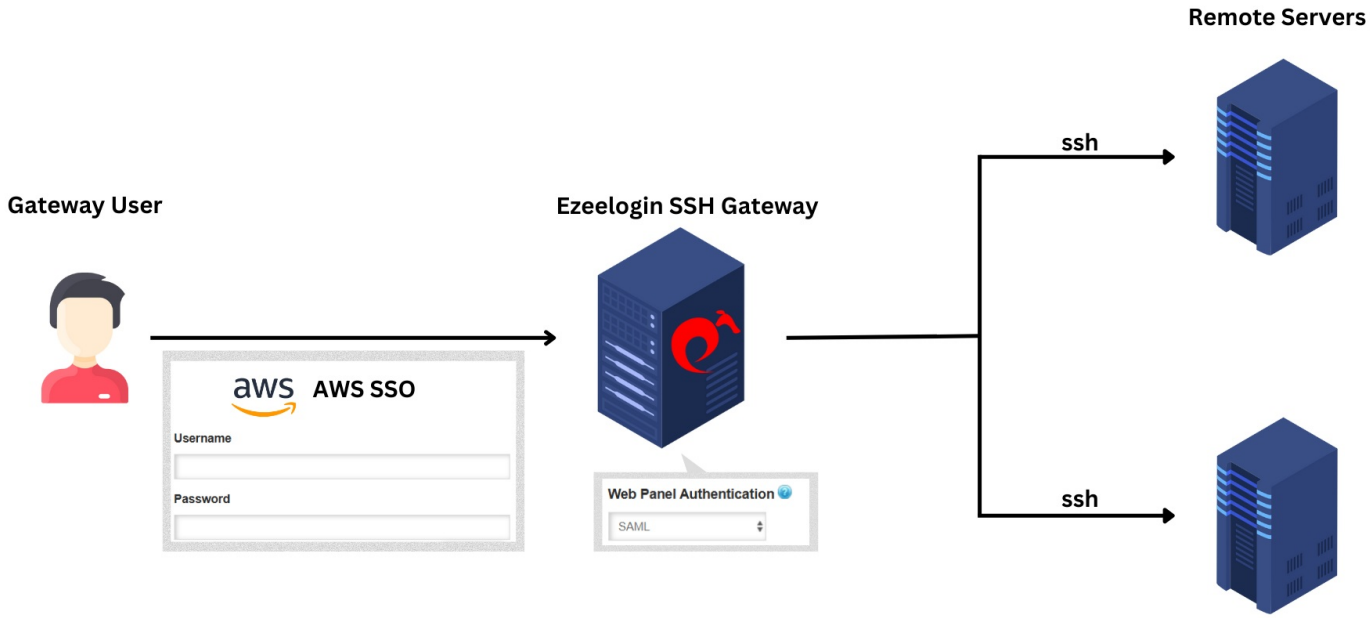
Integrate AWS SSO with Jumpserver

402 Manu Chacko April 28, 2026 Identity & Access Management (IAM), Tweaks & Configuration 10718

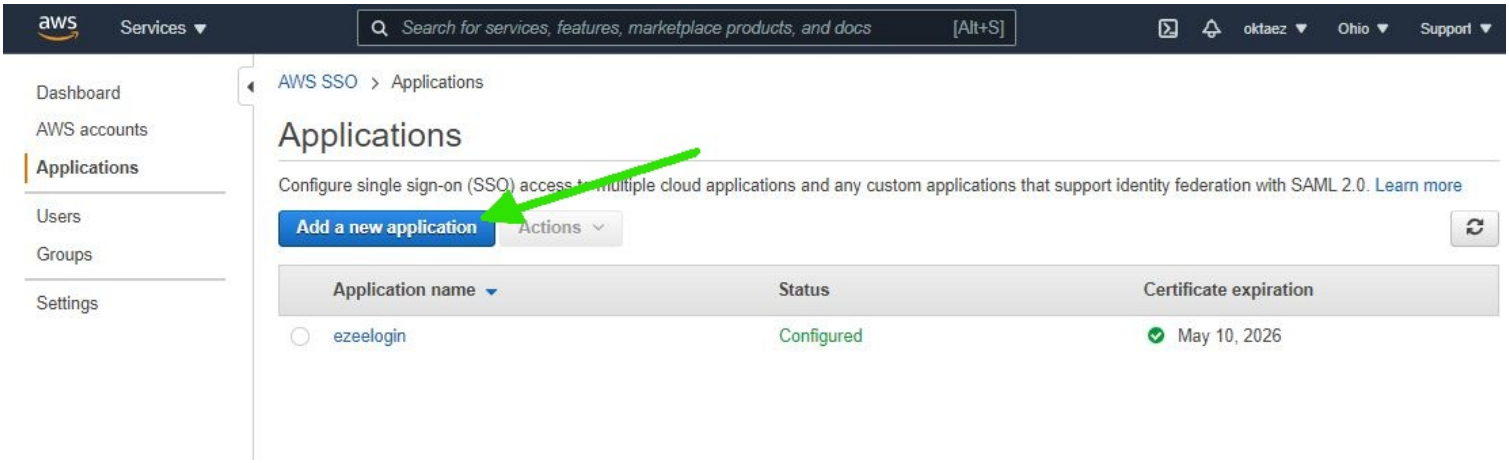
Integrate AWS SSO in Ezeelogin SSH Gateway

Overview: This article provides a comprehensive guide to integrating AWS SSO with Ezeelogin SSH Gateway. It covers the steps to configure a custom SAML 2.0 application in AWS, map user attributes, add and assign users, configure SAML Identity Provider settings in Ezeelogin, and enable SAML authentication. Additionally, it explains how to log into the Ezeelogin GUI and shell using SAML credentials, manage 2FA settings, and emphasizes the convenience of using the web SSH shell for SAML authentication.

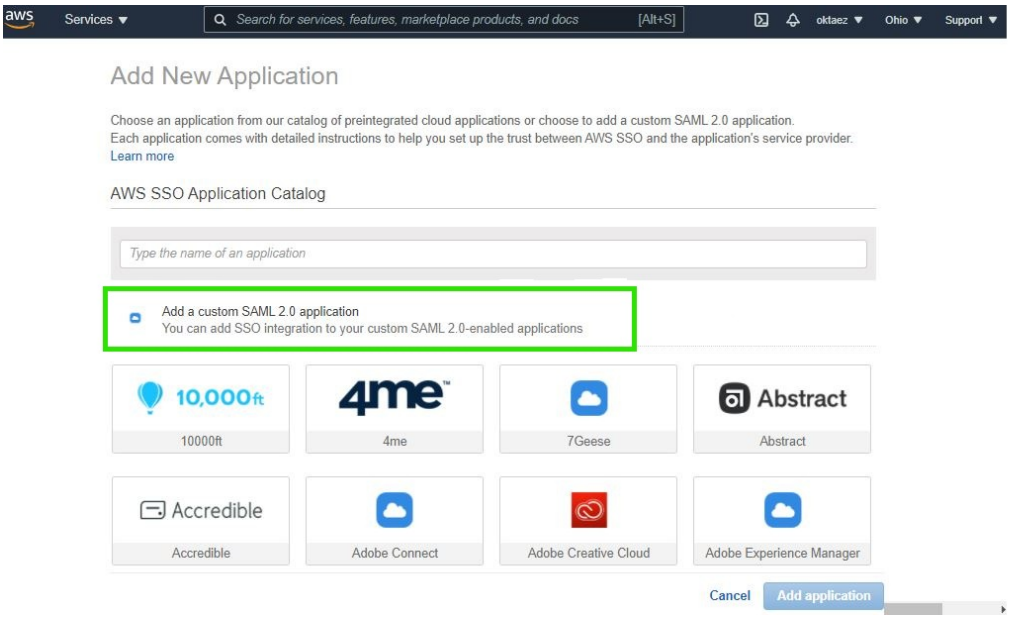


Step 1: Login to AWS console > select AWS Single Sign-On and click on Applications

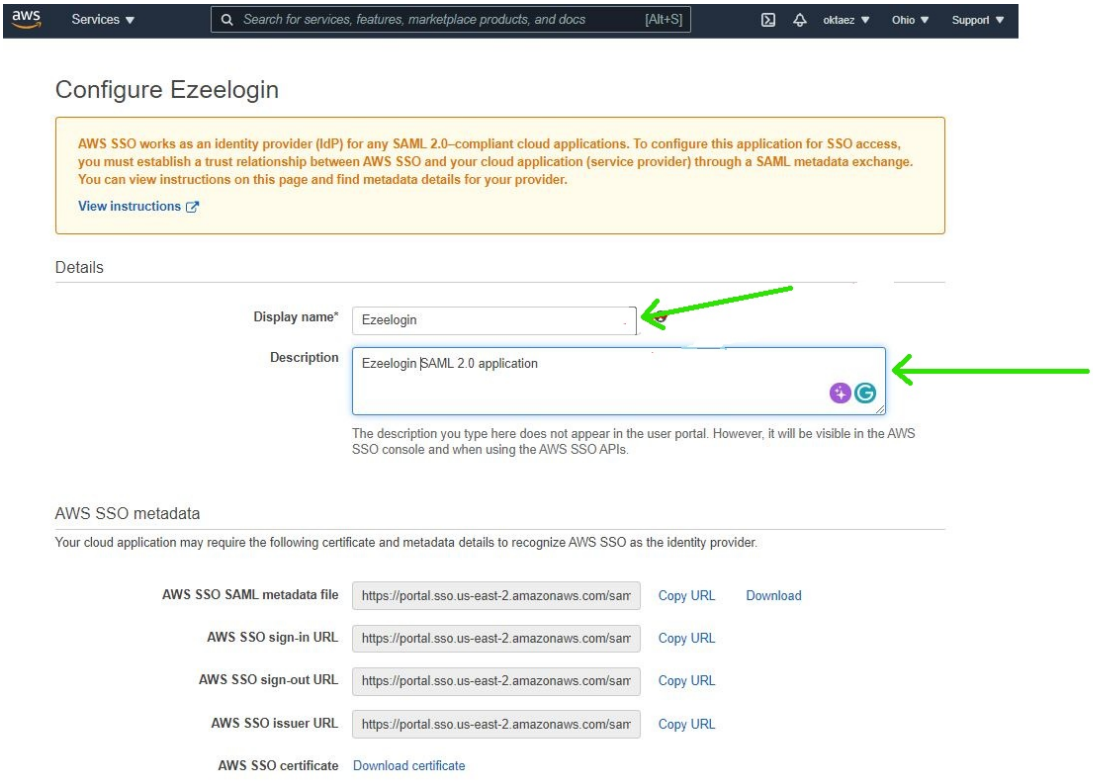
Step 2: Click on Add Application



Step 3. Click on Add a custom SAML 2.0 application

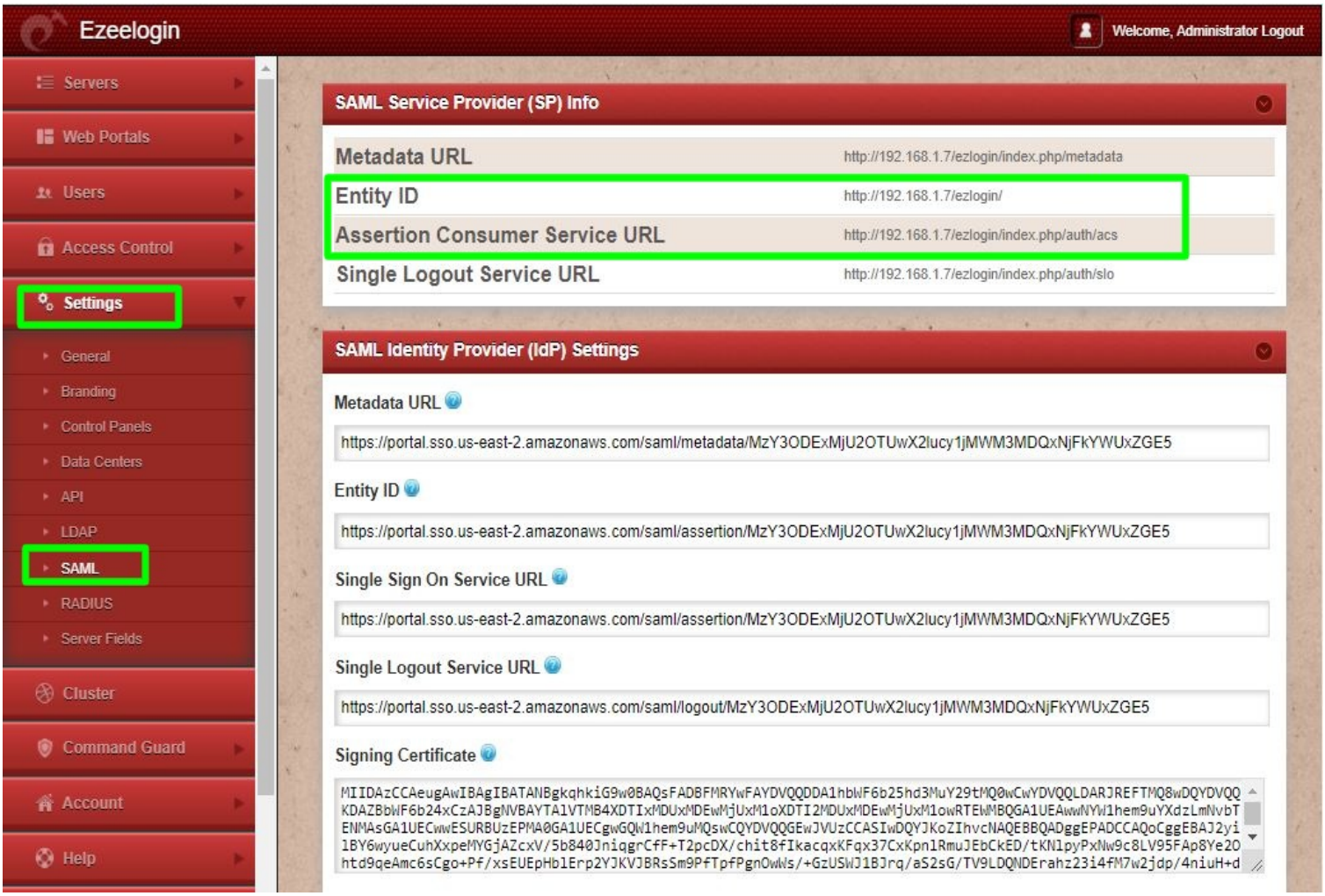


Step 4: Configure Custom SAML 2.0 application. Add **Display name & Description**

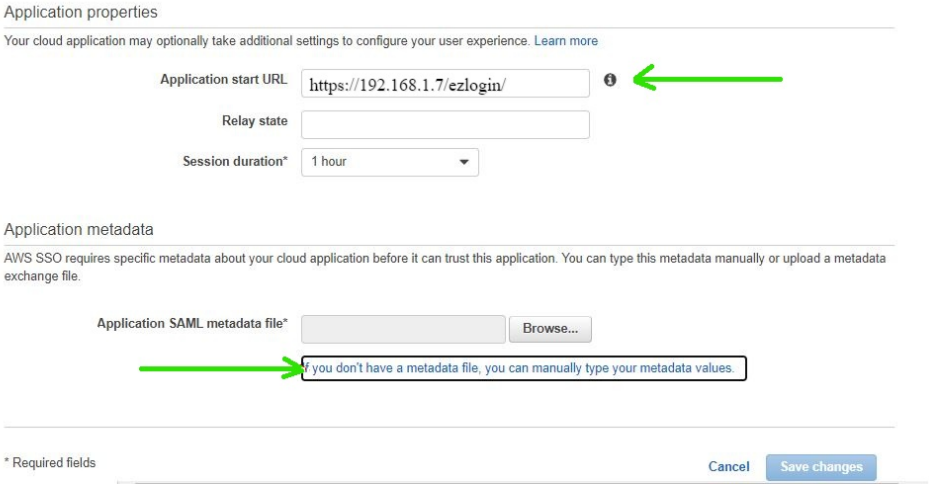


Step 5: Add Application properties & Application metadata

Step 5.a: Fill the **Application start URL .** You can find it from **Ezeelogin GUI > Settings > SAML> Entity ID**



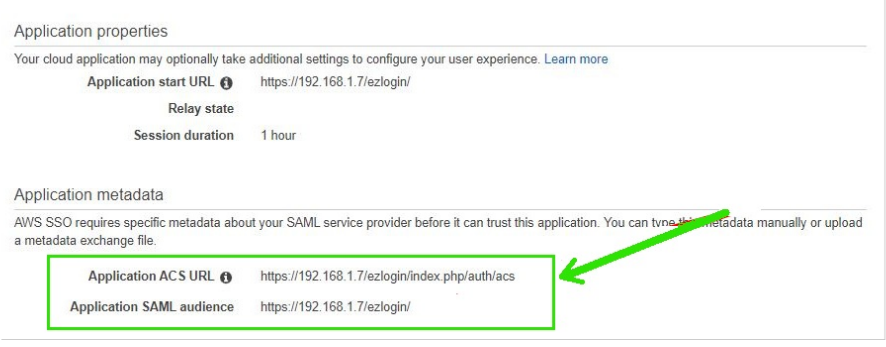
Step 5.b: Fill the **Application start URL &** Click on **If you don't have a metadata file, you can manually type your metadata values.**



Fill the **Application ACS URL & Application SAML audience**

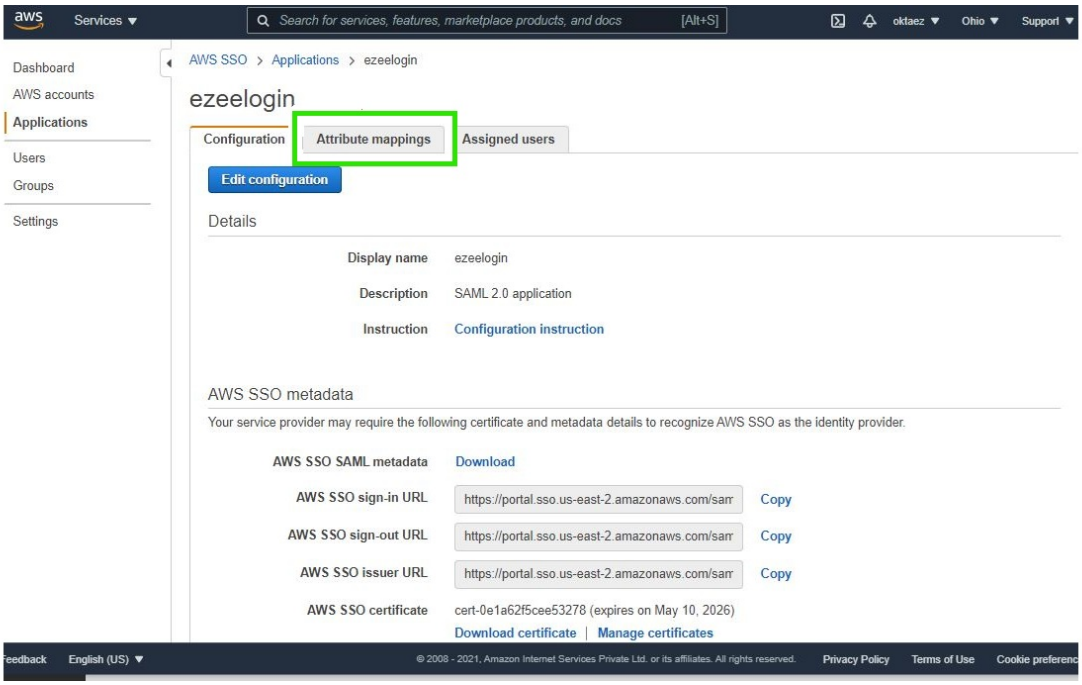
Application ACS URL - Assertion Consumer Service URL (you can find it from Ezeelogin GUI > Settings > SAML> Assertion Consumer Service URL)

Application SAML audience - Entity ID (you can find it from Ezeelogin GUI > Settings > SAML> Entity ID)



Click on save changes.

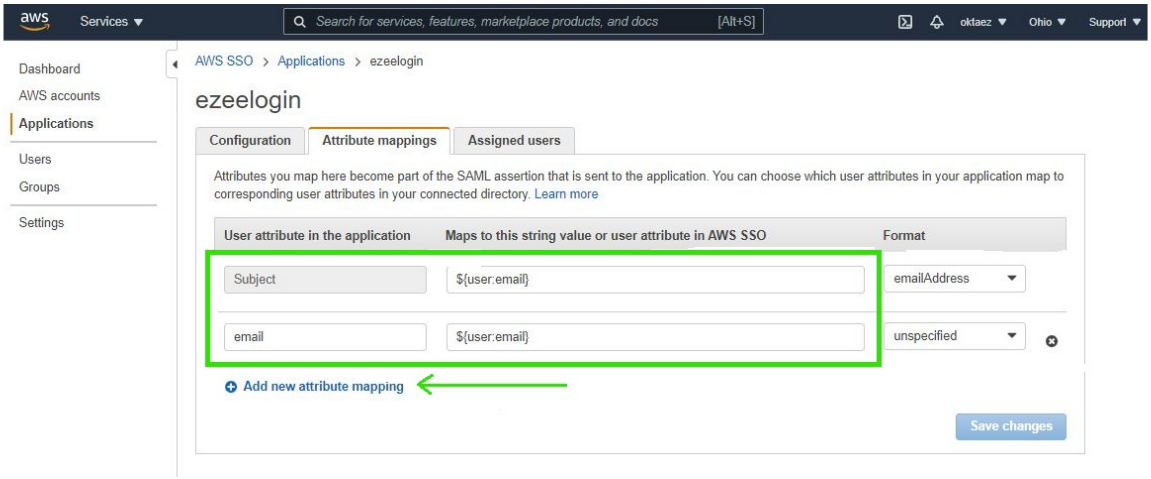
Step 6: Click on Attribute Mappings and Add attributes as follows.



Add attributes

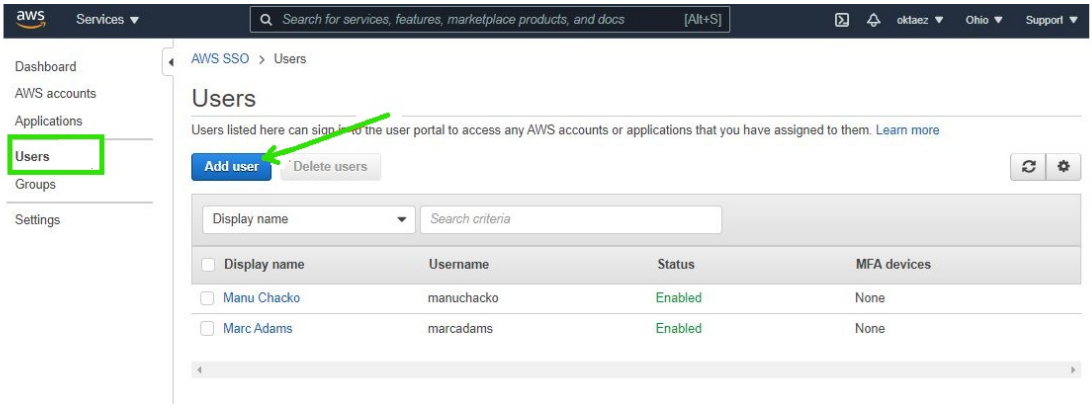
Step 6.a: Add ${user:email} and select **emailAddress** Format

Step 6.b: Click on **Add new attribute mapping** and add **email** to first column, ${user:email} to next column & select **unspecified** Format and **save.**



Step 7: Add and assign users to access our application.

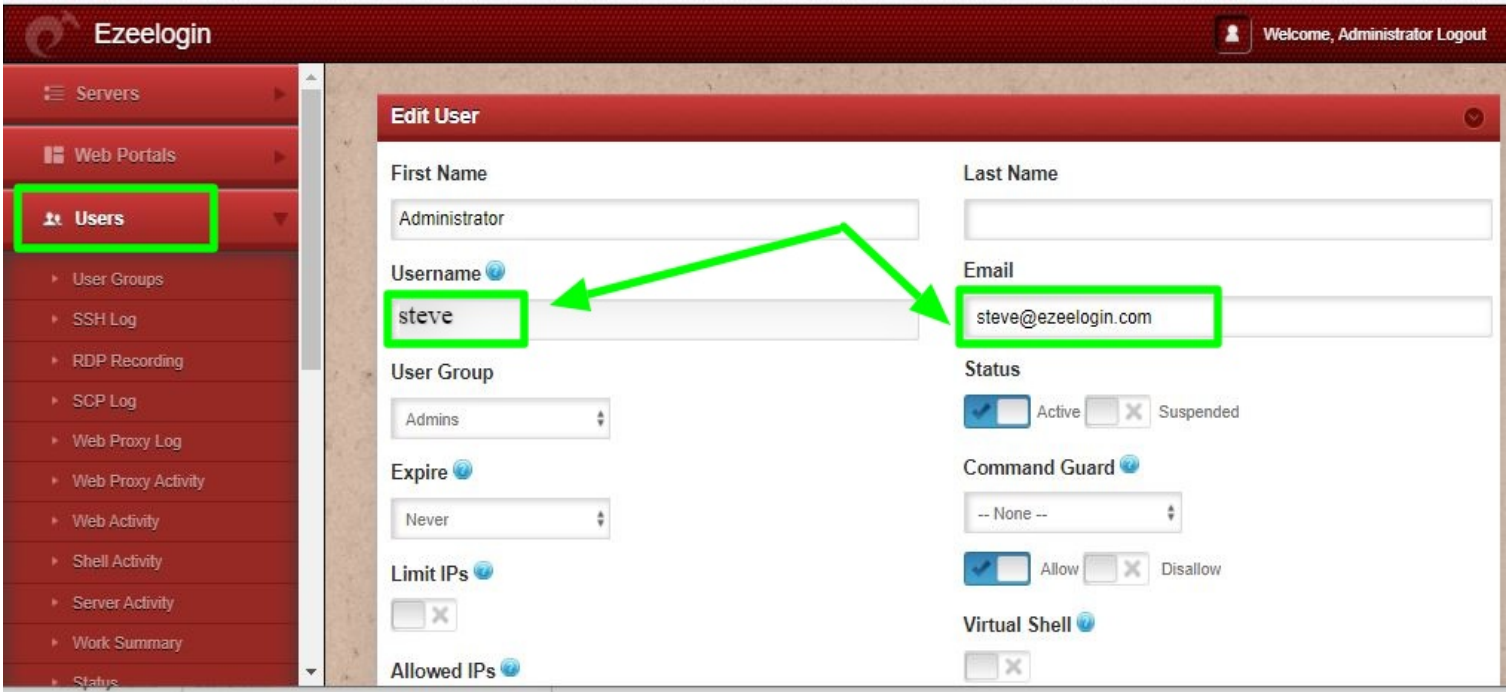
Step 7.a: Add user : Click on **Add user** in **Users** tab in aws sso console

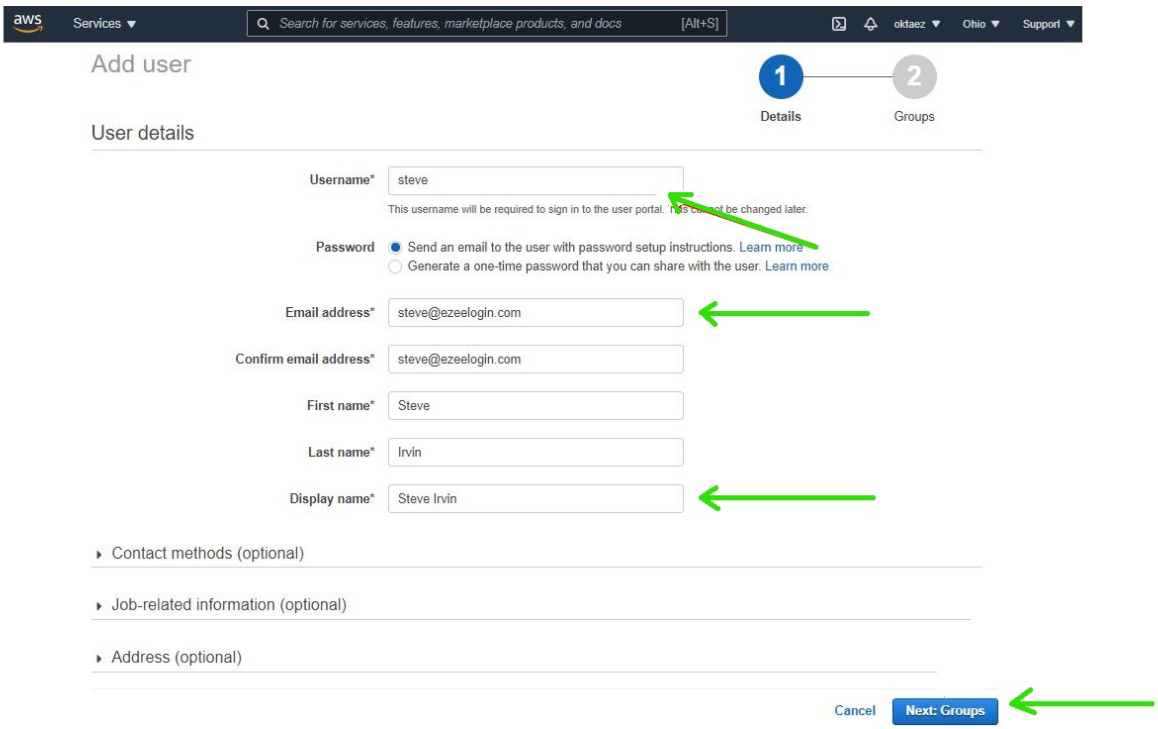


Step 7.b: Add **Username, Password, Email address, First name, Last name & Display name** and Click **Next.** Assign to **a usergroup and Save.**

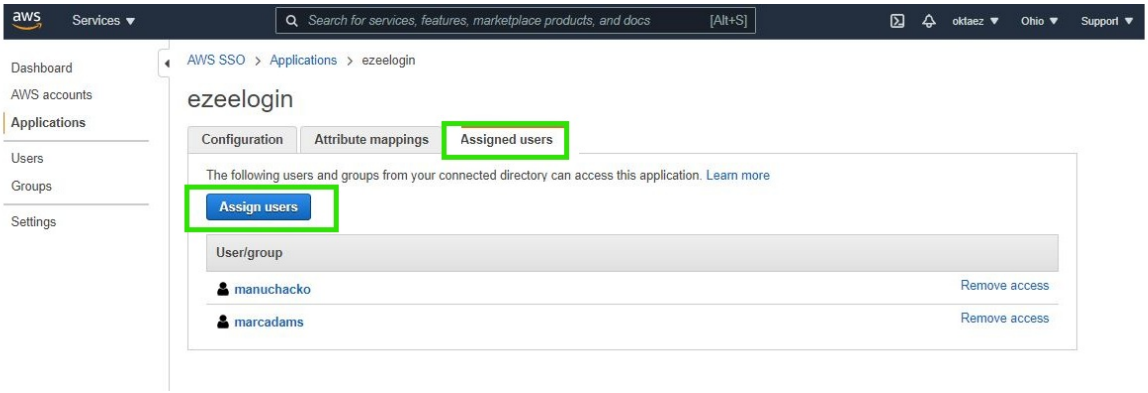
You need to add different email address for each users. By default ezeelogin uses email address for creating

users. You should an email address for superadministrator in ezeelogin(It will be empty by default)
If you want to add an existing user in ezeelogin into SSO, Add the user with exact username, email address as follows. (Ezeelogin will verify with the email address of the users by default)



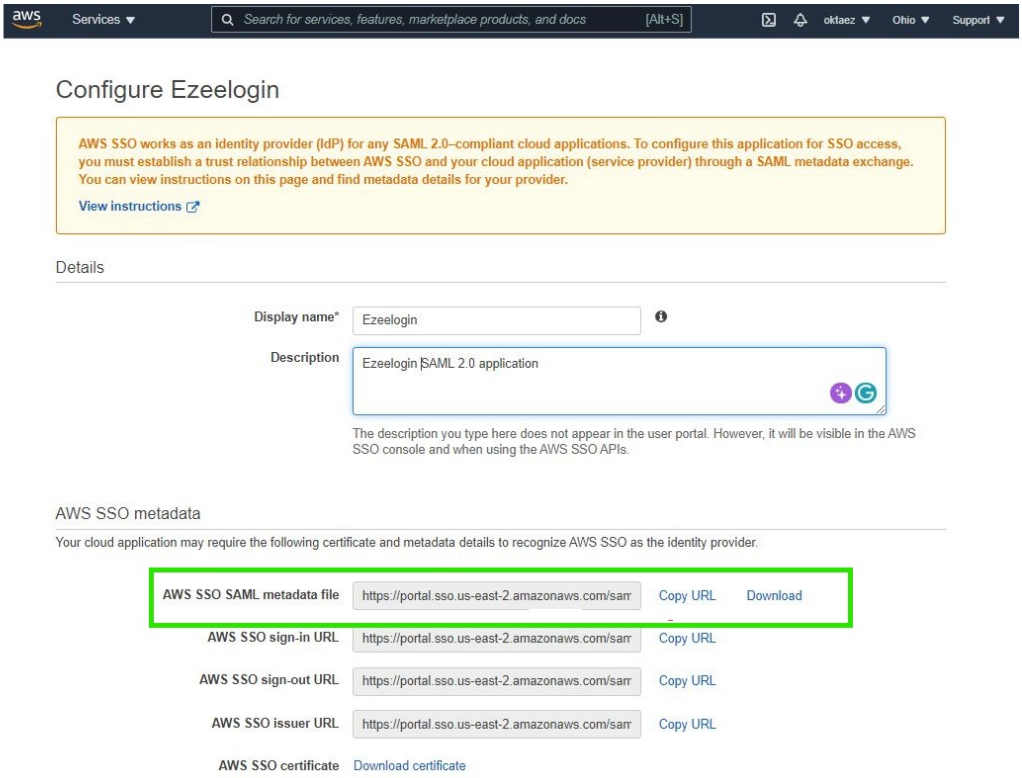


Step 7.c: Click on **Assigned users** tab and click on **Assign users** button to assign users to this application.

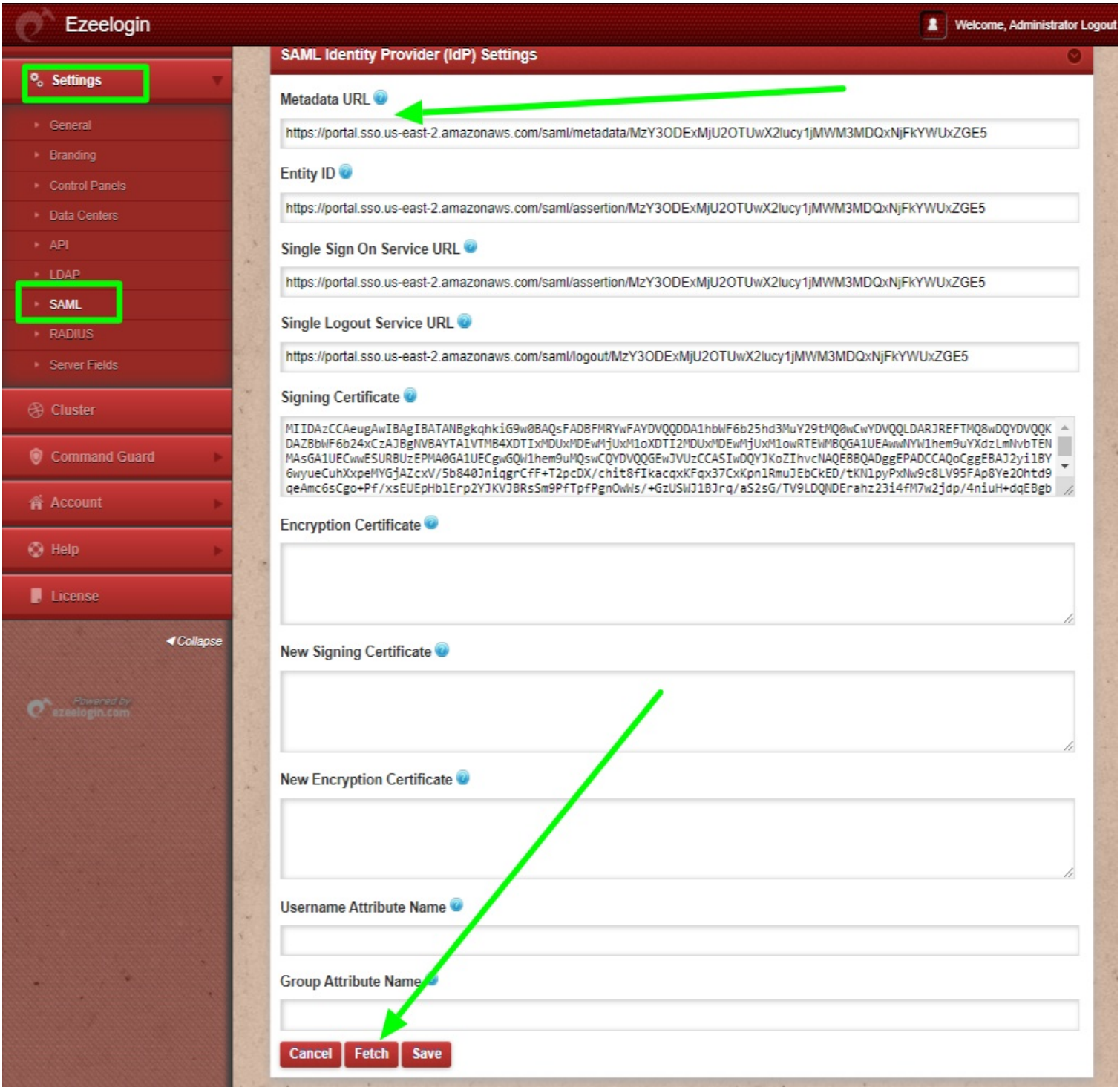


Step 8: Add **SAML Identity Provider (IdP) Settings** on Ezeelogin.

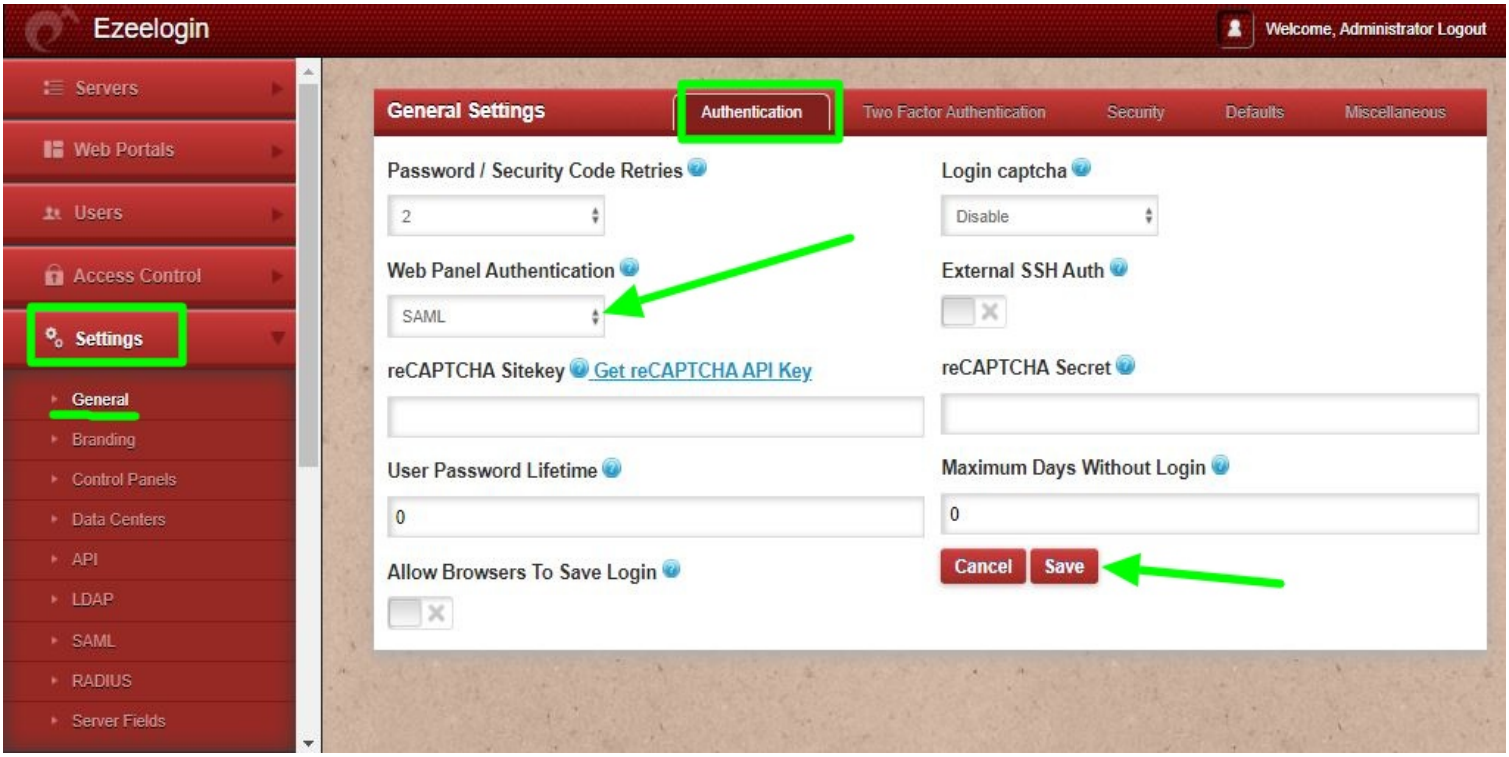
Copy the **AWS SSO SAML metadata url** and paste it to Metadata URL on Ezeelogin GUI > Settings > SAML Metadata URL and click on the fetch button ,It will autofill the SAMLsettings and Save it.



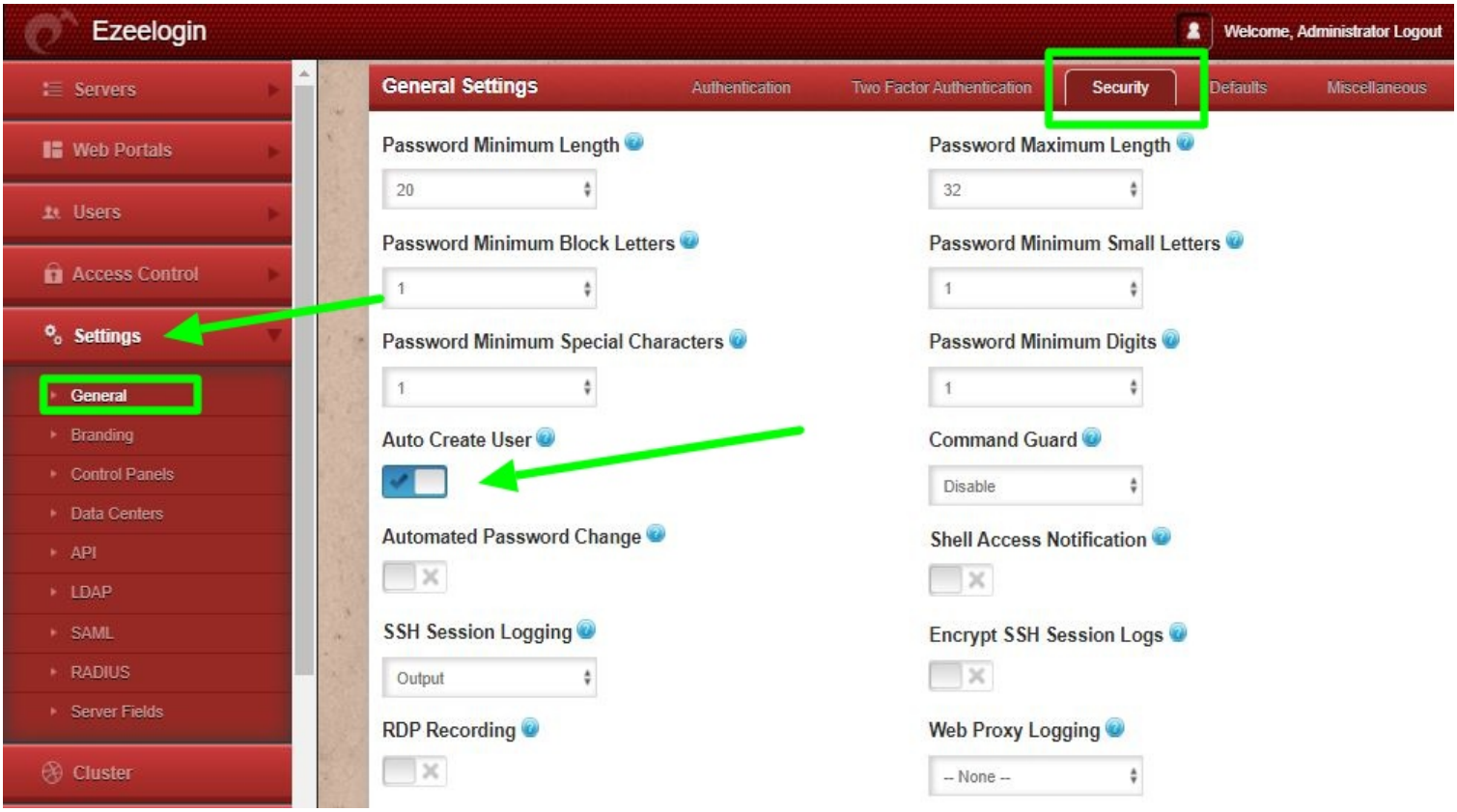
Paste the **Metadata URL** on **Ezeelogin GUI > Settings > SAML Metadata URL** and click on the **Fetch** button & **save** it.



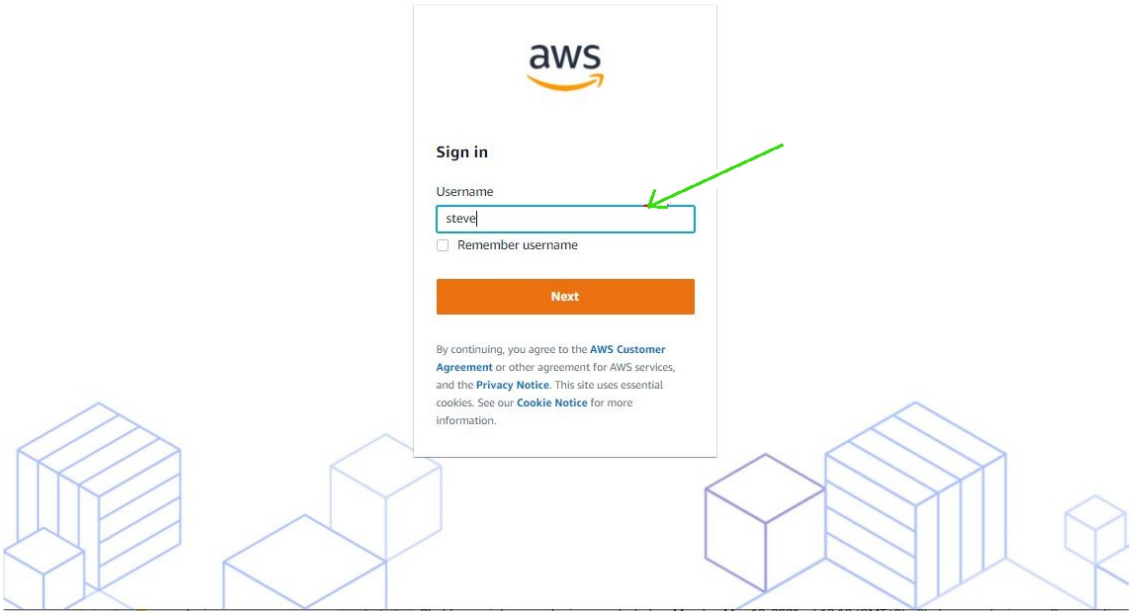
Step 9: Change **Web panel Authentication** to **SAML** from **Ezeelogin GUI > Settings > General > Web Panel Authentication > SAML**



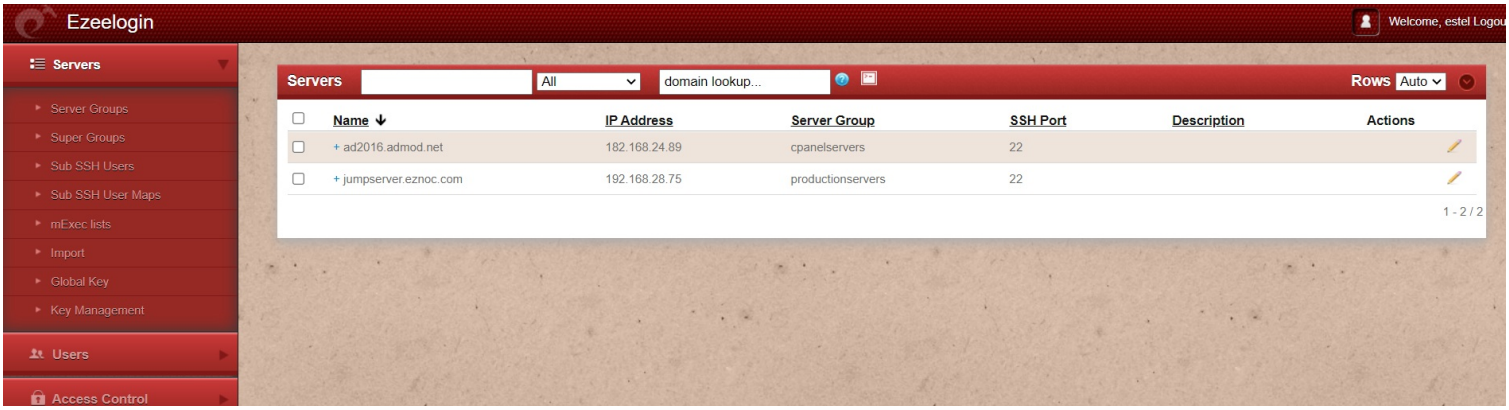
Step 10: Enable **Autocreate user** from **Ezeelogin GUI > Settings > General > Security > Enable Auto create user**



You can now login to ezeelogin GUI with ezeelogin URL and it will redirect to aws sso page. You must log in with aws sso credentails and it will redirect and log in to ezeelogin gui after successful authentication.



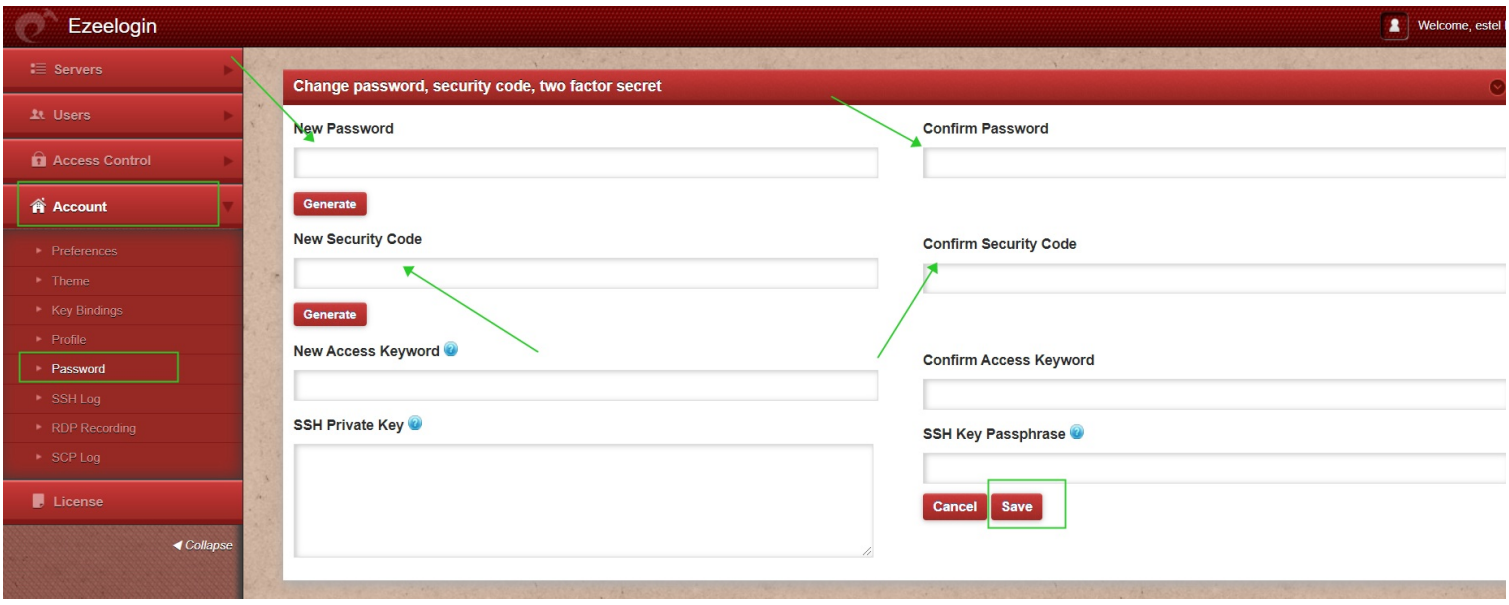
Step 11: Finally, logged into the Ezeelogin GUI using SAML Authentication.



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

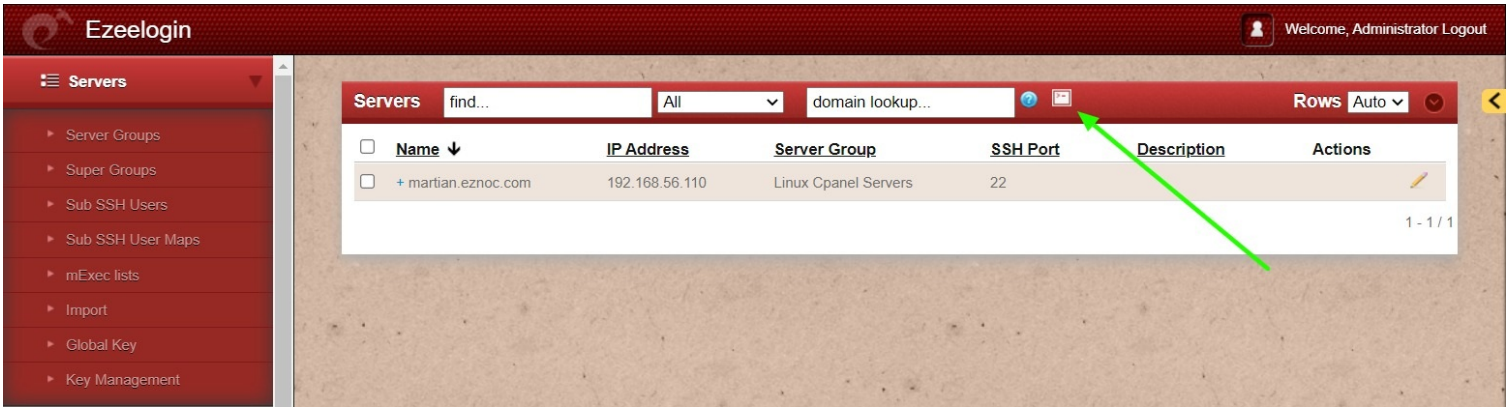
Error: Invalid password

Step 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

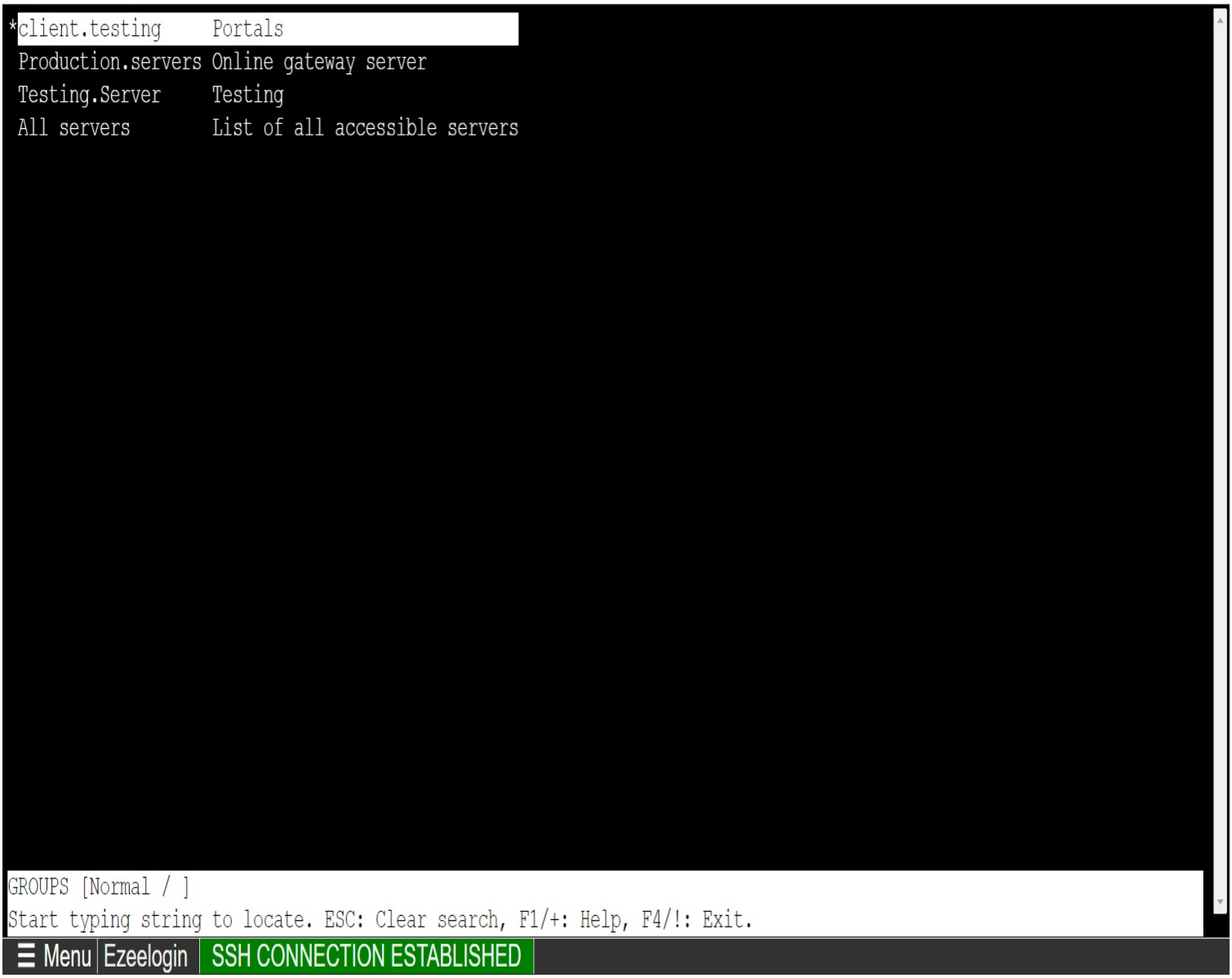


Step 13: You can log in to **Ezeelogin shell** via **Webssh** shell or using any **SSH client** such as Putty or terminal etc.

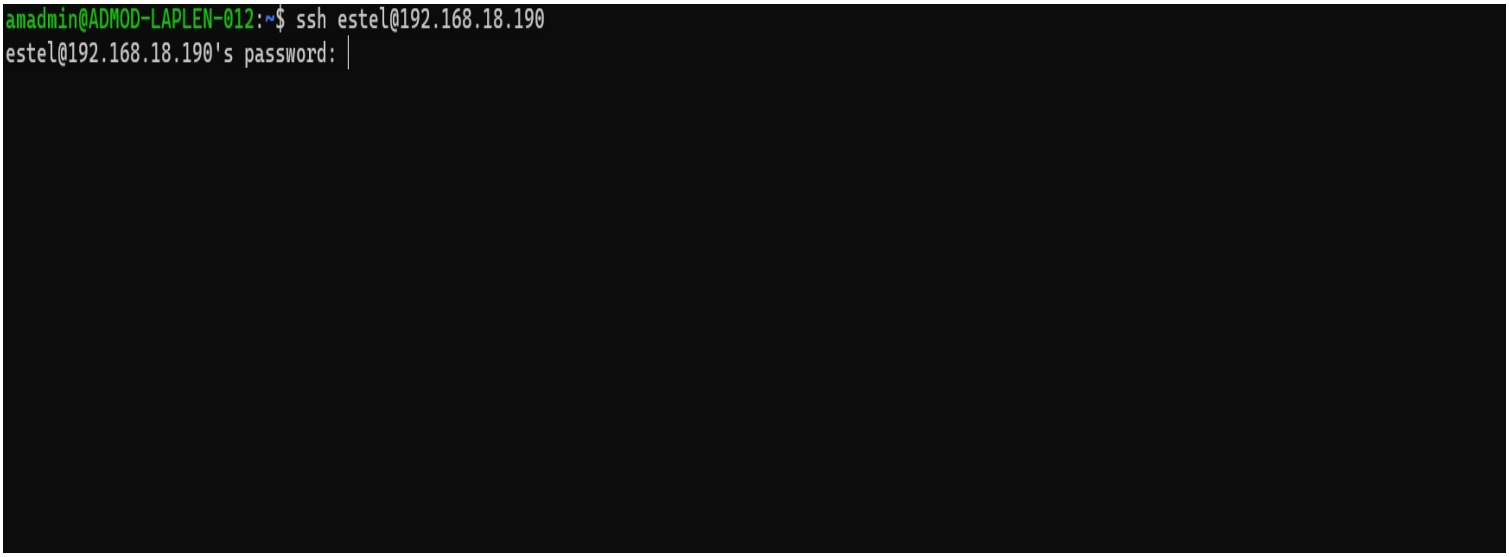
WebSSH: Click on the '**Open Web SSH Console**' icon to SSH via the browser



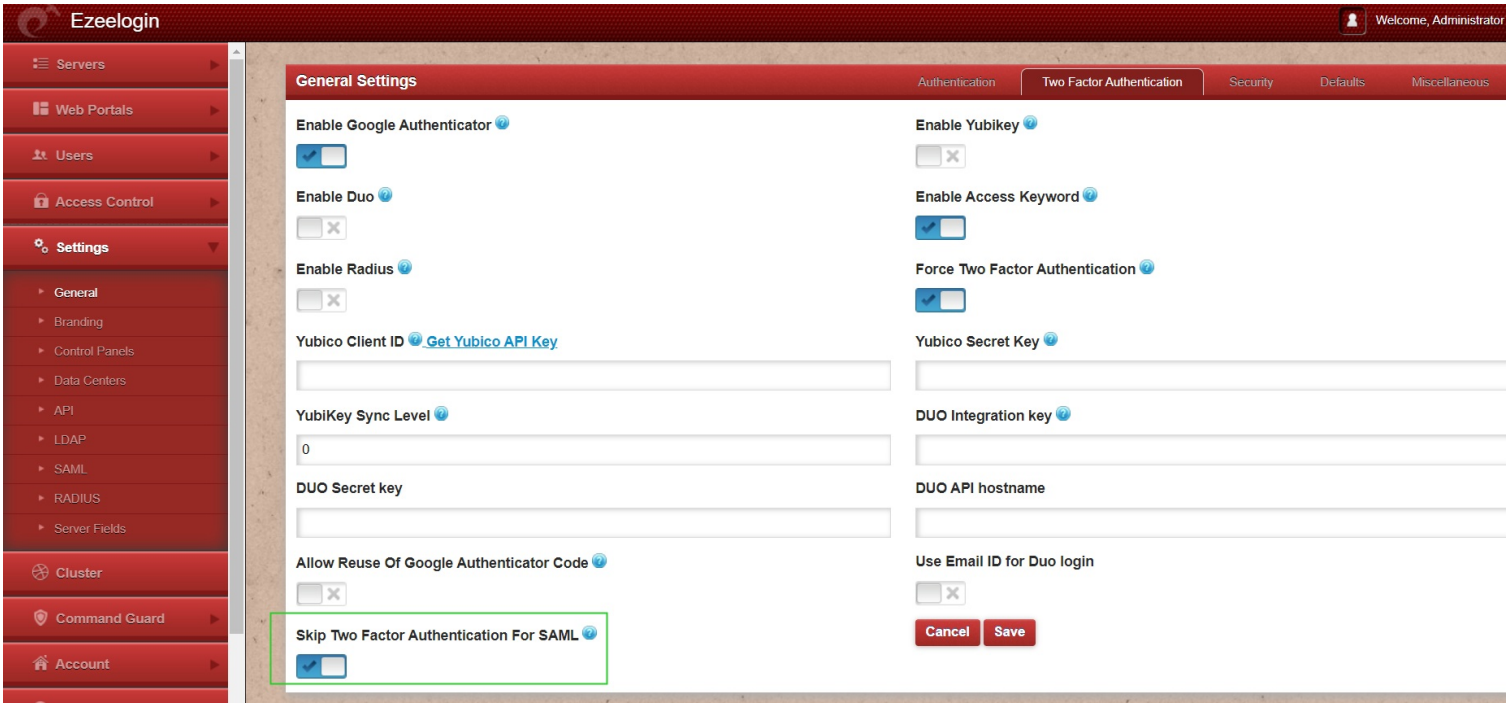
WebSSH terminal will open like below. **Users can navigate the server group with the Up and Down arrow buttons and enter to login into the server**.



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**.



Step 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 webpanel , otherwise if the user is not logged into the webpanel it would prompt for the 2FA codes.



Step 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 webpanel itself and 2fa will not be prompted if you have enabled the Skip Two factor Authentication for SAML.

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

Related Articles:

Login as superadmin when SSO is enabled globally

Integrate OneLogin SSO with jumpserver

Integrate Jumpcloud SSO with Ezeelogin

Integrate GSuite SSO with Jumpserver

Integrate Okta SSO with jumpserver

Disable SAML /SSO Authentication on ezeelogin

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

Map existing user group from SAML provider to ezeelogin.