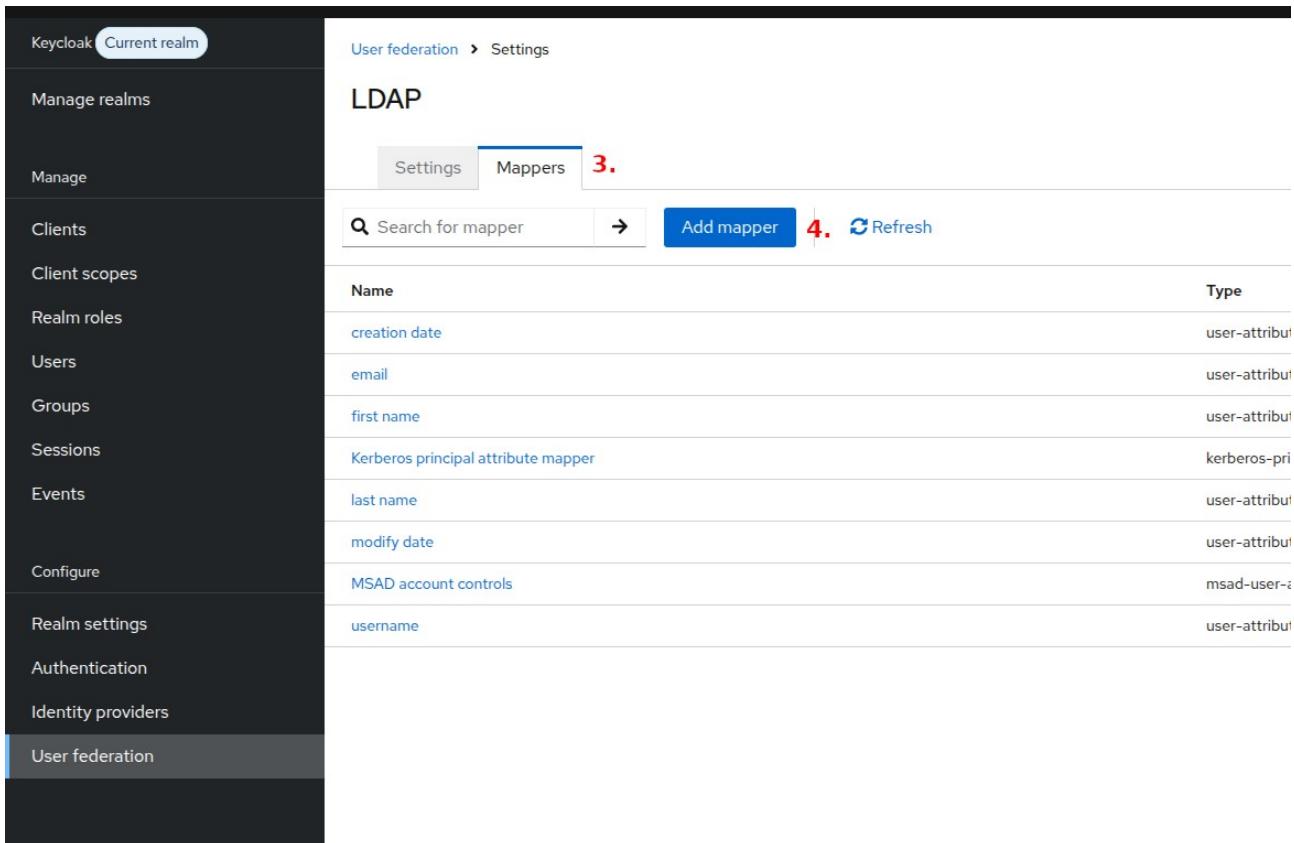


The screenshot shows the Keycloak administration interface. The left sidebar contains a list of management options: Manage realms, Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The 'User federation' option is highlighted with a blue bar and a red number '1.' above it. The main content area is titled 'User federation' and describes it as providing access to external databases and directories like LDAP. It features a 'Add new provider' button, a 'Manage priorities' button, and a list of providers. One provider is listed: 'Ldap' with priority '2.' and status 'Enabled'.

1. Select user federation
2. Select the LDAP provider



Keycloak Current realm

User federation > Settings

## LDAP

Manage realms

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Settings **3.**

Mappers **4.**

Search for mapper → Add mapper Refresh

Name	Type
creation date	user-attribute
email	user-attribute
first name	user-attribute
Kerberos principal attribute mapper	kerberos-principal
last name	user-attribute
modify date	user-attribute
MSAD account controls	msad-user-attribute
username	user-attribute

3. Select the Mappers tab
4. Click on the add mapper button

### Create new mapper

Name \* ② **5.**

Mapper type \* ② **6.**

5. Name the mapper (for example: SAML name id)
6. Set the type to user-attribute-ldap-mapper

## Create new mapper

Name * ②	SAML name id
Mapper type * ②	user-attribute-ldap-mapper
User Model Attribute * ②	saml.persistent.name.id.for.* <b>7.</b>
LDAP Attribute * ②	entryUUID <b>8.</b>
Read Only ②	<input checked="" type="checkbox"/> On
Always Read Value From LDAP ②	<input checked="" type="checkbox"/> On <b>9.</b>
Is Mandatory In LDAP ②	<input type="checkbox"/> Off
Attribute default value ②	
Force a Default Value ②	<input checked="" type="checkbox"/> On
Is Binary Attribute ②	<input type="checkbox"/> Off

**10.** [Save](#) [Cancel](#)

### 7. Set the User model attribute to:

- saml.persistent.name.id.for.\* for all saml clients or
- saml.persistent.name.id.for.id-of-client for only Flexopus (you can see the client id in the url client details page, see image below)

8. Set your desired source attribute, entryUUID should always exist as far as I know

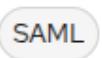
9. Turn on Always Read Value From LDAP

10. Save the new mapper, now it should work.

</admin/master/console/#/master/clients/eef7ef5c-3e57-4391-b758-73ba0c5e23e6/settings>

admin user. To harden security, create a permanent admin account and delete the temporary one.

[Clients](#) > [Client details](#)

<https://demo.flexopus.com/auth/saml2-7> 

Clients are applications and services that can request authentication of a user.