

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

Impressum

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

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

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 Profelfeld-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.

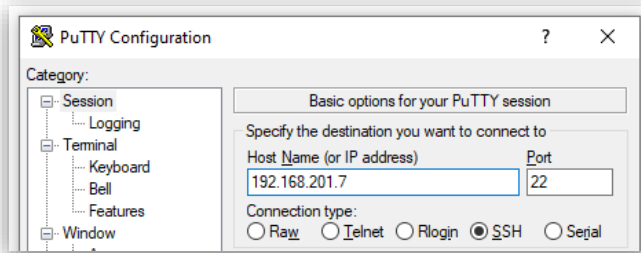
Vergessene Passwörter oder uneinheitliche Benutzernamen sollten damit größtenteils der Vergangenheit angehören. Und falls doch einmal Login-Probleme bestehen, können Lehrerinnen und Lehrer per Schulkonsole die Kennwörter unkompliziert zurücksetzen.

2 Vorgehen 1: LDAPs mit Zertifikat

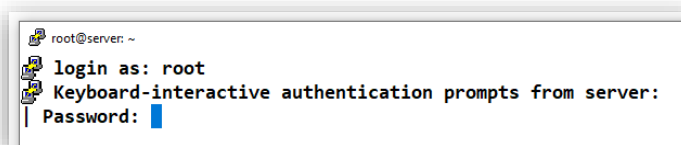
Wir empfehlen Ihnen diese Konfiguration, wenn Sie Dienste per LDAPs mit dem paedML-Server verbinden möchten, die ein öffentliches Zertifikat voraussetzen, z.B. WebUntis. Falls Sie dies nicht benötigen, kann der „einfachere“ Weg mit dem selbst ausgestellten Zertifikat (siehe Kapitel 3) gewählt werden.

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.

Univention Primary Directory Node 5.0-2:



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“:

```
Es müssen 1.760 kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 3.295 kB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren? [J/n]
```

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

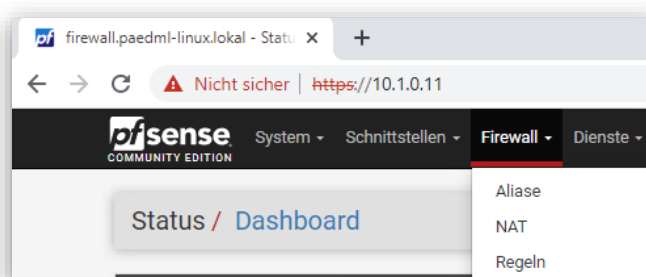
```
[ -x "/etc/init.d/univention-firewall" ] && invoke-rc.d univention-firewall
restart
```

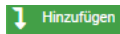
Die Arbeiten auf der Nextcloud sind damit erledigt.

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.

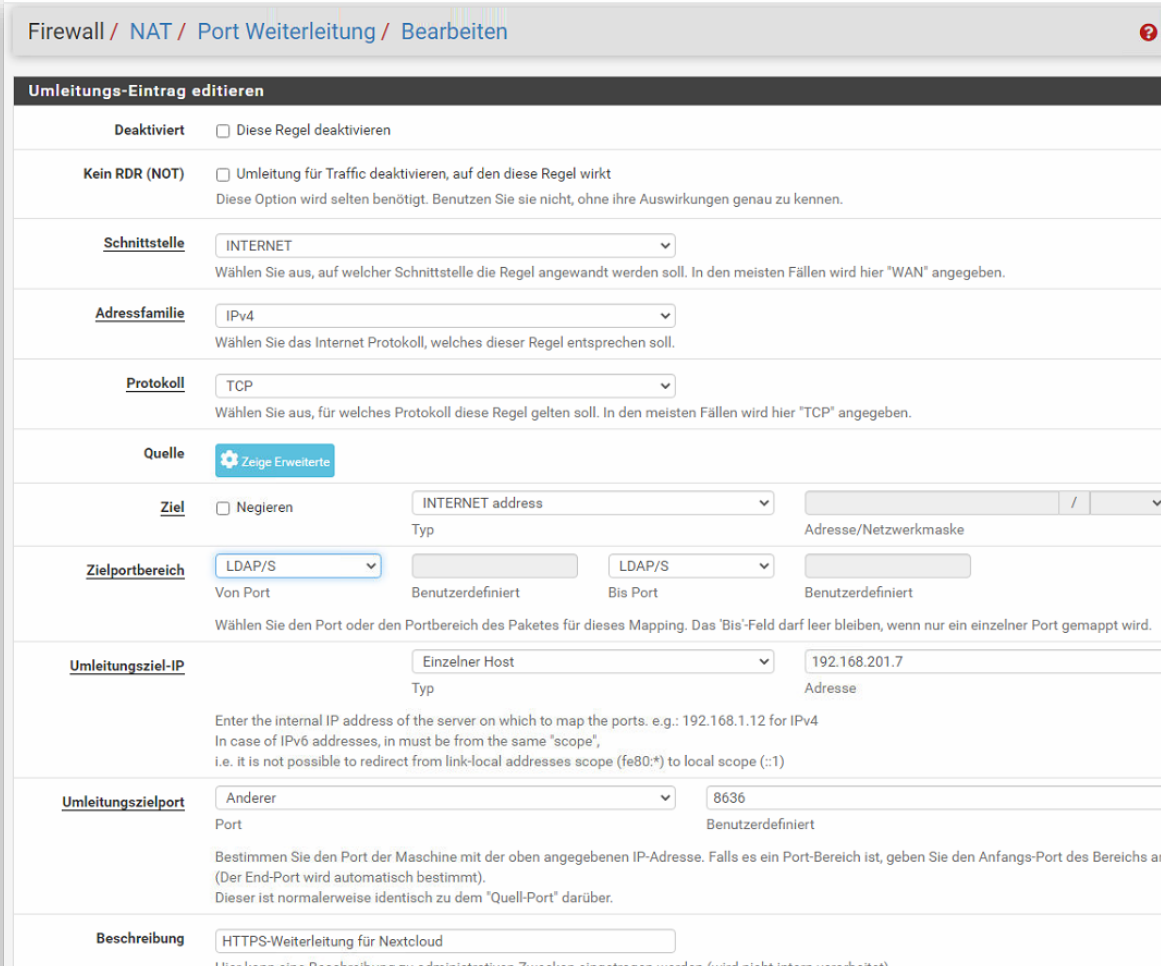
Öffnen Sie die Adresse der Firewall 10.1.0.11 in einem Browser und melden sich als Administrator an. Dort klicken Sie auf Firewall – NAT



Mit einem Klick auf Hinzufügen () 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.



Firewall / NAT / Port Weiterleitung / Bearbeiten

Umleitungs-Eintrag editieren


Deaktiviert ☐ Diese Regel deaktivieren

Kein RDR (NOT) ☐ Umleitung für Traffic deaktivieren, auf den diese Regel wirkt
Diese Option wird selten benötigt. Benutzen Sie sie nicht, ohne ihre Auswirkungen genau zu kennen.

Schnittstelle INTERNET
Wählen Sie aus, auf welcher Schnittstelle die Regel angewandt werden soll. In den meisten Fällen wird hier "WAN" angegeben.

Adressfamilie IPv4
Wählen Sie das Internet Protokoll, welches dieser Regel entsprechen soll.

Protokoll TCP
Wählen Sie aus, für welches Protokoll diese Regel gelten soll. In den meisten Fällen wird hier "TCP" angegeben.

Quelle 

Ziel ☐ Negieren INTERNET address
Typ Adresse/Netzwerkmaske

Zielportbereich LDAP/S
Von Port Benutzerdefiniert Bis Port Benutzerdefiniert
Wählen Sie den Port oder den Portbereich des Paketes für dieses Mapping. Das "Bis"-Feld darf leer bleiben, wenn nur ein einzelner Port gemappt wird.

Umleitungsziel-IP Einzelner Host 192.168.201.7
Typ Adresse
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Umleitungszielport Anderer 8636
Port Benutzerdefiniert
Bestimmen Sie den Port der Maschine mit der oben angegebenen IP-Adresse. Falls es ein Port-Bereich ist, geben Sie den Anfangs-Port des Bereichs an (Der End-Port wird automatisch bestimmt).
Dieser ist normalerweise identisch zu dem "Quell-Port" darüber.

Beschreibung HTTPS-Weiterleitung für Nextcloud
Hier kann eine Beschreibung zu administrativen Zwecken eingetragen werden (wird nicht intern verarbeitet).

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



pfSense COMMUNITY EDITION

System - Schnittstellen - Firewall - Dienste - VPN - Status - Diagnose - Hilfe

Firewall / Regeln / DMZ

Übergreifend INTERNET PAEDAGOGIK GAESTE WLANSCHULE **DMZ** OpenVPN

Regeln (Ziehen, um die Anordnung zu ändern)

<input type="checkbox"/>	States	Protokoll	Quelle	Port	Ziel	Port	Gateway	Queue	Zeitplan	Beschreibung	Aktionen
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	192.168.201.7	*	10.1.0.1	7389	*	nicht gesetzt		LDAP-Zugriff auf den Server erlauben	

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“.

Ziel

Ziel

☐ Invert match

Einzelner Host oder Alias

10.1.0.1

Bereich der Zielports

(anderer)

7636

(anderer)

7636

Von

Benutzerdefiniert

Bis

Benutzerdefiniert

Wählen Sie den ziel Port oder den Portbereich für diese Regel. Das 'Bis'-Feld darf leer bleiben, wenn nur ein einzelner Port gemappt wird.

Zusätzliche Optionen

Protokollieren

☐ Von dieser Regel erfasste Pakete protokollieren

Tipp: Die Firewall hat nur einen begrenzten Platz für die lokale Speicherung von Protokollen. Benutzen Sie diese Option sparsam. Für umfangreicheres Protokollieren empfiehlt sich die Einrichtung eines externen Syslog Servers (Status : System Logs: Einstellungen Seite).

Beschreibung

LDAPs-Zugriff auf den Server erlauben

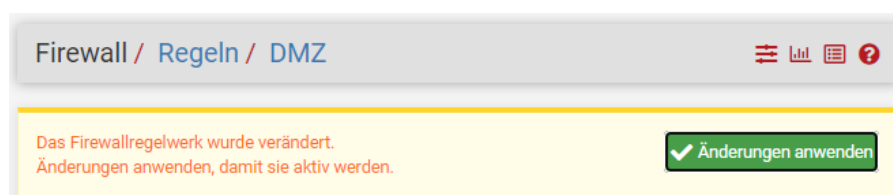
Beschreibung für administrative Zwecke eingeben. Ein Maximum von 52 Buchstaben wird im Regelsatz benutzt und im Firewall Log angezeigt.

Erweiterte Optionen

Zeige Erweiterte

Speichern

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.

SSL Checker

Submit the Hostname and Port in the fields below. This checker supports SNI and STARTTLS.

Hostname*

cloud.meine-schule.de

Port*

636

CHECK

Report

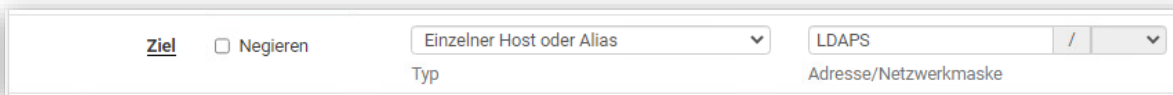
It's all good. We have not detected any issues.

Hostname:	✓ Matches Common Name or/and SAN
Expired:	✓ No (45 days till expiration)
Public Key:	✓ We were unable to find any issues in the public key of end-entity certificate
Trusted:	✓ Yes, we were able to verify the certificate
Self-Signed:	✓ No, the end-entity certificate is not self-signed
Chain Issues:	✓ No, we were unable to detect any issues in the certificate chain sent by the server
Weak signatures:	✓ No, certificates sent by the server were not signed utilizing a weak hash function
OCSP Status:	✓ OCSP Responder returned 'good' status for the end-entity certificate

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

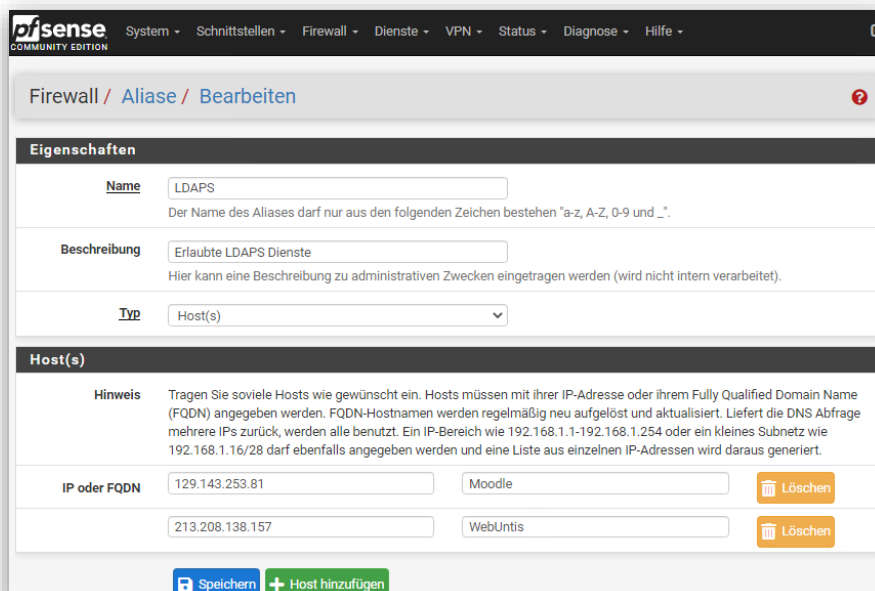
Sobald die Einrichtung abgeschlossen ist, können Sie optional noch einschränken, welche Adressen aus dem Internet den Port 636 auf Ihrem Server erreichen können. Dazu wählen Sie Firewall – Aliase und wählen dort Hinzufügen. Hier vergeben Sie einen Namen, z.B. „LDAPS“, und können die IP-Adressen Ihrer 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 „Einzeln 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

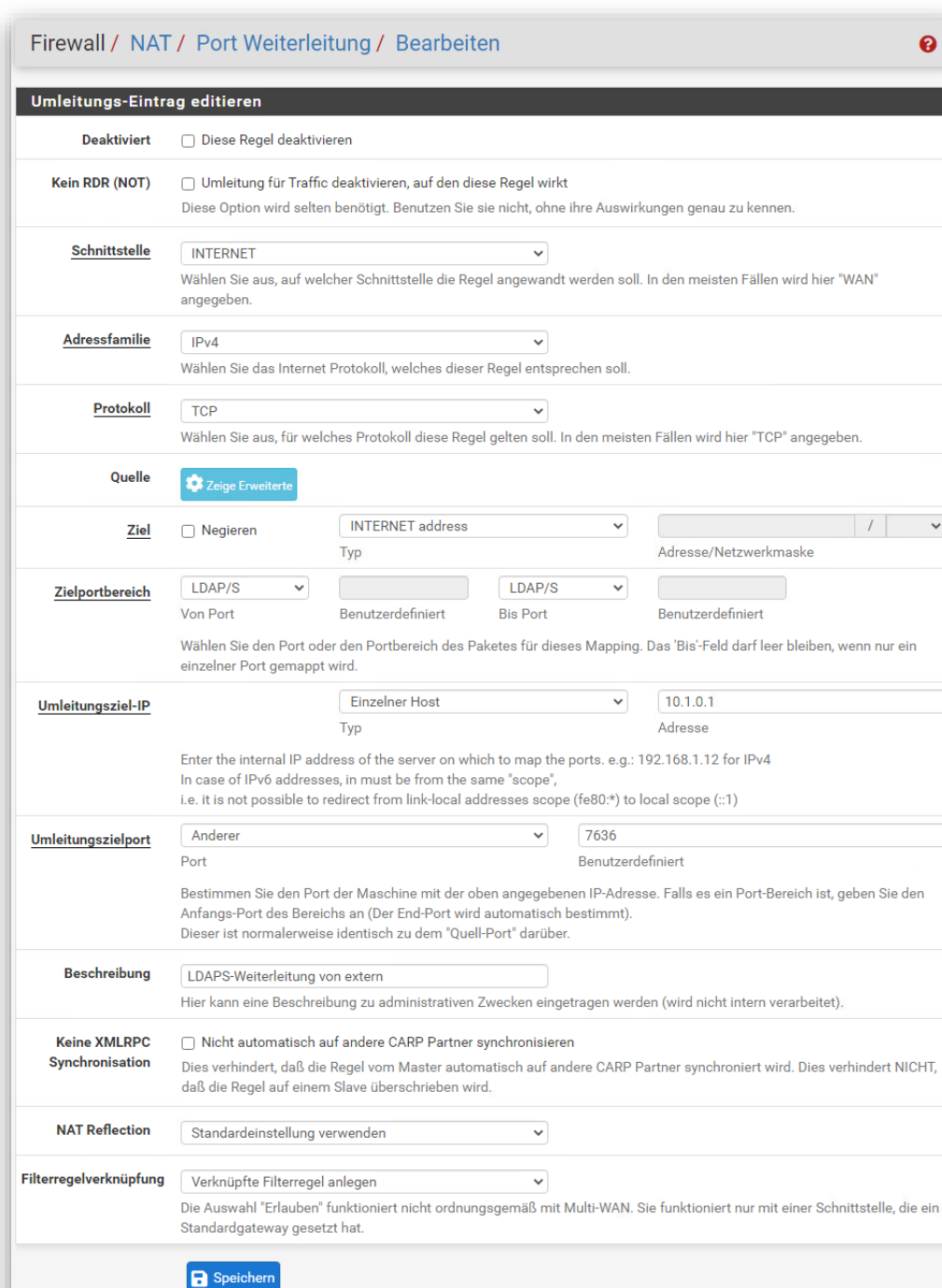
Bis auf WebUntis scheinen die meisten externen Dienste das Zertifikat der LDAPs Verbindung nicht zu prüfen, daher können Sie auch das paedML-interne Zertifikat verwenden und damit die Nextcloud komplett umgehen.

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:



Firewall / NAT / Port Weiterleitung / Bearbeiten

Umleitungs-Eintrag editieren

Deaktiviert ☐ Diese Regel deaktivieren

Kein RDR (NOT) ☐ Umleitung für Traffic deaktivieren, auf den diese Regel wirkt
Diese Option wird selten benötigt. Benutzen Sie sie nicht, ohne ihre Auswirkungen genau zu kennen.

Schnittstelle
Wählen Sie aus, auf welcher Schnittstelle die Regel angewandt werden soll. In den meisten Fällen wird hier "WAN" angegeben.

Adressfamilie
Wählen Sie das Internet Protokoll, welches dieser Regel entsprechen soll.

Protokoll
Wählen Sie aus, für welches Protokoll diese Regel gelten soll. In den meisten Fällen wird hier "TCP" angegeben.

Quelle

Ziel ☐ Negieren
Typ Adresse/Netzwerkmaske

Zielportbereich
Von Port Benutzerdefiniert Bis Port Benutzerdefiniert
Wählen Sie den Port oder den Portbereich des Paketes für dieses Mapping. Das 'Bis'-Feld darf leer bleiben, wenn nur ein einzelner Port gemappt wird.

Umleitungsziel-IP
Typ Adresse
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)

Umleitungszielport
Port Benutzerdefiniert
Bestimmen Sie den Port der Maschine mit der oben angegebenen IP-Adresse. Falls es ein Port-Bereich ist, geben Sie den Anfangs-Port des Bereichs an (Der End-Port wird automatisch bestimmt).
Dieser ist normalerweise identisch zu dem "Quell-Port" darüber.

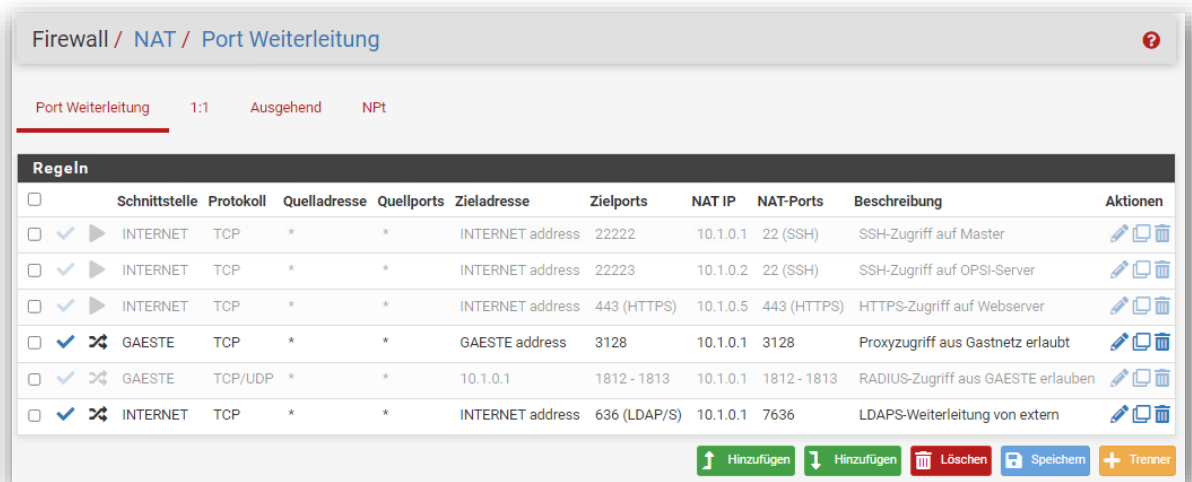
Beschreibung
Hier kann eine Beschreibung zu administrativen Zwecken eingetragen werden (wird nicht intern verarbeitet).



















Keine XMLRPC Synchronisation ☐ Nicht automatisch auf andere CARP Partner synchronisieren
Dies verhindert, daß die Regel vom Master automatisch auf andere CARP Partner synchronisiert wird. Dies verhindert NICHT, daß die Regel auf einem Slave überschrieben wird.






NAT Reflection

Filterregelverknüpfung
Die Auswahl "Erlauben" funktioniert nicht ordnungsgemäß mit Multi-WAN. Sie funktioniert nur mit einer Schnittstelle, die ein Standardgateway gesetzt hat.

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



Firewall / NAT / Port Weiterleitung										
Port Weiterleitung 1:1 Ausgehend NPT										
Regeln										
<input type="checkbox"/>	Schnittstelle	Protokoll	Quelladresse	Quellports	Zieladresse	Zielpports	NAT IP	NAT-Ports	Beschreibung	Aktionen
<input type="checkbox"/>	INTERNET	TCP	*	*	INTERNET address	22222	10.1.0.1	22 (SSH)	SSH-Zugriff auf Master	  
<input type="checkbox"/>	INTERNET	TCP	*	*	INTERNET address	22223	10.1.0.2	22 (SSH)	SSH-Zugriff auf OPSI-Server	  
<input type="checkbox"/>	INTERNET	TCP	*	*	INTERNET address	443 (HTTPS)	10.1.0.5	443 (HTTPS)	HTTPS-Zugriff auf Webserver	  
<input checked="" type="checkbox"/>	GUEST	TCP	*	*	GUEST address	3128	10.1.0.1	3128	Proxyzugriff aus Gastnetz erlaubt	  
<input type="checkbox"/>	GUEST	TCP/UDP	*	*	10.1.0.1	1812 - 1813	10.1.0.1	1812 - 1813	RADIUS-Zugriff aus GUEST erlauben	  
<input type="checkbox"/>	INTERNET	TCP	*	*	INTERNET address	636 (LDAP/S)	10.1.0.1	7636	LDAPS-Weiterleitung von extern	  

 Hinzufügen
  Hinzufügen
  Löschen
  Speichern
  Trenner

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 Profildfeld-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.

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Einstellungen prüfen	Deinstallieren
Manuelle Konten	6			Einstellungen		
Kein Login	0					
Webservices	0		↓			
LDAP-Server	2		↑ ↓	Einstellungen	Einstellungen prüfen	
E-Mail basierte Selbstregistrierung	0		↑	Einstellungen		Deinstallieren

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.

LDAP-Server

Diese Anmeldemethode ermöglicht die Authentifizierung gegenüber einem externen LDAP-Server. Wenn der angegebene Anmeldename und das angegebene Kennwort gültig sind, erstellt Moodle ein neues Nutzerkonto in seiner Datenbank. Dieses Plugin kann Nutzerattribute aus LDAP lesen und gewünschte Felder in Moodle vorab ausfüllen. Bei nachfolgenden Anmeldungen werden nur noch der Anmeldename und das Kennwort überprüft.

LDAP-Server-Einstellungen

Host URL <small>auth_ldap host_url</small>	<input type="text" value="ldaps://1.2.3.4"/> Standard: Leer
Geben Sie einen LDAP-Server in URL-Form an, z.B. 'ldap://ldap.meinserver.de/' oder 'ldaps://ldap.meinserver.de/'. Mehrere LDAP-Server trennen Sie bitte mit ';' (Semikolon), z.B. als LDAP-Failover.	
Version <small>auth_ldap ldap_version</small>	<input type="text" value="3"/> Standard: 3
Tragen Sie verfügbare LDAP-Version auf Ihrem Server ein.	
TLS benutzen <small>auth_ldap start_tls</small>	<input type="text" value="Nein"/> Standard: Nein
LDAP-Service mit TLS (Port 389) verwenden	
LDAP-Codierung <small>auth_ldap ldapencoding</small>	<input type="text" value="utf-8"/> Standard: utf-8
Codierung des LDAP-Servers, meistens utf-8. Wenn LDAP v2 ausgewählt ist, verwendet das Microsoft ActiveDirectory seine Codierungen, z.B. cp1252 oder cp1250.	
Seitengröße <small>auth_ldap pagesize</small>	<input type="text" value="250"/> Standard: 250
Stellen Sie sicher, dass dieser Wert kleiner ist als die Obergrenze Ihres LDAP-Servers für eine einzelne Datenbankabfrage.	


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.

Bind-Einstellungen


Kennwort-Caching verhindern <small>auth_ldap preventpassindb</small>	<input type="text" value="Ja"/> Standard: Nein
Wählen Sie 'ja', um Kennwörter nicht in die Moodle-Datenbank zu übernehmen	
Anmeldename <small>auth_ldap bind_dn</small>	<input type="text" value="uid=ldapsuche,cn=users,dc=paedml-lir"/> Standard: Leer
Falls Sie für die Nutzerabfrage einen 'Bind-User' verwenden müssen, tragen Sie hier dessen Anmeldnamen ein. Der Eintrag hat üblicherweise die Form: 'cn=ldapuser,ou=public,o=org'.	
Kennwort <small>auth_ldap bind_pw</small>	<input type="password" value="....."/> 
Kennwort des Bind-Users	

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




Nutzersuche (user lookup)

Nutzertyp <small>auth_ldap user_type</small>	Standard  <i>Standard: Standard</i>	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 <small>auth_ldap contexts</small>	cn=users,ou=schule,dc=paedml-linux,c <i>Standard: Leer</i>	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 <small>auth_ldap search_sub</small>	Ja  <i>Standard: Nein</i>	Nutzersuche auch in Subkontexten durchführen
Aliase berücksichtigen <small>auth_ldap opt_deref</small>	Nein  <i>Standard: Nein</i>	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 <small>auth_ldap user_attribute</small>	uid <i>Standard: Leer</i>	Optional: Merkmal zur Nutzerbenennung und -suche ändern. Normalerweise 'cn'.

Ausblendemerkmal <small>auth_ldap suspended_attribute</small>	<input type="text"/> <i>Standard: Leer</i>	Optional: Falls verfügbar wird dieses Merkmal verwendet, um das erstellte lokale Nutzerkonto zu aktivieren oder auszublenden.
Mitgliedsmerkmal <small>auth_ldap memberattribute</small>	memberOf <i>Standard: Leer</i>	Optional: Mitgliedsmerkmal ändern, mit dem Nutzer/innen zu einer Gruppe gehören. Normalerweise 'member'
Mitgliedsmerkmal nutzt dn <small>auth_ldap memberattribute_isdn</small>	1 <i>Standard: Leer</i>	Optional: Gebrauch von Mitgliedsmerkmalen ändern, entweder 0 oder 1
ObjectClass <small>auth_ldap objectclass</small>	<input type="text"/> <i>Standard: Leer</i>	Optional: Überschreibt die ObjectClass zur Nutzersuche in LDAP (ldap_user_type). Die Voreinstellung muss normalerweise nicht geändert werden.



4.1.5 Kennwortänderung fordern

Im Abschnitt „Kennwortänderung fordern“ sind die Standardeinstellungen einzustellen.

Kennwortänderung fordern	
Kennwortänderung fordern <small>auth_ldap forcechangepassword</small>	<div>Nein  <i>Standard: Nein</i></div> <p>Nutzer/Innen werden aufgefordert, ihr Kennwort beim ersten Anmelden zu ändern.</p>
Standardseite zur Kennwortänderung nutzen <small>auth_ldap stdchangepassword</small>	<div>Nein  <i>Standard: Nein</i></div> <p>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.</p>
Kennwortformat <small>auth_ldap passtype</small>	<div>Unformatierter Text  <i>Standard: Unformatierter Text</i></div> <p>Geben Sie das Format für neue Kennwörter auf dem LDAP-Server an.</p>
URL zur Kennwortänderung <small>auth_ldap changepasswordurl</small>	<div><input type="text"/> <i>Standard: Leer</i></div> <p>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.</p>

4.1.6 Einstellungen zum Ablauf von LDAP-Kennwörtern

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

Einstellungen zum Ablauf von LDAP-Kennwörtern	
Ablauf <small>auth_ldap expiration</small>	<div>Nein  <i>Standard: Nein</i></div> <p>Wählen Sie 'Nein', um den Ablauf von Kennwörtern nicht zu prüfen. Wenn Sie 'LDAP-Server' wählen, wird Ablaufdatum direkt vom LDAP-Server zu lesen.</p>
Ablaufwarnung <small>auth_ldap expiration_warning</small>	<div><input type="text"/> <i>Standard: Leer</i></div> <p>Anzahl der Tage, an denen vor dem Ablauf eines Kennwortes eine Warnung ausgegeben wird</p>
Ablaufmerkmal <small>auth_ldap expireattr</small>	<div><input type="text"/> <i>Standard: Leer</i></div> <p>Optional: Überschreibt die LDAP-Attribute, die das Ablaufdatum für Kennwörter enthalten.</p>
GraceLogins <small>auth_ldap gracelogins</small>	<div>Nein  <i>Standard: Nein</i></div> <p>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.</p>
Merkmal für GraceLogin <small>auth_ldap graceattr</small>	<div><input type="text"/> <i>Standard: Leer</i></div> <p>Optional: GraceLogin-Attribut überschreiben</p>

4.1.7 Nutzererstellung aktivieren

Im Abschnitt "Nutzererstellung aktivieren" sind die Standardeinstellungen einzustellen.

Nutzererstellung aktivieren

Nutzer/innen extern anlegen

Nein

Standard: Nein

auth_ldap | auth_user_create

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

Standard: Leer

auth_ldap | create_context

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.

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.

Zuordnung von Systemrollen

Manager/in-Kontext

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

Standard: Leer

auth_ldap | managercontext

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

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

Standard: Leer

auth_ldap | coursecreatorcontext

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".

4.1.9 Synchronisierung von Nutzerkonten

Bei „Synchronisierung von Nutzerkonten“ ist einzustellen:

Synchronisierung von Nutzerkonten	
Entfernte externe Nutzer <small>auth_ldap removeuser</small>	<div> Intern löschen <div></div> Standard: Nur intern zugänglich </div> <p>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.</p>
Status von lokalen Nutzerkonten synchronisieren <small>auth_ldap sync_suspended</small>	<div> Nein <div></div> Standard: Nein </div> <p>Die Option legt fest, dass das Ausblendemerkmal bei der Synchronisation von lokalen Nutzerkonten verwendet wird.</p>

4.1.10 NTLM-SSO

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

NTLM-SSO	
Aktivieren <small>auth_ldap ntlmssso_enabled</small>	<div> Nein <div></div> Standard: Nein </div> <p>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.</p>
Subnet <small>auth_ldap ntlmssso_subnet</small>	<div> <div></div> Standard: Leer </div> <p>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</p>
MS IE fast path? <small>auth_ldap ntlmssso_ie_fastpath</small>	<div> NTLM mit allen Browsern versuchen <div></div> Standard: NTLM mit allen Browsern versuchen </div> <p>Wenn diese Option aktiviert ist, wird der 'NTLM SSO fast path' zugelassen. Das funktioniert nur mit dem Internet Explorer.</p>
Authentifizierungsart <small>auth_ldap ntlmssso_type</small>	<div> NTLM <div></div> Standard: NTLM </div> <p>Diese Methode ist beim Webserver eingestellt, um Nutzer/innen zu authentifizieren. Falls Sie sich nicht sicher sind, wählen Sie bitte NTLM.</p>
Format externer Nutzernamen <small>auth_ldap ntlmssso_remoteuserformat</small>	<div> <div></div> Standard: Leer </div> <p>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.</p> <p>Häufig genutzte Formate sind %domain%%username% (MS Windows default), %domain%/%username%, %domain%+username% und einfach %username% (wenn kein Domainteil verwendet wird).</p>

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.

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)	<input type="text" value="givenName"/>	Standard: Leer
<small>auth_ldap field_map_firstname</small>		
Lokal aktualisieren (Vorname)	<input type="button" value="Bei jedem Login"/>	Standard: Beim Anlegen
<small>auth_ldap field_updatelocal_firstname</small>		
Extern aktualisieren (Vorname)	<input type="button" value="Nie"/>	Standard: Nie
<small>auth_ldap field_updateremote_firstname</small>		
Feld sperren (Vorname)	<input type="button" value="Gesperrt"/>	Standard: Bearbeitbar
<small>auth_ldap field_lock_firstname</small>		
Daten übernehmen (Nachname)	<input type="text" value="sn"/>	Standard: Leer
<small>auth_ldap field_map_lastname</small>		
Lokal aktualisieren (Nachname)	<input type="button" value="Bei jedem Login"/>	Standard: Beim Anlegen
<small>auth_ldap field_updatelocal_lastname</small>		
Extern aktualisieren (Nachname)	<input type="button" value="Nie"/>	Standard: Nie
<small>auth_ldap field_updateremote_lastname</small>		
Feld sperren (Nachname)	<input type="button" value="Gesperrt"/>	Standard: Bearbeitbar
<small>auth_ldap field_lock_lastname</small>		
Daten übernehmen (E-Mail-Adresse)	<input type="text" value="mailPrimaryAddress"/>	Standard: Leer
<small>auth_ldap field_map_email</small>		
Lokal aktualisieren (E-Mail-Adresse)	<input type="button" value="Bei jedem Login"/>	Standard: Beim Anlegen
<small>auth_ldap field_updatelocal_email</small>		
Extern aktualisieren (E-Mail-Adresse)	<input type="button" value="Nie"/>	Standard: Nie
<small>auth_ldap field_updateremote_email</small>		
Feld sperren (E-Mail-Adresse)	<input type="button" value="Gesperrt"/>	Standard: Bearbeitbar
<small>auth_ldap field_lock_email</small>		
Daten übernehmen (Stadt)	<input type="text"/>	Standard: Leer
<small>auth_ldap field_map_city</small>		

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

Daten übernehmen (Institution)

auth_idap | field_map_institution

Standard: Leer

Lokal aktualisieren (Institution)

auth_idap | field_updatelocal_institution

Beim Anlegen

Standard: Beim Anlegen

Extern aktualisieren (Institution)

auth_idap | field_updateremote_institution

Nie

Standard: Nie

Feld sperren (Institution)

auth_idap | field_lock_institution

Bearbeitbar

Standard: Bearbeitbar

Daten übernehmen (Abteilung)

auth_idap | field_map_department

Standard: Leer

Lokal aktualisieren (Abteilung)

auth_idap | field_updatelocal_department

Beim Anlegen

Standard: Beim Anlegen

Extern aktualisieren (Abteilung)

auth_idap | field_updateremote_department

Nie

Standard: Nie

Feld sperren (Abteilung)

auth_idap | field_lock_department

Bearbeitbar

Standard: Bearbeitbar

Daten übernehmen (Telefon)

auth_idap | field_map_phone1

Standard: Leer

Lokal aktualisieren (Telefon)

auth_idap | field_updatelocal_phone1

Beim Anlegen

Standard: Beim Anlegen

Extern aktualisieren (Telefon)

auth_idap | field_updateremote_phone1

Nie

Standard: Nie

Feld sperren (Telefon)

auth_idap | field_lock_phone1

Bearbeitbar

Standard: Bearbeitbar

Daten übernehmen (Smartphone)

auth_idap | field_map_phone2

Standard: Leer

Lokal aktualisieren (Smartphone)

auth_idap | field_updatelocal_phone2

Beim Anlegen

Standard: Beim Anlegen

Extern aktualisieren (Smartphone)

auth_idap | field_updateremote_phone2

Nie

Standard: Nie

Feld sperren (Smartphone)

auth_idap | field_lock_phone2

Bearbeitbar

Standard: Bearbeitbar

Daten übernehmen (Adresse)

auth_idap | field_map_address

Standard: Leer

Daten übernehmen (Adresse) <small>auth_idap field_map_address</small>	<input type="text"/>	Standard: Leer
Lokal aktualisieren (Adresse) <small>auth_idap field_updatelocal_address</small>	Beim Anlegen	Standard: Beim Anlegen
Extern aktualisieren (Adresse) <small>auth_idap field_updateremote_address</small>	Nie	Standard: Nie
Feld sperren (Adresse) <small>auth_idap field_lock_address</small>	Bearbeitbar	Standard: Bearbeitbar
Daten übernehmen (Vorname - lautgetreu) <small>auth_idap field_map_firstnamephonetic</small>	<input type="text"/>	Standard: Leer
Lokal aktualisieren (Vorname - lautgetreu) <small>auth_idap field_updatelocal_firstnamephonetic</small>	Beim Anlegen	Standard: Beim Anlegen
Extern aktualisieren (Vorname - lautgetreu) <small>auth_idap field_updateremote_firstnamephonetic</small>	Nie	Standard: Nie
Feld sperren (Vorname - lautgetreu) <small>auth_idap field_lock_firstnamephonetic</small>	Bearbeitbar	Standard: Bearbeitbar
Daten übernehmen (Nachname - lautgetreu) <small>auth_idap field_map_lastnamephonetic</small>	<input type="text"/>	Standard: Leer
Lokal aktualisieren (Nachname - lautgetreu) <small>auth_idap field_updatelocal_lastnamephonetic</small>	Beim Anlegen	Standard: Beim Anlegen
Extern aktualisieren (Nachname - lautgetreu) <small>auth_idap field_updateremote_lastnamephonetic</small>	Nie	Standard: Nie
Feld sperren (Nachname - lautgetreu) <small>auth_idap field_lock_lastnamephonetic</small>	Bearbeitbar	Standard: Bearbeitbar
Daten übernehmen (Mittlerer Name) <small>auth_idap field_map_middlename</small>	<input type="text"/>	Standard: Leer
Lokal aktualisieren (Mittlerer Name) <small>auth_idap field_updatelocal_middlename</small>	Beim Anlegen	Standard: Beim Anlegen
Extern aktualisieren (Mittlerer Name) <small>auth_idap field_updateremote_middlename</small>	Nie	Standard: Nie
Feld sperren (Mittlerer Name) <small>auth_idap field_lock_middlename</small>	Bearbeitbar	Standard: Bearbeitbar
Daten übernehmen (Pseudonym) <small>auth_idap field_map_alternatename</small>	<input type="text"/>	Standard: Leer

Lokal aktualisieren (Pseudonym) <small>auth_idap field_updatelocal_alternatenamen</small>	<div>Beim Anlegen</div>	<i>Standard: Beim Anlegen</i>
Extern aktualisieren (Pseudonym) <small>auth_idap field_updateremote_alternatenamen</small>	<div>Nie</div>	<i>Standard: Nie</i>
Feld sperren (Pseudonym) <small>auth_idap field_lock_alternatenamen</small>	<div>Bearbeitbar</div>	<i>Standard: Bearbeitbar</i>
Daten übernehmen (Geburtsdatum) <small>auth_idap field_map_profile_field_dateofbirth</small>	<div></div>	<i>Standard: Leer</i>
Lokal aktualisieren (Geburtsdatum) <small>auth_idap field_updatelocal_profile_field_dateofbirth</small>	<div>Beim Anlegen</div>	<i>Standard: Beim Anlegen</i>
Extern aktualisieren (Geburtsdatum) <small>auth_idap field_updateremote_profile_field_dateofbirth</small>	<div>Nie</div>	<i>Standard: Nie</i>
Feld sperren (Geburtsdatum) <small>auth_idap field_lock_profile_field_dateofbirth</small>	<div>Bearbeitbar</div>	<i>Standard: Bearbeitbar</i>
Daten übernehmen (Geburtsort) <small>auth_idap field_map_profile_field_placeofbirth</small>	<div></div>	<i>Standard: Leer</i>
Lokal aktualisieren (Geburtsort) <small>uth_idap field_updatelocal_profile_field_placeofbirth</small>	<div>Beim Anlegen</div>	<i>Standard: Beim Anlegen</i>
Extern aktualisieren (Geburtsort) <small>auth_idap field_updateremote_profile_field_placeofbirth</small>	<div>Nie</div>	<i>Standard: Nie</i>
Feld sperren (Geburtsort) <small>auth_idap field_lock_profile_field_placeofbirth</small>	<div>Bearbeitbar</div>	<i>Standard: Bearbeitbar</i>
Daten übernehmen (Geschlecht) <small>auth_idap field_map_profile_field_gender</small>	<div></div>	<i>Standard: Leer</i>
Lokal aktualisieren (Geschlecht) <small>auth_idap field_updatelocal_profile_field_gender</small>	<div>Beim Anlegen</div>	<i>Standard: Beim Anlegen</i>
Extern aktualisieren (Geschlecht) <small>auth_idap field_updateremote_profile_field_gender</small>	<div>Nie</div>	<i>Standard: Nie</i>
Feld sperren (Geschlecht) <small>auth_idap field_lock_profile_field_gender</small>	<div>Bearbeitbar</div>	<i>Standard: Bearbeitbar</i>

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

Daten übernehmen (Klasse/Lerngruppe)	<input type="text" value="description"/>	Standard: Leer
<small>auth_ldap field_map_profile_field_class</small>		
Lokal aktualisieren (Klasse/Lerngruppe)	Bei jedem Login	Standard: Beim Anlegen
<small>auth_ldap field_updatelocal_profile_field_class</small>		
Extern aktualisieren (Klasse/Lerngruppe)	Nie	Standard: Nie
<small>auth_ldap field_updateremote_profile_field_class</small>		
Feld sperren (Klasse/Lerngruppe)	Gesperrt	Standard: Bearbeitbar
<small>auth_ldap field_lock_profile_field_class</small>		
Daten übernehmen (Außerordentlich)	<input type="text"/>	Standard: Leer
<small>auth_ldap field_map_profile_field_ausserordentlich</small>		
Lokal aktualisieren (Außerordentlich)	Beim Anlegen	Standard: Beim Anlegen
<small>auth_ldap field_updatelocal_profile_field_ausserordentlich</small>		
Extern aktualisieren (Außerordentlich)	Nie	Standard: Nie
<small>auth_ldap field_updateremote_profile_field_ausserordentlich</small>		
Feld sperren (Außerordentlich)	Bearbeitbar	Standard: Bearbeitbar
<small>auth_ldap field_lock_profile_field_ausserordentlich</small>		

Änderungen speichern

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.

LDAP-Server-Einstellungen

Host URL <small>auth_ldap host_url</small>	<input type="text" value="ldaps://1.2.3.4"/>	Standard: Leer
Geben Sie einen LDAP-Server in URL-Form an, z.B. 'ldaps://ldap.meinserver.de/' oder 'ldaps://ldap.meinserver.de/'. Mehrere LDAP-Server trennen Sie bitte mit ';' (Semikolon), z.B. als LDAP-Failover.		
Version <small>auth_ldap ldap_version</small>	<input type="text" value="3"/>	Standard: 3
Tragen Sie verfügbare LDAP-Version auf Ihrem Server ein.		
TLS benutzen <small>auth_ldap start_tls</small>	<input type="text" value="Nein"/>	Standard: Nein
LDAP-Service mit TLS (Port 389) verwenden		
LDAP-Codierung <small>auth_ldap ldap_encoding</small>	<input type="text" value="utf-8"/>	Standard: utf-8
Codierung des LDAP-Servers, meistens utf-8. Wenn LDAP v2 ausgewählt ist, verwendet das Microsoft ActiveDirectory seine Codierungen, z.B. cp1252 oder cp1250.		
Seitengröße <small>auth_ldap pagesize</small>	<input type="text" value="250"/>	Standard: 250
Stellen Sie sicher, dass dieser Wert kleiner ist als die Obergrenze Ihres LDAP-Servers für eine einzelne Datenbankabfrage.		

Bind-Einstellungen

Anmeldename des Bind Users <small>enrol_ldap bind_dn</small>	<input type="text" value="uid=ldapsuche,cn=users,dc=paedml"/>	Standard: Leer
Wenn Sie einen sog. bind-user für die LDAP-Suche nach Nutzer/innen verwenden wollen, geben Sie diesen hier an, z.B. 'cn=ldapuser,ou=public,o=org'		
Kennwort <small>enrol_ldap bind_pw</small>	<input type="password" value="....."/> 	
Kennwort für den Bind-User		

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.

Subkontexte <small>enrol_ldap course_search_sub</small>	<input type="button" value="Ja"/> <input type="button" value="Standard: Nein"/>	Gruppenzugehörigkeiten in Subkontexten suchen
Mitgliedsattribut ist dn <small>enrol_ldap memberattribute_isdn</small>	<input type="button" value="Ja"/> <input type="button" value="Standard: Nein"/>	Wenn die Gruppenzugehörigkeit bevorzugte Namen enthält, müssen Sie dies hier angeben und auch alle nachfolgenden Einstellungen dieses Abschnitts vornehmen.
Kontexte <small>enrol_ldap user_contexts</small>	<input type="text" value="cn=schueler,cn=groups,ou=schule,d"/> <input type="button" value="Standard: Leer"/>	Wenn die Gruppenzugehörigkeit bevorzugte Namen enthält, legen Sie die Kontexte fest, wo Nutzer gefunden werden sollen. Trennen Sie unterschiedliche Kontexte mit einem Semikolon ';' wie z.B. 'ou=users,o=org;ou=others,o=org'.
Subkontexte <small>enrol_ldap user_search_sub</small>	<input type="button" value="Ja"/> <input type="button" value="Standard: Nein"/>	Wenn die Gruppenzugehörigkeit bevorzugte Namen enthält, legen Sie die Nutzersuche in Subkontexten gesondert fest.
Nutzertyp <small>enrol_ldap user_type</small>	<input type="button" value="Standard"/> <input type="button" value="Standard: Standard"/>	Wenn die Gruppenzugehörigkeit bevorzugte Namen enthält, legen Sie fest, wie Nutzer/innen in LDAP gespeichert werden
Aliases auflösen <small>enrol_ldap opt_deref</small>	<input type="button" value="Nein"/> <input type="button" value="Standard: Nein"/>	Wenn die Gruppenzugehörigkeit bevorzugte Namen enthält, legen Sie fest, wie Aliase bei der Suche behandelt werden. Wählen Sie einen der folgenden Werte aus: 'Nein' (LDAP_DEREF_NEVER) oder 'Ja' (LDAP_DEREF_ALWAYS)
ID-Nummer <small>enrol_ldap idnumber_attribute</small>	<input type="text" value="uidnumber"/> <input type="button" value="Standard: Leer"/>	Wenn die Gruppenzugehörigkeit bevorzugte Namen enthält, geben Sie hier das gleiche Attribut ein, das Sie für die Zuordnung der 'ID-Nummer' in den Einstellungen zur LDAP-Authentifizierung angegeben haben.

Die ID-Nummer-Zuordnung zu

```
uidnumber
```

wird für die Eintragung der Teilnehmer in die Kurse benötigt.

Einstellungen für Kurse

Object Class <small>enrol_ldap objectclass</small>	<input type="text" value="(objectClass=posixGroup)"/>	Standard: Leer
objectClass für Kurssuche in LDAP, normalerweise 'group' oder 'posixGroup'		
ID-Nummer <small>enrol_ldap course_idnumber</small>	<input type="text" value="cn"/>	Standard: Leer
Bezeichner zur eindeutigen Identifizierung in LDAP, normalerweise cn oder uid. Es wird empfohlen, den Wert zu sperren, wenn Sie Kurse automatisiert anlegen wollen.		
Kurzer Kursname <small>enrol_ldap course_shortname</small>	<input type="text" value="cn"/>	Standard: Leer
Optional: LDAP-Feld für die Kurzbezeichnung des Kurses		
Vollständiger Name <small>enrol_ldap course_fullname</small>	<input type="text" value="cn"/>	Standard: Leer
Optional: LDAP-Feld für vollständigen Kursnamen		
Zusammenfassung <small>enrol_ldap course_summary</small>	<input type="text" value="description"/>	Standard: Leer
Optional: LDAP-Feld für die Beschreibung des Kurses		
Verborgene Kurse ignorieren <small>enrol_ldap ignorehiddencourses</small>	<input type="checkbox"/>	Standard: Nein
Wenn diese Option aktiviert ist, werden Nutzer/innen nicht in Kurse eingeschrieben, die für sie nicht freigegeben sind.		
Externer Abmeldevorgang <small>enrol_ldap unenrolaction</small>	<input type="text" value="Nutzer/in vom Kurs abmelden"/>	Standard: Nutzer/in vom Kurs abmelden
Wählen Sie, welche Aktion ausgeführt werden soll, wenn die Nutzereinschreibung aus der externen Einschreibquelle verschwindet. Beachten Sie bitte, dass bei der Kursabmeldung Nutzerdaten und -einstellungen gelöscht werden.		

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“.

Einstellungen für automatisch angelegte Kurse

Automatisches Erstellen <small>enrol_ldap autcreate</small>	<input type="text" value="Ja"/>	Standard: Nein
Kurse können automatisch in Moodle angelegt werden, wenn es in LDAP Anmeldungen zu einem Kurs gibt, der in Moodle noch nicht existiert.		
Wenn Sie die automatische Kurserstellung nutzen, wird empfohlen, die folgenden Fähigkeiten aus den relevanten Rollen zu entfernen: moodle/course:changeidnumb moodle/course:changeshortname, moodle/course:changefullname and moodle/course:changesummary.		
Kategorie <small>enrol_ldap category</small>	<input type="text" value="Klassen"/>	Standard: Verschiedenes
Kursbereich für automatisch angelegte Kurse		
Vorlage <small>enrol_ldap template</small>	<input type="text"/>	Standard: Leer
Optional: Automatisch angelegte Kurse können ihre Kurseinstellungen aus einer Kursvorlage kopieren. Tragen Sie hier die Kurzbezeichnung dieser Kursvorlage ein.		

Übernehmen Sie die restlichen Einstellungen wie im Bild.

Einstellungen für automatisch aktualisierte Kurse

Wählen Sie die Felder aus, die aktualisiert werden sollen, wenn die geplante Aufgabe "LDAP-Einschreibungen synchronisieren" ausgeführt wird.
Wenn mindestens ein Feld ausgewählt ist, erfolgt die Aktualisierung.

Kurzen Kursnamen aktualisieren <small>enrol_ldap course_shortname_updateasync</small>	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Standard: Nein
Kurzen Namen bei der Synchronisierung aktualisieren	
Vollständigen Kursnamen aktualisieren <small>enrol_ldap course_fullname_updateasync</small>	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Standard: Nein
Vollständigen Namen bei der Synchronisierung aktualisieren	
Beschreibung aktualisieren <small>enrol_ldap course_summary_updateasync</small>	<input type="checkbox"/> Ja <input checked="" type="checkbox"/> Standard: Nein
Zusammenfassung bei der Synchronisierung aktualisieren	

Einstellungen für enthaltene Gruppen

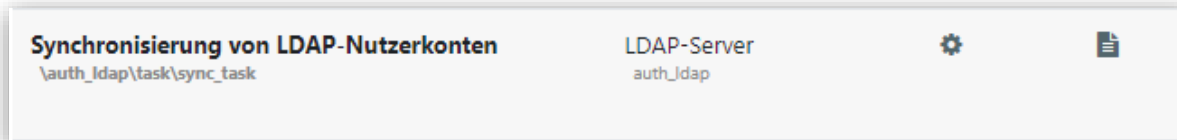
Enthaltene Gruppen <small>enrol_ldap nested_groups</small>	<input type="checkbox"/> Nein <input checked="" type="checkbox"/> Standard: Nein
Möchten Sie enthaltene Gruppen (Gruppen innerhalb von Gruppen) für die Einschreibung benutzen?	
Attribut 'Member of' <small>enrol_ldap group_memberofattribute</small>	<input type="text" value="memberof"/> Standard: Leer
Name des Attribut, das die Zugehörigkeit eines Nutzers zu einer Gruppe festlegt (z.B. memberOf, groupMembership, etc)	

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

4.3 Synchronisierung automatisieren

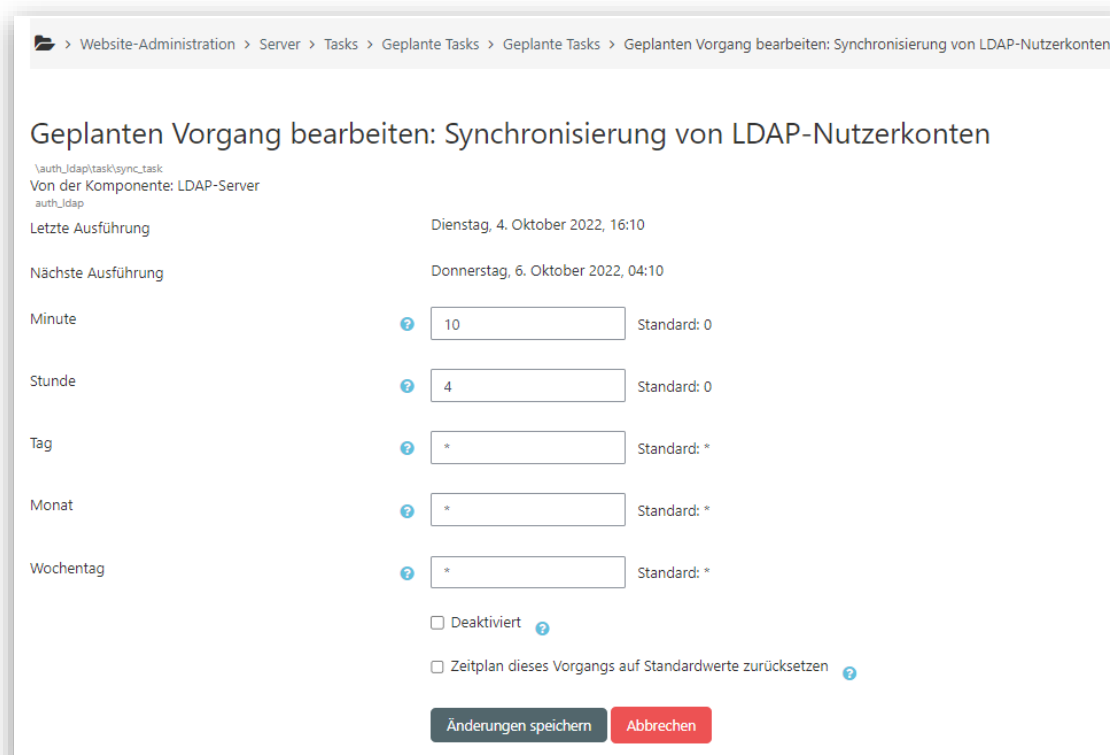
Damit Moodle die Schuldaten automatisch aktualisiert sollten Sie jeweils eine geplante Aufgabe (Cron-Job) für Authentifizierung und Einschreibung einstellen.

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.

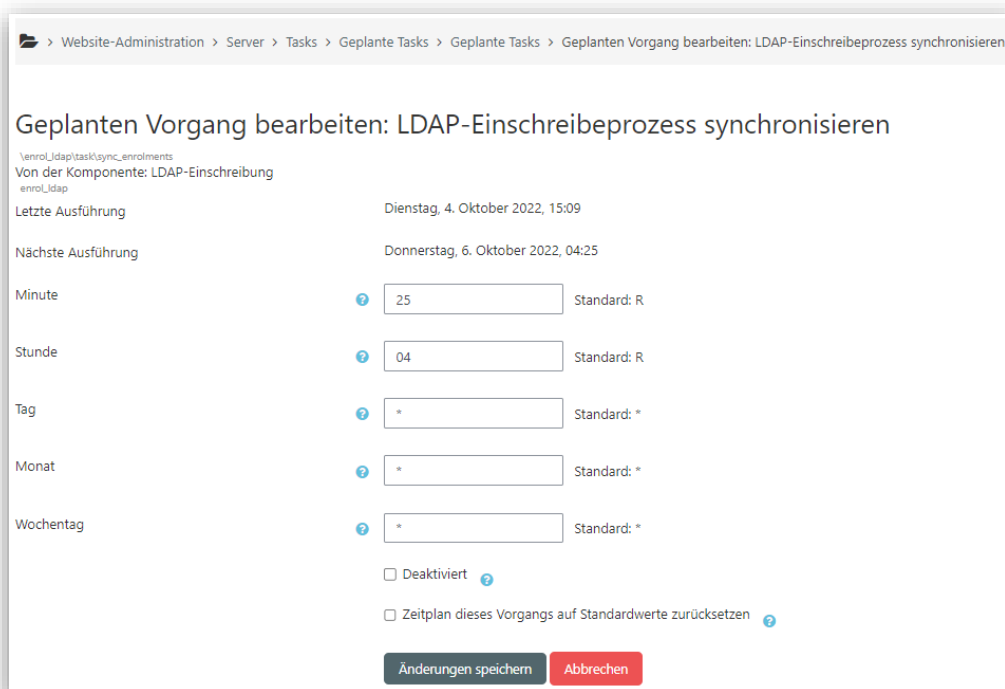


The screenshot shows the Moodle task configuration page. The breadcrumb trail is: Website-Administration > Server > Tasks > Geplante Tasks > Geplante Tasks > Geplanten Vorgang bearbeiten: Synchronisierung von LDAP-Nutzerkonten. The title is 'Geplanten Vorgang bearbeiten: Synchronisierung von LDAP-Nutzerkonten'. Below the title, the path '\auth_ldap\task\sync_task' and the component 'Von der Komponente: LDAP-Server' are shown. The task is currently active. The last execution was on 'Dienstag, 4. Oktober 2022, 16:10'. The next execution is on 'Donnerstag, 6. Oktober 2022, 04:10'. The configuration fields are: Minute (10, Standard: 0), Stunde (4, Standard: 0), Tag (*, Standard: *), Monat (*, Standard: *), and Wochentag (*, Standard: *). There are checkboxes for 'Deaktiviert' and 'Zeitplan dieses Vorgangs auf Standardwerte zurücksetzen'. At the bottom, there are buttons for 'Änderungen speichern' and 'Abbrechen'.

Analog bearbeiten Sie „LDAP-Einschreibeprozess synchronisieren“

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

Damit werden die Benutzerdaten jede Nacht abgeglichen.



The screenshot shows the Moodle task configuration interface. The breadcrumb trail is: Website-Administration > Server > Tasks > Geplante Tasks > Geplante Tasks > Geplanten Vorgang bearbeiten: LDAP-Einschreibeprozess synchronisieren. The title is 'Geplanten Vorgang bearbeiten: LDAP-Einschreibeprozess synchronisieren'. Below the title, it says 'Von der Komponente: LDAP-Einschreibung' and 'enrol_ldap'. The 'Letzte Ausführung' (Last execution) is 'Dienstag, 4. Oktober 2022, 15:09'. The 'Nächste Ausführung' (Next execution) is 'Donnerstag, 6. Oktober 2022, 04:25'. There are input fields for 'Minute' (25), 'Stunde' (04), 'Tag' (*), 'Monat' (*), and 'Wochentag' (*). Each field has a help icon and a 'Standard: R' or 'Standard: *' label. At the bottom, there are checkboxes for 'Deaktiviert' and 'Zeitplan dieses Vorgangs auf Standardwerte zurücksetzen'. There are two buttons: 'Änderungen speichern' (Save changes) and 'Abbrechen' (Cancel).

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

4.4 Profildfeld-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 profildfeld-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.

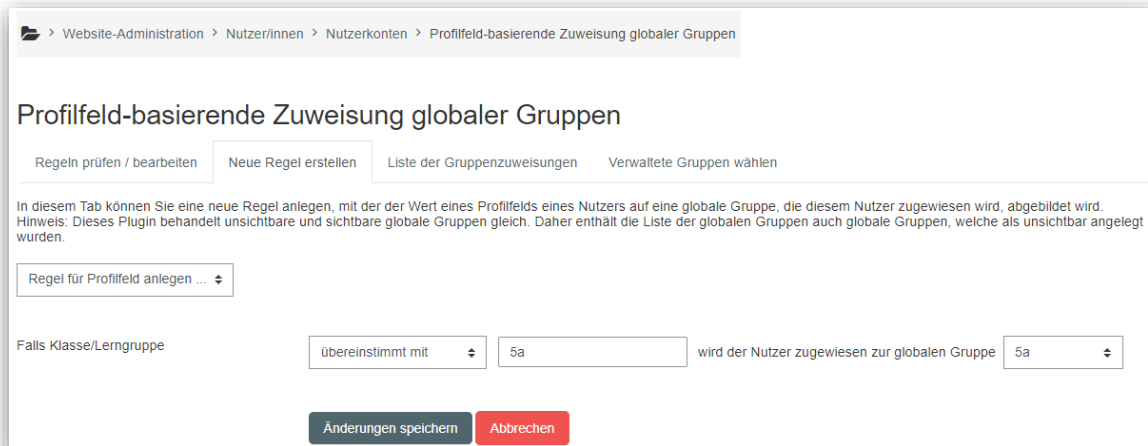
4.4.2 Benutzer zuweisen

Öffnen Sie Website-Administration -> Nutzer/innen -> Nutzerkonten -> Profildfeld-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.





The screenshot shows a web interface for managing global group assignments based on profile fields. The breadcrumb trail is: Website-Administration > Nutzer/innen > Nutzerkonten > Profilfeld-basierende Zuweisung globaler Gruppen. The main title is 'Profilfeld-basierende Zuweisung globaler Gruppen'. Below the title are four tabs: 'Regeln prüfen / bearbeiten' (active), 'Neue Regel erstellen', 'Liste der Gruppenzuweisungen', and 'Verwaltete Gruppen wählen'. A text block explains that in this tab, a new rule can be created, mapping a user's profile field value to a global group. A note states that the plugin treats invisible and visible global groups equally. Below this is a dropdown menu 'Regel für Profilfeld anlegen ...'. The main form has two sections: 'Falls Klasse/Lerngruppe' with a dropdown 'übereinstimmt mit' and a text input '5a', and 'wird der Nutzer zugewiesen zur globalen Gruppe' with a dropdown '5a'. At the bottom are two buttons: 'Änderungen speichern' and 'Abbrechen'.

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.

Synchronisierungsaufgabe der Einschreibung über Globale Gruppen lenrol_cohort/tasklenrol_cohort_sync	Globale Gruppe enrol_cohort			Dienstag, 20. Dezember 2022, 08:26	Dienstag, 20. Dezember 2022, 09:30	* / 15 Standard: R	*	*	*
--	--------------------------------	---	---	---	---	--------------------------	---	---	---

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.

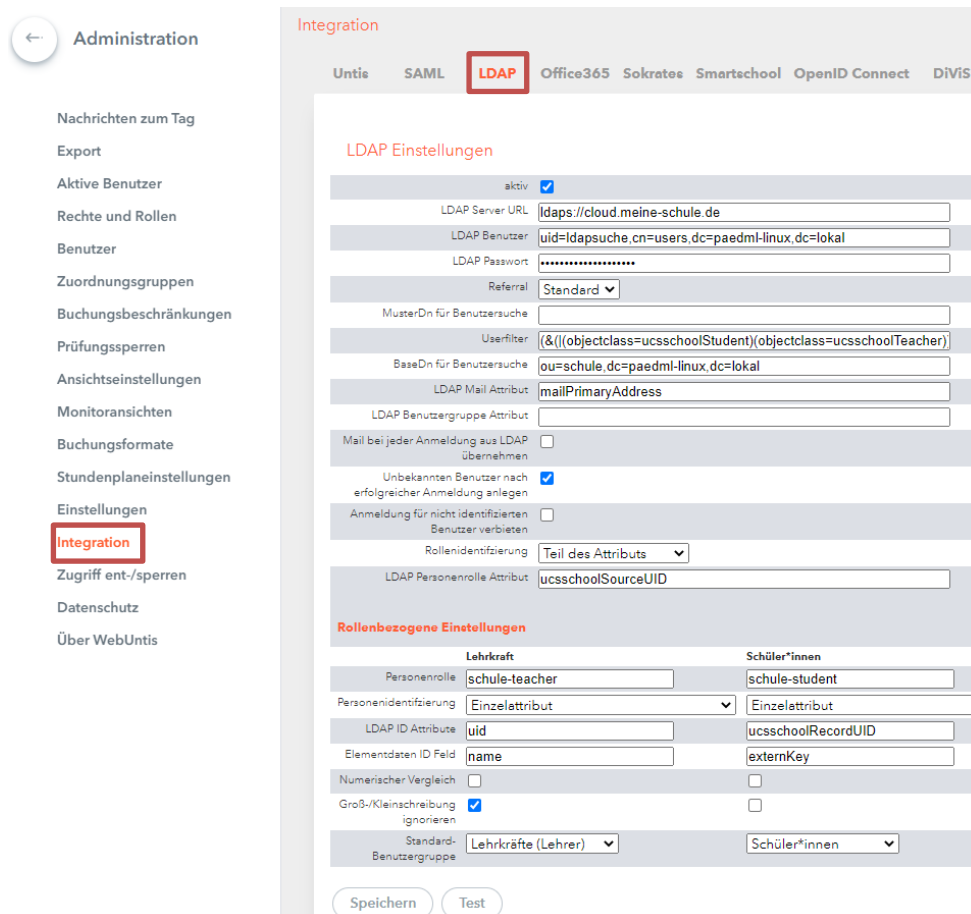
5.1 Konfiguration

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
Personenidentifizierung	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

© Landesmedienzentrum Baden-Württemberg, 2023