

Integrating OneLogin OpenID connect

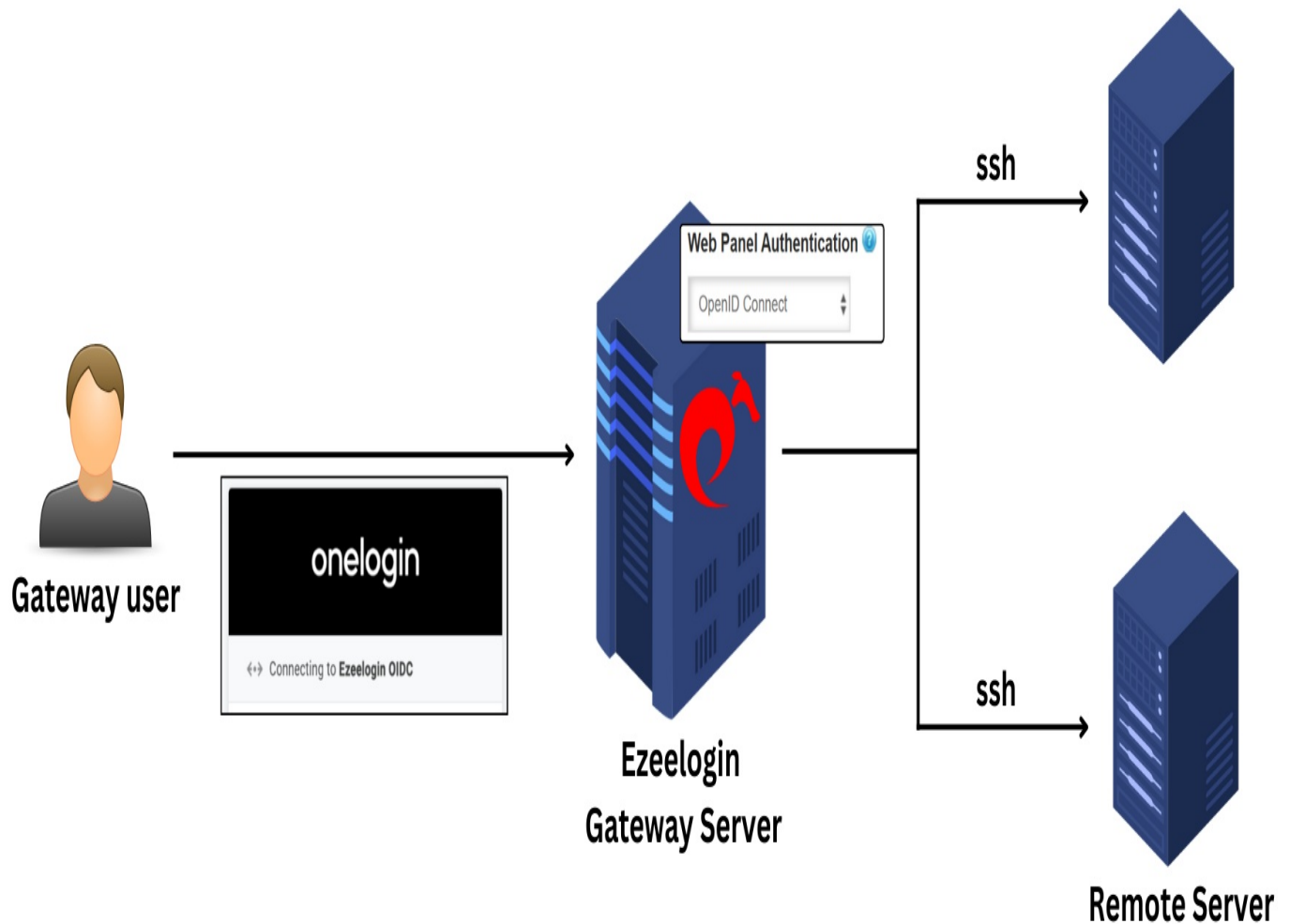
768 Rakhi May 28, 2026 Features & Functionalities

2596

How to integrate OneLogin OpenID Connect with Ezeelogin Jumpserver?

Overview: This article will help the super admin user to integrate OneLogin 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: Login to [OneLogin](#) and click on **Add App** under **Applications**.

onelogin

Users

Applications

Devices

Authentication

Activity

Security

Settings

Developers

Modules

Rakhi

Applications

Add App

Q search company apps...

See the new apps list

No company apps have been added.

Step 2: Search for **oidc** and select **OpenID Connect (OIDC)**.

onelogin

Users

Applications

Devices

Authentication

Activity

Security

Settings

Developers

Modules

Rakhi

Find Applications

Q oidc

Autotask OIDC
Autotask Corporation

OpenID Connect

Borrowbox(OIDC)
OneLogin, Inc.

OpenID Connect

dev_OIDC(under construction)
OneLogin

OpenID Connect

EVAS (OIDC)
EVAS

OpenID Connect2.0

Jamf Connect (OIDC)
OneLogin, Inc.

OpenID Connect

OpenId Connect (OIDC)
OneLogin, Inc.

OpenID Connect

Openpath OIDC
Onenpath

OpenID Connect

Step 3: Change the **Display Name** and **Save** it.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

App Listing / Add OpenId Connect (OIDC) Cancel Save

Configuration

Portal

Display Name
Ezeelogin OIDC

Visible in portal
☒

Rectangular Icon

Square Icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

Description
200 characters
Ezeelogin OpenId Connect

Step 4: Login to **Webpanel**, navigate to **Settings > OpenID Connect**, copy the Redirect URL, and add it to the redirect URLs in OneLogin.

Additionally, modify the last part of the OIDC URL by changing "oidc" to "login" and add it the url in Login Url.
(e.g., change <https://192.168.0.110/ezlogin/index.php/auth/oidc> to <https://192.168.0.110/ezlogin/index.php/auth/login>)

Ezeelogin Welcome, Administrator Logout

Servers Web Portals Users Access Control Settings OpenID Connect FIDO2 RADIUS SIEM

OpenID Connect Client Info

Redirect URL
<https://192.168.0.110/ezlogin/index.php/auth/oidc>

OpenID Connect Settings

Client ID

Client Secret

Provider URL

Email Attribute
email

Username Attribute
user_id

Group Attribute

Save the changes after adding the Url.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Applications / OpenId Connect (OIDC) More Actions Save

Info Configuration Parameters Rules SSO Access Users Privileges Setup

Application details

Login Url
<https://192.168.0.110/ezlogin/index.php/auth/login>

Redirect URI's
<https://192.168.0.110/ezlogin/index.php/auth/oidc>

After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

Step 5: Click on **Show client secret** under **SSO**.

Applications / OpenId Connect (OIDC)

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Enable OpenID Connect

Client ID

3866fe80-d02a-013d-6440-4d2289dcf3bf245803

Client Secret

Show client secret Regenerate client secret

Issuer URL

https://ezadmod25.onelogin.com/oidc/2 Well-known Configuration

Step 6: Copy the **Client ID**, **Client Secret** and **Issuer URL** and paste it in webpanel under OpenID Connect menu parameters.

Applications / OpenId Connect (OIDC)

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Enable OpenID Connect

Client ID

3866fe80-d02a-013d-6440-4d2289dcf3bf245803

Client Secret

Hide client secret Regenerate client secret

9c59c32a935181ef9096bc4595833def5072a0c3be13f55c8c09b96cd7740c3e

Issuer URL

https://ezadmod25.onelogin.com/oidc/2 Well-known Configuration

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

License

OpenID Connect Client Info

Redirect URL

https://192.168.0.110/ezeelogin/index.php/auth/oidc

OpenID Connect Settings

Client ID

3866fe80-d02a-013d-6440-4d2289dcf3bf245803

Client Secret

9c59c32a935181ef9096bc4595833def5072a0c3be13f55c8c09b96cd7740c3e

Provider URL

https://ezadmod25.onelogin.com/oidc/2

Email Attribute

email

Username Attribute

user_id

Group Attribute

groups

Firstname Attribute

given_name

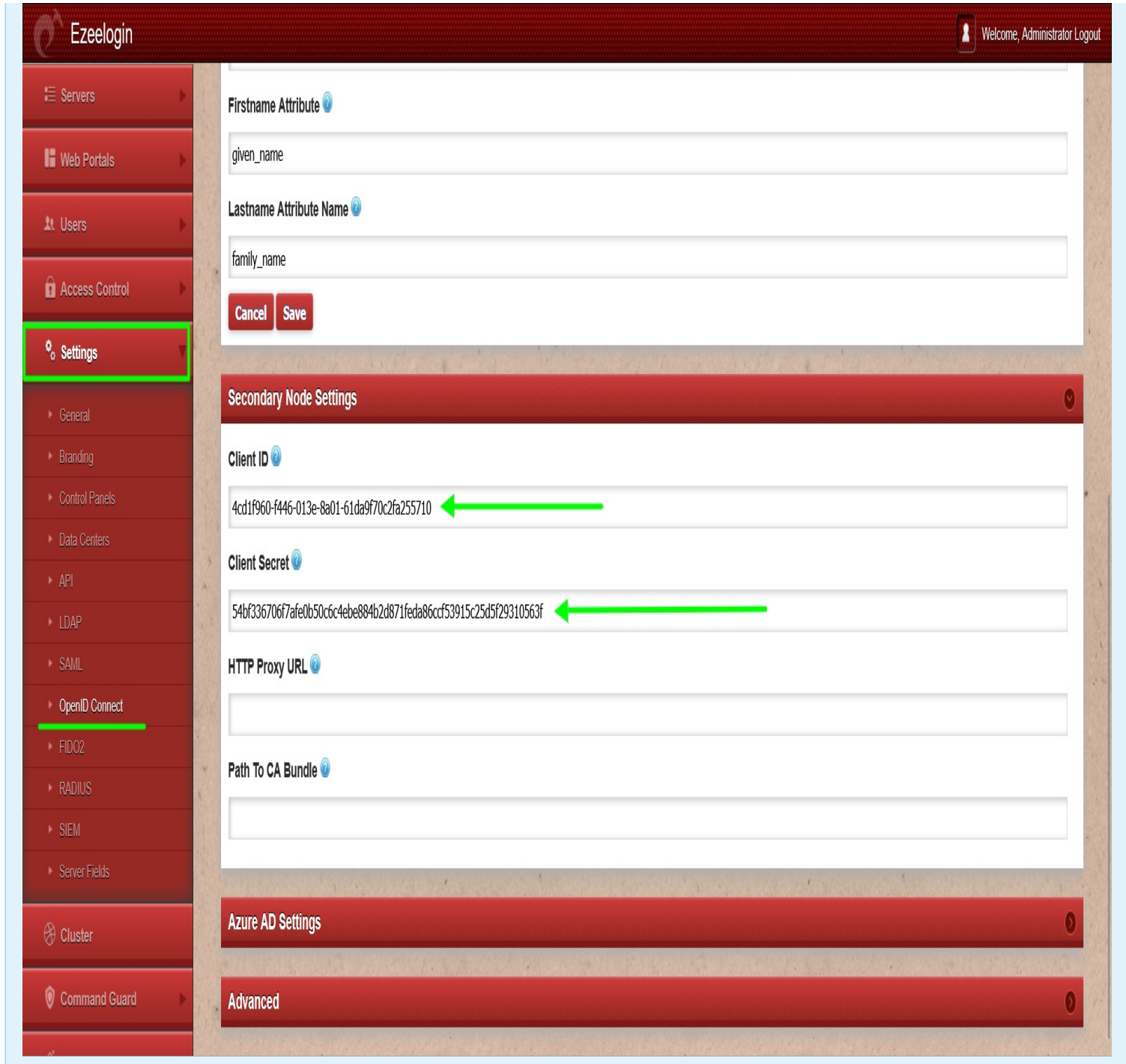
Lastname Attribute Name

family_name

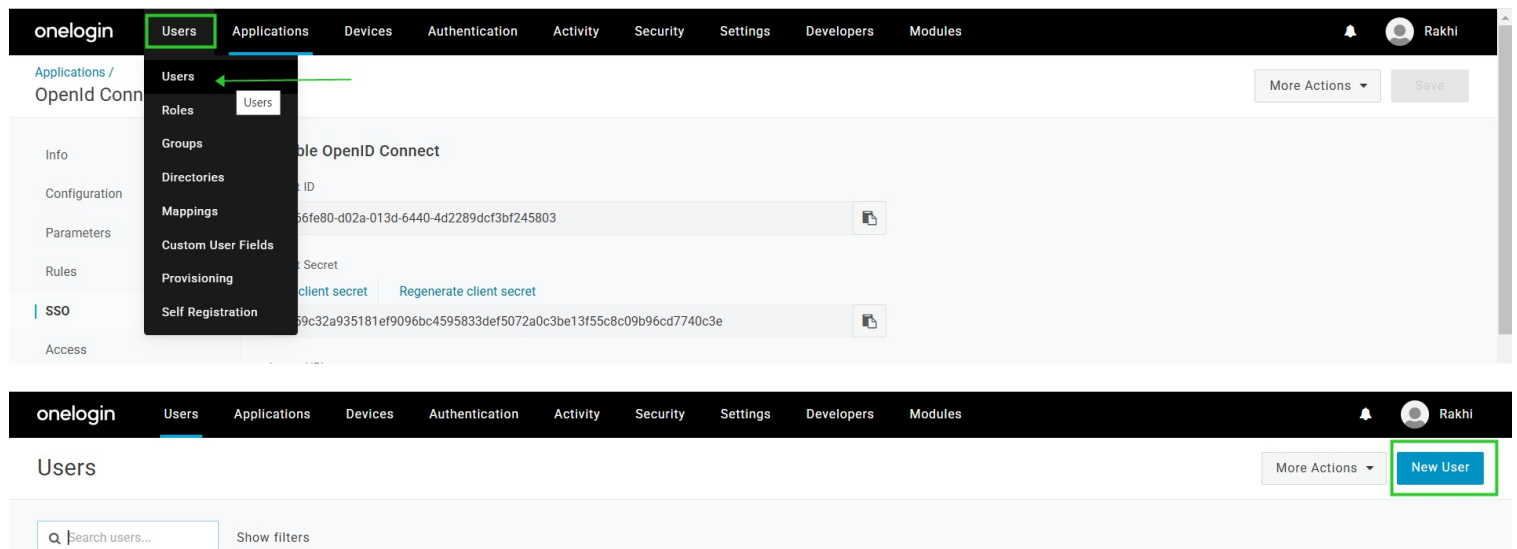
Cancel Save

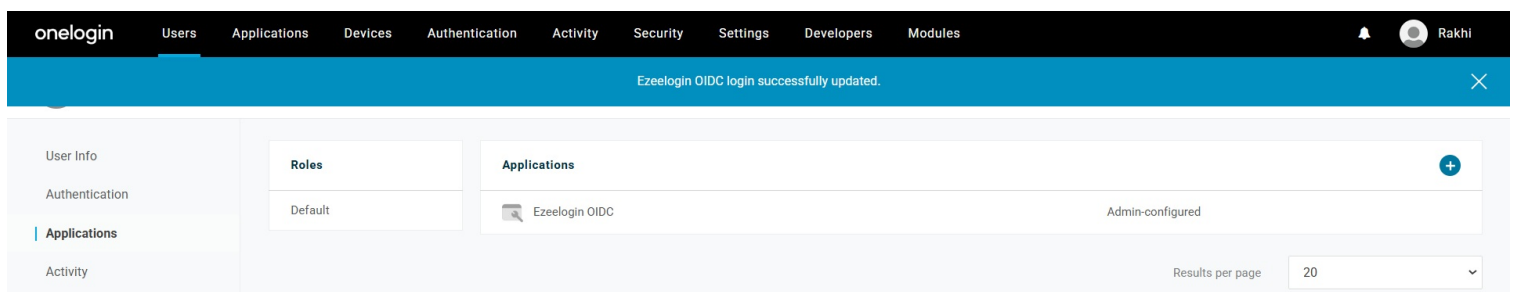
For cluster, add the Client ID and Client Secret from the other OIDC configuration:

Follow steps 1 to 6 to create new application for secondary node. While adding the application details in OneLogin, replace the IP address with the secondary node's IP address.

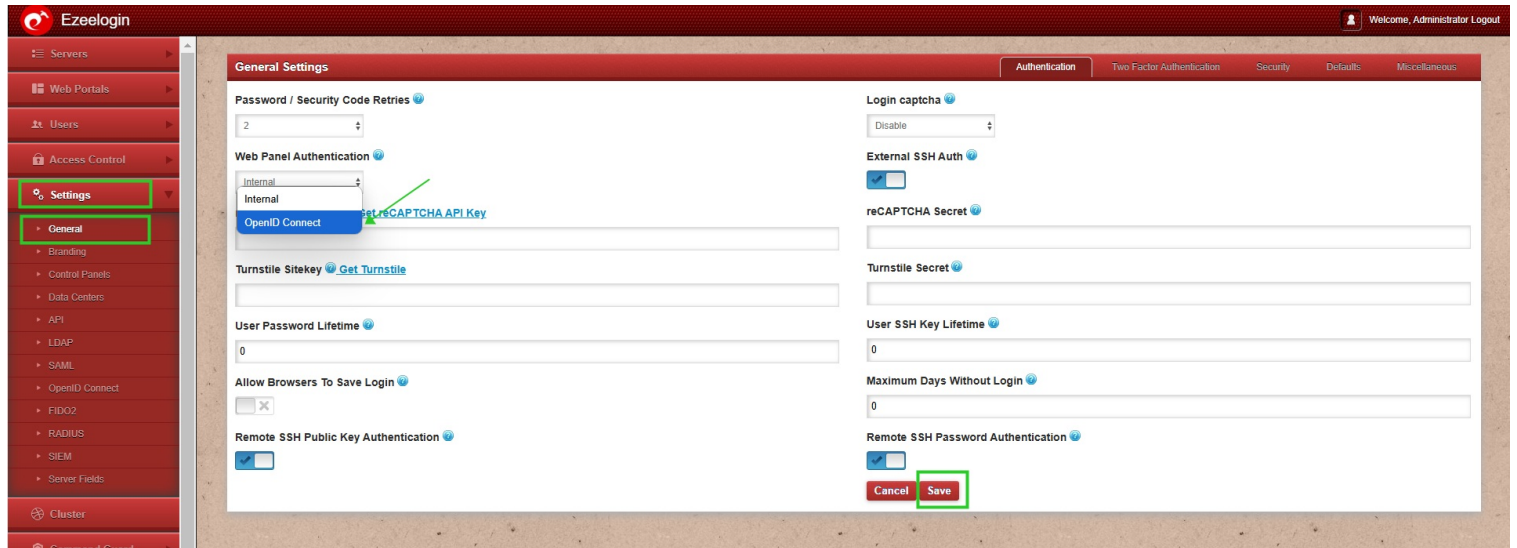


Step 7: Select the **Users** tab and click on **New User** then provide **first name**, **last name**, **username** and **email** to save the user.

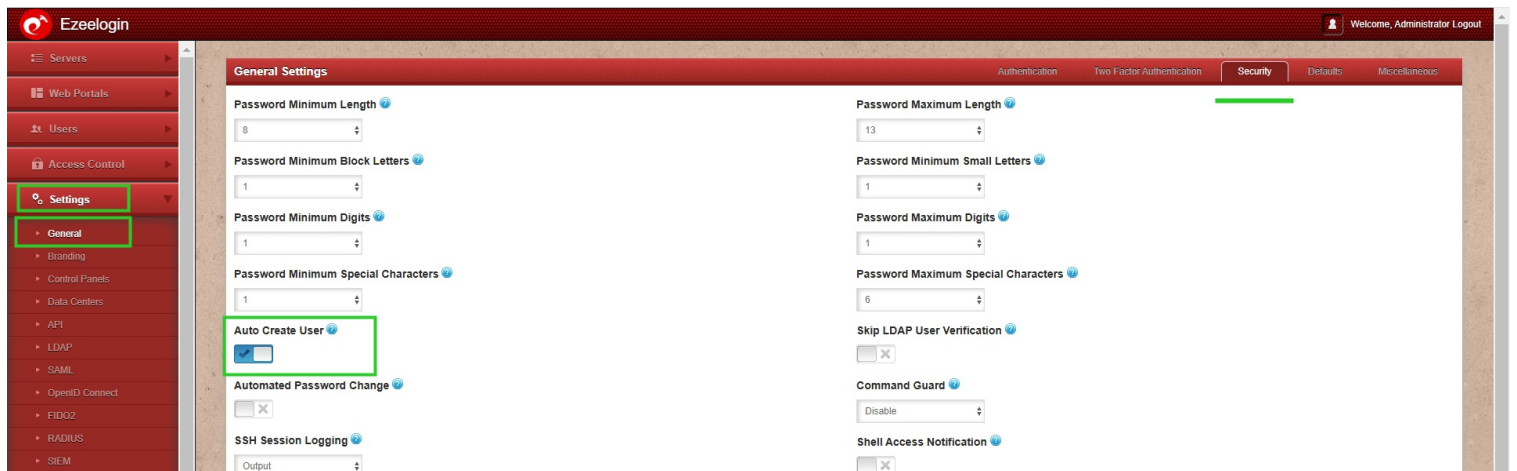




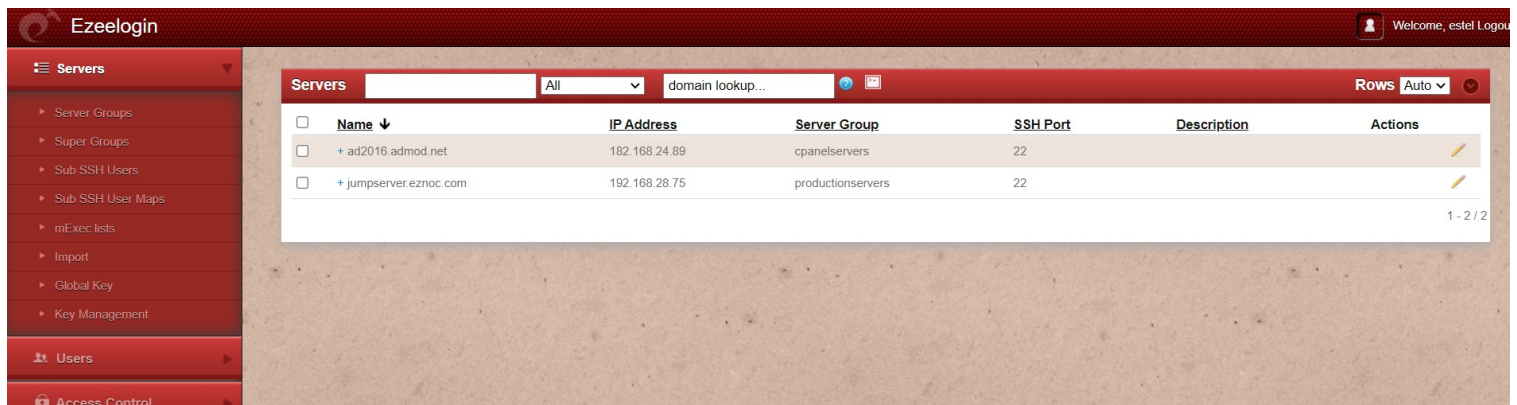
Step 9: Change **Web panel Authentication** to OpenID Connect from **Ezeelogin GUI > Settings > General > Authentication** and Save it.



Step 9 (A): Enable Auto Create User in the Ezeelogin GUI by going to **Settings > General > Security**.



Step 10: Re-login to webpanel 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

Step 11: After logging in, set a new password and security code under **Account > Password**.

The screenshot shows the Ezeelogin web interface. On the left is a red sidebar menu with options like Servers, Web Portals, Users, Access Control, Settings, Cluster, Command Guard, and Account. The 'Account' menu item is highlighted, and its sub-menu 'Password' is also highlighted. The main content area is titled 'Change password, security code, two factor secret'. It contains several input fields: 'New Password' and 'Confirm Password' (with a green arrow pointing to the confirm field), 'New Security Code' and 'Confirm Security Code' (with a green arrow pointing to the confirm field), 'New Access Keyword' and 'Confirm Access Keyword', and 'SSH Private Key' and 'SSH Key Passphrase'. There are 'Generate' buttons for the password and security code fields. At the bottom right of the form are 'Cancel' and 'Save' buttons, with the 'Save' button highlighted by a green box.

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

How to add scope from OneLogin OpenID connect to Ezeelogin jumpserver?

Step 1: Navigate to **Developers > API Access Management**.

The screenshot shows the OneLogin 'Developers' page. The top navigation bar includes 'onelogin', 'Users', 'Applications', 'Devices', 'Authentication', 'Activity', 'Security', 'Settings', 'Developers', and 'Modules'. The 'Developers' menu item is highlighted, and its dropdown menu is open, showing options like 'Documentation', 'API Reference', 'API Access Management' (highlighted with a green box), 'API Credentials', 'Webhooks', and 'Embedding'. The main content area is titled 'Applications' and contains a search bar and a list of applications, including 'Ezeelogin OIDC'.

Step 2: Click on **Add API**.

The screenshot shows the OneLogin 'API Access Management' page. The top navigation bar is the same as the previous screenshot. The main content area is titled 'API Access Management' and contains a search bar. In the top right corner of the main content area, there is a blue 'Add API' button, which is highlighted by a green box.

Step 3: Provide the mentioned details.(Enter redirect URL from gateway server under resource identifier and Audiences)

onelogin

UsersApplicationsDevicesAuthenticationActivitySecuritySettingsDevelopersModules

RP

Rakhi

API Access Management / Add API

Overview

Overview

Name *

Ez_oidc

Description

oidc connect

Resource Identifier *

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

Audiences (comma delimited) *

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

Token Timeout Settings

Access Token

10

minutes

Refresh Token

30

minutes

Save

Step 4: Under **Scope > Add Scope**.

onelogin

UsersApplicationsDevicesAuthenticationActivitySecuritySettingsDevelopersModules

RP

Rakhi

API Access Management / Ez_oidc

Overview

Scopes

Claims

Search

Search

Add Scope

Step 5: Enter the scope details and Save it.

Add Scope

Scope *

groups

Description

group

Cancel

Ok

onelogin

UsersApplicationsDevicesAuthenticationActivitySecuritySettingsDevelopersModules

RP

Rakhi

API Access Management / Ez_oidc

Overview

Scopes

Claims

Clients

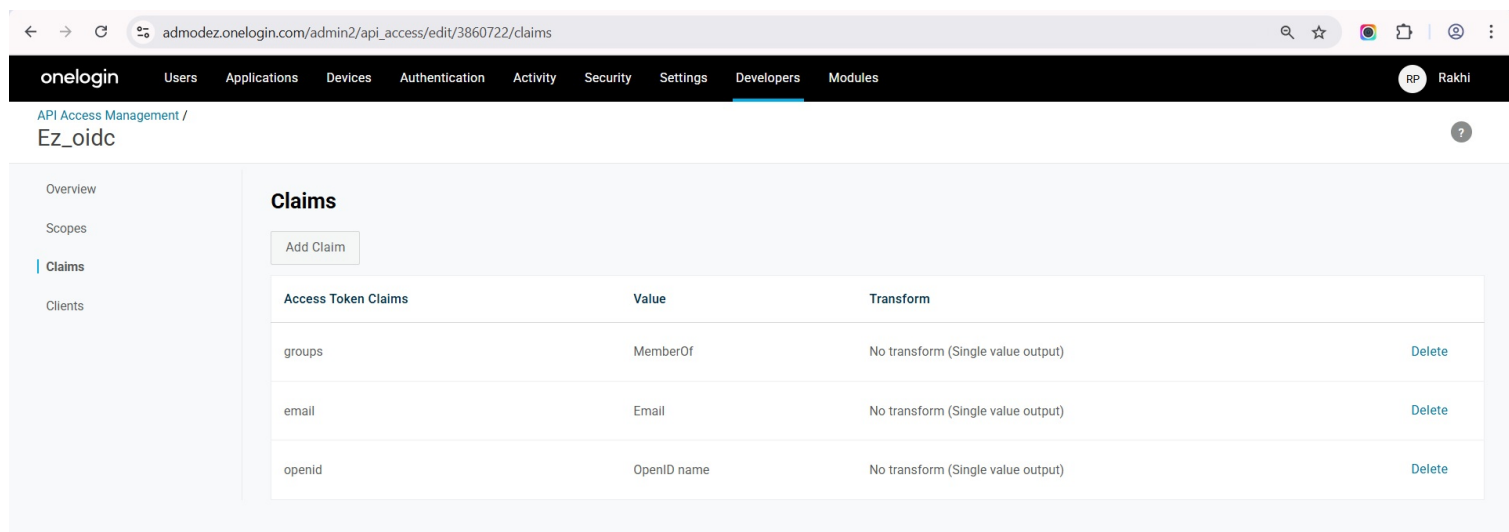
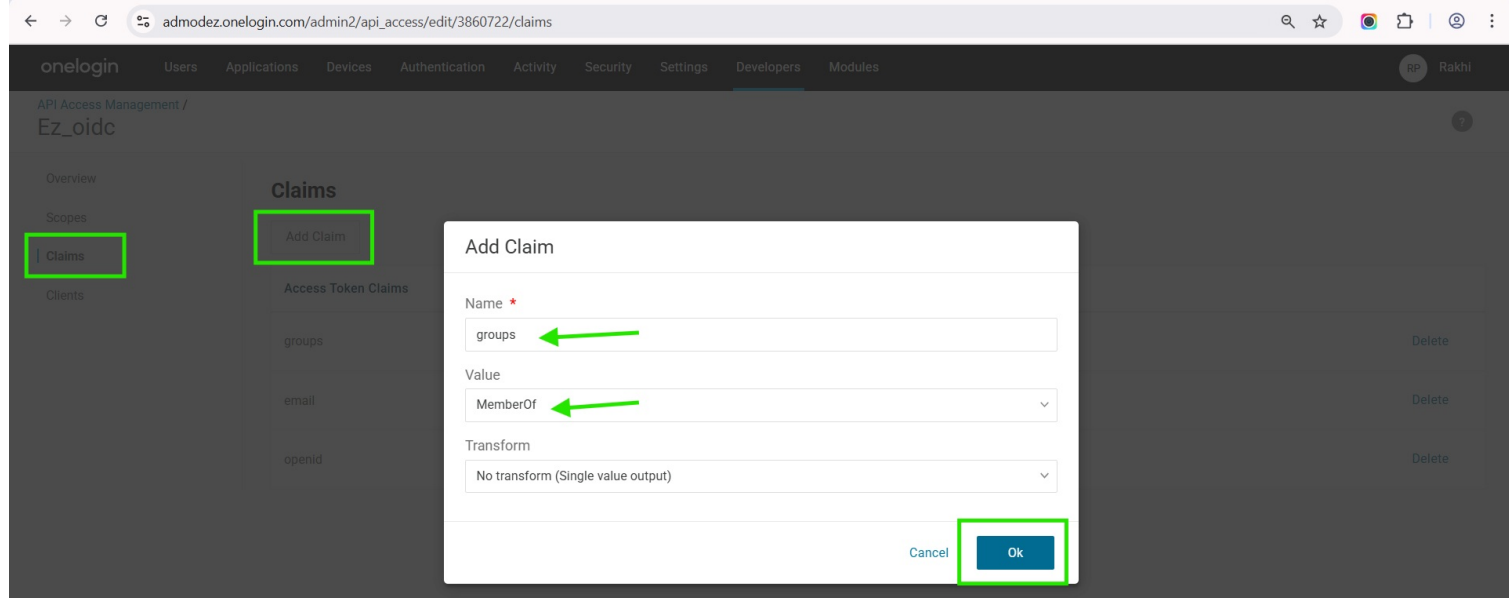
Search

Search

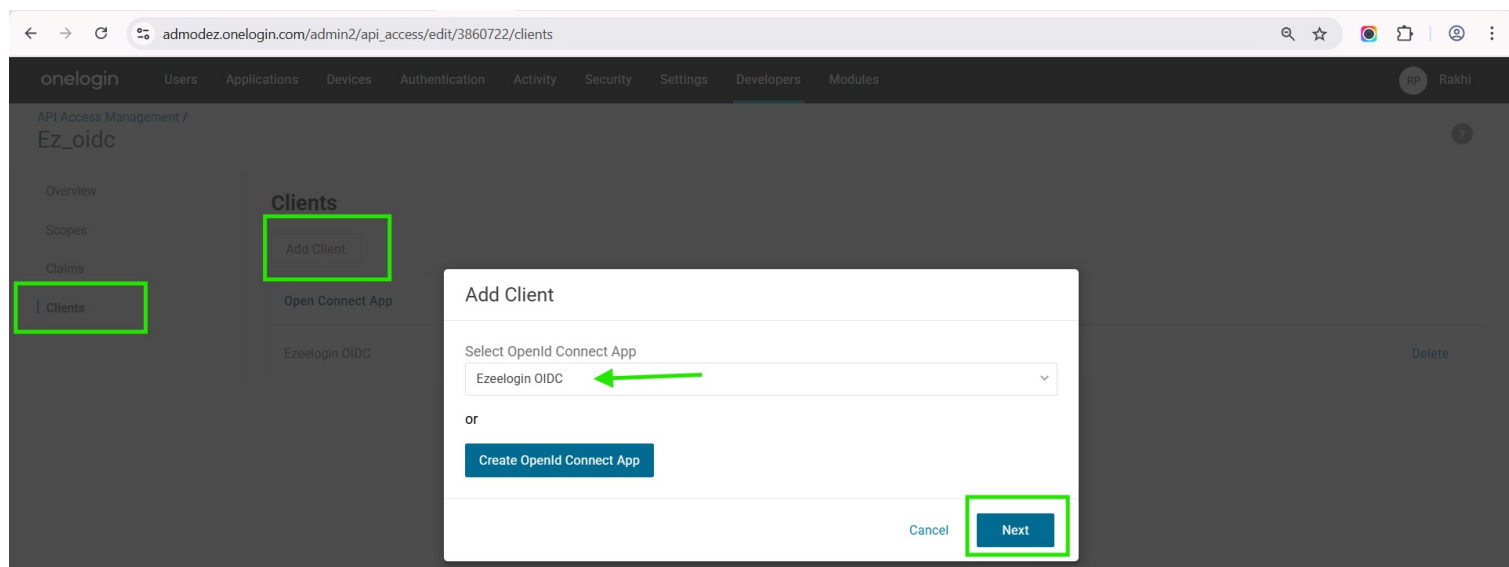
Add Scope

Scope	Description	
groups	group	Delete
email	mail	Delete
openid	mandate	Delete

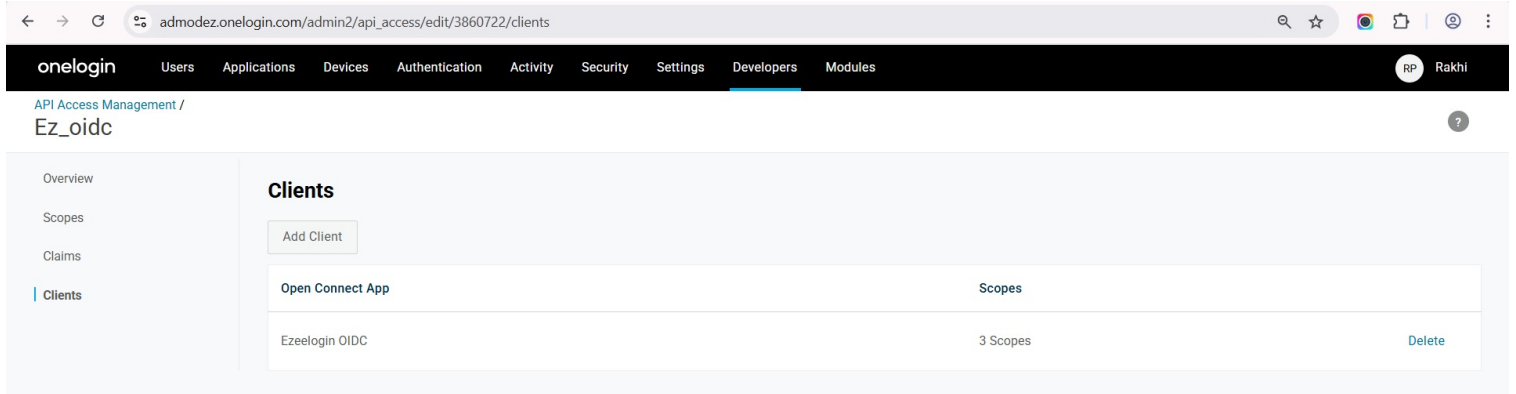
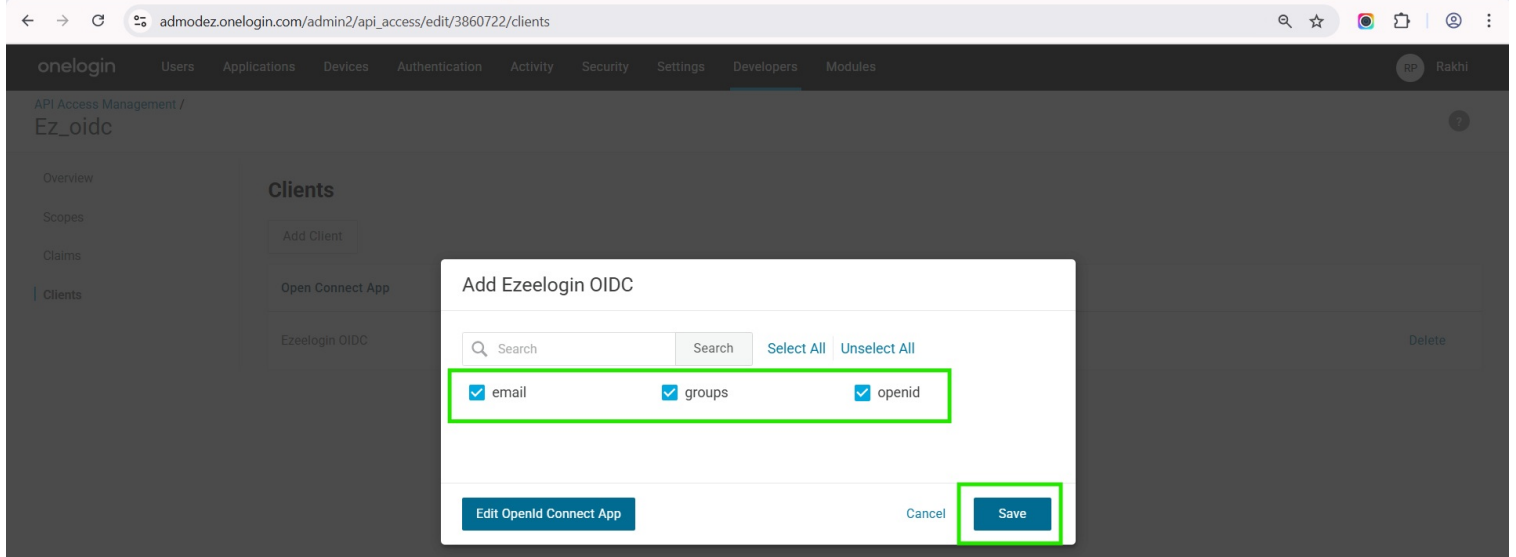
Step 6: Navigate to **Claims > Add Claim > Enter claim details and Save it**.



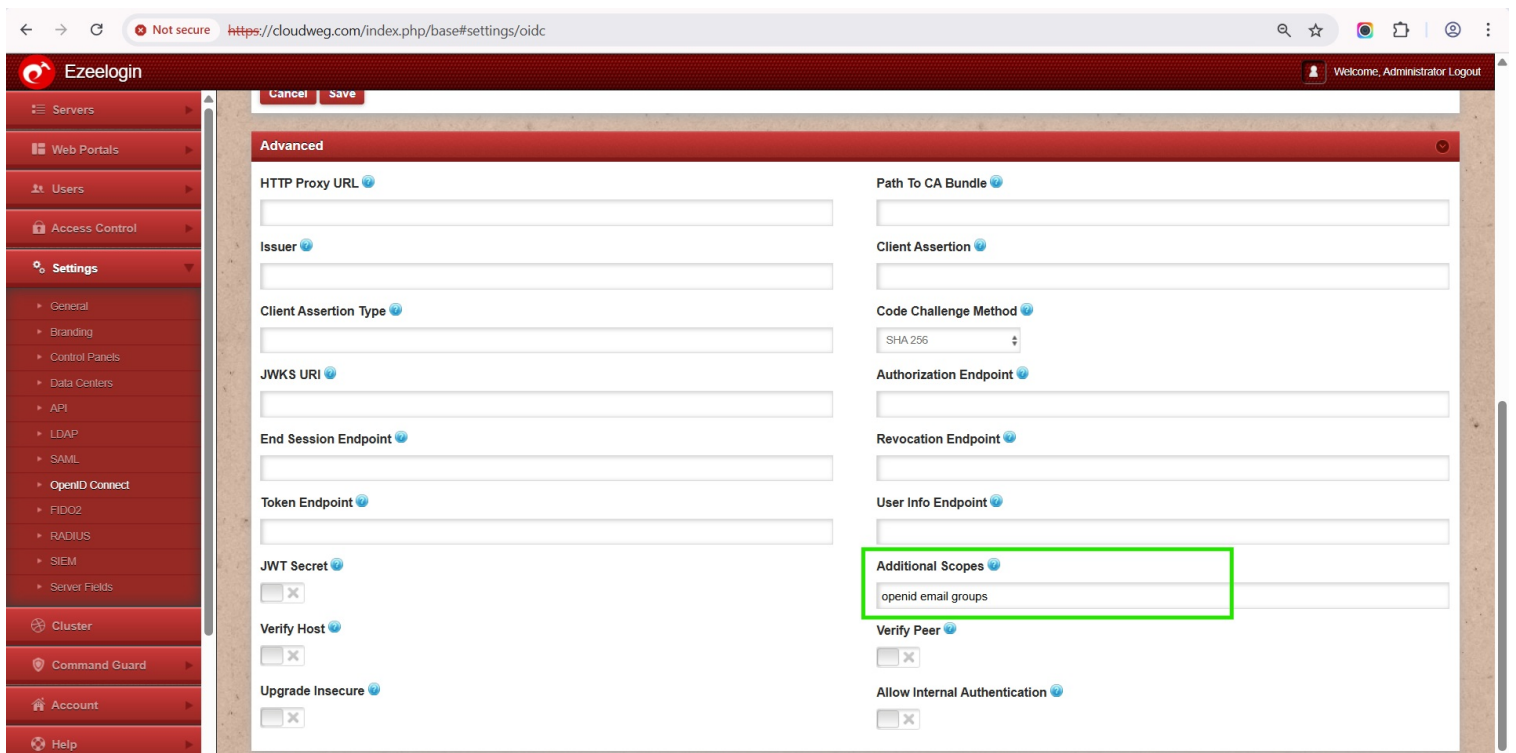
Step 7: Click on **Clients** > **Add client** > Select the **Application** > Next.



Select the scopes you would like to assign and Save it.



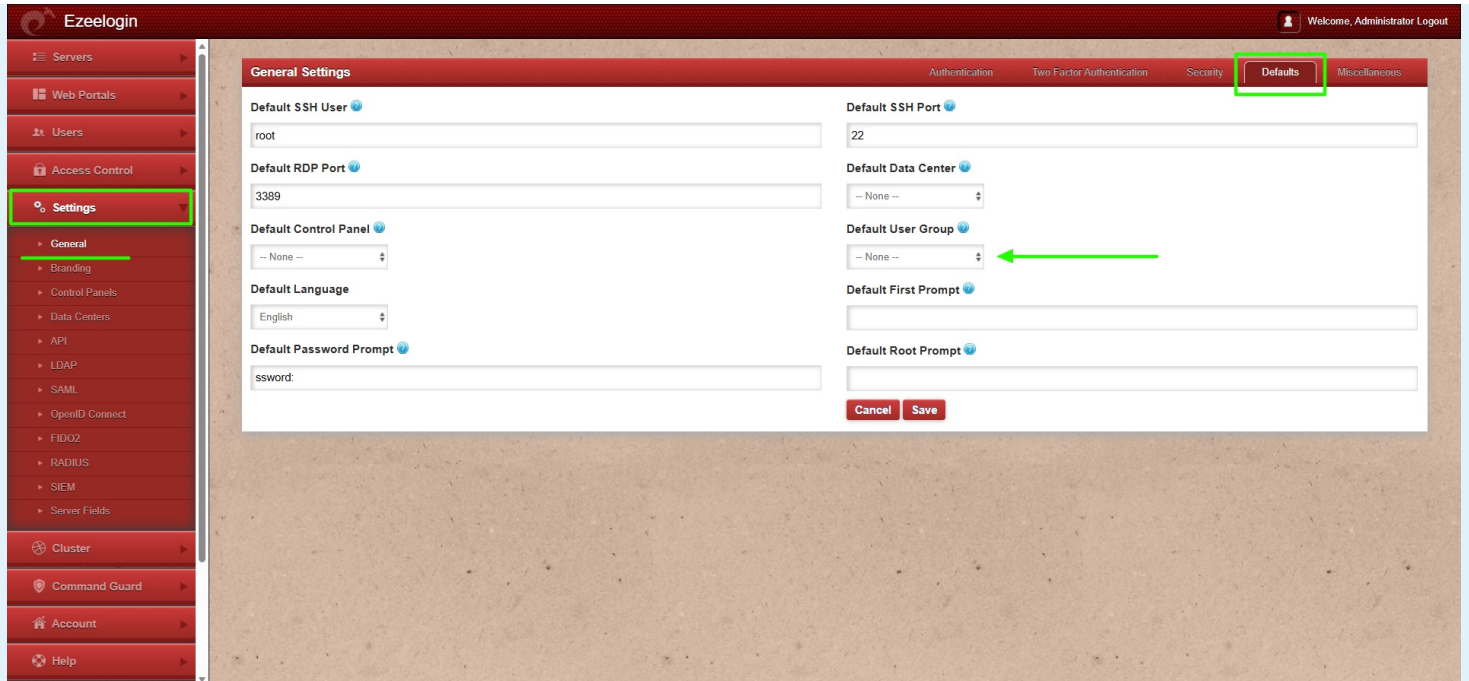
Step 8: Login to Ezeelogin, go to **OIDC advanced settings**, add the **scopes separated by spaces**, and **save the settings**.



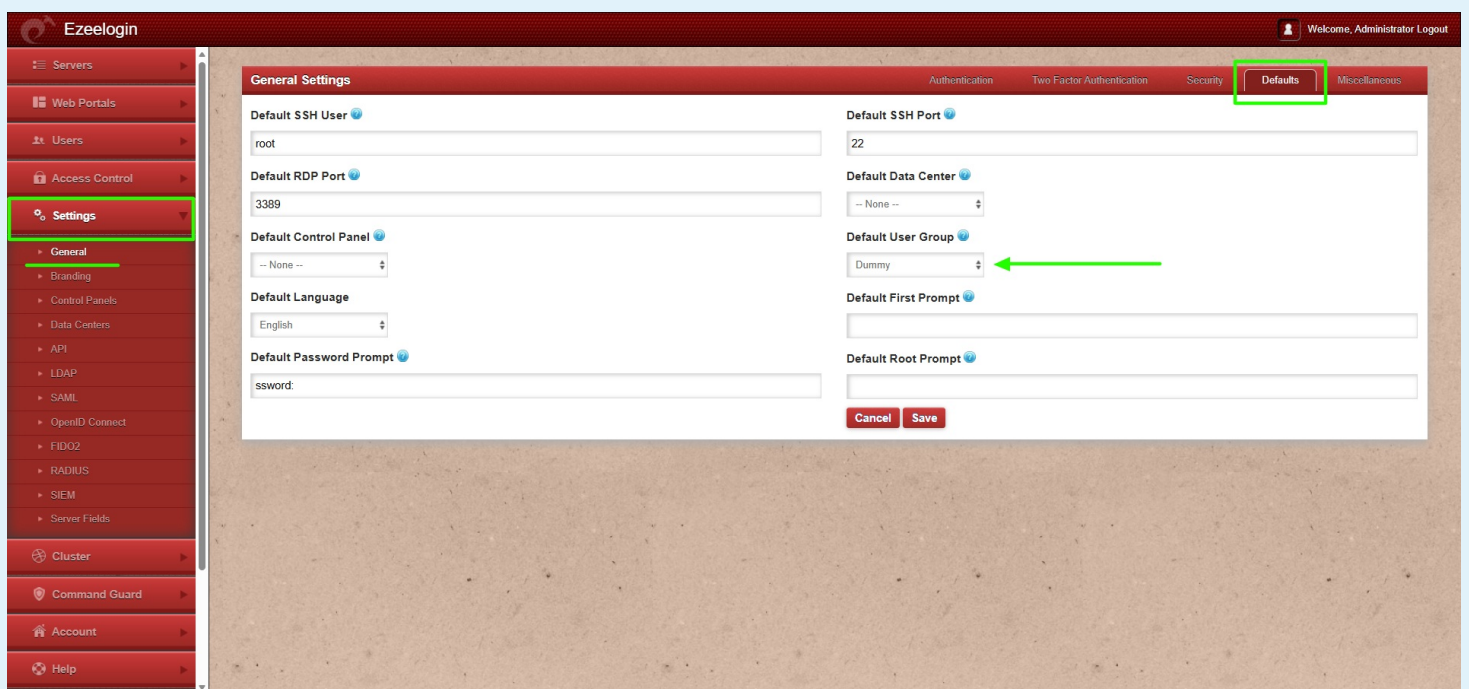
How to map One login users to the same user group in Ezeelogin?

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 OneLogin), 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: Create a user in one login application

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Users / New User Cancel Save User

User Info

Active

First name * Last name * Email

judy travis judy@gmail.com

Username Phone number Manager

judy Choose a manager

Company Department Title

Step 2: Select Authentication > Choose the usergroup for user judy and Save it.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Users / judy travis More Actions Save User

User Info Authentication Applications Activity

Authentication

Group

staff

Trusted IDP

-- NONE --

Authenticated by

OneLogin

User security policy

-- default is Default policy --

Open ID

OpenID ⓘ Change

judy

Step 3: Assign the application for that user under Application and Save it.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules

Users / judy travis More Actions Save User

User Info Roles Authentication Applications Activity

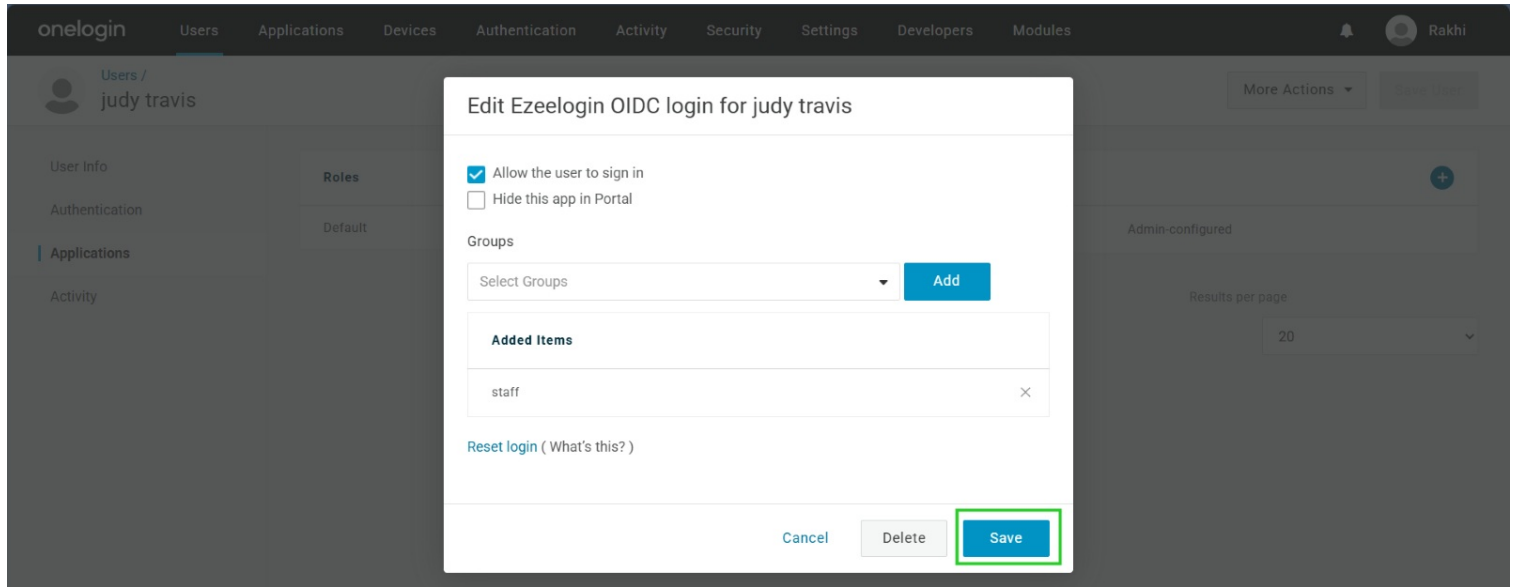
Assign new login to judy travis

This login will override any apps assigned via roles.

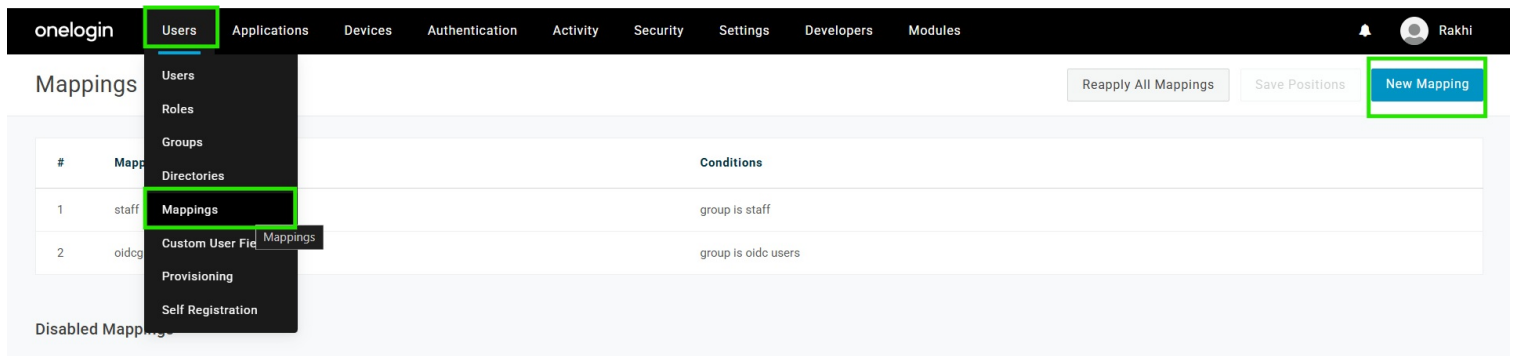
Select application

Ezeelogin OIDC

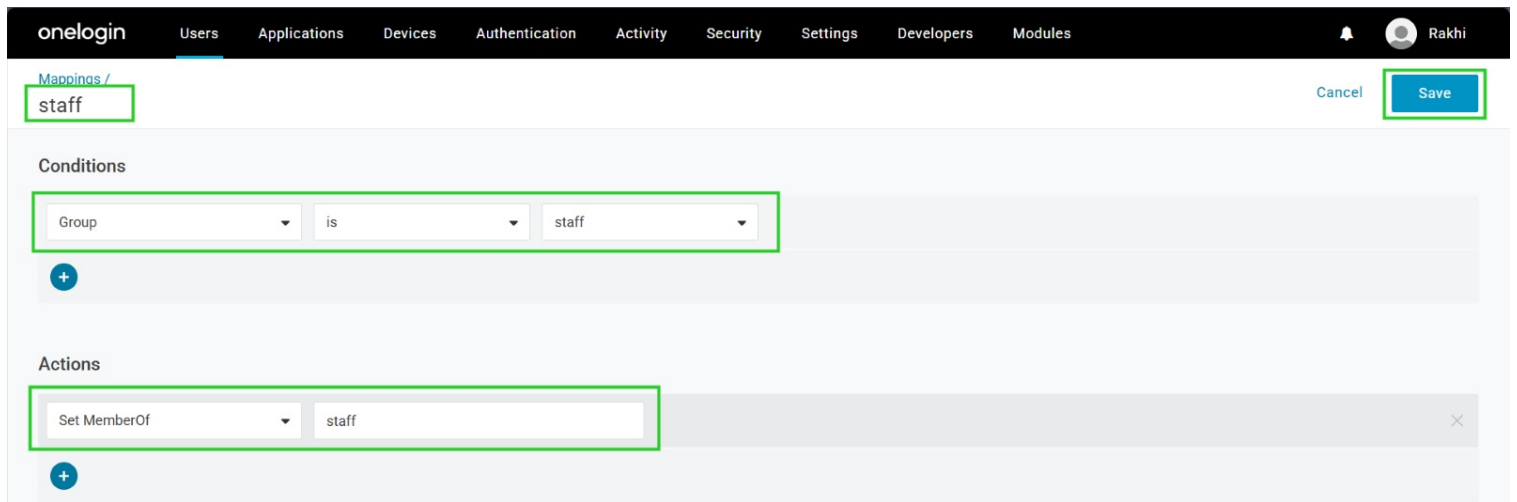
Cancel Continue



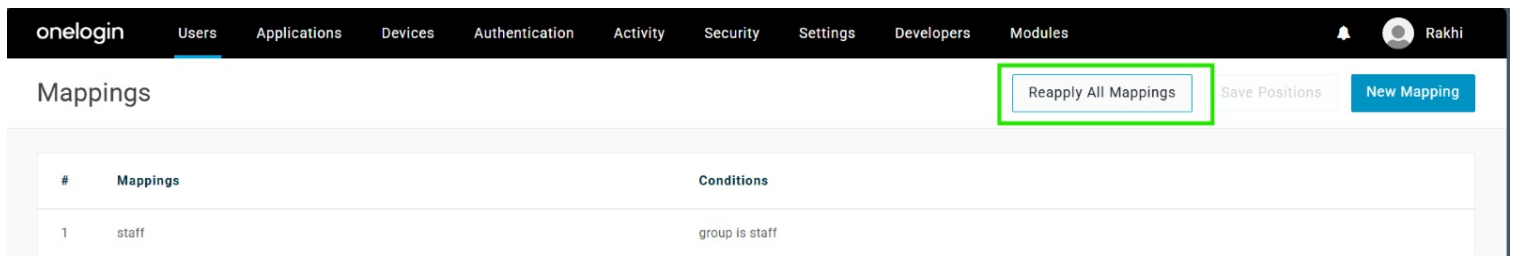
Step 4: Map the user under Users tab > Mappings. Click on create New mapping.



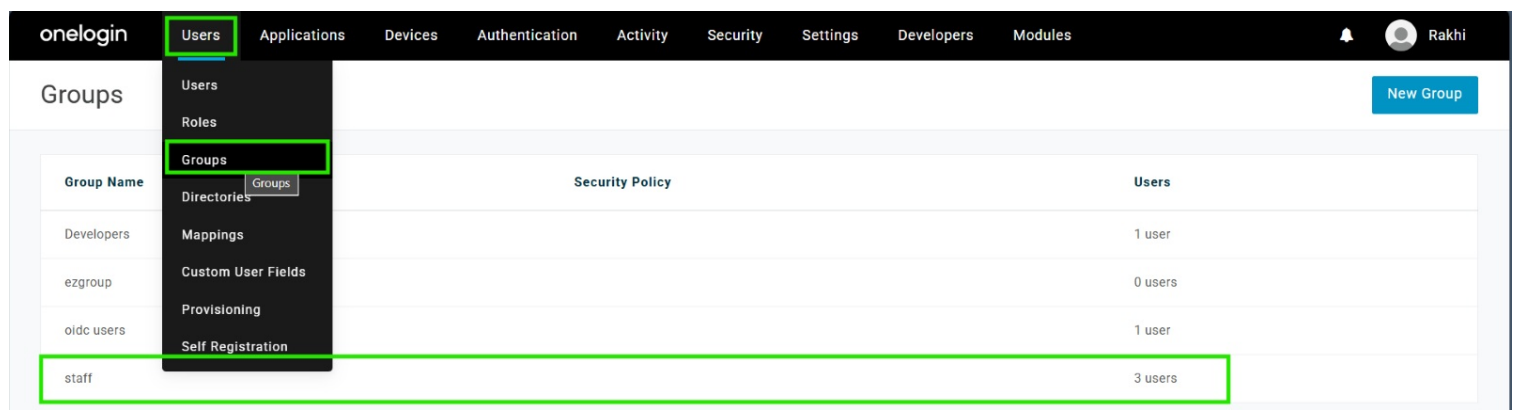
Step 4 (A): Fill the mapping details. Enter the usergroup name under Mappings and enter the condition and Actions > Save it.



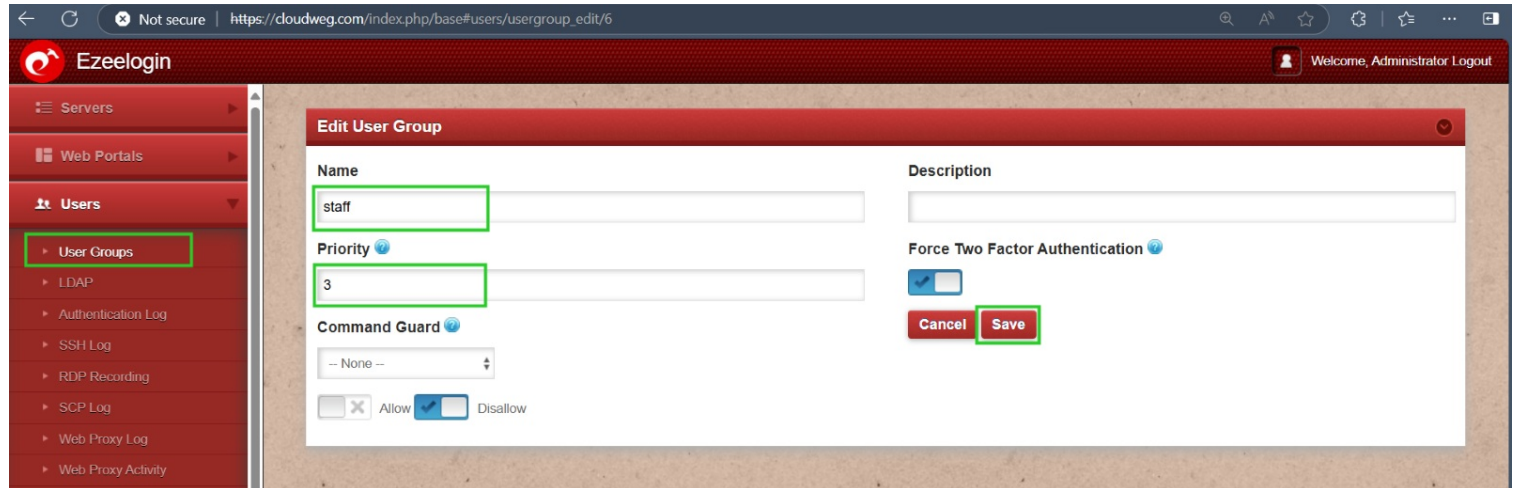
Step 4(B): Click on Reapply all mappings.



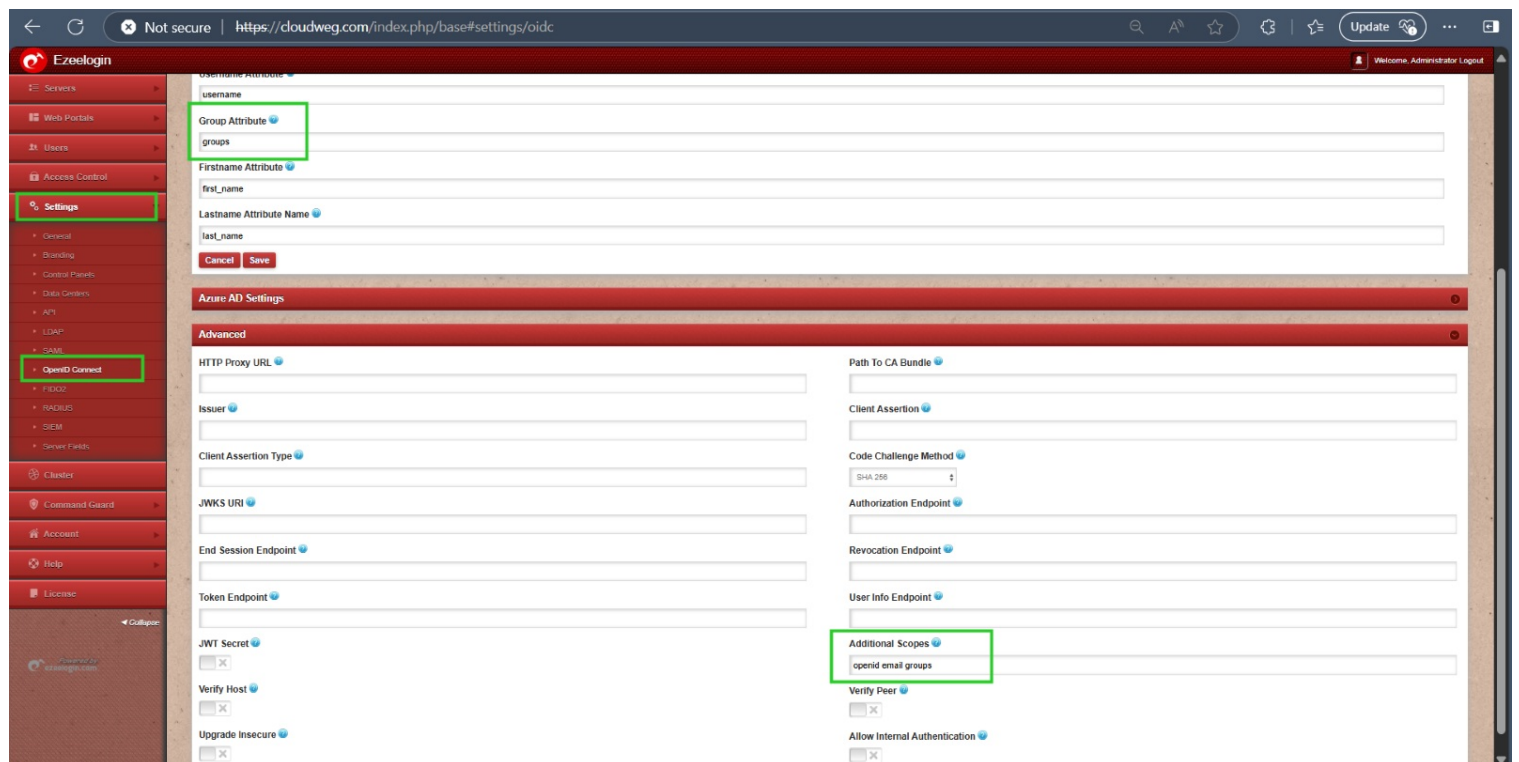
Rechecked mapped users in group Under Users > Groups > mapped 3 users under the group staff similarly



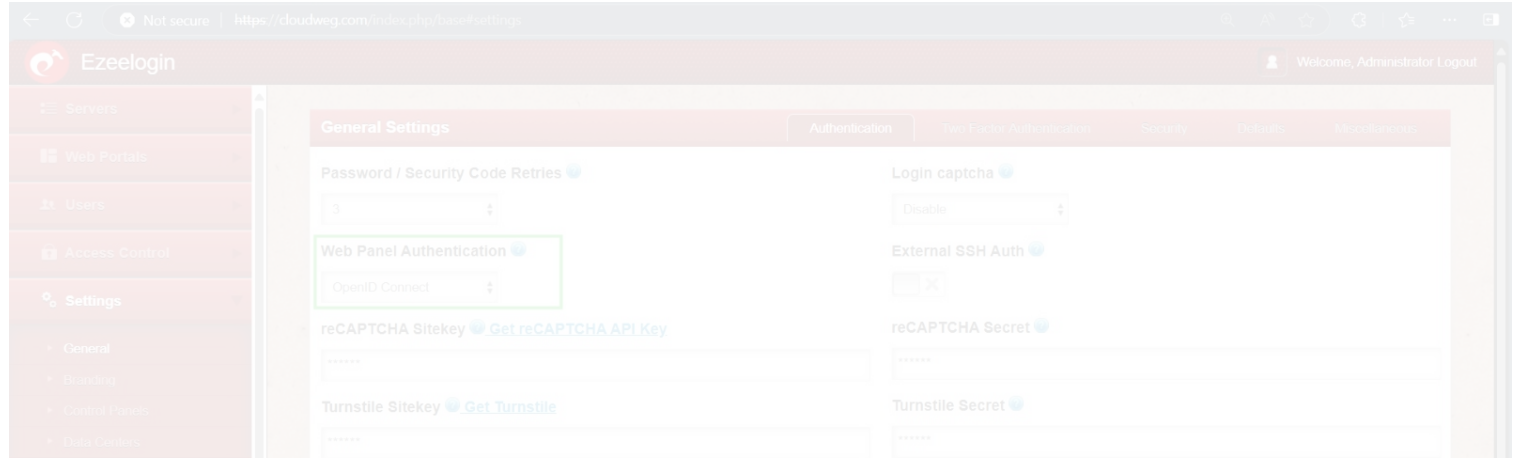
Step 5: Create the same user group in gateway server by setting a priority and save it.



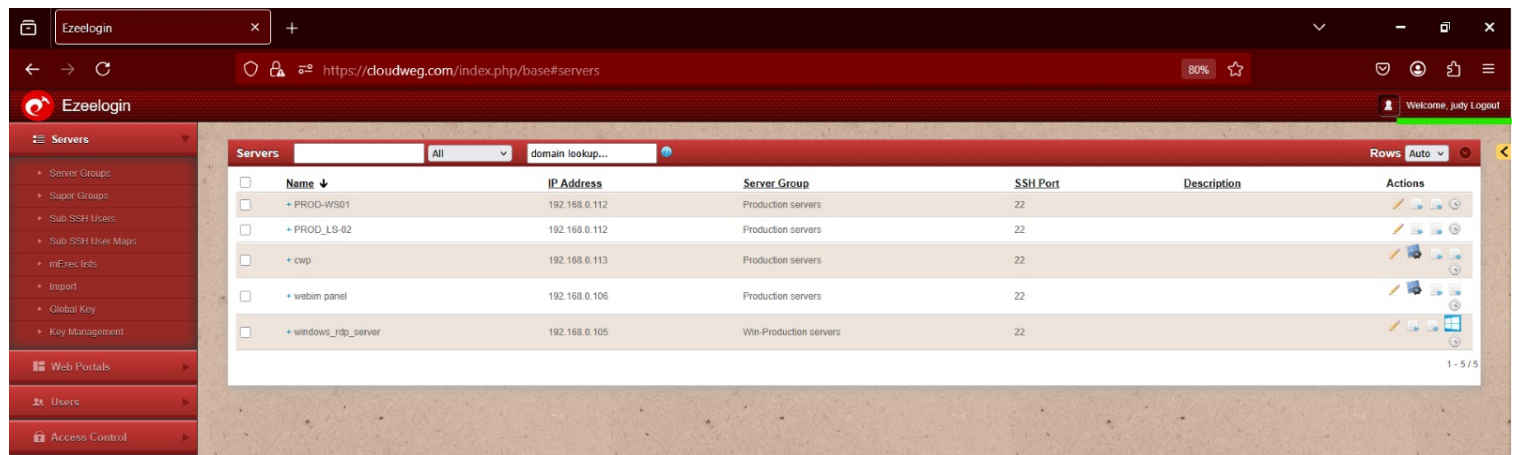
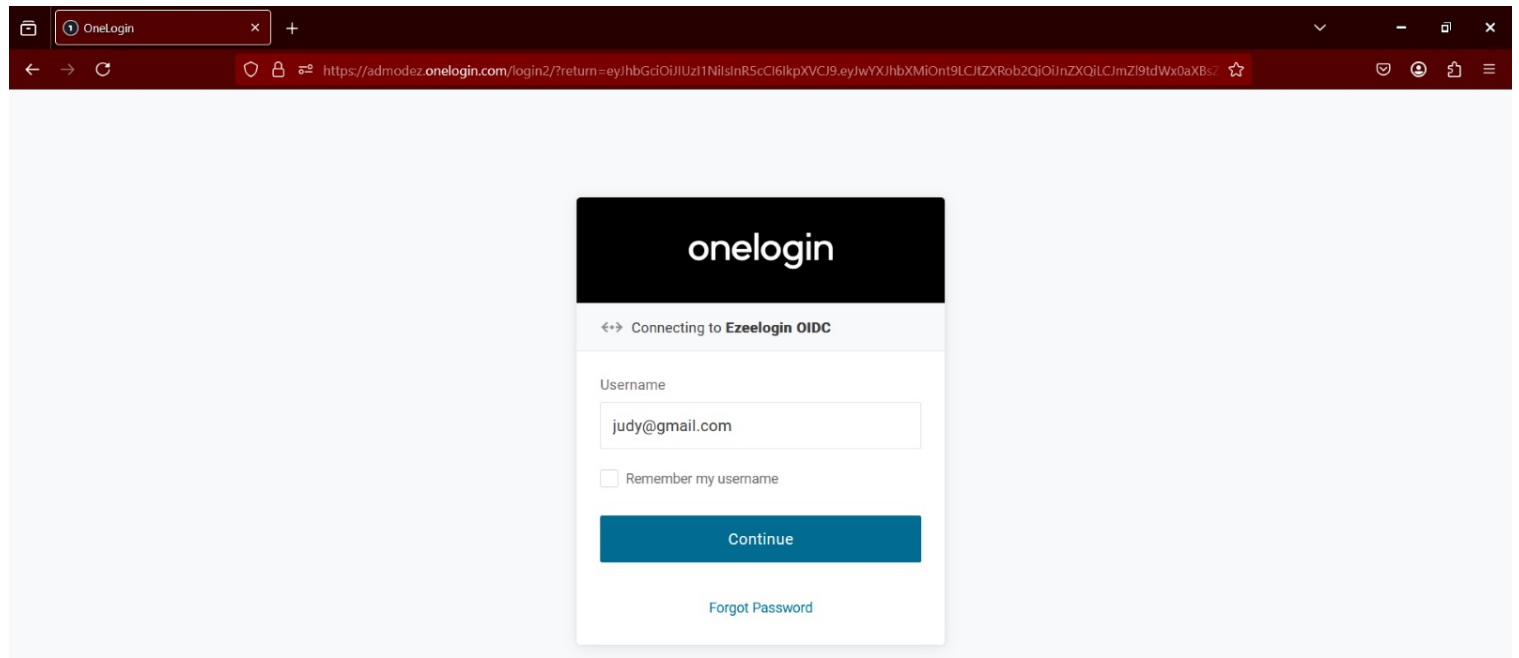
Step 6: In the web GUI. Navigate to **Settings > OpenID Connect > Add the group attribute name**, mention **Additional** scope (groups) and save it.



Step 7: Choose the webpanel authentication under settings tab and enable auto create user.



Step 8: Log in to the web GUI using one login user credentials, and the user will be assigned to the same group in Ezeelogin as in one login.



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

Related Articles:

[Integrate OneLogin SSO with JumpServer.](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrating-onelogin-openid-connect-768.html>