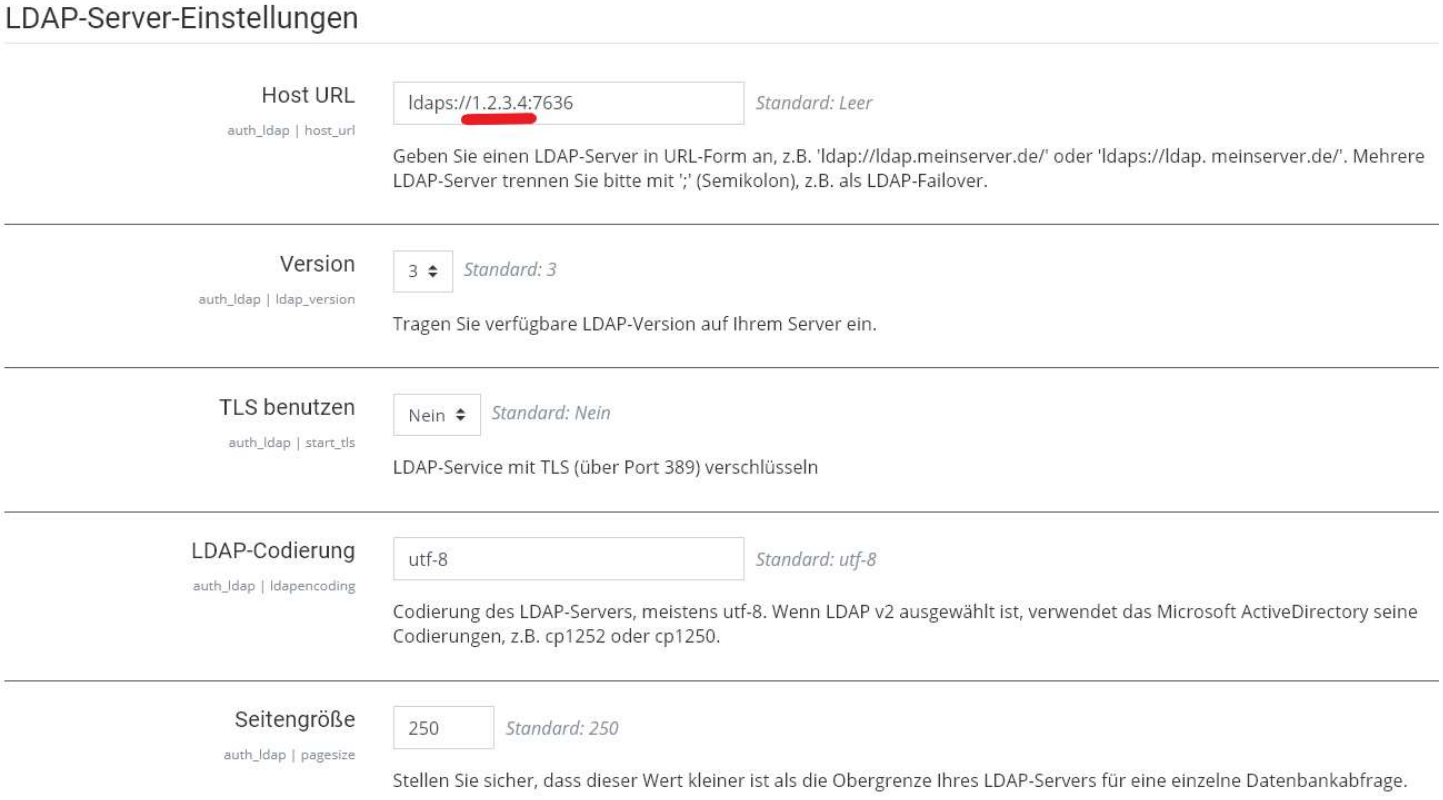
LDAP-Anbindung Moodle

Last updated by | Michael Salm | 1. Apr. 2020 at 09:39 MESZ

LDAP-Einstellungen in Moodle

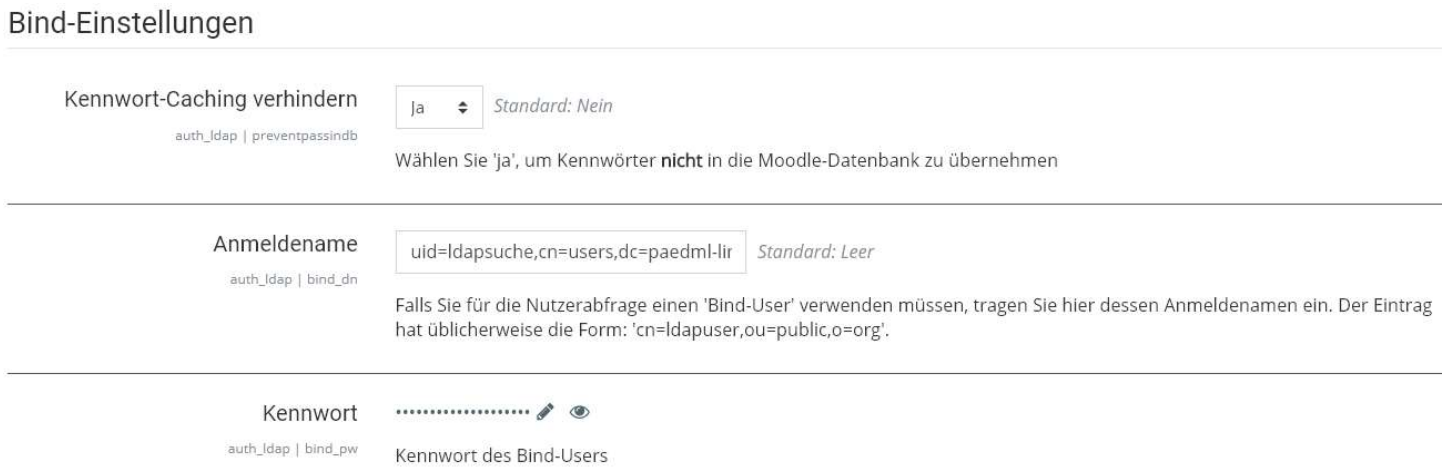
In Moodle muss unter Website-Administration -> Plugins -> Authentifizierung -> Übersicht das Plugin "LDAP-Server" über "Einstellungen" konfiguriert werden.

Der Abschnitt "LDAP-Server-Einstellungen" muss wie folgt aussehen.
Bitte tragen Sie bei "Host URL" statt der IP-Adresse "1.2.3.4" Ihre eigene IP-Adresse oder Ihren Domänennamen ein. Der Port muss 7636 bleiben.



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*



Bei "Nutzersuche (user lookup)" ist folgendes einzustellen.
Der Eintrag unter "Kontexte" lautet: *cn=users,ou=schule,dc=paedml-linux,dc=lokal*

Nutzersuche (user lookup)

Nutzertyp
auth_ldap | user_type
Standard — *Standard: Standard*
Wählen Sie, wie Nutzerkonten in LDAP gespeichert werden. Diese Einstellung legt auch fest, wie das Ablaufdatum für Kennwörter, die GraceLogins und das Anlegen neuer Nutzerkonten in LDAP funktionieren.

Kontexte
auth_ldap | contexts
cn=users,ou=schule,dc=paedml-linux,c — *Standard: Leer*
Liste der Kontexte, in denen Nutzer/innen zu finden sind. Mehrere Kontexte werden durch ein ';' (Semikolon) getrennt, wie z.B.: 'ou=users,o=org; ou=others,o=org'

Subkontexte
auth_ldap | search_sub
Ja — *Standard: Nein*
Nutzersuche auch in Subkontexten durchführen

Aliase berücksichtigen
auth_ldap | opt_deref
Nein — *Standard: Nein*
Legt fest wie Aliasbezeichnungen bei der Suche behandelt werden. Wählen Sie einen der folgenden Werte: 'Nein' (ldap_deref_never) oder 'Ja' (ldap_deref_always)

Nutzermerkmal
auth_ldap | user_attribute
uid — *Standard: Leer*
Optional: Merkmal zur Nutzerbenennung und -suche ändern. Normalerweise 'cn'.

Nutzermerkmal
auth_ldap | user_attribute
uid — *Standard: Leer*
Optional: Merkmal zur Nutzerbenennung und -suche ändern. Normalerweise 'cn'.

Ausblendemerkmal
auth_ldap | suspended_attribute
Standard: Leer
Optional: Falls verfügbar wird dieses Merkmal verwendet, um das erstellte lokale Nutzerkonto zu aktivieren oder auszublenden.

Mitgliedsmerkmal
auth_ldap | memberattribute
memberOf — *Standard: Leer*
Optional: Mitgliedsmerkmal ändern, mit dem Nutzer/innen zu einer Gruppe gehören. Normalerweise 'member'

Mitgliedsmerkmal nutzt dn
auth_ldap | memberattribute_isdn
1 — *Standard: Leer*
Optional: Gebrauch von Mitgliedsmerkmalen ändern, entweder 0 oder 1

ObjectClass
auth_ldap | objectclass
Standard: Leer
Optional: Überschreibt die ObjectClass zur Nutzersuche in LDAP (ldap_user_type). Die Voreinstellung muss normalerweise nicht geändert werden.

Im Abschnitt "Kennwortänderung fordern" sind die Standardeinstellungen einzustellen.

Kennwortänderung fordern

Kennwortänderung fordern
auth_ldap | forcechangepassword
Nein — *Standard: Nein*
Nutzer/innen werden aufgefordert, ihr Kennwort beim ersten Anmelden zu ändern.

Standardseite zur Kennwortänderung nutzen
auth_ldap | stdchangepassword
Nein — *Standard: Nein*
Stellen Sie 'Ja' ein, wenn das externe Authentifizierungssystem eine Änderung des Kennwortes durch Moodle zulässt. Die Einstellungen überschreiben 'URL zur Kennwortänderung' Warnung: LDAP sollte unbedingt SSL-verschlüsselt sein (ldaps://), wenn der LDAP-Server extern betrieben wird.

Kennwortformat
auth_ldap | passtype
Unformatierter Text — *Standard: Unformatierter Text*
Geben Sie das Format für neue Kennwörter auf dem LDAP-Server an.

URL zur Kennwortänderung
auth_ldap | changepasswordurl
Standard: Leer
Hier können Sie eine Adresse angeben, über die die Nutzer ihren Anmeldenamen erfahren und ihr Kennwort zurücksetzen können, sofern sie diese Daten vergessen haben. Diese Option wird als Schaltfläche auf der Anmeldungsseite angeboten. Wenn Sie dieses Feld leer lassen, wird die Option nicht angeboten.

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

Einstellungen zum Ablauf von LDAP-Kennwörtern

Ablauf
auth_ldap | expiration
Nein — *Standard: Nein*
Wählen Sie 'Nein', um den Ablauf von Kennwörtern nicht zu prüfen. Wenn Sie 'LDAP-Server' wählen, wird Ablaufdatum direkt vom LDAP-Server zu lesen.

Ablaufwarnung
auth_ldap | expiration_warning
Standard: Leer
Anzahl der Tage, an denen vor dem Ablauf eines Kennwortes eine Warnung ausgegeben wird

Ablaufmerkmal
auth_ldap | expireattr
Standard: Leer
Optional: Überschreibt die LDAP-Attribute, die das Ablaufdatum für Kennwörter enthalten.

GraceLogins
auth_ldap | gracelogins
Nein — *Standard: Nein*
LDAP-GraceLogin aktivieren. Wenn das Gültigkeitsende von Kennwörtern erreicht ist, können sich die Nutzer/innen weiter einloggen, bis der GraceLogin-Zähler den Wert 0 hat. Mit dem Aktivieren wird eine GraceLogin-Mitteilung angezeigt, sobald das Gültigkeitsende erreicht ist.

Merkmal für GraceLogin
auth_ldap | graceattr
Standard: Leer
Optional: GraceLogin-Attribut überschreiben

Im Abschnitt "Nutzererstellung aktivieren" sind die Standardeinstellungen einzustellen.

Nutzererstellung aktivieren

Nutzer/innen extern anlegen
auth_ldap | auth_user_create

Nein *Standard: Nein*

Neue (anonyme) Nutzer können Nutzerkonten außerhalb der Authentifizierungsquelle erstellen und per E-Mail bestätigen. Wenn Sie diese Option aktivieren, müssen Sie außerdem modulspezifische Optionen zur Erstellung neuer Nutzerkonten konfigurieren.

Kontext für neue Nutzer/innen
auth_ldap | create_context

Standard: Leer

Wenn Sie die Nutzererstellung mit E-Mail-Bestätigung aktivieren, geben Sie den Kontext an, in dem die Nutzer/innen erstellt werden sollen. Dieser Kontext sollte sich von dem anderer Nutzer/innen unterscheiden, um Sicherheitsrisiken zu vermeiden. Sie brauchen diesen Kontext nicht zur Variablen ldap_contexts hinzuzufügen. Moodle sucht in diesem Kontext automatisch nach Nutzer/innen.
Achtung! Sie müssen die Funktion user_create() in der Datei auth/ldap/auth.php anpassen, damit die Nutzererstellung funktioniert.

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 "Manager/-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.

Zuordnung von Systemrollen

Manager/in-Kontext
auth_ldap | managercontext

cn=admins,cn=users,ou=schule,dc=pa *Standard: Leer*

Der LDAP-Kontext wird verwendet, um die *Manager/in* Zuordnung vorzunehmen. Trennen Sie verschiedene Gruppen mit ';'. Normalerweise sieht das so aus: "cn=manager,ou=staff,o=myorg".

Kursersteller/in-Kontext
auth_ldap | coursecreatorcontext

cn=lehrer,cn=users,ou=schule,dc=pae *Standard: Leer*

Der LDAP-Kontext wird verwendet, um die *Kursersteller/in* Zuordnung vorzunehmen. Trennen Sie verschiedene Gruppen mit ';'. Normalerweise sieht das so aus: "cn=coursecreator,ou=staff,o=myorg".

Bei "Synchronisierung von Nutzerkonten" ist einzustellen:

Synchronisierung von Nutzerkonten

Entfernte externe Nutzer
auth_ldap | removeuser

Intern löschen *Standard: Nur intern zugänglich*

Legen Sie fest, was mit einem internen Nutzerprofil passieren soll, wenn bei einer Massensynchronisierung dieser Account im externen System entfernt wurde. Nur gesperrte Nutzer werden automatisch reaktiviert, wenn sie in der externen Quelle wieder erscheinen.

Status von lokalen Nutzerkonten synchronisieren
auth_ldap | sync_suspended

Nein *Standard: Nein*

Die Option legt fest, dass das Ausblendemerkmal bei der Synchronisation von lokalen Nutzerkonten verwendet wird.

Im Abschnitt "NTLM-SSO" sind die Standardeinstellungen einzustellen.

NTLM-SSO

Aktivieren

auth_ldap | ntlmsso_enabled

Nein *Standard: Nein*

Setzen Sie diesen Wert auf "ja", um Single-Sign-On mit der NTLM-Domäne zu versuchen. Beachten Sie, dass dies zusätzliche Einstellungen auf dem Server erfordert, um zu funktionieren. Weitere Informationen finden Sie in der Dokumentation NTLM-Authentifizierung.

Subnet

auth_ldap | ntlmsso_subnet

Standard: Leer

Tragen Sie in dieses Feld eine Maske für ein Subnet ein, um NTLM-SSO auf IP-Adressen aus diesem Subnet zu beschränken. Mehrere Subnetze werden kommagetrennt angegeben. Format: xxx.xxx.xxx.xxx/bitmask

---

MS IE fast path?

auth_ldap | ntlmsso_ie_fastpath

NTLM mit allen Browsern versuchen *Standard: NTLM mit allen Browsern versuchen*

Wenn diese Option aktiviert ist, wird der 'NTLM SSO fast path' zugelassen. Das funktioniert nur mit dem Internet Explorer.

Authentifizierungsart

auth_ldap | ntlmsso_type

NTLM *Standard: NTLM*

Diese Methode ist beim Webserver eingestellt, um Nutzer/innen zu authentifizieren. Falls Sie sich nicht sicher sind, wählen Sie bitte NTLM.

Format externer Nutzernamen

auth_ldap | ntlmsso_remoteuserformat

Standard: Leer

Wenn Sie 'NTLM' als 'Authentifizierungstyp' verwenden, können Sie hier das Format von externen Nutzernamen angeben. Bleibt der Eintrag leer, wird das Standardformat DOMAIN\username verwendet. Verwenden Sie den optionalen **%domain%** Platzhalter, um festzulegen wo der Domainname erscheint, und den erforderlichen Platzhalter **%username%** für den Nutzernamenort.

Häufig genutzte Formate sind `%domain%%username%` (MS Windows default), `%domain%/%username%`, `%domain%+%username%` und einfach `%username%` (wenn kein Domainteil verwendet wird).

Unter "Datenzuordnung" sind einige Felder einzustellen.

Datenzuordnung

Die folgenden Felder sind optional. Im Nutzerprofil können automatisch einige Moodle-Felder mit ausgewählten Nutzerdaten aus **LDAP-Feldern** vorbelegt werden.

Wenn Sie die nachfolgenden Einträge leer lassen, wird nichts von LDAP übertragen und die Moodle-Voreinstellungen werden verwendet. In diesem Fall muss das Nutzerprofil beim ersten Login selbst fertig ausgefüllt werden.

Zusätzlich wird eingestellt, welche Felder im Nutzerprofil bearbeitbar sein sollen.

Lokal aktualisieren: Wenn diese Option aktiviert ist, wird das Feld jedes Mal von extern (external auth) aktualisiert, wenn der Teilnehmer sich einloggt oder eine Nutzersynchronisation erfolgt. Dateneinträge sollten gesperrt sein, wenn sie lokal aktualisiert werden.

Feld sperren: Wenn diese Option aktiviert ist, verhindert Moodle die Änderung des Feldinhalts. Dies ist sinnvoll, wenn die Daten in einer externen Datenbank verwaltet werden.

Extern aktualisieren: Wenn diese Option aktiviert ist, wird die externe Datenbank aktualisiert, sobald der Nutzerdatensatz aktualisiert wird. Die Felder sollten bearbeitbar bleiben, um Datenänderungen zuzulassen.

Anmerkung: Das Update externer LDAP-Daten erfordert die Einstellung 'binddn' und 'bindpw' für einen Bind-Nutzer mit Schreibrechten für alle Nutzerdatensätze. Aktuell werden mehrfach gesetzte Eigenschaften nicht unterstützt und die zusätzlichen Werte bei einem Update entfernt.

Daten übernehmen (Vorname) auth_ldap | field_map_firstname	givenName	*Standard: Leer*
Lokal aktualisieren (Vorname) auth_ldap | field_updatelocal_firstname	Bei jedem Login	*Standard: Beim Anlegen*
Extern aktualisieren (Vorname) auth_ldap | field_updateremote_firstname	Nie	*Standard: Nie*
Feld sperren (Vorname) auth_ldap | field_lock_firstname	Gesperrt	*Standard: Bearbeitbar*
Daten übernehmen (Nachname) auth_ldap | field_map_lastname	sn	*Standard: Leer*
Daten übernehmen (Nachname) auth_ldap | field_map_lastname	sn	*Standard: Leer*
Lokal aktualisieren (Nachname) auth_ldap | field_updatelocal_lastname	Bei jedem Login	*Standard: Beim Anlegen*
Extern aktualisieren (Nachname) auth_ldap | field_updateremote_lastname	Nie	*Standard: Nie*
Feld sperren (Nachname) auth_ldap | field_lock_lastname	Gesperrt	*Standard: Bearbeitbar*
Daten übernehmen (E-Mail-Adresse) auth_ldap | field_map_email	mailPrimaryAddress	*Standard: Leer*
Lokal aktualisieren (E-Mail-Adresse) auth_ldap | field_updatelocal_email	Bei jedem Login	*Standard: Beim Anlegen*
Extern aktualisieren (E-Mail-Adresse)	Nie	*Standard: Nie*

Adresse)

auth_ldap | field_updateremote_email

Feld sperren (E-Mail-Adresse)

auth_ldap | field_lock_email

Gesperrt — *Standard: Bearbeitbar*

Daten übernehmen (Stadt)

auth_ldap | field_map_city

Standard: Leer

Daten übernehmen (Stadt)

auth_ldap | field_map_city

Standard: Leer

Lokal aktualisieren (Stadt)

auth_ldap | field_updatelocal_city

Beim Anlegen — *Standard: Beim Anlegen*

Extern aktualisieren (Stadt)

auth_ldap | field_updateremote_city

Nie — *Standard: Nie*

Feld sperren (Stadt)

auth_ldap | field_lock_city

Bearbeitbar — *Standard: Bearbeitbar*

Daten übernehmen (Land)

auth_ldap | field_map_country

Standard: Leer

Lokal aktualisieren (Land)

auth_ldap | field_updatelocal_country

Beim Anlegen — *Standard: Beim Anlegen*

Extern aktualisieren (Land)

auth_ldap | field_updateremote_country

Nie — *Standard: Nie*

Feld sperren (Land)

auth_ldap | field_lock_country

Bearbeitbar — *Standard: Bearbeitbar*

Daten übernehmen (Sprache)

auth_ldap | field_map_lang

Standard: Leer

Daten übernehmen (Sprache) auth_ldap | field_map_lang		*Standard: Leer*
Lokal aktualisieren (Sprache) auth_ldap | field_updatelocal_lang	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Sprache) auth_ldap | field_updateremote_lang	Nie	*Standard: Nie*
Feld sperren (Sprache) auth_ldap | field_lock_lang	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Beschreibung) auth_ldap | field_map_description	description	*Standard: Leer*
Lokal aktualisieren (Beschreibung) auth_ldap | field_updatelocal_description	Bei jedem Login	*Standard: Beim Anlegen*
Extern aktualisieren (Beschreibung) auth_ldap | field_updateremote_description	Nie	*Standard: Nie*
Feld sperren (Beschreibung) auth_ldap | field_lock_description	Gesperrt	*Standard: Bearbeitbar*
Daten übernehmen (Webseite) auth_ldap | field_map_url		*Standard: Leer*

Daten übernehmen (Webseite) auth_ldap | field_map_url		*Standard: Leer*
Lokal aktualisieren (Webseite) auth_ldap | field_updatelocal_url	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Webseite) auth_ldap | field_updateremote_url	Nie	*Standard: Nie*
Feld sperren (Webseite) auth_ldap | field_lock_url	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (ID-Nummer) auth_ldap | field_map_idnumber	uidNumber	*Standard: Leer*
Lokal aktualisieren (ID-Nummer) auth_ldap | field_updatelocal_idnumber	Bei jedem Login	*Standard: Beim Anlegen*
Extern aktualisieren (ID-Nummer) auth_ldap | field_updateremote_idnumber	Nie	*Standard: Nie*
Feld sperren (ID-Nummer) auth_ldap | field_lock_idnumber	Gesperrt	*Standard: Bearbeitbar*
Daten übernehmen (Institution) auth_ldap | field_map_institution		*Standard: Leer*

Daten übernehmen (Institution) auth_ldap | field_map_institution		*Standard: Leer*
Lokal aktualisieren (Institution) auth_ldap | field_updatelocal_institution	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Institution) auth_ldap | field_updateremote_institution	Nie	*Standard: Nie*
Feld sperren (Institution) auth_ldap | field_lock_institution	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Abteilung) auth_ldap | field_map_department		*Standard: Leer*
Lokal aktualisieren (Abteilung) auth_ldap | field_updatelocal_department	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Abteilung) auth_ldap | field_updateremote_department	Nie	*Standard: Nie*
Feld sperren (Abteilung) auth_ldap | field_lock_department	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Telefon) auth_ldap | field_map_phone1		*Standard: Leer*

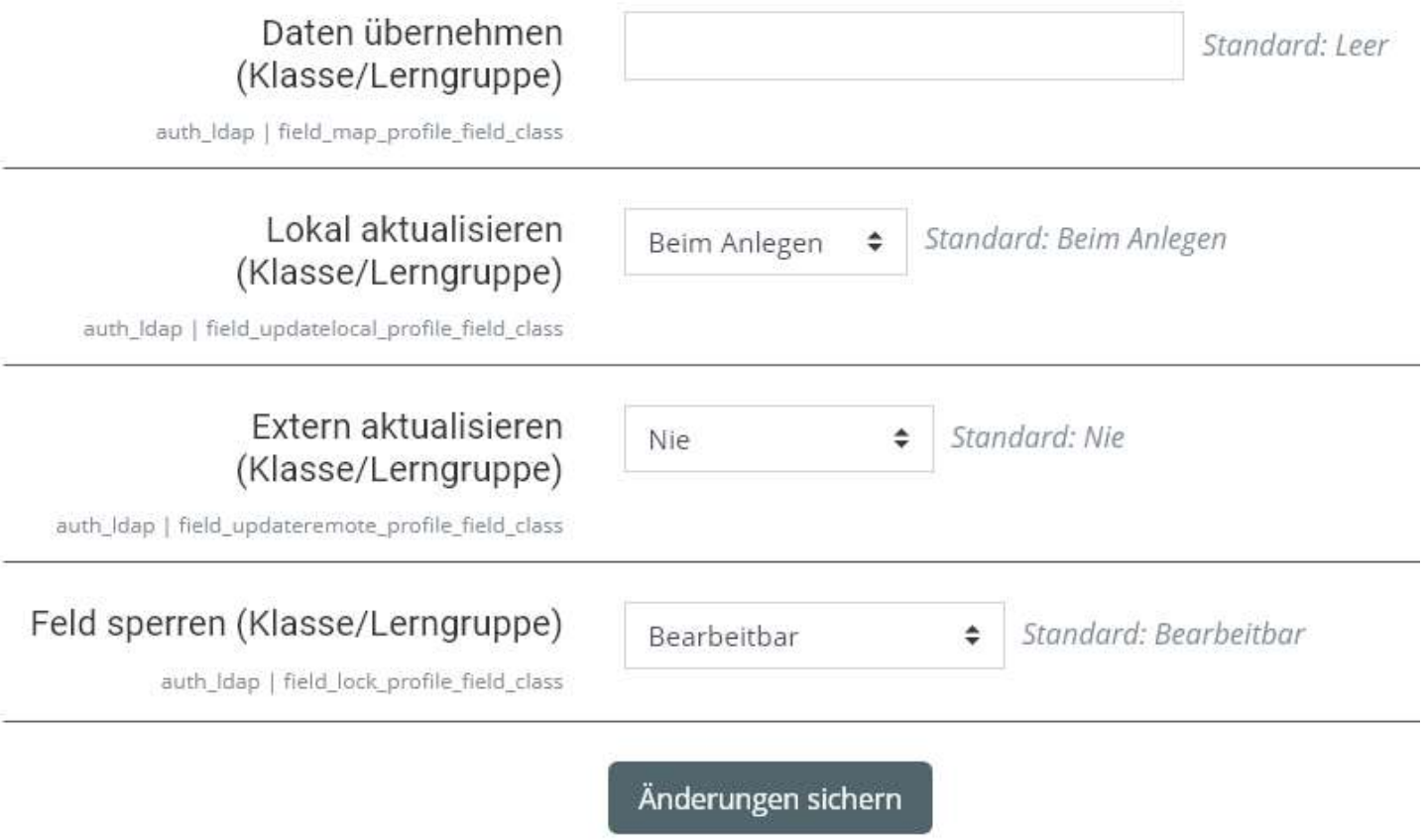
Daten übernehmen (Telefon) auth_ldap | field_map_phone1		*Standard: Leer*
Lokal aktualisieren (Telefon) auth_ldap | field_updatelocal_phone1	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Telefon) auth_ldap | field_updateremote_phone1	Nie	*Standard: Nie*
Feld sperren (Telefon) auth_ldap | field_lock_phone1	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Smartphone) auth_ldap | field_map_phone2		*Standard: Leer*
Lokal aktualisieren (Smartphone) auth_ldap | field_updatelocal_phone2	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Smartphone) auth_ldap | field_updateremote_phone2	Nie	*Standard: Nie*
Feld sperren (Smartphone) auth_ldap | field_lock_phone2	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Adresse) auth_ldap | field_map_address		*Standard: Leer*

Daten übernehmen (Adresse) auth_ldap | field_map_address		*Standard: Leer*
Lokal aktualisieren (Adresse) auth_ldap | field_updatelocal_address	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Adresse) auth_ldap | field_updateremote_address	Nie	*Standard: Nie*
Feld sperren (Adresse) auth_ldap | field_lock_address	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Vorname - lautgetreu) auth_ldap | field_map_firstnamephonetic		*Standard: Leer*
Lokal aktualisieren (Vorname - lautgetreu) auth_ldap | field_updatelocal_firstnamephonetic	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Vorname - lautgetreu) auth_ldap | field_updateremote_firstnamephonetic	Nie	*Standard: Nie*
Feld sperren (Vorname - lautgetreu) auth_ldap | field_lock_firstnamephonetic	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Nachname - lautgetreu) auth_ldap | field_map_lastnamephonetic		*Standard: Leer*

Daten übernehmen (Nachname - lautgetreu) auth_ldap | field_map_lastnamephonetic		*Standard: Leer*
Lokal aktualisieren (Nachname - lautgetreu) auth_ldap | field_updatelocal_lastnamephonetic	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Nachname - lautgetreu) auth_ldap | field_updateremote_lastnamephonetic	Nie	*Standard: Nie*
Feld sperren (Nachname - lautgetreu) auth_ldap | field_lock_lastnamephonetic	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Mittlerer Name) auth_ldap | field_map_middlename		*Standard: Leer*
Lokal aktualisieren (Mittlerer Name) auth_ldap | field_updatelocal_middlename	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Mittlerer Name) auth_ldap | field_updateremote_middlename	Nie	*Standard: Nie*
Feld sperren (Mittlerer Name) auth_ldap | field_lock_middlename	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Pseudonym) auth_ldap | field_map_alternatename		*Standard: Leer*

Daten übernehmen (Pseudonym) auth_ldap | field_map_alternatename		*Standard: Leer*
Lokal aktualisieren (Pseudonym) auth_ldap | field_updatelocal_alternatename	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Pseudonym) auth_ldap | field_updateremote_alternatename	Nie	*Standard: Nie*
Feld sperren (Pseudonym) auth_ldap | field_lock_alternatename	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Geburtsdatum) auth_ldap | field_map_profile_field_dateofbirth		*Standard: Leer*
Lokal aktualisieren (Geburtsdatum) auth_ldap | field_updatelocal_profile_field_dateofbirth	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Geburtsdatum) auth_ldap | field_updateremote_profile_field_dateofbirth	Nie	*Standard: Nie*
Feld sperren (Geburtsdatum) auth_ldap | field_lock_profile_field_dateofbirth	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Geburtsort) auth_ldap | field_map_profile_field_placeofbirth		*Standard: Leer*

Daten übernehmen (Geburtsort) auth_ldap | field_map_profile_field_placeofbirth		*Standard: Leer*
Lokal aktualisieren (Geburtsort) uth_ldap | field_updatelocal_profile_field_placeofbirth	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Geburtsort) auth_ldap | field_updateremote_profile_field_placeofbirth	Nie	*Standard: Nie*
Feld sperren (Geburtsort) auth_ldap | field_lock_profile_field_placeofbirth	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Geschlecht) auth_ldap | field_map_profile_field_gender		*Standard: Leer*
Lokal aktualisieren (Geschlecht) auth_ldap | field_updatelocal_profile_field_gender	Beim Anlegen	*Standard: Beim Anlegen*
Extern aktualisieren (Geschlecht) auth_ldap | field_updateremote_profile_field_gender	Nie	*Standard: Nie*
Feld sperren (Geschlecht) auth_ldap | field_lock_profile_field_gender	Bearbeitbar	*Standard: Bearbeitbar*
Daten übernehmen (Klasse/Lerngruppe) auth_ldap | field_map_profile_field_class		*Standard: Leer*



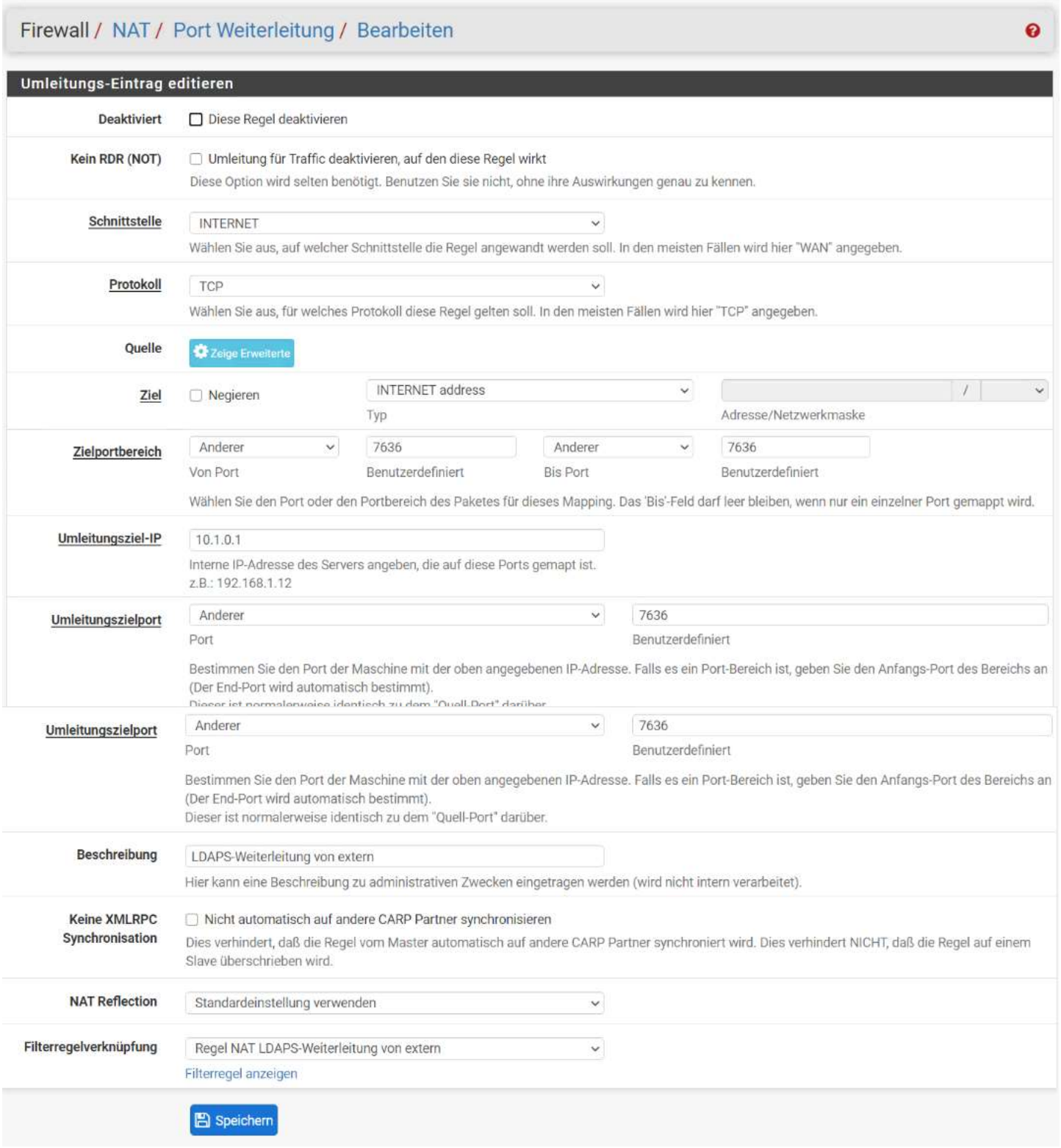
Durch Klicken auf den Button "Änderungen sichern" am Ende der Webseite wird alles gespeichert.

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.

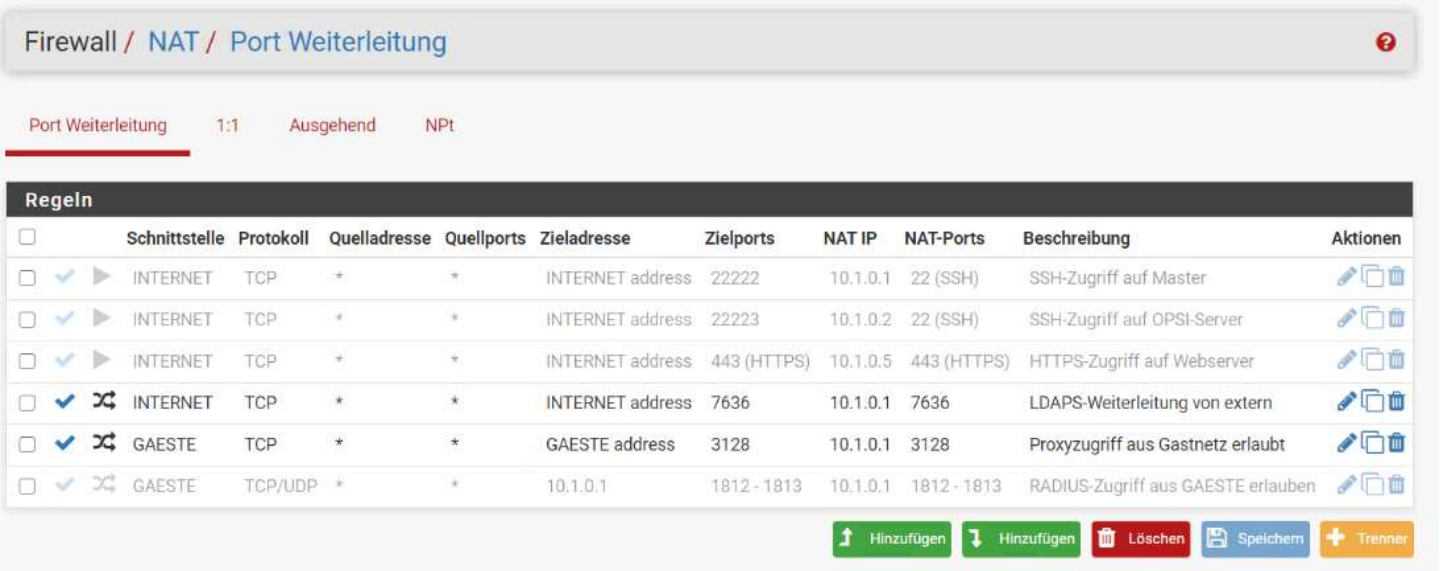
Portweiterleitung in pfSense

In Ihrer lokalen pfSense muss unter Firewall -> NAT -> Portweiterleitung
https://firewall.paedml-linux.lokal/firewall_nat.php
eine Regel für den Zugriff auf das LDAP des Server eingerichtet werden.

Für die Weiterleitungs-Regel werden folgende Einstellungen vorgenommen:



Am Schluß sollte es so aussehen (ggf. haben Sie zusätzliche Weiterleitungen definiert).



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.