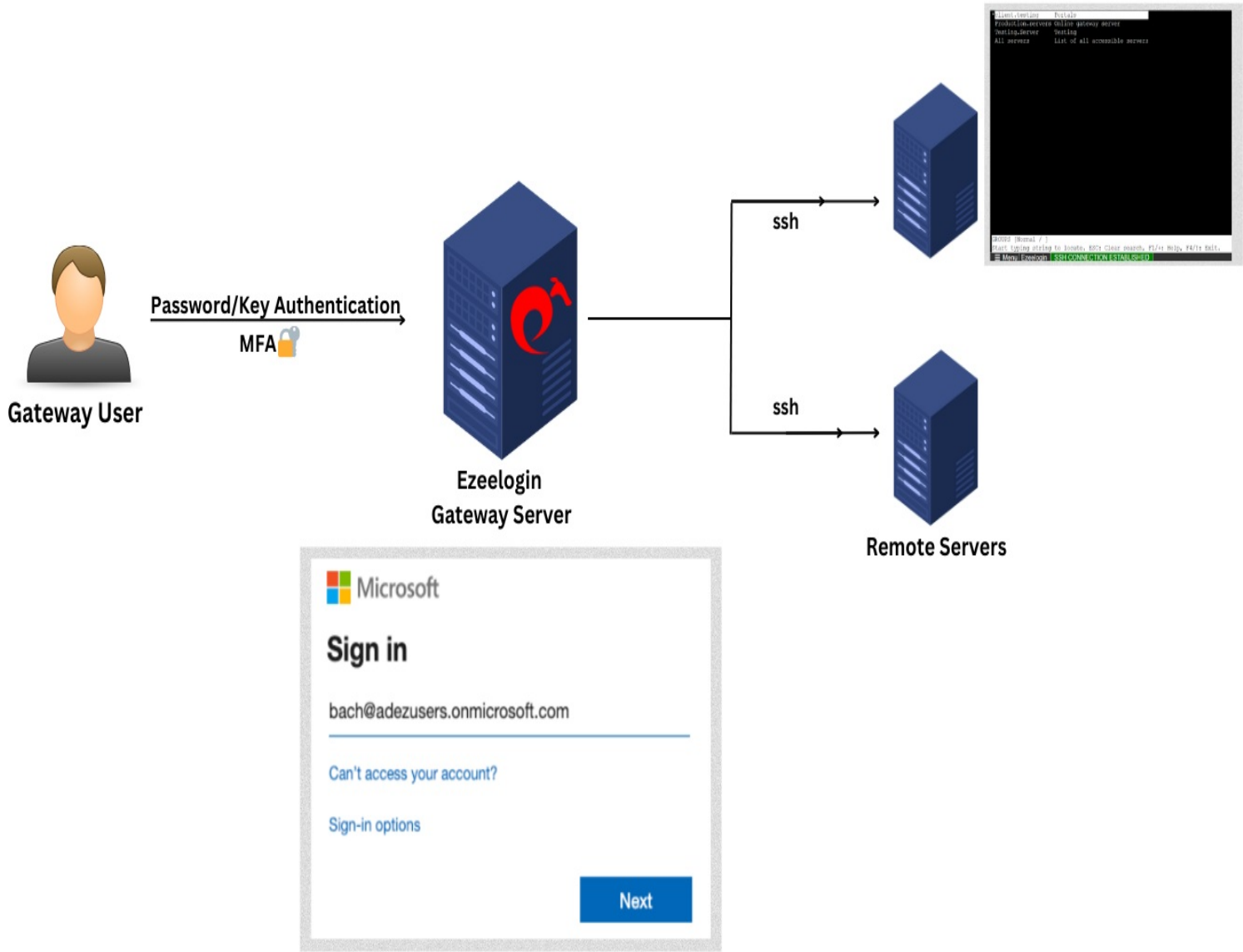


Integrate SAML Authentication in Ezeelogin GUI using Microsoft Azure SSO and Azure Active Directory

Configure Microsoft Azure SSO SAML-based Authentication in Ezeelogin GUI.

Overview: This article describes the brief guide to configuring Microsoft Azure SSO authentication with Ezeelogin GUI.

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



1. Login into your Microsoft Azure account and **Create an Active Directory service**.

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

Home > ez | Overview Azure Active Directory

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

+ Add Manage tenants What's new Preview features Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	ez	Users	22
Tenant ID	f0657038-1ee0-4f27-86d4-180925403f81	Groups	0
Primary domain	ezlogin.onmicrosoft.com	Applications	20
License	Azure AD Premium P2	Devices	0
Workload License	Azure AD Workload Free		
Alerts			

2. Add Users in AD (Skip this step, if Users already exist). This user in turn would authenticate into the Ezeelogin GUI. To create a user in AD, click on **User tab** >> **New user** >> Provide the user name, name, password, etc, and click **Create**.

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

Home > ez | Users

Users

Search

+ New user Download users Bulk operations Refresh Manage view Delete Per-user MFA Preview features

Create new user
Create a new internal user in your organization

Invite external user
Invite an external user to collaborate with your organization

	User principal name	User type	On-premises sy...	Identities	Company name
☐	CH Chris	Member	No	ezlogin.onmicrosoft.com	
☐	EL ellen	Member	No	ezlogin.onmicrosoft.com	
☐	ES estel	Member	No	ezlogin.onmicrosoft.com	
☐	HE hendra	Member	No	ezlogin.onmicrosoft.com	
☐	HE Henry	Member	No	ezlogin.onmicrosoft.com	
☐	IR irin	Member	No	ezlogin.onmicrosoft.com	
☐	JB James B	Member	No	ezlogin.onmicrosoft.com	
☐	JE jenna	Member	No	ezlogin.onmicrosoft.com	

3. Create an **Enterprise Application**. Click on Enterprise applications.

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

Home > ez | Overview Azure Active Directory

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

+ Add Manage tenants What's new Preview features Got feedback?

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Overview Monitoring Properties Recommendations Tutorials

Search your tenant

Basic information

Name	ez	Users	22
Tenant ID	f0657038-1ee0-4f27-86d4-180925403f81	Groups	0
Primary domain	ezlogin.onmicrosoft.com	Applications	20
License	Azure AD Premium P2	Devices	0
Workload License	Azure AD Workload Free		
Alerts			

Click on **All applications** >> **New application**.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The main content area is titled 'Enterprise applications | All applications'. On the left sidebar, the 'Manage' section is expanded, and 'All applications' is highlighted with a red box. In the main content area, the '+ New application' button is highlighted with a red arrow. Below this button, there are options for 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?'. The main content area also displays a search bar, filters for 'Application type == Enterprise Applications' and 'Application ID starts with', and a table of 20 applications found.

Click on **Create your own application** >> **Provide the name for your application** >> Check **Integrate any other application you don't find in the gallery(Non-gallery)** >> **Create**.

The screenshot shows the 'Create your own application' dialog in the Microsoft Azure portal. The dialog is titled 'Create your own application' and has a 'Got feedback?' link. It contains a text input field for 'What's the name of your app?' with the value 'ezlogin' and a green checkmark. Below this, there are three radio buttons for 'What are you looking to do with your application?': 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The 'Integrate any other application you don't find in the gallery (Non-gallery)' option is selected. Below the radio buttons, there is a section titled 'We found the following applications that may match your entry' with a list of applications: 'BlogIn', 'SecureLogin', and 'LogMeIn'. At the bottom of the dialog, there is a 'Create' button highlighted with a red arrow.

4. Assign the user to the Enterprise application. Click on **Assign users and groups**.

The screenshot shows the 'ezlogin | Overview' page in the Microsoft Azure portal. The page is titled 'ezlogin | Overview' and has a 'Enterprise Application' subtitle. The left sidebar shows the 'Manage' section expanded, with 'Properties' highlighted. The main content area is divided into two sections: 'Properties' and 'Getting Started'. The 'Properties' section shows the application name 'ezlogin', the Application ID '33ebe59a-e2ed-45d9-83a5...', and the Object ID '21da370d-efe6-404b-b8f9-...'. The 'Getting Started' section contains two steps: '1. Assign users and groups' and '2. Set up single sign on'. The '1. Assign users and groups' step is highlighted with a red box and includes a link 'Assign users and groups'.

Click on **Add user/group** to assign the user to the application.

Ezeelogin Welcome, Administrator Logout

SAML Service Provider (SP) Info

Metadata URL	https://192.168.0.101/ezlogin/index.php/metadata
Entity ID	https://192.168.0.101/ezlogin/
Assertion Consumer Service URL	https://192.168.0.101/ezlogin/index.php/auth/acs
Single Logout Service URL	https://192.168.0.101/ezlogin/index.php/auth/slo

SAML Identity Provider (IdP) Settings

Metadata URL

Entity ID

Single Sign On Service URL

Single Logout Service URL

Signing Certificate

Click on **Single sign-on >> Basic SAML Configuration Edit >> Copy Entity ID, Assertion Consumer Service URL, and Logout Url** from Ezeelogin and paste in the specified fields.

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

Home > ez | Enterprise applications > Enterprise applications | All applications > ezlogin >

ezlogin | SAML-based Sign-on ...

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the configuration guide [for help integrating ezlogin.](#)

1 Basic SAML Configuration

Identifier (Entity ID)	https://192.168.0.101/ezlogin/
Reply URL (Assertion Consumer Service URL)	https://192.168.0.101/ezlogin/index.php/auth/acs
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	https://192.168.0.101/ezlogin/index.php/auth/slo

6. Copy the Metadata URL and paste it to the Metadata URL on **Ezeelogin GUI > Settings > SAML Metadata URL** and click on the **fetch button**, it will auto-fill the SAML setting and **SAVE** it.

Powered by ezeelogin.com

New Signing Certificate ?

New Encryption Certificate ?

Username Attribute Name ?

Group Attribute Name ?

Firstname Attribute Name ?

Lastname Attribute Name ?

Cancel Fetch Save

Advanced

7. Add users in your Azure AD Directory into the Ezeelogin GUI. Make sure the **email ID entered in GUI is identical to the one in SAML**.

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

User Groups

Authentication Log

SSH Log

RDP Recording

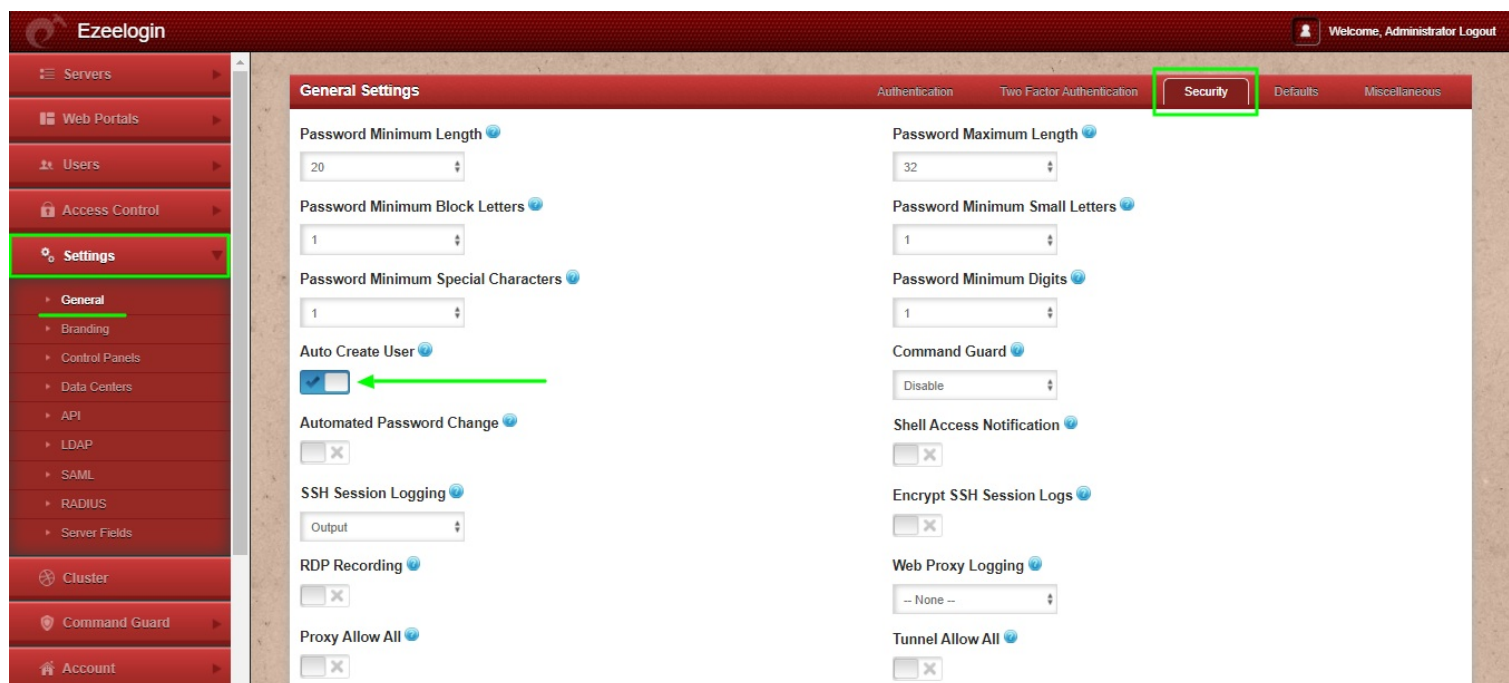
SCP Log

Users find... All Rows Auto

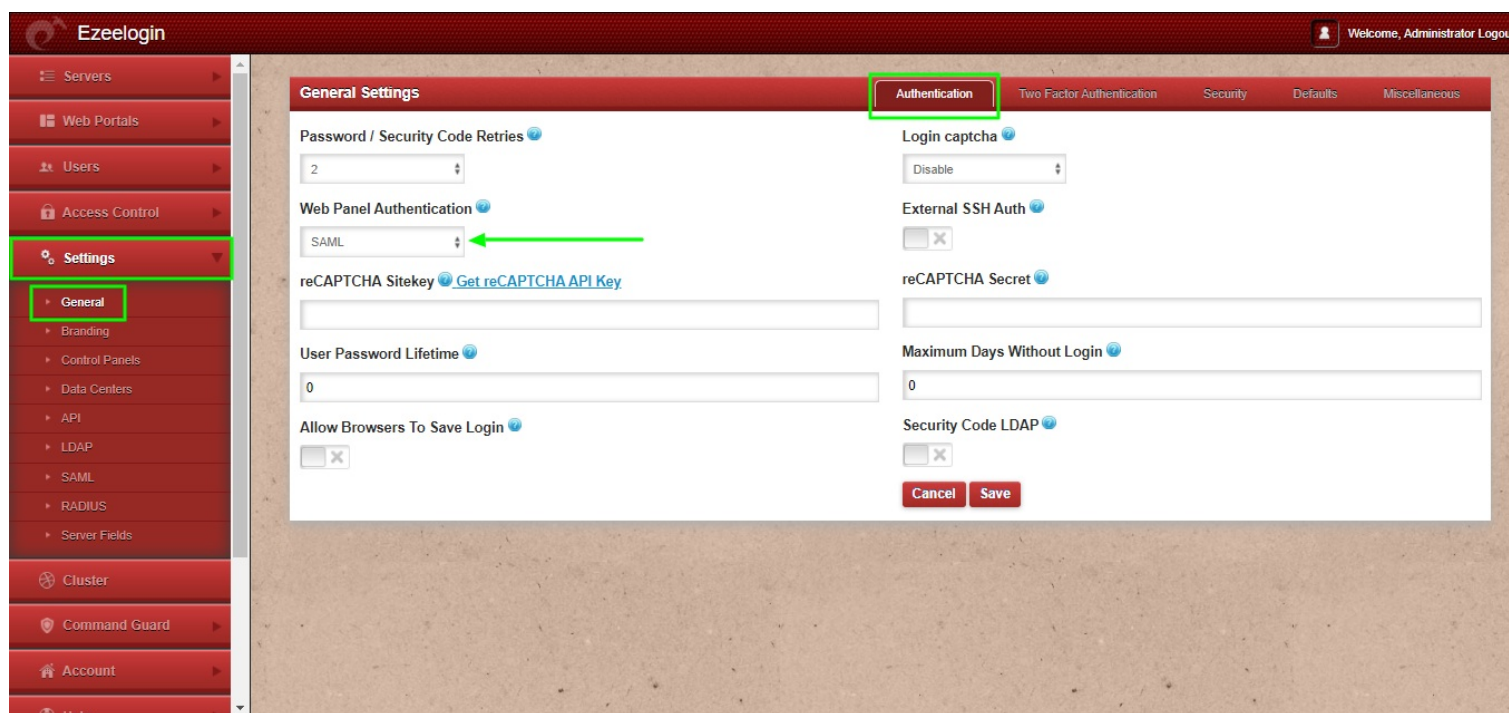
☐	Username ↓	First Name	Last Name	Email	Status	Expiry	User Group	Actions
☐	alex	alex		alex@ezlogin.onmicrosoft.com	Active		Dummy	
☐	ezadmin	Administrator			Active		Admins	

1 - 2 / 2

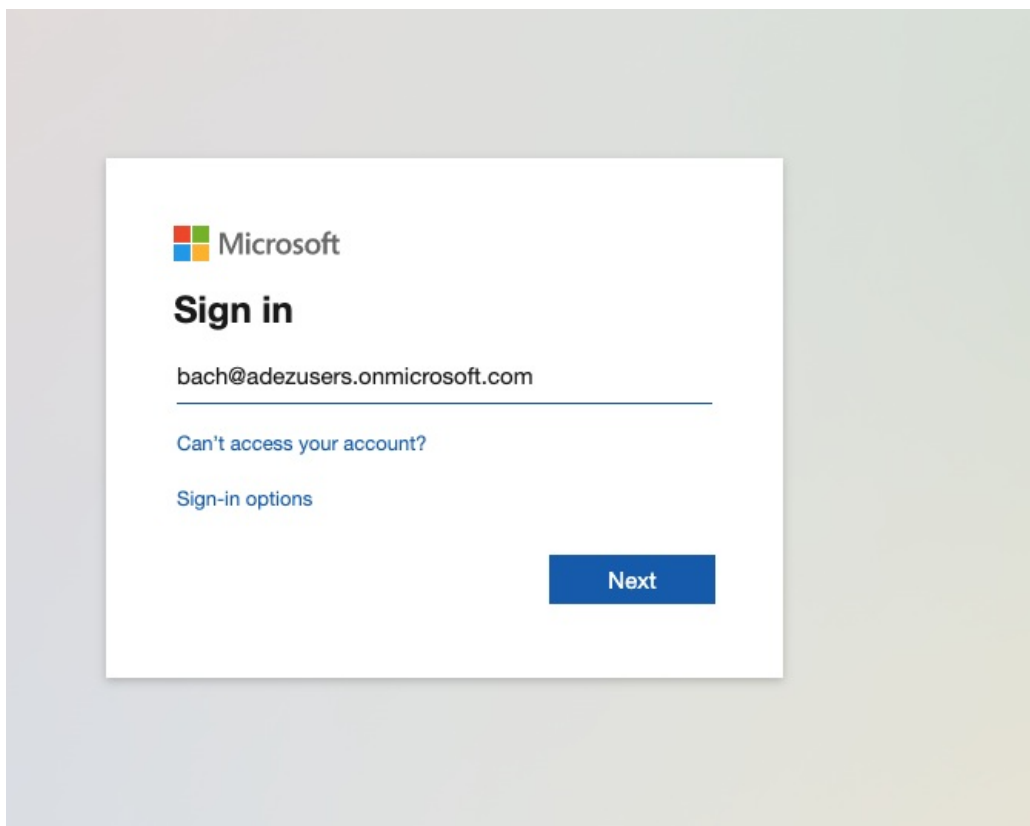
8. Enable Auto Create User from **Ezeelogin GUI -> Settings -> General -> Security -> Enable Auto Create User**, so the user will automatically created after successful authentication from Azure SSO.



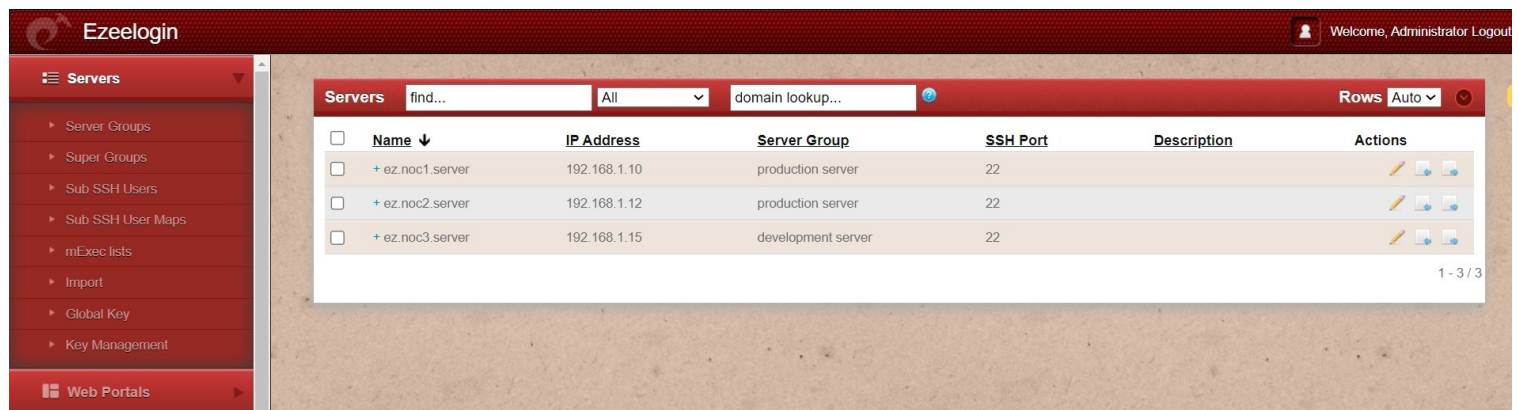
9. Set **Web Panel Authentication to SAML** Under **Settings -> General -> Authentication -> SAML**.



10. Login into the **Ezeelogin 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.



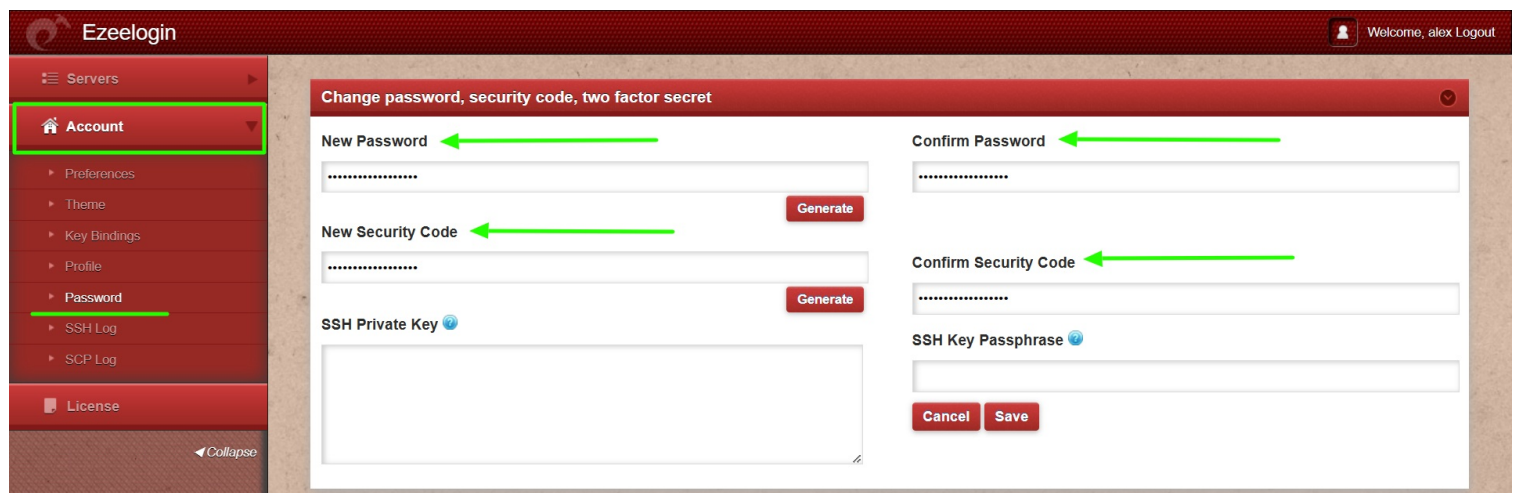
11. Finally, you will be logged into the **Ezeelogin GUI using SAML Authentication**. The user will be created automatically on Ezeelogin after successful authentication from Azure SSO.



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

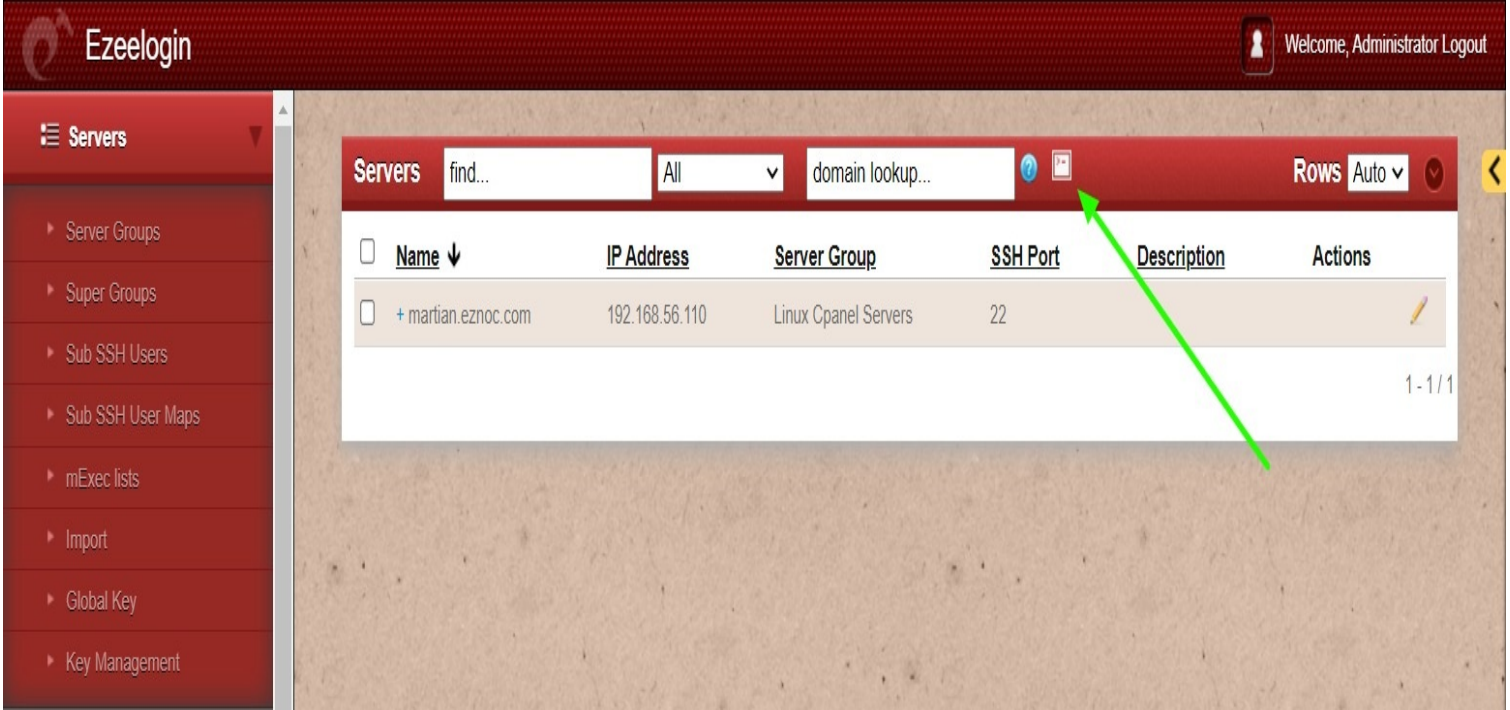
Error: Invalid password

12. After logging into the GUI, you need to **reset the password and security code of the SAML user** under **Account -> Password** in order to SSH to the Ezsh shell.



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

WebSSH: Click on the '**Open Web SSH Console**' icon to SSH via the browser.



WebSSH terminal will open like below. **Users can navigate the server group with the Up and Down arrow buttons and enter to log into the server.**

```
*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.

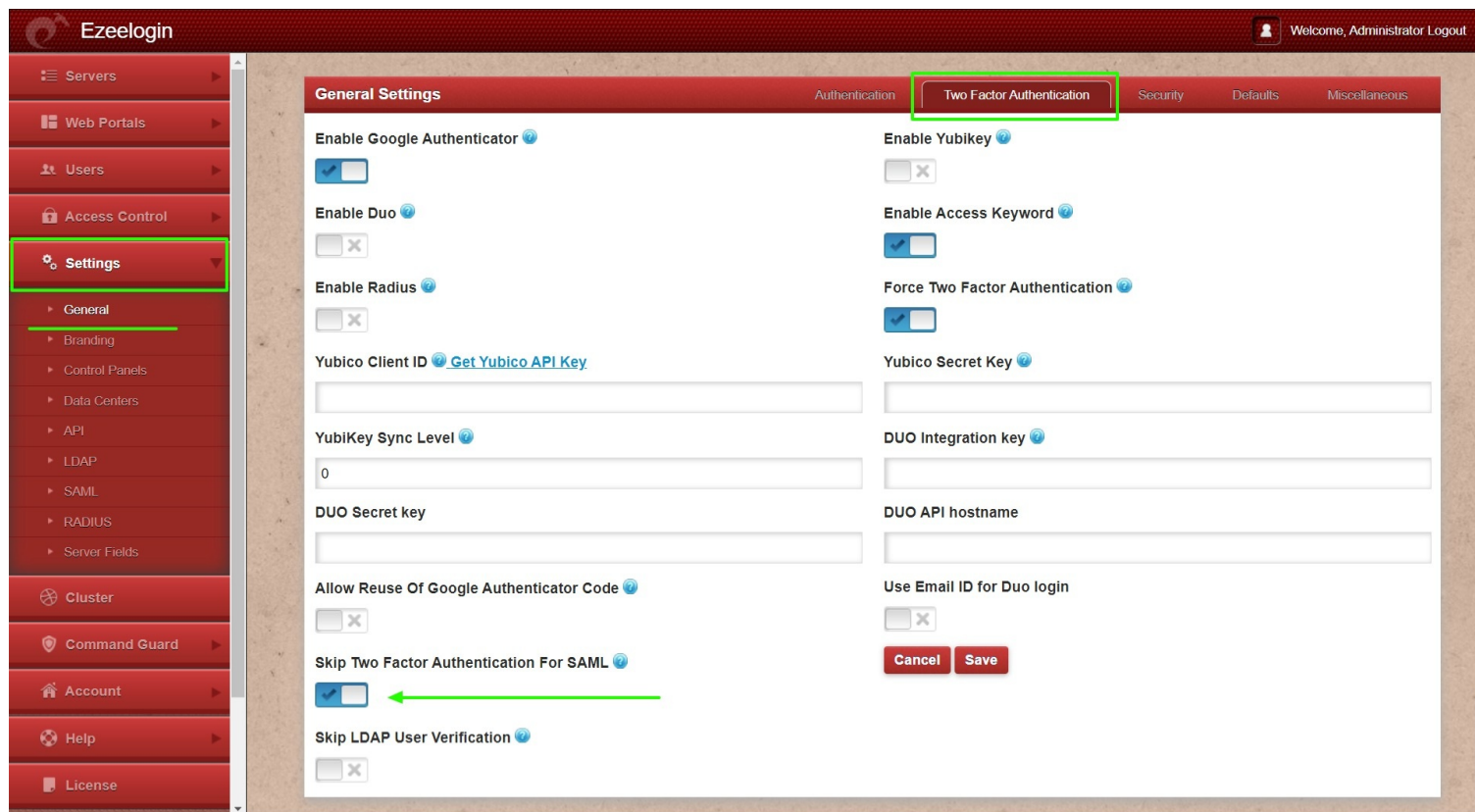
≡ Menu Ezeelogin SSH CONNECTION ESTABLISHED

Native SSH Client: After resetting the password and security code you can **SSH to the Ezsh shell** (using Terminal or Putty) with the **SAML username**.

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

14. If you are SSHing with 2FA enabled using Putty or Terminal it would prompt you to enter the 2FA codes, The 2FA step can be disabled for SAML Authentication under **Settings -> Two Factor Authentication -> Skip Two Factor Authentication for SAML**.

The user will be able to ssh without being prompted for the 2FA codes only if the user is logged into the web panel, otherwise, if the user is not logged into the web panel it would prompt for the 2FA codes.



15. It is **recommended to use the webssh shell for the SAML authentication**. The webssh shell is more convenient as the user would not have to open an SSH client such as Putty/terminal and enter the username/password and 2FA codes.

Using the webssh, the user can ssh from the web panel itself and 2fa will not be prompted if you have enabled the Skip Two factor Authentication for SAML.



Refer article to enable **encryption in Microsoft Azure SSO with Ezeelogin**

How to fetch Username, Firstname, Lastname, and Usergroup Attributes from Azure to Ezeelogin?

Note: Delete and log in again with Azure credentials after configuring the steps below to fetch details from Azure AD to Ezeelogin.

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 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 SAML provider (such as Microsoft Azure), 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](#).

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 web interface. On the left is a sidebar menu with options like Servers, Web Portals, Users, Access Control, and Settings (which is highlighted with a green box). The main content area is titled 'General Settings' and has several tabs: Authentication, Two Factor Authentication, Security, Defaults (highlighted with a green box), and Miscellaneous. Under the 'Defaults' tab, there are two columns of settings. The 'Default User Group' dropdown menu is highlighted with a green arrow pointing to it, indicating it should be set to 'None'. Other settings include Default SSH User (root), Default SSH Port (22), Default RDP Port (3389), Default Data Center (None), Default Control Panel (None), Default Language (English), Default Password Prompt (ssword), Default First Prompt, and Default Root Prompt. At the bottom right of the settings area are 'Cancel' and 'Save' buttons.

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.

The screenshot shows the Ezeelogin web interface. On the left, a sidebar contains navigation links: Servers, Web Portals, Users, Access Control, Settings (highlighted in green), General, Branding, Control Panels, Data Centers, API, LDAP, SAML, OpenID Connect, FIDO2, RADIUS, SIEM, Server Fields, Cluster, Command Guard, Account, and Help. The main content area is titled 'General Settings' and has tabs for Authentication, Two Factor Authentication, Security, Defaults (highlighted in green), and Miscellaneous. The 'Defaults' tab contains the following settings:

- Default SSH User: root
- Default SSH Port: 22
- Default RDP Port: 3389
- Default Data Center: -- None --
- Default Control Panel: -- None --
- Default User Group: Dummy (indicated by a green arrow)
- Default Language: English
- Default Password Prompt: ssword:
- Default First Prompt: (empty field)
- Default Root Prompt: (empty field)

At the bottom right of the settings area are 'Cancel' and 'Save' buttons.

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

1. Click on **Single sign-on** -> **Attributes & Claims Edit** -> Copy **Claim names** and paste them into the **advanced SAML setting** in Ezeelogin.

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

Home > Enterprise applications > Enterprise applications | All applications > ezeelogin >

ezeelogin | SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan
Diagnose and solve problems

Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

Upload metadata file Change single sign-on mode Test this application Got feedback?

1

Basic SAML Configuration

Edit

Identifier (Entity ID) https://192.168.1.36/ezlogin/
Reply URL (Assertion Consumer Service UR https://192.168.1.36/ezlogin/index.php/auth/acs L)
Sign on URL Optional
Relay State (Optional) Optional
Logout Url (Optional) https://192.168.1.36/ezlogin/index.php/auth/slo

2

Attributes & Claims

Edit

givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname

2. 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

Review the attributes listed below if you encounter the following error while attempting to log in as a SAML user.
Could not get the username from the SAML response

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

Access Control

Settings

- General
- Reading
- Global Roles
- Global Groups
- AFS
- LDAP
- SAML
- OAuth2
- Server Health

Cluster

Command Guard

Account

Help

License

Collapse

New Signing Certificate

New Encryption Certificate

Username Attribute Name

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Group Attribute Name

http://schemas.microsoft.com/ws/2008/05/identity/claims/groups

Firstname Attribute Name

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Lastname Attribute Name

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname

Cancel Fetch Save

Azure AD Settings

Advanced

We recommend using the **web ssh** shell when you are using SAML authentication, which is a lot more convenient as you would not have to worry about the SSH password or the security code for the users.

Add a different email address for each user. By default, Ezeelogin uses email addresses for creating users. If you want to add an existing user in Ezeelogin to SSO, Add the user with the exact username, and email address as follows. (Ezeelogin will verify with the email address of the users by default). Make sure to add the email address for the Ezeelogin Administrator user.

Saml authentication is not supported for slaves if the URL is IP-based. If you want to authenticate slave using saml you have to use the domain name.

3. Refer detailed article to create users in Ezeelogin with the same user group in Azure AD.

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

Refer to the article to [map the existing user group from SAML Provider\(AZURE\) to Ezeelogin as the Ezeelogin user group](#).

Related Articles:

[Login as superadmin when SSO is enabled globally](#)

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

[setup web SSH console in Ezeelogin and SSH via browser](#)

[Unable to log in with Azure SSO](#)

[How to auto-create the Azure SSO user to the same group in Ezeelogin?](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-saml-authentication-in-ezeelogin-gui-using-microsoft-azure-ss0-and-azure-active-directory-326.html>