

The screenshot shows the Keycloak administration interface. On the left is a dark sidebar with a menu. The top of the sidebar has the Keycloak logo and a hamburger menu icon. Below it, the menu items are: 'Keycloak' (with a 'Current realm' button), 'Manage realms', 'Manage', 'Clients', 'Client scopes', 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings', 'Authentication', 'Identity providers', and 'User federation' (which is highlighted with a blue bar and a red '1.'). The main content area on the right has a white header with the title 'User federation' and a subtitle 'User federation provides access to external databases and directories, such as LDAP ar'. Below the subtitle are two buttons: 'Add new provider' (blue) and 'Manage priorities' (light blue). The main content area has a light gray background. In the center, there is a white card. Inside the card, the text 'ldap' is followed by a red '2.' and a vertical ellipsis icon. Below this, the text 'Ldap' is followed by a blue 'Enabled' button.

Keycloak **Current realm**

Manage realms

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

**User federation 1.**

## User federation

User federation provides access to external databases and directories, such as LDAP ar

[Add new provider](#) [Manage priorities](#)

ldap 2. ⋮

Ldap [Enabled](#)

1. Select user federation
2. Select the LDAP provider

Keycloak Current realm

Manage realms

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

User federation > Settings

### LDAP

Settings Mappers **3.**

Search for mapper → Add mapper **4.** Refresh

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

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

#### Create new mapper

Name \* ⓘ **5.**

Mapper type \* ⓘ **6.**

Save Cancel

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

## Create new mapper

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

10.

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/ee7ef5c-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> SAML

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