



---

## LDAPS Authentifizierung

paedML Windows 3.x

Kink, Mayer, Wiesler

08.01.2018

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.....	5
4.Zertifikat auf DC01 importieren.....	6
5.LDAPS Zugang testen.....	11
6.Konfiguration des externen Dienstes am Beispiel moodle.....	13
6.1.LDAP Plugin aktivieren.....	13
6.2.LDAP-Zugriff konfigurieren.....	14
6.2.1.Hinweise.....	17



## o. Informationen zum Dokument

---

<b>Titel</b>	LDAPS Authentifizierung mit der paedML Windows 3.x
<b>Untertitel</b>	
<b>Bereich</b>	paedML Windows 3.x
<b>Autor</b>	Daniel Wiesler, Stefan Kink, Andreas Mayer
<b>Datum</b>	08.01.2018
<b>Lizenz</b>	<a href="#">CC BY-SA 4.0</a>

## I. Einführung und Übersicht

---

Das Lightweight Directory Access Protocol bietet vielfältige Kommunikationsmöglichkeiten für die aktuellen Bedürfnisse von schulischen Netzwerkumgebungen. So ist es möglich, die AD-Benutzer des pädagogischen Schulnetzwerks zur Authentifizierung in Moodle oder WebUntis zu nutzen, um ein deutlich schlankeres Benutzermanagement pflegen zu können.

Zur Einrichtung eines Zugriffs von außen per LDAPS, sind in der paedML3.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. In der Standardkonfiguration

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 dies 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 Webserver eintragen<sup>1</sup>.
- 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

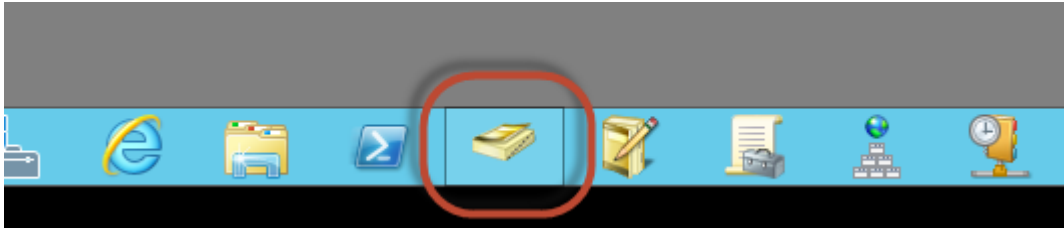
## 3. LDAP-Benutzer einrichten

Die Authentifizierungsanfrage von Moodle möchte auf das ActiveDirectory (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. Richten Sie 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.

<sup>1</sup> Hinweise für moodle bei Belwue: <https://www.belwue.de/support/faq/webdienste10/allgemein0.html>



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:

- Vorschlag für den Namen: ldapbinduser\_Schulkürzel, hier im Beispiel ldapbinduser\_lfb.
- Vergeben Sie keinen Vornamen. **WICHTIG:** vollständiger Name, Nachname und Benutzername sollten gleich sein. Unsere Tests haben ergeben, dass es hier zu Problemen kommen kann, sollte dies nicht der Fall sein.
- Vergeben Sie ein Passwort und aktivieren Sie die beiden Optionen. Beenden Sie dann den Assistenten ohne weitere Änderungen.

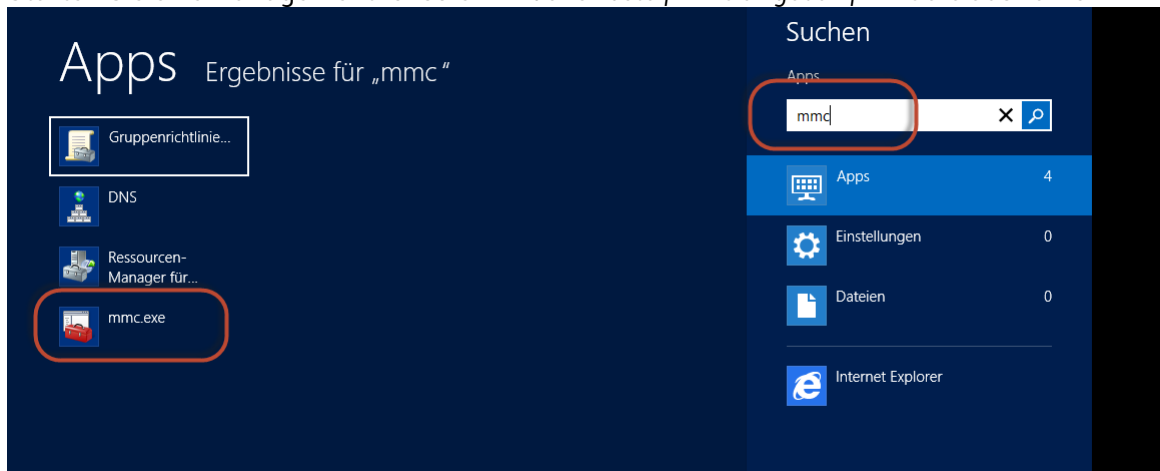
## 4. Zertifikat auf DC01 importieren

Damit der Datenverkehr bei der LDAPS Authentifizierung sicher und vertraulich stattfindet, muss auf dem DC01 noch ein SSL Zertifikat installiert werden. Dieses Zertifikat wird von der Firma Octogate zur Verfügung gestellt. Mit Hilfe dieses Zertifikats kann der DC01 eine verschlüsselte Verbindung aufbauen<sup>2</sup>.

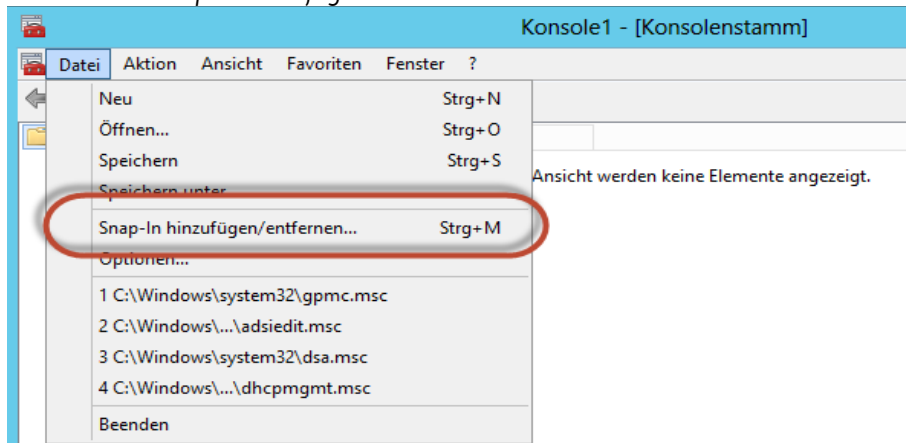
Folgen Sie den hier dargestellten Schritten. Sie arbeiten als Domänenadministrator am DC01.

- 2 Das von der Octogate gelieferte Zertifikat ist selbst-signiert und besitzt weder eine vertrauenswürdige Stammzertifizierungsstelle noch eine vertrauenswürdige Kette. Dies kann mitunter zu Problemen bei extern gehosteten Diensten führen. Je nach Sicherheitsanforderung muss hier ggf. in ein gültiges Zertifikat mit vertrauenswürdiger Stammzertifizierungsstelle investiert werden.

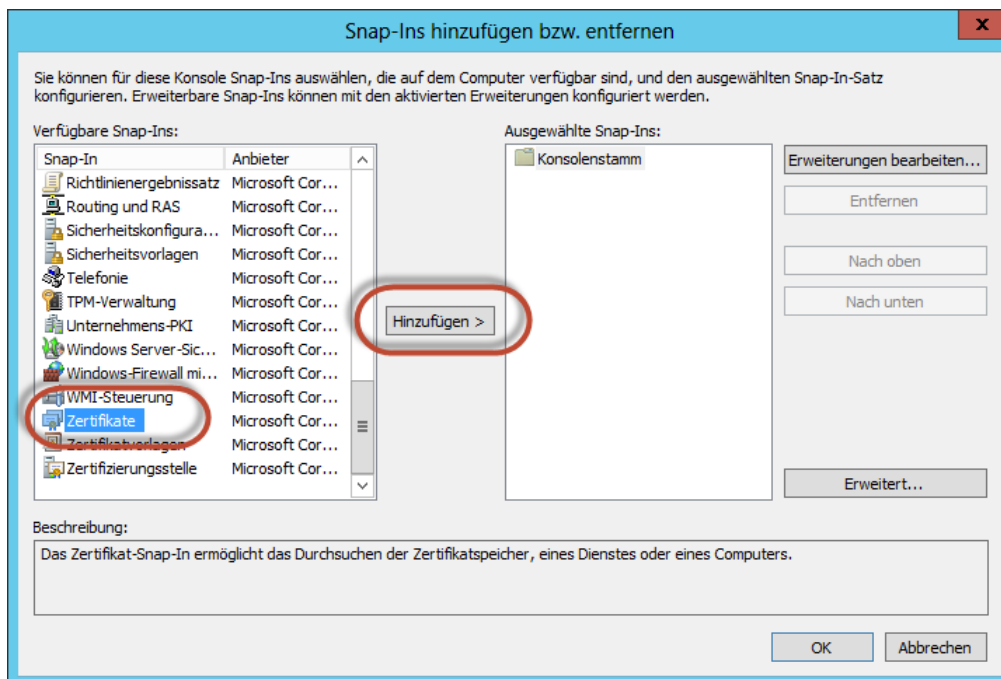
1. Starten Sie eine Managementkonsole.: *Windows Taste* / *mmc* eingeben / *mmc.exe* auswählen.



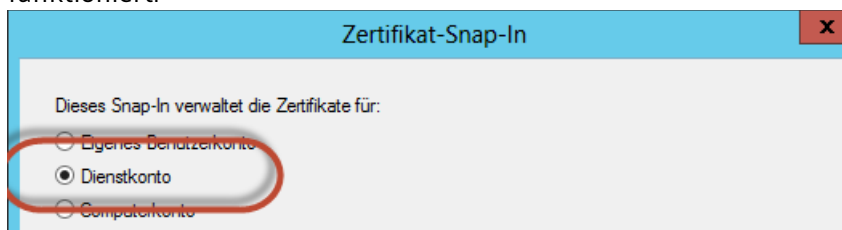
2. Wählen Sie *Snap-In hinzufügen*.



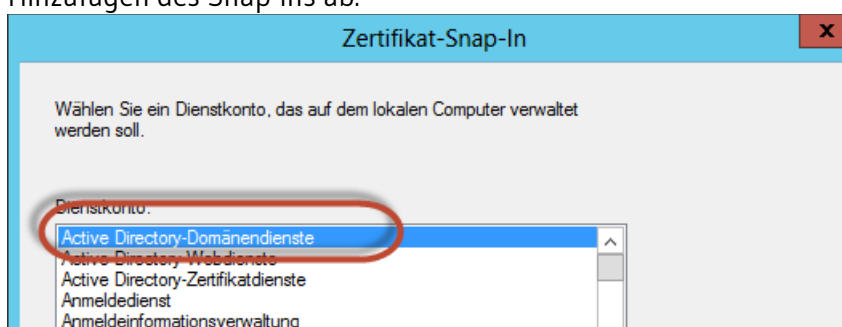
3. Als Snap-In wählen Sie *Zertifikate* aus und klicken auf OK.



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

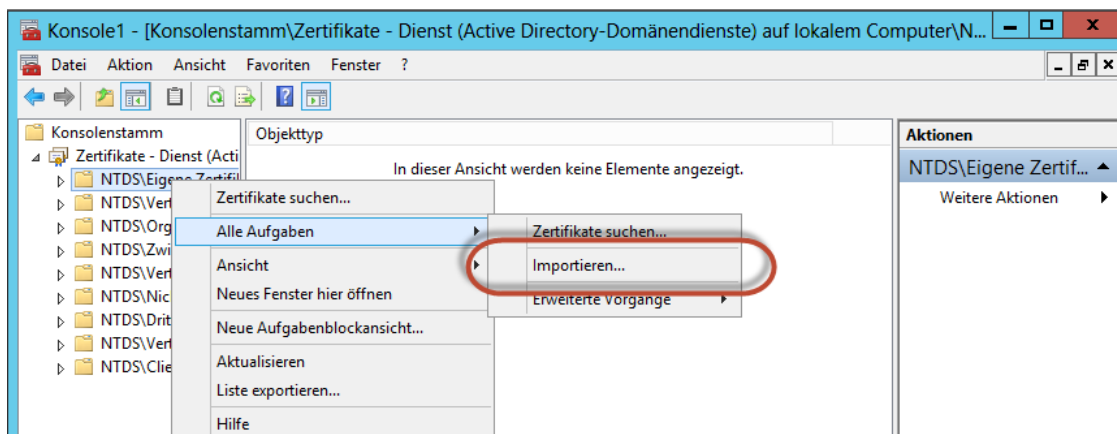


5. Wählen Sie die Active Directory-Domänendienste als Dienstkonto aus und schließen Sie das Hinzufügen des Snap-Ins ab.

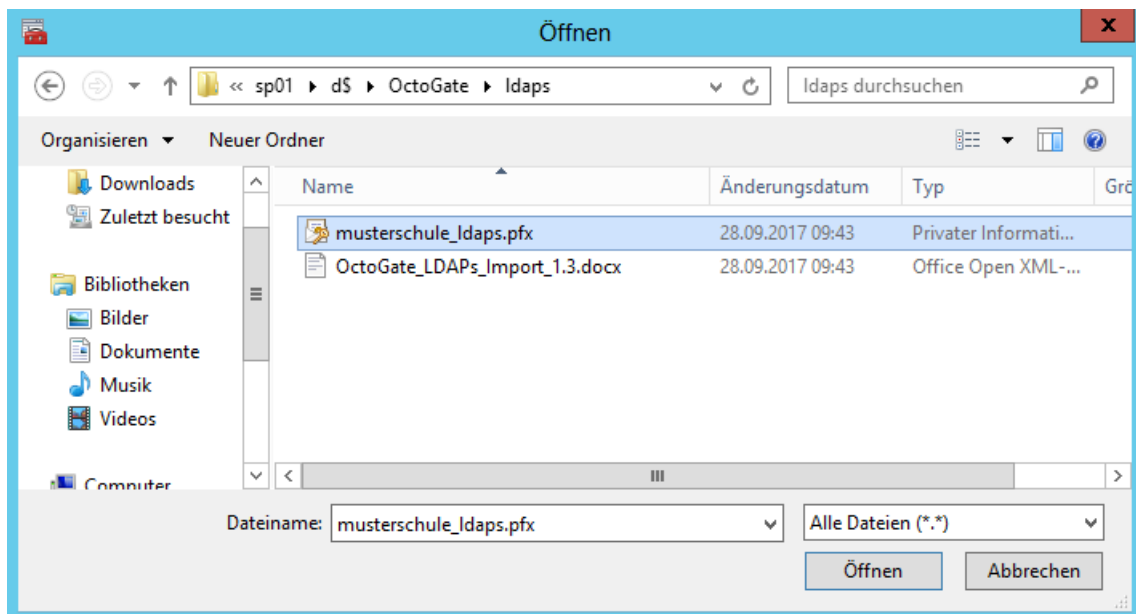


6. Markieren Sie im neuen Fenster Konsolenstamm | Zertifikate – Dienst ... | NTDS\Eigene Zertifikate. Klicken Sie mit der rechten Maustaste ins leere mittlere Fenster und wählen Sie *Alle Aufgaben* | *Importieren*.



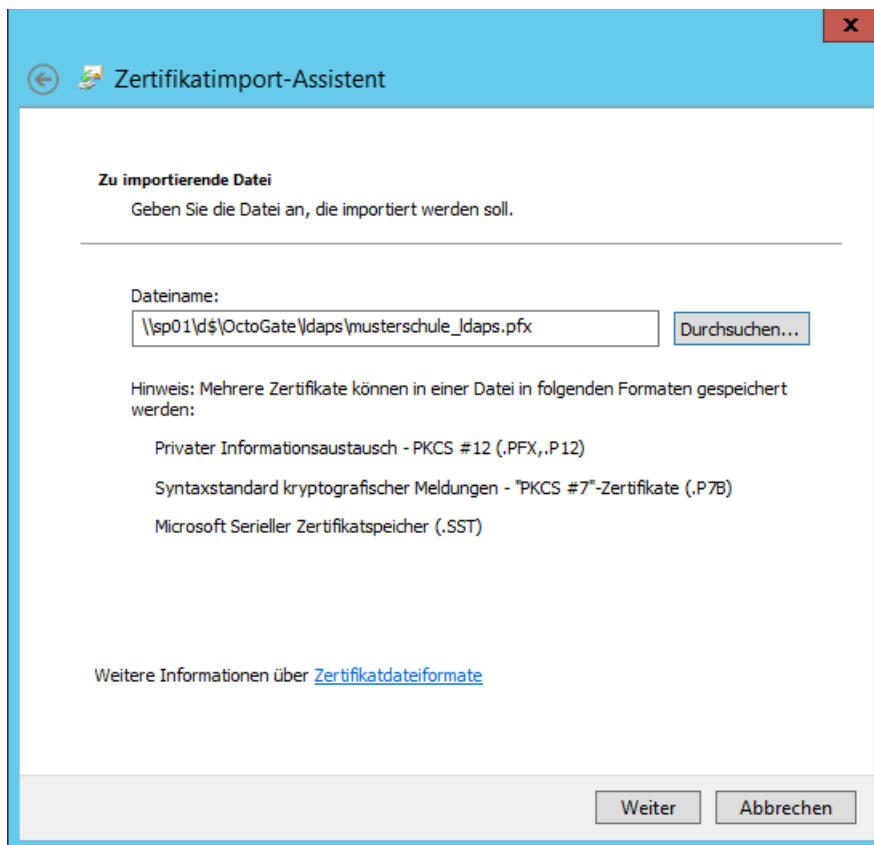


7. Das Zertifikat liegt auf SP01 unter *D:\OctoGate\ldaps*. Über den UNC Pfad kann man vom DC01 darauf zugreifen<sup>3</sup>. Klicken Sie auf *Durchsuchen* und navigieren Sie nach *\\sp01\d\$\octogate\ldaps*. Stellen Sie bei Dateitypen unten rechts *Alle Dateitypen* ein und wählen Sie das Zertifikat *musterschule\_ldaps.pfx* aus. Klicken Sie dann *Öffnen*.



8. Bestätigen Sie mit *Weiter*.

<sup>3</sup> Selbstverständlich können Sie es auch auf den DC01 kopieren.



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

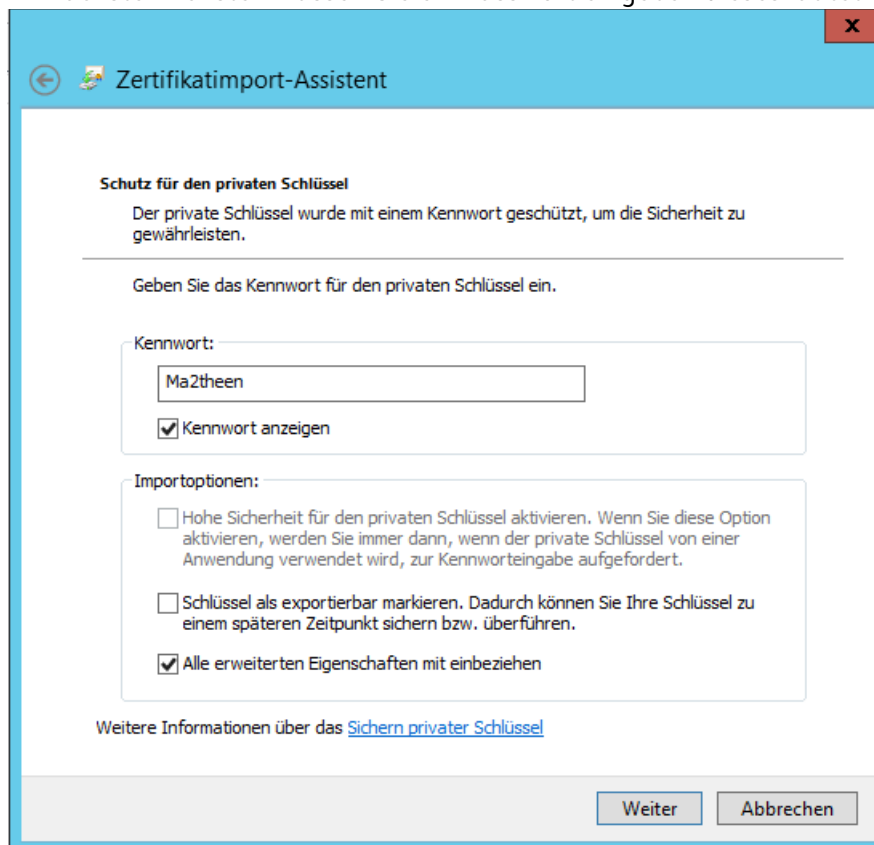
Dateiname:

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 [Zertifikatsdateiformate](#)

9. Im nächsten Fenster müssen Sie ein Passwort eingeben dieses lautet Ma2theen.



**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](#)

10. In den weiteren Fenstern sind keine Änderungen der Einstellungen nötig. Kontrollieren Sie, dass als Zertifikatsspeicher *NTDS\Eigene Zertifikate* eingetragen ist. Schließen Sie den Assistenten ab.

## 5. LDAPS Zugang testen

Bevor Sie im nächsten Schritt ihr moodle konfigurieren, sollten Sie testen, ob der LDAPS Zugriff funktioniert. Dies können Sie recht anschaulich mit dem Programm Softerra LDAP Browser.

Installieren Sie das Programm auf einem beliebigen PC außerhalb des Schulnetzes.

1. Starten Sie das Programm und klicken Sie links oben auf Neu. Vergeben Sie einen beliebigen Profilnamen.
2. Auf der Registerkarte tragen Sie ein:

Profilerrstellungs-Assistent - Schritt 2

**Profil - Allgemeine Information**  
Allgemeine Information angeben

Geben Sie die Server-Hostinformation an und machen Sie Einstellungen für allgemeine Sicherheitsoptionen.

Host-Informationen

Host:  Port:

Basis-DN:

Sicherheits-Optionen

☒ Sichere Verbindung (SSL) verwenden

Geben Sie eine LDAP URL für die anderen Felder an, die auf Basis dieser Information ausgefüllt werden.

LDAP URL:

- Host: IP der externen Netzwerkkarte der Octogate
  - Basis-DN: *dc=musterschule,dc=schule,dc=paedml*
  - Haken setzen bei *Sichere Verbindung (SSL) verwenden*.  
Klicken Sie dann auf weiter. Wenn Sie zum nächsten Fenster kommen sieht es schon gut aus mit der Verbindung.
  - Vorsicht. Nach Setzen des Hakens ändert sich u.U. der von Ihnen eingegeben Port, kontrollieren Sie Diesen (636,3005, 45001, etc.), bevor sie fortfahren.
3. Im nächsten Fenster tragen Sie die Anmeldedaten des *ldapbinduser\_lfb* und das Passwort ein.

Profilerrstellungs-Assistent - Schritt 3

**Benutzerauthentifizierung-Info**  
Mit Hilfe einer der folgenden Authentifizierungsoptionen verbinden.

☐ Anonymer Benutzer  
☐ Aktuell angemeldeter Benutzer (nur für Active Directory)  
☐ Externes (SSL-Zertifikat)  
☒ Andere Anmeldeinformationen

Mechanismus: Einfach Unterstützte erhalten

Principal:   
Beispiel: cn=User,ou=People,o=Company

Kennwort:

☐ Kennwort speichern DE

[Anmeldeinformationen auswählen](#)

☒ Versuchen, die für erneuten Referenzverbindung notwendigen Anmeldeinformationen zu finden

< Zurück Weiter > Fertig stellen Abbrechen Hilfe

4. Im nächsten Fenster belassen Sie die Einstellungen und beenden den Assistenten. Es erscheint unter Umständen ein Zertifikatsauswahl:

Clientauthentifizierung [141.10.47.91:3005]

**Identifikation**

Der von Ihnen abgefragte LDAP-Server erfordert möglicherweise Identifikation. Wählen Sie das Zertifikat aus, das beim Verbindungsaufbau

Zertifikat anzeigen...

☐ Behalten Sie diese Einstellung bis zum Ende der Sitzung

OK Abbrechen

Wählen Sie den Eintrag [MS-Organisation]

5. Dann erhalten Sie einen Sicherheitshinweis:

Eine Zertifikatkette zu einer vertrauenswürdigen Stammzertifizierungsstelle konnte nicht aufgebaut werden.

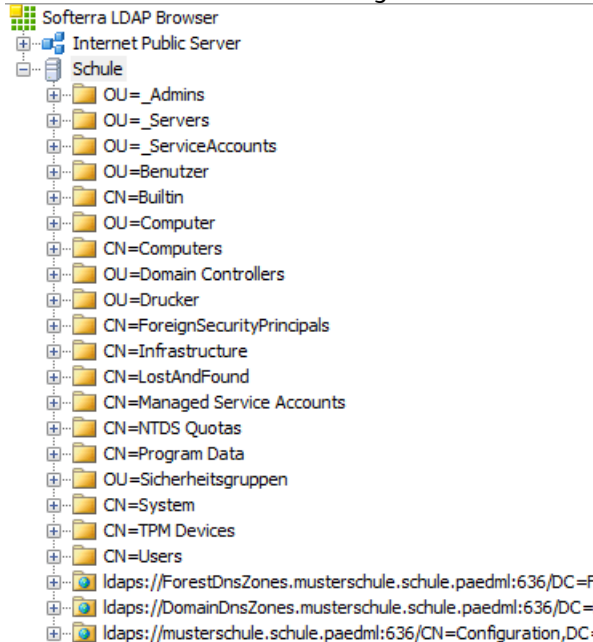
Möchten Sie den Vorgang fortsetzen?

☐ Behalten Sie diese Einstellung bis zum Ende der Sitzung

Ja Nein Zertifikat anzeigen

Dieser liegt darin begründet, dass das Zertifikat von Octogate ist und nicht von einer vertrauenswürdigen Stammzertifizierungsstelle. Klicken Sie auf *Ja*.

6. Hoffentlich erscheint dann folgendes Fenster. Dann hat nämlich der LDAPS Zugriff geklappt.



Sie können mit dem Account des *ldapbinduser* auf das AD zugreifen. Ihr Server erfüllt nun die Voraussetzungen für die LDAPS Authentifizierung.

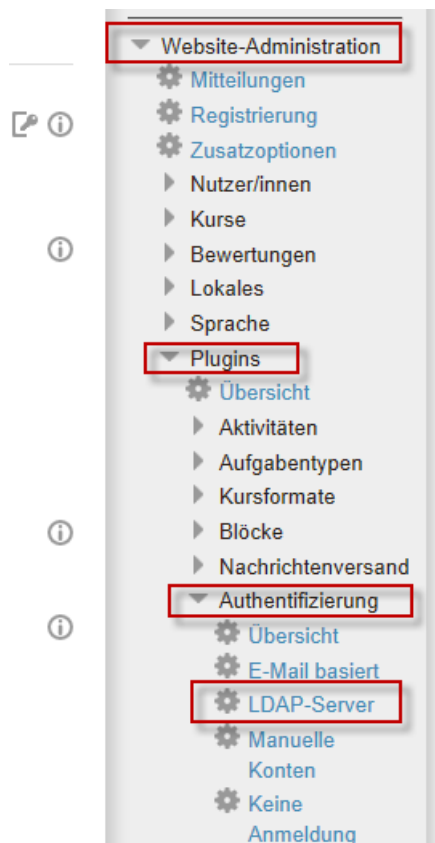
## 6. Konfiguration des externen Dienstes am Beispiel moodle

Für einen Zugriff von außen über das LDAP Protokoll soll am typischen Einsatzbeispiel Moodle besprochen werden, wie der externe Dienst konfiguriert werden muss, um auf die AD-Struktur der Domänenbenutzer zugreifen zu können. Diese Sektion ist damit stark auf diesen einen Spezialfall zugeschnitten. Die Anbindung anderer Dienste kann sich mitunter deutlich von der hier gezeigten Lösung unterscheiden, auch wenn die logischen Schritte die gleichen sind.

Bitte beachten Sie, dass die Autoren dieser Anleitung keine ausgewiesenen moodle Experten sind. Die Einstellungen wurden von einem System mit funktionierender LDAPS Authentifikation übernommen. Bei Problemen bitten Sie Belwue bzw. Ihren moodle-Host um Hilfe.

### 6.1. LDAP Plugin aktivieren

1. Loggen Sie sich als Administrator in Moodle ein.
2. Navigieren Sie zu *Website-Administration | Plugins | Authentifizierung | LDAP-Server*.



## 6.2. LDAP-Zugriff konfigurieren

Hier sind einige, teils sehr komplex wirkende Eingaben zu machen. Wenn in der rechten Spalte Werte fett gedruckt sind, müssen Sie diese mit den für Ihr System geltenden Werte ersetzen. Es handelt sich um die Host URL, den ldapbinduser\_xxx und dessen Passwort.

LDAP Servereinstellungen	
Host URL	ldaps://<IP der Octogate>:Port, z.B. <b>ldaps://141.10.99.199:636</b> <b>ldaps://141.10.99.199:3005</b> <b>ldaps://141.10.99.199:45001</b>
Version	3
TLS benutzen	Nein
LDAP Codierung	utf-8
Einträge pro Seite	250
Bind-Einstellungen	
Kennwörter nicht cachen	nein

Anmeldename	cn=ldapbinduser_1fb,ou=_serviceaccounts,dc=musterschule,dc=schule,dc=paedml (alles ohne Leerzeichen!)
Kennwort	(Kennwort des ldapbindusers)
<b>Nutzersuche (user lookup)</b>	
Nutzertyp	MS ActiveDirectory
Kontexte	ou=benutzer,dc=musterschule,dc=schule,dc=paedml
Subkontexte	ja
Alias berücksichtigen	Nein
Nutzermerkmal	samaccountname
Ausblendungsmerkmal	(leer)
Mitgliedsmerkmal	member
Mitgliedsattribut nutzt dn	(leer)
ObjectClass	(leer)
<b>Kennwortänderung fordern</b>	
Kennwortänderung fordern	nein
Standardseite zur Kennwortänderung nutzen	nein
Kennwortformat	Unformatierter Text
URL zur Kennwortänderung	(leer)
<b>Gültigkeitsablauf von Kennwörtern</b>	
Gültigkeitsende	no
Warnung zum Gültigkeitsende	10
Merkmal für Gültigkeitsende	(leer)
GraceLogins	nein
Merkmal für GraceLogin	(leer)
<b>Nutzereinstellung aktivieren</b>	
Nutzer extern anlegen	nein
Kontext für neue Nutzer	(leer)
<b>Kursersteller/in</b>	
Kursverwalter/innen	ou=Lehrer,ou=Benutzer,dc=musterschule,dc=schule,dc=paedml (oder

	<i>eben eine andere Gruppe, die Kurserstellerrechte erhalten soll)</i>
--	--

### Synchronisierung von Nutzerkonten

Entfernte externe Nutzer	Nur intern zugänglich
Status von lokalen Nutzerkonten synchronisieren	Nein

### NTLM SSO

Aktivieren	nein
Subnet	<i>(leer)</i>
MS IE fast path?	NTLM mit allen Browsern versuchen
Authentifikationsart	NTLM
Entfernter Nutzerdatenformat	<i>(leer)</i>

### Datenzuordnung

Vorname	givenName
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	<i>Gesperrt</i>
Nachname	sn
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	<i>Gesperrt</i>
Alle weiteren Punkte	distinguishedName <i>(braucht man nur, wenn man AD-Gruppen automatisch Kursen zuweisen möchte)</i>
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	<i>Bearbeitbar</i>



### 6.2.1. Hinweise

- Für die Authentifizierungsmethode müssen Sie nun eine Wahl treffen. War die Authentifizierungsmethode vorher "Manuelle Zugänge" läuft erst einmal alles weiter wie bisher, da die Authentifizierungs-Plugins von oben nach unten abgearbeitet werden. Verließ die Authentifizierung vorher emailbasiert, dann muss man sich entscheiden, in welcher Reihenfolge man die Authentifizierungsmethoden in der Übergangsphase bis zur kompletten Umstellung anordnen möchte.
- Bei jedem Anmelden eines Benutzers fragt der Moodleserver beim paedML-Server die Richtigkeit der Benutzerkennung ab. Das Kennwort wird nicht in der Moodledatenbank gespeichert. Beim ersten Anmelden werden Name und Vorname aus der Active Directory übernommen und zusammen mit den eingegebenen Profildaten in der Moodledatenbank gespeichert. Sind die Profildaten unvollständig, das heißt, fehlen Pflichtdaten wie z.B. die Mailadresse, erscheint das untenstehende Fenster, um die Daten zu ergänzen. Die Änderung der Daten muss durch eine Bestätigungsmail, die von Moodle automatisch verschickt wird, bestätigt werden. Erst danach ist ein Arbeiten in Moodle möglich.