HSM IT-Services GmbH

**OctoGate**

**Installation LDAP/S**

OctoGate **-**

**Version 1.3**

Landesmedienzentrum BW

**OctoGate Vertragsvereinbarung**

OctoGate IT Security Systems GmbH, Franz List Str. 42  
33100 Paderborn

Tel.: ++49 5251 18040 0  
Fax: ++49 5251 18040 39  
Email: info@octogate.de  
Internet: www.octogate.de

Verantwortlicher für den Inhalt: Frank Menne

Versionshistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Datum | Person | Version | Kommentar |
| 3.4.2017 | Frank Menne | 1.0 | Initial-Dokument |
| 6.4.2017 | Felix Wischke | 1.1 | Übersetzung auf Deutsch |
| 10.4.2017 | Felix Wischke | 1.2 | Korrektur LDAPS Test |
| 24.5.2017 | Felix Wischke | 1.3 | Erweiterung des Scopes (DNAT/Schannel/..) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhalt

[1 Basis - Konzept 4](#_Toc483582884)

[2 Installation Zertifikat 5](#_Toc483582885)

[2.1 Starten der Microsoft Management Console: 6](#_Toc483582886)

[2.2 Auswahl des Snap-Ins 7](#_Toc483582887)

[2.3 Konfiguration des Zertifikat-Snap-Ins 8](#_Toc483582888)

[2.4 Import des Zertifikates 11](#_Toc483582889)

[3 LDAPs Test 18](#_Toc483582890)

[4 Konfiguration der OctoGate 20](#_Toc483582891)

[4.1 Portweiterleitung an den ADS 21](#_Toc483582892)

[5 Konfiguration des Webservers 23](#_Toc483582893)

[5.1 Verifizierung des Hostnamens in OpenLDAP abschalten 24](#_Toc483582894)

[6 Anhang 26](#_Toc483582895)

[6.1 Import des OctoGate Zertifikates auf dem ADS 27](#_Toc483582896)

[6.2 Test der Port-Weiterleitung 31](#_Toc483582897)

[6.3 Verbindungsproblem LDAPs 32](#_Toc483582898)

# Basis - Konzept

Die Authentifizierung von externen Diensten wie z.B. Moodle gegenüber dem eigenen Active Directory Server der Schule wird über das sogenannte LDAP – Protokoll abgewickelt (Lightweight Directory Access Protocol).

Die OctoGate Firewall leitet wie andere Firewallsysteme auch hier lediglich die Verbindung von außen (Moodle) an den paedML eigenen Active Directory – Server weiter.

Dieses Dokument beschreibt die Konfiguration des AD – Servers in der paedML zur Freischaltung des LDAP/S Dienstes und zum Import des entsprechenden Zertifikates.

# Installation Zertifikat

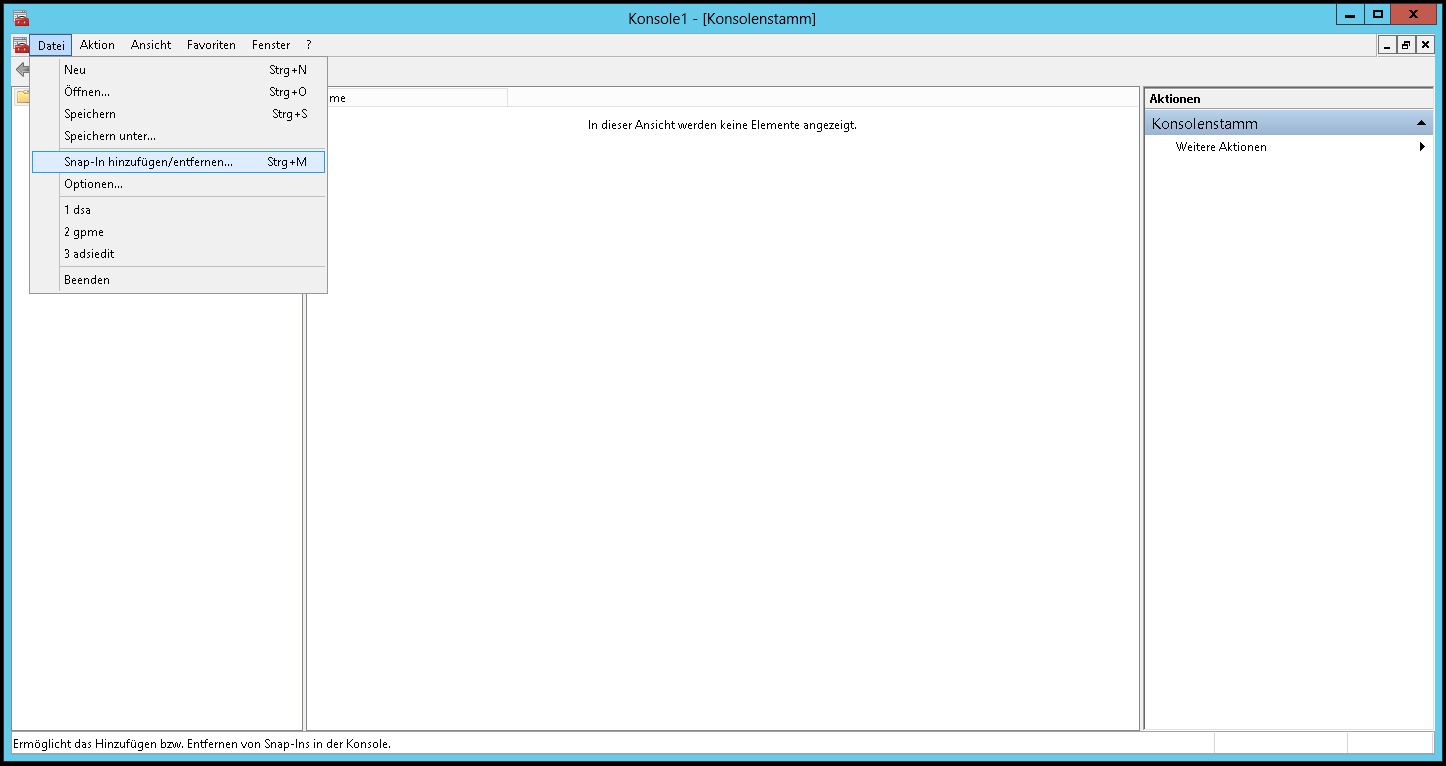
Laden Sie das Zertifikat auf Ihren DC01. Die Datei musterschule\_ldaps.pfx hat das Importpasswort Ma2theen.



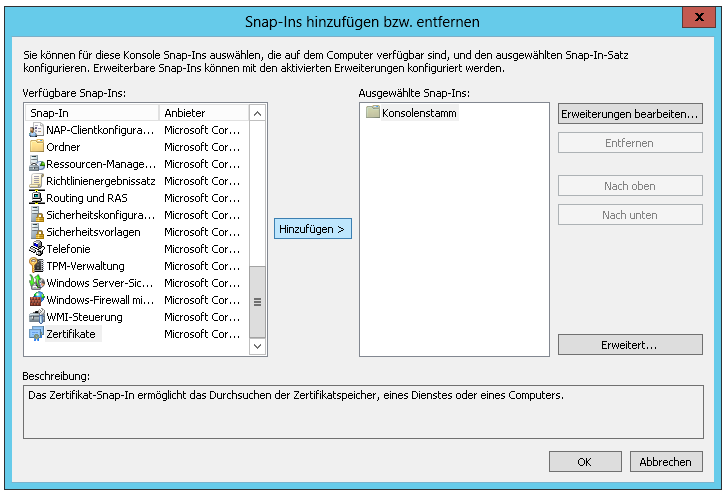
## Starten der Microsoft Management Console:



## Auswahl des Snap-Ins

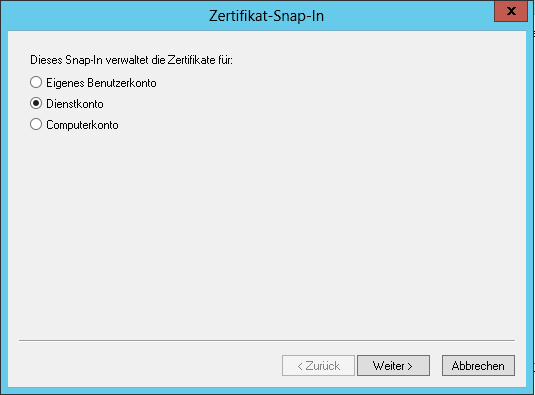


Fügen Sie das Snap-In für Zertifikate hinzu.

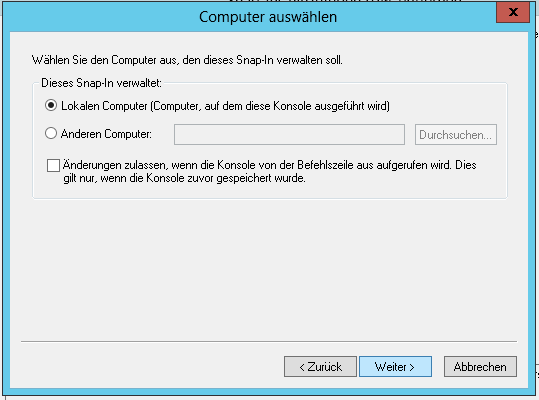


## Konfiguration des Zertifikat-Snap-Ins

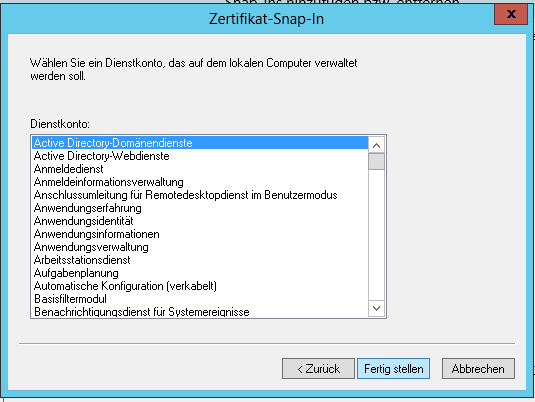
Der Microsoft LDAP Service läuft als Systemdienst. Er hat dementsprechend ein Dienstkonto.



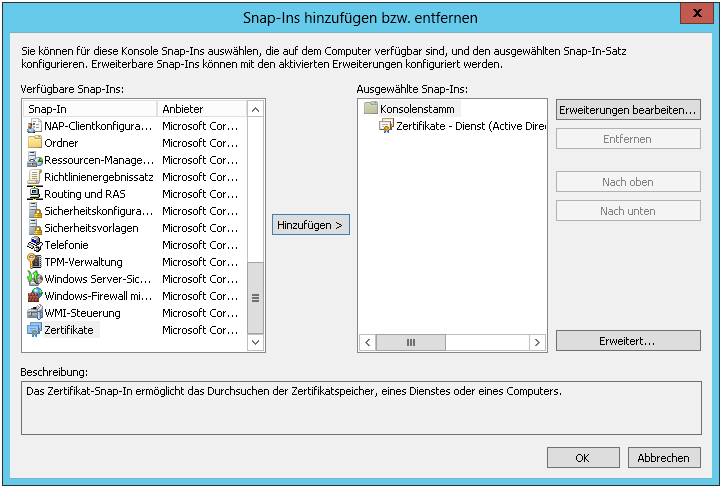
Wählen Sie den lokalen Computer aus (wir gehen davon aus, dass Sie die Konfiguration auf dem DC01 vornehmen).



Wählen sie das Dienstkonto des Active-Directory-Domänendienstes aus.

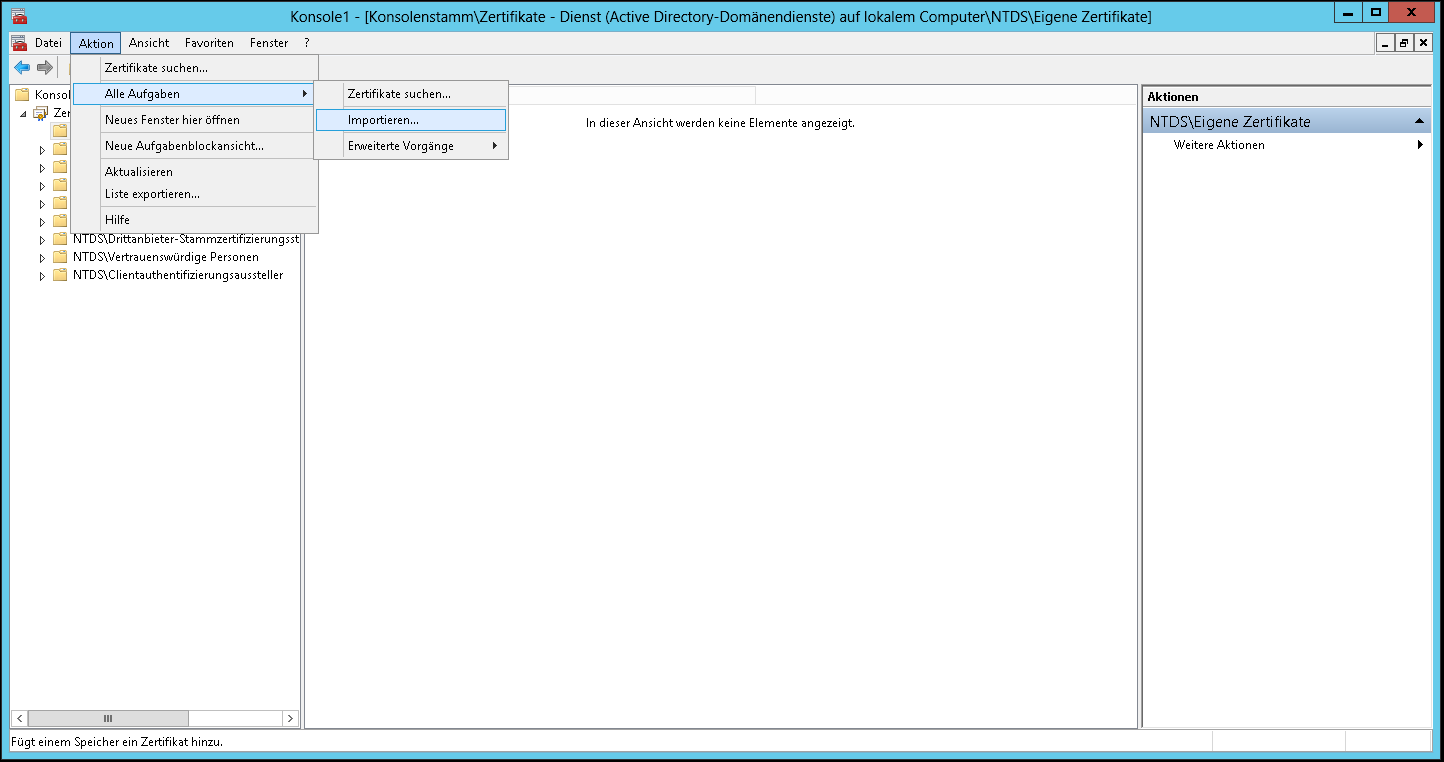


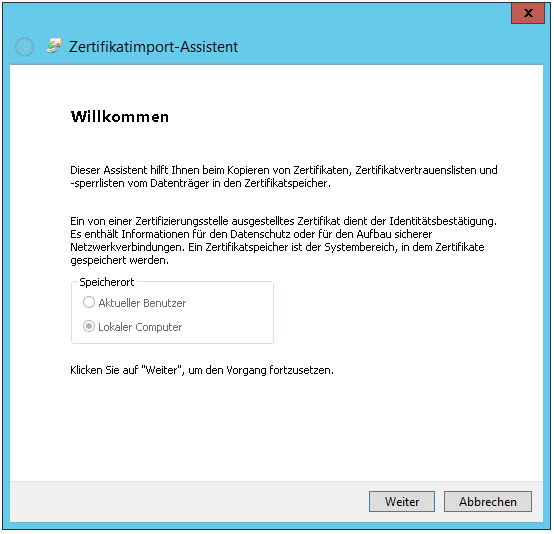
Fügen sie das Snap-In zum Konsolenstamm.



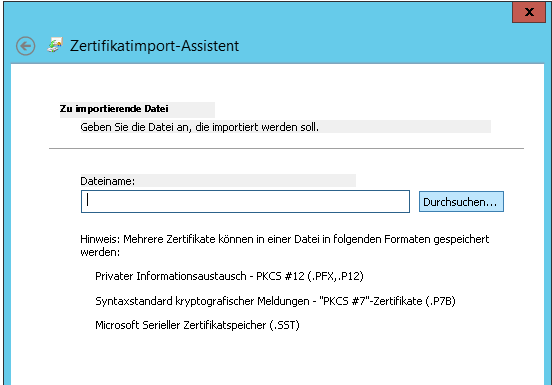
## Import des Zertifikates

Wählen Sie Aktionen->Alle Aufgaben->Importieren.

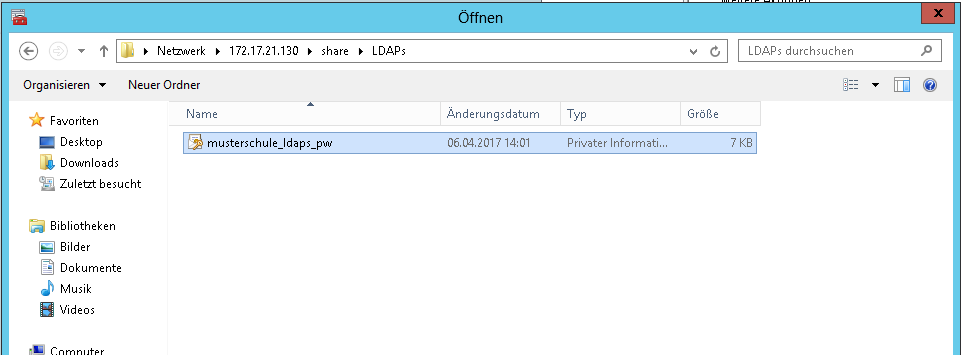


Ein Wizard zum Import von Zertifikaten öffnet sich.

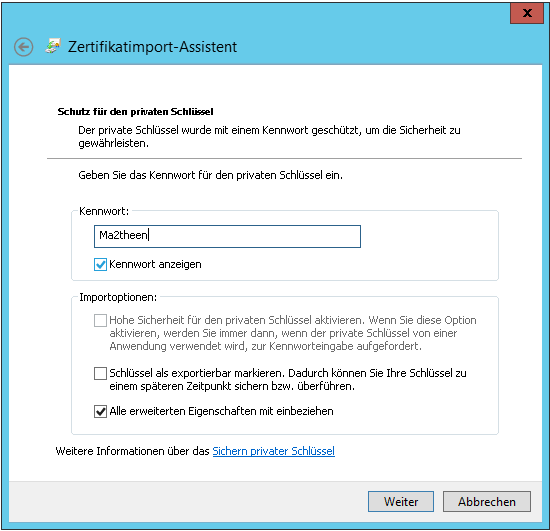
Wählen Sie im nächsten Fenster die Funktion „Durchsuchen…“.

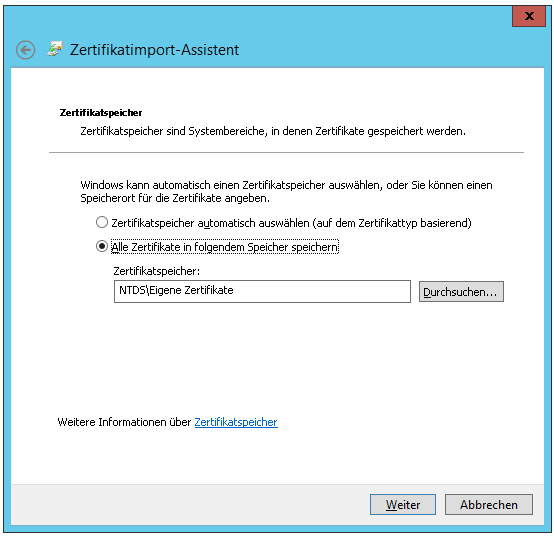


Navigieren Sie zu dem Pfad unter dem Sie das Zertifikat gespeichert haben. Wählen Sie als Filter für Dateiendungen „\*.pfx“.

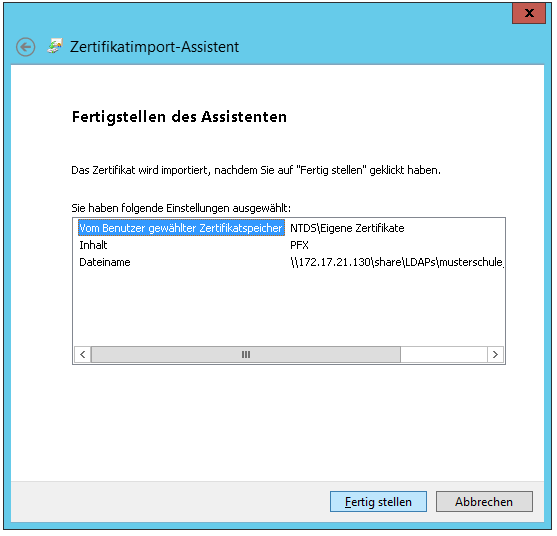


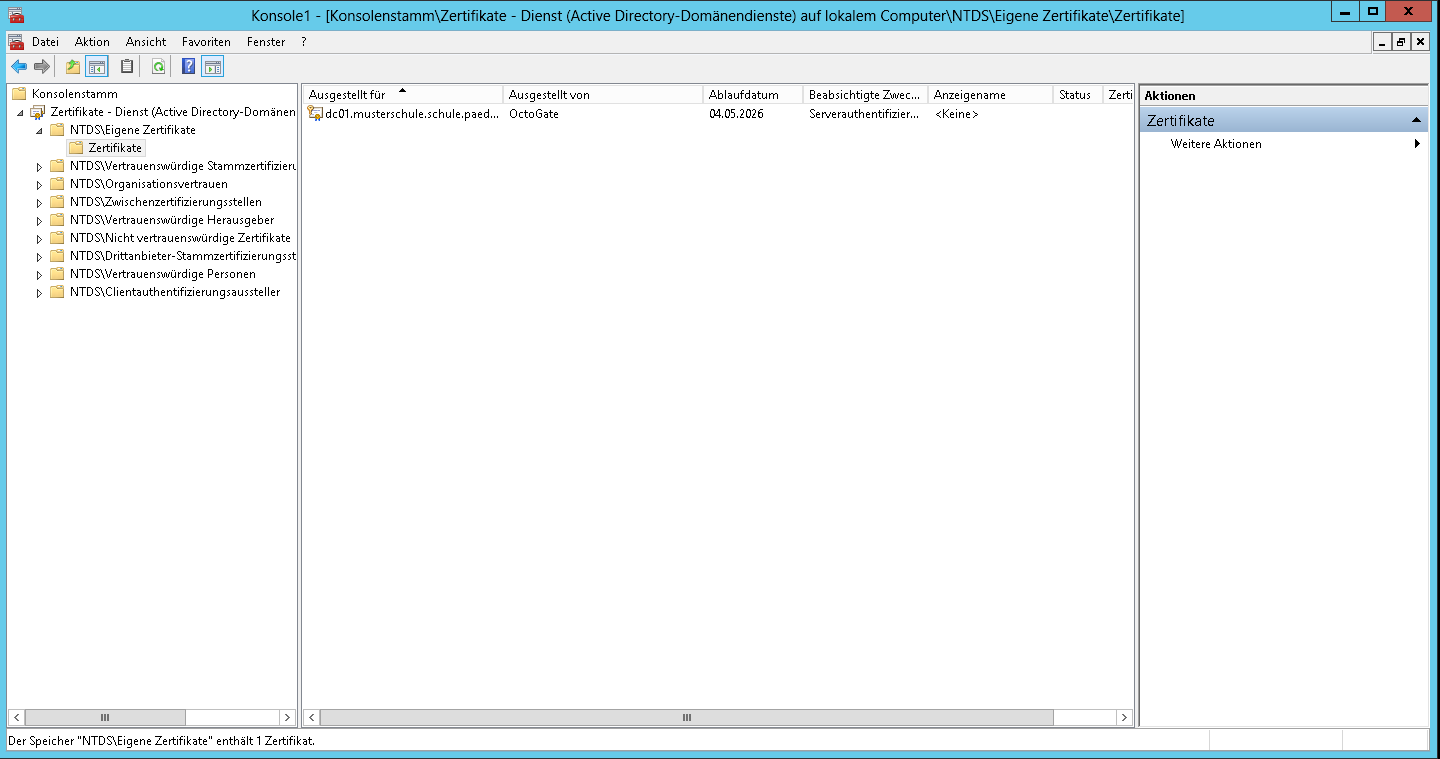
Das Passwort für den Import lautet Ma2theen. Importieren Sie alle erweiterten Eigenschaften (diese sind notwendig, damit der AD-DS das Zertifikat auch benutzt).



Wählen Sie als Zertifikatspeicher „NTDS\Eigene Zertifikate“.

Schließen Sie den Import ab.



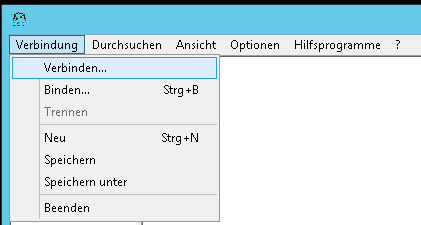
Ihr Zertifikatspeicher sollte jetzt das Zertifikat für den AD-DS beinhalten. 

# LDAPs Test

Starten sie LDP.

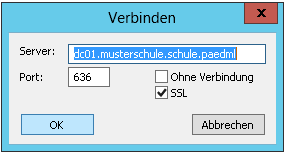


Binden Sie sich an den lokalen AD-DS (wir gehen davon aus, dass Sie als Administrator arbeiten).

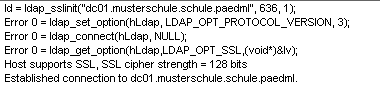


Tragen sie als Server „dc01.musterschule.schule.paedml“ ein. Dies ist notwendig, da ein SSL-Handshake nur fehlerfrei funktioniert, wenn der Name des Hosts zu dem Namen im Zertifikat passt. Das Zertifikat muss außerdem an einer Zertifizierungsstelle geprüft werden. In diesem Fall ist dies das OctoGate-Stammzertifikat (Hilfe zum Import finden Sie im Kapitel 6.1).

Wählen Sie die Checkbox „SSL“ damit zuerst eine Verschlüsselung aufgebaut wird. Der Port für LDAPs ist TCP:636.



Bei einer erfolgreichen LDAPs-Verbindung sehen Sie folgende Zeilen in der Ausgabe von LDP:



# Konfiguration der OctoGate

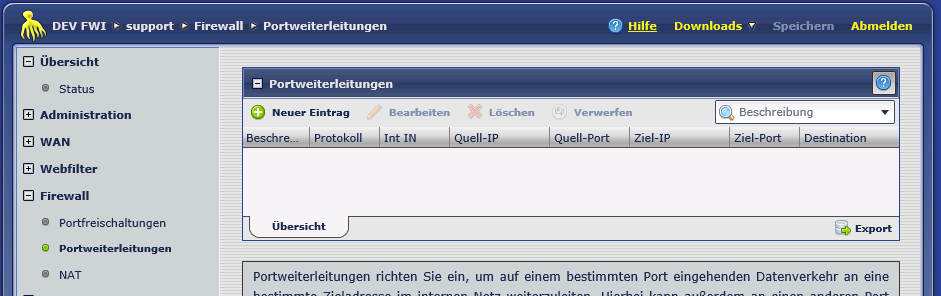
Öffnen Sie die Web-Benutzeroberfläche Ihrer OctoGate. Diese ist aus dem Intranet unter der URL <http://octo.octo/> zu erreichen. Sie werden auf die sichere Login-Page https://<OctoGate>.ozone.octogate.de:444/ weitergeleitet.



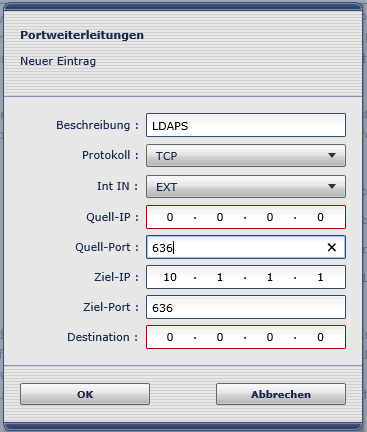
Melden Sie sich als „admin“ an. Sie sollten jetzt zur Statusseite gelangt sein.

## Portweiterleitung an den ADS

Navigieren Sie zum Menüpunkt „Firewall“ -> „Portweiterleitungen“.



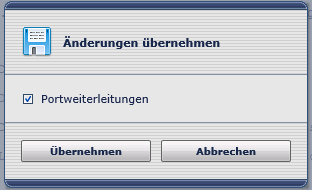
Wählen Sie “Neuer Eintrag”. Eine Maske mit den notwendigen Details für die Firewall-Regel erscheint.



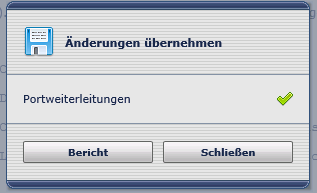
Bitte übernehmen Sie die Werte wie in dem Screenshot. Sie sollten allgemeine Gültigkeit für alle paedMLs haben.

Optional ist die Angabe der Quell-IP. Die IP 0.0.0.0 steht für alle IPs, Sie können aber auch auf die Quell-IP Ihres Webservers einschränken.

Nach der Bestätigung wählen Sie „Speichern“. Eine Bestätigungsbox erscheint.



Wählen Sie „Übernehmen“. Es sollte eine Bestätigung der Übernahme der Regeln erscheinen.



Damit ist die Konfiguration der OctoGate abgeschlossen.

Ein Test dieser Konfiguration kann mit Openssl durchgeführt werden. Dazu sehen Sie bitte im Kapitel 6.2 nach.

# Konfiguration des Webservers

Auf Ihrem Webserver läuft wahrscheinlich eine Webapplikation, die über das LDAP-Protokoll Benutzer authentifizieren soll.

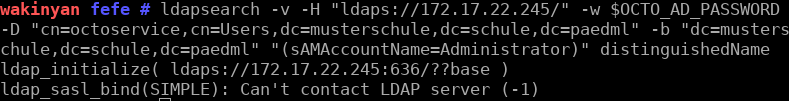
Die Webapplikation wird sich früher oder später wahrscheinlich der OpenLDAP – Bibliothek bedienen, um das LDAP-Protokoll zu benutzen.

Die OpenLDAP – Bibliothek wird sich des Systemeigenen SSL-Providers bedienen, um eine LDAPs-Verbindung aufzubauen.

**Ein SSL-Provider versucht immer, die Identität der Gegenstelle anhand des Hostnamens zu überprüfen. Dies kann in diesem Fall aber nur zu einem Fehler und danach zum Abbruch der Verbindung führen.**

Da der ADS der paedML unter dem Hostnamen DC01.MUSTERSCHULE.SCHULE.PAEDMl läuft, akzeptiert er nur Zertifikate die auf diesen Hostnamen ausgestellt sind. Dieser Hostname ist über das Internet nicht auflösbar, deswegen muss die LDAPs-Verbindung per IP/Hostname der OctoGate aufgebaut werden. Damit ist aber die Verifizierung des Hostnamens ausgeschlossen („octogate.ozone.octogate.de“ ist ungleich „dc01.musterschule.schule.paedml“).

In einem Test sieht das Problem etwa so aus:



Es gibt für dieses Problem zwei Lösungsansätze: Manuell einen Host-Eintrag für „dc01.musterschule.schule.paedml“ auf dem Webserver hinzufügen oder die Verifizierung des Hostnamens deaktivieren.

Da der Hostname nicht einmalig ist kann bei Webhostings für mehrere paedMLs unter Umständen kein solcher Eintrag erstellt werden.

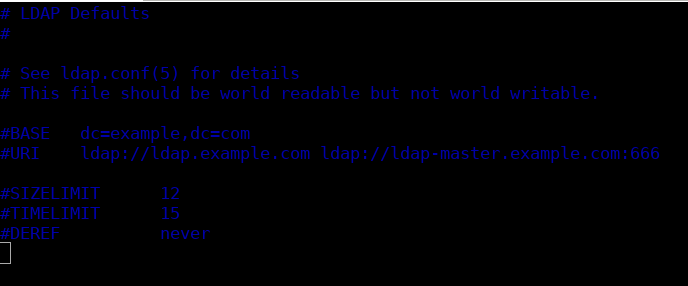
Es bleibt deswegen nur, die Verifizierung des Hostnamens abzustellen. Bitte fragen Sie dazu den zuständigen Administrator Ihres Webhosters.

## Verifizierung des Hostnamens in OpenLDAP abschalten

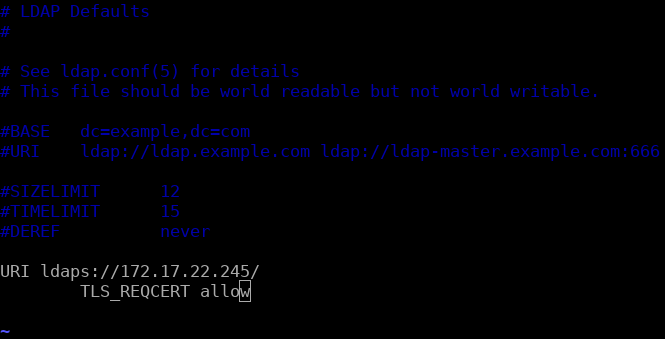
OpenLDAP kann per Konfigurationsdirektive den SSL-Provider anweisen, den Hostnamen nicht zu überprüfen.

Dazu muss die Konfigurationsdatei „ldap.conf“ editiert werden. Der Ort dieser Datei ist je nach Distribution in einem unterschiedlichen Verzeichnis und deshalb der Dokumentation der Distribution zu entnehmen.

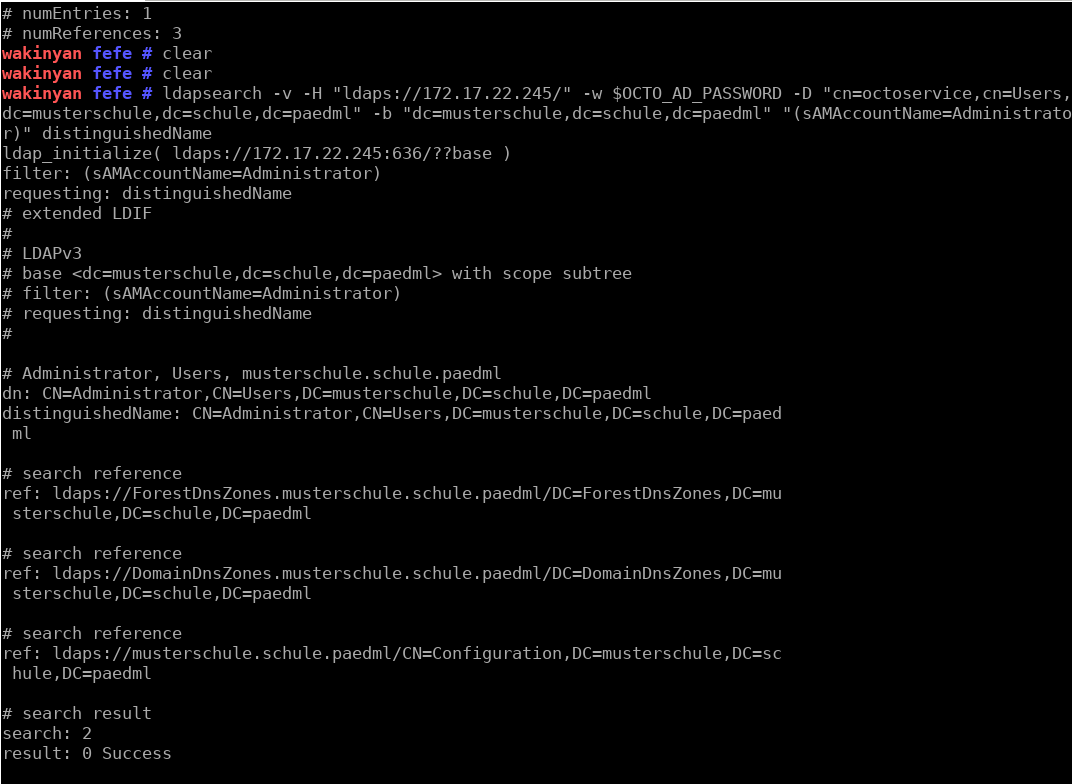
Eine leere OpenLDAP\_Konfigurationsdatei:



In dieser Datei muss eine Sektion für Ihren ADS hinzugefügt werden. Der gültige Syntax ist der Dokumentation von OpenLDAP zu entnehmen:



Danach sieht eine Überprüfung mit ldapsearch folgendermaßen aus:



Funktioniert die Verbindung jetzt steht auch LDAPs in einer Webapplikation nichts mehr im Weg. Haben Sie trotzdem noch Probleme Lesen Sie bitte im Kapitel 6.3.

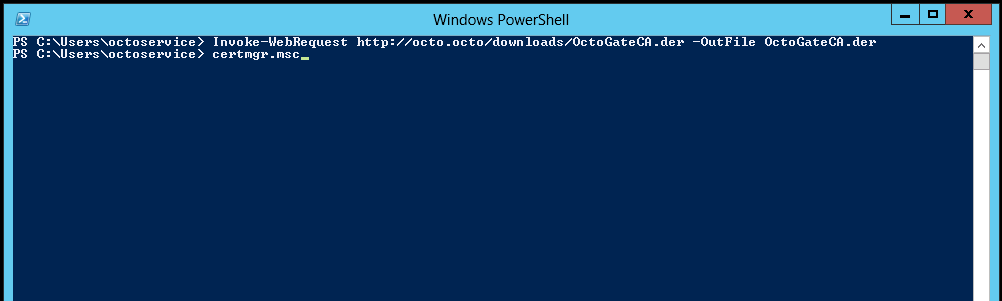
# Anhang

## Import des OctoGate Zertifikates auf dem ADS

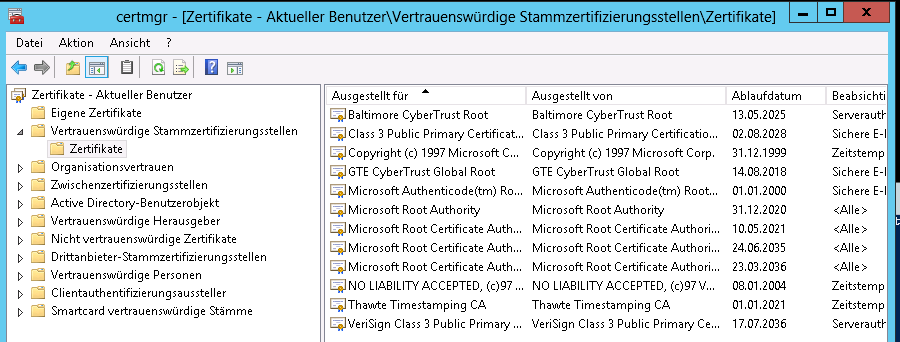
In der paedML kommt das Stammzertifikat der OctoGate nicht vorinstalliert auf dem DC01.

Sollten Sie Probleme mit dem LDP-Test haben, kann dies daher rühren, dass ein gültiges Stammzertifikat benötigt wird, um das Zertifikat des DC01 zu überprüfen (für den Betrieb von LDAPs ist dies aber nicht notwendig).

Um das Stammzertifikat zu importieren, öffnen Sie die Powershell. Laden Sie das Stammzertifikat per „Invoke-Webrequest [http://octo.octo/downloads/OctoGateCA.der -OutFile OctoGateCA.der](http://octo.octo/downloads/OctoGateCA.der%20-OutFile%20OctoGateCA.der)” runter:

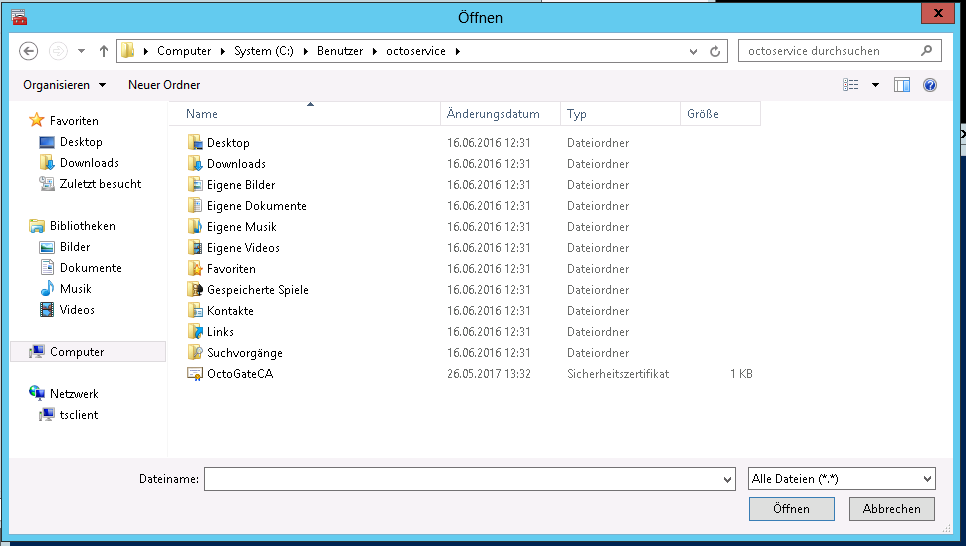


Öffnen Sie anschließend certmgr.msc um das Stammzertifikat zu importieren. Navigieren Sie zu „Vertrauenswürdige Stammzertifizierungsstellen -> Zertifikate“:

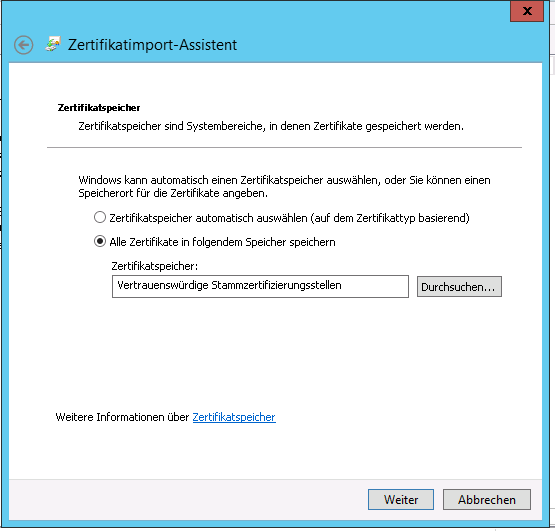


Wählen Sie den Reiter „Aktion -> Alle Aufgaben -> Importieren …“.

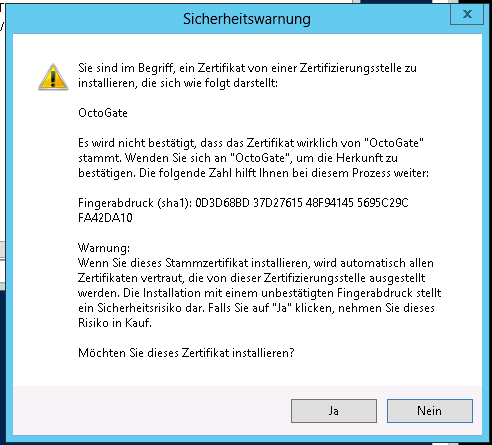
Ein Wizard für den Zertifikatsimport öffnet sich. Selektieren Sie das Zertifikat:



Wählen Sie „vertrauenswürdige Stammzertifizierungsstellen“ als Zertifikatsspeicher.



Bestätigen Sie die Sicherheitsabfrage:



Damit sollte LDP in der Lage sein, eine Verbindung zu „ldaps://dc01.musterschule.schule.paedml/“ aufzubauen.

## Test der Port-Weiterleitung

Die Port-Weiterleitung kann unabhängig von LDAPs getestet werden, in dem nur eine sichere Verbindung aufgebaut wird. Dazu muss der LDP-Test bereits abgeschlossen sein.

Notwendig ist hierfür ein Tool zum aufbauen einer gesicherten Verbindung. Für gewöhnlich wird dazu das Frontend von OpenSSL verwendet.

Der Syntax ist simpel:

„openssl s\_client –connect serverip:636”



Erhalten Sie eine Antwort von „CN = dc01.musterschule.schule.paedml“ sprechen Sie durch die OctoGate mit Ihrem ADS.

## Verbindungsproblem LDAPs

Ein mögliches weiteres Verbindungsproblem ist, dass sich Webhost und ADS nicht auf eine Verschlüsselung einigen können.

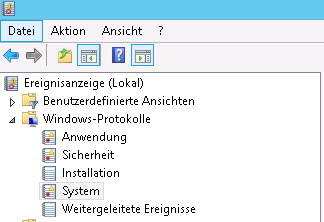
Dies ist eigentlich nur der Fall, wenn der Webhost sehr alt ist, also nur Cipher der SSLv2 oder SSLv3 klasse spricht. Diese Fehlerklasse kann aber trotzdem vorkommen, wenn in der „ldap.conf“ manuell eine Cipherliste spezifiziert wurde.

Ist dies der fall, kann das im Event-Log des ADS nachgelesen werden. Dort werden Fehler der Schannel komponente von Windows protokoliert. Schannel ist der Windowseigene SSL-Provider.

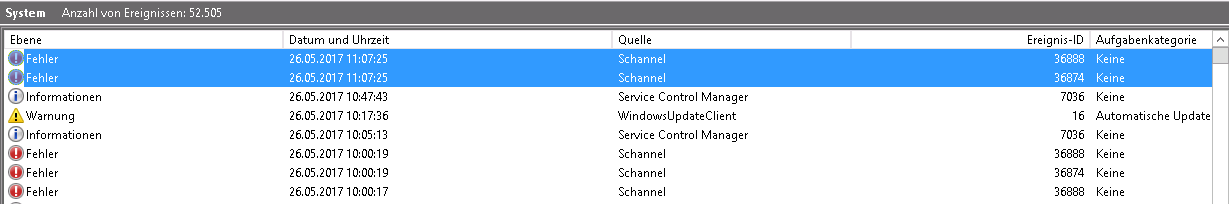
Um die Ereignisanzeige einzusehen öffnen Sie eventvwr.msc.



Navigieren Sie zu „Windows-Protokolle->System“



Fehler von Schannel indizieren einen Cipher-Mismatch:



Sehen Sie sich die Fehlerdetails an:



Steht dort, dass „keine der Verschlüsselungssammmlungen, die von der Clientanwendung unterstützt werden“ vom Server unterstützt werden, sollten Sie Ihren Webhoster informieren.

Kann er dieses Problem nicht lösen, empfehlen wir, aus Sicherheitsgründen auf einen anderen Hoster zu wechseln.