LDAP-Einstellungen für die Authentifizierung und den Import von Personendaten

Gültig ab Web-Version 2.04.11. Die LDAP-Authentifizierung existiert bereits seit vorherigen Versionen, wurde mit Version 2.04.11 jedoch aktualisiert. Für ältere Versionen finden Sie eine passende Anleitung hier.

Diese Anleitung beschreibt die in FlexNow vorzunehmenden Einstellungen, um ein LDAP-System zur Authentifizierung an FN2Web zu verwenden und optional Personendaten aus diesem LDAP-System nach FlexNow zu importieren.

Die Konfiguration sollte von Seiten der Systemadministratoren vorgenommen werden. Es wird ein Zugriff auf die META-Datenbank sowie auf die „context.xml“ des Tomcat Servers benötigt.

Überblick über die notwendige Konfiguration:

LDAP-Authentifizierung:

```
1. context.xml
2. Tabelle SETUPRBAC
```

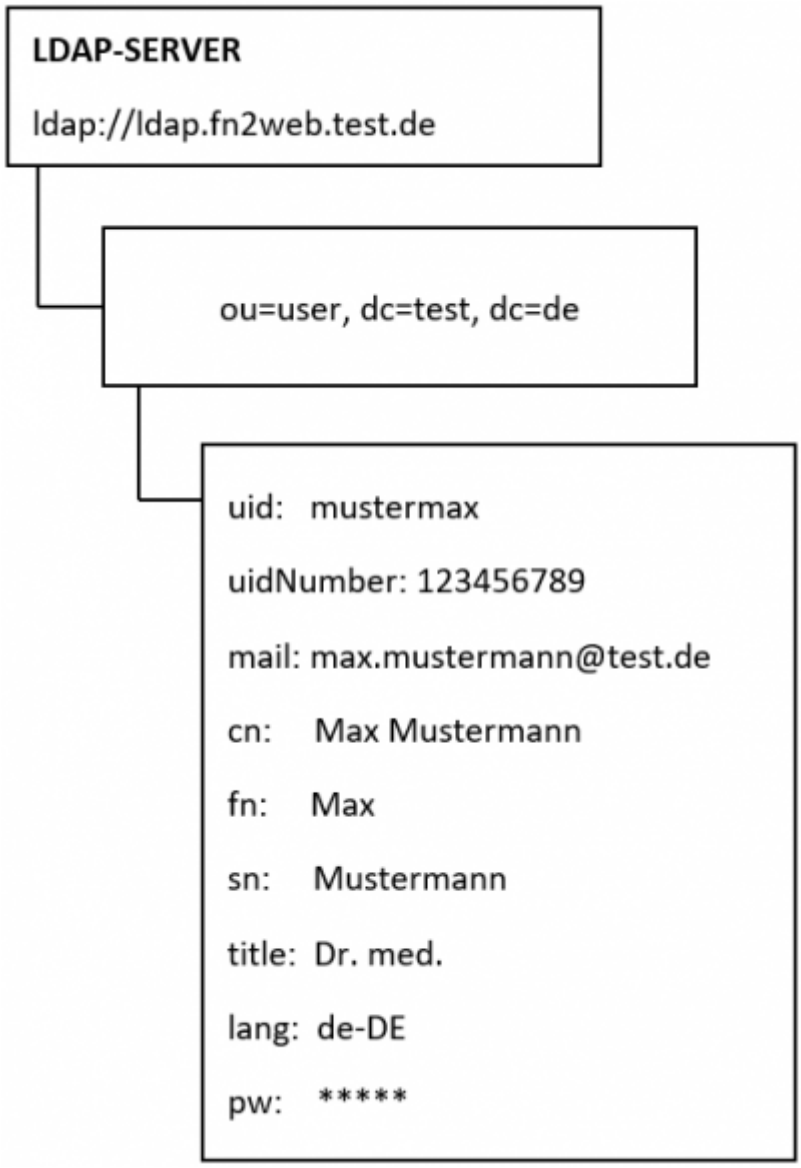
Zusätzlich für den Personenimport:

```
3. Tabelle LDAPSEARCHATTRIBUTE
4. Tabelle LDAPMAPPING
5. optional: Tabelle LDAPSEARCHFILTER
```

Bei Fragen ist Ihr Ansprechpartner Sebastian Düsel.

Beispiel eines LDAP-Systems

Die vorzunehmenden Einstellungen werden anhand der folgenden, repräsentativen LDAP-Struktur illustriert. Für die hochschulspezifische Konfiguration müssen die entsprechenden Daten wie die Serveradresse, der DN-Pfad oder die Attributnamen dem individuellen LDAP-System Ihrer Hochschule angepasst werden.



Dieses Beispiel wurde auch im 2.04.011-Release-Gespräch (

Folien

) verwendet.

Anpassung der context.xml

Für bestimmte LDAP-Funktionen wird ein „Service User“ mit lesenden Zugriffsrechten auf das LDAP-System benötigt. Die Angaben für Login und Passwort dieses LDAP-Users werden als Parameter in der context.xml des Tomcat Servers hinterlegt.

Pfad zur Datei: ***[Tomcat-Verzeichnis]*/conf/context.xml**

Parameter für Service User:

```
<Parameter description="Login für LDAP Service User"
name="LDAP_SERVICE_USER_LOGIN" value="Login des LDAP-Users"/>

<Parameter description="Passwort für LDAP Service User"
```

```
name="LDAP_SERVICE_USER_PASSWORD" value="Passwort des LDAP-Users"/>
```

Anpassungen in der META-Datenbank

__Tabelle SETUPRBAC__

Die Parameter für die LDAP-Authentifizierung und den LDAP-Import werden in der Tabelle **SETUPRBAC** der META-Datenbank verwaltet.

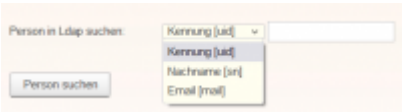
In der Spalte param_ ist der Parameter einzutragen, in der Spalte value_ der dazugehörige Wert des Parameters. Eine Übersicht über die Parameter enthält die folgende Tabelle.

Parameter-Name	Beschreibung
LDAP_HOSTS	LDAP-Hosts, für die Authentifizierung und den Import. Es können mehrere, durch Semikolons getrennte Hosts angegeben werden.
LDAP_BASE_DNS	Base-DNs, für die Authentifizierung und den Import. Es können mehrere, durch Semikolons getrennte Hosts angegeben werden.
LDAP_LOGIN_ATTRIBUTES	LDAP-Attribute, für die Authentifizierung. Es können mehrere, durch Semikolons getrennte Attribute angegeben werden.
LDAP_NAMING_ATTRIBUTE	Optionale Angabe welches der LDAP-Attribute Teil des DN (Distinguished Name) des LDAP-Elements ist. I.d.R. handelt es sich hierbei um das Attribut „uid“. Falls das verwendete Login-Attribut dem Naming-Attribut entspricht, kann ein DN generiert werden. Falls nicht muss der DN via einer Suche in LDAP ermittlet werden, befor die Authentifizierung erfolgen kann. Hierfür wird ggf. ein Service User benötigt.
LDAP_AUTH_TYPE	Optionale Angabe des LDAP-Authentifizierungs-Mechanismus. Mögliche Werte sind „none“, „simple“ oder der Name eines SASL Mechanismus. Falls dieser Parameter nicht gesetzt wird, wird „simple“ verwendet.
LDAP_AUTH_WITH_TLS	Optionale Angabe, ob SSL für die LDAP-Authentifizierung verwendetet werden soll. Mögliche Werte sind „TRUE“ oder „FALSE“. Defaultwert ist „FALSE“.
LDAP_IGNORE_CERTIFICATE	Optionale Angabe, ob bei der LDAP-Authentifizierung die Server-Zertifikate ignoriert werden sollen. Diese Einstellung sollte **ausschließlich** als letzte Möglichkeit verwendet werden. Falls der Parameter LDAP_AUTH_WITH_TLS=false, wird diese Einstellung ignoriert. Mögliche Werte sind „TRUE“ oder „FALSE“. Defaultwert ist „FALSE“.
LDAP_SEARCH_LIST_PATTERN	Pattern für Ausgabe von Suchergebnissen in FN2RBACWeb2 für den Personenimport aus LDAP. LDAP-Attribute werden in Eckigen Klammern angegeben. z.B. „[cn] ([uid])“ → „Wert für Attribut 'cn' (Wert für Attribut 'uid')“.

Parameter-Name	Beschreibung
LDAP_AUTH_PARAM_MAPPING	Optionale Angabe wie die Authentifizierungs-Attribute **LDAP_HOSTS**, **LDAP_BASE_DNS** und **LDAP_LOGIN_ATTRIBUTES** miteinander kombiniert werden sollen. Falls dieser Parameter nicht angegeben wird, werden alle möglichen Kombinationen aus den 3 Parametern verwendet. Als Wert werden die einzelnen Indexe der entsprechenden Parameter angegeben in Gruppen ihrer jeweiligen Indexe angegeben. Diese werden durch ein Semikolon getrennt. z.B. **0;0;0;0;1;1** wären die 2 Kombinationen aus **LDAP-Host[0], Ldap-BaseDN[0], LDAP-LoginAttribut[0]** und **LDAP-Host[0], LDAP-BaseDN[1], LDAP-LoginAttribut[1]**
LDAP_IMPORT_PARAM_MAPPING	Optionale Angabe wie die Import-Attribute **LDAP_HOSTS** und **LDAP_BASE_DNS** miteinander kombiniert werden sollen. Falls dieser Parameter nicht angegeben wird, werden alle möglichen Kombinationen aus den beiden Parametern verwendet. Als Wert werden die einzelnen Indexe der entsprechenden Parameter angegeben in Gruppen ihrer jeweiligen Indexe angegeben. Diese werden durch ein Semikolon getrennt. z.B. **0;0;0;1** wären die 2 Kombinationen aus **LDAP-Host[0], Ldap-BaseDN[0]** und **LDAP-Host[0], LDAP-BaseDN[1]**
LDAP_IMPORT_SEARCH_FILTER	Optionale Angabe eines Filters, welcher bei der Suche nach LDAP-Elementen für den Import hinzugefügt werden soll. Dieser Parameter wird nur bei einer tiefen LDAP-Struktur verwendet. Sollte eine Flache LDAP-Struktur verwendet werden, in der Gruppen-Elemente gepflegt werden können entsprechende Filter über die Tabelle **LDAPSEARCHFILTER** konfiguriert werden.

Beispiel für LDAP_IMPORT_SEARCH_FILTER

Für den Import von Personen aus LDAP wählt der Anwender ein LDAP-Attribut aus und gibt den gewünschten Wert an.



z.B. Attribut **uid** und den Wert **muster***. Das System erzeugt hieraus die Suchanfrage **uid=muster*** welche wie bei LDAPSEARCH an das LDAP-System gesendet wird um alle passenden Elemente unterhalb des verwendeten BaseDNs zurück gibt. Angenommen, es soll sicher gestellt werden, dass nur Element welche innerhalb des **DC=test** gesucht werden sollen, kann für das SETUP-Attribut LDAP_IMPORT_SEARCH_FILTER der Wert **(dc=test)** angegeben werden. Dieser Term wird mittles einer Und-Verknüpfung allen Such-Anfragen aus RBACWeb2 hinzugefügt. Für das Beispiel mit **uid=muster*** würde hieraus die LDAP-Suchanfrage **(&(uid=muster*)(dc=test))** generiert.

__Tabelle LDAPSEARCHATTRIBUTE__

In der Tabelle **LDAPSEARCHATTRIBUTE** in der META-Datenbank können alle LDAP-Attribute hinterlegt werden, nach denen beim Personenimport gesucht werden soll. Die Felder der Tabelle sind in nachfolgender Übersicht beschrieben.

Die Tabelle **LDAPSEARCHATTRIBUTE** ersetzt ab Version 2.04.11 die Tabelle **LDAPSEARCH** aus der Flexnow-Datenbank.

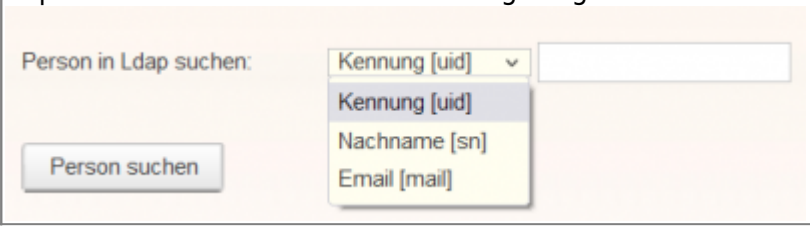
Feld (Spalte) der Tabelle LDAPSEARCHATTRIBUTE	Beschreibung
ldapsearchattribute	Der Name des LDAP-Attributs, welches als Parameter für die Suche von LDAP-Datensätzen verwendet werden soll. Alle eingetragenen Attribute sind beim Personenimport aus LDAP in der Anwendung FN2RBACWeb in einer Dropdown-Liste zur Auswahl vorhanden.
bez	Die Bezeichnung des LDAP-Attributes, die in der Dropdown-Liste des Import-Formulars in FN2RBACWeb angezeigt wird. 

__Tabelle LDAPMAPPING__

Die Tabelle **LDAPMAPPING** ersetzt die Mapping-Properties, welche bis zur FN2Web-Version 2.04.10 im Einsatz waren. Diese werden ab Version 2.04.11 nicht mehr verwendet und können entfernt werden. Das Mapping wird momentan (Stand 2.04.11) nur für den Import von Personen verwendet.

Feld (Spalte) der Tabelle LDAPMAPPING	Beschreibung
ldapmapping_class	Die Flexnow-Tabelle, in welche die Daten aus LDAP importiert werden sollen.
ldapmapping_field	Das Flexnow-Tabellenfeld (Spalte), in welche die Daten aus LDAP importiert werden sollen.
mappingstring	Die LDAP-Felder, aus denen die Daten geladen werden sollen. Es können mehrere LDAP-Attribute angegeben werden.

Zulässige Werte für ldapmapping_class und ldapmapping_field

Zulässige Werte für ldapmapping_class	Zulässige Werte für ldapmapping_field	Verwendung
Personstub	bez, email, sprache	Import von LDAP-Daten in die Tabelle Personstub in FN2RBACWeb.
Person	vorname, nachname, akadgrad, versnr, url, plz, ort, strasse, telefon, email, adrfreitext	Import von LDAP-Daten in die Tabelle Person in FN2RBACWeb.
Person_update	vorname, nachname, akadgrad, versnr, url, plz, ort, strasse, telefon, email, adrfreitext	Update von Person-Daten mit Daten aus LDAP. Die Person muss mit LDAP-Verknüpft sein. Die Verknüpfung erfolgt automatisch beim Import der Person aus LDAP.

Anwendungsbeispiele für 'mappingstring'

1. Verwendung eines LDAP-Attributes als Key

Es kann lediglich das LDAP-Attribut angegeben werden. Der hinterlegte Wert wird dann direkt übernommen.

Beispiel: Es wird der Wert **mail** für **mappingstring** angegeben. Im LDAP-Beispiel wird hierfür **max.mustermann@test.de** übernommen.

2. Verwendung eines oder mehrerer LDAP-Attribute mit Fülltext

Es kann auch ein Pattern angegeben werden, welches aus mehreren LDAP-Attributen und Fülltext bestehen kann. Wichtig ist hierbei, dass die LDAP-Attribute in eckigen Klammern angegeben werden um sie von Fülltext zu unterscheiden zu können.

Beispiel: Es wird der Wert **[title] [fn] [sn] ([uid])** angegeben. Im LDAP-Beispiel wird hierfür **Dr. med. Max Mustermann (mustermax)** übernommen.

__Tabelle LDAPSEARCHFILTER__

Über die Tabelle **LDAPSEARCHFILTER** lässt sich optional die Suche nach LDAP-Datensätzen für den Personenimport mit in LDAP hinterlegten Gruppen einschränken.

Einträge in dieser Tabelle sind für die Konfiguration des Personenimports nicht zwingend notwendig. Dann erfolgt beim Personenimport kein Filtern der LDAP-Suchergebnisse.

Feld (Spalte) der Tabelle LDAPSEARCHFILTER	Beschreibung
ldapsearchfilter	Einmalige, eindeutige ID des Datensatzes. (INTEGER)
sourcedn	Der vollständige DN der Gruppe im LDAP-System.
sourceattribute	Das Attribut in der LDAP-Gruppe, welche die Mitglieds-Schlüssel speichert.
targetattribute	Das Attribut einer Person in LDAP, welches in der LDAP-Gruppe als Zuordnungs-Schlüssel dient.

Anwendungsbeispiel

Angenommen, im Test-LDAP-System gibt ein LDAP-Element mit dem DN **ou=personal, ou=verwaltung, dc=test, dc=de** mit dem Attribut **members** in welchem alle **uidNumber** Attribute von Mitgliedern der Gruppe hinterlegt sind. Um bei der Suche für den Person-Import nur Mitglieder dieser Gruppe anzeigen zu lassen sind folgende Eingaben zu tun:

- **sourcedn** bekommt den Wert **ou=personal, ou=verwaltung, dc=test, dc=de**.
- **sourceattribute** bekommt den Wert **members**, da dies das Feld der Gruppen ist welches die Mitglieder verwaltet.
- **targetattribute** bekommt den Wert **uidNumber** da dies die Felder der Personen sind, welche in **members** hinterlegt werden.

Anpassungen in der FLEXNOW-Datenbank

Eine Anpassung in der Tabelle **EXTERN_FELD** ist nur notwendig, wenn der Personenimport eingesetzt werden soll.

ACHTUNG! Falls hier kein Eintrag hinzugefügt wird, ist der Personenimport aus LDAP deaktiviert.

__Tabelle EXTERN_FELD__

Die Tabelle **EXTERN_FELD** wird zur Verknüpfung von FlexNow-Daten mit Daten von Fremdsystemen verwendet. Im Fall von LDAP werden Personstub-Objekte der META-Datenbank mit den zugehörigen LDAP-Objekten verknüpft.

Feld (Spalte) der Tabelle EXTERN_FELD	**Beschreibung**
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 wurde mit den veröffentlichten SQL-Skripten der Version 2.04.09 hinzugefügt.)*
tabelle	Angabe der Tabelle des externen Systems, auf welche verwiesen wird. 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

Der Wert für „feld“: 'LDAP-Attribut zum Verlinken' ist anzupassen!

```
INSERT INTO extern_feld (extern_feld, extern_system, tabelle, feld) VALUES
(19, 9, 'LDAP', 'LDAP-Attribut zum Verlinken');
```

Beispiel

INSERT INTO extern_feld (extern_feld, extern_system, tabelle, feld) VALUES (19, 9, 'LDAP', 'uidNumber');

extern_feld	extern_system	tabelle	feld
19	9	LDAP	uidNumber