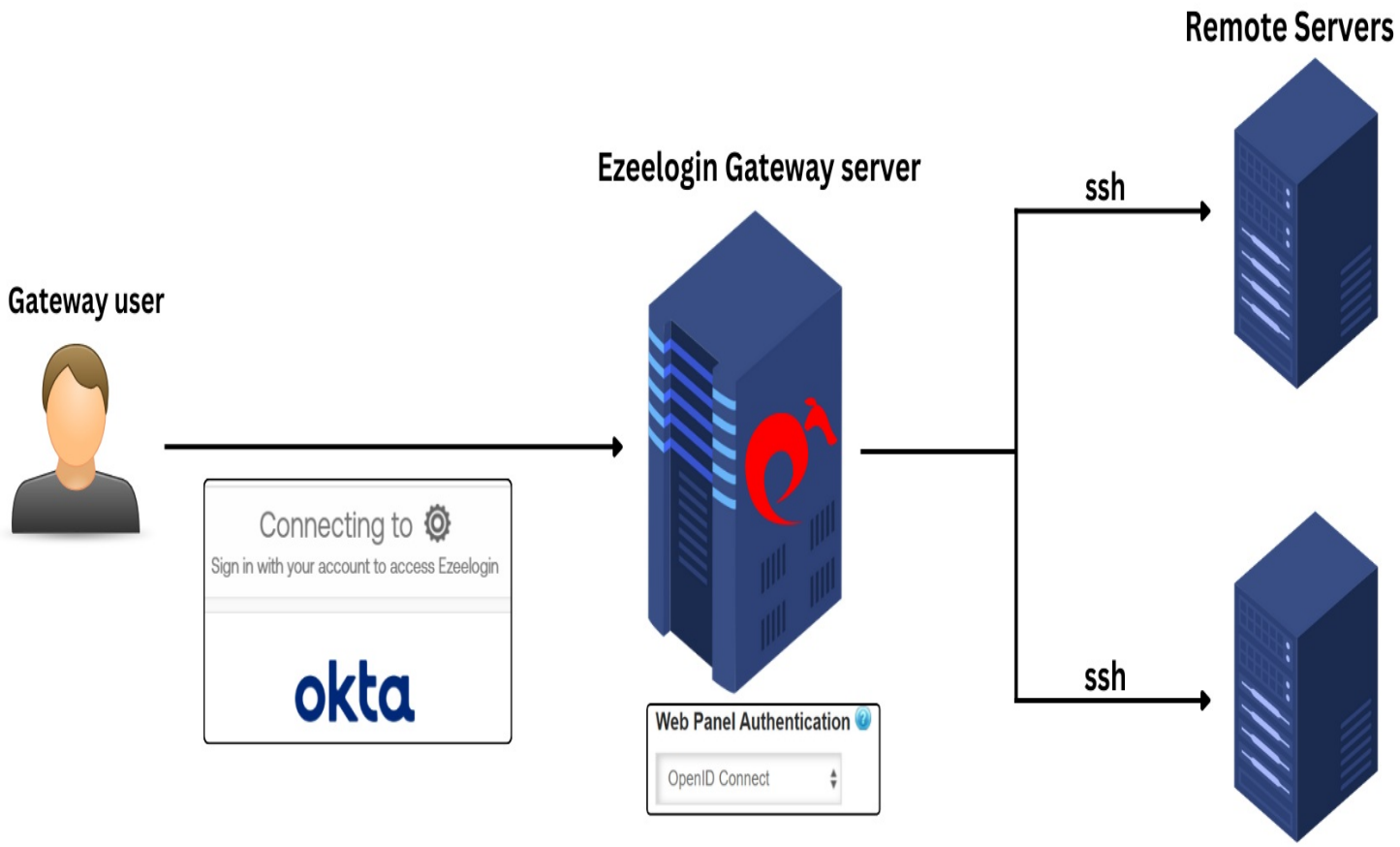
Integrate Okta OpenID connect

771 Lekshmi May 28, 2026 Features & Functionalities 3224

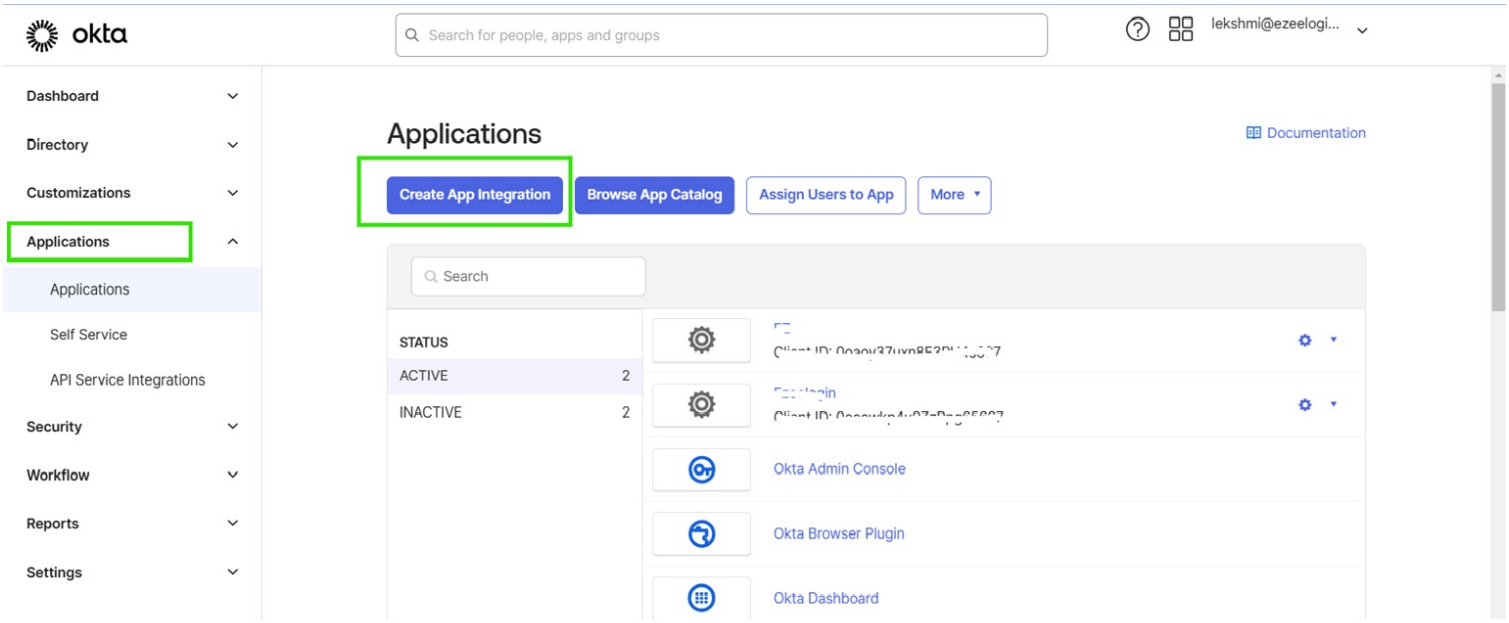
How to integrate Okta OpenID connect with Ezeelogin

Overview: This article will helps to integrate Okta OpenID Connect with the Ezeelogin jump server.

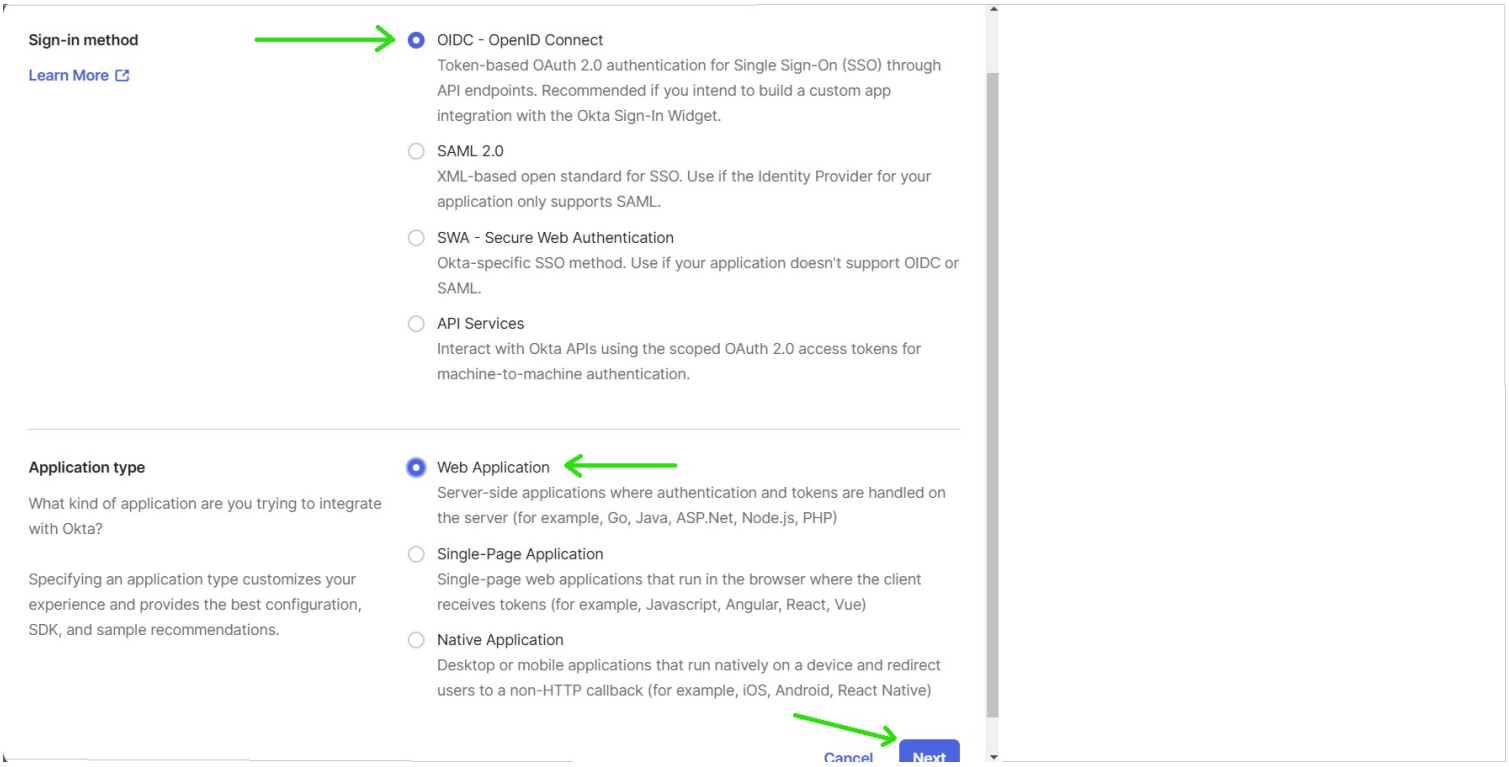
OpenID connect is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



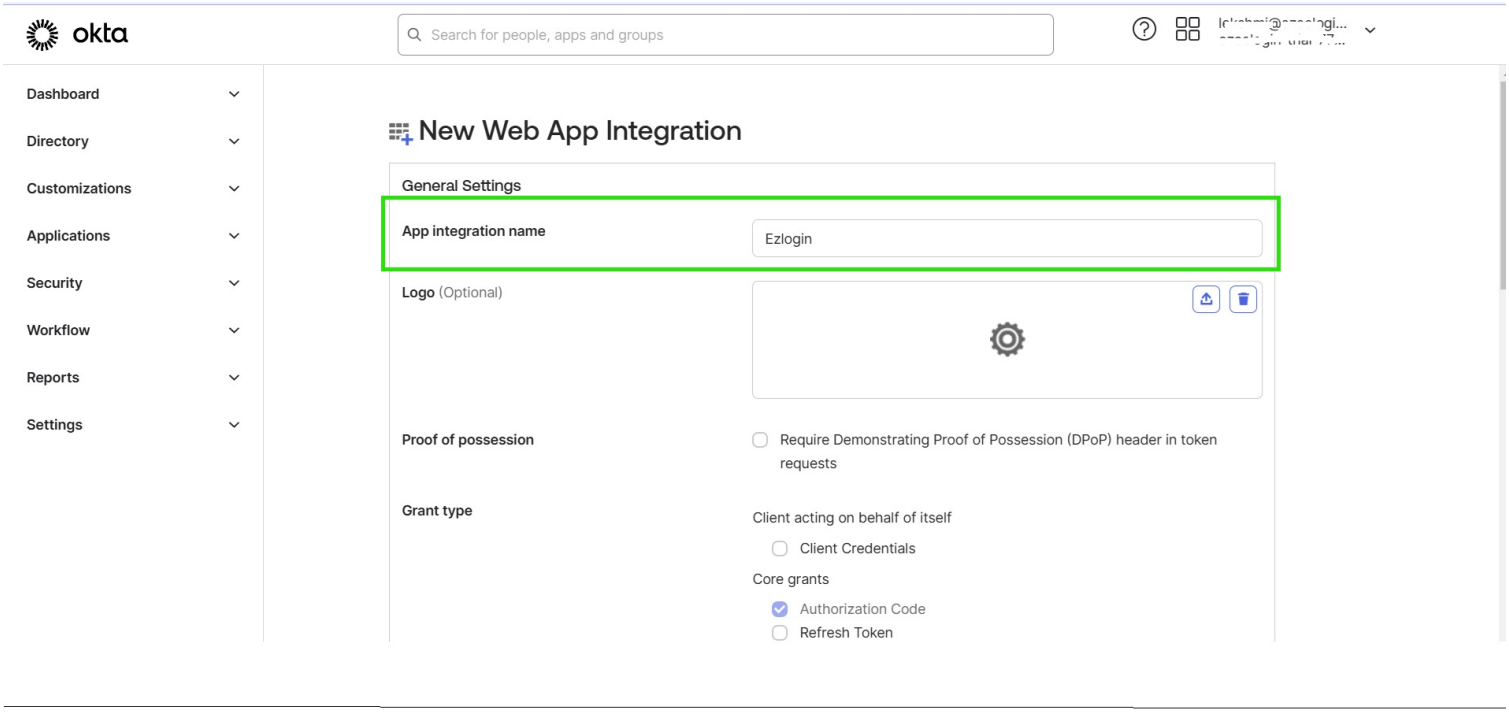
Step 1: Log into Okta and add the application under **Applications -> Create App Integration.**



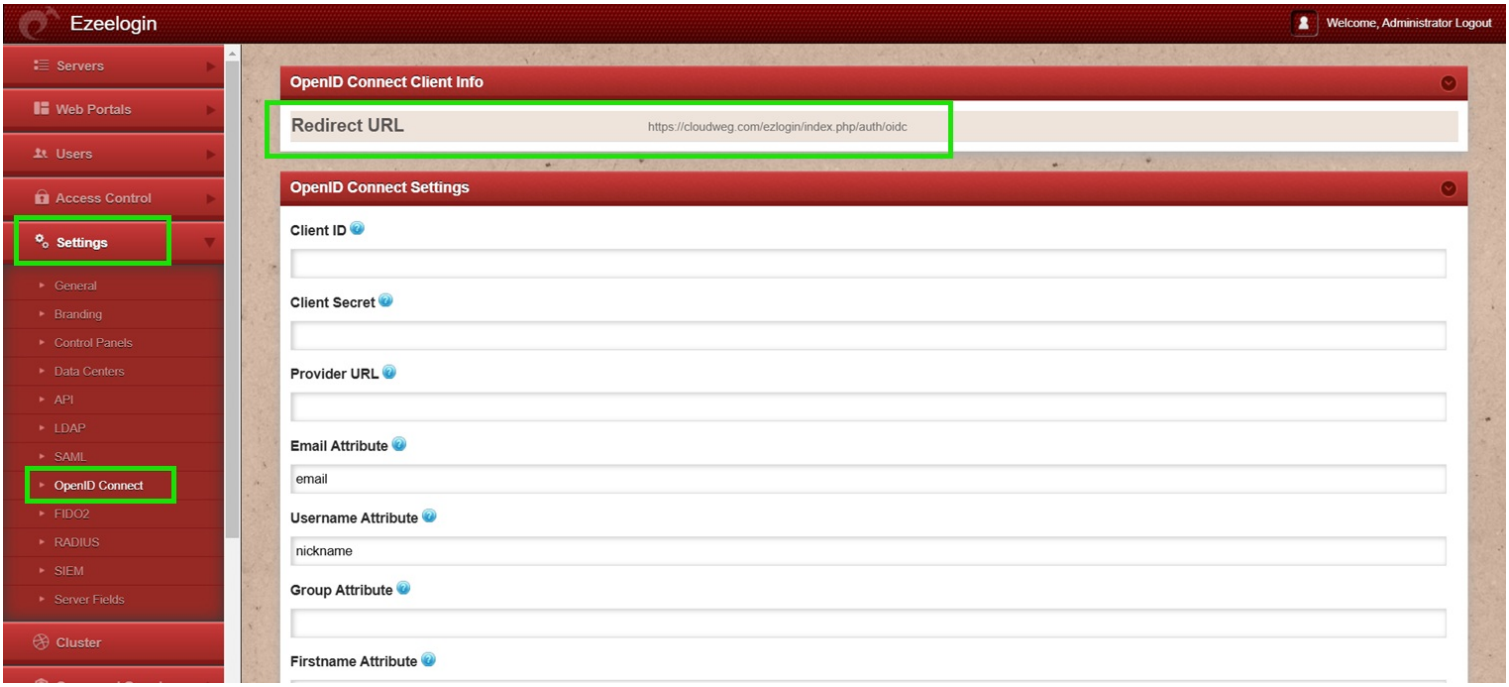
Step 2: Select the sign-in-method as **OIDC -OpenID Connect,** Choose **Application type** and click **Next**.

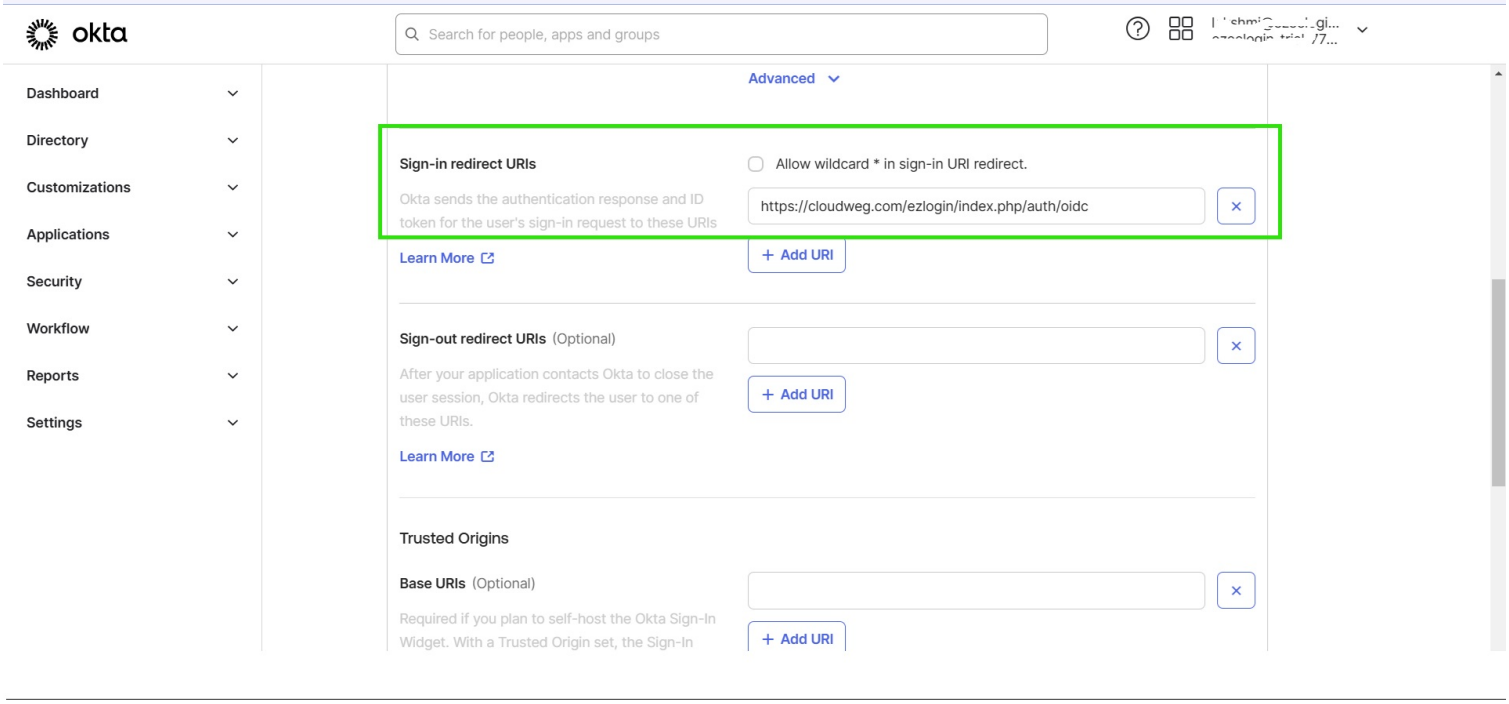


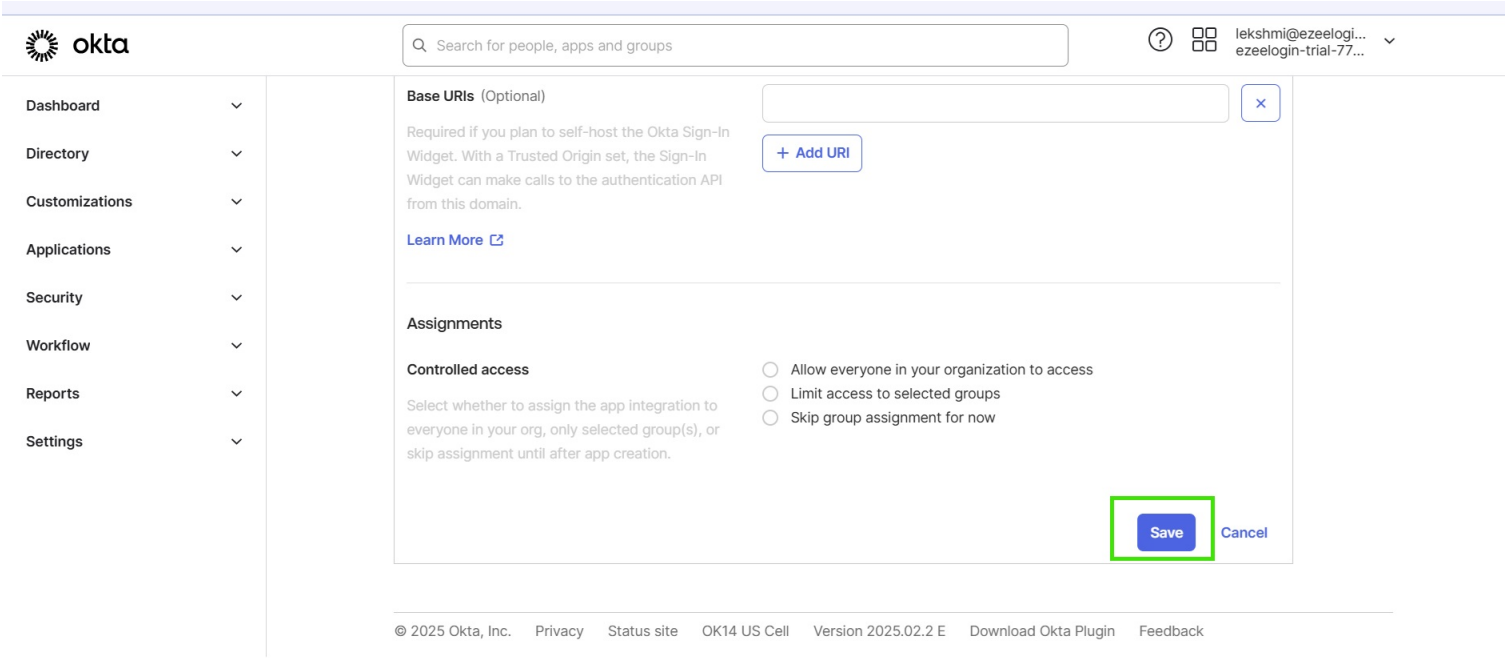
Step 3: Enter the app integration name.



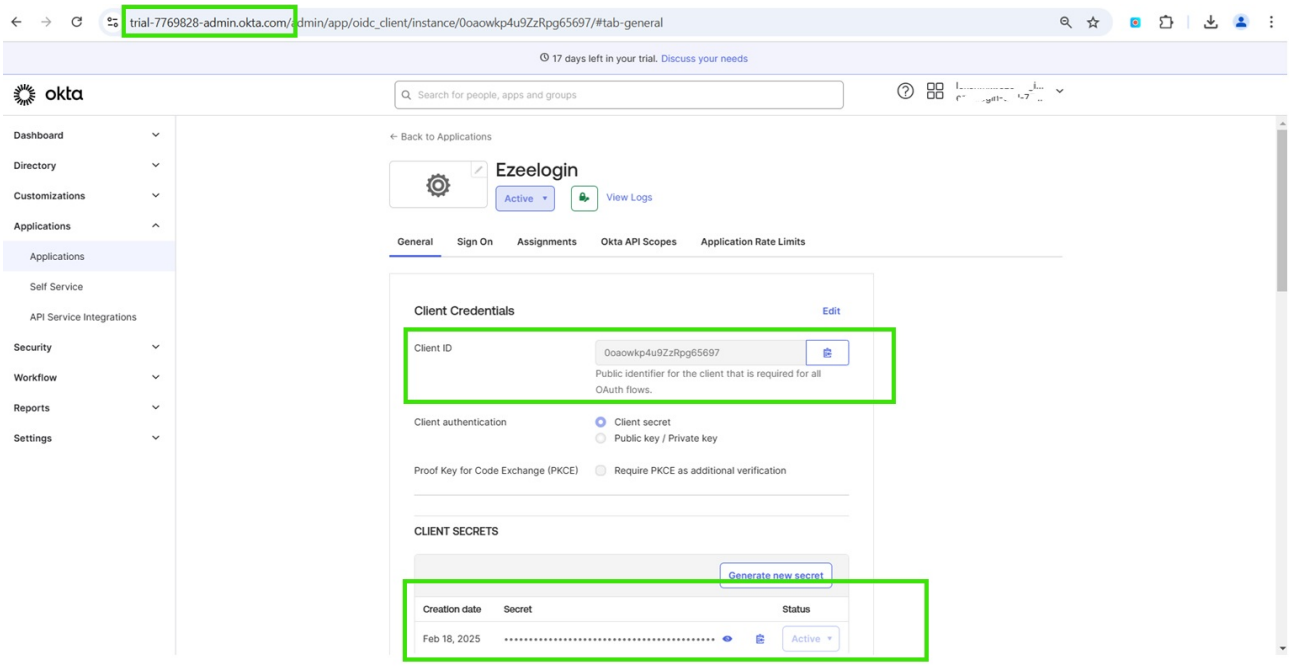
Step 4: Login to the Ezeelogin GUI, go to **Settings -> OpenID Connect** and **copy the redirect URL**(refer to the screenshot below). Then, **paste the URL into** the **Sign-in Redirect URI field in okta** portal and click **save**.

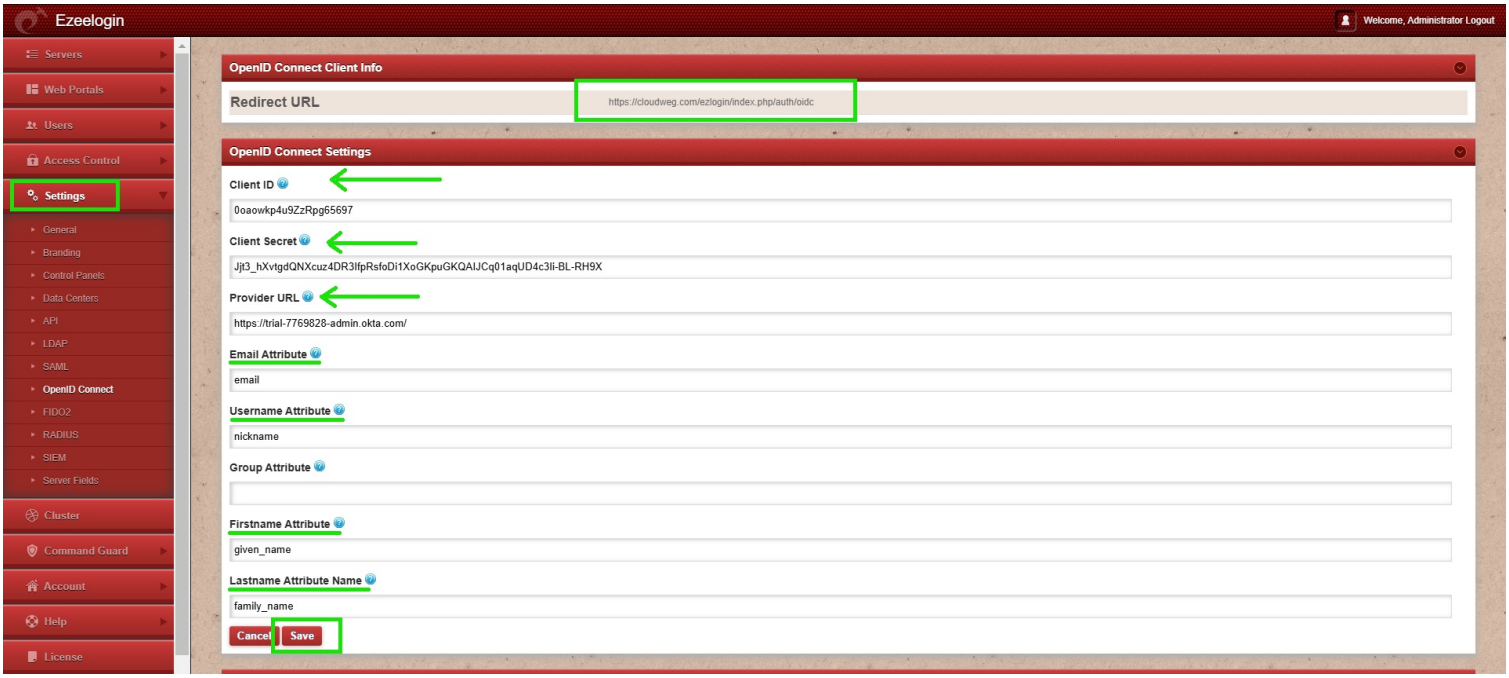






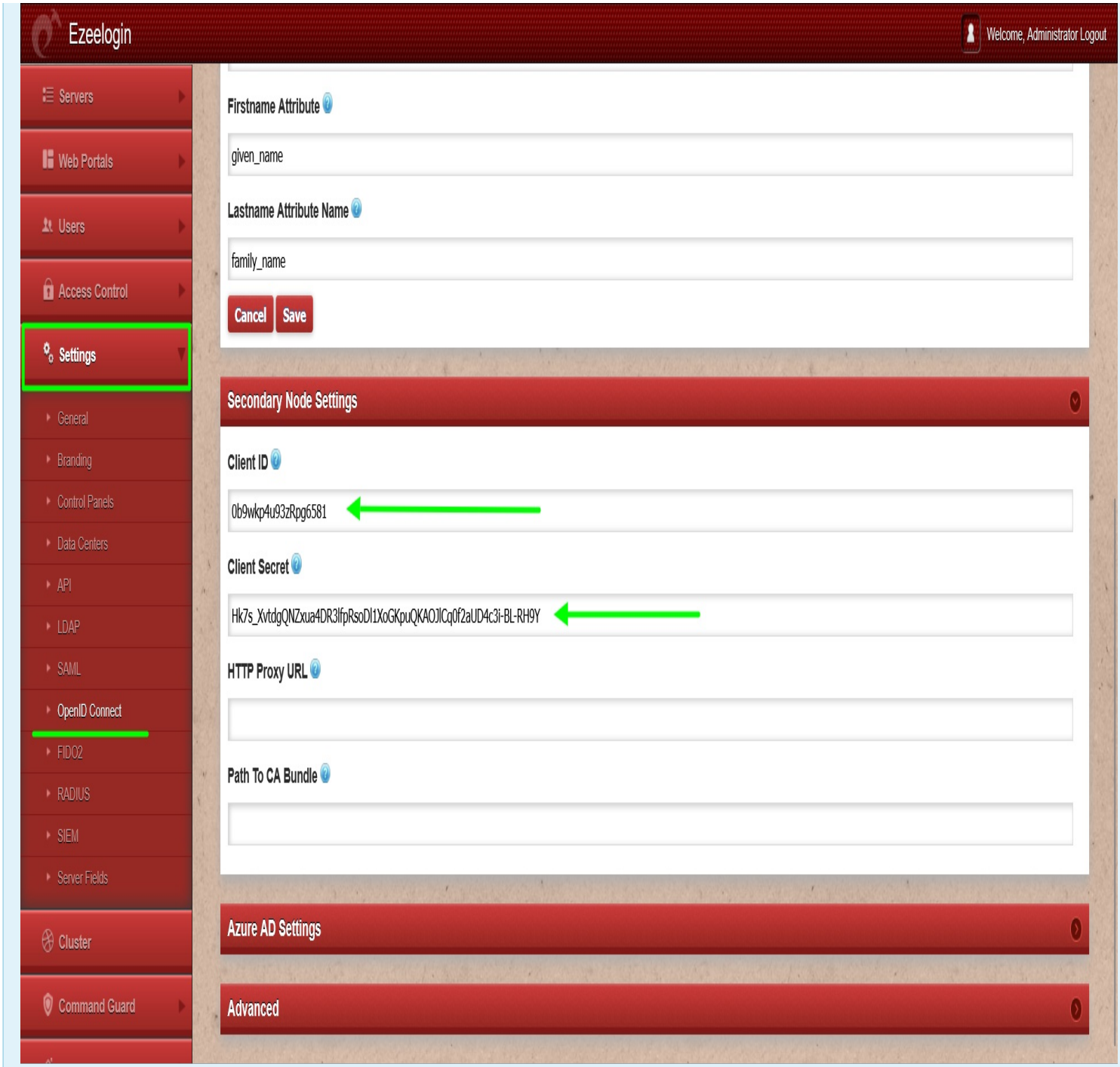
Step 5: Copy the **Client ID, Client Secret** and **URL** then paste them into the Ezeelogin GUI under **Settings -> OpenID Connect** (refer to the screenshot below) and In the Ezeelogin GUI, go to Advanced Settings of OpenID connect, **disable JWT Secret,** and click **Save.**

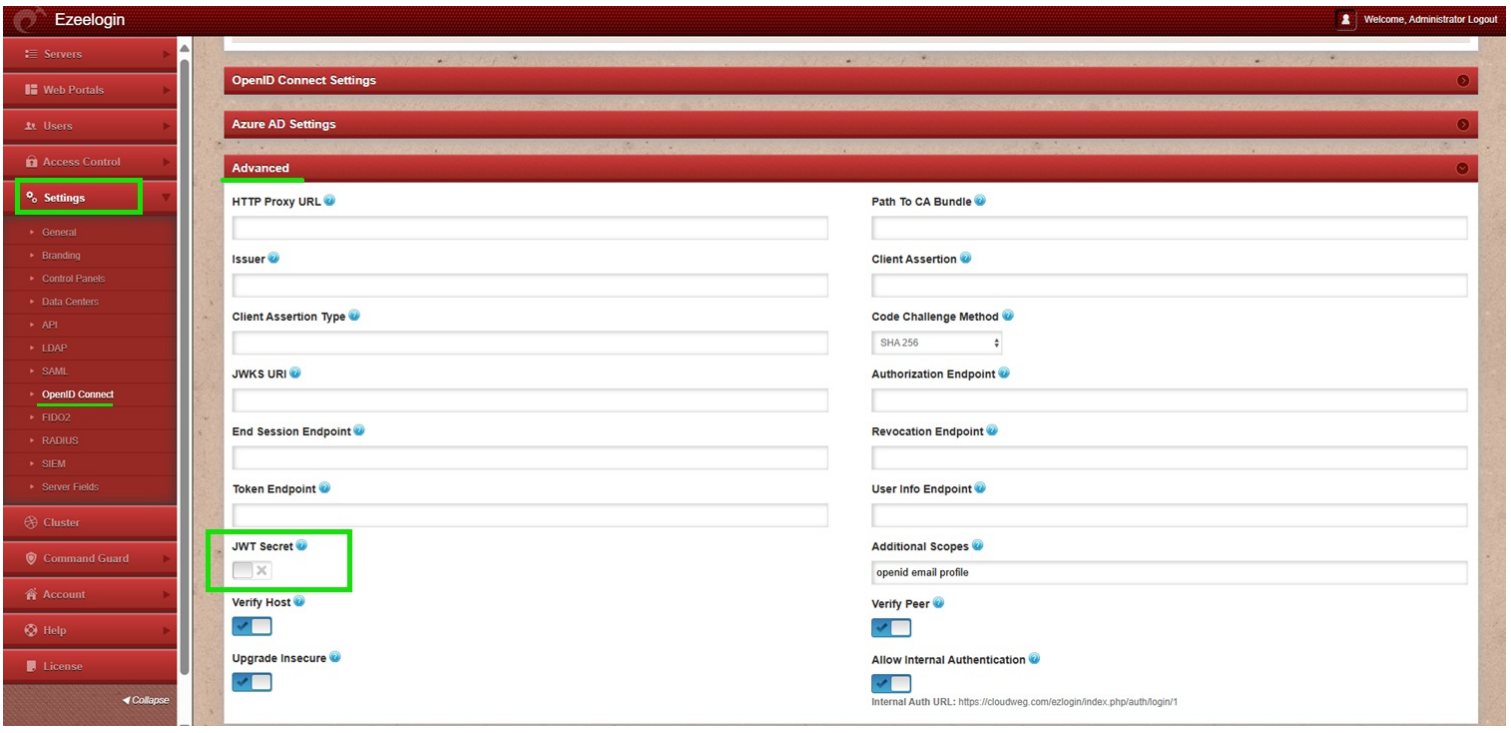




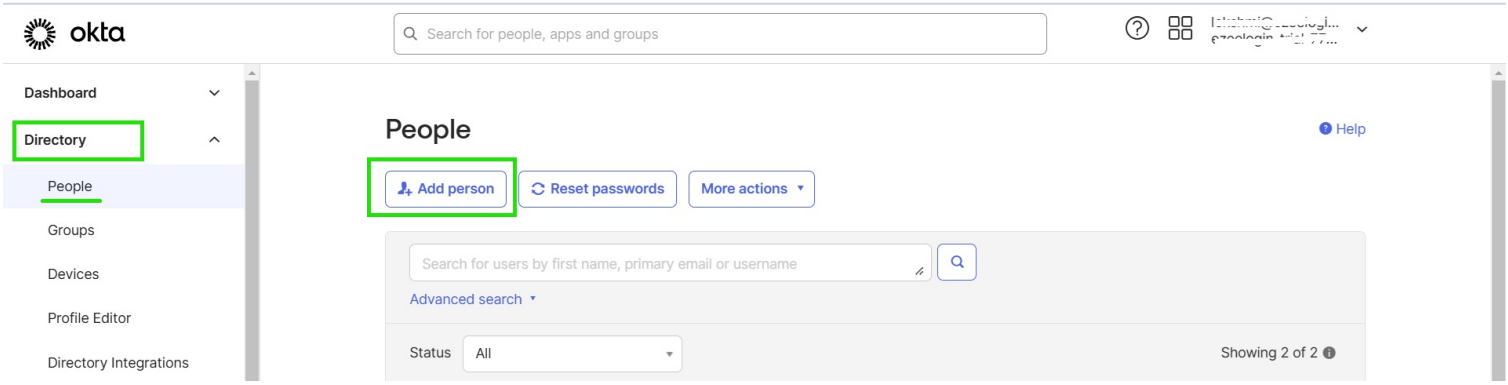
For cluster, add the Client ID and Client Secret from the other OIDC configuration:

Follow steps 1 to 5 to create new application for secondary node. While adding the application details in Okta, replace the IP address with the secondary node's IP address.

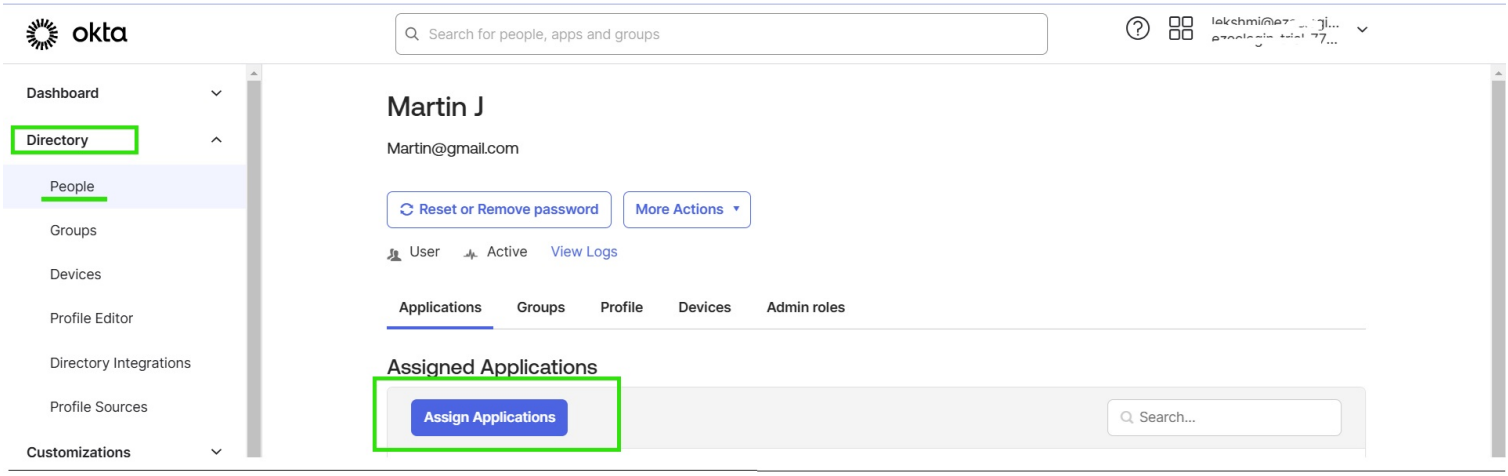

Ezeelogin
Welcome, Administrator Logout
Servers
Web Portals
Users
Access Control
Settings
General
Branding
Control Panels
Data Centers
API
LDAP
SAML
OpenID Connect
FIDO2
RADIUS
SIEM
Server Fields
Cluster
Command Guard
Firstname Attribute
given_name
Lastname Attribute Name
family_name
Cancel
Save
Secondary Node Settings
Client ID
0b9wkp4u93zRpg6581
Client Secret
Hk7s_XvtdgQNZxua4DR3lfpRsoDl1XoGKpuQKAOJlCq0f2aUD4c3i-BL-RH9Y
HTTP Proxy URL
Path To CA Bundle
Azure AD Settings
Advanced

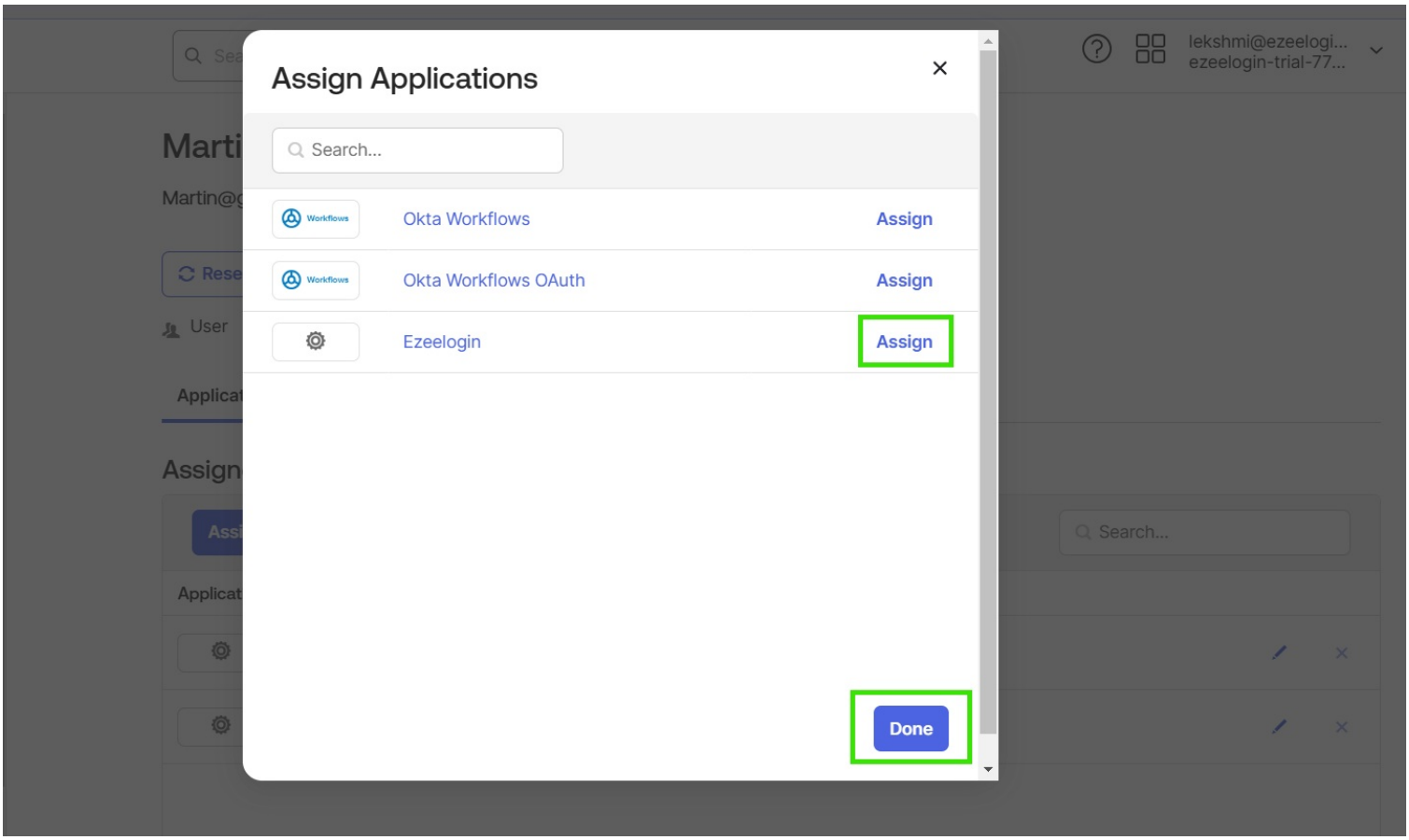

Ezeelogin
Welcome, Administrator Logout
OpenID Connect Settings
Azure AD Settings
Advanced
HTTP Proxy URL
Path To CA Bundle
Issuer
Client Assertion
Client Assertion Type
Code Challenge Method
SHA 256
JWKS URI
Authorization Endpoint
End Session Endpoint
Revocation Endpoint
Token Endpoint
User Info Endpoint
JWT Secret
Additional Scopes
openid email profile
Verify Host
Verify Peer
Upgrade Insecure
Allow Internal Authentication
Internal Auth URL: https://cloudweg.com/ezlogin/index.php/auth/login/1

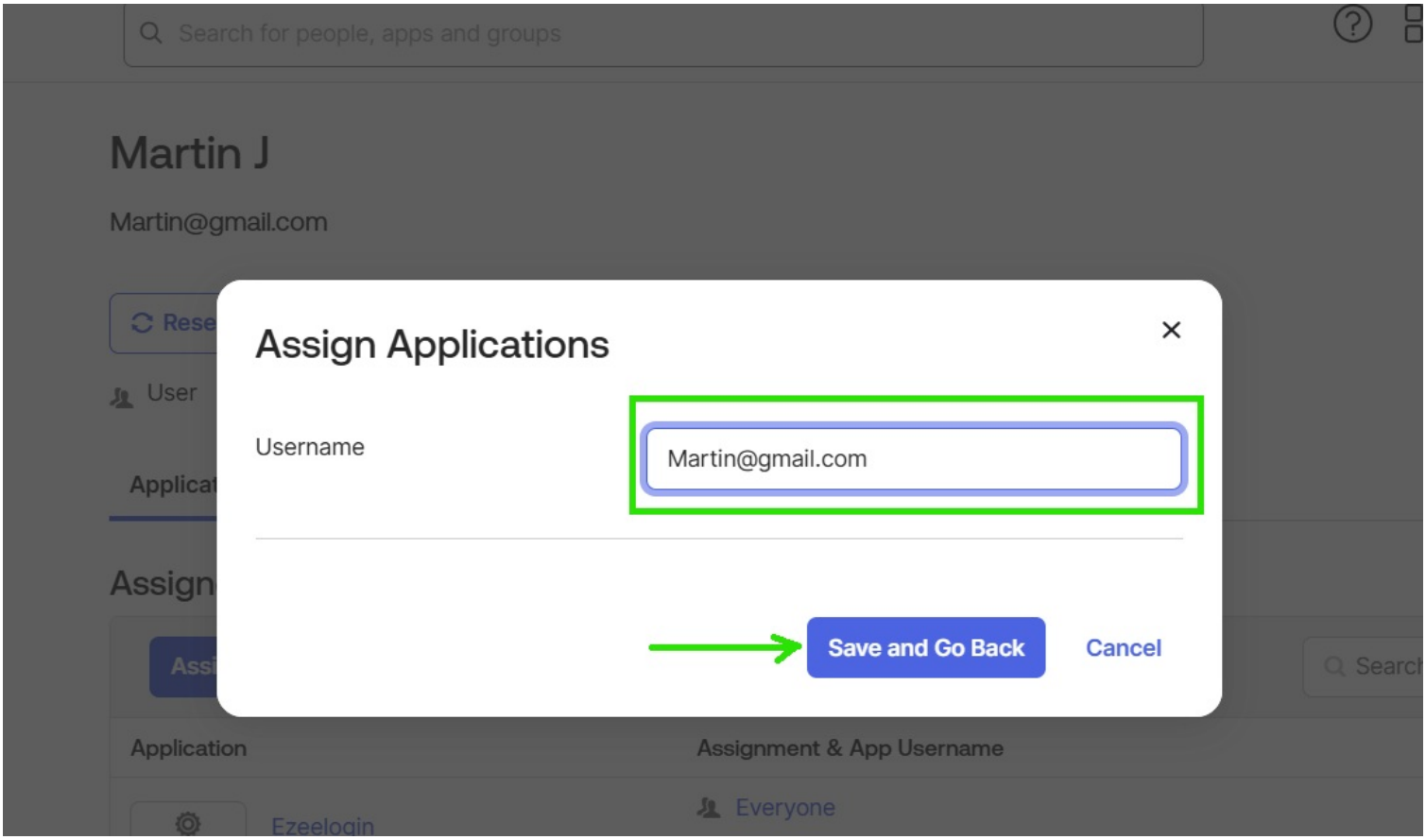
Step 6: To add users, navigate to **Directory**, then **select People,** and **click on Add Person**. This will open a form where you can enter the necessary user details and save them.



Step 7: After adding the user, navigate to the People tab and click Assign Application to assign the user to the application.

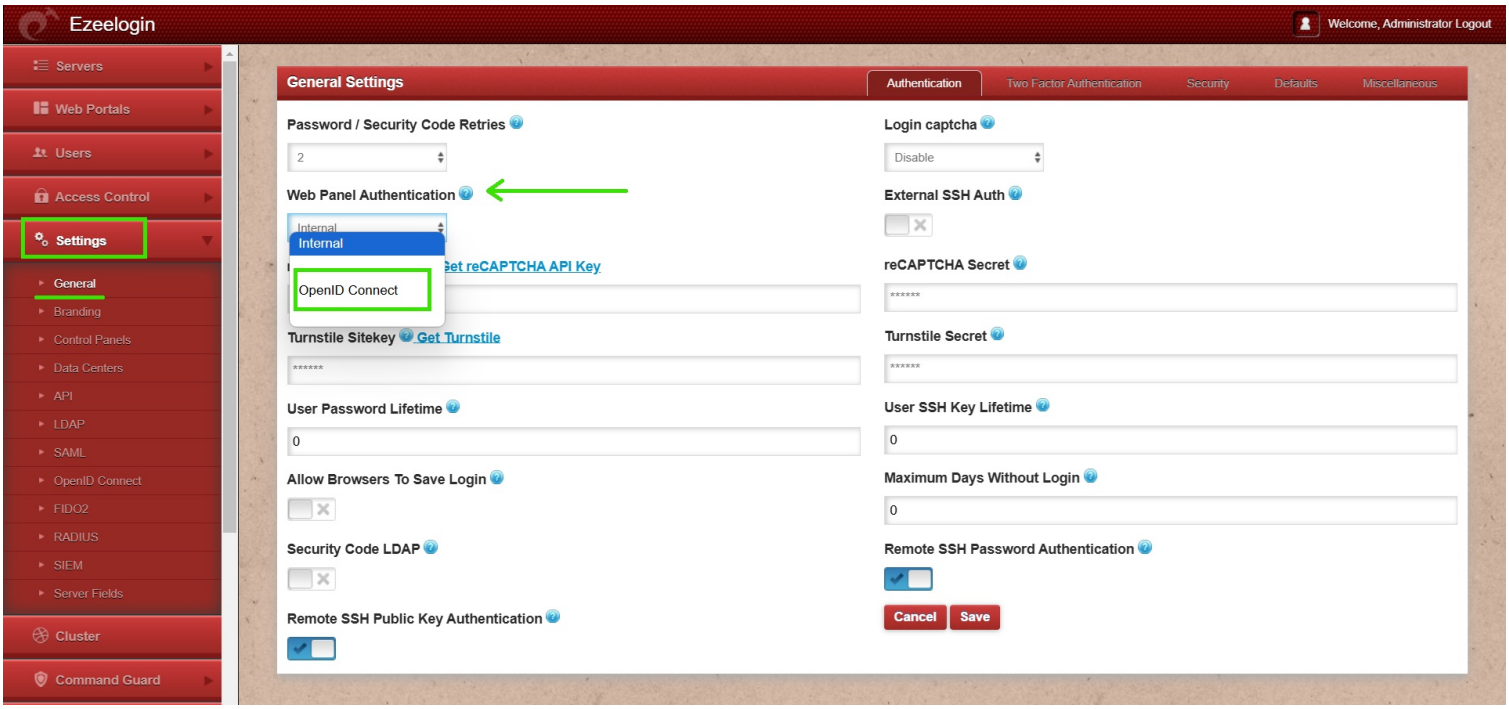




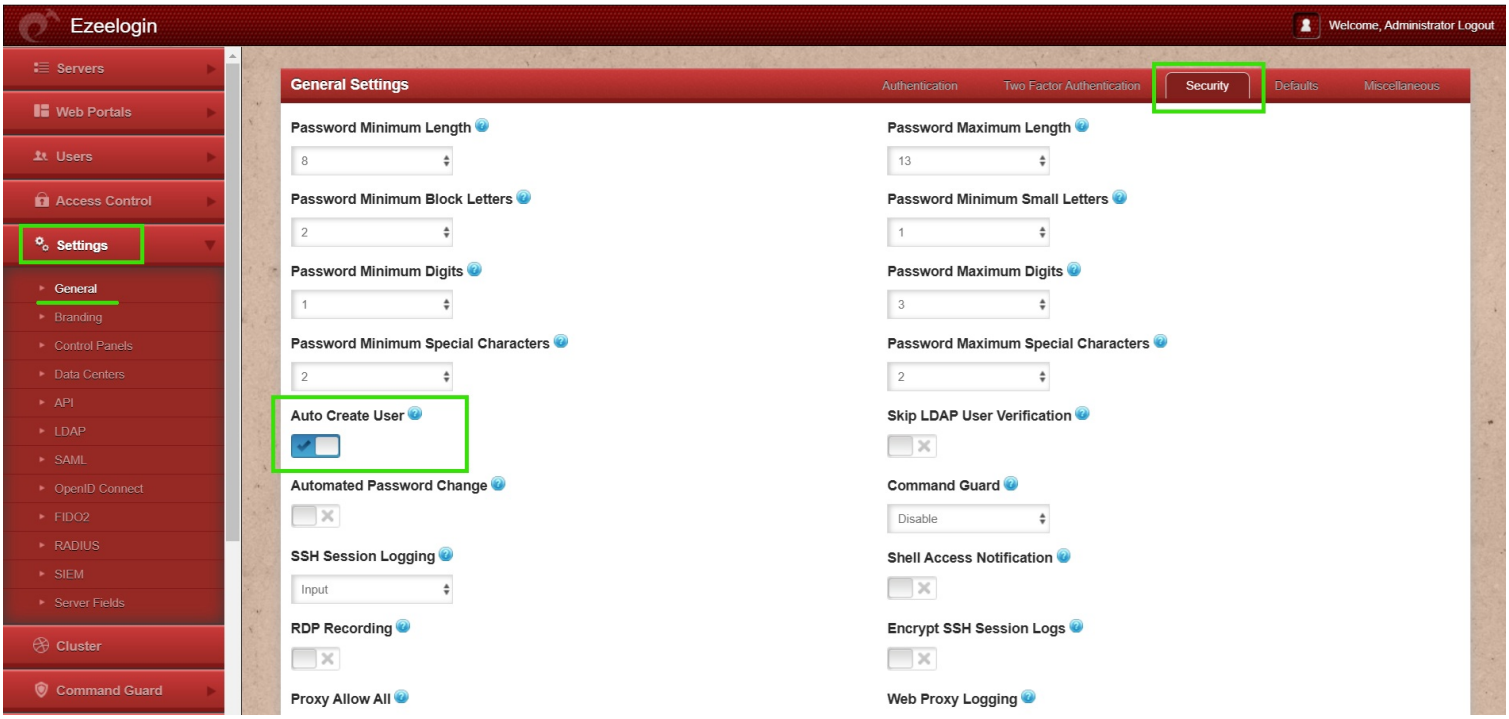


Step 8: After Login to Ezeelogin GUI and do the below steps

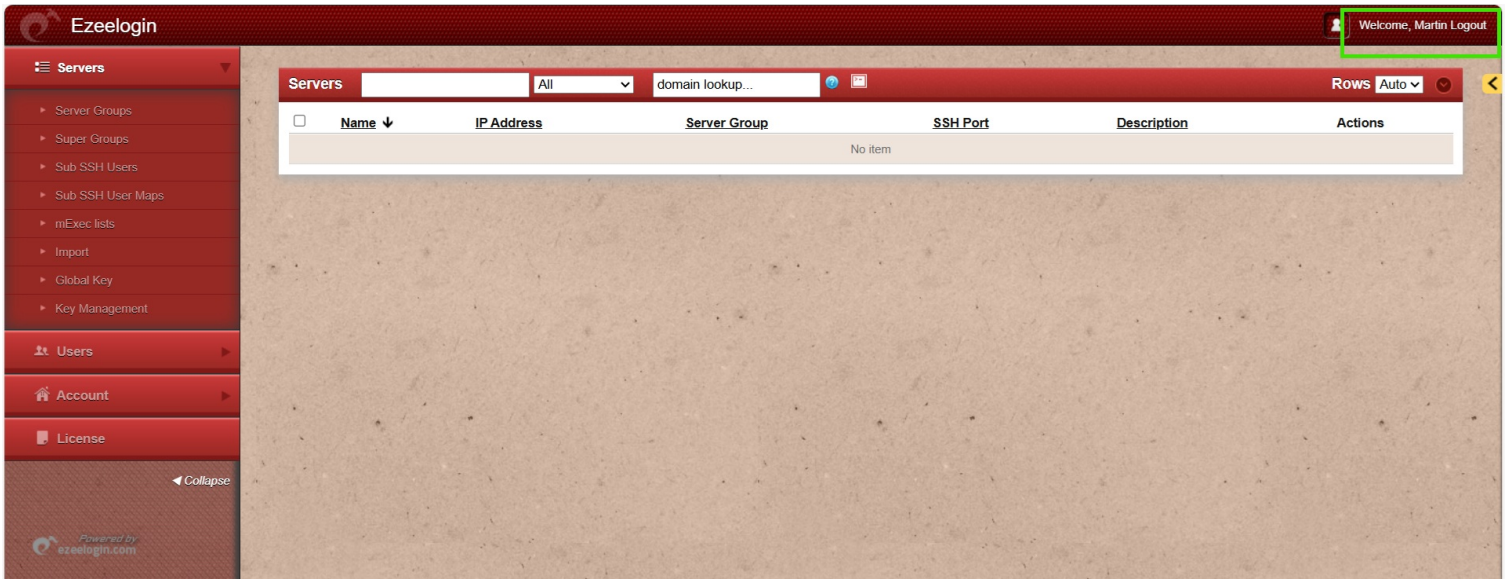
Step 8 (A): Go to **Settings -> General -> Web Panel Authentication**, then change **Web Panel Authentication** to **OpenID Connect**.



Step 8 (B): Enable Auto Create User in the Ezeelogin GUI by going to **Settings -> General -> Security.**



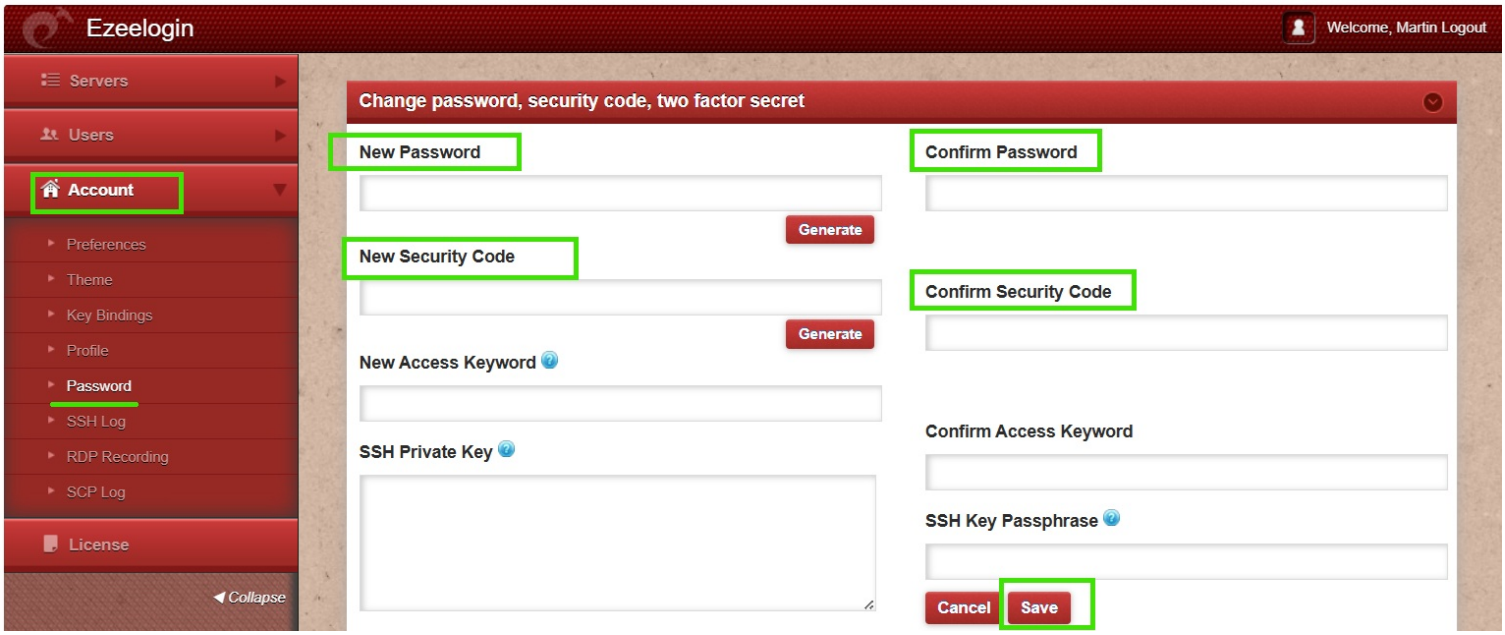
Step 9: Re-login to the Ezeelogin GUI with OpenID connect authentication



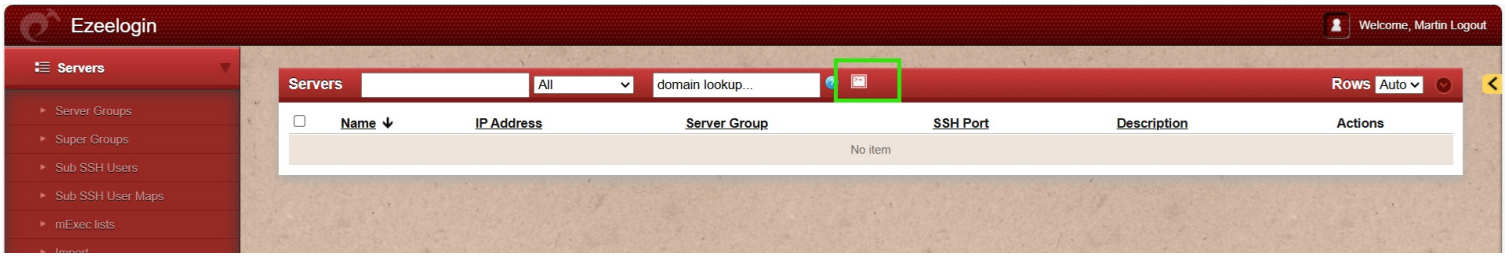
For gateway users who require administrative access, the password must be set manually from the Ezeelogin GUI. Refer below article:

Error: Invalid password

After logging in, set a new password and security code under **Account -> Password**.



Step 10: Also, try logging in to the Ezeelogin shell using **WebSSH** (refer the below screenshot) or any SSH client such as PuTTY or a terminal.

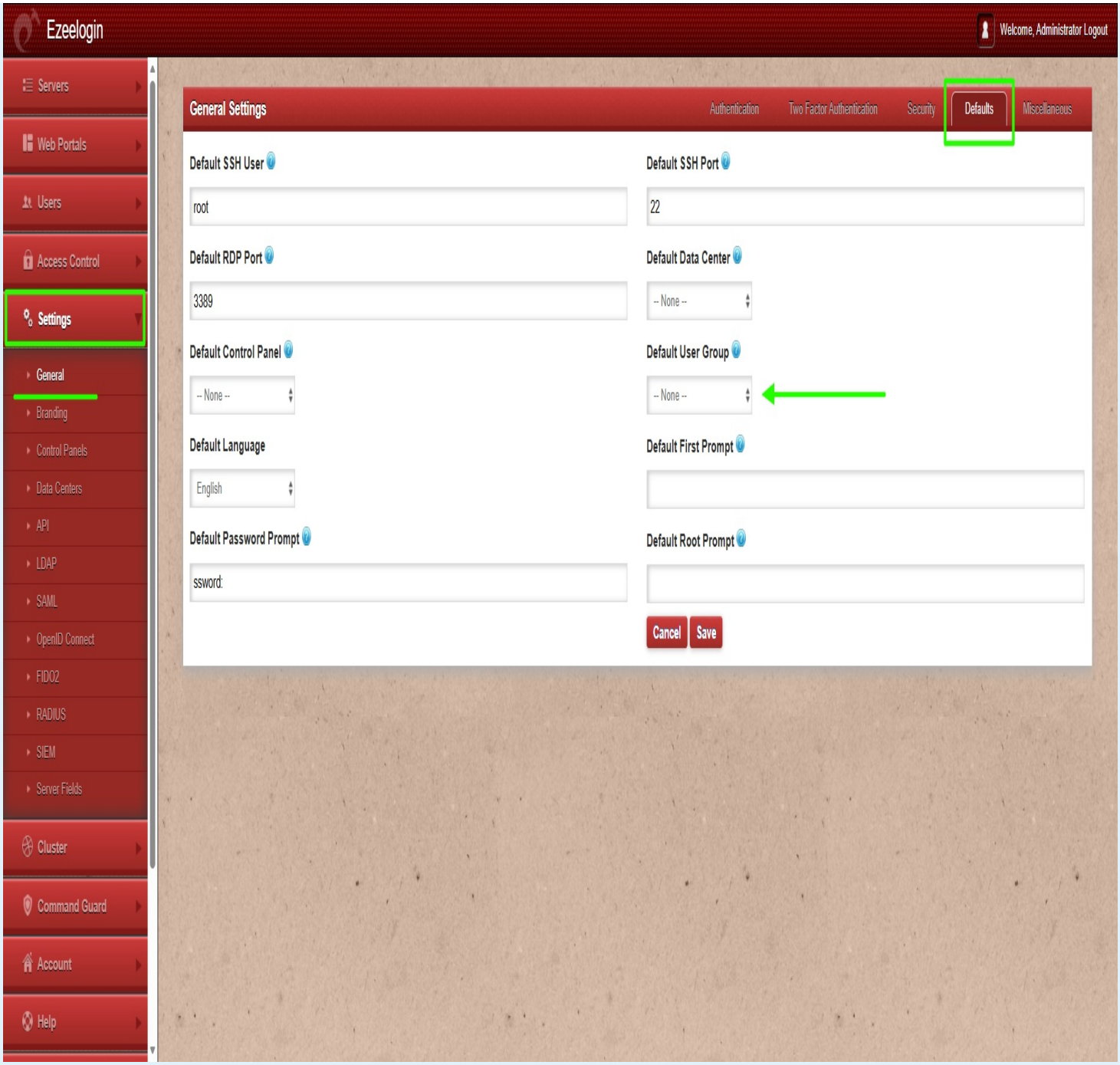


After setting the new password and security code, try logging in using the updated credentials.

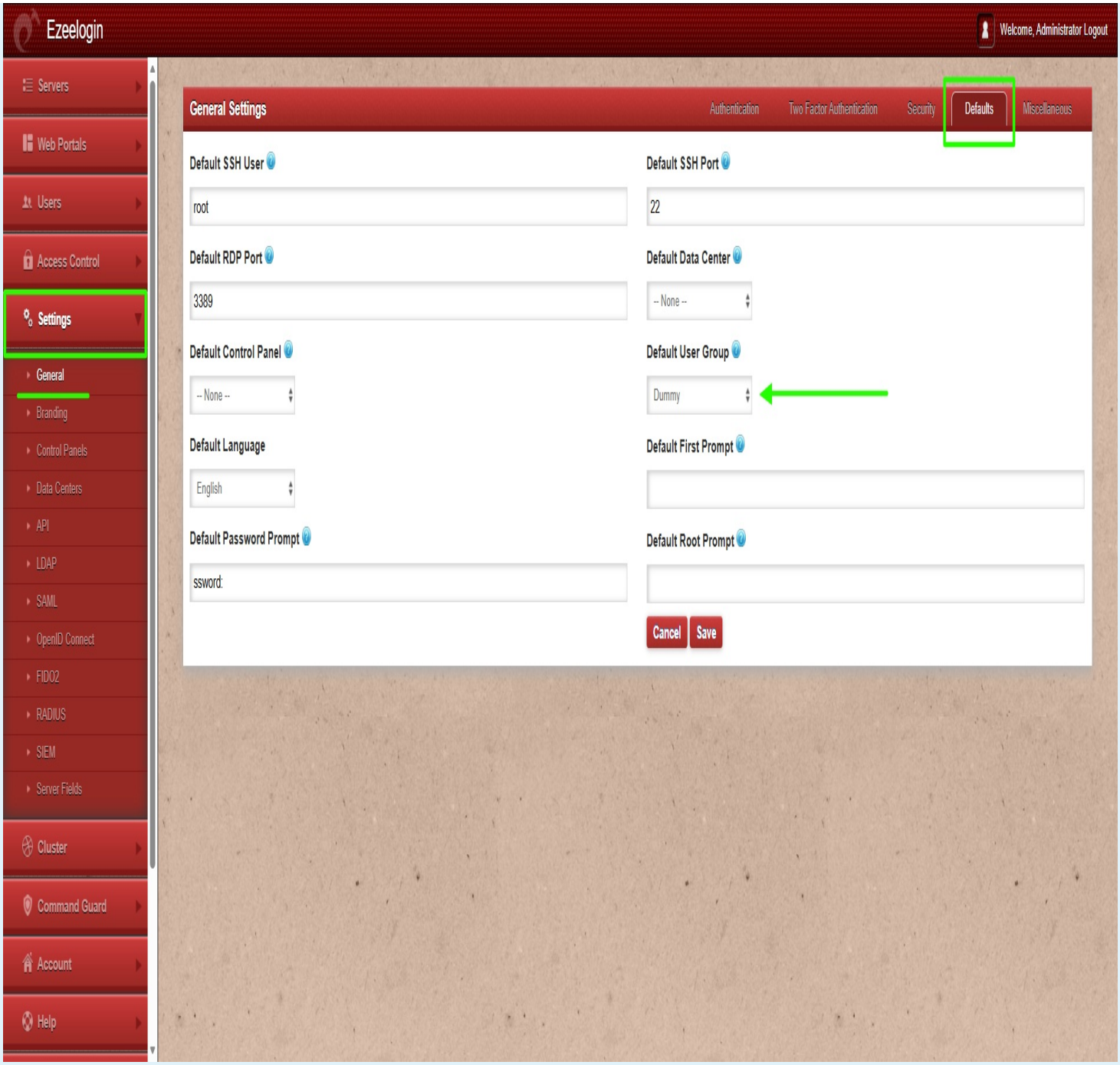
How to map Okta users to the same user group in Ezeelogin?

Note:

1. If users from the OIDC provider need to be auto-created in the corresponding group from OIDC to the same group in Ezeelogin, the admin user must set the default user group to None. If the same group is not present in Ezeelogin, the user will not be auto-created.



2. If the default user group is set to any group other than None, then all users from the OIDC provider will be auto-created in that same group.



This feature is available from Ezeelogin version 7.46.0. Refer article to upgrade Ezeelogin to the latest version.

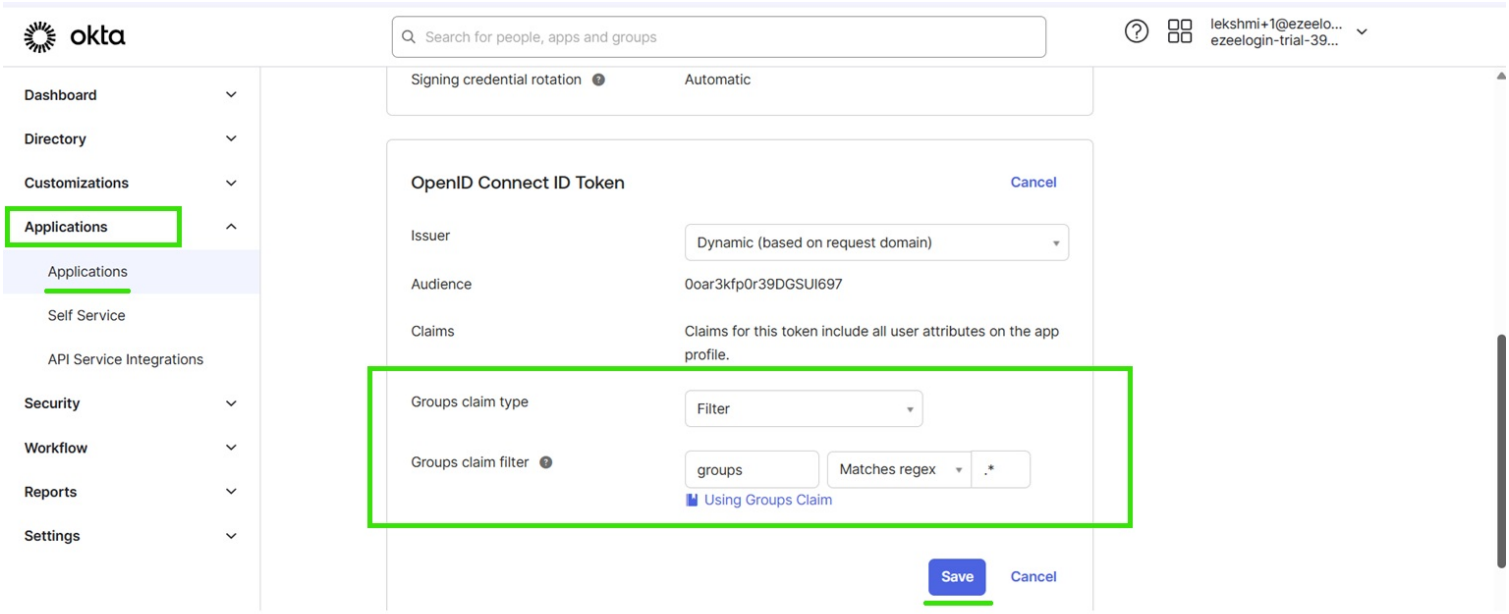
Note:

User attributes (such as groups and other mapped fields) are automatically updated in the Ezeelogin GUI when a user authenticates again. **If any attribute of an existing OIDC user is changed in the identity provider after the user has already logged in, the change will appear in the GUI only after the user logs out and logs back in.**

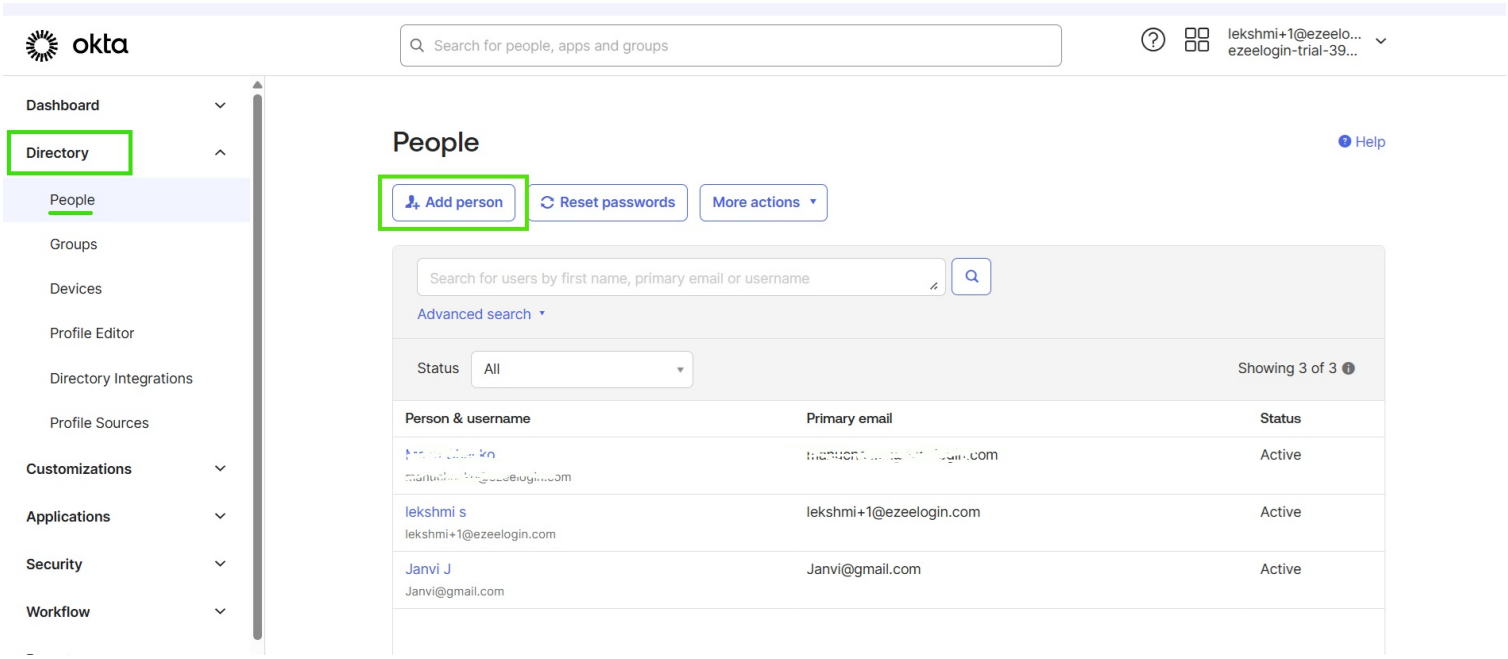
For example, if a user is moved to a different group in the OIDC provider (such as Okta), the updated group will be shown in the Ezeelogin GUI after the user logs in again.

This feature is available from Ezeelogin version 7.46.0. Refer article to upgrade Ezeelogin to the latest version.

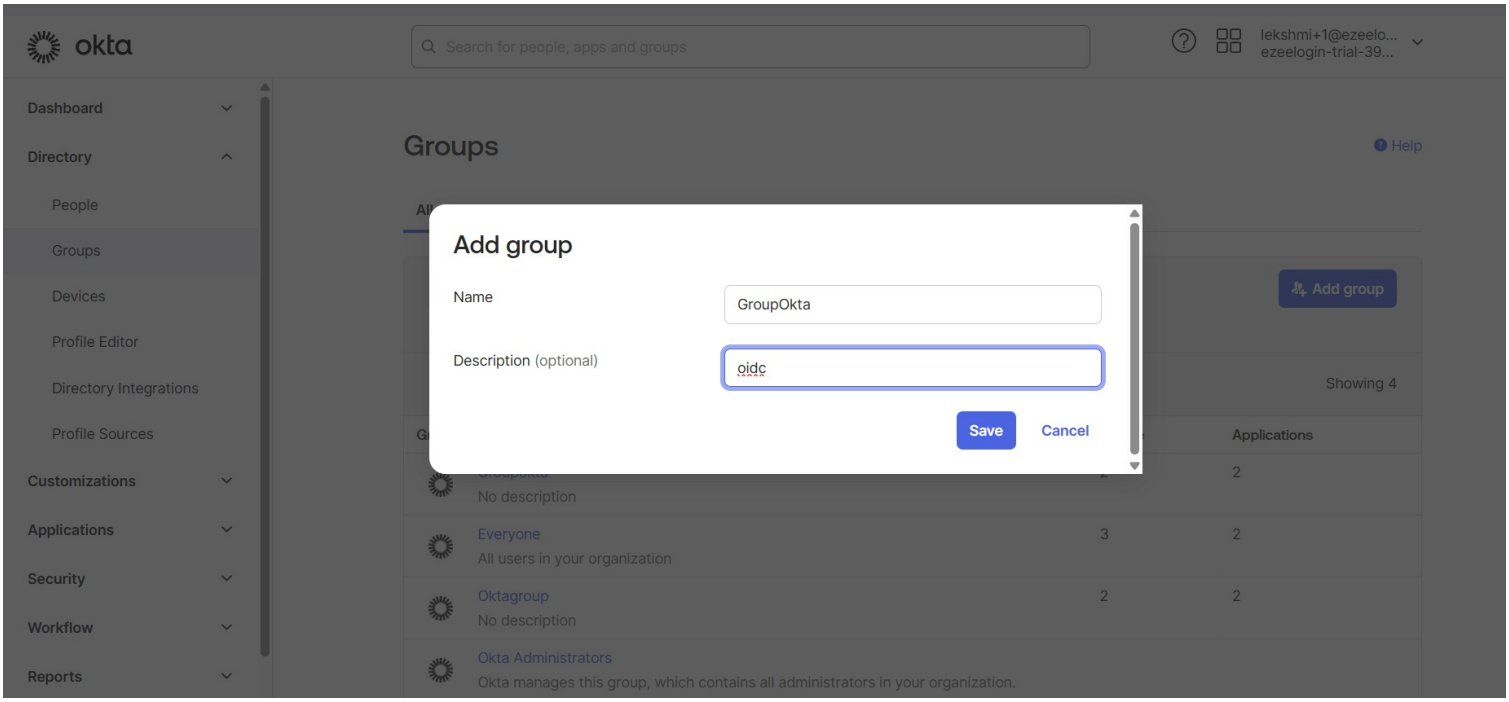
Step 1: Go to the OpenID application and open the Sign On tab. Scroll down to the OpenID Connect ID Token section and click Edit. Set Groups claim type to Filter.
Under Groups claim filter: In the first field, enter the claim name (e.g groups) and in the second field, choose Matches regex and enter **.*** to include all group information. Save the changes.



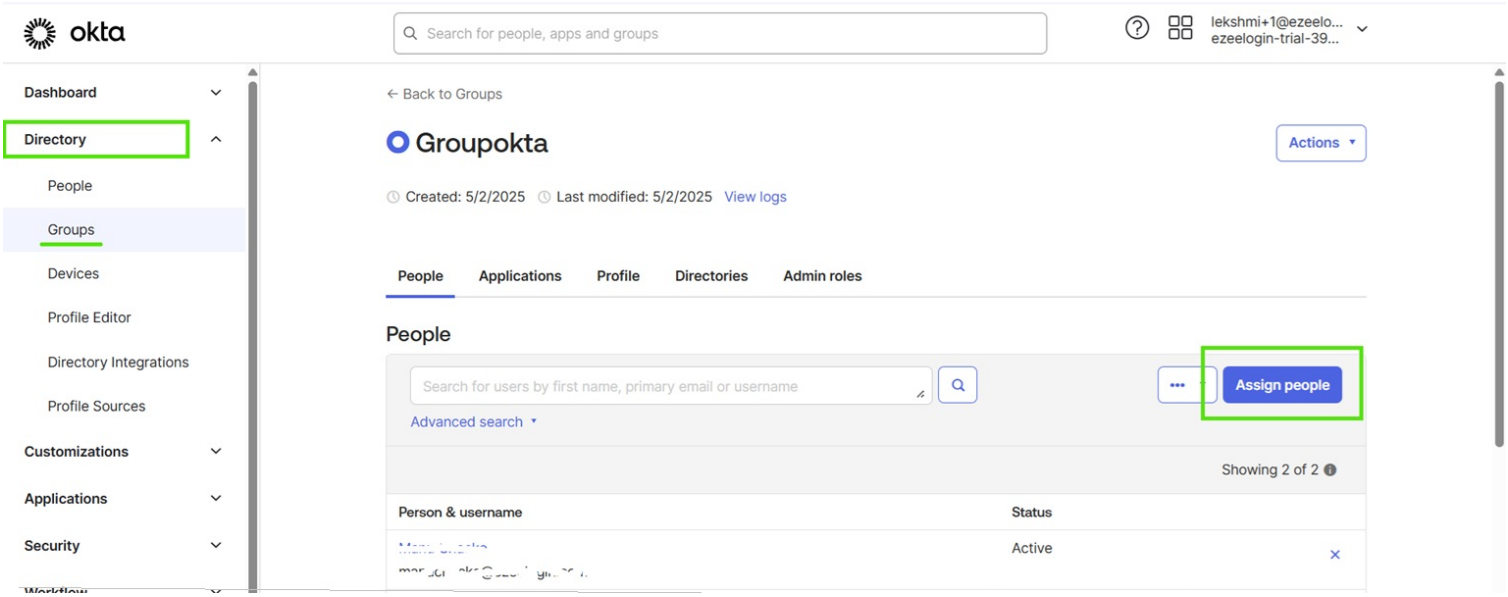
Step 2: Create user in okta . Go to **Directory -> People -> add person**



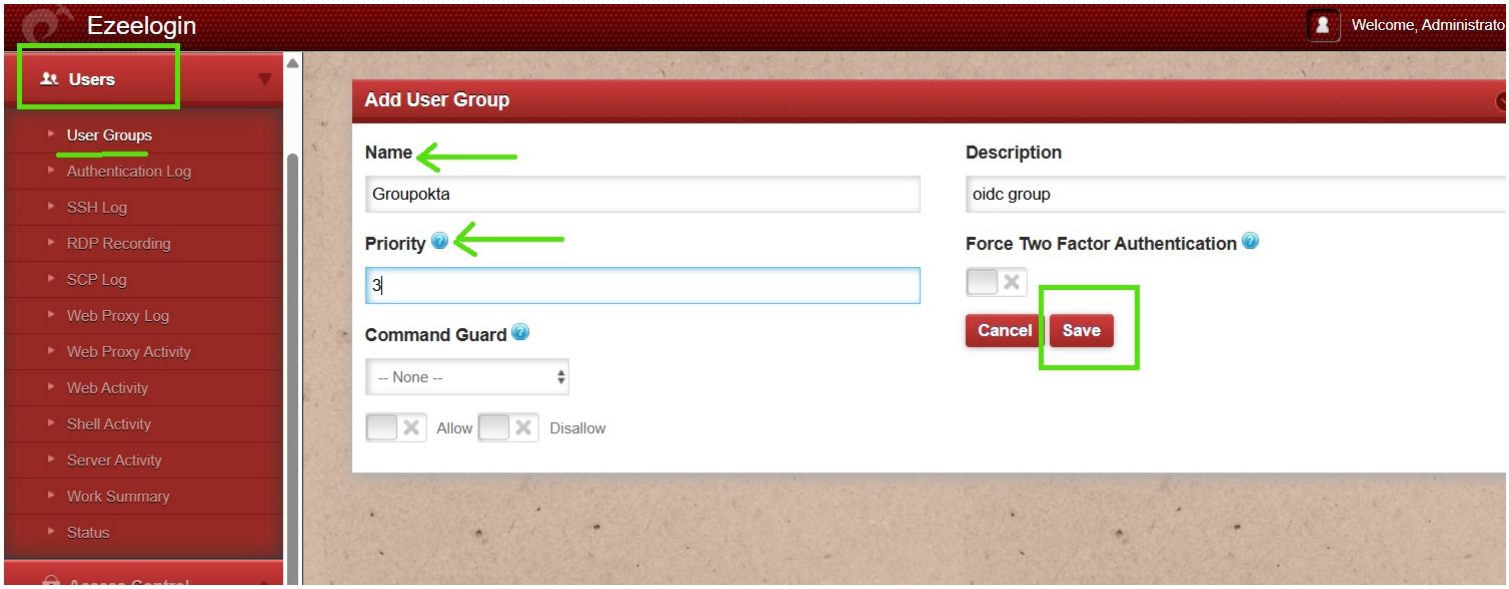
Step 3: Add group and assign the user to that group



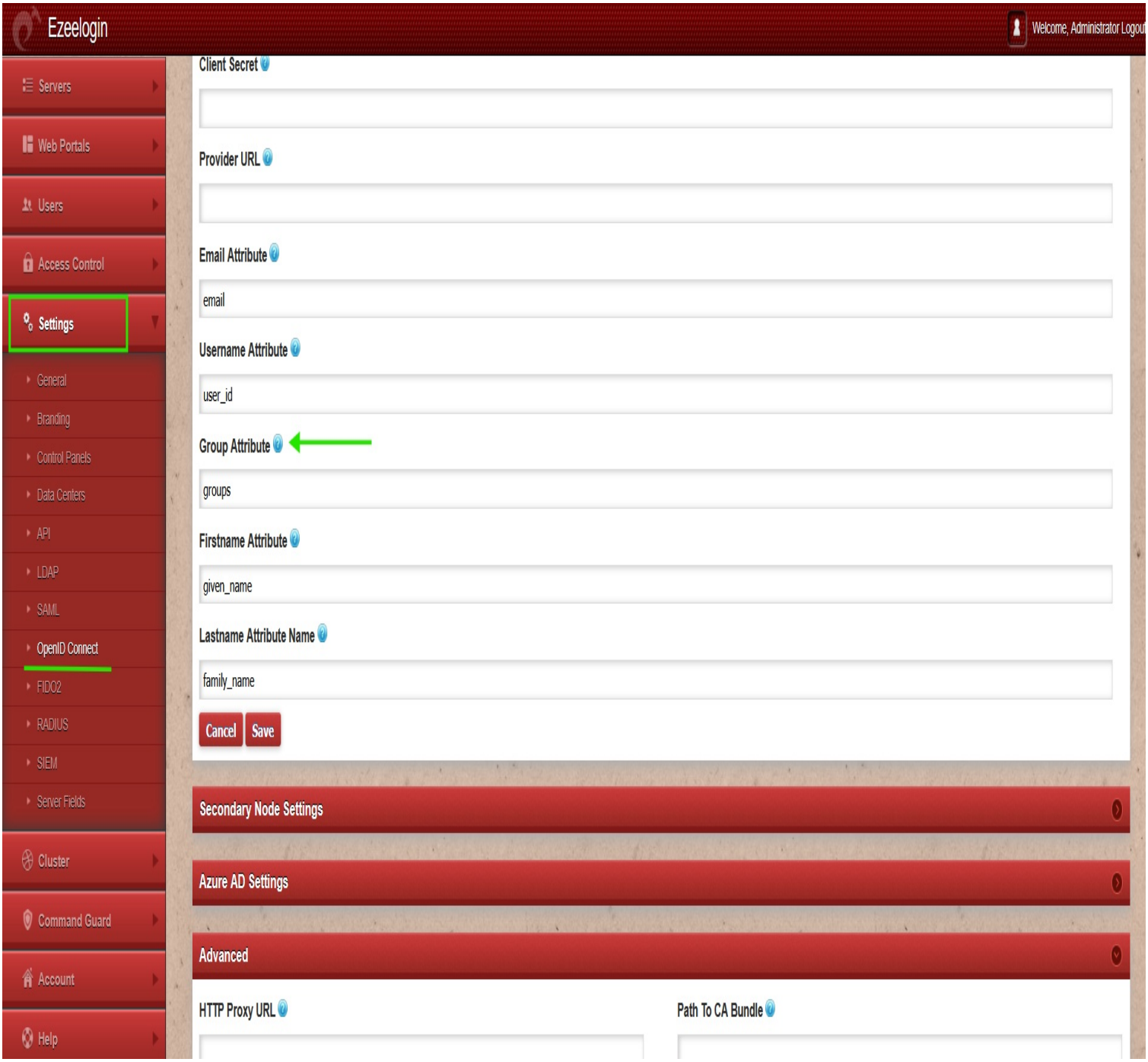
Step 3 A: Click on **Directory -> Groups -> Assign people**

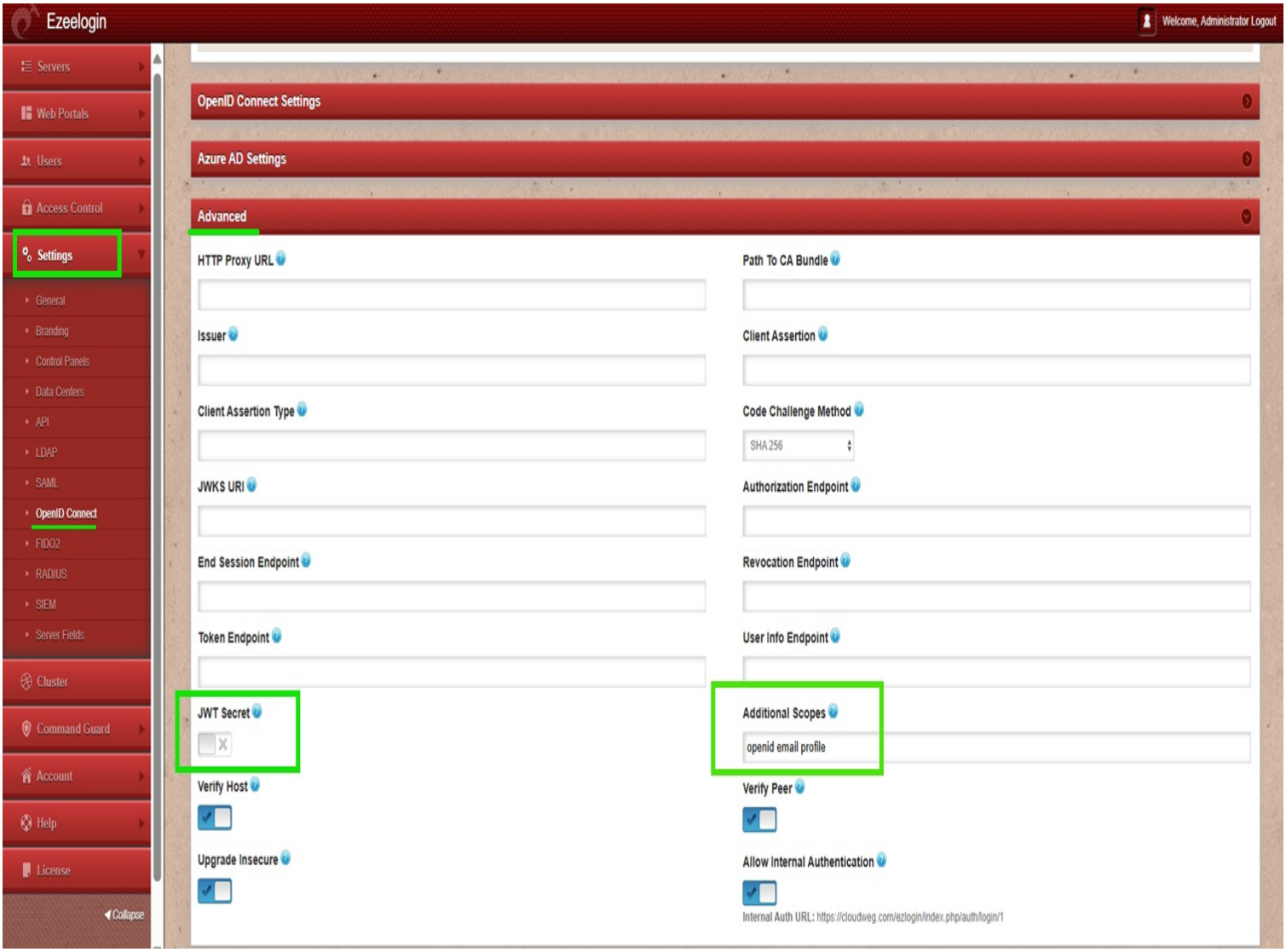


Step 4: Create the same group in gateway server with priority and save it.

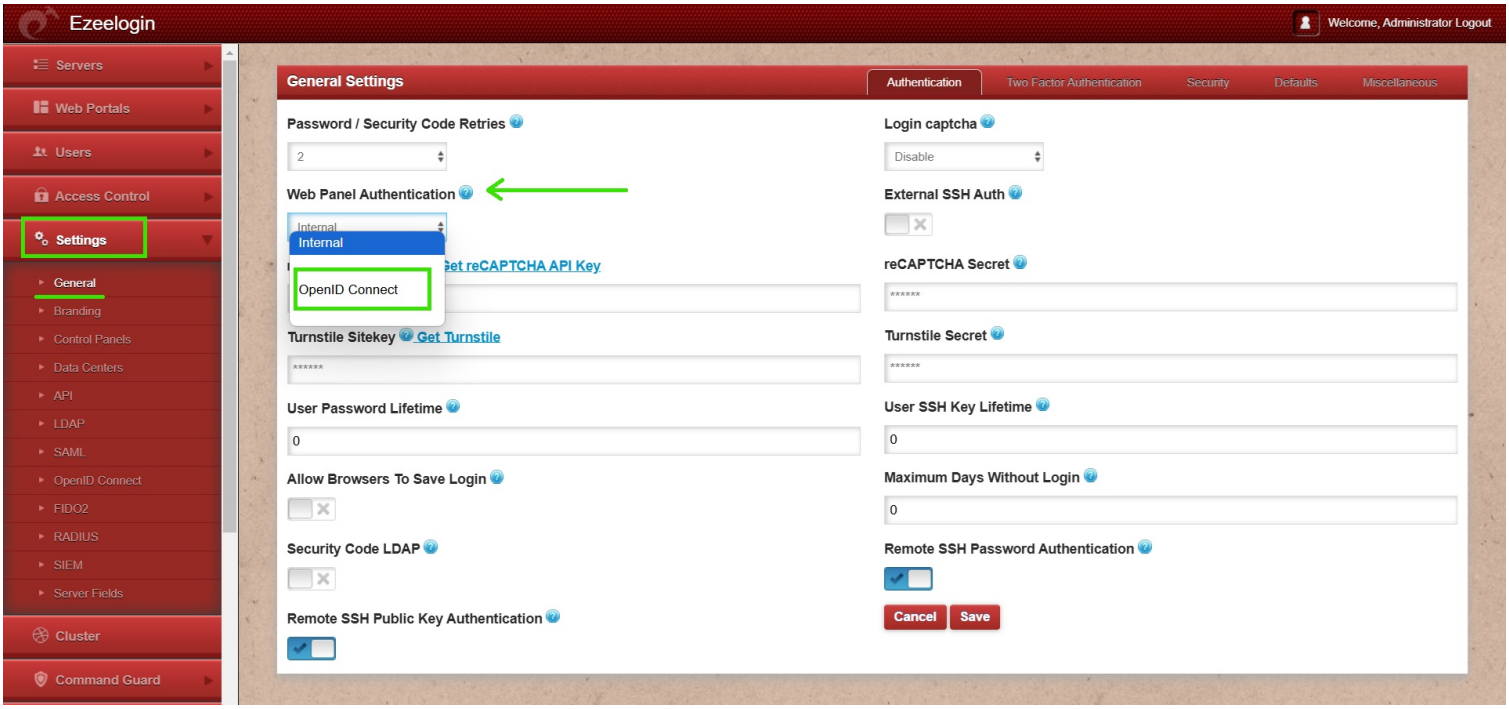


Step 5: In the Ezeelogin web interface, go to **Settings -> OpenID Connect**, add the group attribute name(here groups), specify Additional Scopes and also Disbale JWT Secret and save.

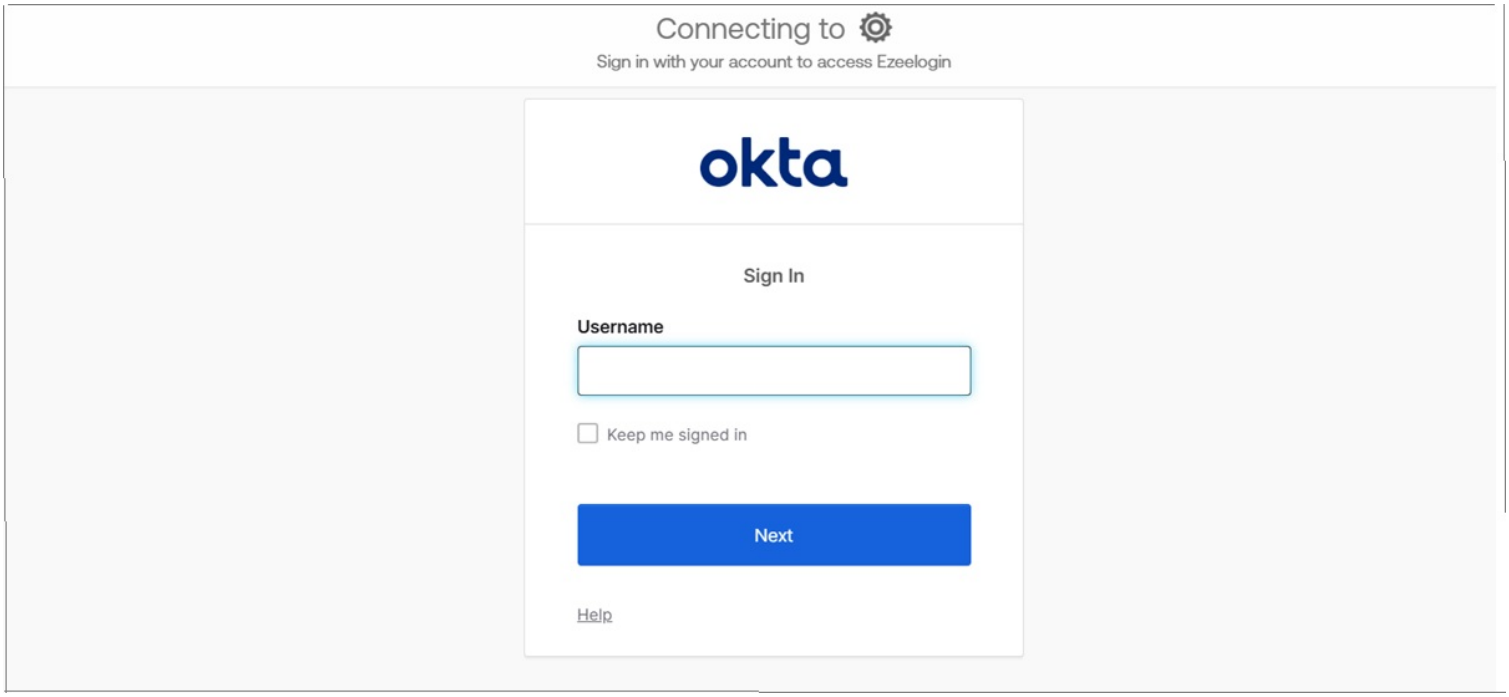


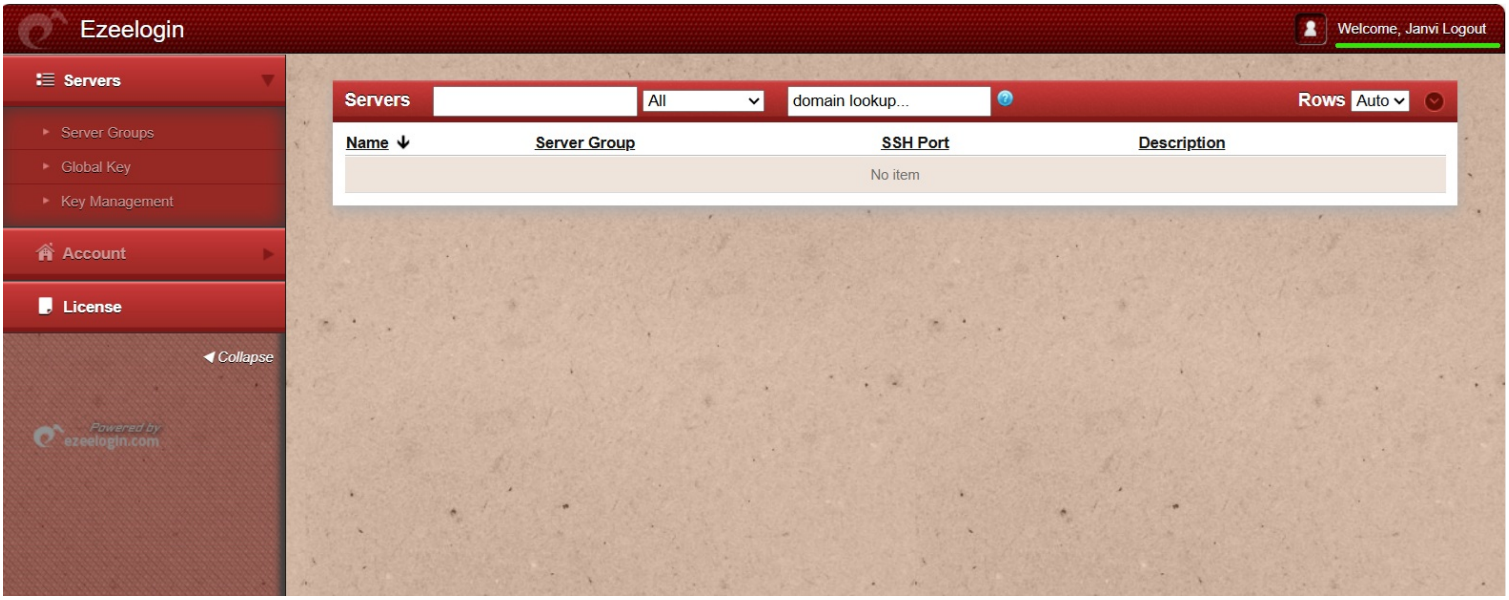


Step 6: Go to **Settings -> General ->** then **change Web Panel Authentication to OpenID Connect.**

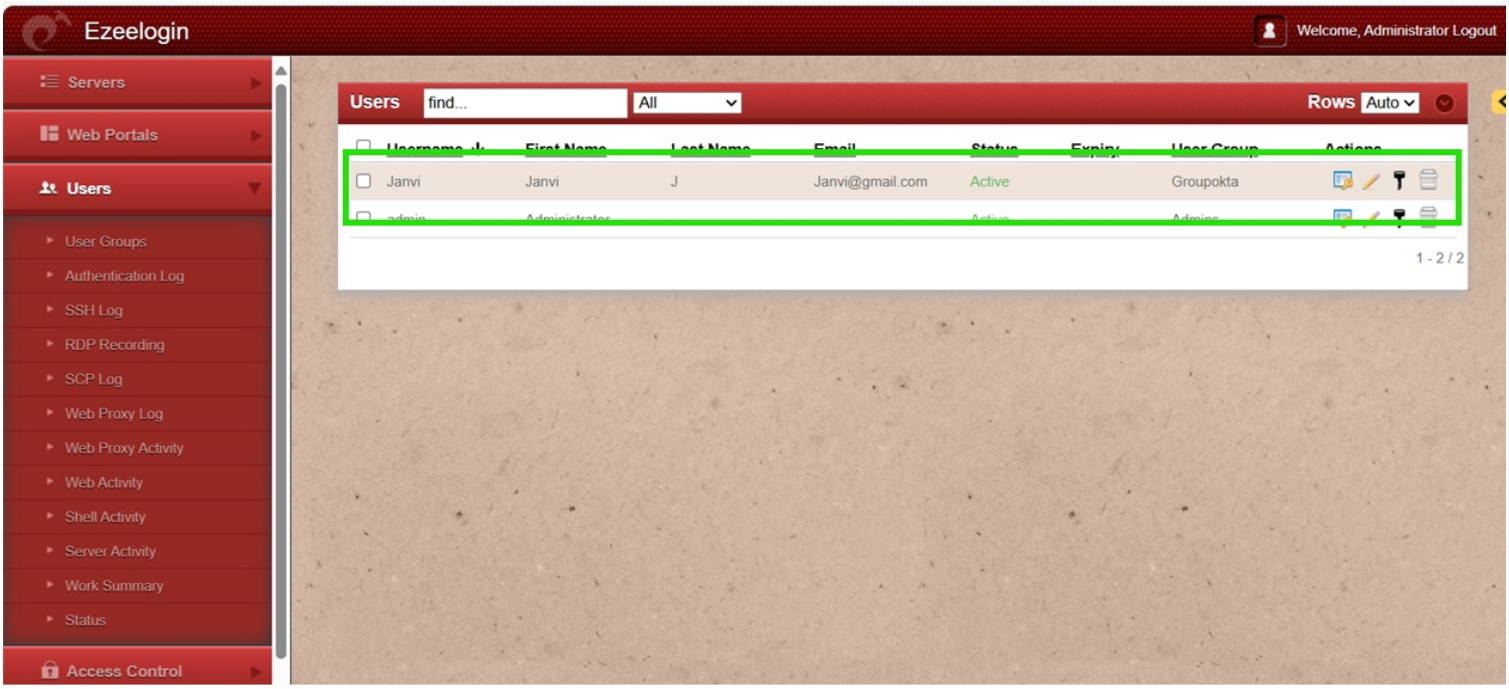


Step 7: Access the Ezeelogin GUI again using OpenID Connect based login and ensure the user is mapped to the corresponding group in Ezeelogin that matches their group in Okta.





The screenshot below shows that the user created in Okta (in this case, Janvi) is assigned to the same group in Ezeelogin as in Okta.



This feature is available from **Ezeelogin version 7.41.0**. Refer article to upgrade Ezeelogin to the latest version.

Related Articles:

Integrate Okta SSO with jumpserver