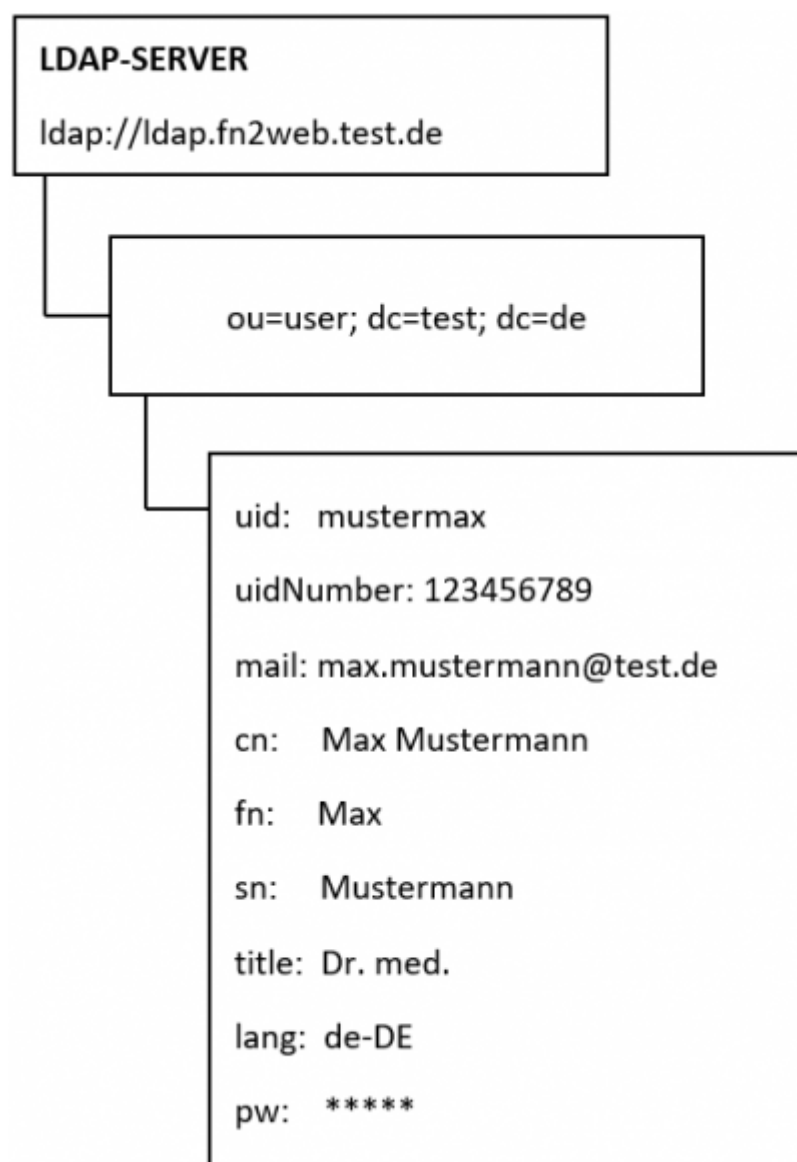


Nutzer aus LDAP anlegen - Konfiguration

Mit der Version 2.04.09 von FN2Web ist möglich Personen mit Daten, die aus einem externen LDAP-System gelesen werden können anzulegen. Um diese Funktion verwenden zu können muss eine entsprechende Konfiguration von Seiten der Systemadministratoren vorgenommen werden. Dies wird hier unter Verwendung eines fiktiven LDAP-Servers erklärt.

Beispiel LDAP-System

Zum Verständnis wird von folgender, repräsentativen LDAP-Struktur ausgegangen. Für die Konfiguration müssen die entsprechenden Daten wie die Serveradresse, der DN-Pfad oder die Attributnamen Ihrem individuellen LDAP-System angepasst werden.



Anpassung von Parametern

Die Parameter müssen in **FN2XML/Web-Inf/web.xml** ergänzt werden. Da einige Parameter bereits durch die LDAP-Authentifizierung verwendet werden müssen ggf. nicht alle Parameter ergänzt werden.

Parameter welche mit der LDAP-Authentifizierung geteilt werden

Diese Parameter sind ggf. bereits vorhanden.

```
<init-param>
<param-name>ldapAuthBaseDN</param-name>
<param-value>ou=users,dc=test,dc=de</param-value>
<description>ldap server used for *auth*entication: LDAP base DN; this
parameter is only relevant if "authenticationMethod" is set to "ldap";
example: "ou=People,dc=myorg,dc=de"</description>
</init-param>
<init-param>
<param-name>ldapAuthHost</param-name>
<param-value>ldap://ldap.fn2web.test</param-value>
<description>ldap server used for *auth*entication: DNS name of the host
that runs the LDAP server; this parameter is only relevant if
"authenticationMethod" is set to "ldap"; example: "ldap://authldap.org.com"
(non-SSL), "ldaps://authldap.org.com" (SSL);</description>
</init-param>
<init-param>
<param-name>ldapAuthUidAttribute</param-name>
<param-value>uid</param-value>
<description>ldap server used for *auth*entication: LDAP attribute used to
search for user; this parameter is only relevant if "authenticationMethod"
is set to "ldap"; example: "uid"</description>
</init-param>
```

Folgende Parameter sind nur anzugeben, wenn ein Login für den Zugriff auf den LDAP-Server benötigt wird.

```
<init-param>
<param-name>ldapAuthType</param-name>
<param-value>simple</param-value>
<description>ldap server used for *auth*entication: ldap authentication
type; default:"simple"; this parameter is only relevant if
"authenticationMethod" is set to "ldap"</description>
</init-param>
<init-param>
<param-name>ldapAuthServiceUser</param-name>
<param-value>mustermax</param-value>
<description>ldap server used for *auth*entication: LDAP user that has
```

```

access to query LDAP for auth and name resolution; this parameter is only
relevant if "authenticationMethod" is set to "ldap"; example:
"surveyService"</description>
</init-param>
<init-param>
<param-name>ldapAuthServiceCredential</param-name>
<param-value>*****</param-value>
<description>ldap server used for *auth*entication: password of the LDAP
user that has access to query LDAP for authentication and name resolution;
this parameter is only relevant if "authenticationMethod" is set to "ldap";
example: "qqe$eu@o"</description>
</init-param>

```

Neue Parameter zum Anlegen von Nutzern aus LDAP

Verpflichtend anzugebene Parameter

```

<init-param>
<param-name>ldapImportSearchListPattern</param-name>
<param-value>[cn] ([uid])</param-value>
<description>Pattern für Ausgabe von Suchergebnissen für Personen in LDAP.
LDAP-Attribute werden in Eckigen Klammern angegeben. z.B. "[cn] ([uid])" ->
"Wert für Attribut 'cn' (Wert für Attribut 'uid')"</description>
</init-param>

```

Optionale Parameter

Diese Parameter werden verwendet um Formular-Daten zu füllen. Wenn kein entsprechendes LDAP-Attribut vorhanden um ein Formular Feld zu füllen kann der entsprechende Parameter weggelassen werden.

```

<init-param>
<param-name>ldapImportPersonstubBezPattern</param-name>
<param-value>[cn]</param-value>
<description>Pattern zum Füllen des Wertes "Bez" für neue Personen aus LDAP.
LDAP-Attribute werden in Eckigen Klammern angegeben. z.B. "[cn]" -> "Wert
für Attribut 'cn'"</description>
</init-param>
<init-param>
<param-name>ldapImportPersonstubEmailKey</param-name>
<param-value>mail</param-value>
<description>Key zum Auslesen des Wertes "Email" für neue Personen aus LDAP.
Angabe des entsprechenden LDAP-Attributes. z.B. "mail" -> "Wert für ,Attribut
'mail'"</description>
</init-param>
<init-param>
<param-name>ldapImportPersonstubSpracheKey</param-name>

```

```
<param-value>lang</param-value>
<description>Key zum Auslesen des Wertes "Sprache" für neue Personen aus
LDAP. Angabe des entsprechenden LDAP-Attributes. z.B. "lang" -> "Wert für
Attribut "lang"</description>
</init-param>
```

Anwendungsbeispiele für die neuen Parameter

Parameter-Namen die mit "Key" enden

Hierbei wird lediglich der Attribut-Name des User-Objekts angegeben welches in LDAP hinterlegt ist.

Beispiel: Für den Parameter **ldapImportPersonstubEmailKey** wird der Wert **mail** angegeben. Im LDAP-Beispiel wird hierfür **max.mustermann@test.de** ausgegeben.

Parameter-Namen die mit "Pattern" enden

Hierbei wird ein Pattern angegeben, welches aus mehreren Attribut-Namen des User-Objekts bestehen kann. Wichtig ist hierbei, dass die Attribut-Namen in eckigen Klammern angegeben werden um sie von Fülltext zu unterscheiden zu können.

Beispiel: Für den Parameter **ldapImportSearchListPattern** wird der Wert **[title] [fn] [sn] ([uid])** angegeben. Im LDAP-Beispiel wird hierfür **Dr. med. Max Mustermann (mustermx)** ausgegeben.

Anpassung von Datenbank-Werten

Tabelle LDAPSEARCH (Flexnow Datenbank)



In der Tabelle **LDAPSEARCH** werden alle LDAP-Attribute angegeben, welche für die Suche von User-Objekten verwendet werden können. Es muss mindestens ein Datensatz angegeben sein um Nutzer aus LDAP anlegen zu können.

Tabellenfelder von **LDAPSEARCH**:

- **ldapsearch**: Die eindeutige ID des Datensatzes (*fortlaufende Nummer*)
- **ldapkey**: Das LDAP-Attribut nach welchem Gesucht werden kann
- **bez**: Eine Beschreibung des Attributs, welches in der Dropdown-Liste des Import-Formulars angezeigt wird.

Beispiel:

Tabelle in SQL

*	 Idapsearch 	Idapkey	bez
1		1 uid	Kennung
2		2 sn	Nachname
3		3 mail	Email

Anzeige in FN2RBACWEB2

Person in Ldap suchen:

Kennung [uid] v
 Kennung [uid]
 Nachname [sn]
 Email [mail]

Tabelle EXTERN_FELD (Flexnow Datenbank)

Die Tabelle **EXTERN_FELD** wird zur Verknüpfung von FlexNow-Daten mit Daten von Fremdsystemen verwendet. Im Fall von LDAP werden Personstube-Objekte der META-Datenbank mit den zugehörigen LDAP-Objekten verknüpft. *(Es ist geplant diese Einstellung auch zur Verknüpfung von Person-Objekten der Flexnow-Datenbank mit LDAP zu verwenden sobald dies implementiert wird.)*

Tabellenfelder von **LDAPSEARCH**:


- **extern_feld**: Die eindeutige ID des Datensatzes (*fortlaufende Nummer*)
- **extern_system**: Das externe System welches verwendet wird. In diesem Fall ist der Wert **9** anzugeben, welcher dem LDAP-System zugewiesen ist. *(Die externen Systeme sind in der Tabelle EXTERN_SYSTEM angegeben. **LDAP** wird mit den veröffentlichten SQL Skript der Version 2.04.09 hinzugefügt.)*
- **tabelle**: Auf welche Tabelle des externen Systems wird verwiesen. Im speziellen Fall von LDAP muss der Wert **LDAP** angegeben werden.
- **feld**: Welches Feld der angegeben Tabelle verwendet werden soll. Im speziellen Fall von LDAP muss das gewünschte Attribut des User-Objekts im LDAP-System verwendet werden. Hierbei ist zu beachten, dass ein persistentes Attribut verwendet wird.

SQL-Statement:

bitte die Werte in eckigen Klammern anpassen.

```
INSERT INTO extern_feld (extern_feld, extern_system, tabelle, feld) VALUES ([Nächste freie ID], 9, 'LDAP', [LDAP-Attribut zum verlinken]);
```

Beispiel

 extern_feld	extern_system	tabelle	feld
19		9 LDAP	uidNumber

Bei Fragen ist Ihr Ansprechpartner [Sebastian Düsel](#).

From:
<https://wiki.ihb-eg.de/> - **FlexWiki**

Permanent link:
https://wiki.ihb-eg.de/doku.php/fn2rbacweb/nutzer_aus_ldap_anlegen_-_konfiguration?rev=1643789373

Last update: **2022/02/02 09:09**

