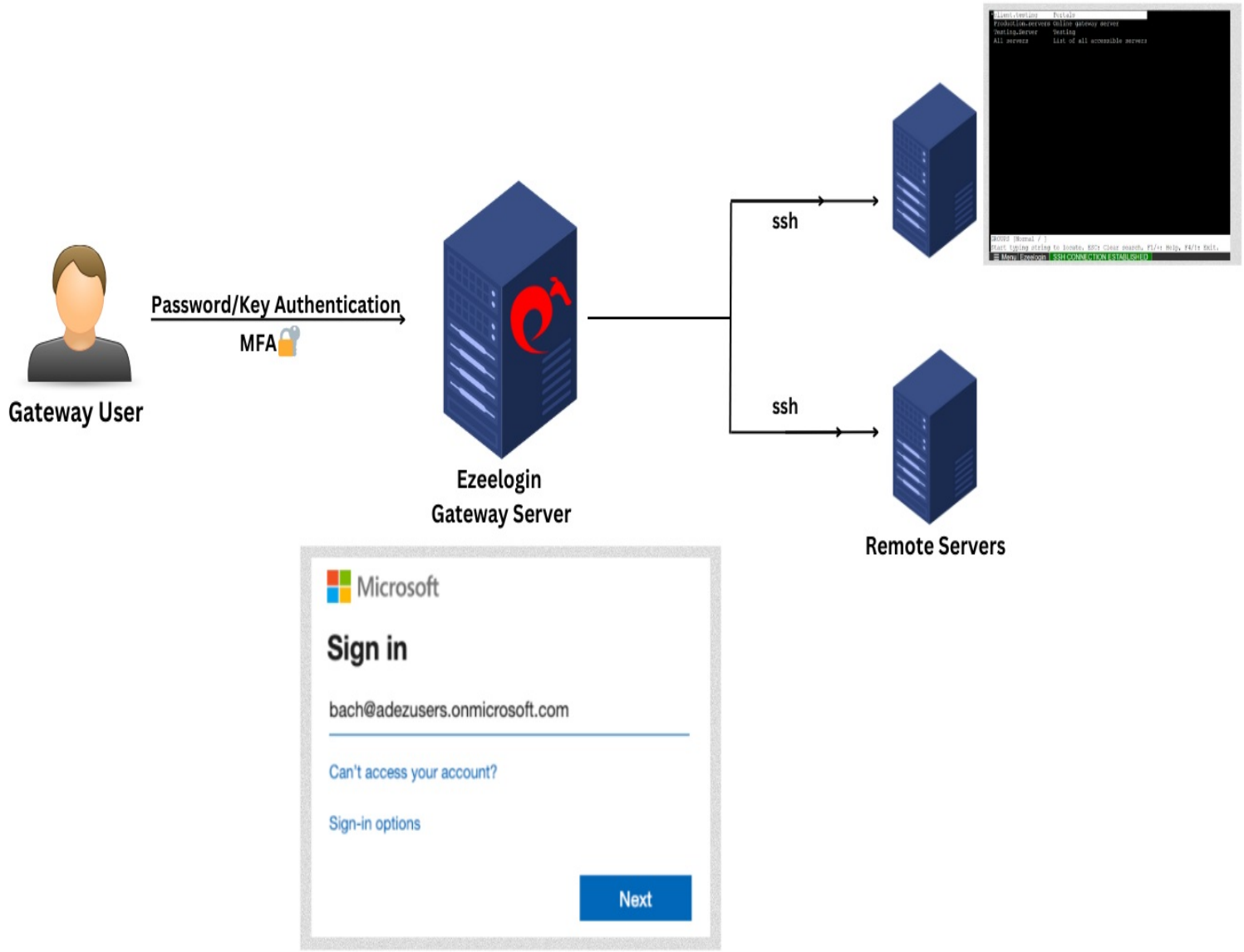
Integrate SAML Authentication in Ezeelogin GUI using Microsoft Azure SSO and Azure Active Directory

326 admin May 28, 2026 Features & Functionalities, Productivity & Efficiency Features, Security Features 11514

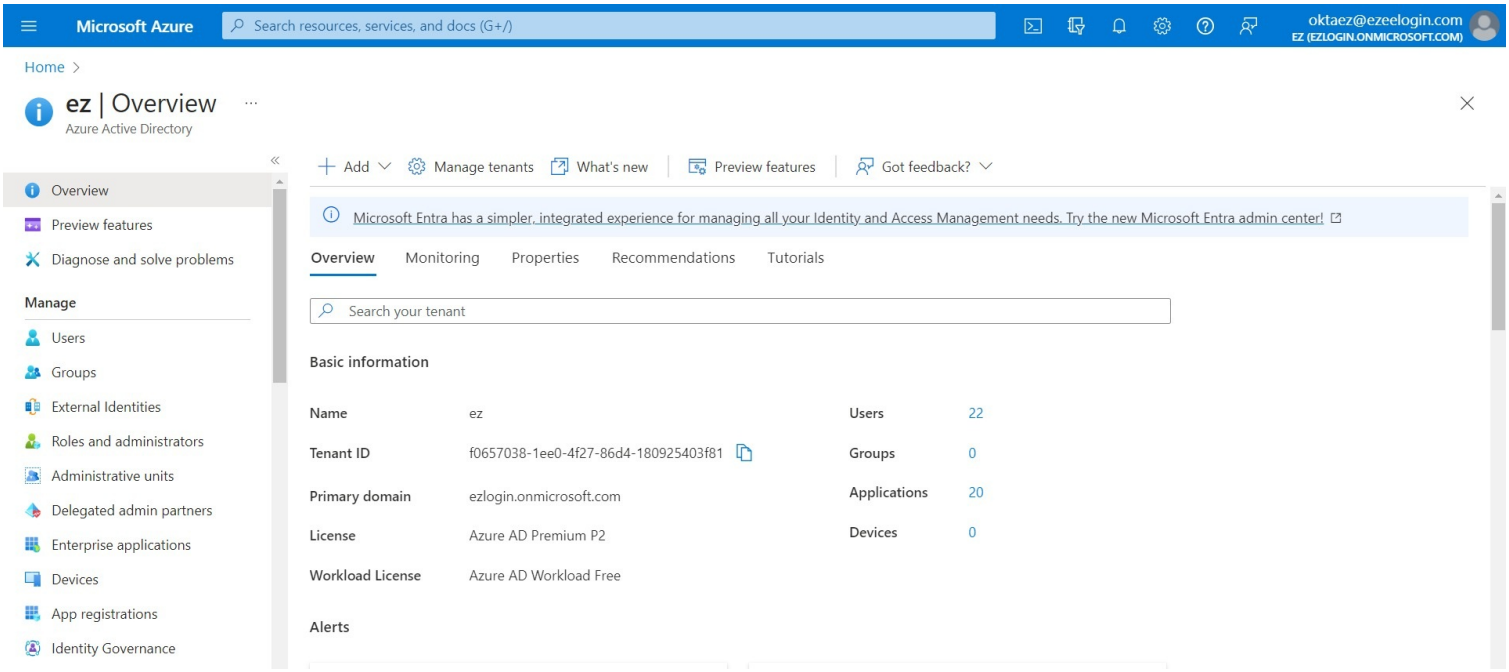
Configure Microsoft Azure SSO SAML-based Authentication in Ezeelogin GUI.

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

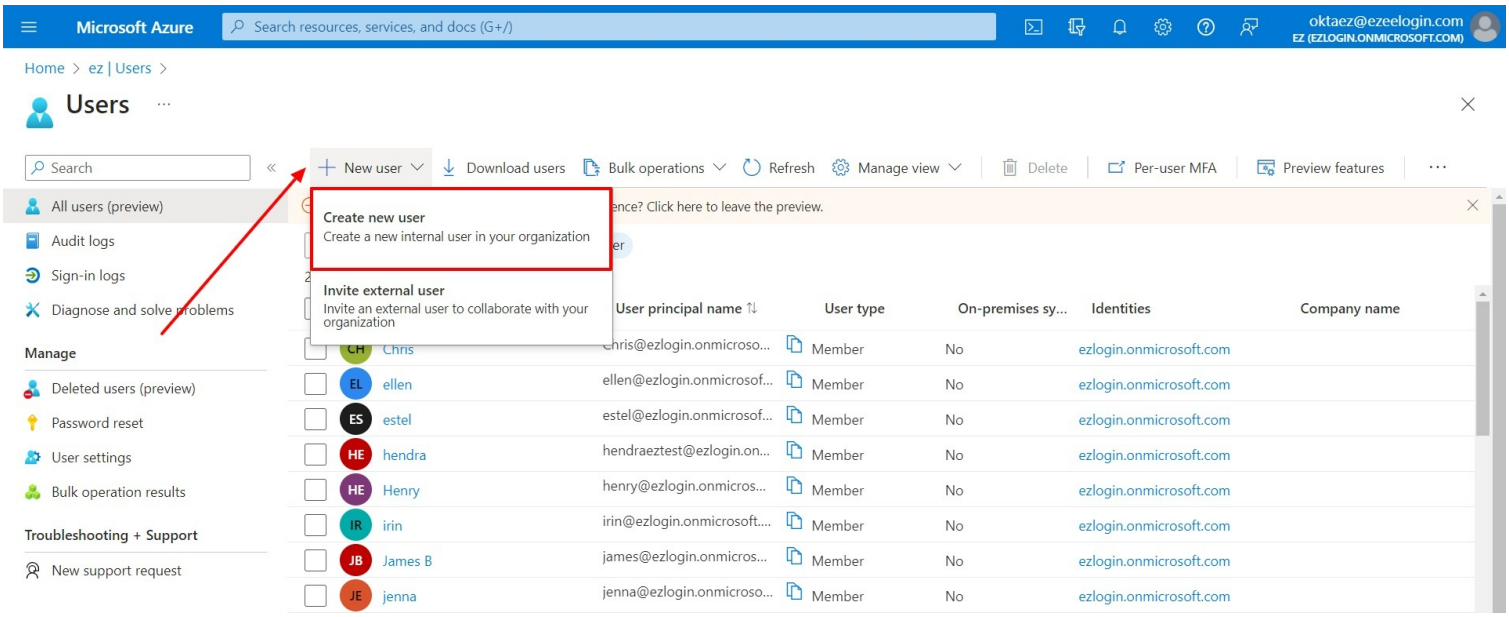
Note: SAML is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



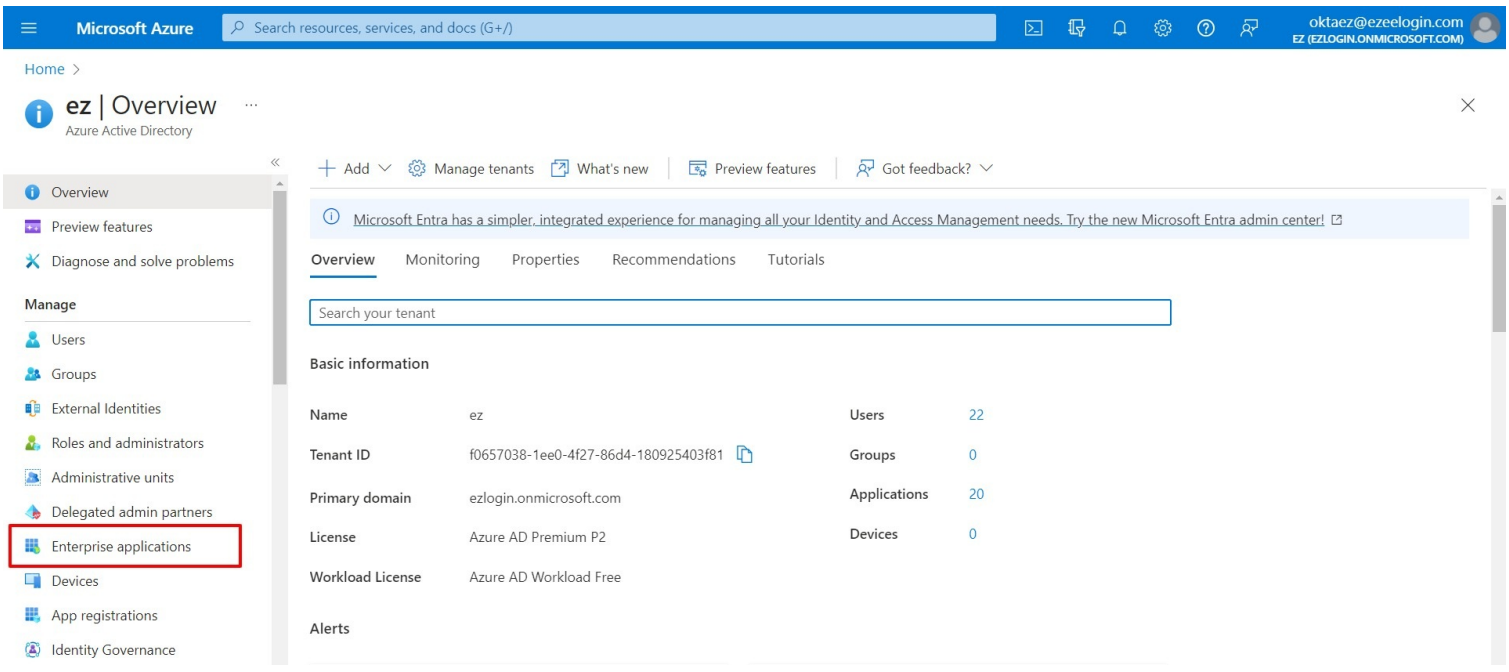
1. Login into your Microsoft Azure account and **Create an Active Directory service**.



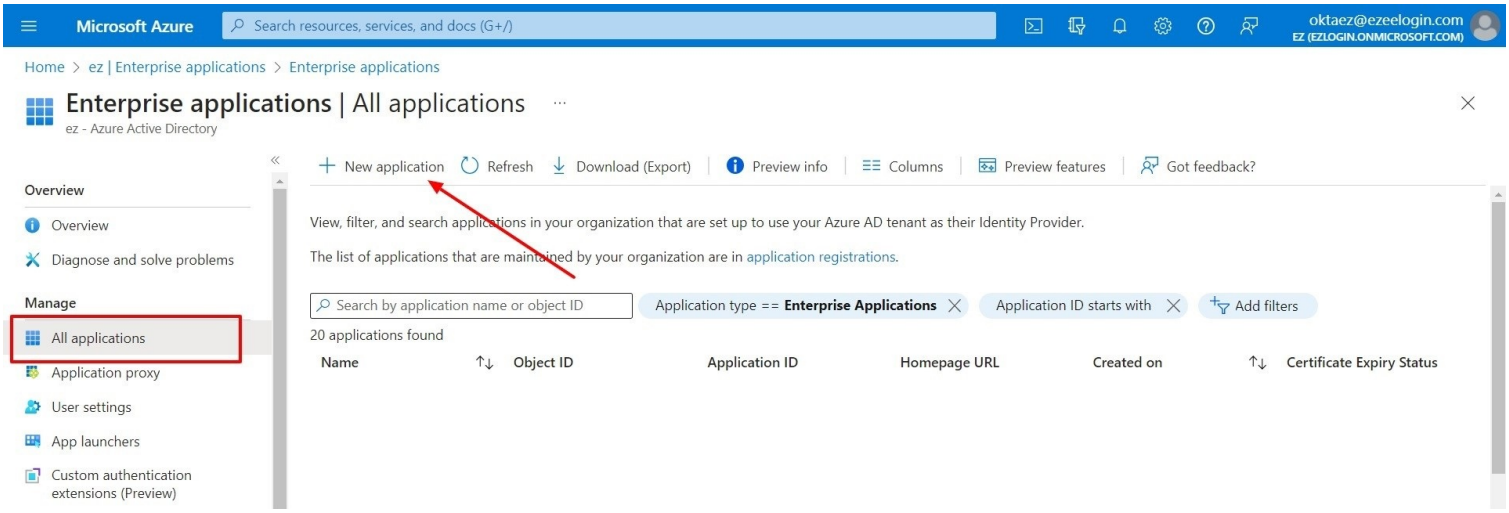
2. Add Users in AD (Skip this step, if Users already exist). This user in turn would authenticate into the Ezeelogin GUI.
To create a user in AD, click on **User tab** >> **New user** >> Provide the user name, name, password, etc, and click **Create**.



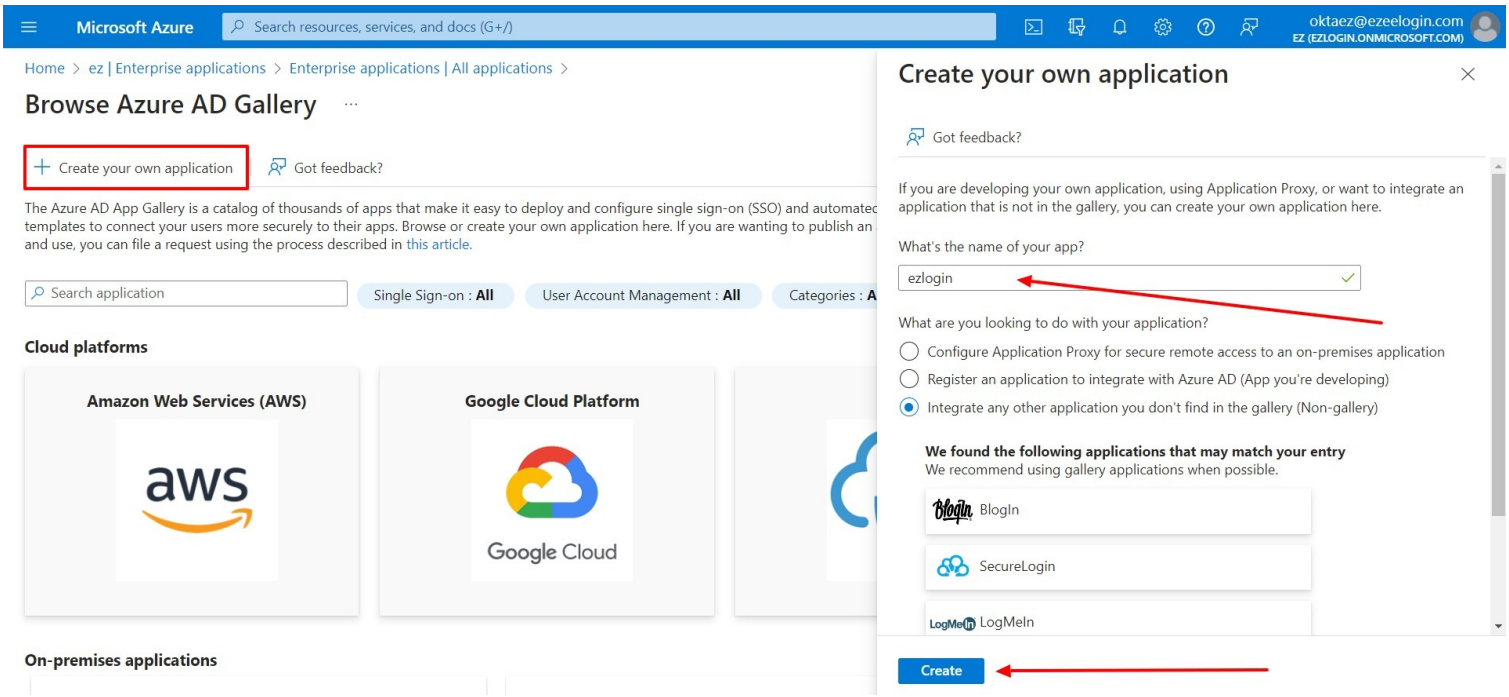
3. Create an **Enterprise Application**. Click on Enterprise applications.



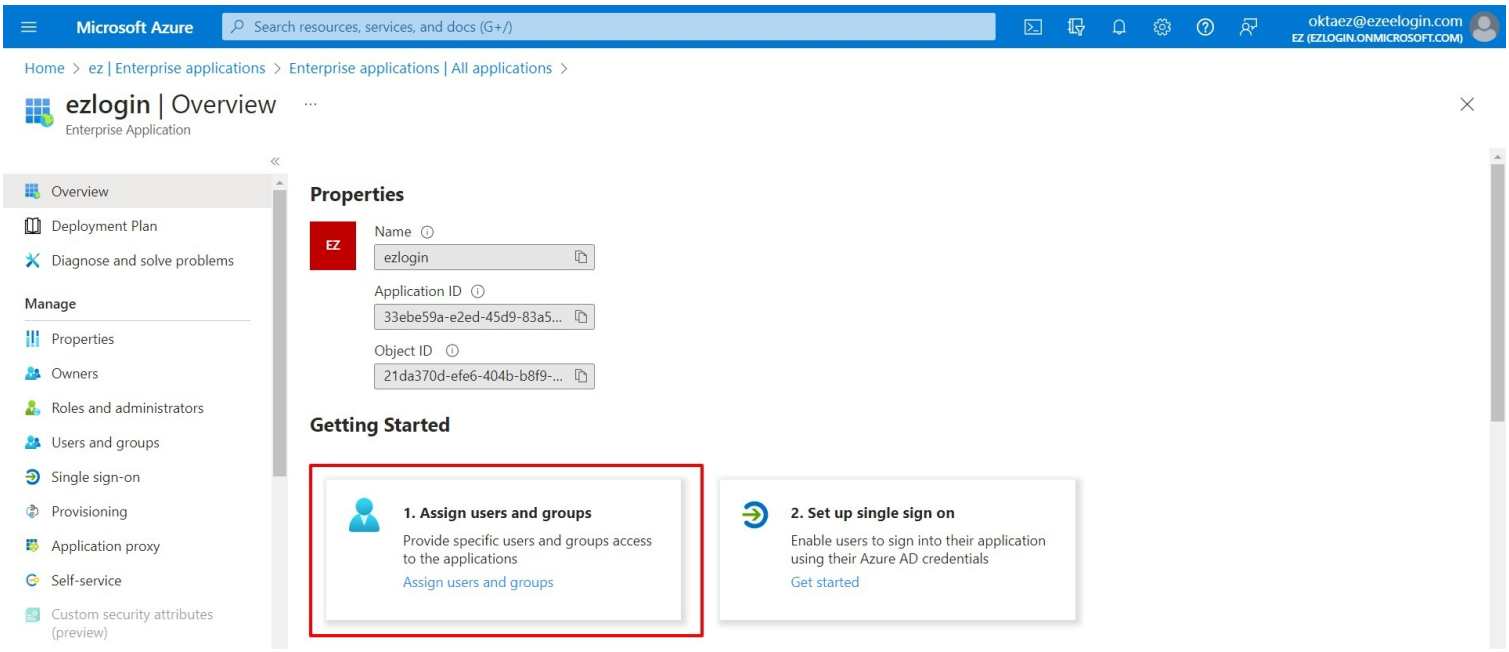
Click on **All applications** >> **New application.**



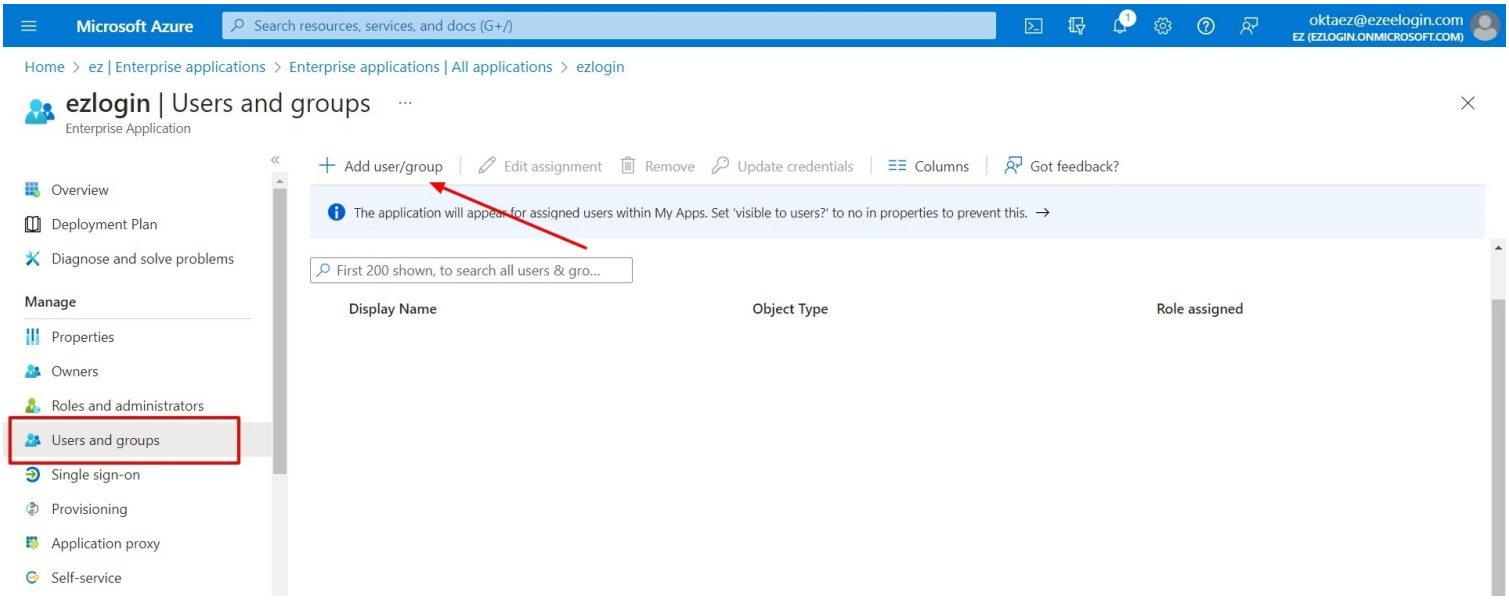
Click on **Create your own application** >> **Provide the name for your application** >> Check **Integrate any other application you don't find in the gallery(Non-gallery)** >> **Create**.



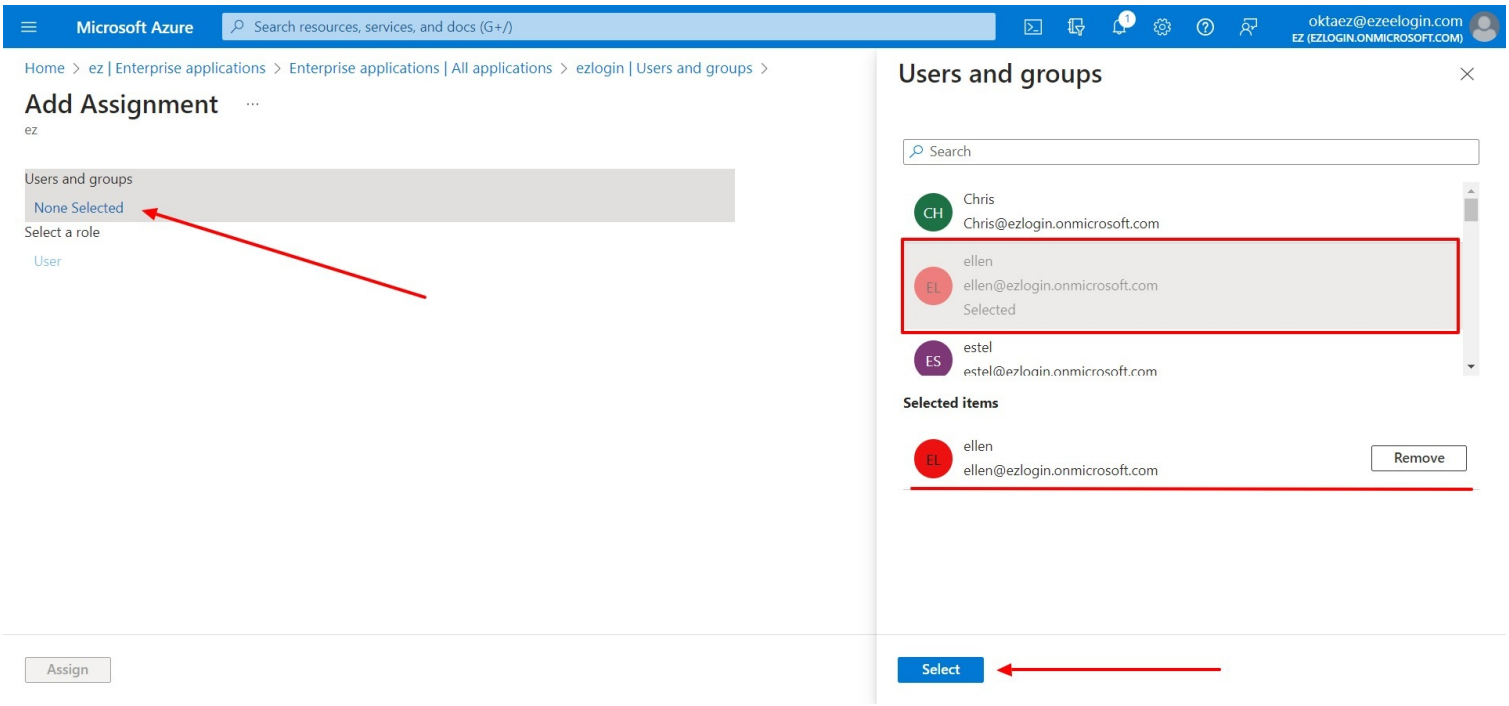
4. Assign the user to the Enterprise application. Click on **Assign users and groups.**



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

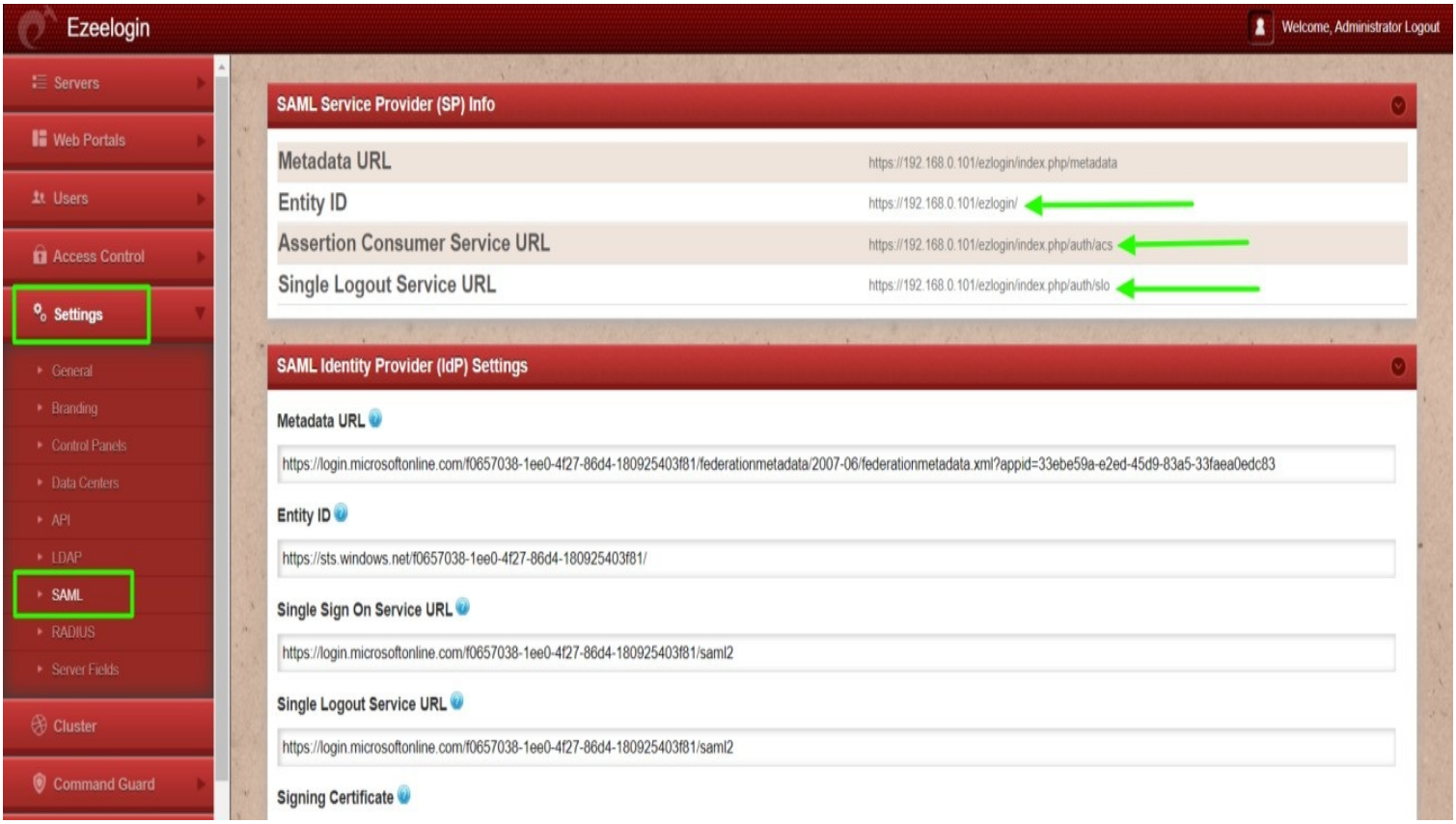


Click on **None Selected** >> **select the users** who want to assign to the application >> **select**.

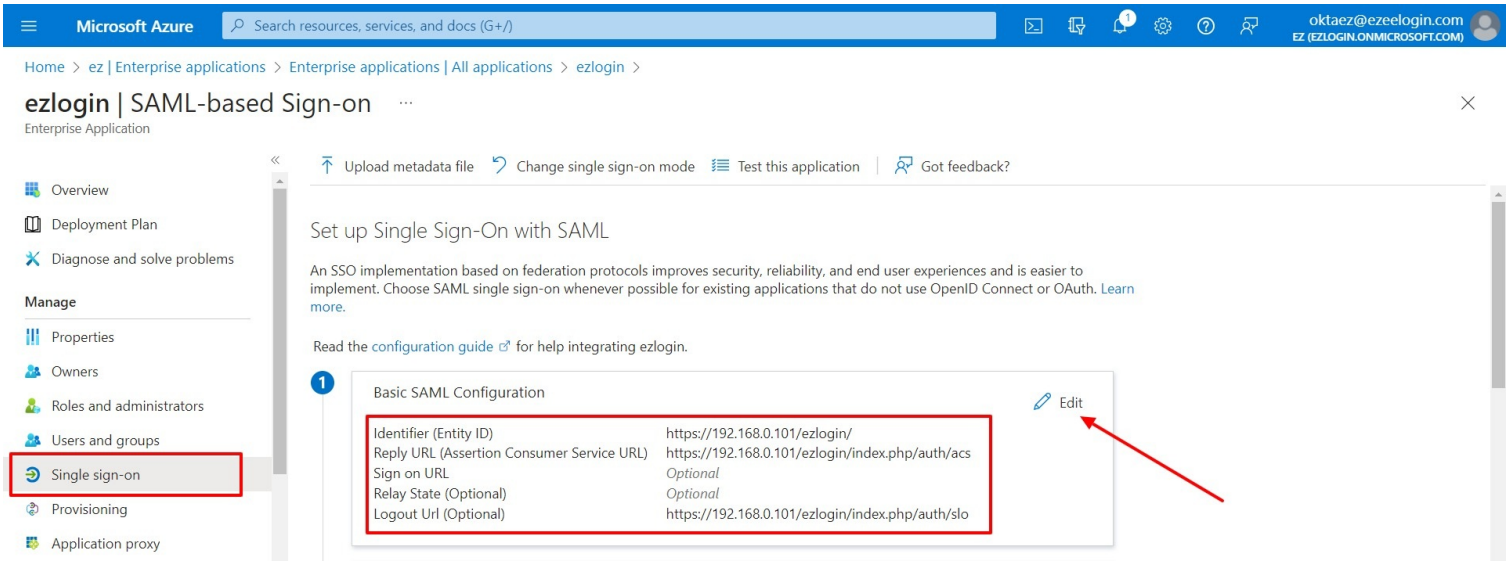


5. Configure Single Sign On (SAML)

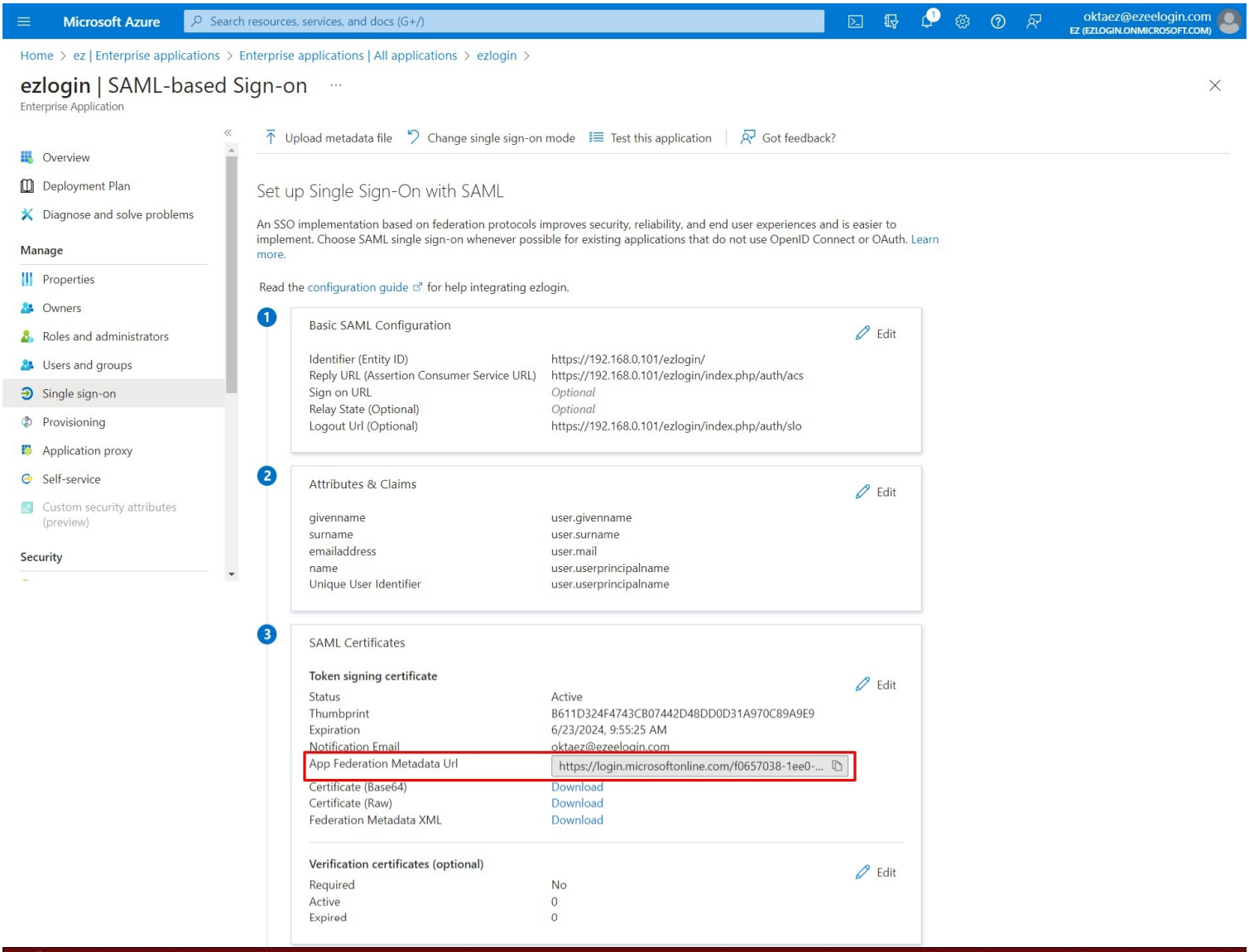
Identifier (Entity ID) - You can find it from **Ezeelogin GUI > Settings > SAML> Entity ID**)
Reply URL (Assertion Consumer Service URL) - You can find it from **Ezeelogin GUI > Settings > SAML>Assertion Consumer Service URL**)
Logout Url (Optional) - You can find it from **Ezeelogin GUI > Settings > SAML>Single Logout Service URL**

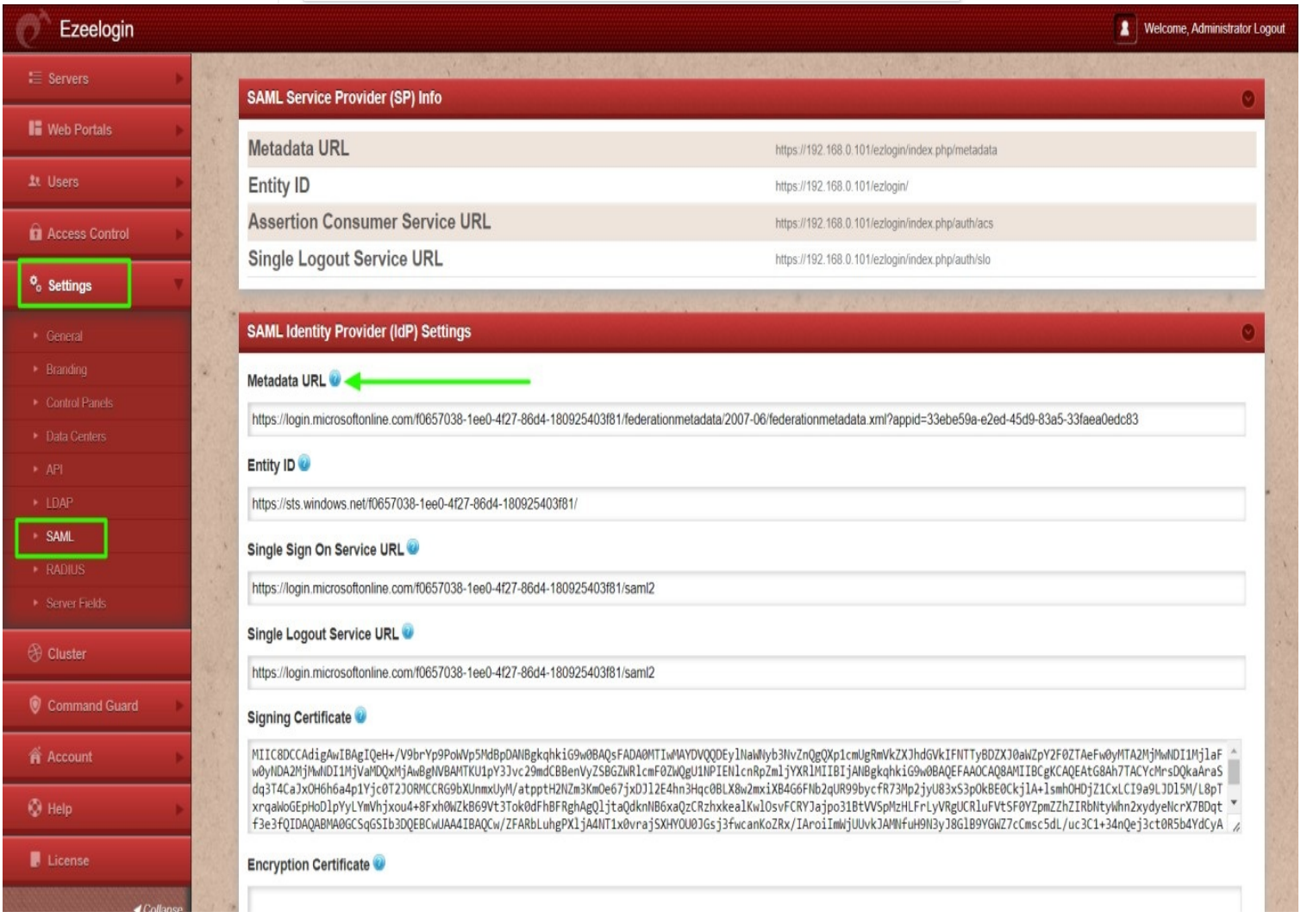


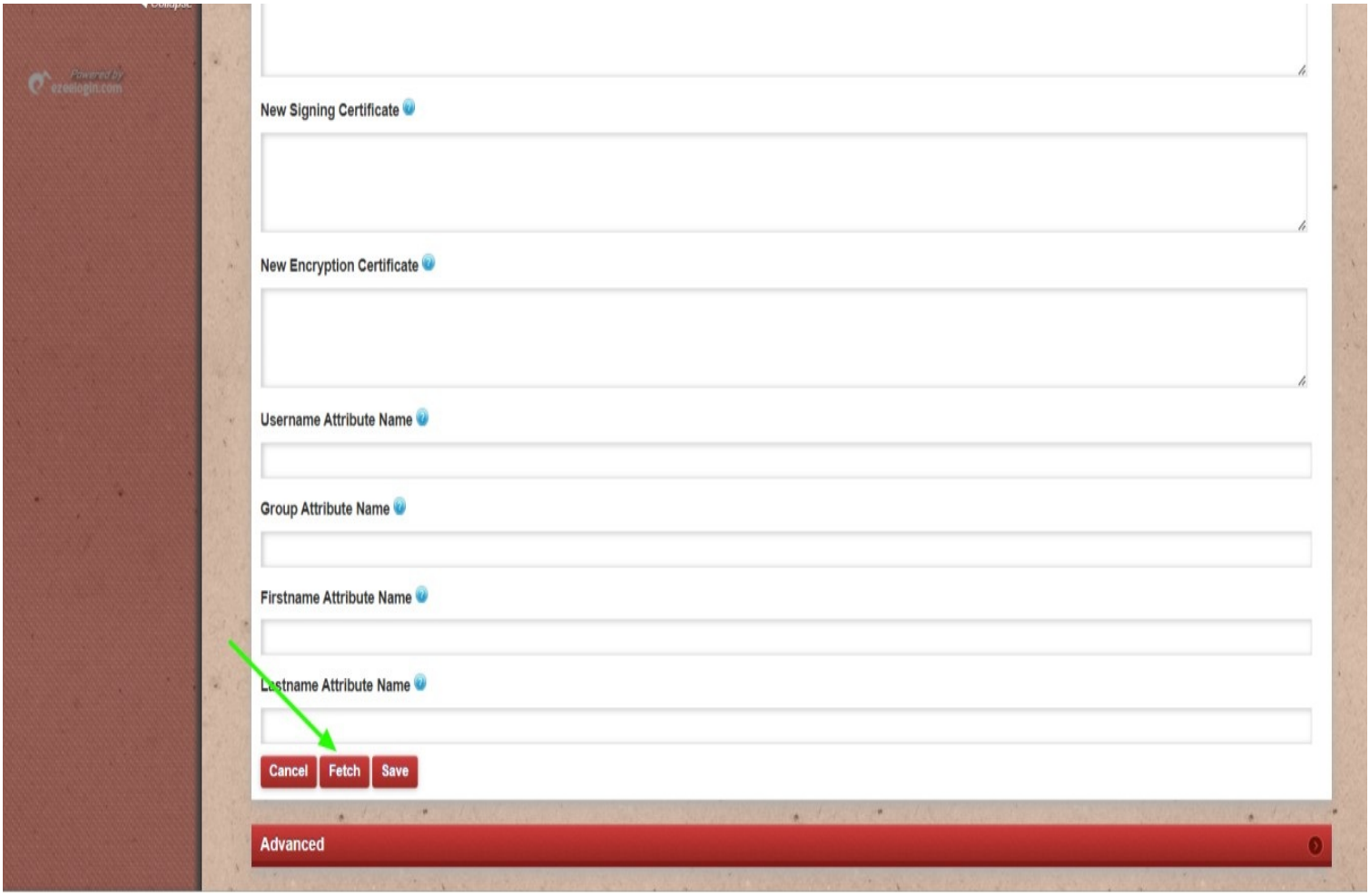
Click on **Single sign-on** >> **Basic SAML Configuration Edit** >> Copy **Entity ID**, **Assertion Consumer Service URL,** and **Logout Url** from Ezeelogin and paste in the specified fields.



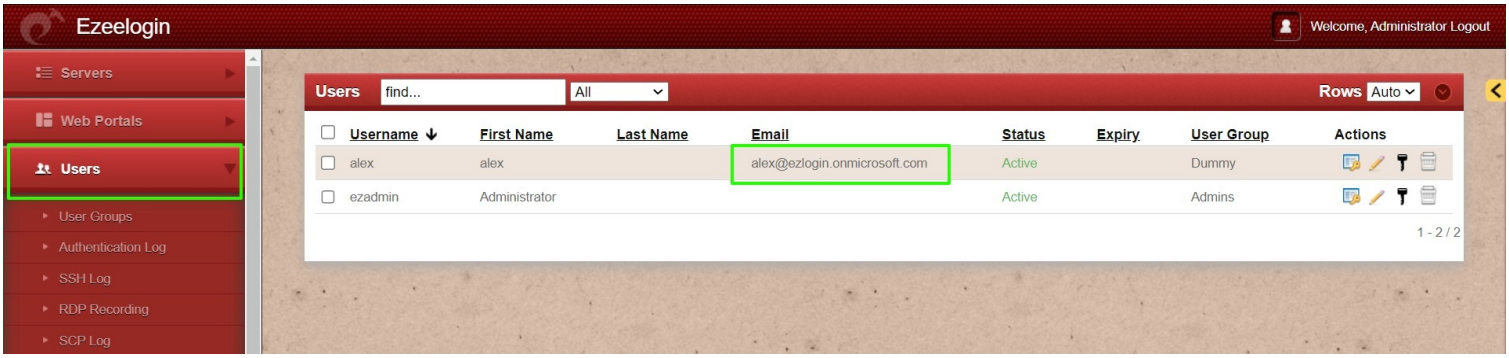
6. Copy the Metadata URL and paste it to the Metadata URL on **Ezeelogin GUI > Settings > SAML Metadata URL** and click on the **fetch button,** it will auto-fill the SAML setting and **SAVE** it**.**


Microsoft Azure
Search resources, services, and docs (G+/)
oktaez@ezeelogin.com
EZ (EZLOGIN.ONMICROSOFT.COM)
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
Self-service
Custom security attributes (preview)
Security
Upload metadata file
Change single sign-on mode
Test this application
Got feedback?
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
Edit
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
2
Attributes & Claims
Edit
givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname
3
SAML Certificates
Token signing certificate
Edit
Status Active
Thumbprint B611D324F4743CB07442D48DD0D31A970C89A9E9
Expiration 6/23/2024, 9:55:25 AM
Notification Email oktaez@ezeelogin.com
App Federation Metadata Url https://login.microsoftonline.com/f0657038-1ee0-...
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download
Verification certificates (optional)
Edit
Required No
Active 0
Expired 0

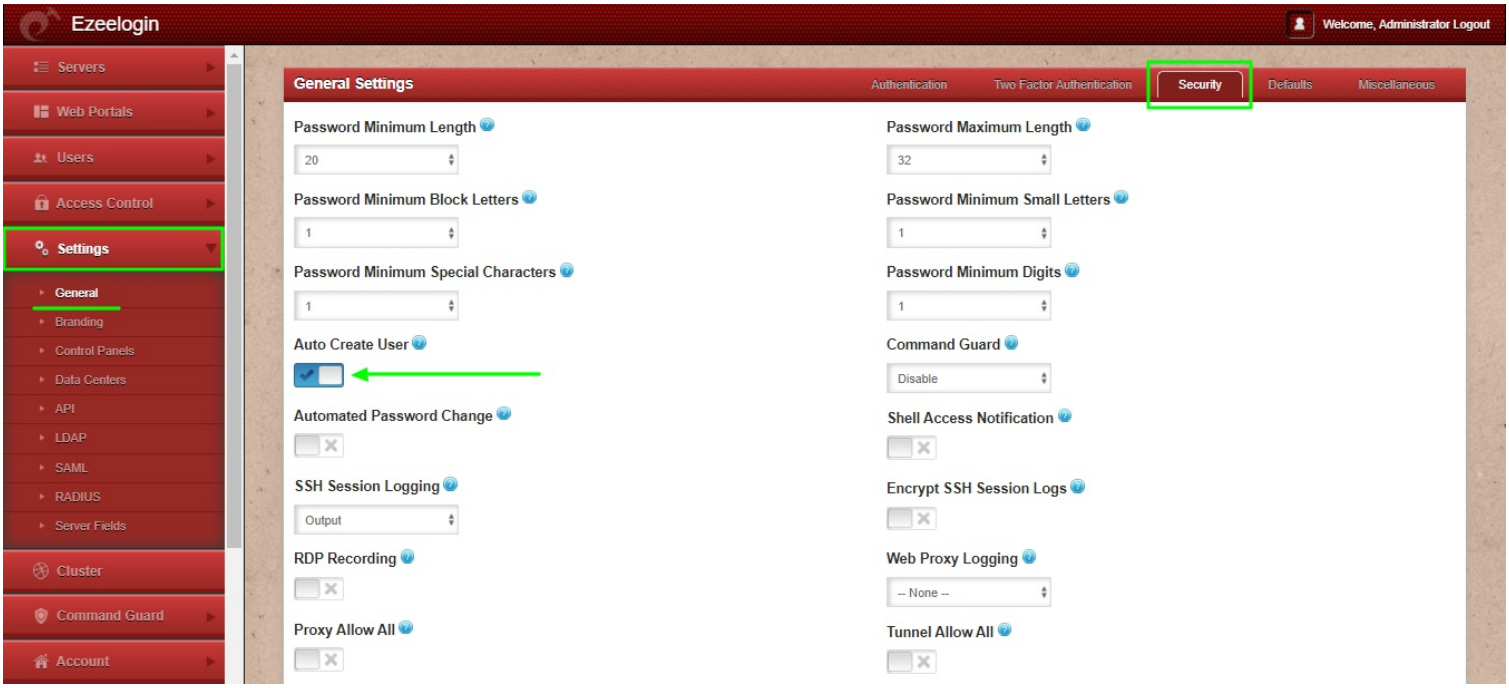

Ezeelogin
Welcome, Administrator Logout
Servers
Web Portals
Users
Access Control
Settings
General
Branding
Control Panels
Data Centers
API
LDAP
SAML
RADIUS
Server Fields
Cluster
Command Guard
Account
Help
License
Collapse
SAML Service Provider (SP) Info
Metadata URL https://192.168.0.101/ezlogin/index.php/metadata
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
https://login.microsoftonline.com/f0657038-1ee0-4f27-86d4-180925403f81/federationmetadata/2007-06/federationmetadata.xml?appid=33ebe59a-e2ed-45d9-83a5-33faea0edc83
Entity ID
https://sts.windows.net/f0657038-1ee0-4f27-86d4-180925403f81/
Single Sign On Service URL
https://login.microsoftonline.com/f0657038-1ee0-4f27-86d4-180925403f81/saml2
Single Logout Service URL
https://login.microsoftonline.com/f0657038-1ee0-4f27-86d4-180925403f81/saml2
Signing Certificate
MIIC8DCCAdigAwIBAgIQeH+/V9brYp9PoWVp5MdBpDANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMTA2MjMwNDI1MjlaFw0yNDA2MjMwNDI1MjVaMDQxMjAwBgNVBAMTKU1pY3Jvc29mdCBBenVyZSBGZWRlcmF0ZWQgU1NPIEN1cnRpZmljYXRlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtG8Ah7TACYcMrsDQkaAraSdq3T4CaJxOH6h6a4p1Yjc0T2JORMCCRG9bXUnmxUyM/atpptH2NZm3KmOe67jxDJl2E4hn3Hqc0BLX8w2mxiXB4G6FNb2qUR99bycfR73Mp2jyU83xS3pOkBE0CkjlA+lsmhOHDjZ1CxLCI9a9LJDl5M/L8pTxrqaWoGEpHoDlpYyLYmVhjxou4+8Fxh0WZkB69Vt3Tok0dFhBFRghAgQljtaQdknNB6xaQzCRzhxkealKwlOsvFCRYJajpo31BtVVSpMzHLFrLyVRgUCRluFVtSF0YZpmZZhZIRbNtyWhn2xydyeNcrX7BDqtf3e3fQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCw/ZFARbLuhgPXljA4NT1x0vrajSXHYOU0JGsj3fwcanKoZRx/IAroiImWjUUvkJAMNfuH9N3yJ8GlB9YGWZ7cCmsc5dL/uc3C1+34nQej3ct0R5b4YdCyA
Encryption Certificate



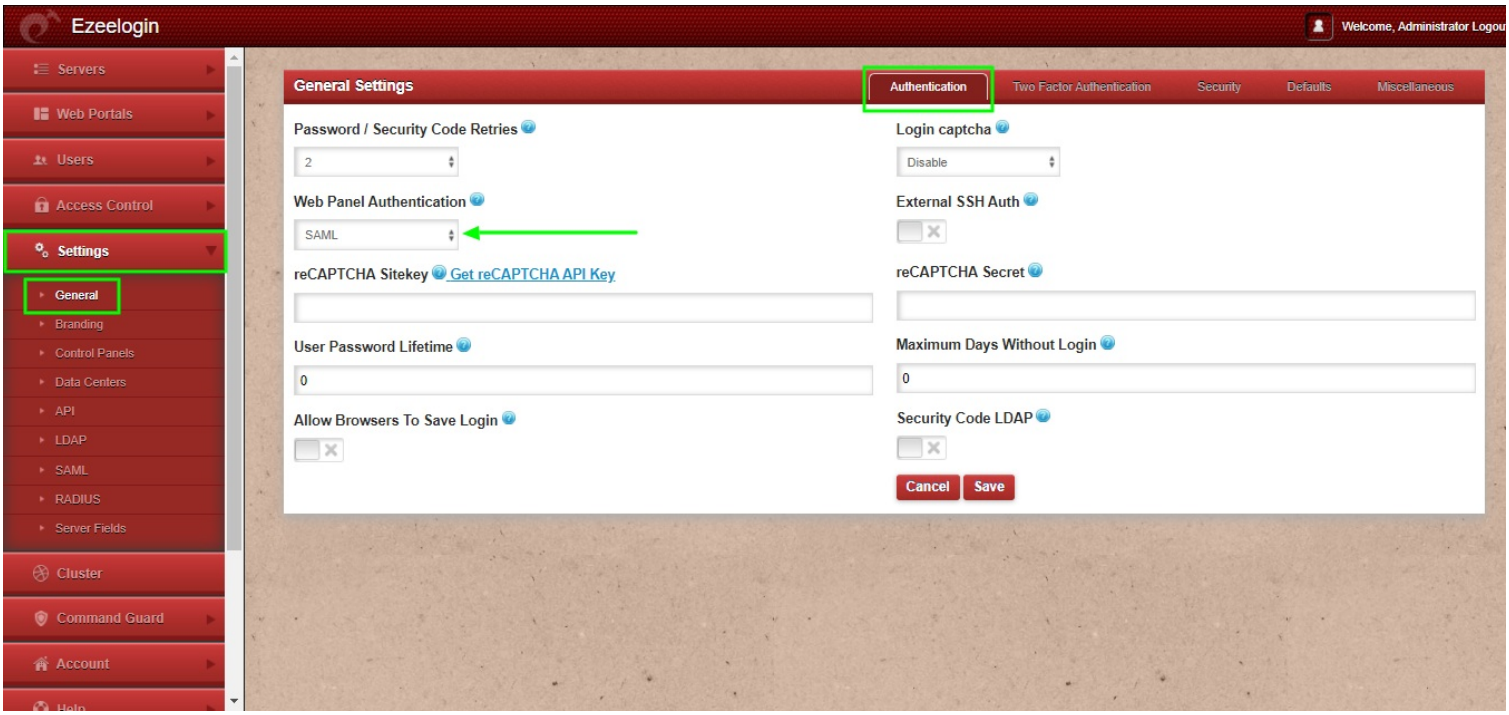
7. Add users in your Azure AD Directory into the Ezeelogin GUI. Make sure the **email ID entered in GUI is identical to the one in SAML.**



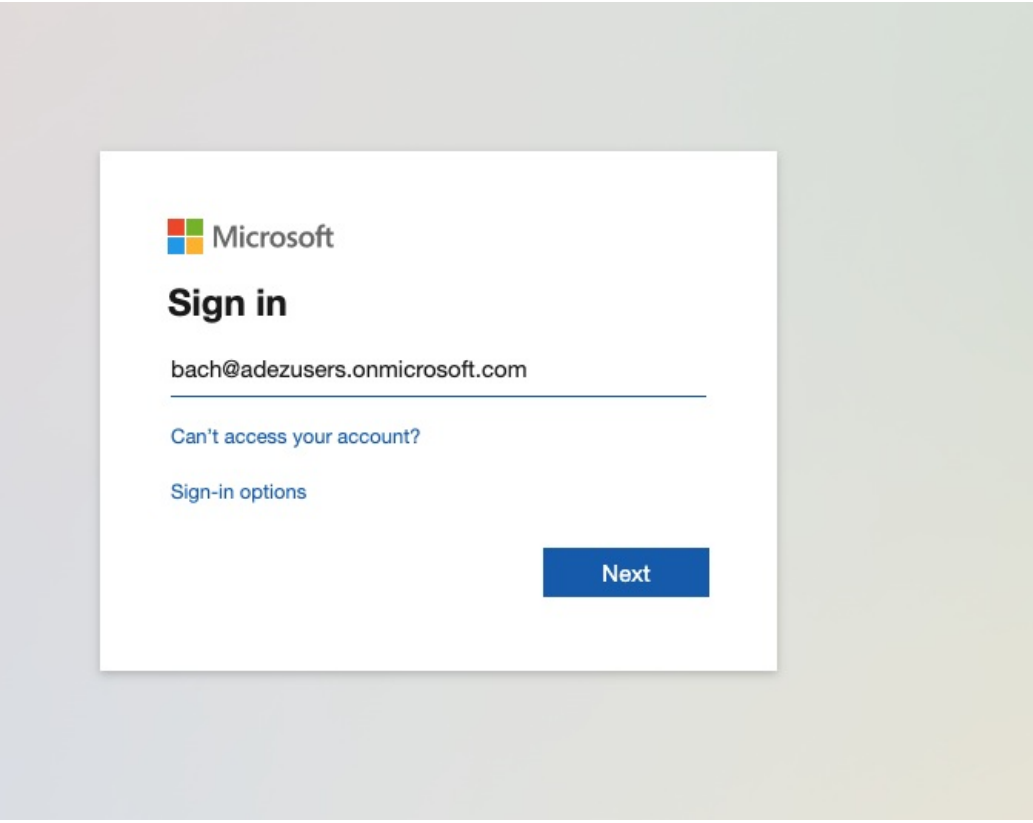
8. Enable Auto Create User from **Ezeelogin GUI** -> **Settings** -> **General** -> **Security** -> **Enable Auto Create User,** so the user will automatically created after successful authentication from Azure SSO.



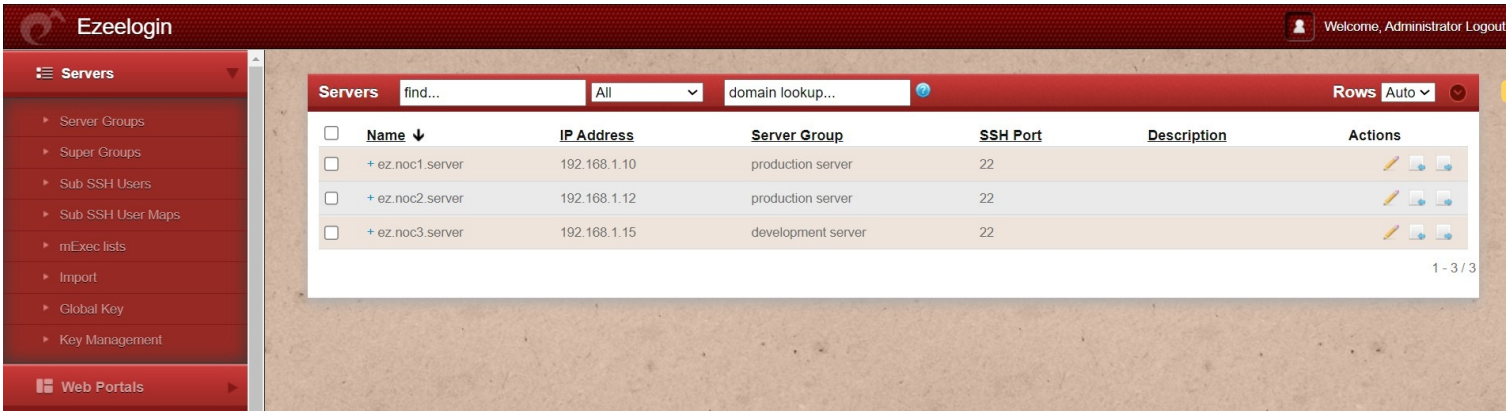
9. Set **Web Panel Authentication to SAML** Under **Settings** -> **General** -> **Authentication** -> **SAML.**



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.



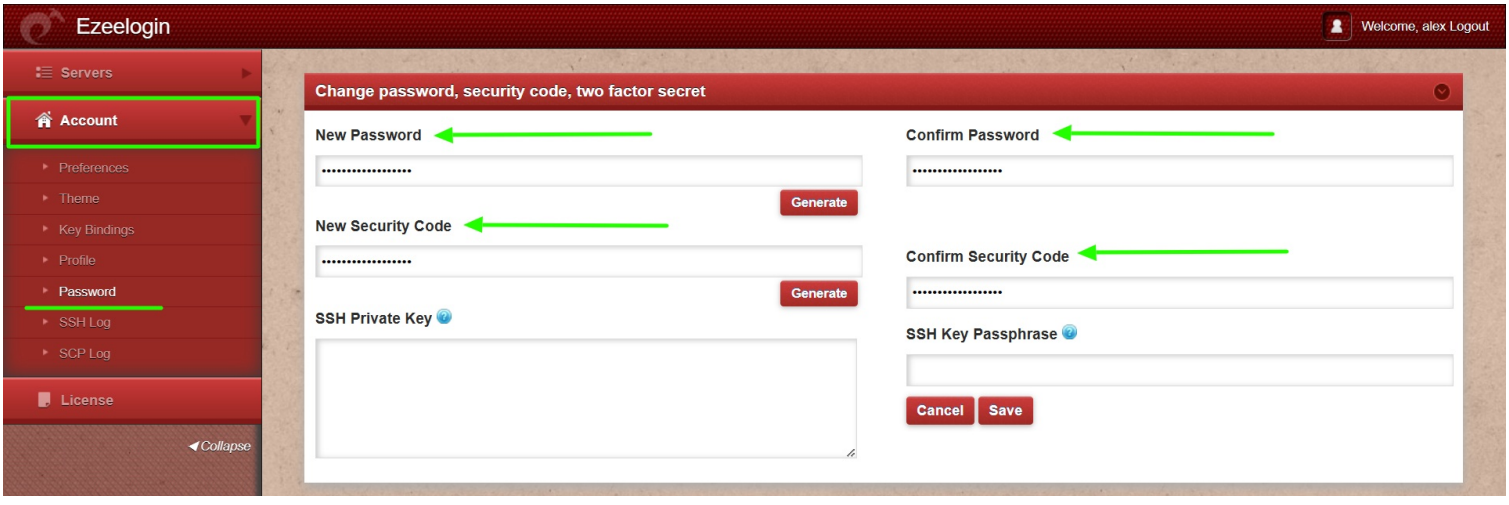
11. Finally, you will be logged into the **Ezeelogin GUI using SAML Authentication**. The user will be created automatically on Ezeelogin after successful authentication from Azure SSO.



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

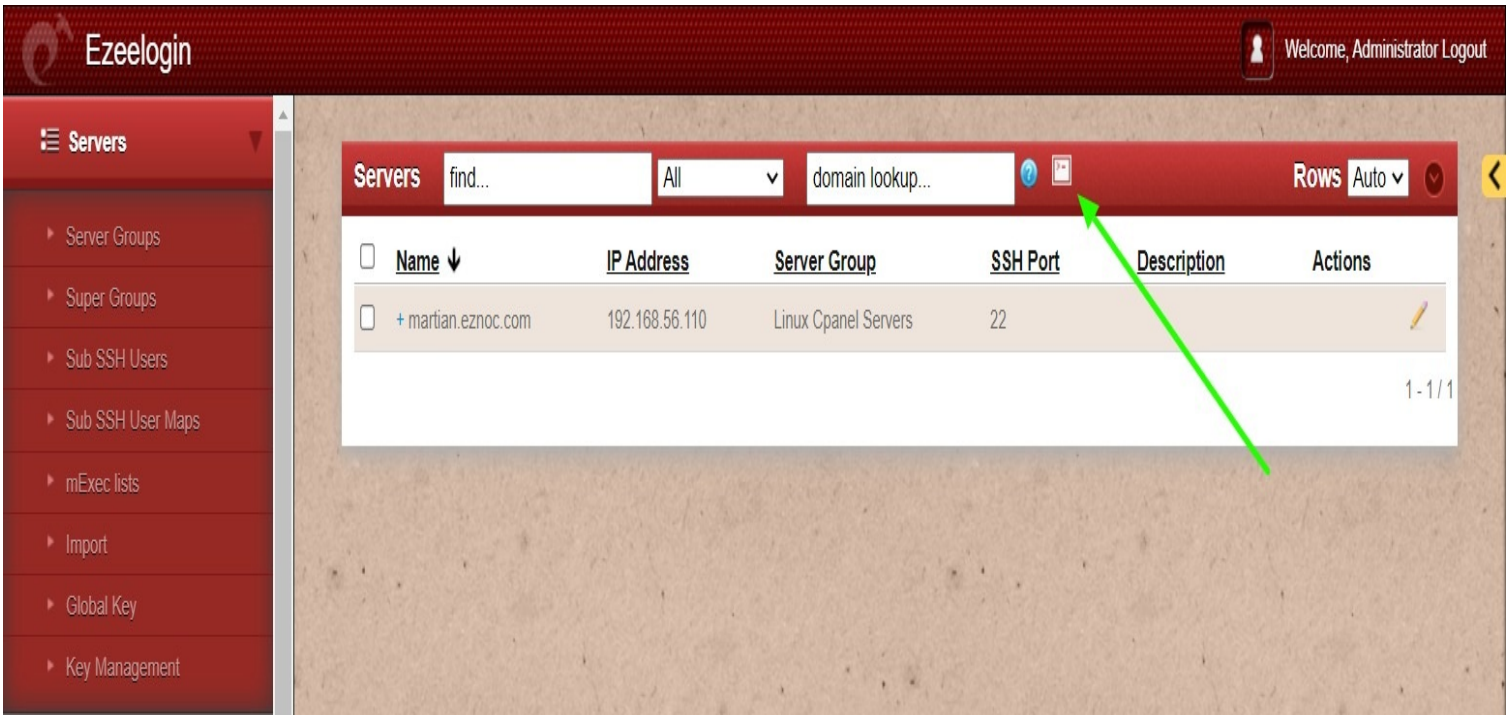
Error: Invalid password

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.

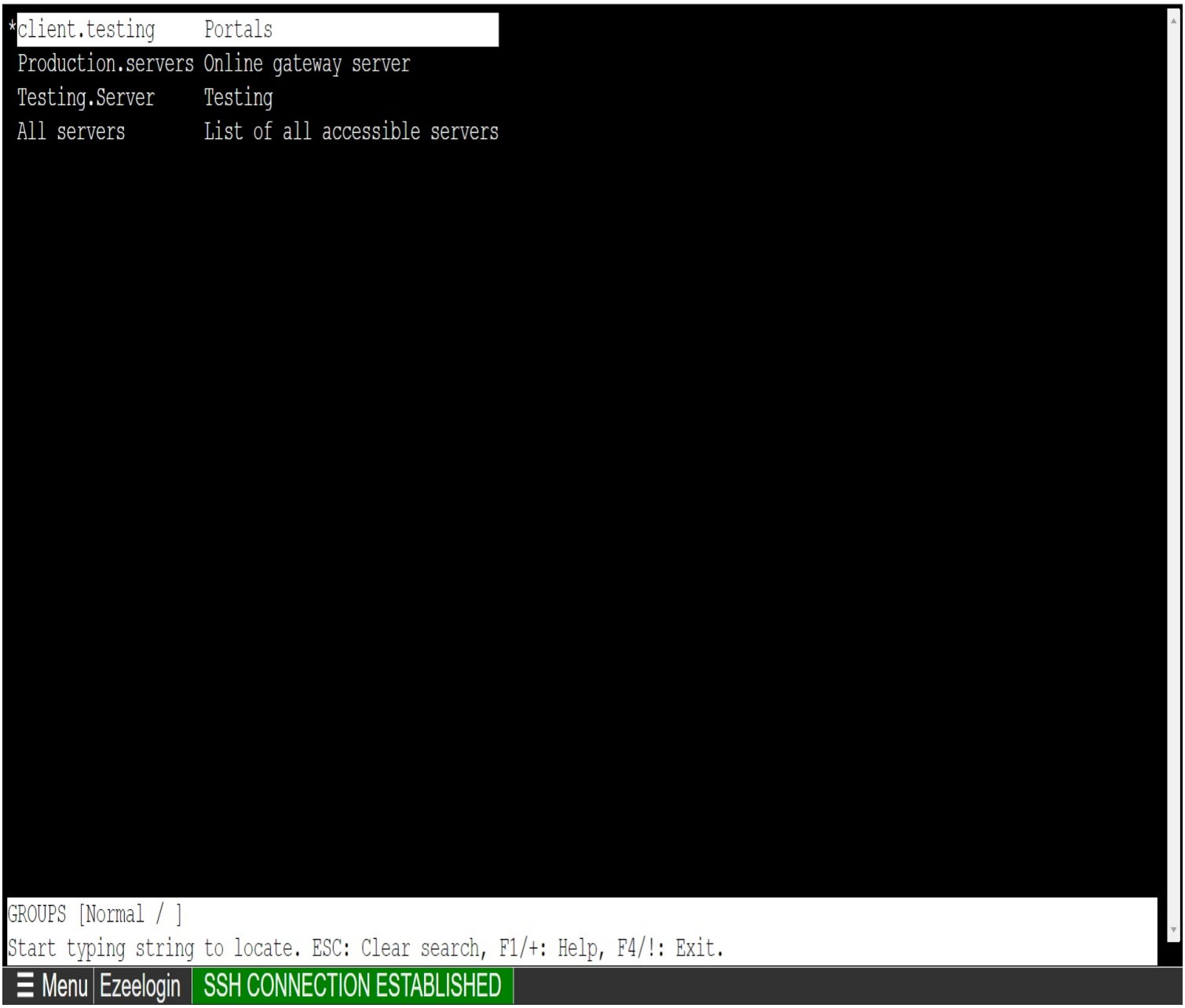


13. You can log in to **Ezeelogin shell** via **Webssh** shell or using any **SSH client** such as Putty or terminal etc.

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.**

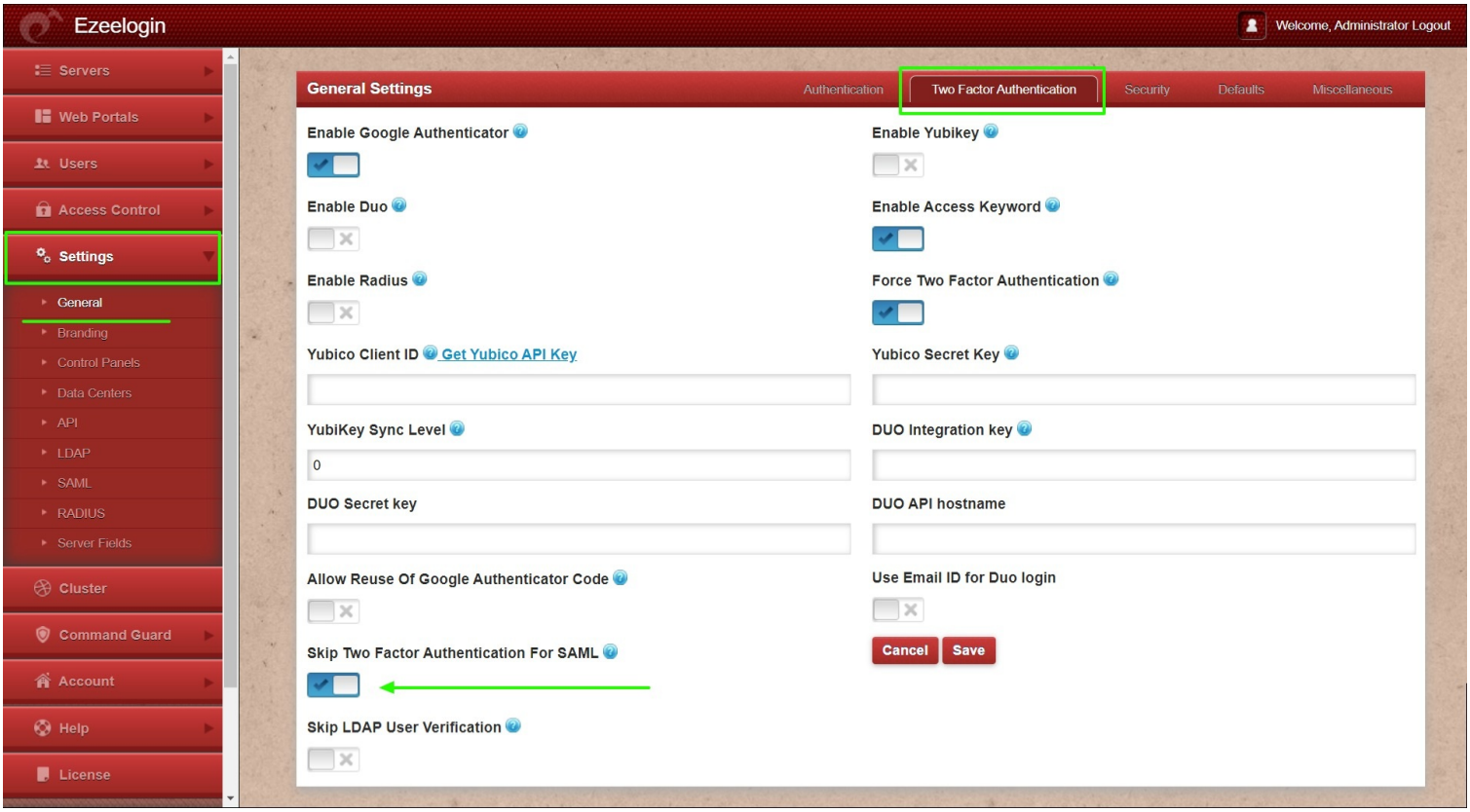


Native SSH Client: After resetting the password and security code you can **SSH to the Ezsh shell** (using Terminal or Putty) with the **SAML username**.



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:

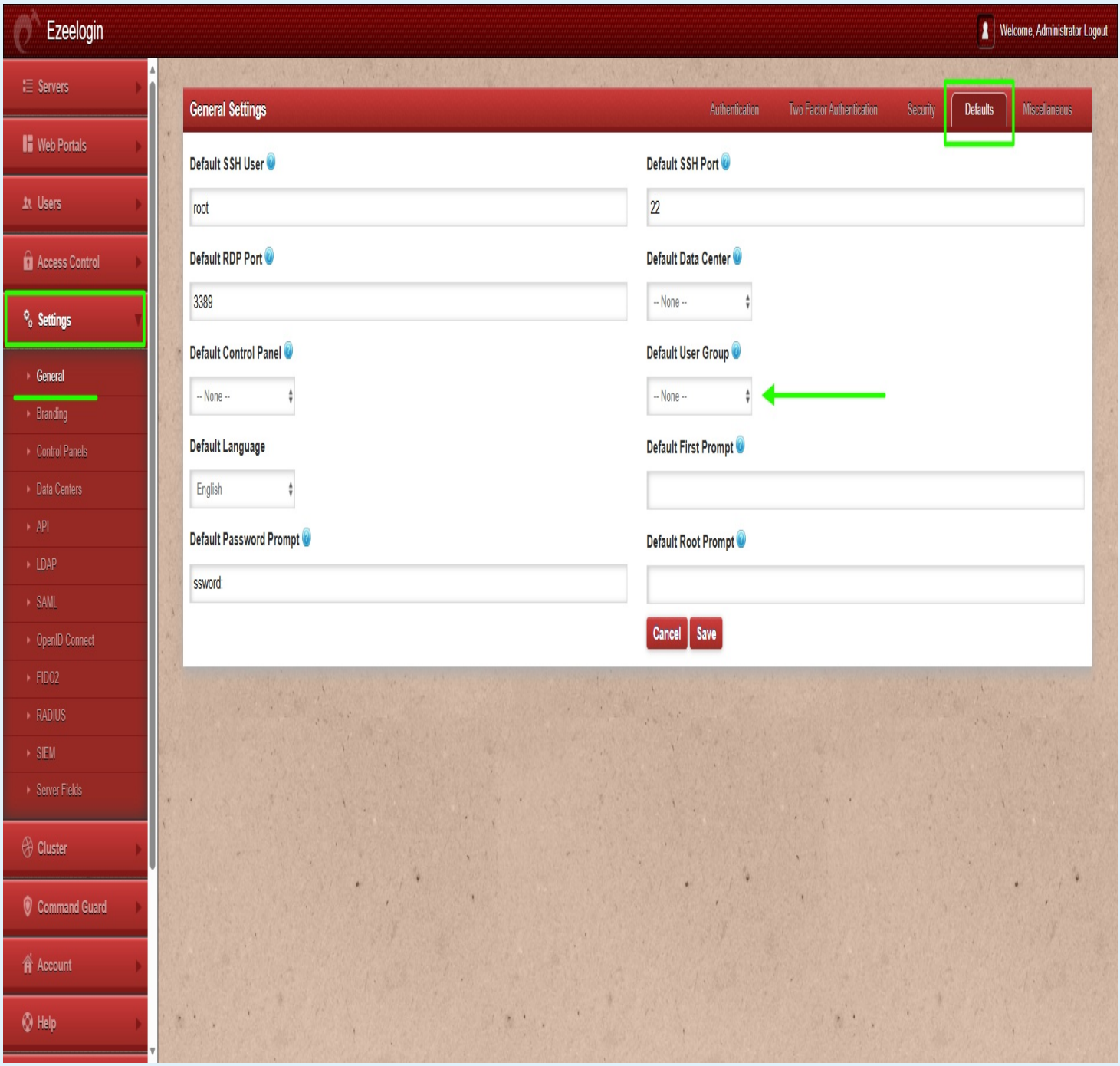
User attributes (such as groups and other mapped fields) are automatically updated in the Ezeelogin GUI when a user authenticates again. **If any attribute of an existing SAML user is changed in the identity provider after the user has already logged in, the change will appear in the GUI only after the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

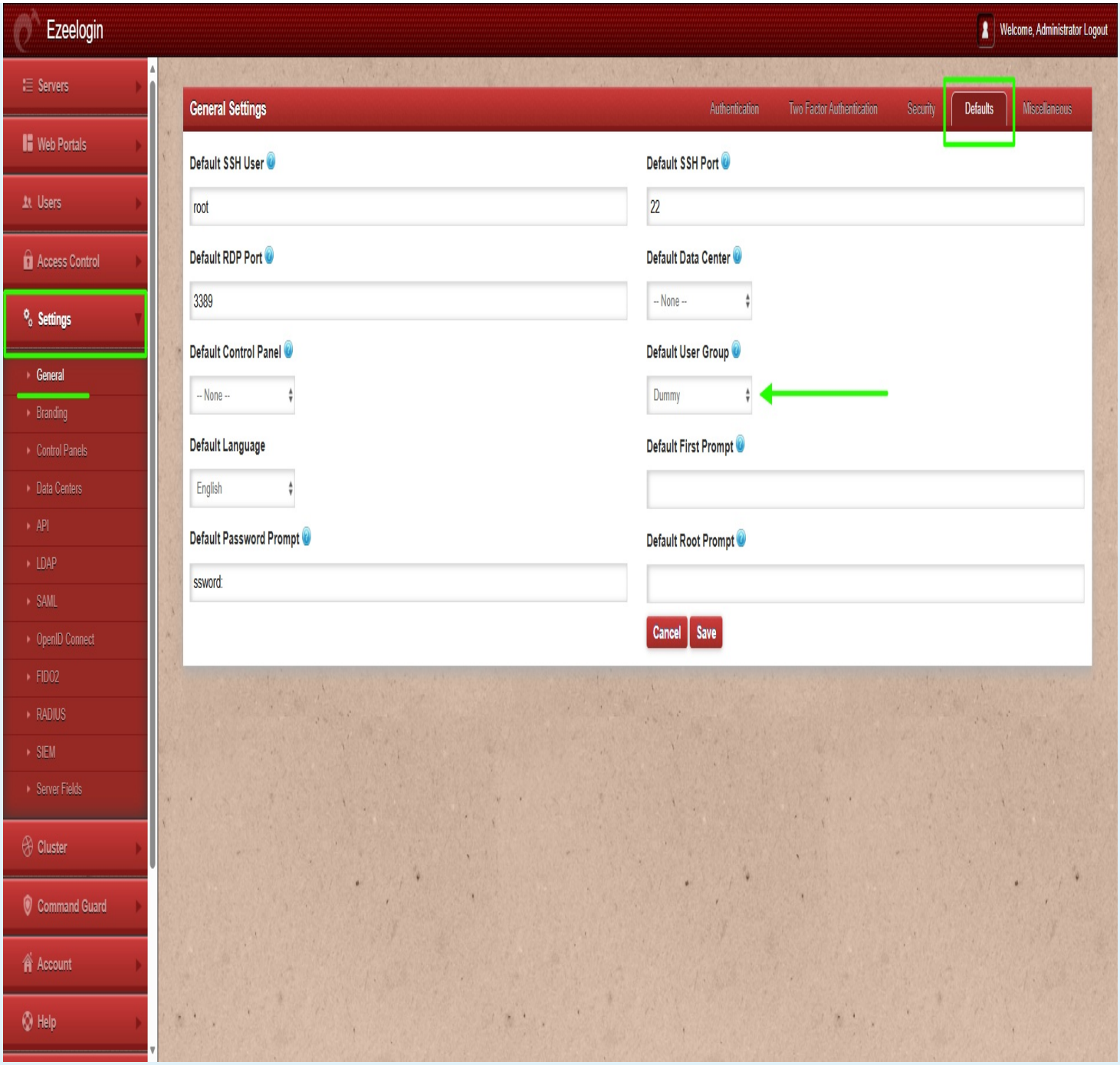
This feature is available from Ezeelogin version 7.46.0. Refer article to upgrade Ezeelogin to the latest version.

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.

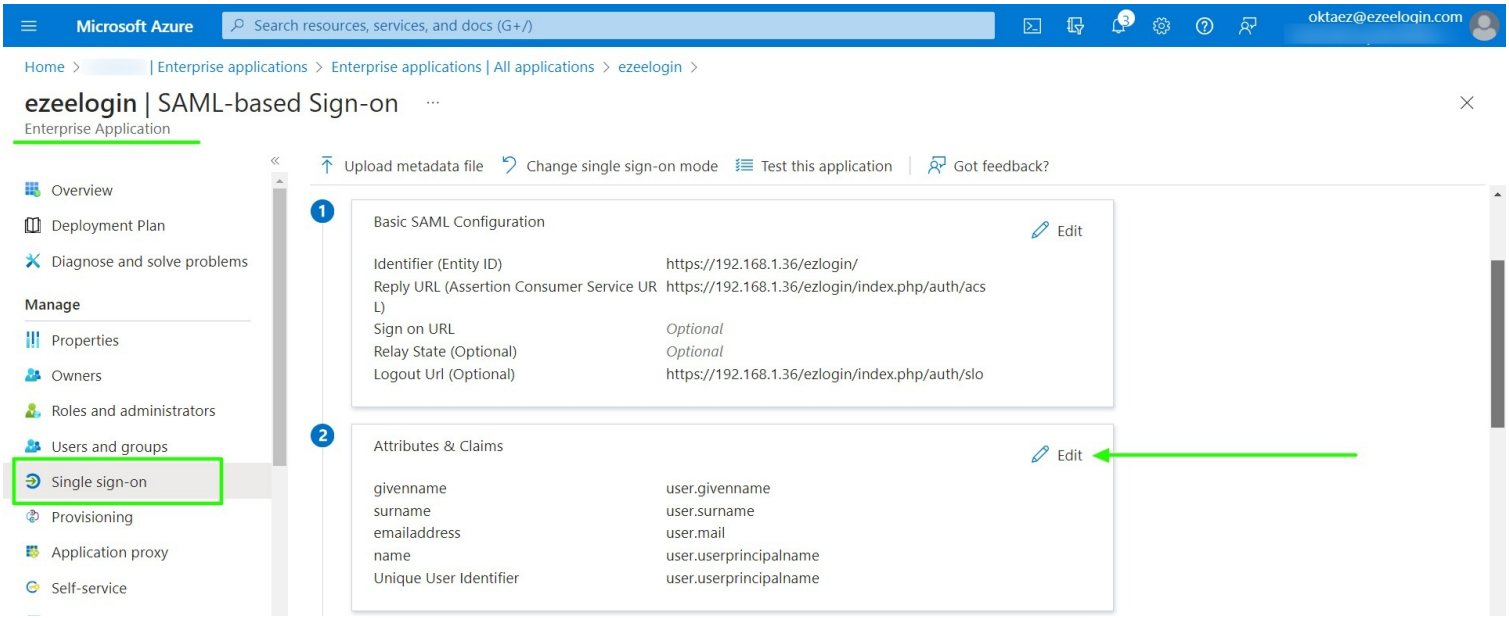


2. If the default user group is set to any group other than None, then all users from the OIDC provider will be auto-created in that same group.

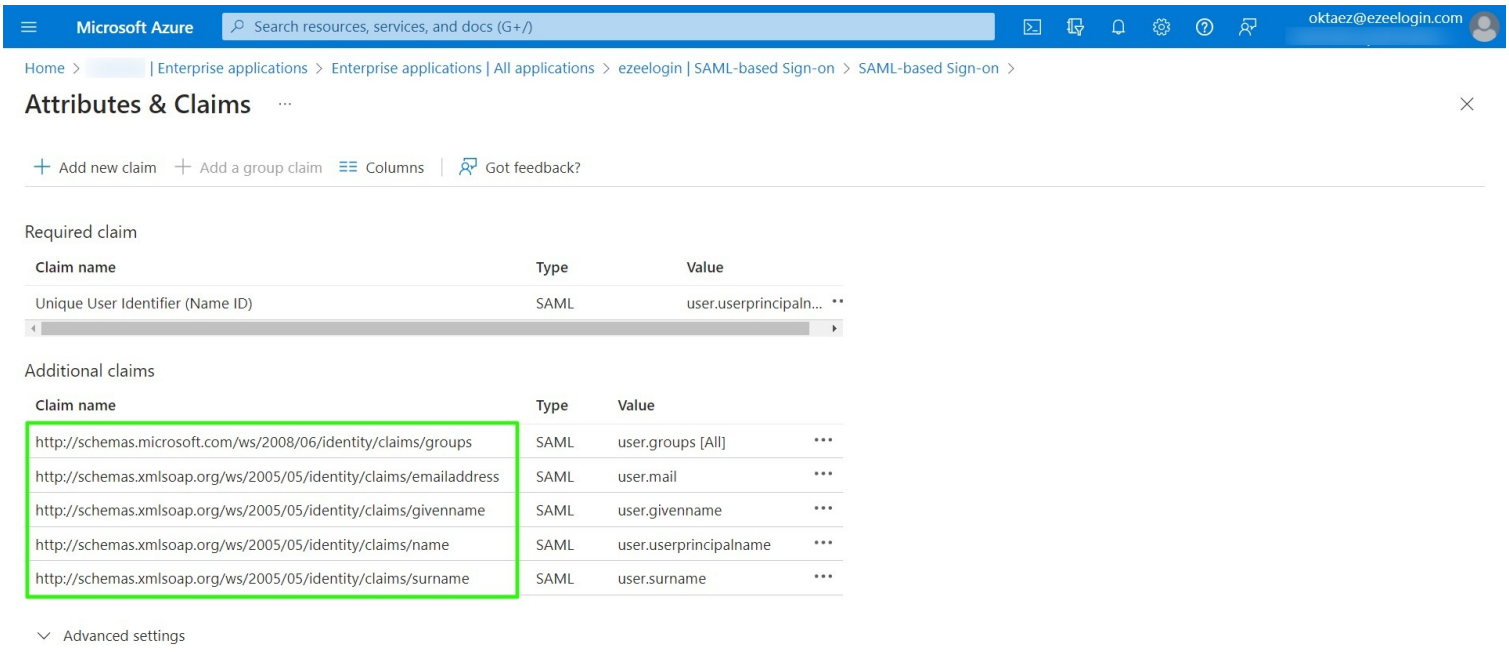


This feature is available from Ezeelogin version 7.46.0. Refer article to upgrade Ezeelogin to the latest version.

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



2. Copy the **Claim names** and paste them into the **SAML setting** of Ezeelogin.



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

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 tomap 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-sso-and-azure-active-directory-326.html