

# Integrate Azure OpenID Connect

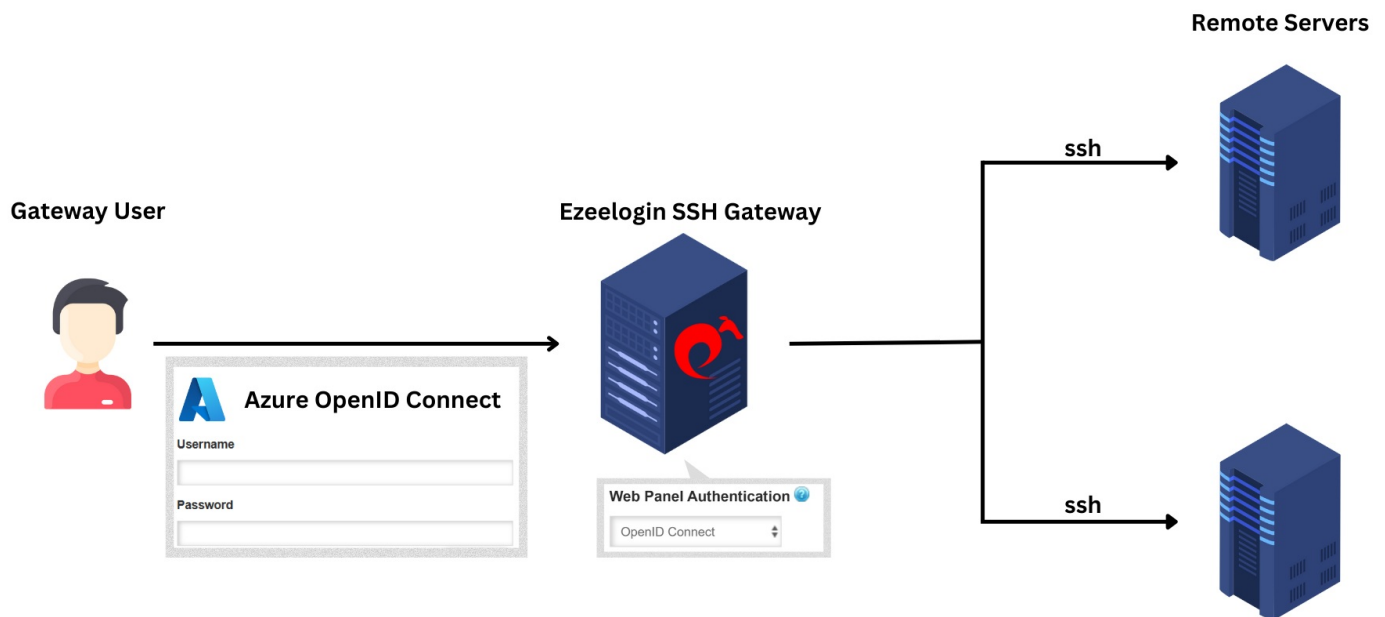
769 Nesvin KN May 28, 2026 Productivity & Efficiency Features

2193

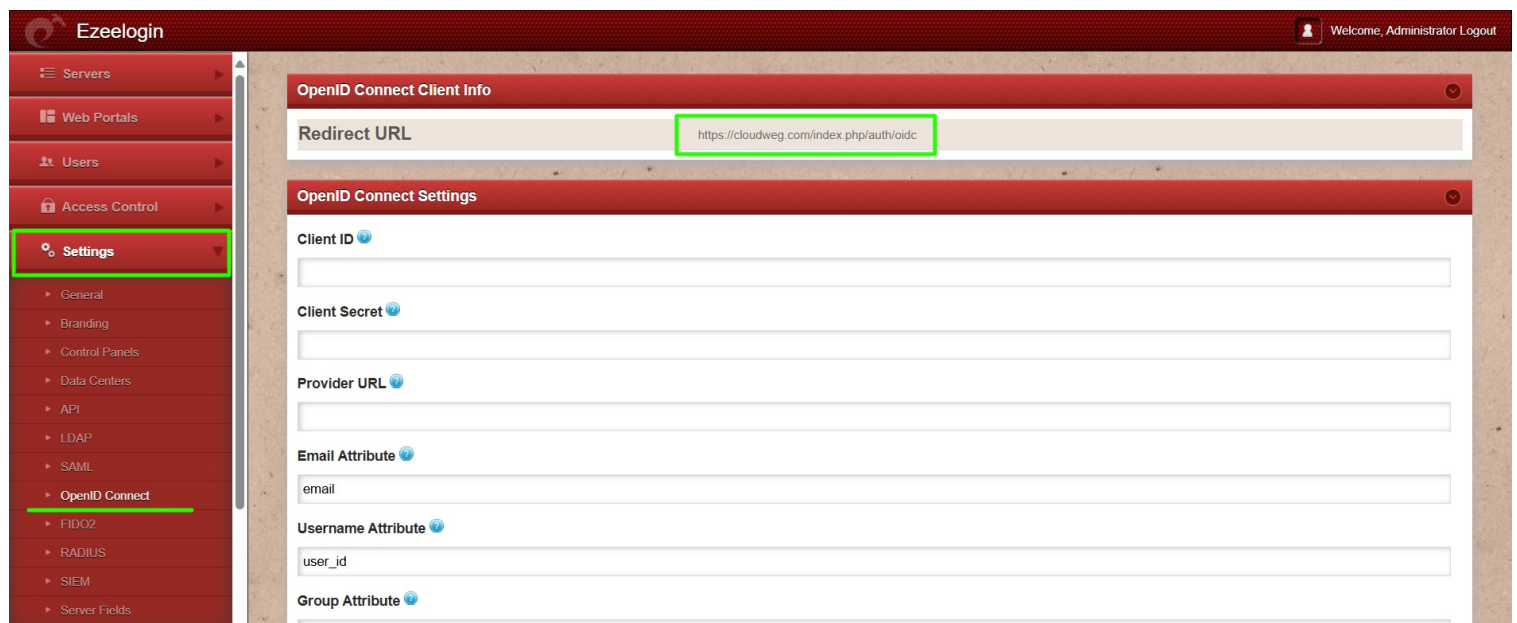
## How to integrate Azure OpenID connect with Ezeelogin jumpserver?

**Overview:** This article will help Ezeelogin super admin user to integrate Azure OpenID Connect with the Ezeelogin jump server.

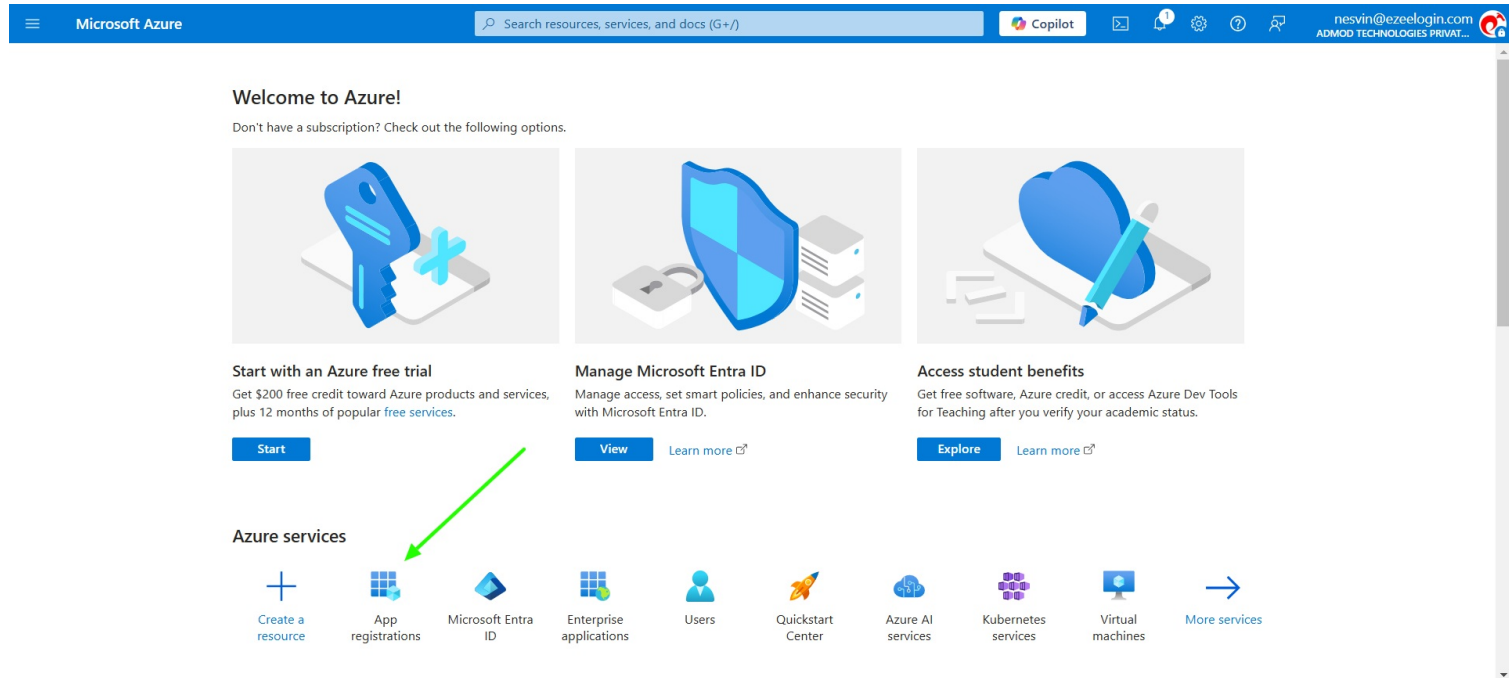
**Note:** OpenID connect is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



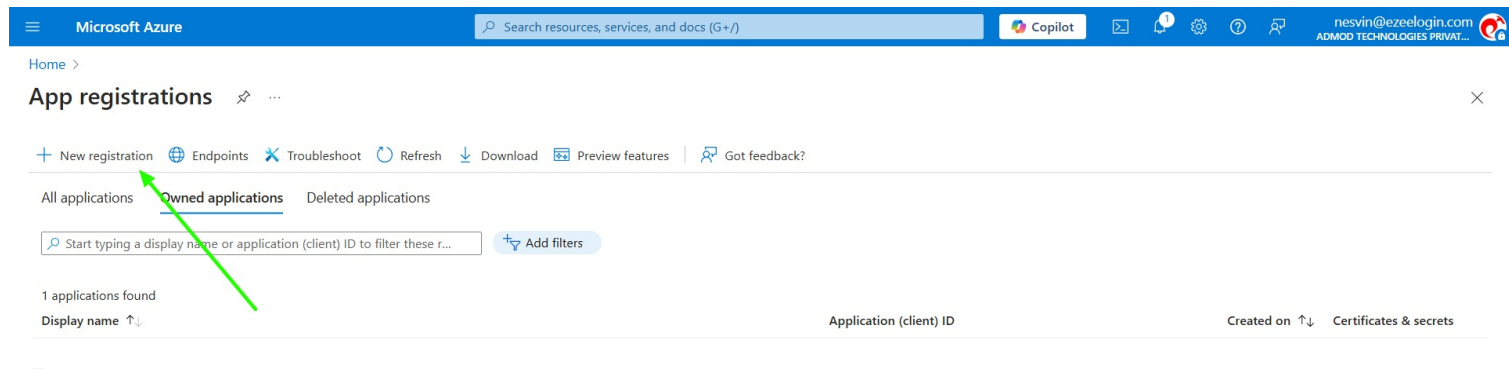
**Step 1:** Login to **web GUI** and click on **Settings** -> **OpenID Connect** and copy '**redirect URL**'.



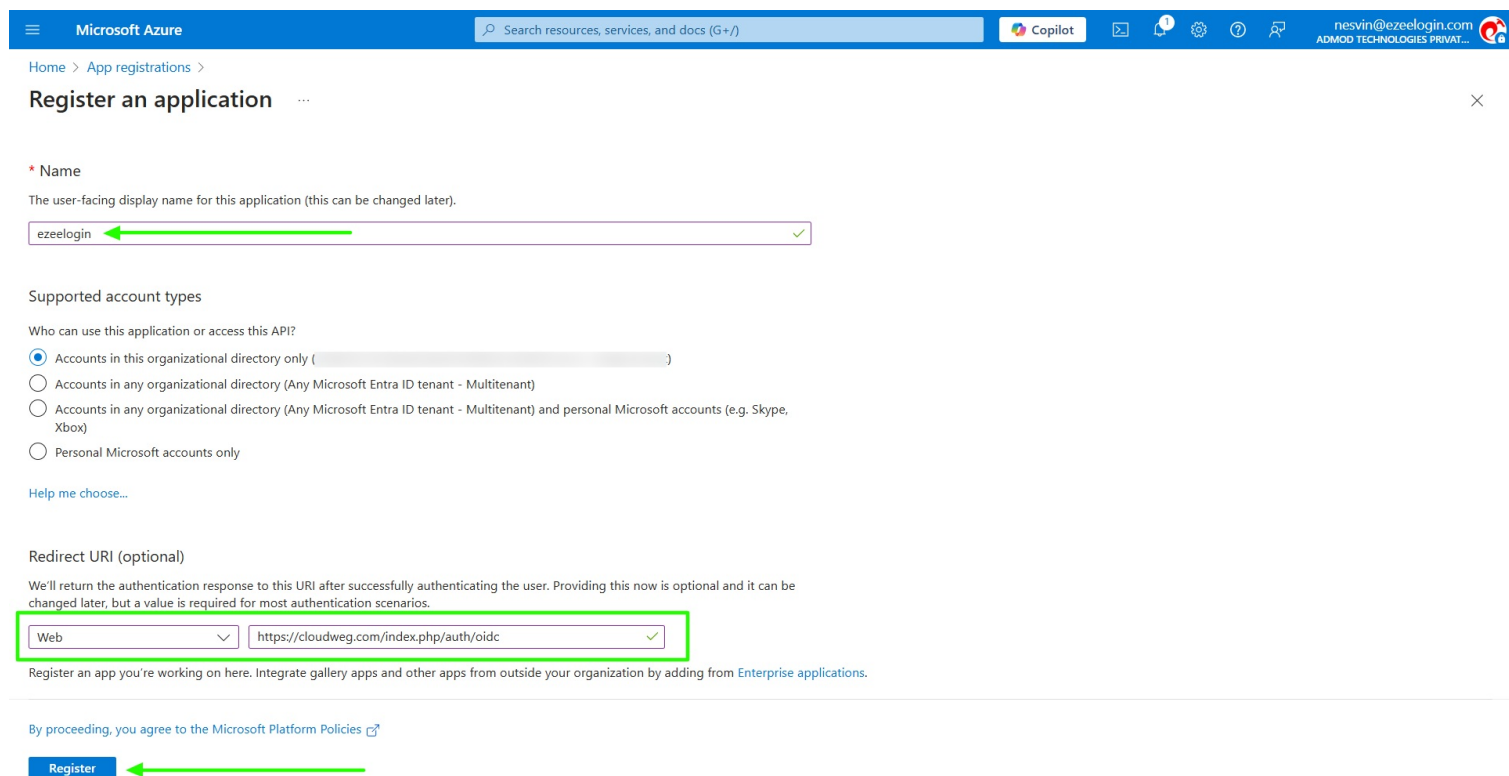
**Step 2:** Login to **Azure portal** and select '**app registration**'.



**Step 3:** Register new application.



**Step 4:** Provide the **application name** and select the **supported account type**. Under the **redirect URL**, select **"Web"** and paste the **OIDC URL from Ezeelogin**.



**Step 5:** Click on **"Add a certificate or secret"** to create a new client secret.

Microsoft Azure

Home > App registrations > ezeelogin

Search resources, services, and docs (G+)

Copilot

nesvin@ezeelogin.com

ADMOD TECHNOLOGIES PRIVAT...

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : ezeelogin

Application (client) ID : 63256dab-2e09-4a0d-b3d9-d06173c2a9fd

Object ID : dc71caf4-2479-4e15-b11f-d5e624ebaa6

Directory (tenant) ID : f36f9ec9-2335-46ca-bb07-eb273cc241ad

Supported account types : My organization only

Client credentials : Add a certificate or secret

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in I... : ezeelogin

**Step 6:** Click on "New client secret", provide a name, and click "Add" to generate a new client secret.

Microsoft Azure

Home > App registrations > ezeelogin

Search resources, services, and docs (G+)

Copilot

nesvin@ezeelogin.com

ADMOD TECHNOLOGIES PRIVAT...

ezeelogin | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

Support + Troubleshooting

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description Expires Value

No client secrets have been created for this application.

Add a client secret

Description ezeelogin

Expires Recommended: 180 days (6 months)

Add Cancel

**Step 7:** Copy the **secret value** from the list and **paste** it into the web GUI OpenID Connect settings. (It will be displayed as encrypted after some time.)

Microsoft Azure

Home > App registrations > ezeelogin

Search resources, services, and docs (G+)

Copilot

nesvin@ezeelogin.com

ADMOD TECHNOLOGIES PRIVAT...

ezeelogin | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Got a second? to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description Expires Value Secret ID

ezeelogin 18/8/2025 7Tc8Q-V0X7gRdRa9-vYaMPsk0\_0Ev-Bk3... 84be42cc-2641-4014-a558-ba99123b35...

**Step 8:** Copy the **Client ID** from the **Overview** tab and paste it into the **web GUI OpenID Connect settings**.

Microsoft Azure

Home > App registrations >

ezeelogin

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

|                         |                                        |                             |                               |
|-------------------------|----------------------------------------|-----------------------------|-------------------------------|
| Display name            | : ezeelogin                            | Client credentials          | : 0 certificate_1 secret      |
| Application (client) ID | : 63256dab-2e09-4a0d-b3d9-d06173c2a9fd | Redirect URIs               | : 1 web_0 spa_0 public client |
| Object ID               | : dc71caf4-2479-4e15-b11f-d5e624ebaea6 | Application ID URI          | : Add an Application ID URI   |
| Directory (tenant) ID   | : f36f9ec9-2335-46ca-bb07-eb273cc241ad | Managed application in I... | : ezeelogin                   |
| Supported account types | : My organization only                 |                             |                               |

**Step 9: Paste** the client ID and **client secret** from **Azure** to **web GUI OpenID connect settings**.

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

OpenID Connect Client Info

Redirect URL

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

OpenID Connect Settings

Client ID

63256dab-2e09-4a0d-b3d9-d06173c2a9fd

Client Secret

7Tc8Q~V0X7gRdRa9-vYaMPsk0\_0Ev-Bk3Pw5haXD

Provider URL

Email Attribute

email

Username Attribute

user\_id

**Step 10: Copy** the **Tenant ID** from **Azure** and paste it into the **Provider URL** field in the **web GUI OpenID Connect settings**, as shown in the example below:

**Provider URL:** **https://login.microsoftonline.com/{tenant}/v2.0**

**Example:** **https://login.microsoftonline.com/f36f9ec9-2335-46ca-bb07-eb273cc241ad/v2.0**

Microsoft Azure

Home > Enterprise applications | All applications >

ezeelogin

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Support + Troubleshooting

Essentials

|                         |                                        |                             |                               |
|-------------------------|----------------------------------------|-----------------------------|-------------------------------|
| Display name            | : ezeelogin                            | Client credentials          | : 0 certificate_1 secret      |
| Application (client) ID | : 63256dab-2e09-4a0d-b3d9-d06173c2a9fd | Redirect URIs               | : 1 web_0 spa_0 public client |
| Object ID               | : dc71caf4-2479-4e15-b11f-d5e624ebaea6 | Application ID URI          | : Add an Application ID URI   |
| Directory (tenant) ID   | : f36f9ec9-2335-46ca-bb07-eb273cc241ad | Managed application in I... | : ezeelogin                   |
| Supported account types | : My organization only                 |                             |                               |

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

Collapse

OpenID Connect Client Info

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

OpenID Connect Settings

Client ID63256dab-2e09-4a0d-b3d9-d06173c2a9fd

Client Secret7Tc8Q~V0X7gRdRa9-vYaMPsk0\_0Ev~Bk3Pw5haXD

Provider URLhttps://login.microsoftonline.com/f36f9ec9-2335-46ca-bb07-eb273cc241ad/v2.0

Email Attributeemail

Username Attributeuser\_id

Group Attribute

Firstname Attributegiven\_name

Lastname Attribute Namefamily\_name

CancelSave

Advanced

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

**Follow steps 1 to 9 to create new application for secondary node. While adding the application details in Azure, 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

8f47c2a1-91b3-4e5d-a7c2-5d9f1b3e6a72

Client Secret

Q9xLp-VT8rDs5-KmZ3pLq\_2Er-Wx7TyUaZ

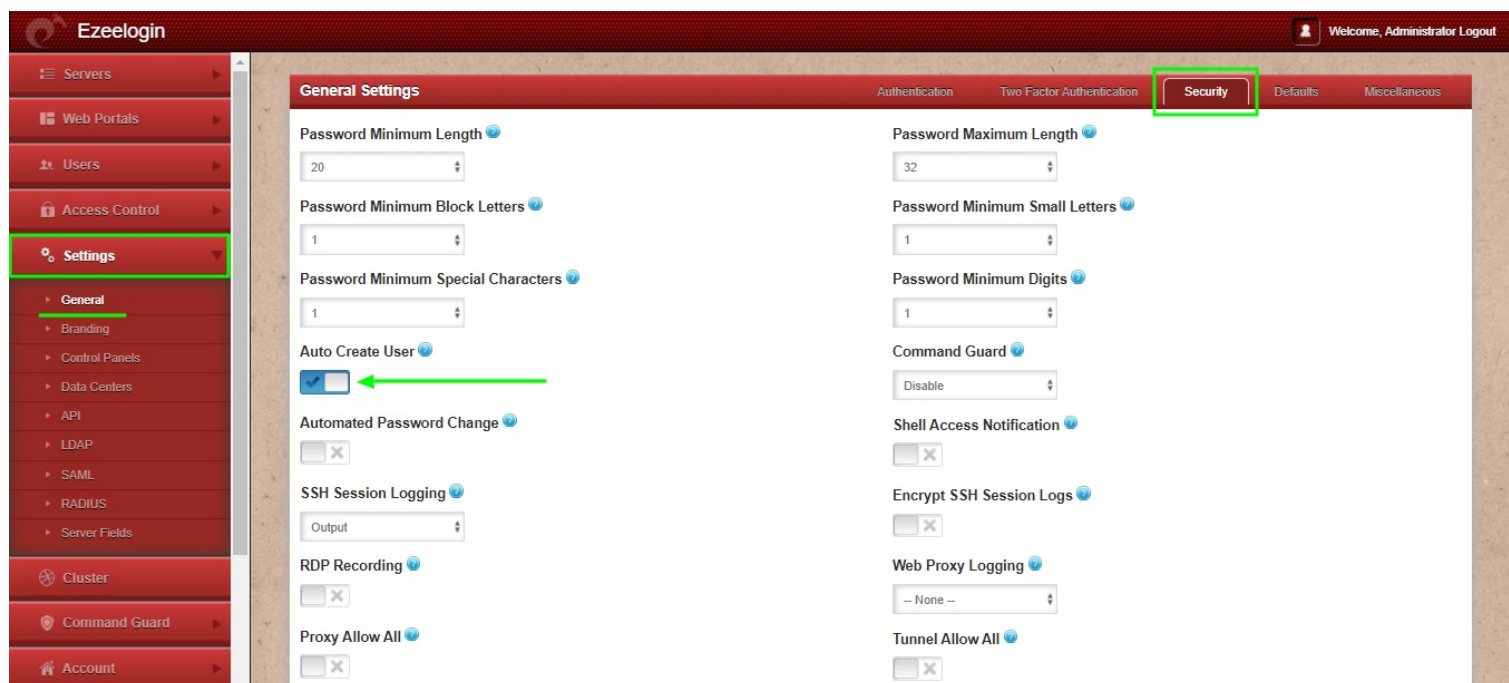
HTTP Proxy URL

Path To CA Bundle

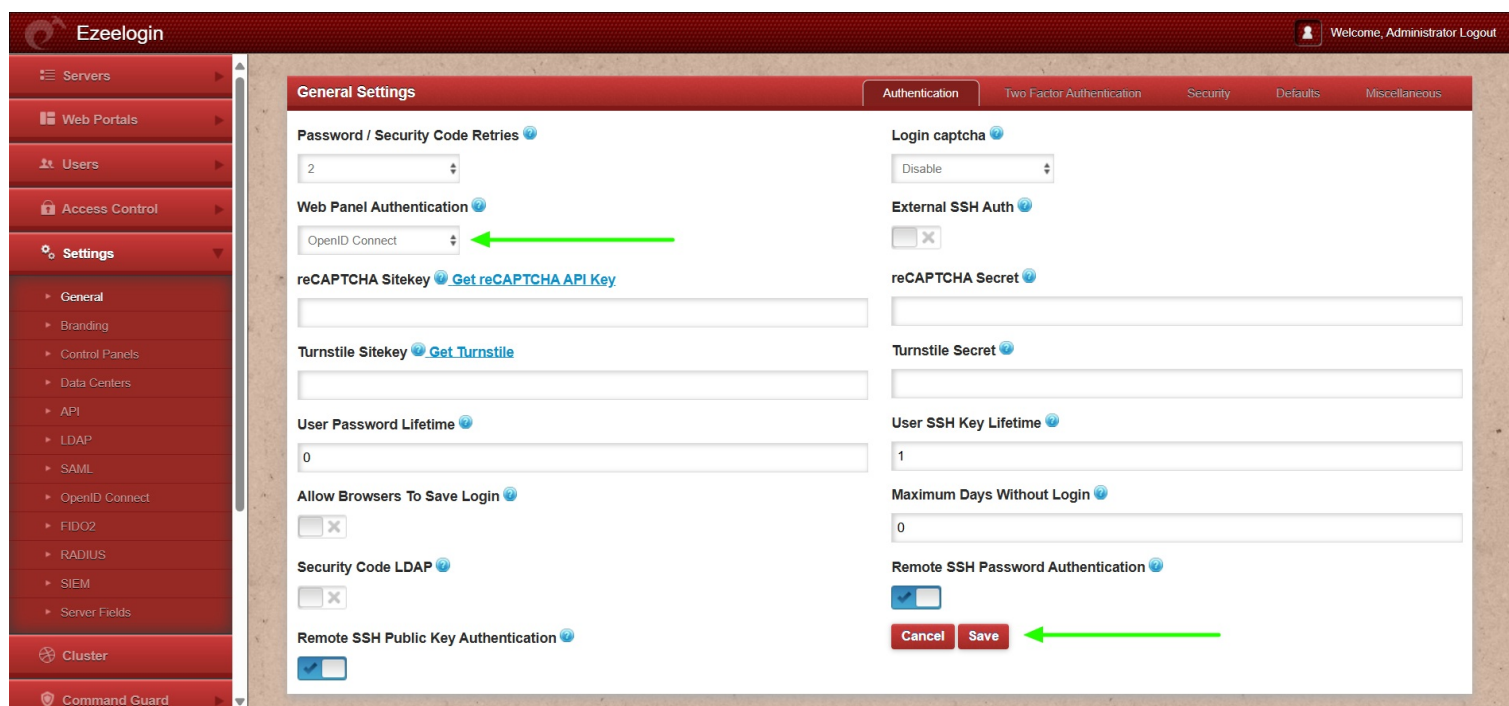
Azure AD Settings

Advanced

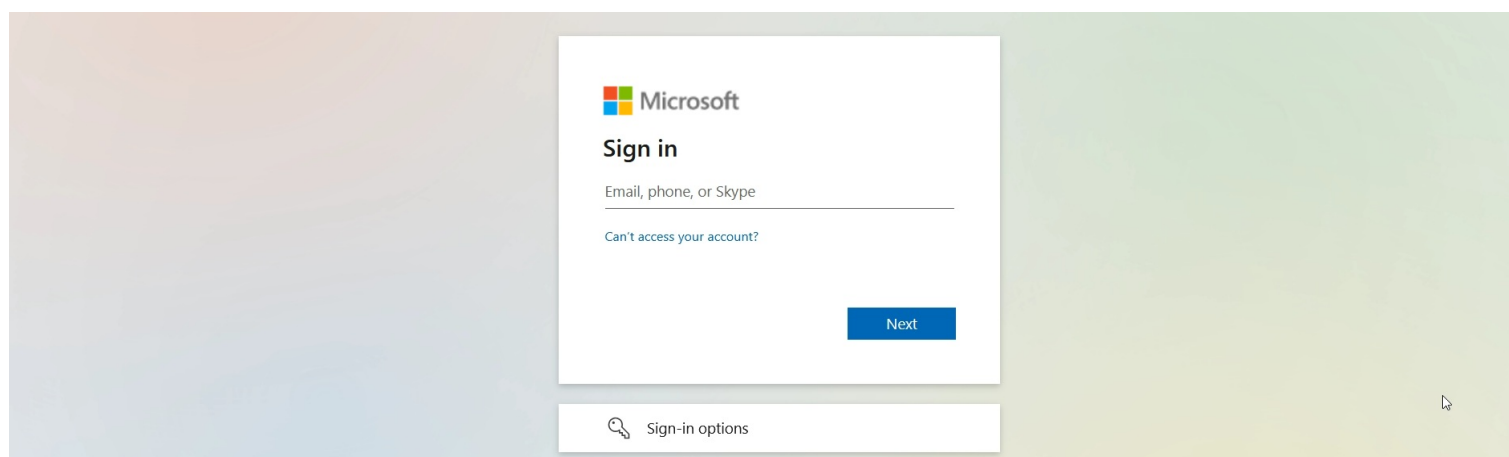
**Step 11:** Enable Auto Create User from **web GUI** -> **Settings** -> **General** -> **Security** -> **Enable Auto Create User**, so the user will automatically created after successful authentication from Azure.



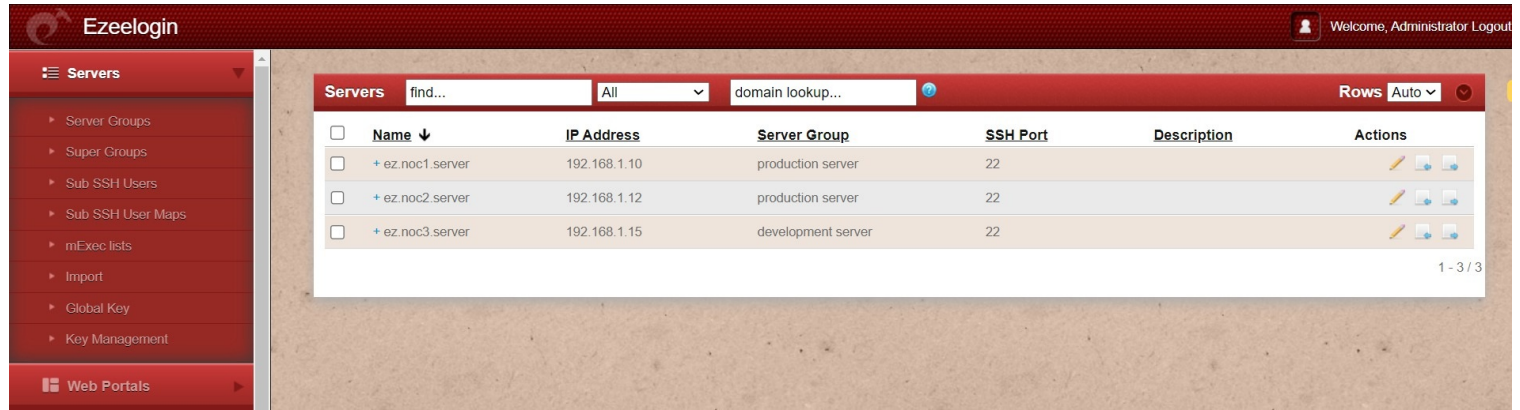
**Step 12:** Set **Web Panel Authentication** to **OpenID Connect** under **Settings -> General -> Authentication -> OpenID Connect**.



**Step 13:** Login into **web GUI** and you will be prompted with the **Microsoft Azure login Page** where you will need to enter the login credentials to be authenticated into the Ezeelogin Application.



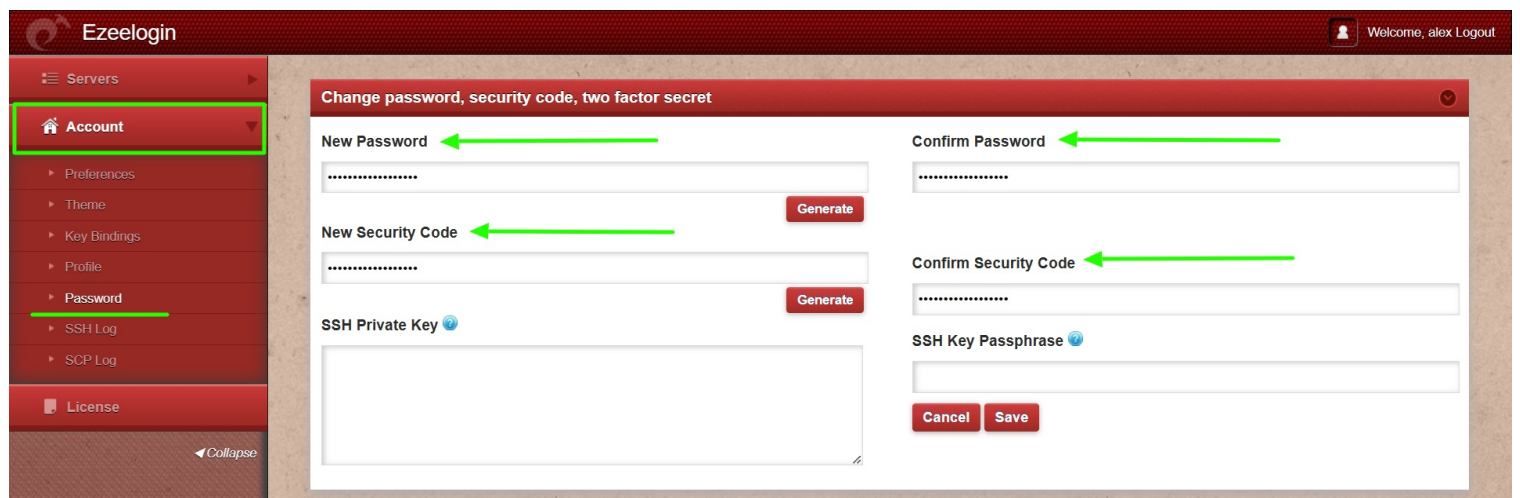
**Step 14:** Finally, you will be logged into the **web GUI using OpenID Connect Authentication**. The user will be created automatically on Ezeelogin after successful authentication from Azure.



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

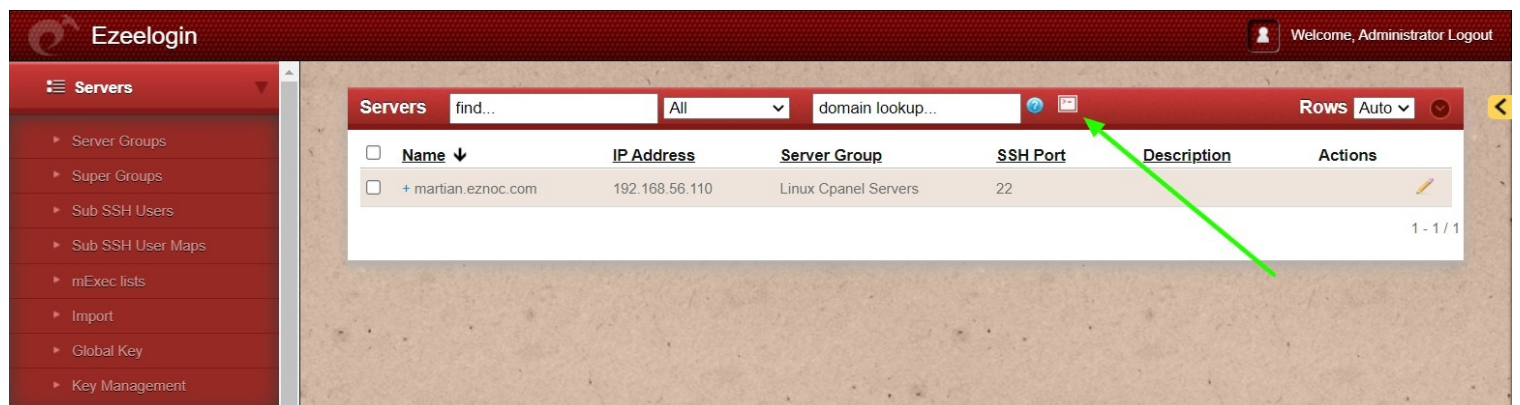
**Error: Invalid password**

**Step 15:** After logging into the GUI, reset the password and security code of the user under **Account** - > **Password** in order to SSH to the ezsh shell.



**Step 16:** You can log in to **Ezeelogin shell** via **Webssh** shell or using any **SSH client** such as Putty or terminal etc.

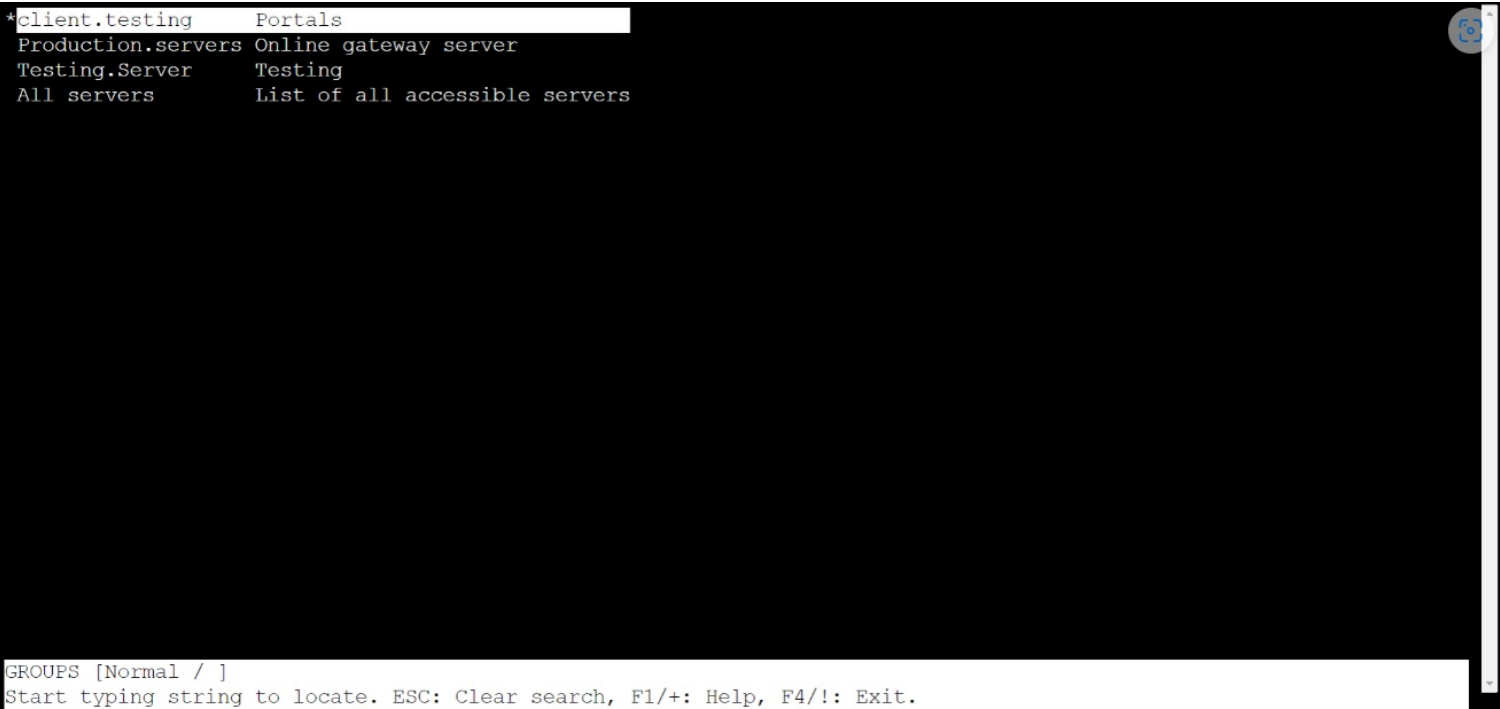
**Step 16(A): WebSSH:** Click on the 'Open Web SSH Console' icon to SSH via the browser.



**Step 16(B): Native SSH Client:** After resetting the password and security code you can **SSH to the ezsh shell** (using Terminal or Putty) with the **OpenID connect username**.

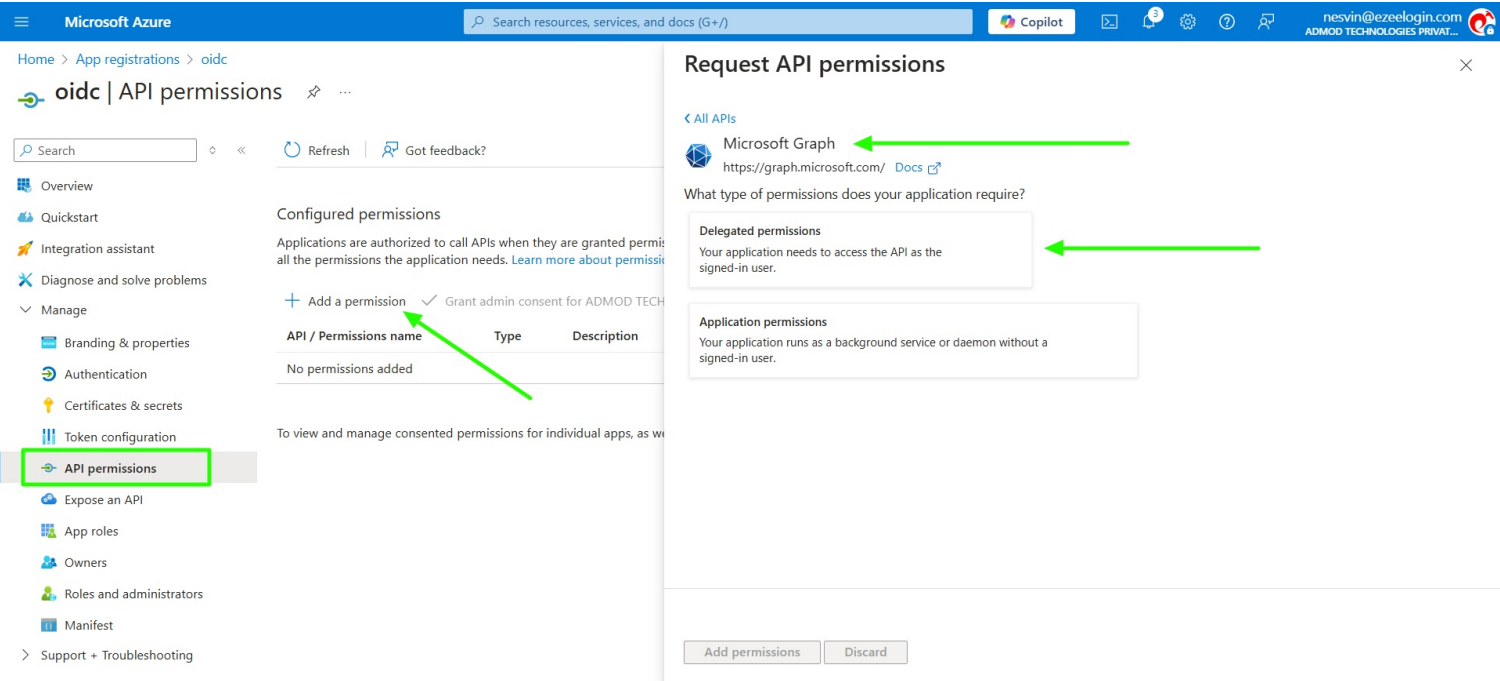
```
alex@adezeelogin.com:~$ ssh alex@adezeelogin.com
alex@adezeelogin.com's password:
```

**Step 17:** After logging into ezsh, the server list will be visible. The user can navigate using the Up and Down arrow keys and select a server using the Enter key.



## How to add scope from Azure OpenID connect to Ezeelogin jumpserver?

**Step 1:** Navigate to **API permissions** -> **add a permission** -> **Micrograph graph** -> **Delegated permissions**



## Step 2: Under **OpenID permissions** select **required scopes** and save the permissions.

The screenshot shows the Microsoft Azure portal interface. On the left, the 'API permissions' section is selected under 'oidc'. The main area displays 'Request API permissions' with a table of permissions. A green box highlights the 'Openid permissions (4)' section, which includes the following permissions:

| Permission                                                                                                | Admin consent required |
|-----------------------------------------------------------------------------------------------------------|------------------------|
| <input checked="" type="checkbox"/> email<br>View users' email address                                    | No                     |
| <input checked="" type="checkbox"/> offline_access<br>Maintain access to data you have given it access to | No                     |
| <input checked="" type="checkbox"/> openid<br>Sign users in                                               | No                     |
| <input checked="" type="checkbox"/> profile<br>View users' basic profile                                  | No                     |

Below the table, there are 'Add permissions' and 'Discard' buttons. A green arrow points to the 'Add permissions' button.

## Step 3: Login to web GUI, go to **OIDC advanced settings**, add the **scopes separated by spaces**, and **save the settings**.

The screenshot shows the Ezeelogin web GUI. The 'Settings' menu is selected, and the 'Advanced' settings page is displayed. The 'Additional Scopes' field is highlighted with a green box and contains the text 'openid email offline\_access profile'. Other fields include 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, and Verify Peer.

## How to map a user from Azure OpenID Connect user group to Ezeelogin user group?

### 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 modified in the identity provider after the user has already logged in, the updated values will be reflected in the GUI only after the user logs out and logs in again.**

For example, if a user is moved from one group to another in the OIDC provider (such as Microsoft Azure), the change will automatically be updated in the Ezeelogin GUI after the user successfully re-logs in.

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

## 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.

The screenshot shows the Ezeelogin administration interface. On the left is a sidebar menu with options like Servers, Web Portals, Users, Access Control, Settings, Cluster, Command Guard, Account, and Help. The 'Settings' menu item is highlighted with a green box. The main content area is titled 'General Settings' and has tabs for Authentication, Two Factor Authentication, Security, Defaults, and Miscellaneous. The 'Defaults' tab is selected and highlighted with a green box. A green arrow points to the 'Default User Group' dropdown menu, which is currently set to '-- None --'. Other settings visible include Default SSH User (root), Default RDP Port (3389), Default Control Panel (-- None --), Default Language (English), Default Password Prompt (ssword), Default SSH Port (22), Default Data Center (-- None --), Default First Prompt, and Default Root Prompt. 'Cancel' and 'Save' buttons are at the bottom right.

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 screenshot is similar to the one above, showing the Ezeelogin 'General Settings' page with the 'Defaults' tab selected. However, the 'Default User Group' dropdown menu is now set to 'Dummy', indicated by a green arrow. All other settings and the interface layout remain the same.

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

**Step 1:** Navigate to **API permissions** -> **Add a permission** -> **Microsoft Graph** -> **Application permissions** -> search for '**Group**' -> enable **Group.Read.All** to grant permission to read Azure user groups."

**Request API permissions**

Delegated permissions  
Your application needs to access the API as the signed-in user.

Application permissions  
Your application runs as a background service or daemon without a signed-in user.

Select permissions

group

Permission Admin consent required

> Calls

> Group-Conversation

Group (1)

☐ Group.Create  
Create groups Yes

☒ Group.Read.All  
Read all groups Yes

☐ Group.ReadWrite.All  
Read and write all groups Yes

Add permissions Discard

**Configured permissions**

Applications are authorized to call APIs when they are granted permissions by users/admins as part of all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for ADMOD TECHNOLOGIES PRIVATE LIMITED

| API / Permissions name | Type        | Description               |
|------------------------|-------------|---------------------------|
| email                  | Delegated   | View users' email address |
| Group.Read.All         | Application | Read all groups           |
| openid                 | Delegated   | Sign users in             |
| profile                | Delegated   | View users' basic profile |

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, go to the [Consent and permissions](#) page.

**Step 2:** Create the **same user group in Ezeelogin** as in **Azure** and **provide priority to auto assign to higher priority group**.

**Groups | All groups**

Search mode Contains

17 groups found

| Name           | Object Id                            | Group type    | Membership type | Email |
|----------------|--------------------------------------|---------------|-----------------|-------|
| Administrators | 19f400de-7954-4ea5-9aa3-f4c48dfa8e6f | Security      | Assigned        |       |
| AT             | 40cfcdda-5bcc-41f6-9ec1-a2f1c6e98849 | Microsoft 365 | Assigned        |       |
| All Company    | 2d69473b-c3af-402b-a5b0-1078d5ddd093 | Microsoft 365 | Assigned        |       |
| All Users      | ec6f9e66-f01d-478d-9419-2f18fa82e468 | Security      | Dynamic         |       |

**Ezeelogin**

Welcome, Administrator Logout

**User Groups** find... All

| Name           | Description    | Priority | Force 2FA | Actions |
|----------------|----------------|----------|-----------|---------|
| Administrators |                | 20       | ×         |         |
| Admins         | Administrators | 0        | ×         |         |
| All Company    |                | 5        | ×         |         |
| All Users      |                | 8        | ×         |         |
| Dummy          | Dummy Group    | 0        | ×         |         |

1 - 5 / 5

**Step 3:** Gateway user will be **auto created** to higher priority user group in Ezeelogin.

**Ezeelogin**

Welcome, Administrator Logout

**Users** find... All

| Username | First Name    | Last Name | Email                | Status | Expiry | User Group     | Actions |
|----------|---------------|-----------|----------------------|--------|--------|----------------|---------|
| alex     | alex          |           | alex@ez.com          | Active |        | Dummy          |         |
| ezadmin  | Administrator |           | admin@ez.com         | Active |        | Admins         |         |
| jake     | jake          | jake      | jake@ez.com          | Active |        | Dummy          |         |
| nesvin   | Nesvin        | KN        | nesvin@ezeelogin.com | Active |        | Administrators |         |

1 - 4 / 4

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

---

**Related Articles:**

Integrate Azure AD in Ezeelogin jump server

Online URL: <https://www.ezeelogin.com/kb/article/integrate-azure-openid-connect-769.html>