

Lehrerinnenfortbildung Baden-Württemberg



ZSL

LDAPS Authentifizierung mit der paedML Windows

Am Beispiel Moodle

paedML Windows 3.x/4x

Wiesler, Kink, Mayer

11.05.2020

Lizenz: CC BY-SA 4.0

<https://creativecommons.org/licenses/by-sa/4.0/>

Inhaltsverzeichnis

0. Informationen zum Dokument.....	3
1. Einführung und Übersicht.....	4
2. Portweiterleitungen einrichten.....	4
2.1. Portöffnung Router (Belwue).....	4
2.2. Portweiterleitung Octogate.....	5
3. LDAP-Benutzer einrichten.....	6
4. Zertifikat auf DC01 importieren.....	7
5. Konfiguration des externen Dienstes am Beispiel Moodle.....	11
5.1. Vorüberlegung Verwendung E-Mails in Moodle.....	11
5.2. LDAP-Zugriff aktivieren.....	12
5.3. LDAP-Zugriff konfigurieren.....	12
5.3.1. Einstellungen prüfen.....	16
5.3.2. Optional: Neue Profildfelder anlegen.....	16
5.4. E-Mail-Adressen @blackhole.belwue.de per Skript erstellen.....	18

o. Informationen zum Dokument

Titel	LDAPS Authentifizierung mit der paedML Windows
Untertitel	Am Beispiel Moodle
Bereich	paedML Windows 3.x/4x
Autor	Daniel Wiesler, Stefan Kink, Andreas Mayer
Datum	11.05.2020
Lizenz	CC BY-SA 4.0

I. Einführung und Übersicht

Das Lightweight Directory Access Protocol (LDAP) ermöglicht es, dass Anwendungen außerhalb des Schulnetzes wie z.B. Moodle oder WebUntis auf die Benutzerdatenbank der paedML Windows zugreifen können. LDAPS bezeichnet die verschlüsselte Form der Datenübertragung.

Die bietet zwei große Vorteile:

- Sie müssen Moodle oder WebUntis keine Benutzer anlegen oder pflegen.
- Die Benutzer können sich mit den selben Anmeldedaten wie im Schulnetz anmelden.

Nachteil der LDAP Authentifizierung ist, dass die Authentifizierung beim externen Dienst nur möglich ist, wenn der Server der paedML über das Internet zu erreichen ist.

Für das Abarbeiten dieser Anleitung benötigen Sie den externen Namen der Octogate Ihres Schulnetzes. Diesen finden Sie auf der WebGUI der Octogate.

Zur Einrichtung eines Zugriffs von außen per LDAPS, sind in der paedML 3.x bzw. 4.x mehrere Schritte erforderlich:

1. Portweiterleitungen im Router und in der Octogate einrichten
2. LDAP-Benutzer zur Kommunikation mit externem Service (z.B. Moodle) anlegen
3. Zertifikatsimport auf DC01.
4. Konfiguration des externen Dienstes (z.B. Moodle): LDAP Authentifizierung aktivieren und als Standard definieren

2. Portweiterleitungen einrichten

Nehmen wir an, Sie haben die LDAPS Authentifizierung für den Moodle Auftritt Ihrer Schule eingerichtet. Was passiert denn da bei der Anmeldung im Hintergrund?

Eine Lehrer gibt bei Moodle seine Benutzerdaten ein. In Ihrem Moodle ist die externe IP Ihrer Octogate eingetragen, zusammen mit dem Port, über den die Anfrage ausgeführt wird.

2.1. Portöffnung Router (Belwue)

Als erstes trifft die Authentifizierungsanfrage auf den Router. Wir gehen hier von der Verwendung eines Routers von Belwue aus.

Als Belwuekunde stehen Ihnen mehrere öffentliche IP Adressen zur Verfügung. Eine davon verwenden Sie für die externe Netzwerkkarte der Octogate. Nehmen wir an, diese lautet 141.10.99.199. Für diese IP Adresse muss ein Port für die LDAPS Authentifizierung geöffnet werden. Dies müssen Sie bei Belwue beantragen. Hierzu gibt es verschiedene Möglichkeiten.

- Sie verwenden den Standardport 636.
- Sie verwenden einen beliebigen Port, der vom Standard abweicht und dadurch die Sicherheit erhöht. Wir verwenden als Beispiel Port 45001.
- Sie haben den Zugriff auf die Sharepoint Freigaben bereits eingerichtet. Wenn Sie dies nach

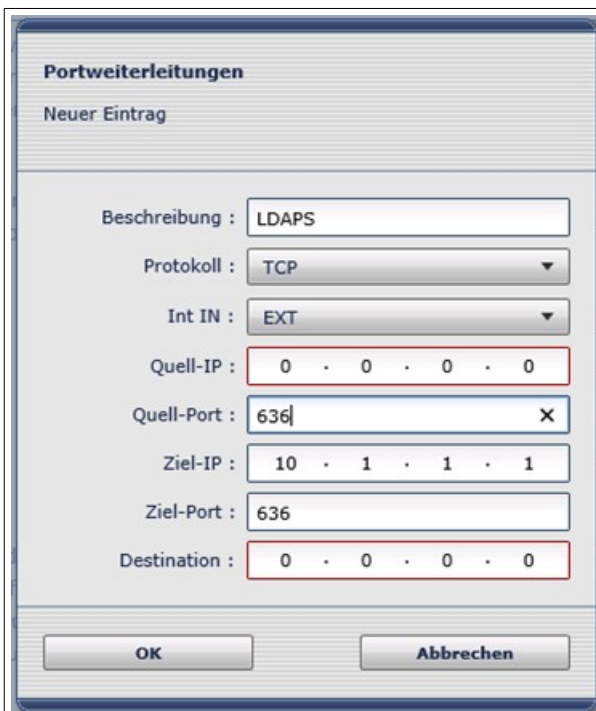
den Angaben des Installationshandbuchs für die paedML Windows 3 veranlasst haben, sind die Ports 3000 bis 3010 bereits geöffnet. Für den Zugriff auf die Sharepoint Freigaben werden derzeit die Ports 3000 bis 3003 verwendet. Sie können also einen der freien Ports für die LDAPS-Anbindung verwenden. Dies erhöht zudem noch die Sicherheit, da die externen Anfragen nicht auf dem Standardport erfolgen. Wir verwenden im Beispiel 3005.

2.2. Portweiterleitung Octogate

Je nachdem, welchen Port Sie im vorigen Kapitel gewählt haben, kommt die Anfrage nun auf Port 636, 45001 oder 3005 zur Octogate. Die Octogate soll diese Anfrage an den DC01 weiterleiten. Dort muss diese auf Port 636 ankommen.

Dazu müssen Sie eine Portweiterleitung in der Firewall einrichten.

1. Öffnen Sie die Octogate Weboberfläche und melden Sie sich als `admin` an.
2. Wählen Sie *Firewall | Portweiterleitungen*. Im rechten Fenster wählen Sie *Neuer Eintrag*.
3. Im neuen Fenster nehmen Sie folgende Eintragung vor:



Erklärung der Einstellungen

- Beschreibung: Können Sie selbst wählen.
- Protokoll: Belassen Sie auf *TCP*.
- Int IN: *EXT*: Die Anfrage kommt von außen auf das externe Interface der Octogate.
- Quell-IP: `0 . 0 . 0 . 0` bedeutet, dass die Anfrage von überall kommen kann. Hier können Sie – falls bekannt – die IP des Webservers eintragen.
Für Moodle wird als Einstellung `129 . 143 . 0 . 0` empfohlen.
- Quell-Port: je nach Auswahl `636`; `45001` oder `3005`
- Ziel-IP: `10 . 1 . 1 . 1` Die Anfrage soll an den DC01 weitergeleitet werden.
- Ziel-Port: `636`, Port für LDAPS für DC01

Hinweis: Da es sich bei dieser Portweiterleitung um eine Öffnung des Systems handelt, sollten Sie diese, wenn möglich, nicht für beliebige IP-Adressen (`0.0.0.0`) zulassen. Aus Sicherheitsgründen sollten Sie dies auf Ihnen bekannte IP-Adressen der Server, welche die Abfrage durchführen, einschränken. Hinweise für Moodle erhalten Sie dazu bei Belwue:

<https://www.belwue.de/support/faq/webdienste10/allgemein0.html> Sollten Sie nur Moodle nutzen, so können Sie beispielsweise mit dem Eintrag `129.143.0.0` bei Quell-IP sämtlichen Belwue-Servern den Zugriff gestatten.

3. LDAP-Benutzer einrichten

Die Authentifizierungsanfrage von Moodle möchte auf das Active Directory (AD) zugreifen um zu prüfen, ob die Anmeldedaten des Benutzers stimmen. Hierfür könnte man jeden beliebigen Benutzer verwenden. In der Praxis verwendet man hierzu einen speziell hierfür eingerichteten Benutzer.

In der paedML existiert in der OU `_ServiceAccounts` schon ein Benutzer `ldapbinduser`, dessen Kennwort jedoch nicht bekannt ist. Lassen Sie diesen unbedingt unverändert, denn mit diesem Benutzer greift die Firewall Octogate auf das AD zu. Richten Sie daher einen zusätzlichen Benutzer ein. Der alleinige Zweck dieses Benutzers ist die Kommunikation einer externen Quelle über das LDAPS Protokoll mit dem AD.

1. Starten Sie zu diesem Zweck die AD-Verwaltung auf dem Server DC01.



2. Gehen Sie in die OU `_ServiceAccounts`.
3. Legen Sie einen neuen Benutzer an: *Rechtsklick ins rechte Fenster | Neu | Benutzer* und nehmen Sie die Einstellungen der Abbildungen vor:

Neues Objekt - Benutzer

Erstellen in: `usterschule.schule.paedml/_ServiceAccounts`

Vorname: Initialen:

Nachname:

Vollständiger Name:

Benutzeranmeldename: @musterschule.schule.paedml

Benutzeranmeldename (Prä-Windows 2000):

Neues Objekt - Benutzer

Erstellen in: `musterschule.schule.paedml/_ServiceAccount`

Kennwort:

Kennwort bestätigen:

Benutzer muss Kennwort bei der nächsten Anmeldung ändern
 Benutzer kann Kennwort nicht ändern
 Kennwort läuft nie ab
 Konto ist deaktiviert

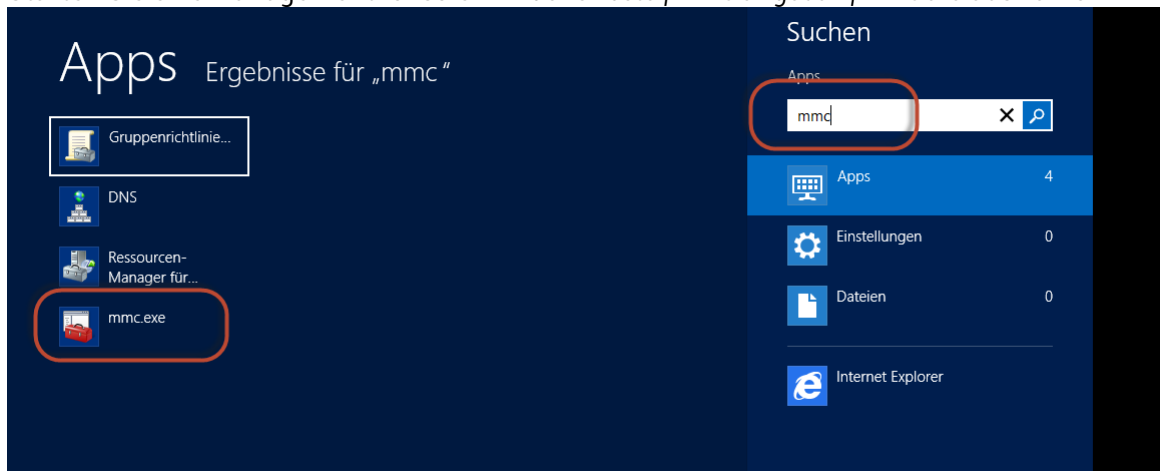
- Benutzername: `ldapbinduser_extem`
- Vergeben Sie keinen Vornamen. **WICHTIG:** vollständiger Name, Nachname und Benutzername sollten gleich sein. Unsere Tests haben ergeben, dass es hier zur Problemen kommen kann, sollte dies nicht der Fall sein.
- Vergeben Sie ein sehr sicheres Passwort und aktivieren Sie die beiden Optionen. Beenden Sie dann den Assistenten ohne weitere Änderungen.

4. Zertifikat auf DC01 importieren

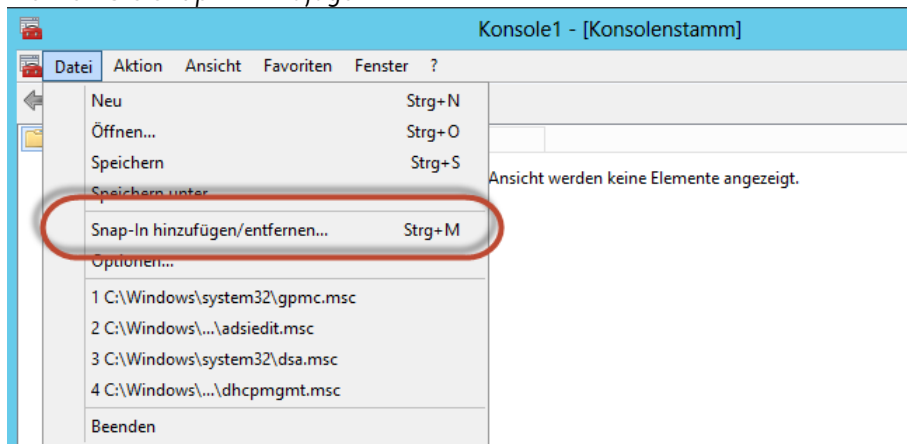
Damit der Datenverkehr bei der LDAPS Authentifizierung sicher und vertraulich stattfindet, muss auf DC01 noch ein SSL Zertifikat installiert werden. Octogate stellt uns ein LDAPS Zertifikat (im Ordner D:\Octogate\ldaps auf SP01) zur Verfügung, welches allerdings nur selbst-signiert ist. Alternativ dazu verwenden wir jenes gültige, extern signierte Zertifikat, das auch für den Zugriff auf die MySites von außen genutzt wird.

Folgen Sie den hier dargestellten Schritten. Sie arbeiten als Domänenadministrator am DC01.

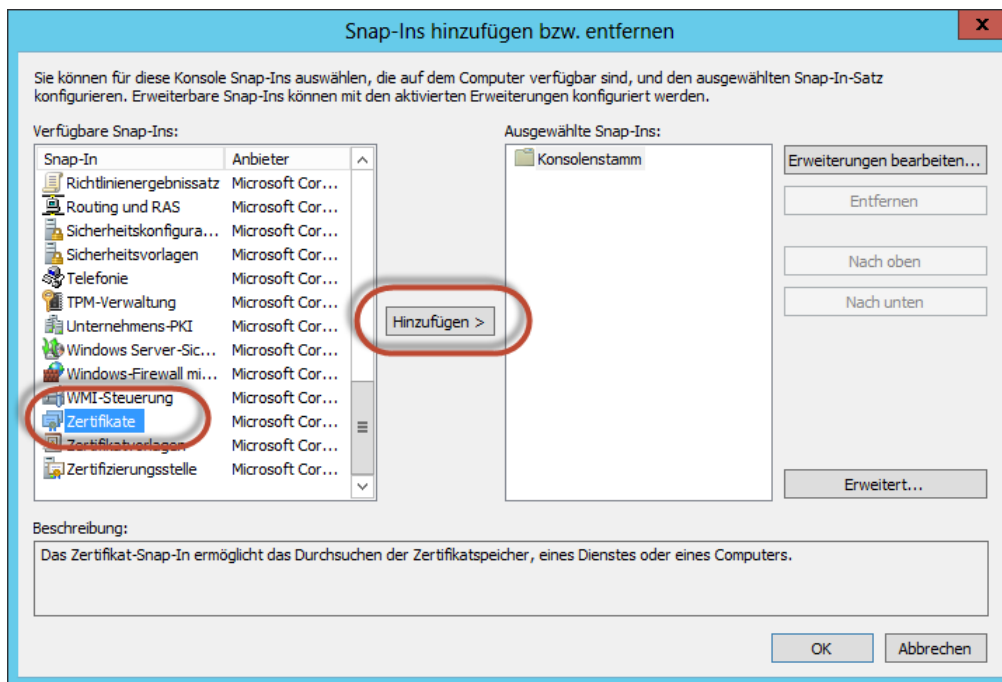
1. Starten Sie eine Managementkonsole.: *Windows Taste | mmc eingeben | mmc.exe auswählen.*



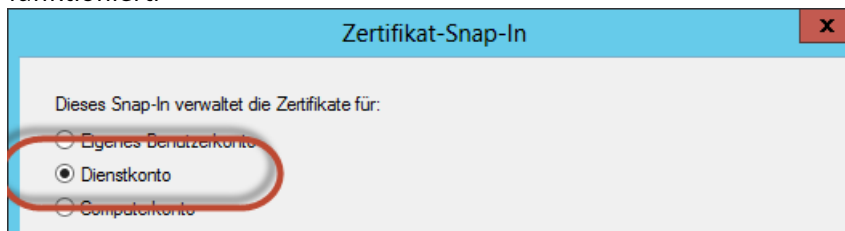
2. Wählen Sie *Snap-In hinzufügen*.



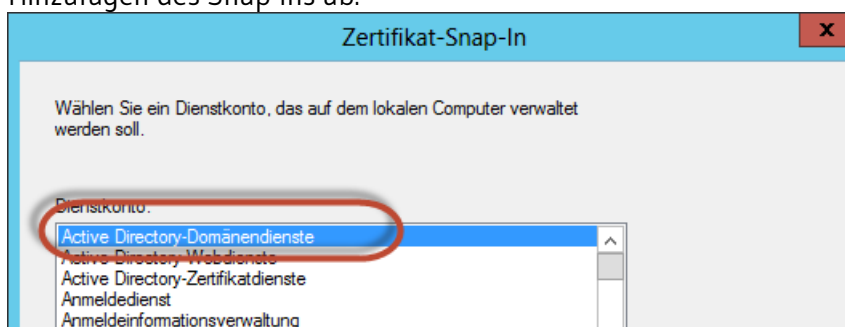
3. Als Snap-In wählen Sie *Zertifikate* aus und klicken auf *OK*.



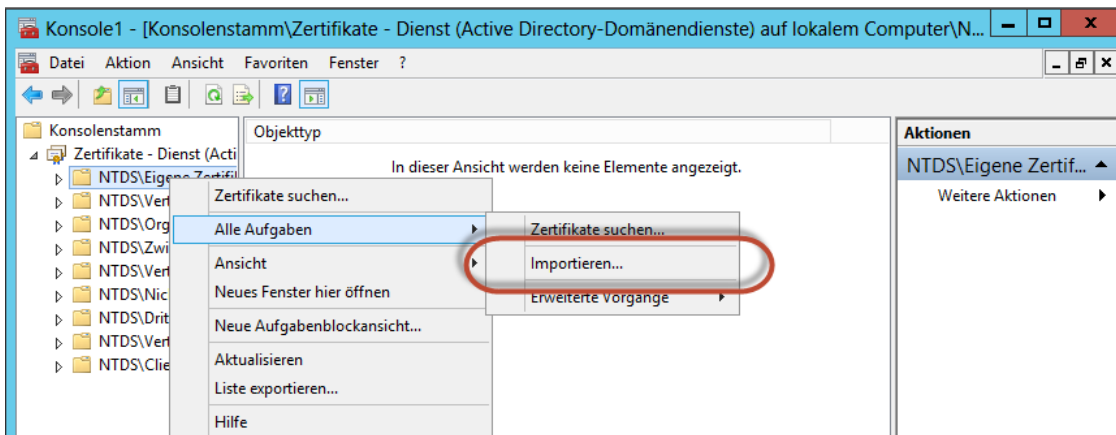
4. Wichtig ist das Hinzufügen als *Dienstkonto*, damit die Zertifikatsverwaltung nutzerunabhängig funktioniert.



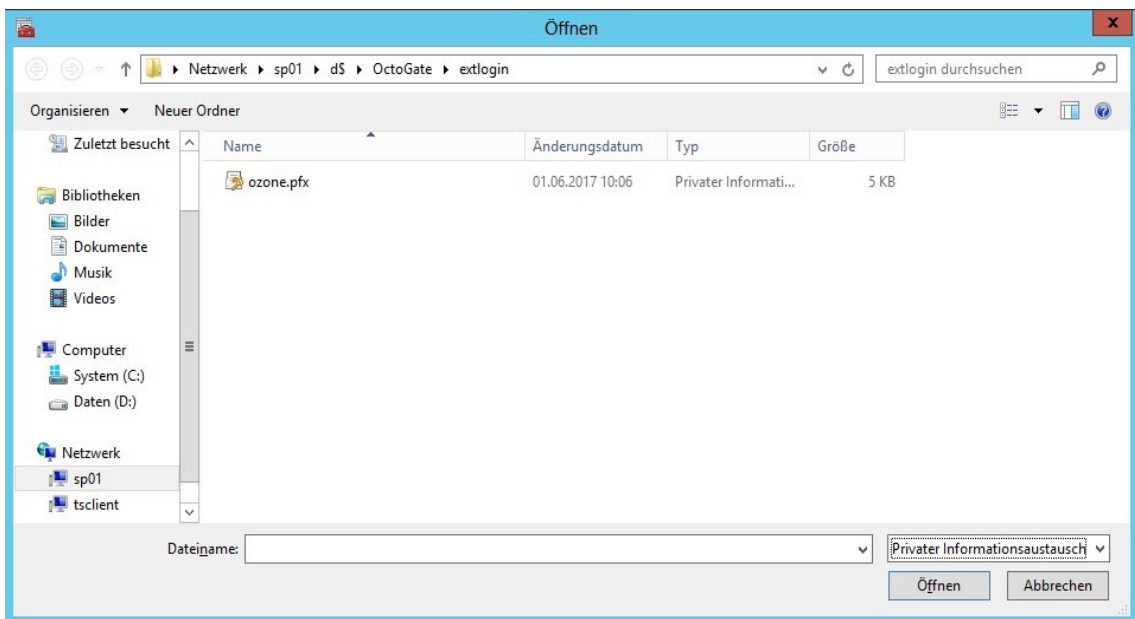
5. Wählen Sie die *Active Directory-Domänendienste* als Dienstkonto aus und schließen Sie das Hinzufügen des Snap-Ins ab.



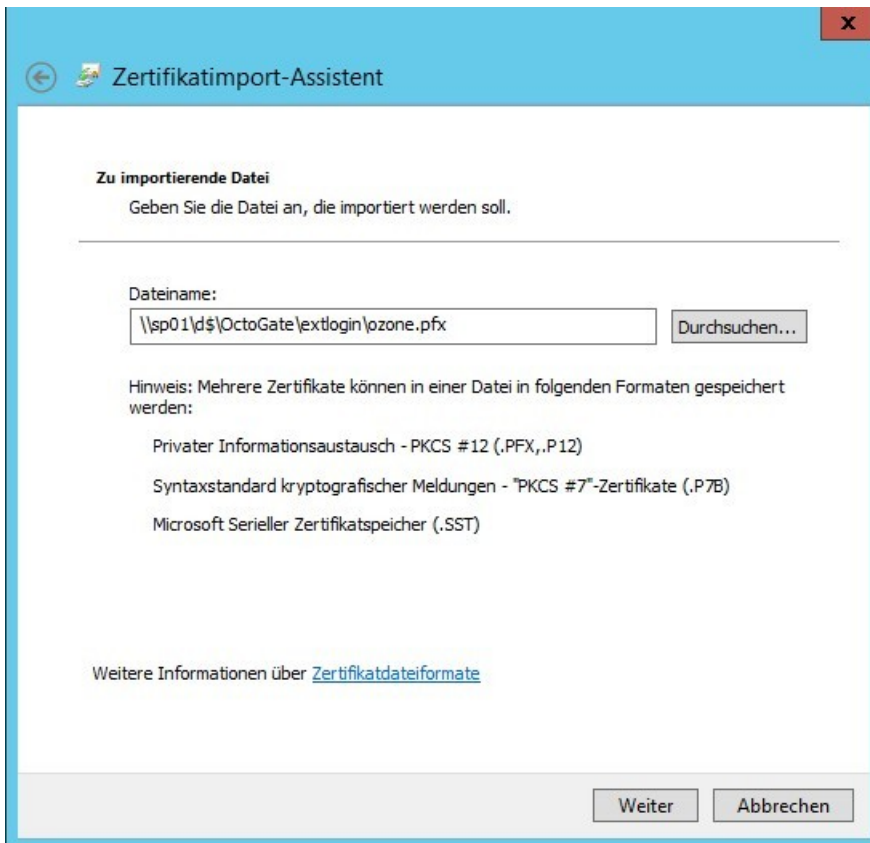
6. Markieren Sie im neuen Fenster *Konsolenstamm | Zertifikate – Dienst ... | NTDS\Eigene Zertifikate*. Klicken Sie mit der rechten Maustaste ins leere mittlere Fenster und wählen Sie *Alle Aufgaben | Importieren*.



7. Das Zertifikat liegt auf SP01 unter *D:\OctoGate\extlogin*. Über den UNC Pfad kann man vom DC01 darauf zugreifen¹. Klicken Sie auf *Durchsuchen* und navigieren Sie zu *\\sp01\d\$\octogate\extlogin*. Stellen Sie bei Dateitypen unten rechts *Privater Informationsaustausch *.pfx* ein und wählen Sie das Zertifikat *ozone.pfx* aus. Klicken Sie dann *Öffnen*.



8. Bestätigen Sie mit *Weiter*.



Zertifikatimport-Assistent

Zu importierende Datei
Geben Sie die Datei an, die importiert werden soll.

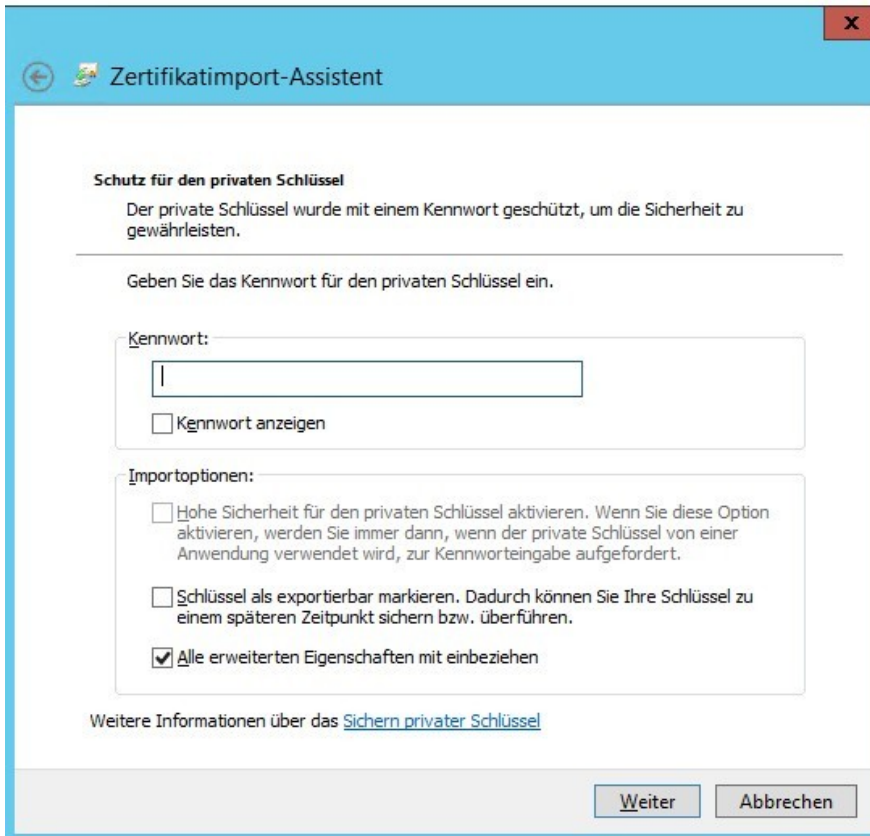
Dateiname:

Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

- Privater Informationsaustausch - PKCS #12 (.PFX, .P12)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
- Microsoft Serieller Zertifikatspeicher (.SST)

Weitere Informationen über [Zertifikatdateiformate](#)

9. Im nächsten Fenster klicken Sie direkt auf Weiter, das Passwort ist leer.



Zertifikatimport-Assistent

Schutz für den privaten Schlüssel
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

Kennwort:

 Kennwort anzeigen

Importoptionen:

- Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie diese Option aktivieren, werden Sie immer dann, wenn der private Schlüssel von einer Anwendung verwendet wird, zur Kennworteingabe aufgefordert.
- Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.
- Alle erweiterten Eigenschaften mit einbeziehen

Weitere Informationen über das [Sichern privater Schlüssel](#)

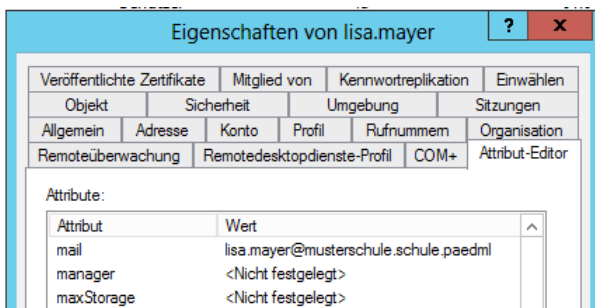
5. Konfiguration des externen Dienstes am Beispiel Moodle

Am Beispiel von Moodle wird nun erläutert, wie Sie diesen externen Dienst konfigurieren, um die LDAPs Authentifizierung einzurichten. Über Moodle hinaus gibt es weitere Anwendungen wie z.B. WebUntis, für die ebenfalls eine LDAPs Authentifizierung sinnvoll sein kann.

5.1. Vorüberlegung Verwendung E-Mails in Moodle

Bevor Sie mit der Konfiguration beginnen, müssen Sie vorab noch eine Entscheidung treffen. Jeder Benutzer in Moodle benötigt eine E-Mail-Adresse. Dies bedeutet: Im Profildfeld jedes Benutzers muss eine E-Mail-Adresse eingetragen sein.

Schaut man sich die Voreinstellungen der paedML Windows an sieht man Folgendes:



Für die Schülerin Lisa Mayer wurde von der paedML Windows beim Anlegen die E-Mail-Adresse lisa.mayer@musterschule.schule.paedml erstellt¹ und im Active Directory eingetragen.

Diese E-Mail-Adresse ist nur für den Gebrauch innerhalb der paedML Windows verwendbar. Für den Einsatz in Moodle kann diese Adresse nicht verwendet werden, denn an diese Adresse kann von extern keine E-Mail gesendet werden. Folgen wären Meldungen über nicht zustellbare Emails für Belwue, was zu vermeiden ist.

Es bedarf also eine Lösung dieses Problems. Hierfür stehen zwei Lösungsmöglichkeiten zur Verfügung

	Möglichkeit 1	Möglichkeit 2
Benachrichtigung an Benutzer von Moodle per E-Mail möglich.	ja	nein
Benutzer müssen selbst eine gültige E-Mail-Adresse in Moodle eintragen und den Erhalt einer Bestätigungsmail bestätigen.	ja	nein
E-Mail-Adresse wird aus dem Active Directory eingelesen	nein	ja
Spezielle E-Mail-Adresse der Form @blackhole.belwue.de muss erzeugt werden.	nein	ja
Eintrag im Feld <i>Daten übernehmen (E-Mail-Adresse)</i>	leer	otherMailbox

¹ Die E-Mail-Adresse wird nur erzeugt, wenn die Option beim Anlegen aktiviert war.

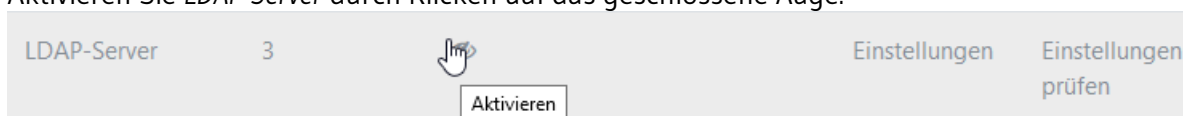
Möglichkeit 1: Ihre Schüler müssen bei der ersten Anmeldung eine gültige E-Mail-Adresse eingeben. Dann bekommen sie von Moodle eine E-Mail, um die Gültigkeit der Adresse zu bestätigen. Erst danach ist die Kontoerstellung abgeschlossen. Wenn dies für die Benutzer Ihrer Schule kein Problem darstellt, können Sie diese Möglichkeit wählen. Dann können Sie auch die Kommunikation über Moodle nutzen.

Möglichkeit 2: Wenn das Eintragen und Bestätigen einer E-Mail-Adresse an Ihrer Schule zu Schwierigkeiten führt und die Kommunikation über E-Mail nicht zwingend benötigt wird, wählen Sie diese Möglichkeit. Hierbei wird für das Benutzerprofil eine spezielle Dummy-Adresse generiert. Die E-Mail-Adressen lauten am Ende @blackhole.belwue.de. Dies bewirkt, dass Belwue E-Mails an diese Adresse nicht zu versendet. Die Adressen erzeugen Sie mit Hilfe einer Powershell Skripts, das Sie am als Domänenadministrator an einem beliebigen Computer im Netz ausführen. Diese Vorgehen ist am Ende dieser Anleitung dokumentiert.

5.2. LDAP-Zugriff aktivieren

Zunächst muss der LDAP Zugriff als Authentifizierungsmethode aktiviert werden. Nur dann können die Einstellungen konfiguriert werden.

1. Loggen Sie sich als Administrator in Moodle ein.
2. Navigieren Sie zu *Website-Administration | Plugins | Authentifizierung*.
3. Suchen Sie nach der Zeile *LDAP Server*.
4. Aktivieren Sie *LDAP-Server* durch Klicken auf das geschlossene Auge.



5. Der LDAP Server erscheint nun oben bei den aktiven Authentifizierungsmethoden

Name	Nutzer/innen	Aktivieren	Aufwärts/Abwärts
Manuelle Konten	12		
Kein Login	0		
E-Mail basierte Selbstregistrierung	0		↓
LDAP-Server	3		↑

Die Authentifizierungsmethode *E-Mail basierte Selbstregistrierung* können Sie deaktivieren, es sei denn Sie möchten diese Methode ebenfalls verwenden.

5.3. LDAP-Zugriff konfigurieren

1. Wählen Sie nun *Einstellungen*, um den LDAP Zugriff zu konfigurieren

Name	Nutzer/Innen	Aktivieren	Aufwärts/Abwärts	Einstellungen
Manuelle Konten	12			Einstellungen
Kein Login	0			
LDAP-Server	3			Einstellungen

Alle Felder, in denen Sie Änderungen vornehmen müssen, sind fett dargestellt.

Eintrag	Vorgaben für die paedML	
LDAP Servereinstellungen		
Host URL	ldaps://[Octogatename].ozone.octogate.de>:Port Beispiel: ldaps://abcdefgh.ozone.octogate.de>:3005	
Version	3	
TLS benutzen	Nein	
LDAP Codierung	utf-8	
Einträge pro Seite	250	
Bind-Einstellungen		Mit dem Zugangsdaten des Bind-Users wird auf die Informationen des AD zugegriffen
Kennwörter nicht cachem	nein	
Anmeldename	cn=ldapbinduser_extern,ou=_serviceaccounts,dc=musterschule,dc=schule,dc=paedml	Mit diesen Informationen wird der Idapbinduser_extern im AD gefunden.
Kennwort	[Kennwort von Idapbinduser_extern]	Tragen Sie hier das Passwort des Idapbinduser_extern ein.
Nutzersuche (user lookup)		
Nutzertyp	MS ActiveDirectory	
Kontexte	ou=benutzer,dc=musterschule,dc=schule,dc=paedml	
Subkontexte	ja	

Alias berücksichtigen	Nein	
Nutzermerkmal	cn	Steht für „common name“, enthält den Benutzernamen der paedML User
Ausblendungsmerkmal	(leer)	
Mitgliedsmerkmal	member	
Mitgliedsattribut nutzt dn	(leer)	
ObjectClass	(leer)	
Kennwortänderung fordern	Keine Änderungen - die Voreinstellungen können übernommen werden.	
Gültigkeitsablauf von Kennwörtern	Keine Änderungen - die Voreinstellungen können übernommen werden.	
Nutzereinstellung aktivieren	Keine Änderungen - die Voreinstellungen können übernommen werden.	
Zuordnung von Systemrollen	Keine Änderungen - die Voreinstellungen können übernommen werden.	Es wird derzeit nicht empfohlen, Systemrollen automatisch zuzuordnen. Vergeben Sie die Berechtigungen in Moodle.
Synchronisierung von Nutzerkonten	Keine Änderungen - die Voreinstellungen können übernommen werden.	
NTLM SSO	Keine Änderungen - die Voreinstellungen können übernommen werden.	

Im nun folgenden Abschnitt wird festgelegt, welche Informationen für einem Benutzer aus dem Active Directory ausgelesen werden

Datenzuordnung			
Vorname		givenName	
	Lokal aktualisieren	Bei jedem Login	Änderungen in der paedML werden beim Login übernommen.
	Extern aktualisieren	Nie	
	<i>Feld sperren</i>	Gesperrt	
Nachname		sn	
	Lokal aktualisieren	Bei jedem Login	Änderungen in der paedML werden beim Login

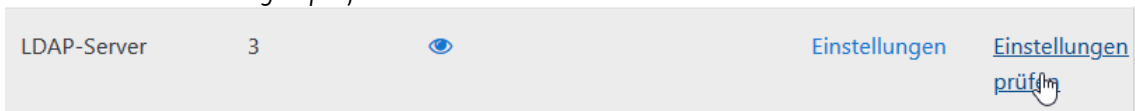
			übernommen.
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	
E-Mail-Adresse Möglichkeit 1			Lassen Sie das Feld leer. Der Benutzer muss selbst eine E-Mail-Adresse eintragen
	Lokal aktualisieren	<i>Beim Anlegen</i>	
	Extern aktualisieren	<i>Nie</i>	
	Feld sperren	<i>Bearbeitbar</i>	
E-Mail-Adresse Möglichkeit 2		otherMailbox	Liefert E-Mail-Adresse mit Endung @blackhole.belwue.de, muss zuvor auf DC01 erzeugt werden.
	Lokal aktualisieren	Bei jedem Login	Falls Benutzer hinzugefügt wurden und das Powershell-Skript zum Erzeugen der @blackhole.belwue.de Adressen noch nicht ausgeführt wurde.
	Extern aktualisieren	nie	
	Feld sperren	<i>Gesperrt</i>	
Stadt			Keine Änderungen
Land			Keine Änderungen
Sprache			Keine Änderungen
Beschreibung			Keine Änderungen
Webseite			Keine Änderungen
ID-Nummer			Keine Änderungen
Institution			Keine Änderungen
Abteilung			Keine Änderungen
Telefon			Keine Änderungen
Smartphone			Keine Änderungen
Adresse			Keine Änderungen
Vorname - lautgetreu			Keine Änderungen
Nachname - lautgetreu			Keine Änderungen
Mittlerer Name			Keine Änderungen
Pseudonym			Keine Änderungen
Geburtsdatum			Keine Änderungen
Geburtsort			Keine Änderungen
Geschlecht			Keine Änderungen

Klasse/Lerngruppe		department	
	Lokal aktualisieren	Bei jedem Login	Wird bei Schuljahreswechsel benötigt.
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	

Nun haben Sie die notwendigen Einstellungen vorgenommen. Speichern Sie diese ganz am Ende der Seite.

5.3.1. Einstellungen prüfen

1. Wechseln Sie nun wieder zu *Website-Administration | Plugins | Authentifizierung*. Wählen Sie *Einstellungen prüfen*.



2. Wenn Ihre Eingaben richtig waren, erhalten Sie eine Erfolgsmeldung.

Authentifizierungseinstellungen prüfen - LDAP-Server

Die Verbindung zum LDAP-Server wurde erfolgreich hergestellt.



Weiter

3. Nun können sich Lehrer und Schüler Ihres Schulnetzes bei Moodle mit den Anmeldedaten des Schulnetzes anmelden.

5.3.2. Optional: Neue Profildfelder anlegen

Zusätzlich zu den vorhandenen Datenzuordnungen können Sie weitere Informationen einlesen, die später z.B. beim Filtern von Benutzern hilfreich sein können. Hierzu müssen Sie zusätzliche Profildfelder anlegen:

1. Gehen Sie zu *Website-Administration | Nutzer/innen*
2. Wählen Sie unter *Nutzerkonten | Profildfelder*

Website-Administration

[Website-Administration](#)
[Nutzer/innen](#)
[Kurse](#)
[Bewertungen](#)
[Plugins](#)
[Darstellung](#)
[Server](#)

Nutzer/innen

Nutzerkonten

[Nutzerliste anzeigen](#)
[Nutzerverwaltung \(Bulk\)](#)
[Nutzer/in anlegen](#)
[Voreingestellte Nutzereinstellungen](#)

[Profilfelder](#)

[Globale Gruppen](#)
[Nutzerliste hochladen](#)
[Nutzerbilder hochladen](#)
[Profilfeld-basierende Zuweisung globaler Gruppen](#)
[Smart Cohort](#)

 3. Wählen Sie *Neues Profelfeld anlegen | Texteingabe*

Neues Profelfeld anlegen: ODER

4. Als Vorschlag können Sie diese drei zusätzlichen Profelfelder anlegen.

- paedML_Schuljahr
- paedML_Benutzertyp
- paedML_Schulart

5. In der Abbildung unten können Sie die empfohlenen Einstellungen entnehmen.

Ist dieses Feld notwendig?

Ist dieses Feld gesperrt?

Sollen die Daten eindeutig sein?

Auf der Anmeldeseite zeigen?

Für wen ist dieses Feld sichtbar?

Kategorie

6. Nachdem Sie die Profelfelder angelegt haben, sehen Sie unter den Datenzuordnungen die drei zusätzlichen Felder.

 7. Wechseln Sie wieder zu *Website-Administration | Plugins | Authentifizierung | LDAP-Server*. Ergänzen

Sie diese Einstellungen.

paedML_Schuljahr		departmentNumber	
	Lokal aktualisieren	Bei jedem Login	Da dieser Wert sich ändert, ist die Einstellung Beim Login sinnvoll oder muss beim Schuljahreswechsel aktiviert werden.
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	
paedML_Benutzertyp		employeeType	Liefert Teacher oder Student
	Lokal aktualisieren	<i>Beim Anlegen</i>	
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	
paedML_Schulart		division	Liefert die Schulart als Kürzel
	Lokal aktualisieren	<i>Beim Anlegen</i>	
	Extern aktualisieren	Nie	
	Feld sperren	Gesperrt	

Schaut man sich nun das Profil eines Schülers an, sieht man die entsprechenden Eintragungen.

▼ Weitere Profileinstellungen

Geburtsdatum	<input type="text"/>
Geburtsort	<input type="text"/>
Geschlecht	<input type="text" value="↓"/>
Klasse/Lerngruppe	<input type="text" value="8b"/>
paedML_Schuljahr	<input type="text" value="2019"/>
paedML_Benutzertyp	<input type="text" value="Student"/>
paedML_Schulart	<input type="text" value="GMS"/>

5.4. E-Mail-Adressen @blackhole.belwue.de per Skript erstellen

Wenn Sie sich bei der Verwendung der E-Mail-Adressen für Möglichkeit 2 mit den @blackhole.belwue.de Adresse entschieden haben, müssen Sie die Einträge hierfür im Active Directory erst erzeugen.

Dies erledigen Sie mit dem Powershellskript *Blackhole Mail-Adressen Belwue erzeugen.ps1*.

Das Skript können Sie zusammen mit dieser Anleitung vom Lehrerfortbildungsserver herunterladen. Sollten dies nicht möglich sein, können Sie dies auch sehr einfach selbst erstellen. Erzeugen Sie hierzu eine neue Textdatei und kopieren Sie die unten stehenden Zeilen hinein.

```
Import-Module ActiveDirectory
Get-ADUser -LDAPFilter '(|(employeeType=teacher)(employeeType=student))' | `
| `
ForEach-Object { Set-ADUser -Add
@{otherMailbox=('{0}@blackhole.belwue.de' -f $_.Name)} -Identity $_.Name
}
pause
```

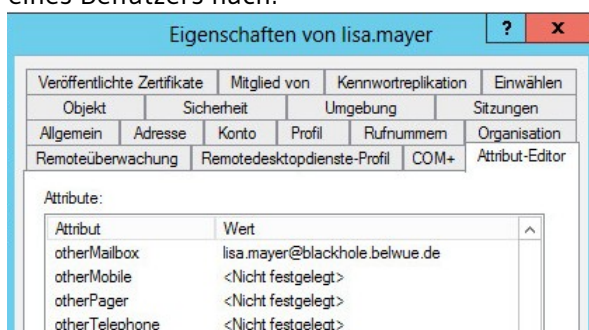
So sehen die vier Zeilen im Editor aus.

```
Import-Module ActiveDirectory
Get-ADUser -LDAPFilter '(|(employeeType=teacher)(employeeType=student))' | `
| `
ForEach-Object { Set-ADUser -Add @{otherMailbox=('{0}@blackhole.belwue.de' -f $_.Name)} -Identity $_.Name }
pause
```

Speichern Sie die Datei dann mit der Dateiendung *.ps1* ab. Kopieren Sie die Datei dann an eine beliebige Stelle auf dem DC01 ab

Um die *@blackhole.belwue.de* Adresse zu erzeugen, gehen Sie so vor:

1. Melden Sie sich am DC01 als Administrator an.
2. Machen Sie einen Rechtsklick auf die Datei *Blackhole Mail-Adressen Belwue erzeugen.ps1*. Wählen Sie Mit Powershell ausführen.
3. Wenn der Vorgang fertig ist, erscheint ein Fenster, das Sie mit der Eingabetaste schließen.
4. Um den erfolgreichen Eintrag sehen, schauen Sie im Active Directory in den Eigenschaften eines Benutzers nach:



Denken Sie daran, dass Sie das Skript immer ausführen müssen, nachdem Sie einen Benutzer angelegt haben.