

Integrate Okta OpenID connect

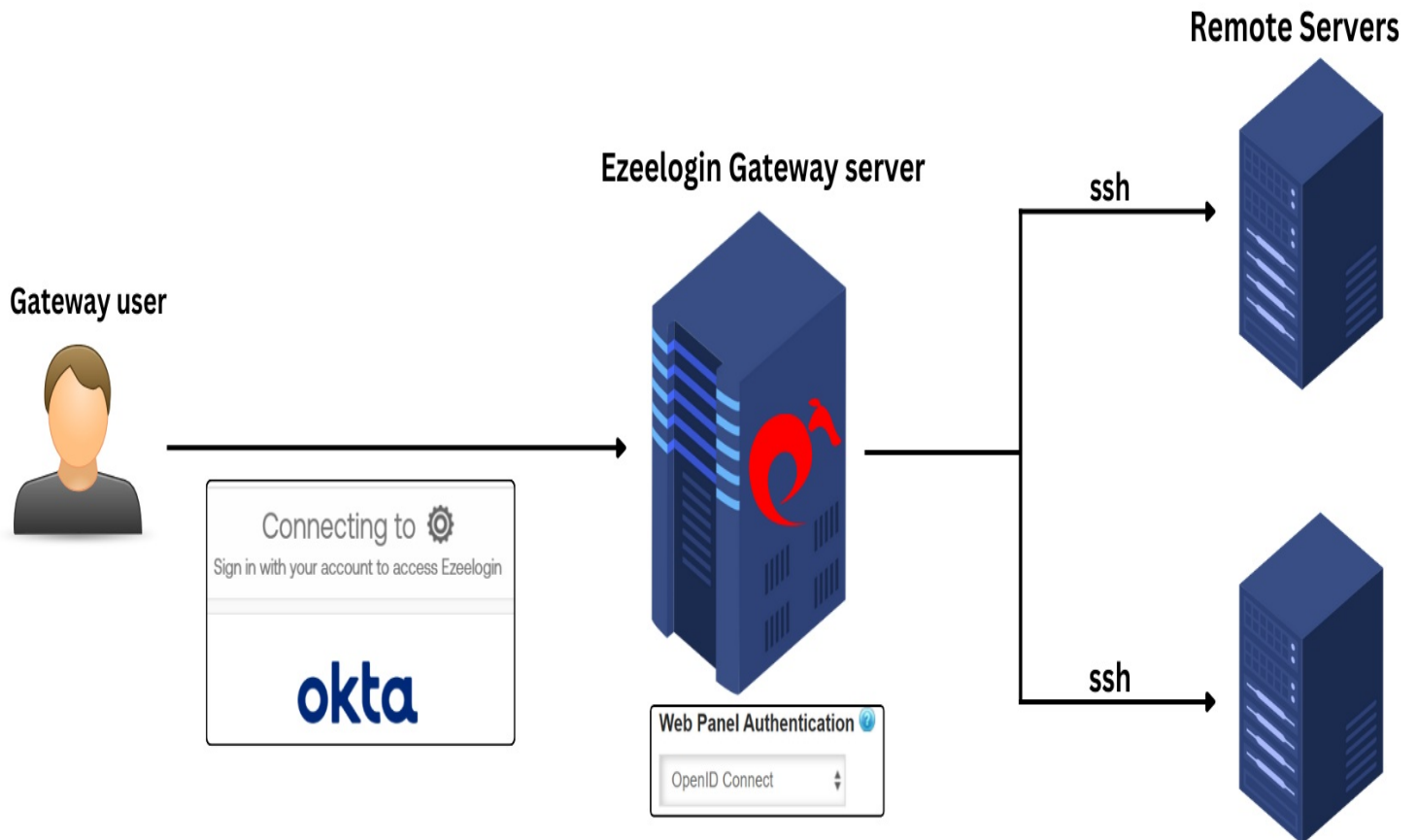
771 Lekshmi May 28, 2026 Features & Functionalities

3224

How to integrate Okta OpenID connect with Ezeelogin

Overview: This article will help 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**.

Dashboard

Directory

Customizations

Applications

Applications

Self Service

API Service Integrations

Security

Workflow

Reports

Settings

Applications

Create App Integration Browse App Catalog Assign Users to App More

Search

STATUS		
ACTIVE	2	Okta Admin Console
INACTIVE	2	Okta Browser Plugin
		Okta Dashboard

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

Sign-in method

[Learn More](#)

☒ **OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

☐ **SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

☐ **SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

☐ **API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Application type

What kind of application are you trying to integrate with Okta?

Specifying an application type customizes your experience and provides the best configuration, SDK, and sample recommendations.

☒ **Web Application**
Server-side applications where authentication and tokens are handled on the server (for example, Go, Java, ASP.Net, Node.js, PHP)

☐ **Single-Page Application**
Single-page web applications that run in the browser where the client receives tokens (for example, Javascript, Angular, React, Vue)

☐ **Native Application**
Desktop or mobile applications that run natively on a device and redirect users to a non-HTTP callback (for example, iOS, Android, React Native)

Cancel Next

Step 3: Enter the app integration name.

Search for people, apps and groups

Dashboard

Directory

Customizations

Applications

Security

Workflow

Reports

Settings

New Web App Integration

General Settings

App integration name

Ezlogin

Logo (Optional)

Proof of possession

☐ Require Demonstrating Proof of Possession (DPoP) header in token requests

Grant type

Client acting on behalf of itself

☐ Client Credentials

Core grants

☒ Authorization Code☐ Refresh Token

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**.

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

OpenID Connect Client Info

Redirect URL

https://cloudweg.com/ezlogin/index.php/auth/oidc

OpenID Connect Settings

Client ID

Client Secret

Provider URL

Email Attribute

email

Username Attribute

nickname

Group Attribute

Firstname Attribute



?

lekshmi@ezeelogi...
ezeelogin-trial-77...

Dashboard

Directory

Customizations

Applications

Security

Workflow

Reports

Settings

Advanced

Sign-in redirect URIs

☐ Allow wildcard * in sign-in URI redirect.

x

Okta sends the authentication response and ID token for the user's sign-in request to these URIs

[Learn More](#)

+ Add URI

Sign-out redirect URIs (Optional)

x

After your application contacts Okta to close the user session, Okta redirects the user to one of these URIs.

+ Add URI

[Learn More](#)

Trusted Origins

Base URIs (Optional)

x

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In

+ Add URI



?

lekshmi@ezeelogi...
ezeelogin-trial-77...

Dashboard

Directory

Customizations

Applications

Security

Workflow

Reports

Settings

Base URIs (Optional)

x

Required if you plan to self-host the Okta Sign-In Widget. With a Trusted Origin set, the Sign-In Widget can make calls to the authentication API from this domain.

+ Add URI

[Learn More](#)

Assignments

Controlled access

☐ Allow everyone in your organization to access

☐ Limit access to selected groups

☐ Skip group assignment for now

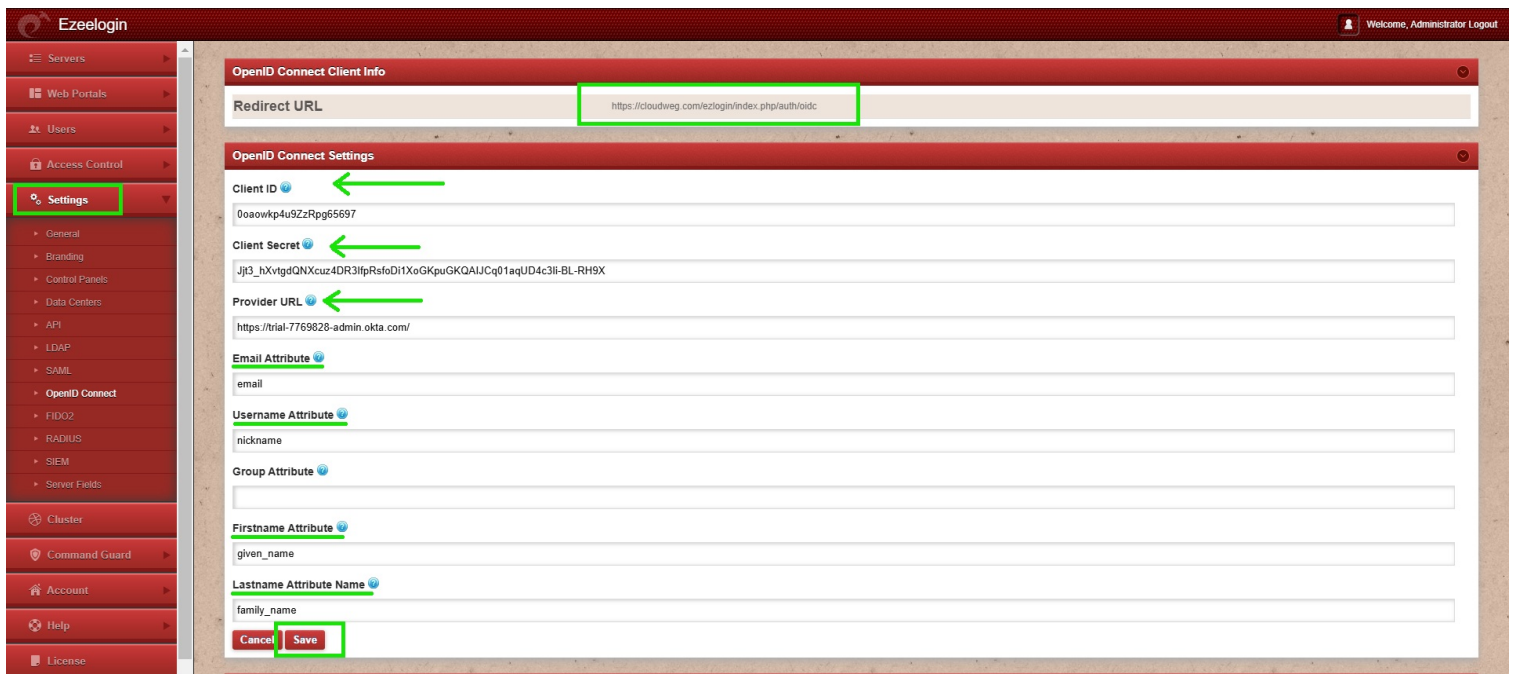
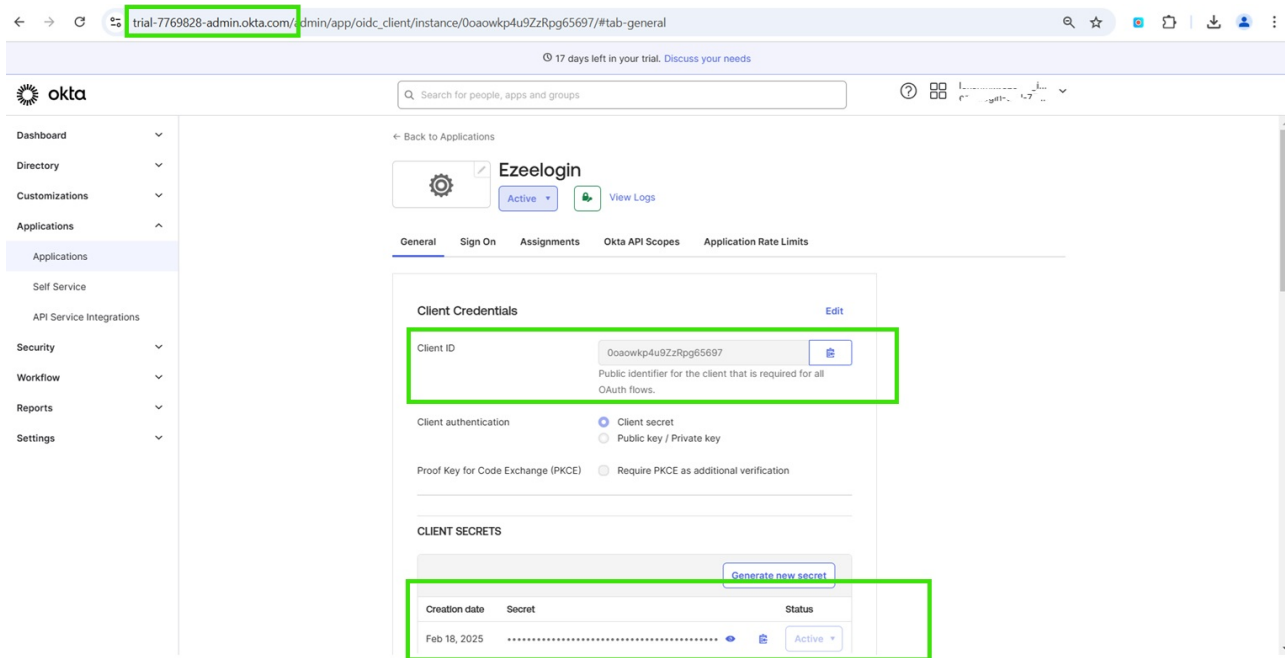
Select whether to assign the app integration to everyone in your org, only selected group(s), or skip assignment until after app creation.

Save

Cancel

© 2025 Okta, Inc. Privacy Status site OK14 US Cell Version 2025.02.2 E Download Okta Plugin Feedback

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.

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_XvtdgQNZxua4DR3lfpRsoDl1XoGKpuQKA0JlCqf2aUD4c3i-BL-RH9Y

HTTP Proxy URL

Path To CA Bundle

Azure AD Settings

Advanced

Firstname Attribute

given_name

Lastname Attribute Name

family_name

Cancel

Save

Secondary Node Settings

Client ID

0b9wkp4u93zRpg6581

Client Secret

Hk7s_XvtdgQNZxua4DR3lfpRsoDl1XoGKpuQKA0JlCqf2aUD4c3i-BL-RH9Y

HTTP Proxy URL

Path To CA Bundle

Azure AD Settings

Advanced

OpenID Connect Settings

Azure AD Settings

Advanced

HTTP Proxy URL

Issuer

Client Assertion Type

JWKS URI

End Session Endpoint

Token Endpoint

JWT Secret

Verify Host

Upgrade Insecure

Path To CA Bundle

Client Assertion

Code Challenge Method

Authorization Endpoint

Revocation Endpoint

User Info Endpoint

Additional Scopes

Verify Peer

Allow Internal Authentication

Internal Auth URL: https://cloudweg.com/ezelogin/index.php/auth/login/1

Firstname Attribute

given_name

Lastname Attribute Name

family_name

Cancel

Save

Secondary Node Settings

Client ID

0b9wkp4u93zRpg6581

Client Secret

Hk7s_XvtdgQNZxua4DR3lfpRsoDl1XoGKpuQKA0JlCqf2aUD4c3i-BL-RH9Y

HTTP Proxy URL

Path To CA Bundle

Azure AD Settings

Advanced

OpenID Connect Settings

Azure AD Settings

Advanced

HTTP Proxy URL

Issuer

Client Assertion Type

JWKS URI

End Session Endpoint

Token Endpoint

JWT Secret

Verify Host

Upgrade Insecure

Path To CA Bundle

Client Assertion

Code Challenge Method

Authorization Endpoint

Revocation Endpoint

User Info Endpoint

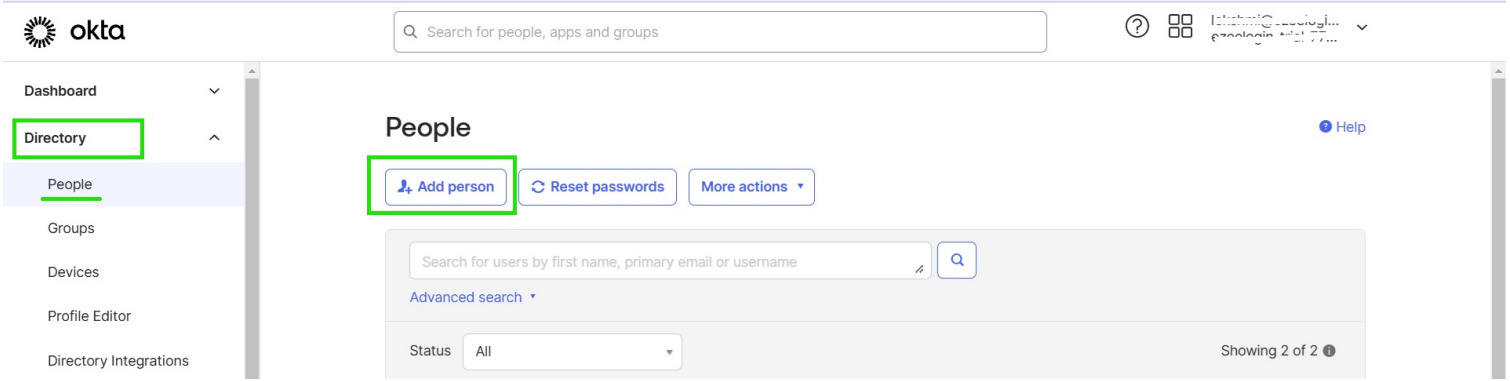
Additional Scopes

Verify Peer

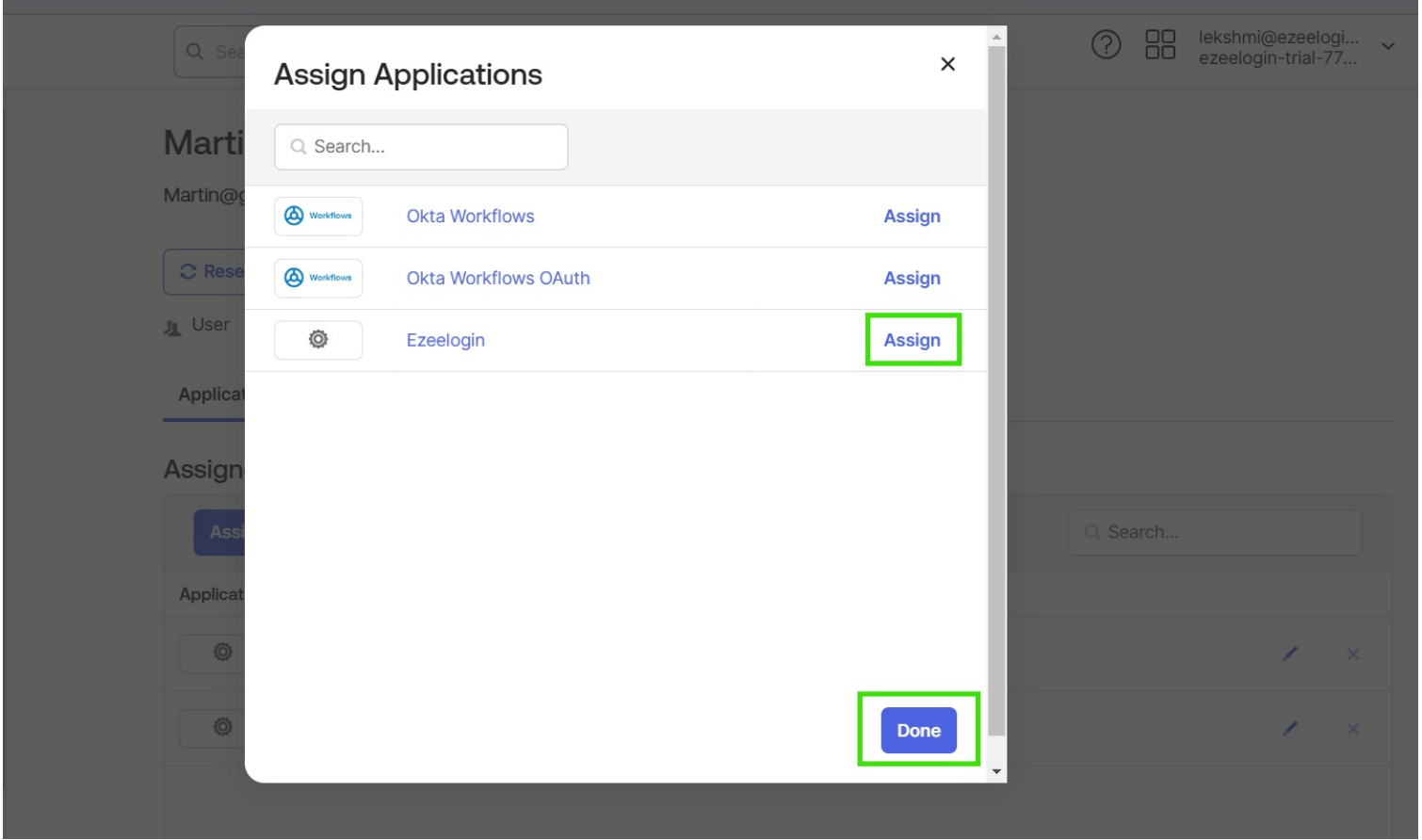
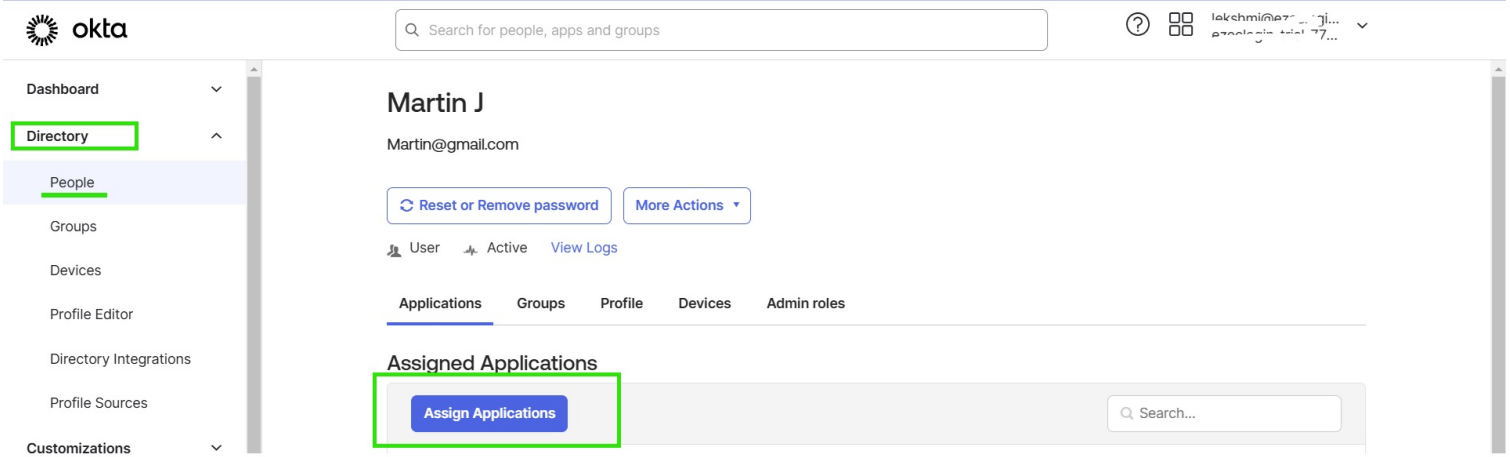
Allow Internal Authentication

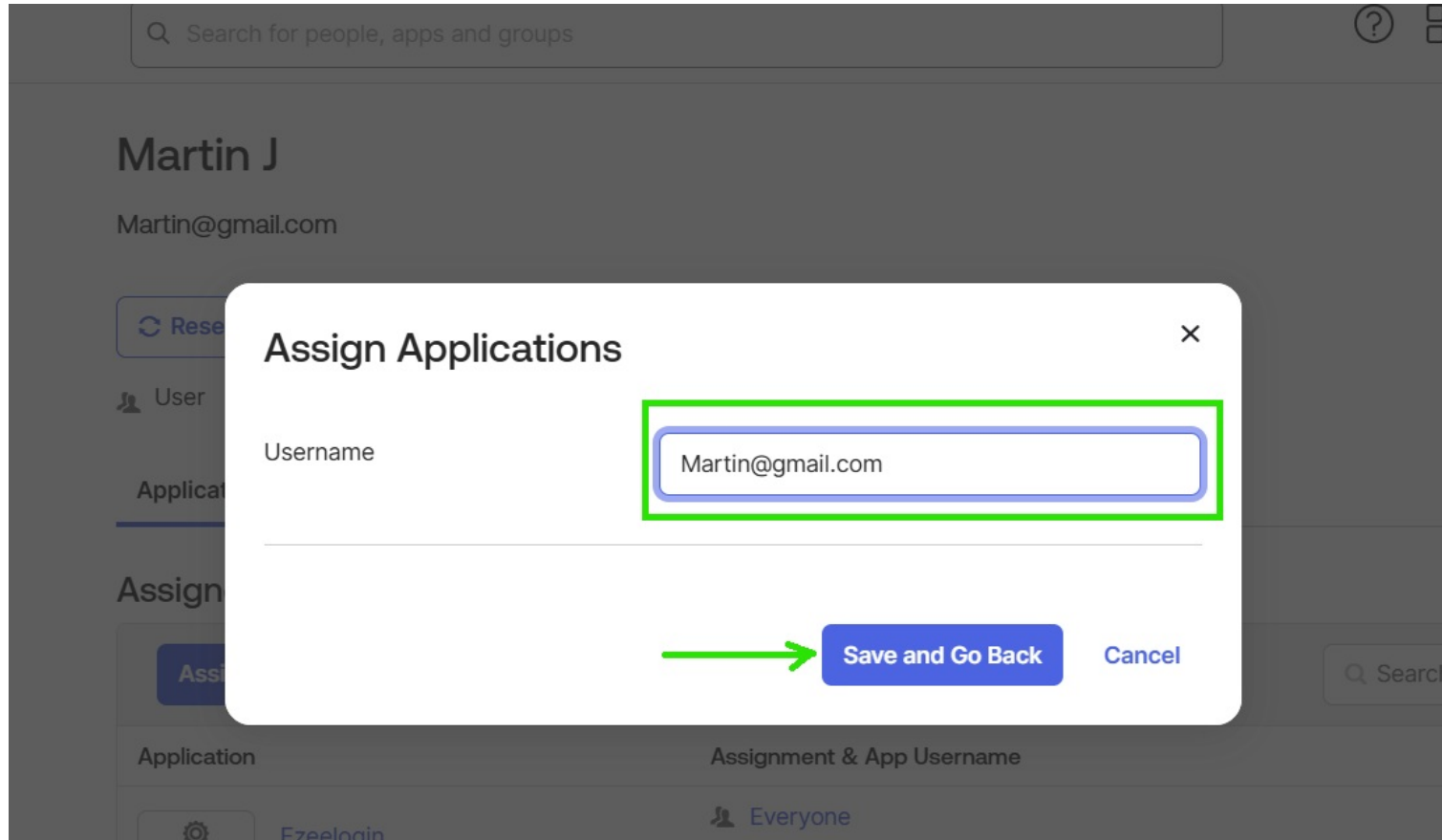
Internal Auth URL: https://cloudweg.com/ezelogin/index.php/auth/login/1

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.



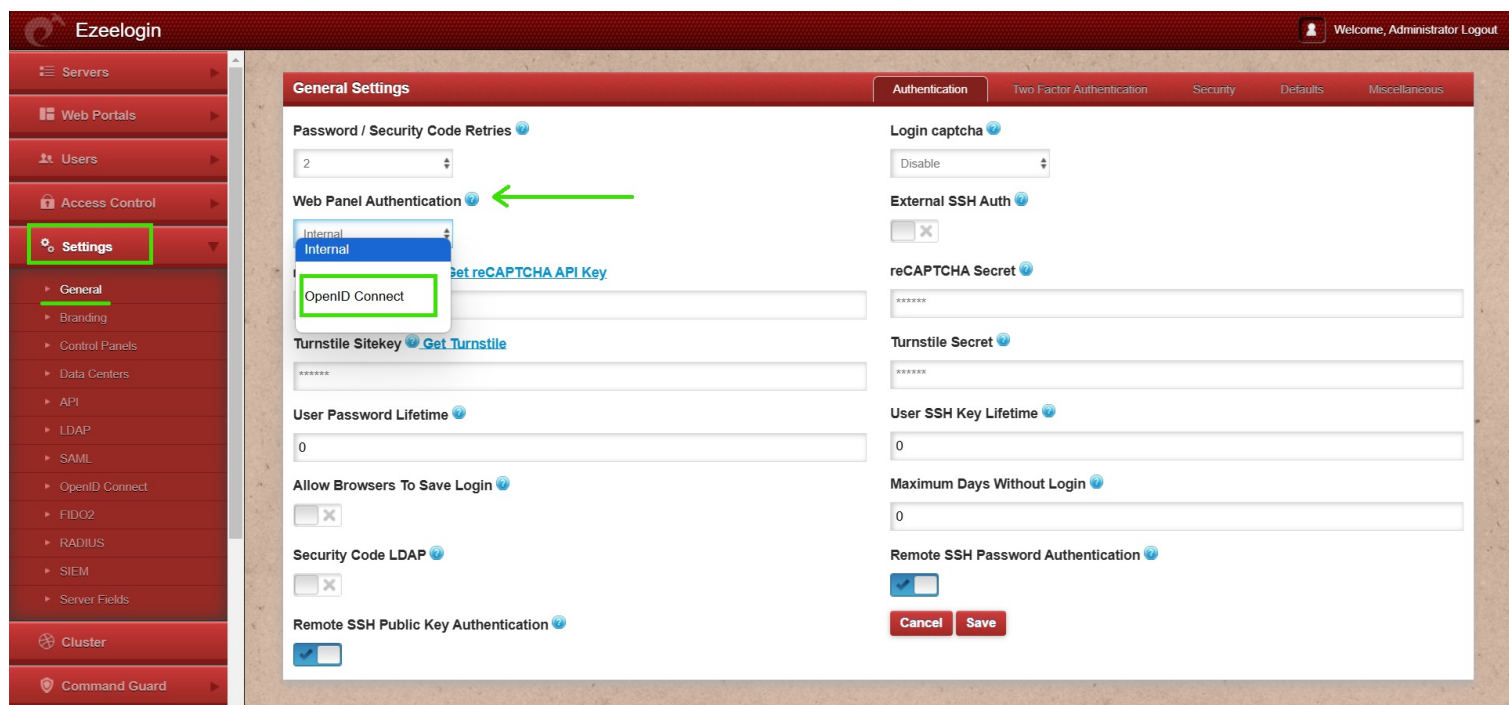
Step 7: After adding the user, navigate to the People tab and click Assign Application to assign the user to the application.



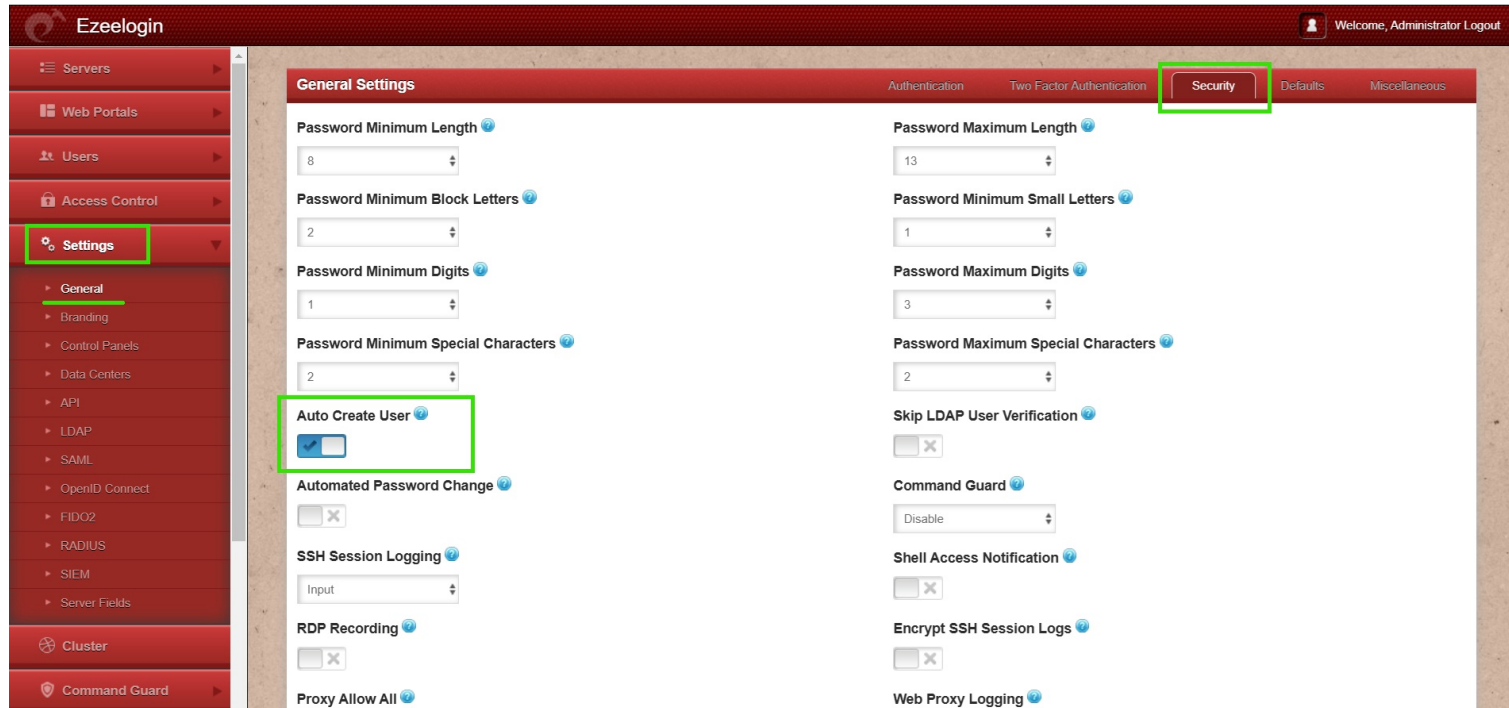


Step 8: After Login to Ezeelogin GUI and do the below steps

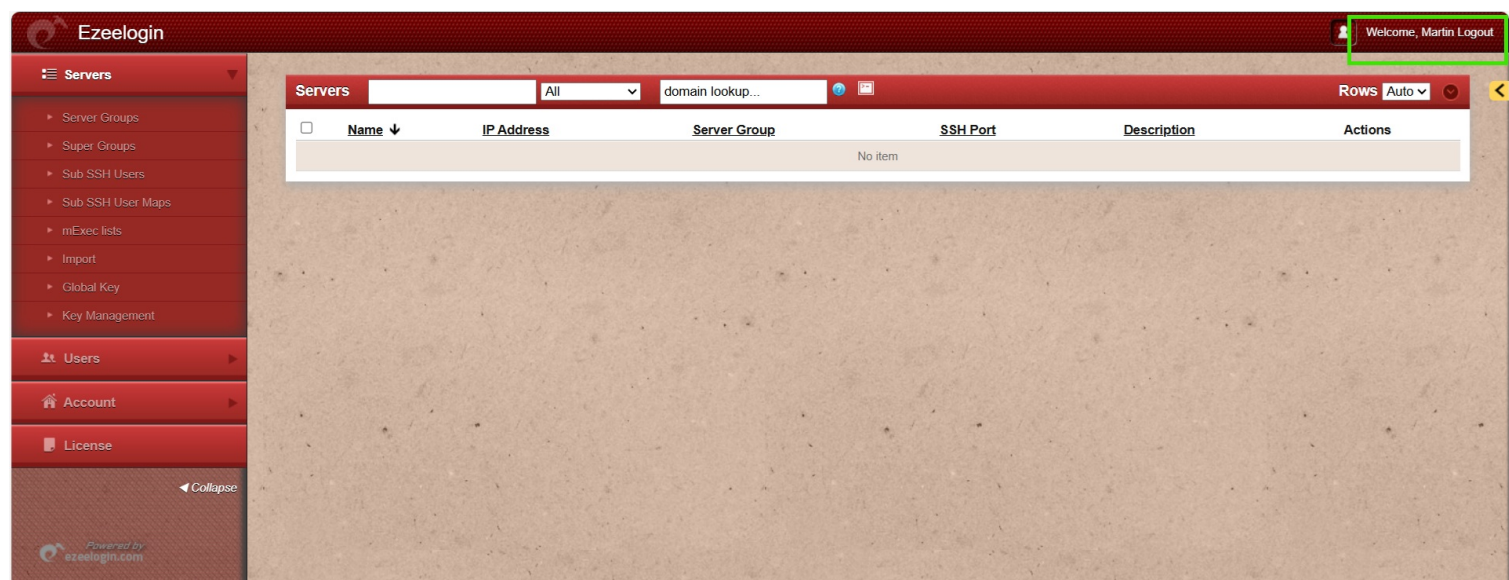
Step 8 (A): Go to **Settings -> General -> Web Panel Authentication**, then change **Web Panel Authentication** to **OpenID Connect**.



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**.

Ezeelogin Welcome, Martin Logout

Change password, security code, two factor secret

New Password **Confirm Password**

New Security Code **Generate** **Confirm Security Code**

New Access Keyword **Generate** **Confirm Access Keyword**

SSH Private Key **SSH Key Passphrase**

Cancel **Save**

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.

Ezeelogin Welcome, Martin Logout

Servers **Rows**

☐	Name ↓	IP Address	Server Group	SSH Port	Description	Actions
						No item

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.

General Settings

Authentication

Two Factor Authentication

Security

Defaults

Miscellaneous

Default SSH User ⓘ

root

Default SSH Port ⓘ

22

Default RDP Port ⓘ

3389

Default Data Center ⓘ

-- None --

Default Control Panel ⓘ

-- None --

Default User Group ⓘ

-- None --

Default Language

English

Default First Prompt ⓘ

Default Password Prompt ⓘ

ssword:

Default Root Prompt ⓘ

Cancel

Save

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.

General Settings Authentication Two Factor Authentication Security **Defaults** Miscellaneous

Default SSH User

root

Default SSH Port

22

Default RDP Port

3389

Default Data Center

-- None --

Default Control Panel

-- None --

Default User Group

Dummy

Default Language

English

Default First Prompt

Default Password Prompt

ssword:

Default Root Prompt

Cancel Save

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.

Okta

Search for people, apps and groups

lekshmi+1@ezeelo...
ezeelogin-trial-39...

Signing credential rotation Automatic

OpenID Connect ID Token Cancel

Issuer Dynamic (based on request domain)

Audience 0oar3kfp0r39DGSUI697

Claims Claims for this token include all user attributes on the app profile.

Groups claim type Filter

Groups claim filter groups Matches regex .*

Using Groups Claim

Save Cancel

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

Okta

Search for people, apps and groups

lekshmi+1@ezeelo...
ezeelogin-trial-39...

People Help

Add person Reset passwords More actions

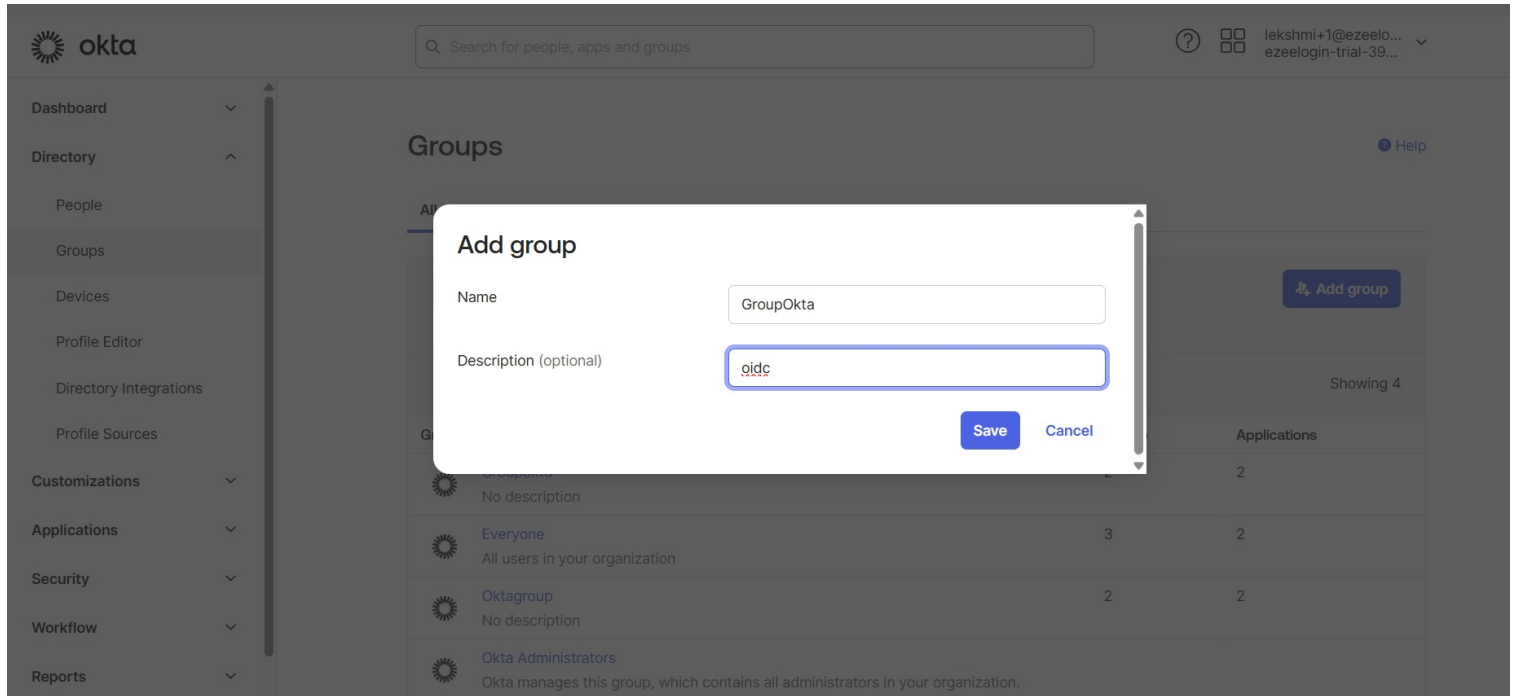
Search for users by first name, primary email or username

Advanced search

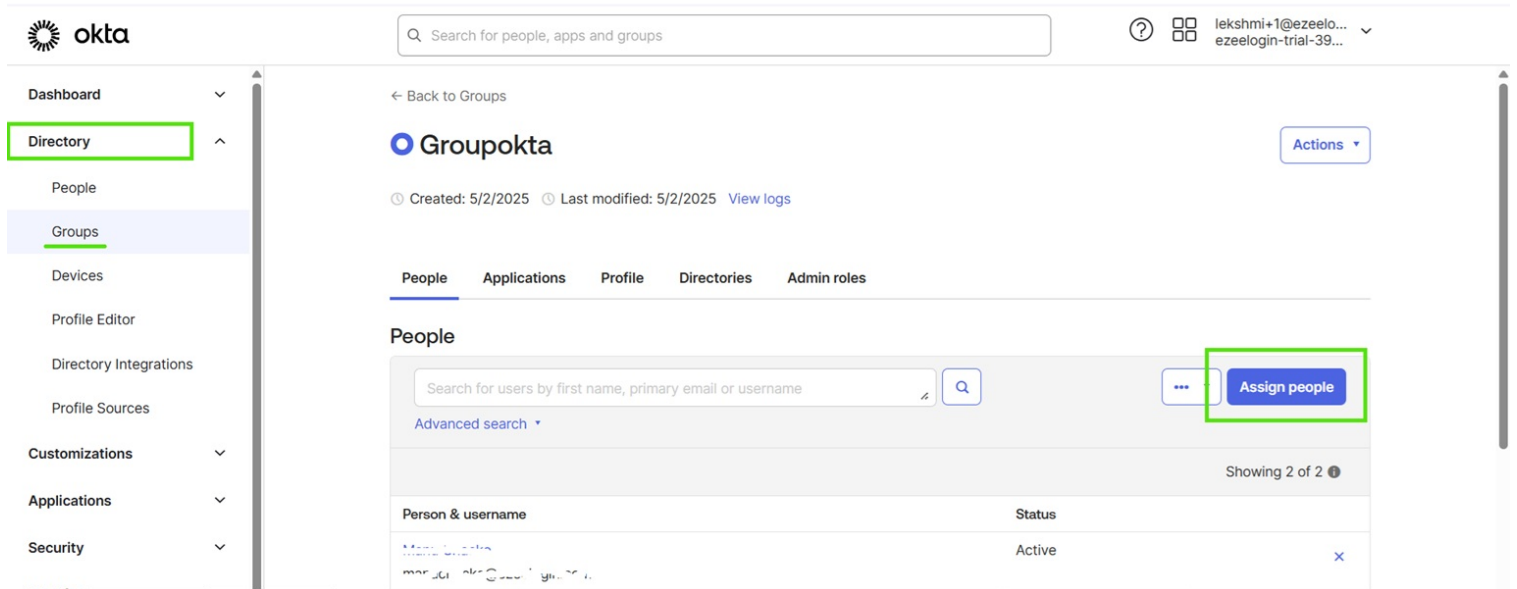
Status All Showing 3 of 3

Person & username	Primary email	Status
manu...@ezeelogin.com	manu...@ezeelogin.com	Active
lekshmi s lekshmi+1@ezeelogin.com	lekshmi+1@ezeelogin.com	Active
Janvi J Janvi@gmail.com	Janvi@gmail.com	Active

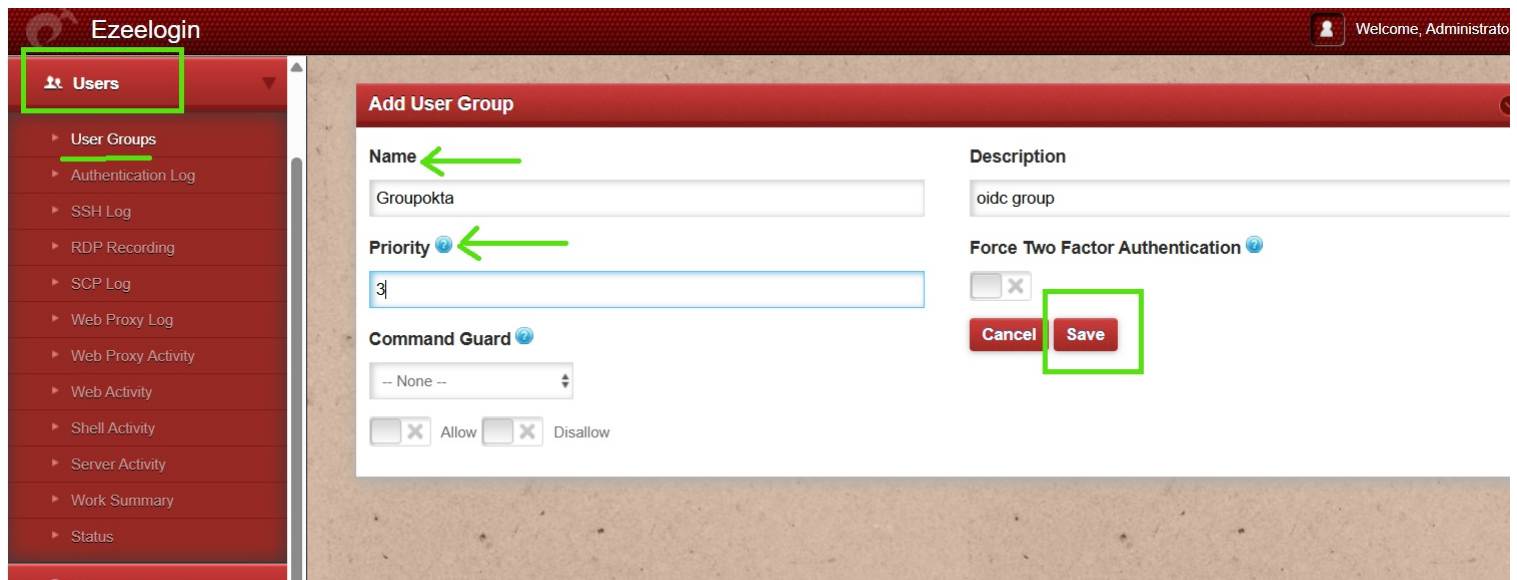
Step 3: Add group and assign the user to that group



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.

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

Account

Help

Client Secret

Provider URL

Email Attribute

email

Username Attribute

user_id

Group Attribute

groups

Firstname Attribute

given_name

Lastname Attribute Name

family_name

Cancel

Save

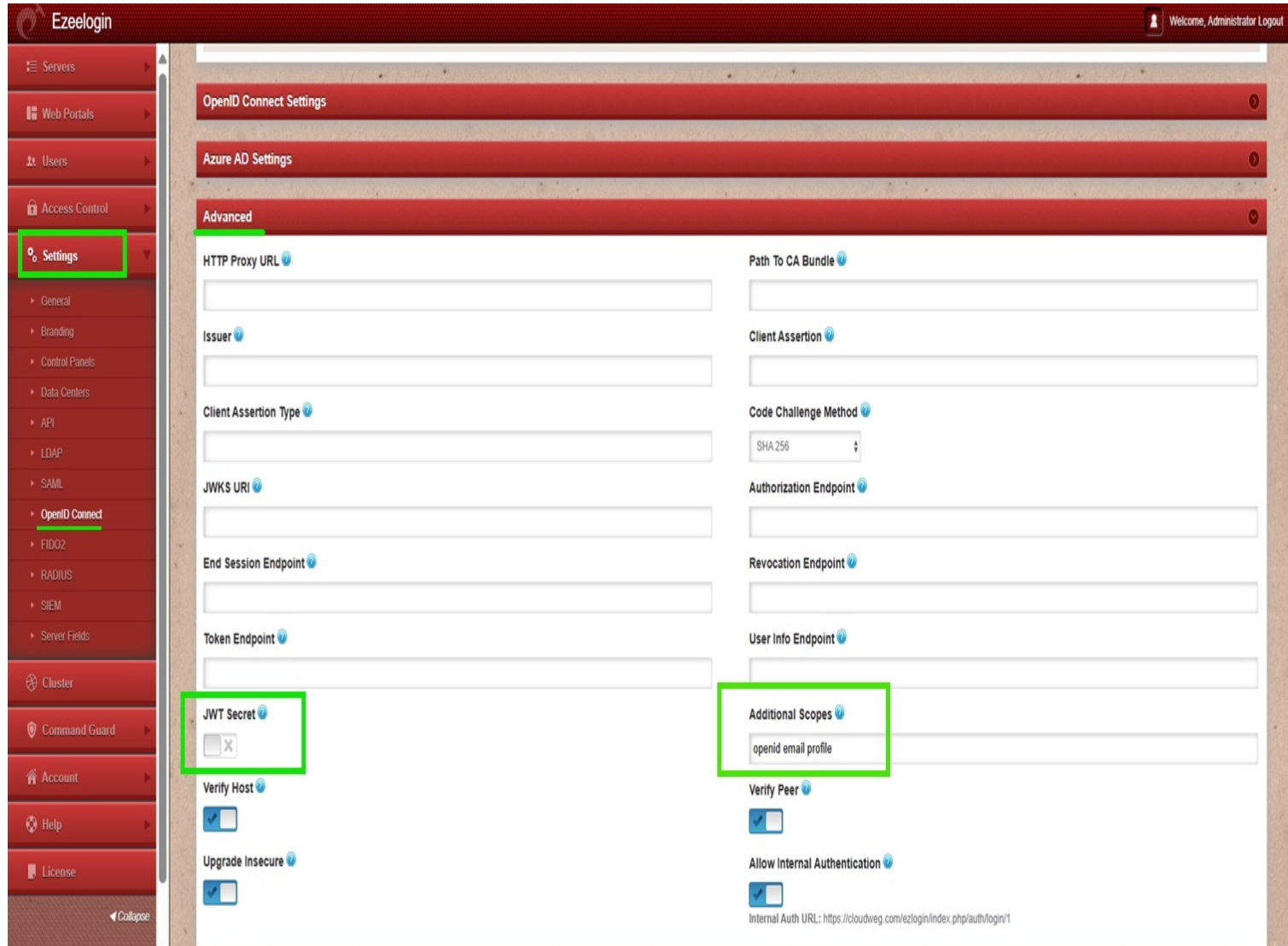
Secondary Node Settings

Azure AD Settings

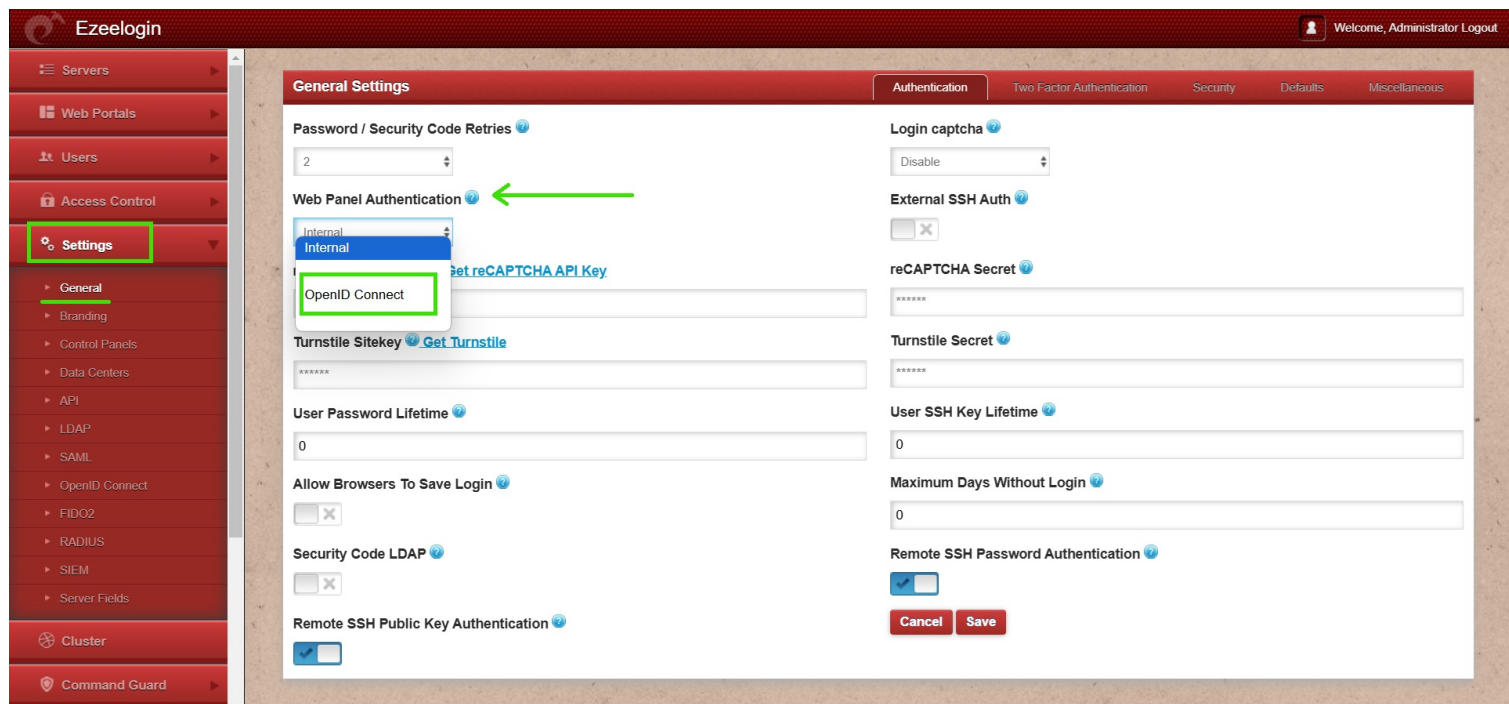
Advanced

HTTP Proxy URL

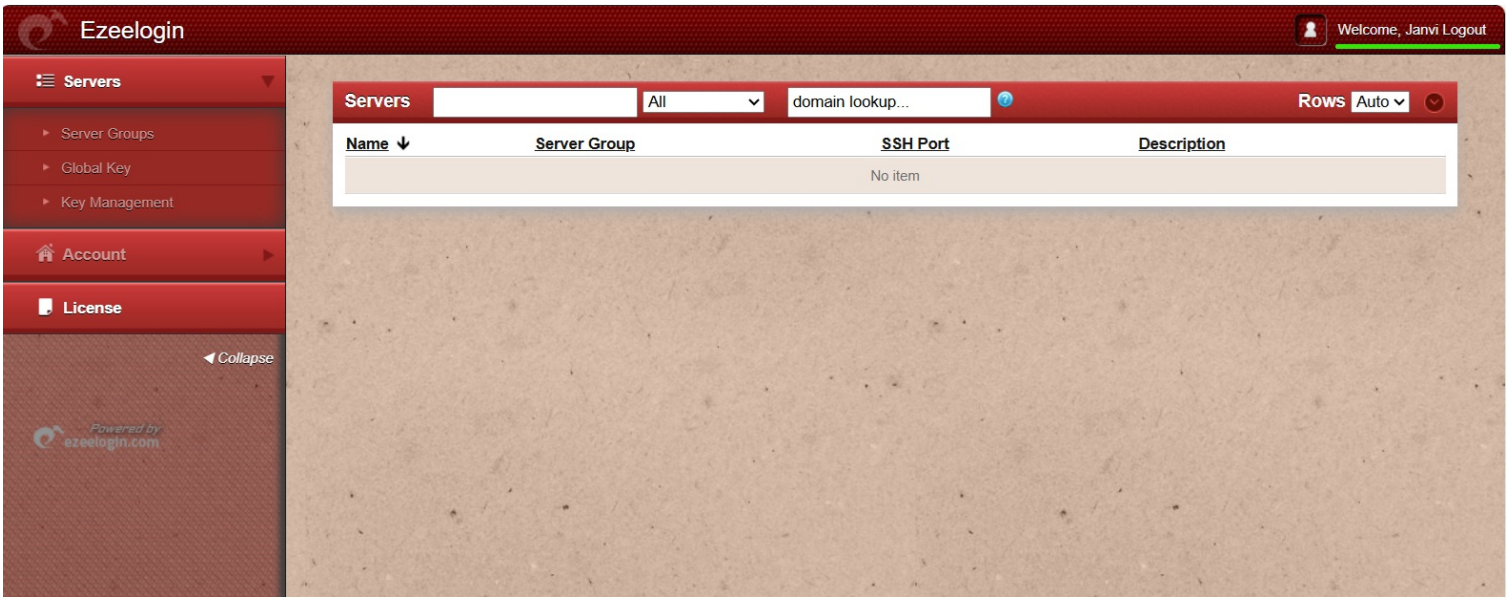
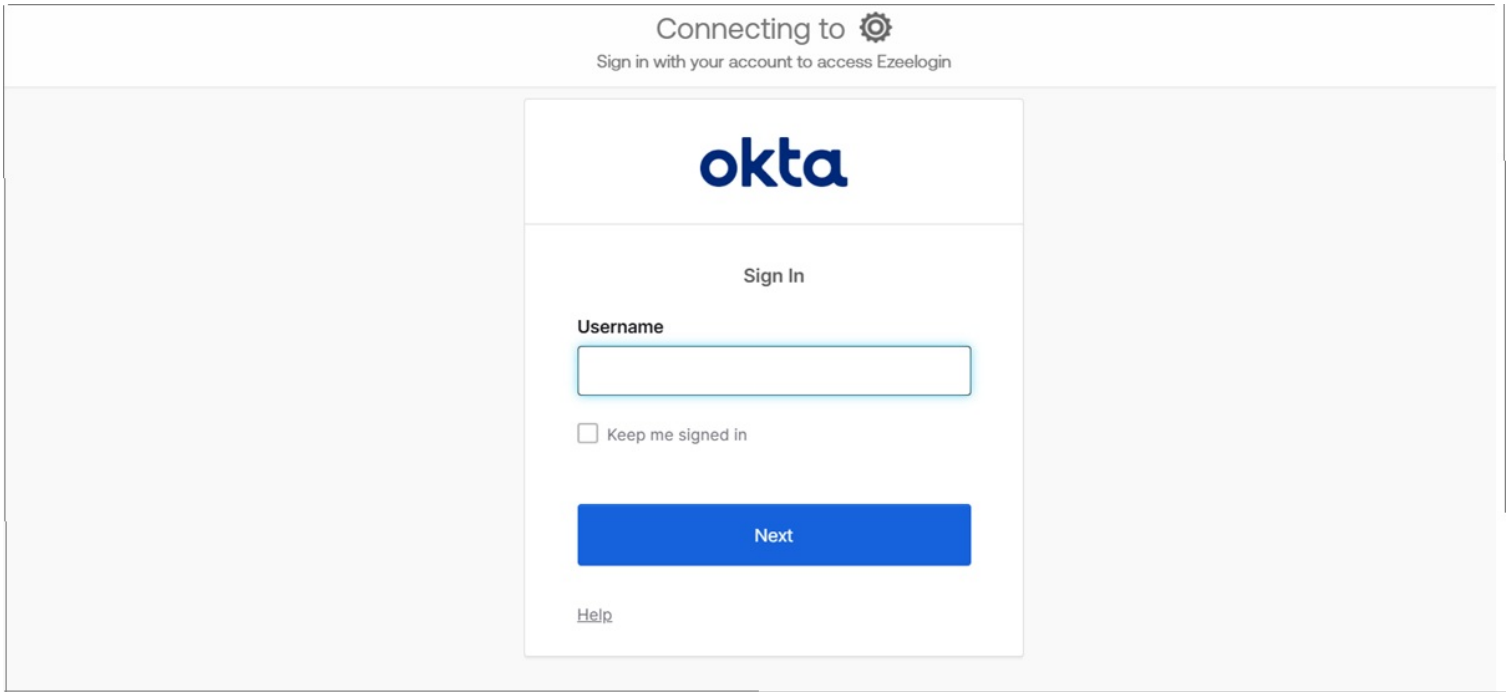
Path To CA Bundle



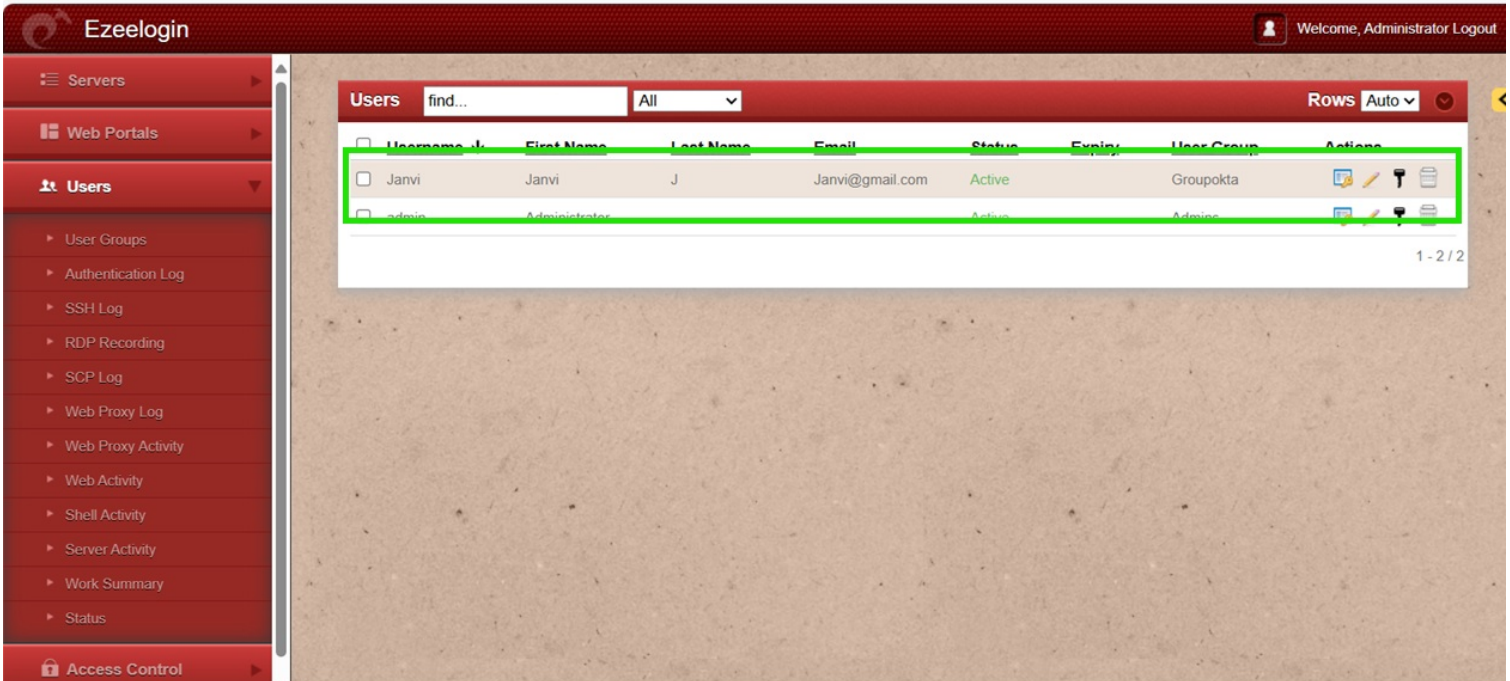
Step 6: Go to **Settings -> General ->** then **change Web Panel Authentication to OpenID Connect.**



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.



Related Articles:

[Integrate Okta SSO with jumpserver](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-okta-openid-connect-771.html>