

LDAP / LDAPS Authentifizierung BelWü Moodle

Für ein bei Belwue gehostetes Moodle ist die Authentifizierung per Idaps gegenüber einem Server der paedML Linux in der Schule möglich. Durch die Verwendung von Idaps werden die Passwörter verschlüsselt übertragen, so dass sie nicht abgehört werden können.

Sicherheitshalber sollte man aber immer einen administrativen Zugang zum Moodle vorsehen, der von Hand eingetragen wurde, und bei dem die Authentifizierung von Moodle intern durchgeführt wird. Dies ist sinnvollerweise der bei der Erstinstallation schon eingerichtete Admin Nutzer, der sowieso nur für Notfälle eingesetzt werden sollte.

Anmerkung: am Moodle kann man sich dann aber nur anmelden, wenn die eigene paedML auch erreichbar ist!

1. Einstellungen im eigenen Netzwerk

Damit das Moodle bei Belwue mit dem LDAP / LDAPS Server der ML kommunizieren kann, muss moodle den Server der paedML4.x erreichen können, deswegen sind folgende Einstellungen erforderlich:

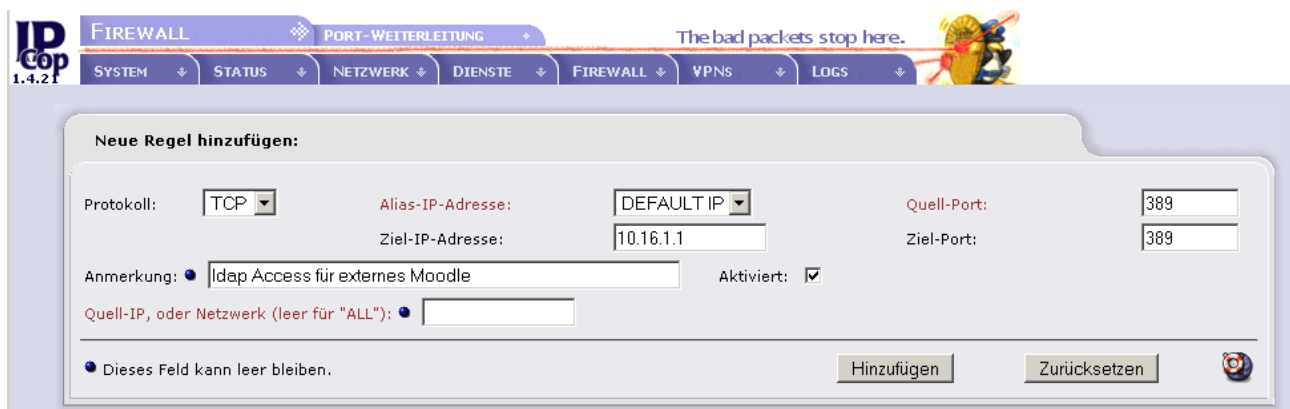
Am Router zum Provider (Belwue):

- Portweiterleitung für die Ports 389 (LDAP) und 636 (LDAPS) im Router von Belwue einrichten lassen bzw. einrichten

Am IPCOP des Schulnetzes:

- Im Webfrontend des IPCop muss unter „Firewall“ - „Port Weiterleitung“ eine neue Regel erstellt werden, die den Port 389 TCP für LDAP bzw. den Port 636 TCP für LDAPS auf den server (normalerweise 10.16.1.1) weiterleitet. Im Feld Quell-IP, oder Netzwerk sollten Sie wie im Bild für die Idaps Regel zu sehen, den Eintrag 129.143.0.0/16 eintragen.

Regel für Idap



The screenshot shows the IPCop 1.4.2.1 firewall configuration page. The 'PORT-WEITERLEITUNG' (Port Forwarding) tab is active. A new rule is being added with the following settings:

- Protokoll: TCP
- Alias-IP-Adresse: DEFAULT IP
- Quell-Port: 389
- Ziel-IP-Adresse: 10.16.1.1
- Ziel-Port: 389
- Anmerkung: Idap Access für externes Moodle
- Aktiviert:
- Quell-IP, oder Netzwerk (leer für "ALL"):

Buttons for 'Hinzufügen' (Add) and 'Zurücksetzen' (Reset) are visible at the bottom right of the rule configuration area.

Regel für Idaps



Neue Regel hinzufügen:

Protokoll: Alias-IP-Adresse: Quell-Port:

Ziel-IP-Adresse: Ziel-Port:

Anmerkung: Aktiviert:

Quell-IP, oder Netzwerk (leer für "ALL"):

Überblick über die existierenden Regeln

Aktuelle Regeln:

Proto	Quelle	Ziel	Anmerkung	Aktion
TCP	DEFAULT IP : 2222	10.16.1.1 : 22(SSH)	ssh remote access on port 2222	<input checked="" type="checkbox"/> <input type="button" value="Bearbeiten"/> <input type="button" value="Löschen"/>
TCP	DEFAULT IP : 443(HTTPS)	10.16.1.1 : 443(HTTPS)	https access on port 443	<input type="checkbox"/> <input type="button" value="Bearbeiten"/> <input type="button" value="Löschen"/>
TCP	DEFAULT IP : 25(SMTP)	10.16.1.1 : 25(SMTP)	smtp access on port 25	<input type="checkbox"/> <input type="button" value="Bearbeiten"/> <input type="button" value="Löschen"/>
TCP	DEFAULT IP : 80(HTTP)	10.16.1.1 : 80(HTTP)	http access on port 80	<input type="checkbox"/> <input type="button" value="Bearbeiten"/> <input type="button" value="Löschen"/>
TCP	DEFAULT IP : 389(LDAP)	10.16.1.1 : 389(LDAP)	ldap Access für externes Moodle	<input checked="" type="checkbox"/> <input type="button" value="Bearbeiten"/> <input type="button" value="Löschen"/>
TCP	DEFAULT IP : 636(LDAPS)	10.16.1.1 : 636(LDAPS)	ldaps Access für externes Moodle	<input checked="" type="checkbox"/> <input type="button" value="Bearbeiten"/> <input type="button" value="Löschen"/>

Zugriff erlaubt von: 129.143.0.0/16 (ldaps Access für externes Moodle)

Legende: Aktiviert (klicken, um zu deaktivieren) Deaktiviert (klicken, um zu aktivieren)

Hinweise

- Es ist darauf zu achten, dass diese Regeln auch aktiviert sind (Häkchen im Kasten am Ende der Zeile).
- Sobald die Authentifizierung per ldaps funktioniert können Sie die Regel für ldap wieder deaktivieren oder sogar löschen.

2. Umstellen auf LDAP

Folgende Einstellungen sind im Moodle vorzunehmen, um die Benutzerauthentifizierung über den LDAP / LDAPS -Server der paedML Linux einzurichten:

Melden Sie sich als admin (s.o.) an Ihrem Moodle an. Gehen Sie im Block Website-Administration auf Nutzer /innen – Authentifizierung – Übersicht. „Öffnen“ Sie dort in der Zeile LDAP Server „das Auge“ und wählen Sie dann Einstellungen.

Website-Administration

- Mitteilungen
- NutzerInnen
 - Authentifizierung
 - Übersicht
 - Kein Login
 - LDAP-Server
 - Manuelle Zugänge
 - Nutzerkonten
 - Zugriffsrechte
- Kurse
- Bewertungen
- Lokales
- Sprache
- Module
- Sicherheit
- Darstellung

Übersicht

Aktive Plugins zur Authentifizierung

Name	Aktivieren	Aufwärts/Abwärts	Einstellungen
Manuelle Zugänge	<input type="checkbox"/>		Einstellungen
Kein Login	<input type="checkbox"/>		Einstellungen
LDAP-Server	<input checked="" type="checkbox"/>		Einstellungen
CAS-Server (SSO)	<input type="checkbox"/>		Einstellungen
Externe Datenbank	<input type="checkbox"/>		Einstellungen

3. LDAP Server Einstellungen

Auf der Konfigurationsseite sind folgende Einstellungen vorzunehmen:

LDAP-Server

Diese Methode bietet die Authentifizierung gegenüber einem externen LDAP-Server. Wenn der vergebene Nutzernamen und Passwort gültig sind, erstellt Moodle einen neuen Nutzereintrag in seiner Datenbank. Dieses Modul kann Nutzereinträge aus LDAP lesen und gewünschte Felder in Moodle vorlegen. Für die nachfolgenden Zugänge werden nur Nutzernamen und Passwort überprüft.

LDAP Server-Einstellungen

Host URL Geben Sie einen LDAP Server in URL-Form an wie 'ldap://ldap.myorg.de/' oder 'ldaps://ldap.myorg.de/'

Version Diese Version des LDAP Protokolls nutzt Ihr Server.

LDAP Codierung Geben Sie die Codierung des LDAP Servers an. Meist ist dies utf-8. MS AD v2 verwendet andere Codierung wie cp1252, cp1250, etc.

Bind-Einstellungen

Kennwörter verbergen Wählen Sie ja, um Passwörter **nicht** in der Moodle-Datenbank zu speichern

Gekennzeichneter Name Möchten Sie Bind-User für die Nutzersuche verwenden, so geben Sie dies hier an. Normalerweise etwas wie 'cn=ldapuser,ou=public,o=org'

Kennwort Passwort für Bind-User.

Einstellung zur Nutzerüberprüfung (user lookup settings)

Nutzertyp Auswahl, wie Nutzer in LDAP hinterlegt werden. Die Einstellungen legen fest wie der Login-Ablauf, grace Logins und Nutzererstellung ablaufen.

Kontexte Liste der Umgebungen, in denen sich Nutzer/innen befinden. Trennen Sie verschiedene Umgebungen durch ';'. Beispiel: 'ou=users,o=org; ou=others,o=org'

Subkontexte suchen Nutzer/innen in Teilumgebungen suchen

Alias berücksichtigen Legt fest wie Aliasbezeichnungen bei der Suche behandelt werden. Wählen Sie einen der folgenden Werte: "No" (LDAP_DEREF_NEVER) or "Yes" (LDAP_DEREF_ALWAYS)

Nutzerattribut Verwendete Eigenschaften, um Nutzer zu benennen/suchen. Normalerweise 'cn'.

Mitgliedsattribut Geben Sie die Mitgliedsoptionen an, wenn Nutzer/innen zu einer Gruppe gehören. Normalerweise 'member'

Mitgliedsattribut nutzt dn Optional: Überschreib-Handlung für Mitgliedsattribut-Werte, entweder 0 oder 1

Objekt Class Filter für die Suche nach Nutzernamen. Normalerweise tragen Sie ein: objectClass=posixAccount . Defaults to objectClass=* what will return all objects from LDAP.

LDAP Server Einstellungen

Host URL:	<i>ldaps: //<IPAdresse></i> aus Sicherheitsgründen lässt der paedML Linux Server eine einfache Abfrage per ldap nicht mehr zu. Es muss ldaps verwendet werden.
Version:	3
LDAP Codierung:	<i>utf-8</i>

Bind-Einstellungen

Kennwörter verbergen (ldap-preventpassindb):	<i>nein</i>
Gekennzeichneter Name (ldap bind dn)	<i>Leer lassen</i>
Kennwort (ldap bind_pw):	<i>Leer lassen</i>



Einstellung zur Nutzerüberprüfung (user lookup settings)

Nutzertyp (ldap user type):	<i>posixAccount (rfc2307)</i>
Kontexte (ldap contexts)	<i>ou=accounts, dc=linuxmuster, dc=local</i> (der komplette Pfad muss wie oben eingetragen werden. Die Information für den fettgedruckten Teil muss in der Datei /etc/ldap/ldap.conf am Server nachgeschaut werden. Der Eintrag nach BASE muss komplett übernommen werden. Die Einträge müssen durch Leerzeichen und Komma getrennt werden.
Suchkontexte: (ldap_search_sub):	<i>ja</i>
Alias berücksichtigen: (ldap opt deref)	<i>nein</i>
Nutzerattribut: (ldap user attribute)	<i>uid</i>
Mitgliedsattribut: (ldap-memberattribute)	<i>member</i>
Mitgliedsattribut nutzt dn	<i>leer</i>
Objekt Class (ldap objectclass)	<i>objektClass=posixAccount</i>

Verbindliche Änderung des Passwortes

Verbindliche Änderung des Passwortes

Nutzer werden aufgefordert, ihr Passwort beim ersten Login zu ändern

Standardseite zur Passwortänderung nutzen

Stellen Sie Ja ein, wenn das externe Authentifizierungssystem eine Änderung des Passwortes durch Moodle zulässt. Die Einstellungen überschreiben 'Passwort-URL ändern'

Anmerkung: Es wird empfohlen LDAP über einen SSL verschlüsselten Tunnel (ldaps://) zu nutzen, wenn der LDAP Server remote verwendet wird.

Passwortformat

Format für neue oder geänderte Passworte auf LDAP-Server

URL zur Kennwortänderung

Hier können Sie eine Adresse angeben, unter der die Nutzer ihren Nutzernamen/Passwort ändern können, sofern sie dies vergessen haben. Diese Option wird den Nutzern als Schaltfläche auf der Anmeldungsseite angeboten. Wenn Sie dieses Feld leer lassen, wird die Option nicht angeboten.

LDAP PasswortablaufEinstellung

Ablauf

Setzen Sie Nein (no) um die Überprüfung abgelaufener Passworte abzuschalten oder LDAP um sie direkt über LDAP abzuwickeln.

Ablaufhinweis

Zahl der Tage vor dem Ablauf der Gültigkeit des Passwortes an denen eine Nachricht versandt wird.

Ablauf-Attribut

optional: Ändert die LDAP-Attribute zur Speicherung der Passwortgültigkeitsdauer passwordExpirationTime

Frist Login

Aktiviert LDAP graclelogin Unterstützung. Wenn das Passwort abgelaufen ist, können die Nutzer/innen sich weiter einloggen bis graclelogin den Wert 0 hat. Nach dem Aktivieren der Einstellung wird eine graclelogin Mitteilung angezeigt, wenn das Passwort abgelaufen ist.

grace Login Attribute

optional: Ändert die graclelogin Attribute

Nutzer-Erstellung aktivieren

Nutzer extern anlegen

Neue (anonyme) Nutzer können Nutzer-Accounts erstellen außerhalb der Authentifizierungsquelle und per E-Mail bestätigen. Sofern Sie dies aktivieren, achten Sie darauf, ebenso modulspezifische Optionen für die Modulerstellung zu konfigurieren.

Kontext für neue Nutzer

Wenn Sie die Nutzererstellung mit E-Mail-Bestätigung aktivieren, geben Sie die Umgebung an, wo die Nutzer/innen erstellt werden sollen. Diese Umgebung sollte sich von der anderer Nutzer/innen unterscheiden, um Sicherheitsrisiken zu vermeiden. Sie brauchen diese Umgebung nicht zur ldap_context Variable hinzuzufügen, Moodle sucht in dieser Umgebung automatisch nach Nutzer/innen.

Verbindliche Änderung des Passwortes

Verbindliche Änderung des Passwortes:	<i>nein</i>
Standardseite zur Passwortänderung nutzen:	<i>nein</i>





Passwortformat:	<i>Reiner Text</i>
URL zur Kennwortänderung:	<i>Leer lassen</i>

LDAP Passwortablaufeinstellung

Ablauf: (ldap expiration)	<i>no</i>
Ablaufhinweis: (ldap expiration warning)	<i>10</i>
Ablaufattribut: (ldap expireattr)	<i>Leer lassen</i>
Frist Login: (ldap_gracelogins)	<i>nein</i>
grade Login Attribute: (ldap_graceattr)	<i>Leer lassen</i>

Nutzer Einstellung aktivieren

Nutzer extern anlegen:	<i>nein</i>
Kontext für neue Nutzer: (ldap_create_context)	<i>Leer lassen</i>

Kursverwalter/in

Kursverwalter/innen Eine Liste von Gruppen, denen es erlaubt ist, Kurse zu verwalten und neu anzulegen (Liste der Kursverwalter/innen). Trennen Sie mehrere Gruppen durch ','. Normalerweise etwas wie 'cn=teachers, ou=staff, o=myorg'

Cron-Synchronisierungsskript

Entfernte externe Nutzer 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.

NTLM SSO

Aktivieren Aktivieren Sie diese Einstellung, um die einmalige Anmeldung (Single Sign On) mit der NTLM-Domain zu versuchen. **Anmerkung:** Zusätzlich sind Einstellungen für den Webserver notwendig. Siehe http://docs.moodle.org/en/NTLM_authentication

Subnet Wenn das Feld nicht leer ist, dann ist SSO nur mit Adressen aus dem Subnet möglich. Format: xxx.xxx.xxx.xxx/bitmask

MS IE fast path? Aktivieren Sie diese Einstellung, um 'NTLM SSO fast path' zuzulassen. Dies funktioniert ausschließlich, wenn mit dem MS Internet Explorer auf Moodle zugegriffen wird.

Kursverwalter/in

Kursverwalter/innen: (ldap_creators):	<i>Leer lassen</i>
---------------------------------------	--------------------

Cron-Synchronisierungsskript

Entfernte externe Nutzer	<i>Nur intern zugänglich</i>
--------------------------	------------------------------

NTLM SSO

Aktivieren	<i>nein</i>
Subnet	<i>Leer lassen</i>
MS IE fast path?	<i>nein</i>

Data mapping

<p>Vorname <input type="text" value="givenName"/></p> <p>Update lokaler Daten <input type="button" value="Bei jedem Login"/></p> <p>Update externer Daten <input type="button" value="Nie"/></p> <p>Sperrwert <input type="button" value="Bearbeitbar wenn Feld leer"/></p>	<p>Diese Felder sind optional. Sie können einige Moodle Nutzer-Felder mit Daten aus LDAP-Feldern vorbelegen, die Sie hier spezifizieren.</p> <p>Wenn Sie diese Felder leer lassen, wird nichts von LDAP transferiert und die Moodle Voreinstellungen werden verwendet.</p>
<p>Nachname <input type="text" value="sn"/></p> <p>Update lokaler Daten <input type="button" value="Bei jedem Login"/></p> <p>Update externer Daten <input type="button" value="Nie"/></p> <p>Sperrwert <input type="button" value="Bearbeitbar wenn Feld leer"/></p>	<p>In jedem Fall können Nutzer diese Felder editieren, nachdem sie sich angemeldet haben.</p> <p>Update lokaler Daten: Wenn dieses Feld aktiviert wird, wird das Feld (aus externer Quelle (external auth)) jedes Mal aktualisiert wenn der Teilnehmer sich einloggt oder eine Nutzersynchronisation erfolgt. Dateneinträge, die lokal aktualisiert werden, sollten geschützt werden.</p>
<p>E-Mail-Adresse <input type="text"/></p> <p>Update lokaler Daten <input type="button" value="Beim Anlegen"/></p> <p>Update externer Daten <input type="button" value="Nie"/></p> <p>Sperrwert <input type="button" value="Bearbeitbar wenn Feld leer"/></p>	<p>Sperrwert: Wenn Sie die Funktion aktivieren, verhindert Moodle die Bearbeitung des Feldes durch Nutzer/innen und Administrator/innen. Dies ist sinnvoll, wenn die Daten in einer externen Datenbank gepflegt werden.</p>

Data mapping

Um Daten der Nutzer per Idaps Abfrage gleich in die Felder des Moodle Profils einzutragen, konfigurieren Sie in *Data mapping* die Felder Vorname und Nachname wie auf dem Bild oben zu sehen. Falls Sie die schulischen e-mail Adressen nutzen wollen, können Sie im Feld *E-Mail-Adresse* den Eintrag *mail* vornehmen. Die restlichen Felder lassen Sie leer.

4. Hinweise zur Umstellung auf Idaps

4.1. Neu installiertes Moodle

Am einfachsten verläuft die Umstellung auf die Idap/Idaps Authentifizierung, wenn man in einem neu eingerichteten Moodle von Anfang per Idap/Idaps authentifizieren lässt. Bis auf administrative Nutzer, die manuell angelegt werden, authentifizieren sich alle Nutzer des Moodle dann über Idaps gegenüber dem eingetragenen Server.

4.2. Laufendes Moodle

Auf einem laufenden Moodle muss man je nach Situation unterschiedlich vorgehen.

4.2.1. Manuelle Änderung

Wenn bisher nur wenige Nutzer manuell aufgenommen wurden, dann kann man diese von Hand auf die neue Authentifizierung umstellen. Voraussetzung dazu ist, dass der manuell vergebene Nutzernamen mit dem Nutzernamen auf der paedML übereinstimmt.

Vorgehensweise

Melden Sie sich als admin an Ihrem Moodle an. Gehen Sie im Administrationsblock zu *Nutzer/innen – Nutzerkonten – Nutzerliste* anzeigen. Wählen Sie die Nutzer nacheinander über *Bearbeiten* aus.



25 Nutzer/innen

Neue Suche

Vollständiger Name enthält * Zusätzliche Felder anzeigen

Nutzer/in neu anlegen

Nachname / Vorname	E-Mail-Adresse	Stadt/Ort	Land	Letzter Zugriff		
moodle admin	moodleadmin@semghs.hn.bw.schule.de	Heilbronn	Deutschland	299 Tage 11 Stunden	Bearbeiten	Löschen
Nutzer/in Administration	admin@ugb.hn.schule-bw.de	Untergruppenbach	Deutschland	3 Sekunden	Bearbeiten	
Müller Eva	eva-mueller@email.de	Stuttgart	Deutschland	2 Jahre 102 Tage	Bearbeiten	Löschen
Katz Florian	katzflorian@ugb.hn.schule-bw.de	Untergruppenbach	Deutschland	1 Jahr 88 Tage	Bearbeiten	Löschen
Cakmak Halise	cakmakhalise@ugb.hn.schule-bw.de	Untergruppenbach	Deutschland	1 Jahr 88 Tage	Bearbeiten	Löschen
meyer hans	meyer@ugb.xx	Untergruppenbach	Deutschland	Nie	Bearbeiten	Löschen
meyer heinz	mayer@ugb.xx	Untergruppenbach	Deutschland	Nie	Bearbeiten	Löschen

und aktivieren Sie **Zusätzliche Felder anzeigen**.

Allgemein * Zusätzliche Felder verbergen

Anmeldename*

Authentifizierungsmethode*

Neues Kennwort Klartext

Ändern Sie nun die Authentifizierungsmethode von **Manuelle Zugänge** auf **LDAP-Server**.

meyer hans

Allgemein * Zusätzliche Felder verbergen

Anmeldename*

Authentifizierungsmethode*

Neues Kennwort Klartext

Führen Sie diesen Vorgang bei allen Nutzern durch.

4.2.2. Manuelle angelegte Nutzer löschen

Ist die Anzahl der manuell angelegten Nutzer zu groß, so ist die folgende Vorgehensweise sinnvoll:

- Sichern sie alle Kurse ohne Nutzer
- löschen Sie alle Nutzer per bulk Verwaltung
- löschen Sie alle Kurse
- importieren Sie die Kurse wieder in Ihr Moodle
- stellen Sie sicher, dass sich alle Nutzer wieder an Ihrem Moodle registrieren.