LDAP

Übersicht

Ziel des LDAP-Synchronisations-Moduls ist es, eine nahezu beliebige Gruppen- und User-Struktur aus einem LDAP-Dienst zu übernehmen und mit den nötigen Informationen anzureichern, um diese als Basis für die T!M Gruppen-/User-Struktur zu nutzen. Die Grundlage für dieses Modul bildet die TimedService-Komponente, mit der die Synchronisation zeitgesteuert ausgeführt wird.

Das Modul besteht aus zwei wesentlichen Teilen, die zusammen die Synchronisation nahezu beliebiger LDAP-Strukturen erlauben. Um das LDAP-Modul einzurichten, sind mehrere Schritte notwendig, die in diesem Eintrag erläutert werden.

> ACHTUNG! Diese Einstellungen und Methoden sollten nur von erfahrenen Benutzer angewendet werden.

Grundkonfiguration LDAP

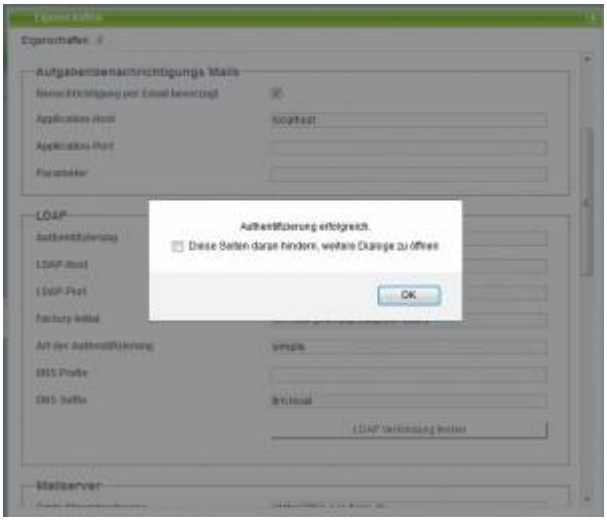
Um T!M - Task !n Motion den grundsätzlichen Zugang zu einem LDAP-Server zu ermöglichen, muss folgende Datei angepasst werden:

```
loom.ear/config/ldap.properties
```

Diese Einstellungen greifen für alle Mandanten! Für eine genauere Erklärung der einzelnen Zeilen, können Sie sich hier näher informieren.

LDAP Verbindung testen

Um die Grundsätzliche LDAP Verbindung zu testen, müssen im Clientprofil noch einige Einstellungen vorgenommen werden. Hierzu werden folgende Werte benötigt:



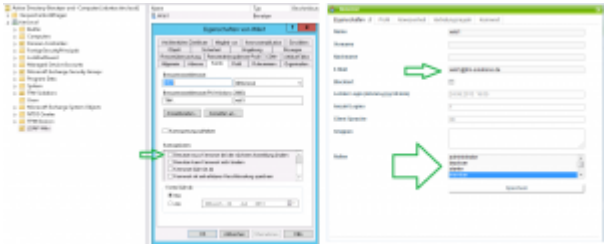
Authentifizierung	Kann leer bleiben

LDAP-Host	Host oder IP des LDAP Servers
LDAP-Port	Port auf dem der LDAP Server hört (Standard 389)
Factory Initial	Muss folgenden Wert enthalten „com.sun.jndi.ldap.LdapCtxFactory“
Art der Authentifizierung	Kann „simple“ oder „digest-md5“ sein (Standard „**simple**“)
DNS Prefix	Kann leer bleiben
DNS Suffix	Hier muss das DNS Suffix der Firma hinterlegt werden

Danach kann mit der Schaltfläche **„LDAP-Verbindung testen“** ein LDAP-Lookup gestartet werden. Hierzu wird einfach ein LDAP User + Passwort eingegeben.

> ACHTUNG! Das Passwort wird im Klartext angezeigt!

LDAP Lookup einrichten



LDAP Lookup heißt, dass T!M Authentifizierungsanfragen an den LDAP Server weiterleitet und erfragt werden, ob der User berechtigt ist, sich anzumelden. Da das Rechtemanagement aktuell noch weiterhin in T!M hinterlegt ist, muss der User in T!M angelegt sein!

> WICHTIG! (siehe Screenshot)
>
> Eine E-Mailadresse muss im Userprofil hinterlegt sein
> Der Login ist nicht gestattet, solang der Nutzer sein Kennwort im AD ändern muss
> Die Rechte des Nutzers werden in T!M verwaltet

LDAP Sync

Der LDAP Sync ermöglicht es, Benutzer in T!M anzulegen und die Attribute aus dem LDAP heraus zu übernehmen. Wie man die LDAP-Attribute auf die T!M-Attribute verknüpft, kann auf folgender Seite entnommen werden.
Um den LDAP-Sync zu aktivieren, wird folgender Timer benötigt.

Praktisches Beispiel

Solch eine Gruppenstruktur und die Konfiguration von 4 Timern (je Timer eine Gruppe), ermöglicht es dem Admin bequem die Rechte in T!M zu verteilen. Wichtig ist nur, dass alle T!M-Benutzer in der Gruppe **TIM-Member** sind, da sonst beispielsweise ein Admin keine Smartform öffnen könnte, da

hierzu ein member-Recht benötigt wird.