Inhaltsverzeichnis

1. Allgemeines 2
1.1. Überblick 2
1.2. Voraussetzungen 2
2. LDAP-Konfiguration 3
2.1. LDAP-Konfiguration für Microsoft Active Directory (AD) 3
2.2. LDAP-Konfiguration für Novell eDirectory und OpenLDAP 7
3. Auswirkungen der LDAP-Einrichtung 12
3.1. Anwendungsbeispiele 12

LDAP-Schnittstelle für CaliforniaX

In diesem Dokument wird die Einrichtung der LDAP-Schnittstelle für CaliforniaX beschrieben.

1. Allgemeines

1.1. Überblick

Das Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll aus der Netzwerktechnik. Es erlaubt die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes über ein IP-Netzwerk.

LDAP basiert auf dem Client-Server-Modell und kommt bei Verzeichnisdiensten zum Einsatz. Es beschreibt die Kommunikation zwischen dem LDAP-Client (hier CaliforniaX) und dem Verzeichnis-Server. Aus einem solchen Verzeichnis können objektbezogene Daten, wie zum Beispiel Rechnerkonfigurationen oder wie hier Gruppenzugehörigkeiten von Personen, ausgelesen werden. Die Kommunikation erfolgt auf Basis von Abfragen.

CaliforniaX ist in der Lage, die Benutzeranmeldung über LDAP-Abfragen zu automatisieren. Hierzu wird im Anmeldefenster der Benutzername automatisch über eine LDAP-Anfrage gefüllt. Dies ist der Name, mit dem sich der Benutzer am Rechner angemeldet hat. Auch das Kennwort für die Anmeldung an CaliforniaX wird voreingestellt, so dass hier im Allgemeinen keine manuellen Angaben mehr notwendig sind.



Abbildung 1 CaliforniaX Anmeldedialog bei aktivierter LDAP-Schnittstelle

1.2. Voraussetzungen

Am LDAP-Server:

- Die drei LDAP-Varianten *Microsoft Active Directory*, *Novel eDirectory* und *OpenLDAP* mit aktivierter *memberOf*-Option werden unterstützt.
- Alle CaliforniaX–Benutzer sind Mitglied von eigens angelegten Gruppen. Die Namen dieser Gruppen beginnen mit einem gemeinsamen Präfix, welches frei wählbar ist, z.B. Cal_. Eine LDAP-Gruppe für CaliforniaX heißt dann z.B. Cal_Administrator oder Cal_User.
- Ein Benutzer kann auch mehreren Gruppen angehören.
- Verschachtelte Gruppen werden nicht unterstützt

In CaliforniaX:

- Die LDAP-Erweiterung muss lizenziert sein.
- Der Gruppenname ohne Präfix (im obigen Beispiel Administrator bzw. User) sollte in den Zugriffsrechten bereits als Rechtegruppe existieren und mit den gewünschten Rechten versehen sein.
- Beides ist nicht zwingend notwendig, da das LDAP-Modul in CaliforniaX fehlende Gruppen im Allgemeinen automatisch anlegt und außerdem den Benutzer zum Mitglied der neuen Gruppe(n)/Rolle(n) macht. Wir empfehlen aber ausdrücklich, schon aus Gründen der Steuerung der gewünschten Zugriffsrechte, die Erfassung von gleichlautenden Rechtegruppen in CaliforniaX.

2. LDAP-Konfiguration

2.1. LDAP-Konfiguration für Microsoft Active Directory (AD)

Starten Sie das CaliforniaX-ConfigurationCenter bzw. die Datei „*…\Program Files\G&W Software\CaliforniaX.ConfigurationCenter.exe*". Dadurch wird aktuell das Datenbankwerkzeug DBTool gestartet. Melden Sie sich am CaliforniaX-Datenbankserver an. Erfragen Sie ggf. Benutzername und Kennwort bei Ihrem Datenbank-Administrator oder beim G&W-Support.

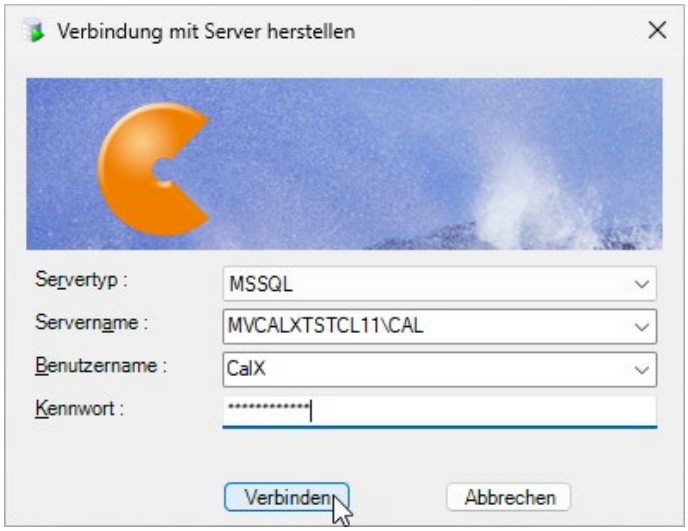


Abbildung 2 Anmeldedialog DBTool

Öffnen Sie in der Baumstruktur den Bereich *Datenbanken* und dort die CaliforniaX-Datenbank *CalX* bzw. das Oracle-Benutzerschema CALX. Klicken Sie mit der rechten Maustaste auf *Benutzertabellen* und wählen im Kontextmenü den Menüpunkt *LDAP einrichten*.

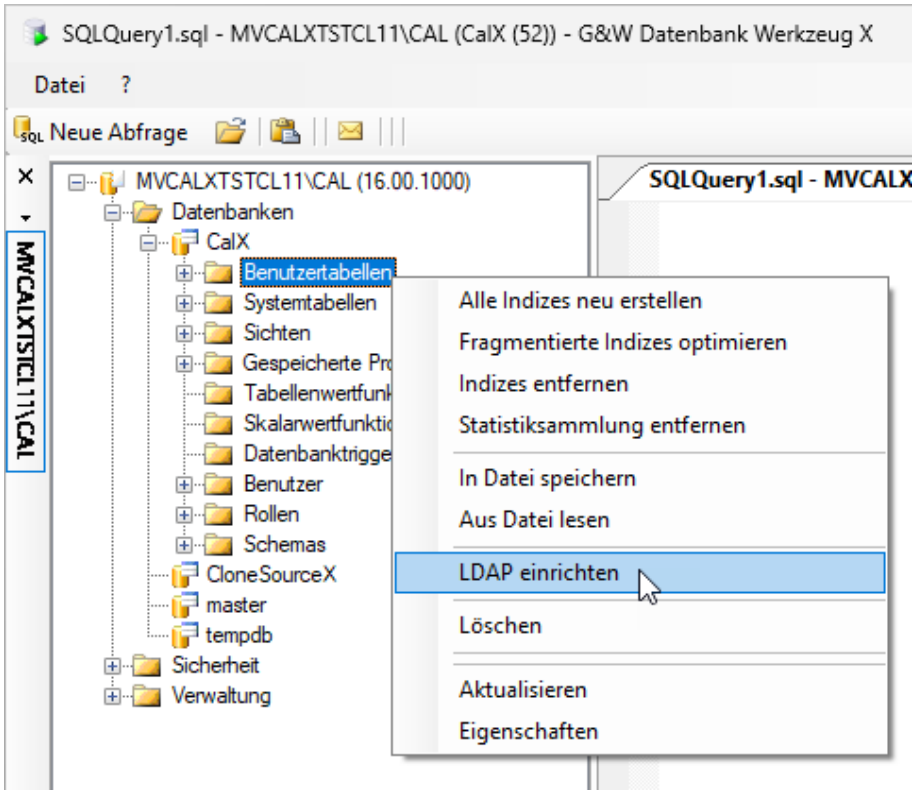


Abbildung 3 Aufruf Menüpunkt „LDAP einrichten"

Im ersten Schritt der Konfiguration wird die noch leere Datenbanktabelle *GW_LDAP_CONF* mit Vorbelegungen befüllt und für kundenspezifische Anpassungen im Datenbereich des DBTool geöffnet.

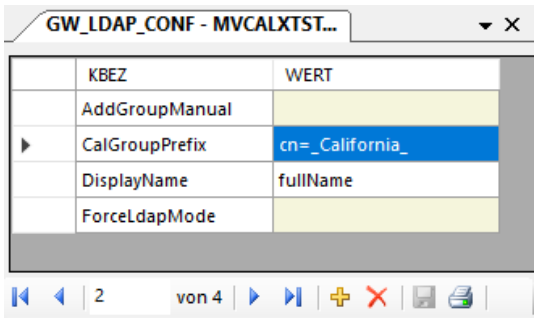


Abbildung 4 Benutzertabelle GW_LDAP_CONF

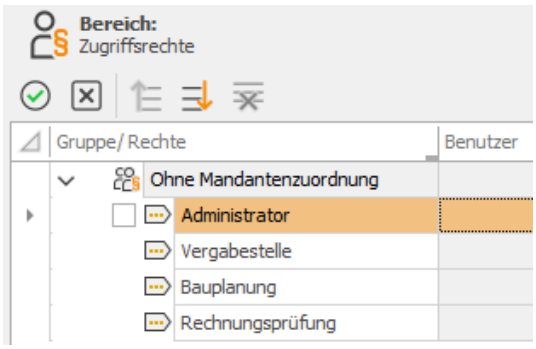


Abbildung 5 CaliforniaX Zugriffsrechteverwaltung

Die Namen der LDAP-Gruppen für CaliforniaX setzen sich i.d.R. aus einem gemeinsamen Präfix und dem Namen der Rechtegruppe in CaliforniaX zusammen.

Beispielsweise wäre für die LDAP-Gruppen *Cal_Adminstrator, Cal_Vergabestelle, Cal_Bauplanung usw.* das Präfix *„Cal_"*. Die CaliforniaX-Rechtegruppen hießen entsprechend *Administrator, Vergabestelle, Bauplanung* usw.

In der Zeile CalGroupPrefix der Tabelle GW_LDAP-CONF wird das CaliforniaX-Gruppenpräfix der LDAP-Gruppen mit *„cn=_California_"* vorgeschlagen.

Ersetzen Sie den Wert *„cn=_California_"* durch das LDAP-Gruppenpräfix z.B. *„Cal_"*.

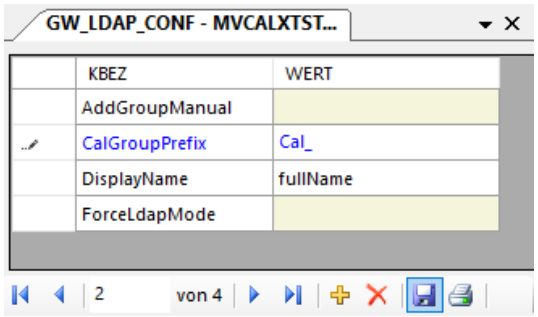


Abbildung 6 Benutzertabelle GW_LDAP_CONF

Speichern Sie Ihre Eingabe und schließen Sie die Tabelle über das X.

Wiederholen Sie im nächsten Schritt den Menüaufruf *LDAP einrichten* durch Klick mit der rechten Maustaste auf *Benutzertabellen* in der Baumstruktur des DBTool.

Es öffnet sich ein Dialog zur Eingabe der Verbindungsparameter zu einem LDAP-Verzeichnisserver. Dieser wird nur im Fall von Novell eDirectory, OpenLDAP und LDAPS benötigt siehe Abschnitt 2.2.

Für Microsoft Active Directory überspringen Sie diesen Dialog durch Klick auf *Abbrechen*.

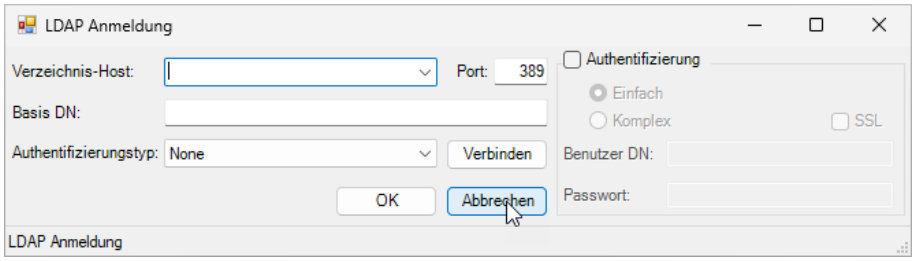


Abbildung 7 Verbindungsparameter zum LDAP-Server (nicht benötigt)

Im Datenbereich von DBTool wurde die Tabelle *GW_LDAP_GROUPMAP* geöffnet und befüllt. Die Tabelle regelt die Zuordnung der CaliforniaX-Active Directory Gruppen (Spalte *CN*) zu den CaliforniaX-Rechtegruppen (Spalten GRUPPENID und KOMMENTAR).

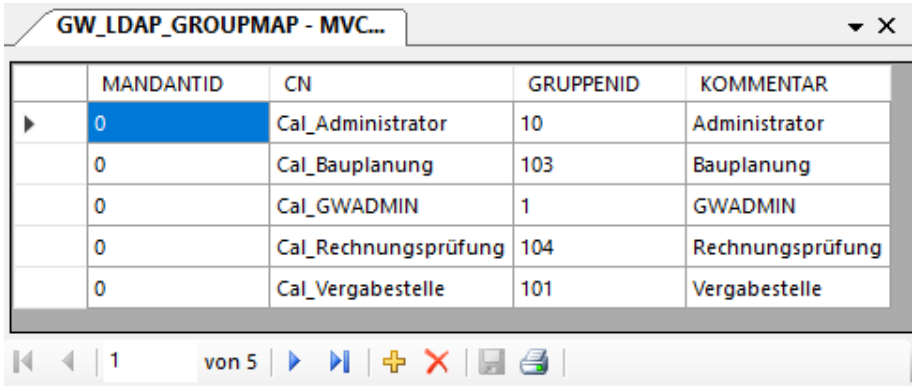


Abbildung 8 Benutzertabelle GW_LDAP-GROUPMAP

Wenn die Gruppennamen im LDAP-Verzeichnisdienst und CaliforniaX bis auf die Präfixe gleich lauten (Empfehlung), ist hier keine Anpassung notwendig. Im seltenen Fall, dass zwei unterschiedliche Active Directory-Gruppen ein und derselben CaliforniaX-Gruppe zugeordnet werden sollen, kann dies durch eine gleichlautende Gruppen-ID in der Spalte GRUPPENID erreicht werden.

Speichern Sie Ihre Änderungen ab und beenden Sie das DBTool.

Im letzten Schritt der Konfiguration öffnen Sie die Datei *CalX.config* aus den CaliforniaX-Programmdateien *…\Program Files\G&W Software\CaliforniaX\Setup* zur Bearbeitung mit einem beliebigen Editor. Ergänzen Sie in der Sektion <CaliforniaX> den folgenden Eintrag:

<add key="LdapMode" value="2" />

```
1   <?xml version="1.0" encoding="utf-8"?>
2   <configuration>
3       <configSections>
4           <section name="CaliforniaX" type="System.Configura
5       </configSections>
6       <CaliforniaX>
7           <add key="DBServer" value="MVCALXTSTCL11\CAL" />
8           <add key="DBName" value="CalX" />
9           <add key="DBTyp" value="SQL Server" />
10          <add key="LdapMode" value="2" />
11      </CaliforniaX>
12  </configuration>
```

Abbildung 9 Konfigurationsdatei CaliforniaX.config

Hinweis:

- Wert „2" aktiviert die LDAP-Anmeldung für Microsoft Active Directory
- Wert „0" deaktivert die LDAP-Anmeldung

Damit ist die Konfiguration abgeschlossen. Eventuelle Rechteeinstellungen innerhalb von CaliforniaX werden unabhängig von LDAP in der Zugriffsrechteverwaltung von CaliforniaX vorgenommen.

Das Anmeldefenster von CaliforniaX wird nun immer den unter Windows angemeldeten (LDAP-) Benutzer voreinstellen.



Abbildung 10 CaliforniaX Anmeldedialog bei aktivierter LDAP-Schnittstelle (Aktive Directory)

Sollte sich ein unberechtigter Nutzer (nicht Mitglied der entsprechenden AD-CaliforniaX-Benutzergruppe) anmelden, erscheint folgende Meldung:

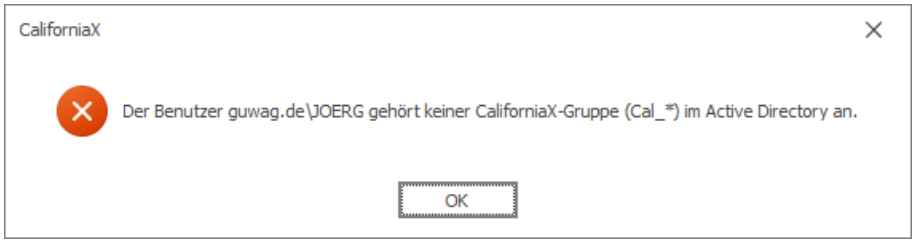


Abbildung 11 Warnhinweis bei Anmeldung unberechtigter Benutzer (Aktive Directory)

2.2. LDAP-Konfiguration für Novell eDirectory und OpenLDAP

Starten Sie das CaliforniaX-ConfigurationCenter bzw. die Datei „*…\Program Files\G&W Software\CaliforniaX.ConfigurationCenter.exe*". Dadurch wird aktuell das Datenbankwerkzeug DBTool gestartet. Melden Sie sich am CaliforniaX-Datenbankserver an. Erfragen Sie ggf. Benutzername und Kennwort bei Ihrem Datenbank-Administrator oder beim G&W-Support.

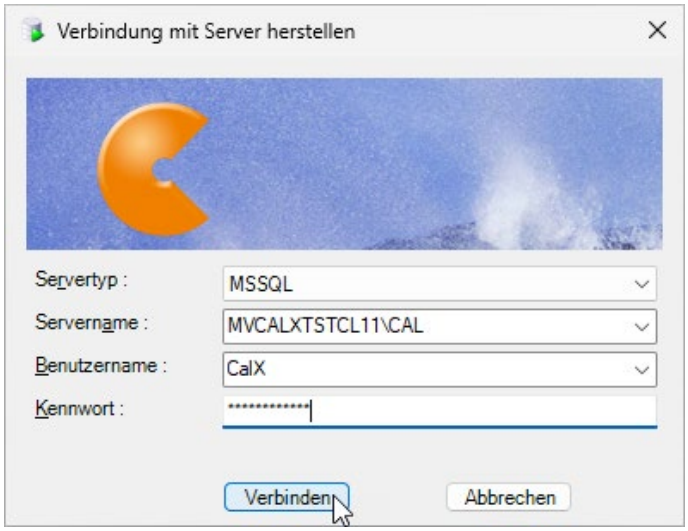


Abbildung 12 Anmeldedialog DBTool

Öffnen Sie in der Baumstruktur den Bereich *Datenbanken* und dort die CaliforniaX-Datenbank *CalX* bzw. das Oracle-Benutzerschema CALX. Klicken Sie mit der rechten Maustaste auf *Benutzertabellen* und wählen im Kontextmenü den Menüpunkt *LDAP einrichten*.

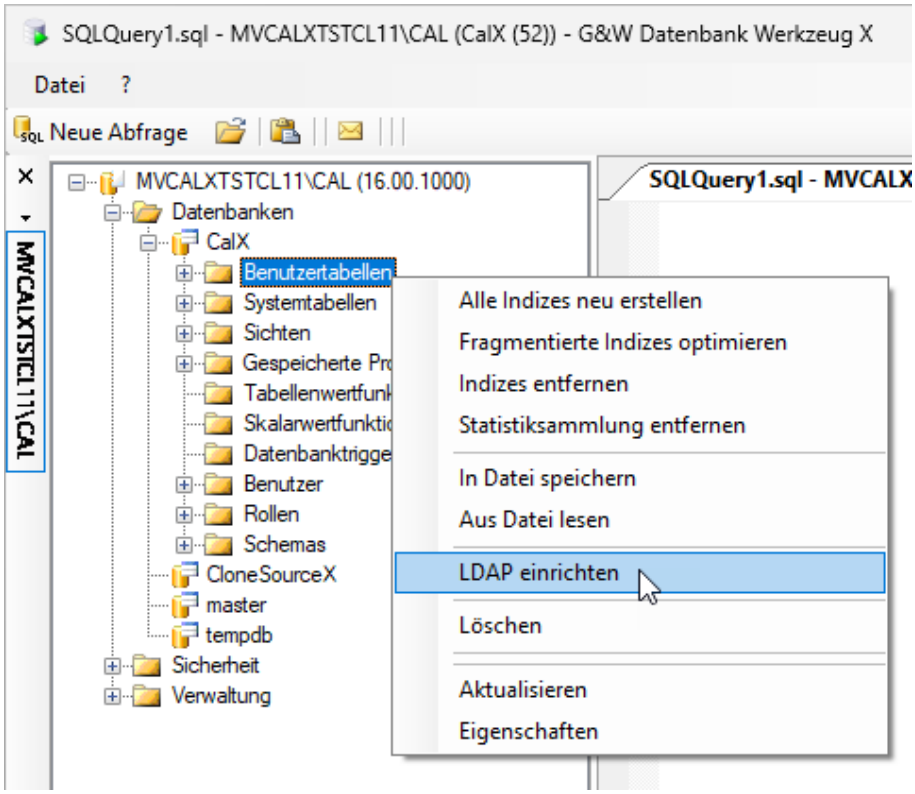


Abbildung 13 Aufruf Menüpunkt „LDAP einrichten"

Im ersten Schritt der Konfiguration wird die noch leere Datenbanktabelle *GW_LDAP_CONF* mit Vorbelegungen befüllt und für kundenspezifische Anpassungen im Datenbereich des DBTool geöffnet.

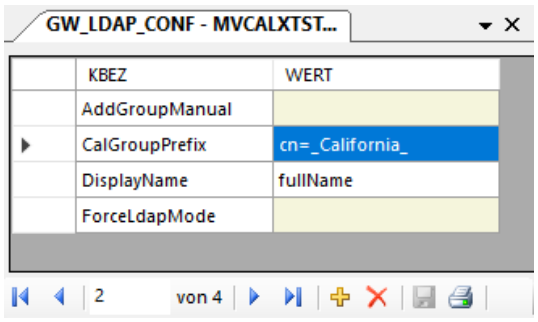


Abbildung 14 Benutzertabelle GW_LDAP_CONF

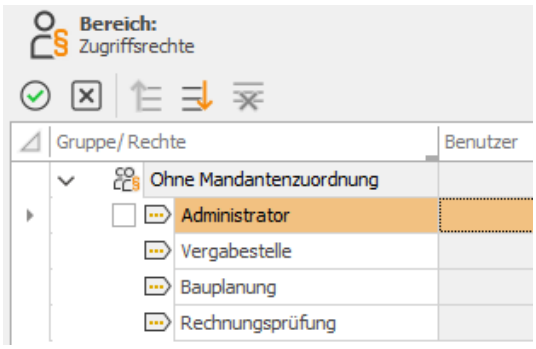


Abbildung 15 CaliforniaX Zugriffsrechteverwaltung

Die Namen der LDAP-Gruppen für CaliforniaX setzen sich i.d.R. aus einem gemeinsamen Präfix und den Namen der Rechtegruppe in CaliforniaX zusammen.

Beispielsweise wäre für die LDAP-Gruppen *Cal_Adminstrator, Cal_Vergabestelle, Cal_Bauplanung usw.* das Präfix *„Cal_"*. Die CaliforniaX-Rechtegruppen hießen entsprechend *Administrator, Vergabestelle, Bauplanung* usw.

In der Zeile *CalGroupPrefix* der Tabelle *GW_LDAP-CONF* wird das CaliforniaX-Gruppenpräfix der LDAP-Gruppen mit *„cn=_California_"* vorgeschlagen.

Ändern oder übernehmen Sie den Vorschlag durch das im LDAP genutzte Präfix, z.B. „cn=Cal_"

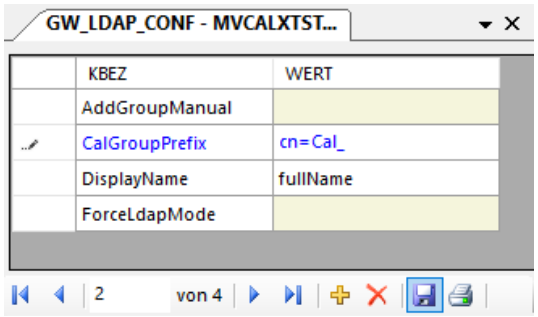


Abbildung 16 Benutzertabelle GW_LDAP_CONF

Speichern Sie ggf. Ihre Eingabe und schließen Sie die Tabelle über das X.

Wiederholen Sie im nächsten Schritt den Menüaufruf *LDAP einrichten* durch Klick mit der rechten Maustaste auf *Benutzertabellen* in der Baumstruktur des DBTool.

Es öffnet sich ein Dialog zur Eingabe der Verbindungsparameter zu einem LDAP-Verzeichnisserver.

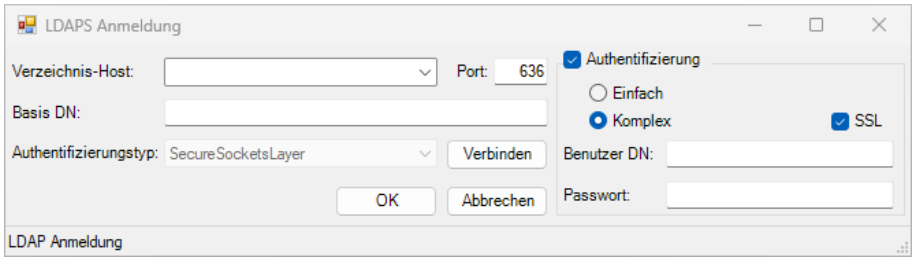


Abbildung 17 Verbindungsparameter zum LDAP-Server

Tragen Sie die notwendigen Angaben zum LDAP-Verzeichnisserver wie Port, Basis- und Benutzer-DN (Distinguished Name) sowie Kennwort ein.

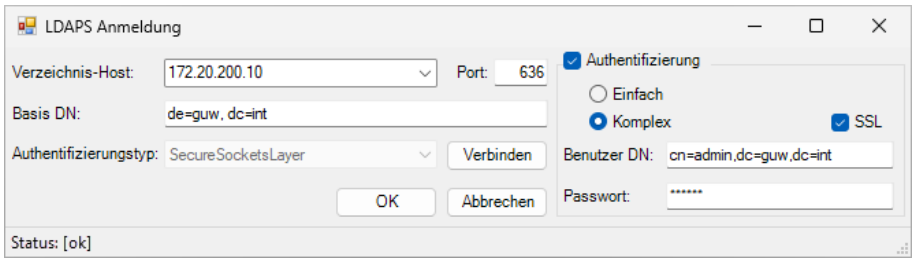


Abbildung 18 Konfiguration LDAP-Server (Beispiel)

Prüfen Sie im Anschluss der Eingaben mit Klick auf *Verbinden*, ob ein Verbindungsaufbau zum LDAP-Server möglich ist.

Dargestellt wird dies durch Status: [ok] in der Fußzeile des Fensters.

Im obigen Beispiel sieht man, dass die Verbindung zum LDAP-Server über den Port 636 SSL-verschlüsselt stattfindet. Dazu ist es notwendig, dass der LDAP-Server über ein gültiges Zertifikat verfügt. Diese gesicherte Verbindung (LDAPS) ist ab California.pro V6.1 und CaliforniaX möglich.

Mit *OK* wird die Konfiguration des LDAP-Verzeichnisservers abgeschlossen.

Hinweis:

Die Anmeldedaten werden in der Datenbanktabelle GW_LDAP_SERVER gespeichert. Falls mehrere LDAP-Server existieren, können weitere Zeilen in dieser Tabelle ergänzt werden.

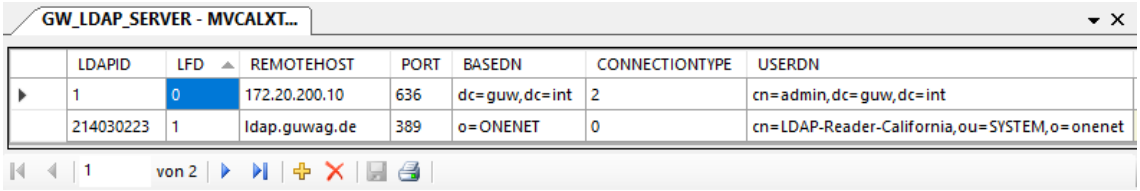


Abbildung 19 Benutzertabelle GW_LDAP_SERVER

Beim Aufruf von CaliforniaX werden alle LDAP-Server in der Reihenfolge der numerischen Spalte LFD abgefragt.

Im Datenbereich von DBTool wurde die Tabelle *GW_LDAP_GROUPMAP* geöffnet und befüllt. Die Tabelle regelt die Zuordnung der CaliforniaX-Active Directory Gruppen (Spalte *CN*) zu den CaliforniaX-Rechtegruppen (Spalten GRUPPENID und KOMMENTAR).

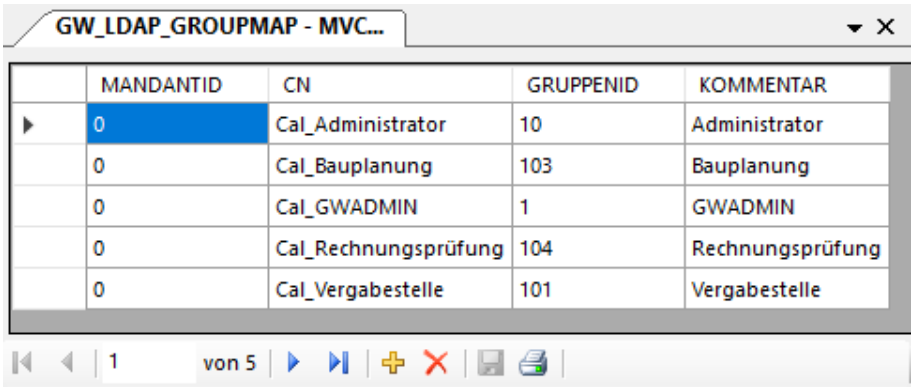


Abbildung 20 Benutzertabelle GW_LDAP-GROUPMAP

Wenn die Gruppennamen im LDAP-Verzeichnisdienst und CaliforniaX bis auf die Präfixe gleich lauten (Empfehlung), ist hier keine Anpassung notwendig. Im seltenen Fall, dass zwei unterschiedliche LDAP-Gruppen ein und derselben CaliforniaX-Gruppe zugeordnet werden sollen, kann dies durch eine gleichlautende Gruppen-ID in der Spalte GRUPPENID erreicht werden.

Speichern Sie Ihre Änderungen ab und beenden Sie das DBTool.

Im letzten Schritt der Konfiguration öffnen Sie die Datei *CalX.config* aus den CaliforniaX-Programmdateien *…\Program Files\G&W Software\CaliforniaX\Setup* zur Bearbeitung mit einem beliebigen Editor. Ergänzen Sie in der Sektion <CaliforniaX> den folgenden Eintrag:

<add key="LdapMode" value="3" />

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
    <configSections>
        <section name="CaliforniaX" type="System.Configura
    </configSections>
    <CaliforniaX>
        <add key="DBServer" value="MVCALXTSTCL11\CAL" />
        <add key="DBName" value="CalX" />
        <add key="DBTyp" value="SQL Server" />
        <add key="LdapMode" value="3" />
    </CaliforniaX>
</configuration>
```

Abbildung 21 Konfigurationsdatei CaliforniaX.config

Hinweis:

- Wert „3" aktiviert die LDAP-Anmeldung für eDirektory und OpenLDAP
- Wert „0" deaktivert die LDAP-Anmeldung

Damit ist die Konfiguration abgeschlossen. Eventuelle Rechteeinstellungen innerhalb von CaliforniaX werden unabhängig von LDAP in der Zugriffsrechteverwaltung von CaliforniaX vorgenommen.

Das Anmeldefenster von CaliforniaX wird nun immer den unter Windows angemeldeten (LDAP-) Benutzer voreinstellen.

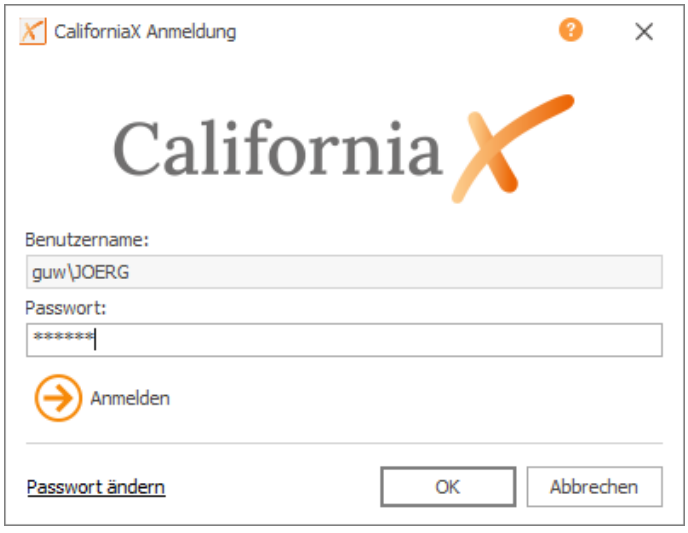


Abbildung 22 CaliforniaX Anmeldedialog bei aktivierter LDAP-Schnittstelle (e-Directory, OpenLDAP)

Beim ersten Aufruf wird das (Windows-)Passwort abgefragt und nach Anmeldung in CaliforniaX in der Datenbank (verschlüsselt) abgelegt. Bei allen Folgeaufrufen muss das Kennwort nicht mehr eingegeben werden.

Falls eine Kennwort-Erneuerung zur Windows-Anmeldung in regelmäßigen Zeitabständen erwünscht und unter LDAP eingestellt wurde, erfolgt die Abfrage dieses neuen Kennwortes sowie dessen Ablage in CaliforniaX erneut.

Sollte sich ein unberechtigter Nutzer (nicht im LDAP-Verzeichnis angelegt) anmelden, erscheint folgende Meldung:

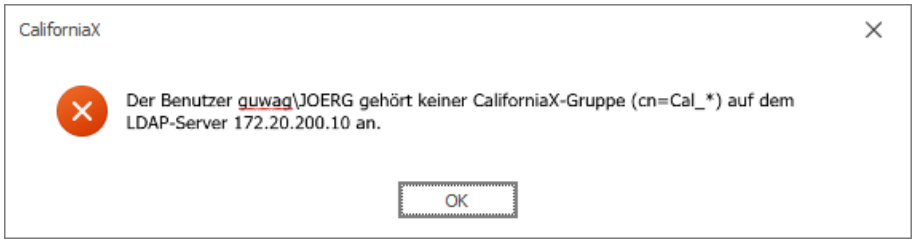


Abbildung 23 Warnhinweis bei Anmeldung unberechtigter Benutzer (e-Directory, OpenLDAP)

3. Auswirkungen der LDAP-Einrichtung

Mit der Nutzung von LDAP geht die Steuerung der Gruppenmitgliedschaften von der CaliforniaX-Zugriffsrechteverwaltung an das LDAP-basierende Benutzermanagement des Netzwerks über. In CaliforniaX werden lediglich die Detail- und Erbrechte einer Benutzergruppe definiert.

Wichtiger Hinweis:

Ohne Verwendung von Mandanten in CaliforniaX, werden nicht vorhandene Rechtegruppen durch den Anmeldeprozess automatisch neu angelegt. Da diese Rechtegruppen *optimistisch*, also ohne Rechteeinschränkungen angelegt werden, haben Benutzer bis zur Festlegung der gewünschten Rechteeinschränkungen in CaliforniaX erhöhte Rechte. Die Gruppenrechte sollten daher in CaliforniaX angepasst werden.

Es wird ausdrücklich empfohlen, die Rechtegruppen in CaliforniaX vorher zu definieren.

3.1. Anwendungsbeispiele

Die LDAP-Anbindung steuert die Gruppenmitgliedschaften von Benutzern wie folgt:

Fall A - Regelfall

- In CaliforniaX sind Rechtegruppen vorhanden.
- Den Rechtegruppen sind CaliforniaX-Benutzer zugeordnet.
- Die Rechtegruppen und Benutzernamen stimmen mit der LDAP-Anmeldeinformation überein.

Anmeldevorgang:

Die Anmeldung wird mit dem vorhandenen CaliforniaX-Benutzer und den Rechtegruppen gemäß LDAP-Zuordnung durchgeführt.

Wird ein Benutzer einer anderen LDAP-Gruppe zugeordnet, wird die Zuordnung zu den Rechtegruppen mit dem nächsten Anmeldevorgang in CaliforniaX aktualisiert.

Fall B

- In CaliforniaX sind Rechtegruppen vorhanden.
- Den Rechtegruppen sind noch keine CaliforniaX-Benutzer zugeordnet.

Anmeldevorgang:

Der Benutzer wird automatisch in CaliforniaX angelegt und den Rechtegruppen gemäß LDAP-Zuordnung zugeordnet.

Fall C

- In CaliforniaX sind noch keine Rechtegruppen angelegt.
- Es wurde eine LDAP-Gruppe für CaliforniaX angelegt und ein Benutzer dieser LDAP-Gruppe zugeordnet.

Anmeldevorgang:

Ohne die Verwendung von Mandanten in CaliforniaX werden die Rechtegruppen automatisch in CaliforniaX neu angelegt und der Benutzer diesen Rechtegruppen zugewiesen.

Neue Rechtegruppen werden in CaliforniaX *optimistisch*, also zunächst ohne Rechteeinschränkungen angelegt.