

## Übersicht

Stand: 14.05.2016

1. Voraussetzungen .....	2
2. Erweiterungen an der ASG Firewall.....	3
3. Moodle LDAPS Authentifizierung.....	7
4. Organisatorische Hinweise .....	11

In der folgenden Anleitung werden die Voraussetzungen sowie die notwendigen Erweiterungen / Änderungen beschrieben, damit Standorte mit der paedML Novell 3.x auf einfache Art und Weise (gleicher Account, gleiches Passwort) die Moodle Umgebung bei BelWü nutzen können.

Im vorletzten Abschnitt wird das Problem „Dass sich die Benutzer nur dann am Belwue-Moodle anmelden können, wenn der Server im päd. Netz am Standort fehlerfrei läuft und von außen erreichbar ist!“, näher beschrieben. Im letzten Kapitel finden Sie einige organisatorische Empfehlungen für die Umstellung auf LDAPS.

## 1. Voraussetzungen

---

1. Die Schule / das Seminar besitzt einen BelWü Anschluss
2. Auf dem BelWü Webserver wurde von BelWü eine eigene Moodle-Umgebung für die Schule / das Seminar eingerichtet.
3. Auf dem BelWü Router der Schule / des Seminars muss der LDAPS Port 636 frei geschaltet werden. Über die Mailadresse [ip@belwue.de](mailto:ip@belwue.de) kann der Port unter Angabe der BelWü Kundennummer freigeschaltet werden.
4. An der Schule / das Seminar wird die paedML Novell 3.x / Novell 4.x eingesetzt.

## 2. Erweiterungen an der ASG Firewall

### Schritt 1: ASG Firewall - Erweiterungen

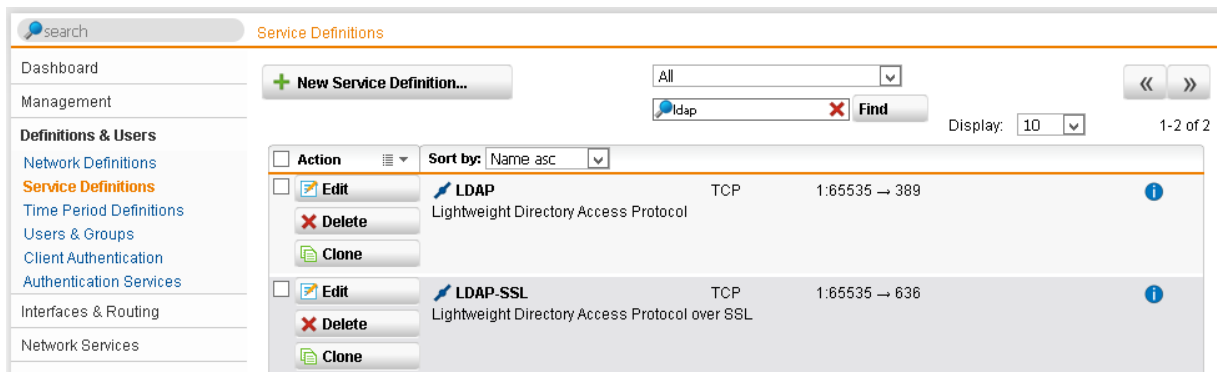
Ziel: Die LDAPS Authentifizierung soll nur zwischen Standort und BelWü möglich sein.

1. Melden Sie sich als Admin an Ihrer ASG Firewall an (<https://.....:4444>)
2. Über das Menü DEFINITIONS | NETWORKS werden zuerst der IP-Adressbereich der BelWü Webserver, auf den sich Ihrer Moodle-Umgebung befindet, angelegt.  
Erzeugen Sie über die Schaltfläche „New network definitions“ einen neuen Eintrag mit folgendem Inhalt:

The screenshot shows the 'Network Definitions' page in the ASG Firewall management interface. The left sidebar contains a search bar and a menu with the following items: Dashboard, Management, Definitions & Users (highlighted), Network Definitions (highlighted), Service Definitions, Time Period Definitions, Users & Groups, Client Authentication, Authentication Services, Interfaces & Routing, Network Services, Network Protection, Web Protection, and Email Protection. The main content area has a 'Network Definitions' header with a search bar and a 'New Network Definition...' button. Below this is the 'Edit Network Definition' dialog box, which contains the following fields: Name: 'BelWue Server', Type: 'Network' (dropdown), IPv4 address: '129.143.0.0', Netmask: '/16 (255.255.0.0)' (dropdown), and Comment: 'BelWue WebServer, Moodle'. There is also an 'Advanced' section with a plus icon. At the bottom right are 'Save' and 'Cancel' buttons.

**Hinweis:** Die IP-Adresse bzw. IP-Adressbereich (z.B. 129.143.0.0/16) des BeWü Webservers erfahren Sie über die Mailadresse [webmaster@belwue.de](mailto:webmaster@belwue.de).  
Speichern Sie über die Änderung über die Schaltfläche SAVE

3. Kontrollieren Sie über den Menüpunkt DEFINITIONS | SERVICES, ob der Filter LDAPS vorhanden ist. Dies sollte i.d.R. schon der Fall sein.



Service Definitions

Dashboard Management

Definitions & Users

- Network Definitions
- Service Definitions**
- Time Period Definitions
- Users & Groups
- Client Authentication
- Authentication Services

Interfaces & Routing

Network Services

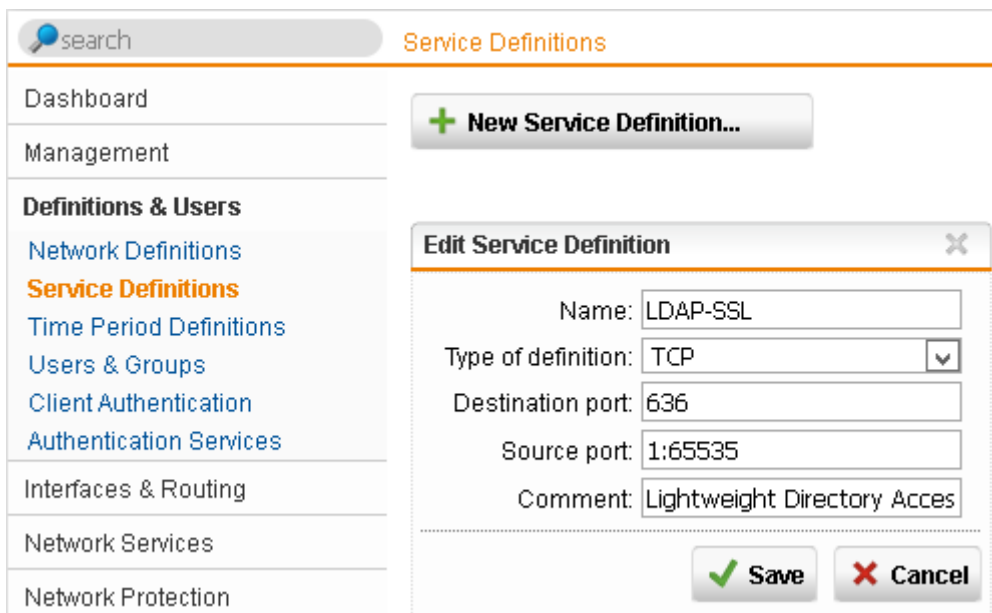
Network Protection

+ New Service Definition...

Search: ldap Find

Display: 10 1-2 of 2

Action	Name	Type	Port
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone	LDAP	TCP	1:65535 → 389
<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone	LDAP-SSL	TCP	1:65535 → 636



Service Definitions

Dashboard Management

Definitions & Users

- Network Definitions
- Service Definitions**
- Time Period Definitions
- Users & Groups
- Client Authentication
- Authentication Services

Interfaces & Routing

Network Services

Network Protection

+ New Service Definition...

Edit Service Definition

Name: LDAP-SSL

Type of definition: TCP

Destination port: 636

Source port: 1:65535

Comment: Lightweight Directory Acces

Save Cancel

4. Aus Sicherheitsgründen wird über ETWORK PROTECTION | NAT FILTER) die LDAPS Anfragemöglichkeiten auf die WebServer von BelWü eingeschränkt.
- Legen Sie über das Menü NETWORK PROTECTION | NAT „New NAT Rule..“ für den Zugriff von BelWü eine neue Regel an.

search NAT

Dashboard Masquerading NAT

Management **1** + New NAT Rule...

Definitions & Users

Interfaces & Routing

Network Services

**Network Protection**

Firewall

**NAT** **2**

Advanced Threat Protection

Intrusion Prevention

Server Load Balancing

VoIP

Advanced

Web Protection

Email Protection

Endpoint Protection

Wireless Protection

Webserver Protection

RED Management

Site-to-site VPN

Remote Access

Logging & Reporting

Support

Log off

**Edit NAT rule**

Group: Gserver03

Position: 17

Rule type: DNAT (destination)

**Matching condition**

For traffic from: BelWue Server

Using service: LDAP-SSL

Going to: External (Add)

**Action**

Change the destination to: DMZ Gserver03

And the service to: LDAP-SSL

☐ Automatic firewall rule

Comment: DMZ Gserver03 LDAP

☒ **Advanced**

☒ Log initial packets

**9** Save Cancel

Nr	Feld	Eintrag	Hinweis
1	Neu NAT Regel erzeugen Group: GServer03		
2	Rule type	DNAT (destination)	
3	For traffic form:	BelWue Server	siehe Punkt 1)
4	Using service:	LDAP-SSL	Port 636
5	Going to:	External (Address)	Öffentliche IP Adresse der Schule
6	Change the destination to:	DMZ GServer	192.168.1.2
7	And the service to:	LDAP-SSL	Port 636
8	Commnet	DMZ GServer03 LDAP	

5. Speichern Sie Ihre Änderungen am Ende über die Schaltfläche SAVE ab.

### 3. Moodle LDAPS Authentifizierung

Melden Sie sich als Admin an und aktivieren Sie den Menüpunkt

[Dashboard](#) ► [Website-Administration](#) ► [Plugins](#) ► [Authentifizierung](#) ► [Übersicht](#)

den LDAP-Server

#### Aktive Plugins zur Authentifizierung

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Testeinstellungen	Deinstallieren
Manuelle Konten	2			<a href="#">Einstellungen</a>		
Kein Login	0			<a href="#">Einstellungen</a>		
E-Mail basiert	0			<a href="#">Einstellungen</a>		<a href="#">Deinstallieren</a>
CAS-Server (SSO)	0			<a href="#">Einstellungen</a>		<a href="#">Deinstallieren</a>
Externe Datenbank	0			<a href="#">Einstellungen</a>	<a href="#">Testeinstellungen</a>	<a href="#">Deinstallieren</a>
FirstClass-Server	0			<a href="#">Einstellungen</a>		<a href="#">Deinstallieren</a>
IMAP-Server	0			<a href="#">Einstellungen</a>		<a href="#">Deinstallieren</a>
LDAP-Server	0			<a href="#">Einstellungen</a>		

#### Aktive Plugins zur Authentifizierung

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Testeinstellungen	Deinstallieren
Manuelle Konten	2			<a href="#">Einstellungen</a>		
Kein Login	0			<a href="#">Einstellungen</a>		
E-Mail basiert	0		↓	<a href="#">Einstellungen</a>		<a href="#">Deinstallieren</a>
LDAP-Server	0		↑	<a href="#">Einstellungen</a>		

Nehmen Sie anschließend in der Zeile LDAP-Server über EINSTELLUNGEN folgenden Änderungen vor.

## LDAP-Server

Diese Anmeldemethode ermöglicht die Authentifizierung über einen externen LDAP-Server.

Um ein neues LDAP-basiertes Nutzerkonto in Moodle anzulegen, muss vorher das LDAP-Nutzerkonto existieren. Beim ersten Login wird automatisch ein neues Nutzerkonto in der Moodle-Datenbank, wobei Anmeldename und Kennwort vorher von LDAP geprüft werden. Das Modul sorgt dafür, dass ausgewählte Nutzerdaten von LDAP in die Moodle-Datenbank übernommen werden können. Wenn das Kennwort weiterhin ausschließlich von LDAP verwaltet wird, ermöglicht dies einheitliche Anmeldedaten in unterschiedlichen Moodle-Instanzen und bei anderen Servern.

Bei allen weiteren Logins werden weiterhin Anmeldename und Kennwort vom LDAP-Server überprüft.

### LDAP-Server-Einstellungen

<div style="background-color: #fff9c4; padding: 2px; display: inline-block; margin-bottom: 10px;">1</div> <div>Host URL <input type="text"/></div>	<p>Geben Sie einen LDAP-Server in URL-Form an, wie etwa 'ldap://ldap.meinserver.de' oder 'ldaps://ldap.meinserver.de'. Mehrere LDAP-Server trennen Sie bitte mit ';' (Semikolon), z.B. als LDAP-Failover.</p>
<div style="background-color: #fff9c4; padding: 2px; display: inline-block; margin-bottom: 10px;">2</div> <div>Version <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; text-align: center;">3</div></div>	<p>Tragen Sie verfügbare LDAP-Version auf Ihrem Server ein.</p>
<div style="background-color: #fff9c4; padding: 2px; display: inline-block; margin-bottom: 10px;">3</div> <div>TLS benutzen <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; text-align: center;">Nein</div></div>	<p>LDAP-Service mit TLS (über Port 389) verschlüsseln</p>
<div style="background-color: #fff9c4; padding: 2px; display: inline-block; margin-bottom: 10px;">4</div> <div>LDAP-Codierung <input type="text" value="utf-8"/></div>	<p>Die Codierung des LDAP-Servers sollte standardmäßig utf-8 sein, aber das Microsoft ActiveDirectory v2 verwendet andere Codierungen, z.B. cp1252 oder cp1250.</p>

Eintrag	Vorgaben für die paedML 3.x / 4.x	Hinweise
LDAP- Server-Einstellungen		
Host URL	ldaps://[öffentliche IP Adresse der Schule]	
Version	3	
TLS benutzen	nein	
LDAP-Codierung	utf-8	
Bind-Einstellungen		
Nutzersuche (user lookup)		
Nutzertyp	Novell Edirectory	
Kontext	ou=benutzer,ou=xyz,ou=schulen,o=ml3 Beispiel: ou=benutzer,ou=sembw,ou=schulen,o=ml3	Ersetzen Sie <b>xyz</b> durch Ihr Schulkürzel. Beachten Sie bitte die Schreibweise sowie das Komma als Trennzeichen.
Subkontexte	Ja	
Aliase berücksichtigen	Nein	
Nutzermerkmal	cn	Es wird der paedML



Eintrag	Vorgaben für die paedML 3.x / 4.x		Hinweise
			Anmeldname übernommen.
Object Class	<b>objectClass= *</b>		
Kennwortänderung fordern			
	Keine Änderungen - die Einstellungen können übernommen werden.		
Gültigkeitsablauf von Kennwörtern			
	Keine Änderungen - die Einstellungen können übernommen werden.		
Nutzererstellung aktivieren			
	Keine Änderungen - die Einstellungen können übernommen werden.		
Kursersteller/in			
	Keine Änderungen - die Einstellungen können übernommen werden.		
Synchronisierung der Nutzerkonten			
	Keine Änderungen - die Einstellungen können übernommen werden.		
NTLM-SSO			
	Keine Änderungen - die Einstellungen können übernommen werden.		
Datenzuordnung			
Vorname	<b>givenName</b>		Schreibweise beachten
	Lokal aktualisieren	<b>Beim Anlegen</b>	
	Extern aktualisieren	<b>Bei Aktualisierung</b>	
	Feld sperren	<b>Gesperrt</b>	
Nachname	<b>sn</b>		Kleinbuchstaben
	Lokal aktualisieren	<b>Beim Anlegen</b>	
	Extern aktualisieren	<b>Bei Aktualisierung</b>	
	Feld sperren	<b>Gesperrt</b>	
E-Mail-Adresse	<b>mail</b>		Kleinbuchstaben
	Lokal aktualisieren	<b>Beim Anlegen</b>	
	Extern aktualisieren	<b>Bei Aktualisierung</b>	
	Feld sperren	<b>Gesperrt</b>	
Abteilung	<b>dn</b>		<b>in Kleinbuchstaben</b>  Hier wird der Benutzername inkl. Kontext

Eintrag	Vorgaben für die paedML 3.x / 4.x		Hinweise
			übernommen. Beispiel: cn=SpechtB- SEMBW,ou=Lehrer,ou=
	Lokal aktualisieren	<b>Beim Anlegen</b>	
	Extern aktualisieren	<b>Bei Aktualisierung</b>	
	Feld sperren	<b>Gesperrt</b>	

## Hinweise

Einstellung	Option	Vorgaben für die paedML 3.x
Lokal aktualisieren	<b>Beim Anlegen</b> <b>Bei jedem Login</b>	<b>Update lokaler Daten:</b> 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.
Extern aktualisieren	<b>Nie</b> Bei der Aktualisierung	<b>Update externer Daten:</b> Wenn diese Einstellung aktiviert ist, dann wird die externe Authentifizierung aktualisiert, sobald der Nutzerdatensatz aktualisiert wird. Die Felder sollten bearbeitbar bleiben, um Dateneinträge zuzulassen
Feld sperren	Bearbeitbar Bearbeitbar wenn Feld leer <b>Gesperrt</b>	<b>Sperrwert:</b> 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.

**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.

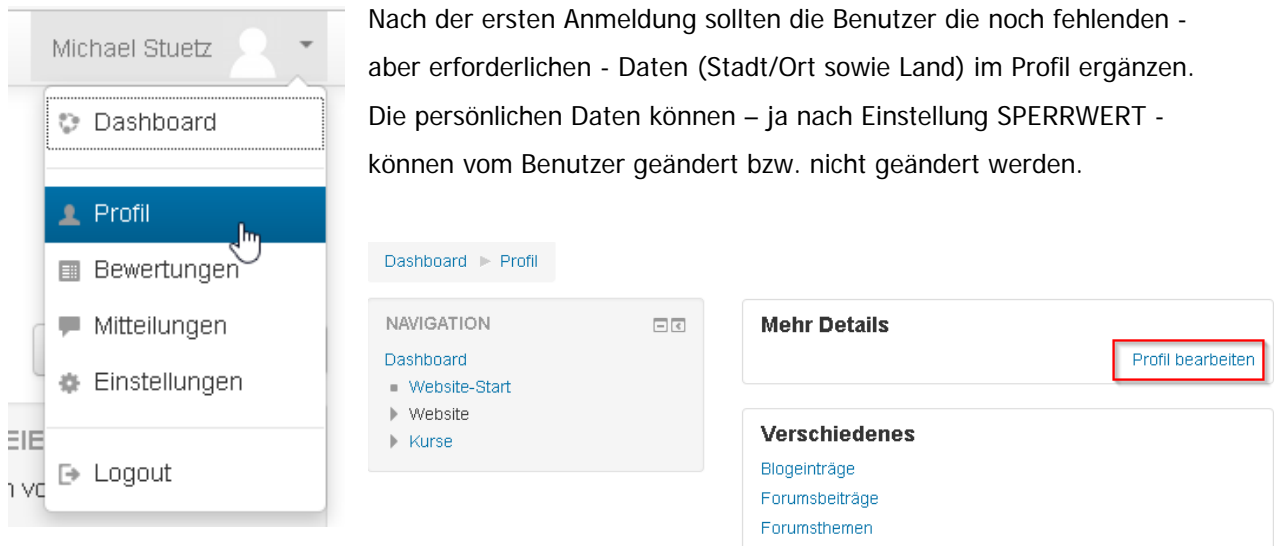
Hinweis: Zur Verwaltung Klassenbezeichnung sollte in Moodle über

[Dashboard](#) ► [Website-Administration](#) ► [Nutzer/innen](#) ► [Nutzerkonten](#) ► [Profilfelder](#)

ein zusätzliches Profilfeld (Texteingabe bzw. Auswahlménü) mit der entsprechenden Bezeichnung angelegt werden.

## 4. Organisatorische Hinweise

### Moodle - Eingabe der fehlenden Daten



Nach der ersten Anmeldung sollten die Benutzer die noch fehlenden - aber erforderlichen - Daten (Stadt/Ort sowie Land) im Profil ergänzen. Die persönlichen Daten können – ja nach Einstellung SPERRWERT - können vom Benutzer geändert bzw. nicht geändert werden.

### ▼ Grundeinträge

<b>Vorname</b>	<input type="text"/>
<b>Nachname</b>	<input type="text"/>
<b>E-Mail-Adresse</b>	<input type="text"/>
<b>E-Mail-Adresse anzeigen</b>	<input type="text" value="E-Mail-Adresse nur für Kursteilnehmer/innen anzeigen"/> ▼
<b>1 Stadt/Ort</b>	<input type="text"/>
<b>2 Land auswählen</b>	<input type="text" value="Land auswählen..."/> ▼
<b>Zeitzone</b>	<input type="text" value="Serverzeitzone (Europa/Berlin)"/> ▼