California.pro
AVA-Software by G&W

LDAP – Erweiterung

California.pro – LDAP (Lightweight Directory Access Protocol)

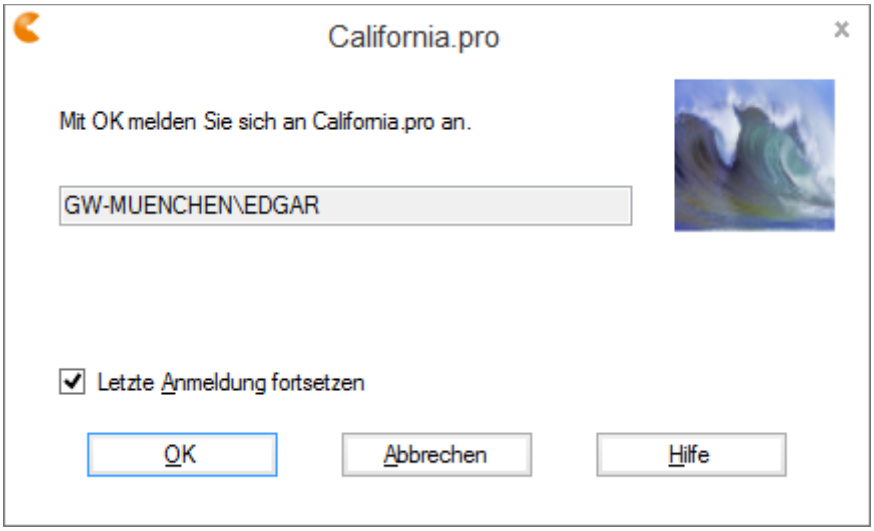
In diesem Dokument wird die Einrichtung der LDAP-Schnittstelle für **California.pro** beschrieben.

Allgemeiner 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 sogenannten Verzeichnisdiensten zum Einsatz. Es beschreibt die Kommunikation zwischen dem sogenannten *LDAP-Client* (hier **California.pro**) 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.

California.pro 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 **California.pro** wird voreingestellt, so dass hier i.A. keine manuellen Angaben mehr notwendig sind.



G&W Software AG

Stammhaus München
Rosenheimer Str. 141h
81671 München
Tel. 089 / 51 506 - 4
Fax 089 / 51 506 - 999

Niederlassung Berlin
Danckelmannstr. 9b
14059 Berlin
Tel. 030 / 42 02 47 - 7
Fax 030 / 42 02 47 - 99

Niederlassung Essen
Borbecker Platz 5
45355 Essen
Tel. 0201 / 6 13 54 - 0
Fax 0201 / 6 13 54 - 22

www.gw-software.de
info@gw-software.de

Im obigen Beispiel wird der Benutzer *EDGAR* der Domäne *GW-MUENCHEN* zur Anmeldung an **California.pro** voreingestellt. Die Eingabe des Kennwortes ist nicht notwendig.

Voraussetzungen

Folgende Voraussetzungen sollten erfüllt sein:

- Am LDAP-Server:

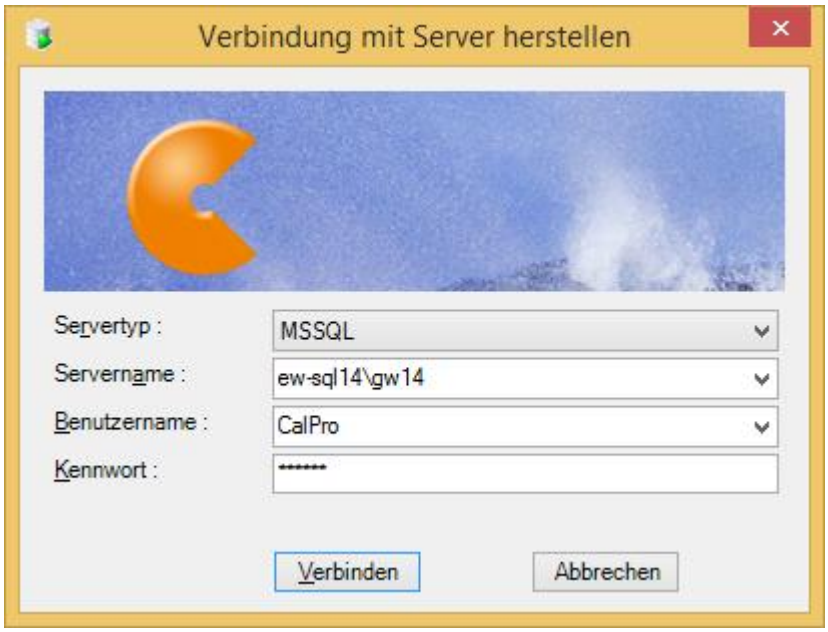
  Die drei LDAP-Varianten *Microsoft Active Directory*, *Novel eDirectory* und *OpenLDAP* mit aktivierter *memberOf*-Option werden unterstützt. Alle **California.pro**–Benutzer sind Mitglied von eigens angelegten Gruppen. Die Namen dieser Gruppen beginnen mit einem gemeinsamen Präfix, welcher frei wählbar ist, z.B. *_CalPro_*. Eine LDAP-Gruppe für **California.pro** heißt dann z.B. *_CalPro_Administrator* oder *_CalPro_Kostenplaner*. Ein Benutzer kann auch mehreren Gruppen (dann meist Rollen genannt) angehören.

- In **California.pro:**

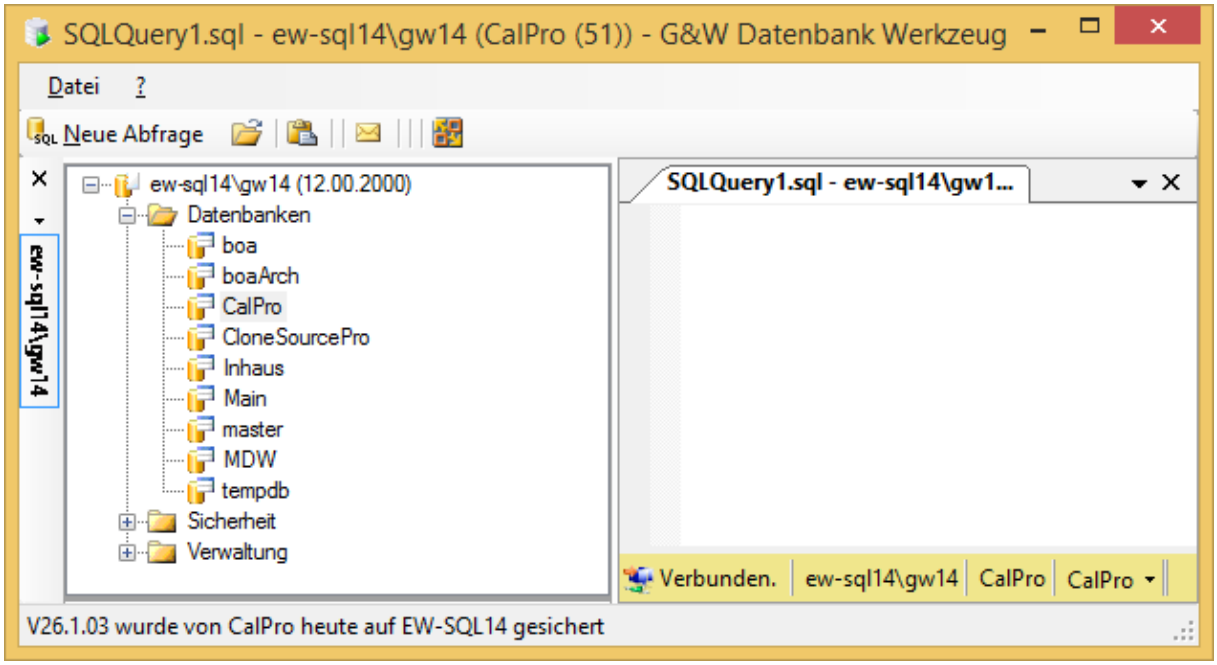
  Der Gruppenname ohne Präfix (im obigen Beispiel *Administrator* bzw. *Kostenplaner*) sollte in den Zugriffsrechten bereits als Rechtegruppe existieren und mit den gewünschten Rechten versehen sein.
  Beides ist nicht zwingend notwendig, da das LDAP-Modul in **California.pro** fehlende Gruppen i.A. automatisch anlegt und außerdem den Benutzer zum Mitglied der neuen Gruppe(n)/Rollen macht. Wir empfehlen aber ausdrücklich, schon aus Gründen der Steuerung der gewünschten Zugriffsrechte, zumindest die Erfassung der gleichlautenden Gruppen in **California.pro**.

LDAP-Konfiguration für Microsoft Active Directory

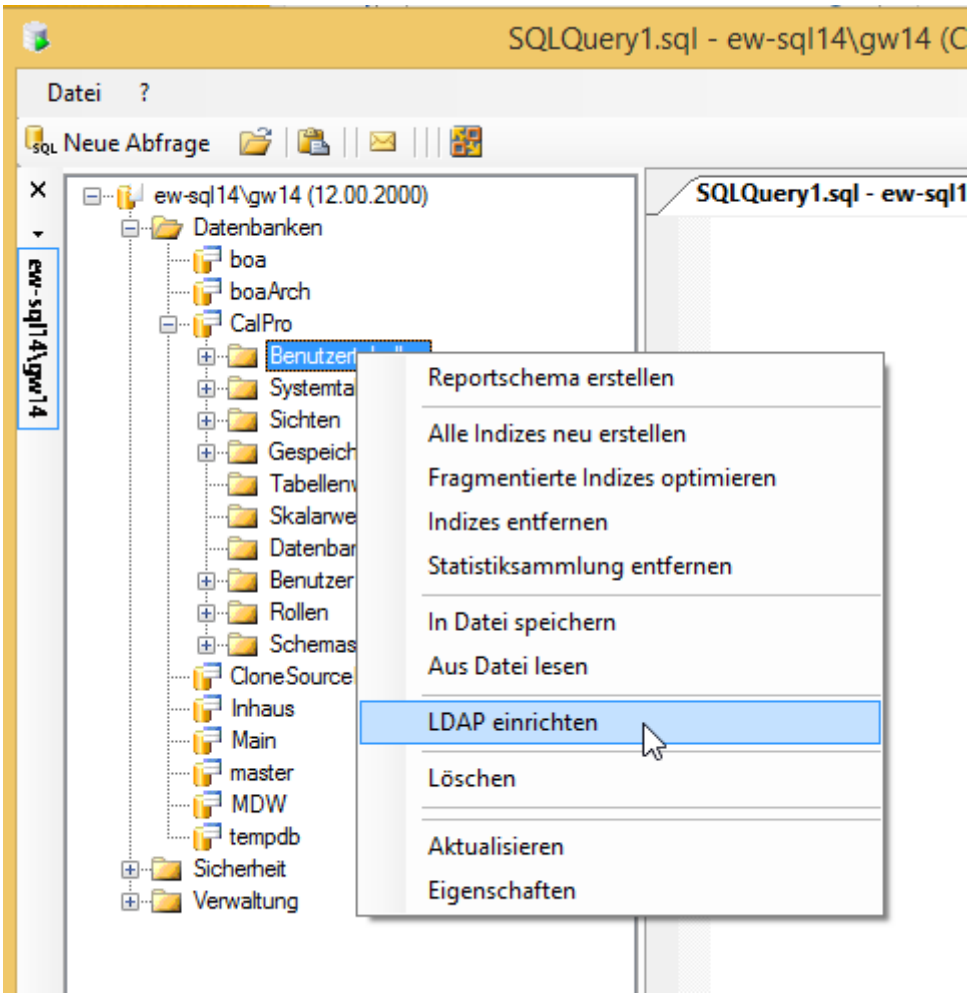
Starten Sie *Bin\DBTool.exe* aus dem **California.pro**-Installationsverzeichnis und melden sich am **California.pro** Datenbankserver an. Erfragen Sie ggf. Benutzername und Kennwort bei Ihrem Datenbank-Administrator oder G&W.



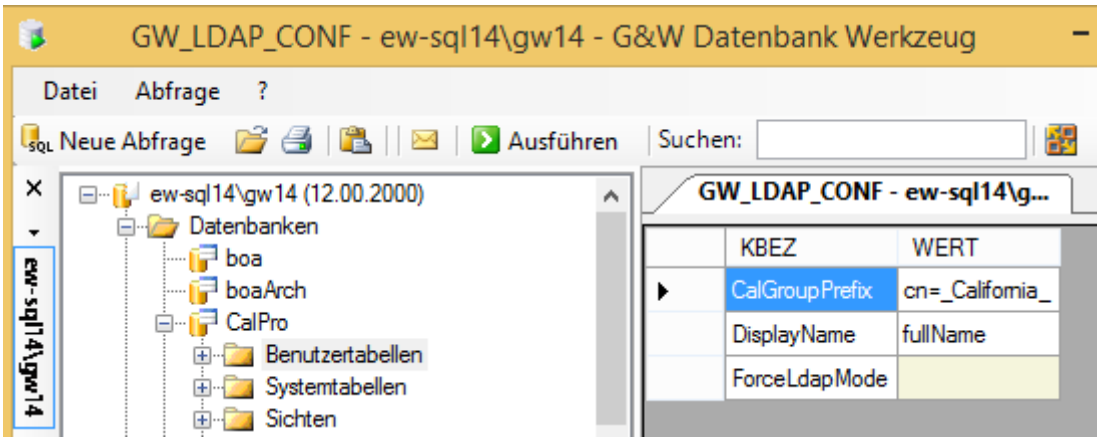
Es öffnet sich folgendes Fenster.



Öffnen Sie die **California.pro** Datenbank (üblicherweise ist dies *CalPro*) und klicken mit der rechten Maustaste auf den Eintrag *Benutzertabellen*.

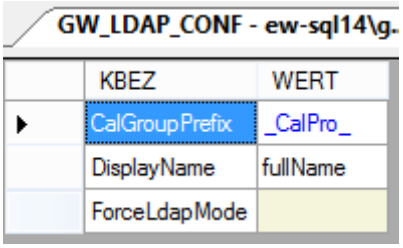


Über den Menüpunkt *LDAP einrichten* wird der erste Schritt der Konfiguration ausgelöst. Es wird die Datenbanktabelle *GW_LDAP_CONF* geöffnet, in der unter anderem das im *Microsoft Active Directory* benutzte Präfix (hier *_CalPro_*) für die **California.pro**-Benutzergruppen eingetragen wird.



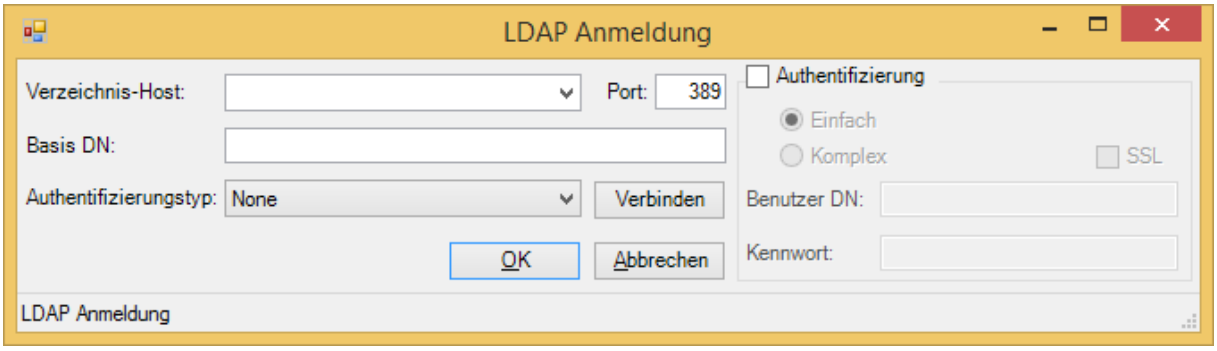
Voreingestellt ist hier *cn=_California_*. Das in *Microsoft Active Directory* genutzte Präfix wird in der Spalte *WERT* geändert.

Für das Einrichten der LDAP-Schnittstelle für *Microsoft Active Directory (AD)* entfernen Sie in jedem Fall bitte die Zeichenfolge *cn=* und modifizieren ggf. die Zeichenfolge *_California_* in das gewünschte Gruppenpräfix (hier *_CalPro_*), welches allen **California.pro**-*Active Directory* Gruppen in Ihrer *AD*-Domäne gemeinsam ist.

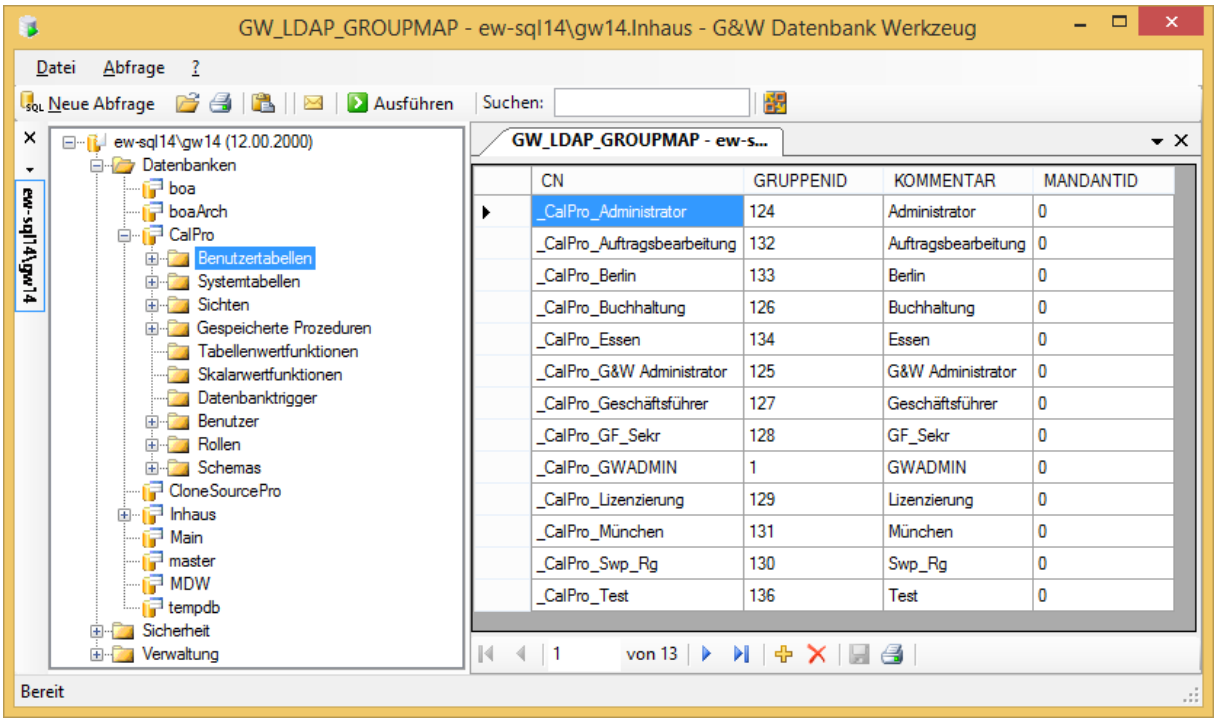


Schließen und speichern sie das *GW_LDAP_CONF*-Fenster.

Im nächsten Schritt wird der rechte Mausklick auf *Benutzertabellen* und Aufruf von *LDAP einrichten* wiederholt. Nun öffnet sich folgendes Fenster:



Beenden Sie dieses über *Abbrechen* (es ist nicht für *Microsoft Active Directory* erforderlich), und Sie stehen in der Konfigurationstabelle *GW_LDAP_GROUPMAP*, in welcher sich die Zuordnung Ihrer **California.pro**-*Active Directory* Gruppen (Spalte *CN*) zu den Rechtegruppen in **California.pro** (Spalten *GRUPPENID* und *KOMMENTAR*) befindet.



Wenn die Gruppennamen in *Microsoft Active Directory* und **California.pro** bis auf dem Präfix gleich lauten (unsere Empfehlung), ist hier keine Anpassung notwendig. Im seltenen Fall, dass zwei unterschiedliche AD-Gruppen ein und derselben **California.pro**-

Gruppe zugeordnet werden, kann dies durch eine gleichlautende *Gruppen-ID* in der Spalte *GRUPPENID* erreicht werden.

Speichern Sie Ihre Änderungen ab und beenden Sie *DBTool.exe*.

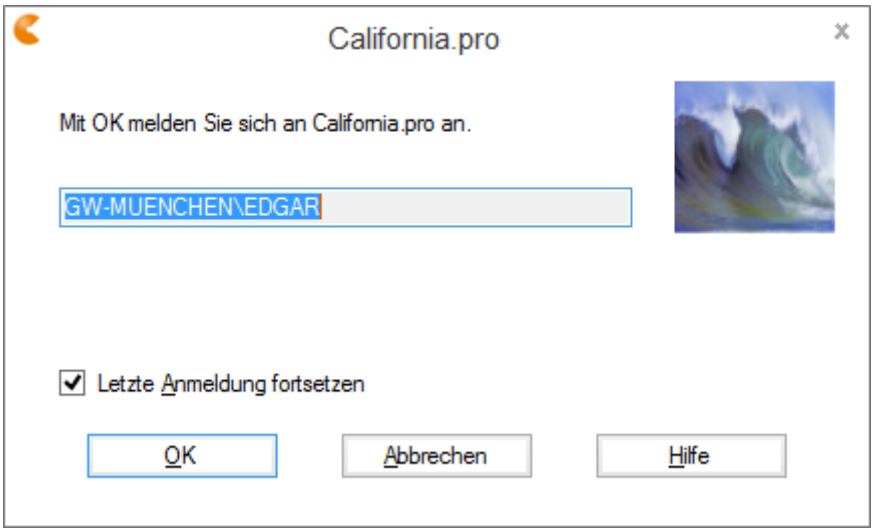
Im letzten Schritt der Konfiguration wird die Datei *Calpro.config* im Verzeichnis *Setup* der **California.pro**-Installation mit einem beliebigen Editor geöffnet. Hier wird folgender Eintrag in der Sektion <*CalPro*> erstellt:

```
<CalPro>
  <add key="DBServer" value="ew-sql14\gw14"/>
  <add key="DBName" value="calpro"/>
  <add key="DBTyp" value="SQL"/>
  <add key="LdapMode" value="2"/>
```

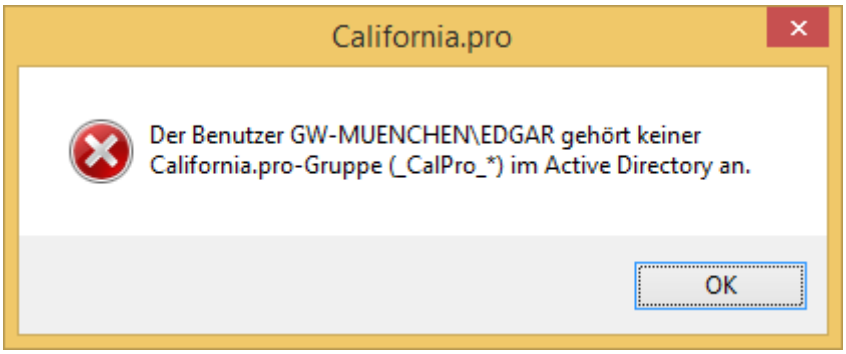
Mit **value="2" wird LDAP in der Variante *Active Directory* aktiviert**, eine „0" (Null) schaltet die LDAP-Anmeldung aus.

Damit ist die Konfiguration abgeschlossen. Eventuelle Rechteeinstellungen innerhalb von **California.pro** werden unabhängig von LDAP im Menüpunkt *Service/Zugriffsrechte* vorgenommen.

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



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



G&W Software AG

Stammhaus München
Rosenheimer Str. 141h
81671 München
Tel. 089 / 51 506 - 4
Fax 089 / 51 506 - 999

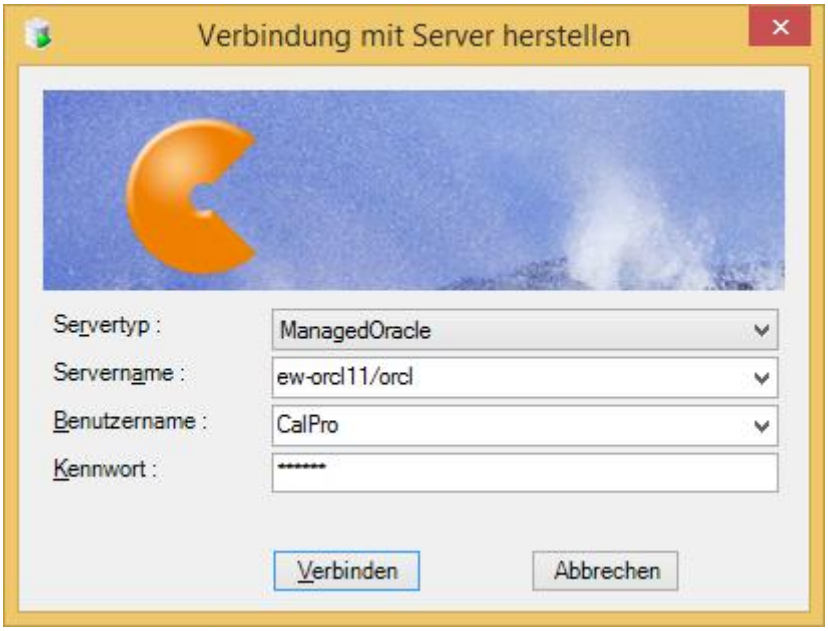
Niederlassung Berlin
Danckelmannstr. 9b
14059 Berlin
Tel. 030 / 42 02 47 - 7
Fax 030 / 42 02 47 - 99

Niederlassung Essen
Borbecker Platz 5
45355 Essen
Tel. 0201 / 6 13 54 - 0
Fax 0201 / 6 13 54 - 22

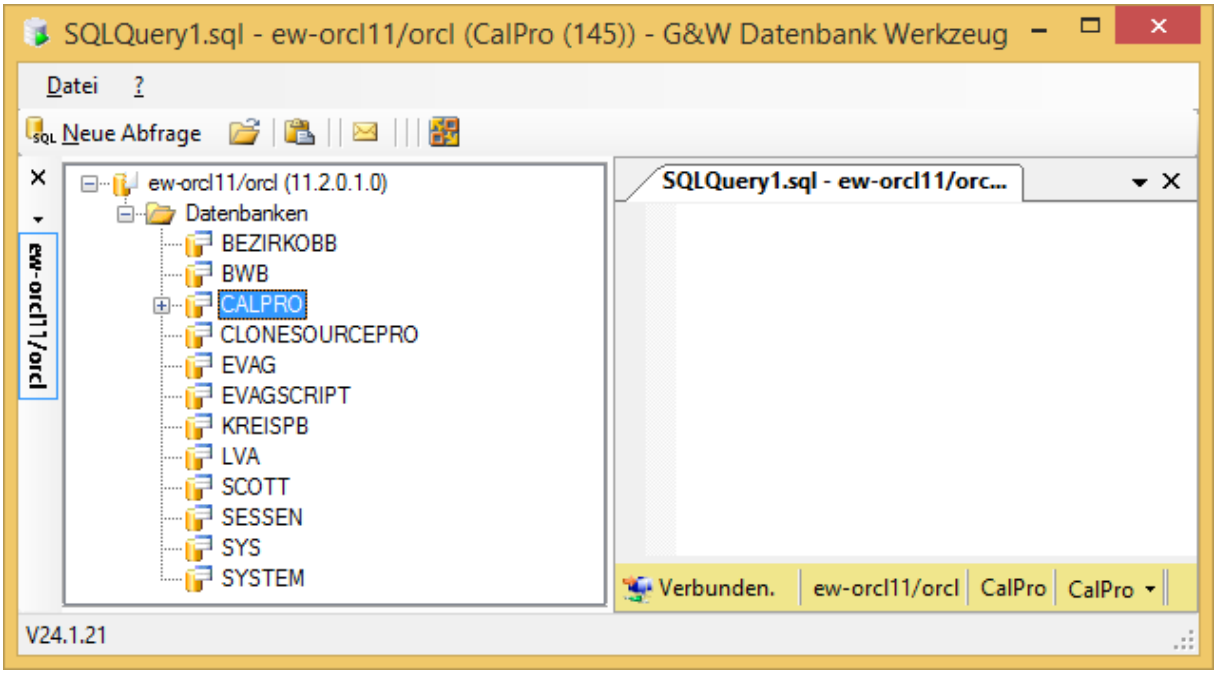
www.gw-software.de
info@gw-software.de

LDAP-Konfiguration für Novell eDirectory und OpenLDAP

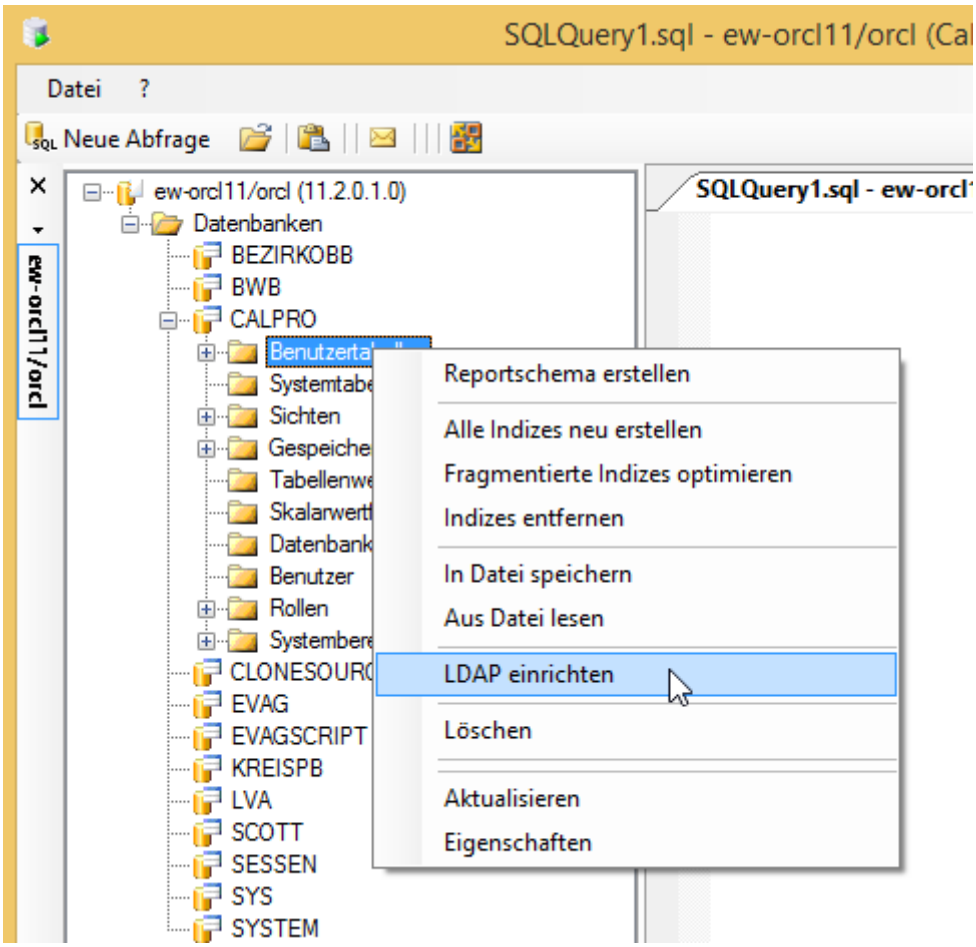
Starten Sie *Bin\DBTool.exe* aus dem **California.pro**-Installationsverzeichnis und melden sich am **California.pro** Datenbankserver an. Erfragen Sie ggf. Benutzername und Kennwort bei Ihrem Datenbank-Administrator oder G&W.



Es öffnet sich folgendes Fenster.

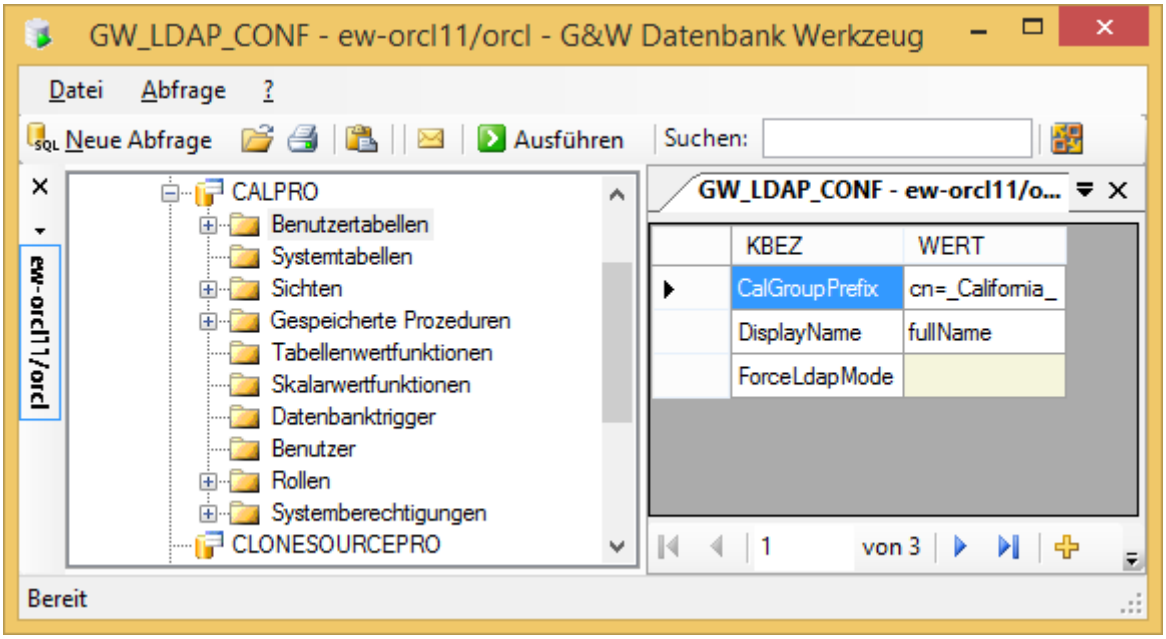


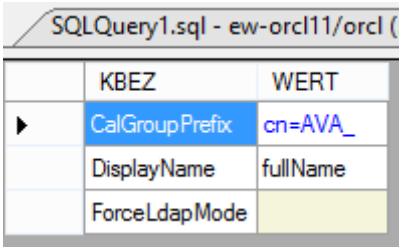
Öffnen Sie die **California.pro** Datenbank *CalPro* bzw. das *Oracle*-Benutzerschema *CALPRO* und klicken mit der rechten Maustaste auf den Eintrag *Benutzertabellen*.



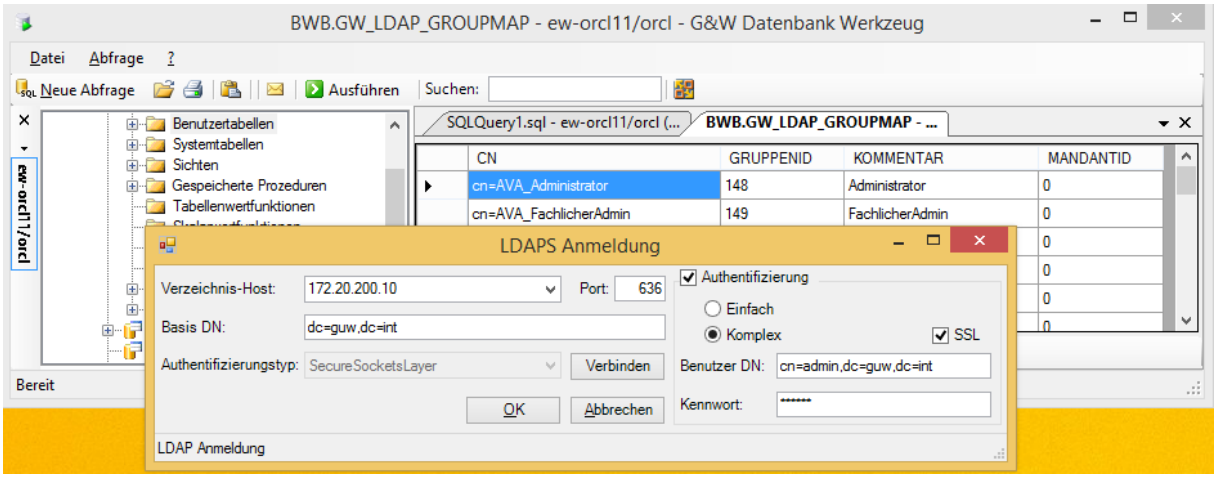
Über den Menüpunkt *LDAP einrichten* wird der erste Schritt der Konfiguration ausgelöst. Es wird die Datenbanktabelle *GW_LDAP_CONF* geöffnet, in der unter anderem das in LDAP benutzte Präfix (hier *AVA_*) für die **California.pro**-Benutzergruppen eingetragen wird.

Voreingestellt ist hier *cn=_California_*. Das im *LDAP* genutzte Präfix wird in der Spalte *WERT* geändert oder der Vorschlag übernommen.





Im nächsten Schritt wird der rechte Mausklick auf *Benutzertabellen* und Aufruf von *LDAP einrichten* wiederholt. Nun öffnet sich folgendes Fenster:

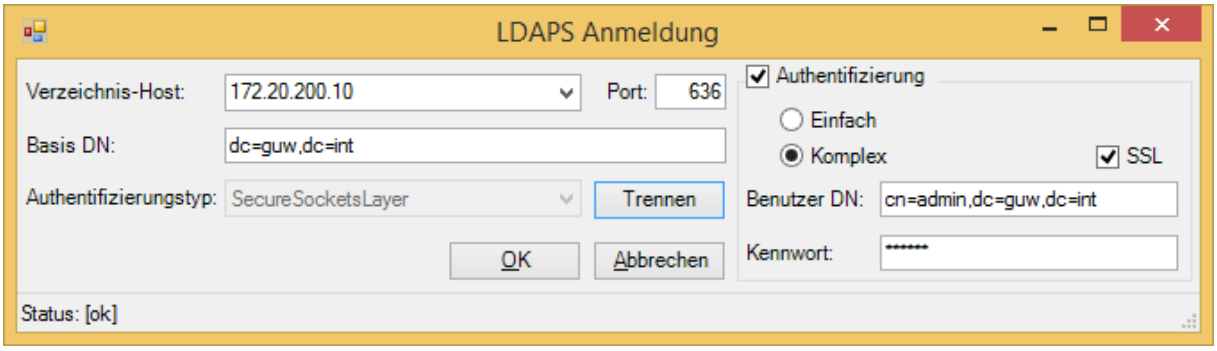


Im Hintergrund erkennt man die Tabelle *GW_LDAP_GROUPMAP*, in der eine Zuordnung zwischen dem Gruppennamen im LDAP (Spalte CN) und dem Gruppennamen in den **California.pro**-Zugriffsrechten (Spalte *GRUPPENID* und *KOMMENTAR*) hergestellt werden kann.

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

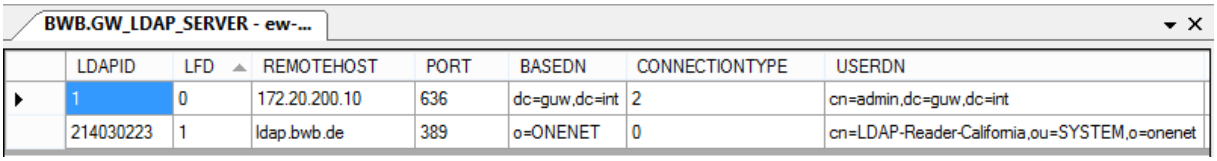
Die im Vordergrundfenster notwendigen Angaben zum LDAP-Verzeichnis-Server, Port, Basis- und Benutzer-DN sowie Kennwort erfahren Sie von Ihrem LDAP-Administrator. Wenn alle Angaben erfasst wurden, kann über den Button *Verbinden* überprüft werden, ob ein Verbindungsaufbau zum LDAP-Server möglich ist.

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** möglich.

Mit *OK* wird die Konfiguration beendet, die Anmeldedaten werden dauerhaft in der Datenbank in der Tabelle *GW_LDAP_SERVER* abgelegt. Falls mehrere LDAP-Server existieren, kann in dieser Tabelle eine beliebige Anzahl von derartigen Einträgen erfolgen.



LDAPID	LFD	REMOTEHOST	PORT	BASEDN	CONNECTIONTYPE	USERDN
1	0	172.20.200.10	636	dc=guw,dc=int	2	cn=admin,dc=guw,dc=int
214030223	1	ldap.bwb.de	389	o=ONENET	0	cn=LDAP-Reader-California,ou=SYSTEM,o=onenet

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

Das G&W Datenbank Werkzeug (*DBTool.exe*) kann nun geschlossen werden.

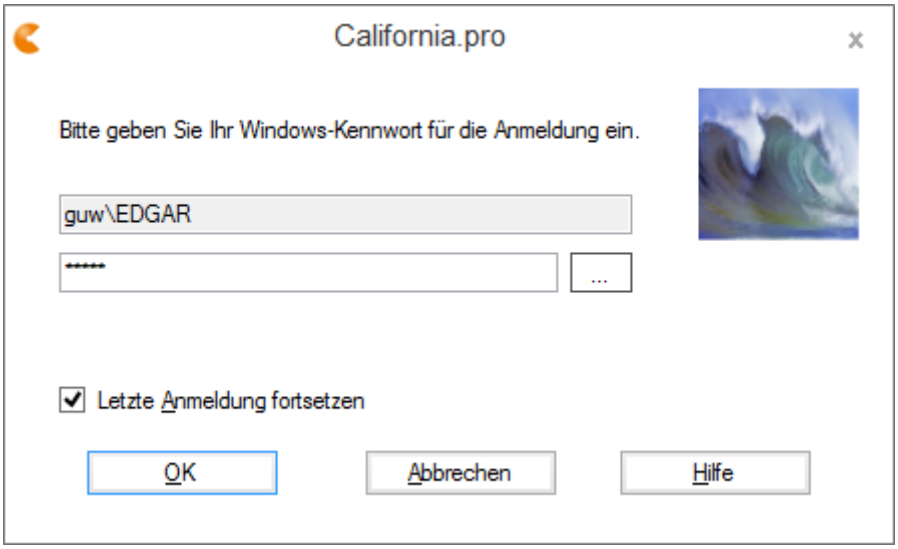
Im letzten Schritt der Konfiguration wird die Datei *Calpro.config* im Verzeichnis *Setup* der **California.pro**-Installation mit einem beliebigen Editor geöffnet. Hier wird folgender Eintrag in der Sektion *<CalPro>* erstellt:

```
<CalPro>
  <add key="DBServer" value="gw-dev-002/ORCL"/>
  <add key="DBName" value="CalPro"/>
  <add key="DBTyp" value="oracle.managed"/>
  <add key="LdapMode" value="3"/>
</CalPro>
```

Mit **value="3" wird LDAP(S) für eDirectory bzw. OpenLDAP aktiviert**, eine „0" (Null) schaltet die LDAP-Anmeldung aus.

Damit ist die Konfiguration abgeschlossen. Eventuelle Rechteeinstellungen innerhalb von **California.pro** werden unabhängig von LDAP im Menüpunkt *Service/Zugriffsrechte* vorgenommen.

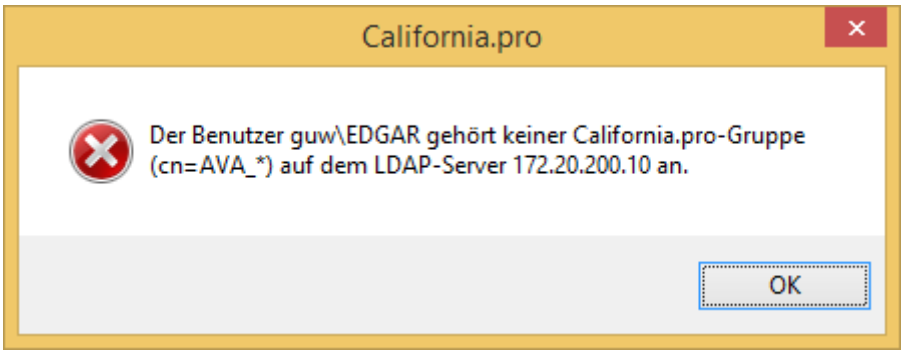
Das Anmeldefenster von **California.pro** wird nun immer den unter Windows angemeldeten (LDAP-)Benutzer voreinstellen.



Beim ersten Aufruf wird das (Windows-)Kennwort abgefragt und nach Anmeldung in **California.pro** 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 **California.pro** erneut.

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



Auswirkungen der LDAP-Einrichtung

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

Wichtig: Wenn keine Mandanten in **California.pro** Verwendung finden, werden nicht vorhandene Rechtegruppen durch den Anmeldeprozess automatisch neu angelegt. Da diese Rechtegruppen *OPTIMISTISCH* angelegt werden, haben Anwender dieser Gruppen fast keine Einschränkungen in der Nutzung von **California.pro**. Die Gruppenrechte sollten in **California.**pro in diesem Falle nachträglich angepasst werden.

Es wird deshalb ausdrücklich empfohlen, die Gruppenstruktur in **California.pro** vorab zu definieren.

Anwendungsbeispiele

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

Fall A Regelfall

In **California.pro** sind Benutzer und Rechtegruppe(n) vorhanden und stimmen mit der LDAP-Anmeldeinformation überein.

Aktion: Die Anmeldung wird durchgeführt.

Fall B

In **California.pro** ist (sind) die Rechtegruppe(n) vorhanden, der Benutzer jedoch nicht.

Aktion: Der Benutzer wird automatisch Mitglied die Rechtegruppe(n) gemäß LDAP-Zuordnung.

Fall C

Der Benutzer ist Mitglied von **California.pro** LDAP-Gruppen, die keine entsprechende(n) Zugriffrechtegruppe(n) in **California.pro** haben.

Aktion: Wenn keine Mandanten in **California.pro** Verwendung finden, werden die Gruppen automatisch in **California.pro** *OPTIMISTISCH* angelegt und der Benutzer wird automatisch Mitglied dieser neuen Gruppe(n).

G&W Software AG

Stammhaus München
Rosenheimer Str. 141h
81671 München
Tel. 089 / 51 506 - 4
Fax 089 / 51 506 - 999

Niederlassung Berlin
Danckelmannstr. 9b
14059 Berlin
Tel. 030 / 42 02 47 - 7
Fax 030 / 42 02 47 - 99

Niederlassung Essen
Borbecker Platz 5
45355 Essen
Tel. 0201 / 6 13 54 - 0
Fax 0201 / 6 13 54 - 22

www.gw-software.de
info@gw-software.de