

paedML Novell – Moodle LDAPS Authentifizierung

Übersicht

Stand: 28.04.2020

1. Voraussetzungen	2
2. Erweiterungen an der Spohos Firewall	3
3. Moodle LDAPS Authentifizierung.....	6
4. Zeitgesteuerte Synchronisierung der LDAP-Nutzerkonten.....	11
5. Organisatorische Hinweise	12

In der folgenden Anleitung werden die Voraussetzungen sowie die notwendigen Erweiterungen / Änderungen beschrieben, damit Standorte mit der paedML Novell 3.x / 4.x (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 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.

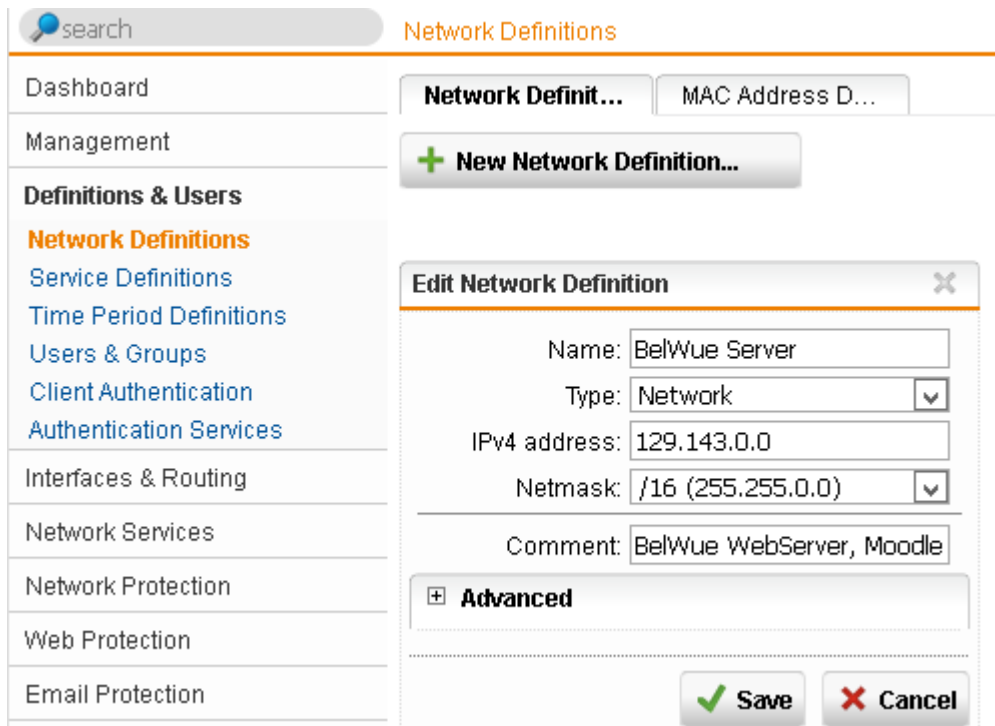
2. Erweiterungen an der Sophos Firewall

Schritt 1: Sophos 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 Sophos Firewall web interface. The left sidebar contains a navigation menu with categories like 'Definitions & Users', 'Interfaces & Routing', 'Network Services', 'Network Protection', 'Web Protection', and 'Email Protection'. The 'Network Definitions' section is active. The main content area shows a 'New Network Definition...' button and an 'Edit Network Definition' dialog box. The dialog box has the following fields:

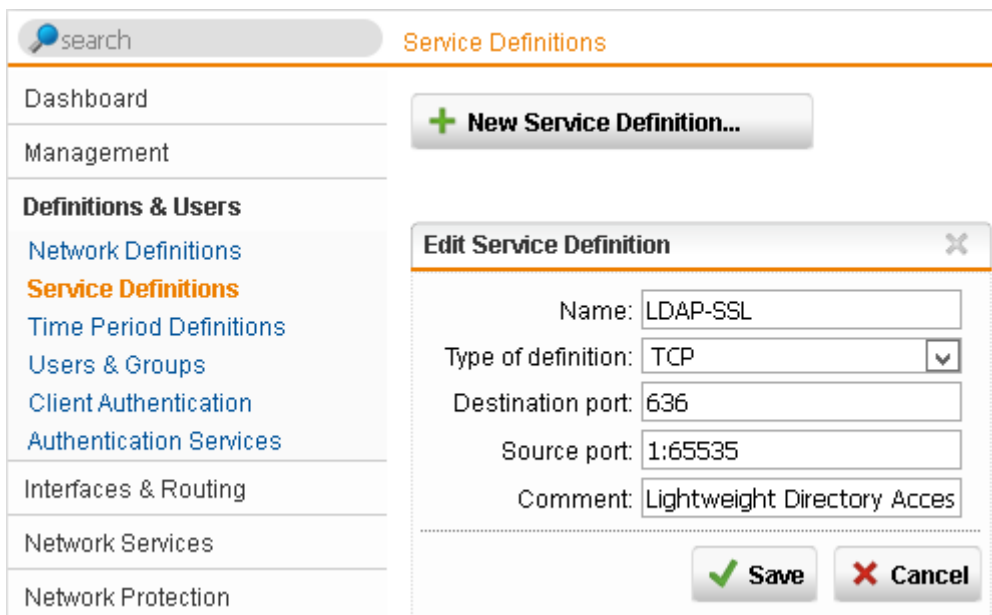
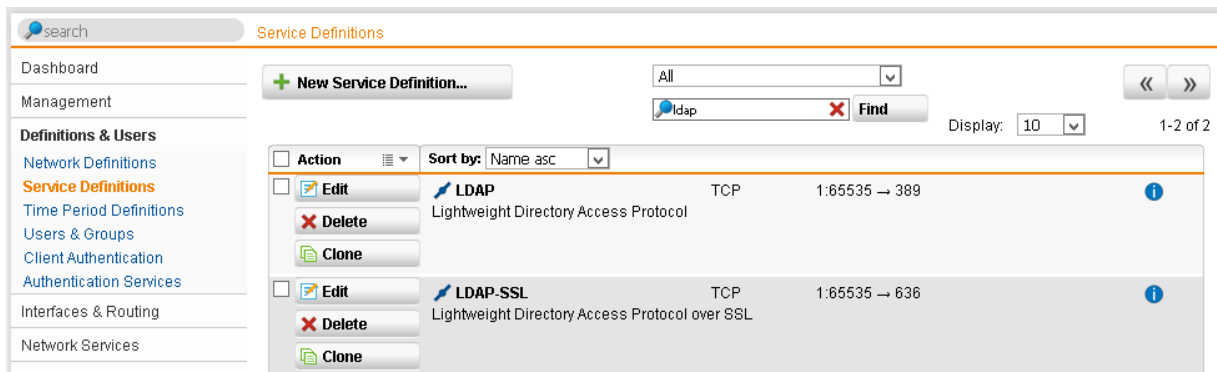
- Name: BelWue Server
- Type: Network (dropdown menu)
- IPv4 address: 129.143.0.0
- Netmask: /16 (255.255.0.0) (dropdown menu)
- Comment: BelWue WebServer, Moodle

Below the main fields is an 'Advanced' section, which is currently collapsed. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

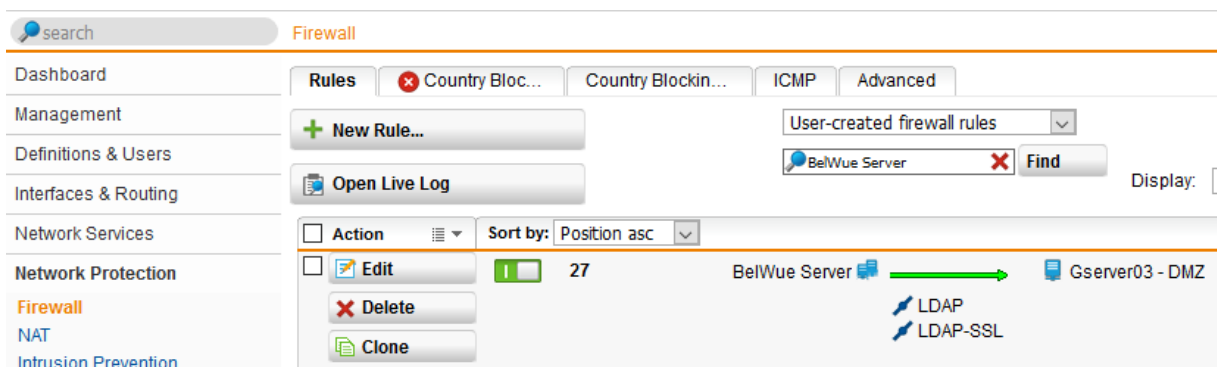
Hinweis: Die IP-Adresse bzw. IP-Adressbereich (z.B. 129.143.0.0/16) des BeWü Webservers erfahren Sie über die Mailadresse webmaster@belwue.de.

Speichern Sie über die Änderung über die Schaltfläche SAVE

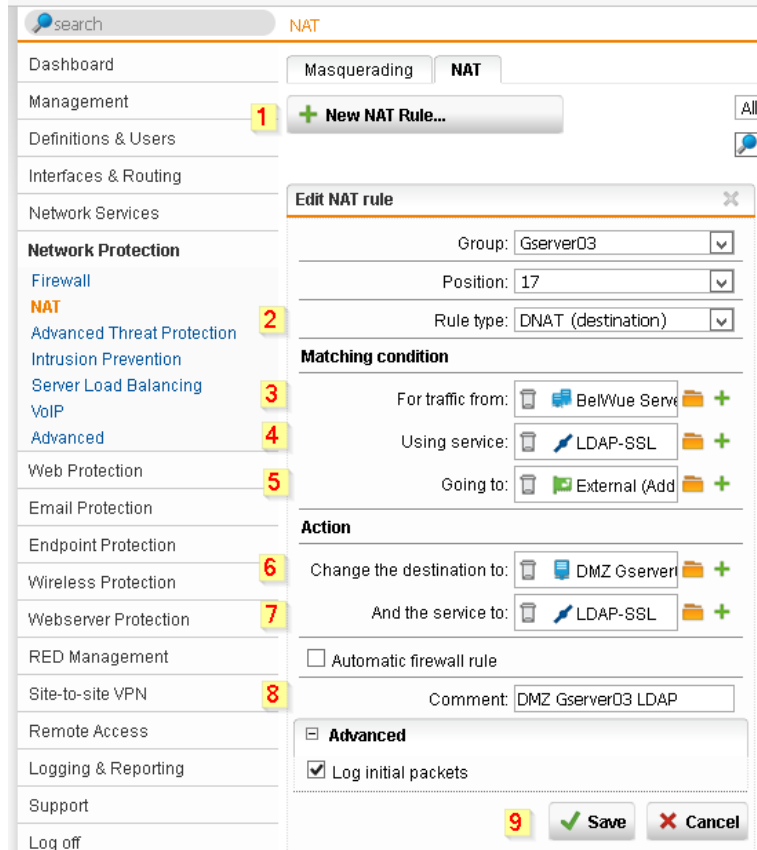
- Kontrollieren Sie über den Menüpunkt DEFINITIONS | SERVICES, ob der Filter LDAPs vorhanden ist. Dies sollte i.d.R. schon der Fall sein.



- Über das Menü NETWORK PROTECTION | FIREWALL werden die LDAP / LDAPS Port geöffnet. Der Zugriff auf das päd. Netz wird auf die BelWü Server beschränkt. Der LDAP Port wird nur für Testzwecke geöffnet. Wenn die LDAPS Anbindung funktioniert kann die Portfreigabe auf LDAP-SSL beschränkt werden.



- Aus Sicherheitsgründen wird über NETWORK 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.



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	

- 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			Einstellungen		
Kein Login	0			Einstellungen		
E-Mail basiert	0			Einstellungen		Deinstallieren
CAS-Server (SSO)	0			Einstellungen		Deinstallieren
Externe Datenbank	0			Einstellungen	Testeinstellungen	Deinstallieren
FirstClass-Server	0			Einstellungen		Deinstallieren
IMAP-Server	0			Einstellungen		Deinstallieren
LDAP-Server	0			Einstellungen		

Aktive Plugins zur Authentifizierung

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts	Einstellungen	Testeinstellungen	Deinstallieren
Manuelle Konten	2			Einstellungen		
Kein Login	0			Einstellungen		
E-Mail basiert	0		↓	Einstellungen		Deinstallieren
LDAP-Server	0		↑	Einstellungen		

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

LDAP-Server

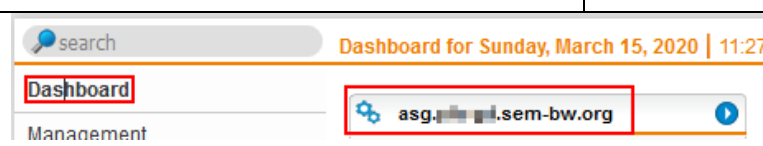
Diese Anmeldemethode ermöglicht die Authentifizierung über einen externen LDAP-Server.

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 Anmelde- 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 Anmelde- und Kennwort vom LDAP-Server überprüft.

LDAP-Server-Einstellungen

<p>1 Host URL <input type="text"/></p>	<p>2 Version <input type="text" value="3"/></p>	<p>3 TLS benutzen <input type="text" value="Nein"/></p>	<p>4 LDAP-Codierung <input type="text" value="utf-8"/></p>	<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> <p>Tragen Sie verfügbare LDAP-Version auf Ihrem Server ein.</p> <p>LDAP-Service mit TLS (über Port 389) verschlüsseln</p> <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:// [öffentlicher DNS Sophos Firewall] ldaps://asg.[Schulkürzel].schule-bw.de alternativ ldaps:// [öffentlicher IP Adresse der Schule]	Hinweis: Die DNS Bezeichnung wird über das Dashboard der Sophos Firewall angezeigt
		
Version	3	
TLS benutzen	nein	
LDAP-Codierung	utf-8	
Bind-Einstellungen		
Kennwort-Caching verhindern	Nein	
Anmelde-Name	cn=ldap2edirbinduser,ou=server,ou=dienste,o=m13	
Kennwort	Bitte hier das entsprechende Passwort eingeben	Kontrolle. Funktioniert die Anmeldung unter https://10.1.1.32/nps

Eintrag	Vorgaben für die paedML 3.x / 4.x	Hinweise	
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 xyz durch Ihr Schulkürzel. Beachten Sie bitte die Schreibweise sowie das Komma als Trennzeichen.	
Subkontexte	Ja		
Aliase berücksichtigen	Nein		
Nutzermerkmal	cn	Es wird der paedML Anmelde-name übernommen.	
Object Class	objectClass=inetOrgPerson	Es werden nur Benutzer synchronisiert.	
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	givenName		Schreibweise beachten
	Lokal aktualisieren	Beim Anlegen	Da der Vorname i.d.R. nachträglich nicht aktualisiert werden muss.
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	
Nachname	sn		Kleinbuchstaben
	Lokal aktualisieren	Bei jedem Login	Die Änderung des Familiennamens wird synchronisiert.

Eintrag	Vorgaben für die paedML 3.x / 4.x		Hinweise
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	
E-Mail-Adresse	mail		Kleinbuchstaben
	Lokal aktualisieren	Beim Anlegen	Schüler erhalten von der Schule einen Mailaccount
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	
Abteilung	dn		in Kleinbuchstaben Hier wird der Benutzername inkl. Kontext übernommen. Beispiel: cn=SpechtB-SEMBW,ou=Lehrer,ou=...
	Lokal aktualisieren	Beim Anlegen	
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	

Hinweise

Einstellung	Option	Vorgaben für die paedML 3.x
Lokal aktualisieren	Beim Anlegen Bei jedem Login	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.
Extern aktualisieren	Nie Bei der Aktualisierung	Update externer Daten: 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 Gesperrt	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.

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.

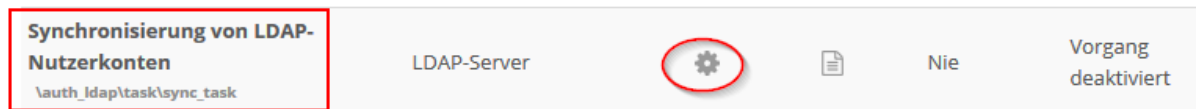
Hinweis: Zur Verwaltung Klassenbezeichnung sollte in Moodle über

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

ein zusätzliches Profelfeld (Texteingabe bzw. Auswahlménú) mit der entsprechenden Bezeichnung angelegt werden.

4. Zeitgesteuerte Synchronisierung der LDAP-Nutzerkonten

- Melden Sie sich als Moodle Admin an.
- Wählen Sie über *Website-Administration* / *Server* / *Tasks* / *Geplante Vorgänge* den Eintrag Synchronisierung von LDAP-Nutzerkonten aus.



- Aktivieren Sie über das „Zahnrad“ den Task und speichern Sie anschließend die Änderung ab. Die restlichen Einstellungen können übernommen werden

Geplanten Vorgang bearbeiten: Synchronisierung von LDAP-Nutzerkonten

Letzte Ausführung
Nie

Nächste Ausführung
Vorgang deaktiviert

Minute

Stunde

Tag

Monat

Wochentag

Deaktiviert

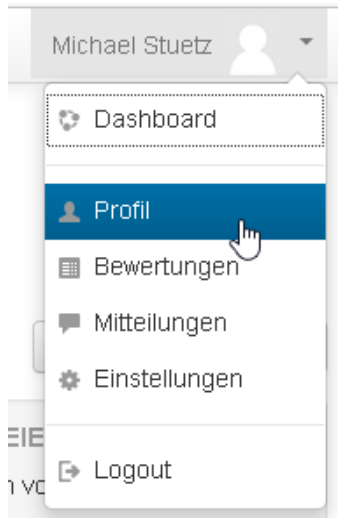
Um den Task zu aktivieren, muss das "Häkchen" entfernt werden.

Zeitplan dieses Vorgangs auf Standardwerte zurücksetzen

- Sobald der Task aktiviert wurden, werden die Benutzerdaten einmal am Tag um Mitternacht synchronisiert. Weitere Information zum Cron Job finden Sie unter <https://wiki.ubuntuusers.de/Cron/>

5. 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 - vom Benutzer geändert bzw. nicht geändert werden.



▼ Grundeinträge

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

