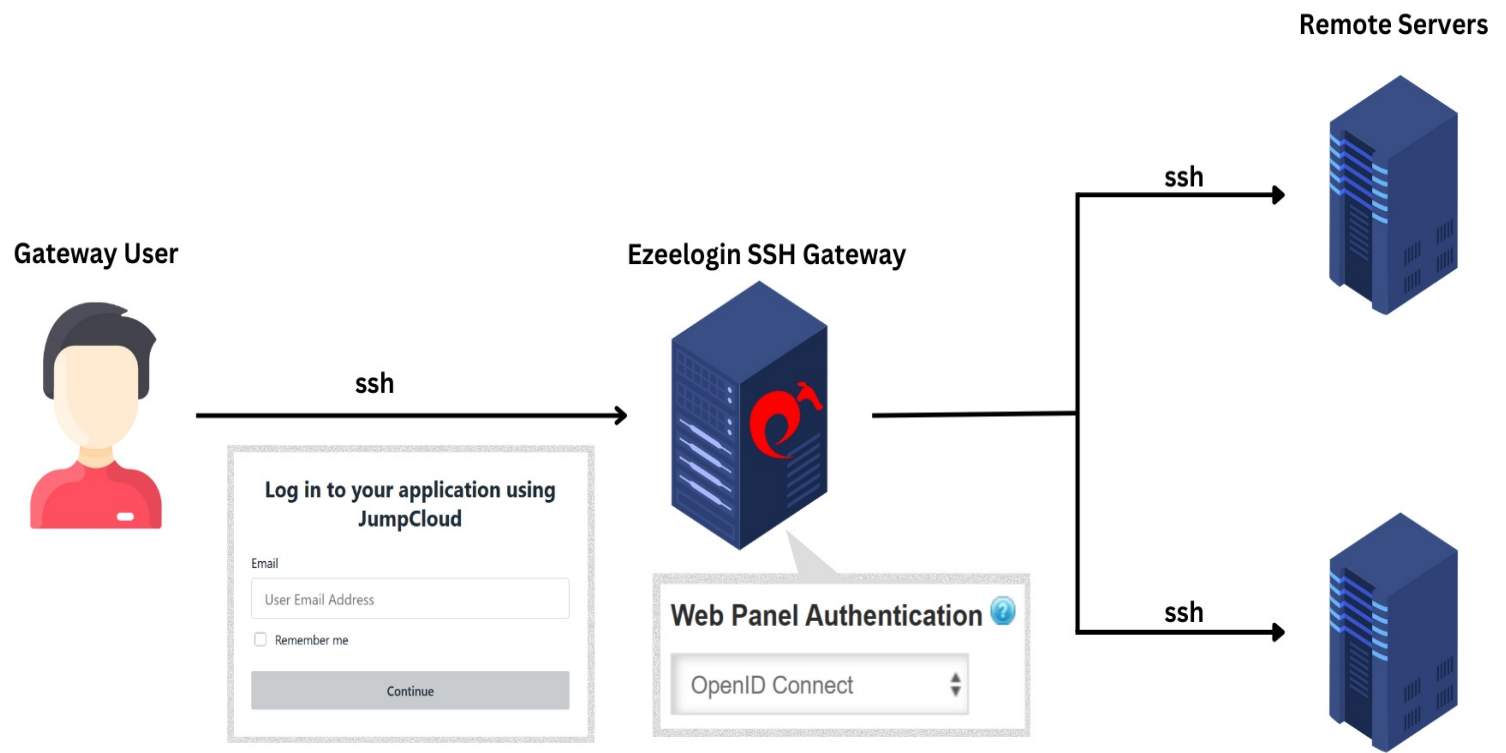


Integrate Jumpcloud OpenID Connect

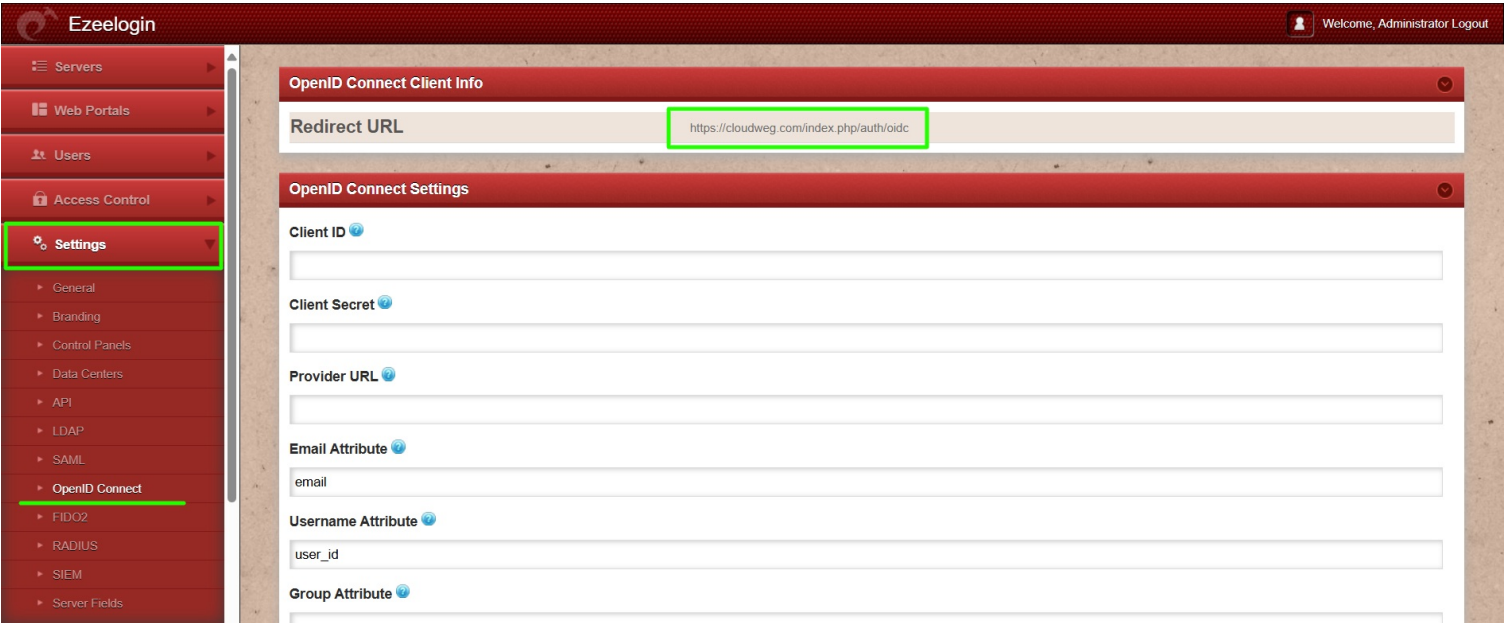
How to integrate Jumpcloud OpenID connect with Ezeelogin jumpserver?

Overview: This article will help Ezeelogin super admin user to integrate Jumpcloud 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 **Ezeelogin GUI** and click on **Settings -> OpenID Connect** and copy 'redirect URL'.



Step 2: Login to **Jumpcloud** and add the **Application**.

jumpcloud

Go To %/Ctrl + K

Get Started

Home

USER MANAGEMENT

Users

User Groups

USER AUTHENTICATION

LDAP

RADIUS

SSO Applications

Password Manager

DEVICE MANAGEMENT

Devices

Device Groups

Chat

Settings

Account

Collapse Menu

Applications

Alerts Checklist Pricing Cart JJ

Configured Applications

+ Add New Application

Search Configured Applications

2 Applications

Export Metadata

Delete

Run Users To SSO Applications Report

	Status	Logo	Display Label ^	Show In User Portal ^	Supported Functionality	IdP Certificate Status
☐		Custom SAML App		Yes		Expires 03-03-2030 >
☐		Custom SAML App		Yes		Expires 03-05-2030 >

Step 2: Search for **OpenID** and select **"Custom OIDC App"** and click on **"Next"**

Create New Application Integration

X

1 Select Application

2 Select Options

3 Enter General Info

4 Review

Which application would you like to integrate?

Search from our ever-growing app catalog, or create a custom integration.

OpenID Connect

Logo	Application	Supported Functionality
	OpenID Connect	
Custom OIDC App		

Pro Tip: You may also be able to configure identity management with SCIM or through a custom REST API. Check with *OpenID Connect* to confirm what is supported.

Cancel

Back

Next

Step 3: Change the **Display Label** and click on **Next**

Create New Application Integration



Progress bar: 1. Select Application, 2. Select Options, 3. Enter General Info, 4. Review

Display Label *

Ezeelogin OIDC

Description

Add a description that users will see if the application is set to show in user portal.

Show in User Portal

Applications appear in the User Portal for any bound users by default. When deselected, the application will not appear in the User Portal for any users, and any users bound to the application will still be enabled for SSO access.

☒ Show this application in User Portal

User Portal Image

☒ Logo

☐ Color Indicator

Preview Image

Custom OIDC App

Upload or drag a file

Choose A File

Default file displayed.

Cancel Back Next

Step 4: On the next page click on **"Configure Application"**

Create New Application Integration



Progress bar: 1. Select Application, 2. Select Options, 3. Enter General Info, 4. Review

Custom OIDC App

Ezeelogin OIDC is about to be added

Ezeelogin OIDC must be configured in order to be added to the app catalog.
Click Configure Application to complete the setup.

Application Summary

Display Label	Ezeelogin OIDC
Visibility	This application will appear in User Portal for all assigned users.
Enabled Features	SSO with OIDC

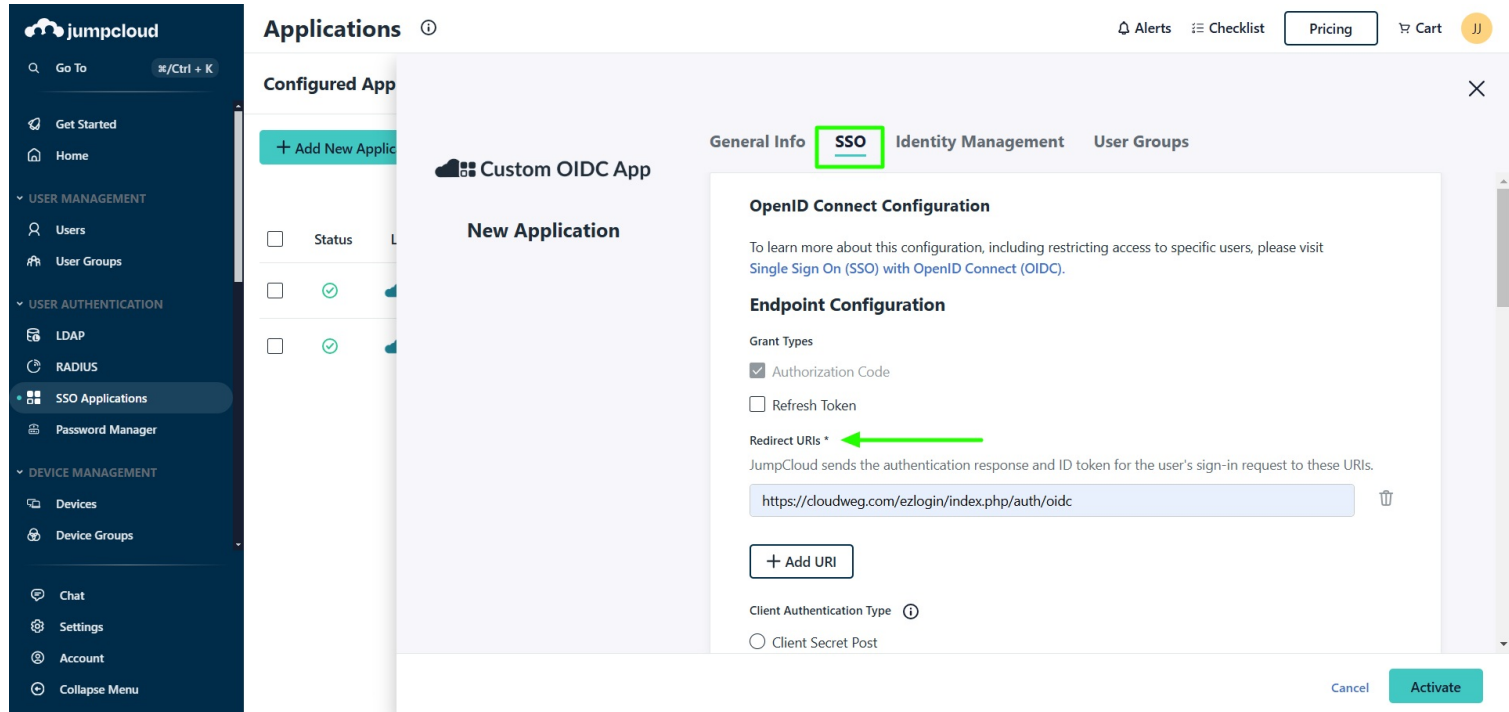
Up Next: Configure Your New Application

Configure the enabled features to activate and save the integration with this application.

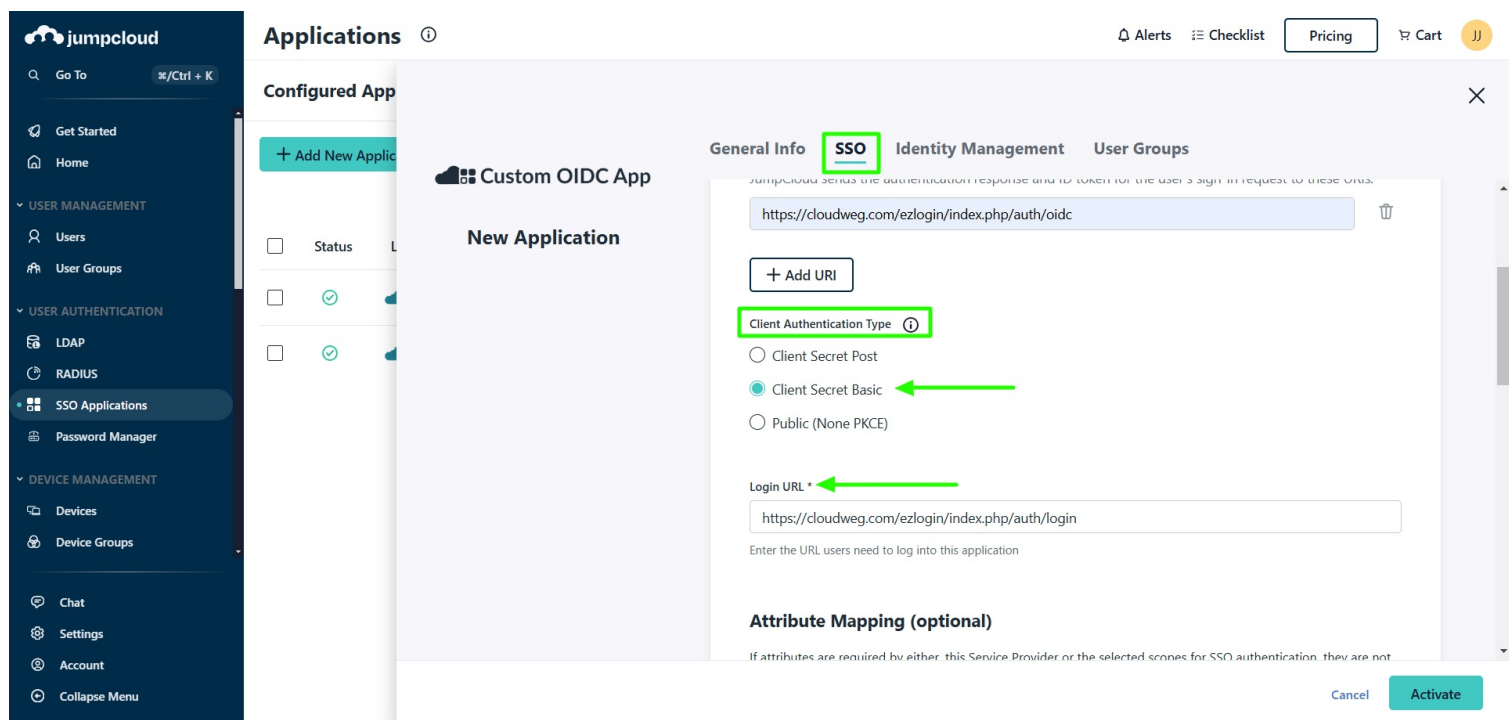
[Learn More](#)

Cancel Back Configure Application

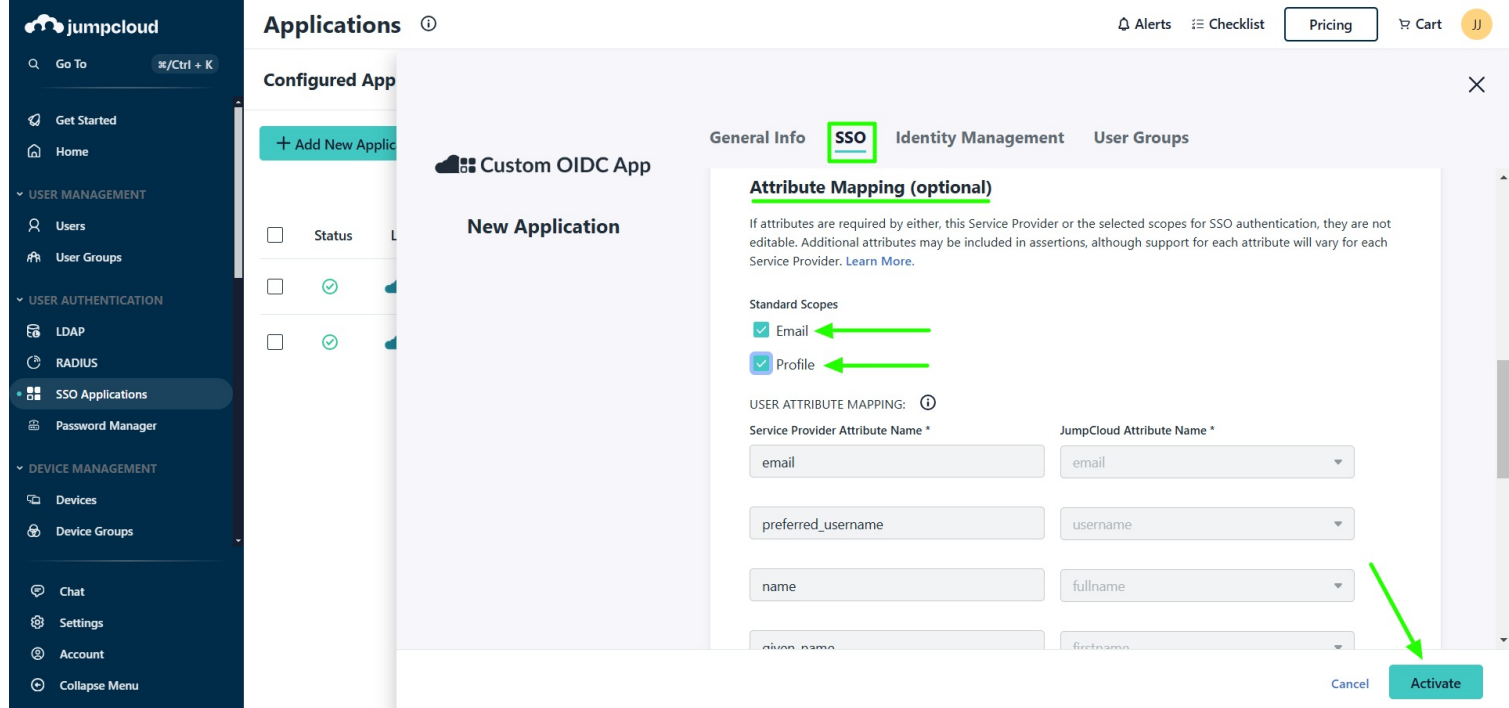
Step 5: Under the **Redirect URL**, paste the **OIDC URL** obtained from Ezeelogin in **Step 1**.



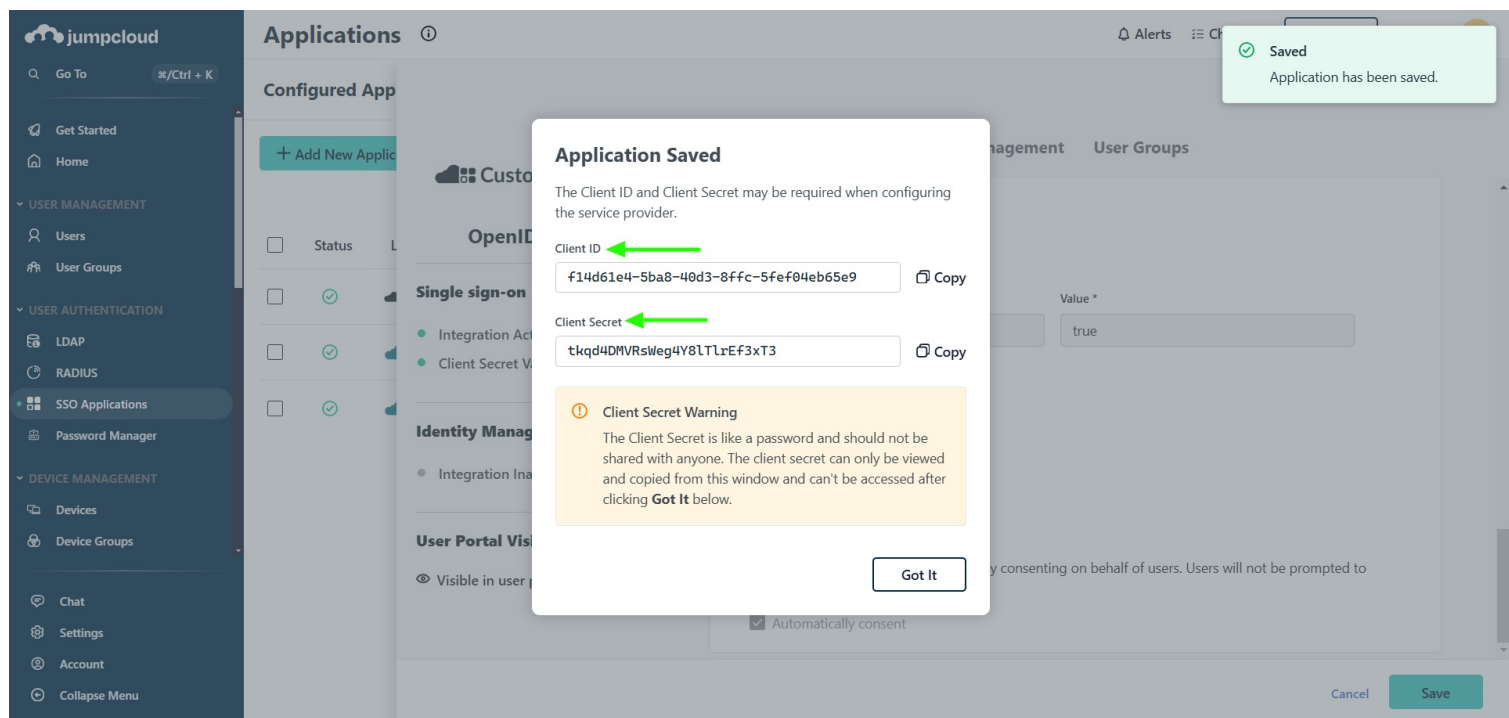
Step 6: Select "**Client Authentication Type**" as "**Client Secret Basic**". Also provide the login URL. For the Login URL, modify the OIDC URL by replacing the last part "**OIDC**" with "**login**". (Example : change <https://cloudweg.com/ezlogin/index.php/auth/oidc> to <https://cloudweg.com/ezlogin/index.php/auth/login>)



Step 7: Under "**Attribute Mapping**" enable "**Email**" and "**Profile**". After providing all the above details click on "**Activate**".



Step 8: From the next page, copy the **Client ID** and **Client Secret**, then paste them into the web GUI OpenID Connect settings. Additionally, enter the Provider URL as **https://oauth.id.jumpcloud.com/** in the web GUI.



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

OpenID Connect Client Info

Redirect URLhttps://cloudweg.com/ezeelogin/index.php/auth/oidc

OpenID Connect Settings

Client ID5a4a4040-4e22-4401-89dc-69bc2a2567cb

Client Secretv-gTZ2QMmDxE_btzF34qxb58v6

Provider URLhttps://oauth.id.jumpcloud.com/

Email Attribute

Username Attribute

Group Attribute

Firstname Attribute

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

Follow steps 1 to 8 to create new application for secondary node. While adding the application details in Jumpcloud, 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

c2b7f9a4-3d81-4f6e-9a2c-7e5b1d4f8c90

Client Secret

mX9rT2QpLs_ztF6aW8yK3b

HTTP Proxy URL

Path To CA Bundle

Azure AD Settings

Advanced

Step 9: Provide the attribute names in the web GUI which can be found under "**Service Provider Attribute Name**" section of JumpCloud. After providing all the attributes click on "**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

OpenID Connect Settings

Client ID

3dd3a07b-d6b1-4798-baf6-8bbcc6ffa4cb

Client Secret

2DKrNxUY.DBNdVpg8iYM8pErSc

Provider URL

https://oauth.id.jumpcloud.com/

Email Attribute

email

Username Attribute

preferred_username

Group Attribute

groups

Firstname Attribute

given_name

Lastname Attribute Name

family_name

Cancel

Save

Custom OIDC App

OpenID Connect

Single sign-on

Integration Active

Client Secret Valid

Identity Management

Integration Inactive

User Portal Visibility

Visible in user portal

General Info

SSO

Identity Management

User Groups

Attribute Mapping (optional)

If attributes are required by either, this Service Provider or the selected scopes for SSO authentication, they are not editable. Additional attributes may be included in assertions, although support for each attribute will vary for each Service Provider. [Learn More](#).

Standard Scopes

Email

Profile

USER ATTRIBUTE MAPPING:

Service Provider Attribute Name *

email

preferred_username

name

given_name

family_name

middle_name

JumpCloud Attribute Name *

email

username

fullname

firstname

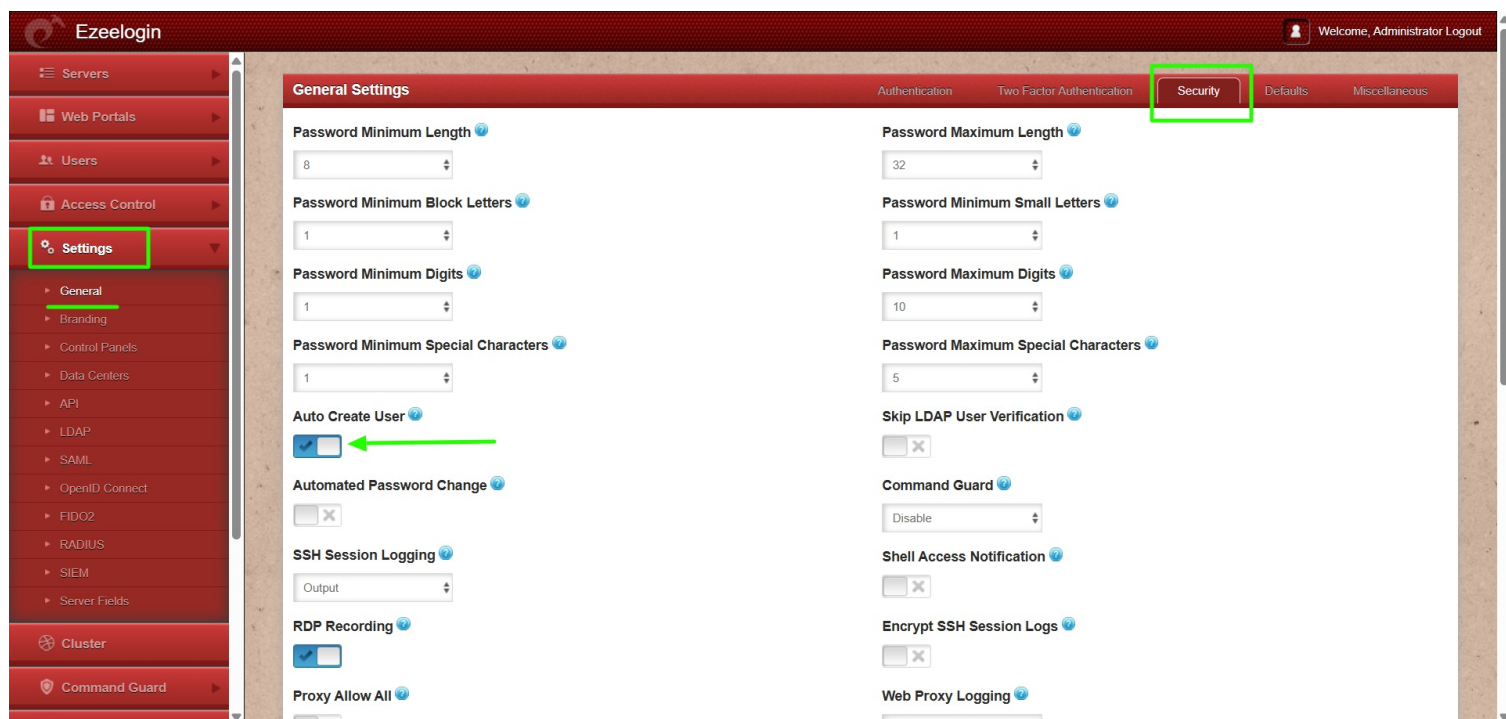
lastname

middlename

Cancel

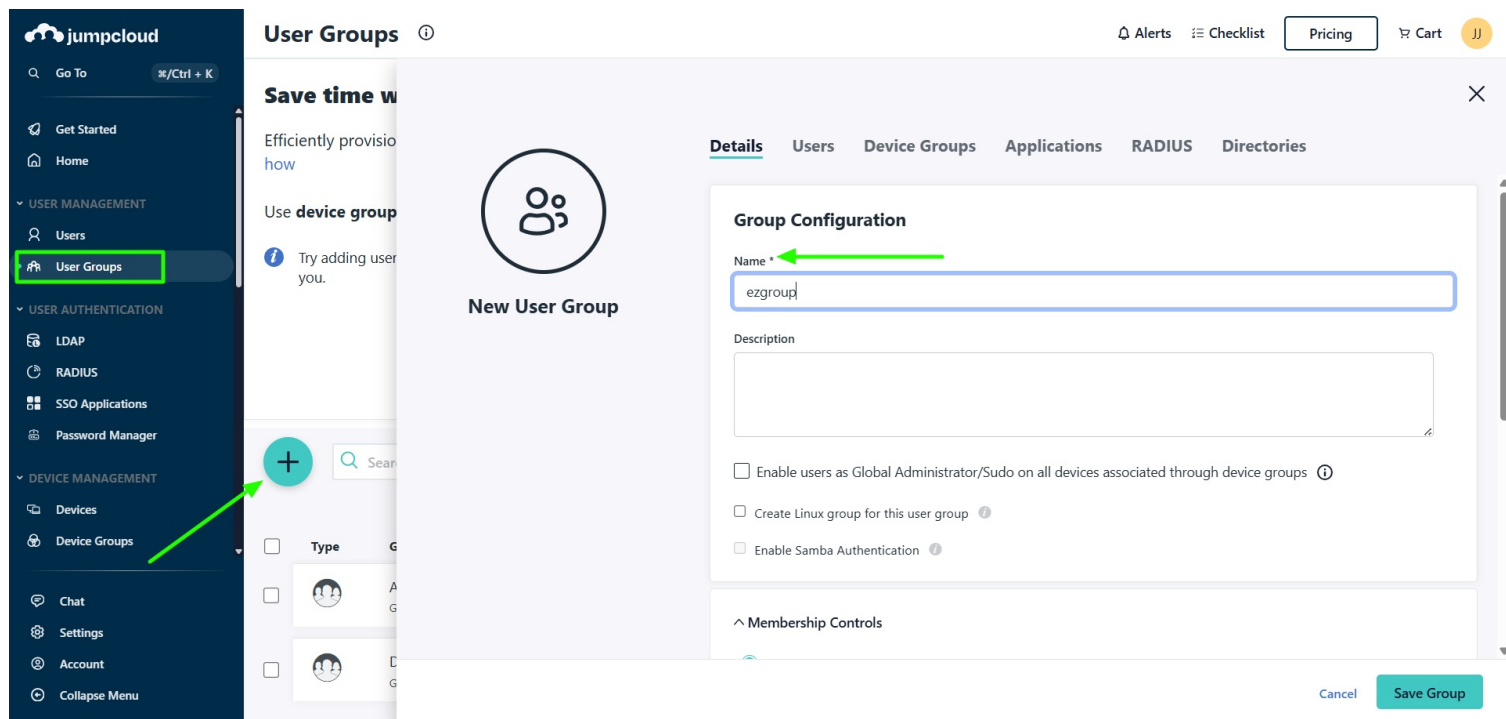
Save

Step 10: Enable Auto Create User from **Ezeelogin GUI** -> **Settings** -> **General** -> **Security** -> **Enable Auto Create User**, so the user will automatically created after successful authentication from Jumpcloud.



Step 11: Create usergroup in Jumpcloud

Step 11(A): Select the user group tab from the left panel, add the user group name.



Step 11(B): Assign the usergroup to the OIDC application and save it.

jumpcloud

Go To %/Ctrl + K

Get Started

Home

USER MANAGEMENT

Users

User Groups

USER AUTHENTICATION

LDAP

RADIUS

SSO Applications

Password Manager

DEVICE MANAGEMENT

Devices

Device Groups

Chat

Settings

Account

Collapse Menu

User Groups

Save time w

Efficiently provision how

Use device group

Try adding user you.

New User Group

Details Users Device Groups **Applications** RADIUS Directories

This user group is bound to the following applications:

Search

Run Users To SSO Applications Report

Status	Name	Display Label	Supported Functionality	Show in User Portal
☒	Custom OIDC App	Ezeelogin OIDC		Yes
☐	Custom SAML App	Ezeelogin SAML 20		Yes
☐	Custom SAML App	SLAVE SAML		Yes

Cancel Save Group

Step 12: Create users in Jumpcloud

Step 12(A): To add users, navigate to Users tab, and click on + icon. This will open a form where you can enter the necessary user details and set a password for the user.

jumpcloud

Go To ⌘/Ctrl + K

Get Started

Home

USER MANAGEMENT

- Users
- User Groups

USER AUTHENTICATION

- LDAP
- RADIUS
- SSO Applications
- Password Manager

DEVICE MANAGEMENT

- Devices
- Device Groups

Chat

Settings

Users 1

Set the default

All 2 Staged

User State

Suspended

Active

Staged

New User

Jake@gmail.com

Staged

Security Status

Password Pending

Details

User Groups

Devices

Directories

User Information

First Name

Middle Name

Last Name

Jake

Lee

* Username

Display Name

Jake

+ local user account

Managed Apple ID

* Company Email

Alternate Email

Jake@gmail.com

Description

^ User Security Settings and Permissions

Externally Managed Password

If you select something other than **None (JumpCloud)**, you are enabling an externally managed password authority and the user will be prevented from making password updates in JumpCloud.
[Learn More](#)

Password Authority

None (JumpCloud)

Delegated Authentication

Selecting a delegated authority means the user's password will be validated by the selected application. [Learn More](#)

Delegated Authority

None

Password Recovery Email

Password Settings

Specify initial password

Use this setting if the user's email address does not exist yet.

New Password *

.....

Not contain your username

Have at least 8 characters

Have less than 64 characters

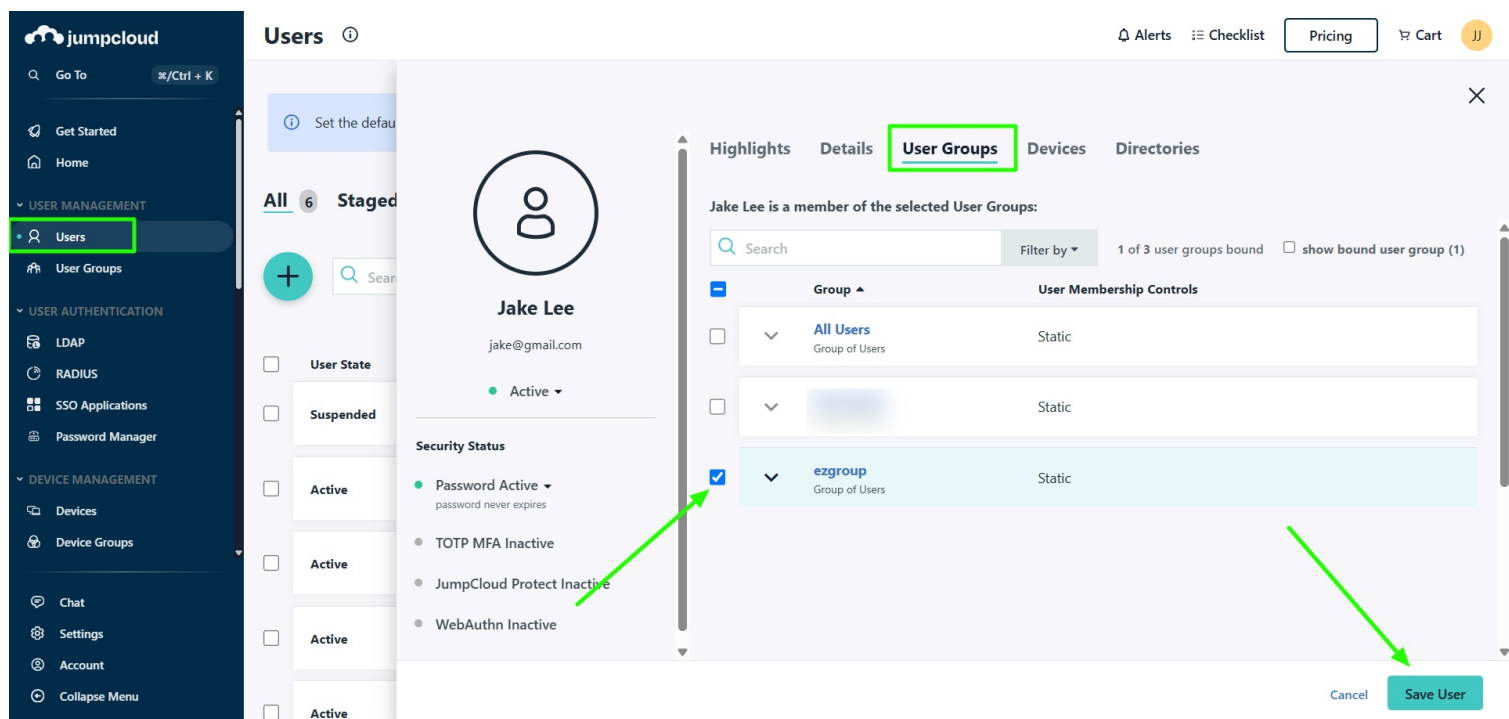
Have one lowercase character

Have one capital letter

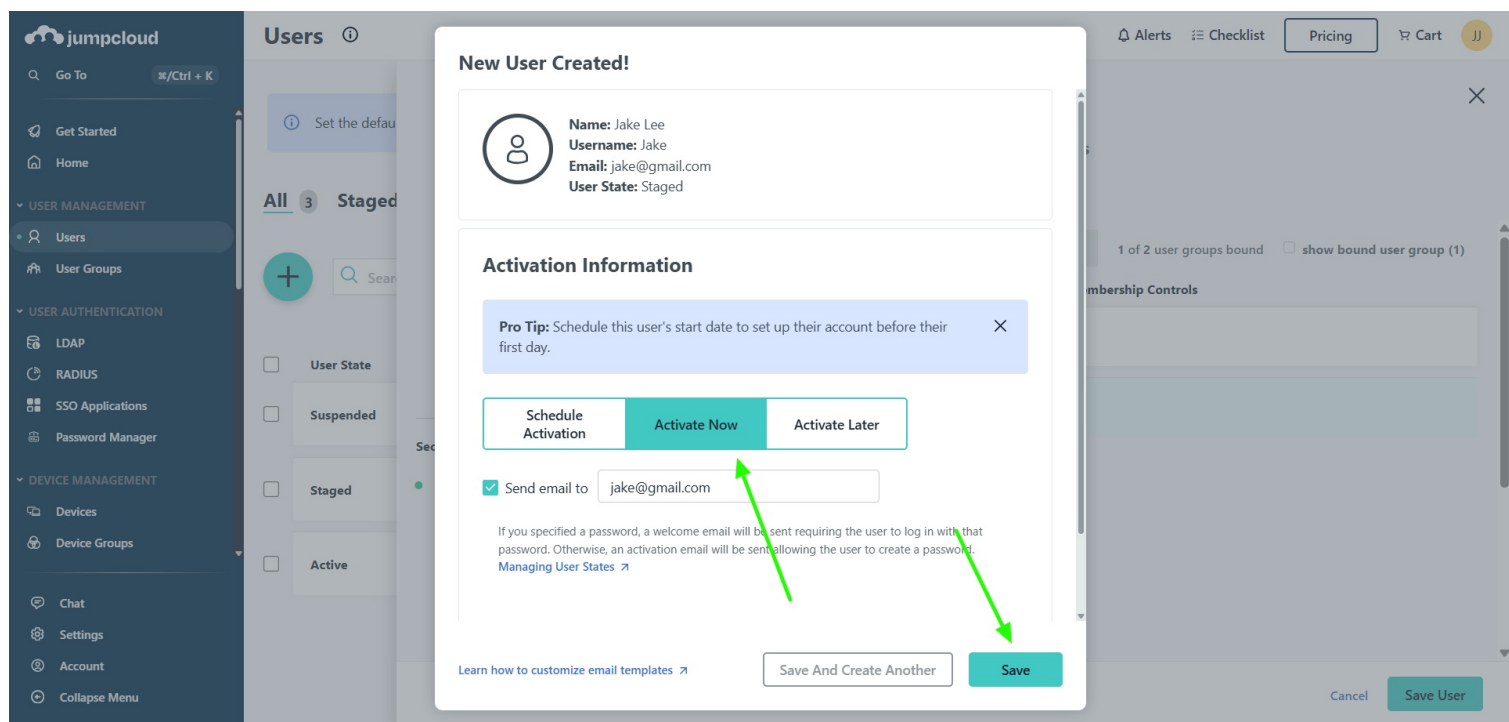
Have one number

Have one special character (!@#\$%^&*~_)

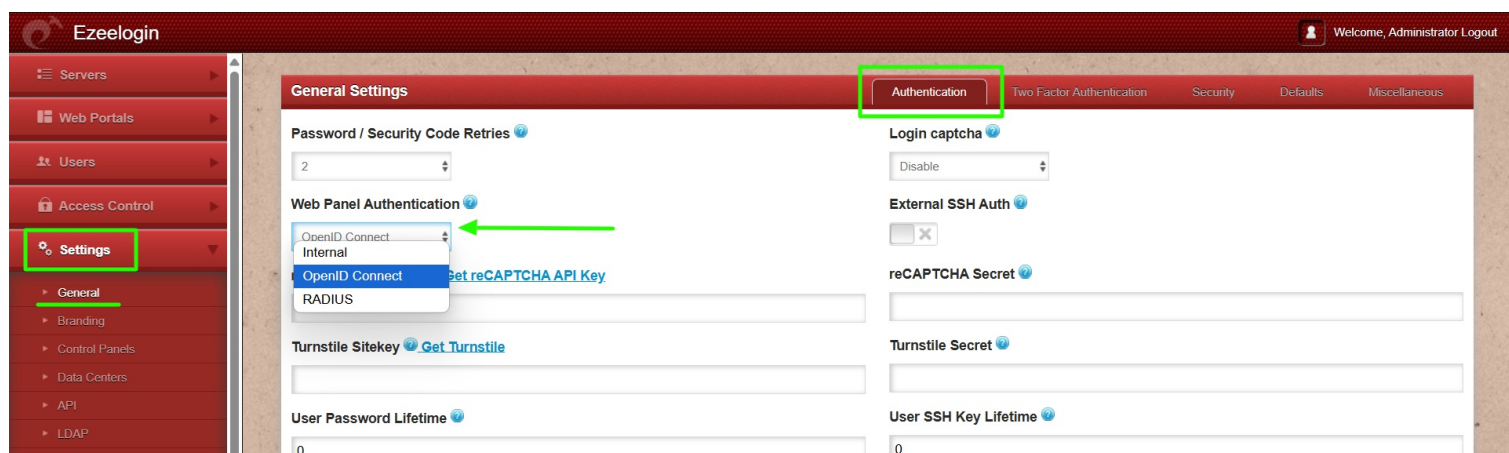
Step 12(B): Assign usergroup for the new user and save it



Step 12(C): Next activate the new user and click on save.



Step 13: Set **Web Panel Authentication** to **OpenID Connect** under **Settings** -> **General** -> **Authentication** -> **OpenID Connect**.



Step 14: Login into the **Ezeelogin GUI** and you will see the **Jumpcloud login Page** where you will need to enter the Jumpcloud user login credentials to be authenticated into the Ezeelogin.

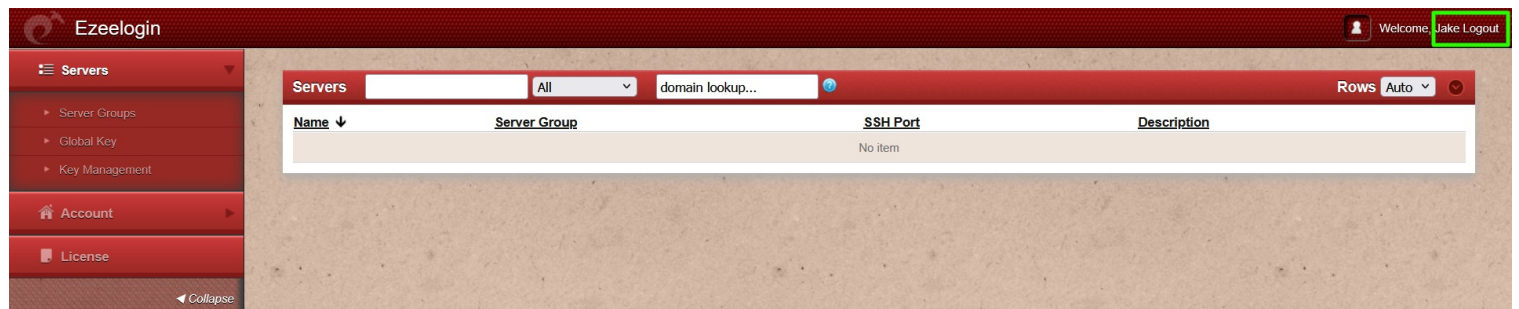
**Log in to your application using
JumpCloud**

Email

☐ Remember me

[Continue](#)

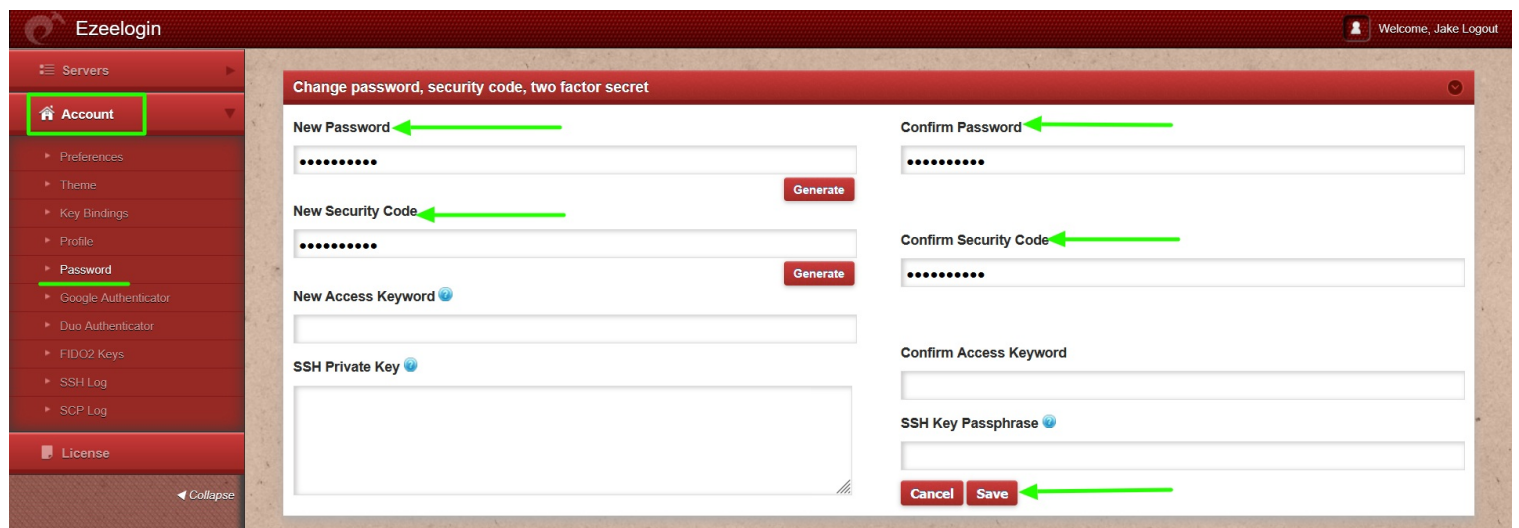
Step 15: Finally, you will be logged into the **web GUI using OpenID Connect Authentication**. The user will be created automatically in Ezeelogin after successful authentication from Jumpcloud.



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

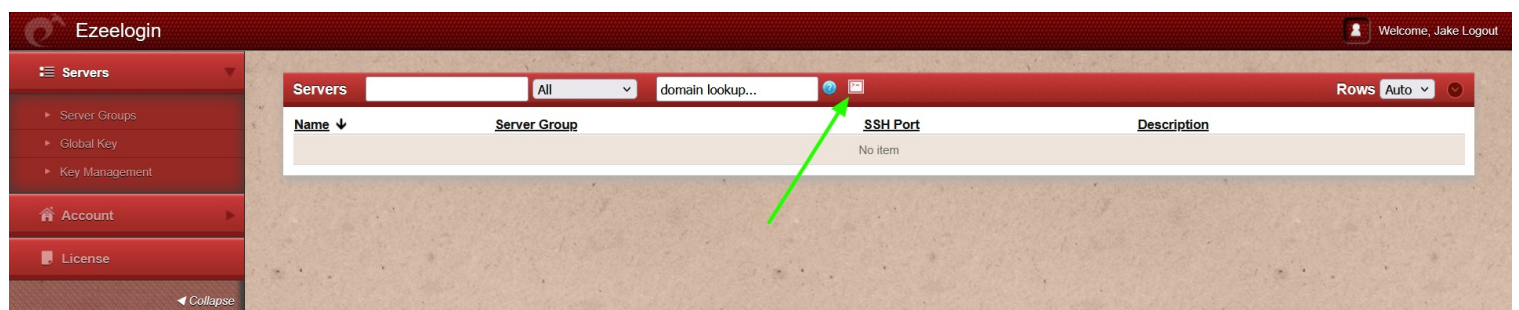
Error: Invalid password

Step 16: After logging into the GUI, you need to **reset the password and security code of the user** under **Account -> Password** in order to SSH to the ezsh shell.



Step 17: You can log in to Ezeelogin shell via **Webssh** shell or using any SSH client such as Putty or terminal etc.

Step 17(A): Click on the '**Open Web SSH Console**' icon to SSH via the browser.



Step 17(B): After resetting the password and security code you can **SSH to the ezsh shell** (using Terminal or Putty) with the **OpenID connect username**.

```
root@desktop:~#
root@desktop:~# ssh Jake@cloudweg.com
Jake@cloudweg.com's password: 
```

Step 18: After logging into ezsh, the server list will be visible. The user can navigate using the Up and Down arrow keys and login to a server by pressing the Enter key.

```
*client.testing      Portals
Production.servers  Online gateway server
Testing.Server       Testing
All servers          List of all accessible servers

GROUPS [Normal / ]
Start typing string to locate. ESC: Clear search, F1/+: Help, F4/!: Exit.
≡ Menu | Ezeelogin | SSH CONNECTION ESTABLISHED
```

How to map Jumpcloud 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.

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

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](#).

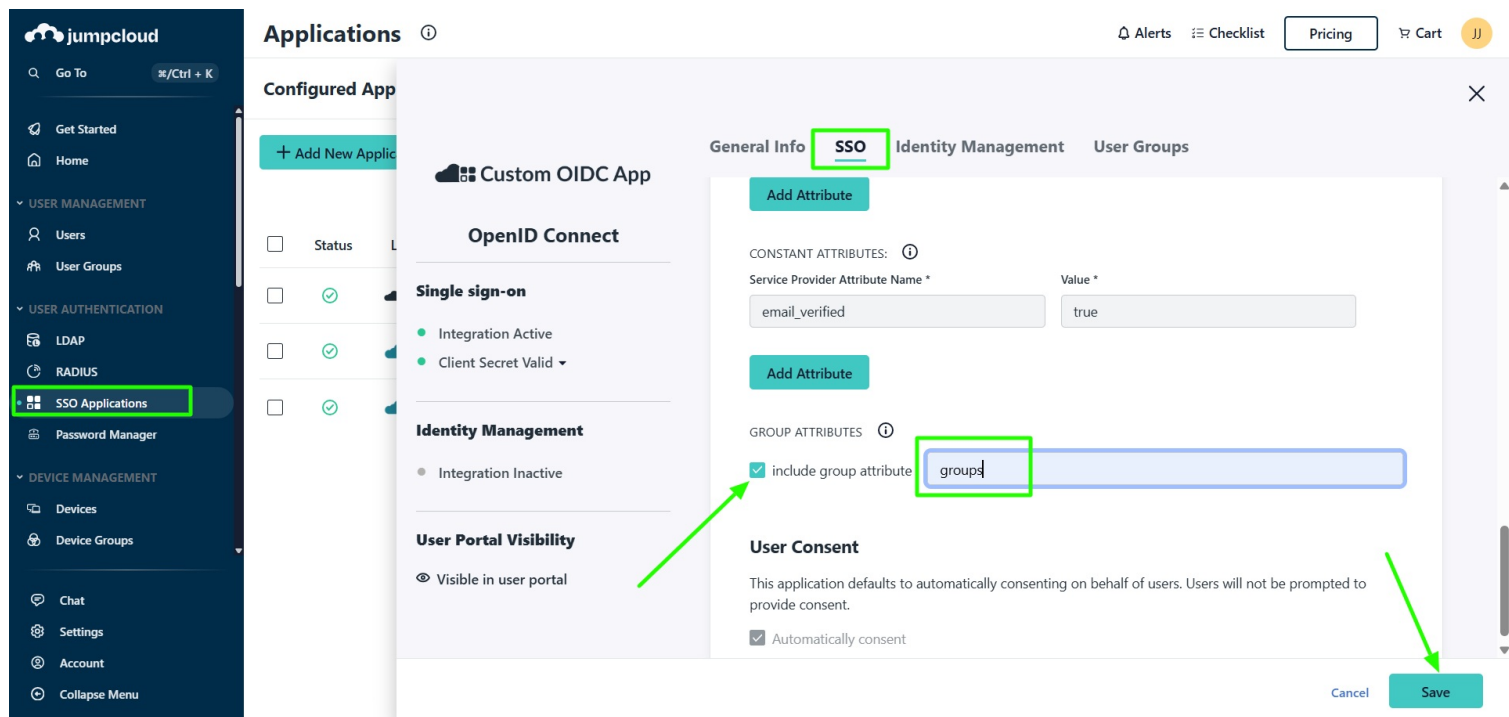
Note:

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 JumpCloud), the updated group will be shown in the Ezeelogin GUI after the user logs in again.

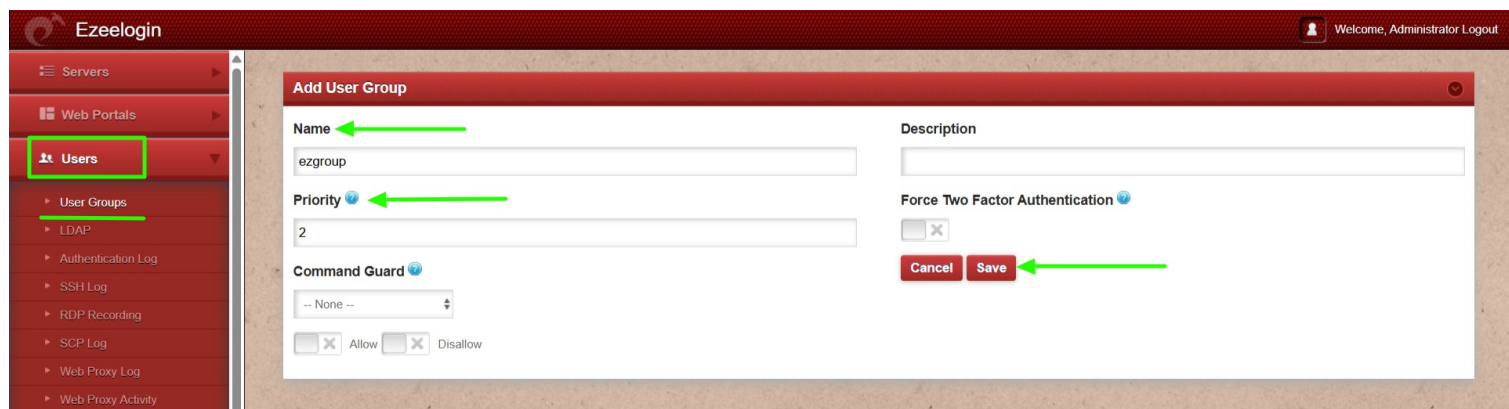
This feature is available from Ezeelogin version 7.46.0. Refer article to [upgrade Ezeelogin to the latest version](#).

Step 1: Edit your custom OIDC app, navigate to **SSO**, enable "**Include Group Attribute**," enter "**groups**" in the field, and save the changes.

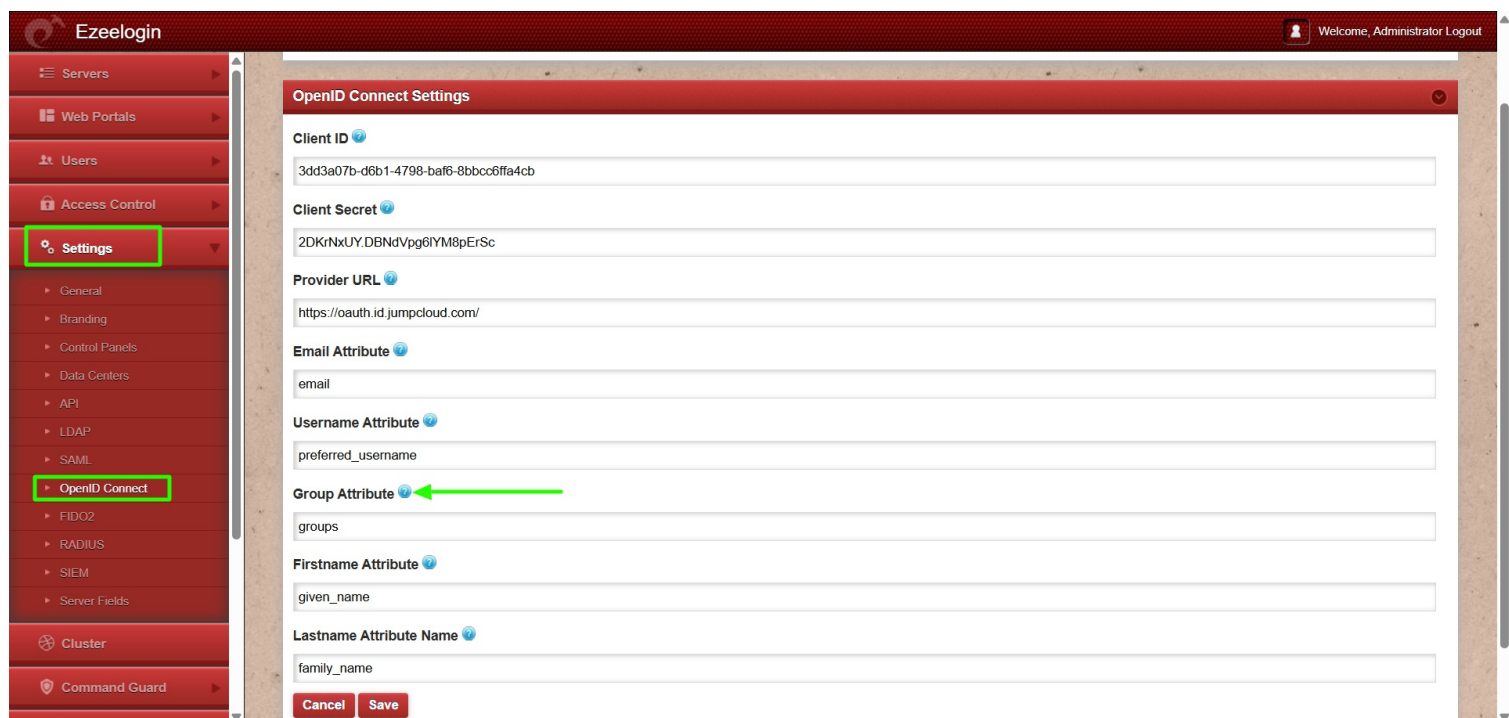


Step 2: Create the user group and users, then assign the user group for the users as specified in Steps 11 and 12.

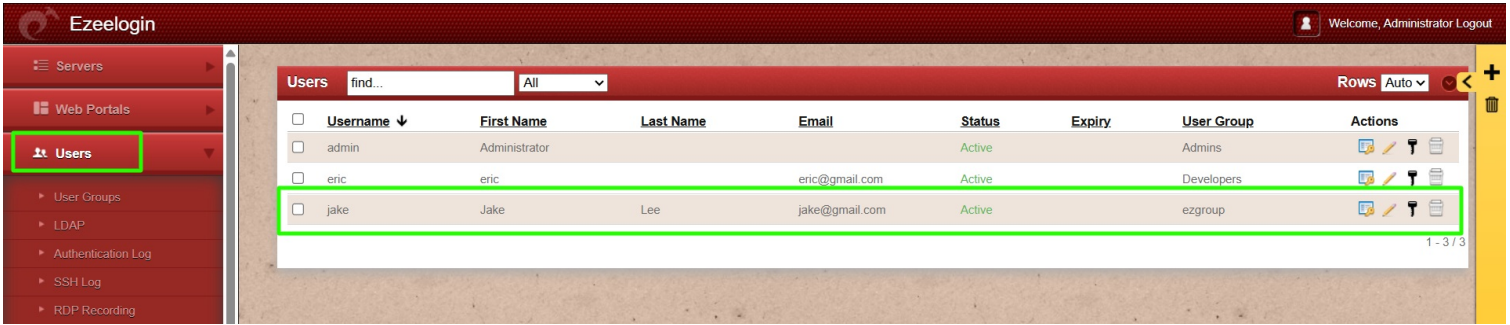
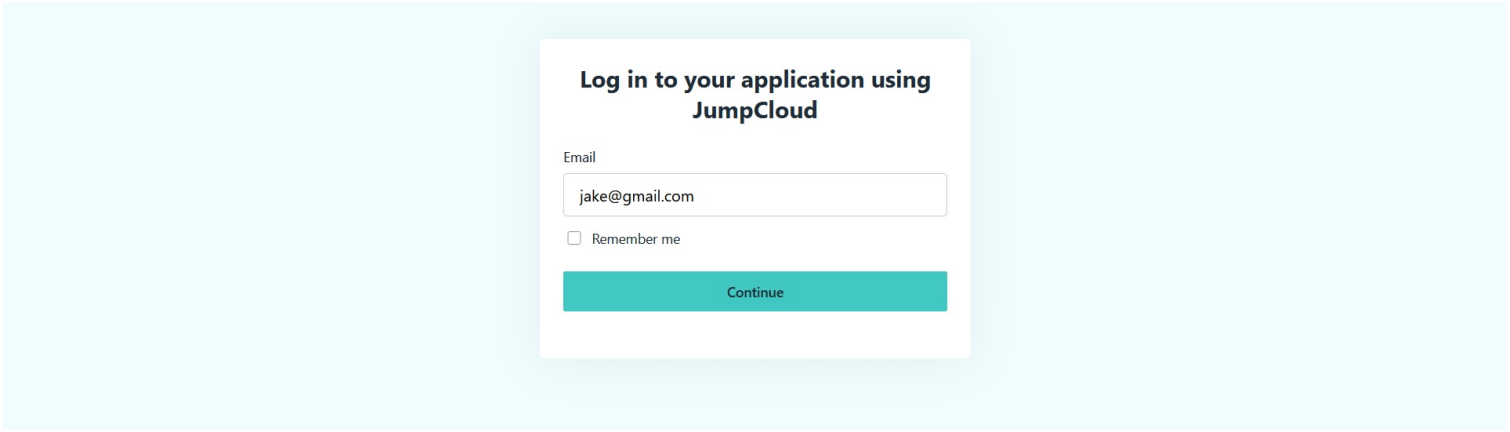
Step 3: Create a user group in the web GUI with the same name as in Jumpcloud with priority set as mentioned below.



Step 4: In the web GUI. Navigate to **Settings > OpenID Connect > Add the group attribute name** and save it.

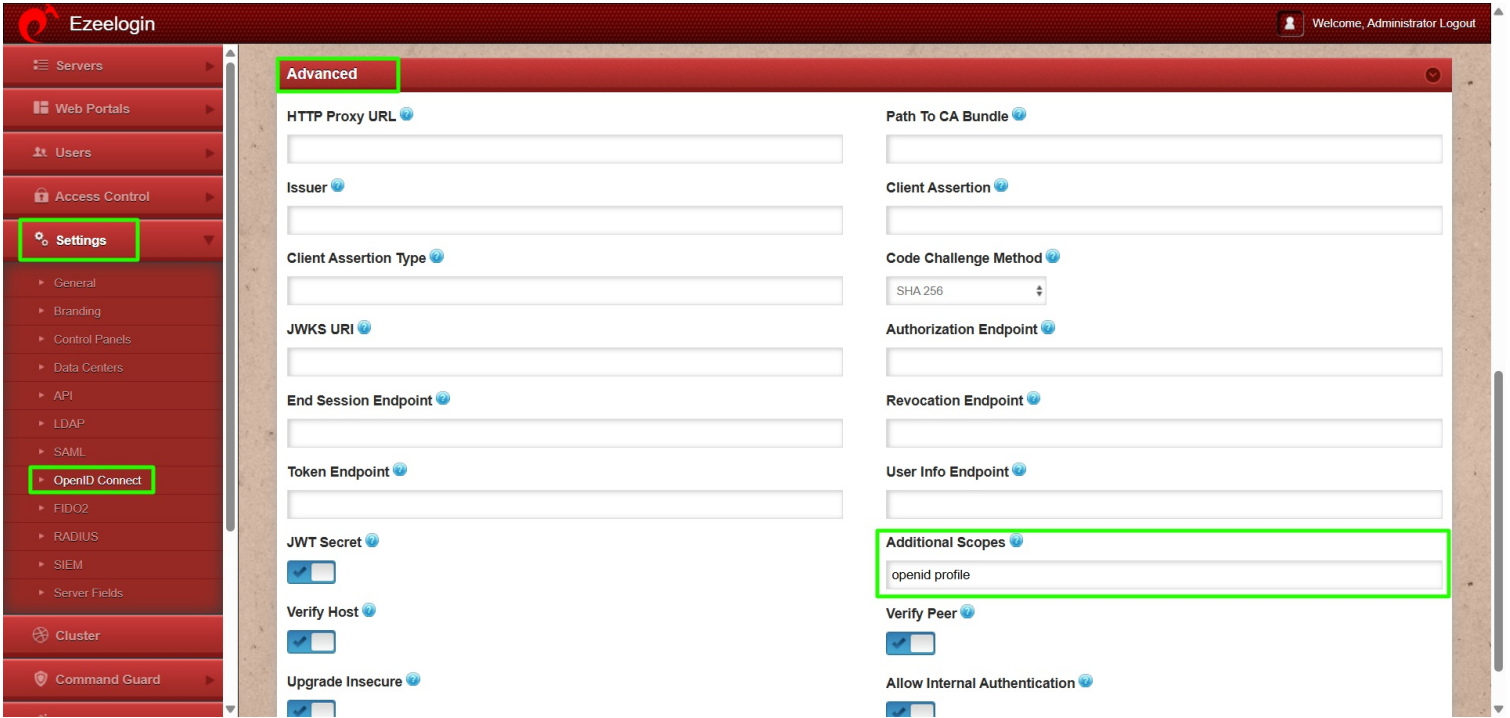


Step 5: Log in to the web GUI using JumpCloud user credentials, and the user will be assigned to the same group in Ezeelogin as in JumpCloud.



How to add additional scope from Jumpcloud OpenID connect to Ezeelogin jumpserver?

Step 1: Navigate to **Settings -> OpenID Connect** under OIDC advanced settings, specify the additional scopes separated by spaces, and save the settings.



This feature is available from **Ezeelogin version 7.41.0**. Refer article to [upgrade Ezeelogin to the latest version](#).

Related Articles:

[Integrate Jumpcloud SSO with Ezeelogin](#)

[Integrating SSO/SAML with Ezeelogin PAM](#)

