LDAP und Active Directory

FTAPI besitzt eine eigene, leistungsfähige Benutzerverwaltung. In manchen Situationen ist es jedoch sinnvoll, bereits bestehende Benutzer-Accounts aus einem
LDAP- oder Active-Directory-System zu verwenden, um eine doppelte Verwaltung dieser Konten zu vermeiden. Nachfolgend wird erläutert, wie Sie FTAPI SecuTransfer
so konfigurieren, dass es Benutzer-Konten aus einem LDAP- oder Active-Directory-System akzeptiert.

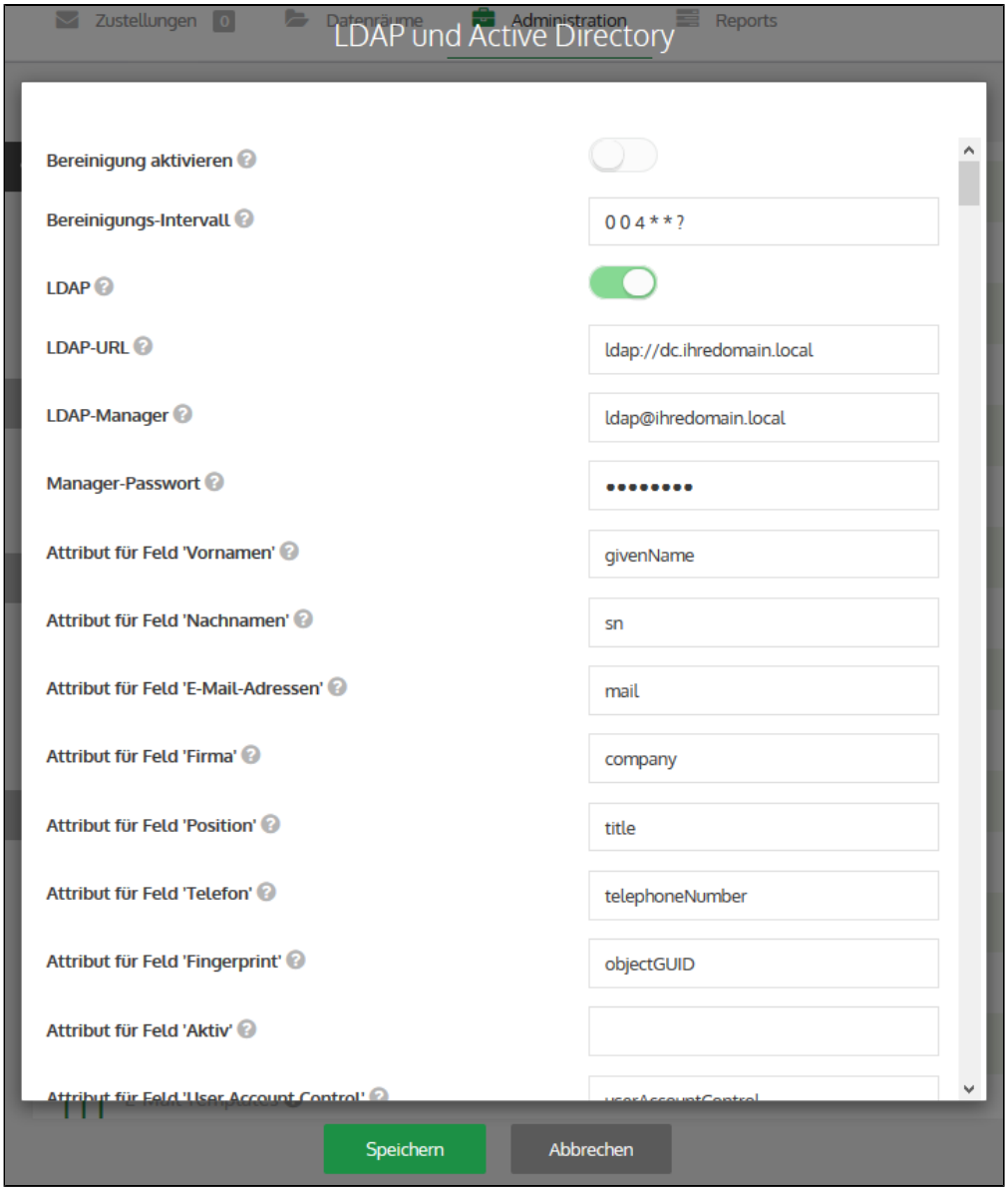
Bevor Sie mit der Konfiguration in FTAPI beginnen, stellen Sie bitte sicher, dass Ihr LDAP-System über das Netzwerk erreichbar ist und Sie sich erfolgreich
per LDAP verbinden können. Dies können Sie beispielweise überprüfen, indem Sie sich mit einem der zahlreichen kostenloses LDAP-Clients, wie z.B. dem
LDAP Browser von Softerra auf Ihren LDAP-Server verbinden.
Im folgenden Abschnitt wird der Begriff LDAP-Server als Synonym für ein LDAP- wie auch ein Active-Directory-System verwendet.

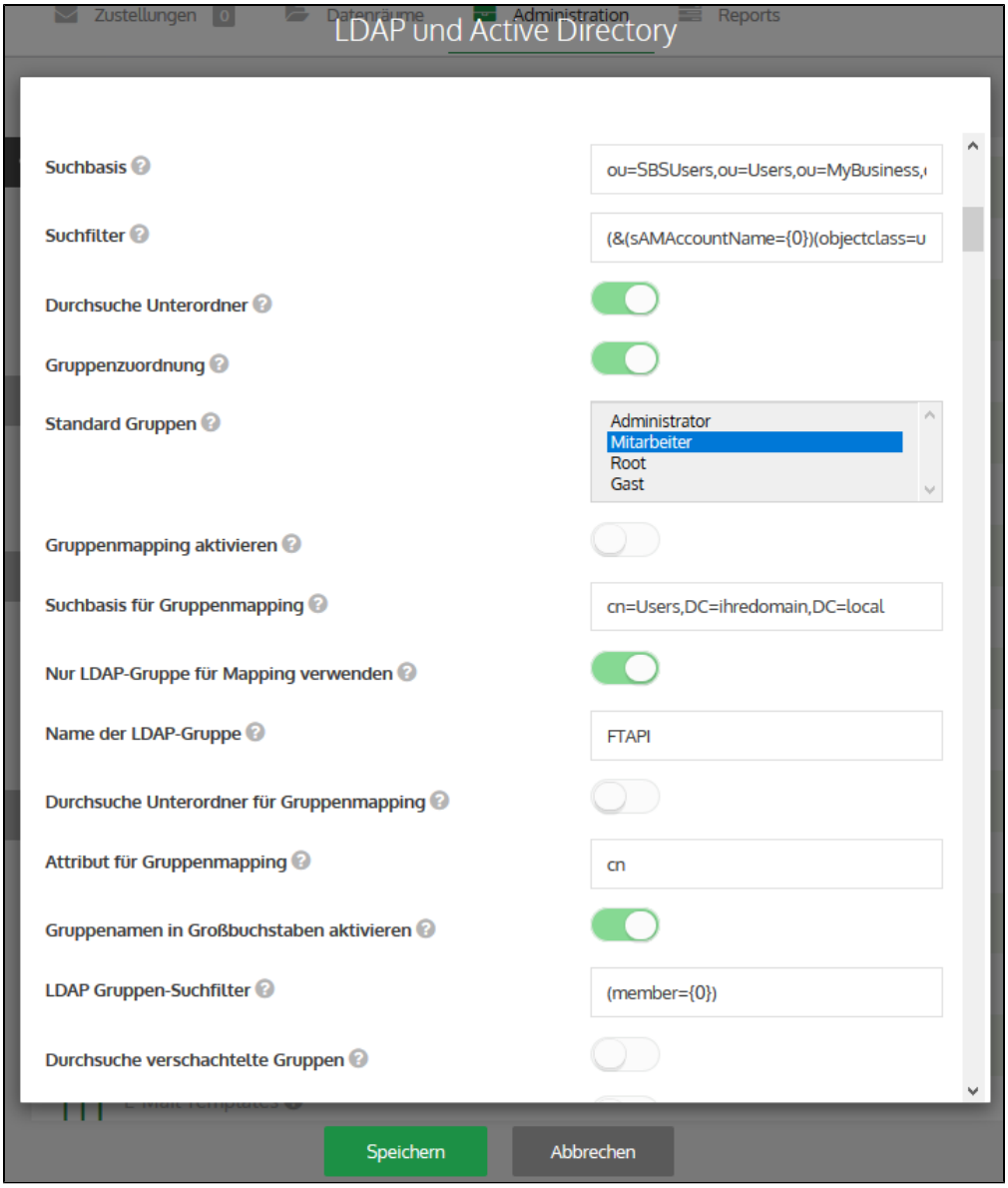
Beim Upgrade auf die Version 3.5 werden Änderungen an den bestehenden Gruppen GAST und PARTNER vorgenommen:
Die Gruppe Gast GROUP_GUEST wird aufgewertet und mit den Berechtigungen der Gruppe Partner GROUP_PARTNER versehen.
Die Gruppe Partner GROUP_PARTNER wird aus dem System entfernt.

Nach Aktivierung der LDAP-Anbindung werden die Benutzerdaten erst dann übernommen, wenn sich einer der LDAP-Benutzer erstmalig am FTAPI SecuTransfer System angemeldet hat.

Konfiguration anpassen

Klappen Sie im Reiter Konfiguration den Bereich *LDAP und Active Directory* auf:


Zustellungen
Datenräume
Administration
Reports
LDAP und Active Directory
Bereinigung aktivieren
Bereinigungs-Intervall
0 0 4 * * ?
LDAP
LDAP-URL
ldap://dc.ihredomain.local
LDAP-Manager
ldap@ihredomain.local
Manager-Passwort
Attribut für Feld 'Vornamen'
givenName
Attribut für Feld 'Nachnamen'
sn
Attribut für Feld 'E-Mail-Adressen'
mail
Attribut für Feld 'Firma'
company
Attribut für Feld 'Position'
title
Attribut für Feld 'Telefon'
telephoneNumber
Attribut für Feld 'Fingerprint'
objectGUID
Attribut für Feld 'Aktiv'
Speichern
Abbrechen



Klicken Sie auf das gewünschte Feld, ändern Sie die Parameter entsprechend Ihren Gegebenheiten ab und speichern Sie abschließend.

Neustart

Anschließend müssen Sie, falls oben rechts ein entsprechender Hinweis erscheint, den FTAPI-Server neu starten, damit diese Änderungen aktiv werden.

Parameter für den Cleanup

FTAPI besitzt einen Mechanismus um FTAPI Accounts, die zwar über LDAP angelegt wurden aber im LDAP System nicht mehr existieren, auch aus der FTAPI
Benutzerdatenbank wieder zu entfernen. Dies stellt vor allem bei großen Benutzerdatenbanken eine deutliche Erleichterung für den LDAP-Administrator dar.

Bereinigung aktivieren

Dieser Parameter gibt an, ob die LDAP Cleanup-Funktion aktiv sein soll oder nicht. Der Standardwert ist false.

Bereinigungs-Interval

Dieser Parameter ist ein Cron-Ausdruck, der angibt, in welchen Intervallen ein Abgleich der FTAPI Accounts mit dem LDAP-System erfolgen soll.

Im nachfolgenden Beispiel erfolgt eine solche Überprüfung täglich um 4:00 Uhr Morgens. Dies ist auch die Standardeinstellung.

```
ftapi.ldap.cleanup.interval=0 0 4 * * ?
```

Mehr Informationen zu Cron-Job Ausdrücken finden sie hier: http://quartz-scheduler.org/documentation/quartz-1.x/tutorials/crontrigger

Beschreibung Konfigurationsparameter

Die folgenden Parameter werden für die Aktivierung der Verbindung zu einem LDAP-System benötigt.

LDAP

Mit diesem Parameter können Sie LDAP generell aktivieren (Haken gesetzt) oder deaktivieren (Haken nicht gesetzt).Wird kein Wert angegeben, so wird der Standardstatus "deaktiviert" verwendet. Wenn die LDAP-Anbindung aktiviert und funktionsfähig ist, so führt FTAPI die Benutzerauthentifizierung stets in folgenden Schritten durch:

1. Es wird zuerst im LDAP-System nach dem entsprechenden Benutzer gesucht und bei einem Fund, dessen Login-Daten für die Authentifizierung verwendet.
2. Konnte im LDAP-System kein Benutzer mit dem angegebenen Benutzernamen gefunden werden, so wird die FTAPI eigene Benutzerverwaltung überprüft und falls sich hier der gewünschte Benutzer befindet, dessen Daten für die Authentifizierung verwendet.
3. Konnten weder im LDAP-System noch in der FTAPI-Benutzerverwaltung der Benutzer gefunden werden, so wird der Login mit einem "Login Failed" zurückgewiesen.

Wenn sich ein LDAP-Benutzer erstmalig bei FTAPI anmeldet, so werden alle notwendigen und nicht-sensiblen Daten von dessen LDAP-Account in die FTAPI-Benutzerverwaltung übernommen. Dies ist notwendig, um weitere Einstellungen an diesem FTAPI-Account vornehmen zu können (z.B. Gruppen zuordnen/entfernen), ohne den LDAP-Account ändern zu müssen. Einige Felder, wie z.B. das Passwort oder der Benutzername selbst, können dann nicht über die Oberfläche der FTAPI-Benutzerverwaltung verändert werden. Dies muss im LDAP-System selbst vorgenommen werden.

> **Gleichnamige Benutzer-Accounts**
> Bitte beachten Sie, dass es aus Sicherheitsgründen nicht erlaubt ist, dass ein manuell angelegter FTAPI-Account und ein LDAP-Account mit demselben Benutzernamen existieren. In diesem Fall wird beim Login eine Fehlermeldung angezeigt. Um dieses Problem zu umgehen, loggen Sie sich bitte als Administrator ein und geben Sie dem FTAPI-Account einen anderen Benutzernamen.

LDAP-URL

Dieser Parameter ist Pflicht und gibt die URL zu Ihrem LDAP-Server im Format ldap://<host>:<port> an. Über diese URL muss der LDAP-Server vom FTAPI-System aus erreichbar sein. Ein Beispiel:

```
ldap://ad-server:389
```

LDAP-Manager

Mit diesem Parameter wird der sogenannte DN (Benutzername) des LDAP-Managers angegeben, über den die Verbindung zum LDAP-System aufgebaut werden soll. Diese Angabe ist Pflicht. Ein Beispiel:

```
MaxHuber@company.local
```

Manager-Passwort

Das Passwort des LDAP-Managers. Diese Angabe ist optional, je nach dem, ob der LDAP-Manager ein Passwort besitzt oder nicht.

Parameter für das Attribut-Mapping

Mit den nachfolgend beschriebenen Parametern können Sie bestimmen, welche Felder aus einem LDAP-Account verwendet werden, um dessen Werte in den FTAPI-Account zu übernehmen.

> Im Regelfall ist keine Änderung dieser Parameter notwendig.

Attribut für Feld 'Vornamen'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als **Vorname** in den lokalen FTAPI-Account übernommen werden soll.

Attribut für Feld 'Nachnamen'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als **Nachname** in den lokalen FTAPI-Account übernommen werden soll.

Attribut für Feld 'E-Mail-Adressen'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als **E-Mail** in den lokalen FTAPI-Account übernommen werden soll.

Attribut für Feld 'Firma'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als **Firma** in den lokalen FTAPI-Account übernommen werden soll.

Attribut für Feld 'Position'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als **Position** in den lokalen FTAPI-Account übernommen werden soll.

Attribut für Feld 'Telefon'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als **Telefon** in den lokalen FTAPI-Account übernommen werden soll.

Attribut für Feld 'Fingerprint'

Bestimmt den Namen des LDAP-Context-Felds, dessen Wert als eindeutiger **Fingerprint** in den lokalen FTAPI-Account übernommen werden soll. Dies ist aus Sicherheitsgründen notwendig, um sicher zu stellen, dass der LDAP-Context nicht durch einen anderen "ausgetauscht" wird und kann jedes beliebige Feld sein, welches einen eindeutigen Wert besitzt.

Attribut für Feld 'Aktiv'

Ein Feld, das bestimmt, ob der jeweilige LDAP-User in das FTAPI System übernommen werden soll.

Attribut für Feld 'User Account Control'

Ein Feld, das...

Parameter für die LDAP-Suche

Nachdem mit dem LDAP-System eine Verbindung hergestellt wurde, wird in einem ganz bestimmten Bereich im "LDAP-Baum" nach dem Login-Benutzer gesucht.
Welcher Bereich dies ist und wie diese Suche durchgeführt werden soll, wird durch die nachfolgenden Parameter bestimmt.

Suchbasis

Dieser Parameter bestimmt den Basis-Knoten im LDAP-Baum, ab dem mit der Suche begonnen werden soll.
Ein solcher Pfad könnte beispielsweise für einen Active-Directory-Server auf einem Microsoft Small Business Server folgendermaßen aussehen:

```
ou=SBSUsers,ou=Users,ou=MyBusiness,dc=ftapi,dc=local
```

Weitergehende Informationen, wie LDAP-Pfade aufgebaut sein können, entnehmen Sie bitte der Dokumentation zu Ihrem LDAP-Serversystem.

Suchfilter

Mit diesem Parameter werden die Context-Typen bestimmt, die für eine Überprüfung heran gezogen werden sollen. Es stellt somit einen Filter dar.
Unter einem Active-Directory-Server sollte diese Angabe stets folgendermaßen belassen werden:

```
(&(cn={0})(objectclass=user))
```

Durchsuche Unterordner

Dieser Parameter bestimmt, ob rekursiv gesucht werden soll (true) oder nicht (false). D.h., ob auch in den Kinderknoten nach dem Login-Benutzer gesucht werden soll.
Vor allem bei großen LDAP-Bäumen ist es häufig sinnvoll, diesen Wert auf false zu setzen, um die Systemlast zu vermindern. Allerdings muss dann der Parameter
ftapi.search.base direkt auf die korrekte Ebene zeigen.

Standard Gruppen

Wird für das Single Mapping weiter unten benötigt.

Mapping von LDAP-Gruppen zu FTAPI-Gruppen

Standardmäßig kann sich jeder Benutzer, der einen gültigen Account im LDAP-System besitzt, in FTAPI einloggen.
Er erhält in diesem Fall automatisch alle Gruppen zugeordnet, die durch **ftapi.ldap.default.groups** spezifiziert wurden.

Vor allem in größeren Umgebungen ist es oft gewollt, dass nur eine bestimme, privilegierte Gruppe von LDAP-Benutzern Zugang zum FTAPI-System erhält.

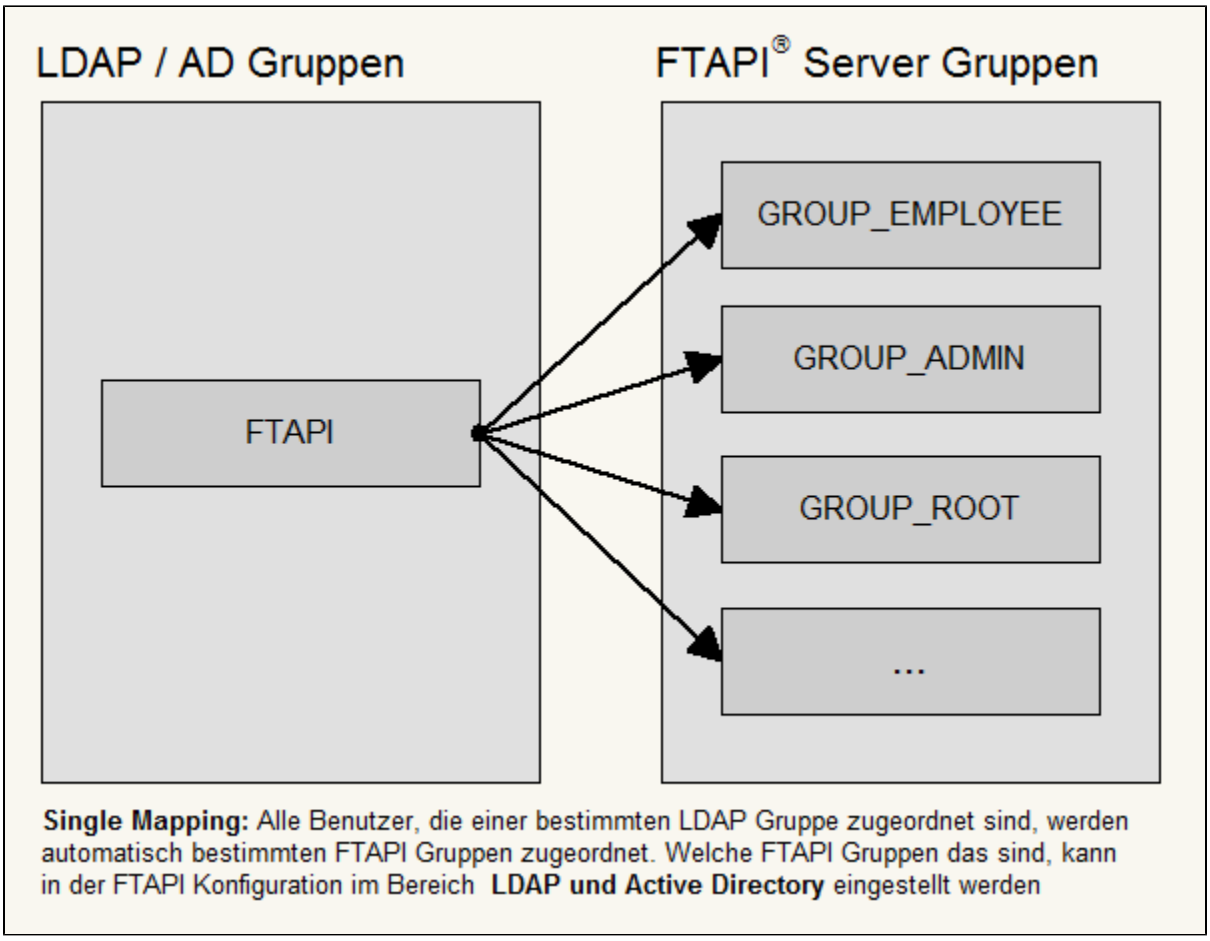
FTAPI bietet hierfür zwei verschiedene Möglichkeiten an, wie eine Zuordnung von LDAP zu FTAPI-Gruppen erfolgen kann.

- Single Mapping &
- Multi Mapping

Diese werden nachfolgend näher erklärt.

Single Mapping

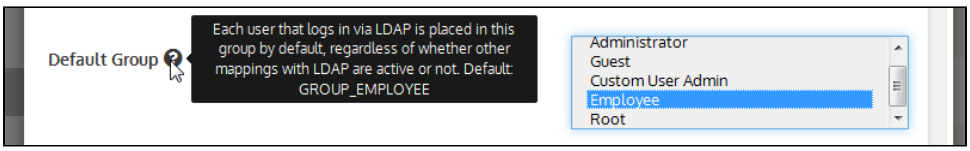
Dies ist die einfachere Variante von beiden, um von LDAP zu FTAPI Gruppen zu mappen und wird deshalb vor allem dann empfohlen, falls Sie keine feingranulare Zuordnung je Benutzer zu FTAPI-Gruppen benötigen.
Hier muss nur eine einzige Gruppe in LDAP angelegt werden (z.B. mit dem Namen *FTAPI*). Alle LDAP-Benutzer, die dieser Gruppe angehören, erhalten beim Login dann automatisch die FTAPI-Gruppe zugeordnet, die durch das Property **ftapi.ldap.default.groups** definiert wurden.



Innerhalb der Organisationseinheit SBSUsers wurde hier die Gruppe *FTAPI* angelegt, welcher die für FTAPI privilegierten Benutzer hinzugefügt werden.

Die wichtigsten Einstellungen zu den obigen Properties sind nachfolgend noch einmal zusammengefasst:

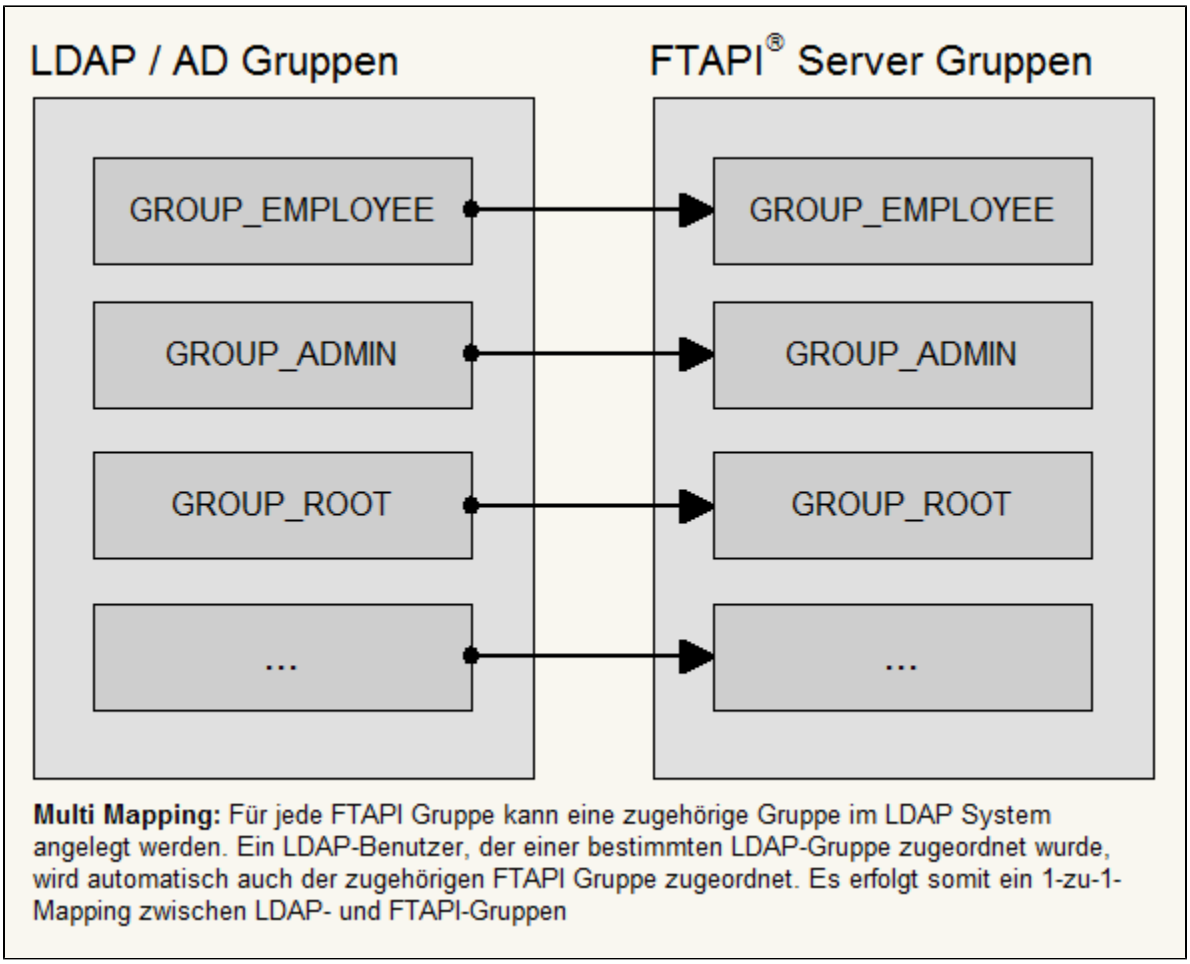
- **Gruppenmapping aktivieren -> aktiv**
  aktiviert das generelle Mapping von LDAP-Gruppen zu FTAPI-Gruppen
- **Suchbasis für Gruppenmapping**
  Angabe des LDAP-Pfades zum Verzeichnis, in welchem sich die LDAP-Gruppe befindet
- **Nur LDAP-Gruppe für Mapping verwenden -> aktiv**
  aktiviert das Single Mapping
- **Name der LDAP-Gruppe**
  Name der LDAP-Gruppe, welcher alle LDAP-Benutzer zugeordnet sein müssen, um FTAPI verwenden zu können.
  Diese Gruppe muss sich innerhalb des Pfads befinden, der durch **Suchbasis für Gruppenmapping** angegeben wurde
- **Standard Gruppen**
  Stellen Sie hier all diejenigen FTAPI-Gruppen ein, die ein Benutzer der der LDAP-Gruppe FTAPI standardmäßig erhält.
  Nachfolgend als Beispiel die Standard-Zuordnungen:



Multi Mapping

Im Gegensatz zum Single Mapping, bietet das Multi Mapping die Möglichkeit der 1-zu-1-Zuordnung von LDAP-Gruppen zu FTAPI-Gruppen.

Legen Sie hierfür in LDAP einfach eine Gruppe an, die denselben Namen wie die zugehörige FTAPI-Gruppe (z.B. GROUP_EMPLOYEE) besitzt und fügen Sie dieser die entsprechenden LDAP-Benutzer hinzu. Sobald sich diese LDAP-Benutzer in FTAPI einloggen, werden sie automatisch der gleichnamigen FTAPI-Gruppe zugeordnet. Dies können Sie für alle anderen FTAPI-Gruppen gleichermaßen durchführen.



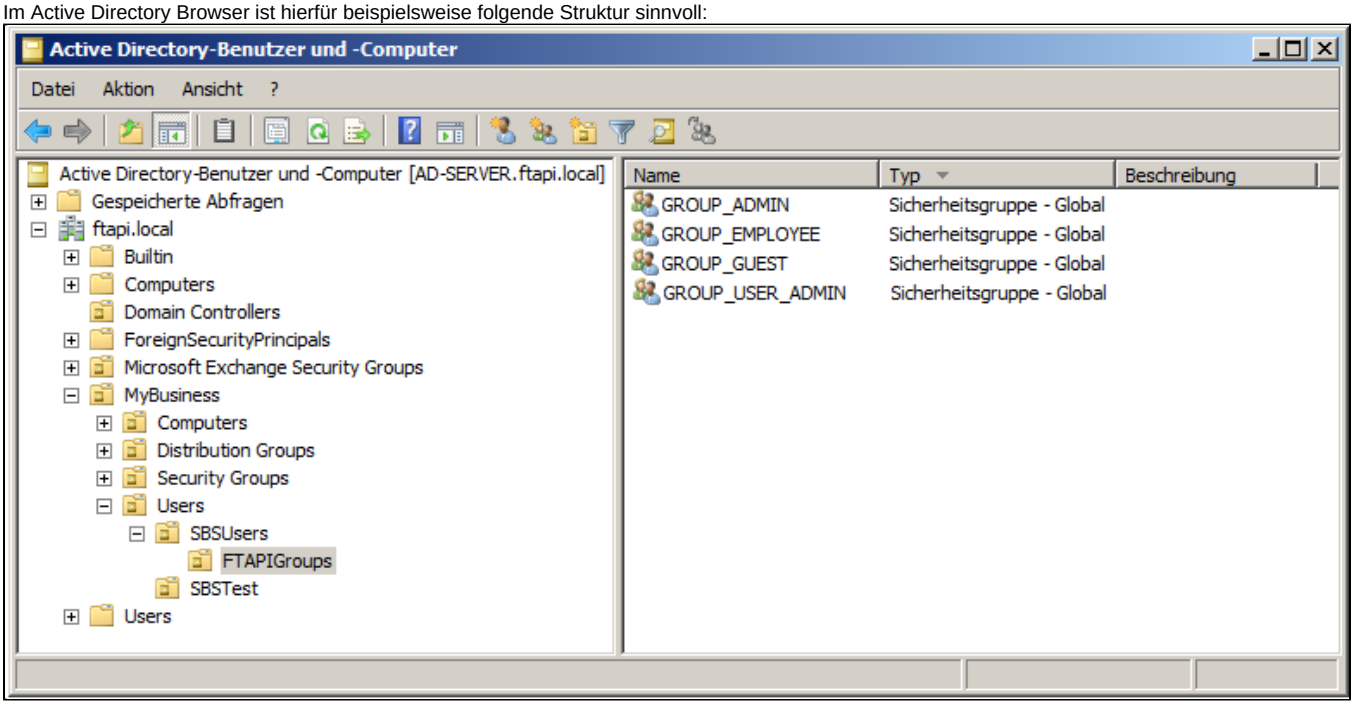
Multi Mapping: Für jede FTAPI Gruppe kann eine zugehörige Gruppe im LDAP System angelegt werden. Ein LDAP-Benutzer, der einer bestimmten LDAP-Gruppe zugeordnet wurde, wird automatisch auch der zugehörigen FTAPI Gruppe zugeordnet. Es erfolgt somit ein 1-zu-1-Mapping zwischen LDAP- und FTAPI-Gruppen

Gleiche Namen

Beachten Sie, dass die Gruppen Name im AD **exakt gleich** zu den Gruppen Namen im FTAPI sein müssen.

Im Falle der System Gruppen sehen Sie die Namen im obigen Bild

Im Active Directory Browser ist hierfür beispielsweise folgende Struktur sinnvoll:



Innerhalb der Organisationseinheit SBSUsers wurde eine weitere Organisationseinheit *FTAPIGroups* erstellt, in welcher sich alle Gruppen befinden.

Beim Multi Mapping ist - im Vergleich zum Single Mapping (s. oben) - lediglich das folgende Property anders einzustellen.

- **Nur LDAP-Gruppe für Mapping verwenden -> deaktiviert**
  deaktiviert das Single Mapping und aktiviert das Multi Mapping

Kein Gruppen Mapping

Sie können das AD Mapping des FTAPI Systems auch so einstellen, dass **alle AD User innerhalb des Suchpfades** importiert werden.

- **Gruppenmapping aktivieren -> deaktiviert**
  deaktiviert das Gruppenmapping und lässt jeden User, der im AD gefunden wird (alle user in *Suchfilter*) in das FTAPI System

Einrichtung mehrerer LDAP-Systeme

Es können bis zu zehn (10) LDAP-Systeme über die FTAPI Konfiguration hinterlegt werden. Diese werden dann hintereinander bei einem Loginversuch eines Benutzers auf dessen korrekten Login hin überprüft.