



Lernen Online
mit Moodle |
Vorarlberger
Bildungsservice

Moodle-Authentifizierung mit LDAPS



Besuchen Sie uns im Internet unter
<http://www.vobs.at/>

© Vorarlberger Bildungsservice 2009
Schulmediencenter des Landes Vorarlberg

6900 Bregenz, Römerstraße 15
Alle Rechte vorbehalten

Moodle -Authentifizierung

**Anbindung an das lokale LDAP-
Benutzerverzeichnis der Schule**

Inhalt

1.	Vorbemerkung.....	3
2.	LDAPS – Anbindung	3
2.1.	Zertifizierungsdienst	4
2.1.1.	Zertifizierungsdienst auf einem „Microsoft 2003 – Server“ nachinstallieren.....	4
2.1.2.	Zertifizierungsdienst auf einem „Microsoft 2008 – Server“ nachinstallieren.....	6
2.2.	„BindUser“ anlegen	10
2.3.	Portweiterleitung auf der Firewall einrichten	11
2.3.1.	Am Beispiel IP-COP: Eintrag für die Portweiterleitung:.....	11
2.3.2.	Am Beispiel IP-Fire: Eintrag für die Portweiterleitung:	11
2.4.	LDAP-Einstellungen auf der Moodleinstanz:	13
3.	Anhang – zusätzliche Informationen	15
3.1.	Zuordnung MS-AD Benutzerattribute – Moodle Profelfelder:	15
3.2.	ADModify	16
3.3.	LDAP-Browser	18

1. Vorbemerkung

Die Verknüpfung der Moodle-Benutzerauthentifizierung mit dem Benutzerverzeichnis der jeweiligen Schule (z.B. Microsoft Active Directory Service – ADS) ist eine elegante und für die/den IT-BetreuerIn ressourcenschonende Möglichkeit der Benutzerkonteneinbindung in die schuleigene Moodle-Instanz.

Vorteile:

- Es müssen keinerlei Benutzerdaten über Listen oder händische Eingaben in die Moodle-Plattform übertragen oder gepflegt werden. Jeder Benutzer, der im lokalen LAN der Schule über einen Benutzeraccount verfügt, kann sich mit den gleichen Daten (Benutzername und Kennwort) auch auf der Moodle-Instanz der jeweiligen Schule anmelden. Kommen am Schuljahresanfang Benutzer dazu, so können diese sich bei Moodle anmelden, sobald sie über einen Benutzeraccount an der Schule verfügen. Es gibt keine vergessenen Passwörter bzw. das damit einhergehende Prozedere der Kennwortrücksetzung durch den Administrator innerhalb der Moodleplattform.
- Die Benutzernamen sind automatisch standardisiert, eindeutig und leicht zuzuordnen.
- Bestimmten Gruppen bzw. OUs (z.B. LehrerInnen) kann vorab das Recht zur Kurserstellung zugeordnet werden
- Werden Benutzeraccounts im lokalen Benutzerverzeichnis (AD) der Schule gelöscht (z.B. SchülerInnen, die nicht mehr an der Schule sind), so wird damit diesen Usern auch automatisch die Möglichkeit zum Moodle-Login genommen.
- Die KurserstellerInnen (LehrerInnen) vergeben für ihre Kurse Passwörter. Am Unterrichtsbeginn loggen sich die SchülerInnen auf der Lernplattform ein, klicken auf den Kursbereich des Lehrers (oder eines Fachbereichs, oder ...) und dann auf den gewünschten Kurs. Es erfolgt die Abfrage nach dem vorher vergebenen Kurspasswort. Mit der einmaligen Eingabe dieses Passwortes sind die SchülerInnen somit automatisch für diesen Kurs eingeschrieben.
- Sollen Kurse für die ganze Schule zugänglich sein, so werden sie ohne Passwort angelegt.

Nachteile:

- Einmalig müssen einige Einstellungen gemacht werden (LDAP-Daten innerhalb der Moodleinstanz eingeben, Portweiterleitung auf der Firewall einrichten und eigenen „BindUser“ im AD bzw. LDAP anlegen), sowie (bei MS-Servern) unter Umständen der Microsoft-Zertifikatsdienst auf dem Domänencontroller nachinstalliert werden. Alles in allem im Normalfall bzw. bei standardisierten Installationen mit Hilfe dieser Anleitung in weniger als einer halben Stunde erledigt.
- Sollte der/die Domänencontroller der Schule ausfallen, so ist natürlich auch keine Anmeldung bei der Moodleplattform möglich. In diesem Fall dürfte Letzteres aber vermutlich das kleinere Problem sein ;-)

Relevante Geschwindigkeitsunterschiede im Vergleich zur moodleinternen Authentifizierung sind während der Test- und Pilotphasen keine zu Tage getreten.

Auch bezüglich Sicherheit stellen die Experten dieser Lösung ein gutes Zeugnis aus:

1. Auf der schuleigenen Firewall muss „nur“ der LDAPS-Port 636 geöffnet werden. Zusätzlich wird einzig und allein der IP-Adresse des Moodle-Servers Zugriff gewährt.
2. Sämtlicher, für die Authentifizierung notwendiger Datenverkehr wird verschlüsselt: LDAPS .

Natürlich können unabhängig von der Aktivierung der LDAP-Authentifizierung und den damit verknüpften Einstellungen Benutzerkonten über Listen importiert und angelegt werden.

2. LDAPS – Anbindung

Getestet wurde diese Anbindung bis dato auf Domänencontrollern mit den Betriebssystemen „Windows Server 2003“, „Windows Server 2008 R1/R2“ und „Windows Server 2012 R1/R2“. Es sollte aber in ähnlicher Form auch mit anderen Betriebssystemen möglich sein.

Weitere Infos dazu:

http://docs.moodle.org/en/LDAP_authentication

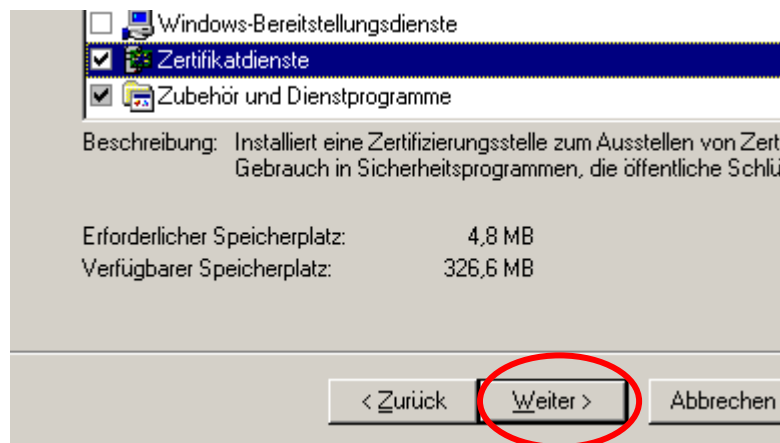
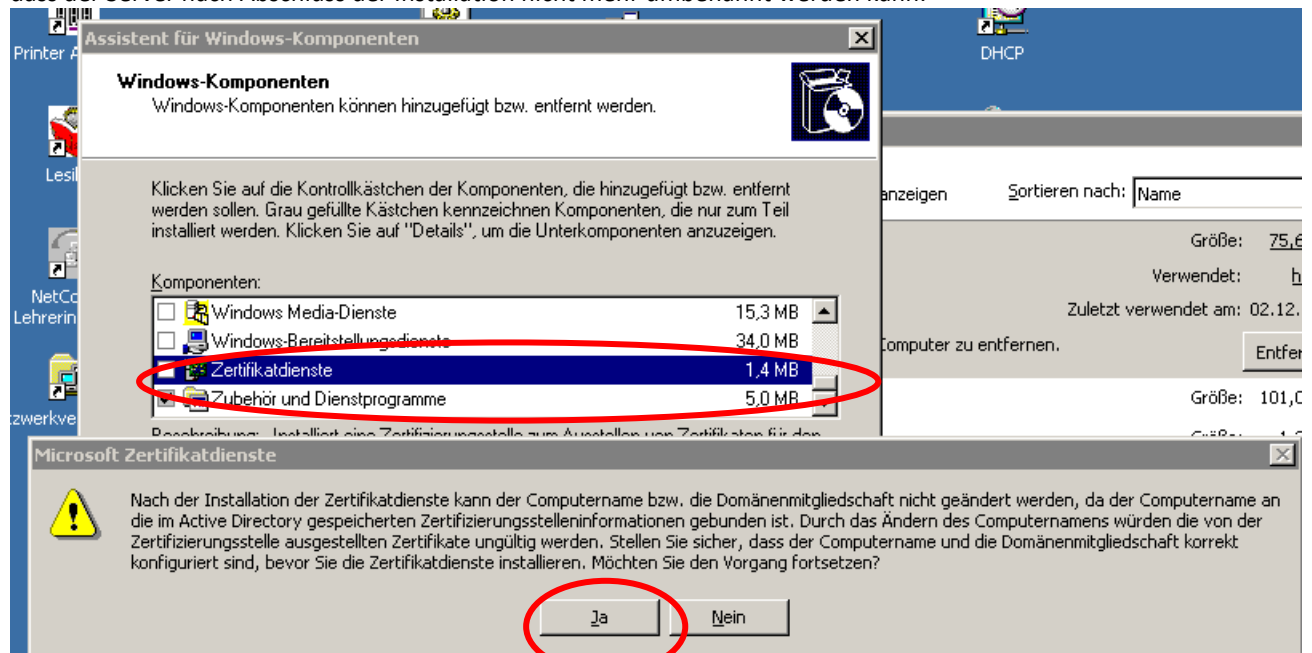
2.1. Zertifizierungsdienst

Hinweis: Im Normalfall wird dazu die MS-Server 2003 – Installations-CD benötigt (bzw. der Ordner „i386“ dieser CD)

Für MS-Server: Damit die LDAP-Authentifizierung auf SSL-Basis vom Microsoft-Server akzeptiert wird, muss auf dem MS-Server der Zertifizierungsdienst verfügbar sein werden

2.1.1. Zertifizierungsdienst auf einem „Microsoft 2003 – Server“ nachinstallieren

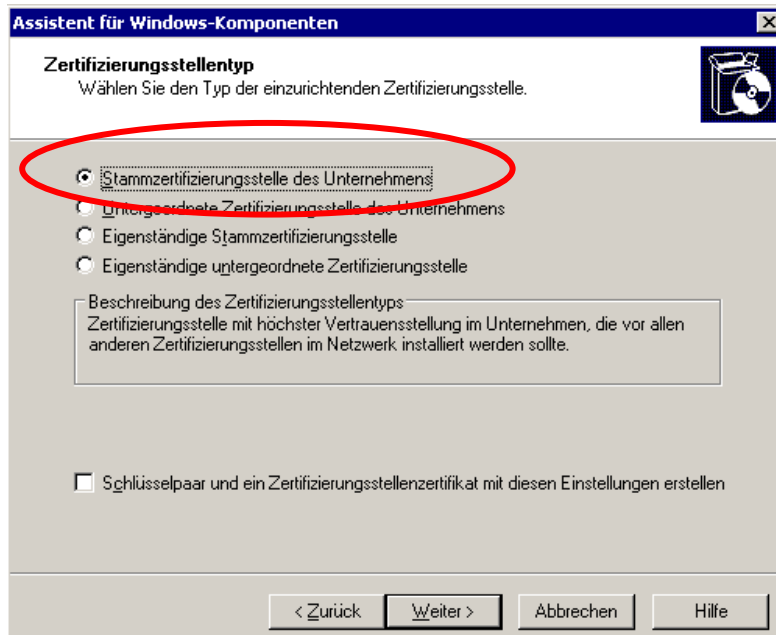
Auf dem Domänencontroller öffnen wir hierzu über Start -> Einstellungen -> Systemsteuerung -> Software den Menüpunkt *Windowskomponenten hinzufügen/entfernen* und wählen die *Zertifikatsdienste* aus. Es erscheint ein Hinweis, dass der Server nach Abschluss der Installation nicht mehr umbenannt werden kann.



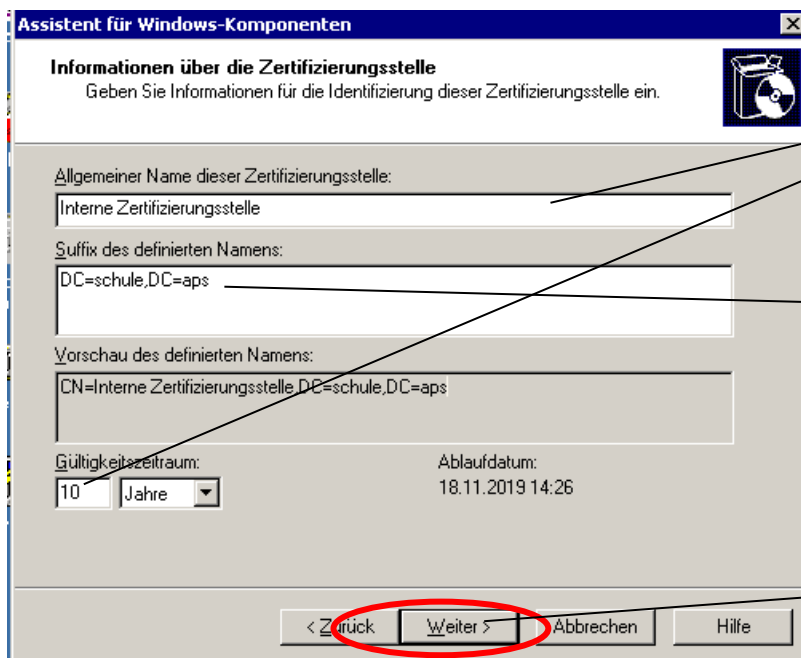
Die Microsoft Zertifikatsdienste unterstützen zwei Arten von Zertifizierungsstellen.

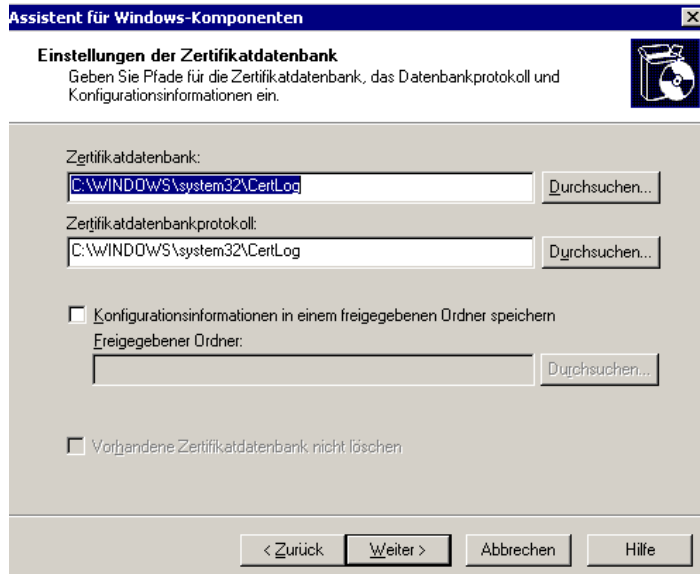
- Unternehmens Zertifizierungsstelle
- Alleinstehende Zertifizierungsstelle

Der grundsätzliche Unterschied besteht darin, dass die Unternehmens Zertifizierungsstelle in das Active Directory integriert ist und die Alleinstehende nicht. Wir entscheiden uns in unserer Anleitung für eine im Active Directory integrierte Stammzertifizierungsstelle.



Nun müssen Sie der Zertifizierungsstelle einen *Namen* geben, wir nennen diese *Interne Zertifizierungsstelle* und setzen den *Gültigkeitszeitraum* auf *10 Jahre* fest:





→ CD wird benötigt (oder Ordnerinhalte von „i386“ ...

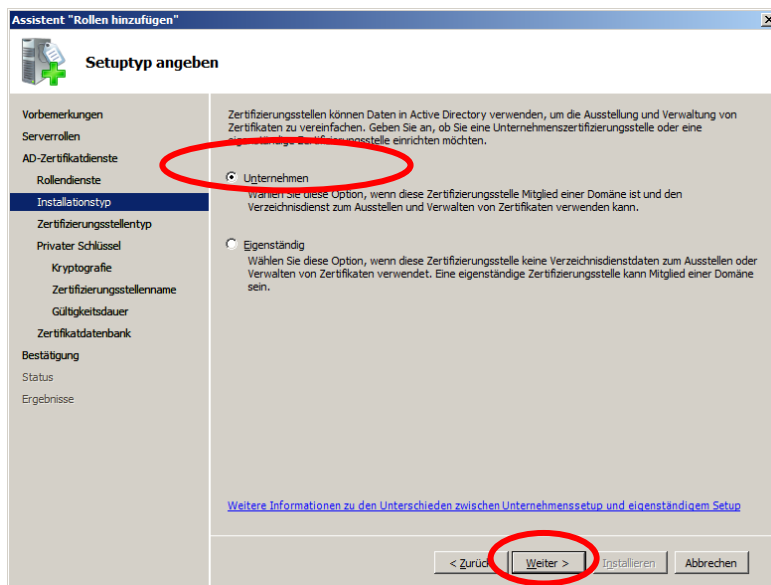
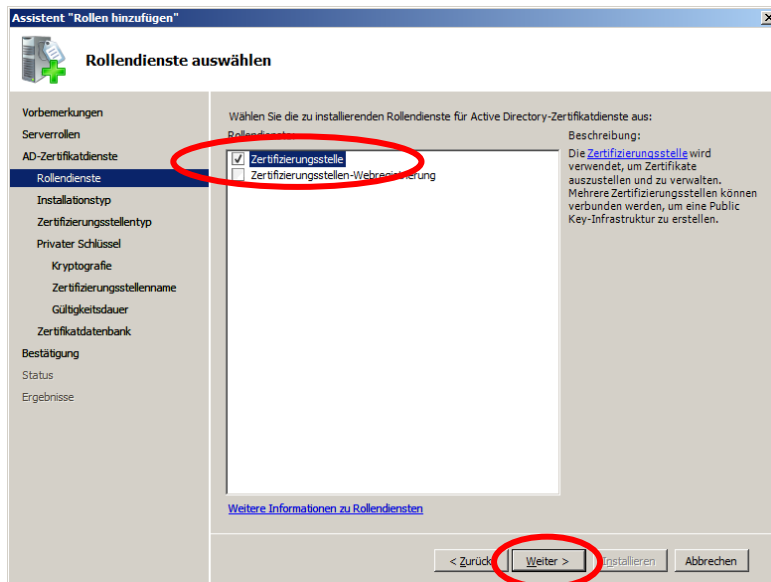
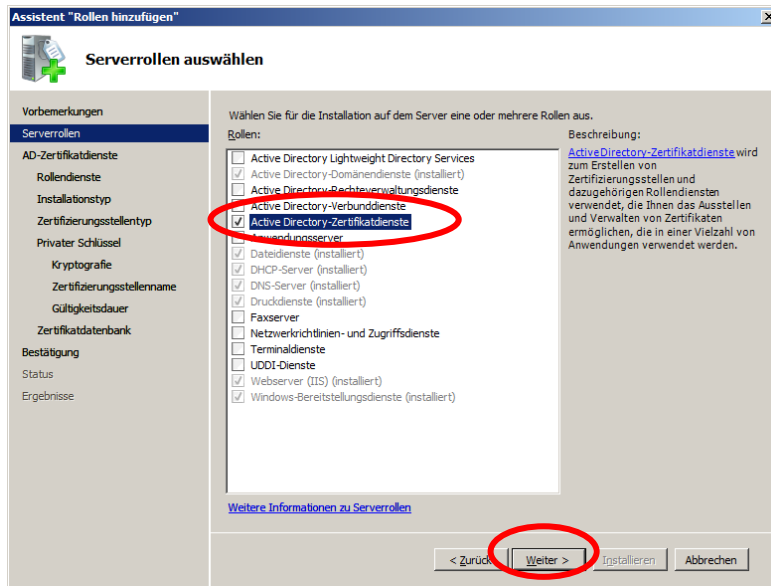


→ fertig!

2.1.2. Zertifizierungsdienst auf einem „Microsoft 2008 – Server“ nachinstallieren

Auf dem Domänencontroller wählen wir über den Server-Manager den Menüpunkt „Rollen“ und dann oben rechts die Option „Rollen hinzufügen“.





Assistent "Rollen hinzufügen"

Zertifizierungsstellentyp angeben

Vorbemerkungen
Serverrollen
AD-Zertifizierungsstelle
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstellename
Gültigkeitsdauer
Zertifikatsdatenbank
Bestätigung
Status
Ergebnisse

Sie können eine Kombination aus Stammzertifizierungsstellen und untergeordneten Zertifizierungsstellen konfigurieren, um eine hierarchische Public Key-Infrastruktur (PKI) zu erstellen. Eine Stammzertifizierungsstelle ist eine Zertifizierungsstelle, die eigene selbstsignierte Zertifikate ausstellt. Eine untergeordnete Zertifizierungsstelle empfängt Zertifikate von einer anderen Zertifizierungsstelle. Geben Sie an, ob Sie eine Stammzertifizierungsstelle oder eine untergeordnete Zertifizierungsstelle einrichten möchten.

☒ Stammzertifizierungsstelle
Wählen Sie diese Option, wenn Sie die erste oder einzige Zertifizierungsstelle in einer Public Key-Infrastruktur installieren.

☐ Untergeordnete Zertifizierungsstelle
Wählen Sie diese Option, wenn die Zertifizierungsstelle das Zertifizierungsstellenzertifikat von einer anderen übergeordneten Zertifizierungsstelle in einer Public Key-Infrastruktur erhält.

[Weitere Informationen zur Public Key-Infrastruktur](#)

< Zurück Weiter > Installieren Abbrechen

Assistent "Rollen hinzufügen"

Privaten Schlüssel einrichten

Vorbemerkungen
Serverrollen
AD-Zertifizierungsstelle
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstellename
Gültigkeitsdauer
Zertifikatsdatenbank
Bestätigung
Status
Ergebnisse

Die Zertifizierungsstelle benötigt einen privaten Schlüssel, um Zertifikate für Clients zu generieren und auszustellen. Geben Sie an, ob Sie einen neuen privaten Schlüssel erstellen oder einen vorhandenen Schlüssel verwenden möchten.

☒ Neuen privaten Schlüssel erstellen
Verwenden Sie diese Option, wenn Sie keinen privaten Schlüssel besitzen oder einen neuen privaten Schlüssel erstellen möchten, um die Sicherheit zu erhöhen. Sie werden aufgefordert, für den privaten Schlüssel einen Kryptografiedienstanbieter auszuwählen und eine Schlüssellänge anzugeben. Zum Ausstellen neuer Zertifikate müssen Sie zudem einen Hashalgorithmus auswählen.

☐ Vorhandenen privaten Schlüssel verwenden
Verwenden Sie diese Option, um beim erneuten Installieren einer Zertifizierungsstelle zuvor ausgestellte Zertifikate weiterverwenden zu können, um die Kontinuität zu gewährleisten.

☐ Zertifikat auswählen und dazugehörigen privaten Schlüssel verwenden
Wählen Sie diese Option, wenn auf diesem Computer ein Zertifikat vorhanden ist oder wenn Sie ein Zertifikat importieren und den dazugehörigen privaten Schlüssel verwenden möchten.

☐ Vorhandenen privaten Schlüssel auf diesem Computer auswählen
Wählen Sie diese Option, wenn Sie private Schlüssel von einer vorherigen Installation beibehalten haben oder einen privaten Schlüssel aus einer anderen Quelle verwenden möchten.

[Weitere Informationen zu öffentlichen und privaten Schlüsseln](#)

< Zurück Weiter > Installieren Abbrechen

Assistent "Rollen hinzufügen"

Kryptografie für ZS konfigurieren

Vorbemerkungen
Serverrollen
AD-Zertifizierungsstelle
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstellename
Gültigkeitsdauer
Zertifikatsdatenbank
Bestätigung
Status
Ergebnisse

Zum Erstellen eines neuen privaten Schlüssels müssen Sie zunächst einen **Kryptografiedienstanbieter**, einen **Hashalgorithmus** und eine Schlüssellänge auswählen, die für den beabsichtigten Zweck der von Ihnen ausgestellten Zertifikate geeignet sind. Ein höherer Wert für die Schlüssellänge verstärkt die Sicherheit, erhöht aber auch den Zeitaufwand zum Abschließen von Signaturvorgängen.

Wählen Sie einen Kryptografiedienstanbieter (CSP) aus: RSA#Microsoft Software Key Storage Provider Schlüssellänge: 2048

Wählen Sie den Hashalgorithmus zum Signieren von Zertifikaten aus, die von dieser Zertifizierungsstelle ausgestellt werden:

md4
md5
sha256
sha384

☐ Verstärkte Sicherheitsfeatures für den privaten Schlüssel verwenden, die vom Kryptografiedienstanbieter bereitgestellt werden (dies erfordert möglicherweise eine Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schlüssel)

[Weitere Informationen zu kryptografischen Optionen für eine Zertifizierungsstelle](#)

< Zurück Weiter > Installieren Abbrechen

Assistent "Rollen hinzufügen"

Name der Zertifizierungsstelle konfigurieren

Vorbemerkungen
Serverrollen
AD-Zertifizierungsstellen
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstellenname
Gültigkeitsdauer
Zertifikatsdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie einen allgemeinen Namen zur Identifizierung der Zertifizierungsstelle an. Dieser Name wird allen von der Zertifizierungsstelle ausgestellten Zertifikaten hinzugefügt. Die Werte für das DN-Suffix werden automatisch generiert, können jedoch geändert werden.

Allgemeiner Name dieser Zertifizierungsstelle:

Suffix des definierten Namens:

Vorschau des definierten Namens:
CN=Interne Zertifizierungsstelle,DC=schule,DC=aps

[Weitere Informationen zum Konfigurieren eines Zertifizierungsstellennamens](#)

< Zurück **Weiter >** Installieren Abbrechen

Assistent "Rollen hinzufügen"

Festlegen der Gültigkeitsdauer

Vorbemerkungen
Serverrollen
AD-Zertifizierungsstellen
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstellenname
Gültigkeitsdauer
Zertifikatsdatenbank
Bestätigung
Status
Ergebnisse

Ein Zertifikat wird an diese Zertifizierungsstelle ausgestellt, um die Kommunikation mit anderen Zertifizierungsstellen und mit Clients, die Zertifikate anfordern, zu sichern. Die Gültigkeitsdauer eines Zertifizierungsstellenzertifikats kann von einer Reihe von Faktoren abhängen, beispielsweise dem beabsichtigten Zweck der Zertifizierungsstelle und den Sicherheitsmaßnahmen, die Sie zum Schutz dieser Zertifizierungsstelle getroffen haben.

Wählen Sie die Gültigkeitsdauer für das für diese Zertifizierungsstelle generierte Zertifikat aus:
 Jahre

Abgabedatum der Zertifizierungsstelle: 20.11.2019 13:40

Beachten Sie, dass die von der Zertifizierungsstelle ausgestellten Zertifikate nur bis zu diesem Ablaufdatum gültig sind.

[Weitere Informationen zum Festlegen der Zertifikatsgültigkeitsdauer](#)

< Zurück **Weiter >** Installieren Abbrechen

Assistent "Rollen hinzufügen"

Zertifikatsdatenbank konfigurieren

Vorbemerkungen
Serverrollen
AD-Zertifizierungsstellen
Rollendienste
Installationstyp
Zertifizierungsstellentyp
Privater Schlüssel
Kryptografie
Zertifizierungsstellenname
Gültigkeitsdauer
Zertifikatsdatenbank
Bestätigung
Status
Ergebnisse

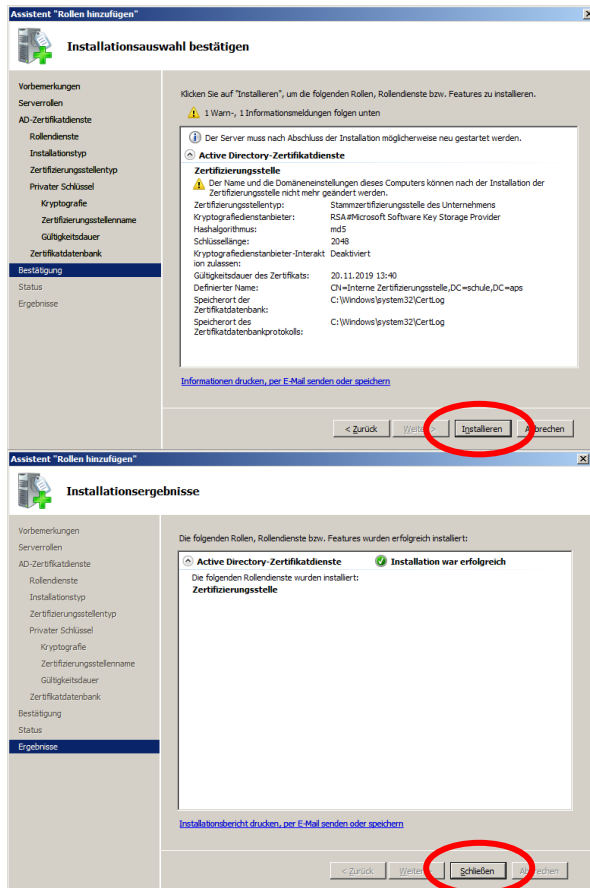
In der Zertifikatsdatenbank werden alle Zertifikatanforderungen, ausgestellte Zertifikate sowie gesperrte oder abgelaufene Zertifikate aufgezeichnet. Mit dem Datenbankprotokoll kann die Verwaltungsaktivität für eine Zertifizierungsstelle überwacht werden.

Speicherort der Zertifikatsdatenbank:

☐ Vorhandene Zertifikatsdatenbank aus vorheriger Installation an diesem Speicherort verwenden

Speicherort des Zertifikatsdatenbankprotokolls:

< Zurück **Weiter >** Installieren Abbrechen



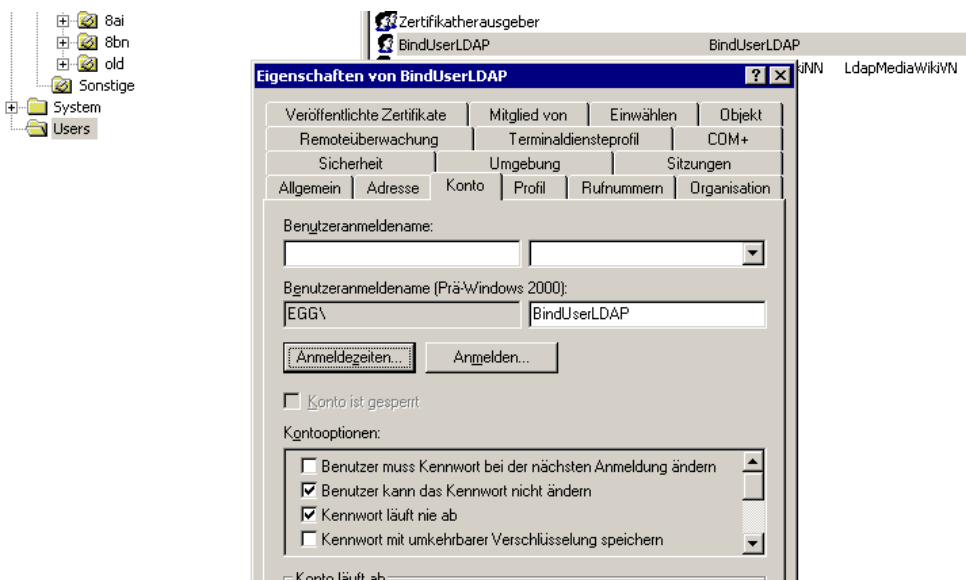
→ fertig!

Eventuell ist noch ein Neustart des Servers notwendig (Ereignisprotokollierung zum „Active Directory-Zertifikatsdienst“ beachten).

Analog dazu funktioniert die Einrichtung auf einem „Windows Server 2012“!

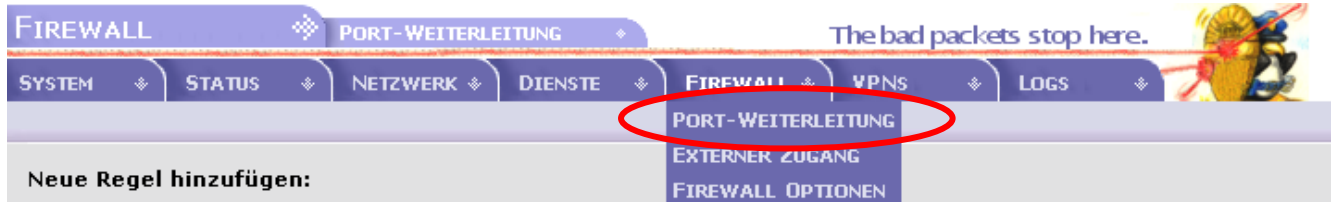
2.2. „BindUser“ anlegen

Um der Moodle-Instanz Leserechte für das lokale Benutzerverzeichnis (AD) gewähren zu können, muss ein User mit entsprechenden Rechten angelegt werden. Dazu wird im AD ein Benutzer mit Namen „BindUserLDAP“ und starkem Passwort angelegt. Es reicht, wenn dieser Benutzer Mitglied der Gruppe „Domänen-Benutzer“ ist (= Standard):



2.3. Portweiterleitung auf der Firewall einrichten

2.3.1. Am Beispiel IP-COP: Eintrag für die Portweiterleitung:



Neue Regel hinzufügen:

Protokoll: **TCP** Alias-IP-Adresse: **DEFAULT IP** Quell-Port: **636**

Ziel-IP-Adresse: **192.168.100.200** Ziel-Port: **636**

Anmerkung: **LDAPS vom Moodleserver VOBS** Aktiviert: ☒

Quell-IP, oder Netzwerk (leer für "ALL"): **193.171.140.14**

☒ Dieses Feld kann leer bleiben.

Hinzufügen **Zurücksetzen**

LDAPS-Port

IP-Adresse des Domänencontrollers

Text frei wählbar

IP-Adresse des VOBS-Moodleservers- neuer Server 2015: **193.171.140.14**

Ergebnis:

TCP	DEFAULT IP : 636(LDAPS)	192.168.100.200 : 636(LDAPS)	LDAPS vom Moodleserver VOBS	<input checked="" type="checkbox"/>		
Zugriff erlaubt von: 193.171.140.2 (LDAPS vom Moodleserver VOBS)				<input checked="" type="checkbox"/>		

fertig!

2.3.2. Am Beispiel IP-Fire: Eintrag für die Portweiterleitung:



Neue Regel erstellen

Firewallregeln

Quelle

☒ Quelladresse (IP/MAC-Adresse oder Netzwerk): 193.171.140.14

☐ Firewall: Alle

☐ Standard-Netzwerke: Alle

NAT

☒ Network Address Translation (NAT) benutzen

☒ Destination-NAT (Port-Weiterleitung)

☐ Source-NAT

Firewall-Interface: ROT (193.170.42.210)

Neue Quell-IP-Adresse: GRÜN (192.168.100.254)

Ziel

☒ Zieladresse (IP-Adresse oder Netzwerk): 192.168.100.200

☐ Firewall: Alle

☐ Standard-Netzwerke: Alle

Protokoll

☒ TCP

Quellport:

Zielport: 636

Externer Port (NAT):

Weitere Einstellungen

Anmerkung: LDAPS vom MoodleserverNeu Land

Regelposition:

☐ Logging aktivieren

☐ Zeitrahmen hinzufügen

Hinzufügen

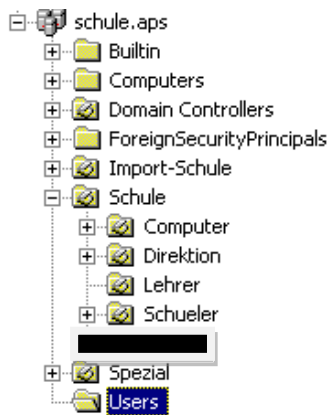
Zurück

Ergebnis:

5	TCP	193.171.140.14	<input type="checkbox"/>	Firewall (ROT): 636 ->192.168.100.200: 636	<input checked="" type="checkbox"/>				
		LDAPS vom MoodleserverNeu Land							

2.4. LDAP-Einstellungen auf der Moodleinstanz:

Als Moodle-Admin auf der schuleigenen Moodle-Instanz einloggen: Nutzer/innen – Authentifizierung – LDAP-Server



exemplarischer Screenshot vom MS-AD –
passend zu den Einstellungen unten

LDAP Server-Einstellungen

Host URL: Geben Sie die Host URL des LDAP-Servers an.
 Version: Diese Version des LDAP-Protokolls wird verwendet.
 LDAP Codierung: Geben Sie die LDAP Codierung an.

Bind-Einstellungen

Kennwörter verbergen: Wählen Sie, ob die Kennwörter im Klartext eingegeben werden sollen.
 Gekennzeichneter Name: Möchten Sie einen bestimmten Benutzer für die Bindung angeben?
 Kennwort: Passwort des Benutzers.

Einstellung zur Nutzerüberprüfung (user lookup settings)

Nutzertyp: Auswahl, Ablauf, Gruppen etc.
 Kontexte: Liste der Umgebungen.
 Subkontexte suchen: Legt fest, ob Subkontexte gesucht werden.
 Alias berücksichtigen: Legt fest, ob Alias berücksichtigt werden.
 Nutzerattribut: Verwenden Sie ein bestimmtes Attribut.
 Mitgliedsattribut: Geben Sie ein Mitgliedsattribut an.
 Mitgliedsattribut nutzt dn: Optional: Mitgliedsattribut nutzt dn.
 Objekt Class: Filter für die Objekt Class.

Protokoll + öffentliche IP-Adresse der Firewall (des IP-Cop) + Port:
ldaps://193.170.42.210:636

Bind-User Anbindung:
CN=BindUserLDAP,CN=Users,DC=schule,DC=aps
In diesem Fall hat der Bind-User den Namen „BindUserLDAP“ (=CN) und befindet sich im AD im Container (=CN) „Users“; Der Domänenname lautet „schule.aps“ (DC=schule, DC=aps)

Kennwort des Users „BindUserLDAP“

„Wo soll nach berechtigten Benutzern gesucht werden?“
OU=Schule,DC=schule,DC=aps
In diesem Fall in der Organisationseinheit „Schule“ (=OU) und den darunter liegenden OUs.

Der Domänenname lautet „schule.aps“ (DC=schule, DC=aps)

Welches Nutzerattribut soll als Loginname Verwendung finden?
sAMAccountName oder cn oder ... → siehe Anhang

Weiter geht's mit den Einstellungen für die KursverwalterInnen:

Kursverwalter/in

Kursverwalter/innen

Kursverwalterrechte bekommen in diesem Falle automatisch alle User, die sich in der OU „Lehrer“ befinden. Diese OU „Lehrer“ ist Teil der übergeordneten OU „Schule“.

OU=Lehrer,OU=Schule,DC=schule,DC=aps

Somit fehlt nur noch das „Data-Mapping“: Beim ersten Login jedes Users werden hier definierte Daten vom lokalen Benutzerverzeichnis (=AD) übernommen und die entsprechenden Profelfelder in der Moodle-Benutzerumgebung befüllt. Hinweis: Die Passwörter werden nicht in der Moodle-Datenbank gespeichert. Bei jedem Login erfolgt die Authentifizierung über das lokale LDAP-Verzeichnis der Schule.

Data mapping

Vorname	<input type="text" value="givenName"/>	Diese f
	Update lokaler Daten	Moodle
	<input type="button" value="Beim Anlegen"/>	LDAP-I
	Update externer Daten	spezif
	<input type="button" value="Nie"/>	
	Sperrwert	Wenn (
	<input type="button" value="Bearbeitbar wenn Feld leer"/>	nichts
		Voreins
Nachname	<input type="text" value="sn"/>	
	Update lokaler Daten	In jeder
	<input type="button" value="Beim Anlegen"/>	editiere
	Update externer Daten	haben.
	<input type="button" value="Nie"/>	
	Sperrwert	Update
	<input type="button" value="Bearbeitbar wenn Feld leer"/>	aktivier
		Quelle
E-Mail-Adresse	<input type="text" value="mail"/>	wenn d
	Update lokaler Daten	Nutzer:
	<input type="button" value="Beim Anlegen"/>	die lok
	Update externer Daten	geschü
	<input type="button" value="Nie"/>	
	Sperrwert	Sperrv
	<input type="button" value="Bearbeitbar"/>	aktivier
		des Fe
Stadt/Ort	<input type="text" value="l"/>	Admini
	Update lokaler Daten	die Dat
	<input type="button" value="Beim Anlegen"/>	gepfleg
	Update externer Daten	Update
	<input type="button" value="Nie"/>	Einstel
	Sperrwert	Authen
	<input type="button" value="Bearbeitbar"/>	Nutzer:

givenName

sn

mail

Hinweis: Ist das Feld im AD belegt, so wird der Wert übernommen, ansonsten muss die Emailadresse beim 1. Login angegeben werden

l (kleines „L“ - Abkürzung für „location“)

Hinweis: Ist das Feld im AD belegt, so wird der Wert übernommen, ansonsten muss der Ort beim 1. Login angegeben werden

Die Belegung dieser 4 Datenfelder wird von der Moodle-Benutzerverwaltung zwingend verlangt. Können diese Daten nicht vollständig aus dem lokalen LDAP-Verzeichnis übernommen werden, so muss der/die Benutzerin dies beim ersten Login nachholen.

Für die KurserstellerInnen (= im Normalfall die „LehrerInnen“) verlangt Moodle zusätzlich das Belegen des Benutzerprofilfeldes „Beschreibung“. Auch das könnte man aus dem AD übernehmen (= Feld Beschreibung – description):

The screenshot shows the 'Eigenschaften von Thomas Muster' window. The 'Beschreibung' field is highlighted with a red circle and contains the text 'description'. Below it are buttons for 'Update lokaler Daten', 'Update externer Daten', and 'Sperrwert', each with a dropdown menu.

Wie oben gilt: Können diese Daten nicht aus dem lokalen LDAP-Verzeichnis übernommen werden (z.B. weil dieses Feld im MS-AD leer ist), so muss der/die BenutzerIn dies beim ersten Login nachholen.

3. Anhang – zusätzliche Informationen

3.1. Zuordnung MS-AD Benutzerattribute – Moodle Profelfelder:

The screenshot shows the 'Eigenschaften von Thomas Muster' window. The 'Benutzeranmeldename' field is highlighted with a red box and contains 'thomas.muster' and '@schule.aps'. Below it is the 'Benutzeranmeldename (für Windows 2000)' field with 'SCHULE\' and 'thomas.muster'.

userPrincipalName

sAMAccountName

The screenshot shows the 'Eigenschaften von Thomas Muster' window. The 'Straße' field is highlighted with a red box and contains a small 'L' character.

l (= kleines „L“)

The screenshot shows the 'Eigenschaften von Thomas Muster' window. The 'Vorname' field is highlighted with a red box and contains 'Thomas' and 'Muster'. Below it are fields for 'Nachname', 'Anzeigename', 'Beschreibung', 'Büro', 'Rufnummer', 'E-Mail', and 'Webseite'.

givenname

sn

cn

description

mail

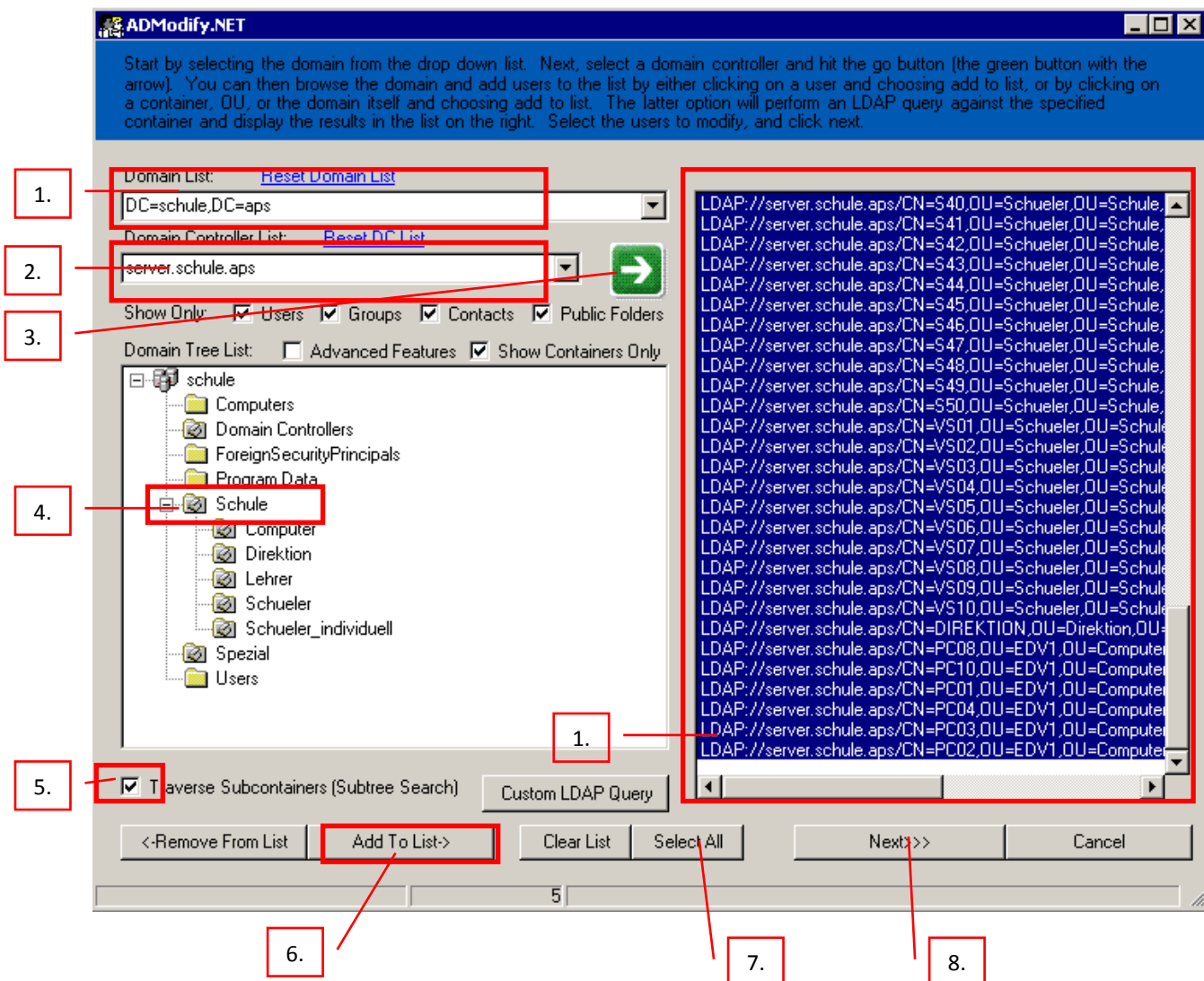
3.2. ADModify

Ein hilfreiches Tool, um umfangreiche Änderungen im Active Directory vorzunehmen.

Damit können über eine grafische Benutzeroberfläche bei beliebig vielen Benutzern gemeinsam nachträglich AD-Felder mit Daten belegt werden (z.B. bei allen Usern den Schulort im Datenfeld „Ort“ und die Emailadresse nach dem Muster benutzerloginname@schulkürzel.snv.at nachträglich eintragen).

Wird das gemacht, so muss kein User beim Moodle-Login für die Profilerstellung zusätzliche Angaben machen. Außerdem kann so in Kombination mit dem Mailserver mail.vobs.at erreicht werden, dass valide Emailadressen bei allen Benutzern hinterlegt sind.

Beispiel 1: Bei allen AD-Usern soll nachträglich die Emailadresse (im Format benutzerloginname@borge.snv.at und der Schulort (im Datenfeld Adresse – Ort) eingetragen werden.



ADModify.NET - General tab

Type the word null into a field to clear an attribute.

E-mail Address: %sAMAccountName%@borge.snv.at

Buttons: Go!, Cancel

ADModify.NET - Environment tab

City: Eggl

Buttons: Go!, Cancel

Beispiel 2: Die Benutzergruppe in der OU „Lehrer“ soll zusätzlich die Beschreibung „Lehrer“ erhalten:

ADModify.NET - Main Window

1. Domain List: **DC=schule,DC=aps**

2. Domain Controller List: **server.schule.aps**

3. Show Only: ☒ Users ☒ Groups ☒ Contacts ☒ Public Folders

4. Domain Tree List: **Lehrer**

5. ☒ Traverse Subcontainers (Subtree Search)

6. **Add To List->**

7. **Select All**

8. **Next>>**

LDAP://CN=Thomas Muster,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=grpLehrer,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=lt1,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=lt3,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=ruthilde,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=josef,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=erika,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=monika,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=gerlinde,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=gerda,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=margit,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=andrea,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=herlinde,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=annelies,OU=Lehrer,OU=Schule,DC=schule,DC=aps
 LDAP://CN=ggLehrerADAM,OU=Lehrer,OU=Schule,DC=schule,DC=aps

ADModify.NET

Mailbox Rights | Environment | Sessions | Terminal Services Profile

Remote Control | Member Of | Dialin | Custom | Exchange Features | Exchange General

General | Address | Account | Profile | Telephones | Organization | E-Mail Addresses

Type the word null into a field to clear an attribute.

☐ First Name

☐ Middle Initial

☐ Last Name

☐ Display Name [LastName.FirstName](#) [FirstName.LastName](#)

☒ Description **Lehrei**

☐ Office

☐ Telephone Number

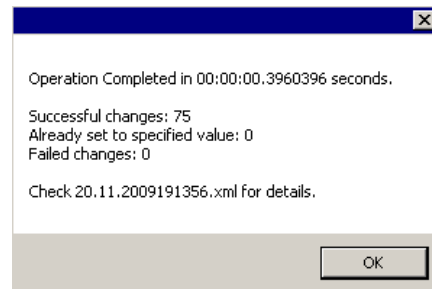
☐ E-mail Address

☐ Web Page

☐ Change CN (RDN) [LastName.FirstName](#) [FirstName.LastName](#)

Go! Cancel

Terminal Server and CDOEXM Modifications Disabled. See help for details.



Achtung: Das Tool ist sehr mächtig! Ein sehr sensibler Umgang damit ist angebracht ;-)

Download über den VoBS: ftp://ftp.vobs.at/admodify_2.1.zip

Entpacken + starten (keine Installation notwendig).

3.3. LDAP-Browser

Als Troubleshooting-Tool im Bereich LDAP-Anbindung empfiehlt sich der Einsatz des Freeware-Programmes „LDAP Browser 2.6“ von der Firma „Softerra“:

<http://www.softerra.com/download.htm>

Außerdem empfiehlt es sich, dass bei Problemen zuerst ldap ohne ssl versucht wird, dann kann die Fehlerursache besser identifiziert werden. Sollte es ohne die „Secure-Variante“ funktionieren, dann liegt der Fehler vermutlich beim Zertifikatsdienst auf dem Server.

Einstellungen (nur für den Testbetrieb) ldap (ohne „s“):

1. In Moodle bei den LDAP Servereinstellungen statt:

LDAP Server-Einstellungen

Host URL **ldaps://80.120.104.120:636**

Andere Host URL: ldap://80.120.104.120:389 → „s“ bei „ldap“ fehlt und anderer Port

2. Bei den Firewall-Einstellungen ebenfalls den Port auf „389“ statt „636“ stellen:

8	TCP	193.171.140.14	<input type="checkbox"/>	Firewall (ROT): 389 ->192.168.1.200: 389	<input checked="" type="checkbox"/>					
LDAP vom MoodleserverNeu Land - Test										