

LDAP Authentifizierung/Synchronisation für Moodle im IServ & Benutzerimport für globale Gruppen

Moodle ermöglicht die Authentifizierung per LDAP, also die Überprüfung der Zugangsdaten beim Login über die Schnittstelle. Bei jedem Login in Moodle wird also bei IServ angefragt, ob die Benutzerdaten korrekt sind. Außerdem kann man recht einfach sämtliche IServ-Gruppen in Moodle hochladen.

Inhaltsverzeichnis

Ziele:	1
LDAP	1
Schritte am Router (falls IServ nicht selbst für Internetverbindung sorgt).....	1
Schritte am IServ (lokal als root)	1
Einstellungen in Moodle.....	2
Authentifizierung:.....	2
Synchronisierung.....	4
Gruppenimport.....	4
Allgemeines zum Umgang mit globalen Gruppen.....	4
Benutzerimport, um IServ-Gruppen als Globale Gruppen zu übernehmen	4
Variante A (nach erfolgter Synchronisation, Benutzer bereits vorhanden).....	4
Variante B (ohne Synchronisation, Benutzer noch nicht angelegt – sehr umständlich).....	6
Schnelles Löschen von globalen Gruppen.....	7
Quellen:	7

Ziele:

- Authentifizierung in Moodle mit Benutzerzugangsdaten aus IServ
- Synchronisierung aller Benutzerkonten vor dem 1. Einloggen
- Möglichst automatisiertes Anlegen von globalen Gruppen, damit Lehrer beim Einrichten eines Moodle-Kurses alle Schüler auf einmal einschreiben können.
- Einschreibemethode *Globale Gruppe* datenschutzkonform verwendbar machen.
- Möglichst schnelles Löschen von globalen Gruppen (was nur einzeln von Hand geht)
- Synchronisation von festen Gruppen (z.B. Fachbereichs-, Jahrgangs- & Kollegiumsgruppen)

LDAP

Schritte am Router (falls IServ nicht selbst für Internetverbindung sorgt)

1. Portforwarding TCP/UDP für Port 10636 auf IServ einstellen.

Schritte am IServ (lokal als root)

1. Einloggen am Server
2. Zugriff auf Konfigurationsdatei (z.B. mit vim) `vi /etc/iserv/ldapusers`

Wichtige Befehle in vim:

Taste i: Einfügemodus (in unterster Zeile steht dann – EINFÜGEN --), Bedienung ist dann wie im Windows Texteditor

Taste ESC: zurück in den Befehlsmodus (Eingaben sind unten sichtbar)

Zeichen : Befehlsmodus (Cursor blinkt unten links): Eingabe von **W Q** und Bestätigung mit Eingabetaste zum Speichern & Beenden des Programms

VORSICHT: bei englischer Tastatur schreibt man den Doppelpunkt mit Shift + ö

3. Eintrag in Konfigurationsdatei hinter dem Hinweis # Please add additional user definitions after... nach Schema {username}:+{fieldName}:{client-ip-address}:
moodle:+userPassword:213.23.76.123

Der Benutzerzugang zum Verzeichnis lautet *moodle*. Der Lesezugriff auf den Passworthash und die Gruppenmitgliedschaften muss extra freigegeben werden. Nur von der IP-Adresse darf auf das Verzeichnis zugegriffen werden, sie stammt vom Server *moodle.nibis.de*.

4. Ausführen von *iconf save /etc/iserv/ldapusers* zur Einbindung der Änderungen
5. Ausführen von *iservchk ldap ferm* zur Übernahme der Änderungen ins System
6. Auslesen des Passworts mit *vim /var/lib/iserv/server-ldap/pwd/moodle.pwd*
7. Auslesen des BaseDN mit *vim /var/lib/iserv/server-ldap/ldapdn*
In unserem Fall lautet er *dc=igs-roderbruch,dc=org*
8. Zur Kontrolle Probeabfrage machen: *ldapsearch -o ldif-wrap=no -H ldap:/// -D "cn=moodle,ou=ldap,\$(cat /var/lib/iserv/server-ldap/ldapdn)" -y /var/lib/iserv/server-ldap/pwd/moodle.pwd -Y EXTERNAL -b "cn=Nutzername,ou=users,\$(cat/var/lib/iserv/server-ldap/ldapdn)"*

Nutzername sollte ein existierender IServ-Benutzername sein. Falls ein Fehler ausgegeben wird, sollte man *cn=Nutzername* durch *uid=Nutzername* ersetzen.

IServ hat im April 2019 eine Änderung in ihrer Datenbank vorgenommen, wo von uid zu cn gewechselt wurde (oder umgekehrt)

Einstellungen in Moodle

Authentifizierung:

1. In Moodle mit Adminaccount einloggen
2. Plugin für LDAP aktivieren: ->Website-Administration -> Plugins-> Authentifizierung dort in der Zeile vom Namen LDAP-Server unter der Spalte Aktivieren durch Klick auf das durchgestrichene, graue Auge. Sobald es blau ist, ist es aktiviert.
3. In der Zeile LDAP-Server auf Einstellungen klicken.
4. Einstellungen sind überwiegend Standardwerte. Solche, die nicht der Standardwert habe ich hier unten mit Bemerkungen dazu aufgeführt:

LDAP-Server-Einstellungen

- a. Host URL: *ldaps://igs-roderbruch.org:10636/* <- es muss ldaps sein, da IServ den Zugriff nur über SSL zulässt (s. Iserv-Doku)

Bind-Einstellungen:

- b. Kennwort-Caching verhindern: *Ja* <- aus Datenschutzgründen besser keine Kennwörter außerhalb vom IServ speichern. Es wird also bei jedem Login mit dem Passwort im IServ kontrolliert.
- c. Anmeldename: *cn=moodle,ou=ldap,dc=igs-roderbruch,dc=org*
- d. Kennwort: ist 64-stellig, wurde ausgelesen s.o.

Nutzersuche (user lookup)

- e. Nutzertyp: *posixAccount (rfc2307)*

- f. Kontexte: *ou=users,dc=igs-roderbruch, dc=org* <- IServ speichert alle Accounts in der ou Users
- g. Nutzermerkmal: *uid* (s. IServ-Doku)
- h. Mitgliedsmerkmal: *memberuid* (s. IServ-Doku)
- i. ObjectClass: *uuidObject* <- damit erkennt man Personenaccounts. Sonst werden Klassenaccounts in Moodle übernommen

Synchronisierung von Nutzerkonten

- j. Entfernte externe Nutzer: *Intern sperren* <- so wird Nutzern parallel zum IServ der Zugriff entzogen, es bleiben aber notenrelevante Daten erhalten, falls ein Schüler die Schule verlässt. Löschung zum erforderlichen Zeitpunkt muss koordiniert werden.

Datenzuordnung (s. IServ-Doku)

- k. Daten übernehmen (Vorname): *givenName*
 - l. Lokal aktualisieren (Vorname): *Bei jedem Login*
 - m. Feld sperren (Vorname): *Gesperrt*
 - n. Daten übernehmen (Nachname): *sn*
 - o. Lokal aktualisieren (Nachname): *Bei jedem Login*
 - p. Feld sperren (Nachname): *Gesperrt*
 - q. Daten übernehmen (E-Mail-Adresse): *mail*
 - r. Lokal aktualisieren (E-Mail-Adresse): *Beim Anlegen*
 - s. Feld sperren (E-Mail-Adresse): *Bearbeitbar*
 - t. Daten übernehmen (ID-Nummer): *uidNumber* <- Das Feld ist für die LDAP-Kurseinschreibung notwendig und bei Offline-Tests hilfreich
 - u. Lokal aktualisieren (ID-Nummer): *Bei jedem Login*
 - v. Feld sperren (ID-Nummer): *Gesperrt*
5. Button Änderungen sichern klicken.
 6. Einstellungen testen: oben auf Authentifizierung klicken, um zur Seite mit Pluginübersicht für Authentifizierung zu kommen. Anschließend in der Zeile von LDAP-Server auf *Einstellungen prüfen* klicken.

Falls folgender Fehler angezeigt wird, wurde der LDAP-Server vermutlich nicht erreicht (z.B. wegen falscher Adresse, fehlender Portweiterleitung o.ä.).

LDAP paged results werden nicht unterstützt. Entweder unterstützt Ihre PHP Version dies nicht oder Sie haben Moodle zur Verwendung der LDAP-Protokollversion 2 konfiguriert oder Moodle kann bei Ihren LDAP-Server den paged Support nicht erkennen. ✕

- Auf der Seite zur Pluginübersicht dafür sorgen, das LDAP-Server direkt in der 3. Zeile steht (durch Deaktivieren anderer Plugins oder Klicken auf die blauen Pfeile, s. Bild)

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Einstellungen prüfen
Manuelle Konten	5			Einstellungen	
Kein Login	0				
LDAP-Server	178			Einstellungen	Einstellungen prüfen
E-Mail basiert	0			Einstellungen	

- Login mit IServ-Account testen, ggf. Rollen (für Lehrer) überprüfen.

Synchronisierung

- In der Website-Administration unter Server->Geplante Vorgänge den Punkt *Synchronisierung von LDAP Nutzerkonten* durch Klicken auf das Zahnrad bearbeiten.
- Einstellungen für die Zeit nutzen (z.B. Stunde 5, Minute 0, sonst *, damit täglich um 5:00 synchronisiert wird) und Haken bei Deaktiviert entfernen. Dann Änderungen speichern. Die Ausführung erfolgt (auf unseren NiBiS-Instanzen) scheinbar immer nur nachts, egal ob wir andere Zeiten angeben.
- Falls** alle Lehrer eine Systemweite Rolle erhalten sollen: In der Website-Administration unter Server->Geplante Vorgänge den Punkt Systemrollen aus LDAP synchronisieren durch Klicken auf das Zahnrad bearbeiten. Einstellungen wie bei Punkt 2, wobei eine andere Minutenzeit gewählt werden sollte.

Gruppenimport

Allgemeines zum Umgang mit globalen Gruppen

Globale Gruppen in Moodle sind nicht auf den Schulbetrieb ausgelegt und unbequem, zu verändern oder bereinigen. Mitglieder können zwar per CSV hinzugefügt, aber nicht entfernt werden. Im Gegensatz zu den IServ-Gruppen lassen sich globale Gruppen in Moodle auch nicht fortschreiben, also von einer Klasse 09-6 automatisiert in die Klasse 10-6 überführen. Daher empfehle ich, die globalen Gruppen in Moodle für ein Schuljahr anzulegen und dies im Namen kenntlich zu machen. Für die IServ-Gruppe Klasse-09-6 sollte die globale Gruppe 19/20-Klasse-09-6 für das Schuljahr 19/20 angelegt werden. So kann man die Einschreibemethode *Globale Gruppe* verwenden und Benutzer in Kursen bequem ein- und ausschreiben, z.B. wenn die Löschrufen dies erfordern.

Benutzerimport, um IServ-Gruppen als Globale Gruppen zu übernehmen

Variante A (nach erfolgter Synchronisation, Benutzer bereits vorhanden)

Dadurch, dass alle IServ-Benutzer bereits vorhanden sind, müssen Nutzer nur aktualisiert werden. Moodle benötigt ein eindeutiges Feld zur Zuordnung der Nutzer und kann sonst beliebige Felder bekommen. Wir nutzen cohort1 bis cohort30, wobei manchmal auch mehr Spalten nötig sein können. Leere Einträge werden einfach ignoriert, also sollte man eher zu viele Spalten anlegen.

Man benötigt das [Gruppenlisten-Modul für IServ 3](#), einen brauchbaren Texteditor, z.B. [Notepad++](#) (npp) und ggf. Excel/Calc/Numbers. Es ist sehr hilfreich, wenn es eine IServ-Gruppe *Schüler* und *Lehrer* oder *Kollegium* gibt.

Das Gruppenlistenmodul kann ein Feld *Alle Gruppen* ausgeben, wo alle Gruppen eines Nutzers aufgelistet sind. Außerdem kann man nur Schüler aus den Gruppen ausgeben lassen, damit man keine Lehrkräfte hinterher aus den Gruppen sortieren muss. Man importiert Schüler in Lehrer einzeln in Moodle, erstellt also zwei csv-Dateien. Die Dateien haben folgende Struktur:

```
username;cohort1;cohort2;cohort3;cohort4...
z-test.lehrer;Kollegium;Klasse-09-6;;...
```

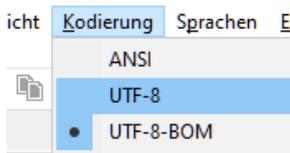
Bei mir deutlich gewordene Stolpersteine auf dem Weg habe ich unter Fehlerbehandlung aufgeführt.

Schülergruppenimport

1. Im Modul Gruppenlisten wählt man die Gruppe *Schüler*, und bei Auswahl *Account*, *Alle Gruppen* und *Nur Schüler zeigen*. Über den Button *Exportieren* erhält man eine csv-Datei.



2. Öffne die csv-Datei in npp. Die Kodierung der Exportdatei ist



standardmäßig UTF-8 BOM, was in Moodle zu Problemen mit Umlauten führt. Daher muss sie unter dem Menüpunkt Kodierung auf UTF8 geändert werden.

Auswahl *

Nachname

Vorname

Account

Status

Klasse/Information

Import-ID

Alle Gruppen

Alle Gruppen mit Gru

Nur Schüler zeigen

3. Die Gruppen liegen derzeit noch alle in einem Feld. Drücke STRG+H. Suche nach , und lasse es durch ; ersetzen. Mit ALT+T wird alles auf einmal erledigt. So wird aus einem Feld, in dem alle Gruppen stehen ein Feld pro Gruppe, wenn wir die Datei nach dem Speichern in Excel öffnen.

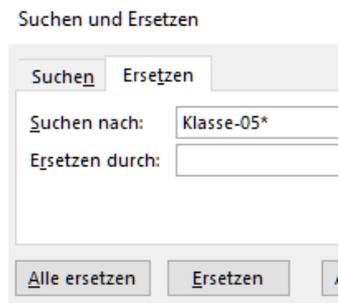
4. Die Kopfzeilen müssen angepasst werden, was in Excel schnell geht:

- a. Account -> username
- b. cohort1 mit dem Ausfüllkästchen ausreichend nach rechts ziehen, um ausreichend Datenfelder zu haben. Lege lieber 50 zu viel als eins zu wenig an.

5. Bei Bedarf: Besondere Anpassungen:

Hier hat man im Normalfall alles vorbereitet und kann zum nächsten Schritt springen.

- a. **Gruppen vom Import ausschließen:** Falls bestimmte Gruppen nicht in Moodle importiert werden sollen, kann man in Excel (STRG+H) danach suchen und sie durch nichts ersetzen. Bei Einträgen mit Laufnummern o.ä., kann man * als Platzhalter nutzen. Im Bild Rechts werden alle Gruppen der Klassenstufe 5, wenn man ALT+A drückt.
- b. **Gruppenpräfixe ergänzen:** Falls Präfixe gewünscht sind, nach entsprechendem Textteil suchen (ohne *) und durch. Falls man z.B. das Schuljahr für alle Klassen als Präfix führen möchte, sucht man nach Klasse- und ersetzt durch 19/20-Klasse- .



6. In Moodle mit Manager- oder Administratoraccount einloggen.

7. Zum Nutzerimport navigieren: ->Website-Administration-> Nutzer/innen->Nutzerliste hochladen

8. Datei auswählen: *Datei wählen* -> *Durchsuchen* -> csv-Datei auswählen, auf Button *Öffnen* klicken -> Button *Datei hochladen* klicken.

9. Auf Button *Nutzerliste hochladen* klicken

10. Prüfen, ob Datei korrekt erkannt und Namen in den passenden Feldern sind.

11. Einstellungen -> Upload Typ auf *Nur vorhandene aktualisieren* einstellen.

12. Jetzt ist die letzte Chance, Dateieinträge an Beispielen zu prüfen. Es werden nur Zeilen mit Änderungen angezeigt (z.B. bei Sonderzeichen, Präfixen usw.). Danach durch Klick auf den Button *Nutzerliste hochladen* Änderungen in Moodle übernehmen.

Kollegiumsgruppenimport

Hierbei sind die Bedarfe vermutlich sehr unterschiedlich. Im Prinzip funktioniert es wie für Schüler. Die zwei wichtigen Unterschiede sind hier unter dem entsprechenden Punkt notiert.

1. Die Gruppe *Kollegium* oder *Lehrer* wird gewählt und kein Haken bei *Nur Schüler zeigen*.
5. Hier ist es vermutlich notwendig, sämtliche Klassen- und Kursgruppen zu entfernen. Lehrer sollten nicht in globalen Gruppen von Moodle vorhanden sein.

Fehlerbehandlung:

Beim IServ-Gruppenlisten-Export:

- Keine Gruppen im Modul sichtbar: Unter Verwaltung->Gruppen-> Gruppenmerkmale beim Punkt *Gruppenlisten* anpassen.

Beim Moodle-Import:

- „Unbekannte Feldbezeichnung „“““ bedeutet, dass zu wenig Spalten den Titel cohort mit Laufnummer tragen. Einfach ein paar mehr anlegen.
- „Unbekannte Feldbezeichnung ?username“: Excel ergänzt manchmal beim Speichern als csv ein ? zu Beginn der Datei. In npp kann man das schnell entfernen.

Variante B (ohne Synchronisation, Benutzer noch nicht angelegt – sehr umständlich)

Der Import erfolgt über eine csv-Datei. Benötigt werden die Felder *username*, *firstname*, *lastname*, *email*, *auth*, *cohort1* bis *cohort5* oder mehr. Wir verwenden der Einfachheit wegen Spalten bis *cohort29*, wobei die meisten davon leer bleiben. So ist es in der Datenbank zur Aufbereitung der Datei einfacher umzusetzen. Moodle ist beim Import recht flexibel und lässt über die erste Zeile der csv-Datei festlegen, welche Felder importiert werden.

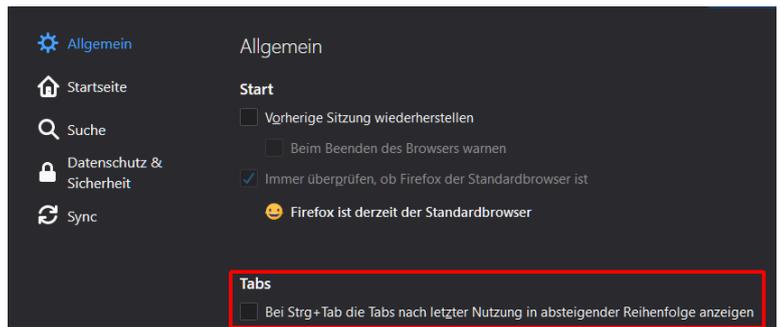
Beim Import müssen neben den verpflichtenden Angaben zu Name und Email auch eingestellt werden, mit welchem Plugin der importierte Nutzer angemeldet werden soll. Dafür muss in der Spalte *auth* immer und **kleingeschrieben** *ldap* stehen. Für jede globale Gruppe benötigt man eine Spalte *cohort1*, *cohort2*, o.ä. Die Datei könnte z.B. so aussehen:

```
username;firstname;last-  
name;email;auth;cohort1;cohort2;cohort3  
z-test.lehrer;Z-test;Lehrer;z-test.lehrer@igs-ro-  
derbruch.org;ldap;Kollegium;Klasse-09-6;1920-Kurs-  
09WPK2-IN-Grw  
z-test.schueler;Z-Test;Schüler;z-test.schueler@igs-ro-  
derbruch.org;ldap;Schüler;1920-Klasse-09-6;
```

13. csv-Datei mit gewünschten Daten vorbereiten (am besten aus Excel o.ä. als csv abspeichern).
14. In Moodle mit Account in Managerrolle einloggen.
15. Zum Nutzerimport navigieren: ->Website-Administration-> Nutzer/innen->Nutzerliste hochladen
16. Datei auswählen: *Datei wählen* -> *Durchsuchen* -> csv-Datei auswählen, auf Button *Öffnen* klicken -> Button *Datei hochladen* klicken.
17. CSV Trennzeichen, Encoding passend einstellen, auf Button *Nutzerliste hochladen* klicken
18. Prüfen, ob Datei korrekt erkannt und Namen in den passenden Feldern sind.
19. Einstellungen -> Upload Typ auf *Neue hinzufügen*, *vorhandene aktualisieren* einstellen.
20. Button *Nutzerliste hochladen* klicken.
21. Ergebnisse prüfen

Schnelles Löschen von globalen Gruppen

Wenn man aufräumen muss, zum Schuljahreswechsel o.ä. Man sollte das nicht am Tablet machen. Eine wichtige Voraussetzung ist die Einstellung im Browser, mit STRG+TAB den nächsten Tab recht aufzurufen. Meistens ist das die Standardeinstellung. Die Alternative kann man in der Regel deaktivieren (s. Bild).



1. Neues Browserfenster öffnen & zur Seite mit globalen Gruppen navigieren. Ggf. die angezeigten Gruppen durch Suchen (z.B. nach 1920) einschränken.
2. Mit *STRG+klicken* auf alle Löschbuttons nacheinander drücken, damit die Bestätigungsseite zum Löschen in einem neuen Tab geöffnet wird. Das kann man ruhig mit 60 Gruppen machen, bevor man zum nächsten Schritt übergeht.
3. Mit STRG+TAB durch die Tabs wechseln und mit der Maus auf den Weiter-Button. Man bekommt so einige Löschungen pro Sekunde hin, weil man immer die Routine STRG+TAB und Mausklick abwechselt, ohne etwas sehen zu müssen.
4. Nach einem Satz Löschungen von 20/40/60 den Arbeitsspeicher etwas entlasten, indem man einen Tab zu einem neuen Fenster verschiebt und das Fenster mit allen anderen Tabs schließt.
5. Übersichtsseite zu globalen Gruppen aktualisieren, um sich den aktuellen Stand der vorhandenen Gruppen anzeigen zu lassen und nicht bereits gelöschte Gruppen zu löschen versuchen. Danach von vorne beginnen.

Quellen:

Grundsätzliche Info zu LDAP: <http://www.selfadsi.de> und <http://www.effinger.org/blog/wp-content/uploads/2008/12/ldap-grundlagen.pdf>

IServ-Doku zur LDAP-Anbindung: <https://iserv.eu/doc//v3/advanced/openldap/#zugangsdaten-fur-die-nutzung-des-ldap-servers>

vim Befehlsreferenz: <http://tnerual.eriogerg.free.fr/vimqrc-ge.html>

Moodle-Doku zu LDAP-Anbindung: https://docs.moodle.org/37/en/LDAP_authentication

Moodle-Doku zu Nutzerlisten/globalen Gruppen: https://docs.moodle.org/37/de/Nutzerliste_hochladen