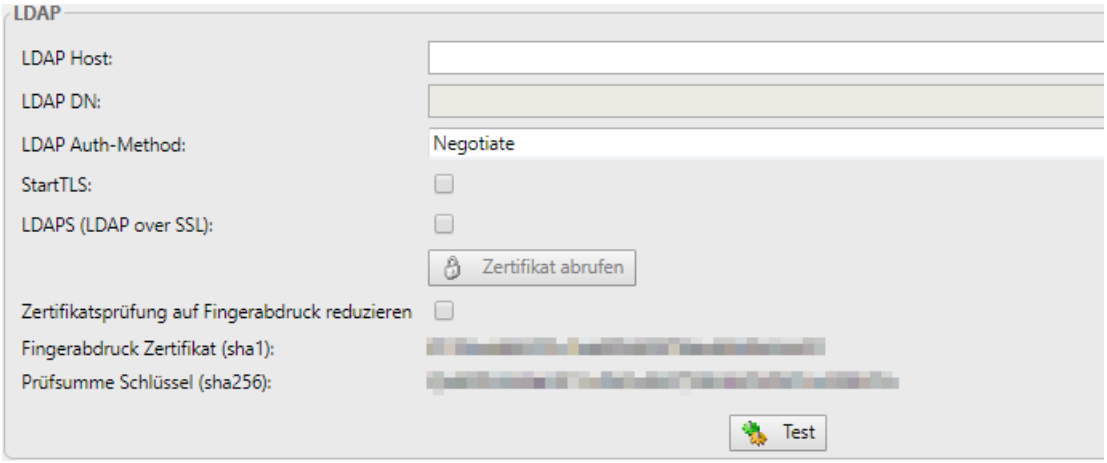
Anleitung LDAP

(Stand 07.10.2021)

Inhaltsverzeichnis

1 LDAP Serverseitig aktivieren

Die Vertrauensstellung des LDAP-Servers kann nun wahlweise über ein in GDix gespeicherten Fingerabdruck oder den Zertifikatsspeicher von Windows (certmgr.msc) erfolgen. Um sich in GDix über LDAP anmelden zu können, müssen in eBase unter dem Reiter „Benutzerverwaltung / Einstellungen“ einige Einstellungen vorgenommen werden.



Hier sollte zunächst die „LDAP Auth-Method“ auf „Negotiate“ gestellt werden.

Im Anschluss tragen Sie bitte den „LDAP Host“ ein. Dies ist entweder nur der der DNS-Suffix oder der Fully Qualified Domain Name (FQDN) des LDAP-Servers. Sie können den FQDN erfahren, indem Sie auf dem Server in einer Kommandozeile „ipconfig /all“ eingeben und hier den Hostnamen sowie den DNS- Suffix auslesen. Hier ein Beispiel für eine „ipconfig“ Ausgabe:

```
Hostname ..........................: FWXXXXXXX
Primäres DNS-Suffix ...............: pb.rz.in.gad.de
Knotentyp .........................: Hybrid
IP-Routing aktiviert ..............: Nein
WINS-Proxy aktiviert ..............: Nein
DNS-Suffixsuchliste ...............: sd4817.gad.de
```

Hinter dem angegebenen LDAP Host geben Sie den Port mit an. Der Standard-Port für LDAP lautet „:389“. Wenn Sie die Daten verschlüsselt versenden möchten, benötigen Sie zudem die Checkbox „StartTLS“. Wenn Sie LDAPS verwenden, benötigen Sie den Port „:636“ und die Checkbox „LDAPS (LDAP over SSL)“. Wenn Sie „LDAPS (LDAP over SSL)“ verwenden, gibt es zwei Arten der Zertifikatsprüfung; die Prüfung auf den Fingerabdruck und Prüfung über das Root-Zertifikat.

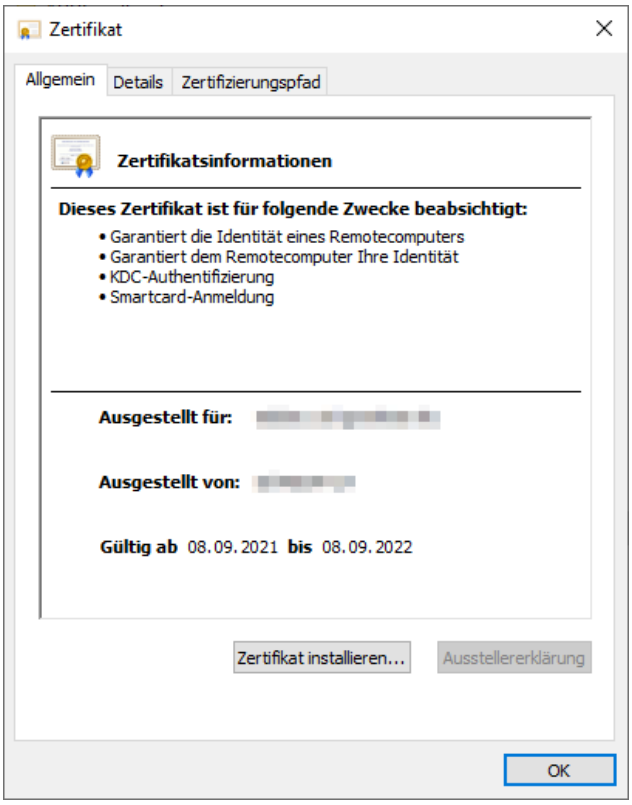
In beiden Fällen müssen Sie nach der Aktivierung von LDAPS einmal auf den Button „Zertifikat abrufen“ klicken. Es öffnet sich ein Fenster in dem Sie aufgefordert werden, das aktuelle Zertifikat Ihres LDAP zu speichern. Das gespeicherte Zertifikat kann dazu verwendet werden, das Root-Zertifikat herauszufinden und ggf. auf dem Server zu hinterlegten (siehe Punkt 2).

Die Option „Zertifikatsprüfung auf Fingerabdruck reduzieren“ dient der Auswahl zwischen den zwei Arten der Zertifikatsprüfung. Wird der Haken nicht gesetzt (Standard), wird das auf dem Server im Zertifikatsspeicher hinterlegte Root-Zertifikat geprüft. Bei gesetztem Haken wird der Fingerabdruck des Zertifikats abgeglichen.

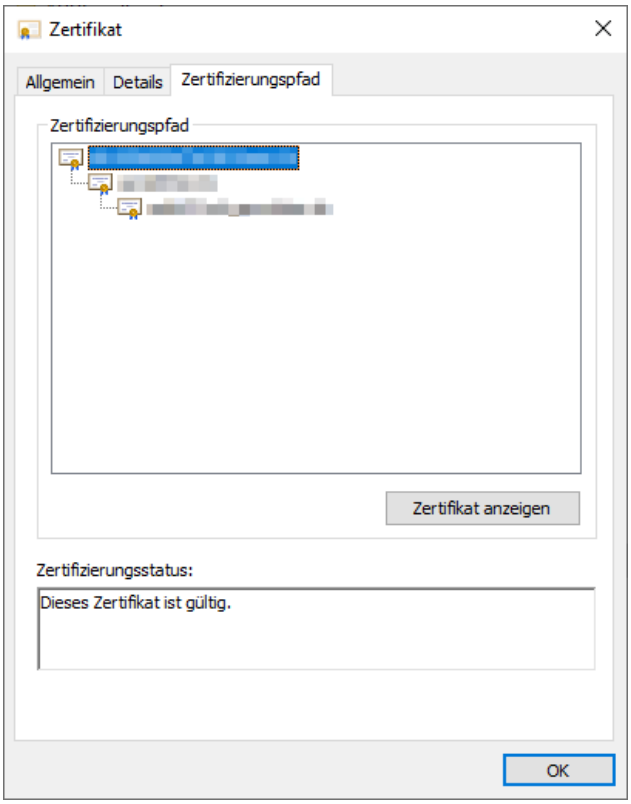
2 Prüfung und Installation des Root-Zertifikat

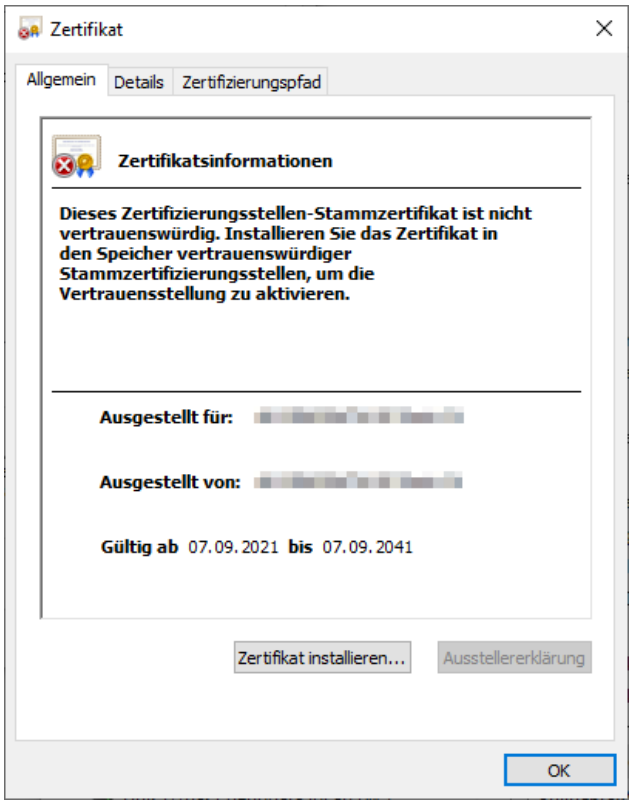
Das Root-Zertifikat muss nur auf dem Server installiert werden.

Durch Klick auf den Button „`Zertifikat abrufen`“ kann das aktuelle Zertifikat Ihres LDAP unter einem beliebigen Ordner gespeichert werden. Sobald das Zertifikat gespeichert wurde, wird durch Doppelklick auf dieses die Zertifikatinformationen geöffnet. (s. rechts)

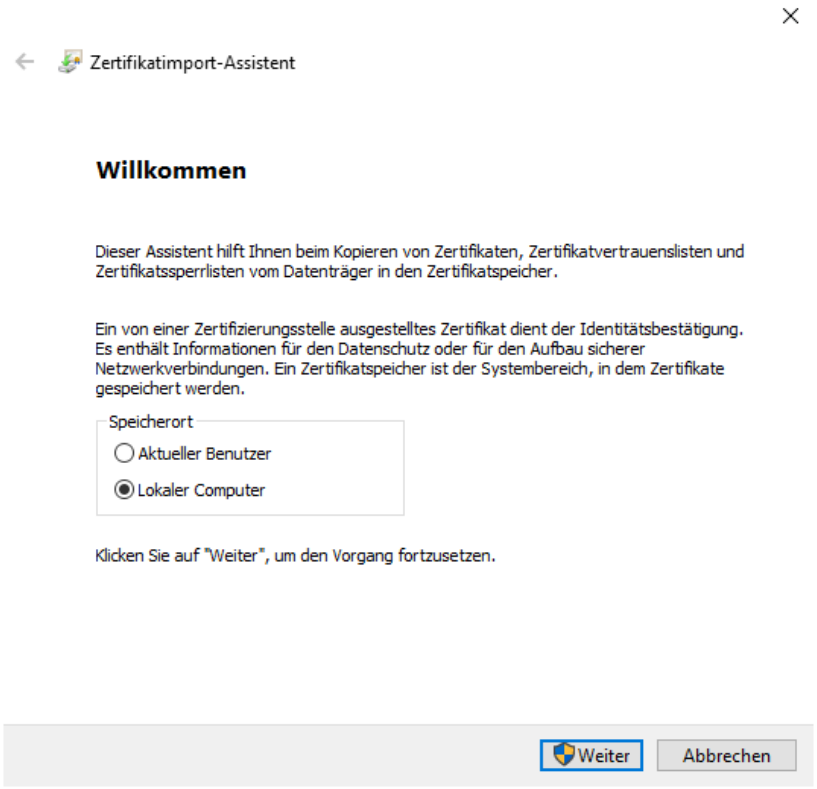


In diesen kann unter dem Reiter „`Zertifizierungspfad`“ durch Markierung des ersten Eintrages und klick des Buttons „`Zertifikat anzeigen`“ (s. links unten) das aktuelle Root-Zertifikat eingesehen werden. (s. rechts unten)

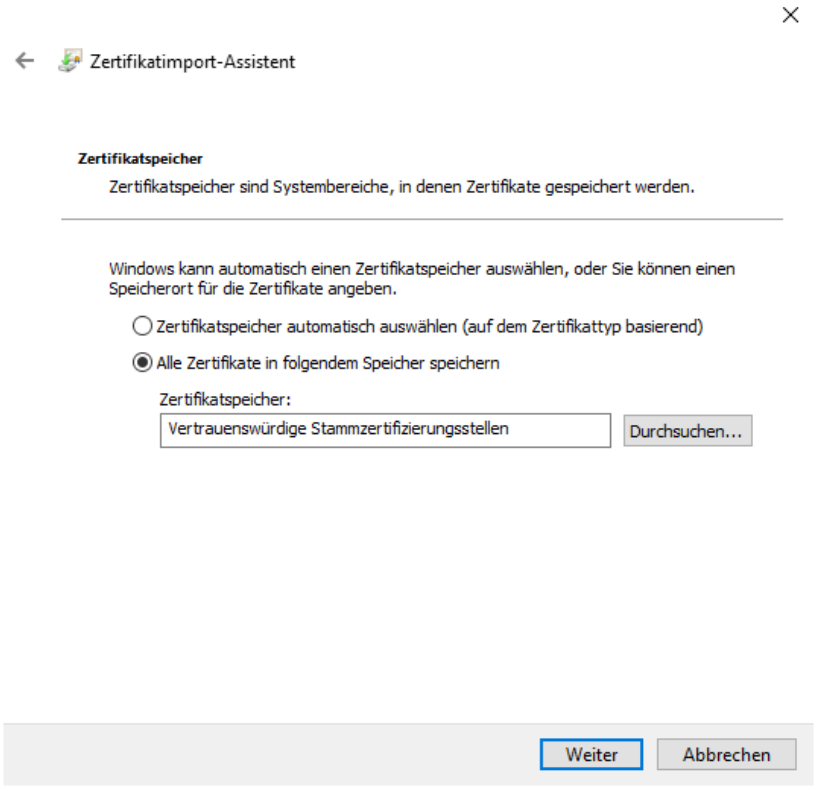




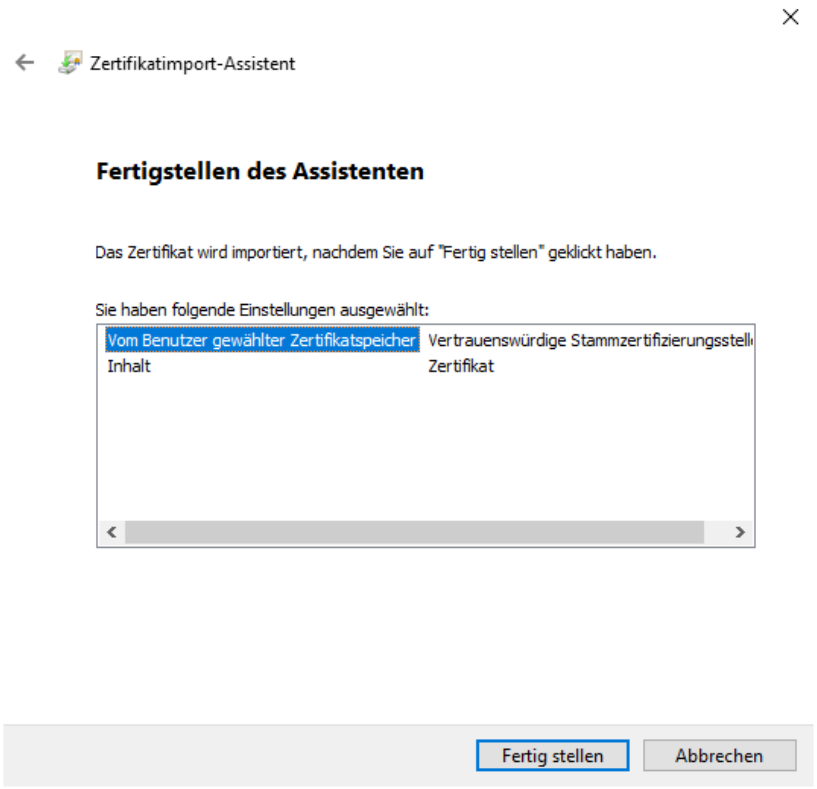
Durch den Button „Zertifikat installieren“ wird der Zertifikatimport-Assistent geöffnet. In diesem wird der Punkt „Lokaler Computer“ gewählt und der Vorgang fortgesetzt.



Im folgenden Fenster muss die Checkbox „Alle Zertifikate in folgendem Speicher speichern“ ausgewählt sein und als Speicher „Vertrauenswürdige Stammzertifizierungsstellen“ gewählt werden. Über „Weiter“ kommt man zum letzten Fenster.

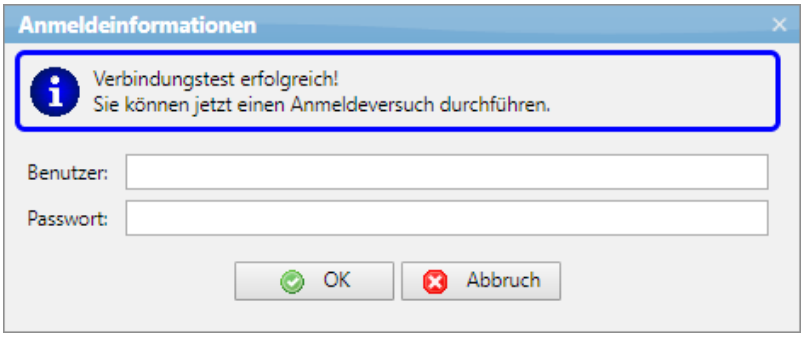


Durch den Klick auf den Button „`Fertig stellen`“ wird das neue Zertifikat erstellt und aktiviert.



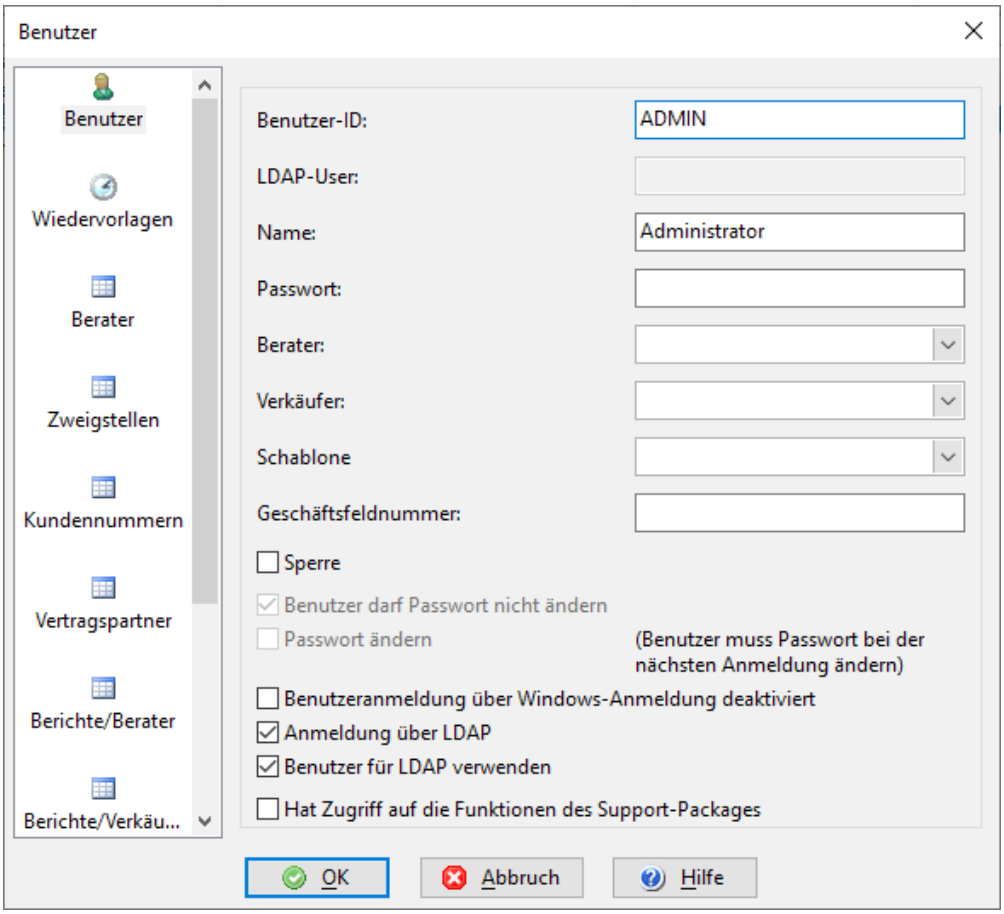
3 Testen der Verbindung zum LDAP-Server

Im Anschluss können Sie ihre Konfiguration mit dem Button „`Test`“ einmal durch einen Anmeldeversuch kontrollieren. Werden hier nun Ihre Anmeldeinformationen angefordert, konnte der Server die Verbindung zum LDAP-Server herstellen.



4 LDAP für die Benutzer aktivieren

Bei jedem Benutzer, der über LDAP angemeldet werden soll, muss zunächst in der Benutzerverwaltung der Haken „Anmeldung über LDAP“ gesetzt werden.



Nun gibt es zwei Möglichkeiten, entweder man setzt den zweiten Haken „Benutzer für LDAP verwenden“, welcher die GDix-Benutzer-ID als LDAP-Anmeldenamen verwendet, oder man füllt das Feld „LDAP-User“ aus.

Beim zweiten Fall wird der eingetragene Wert als Benutzername für die LDAP-Authentifizierung verwendet.