese mit einem Klick auf das Quadratische Symbol bei „Aktionen“.




Ändern Sie bei „Ziel“ den Port an beiden Stellen von 7389 auf 7636 und Passen Sie die Beschreibung so an, dass es als LDAPS erkennbar ist. Mit einem Klick auf Speichern ist die Konfiguration beendet. Klicken Sie oben noch auf „Änderungen anwenden“ um die Regel sofort zu aktivieren.



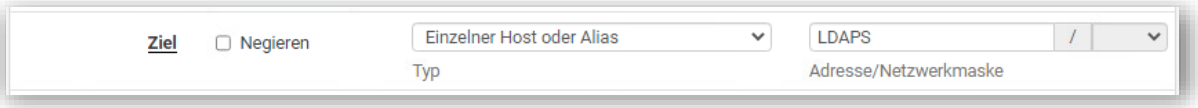

Optional können Sie testen, ob der Server unter der Adresse Ihrer Nextcloud auf dem Port 636 erreichbar ist, z.B. mit der Seite https://decoder.link/sslchecker. Geben Sie dort die Adresse Ihrer Nextcloud und den Port 636 ein. Mit einem Klick auf CHECK sollte das Zertifikat erkannt werden.



Falls Ihr System nicht antworten sollte, müssen Sie gegebenenfalls an Ihrem Internetzugang Portweiterleitungen konfigurieren, siehe Kapitel 3.2.

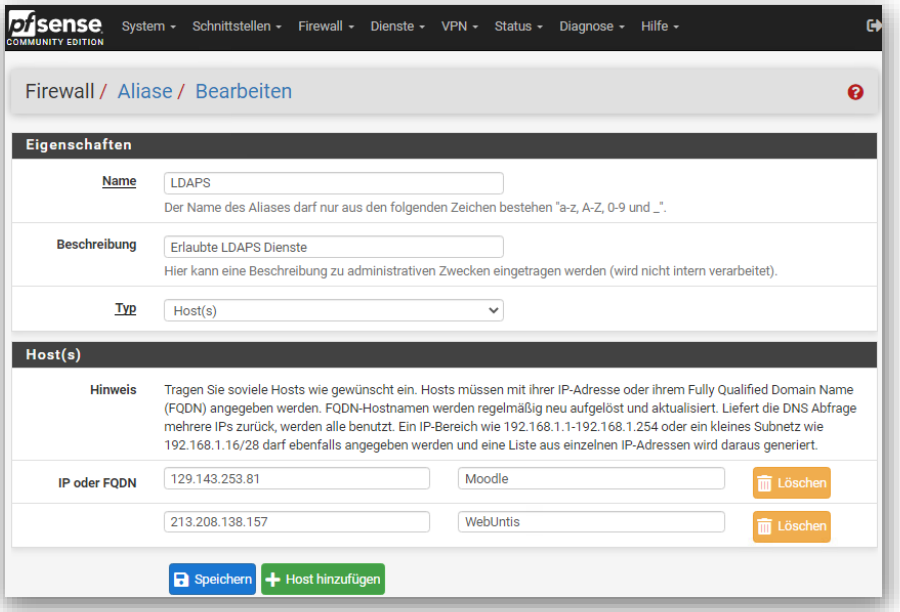
Sobald die Einrichtung abgeschlossen ist, können Sie optional noch einschränken, welche Adressen aus dem Internet den Port 636 auf Ihrem Server erreichen können. Dazu wählen Sie Firewall – Aliase und wählen dort Hinzufügen. Hier vergeben Sie einen Namen, z.B. „LDAPS“, und können die IP-Adressen Ihrer Dienste eintragen, welche für die LDAPs Verbindung freigegeben werden. Die IP-Adressen der benötigten Dienste können Sie über einen Ping Befehl herausfinden oder beim jeweiligen Dienstleister erfragen.

Klicken Sie im Anschluss auf Speichern, um das Alias zu erstellen. Öffnen Sie erneut die NAT – Regel und bearbeiten Sie die gerade angelegte Weiterleitung mit dem „Stift Symbol“.




Das Feld „Ziel“ ändern Sie nun von „INTERNET adress“ auf „Einzelner Host oder Alias“ und tragen dort den Namen des Alias ein, also „LDAPS“. Klicken Sie erneut auf Speichern.

Für Fehlersuche oder Einrichtung von neuen Diensten kann es sinnvoll sein das Ziel wieder auf „INTERNET adress“ umzustellen, bis die Einrichtung abgeschlossen und erfolgreich ist.



# 3 Vorgehen 2: LDAPs ohne öffentliches Zertifikat

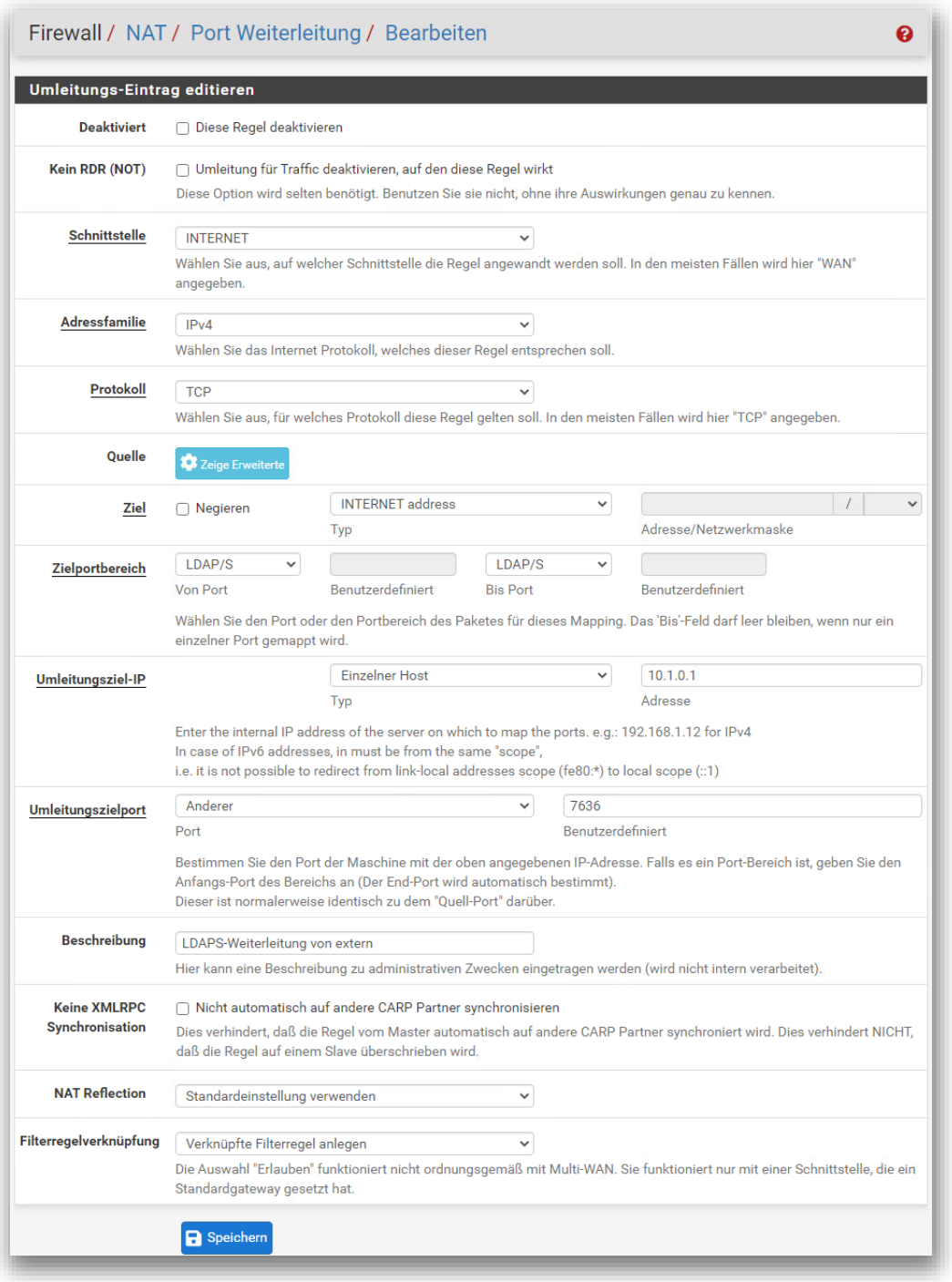
Bis auf WebUntis scheinen die meisten externen Dienste das Zertifikat der LDAPs Verbindung nicht zu prüfen, daher können Sie auch das paedML-interne Zertifikat verwenden und damit die Nextcloud komplett umgehen.

## 3.1 PfSense NAT Einstellungen

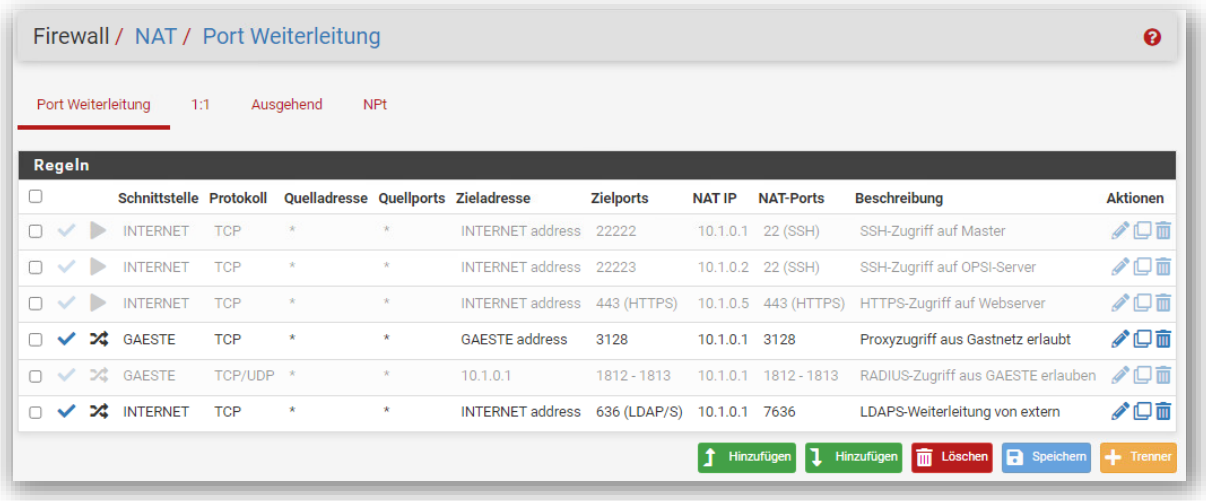
In Ihrer lokalen pfSense muss unter Firewall --> NAT --> Portweiterleitung

eine Regel für den Zugriff auf das LDAP des Servers eingerichtet werden.

Für die Weiterleitungs-Regel werden folgende Einstellungen vorgenommen:



Die Regel sollten nach dem Speichern wie folgt angezeigt werden. Gegebenenfalls sind in Ihrer Firewall noch weitere Regeln definiert.




## 3.2 Portweiterleitung am Router

An Ihrem Router oder weiterer Firewall müssen Sie möglicherweise eine Portweiterleitung für den Port 7636 einrichten. Diese Weiterleitung muss auf die externe IP-Adresse der pfSense zeigen.

Falls Sie eine feste IP-Adresse bei BelWue bzw. einen Internetanschluss von BelWue haben, so nehmen Sie bitte Kontakt mit BelWue zur Freischaltung des Ports 7636 auf.

Falls Sie einen anderen Anbieter nutzen, z.B. ein Telekom@School-Anschluss, so müssen Sie die Portweiterleitung an Ihrem Router einrichten.

# 4 Moodle per LDAP anbinden

Die LDAP-Verbindung mit Moodle unterteilt sich in mehrere Abschnitte. Bei der Authentifizierung von Benutzern (Kapitel 4.1) ermöglichen Sie Lehrer*innen und Schüler*innen sich bei Moodle mit den paedML Benutzerdaten anzumelden. Automatisches Einschreiben (Kapitel 4.2) erstellt für Gruppen und Klassen der paedML entsprechende Moodle-Kurse und schreibt Schüler*innen als Teilnehmer und Lehrer*innen als Trainer/Lehrer in die jeweiligen Kurse ein.

Die Teilnehmer können in der Schulkonsole definiert werden und die Änderungen werden nachts von Moodle von einer geplanten Aufgabe übernommen (Kapitel 4.3). Außerdem können Sie Profilfeld-basierende Zuweisung globaler Gruppen verwenden (Kapitel 4.4). Dies ermöglicht das Definieren von Gruppen innerhalb von Moodle. Anhand der Klassenzugehörigkeit werden Schüler-Konten automatisch in diese Gruppen eingeteilt. Diese Option ist vor allem für bestehende Moodle-Kurse sinnvoll da Schülerinnen und Schüler nicht einzeln dem Kurs hinzugefügt werden müssen sondern einfach die Klasse ausgewählt werden kann.

## 4.1 Authentifizierung von Benutzern

### 4.1.1 Aktive Plugins

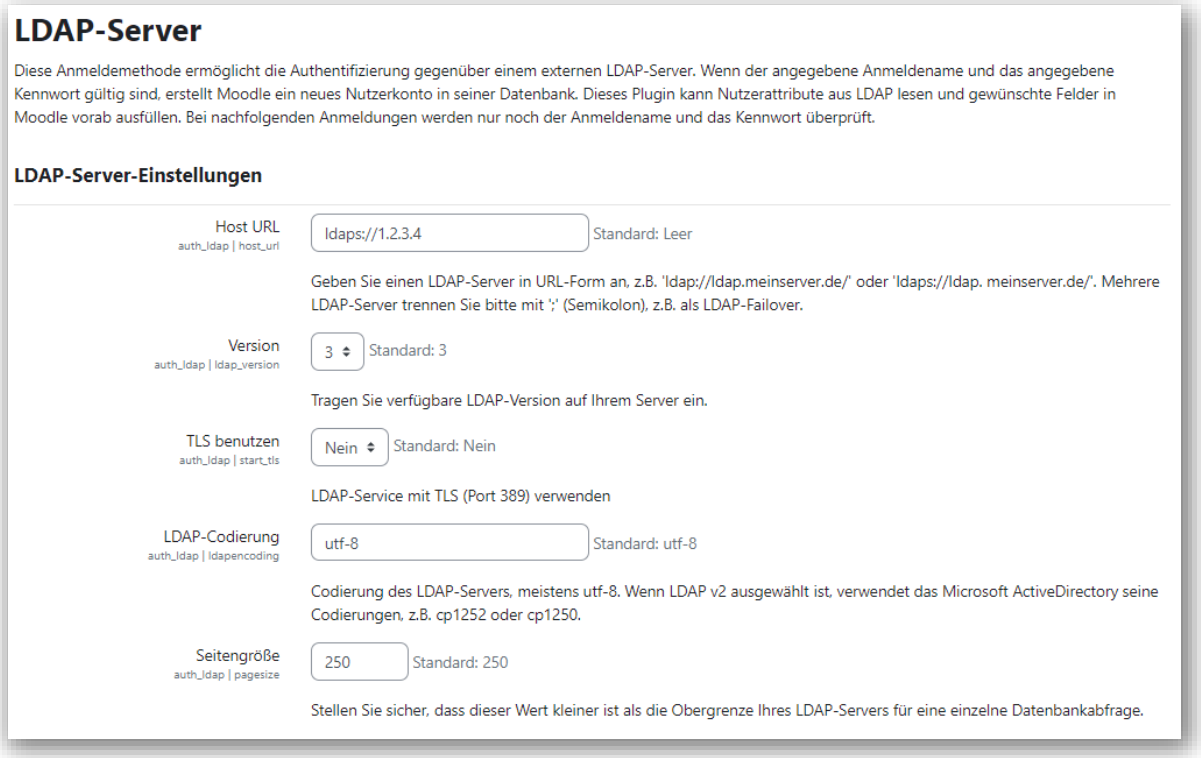
In Moodle muss unter *Website-Administration -> Plugins -> Authentifizierung -> Übersicht* das Plugin „LDAP-Server“ über „Einstellungen“ konfiguriert werden.


### 4.1.2 LDAP-Server-Einstellungen

Der Abschnitt „LDAP-Server-Einstellungen“ muss wie folgt konfiguriert werden.

Für „Host URL“ müssen Sie unterscheiden, welche LDAPs-Konfiguration Sie haben. Für LDAPs mit Zertifikat tragen Sie an der Stelle ldaps://1.2.3.4 die Adresse Ihrer Nextcloud ein, also z.B. ldaps://cloud.meine-schule.de, wobei Sie cloud.meine-schule.de durch Ihre Nextcloud-Adresse ersetzen.

Für LDAPs ohne öffentliches Zertifikat tragen Sie bei „Host URL“ statt der IP-Adresse „1.2.3.4“ Ihre eigene IP-Adresse ein. Falls Sie eine Nextcloud haben, wird der Domänenname anstelle der IP-Adresse von Moodle auch akzeptiert.

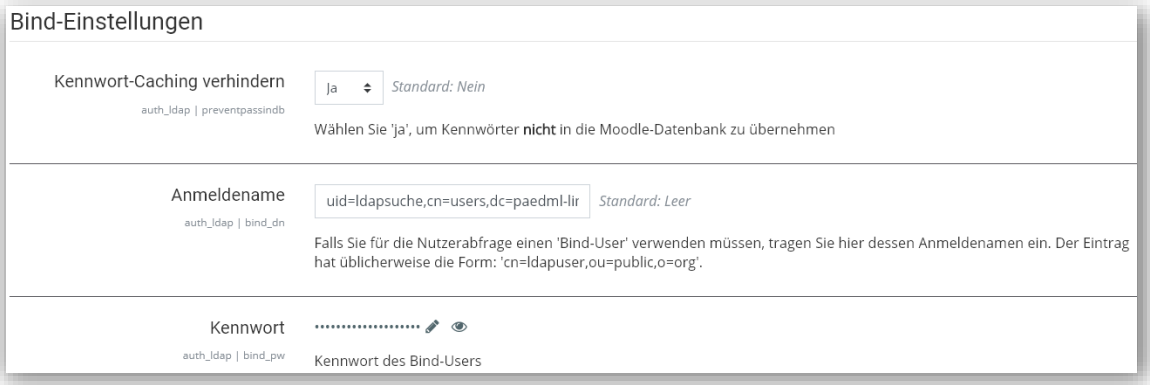



### 4.1.3 Bind-Einstellungen

Unter „Bind-Einstellungen“ tragen Sie ein:

Anmeldename: uid=ldapsuche,cn=users,dc=paedml-linux,dc=lokal

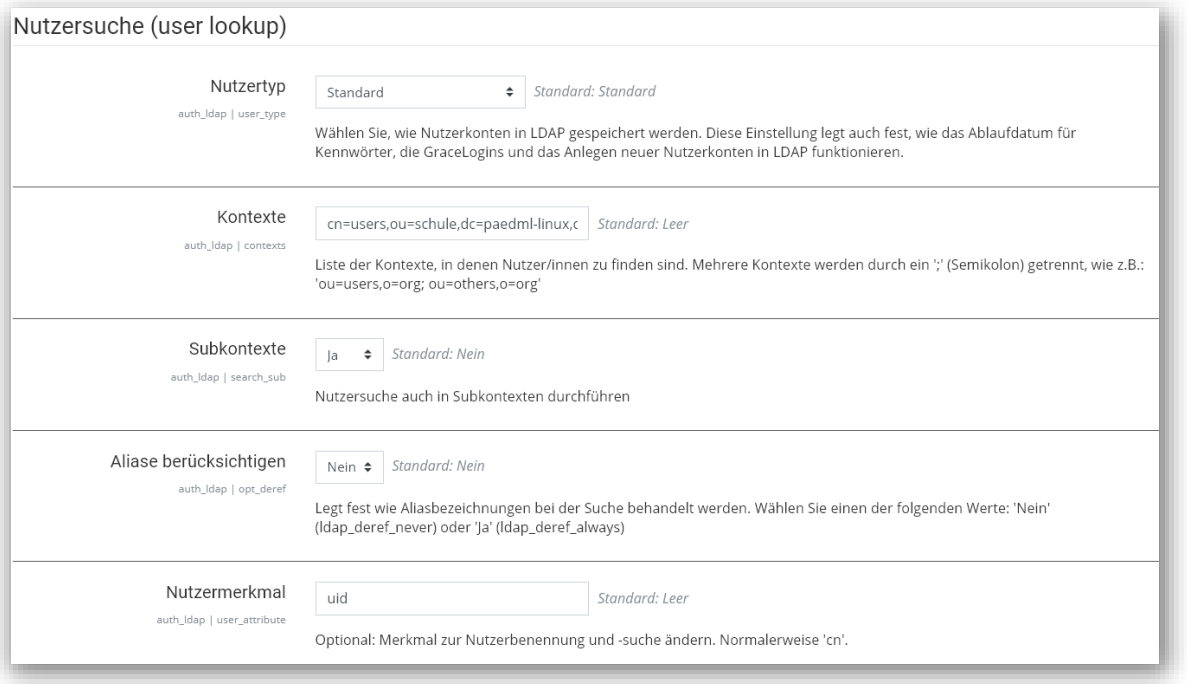
Kennwort: Dieses steht auf dem Server in der Datei /etc/ldapsuche.secret.

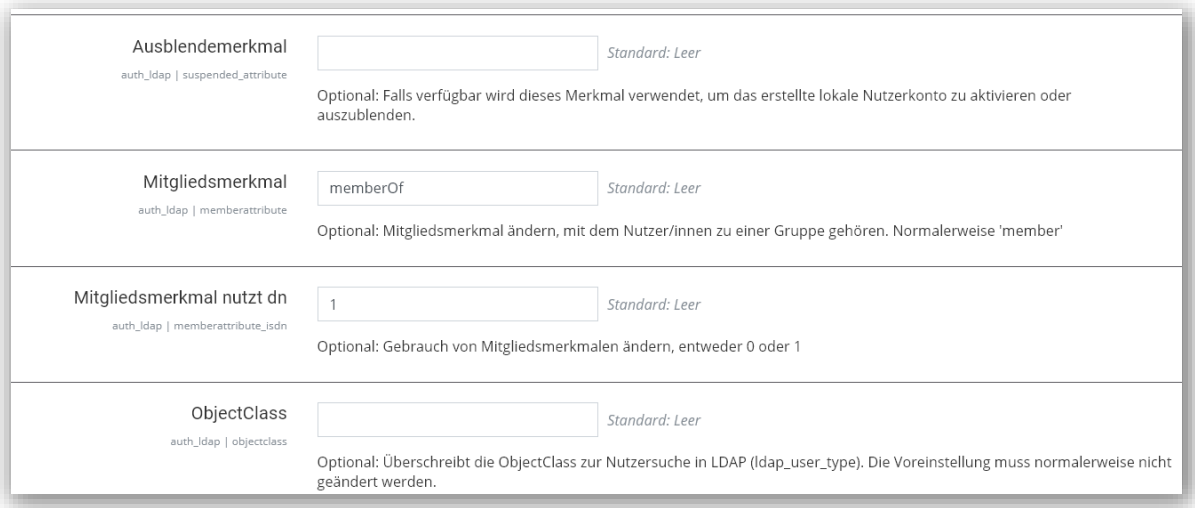


### 4.1.4 Nutzersuche (user lookup)

Bei „Nutzersuche (user lookup)“ ist folgendes einzustellen.

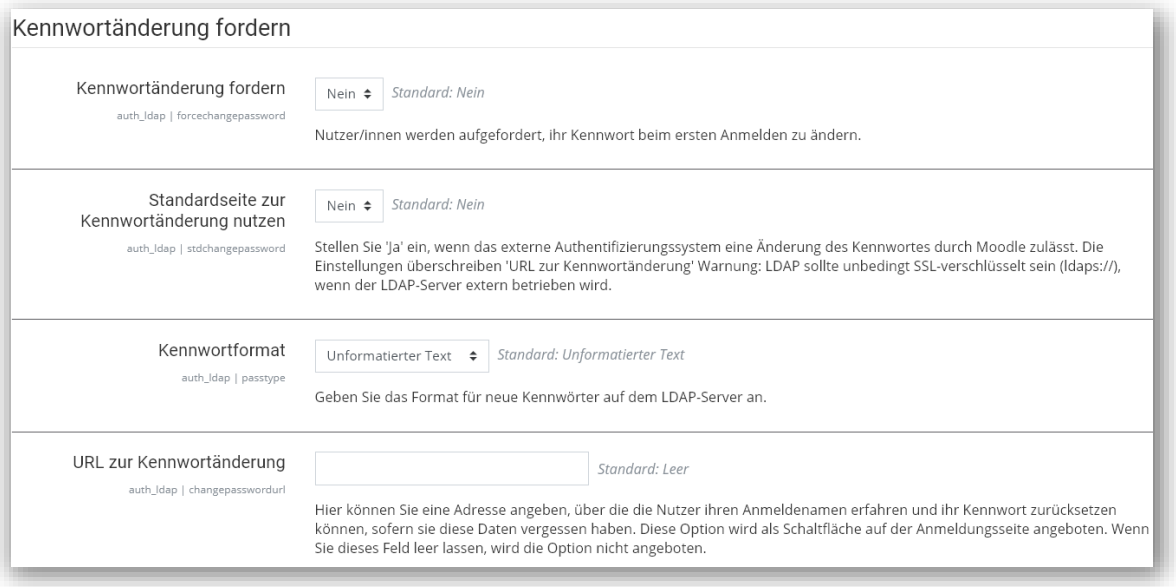
Der Eintrag unter „Kontexte“ lautet: cn=users,ou=schule,dc=paedml-linux,dc=lokal



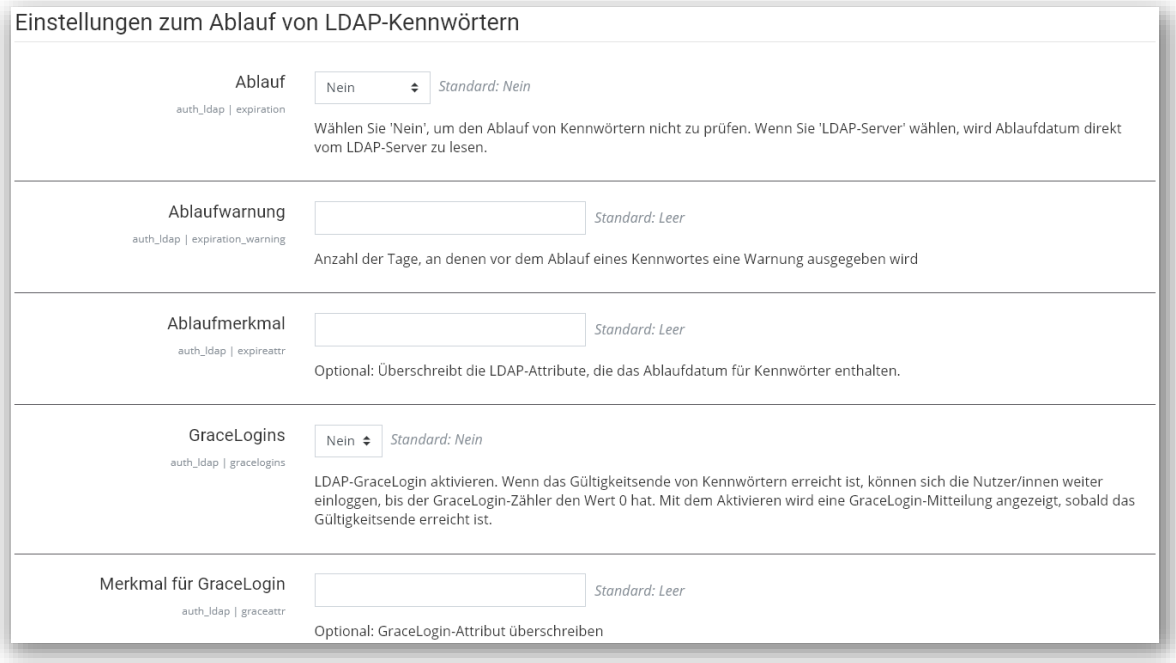
### 4.1.5 Kennwortänderung fordern

Im Abschnitt „Kennwortänderung fordern“ sind die Standardeinstellungen einzustellen.



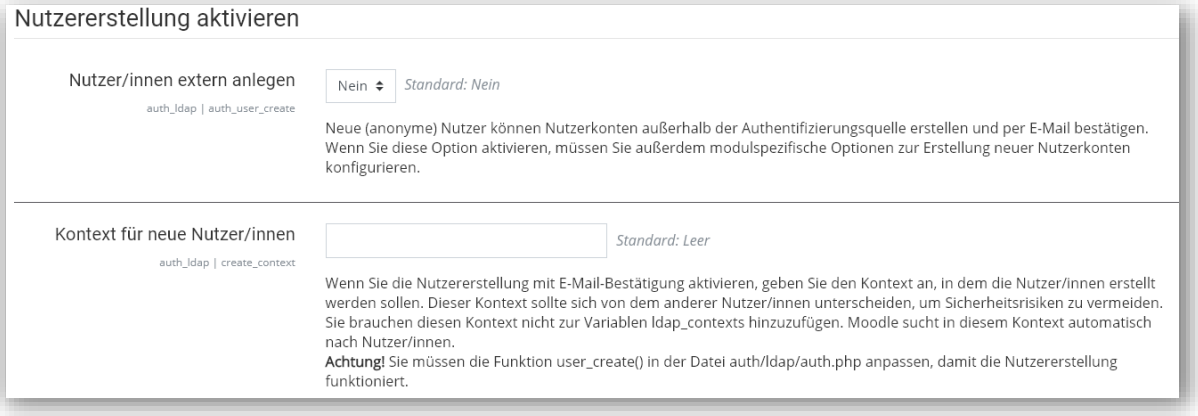

### 4.1.6 Einstellungen zum Ablauf von LDAP-Kennwörtern

Im Abschnitt „Einstellungen zum Ablauf von LDAP-Kennwörtern“ sind die Standardeinstellungen einzustellen.



### 4.1.7 Nutzererstellung aktivieren

Im Abschnitt "Nutzererstellung aktivieren" sind die Standardeinstellungen einzustellen.




### 4.1.8 Zuordnung von Systemrollen

Unter „Zuordnung von Systemrollen“ ist folgendes einzustellen:

Der Eintrag bei „Manager/-in Kontext“ lautet:

*cn=admins,cn=users,ou=schule,dc=paedml-linux,dc=lokal*

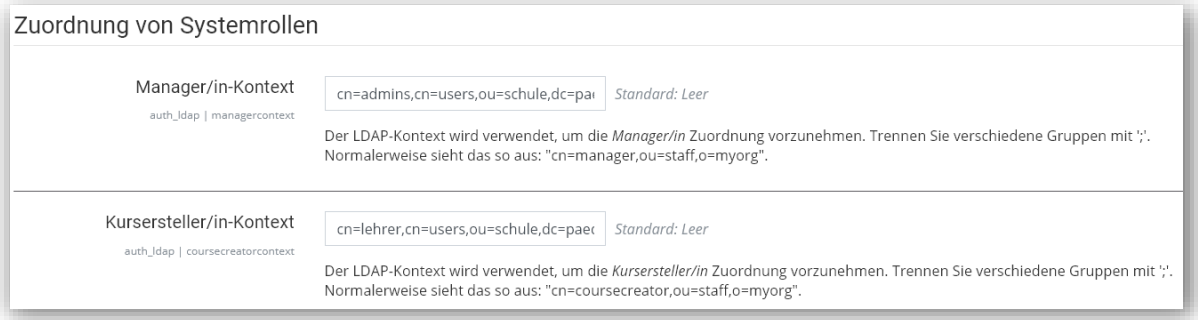
Dies ist in paedML Linux / GS der Benutzer „netzwerkberater“.

Der Eintrag bei „Kursersteller/-in Kontext“ lautet:

*cn=lehrer,cn=users,ou=schule,dc=paedml-linux,dc=lokal*

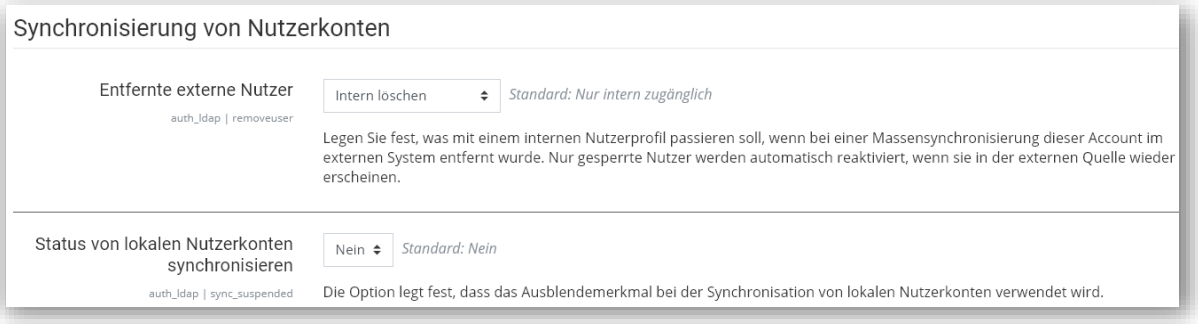
Dies sind in paedML Linux / GS alle Lehrer.

Die anderen Einträge bleiben leer.



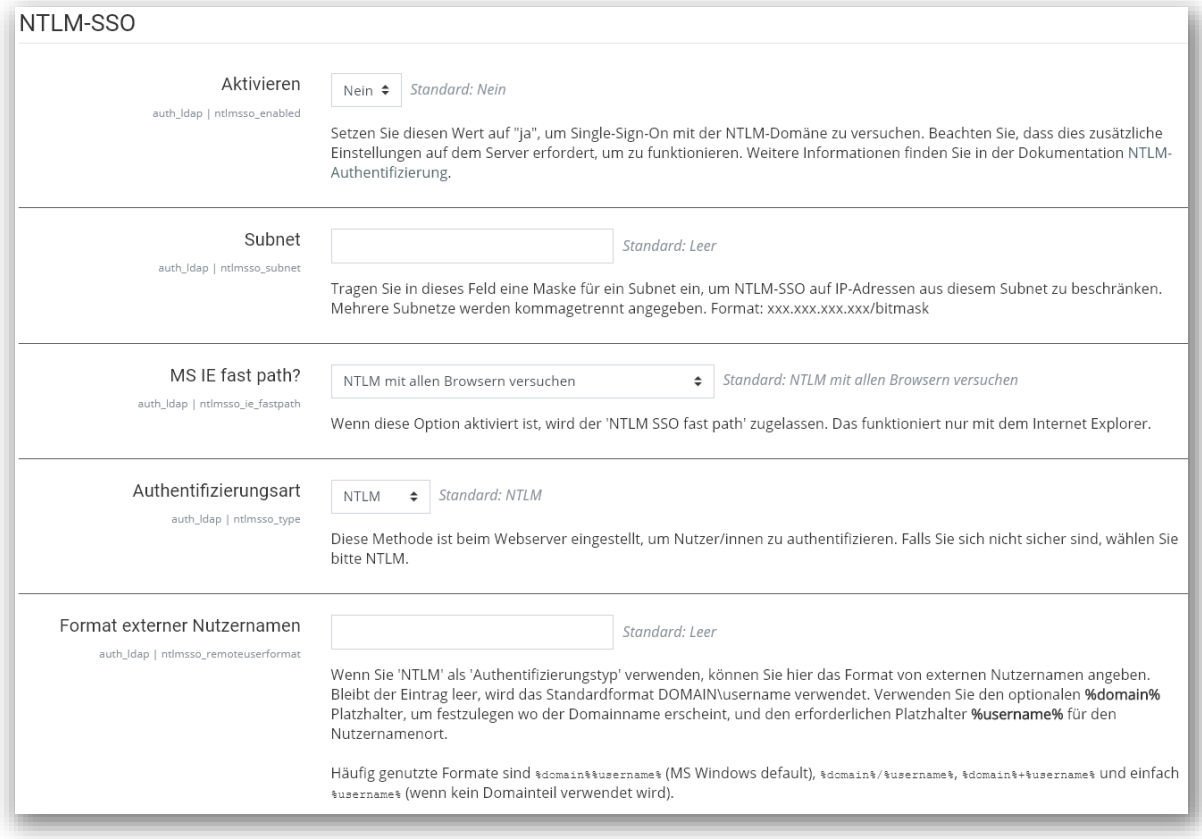
### 4.1.9 Synchronisierung von Nutzerkonten

Bei „Synchronisierung von Nutzerkonten“ ist einzustellen:




### 4.1.10 NTLM-SSO

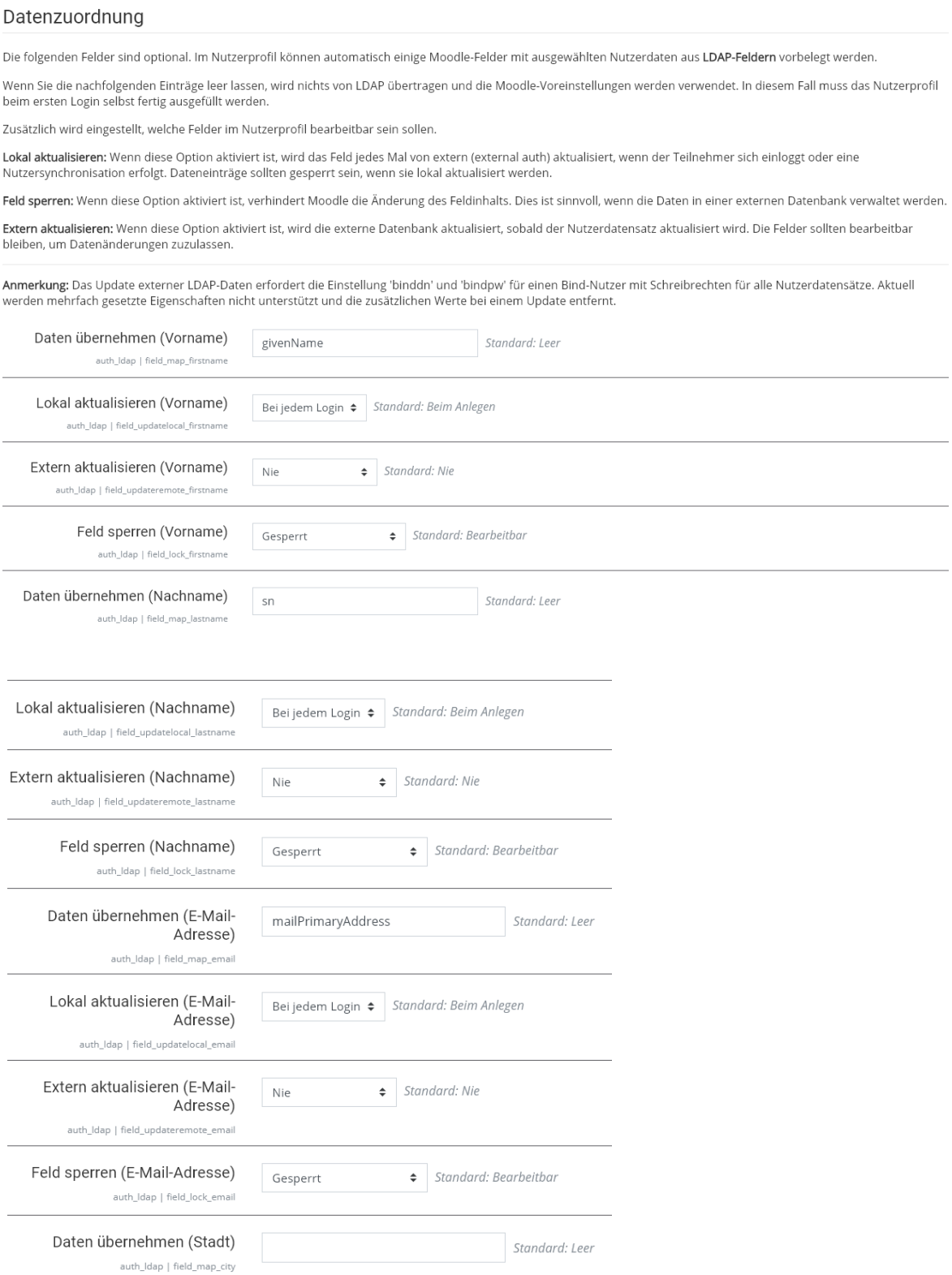
Im Abschnitt „NTLM-SSO“ sind die Standardeinstellungen einzustellen.



### 4.1.11 Datenzuordnung

Unter „Datenzuordnung“ sind einige Felder einzustellen.

Vorsicht: Das Feld „Daten übernehmen (ID-Nummer)“ ist für das automatisierte Anlegen von Moodle-Kursen von Klassen Voraussetzung.



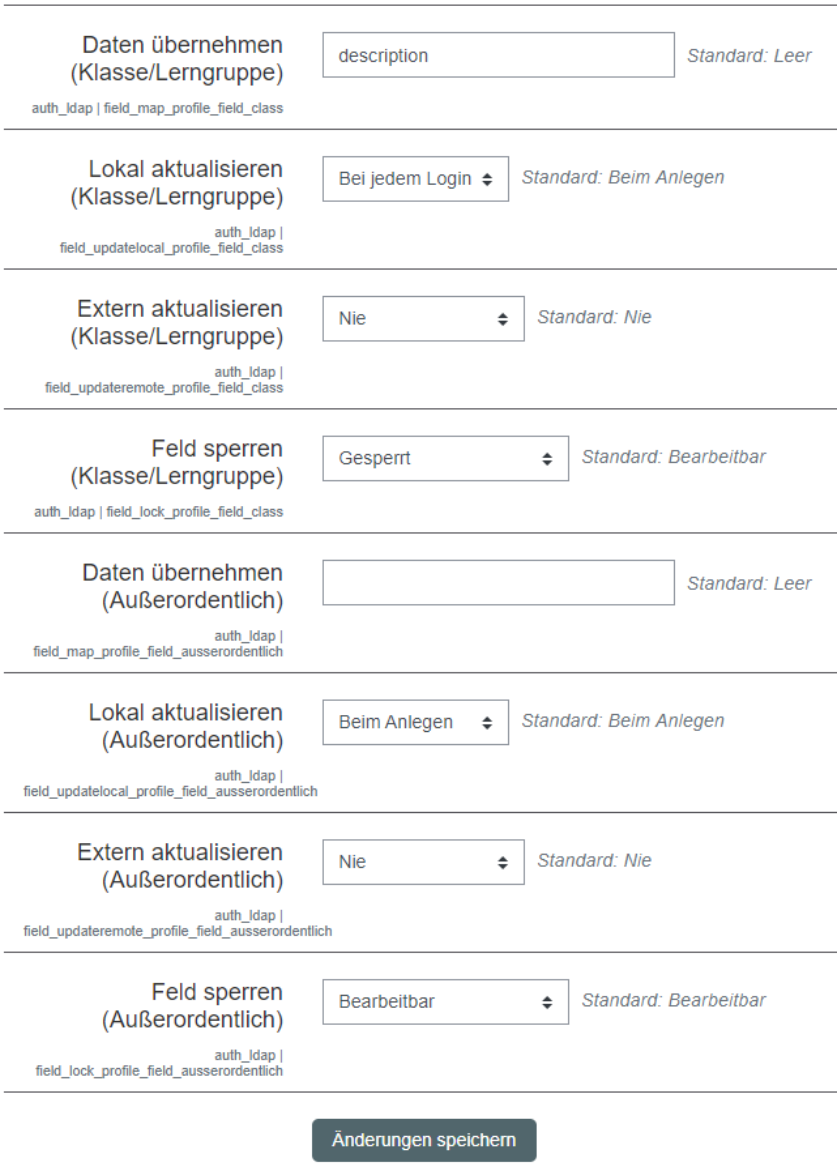
| | | |
|---|---|---|
| Lokal aktualisieren (Stadt)<br>auth_ldap \| field_updatelocal_city | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Stadt)<br>auth_ldap \| field_updateremote_city | Nie | *Standard: Nie* |
| Feld sperren (Stadt)<br>auth_ldap \| field_lock_city | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Land)<br>auth_ldap \| field_map_country | | *Standard: Leer* |
| Lokal aktualisieren (Land)<br>auth_ldap \| field_updatelocal_country | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Land)<br>auth_ldap \| field_updateremote_country | Nie | *Standard: Nie* |
| Feld sperren (Land)<br>auth_ldap \| field_lock_country | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Sprache)<br>auth_ldap \| field_map_lang | | *Standard: Leer* |
| Daten übernehmen (Webseite)<br>auth_ldap \| field_map_url | | *Standard: Leer* |
| Lokal aktualisieren (Webseite)<br>auth_ldap \| field_updatelocal_url | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Webseite)<br>auth_ldap \| field_updateremote_url | Nie | *Standard: Nie* |
| Feld sperren (Webseite)<br>auth_ldap \| field_lock_url | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (ID-Nummer)<br>auth_ldap \| field_map_idnumber | uidNumber | *Standard: Leer* |
| Lokal aktualisieren (ID-Nummer)<br>auth_ldap \| field_updatelocal_idnumber | Bei jedem Login | *Standard: Beim Anlegen* |
| Extern aktualisieren (ID-Nummer)<br>auth_ldap \| field_updateremote_idnumber | Nie | *Standard: Nie* |
| Feld sperren (ID-Nummer)<br>auth_ldap \| field_lock_idnumber | Gesperrt | *Standard: Bearbeitbar* |
| Daten übernehmen (Institution)<br>auth_ldap \| field_map_institution | | *Standard: Leer* |

| | | |
|---|---|---|
| Daten übernehmen (Institution)<br>auth_ldap \| field_map_institution | | Standard: Leer |
| Lokal aktualisieren (Institution)<br>auth_ldap \| field_updatelocal_institution | Beim Anlegen | Standard: Beim Anlegen |
| Extern aktualisieren (Institution)<br>auth_ldap \| field_updateremote_institution | Nie | Standard: Nie |
| Feld sperren (Institution)<br>auth_ldap \| field_lock_institution | Bearbeitbar | Standard: Bearbeitbar |
| Daten übernehmen (Abteilung)<br>auth_ldap \| field_map_department | | Standard: Leer |
| Lokal aktualisieren (Abteilung)<br>auth_ldap \| field_updatelocal_department | Beim Anlegen | Standard: Beim Anlegen |
| Extern aktualisieren (Abteilung)<br>auth_ldap \| field_updateremote_department | Nie | Standard: Nie |
| Feld sperren (Abteilung)<br>auth_ldap \| field_lock_department | Bearbeitbar | Standard: Bearbeitbar |
| Daten übernehmen (Telefon)<br>auth_ldap \| field_map_phone1 | | Standard: Leer |
| Lokal aktualisieren (Telefon)<br>auth_ldap \| field_updatelocal_phone1 | Beim Anlegen | Standard: Beim Anlegen |
| Extern aktualisieren (Telefon)<br>auth_ldap \| field_updateremote_phone1 | Nie | Standard: Nie |
| Feld sperren (Telefon)<br>auth_ldap \| field_lock_phone1 | Bearbeitbar | Standard: Bearbeitbar |
| Daten übernehmen (Smartphone)<br>auth_ldap \| field_map_phone2 | | Standard: Leer |
| Lokal aktualisieren (Smartphone)<br>auth_ldap \| field_updatelocal_phone2 | Beim Anlegen | Standard: Beim Anlegen |
| Extern aktualisieren (Smartphone)<br>auth_ldap \| field_updateremote_phone2 | Nie | Standard: Nie |
| Feld sperren (Smartphone)<br>auth_ldap \| field_lock_phone2 | Bearbeitbar | Standard: Bearbeitbar |
| Daten übernehmen (Adresse)<br>auth_ldap \| field_map_address | | Standard: Leer |

| | | |
|---|---|---|
| Daten übernehmen (Adresse)<br>auth_ldap \| field_map_address | | *Standard: Leer* |
| Lokal aktualisieren (Adresse)<br>auth_ldap \| field_updatelocal_address | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Adresse)<br>auth_ldap \| field_updateremote_address | Nie | *Standard: Nie* |
| Feld sperren (Adresse)<br>auth_ldap \| field_lock_address | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Vorname - lautgetreu)<br>auth_ldap \| field_map_firstnamephonetic | | *Standard: Leer* |
| Lokal aktualisieren (Vorname - lautgetreu)<br>auth_ldap \| field_updatelocal_firstnamephonetic | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Vorname - lautgetreu)<br>auth_ldap \| field_updateremote_firstnamephonetic | Nie | *Standard: Nie* |
| Feld sperren (Vorname - lautgetreu)<br>auth_ldap \| field_lock_firstnamephonetic | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Nachname - lautgetreu)<br>auth_ldap \| field_map_lastnamephonetic | | *Standard: Leer* |
| Lokal aktualisieren (Nachname - lautgetreu)<br>auth_ldap \| field_updatelocal_lastnamephonetic | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Nachname - lautgetreu)<br>auth_ldap \| field_updateremote_lastnamephonetic | Nie | *Standard: Nie* |
| Feld sperren (Nachname - lautgetreu)<br>auth_ldap \| field_lock_lastnamephonetic | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Mittlerer Name)<br>auth_ldap \| field_map_middlename | | *Standard: Leer* |
| Lokal aktualisieren (Mittlerer Name)<br>auth_ldap \| field_updatelocal_middlename | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Mittlerer Name)<br>auth_ldap \| field_updateremote_middlename | Nie | *Standard: Nie* |
| Feld sperren (Mittlerer Name)<br>auth_ldap \| field_lock_middlename | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Pseudonym)<br>auth_ldap \| field_map_alternatename | | *Standard: Leer* |

| | | |
|---|---|---|
| Lokal aktualisieren (Pseudonym)<br>auth_ldap \| field_updatelocal_alternatename | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Pseudonym)<br>auth_ldap \| field_updateremote_alternatename | Nie | *Standard: Nie* |
| Feld sperren (Pseudonym)<br>auth_ldap \| field_lock_alternatename | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Geburtsdatum)<br>auth_ldap \| field_map_profile_field_dateofbirth | | *Standard: Leer* |
| Lokal aktualisieren (Geburtsdatum)<br>auth_ldap \| field_updatelocal_profile_field_dateofbirth | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Geburtsdatum)<br>auth_ldap \| field_updateremote_profile_field_dateofbirth | Nie | *Standard: Nie* |
| Feld sperren (Geburtsdatum)<br>auth_ldap \| field_lock_profile_field_dateofbirth | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Geburtsort)<br>auth_ldap \| field_map_profile_field_placeofbirth | | *Standard: Leer* |
| Lokal aktualisieren (Geburtsort)<br>uth_ldap \| field_updatelocal_profile_field_placeofbirth | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Geburtsort)<br>auth_ldap \| field_updateremote_profile_field_placeofbirth | Nie | *Standard: Nie* |
| Feld sperren (Geburtsort)<br>auth_ldap \| field_lock_profile_field_placeofbirth | Bearbeitbar | *Standard: Bearbeitbar* |
| Daten übernehmen (Geschlecht)<br>auth_ldap \| field_map_profile_field_gender | | *Standard: Leer* |
| Lokal aktualisieren (Geschlecht)<br>auth_ldap \| field_updatelocal_profile_field_gender | Beim Anlegen | *Standard: Beim Anlegen* |
| Extern aktualisieren (Geschlecht)<br>auth_ldap \| field_updateremote_profile_field_gender | Nie | *Standard: Nie* |
| Feld sperren (Geschlecht)<br>auth_ldap \| field_lock_profile_field_gender | Bearbeitbar | *Standard: Bearbeitbar* |

Und letztendlich die Zuordnung der Lerngruppe. Dort wird für die Klasse/Lerngruppe die „description“ verwendet. Diese Zuordnung ist für die Profilfeld-basierende Zuweisung globaler Gruppen (Kapitel 4.4) zwingend erforderlich.




### 4.1.12 Abschluss

Durch Klicken auf den Button „Änderungen sichern“ am Ende der Webseite wird alles gespeichert.

Danach ist wieder zu wechseln zu Website-Administration -> Plugins -> Authentifizierung -> Übersicht. Nun kann durch Anklicken des durchgestrichenen Auges in der Zeile „LDAP-Server“ (siehe erster Screenshot) das LDAP-Plugin aktiviert werden.

## 4.2 Automatisches Einschreiben

Sie können für alle in ihrer paedML angelegten Arbeitsgruppen und Klasse in Moodle jeweils einen Kurs anlegen lassen. In diesen werden dann alle Schülerinnen und Schüler dieser Klassen/Gruppen als TeilnehmerIn, die Lehrkräfte als LehrerInnen/KurserstellerIn. Diese Einstellung ist optional und kann auch übersprungen werden.

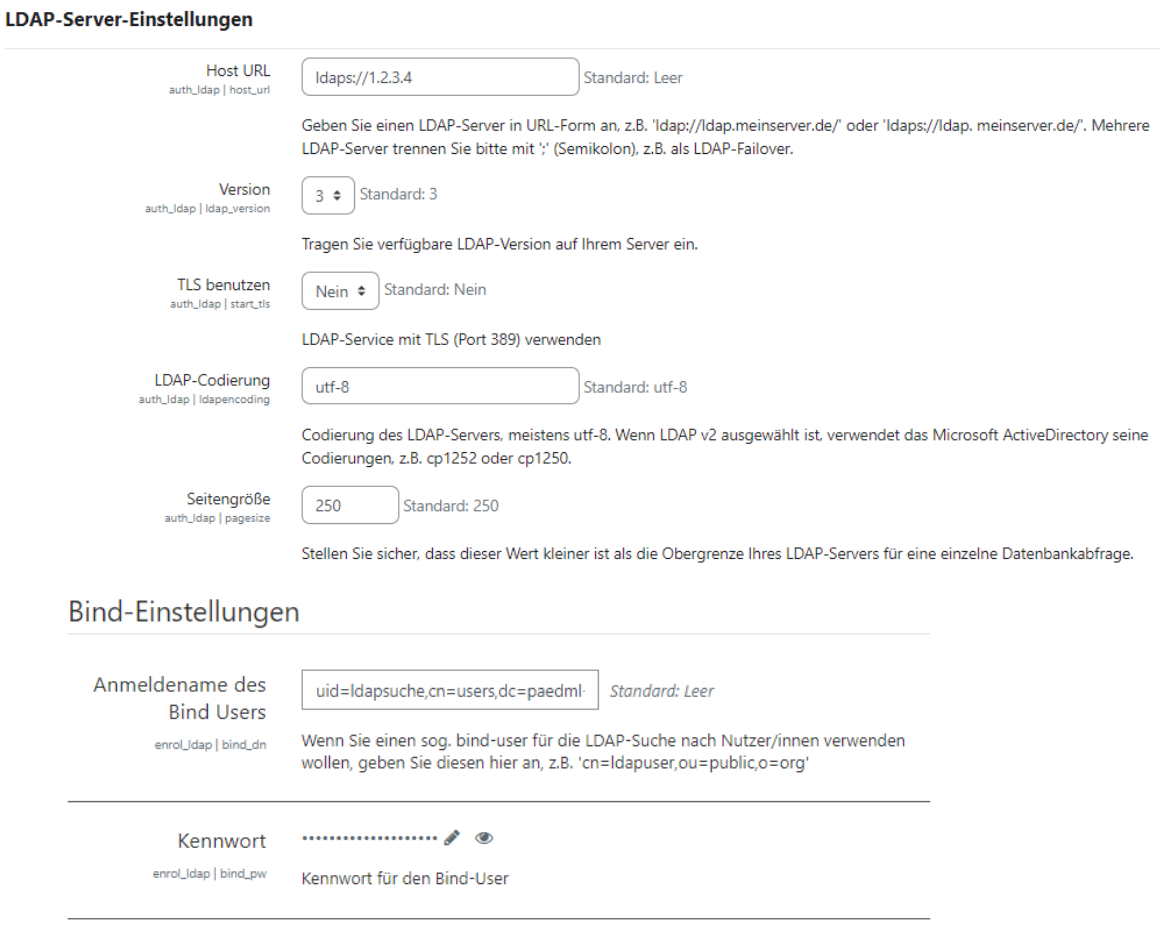
### 4.2.1 Aktive Plugins

In Moodle muss unter Website-Administration -> Plugins -> Einschreibung -> LDAP-Einschreibung die Konfiguration durchgeführt werden.

Die Einstellungen für den LDAP-Server und die Bind-Einstellungen sind analog zu denen bei der LDAP-Authentifizierung.

### 4.2.2 Einstellung für LDAP-Server und Bind-Einstellungen

Die Einstellungen sind analog zu Kapitel 4.1.2.



### 4.2.3 Rollenabbildung

Bei Rollenabbildung für LehrerInnen (bzw. KurserstellerIn) muss

```
cn=lehrer,cn=users,ou=schule,dc=paedml-linux,dc=lokal
```

und

```
uniquemember
```

eingetragen werden, bei SchülerIn (bzw. TeilnehmerIn)

```
cn=schueler,cn=groups,ou=schule,dc=paedml-linux,dc=lokal
```

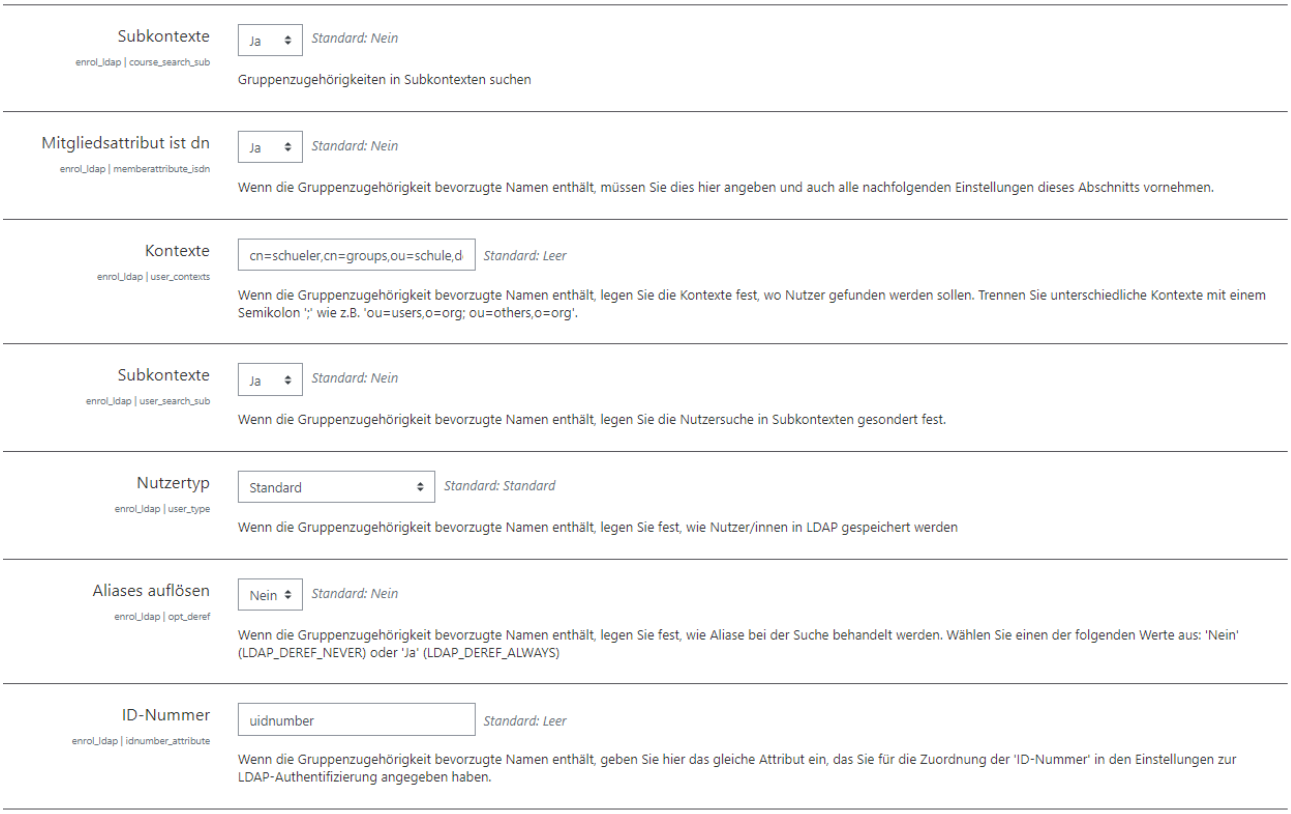
und

```
uniquemember
```

Die weiteren Einstellungen sind auf den Bildern zu sehen, bei „Kontexte“ ist der Wert

```
cn=schueler,cn=groups,ou=schule,dc=paedml-
linux,dc=lokal;cn=lehrer,cn=users,ou=schule,dc=paedml-linux,dc=lokal
```

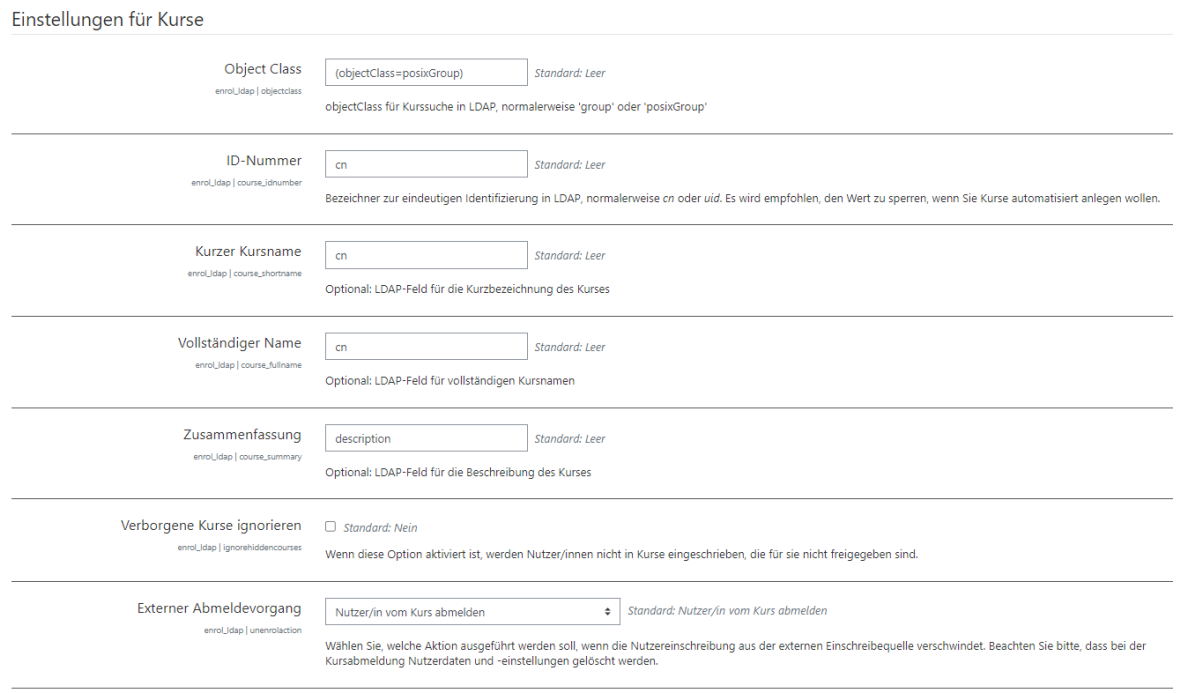
einzutragen.




Die ID-Nummer-Zuordnung zu

```
uidnumber
```

wird für die Eintragung der Teilnehmer in die Kurse benötigt.

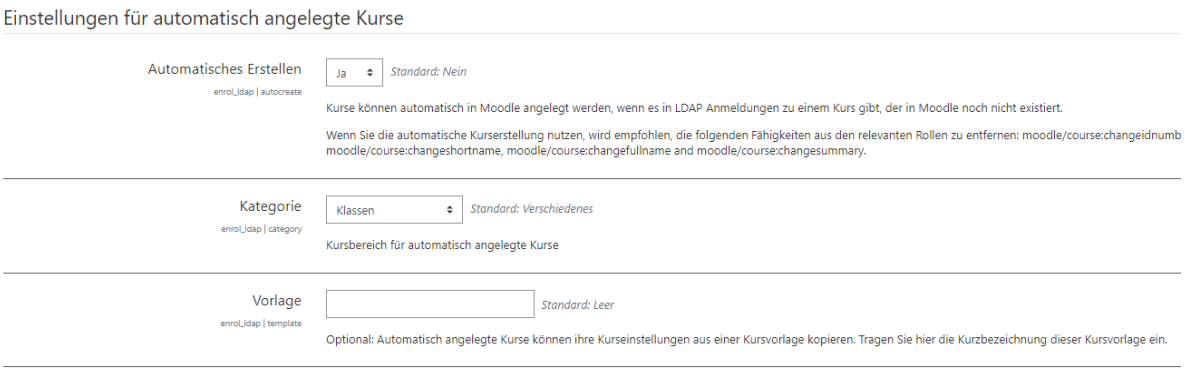



Bei der Einstellung für „Kategorie“ können Sie selbst auswählen, wo die Gruppen der paedML eingeordnet werden.

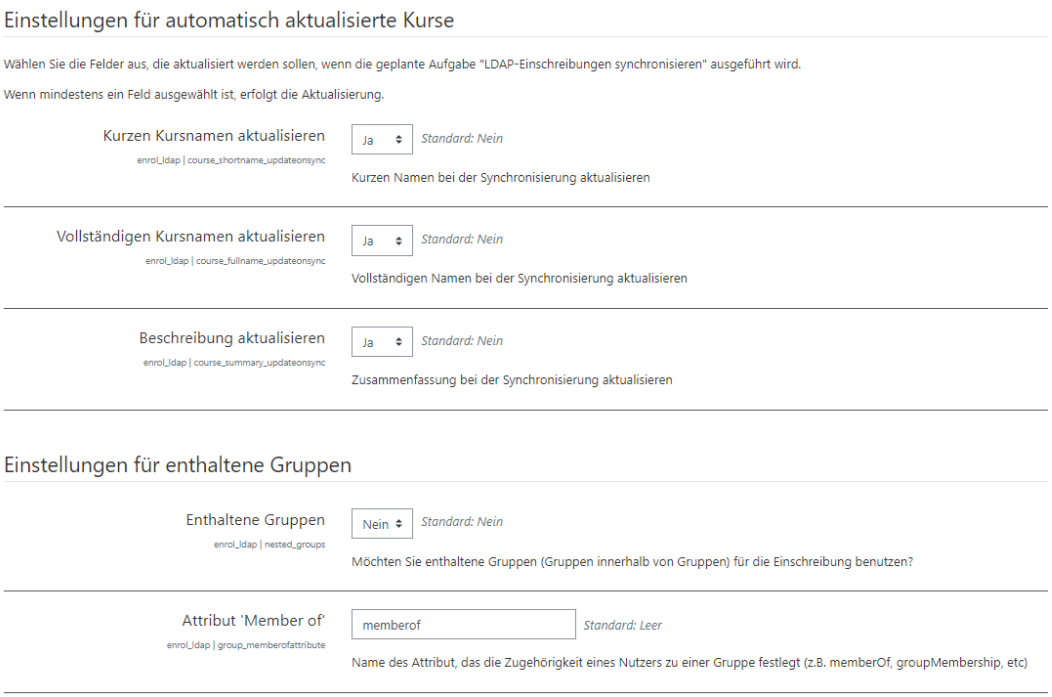
Kategorien können Sie über Website-Administration -> Zusatzoptionen -> Kurse -> Kurse und Kursbereiche verwalten.

Klicken Sie auf „Neuen Kursbereich anlegen“. Wählen Sie als Namen z.B. „Klassen“ oder „paedML Gruppen“.

Wählen Sie die Kategorie mit dem Drop-Down-Menü aus und setzen das Automatische Erstellen auf „Ja“.



Übernehmen Sie die restlichen Einstellungen wie im Bild.

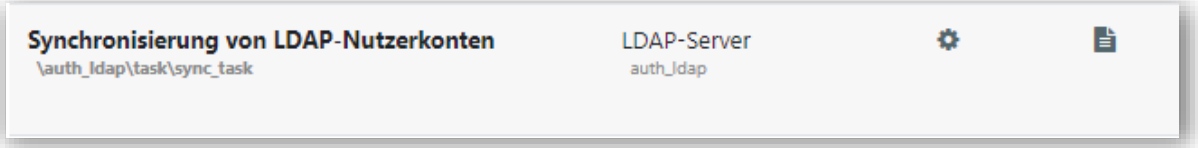



Mit einem Klick auf „Änderungen Speichern“ am Seitenende ist die Konfiguration beendet.

## 4.3 Synchronisierung automatisieren

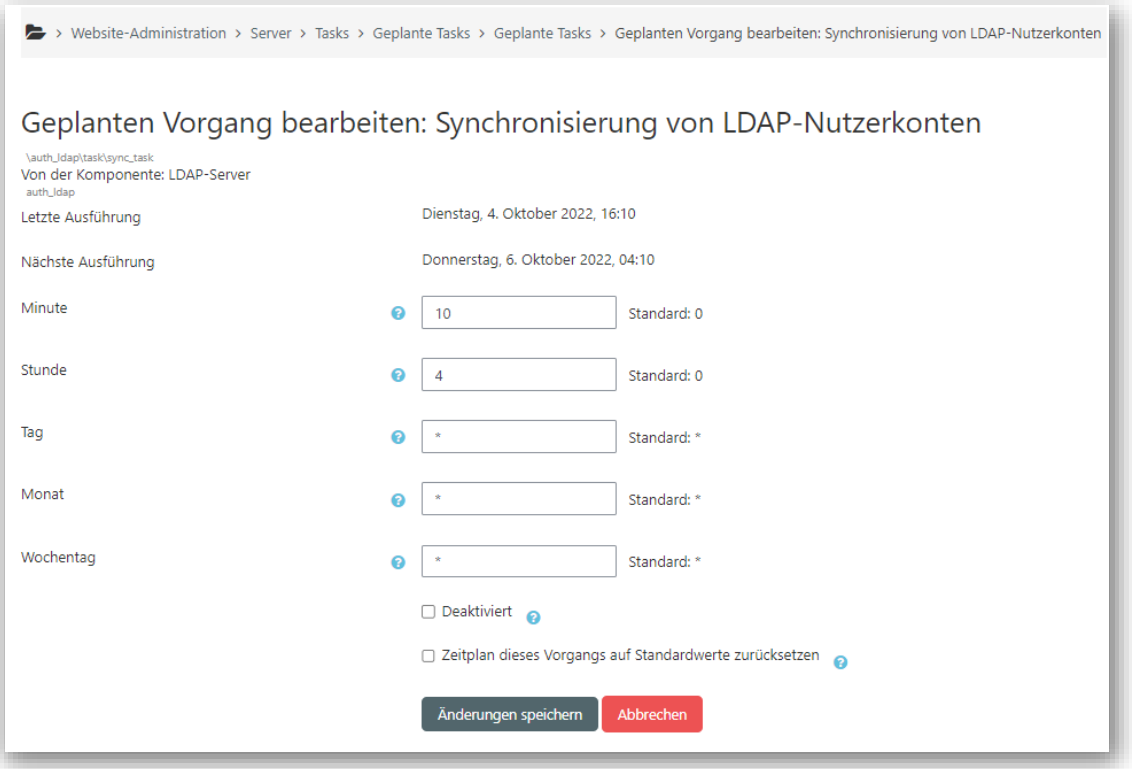
Damit Moodle die Schuldaten automatisch aktualisiert sollten Sie jeweils eine geplante Aufgabe (Cron-Job) für Authentifizierung und Einschreibung einstellen.

Öffnen Sie Unter Website-Administration -> Server -> Tasks -> Geplante Tasks.




Wählen Sie „Synchronisierung von LDAP-Nutzerkonten“ und klicken auf das Zahnrad, um den Task zu konfigurieren.

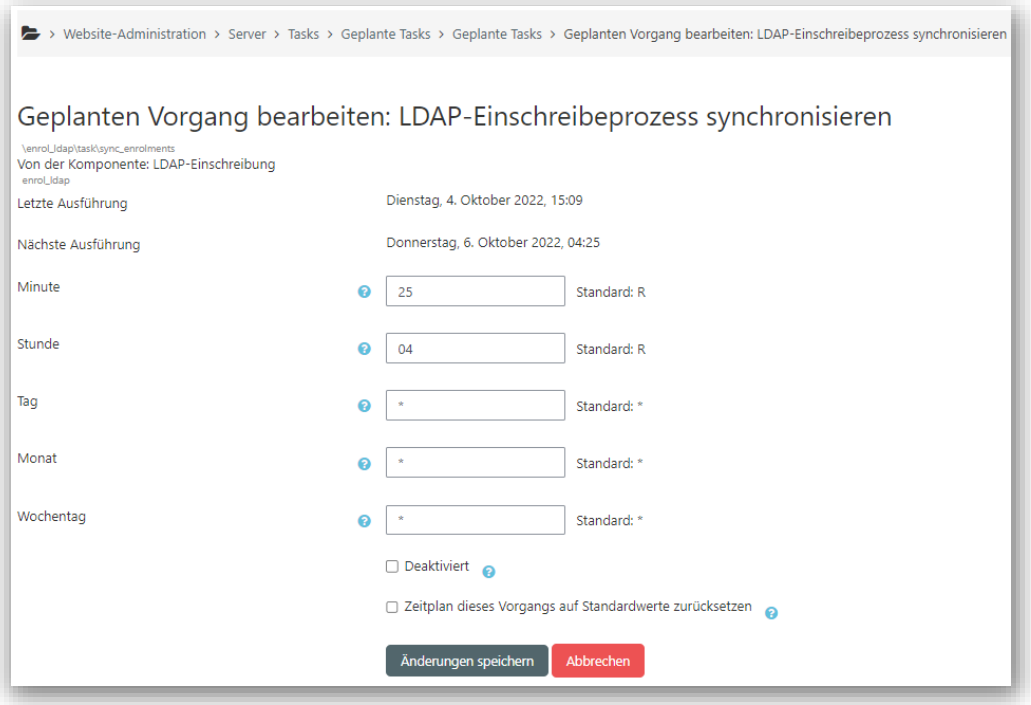
Stellen Sie dort einen Zeitpunkt zur Synchronisation ein, z.B. um 4.10Uhr morgens und entfernen Sie bei "Deaktiviert" gegebenenfalls den Haken.




Analog bearbeiten Sie „LDAP-Einschreibeprozess synchronisieren“

Setzen Sie dort die Zeit 10-15 Minuten später an.

Damit werden die Benutzerdaten jede Nacht abgeglichen.




Die Synchronisation können Sie auch nach eigenen Vorlieben beliebig ändern, z.B. nur einmal pro Woche oder Monat.

## 4.4 Profilfeld-basierende Zuweisung globaler Gruppen

Mit einem Update wurde ein Import-Hook für den Benutzerimport installiert. Dieser setzt beim Import von Schülerinnen und Schülern bei allen Accounts das Feld „description“ auf die besuchte Klasse. Somit ist ein lang ersehntes Feature für Moodle endlich verfügbar: die profilfeld-basierende Zuweisung globaler Gruppen.

### 4.4.1 Gruppen anlegen

Falls Sie bisher keine globalen Gruppen in Moodle verwenden, müssen Sie diese zuerst anlegen.

Öffnen Sie dazu Website-Administration -> Nutzer/innen -> Nutzerkonten -> Globale Gruppen -> Systemweite globale Gruppen.

Dort können Sie über „Globale Gruppen hochladen“ eine CSV-Datei mit allen Klassenbezeichnungen hochladen. Alternativ können Sie hier auf „Neue globale Gruppe anlegen“ die Klassen über die Moodle Oberfläche anlegen. Sobald die Gruppen angelegt sind, können Sie die Schülerinnen und Schüler automatisiert darin aufnehmen lassen.

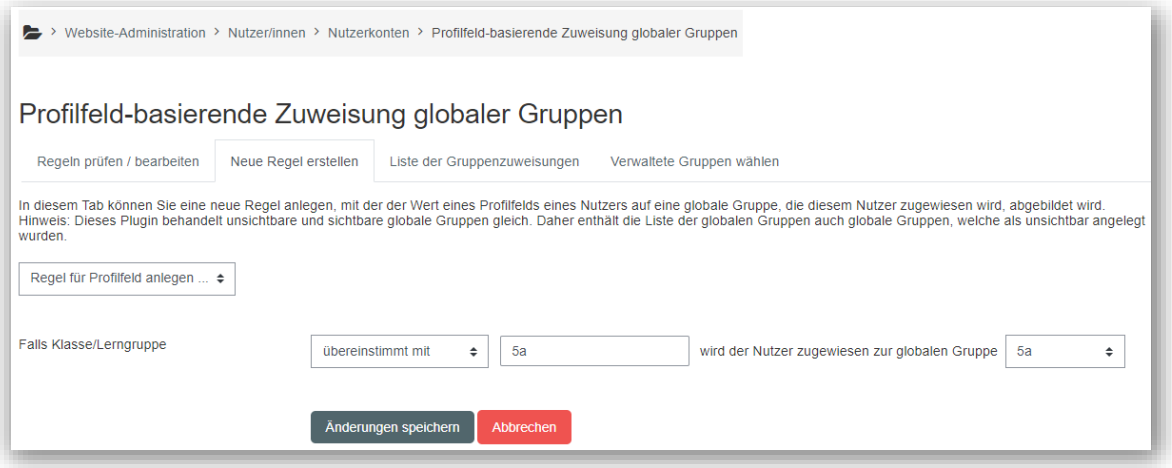
### 4.4.2 Benutzer zuweisen

Öffnen Sie Website-Administration -> Nutzer/innen -> Nutzerkonten -> Profilfeld-basierende Zuweisung globaler Gruppen.

Klicken Sie hier auf „Neue Regel erstellen“. Wählen Sie im Dropdown-Menü „Klasse/Lerngruppe“.

In der neu erschienenen Zeile belassen Sie die Einstellung „übereinstimmt mit“ und tragen den Namen einer Klasse ein und wählen dann die passende Gruppe zur Verteilung aus wie im Bild unten zu sehen.

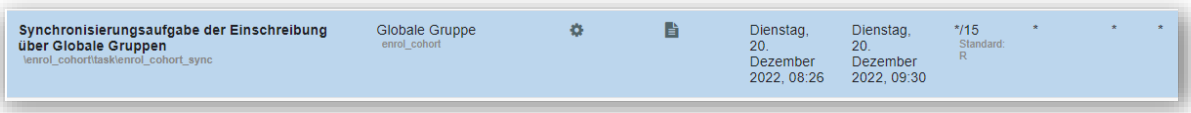
Achten Sie darauf, dass die Klasse die gleiche Schreibweise hat, welche auch in der paedML Linux/GS verwendet wird. Mit „Änderungen speichern“ wird die Regel erstellt. Wiederholen Sie diesen Vorgang für alle Klassen. Leider ist dieser aufwendige Schritt anscheinend nicht weiter automatisierbar.




### 4.4.3 Geplante Aufgabe prüfen

Abschließend kontrollieren Sie unter Website-Administration -> Server -> Tasks -> Geplante Tasks

Ob die „Synchronisierungsaufgabe der Einschreibung über Globale Gruppen“ aktiv ist.



# 5 WebUntis

Diese Anleitung bezieht sich auf die Verbindung zu WebUntis über **LDAPS mit öffentlichem Zertifikat**.

Vorsicht! In WebUntis gibt es für Schülerinnen und Schüler sowohl **Stammdaten** als auch **Accounts**.

Die Stammdaten enthalten Informationen wie Stundenpläne, Kontaktpersonen und vieles mehr. Stammdaten werden in der Regel von der Schulleitung importiert. Die LDAP-Verbindung erstellt nur die Accounts zur Anmeldung. Diese werden anhand der SchülerID den Stammdaten zugeordnet.

Bitte beachten Sie, dass der Import die SchülerID aus ASV-BW verwendet, um eine Verbindung zwischen Accounts und Stammdaten herzustellen. Wenn Sie Benutzer ohne den offiziellen Benutzerimport erstellen, oder Accounts manuell anlegen, können diese durch die hier beschriebene Konfiguration in WebUntis nicht erkannt werden.

Beim Import der Stammdaten müssen auch zwingend die SchülerIDs mit in WebUntis importiert werden. Falls Ihre Schule sich an diesen Standard nicht halten kann oder will, bietet WebUntis die Möglichkeit, das Feld Personenidentifizierung anzupassen, um z.B. anhand von Vor- und Nachnamen eine Übereinstimmung zwischen Account und Stammdaten zu finden. In diesem Fall sollte auch *„Anmeldung für nicht Identifizierbare Benutzer verbieten“* nicht aktiviert sein, damit ein WebUntis Admin Accounts manuell mit Stammdaten verbinden kann.

Für Lehrkräfte werden zur Identifizierung die Kürzel verwendet. Achten Sie darauf, dass die paedML die Kürzel nur ohne Umlaute importiert, WebUntis könnte diese auch mit Umlauten darstellen, dies würde jedoch zu Problemen beim Vergleich führen. Falls Sie Lehrkräfte nicht über LDAP versorgen möchten, können Sie die Felder für *„Lehrkraft“* in der Konfiguration auch frei lassen.

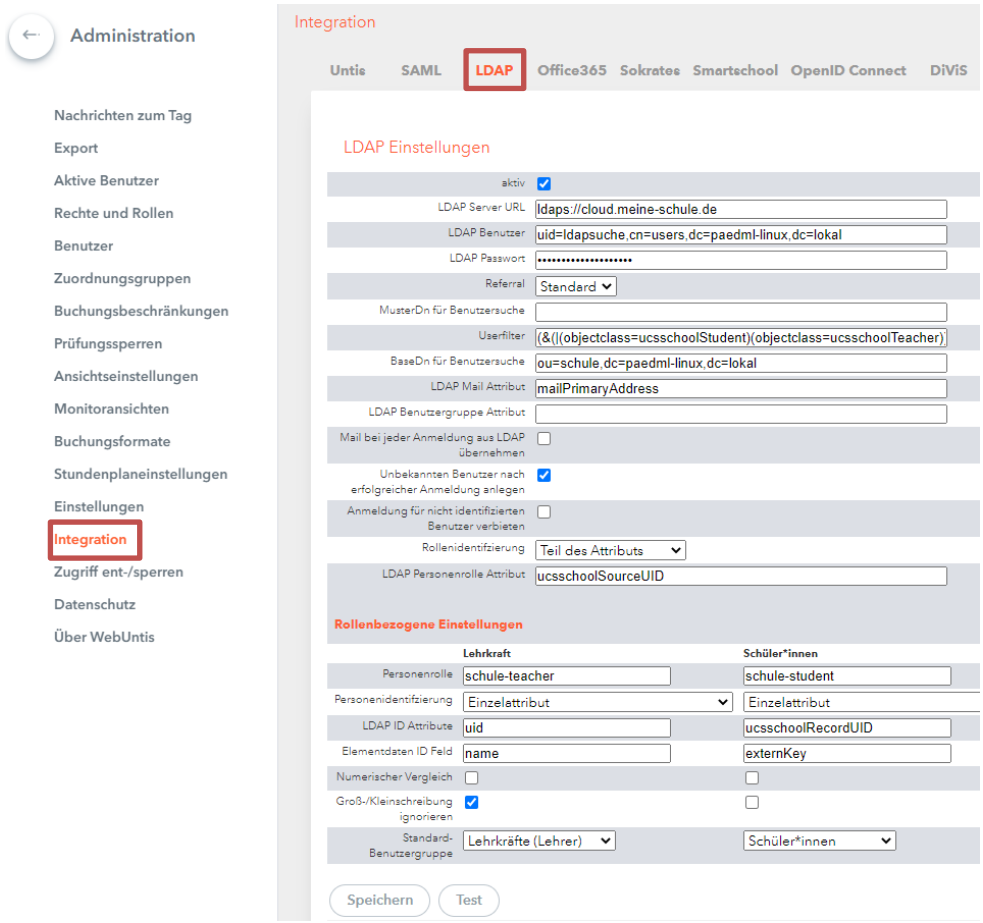
## 5.1 Konfiguration

Melden Sie sich auf der WebUntis Seite als Admin an. Klicken Sie auf Administration – Integration und wählen Sie dort den Reiter LDAP.

Der Haken *„aktiv“* sollte deaktiviert bleiben, bis die Konfiguration abgeschlossen ist.

Tragen Sie für *„LDAP Server URL“* der Wert *„ldaps://cloud.meine-schule.de“* ein, ersetzen Sie dabei die Adresse *cloud.meine-schule.de* durch die Nextcloud Adresse ihrer Schule.

Bei *„LDAP Benutzer“* tragen Sie *„uid=ldapsuche,cn=users,dc=paedml-linux,dc=lokal“* ein.




Das *„LDAP Passwort“* müssen Sie auf Ihrem Server (10.1.0.1) per Putty oder WinSCP in der Datei /etc/ldapsuche.secret nachschlagen.

Tragen Sie außerdem die folgenden Einstellungen ein:

| **Feldname** | **Wert** |
|---|---|
| UserFilter | (&(\|(objectclass=ucsschoolStudent)(objectclass=ucsschoolTeacher))(uid={0})) |
| BaseDn für Benutzersuche | ou=schule,dc=paedml-linux,dc=lokal |
| LDAP Mail Attribut | mailPrimaryAddress |
| Unbekannten Benutzer nach erfolgreicher Anmeldung anlegen | aktivieren (Haken setzen) |
| Anmeldung für nicht identifizierte Benutzer verbieten | aktivieren (Haken setzen) |

| Feldname | Wert (Lehrkraft) | Wert (Schüler*innen) |
|---|---|---|
| Personenrolle | schule-teacher | schule-student |
| Personenidentifzierung | Einzelattribut | Einzelattribut |
| LDAP ID Attribute | uid | ucsschoolRecordUID |
| Elementdaten ID Feld | name | externKey |
| Numerischer Vergleich | Nicht aktivieren (kein Haken) | Nicht aktivieren (kein Haken) |
| Groß-/Kleinschreibung ignorieren | aktivieren (Haken setzen) | Nicht aktivieren (kein Haken) |
| Standard-Benutzergruppe | Lehrkräfte (Lehrer) | Schüler*innen |

Nun können sich Benutzer der paedML in Ihrer WebUntis Instanz anmelden, jedoch nur, wenn WebUntis einen erfolgreichen Vergleich der ID durchführen kann.

Falls Sie Probleme haben können Sie den Haken *„Anmeldung für nicht identifizierten Benutzer verbieten"* entfernen, so können sich alle Benutzer der paedML bei WebUntis anmelden. Aber Vorsicht, die Accounts sind dann nicht garantiert mit den Stammdaten verbunden, wodurch gegebenenfalls kein Stundenplan einsehbar ist.

**Landesmedienzentrum Baden-Württemberg (LMZ)**
**Support Netz**
**Rotenbergstraße 111**

**70190 Stuttgart**



paedML L

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG