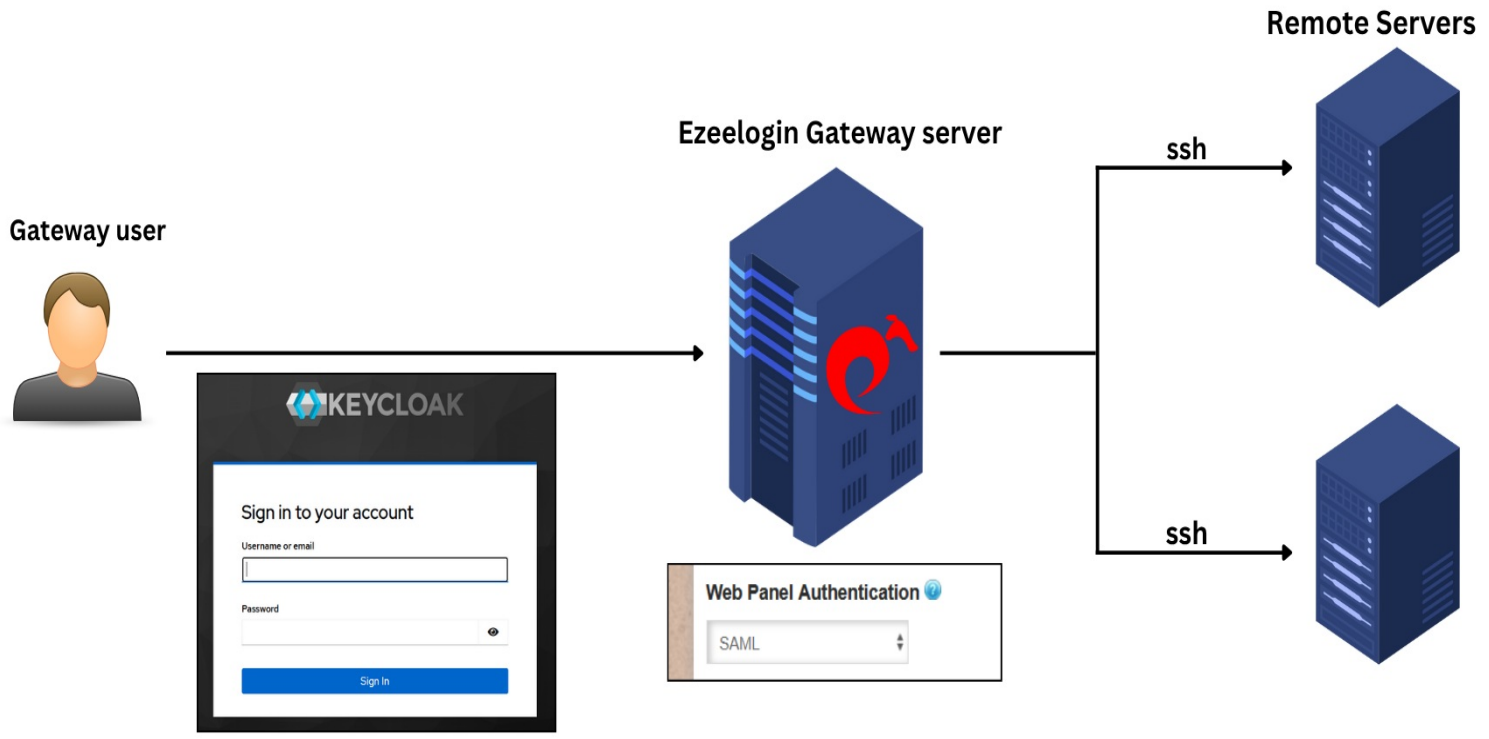
Integrating Keycloak SSO

779 Lekshmi April 28, 2026 Features & Functionalities 2991

How to integrate Keycloak with Ezeelogin

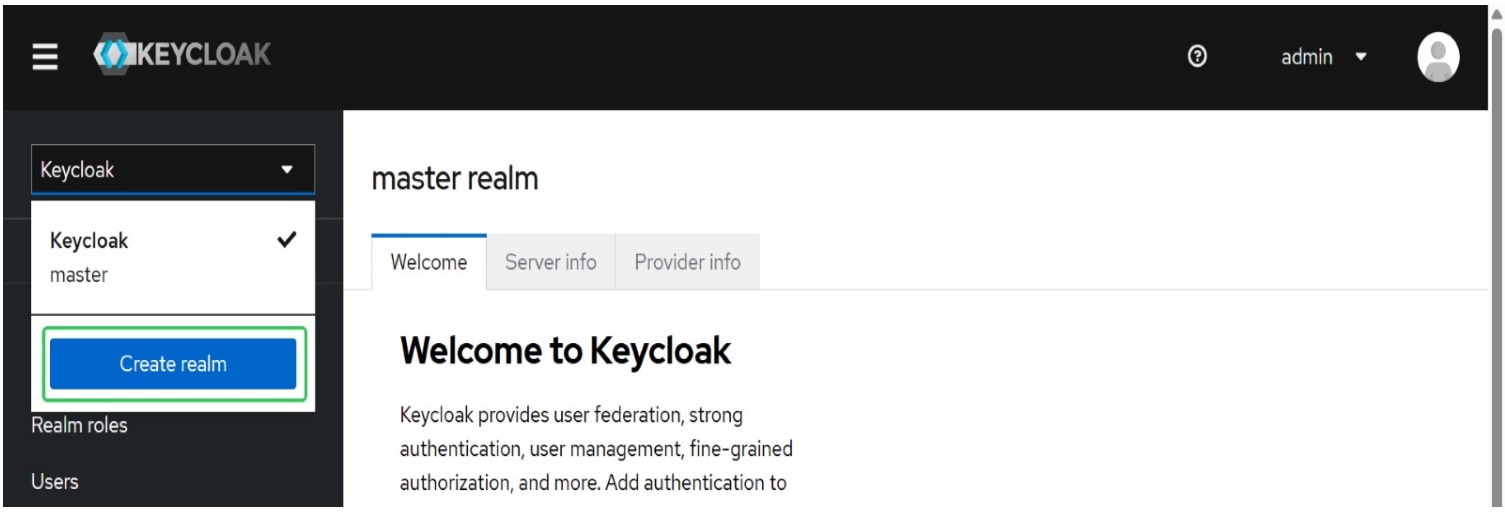
Overview: This article will help to integrate keycloak sso with the Ezeelogin jump server.

SAML is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



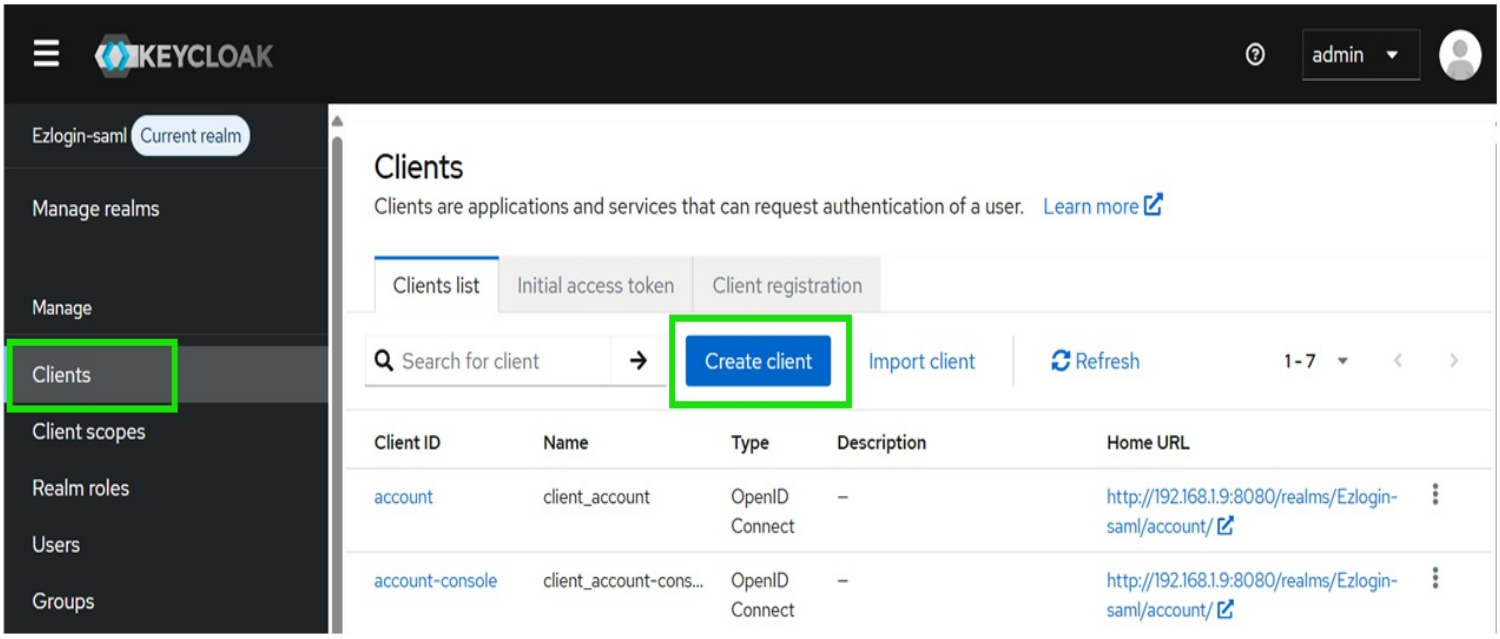
Step 1: Install the latest Keycloak server.

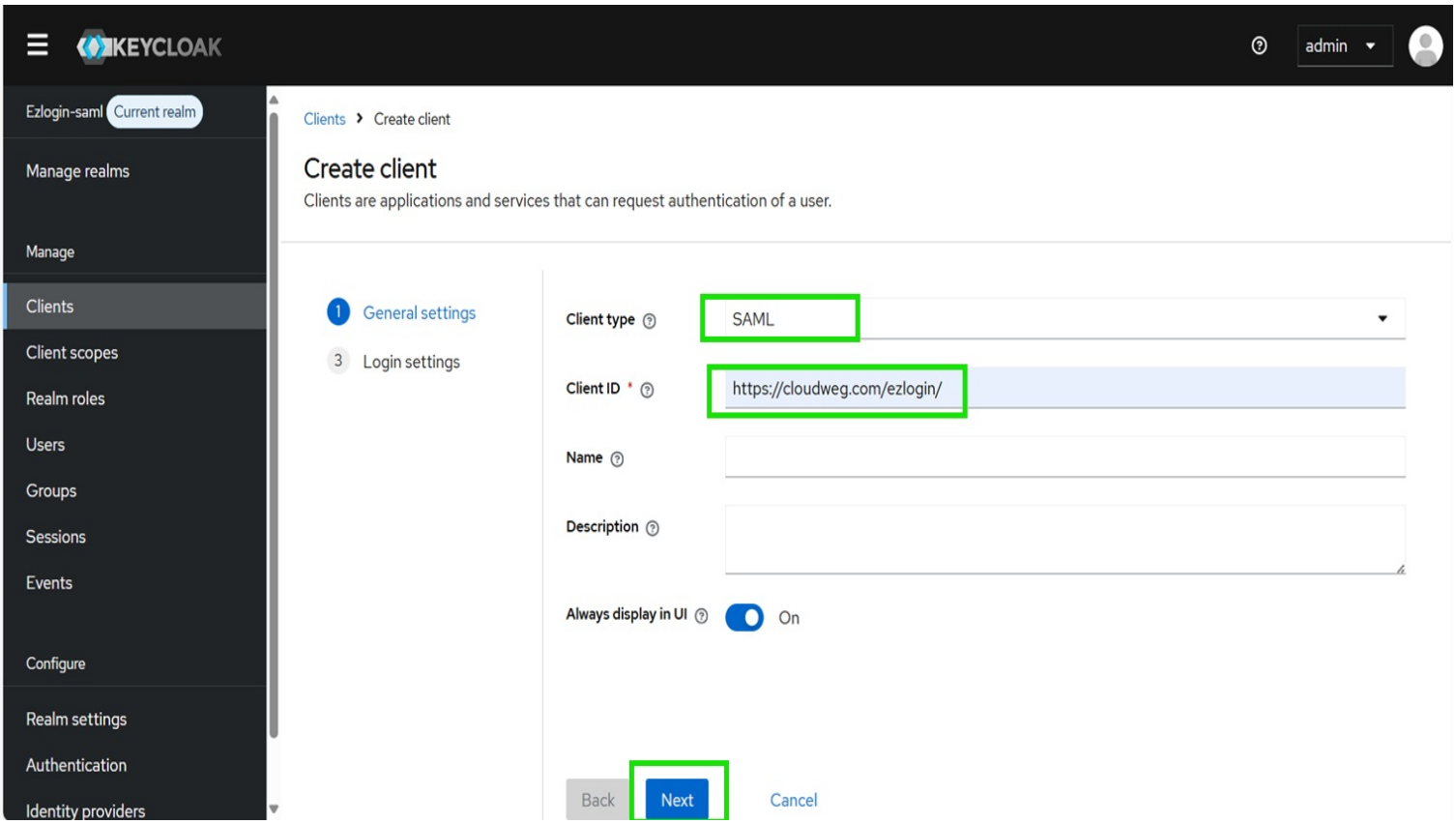
Step 2: Click on **Create realm.**



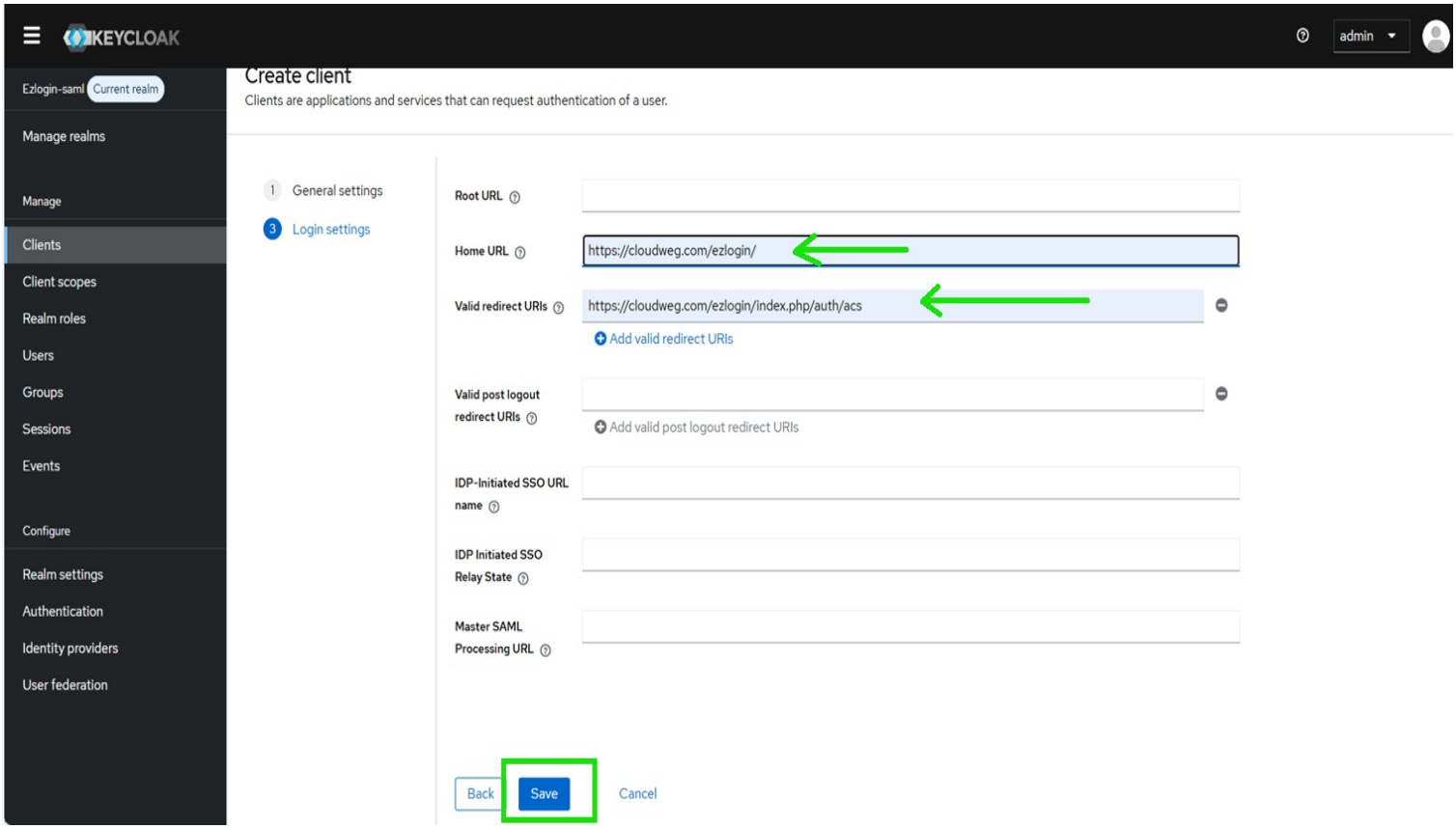
Step 2(A): Enter the **Realm name** and click on **Create.**

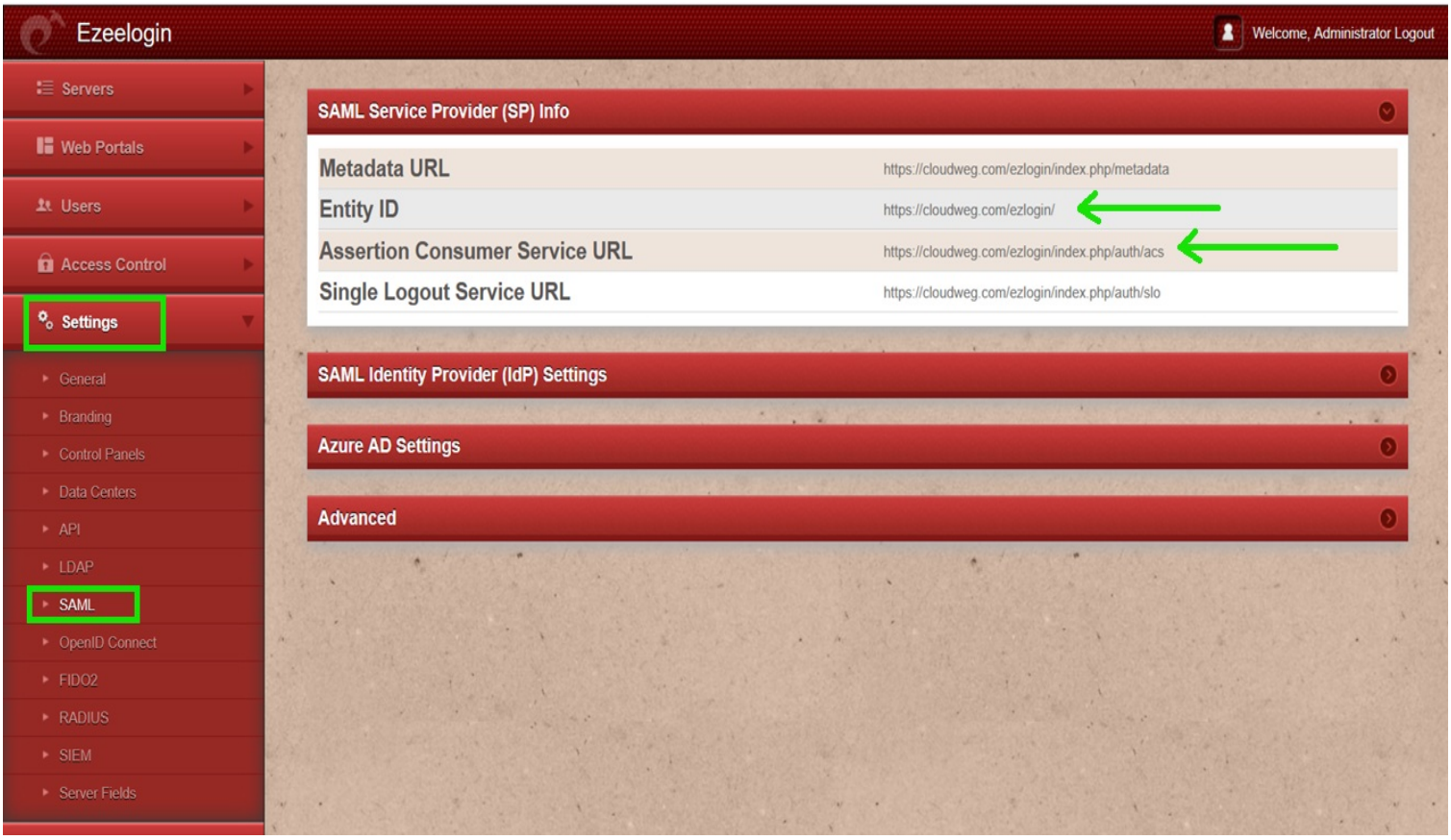
Step 2(B): Create client. Go to clients and click on **create client** -> Enter **client type**(saml) and **client id**(Entity ID from Ezeelogin GUI under settings -> SAML) -> **Next**



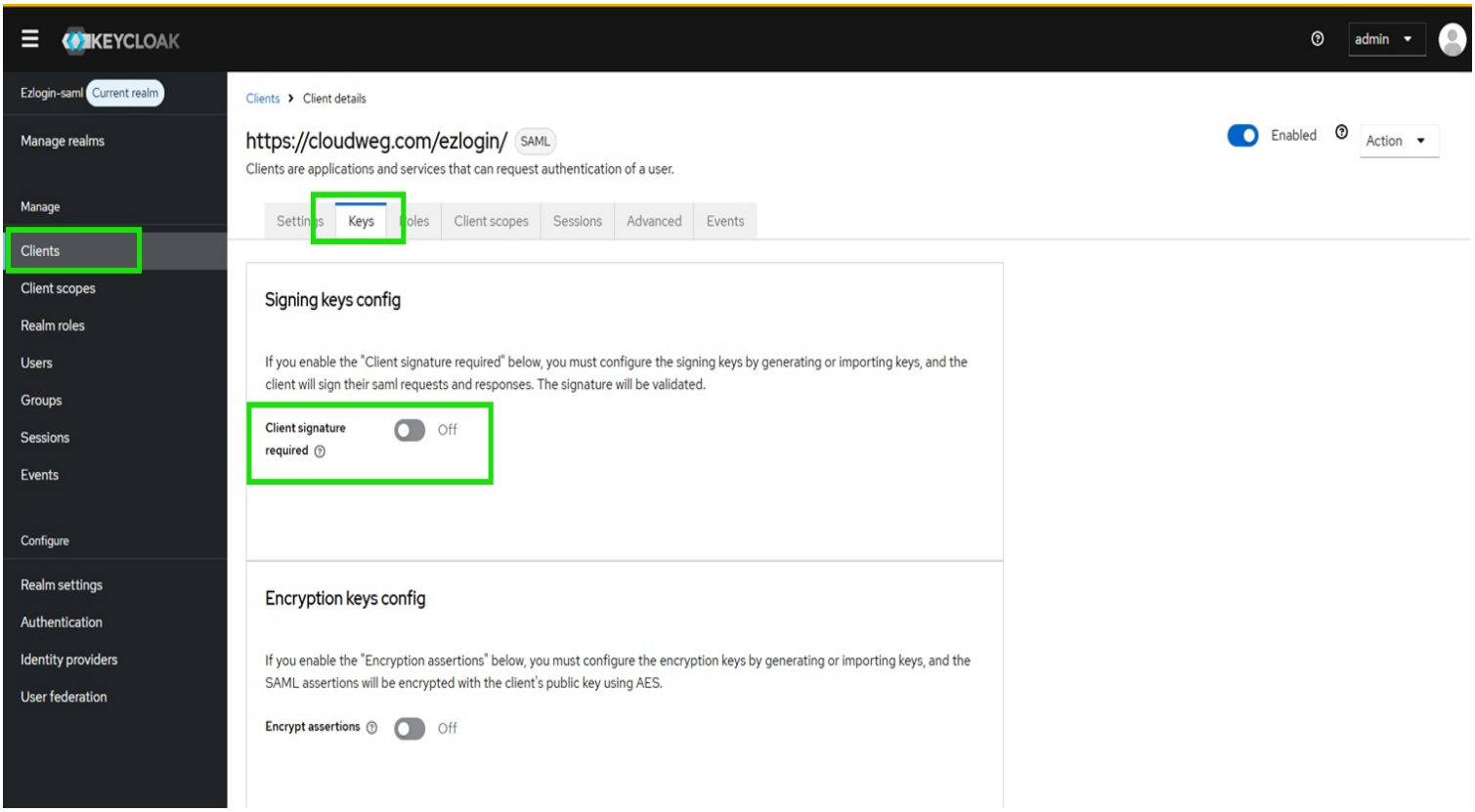


Step 3: Enter **Home URL**(Copy paste the Entity ID from Ezeelogin GUI), **Valid redirect URIs**(copy paste **Assertion Consumer Service URL** from Ezeelogin SAML settings) -> **Save it.**

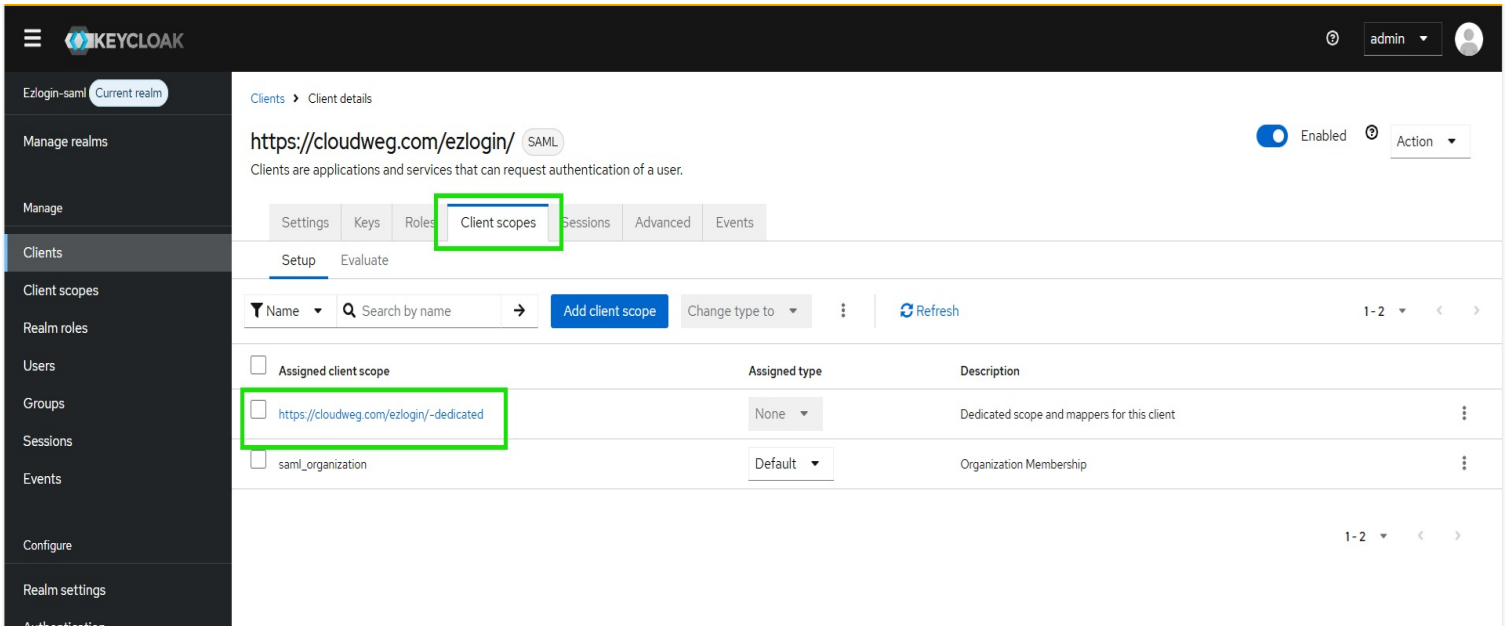




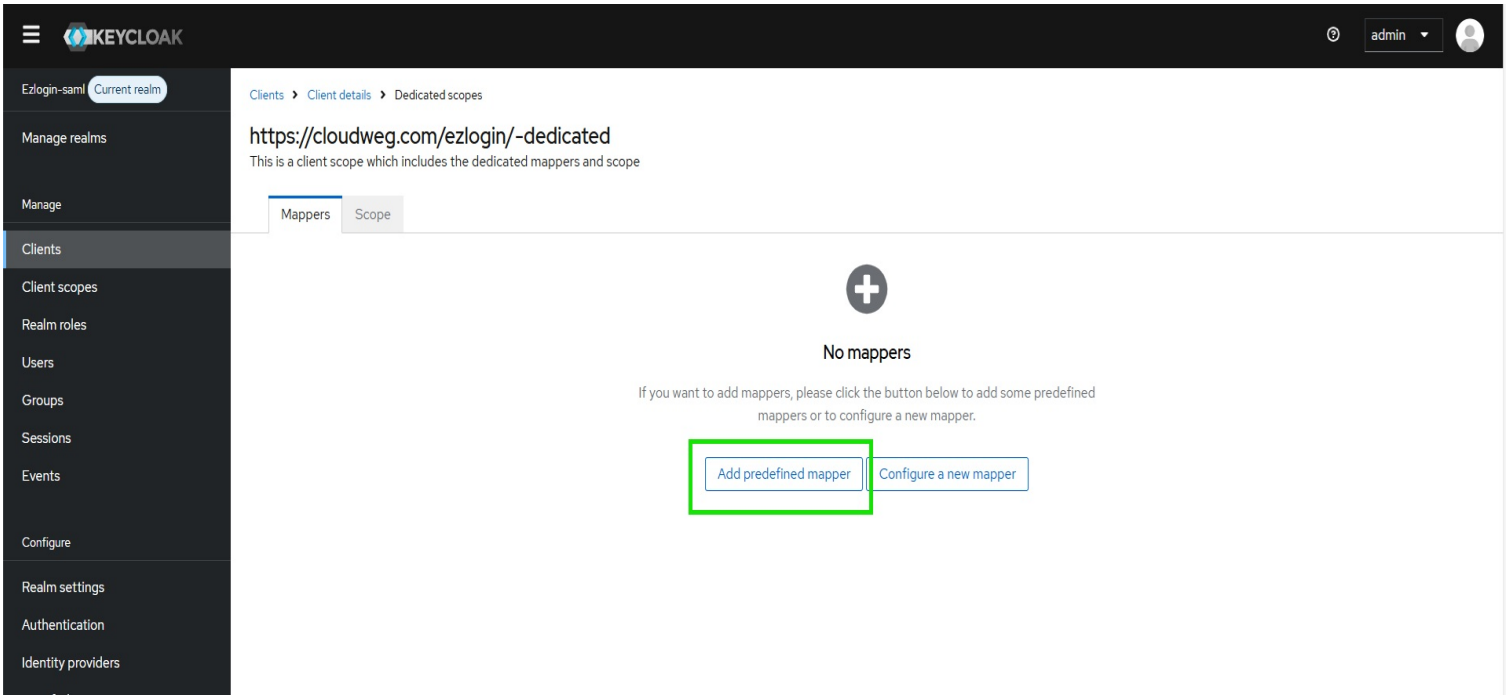
Step 3 (A): Disable Client Signature required from Keys .

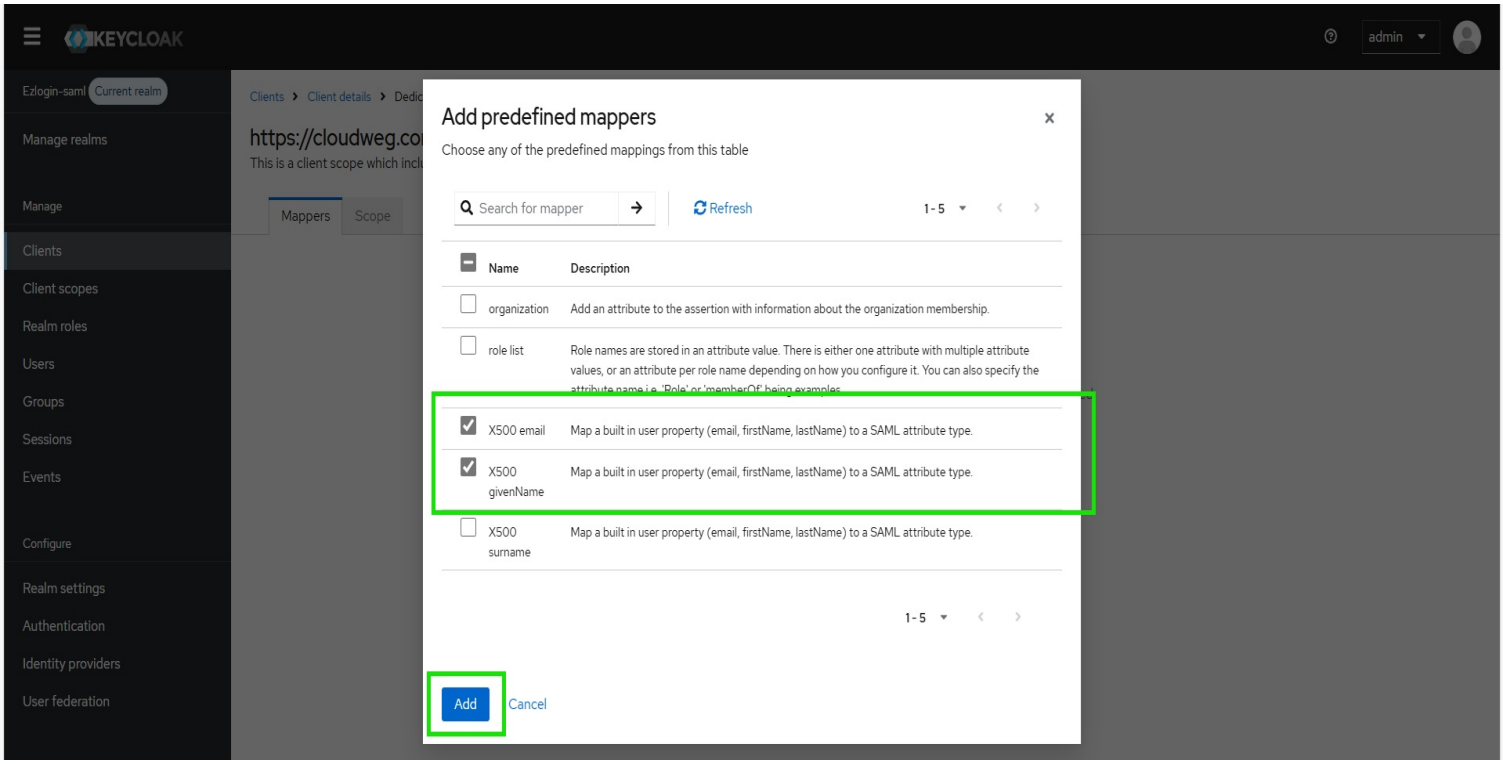


Step 3(B): Add mappers. Go to client scope and select the assigned client scope

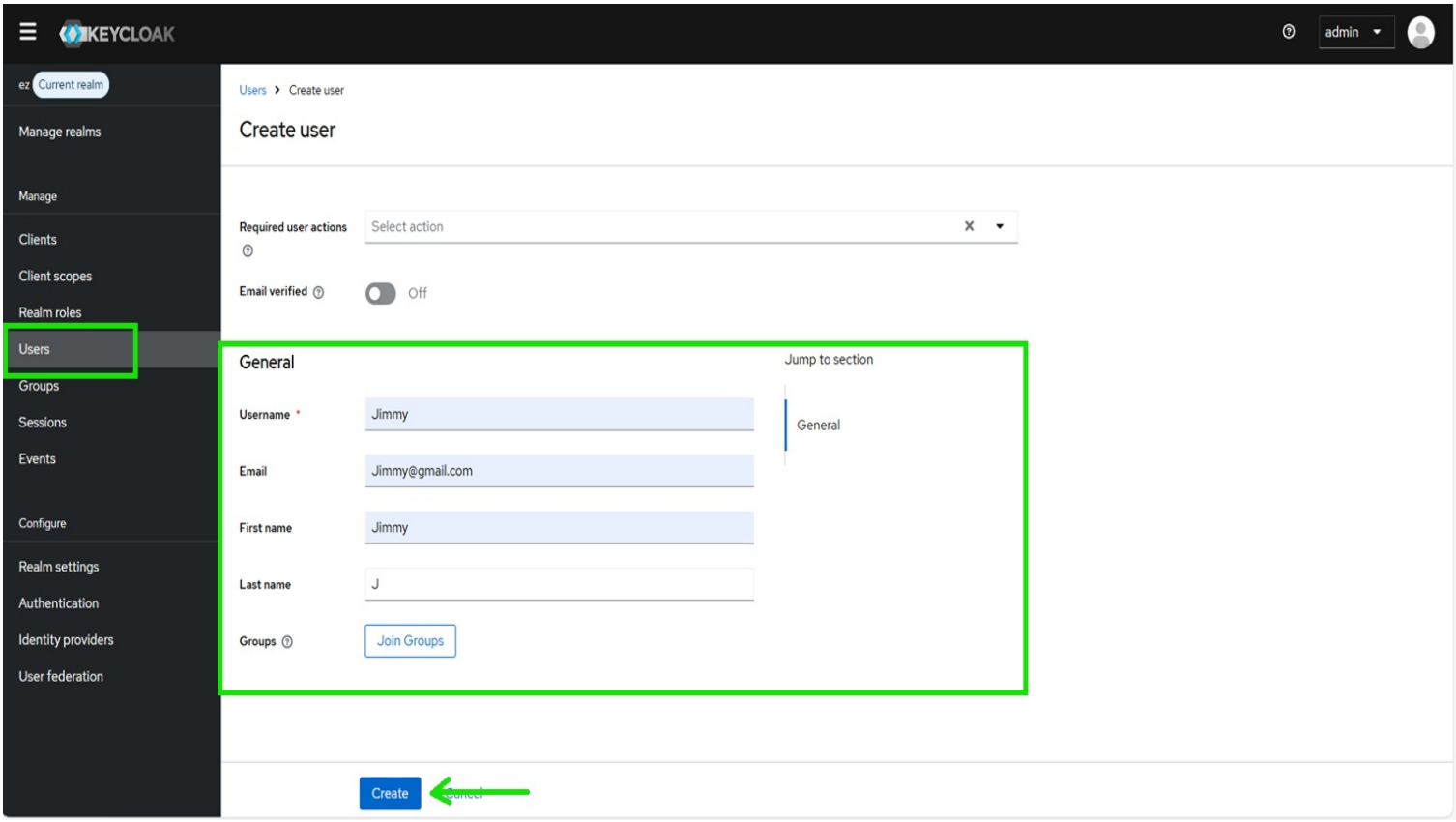


Add predefined Mapper



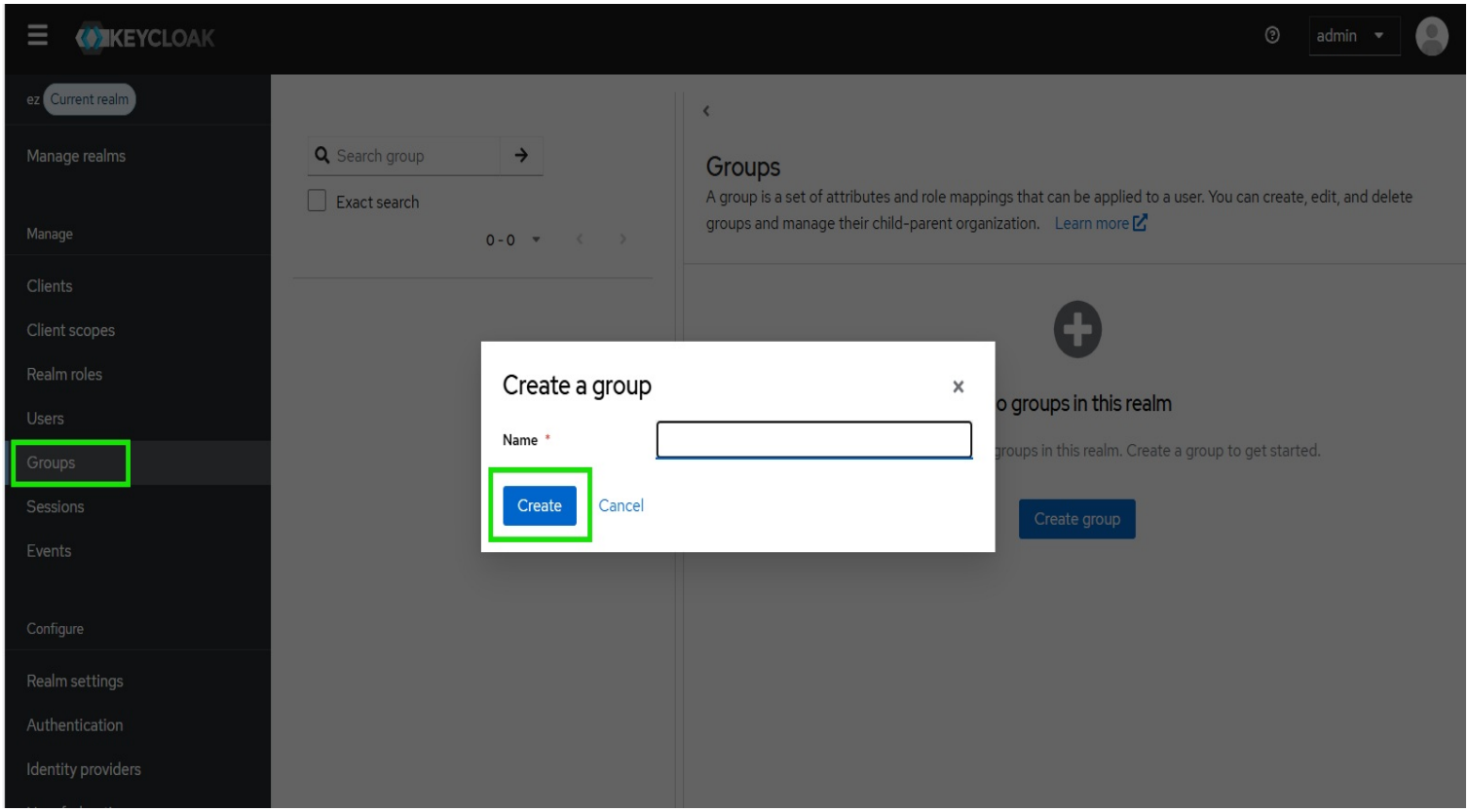


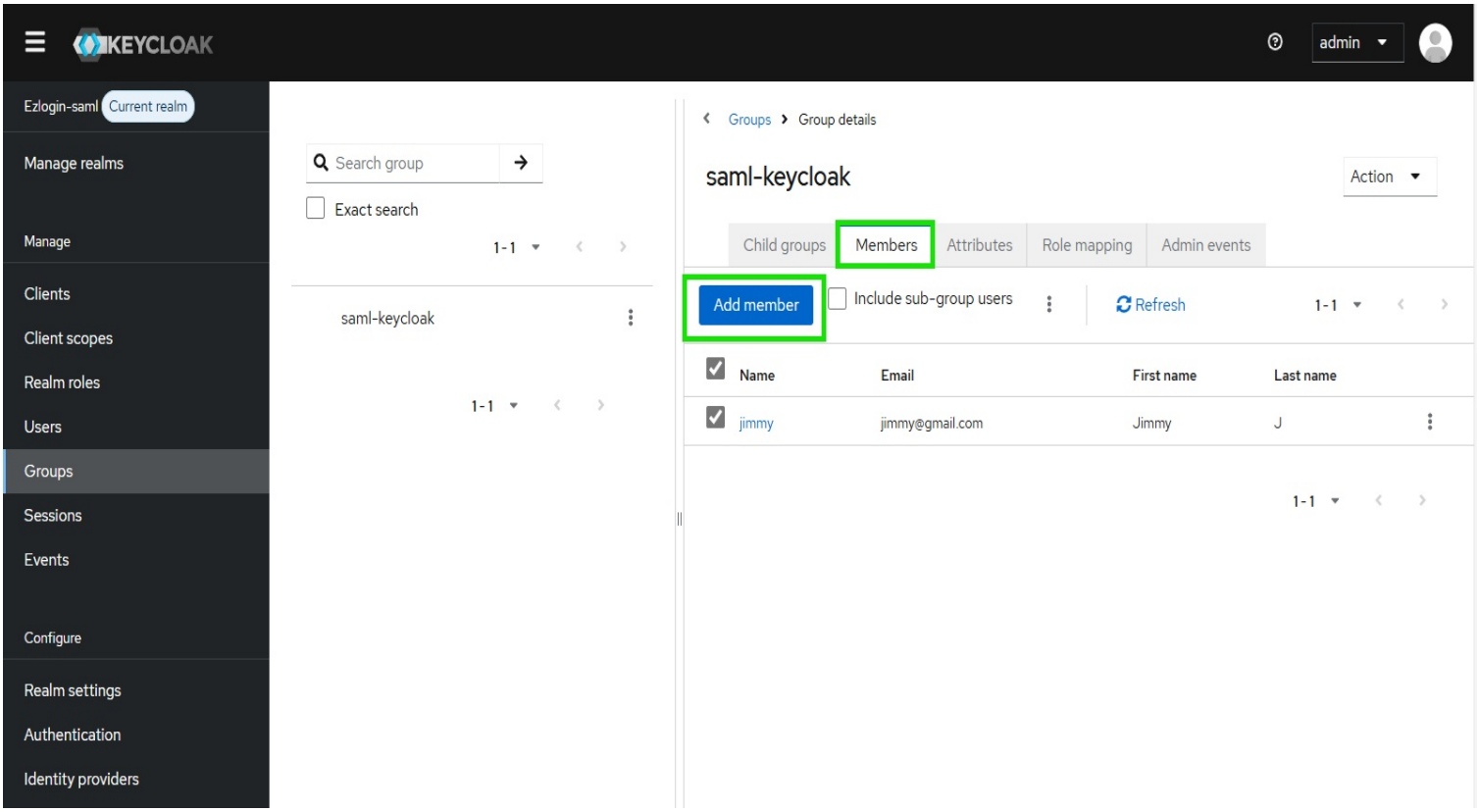
Step 4: Go to the **Users** tab, click **Add User**, and enter the **Username**, **Email**, **First Name**, and **Last Name**, then click **Create**.



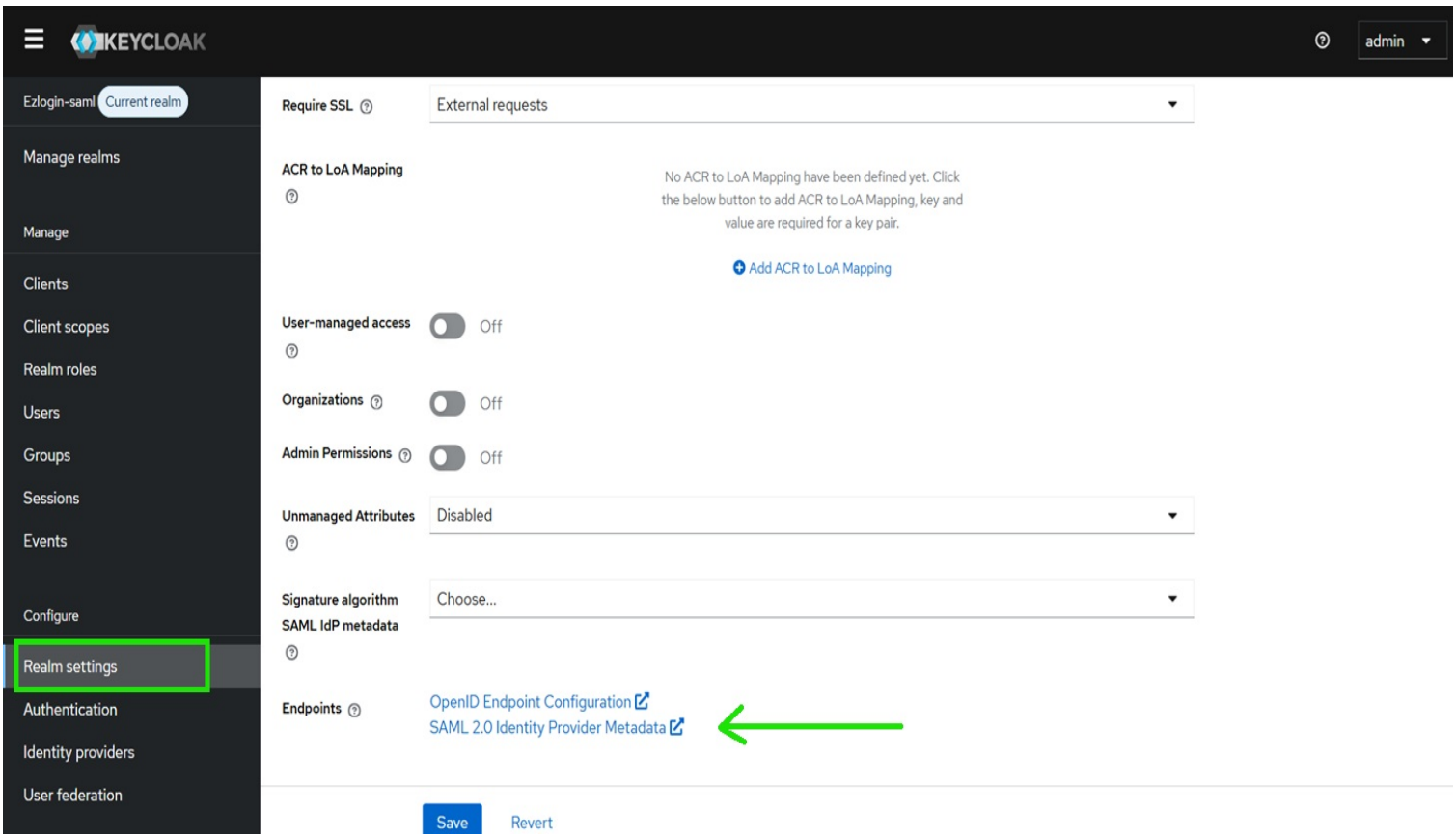
Next, open the **Credentials** tab, set a **password** and disable the **temporary** option.

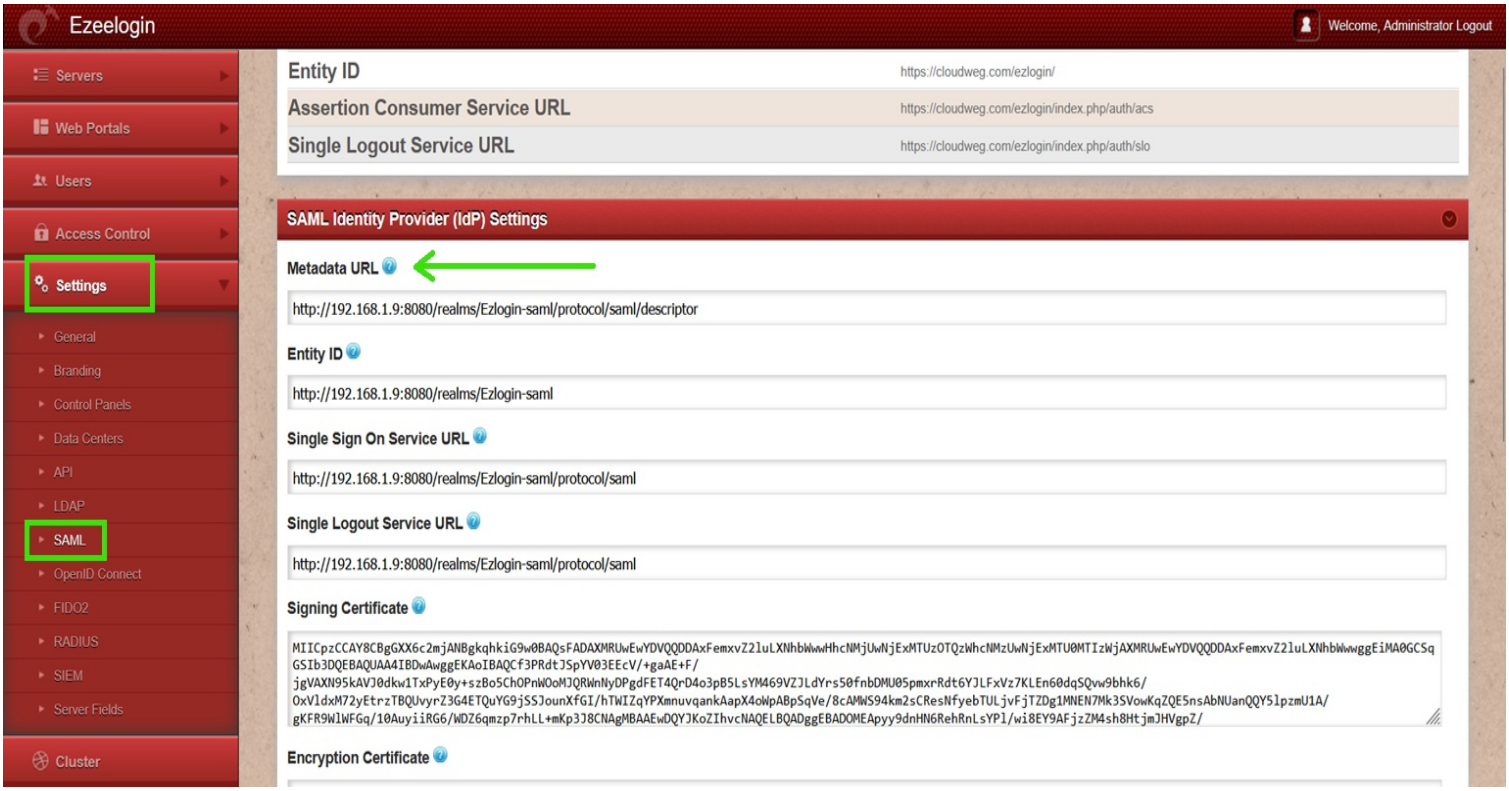
Step 5: Create a group, then add a user as a member of that group.

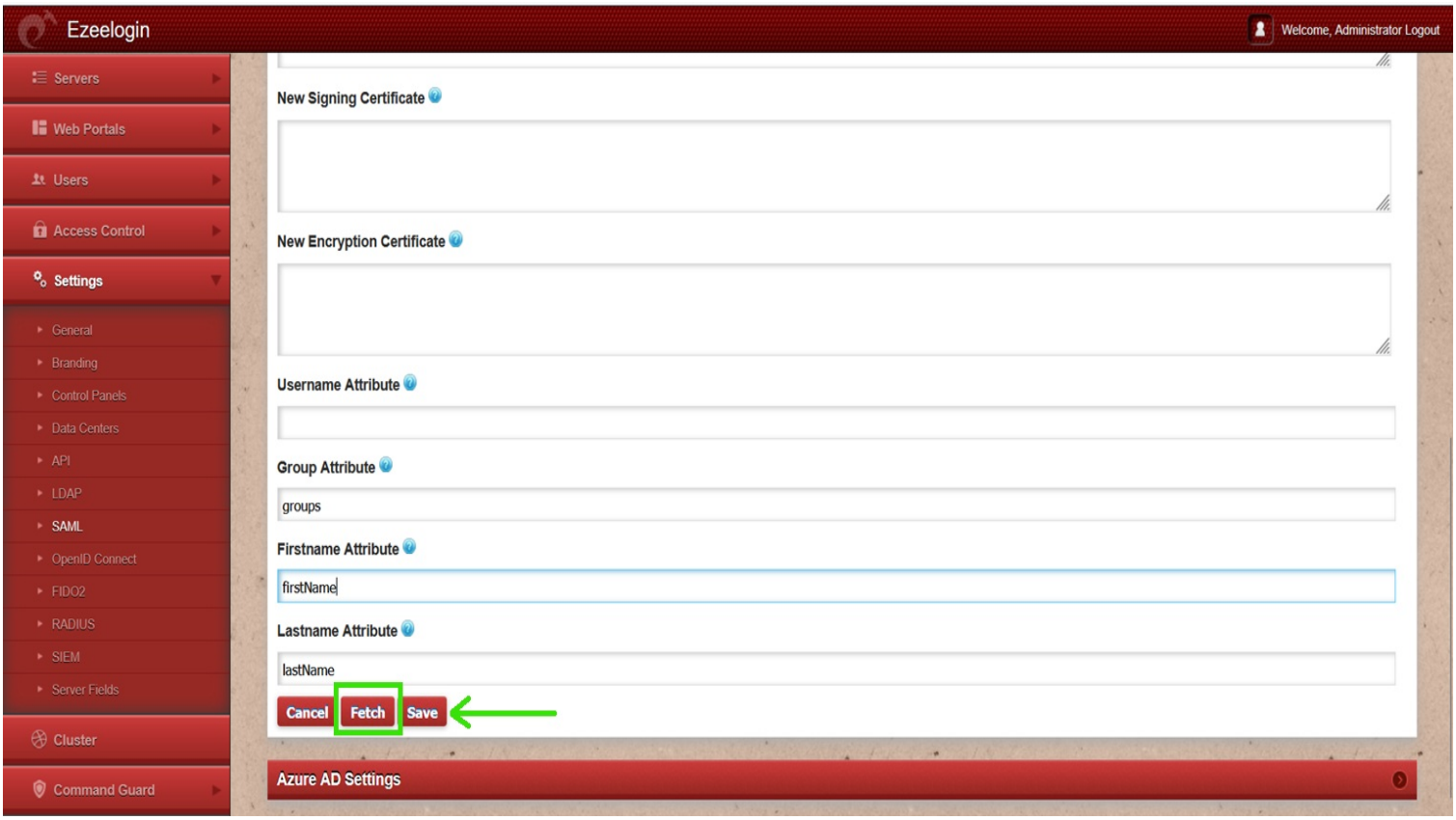




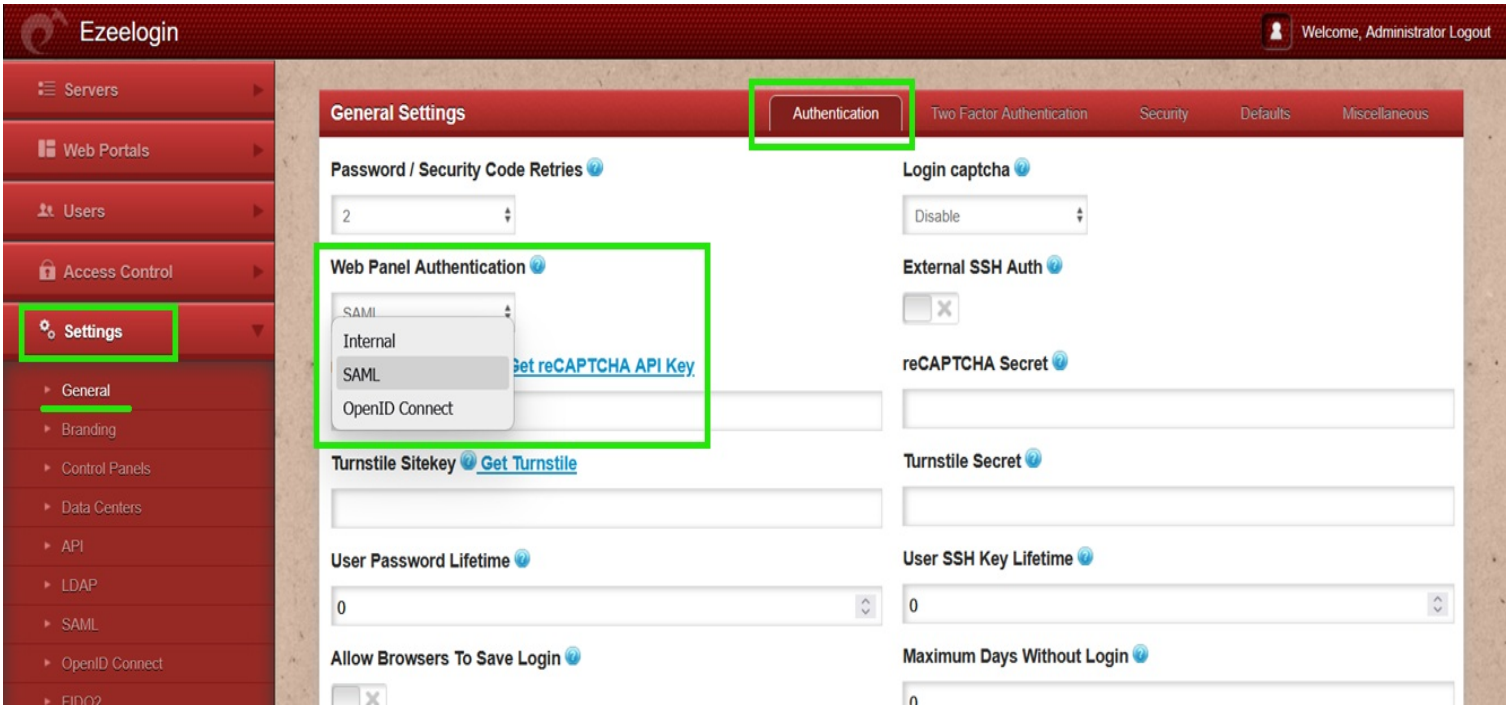
Step 6: Navigate to **Realm Settings -> Endpoints**, copy the SAML 2.0 Identity Provider Metadata link, paste it into the Metadata URL field in the Ezeelogin GUI, then click Fetch and Save.



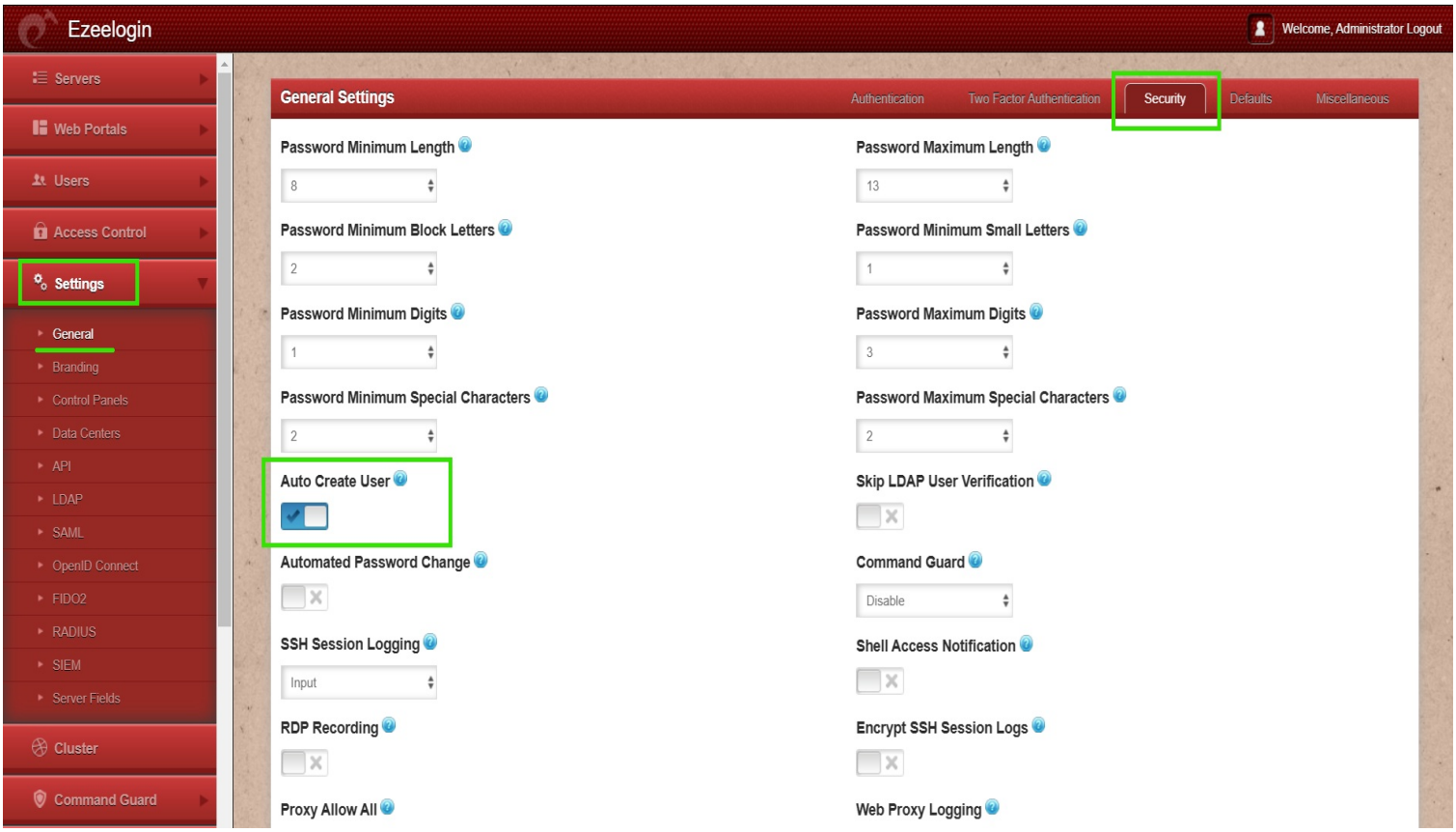




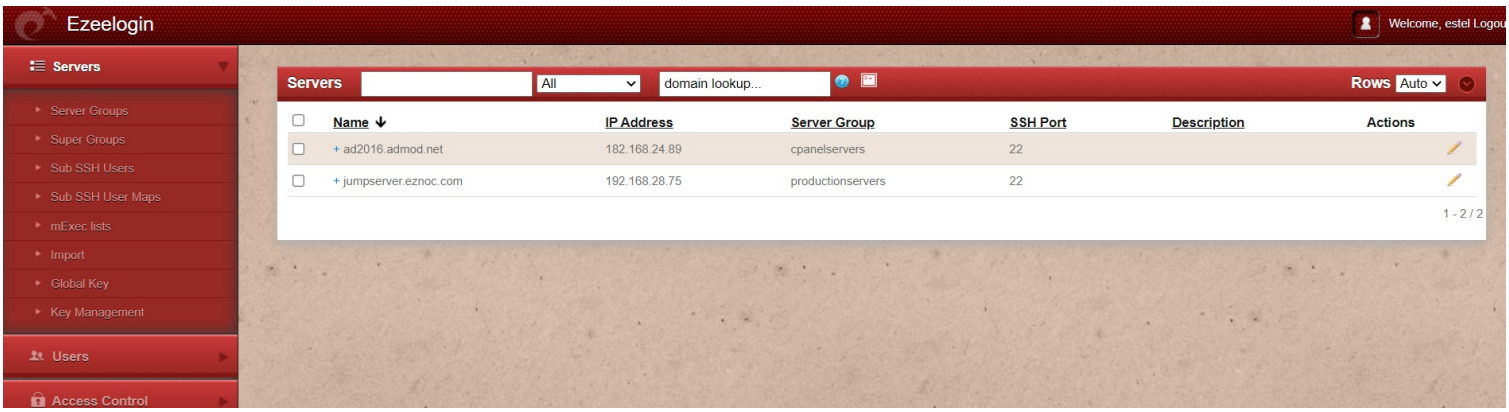
Step 7: Now change Web Panel Authentication Ezeelogin to SAML.



Step 7 (A): Enable Auto Create User in the Ezeelogin GUI by going to **Settings -> General -> Security.**



Step 7(B): Re-login to the Ezeelogin GUI with SAML authentication



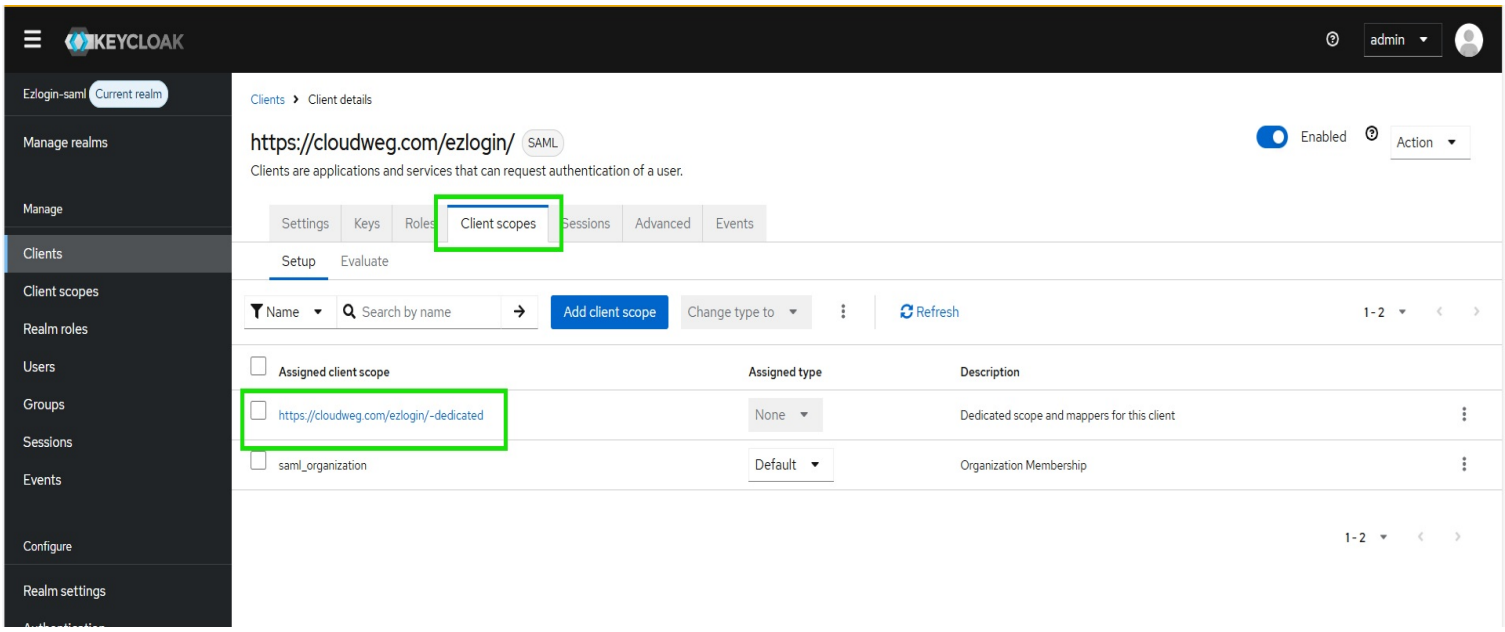
For gateway users who require administrative access, the password must be set manually from the Ezeelogin GUI. Refer below article:

Error: Invalid password

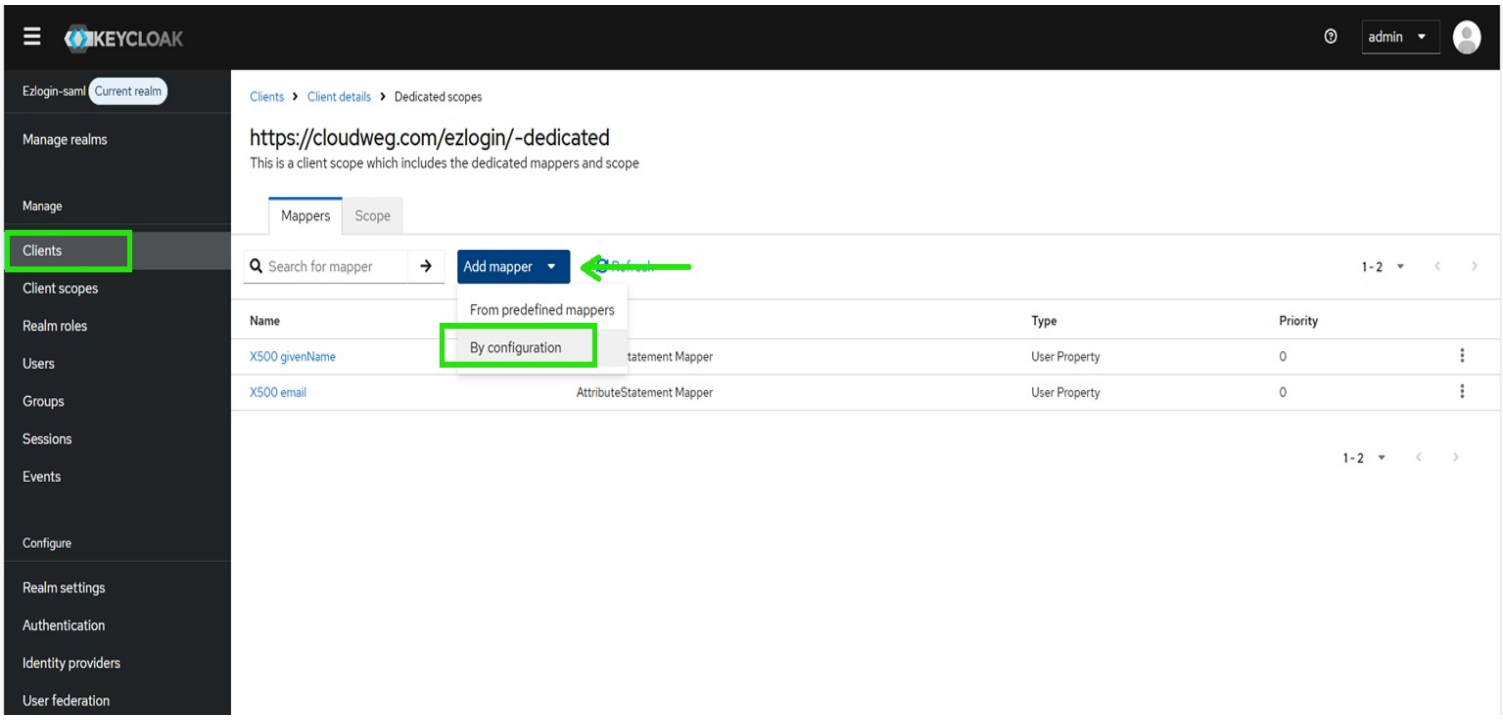
How to map keycloak users to the same user group in Ezeelogin?

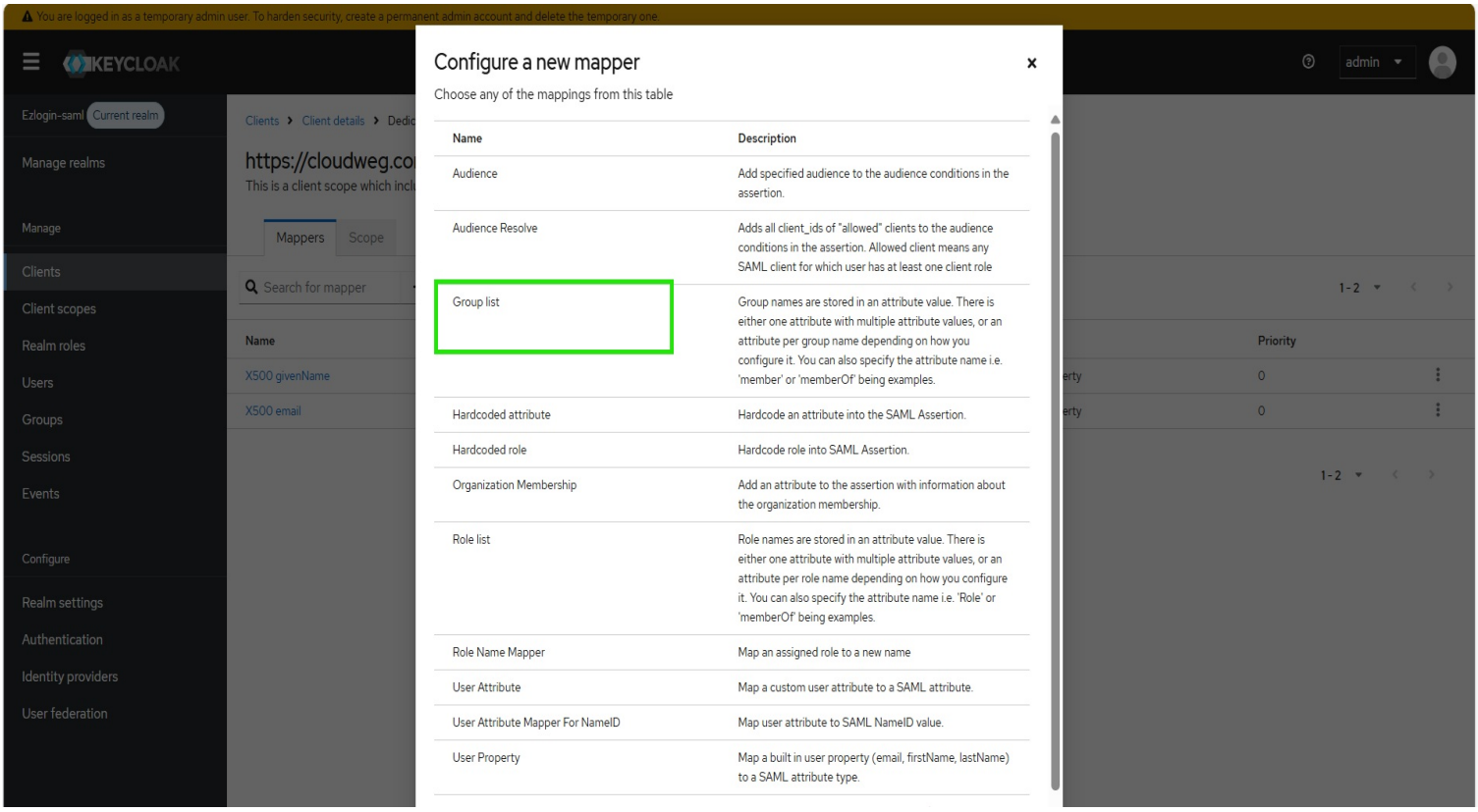
Step 1: From the Clients, select the required client, then open the Client Scopes section.

Choose the assigned client scope and click Add Mapper.

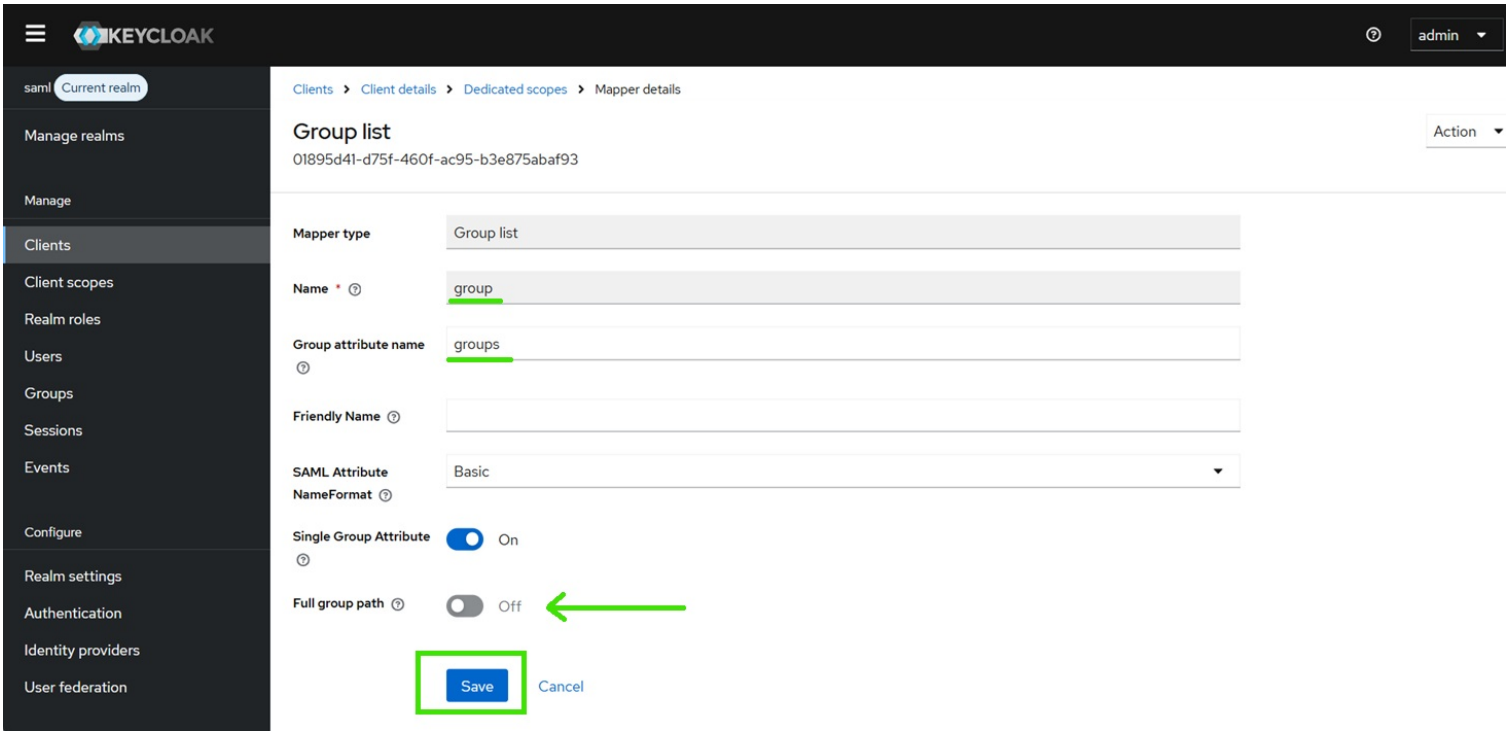


Step 1 (A): Here, add mapper by configuration.

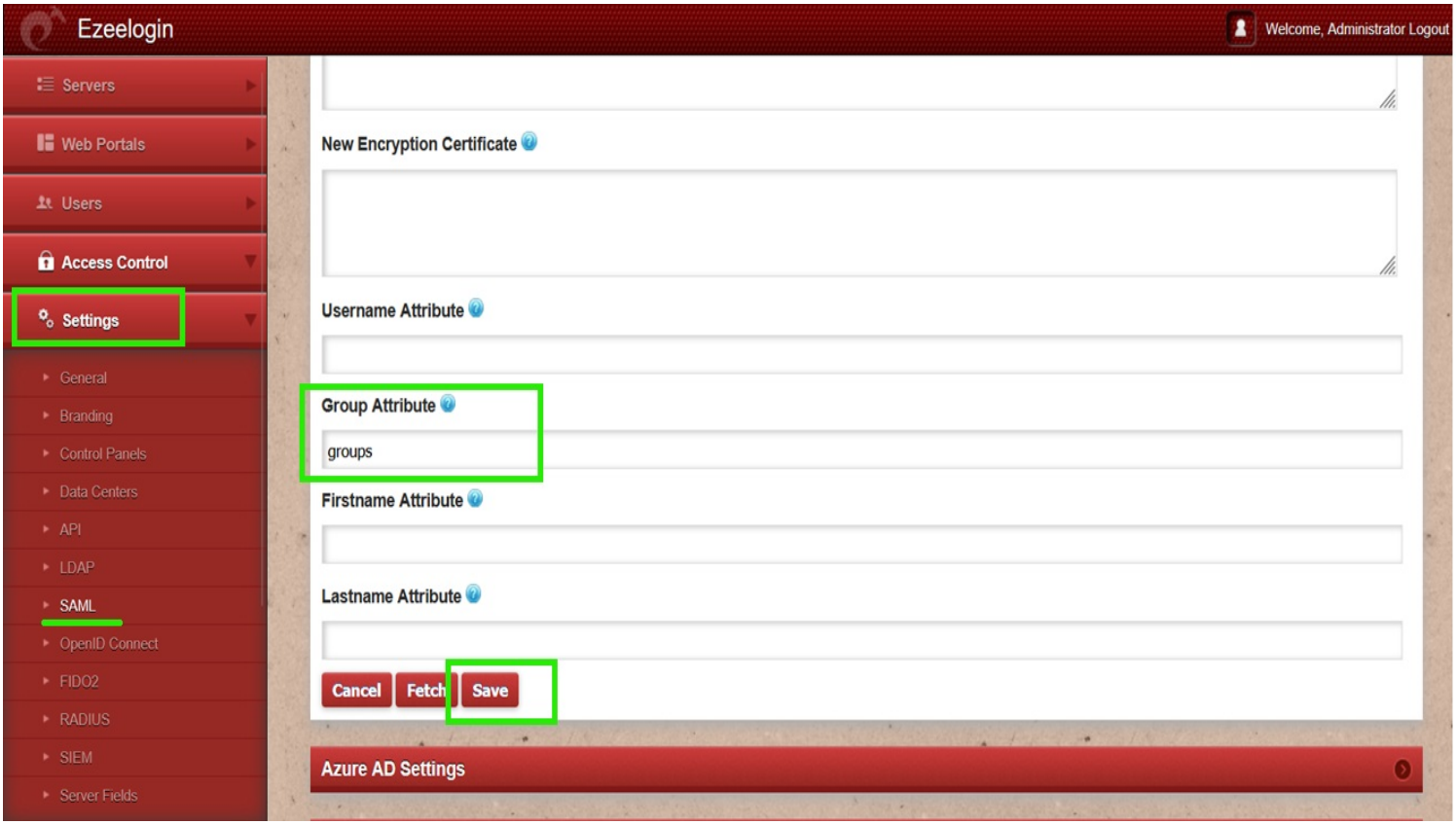




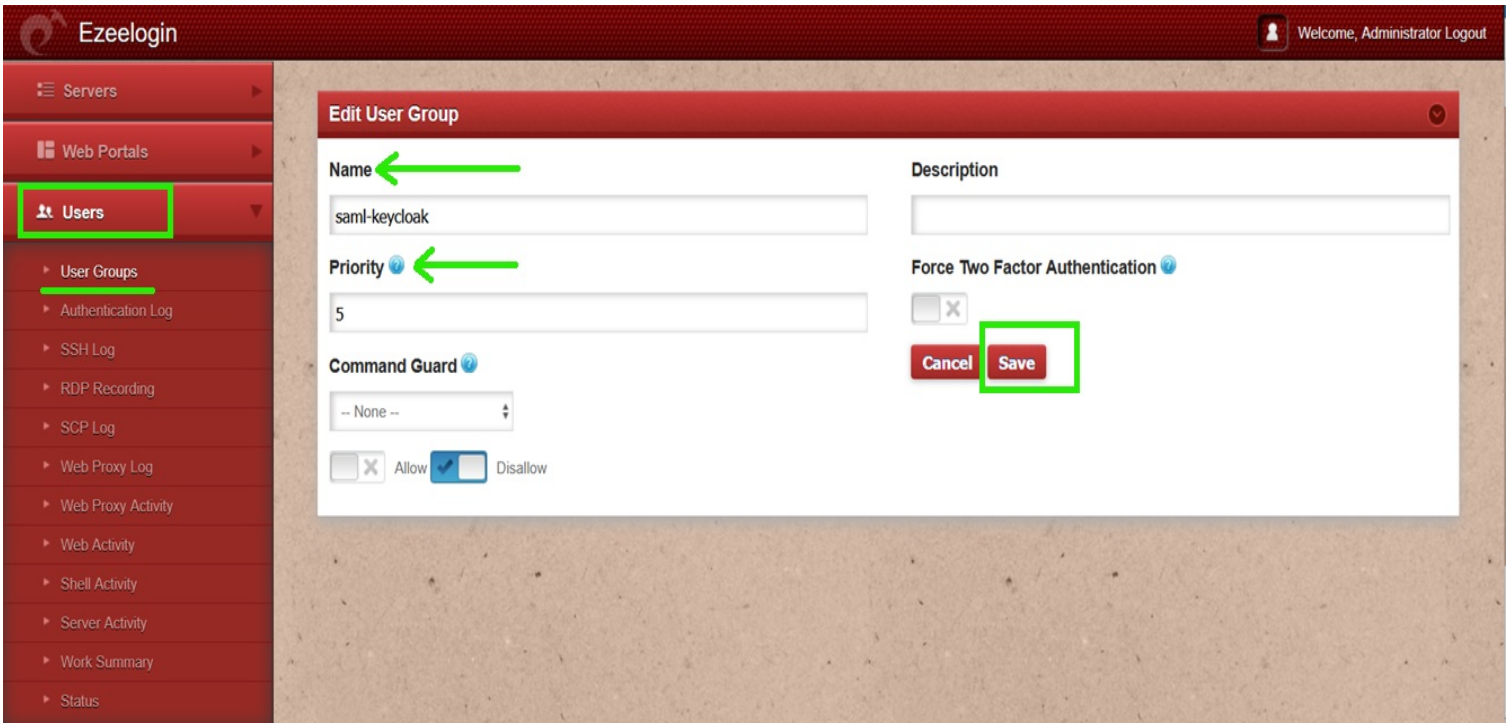
Enter the **name and group attribute name**, **disable the full group path** option, and then save.



Step 2: Go to **Settings -> SAML** in the Ezeelogin GUI and enter the group attribute name in the **Group Attribute**(here groups) field and then click save



Step 3: Create the same group(already created in keycloak under Groups) in Ezeelogin Gui with priority and save it.



Step 4: In the Ezeelogin GUI, go to **Settings -> General ->** then **change Web Panel Authentication to SAML** and access the Ezeelogin GUI and ensure the user is mapped to the corresponding group in Ezeelogin that matches their group in keycloak.

Related Articles:

Disable SAML /SSO Authentication on ezeelogin

Integrating SSO/SAML with Ezeelogin PAM

Integrate SAML Authentication in Ezeelogin GUI using Microsoft Azure SSO and Azure Active Directory

Map existing user group from SAML provider to ezeelogin.

Online URL: https://www.ezeelogin.com/kb/article/integrating-keycloak-sso-779.html