

LDAP-Authentifizierung in Moodle

I

Stand: 19.02.2013



zkn

Zentrale Konzeptionsgruppe Netze

Impressum

Herausgeber

Zentrale Konzeptionsgruppe Netze (ZKN)
an der Landesakademie für Fortbildung und Personalentwicklung an Schulen

Autoren

Johannes Kühn

Endredaktion

Adrian Koch

Weitere Informationen

<http://www.lehrerfortbildung-bw.de/netz/>

Veröffentlicht: 2013

Lizenz: CC-BY-NC-SA



Inhaltsverzeichnis

1.	LDAP-Authentifizierung in Moodle.....	4
1.1.	Einführung.....	4
1.2.	LDAP-Authentifizierung konfigurieren.....	5
1.2.1.	Portfreischaltung.....	5
1.2.2.	LDAP-Benutzer einrichten.....	5
1.2.3.	Konfigurieren des LDAP-Servers in Moodle.....	7
1.2.4.	Erstellen einer ISA-Zulassungsregel für das LDAP-Protokoll.....	10
1.2.5.	Aktivierung der LDAP-Authentifizierung in Moodle.....	15
1.2.6.	Umstellung vorhandener Benutzer auf LDAP-Authentifizierung.....	16
1.3.	Ergänzende Hinweise:.....	16

1. LDAP-Authentifizierung in Moodle

1.1. Einführung

Es gibt für Moodle verschiedene Authentifizierungsverfahren, die sich im Aufwand für den Betreuer, der Sicherheit für das Moodlesystem und dem Komfort für die Benutzer unterscheiden.

Das LDAP-Authentifizierungsverfahren vereint alle Vorteile. Es ist

- von überschaubarem Betreuungsaufwand, da sich alle Nutzer des pädagogischen Netzes automatisch auch in Moodle anmelden können. Auch die Rechtevergabe für Lehrer (dürfen in Moodle Kurse erstellen) und Schüler (dürfen dies nicht) erfolgt automatisch
- sicher, da sich ausschließlich Nutzer des pädagogischen Netzes in Moodle anmelden können und keine Schulfremden
- komfortabel, da sich die Nutzer mit nur einer Benutzerkennung sowohl im pädagogischen Netz als auch in Moodle anmelden können. Kennwortänderungen erfolgen im pädagogischen Netz und wirken sich sofort auf Moodle aus.

Um Moodle nutzen zu können, ist es allerdings notwendig, dass der paedML-Server zur Verfügung steht.

Der Moodleadministrator kann sich allerdings immer anmelden.

Hinweise:

- Die vorliegenden Dokumentation basiert auf einer Kurzanleitung auf www.ml-tipp-s.de. Der Autor des dortigen Textes ist Helge Hauptfleisch.
- Diese Anleitung bezieht sich auf die 1-Server-Lösung der paedML-Windows. Bei den Mehrserverlösungen müssen gegebenenfalls in den ISA-Zugriffsregeln andere Einstellungen vorgenommen werden.

1.2. LDAP-Authentifizierung konfigurieren

Das Einrichten des LDAP-Authentifizierungsverfahrens erfolgt in sechs Schritten:

1. Freischaltung des Ports 389 TCP für das LDAP-Protokoll
2. Anlegen eines Benutzers ldapuser auf dem Musterlösungsserver
3. Einrichten des LDAP-Servers in Moodle
4. Erstellen einer ISA-Zulassungsregel für das LDAP-Protokoll
5. Aktivieren der LDAP-Authentifizierung in Moodle
6. Umstellen der bisherigen Benutzer in Moodle auf das LDAP-Authentifizierungsverfahren

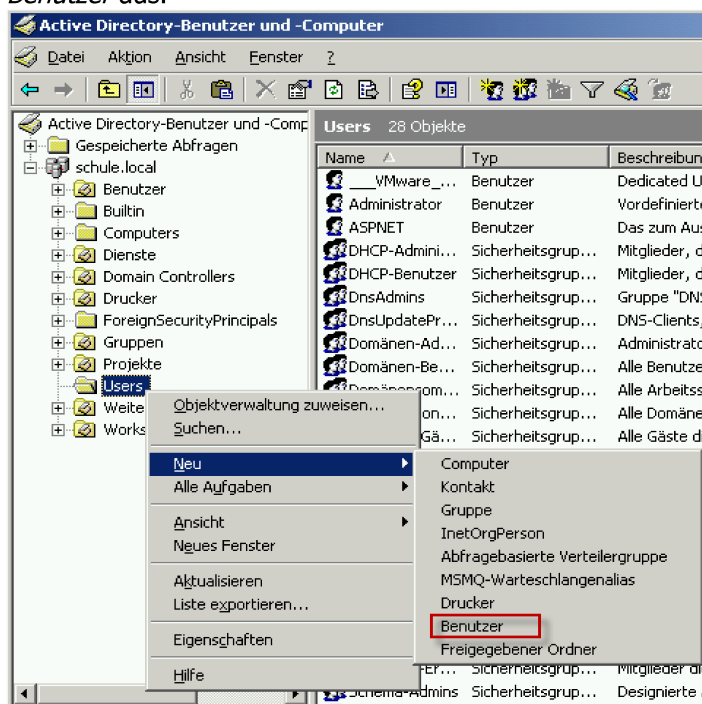
1.2.1. Portfreischaltung

Für den Zugriff über LDAP muss am Router der Port 389 TCP freigeschaltet werden. Haben Sie einen Router von BelWü, müssen Sie die Portfreischaltung dort beantragen (anschluss@belwue.de) oder am Router selbst durchführen.

1.2.2. LDAP-Benutzer einrichten

In der LDAP-Konfiguration wird ein Domänenbenutzer benötigt. Es ist sinnvoll, dafür einen eigenen Benutzer anzulegen.

1. Starten Sie die „Active Directory-Benutzer und -Computer“-Verwaltungskonzole.
2. Klicken Sie mit der rechten Maustaste auf die OU „Users“ und wählen Sie *Neu / Benutzer* aus.



3. Geben Sie im Feld „Nachname“ und bei „Benutzeranmeldename“ den Namen „ldapuser“ ein (selbstverständlich ist auch jeder andere Name möglich). Klicken Sie

dann auf *Weiter*

Neues Objekt - Benutzer

Erstellen in: schule.local/Users

Vorname: Initialen:

Nachname:

Vollständiger Name:

Benutzeranmeldename:

Benutzeranmeldename (Prä-Windows 2000):

< Zurück **Weiter >** Abbrechen

- Aktivieren Sie die beiden Optionen „Benutzer kann Kennwort nicht ändern“ und „Kennwort läuft nie ab“ und klicken Sie auf *Weiter*.

Neues Objekt - Benutzer

Erstellen in: schule.local/Users

Kennwort:

Kennwort bestätigen:

☐ Benutzer muss Kennwort bei der nächsten Anmeldung ändern

☒ Benutzer kann Kennwort nicht ändern

☒ Kennwort läuft nie ab

☐ Konto ist deaktiviert

< Zurück **Weiter >** Abbrechen

- Ein Exchange Postfach benötigen wir nicht. Deaktivieren Sie die Option „Exchange-Postfach erstellen“ und klicken Sie auf *Weiter*.

Neues Objekt - Benutzer

Erstellen in: schule.local/Users

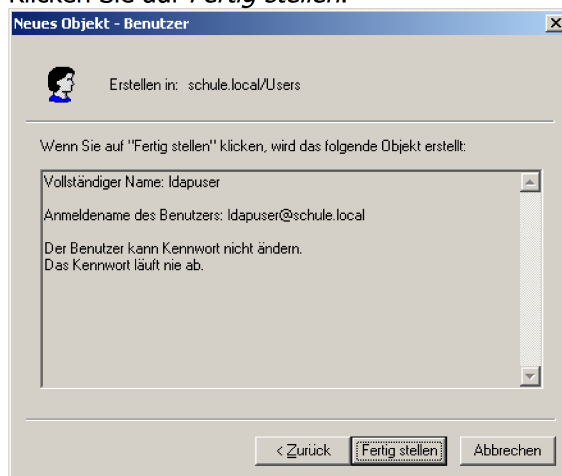
☐ Exchange-Postfach erstellen

Alias:

Server:

Postfachspeicher:

< Zurück **Weiter >** Abbrechen

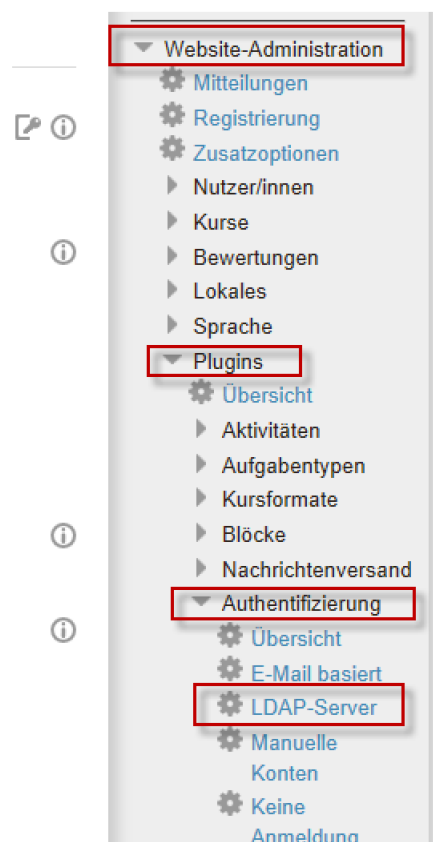
6. Klicken Sie auf *Fertig stellen*.

1.2.3. Konfigurieren des LDAP-Servers in Moodle

Zur Konfiguration des LDAP-Servers in Moodle müssen Sie als Administrator angemeldet sein. Die folgende Beschreibung orientiert sich an Moodle 2.x, ist aber auch in der älteren 1.9X anwendbar.



Linkes Bild: Menüpfad Moodle 1.9X



Rechtes Bild: Menüpfad Moodle 2.4X

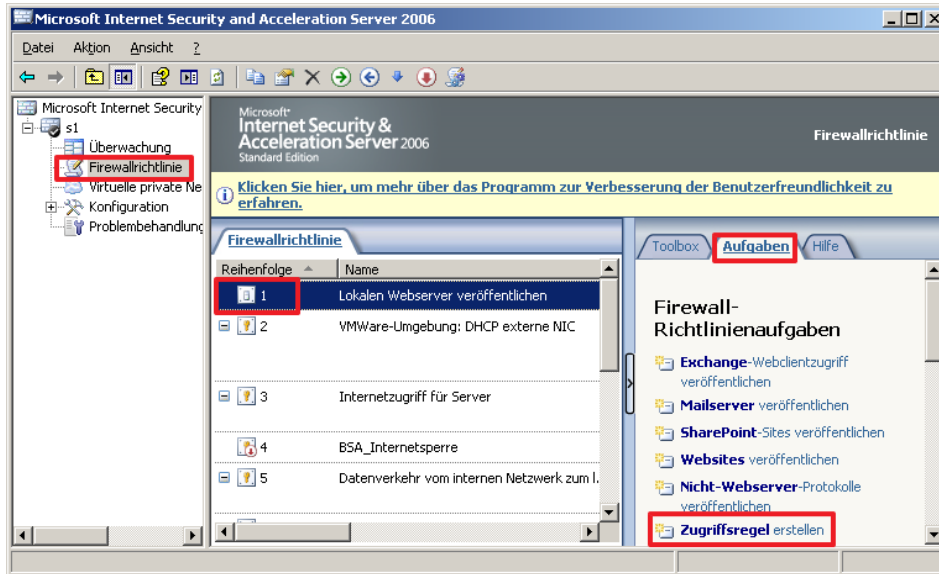
LDAP Servereinstellungen	
Host URL	<IP>:389 oder ldap://<IP>:389 (IP ist die externe IP-Adresse des Musterlösungsservers oder der DYNDNS-Eintrag)
Version	3
LDAP Codierung	utf-8
Einträge pro Seite	
Bind-Einstellungen	
Kennwörter verbergen	nein
Anmeldename	cn=ldapuser,cn=users,dc=schule,dc=local (alles ohne Leerzeichen!)
Kennwort	(Kennwort des ldapusers)
Nutzersuche (user lookup)	
Nutzertyp	MS ActiveDirectory
Kontexte	ou=Benutzer,dc=schule,dc=local
Subkontexte	ja
Alias berücksichtigen	Nein
Nutzermerkmal	sAMAccountName
Mitgliedsmerkmal	member
Mitgliedsmerkmal nutzt dn	(leer)
ObjectClass	objectClass=*
Kennwortänderung verlangen	
Kennwortänderung verlangen	nein
Standardseite zur Kennwortänderung nutzen	nein
Kennwortformat	Reiner Text
URL zur Kennwortänderung	(leer)
Gültigkeitsablauf von Kennwörtern	
Gültigkeitsende	no
Warnung zum Gültigkeitsende	10

Merkmal für Gültigkeitsende	(<i>leer</i>)
GraceLogins	nein
Merkmal für GraceLogin	(<i>leer</i>)
Nutzereinstellung aktivieren	
Nutzer extern anlegen	nein
Kontext für neue Nutzer	(<i>leer</i>)
Kursersteller/in	
Kursverwalter/innen	cn=G_Lehrer_Gymnasium,ou=Gymnasium,ou=Lehrer,ou=Gruppen,dc=schule,dc=local (<i>oder eben eine andere Gruppe, die Kurserstellerrechte erhalten soll</i>)
Cron-Synchronisierungsskript	
Entfernte externe Nutzer	nur intern zugänglich
NTLM SS	
Aktivieren	nein
Subnet	(<i>leer</i>)
MS IE fast path?	nein
Authentifikationsart	NTLM
Entfernter Nutzerdaten format	(<i>leer</i>)
Datenzuordnung	
Vorname	givenName
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	bearbeitbar (<i>Hinweis: hier kann man auch "Gesperrt" angeben, dann können die Nutzer ihren Namen im Profil nicht ändern, was durchaus Sinn machen kann</i>)
Nachname	sn
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	bearbeitbar (<i>Hinweis siehe Vorname</i>)
ID-Nummer	distinguishedName (<i>kann man auch leer lassen, braucht man nur, wenn man AD-Gruppen automatisch Kursen zuweisen möchte</i>)

Alle nachfolgenden Einstellungen bleiben unverändert bzw. leer. Danach bitte *Änderungen speichern* klicken.

1.2.4. Erstellen einer ISA-Zulassungsregel für das LDAP-Protokoll

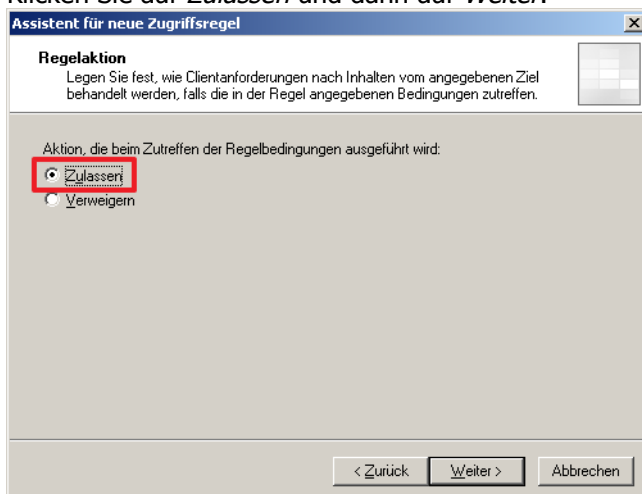
1. Starten Sie die „ISA-Server“-Verwaltungskonsole.
2. Klicken Sie auf *Firewallrichtlinie* und dann auf den ersten Punkt in der Liste mit den Firewallrichtlinien. Klicken Sie dann auf *Aufgaben* und dann auf *Zugriffsregel erstellen*.



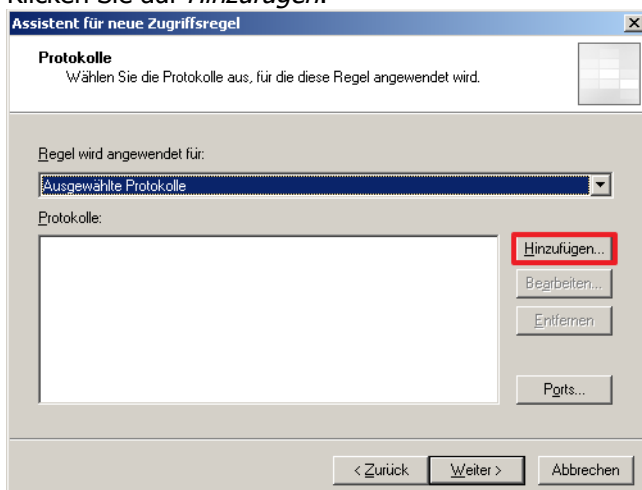
3. Geben Sie als Namen für die Zugriffsrichtlinie *LDAP-Moodle* ein und klicken Sie auf *Weiter*.



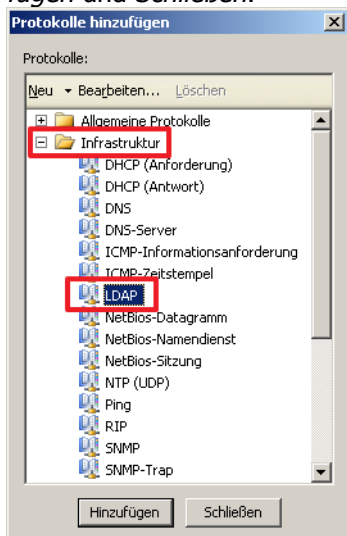
4. Klicken Sie auf *Zulassen* und dann auf *Weiter*.



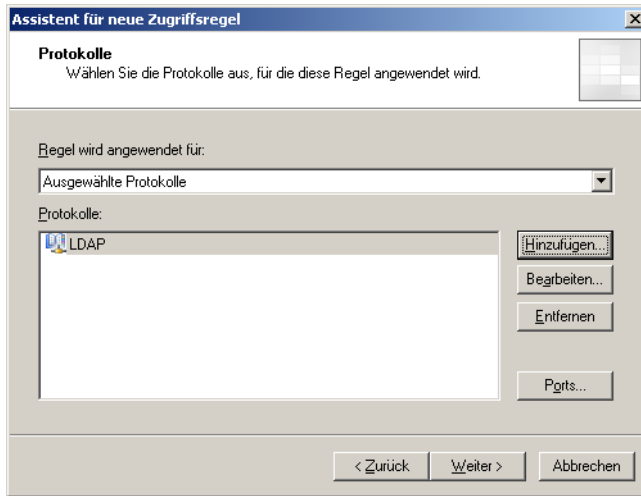
5. Klicken Sie auf *Hinzufügen*.



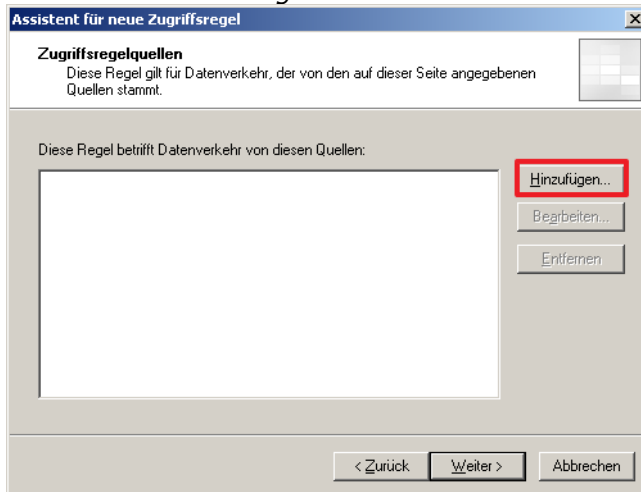
6. Wählen Sie unter *Infrastruktur* das Protokoll *LDAP* aus und klicken Sie auf *Hinzufügen* und *Schließen*.



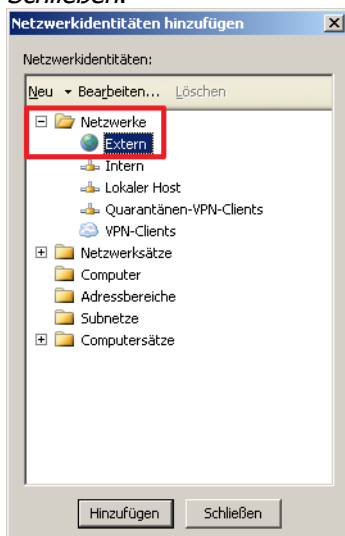
7. Klicken Sie auf *Weiter*.



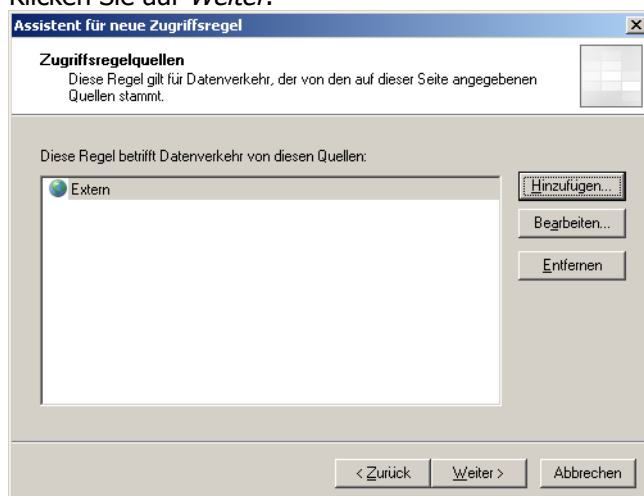
8. Klicken Sie auf *Hinzufügen*.



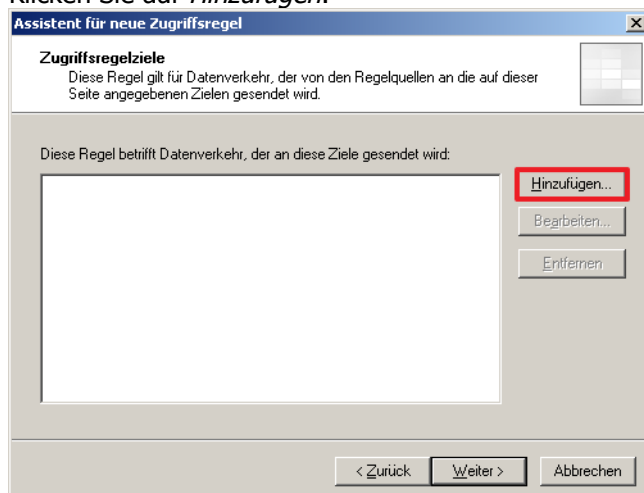
9. Wählen Sie unter *Netzwerke* *Extern* aus und klicken Sie auf *Hinzufügen* und *Schließen*.



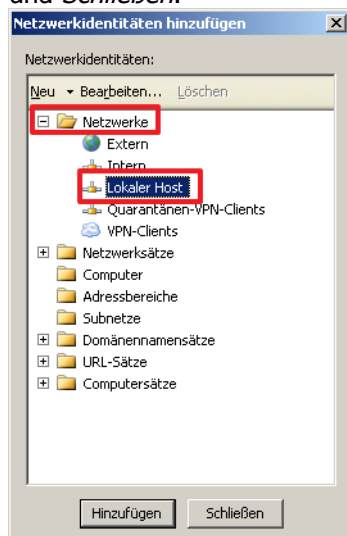
10. Klicken Sie auf *Weiter*.



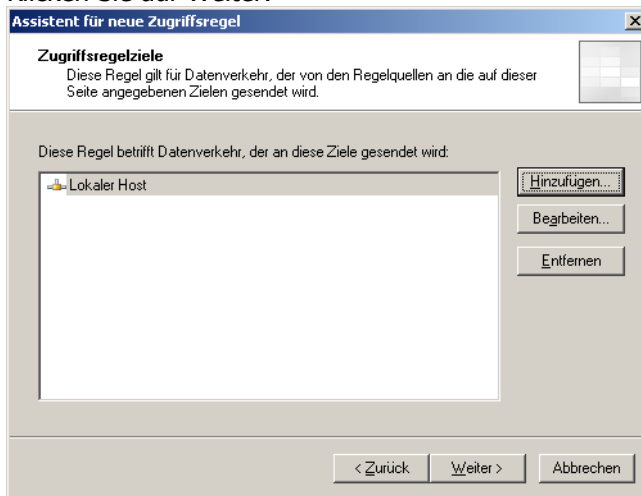
11. Klicken Sie auf *Hinzufügen*.



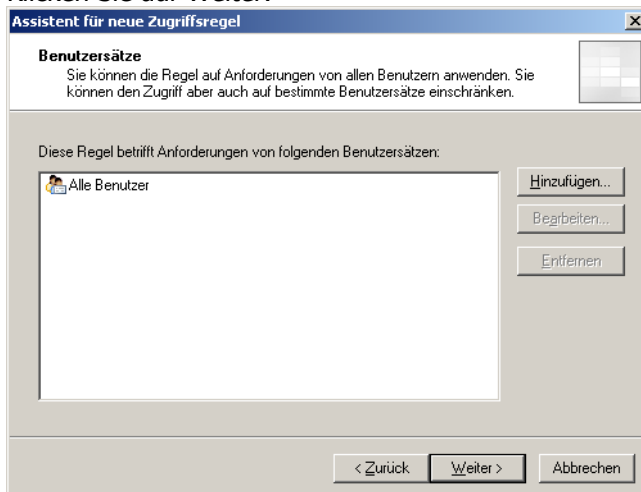
12. Wählen Sie bei *Netzwerke* den *Lokalen Host* aus und klicken Sie auf *Hinzufügen* und *Schließen*.



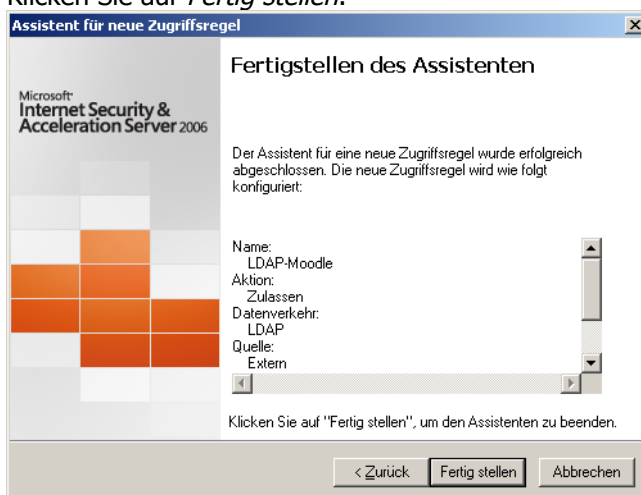
13. Klicken Sie auf *Weiter*.



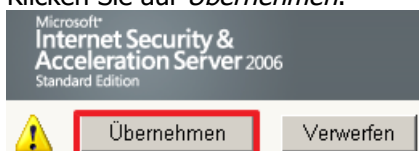
14. Klicken Sie auf *Weiter*.



15. Klicken Sie auf *Fertig stellen*.



16. Klicken Sie auf *Übernehmen*.



1.2.5. Aktivierung der LDAP-Authentifizierung in Moodle

Zur Aktivierung der LDAP-Authentifizierung melden Sie sich als Administrator an. Bei Moodle 2.4x wählen Sie *Website Administration / Plugins / Authentifizierung / Übersicht*. Klicken Sie anschließend bei LDAP-Server in die Spalte *Aktiviert*.

Aktive Plugins zur Authentifizierung

Name	Aktiviert	Aufwärts/Abwärts	Einstellungen
Manuelle Konten			Einstellungen
Keine Anmeldung			Einstellungen
E-Mail basiert	👁		Einstellungen
CAS-Server (SSO)	🔌		Einstellungen
Externe Datenbank	🔌		Einstellungen
FirstClass-Server	🔌		Einstellungen
IMAP-Server	🔌		Einstellungen
LDAP-Server	🔌		Einstellungen
MNET Authentifizierung	🔌		Einstellungen
NNTP-Server	🔌		Einstellungen
Ohne Authentifizierung	🔌		Einstellungen
PAM Authentifizierung	🔌		Einstellungen
POP3-Server	🔌		Einstellungen
RADIUS-Server	🔌		Einstellungen
Shibboleth	🔌		Einstellungen
Webservices	🔌		Einstellungen

EINSTELLUNGEN ⊞ ⊞

- Mein Profil
- ▾ Website-Administration
- ⚙ Mittellungen
- ⚙ Registrierung
- ⚙ Zusatzoptionen
- Nutzer/innen
- Kurse
- Bewertungen
- Lokales
- Sprache
- ▾ Plugins
- ⚙ Übersicht
- Aktivitäten
- Aufgabentypen
- Kursformate
- Blöcke
- Nachrichtensend
- ▾ Authentifizierung
- ⚙ Übersicht
- ⚙ E-Mail basiert
- ⚙ Manuelle Konten
- ⚙ Keine Anmeldung
- Einschreibung
- Texteditoren

Übersicht

Aktive Plugins zur Authentifizierung

Name	Aktiviert	Aufwärts/Abwärts	Einstellungen
Manuelle Konten			Einstellungen
Keine Anmeldung			Einstellungen
LDAP-Server	👁	↓	Einstellungen
E-Mail basiert	👁	↑	Einstellungen
CAS-Server (SSO)	🔌		Einstellungen
Externe Datenbank	🔌		Einstellungen

Das aktivierte Plugin erkennen Sie am geöffneten Auge bei *Aktiviert*.

Unter Aufwärts/Abwärts lässt sich die Reihenfolge wählen, in der die Authentifizierungsplugins abgearbeitet werden.

War die Authentifizierungsmethode vorher "Manuelle Zugänge" läuft erst einmal alles weiter wie bisher, da die Authentifizierungs-Plugins von oben nach unten abgearbeitet werden. Verliefe die Authentifizierung vorher emailbasiert, dann muss man sich entscheiden, in welcher Reihenfolge man die Authentifizierungsmethoden in der Übergangsphase bis zur kompletten Umstellung anordnen möchte.

1.2.6. Umstellung vorhandener Benutzer auf LDAP-Authentifizierung

In Moodle müssen Sie als Administrator angemeldet sein. Unter *Website Administration/ Nutzer/innen /Nutzerkonten /Nutzerliste anzeigen* klicken Sie bei dem jeweiligen Nutzer auf *Bearbeiten*.

Nutzer/in anlegen

Nachname / Vorname	E-Mail-Adresse	Stadt/Ort	Land	Letzter Zugriff	Bearbeiten
[Redacted]	[Redacted]	[Redacted]	Deutschland	1 Sekunde	[Gear icon]
[Redacted]	[Redacted]	[Redacted]	Deutschland	12 Stunden 42 Minuten	[X] [Eye] [Gear]
Prof.Lehrer Prof.Lehrer				12 Stunden 44 Minuten	[X] [Eye] [Gear]
Prof.Schueler Prof.Schueler				31 Minuten 50 Sekunden	[X] [Eye] [Gear]

Website-Administration
 Mitteilungen
 Registrierung
 Zusatzoptionen
 Nutzer/innen
 Nutzerkonten
Nutzerliste anzeigen
 Nutzerverwaltung (Bulk)
 Nutzer/in anlegen
 Profildfelder
 Globale Gruppen
 Nutzerliste hochladen

Unter *Authentifizierung wählen*, stellen Sie auf *LDAP-Server* um. Nun kann sich die Nutzer nur noch mit der Benutzerkennung der paedML anmelden.

ProfLe

Allgemein

Anmeldename*

Authentifizierung wählen ?

Gesperrtes Nutzerkonto ? ☐

Kennwortregeln:
mindestens 8 Zeichen, 1 Ziffer(n), 1 Kleinbuchstabe(n), 1 Großbuchstabe(n), 1

Neues Kennwort ? ☐ Klartext

Kennwortänderung ? ☐

Nachname*

Vorname*

E-Mail-Adresse*

E-Mail-Adresse anzeigen

1.3. Ergänzende Hinweise:

- Bei jedem Anmelden eines Benutzers fragt der Moodleserver beim paedML-Server die Richtigkeit der Benutzerkennung ab. Das Kennwort wird nicht in der Moodle-datenbank gespeichert. Beim ersten Anmelden werden Name und Vorname aus der Active Directory übernommen und zusammen mit den eingegebenen Profildaten in der Moodledatenbank gespeichert. Sind die Profildaten unvollständig, das heißt, fehlen Pflichtdaten wie z.B. die Mailadresse, erscheint das untenstehende Fenster, um die Daten zu ergänzen. Die Änderung der Daten muss durch eine Bestätigungsmail, die von Moodle automatisch verschickt wird, bestätigt werden. Erst danach ist ein Arbeiten in Moodle möglich.

ProfSchueler ProfSchueler

Allgemein

Nachname*	<input type="text" value="ProfSchueler"/>
Vorname*	<input type="text" value="ProfSchueler"/>
E-Mail-Adresse*	<input type="text"/>
E-Mail-Adresse anzeigen	<input type="button" value="E-Mail-Adresse nur für Kursteilnehmer/innen anzeigen"/>
E-Mail-Format	<input type="button" value="HTML-Format"/>
Forenbeiträge zusammenfassen	<input type="button" value="Einzel (alle Forumsbeiträge einzeln als E-Mail)"/>
Forum abonnieren	<input type="button" value="Ja, Forum abonnieren, in dem ich einen Beitrag schreibe"/>
Forenbeiträge markieren	<input type="button" value="Nein, keine Beiträge markieren"/>
Texte bearbeiten	<input type="button" value="HTML-Editor verwenden"/>
Stadt/Ort*	<input type="text"/>
Land auswählen*	<input type="button" value="Land auswählen..."/>
Zeitzone	<input type="button" value="Lokale Serverzeit"/>
Bevorzugte Sprache	<input type="button" value="Deutsch (de)"/>

- Alternativ zu dem LDAP-Protokoll kann man das LDAPS-Protokoll über Port 636 verwenden. Bei LDAPS erfolgt der Kennwortabgleich über das Internet verschlüsselt. Eventuell sind hierzu weitere Einstellungen am Musterlösungsserver notwendig.