

Create users in Ezeelogin with the same user group in Azure AD

646 Nesvin KN May 28, 2026 Productivity & Efficiency Features

3063

How to auto-create the Azure SSO user to the same group in Ezeelogin?

Overview: This article explains how to auto-create Azure SSO users in Ezeelogin and assign them to matching Azure groups using SAML configuration and Microsoft Graph API.

This feature is **available from Ezeelogin version 7.36.0**.

Refer article to [upgrade Ezeelogin to the latest version](#).

Note:

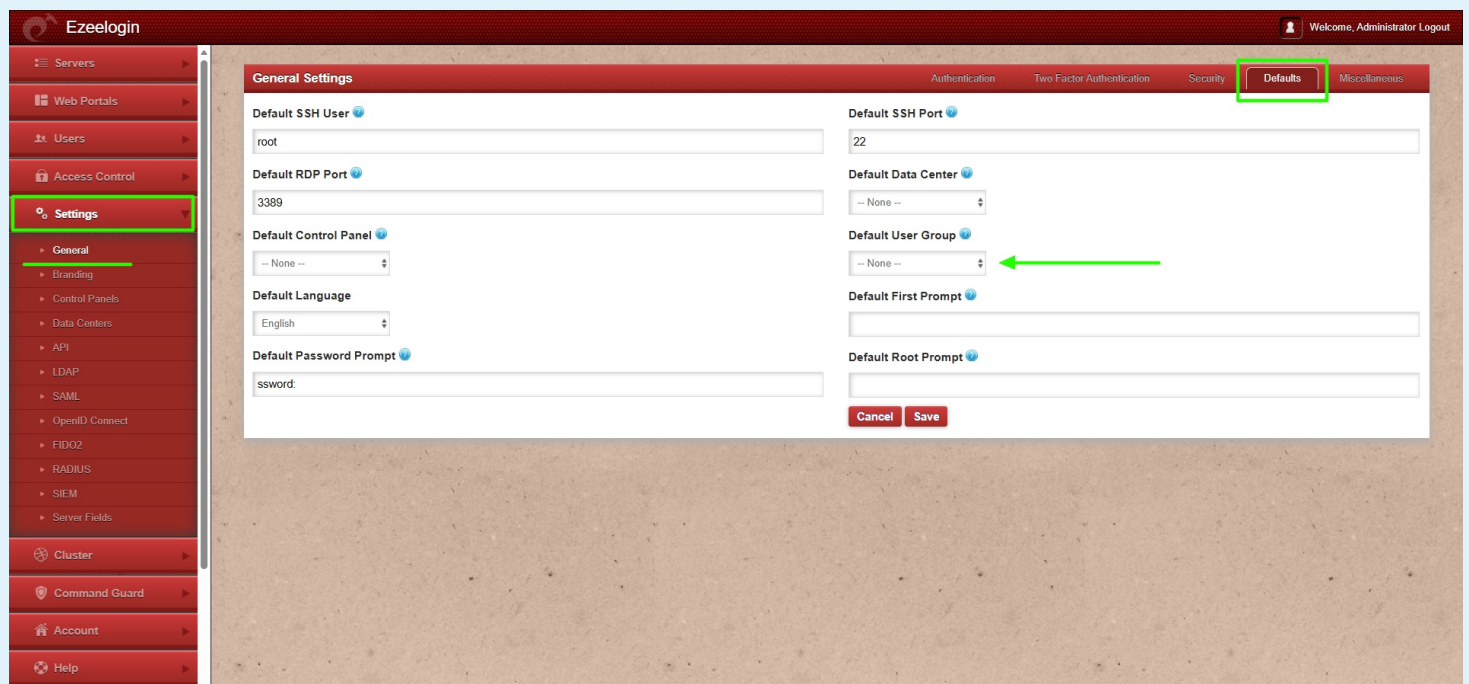
User attributes (such as groups and other mapped fields) are automatically updated in the Ezeelogin GUI when a user authenticates again. **If any attribute of an existing SAML user is modified in the identity provider after the user has already logged in, the updated values will be reflected in the GUI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

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

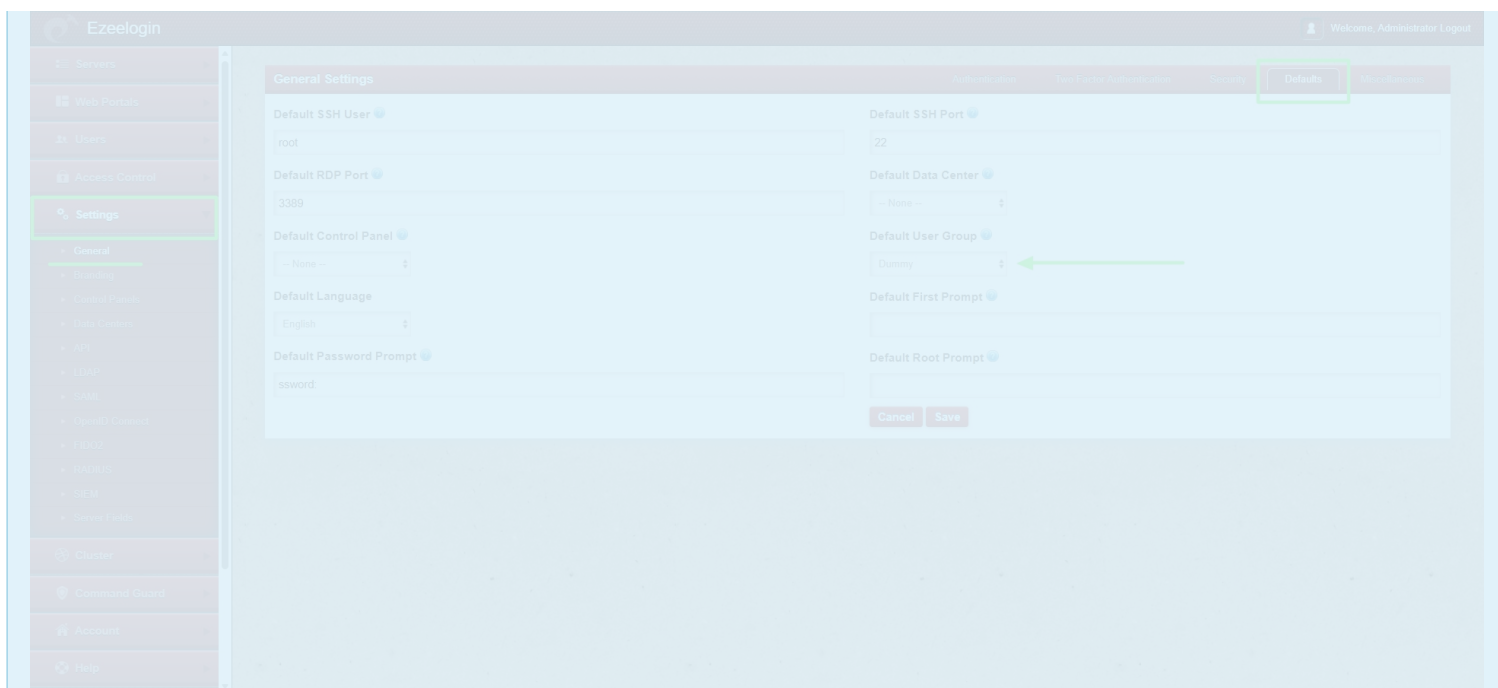
This feature is available from Ezeelogin version 7.46.0. Refer article to [upgrade Ezeelogin to the latest version](#).

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.

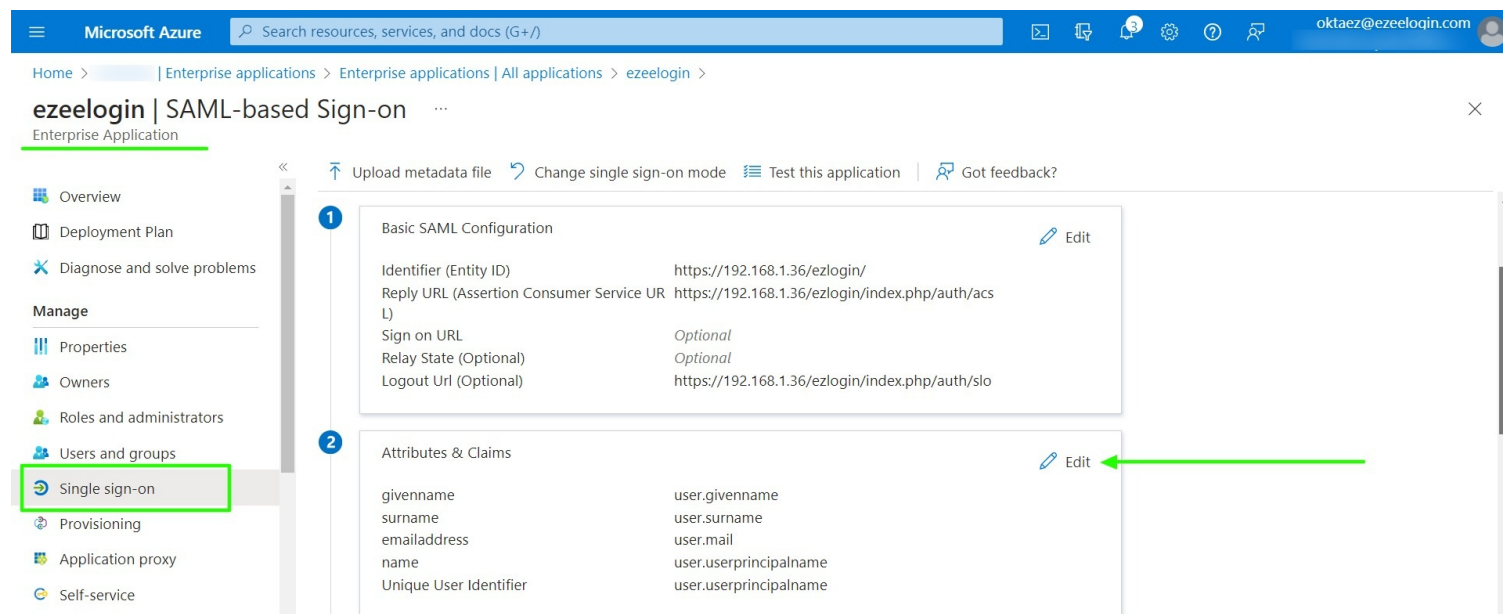


2. If the default user group is set to any group other than None, then all users from the OIDC provider will be auto-created in that same group.



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

Step 1: Login to Azure and in **enterprise application** click on **Single sign-on -> Attributes & Claims Edit ->** Copy **Claim names** and paste them into the **advanced SAML setting in Ezeelogin**.



Step 2: Click on **Add a group claim -> select All groups -> Save**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications > Enterprise applications | All applications > ezeelogin | SAML-based Sign-on > SA

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname... ***

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ema...	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/give...	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surn...	SAML	user.surname ***

Advanced settings

Group Claims

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued ...

Which groups associated with the user should be returned in the claim?

☐ None

☒ All groups

☐ Security groups

☐ Directory roles

☐ Groups assigned to the application

Source attribute *

Group ID

☐ Emit group name for cloud-only groups

Advanced options

Save

Step 3: Copy the **Claim names** and paste them into the **SAML setting** of Ezeelogin.

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications > Enterprise applications | All applications > ezeelogin | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipaln... **

Additional claims

Claim name	Type	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	SAML	user.groups [All] ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***

Advanced settings

Please review the attributes listed below if you encounter the following error while attempting to log in as a SAML user:

Could not get username from SAML response

Ezeelogin Welcome, Administrator Logout

- Servers
- Web Portals
- Users
- Access Control
- Settings**
 - General
 - Branding
 - Control Panels
 - Data Centers
 - API
 - LDAP
 - SAML**
 - RADIUS
 - Server Fields
- Cluster
- Command Guard
- Account
- Help
- License

New Signing Certificate

New Encryption Certificate

Username Attribute Name

Group Attribute Name

Firstname Attribute Name

Lastname Attribute Name

Cancel Fetch Save

Azure AD Settings

Advanced

Step 4: Create a new app registration in Azure Microsoft Entra ID.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Default Directory

Default Directory | App registrations Microsoft Entra ID

+ New registration Endpoints Troubleshooting Refresh Download Preview features Got feedback?

All applications **Owned applications** Deleted applications Applications from personal account

Add filters

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
-----------------	-------------------------	---------------	------------------------

App registrations

Step 5: Register the application with a name and select **Accounts in any organizational directory.**

Microsoft Azure

Search resources, services, and docs (G+/I)



oktaez@ezeelogin.com
DEFAULT DIRECTORY (...)

Home > Default Directory | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

ezlogin

Supported account types

Who can use this application or access this API?

☐ Accounts in this organizational directory only (Default Directory only - Single tenant)

☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

☒ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

Help me choose...

By proceeding, you agree to the Microsoft Platform Policies

Register

Step 6: Click on the application created, **certificate & secrets**, and create a **new client secret**.

Microsoft Azure

Search resources, services, and docs (G+/I)



oktaez@ezeelogin.com
DEFAULT DIRECTORY (...)

Home > Default Directory

Default Directory | App registrations

Overview

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

Enterprise applications

Devices

App registrations

Identity Governance

+ New registration

Endpoints

Troubleshooting

Refresh

Download

Preview features

Got feedback?

All applications

Owned applications

Deleted applications

Applications from personal account

Start typing a display name or application (client) ID to filter th...

Add filters

2 applications found

Display name	Application (client) ID	Created on	Certificates & secrets
ezlogin	a2fef56b-20b9-40eb-b70f-9f5d2a0ff7bf	10/23/2023	Current

Microsoft Azure

Search resources, services, and docs (G+/I)



oktaez@ezeelogin.com
DEFAULT DIRECTORY (...)

Home > Default Directory | App registrations > ezlogin

ezlogin | Certificates & secrets

Search

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding & properties

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest

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
ezlogin_client	4/20/2024	auc*****	0b846cdf-88a6-4989-921d-7fb0f5535...  

Step 7: Copy the **new secret value**, **client ID**, and **tenant ID**, then paste them into **Ezeelogin SAML Azure AD Settings**.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Default Directory | App registrations > ezlogin

ezlogin | Certificates & secrets

Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest

Got 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 (2) 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
ezlogin_client	4/20/2024	auc*****	0b846cdf-88a6-4989-921d-7fb0f5535...
ezlogin	4/24/2024	3eX8Q~cw9Gsqv2mMkft9ez3SNamH...	964c66e1-5e1c-4617-881e-5197ca53...

Microsoft Azure | Search resources, services, and docs (G+)

Home > Default Directory | App registrations >

ezlogin

Overview, Quickstart, Integration assistant, Manage, Branding & properties, Authentication, Certificates & secrets, Token configuration

Delete, Endpoints, Preview features

Essentials

Display name	: ezlogin	Client credentials	: 0 certificate, 2 secret
Application (client) ID	: a2fef56b-20b9-40eb-b70f-9f5d2a0ff7bf	Redirect URIs	: Add a Redirect URI
Object ID	: b6e9ed2e-53b5-4d3c-b8db-9fddc602280c	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: e33a58db-50a9-4af2-992a-ab3ec9edf1a9	Managed application i...	: ezlogin

Supported account types : All Microsoft account users

Get Started, Documentation

Ezeelogin | Welcome, Administrator Logout

Servers, Web Portals, Users, Access Control, Settings, Cluster, Command Guard, Account, Preferences, Theme, Key Bindings, Profile, Password, SSH Log, RDP Recording, SCP Log, Help

SAML Service Provider (SP) Info

Metadata URL	http://192.168.1.36/ezlogin/index.php/metadata
Entity ID	http://192.168.1.36/ezlogin/
Assertion Consumer Service URL	http://192.168.1.36/ezlogin/index.php/auth/acs
Single Logout Service URL	http://192.168.1.36/ezlogin/index.php/auth/slo

SAML Identity Provider (IdP) Settings

Azure AD Settings

Azure AD Tenant ID	e33a58db-50a9-4af2-992a-ab3ec9edf1a9
Azure AD Client ID	a2fef56b-20b9-40eb-b70f-9f5d2a0ff7bf
Azure AD Client Secret	auc8Q~rB5w1N-eaUH1Ng~VET5eVlnJV~OYYHKcct

Advanced

Step 8: Click on **application permission** -> **add a permission** -> **Microsoft graph** -> **application permission** -> enable **Group.Read.All**.

Microsoft Azure Search resources, services, and docs (G+/I) oktaez@ezeelogin.com DEFAULT DIRECTORY (...)

Home > Default Directory | App registrations > ezlogin

ezlogin | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration **API permissions** Expose an API App roles

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

+ Add a permission ✓ Grant admin consent for Default Directory

API / Permissions name Type Description Admin consent req... Status

Microsoft Graph (1)

API / Permissions name	Type	Description	Admin consent req...	Status
Group.Read.All	Applicati...	Read all groups	Yes	⚠ Not granted for Def...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Request API permissions

< All APIs

Microsoft Graph <https://graph.microsoft.com/> Docs

What type of permissions does your application require?

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 expand all

group

Permission Admin consent required

> Calls

Group (1)

Permission	Admin consent required
Group.Create	Yes
Group.Read.All	Yes
Group.ReadWrite.All	Yes

Step 9: Click on **grant admin consent for default directory**.

Microsoft Azure Search resources, services, and docs (G+/I) oktaez@ezeelogin.com DEFAULT DIRECTORY (...)

Home > Default Directory | App registrations > ezlogin

ezlogin | API permissions

Search Refresh Got feedback?

Overview Quickstart Integration assistant

Manage Branding & properties Authentication Certificates & secrets Token configuration **API permissions** Expose an API

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

+ Add a permission ✓ Grant admin consent for Default Directory

API / Permissions name Type Description Admin consent req... Status

Microsoft Graph (1)

API / Permissions name	Type	Description	Admin consent req...	Status
Group.Read.All	Applicati...	Read all groups	Yes	⚠ Not granted for Def...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Step10: Create the **user group** in **Ezeelogin** with the **exact same group name that exists in Azure** and set a **higher priority for auto-creation for that group**.

Microsoft Azure Search resources, services, and docs (G+/I) oktaez@ezeelogin.com DEFAULT DIRECTORY (...)

Home >

Groups | All groups

Default Directory - Microsoft Entra ID

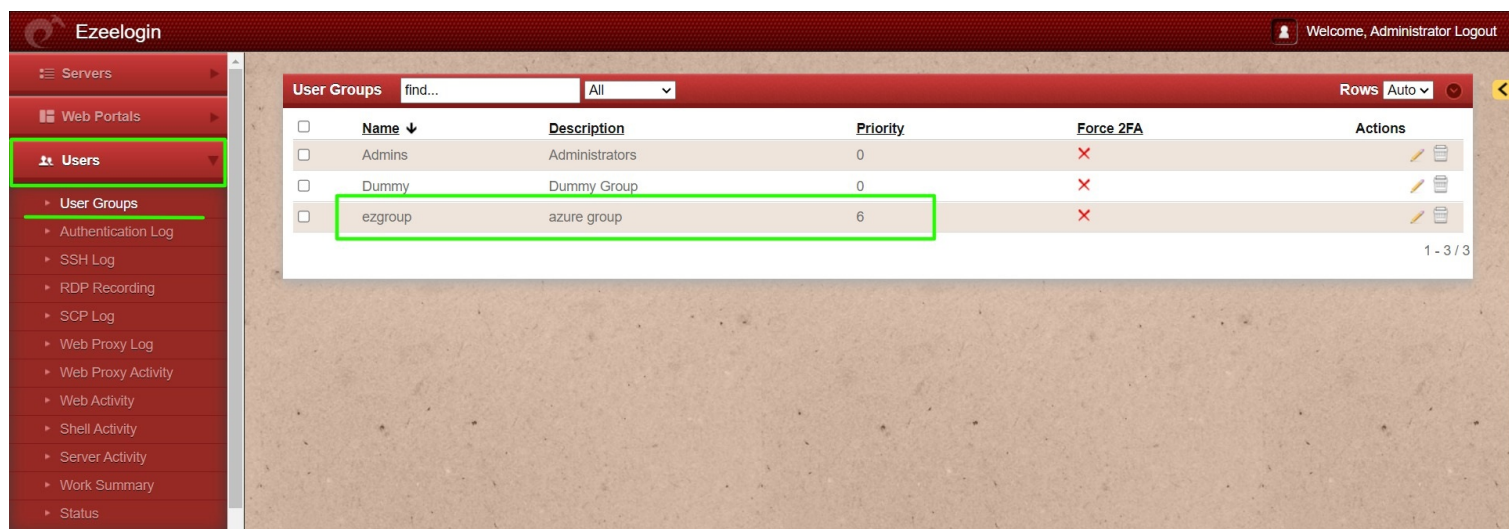
New group Download groups Refresh Manage view Delete Got feedback?

Search Add filter

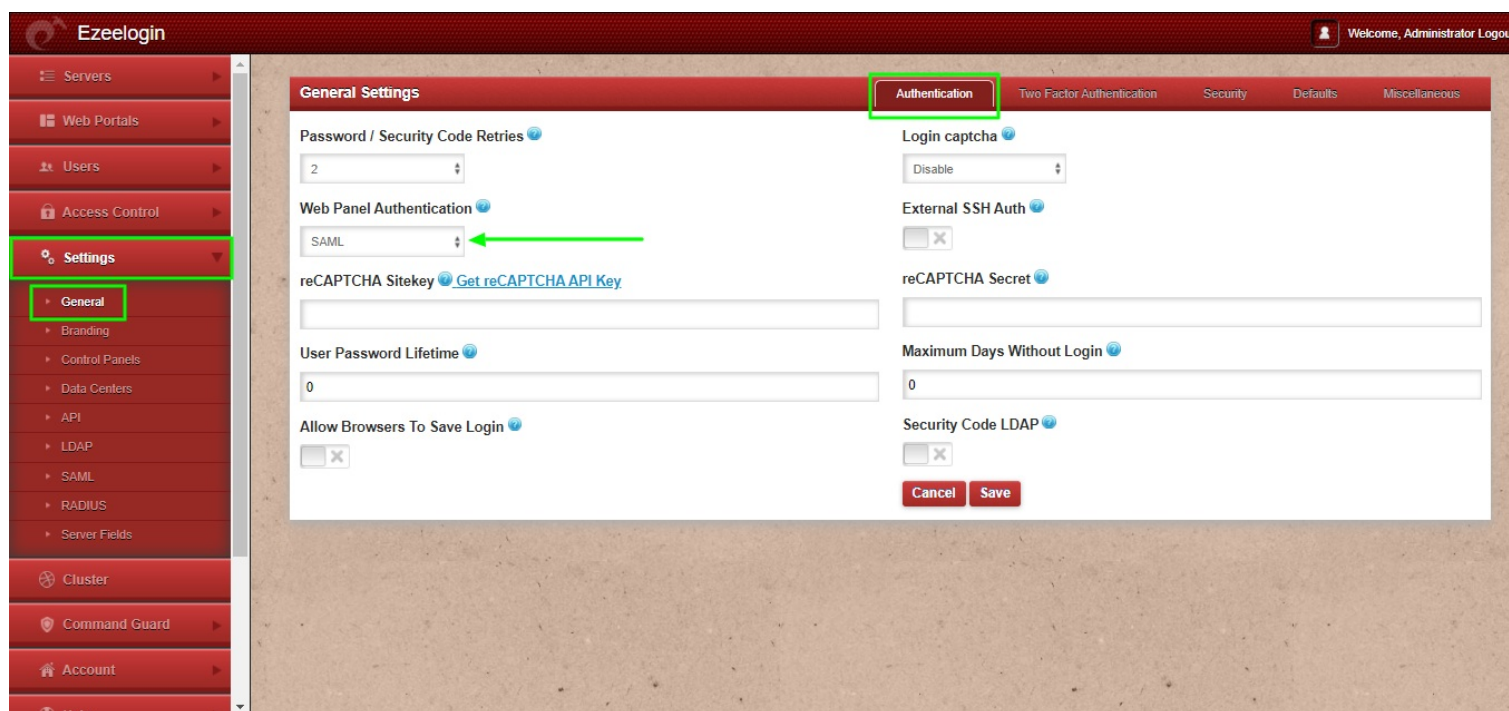
Search mode Contains

4 groups found

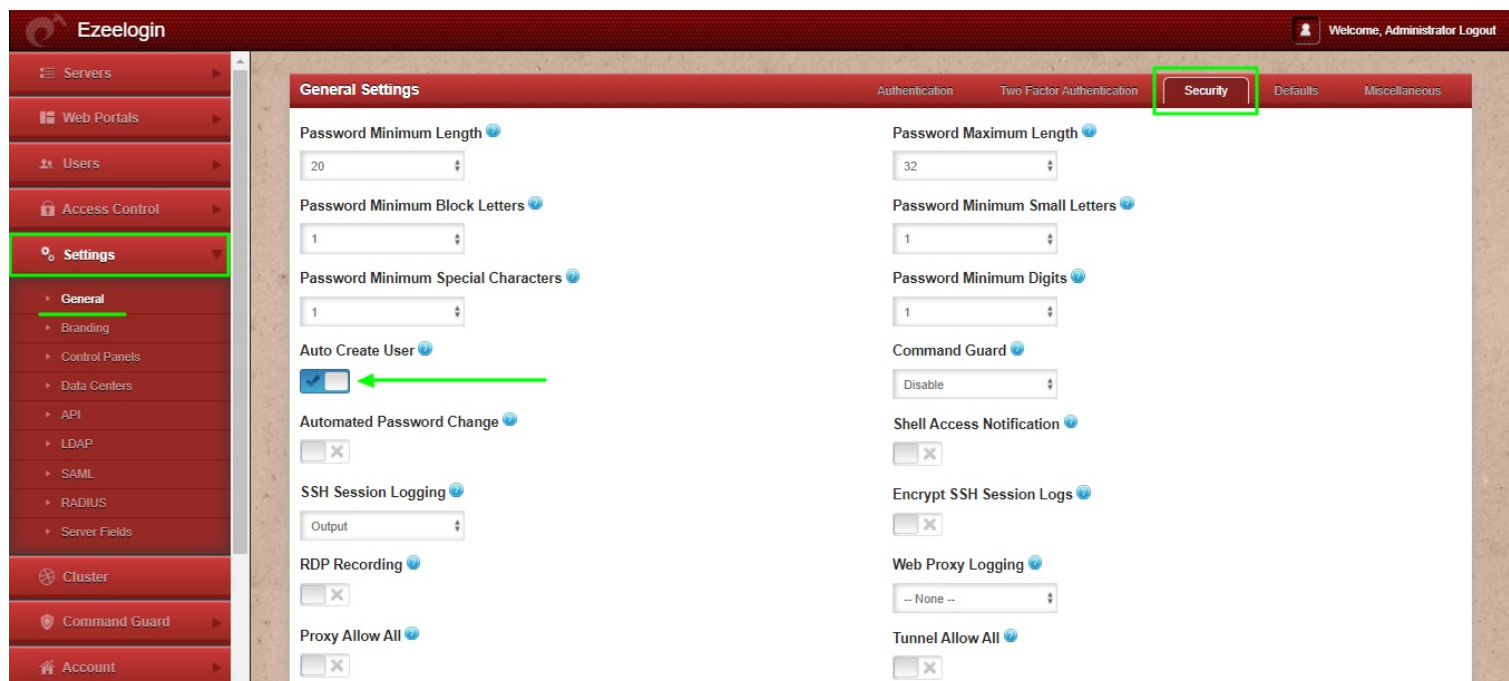
Name	Object Id	Group type	Membership type	Er
AD AAD DC Administrators	867a3baa-2e91-4761-80b9-e5da756e859	Security	Assigned	
AD admins	78cfb9e8-f5f4-48b5-bf4d-7753a53e96d0	Security	Assigned	
DE developer	70f31de2-8b2f-406d-b8f1-411587a92c30	Security	Assigned	
EZ ezgroup	e348af2e-8612-48e3-85d4-9d6aa007424c	Security	Assigned	



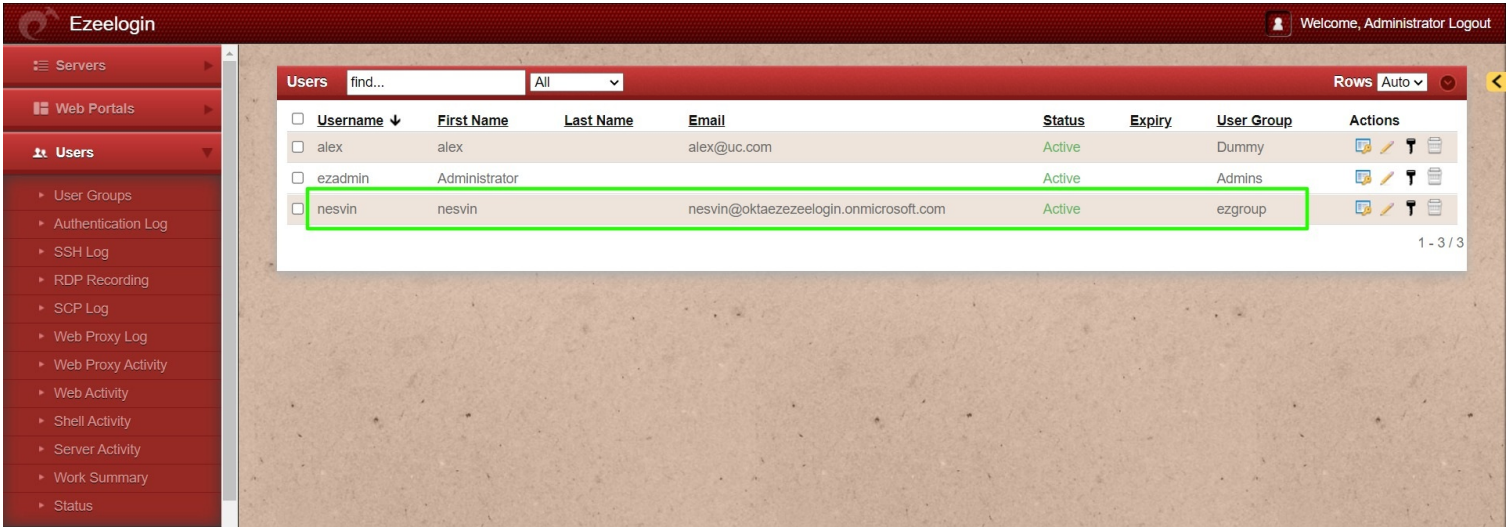
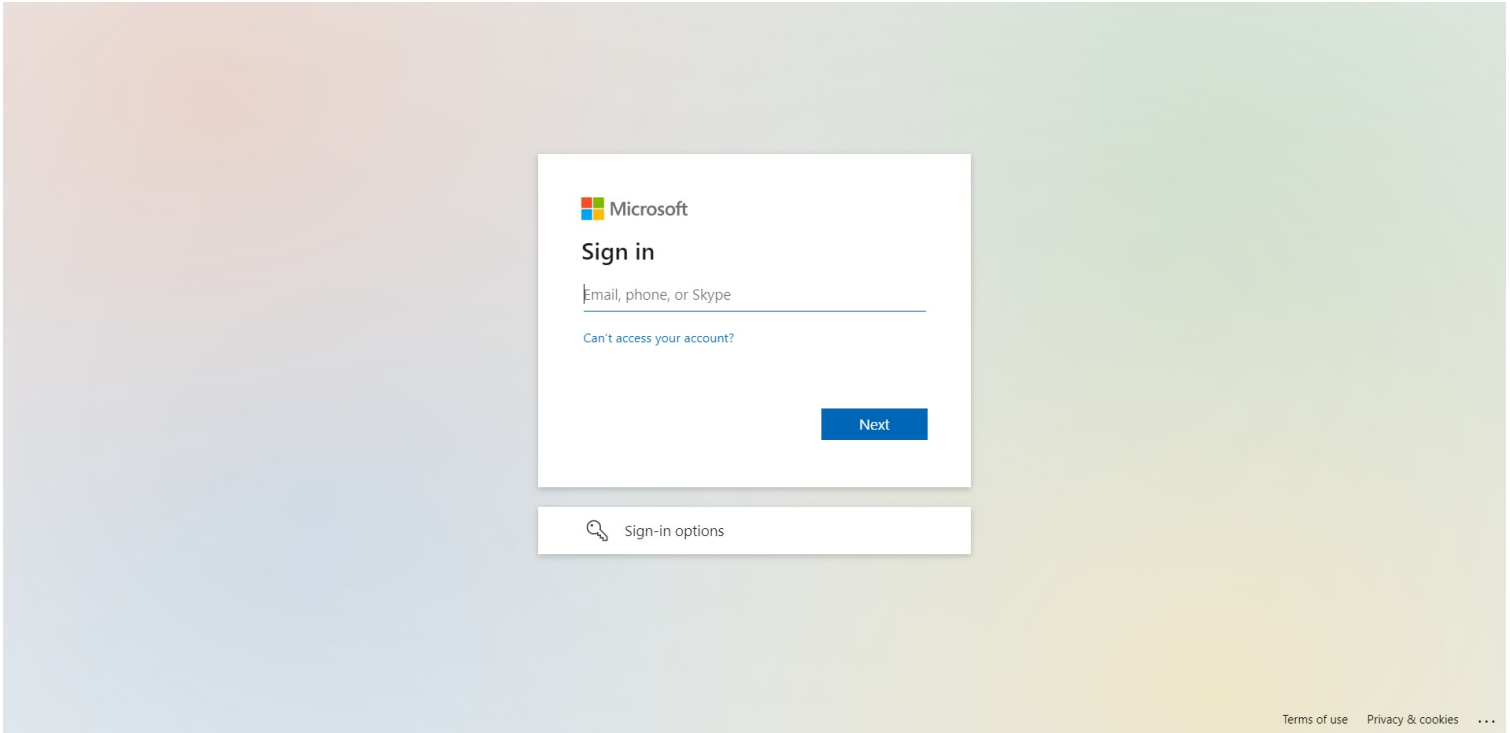
Step 11: Change Web panel Authentication to SAML from **Ezeelogin GUI -> Settings -> General -> Authentication.**



Step 12: Enable auto create user from **Ezeelogin GUI -> Settings -> General -> Security -> Enable Auto Create User.**



Step 13: Relogin to Ezeelogin GUI with Azure user credentials and the user will be auto-created to the same group in Azure.



Related Article:

[Integrate Microsoft Azure SSO and with Ezeelogin](#)

[Token encryption in Microsoft Azure SSO with Ezeelogin](#)

[Unable to login with Azure SSO](#)

Online URL: <https://www.ezeelogin.com/kb/article/create-users-in-ezeelogin-with-the-same-user-group-in-azure-ad-646.html>