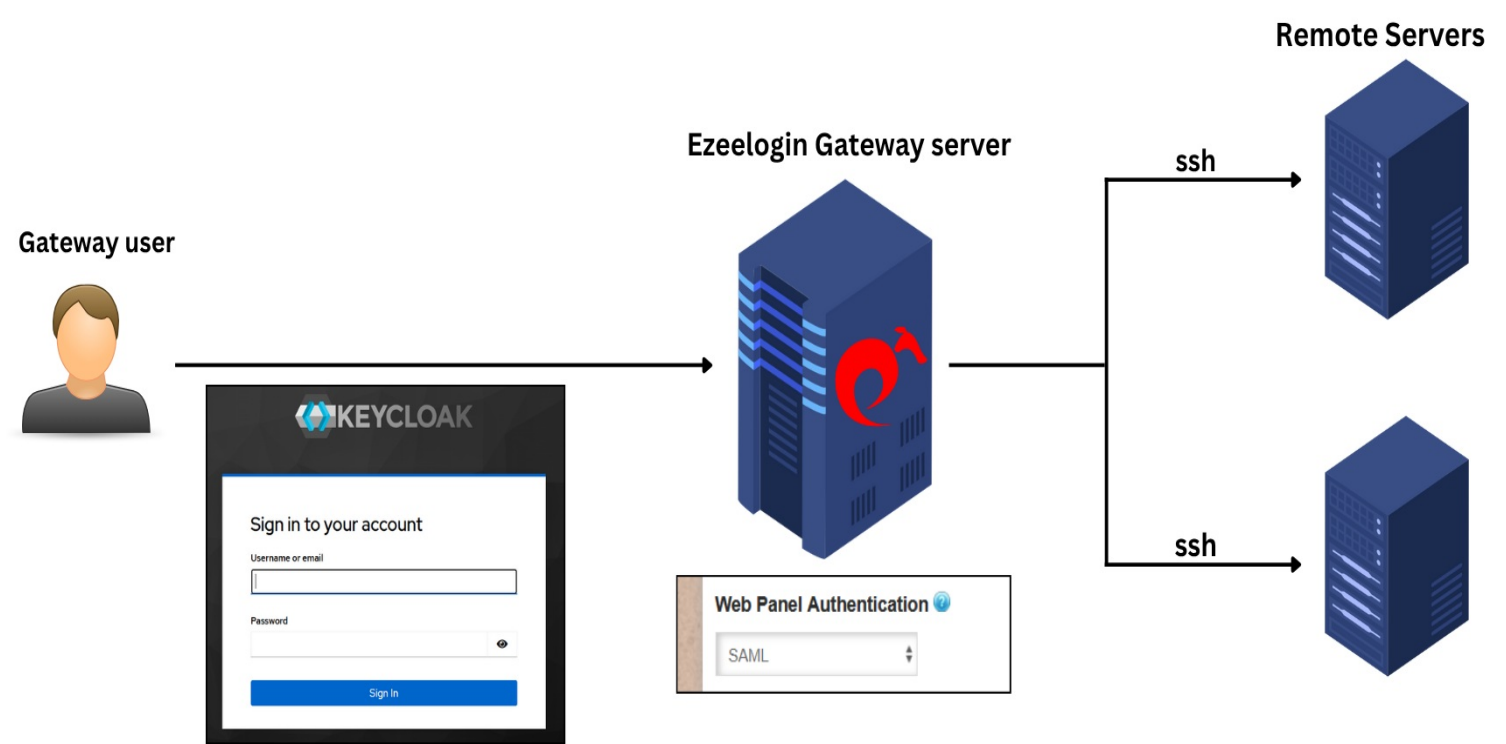


Integrating Keycloak SSO

How to integrate Keycloak with Ezeelogin

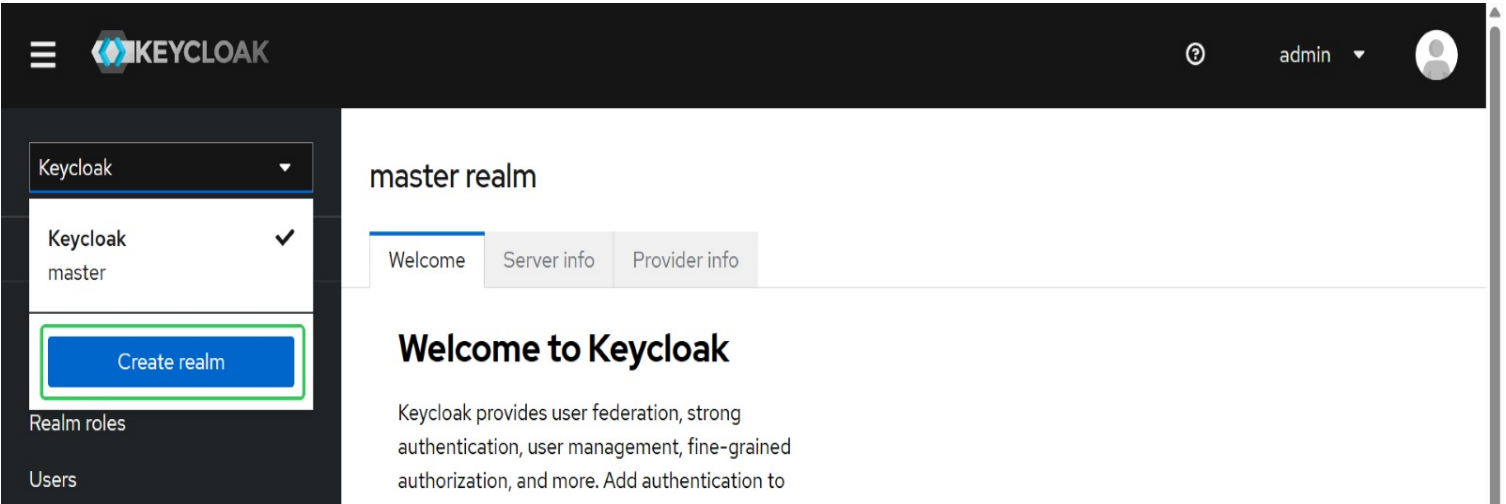
Overview: This article will help to integrate keycloak sso with the Ezeelogin jump server.

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



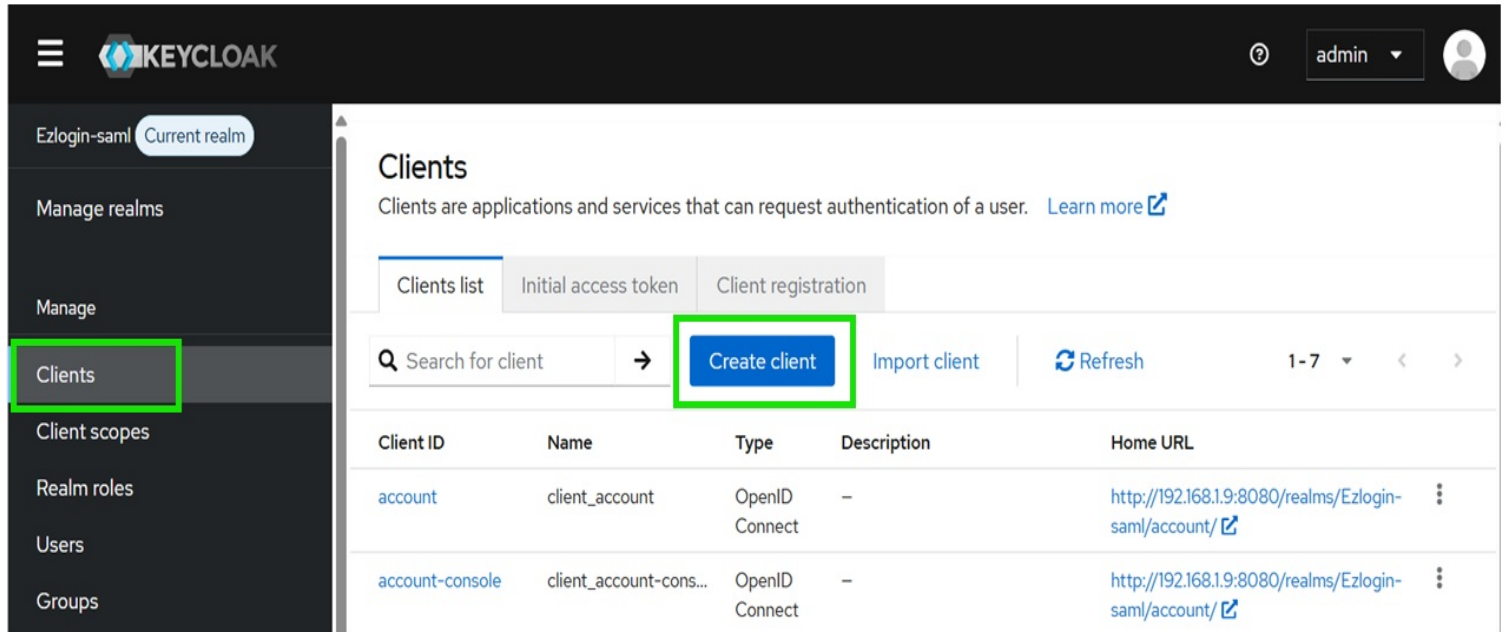
Step 1: Install the latest [Keycloak server](#).

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**



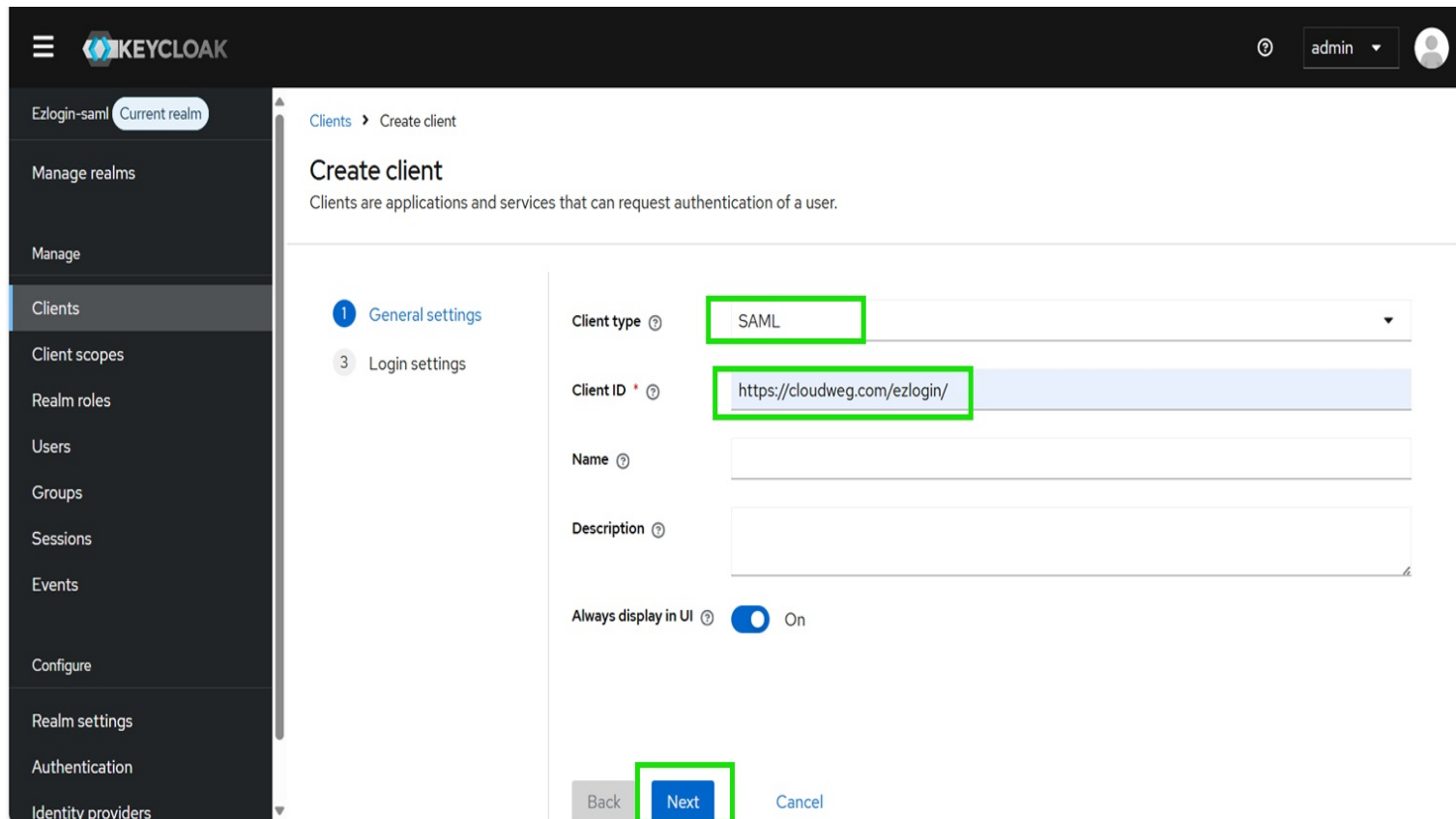
Clients

Clients are applications and services that can request authentication of a user. [Learn more](#)

Clients list Initial access token Client registration

Search for client → Create client Import client Refresh 1-7

Client ID	Name	Type	Description	Home URL
account	client_account	OpenID Connect	—	http://192.168.1.9:8080/realms/Ezlogin-saml/account/
account-console	client_account-cons...	OpenID Connect	—	http://192.168.1.9:8080/realms/Ezlogin-saml/account/



Create client

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

1 General settings 3 Login settings

Client type SAML

Client ID * https://cloudweg.com/ezlogin/

Name

Description

Always display in UI On

Back Next Cancel

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.**

 KEYCLOAK admin

Ezlogin-saml Current realm

Manage realms

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Create client

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

1 General settings

3 Login settings

Root URL 

Home URL  <https://cloudweg.com/ezlogin/>

Valid redirect URIs  <https://cloudweg.com/ezlogin/index.php/auth/acs> 

[+ Add valid redirect URIs](#)

Valid post logout redirect URIs  

[+ Add valid post logout redirect URIs](#)

IDP-Initiated SSO URL name 

IDP Initiated SSO Relay State 

Master SAML Processing URL 

[Back](#) [Save](#) [Cancel](#)

 Ezeelogin Welcome, Administrator Logout

Servers

Web Portals

Users

Access Control

Settings

General

Branding

Control Panels

Data Centers

API

LDAP

SAML

OpenID Connect

FIDO2

RADIUS

SIEM

Server Fields

SAML Service Provider (SP) Info

Metadata URL <https://cloudweg.com/ezlogin/index.php/metadata>

Entity ID <https://cloudweg.com/ezlogin/>

Assertion Consumer Service URL <https://cloudweg.com/ezlogin/index.php/auth/acs>

Single Logout Service URL <https://cloudweg.com/ezlogin/index.php/auth/slo>

SAML Identity Provider (IdP) Settings

Azure AD Settings

Advanced

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

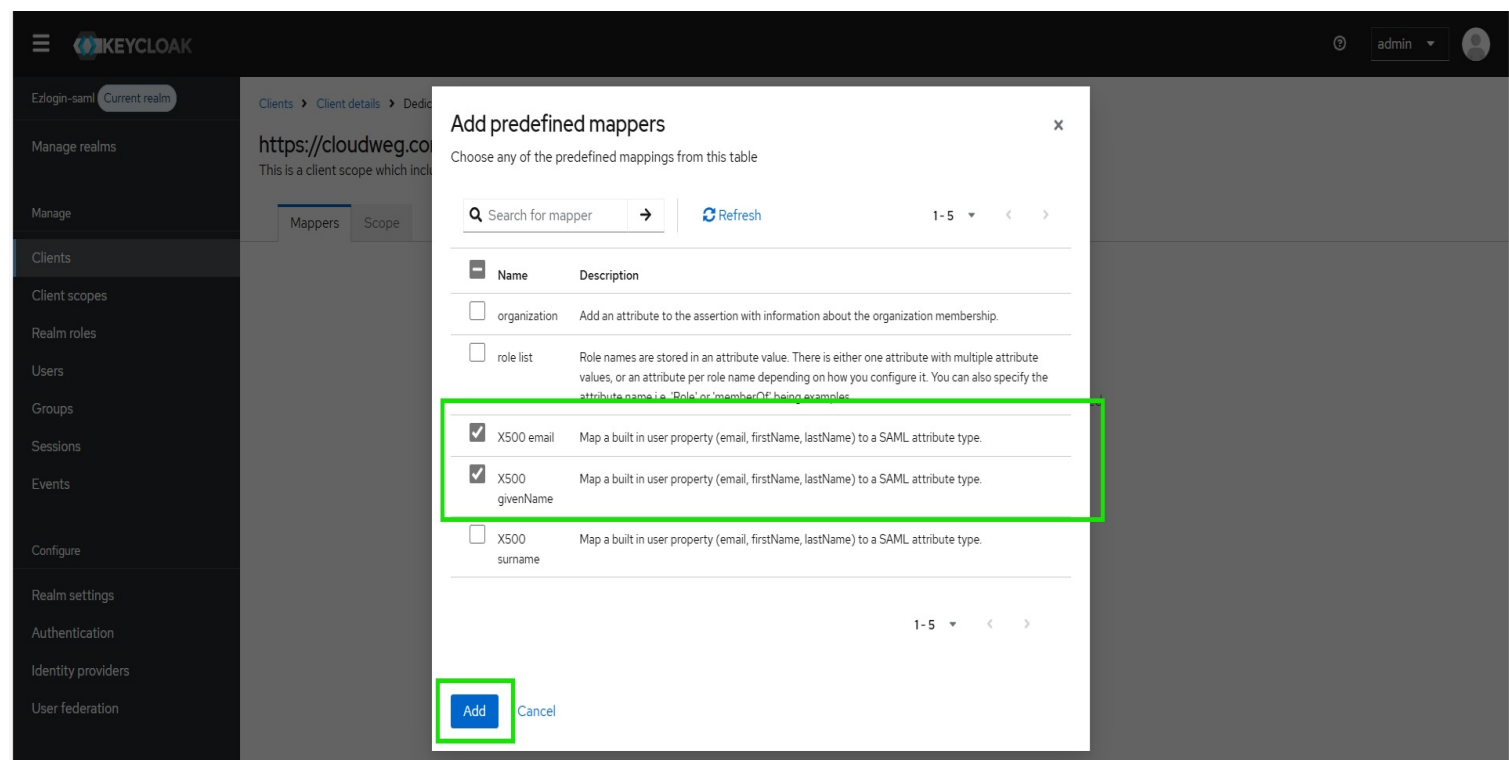
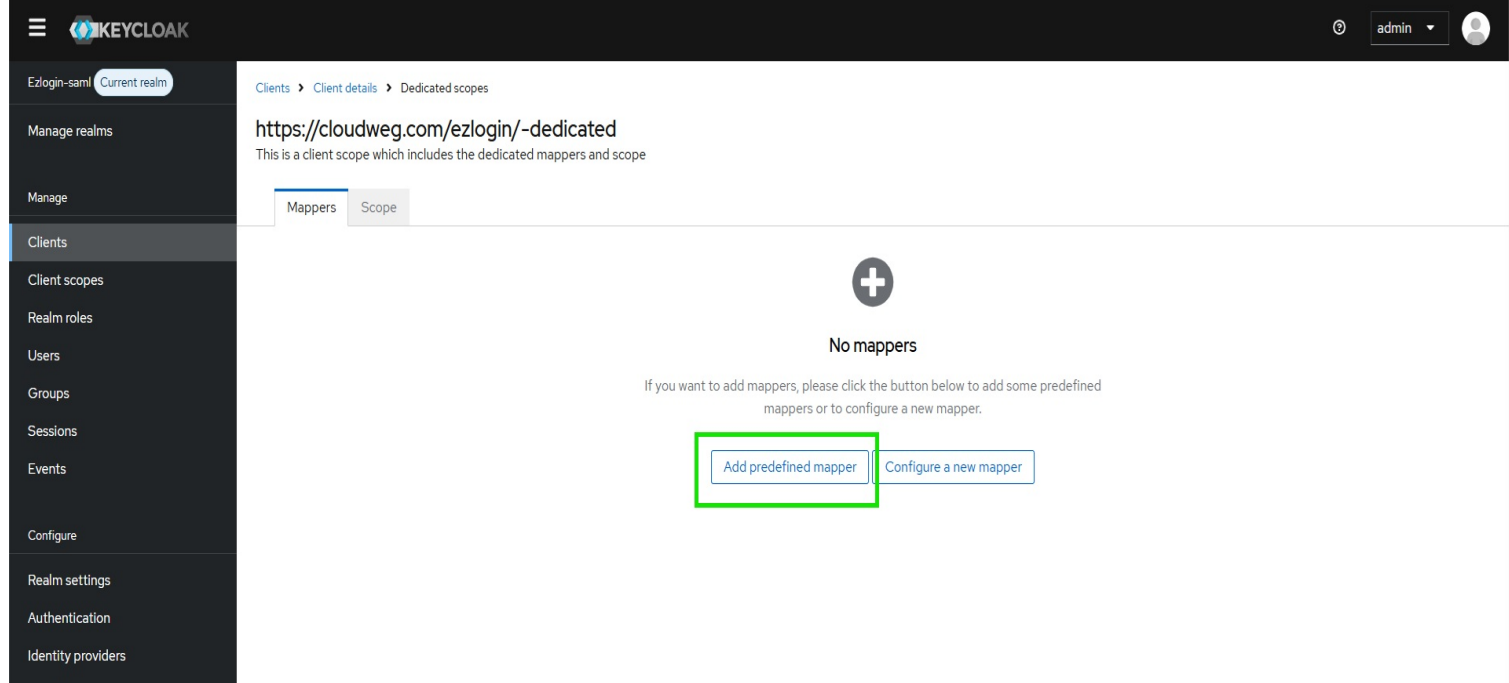
The screenshot shows the Keycloak interface with the 'Clients' menu item highlighted in the left sidebar. The main content area is the 'Client details' page for the client 'https://cloudweg.com/ezlogin/'. The 'Keys' tab is selected and highlighted with a green box. Below the tabs, there are two configuration sections: 'Signing keys config' and 'Encryption keys config'. In the 'Signing keys config' section, the 'Client signature required' toggle is set to 'Off' and is highlighted with a green box. The 'Encryption keys config' section has the 'Encrypt assertions' toggle set to 'Off'.

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

The screenshot shows the 'Client scopes' tab selected and highlighted with a green box. Below the tabs, there is a table of client scopes. The table has columns for 'Assigned client scope', 'Assigned type', and 'Description'. The first row is 'https://cloudweg.com/ezlogin/-dedicated', which is highlighted with a green box. The second row is 'saml_organization'. The 'Assigned type' for the first row is 'None' and for the second row is 'Default'. The 'Description' for the first row is 'Dedicated scope and mappers for this client' and for the second row is 'Organization Membership'.

Assigned client scope	Assigned type	Description
☐ https://cloudweg.com/ezlogin/-dedicated	None	Dedicated scope and mappers for this client
☐ saml_organization	Default	Organization Membership

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**.

Keycloak interface showing the 'Create user' form. The 'Users' menu item is highlighted in the left sidebar. The 'General' tab is active, showing fields for Username (Jimmy), Email (Jimmy@gmail.com), First name (Jimmy), and Last name (J). A green box highlights the 'General' tab and the 'Create' button at the bottom. A green arrow points to the 'Create' button.

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.

Keycloak interface showing the 'Groups' page. The 'Groups' menu item is highlighted in the left sidebar. A 'Create a group' modal dialog is open, showing a 'Name' field and 'Create' and 'Cancel' buttons. The 'Create' button is highlighted with a green box.

The screenshot shows the Keycloak administration interface. On the left is a sidebar with navigation options: Ezlogin-saml, Manage realms, Manage, Clients, Client scopes, Realm roles, Users, Groups (highlighted), Sessions, Events, Configure, Realm settings, Authentication, and Identity providers. The main content area is titled 'Groups > Group details' for the group 'saml-keycloak'. It features tabs for 'Child groups', 'Members' (highlighted), 'Attributes', 'Role mapping', and 'Admin events'. Below the tabs, there is an 'Add member' button (highlighted) and a checkbox for 'Include sub-group users'. A table lists the group's members, with one member 'jimmy' (jimmy@gmail.com) shown. The table has columns for Name, Email, First name, and Last name.

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.

The screenshot shows the 'Realm settings' page in Keycloak. The sidebar on the left has 'Realm settings' highlighted. The main content area is titled 'Require SSL' and 'External requests'. It includes sections for 'ACR to LoA Mapping', 'User-managed access', 'Organizations', 'Admin Permissions', 'Unmanaged Attributes', 'Signature algorithm', and 'SAML IdP metadata'. The 'Endpoints' section at the bottom contains two links: 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata', with a green arrow pointing to the latter. At the bottom of the page are 'Save' and 'Revert' buttons.

Ezeelogin

Welcome, Administrator Logout

- Servers
- Web Portals
- Users
- Access Control
- Settings**
 - General
 - Branding
 - Control Panels
 - Data Centers
 - API
 - LDAP
 - SAML**
 - OpenID Connect
 - FIDO2
 - RADIUS
 - SIEM
 - Server Fields
- Cluster

Entity ID <https://cloudweg.com/ezlogin/>

Assertion Consumer Service URL <https://cloudweg.com/ezlogin/index.php/auth/acs>

Single Logout Service URL <https://cloudweg.com/ezlogin/index.php/auth/slo>

SAML Identity Provider (IdP) Settings

Metadata URL 

Entity ID 

Single Sign On Service URL 

Single Logout Service URL 

Signing Certificate 

Encryption Certificate 

Ezeelogin

Welcome, Administrator Logout

- Servers
- Web Portals
- Users
- Access Control
- Settings**
 - General
 - Branding
 - Control Panels
 - Data Centers
 - API
 - LDAP
 - SAML**
 - OpenID Connect
 - FIDO2
 - RADIUS
 - SIEM
 - Server Fields
- Cluster
- Command Guard

New Signing Certificate 

New Encryption Certificate 

Username Attribute 

Group Attribute 

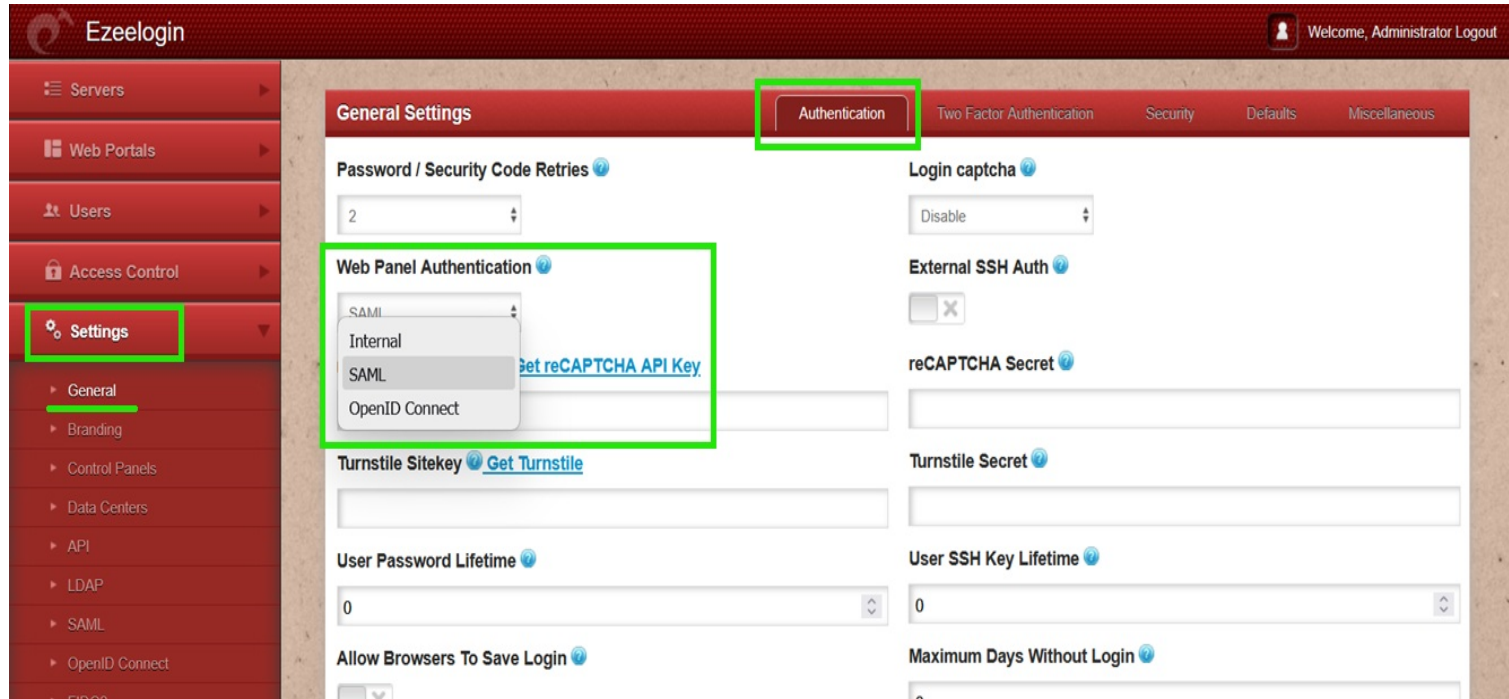
Firstname Attribute 

Lastname Attribute 

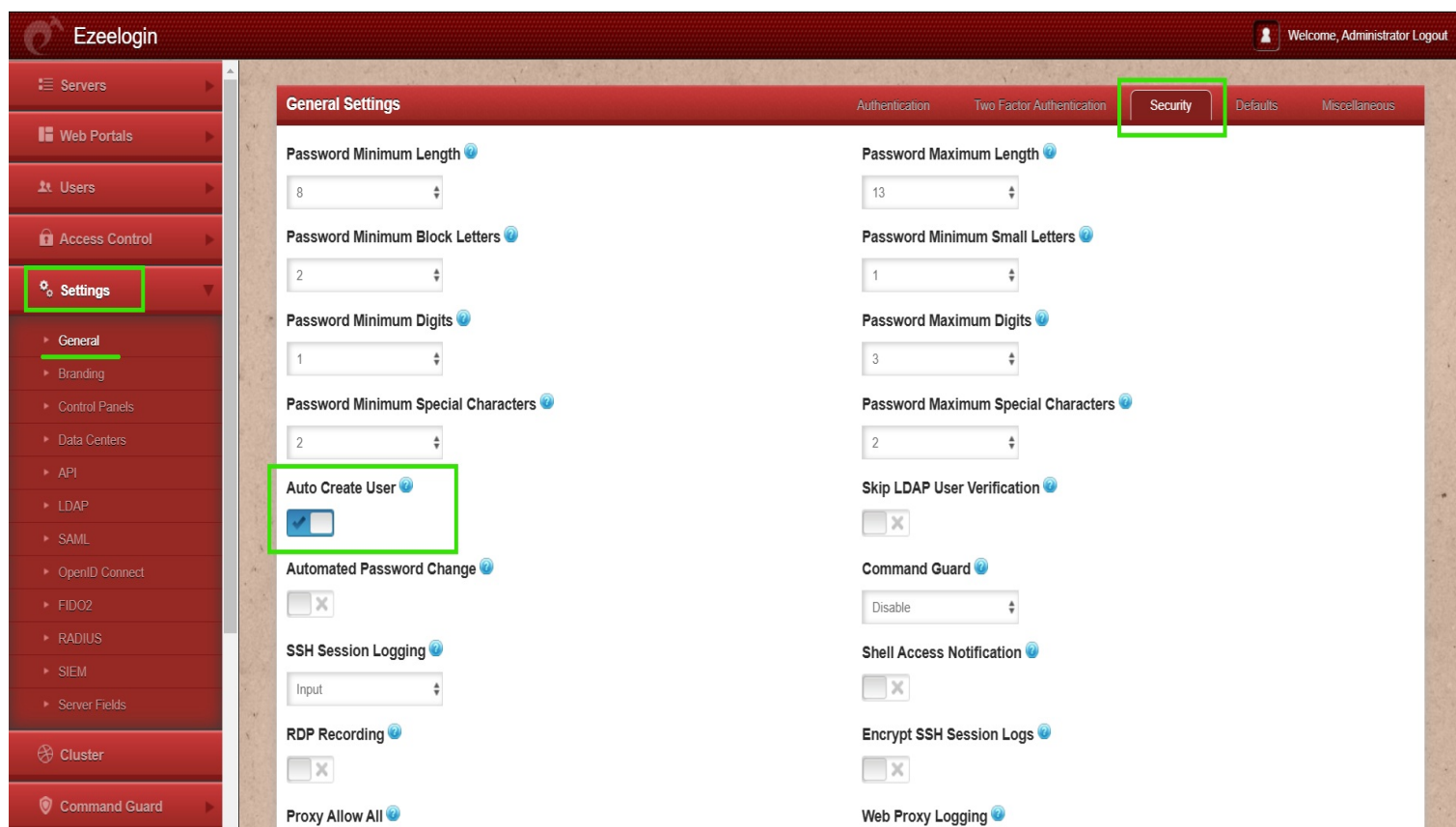


Azure AD Settings

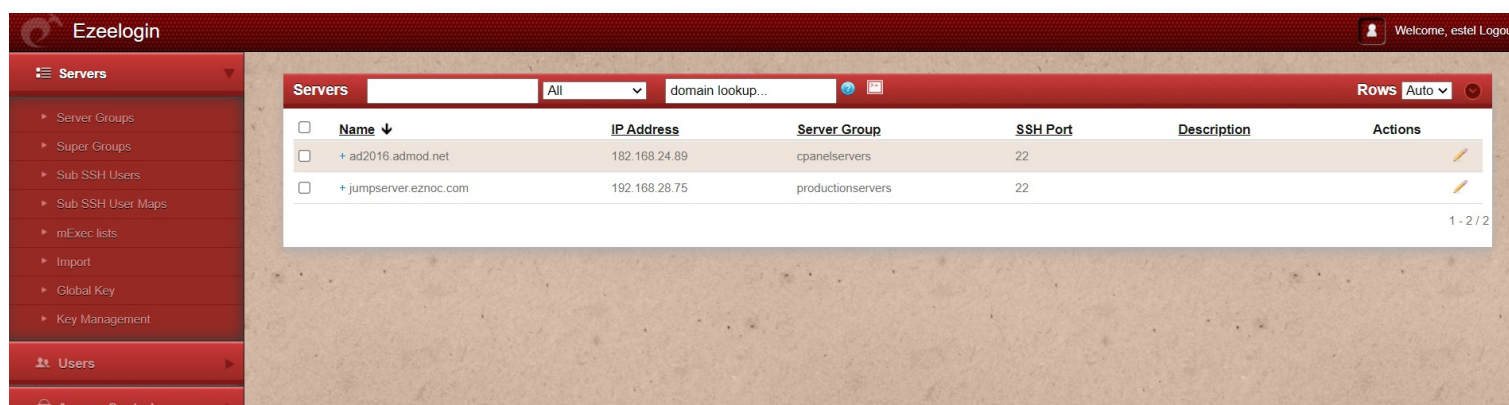
Step 7: Now change Web Panel Authentication Ezeelogin to SAML.



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:

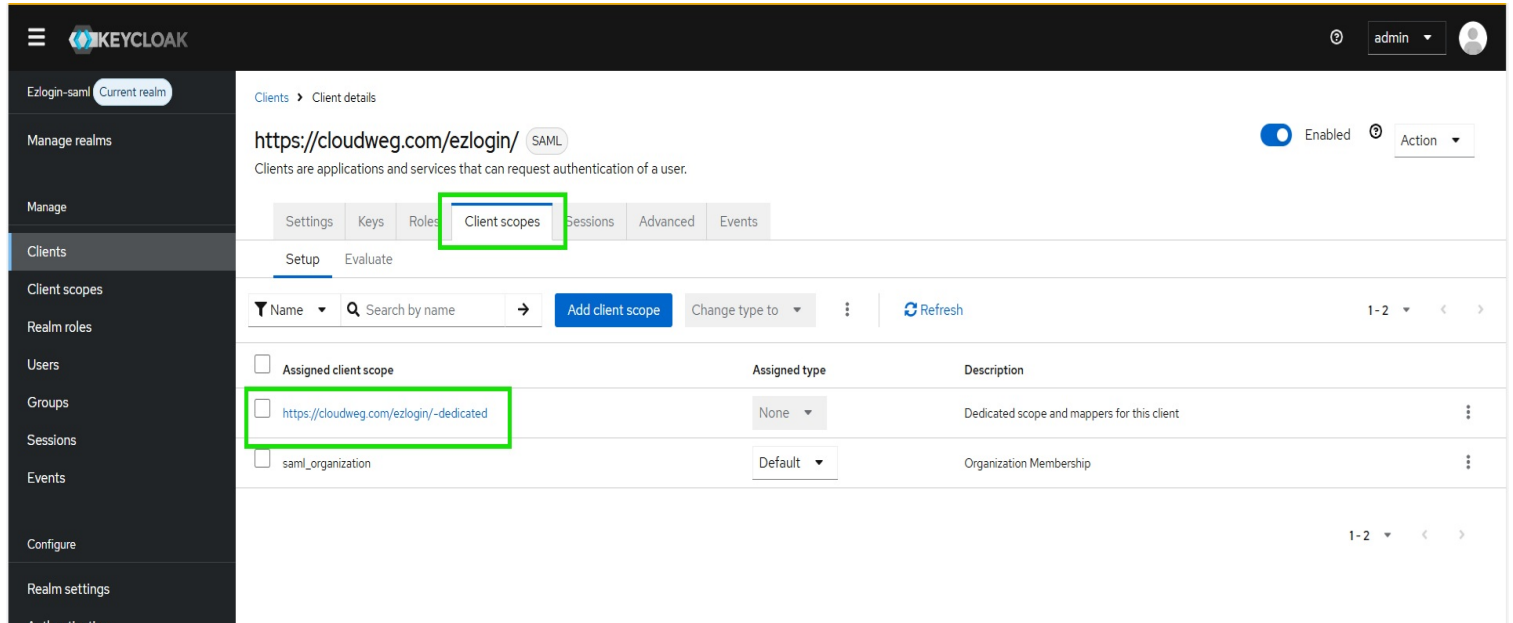
Error: Invalid password

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.



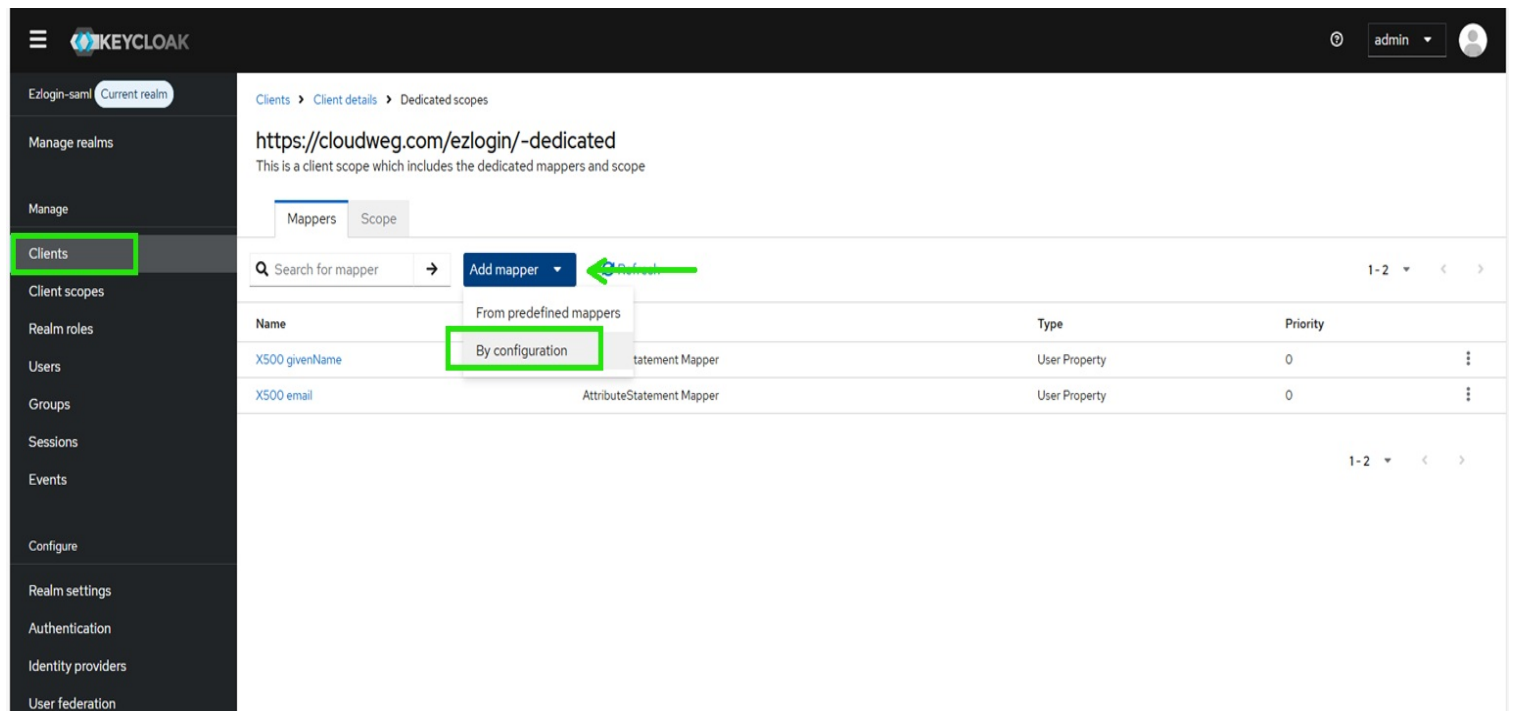
Choose the assigned client scope and click Add Mapper.



The screenshot shows the Keycloak administration console. The left sidebar has the 'Clients' menu item highlighted. The main content area is titled 'Client details' for the client 'https://cloudweg.com/ezlogin/'. The 'Client scopes' tab is selected and highlighted with a green box. Below the tabs, there is a table of assigned client scopes. The first row, 'https://cloudweg.com/ezlogin/-dedicated', is highlighted with a green box. The table has columns for 'Assigned client scope', 'Assigned type', and 'Description'.

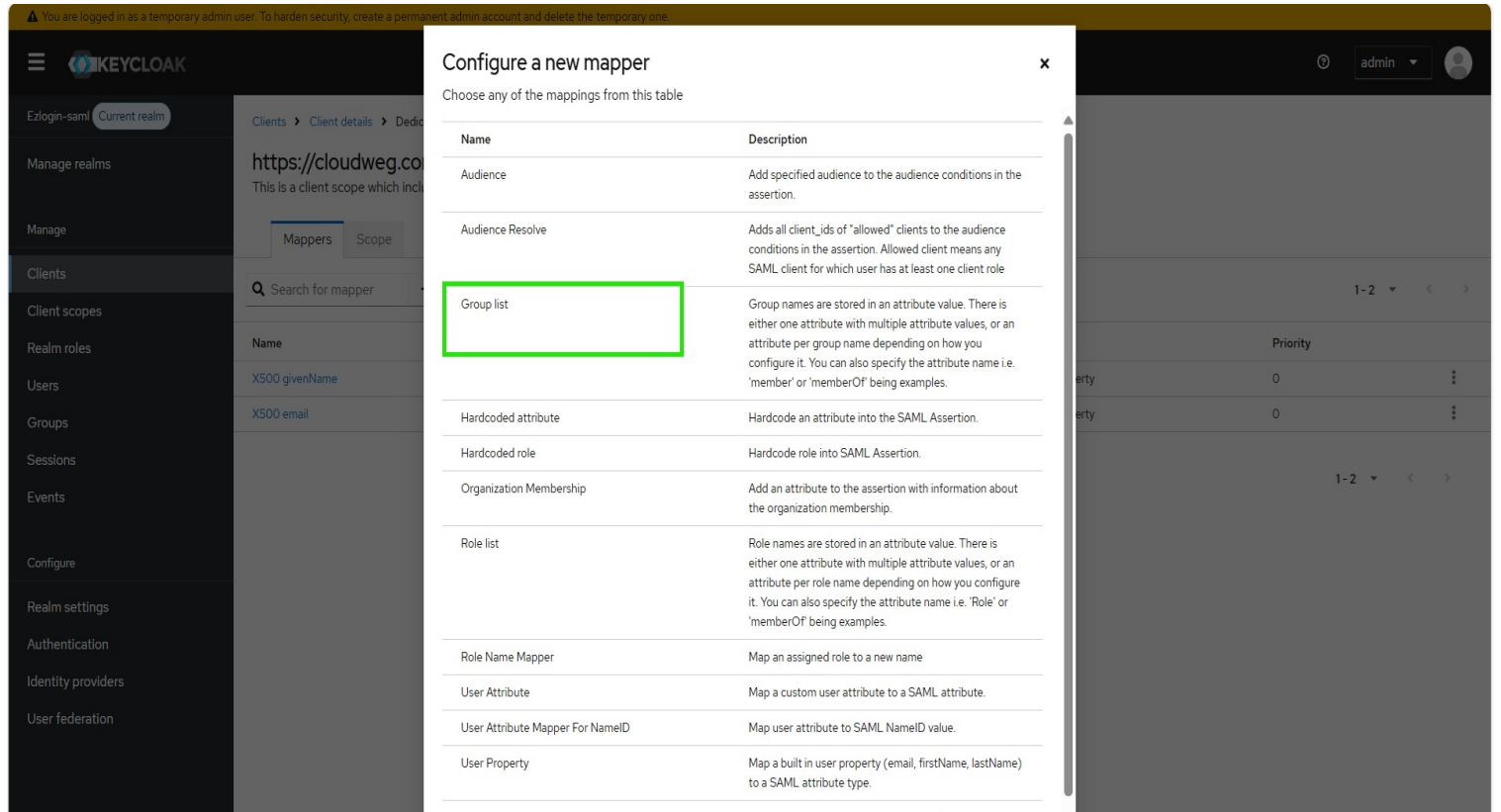
Assigned client scope	Assigned type	Description
☐ https://cloudweg.com/ezlogin/-dedicated	None	Dedicated scope and mappers for this client
☐ saml_organization	Default	Organization Membership

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

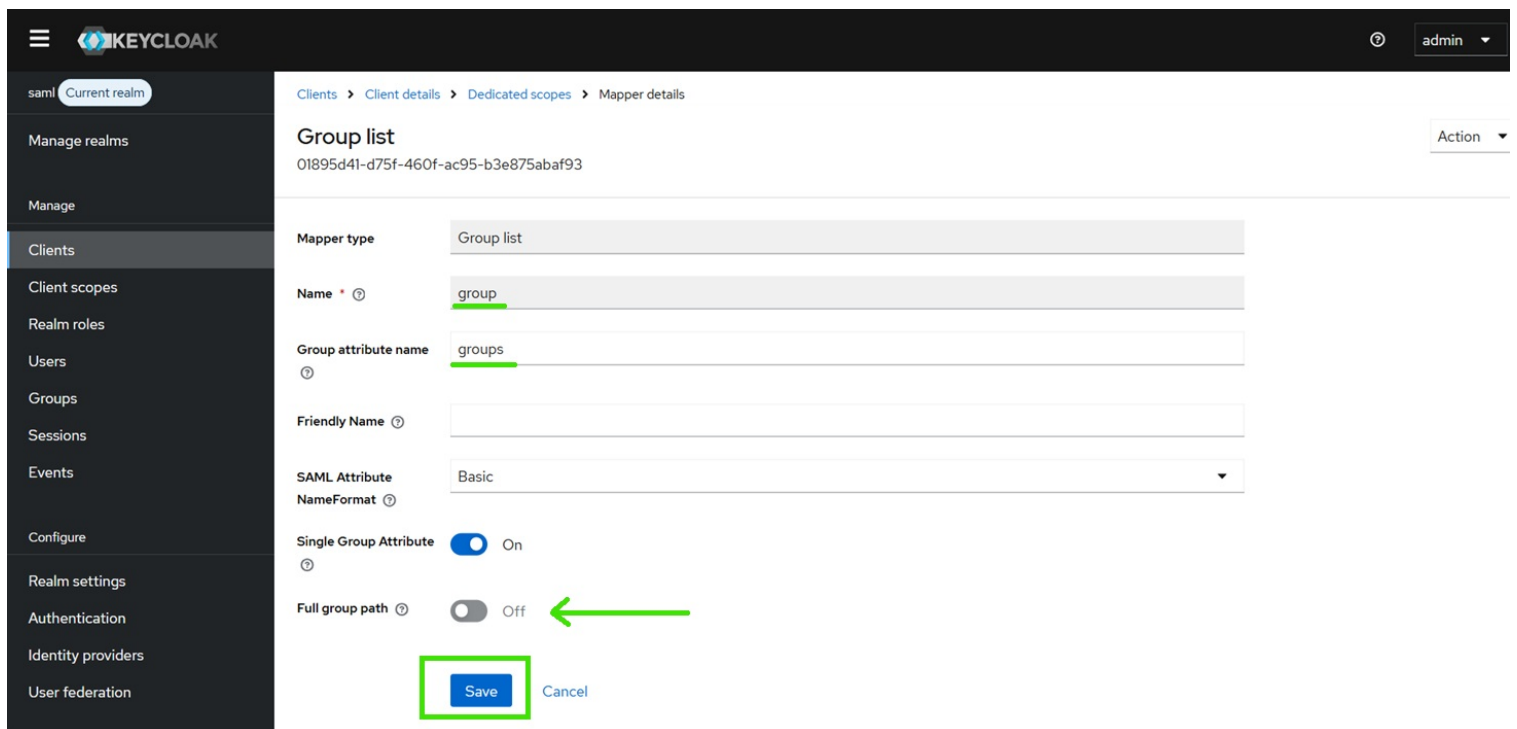


The screenshot shows the Keycloak administration console. The left sidebar has the 'Clients' menu item highlighted. The main content area is titled 'Dedicated scopes' for the client scope 'https://cloudweg.com/ezlogin/-dedicated'. The 'Mappers' tab is selected. Below the tabs, there is a table of mappers. The 'Add mapper' button is highlighted with a green box, and a green arrow points to it. The dropdown menu for 'Add mapper' is open, showing 'By configuration' as the selected option, which is also highlighted with a green box. The table has columns for 'Name', 'Type', and 'Priority'.

Name	Type	Priority
X500 givenName	Statement Mapper	0
X500 email	AttributeStatement Mapper	0



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

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

Access Control

Settings

General

Branding

Control Panels

Data Centers

API

LDAP

SAML

OpenID Connect

FIDO2

RADIUS

SIEM

Server Fields

New Encryption Certificate ?

Username Attribute ?

Group Attribute ?

groups

Firstname Attribute ?

Lastname Attribute ?

Cancel Fetch Save

Azure AD Settings

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

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

User Groups

Authentication Log

SSH Log

RDP Recording

SCP Log

Web Proxy Log

Web Proxy Activity

Web Activity

Shell Activity

Server Activity

Work Summary

Status

Edit User Group

Name

saml-keycloak

Priority

5

Description

Force Two Factor Authentication

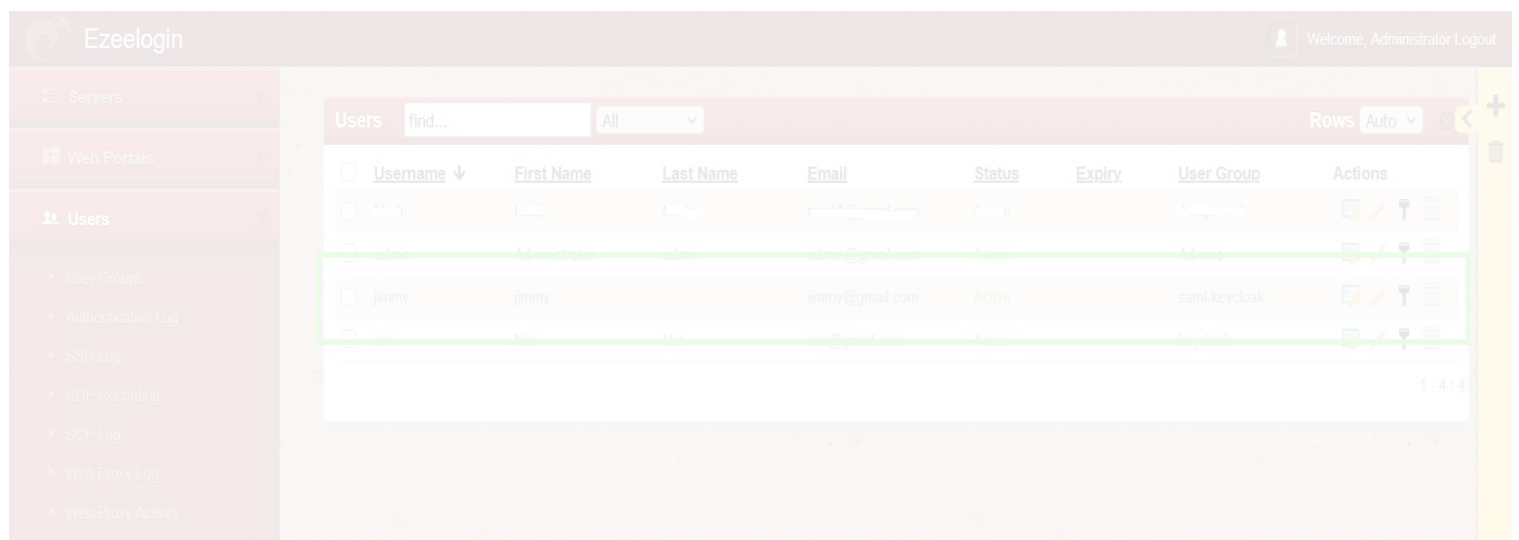
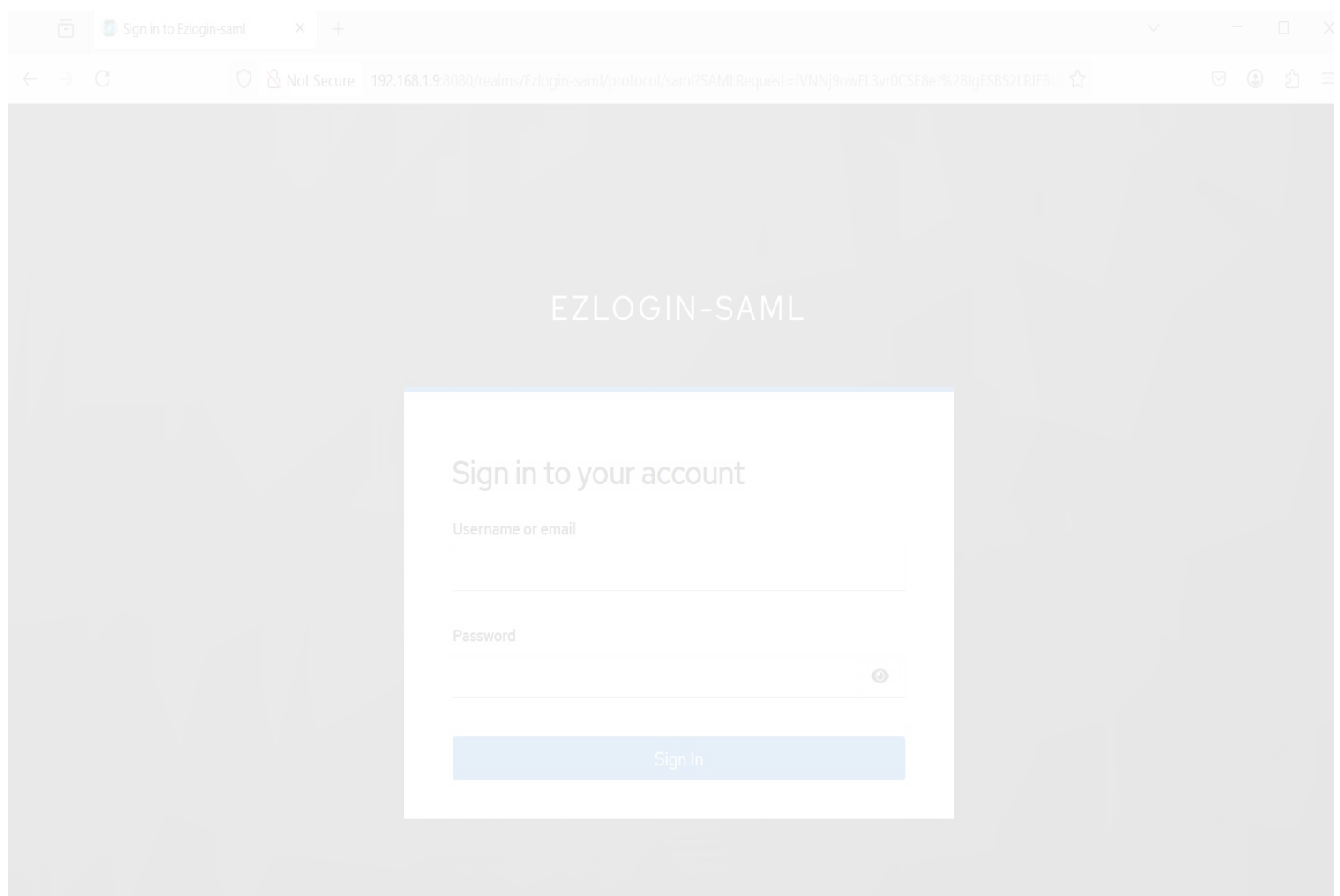
Cancel Save

Command Guard

-- None --

Allow Disallow

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-ss0-779.html>