Integrate GSuite SSO with Jumpserver

513 Nesvin KN April 28, 2026 Features & Functionalities 6715

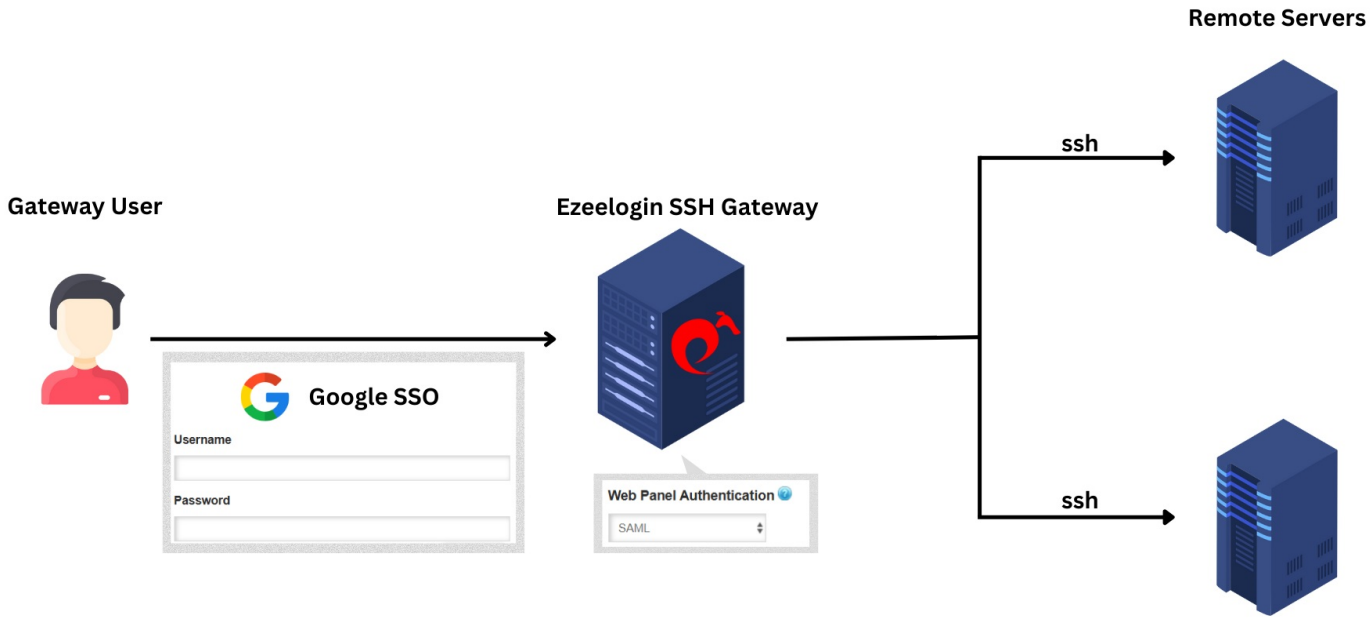
Integrate GSuite with Ezeelogin SSH Gateway

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

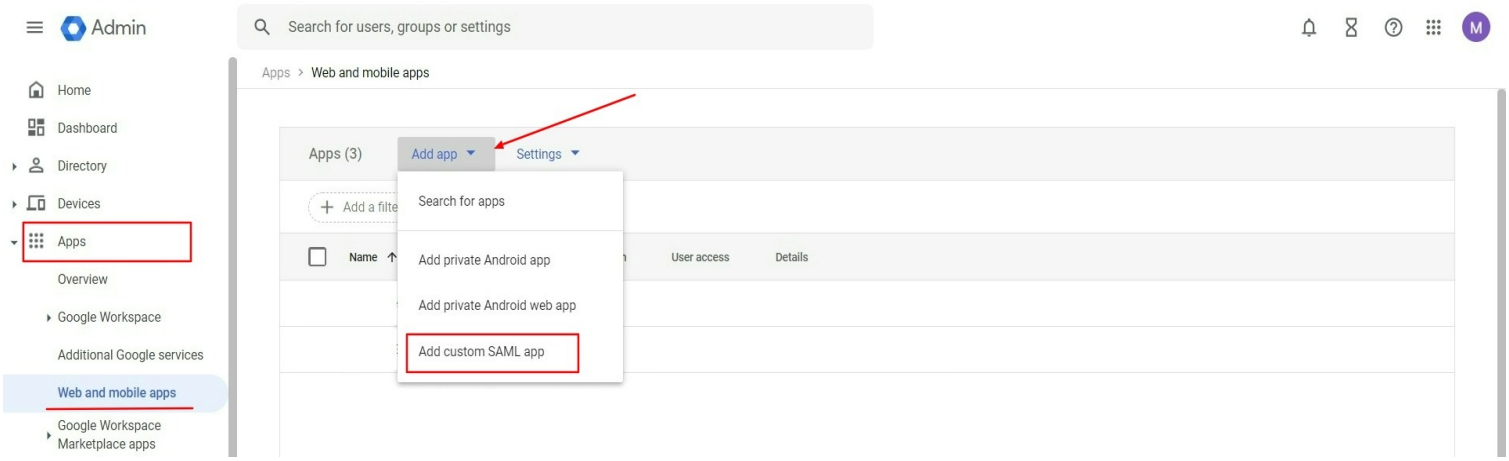
Note:

SAML is an authentication mechanism for web applications.

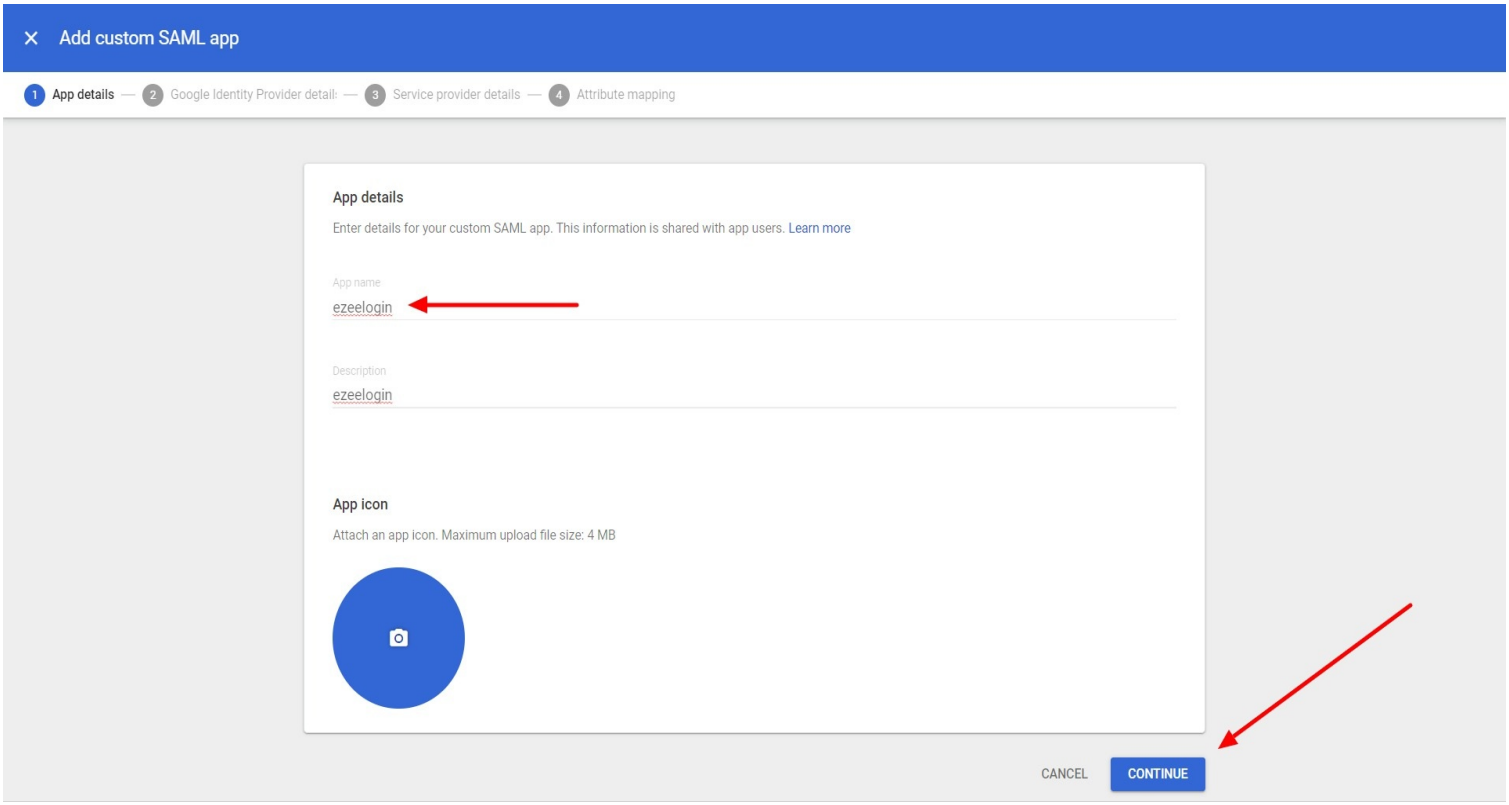
It's based on web protocols and it cannot be used for user authentication over SSH.



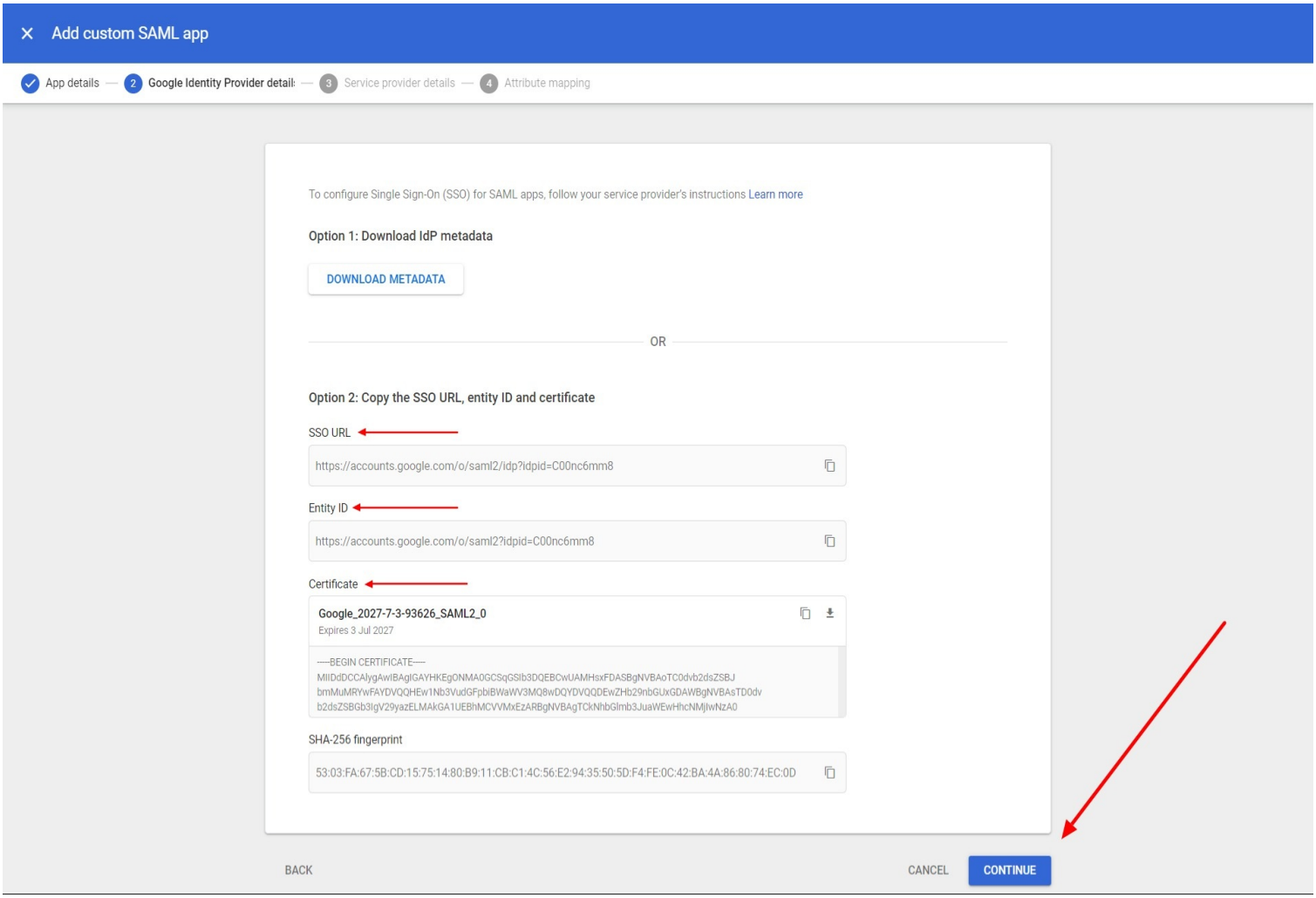
Step 1: Log in to the **Google Workspace Admin console** and add the application.



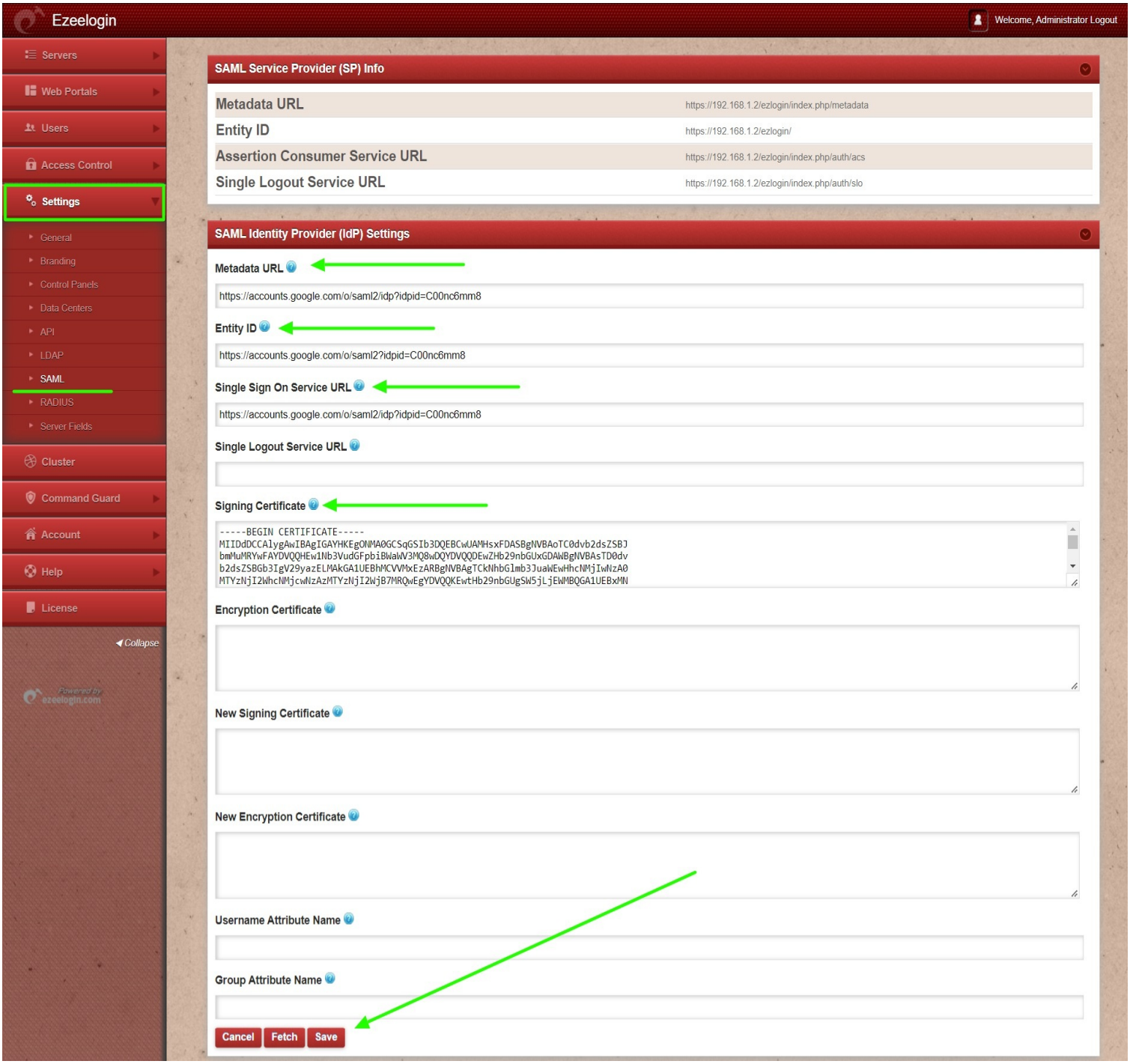
Step 2: Add the application name and click on the continue button.



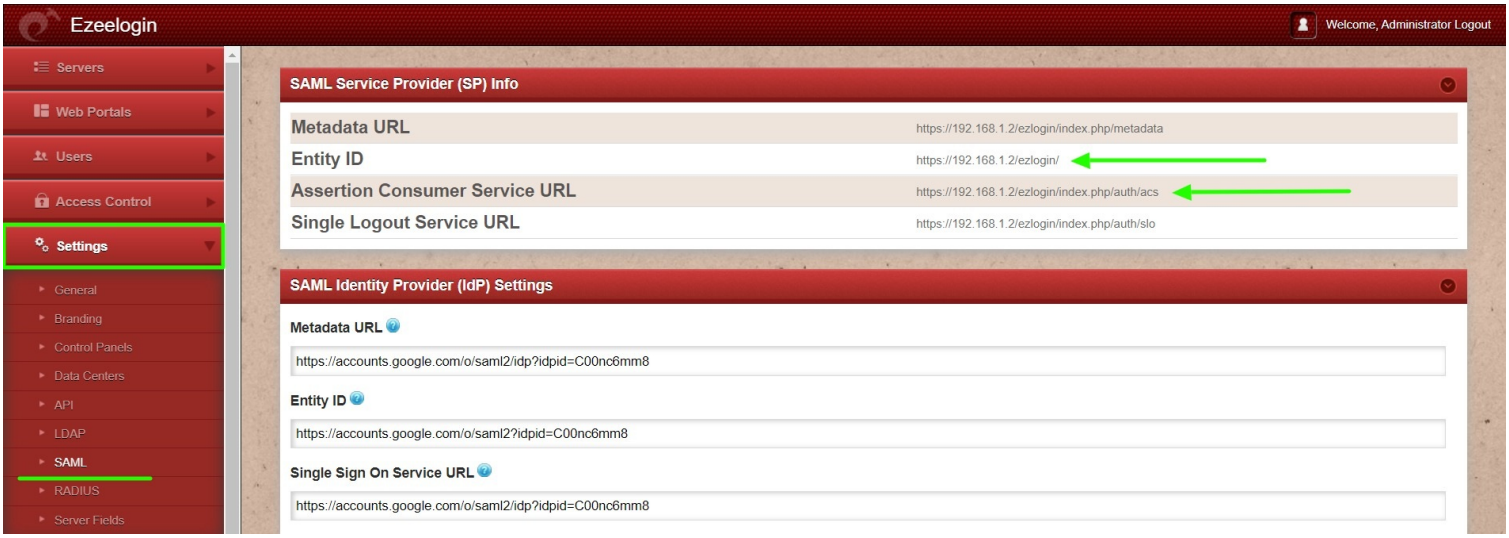
Step 3: Copy **SSO URL, Entity ID**, **Certificate** and paste them into Ezeelogin GUI and save the SAML settings.



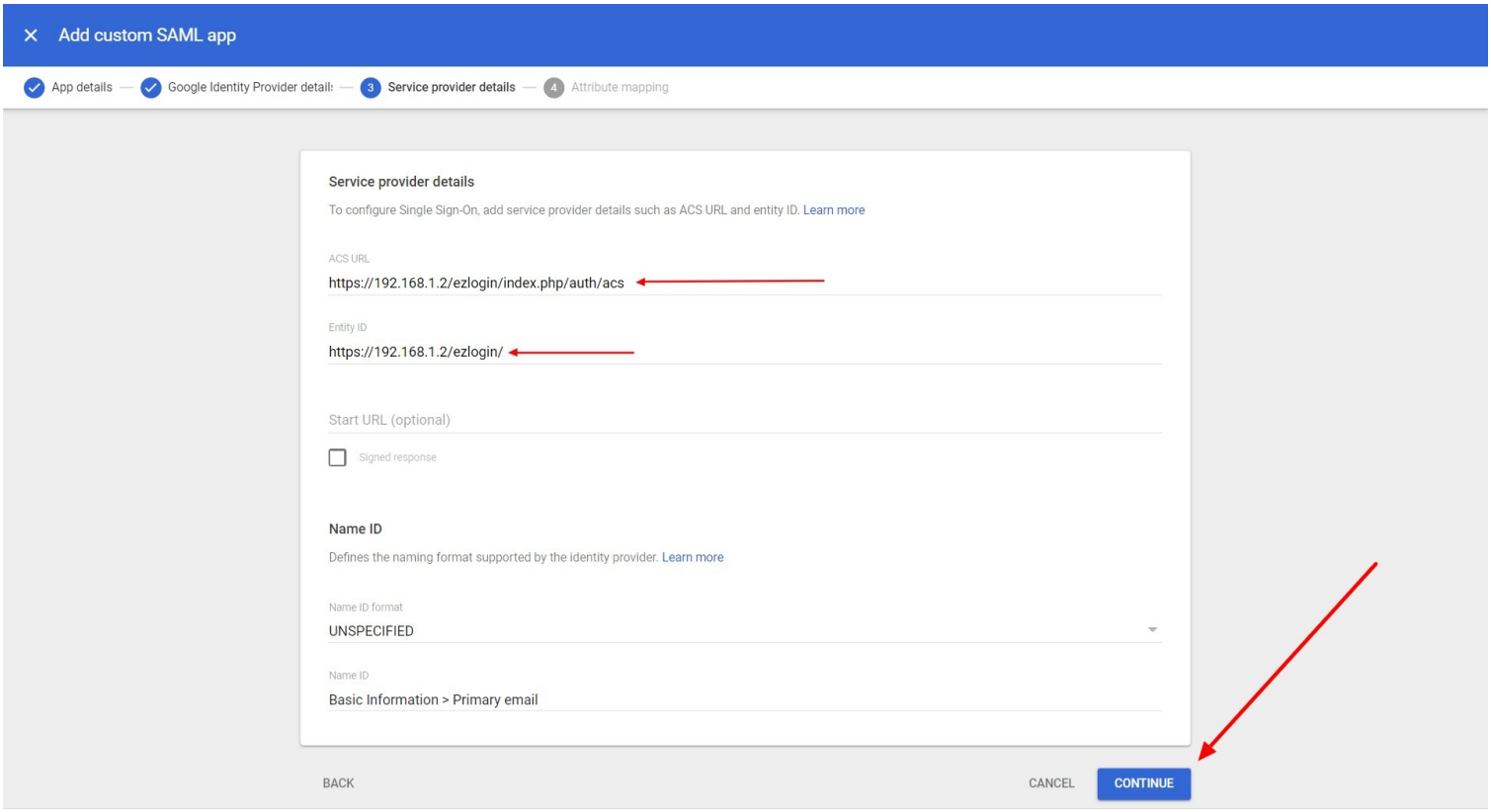
Metadata URL -> SSO URL
Entity ID -> Entity ID
Single Sign On Service URL -> SSO URL
Signing Certificate -> Certificate



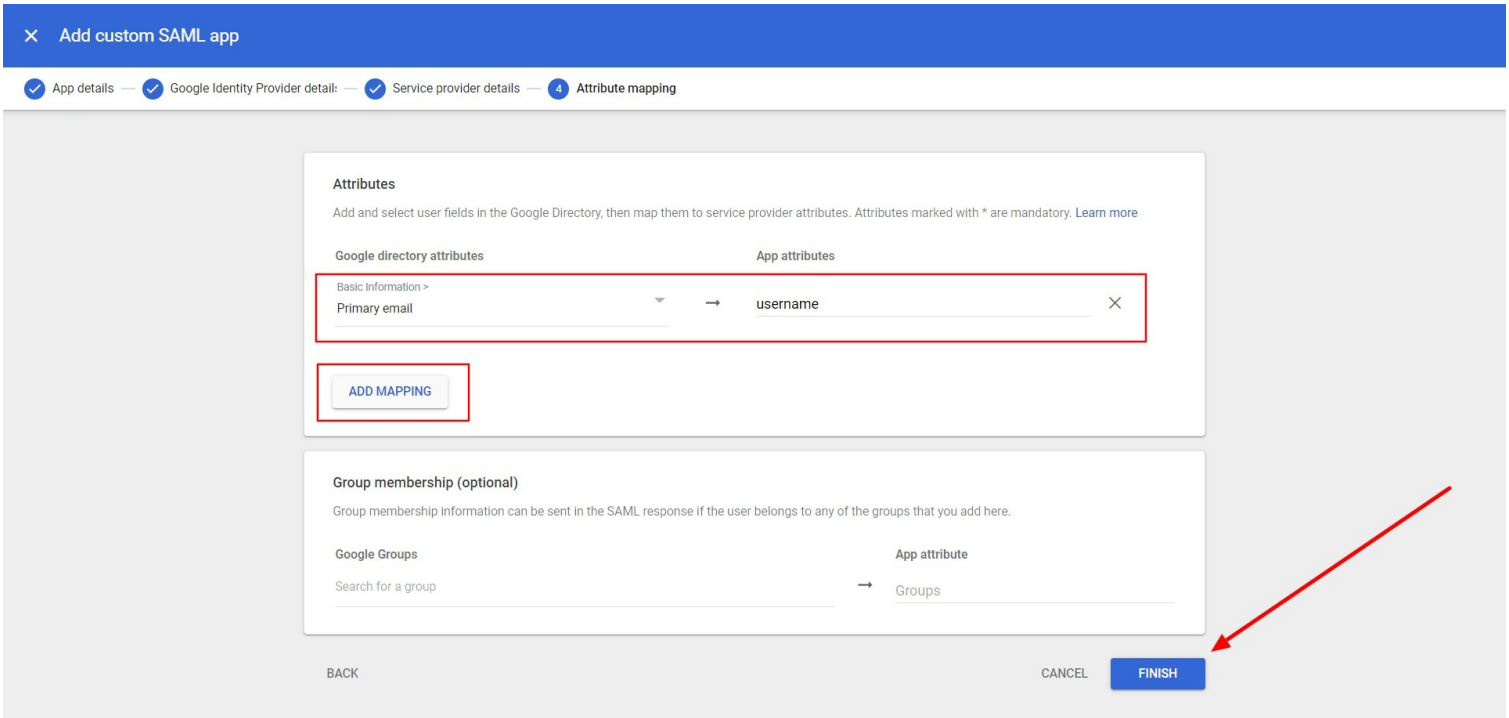
Step 4: Copy **ACS URL** and **Entity ID** from Ezeelogin GUI and paste them into **google console service provider details**.



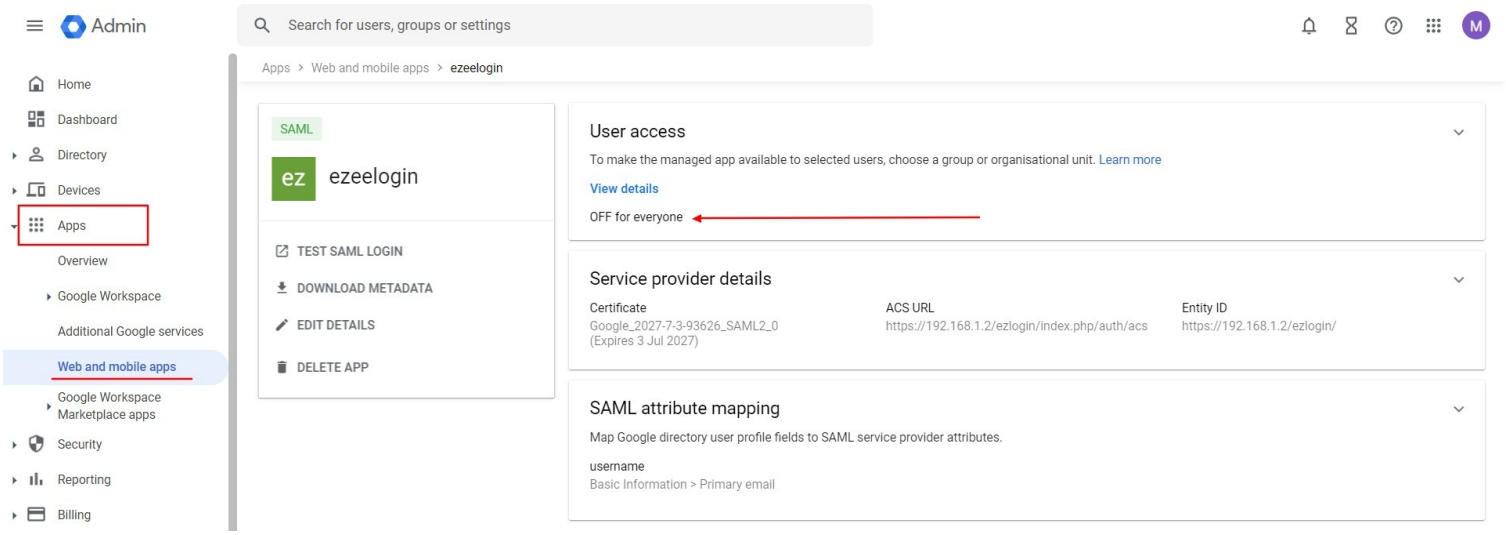
ACS URl -> Assertion Consumer Service URL
Entity ID -> Entity ID

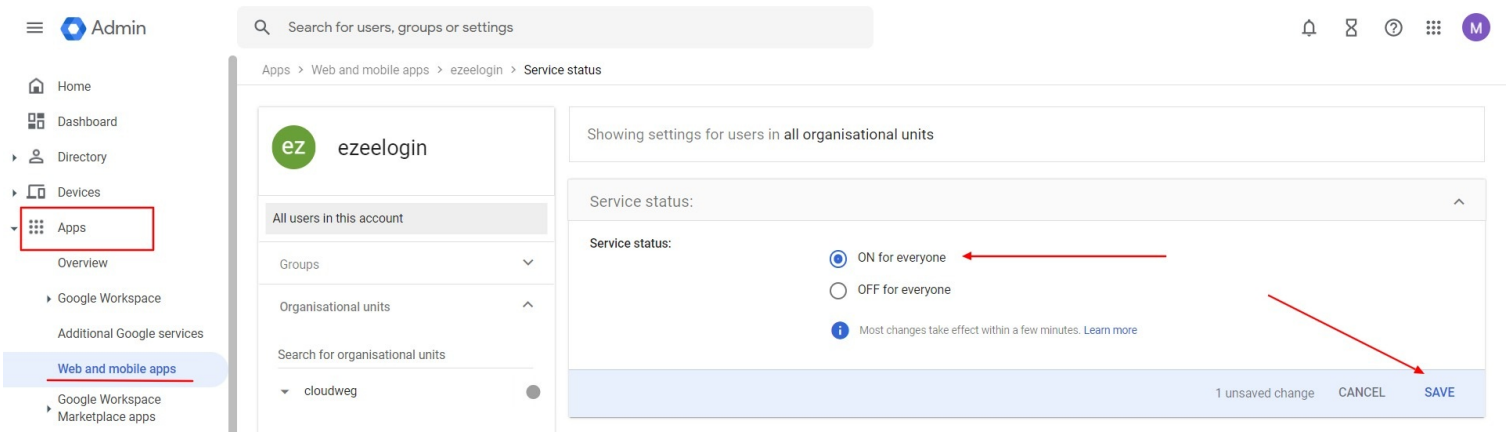


Step 5: Map **primary email** with the **username** and click on the finish button.

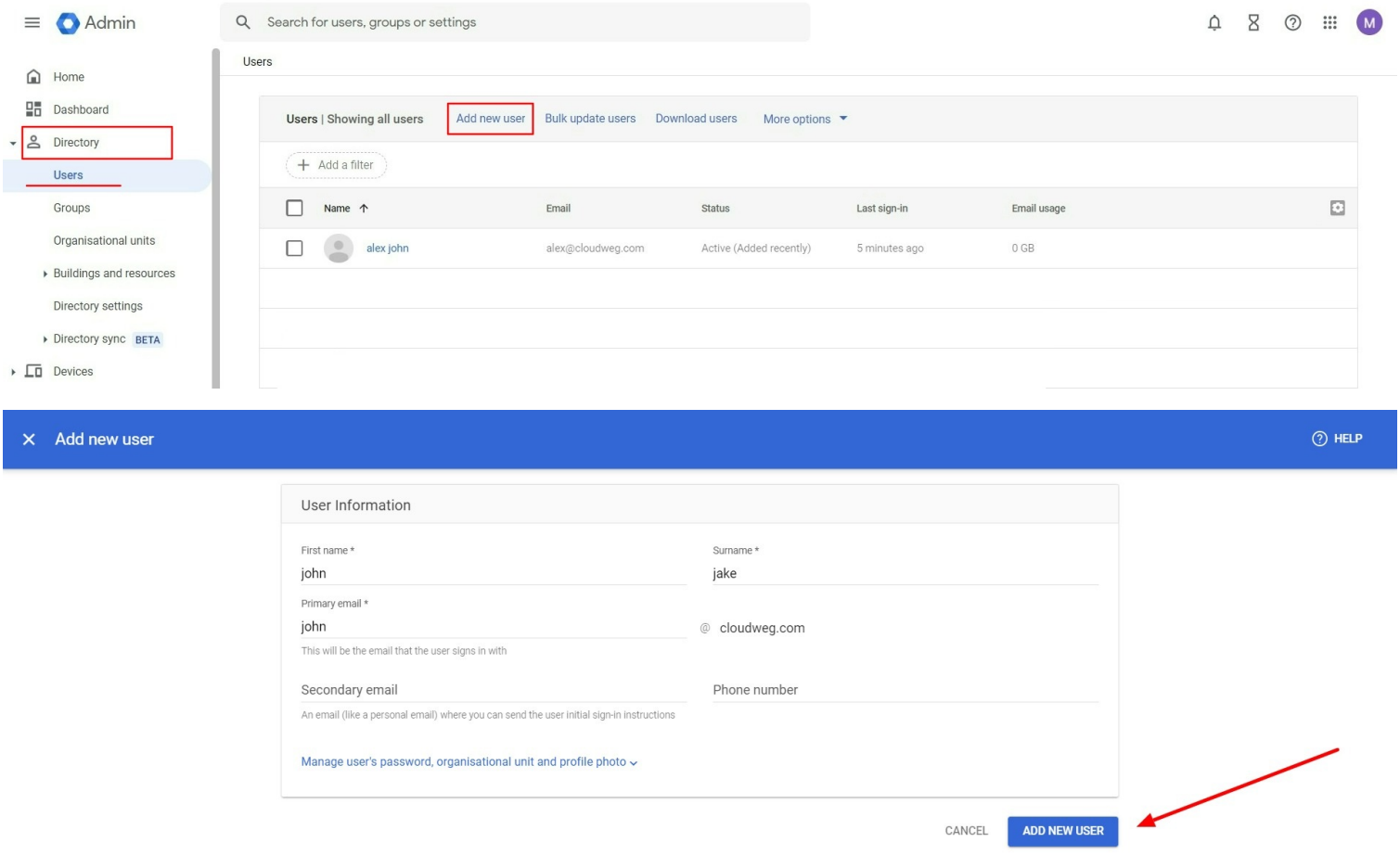


Step 6: Turn on access to every user to use the application. Click on **OFF for everyone** and change the access to **ON for everyone** and click on the save button.

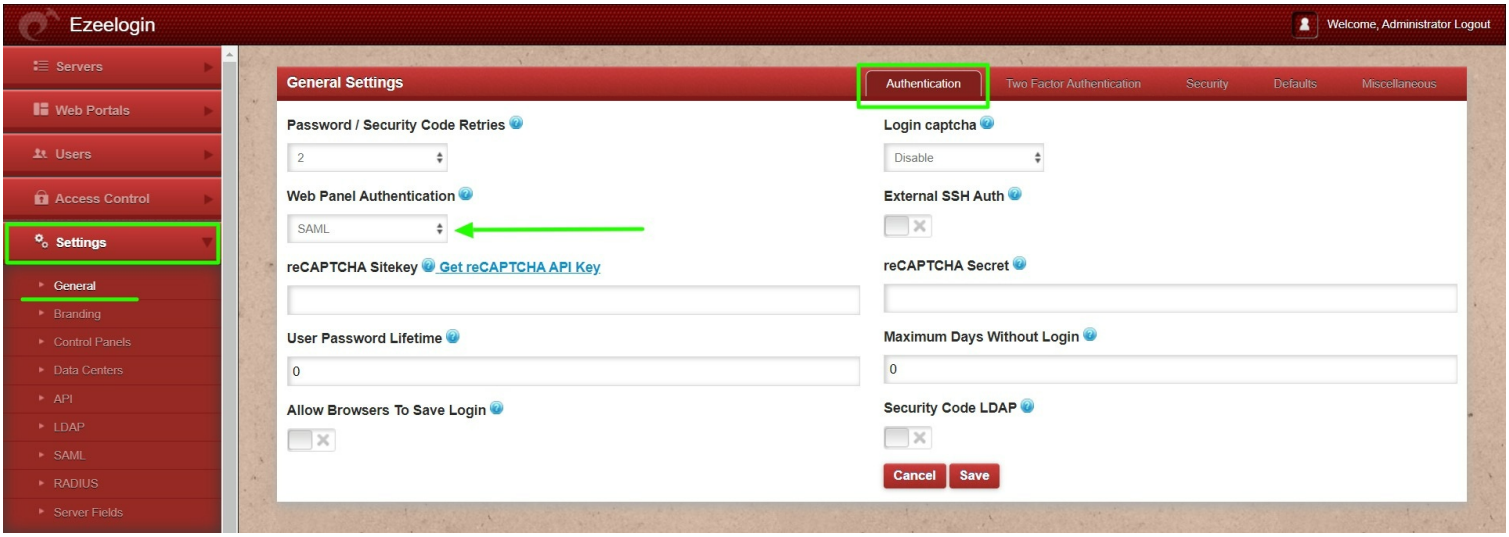




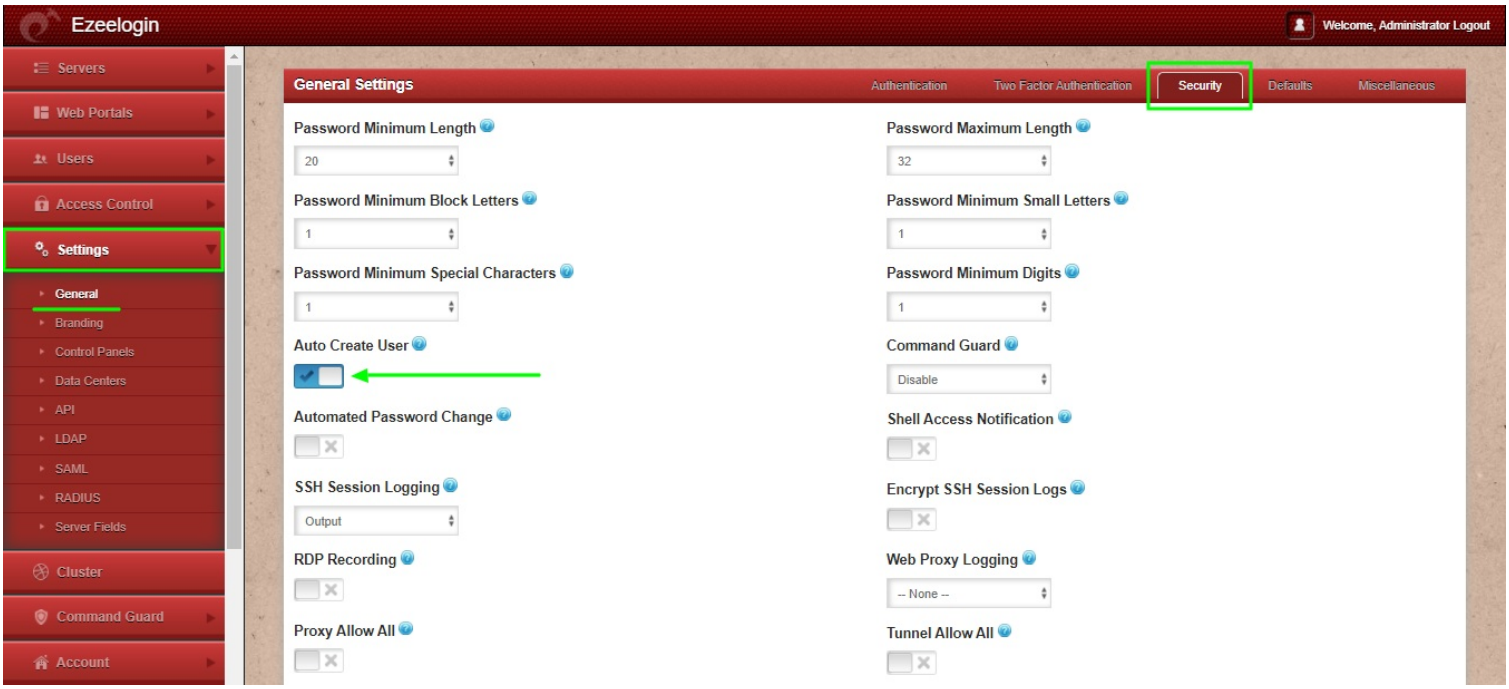
Step 7: Add a **new user** to use the application.



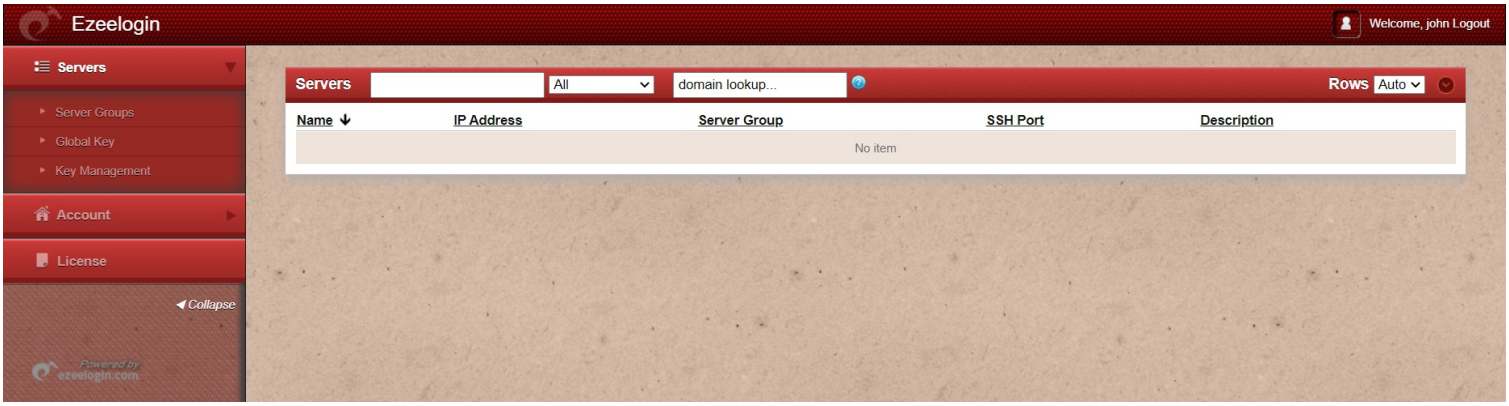
Step 8: Change Web panel Authentication to SAML from **Ezeelogin GUI > Settings > General >Authentication**



Step 9: Enable Auto Create User from **Ezeelogin GUI -> Settings -> General -> Security -> Enable Auto Create User**



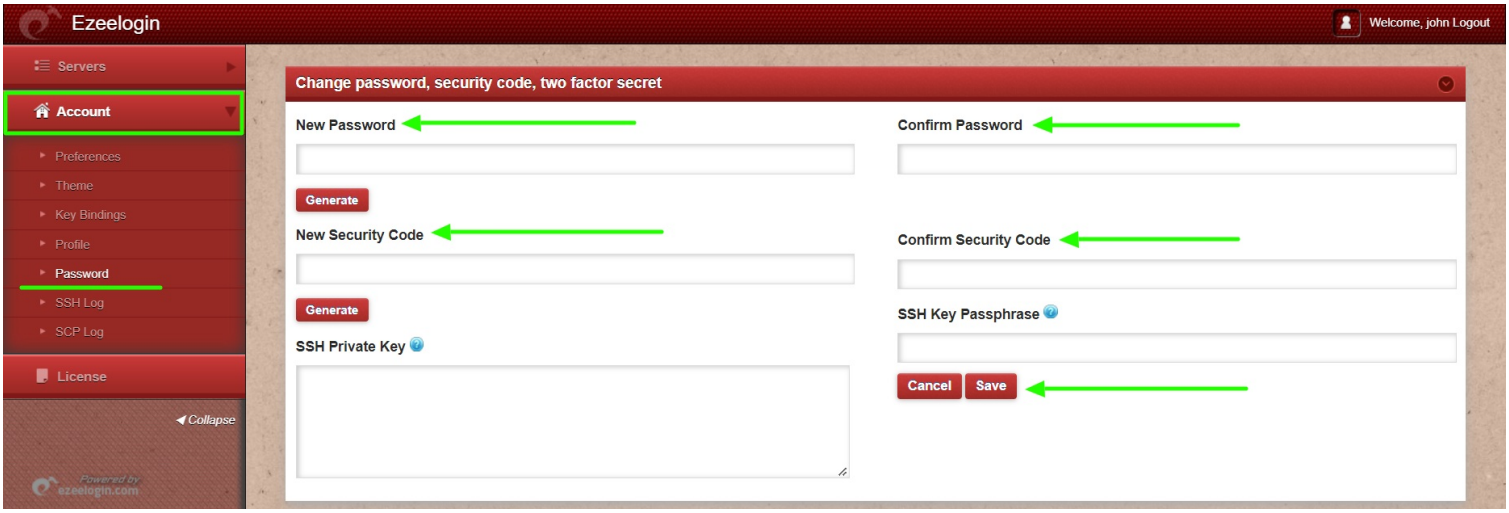
Step 10: Login to Ezeelogin GUI with SAML authentication.



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

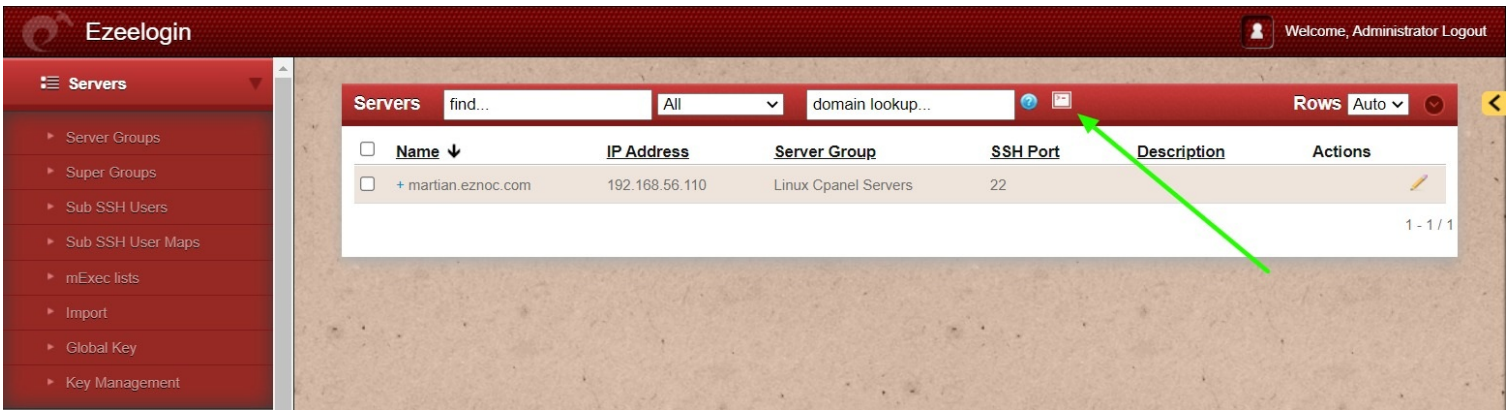
Error: Invalid password

Step 11: After logging into the GUI, resetting the password and security code of the SAML user under Account -> Password is required to enable SSH access to the EZSH shell.

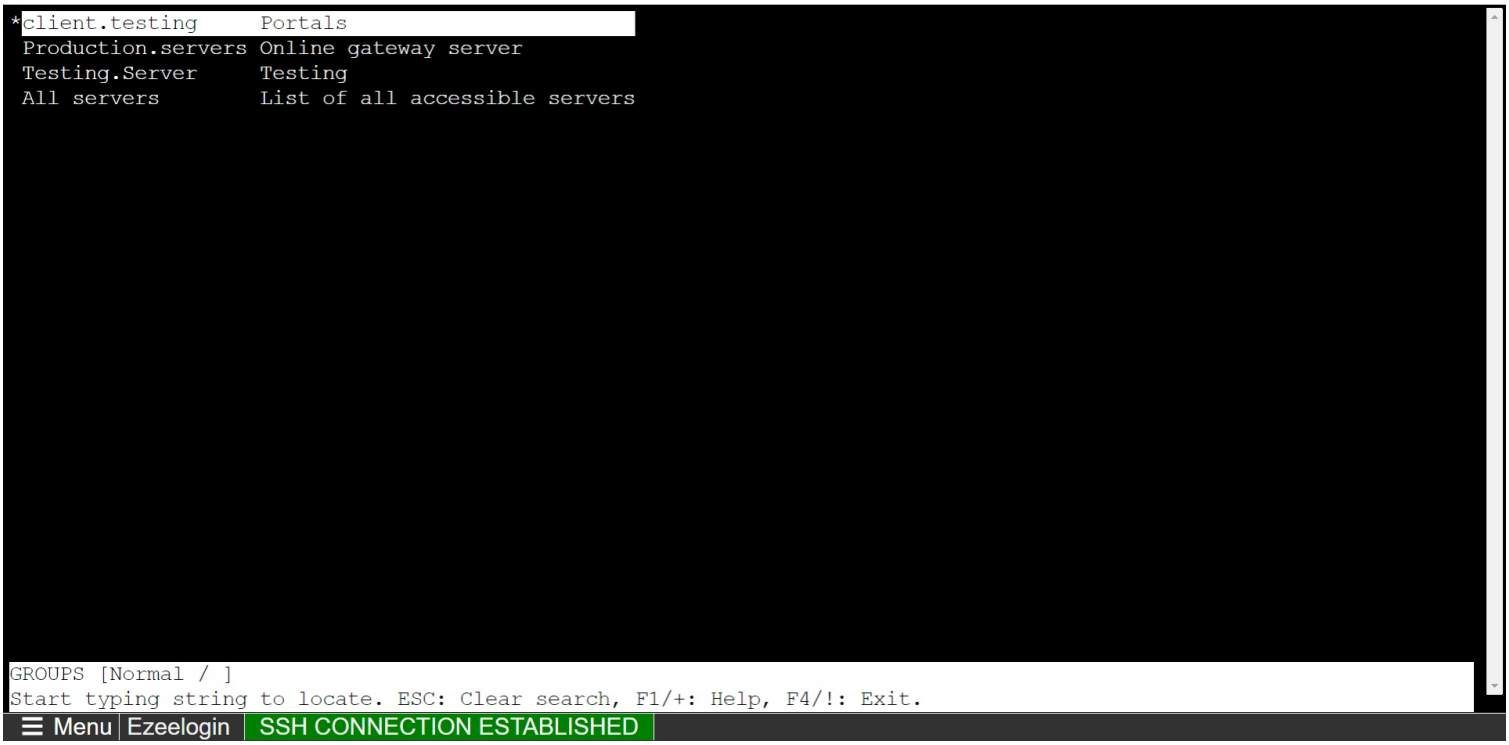


Step 12: Logging into the Ezeelogin shell can be done via the WebSSH shell or through any SSH client, such as Putty or a terminal.

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



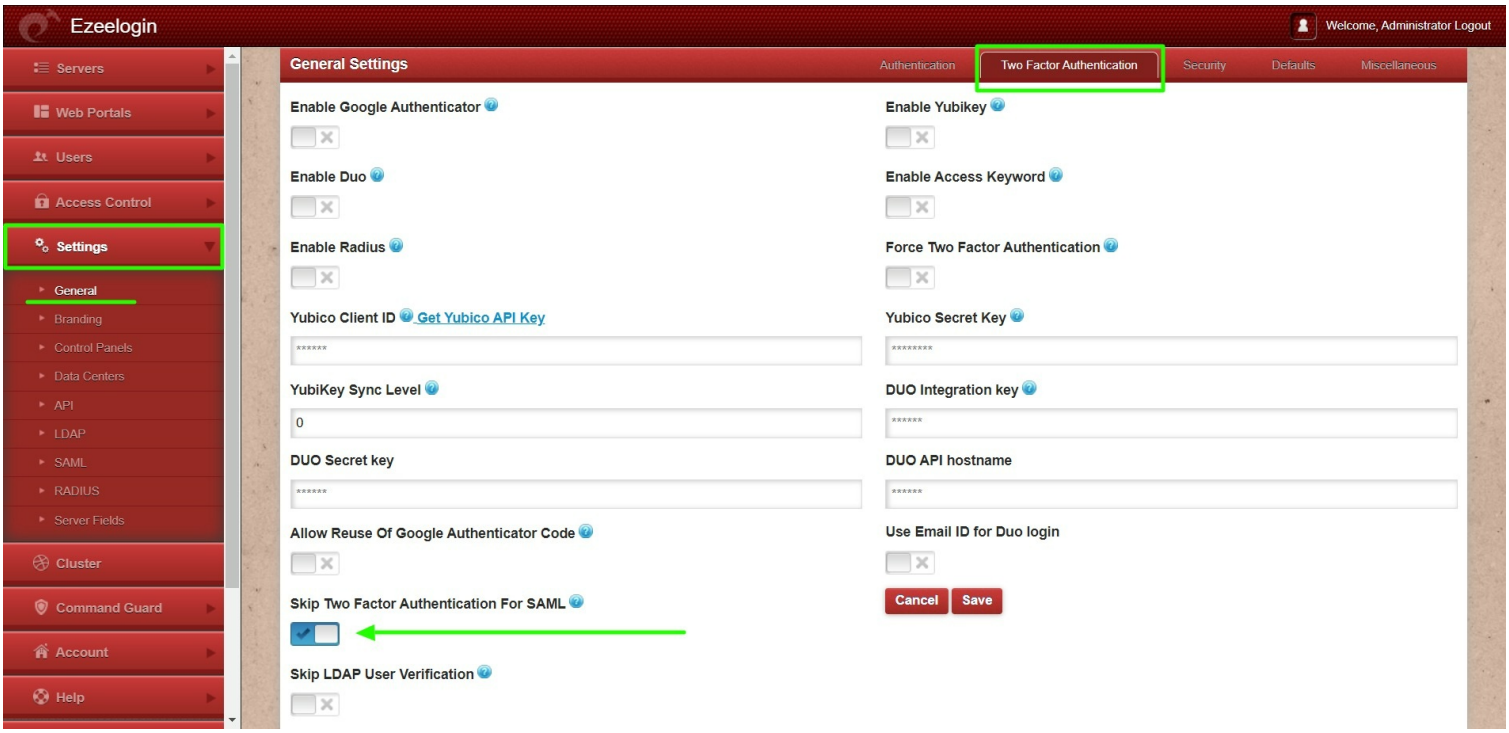
WebSSH terminal will open like below. **Users can navigate the server group with the Up and Down arrow buttons and enter to login into the server**.



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

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

Step 13: When SSH-ing with 2FA enabled using Putty or Terminal, a prompt will appear 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 webpanel it would prompt for the 2FA codes.



Note:

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.

Note:
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.

Related Articles:

Login as superadmin when SSO is enabled globally

Check the standard security configurations in Ezeelogin.

Mapping existing user group from SAML provider to Ezeelogin user groups.

Disable SAML/SSO authentication.

Integrate Gsuite SSO with Jumpserver.

Integrate Onelogin SSO with Jumpserver.

Integrate Jumpcloud SSO with Jumpserver.

Online URL: https://www.ezeelogin.com/kb/article/integrate-gsuite-sso-with-jumpserver-513.html