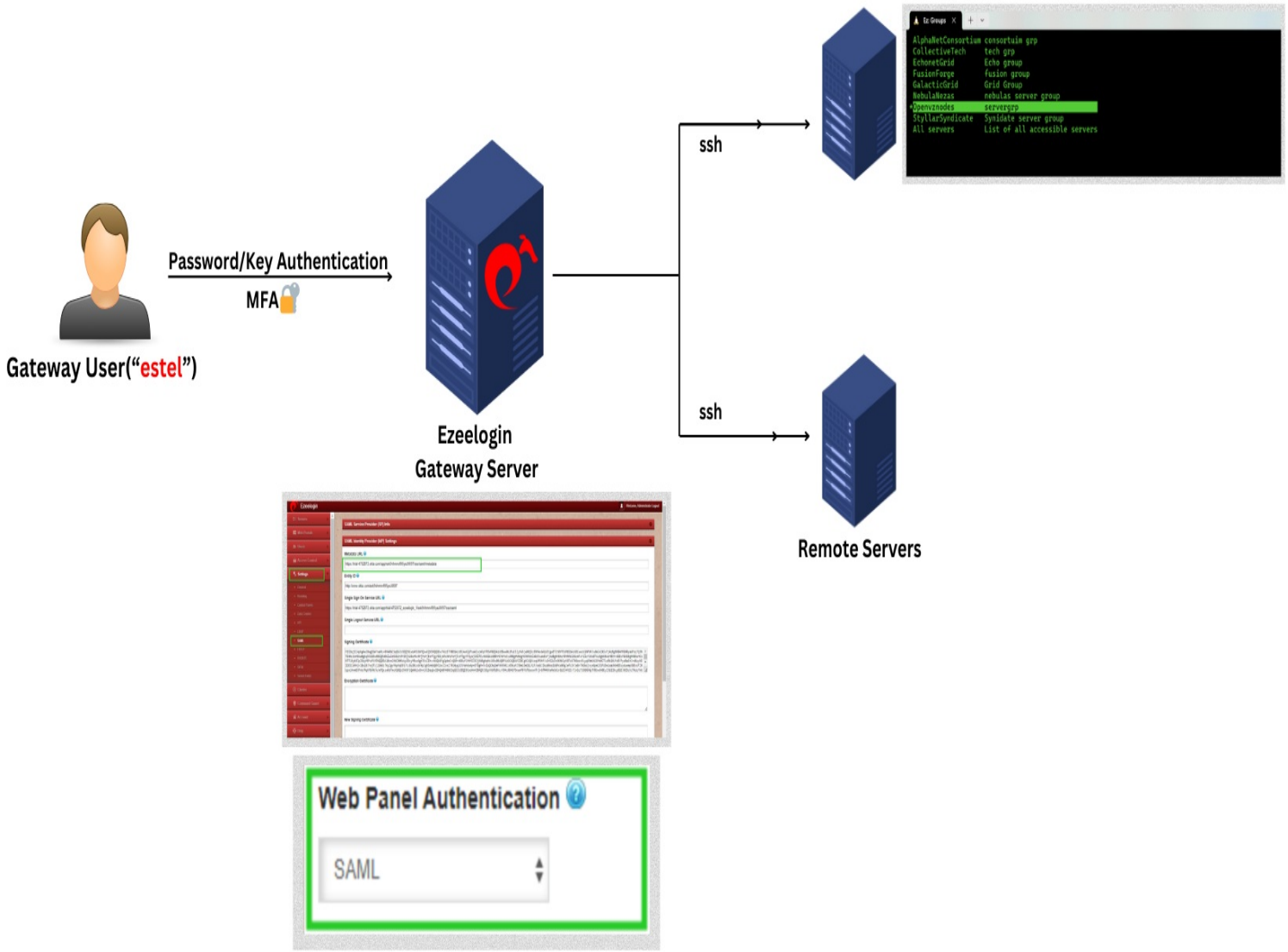
Integrate OneLogin SSO with jumpserver

273 Manu Chacko April 28, 2026 Productivity & Efficiency Features, Tweaks & Configuration 11146

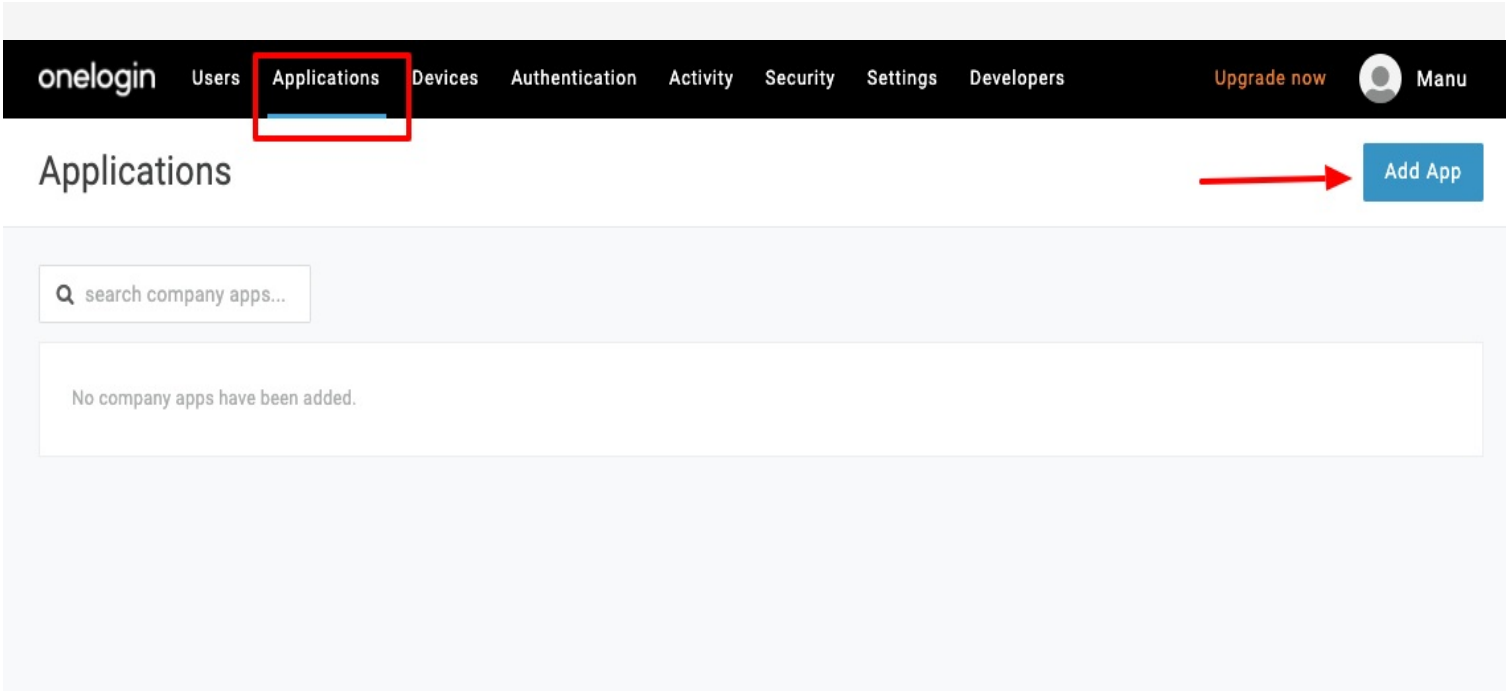
Integrating OneLogin Single Sign-On (SSO) with Jumpserver

Overview: This article describes integrating OneLogin Single Sign-On (SSO) with Jumpserver, focusing on configuring SAML settings in OneLogin and Jumpserver for web application authentication.

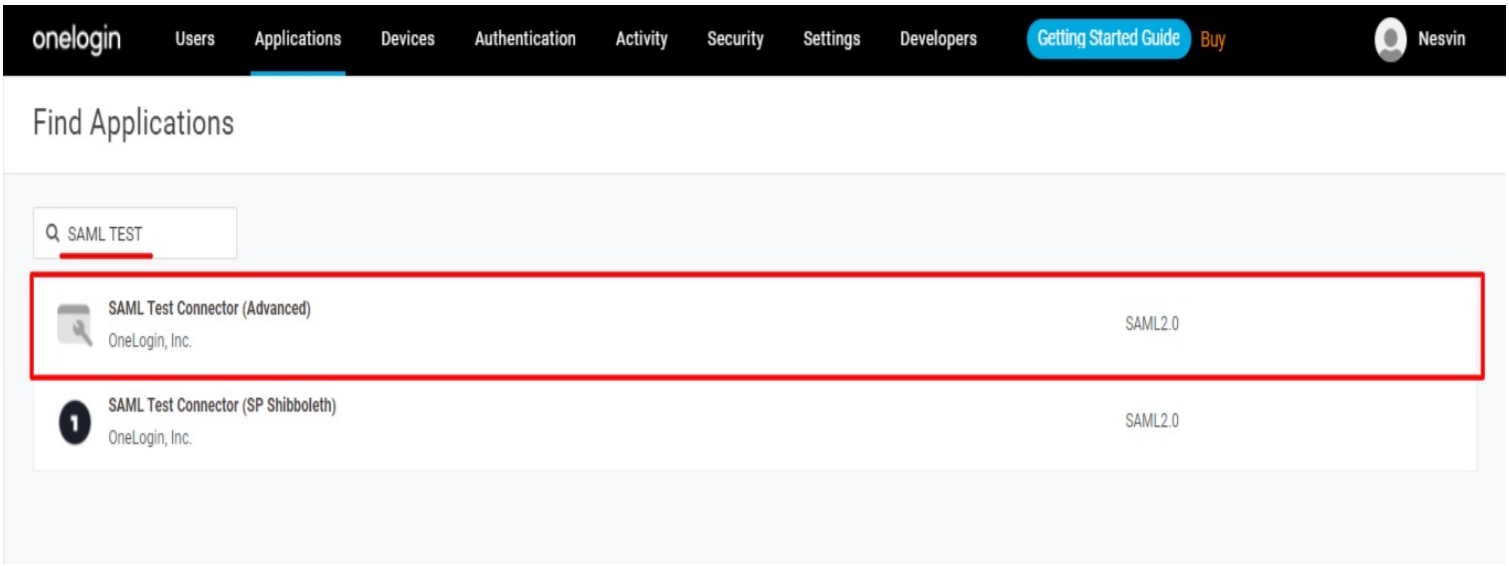
> SAML is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



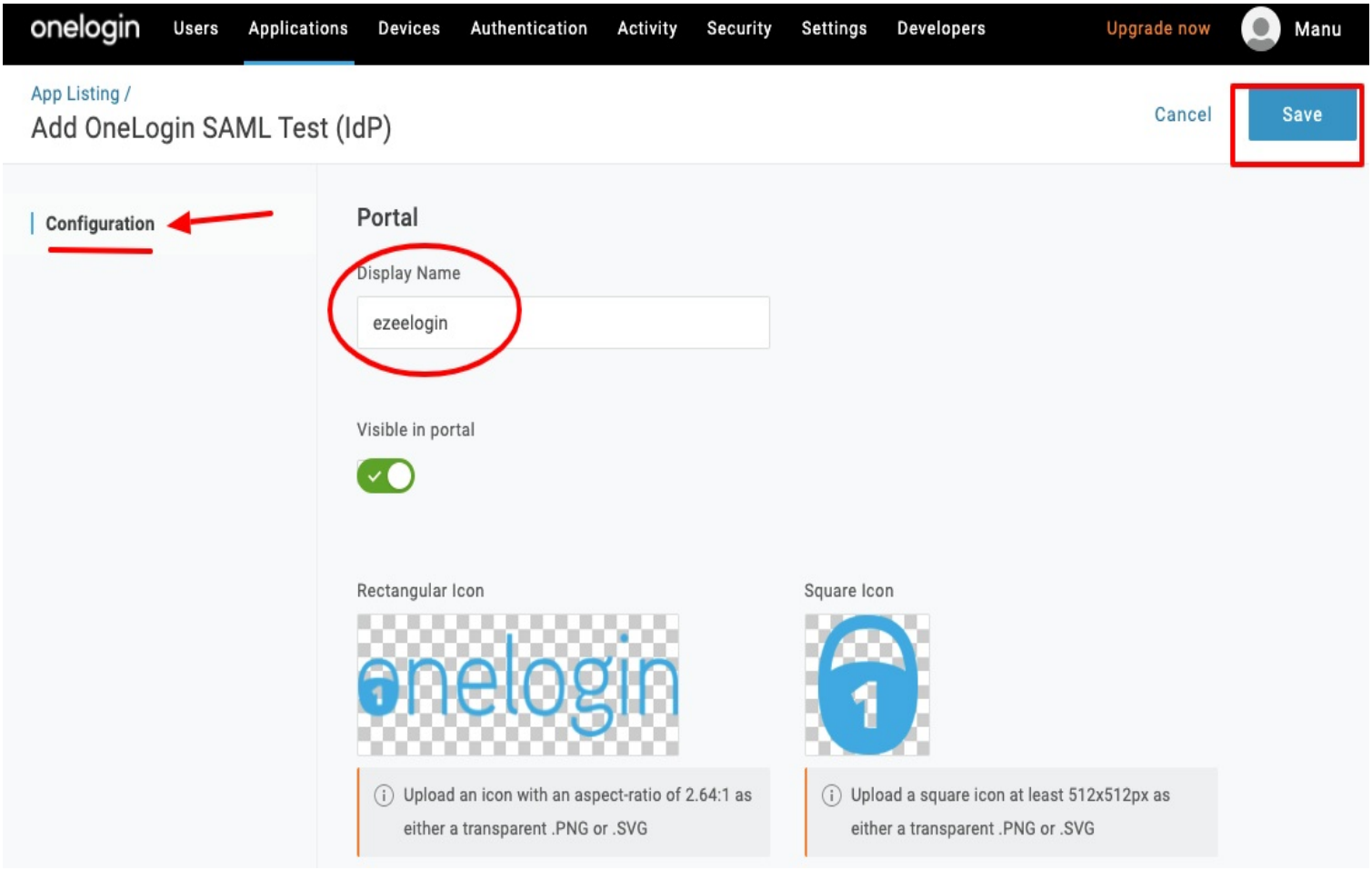
Step 1: Log in to OneLogin and **Add the Application**.



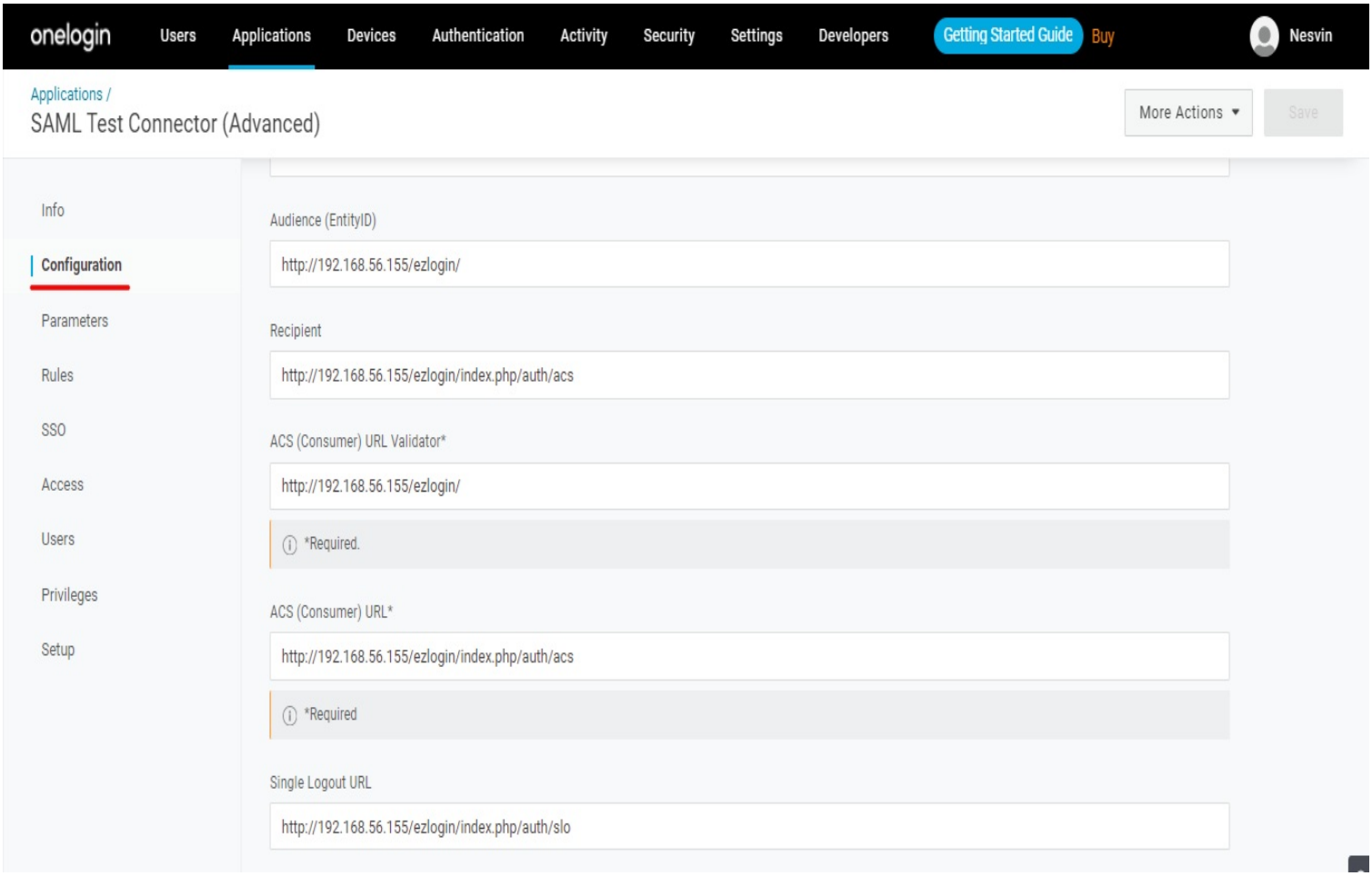
Step 2: Search for **SAML TEST** and select **SAML Test Connector** (Advanced).



Step 3: Change the **Display name** and save.

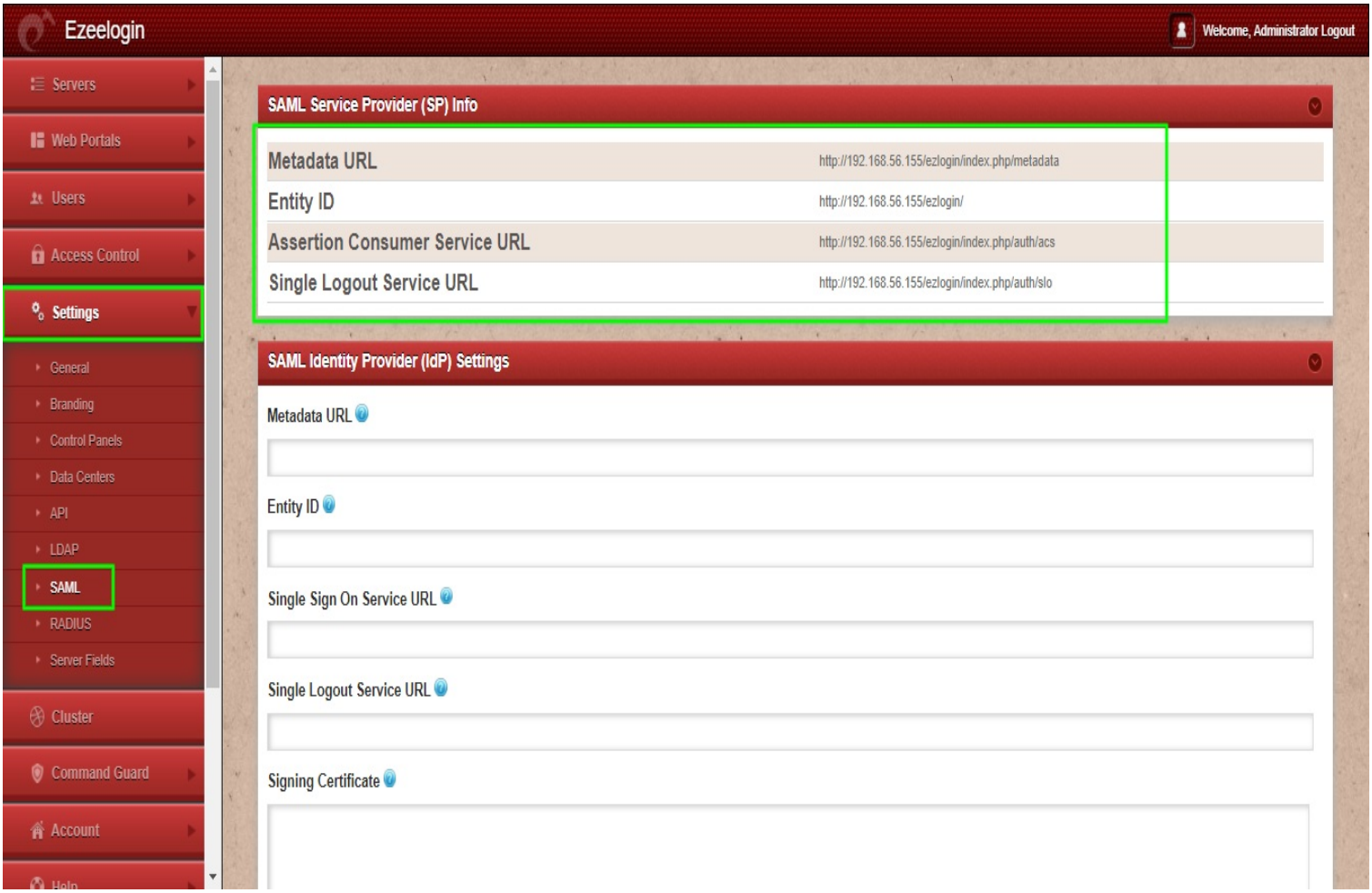


Step 4: Select the **configuration tab** from the right panel and fill in the **Application details**.

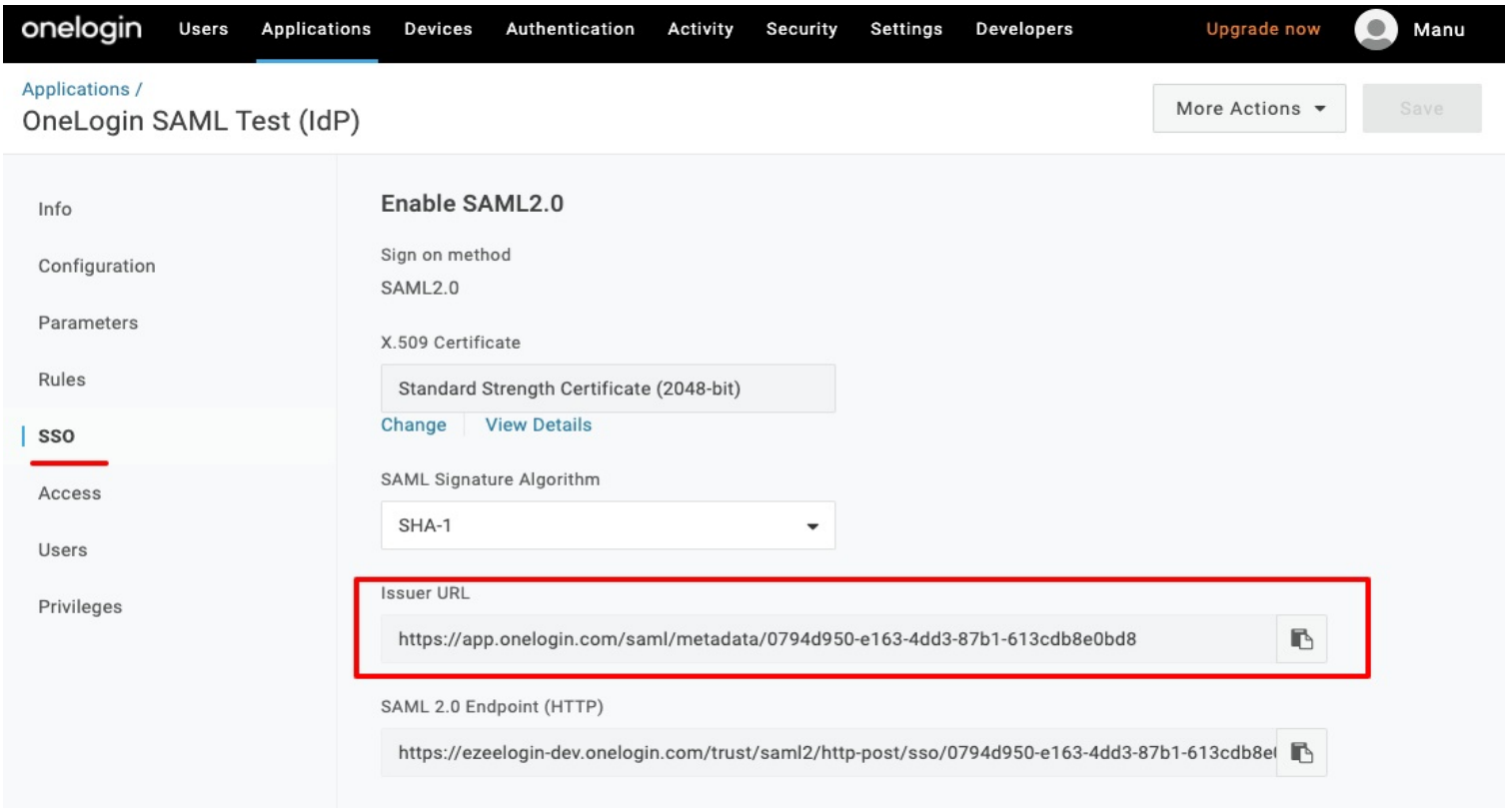


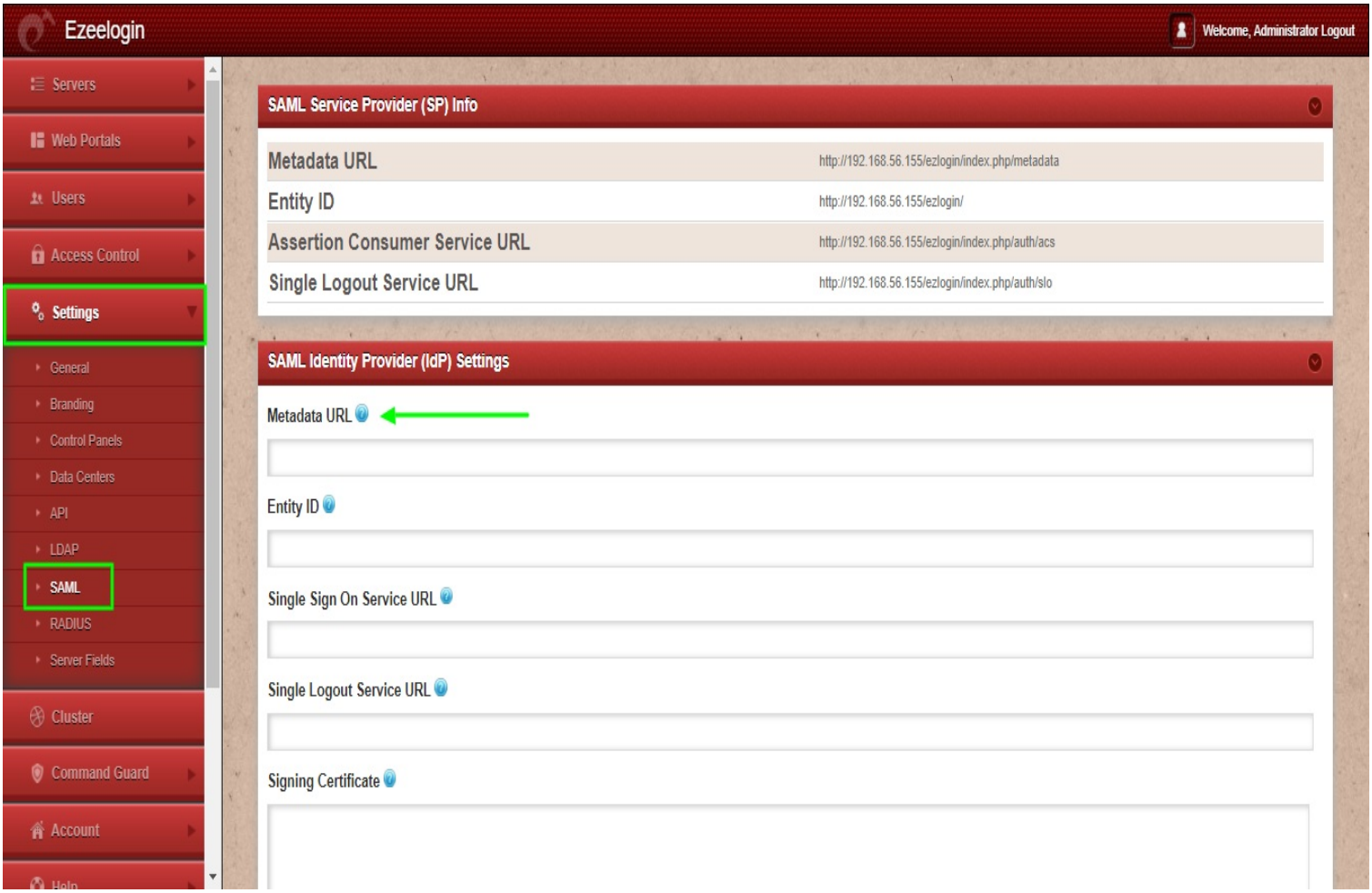
Audience (EntityID) - Entity ID (you can find it from ezeelogin GU > Settings > SAML)
Recipient - Assertion Consumer Service URL (you can find it from ezeelogin GU > Settings > SAML)
ACS (Consumer) URL Validator - Entity ID (you can find it from ezeelogin GU > Settings > SAML)
ACS (Consumer) URL - Assertion Consumer Service URL (you can find it from ezeelogin GU > Settings > SAML)

Single Logout URL - Single Logout Service URL (you can find it from ezeelogin GU > Settings > SAML)

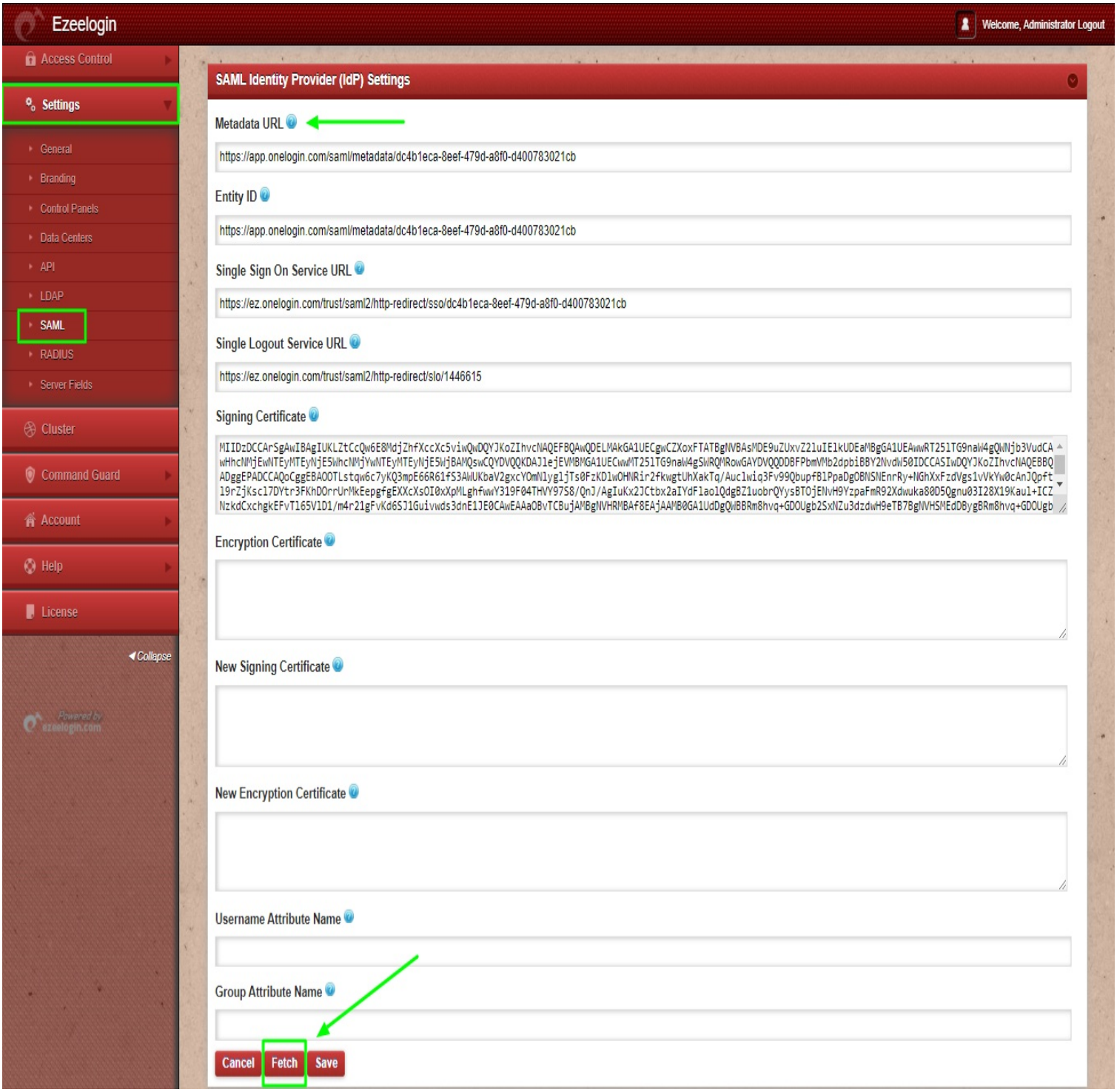


Step 5: Select the **SSO tab** from the right panel & Copy the **Issuer URL** and paste it to the **Metadata URL** on **Ezeelogin GUI -> Settings -> SAML Metadata URL**

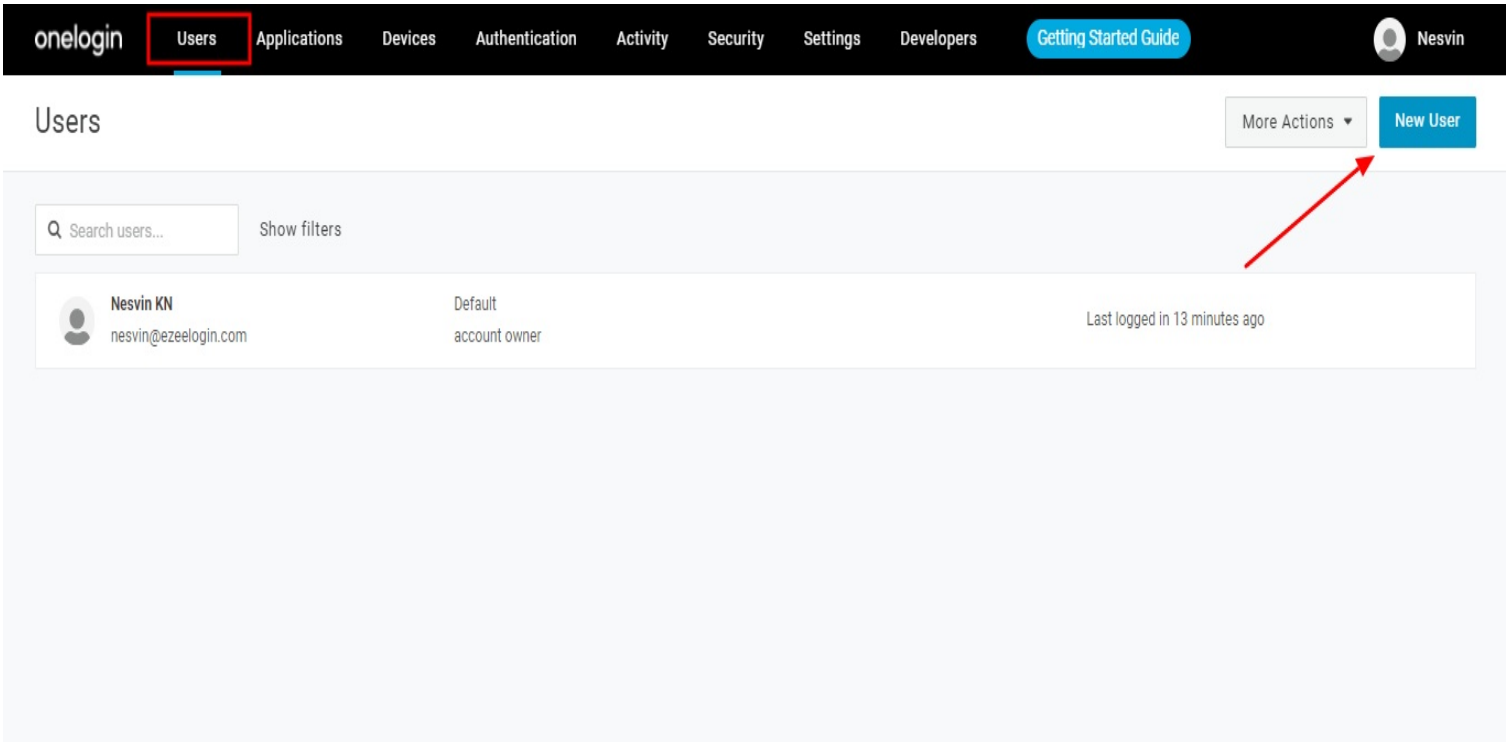


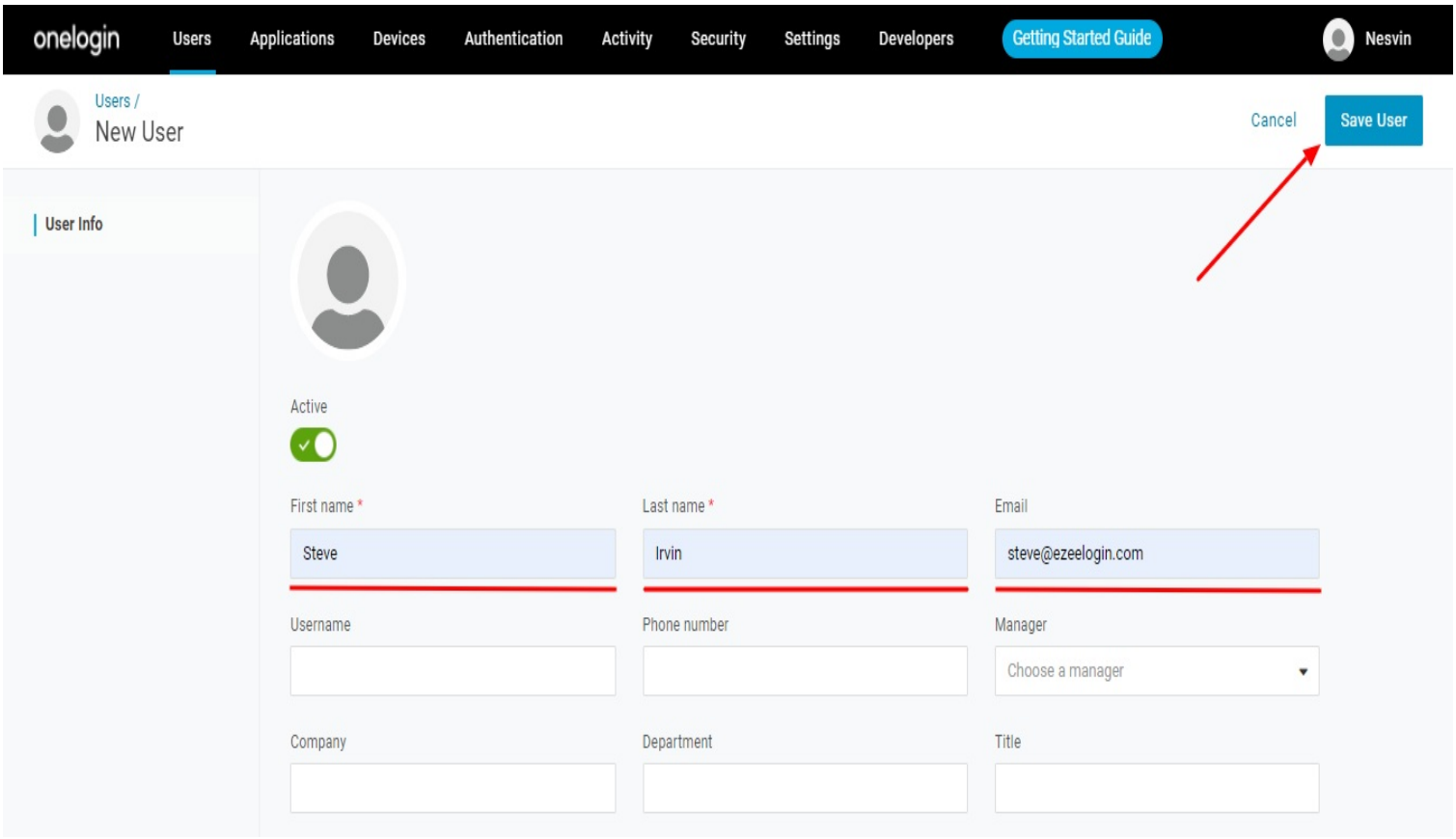


Step 6: Click on the **fetch** button, it will auto-fill the SAML setting and **SAVE** it.

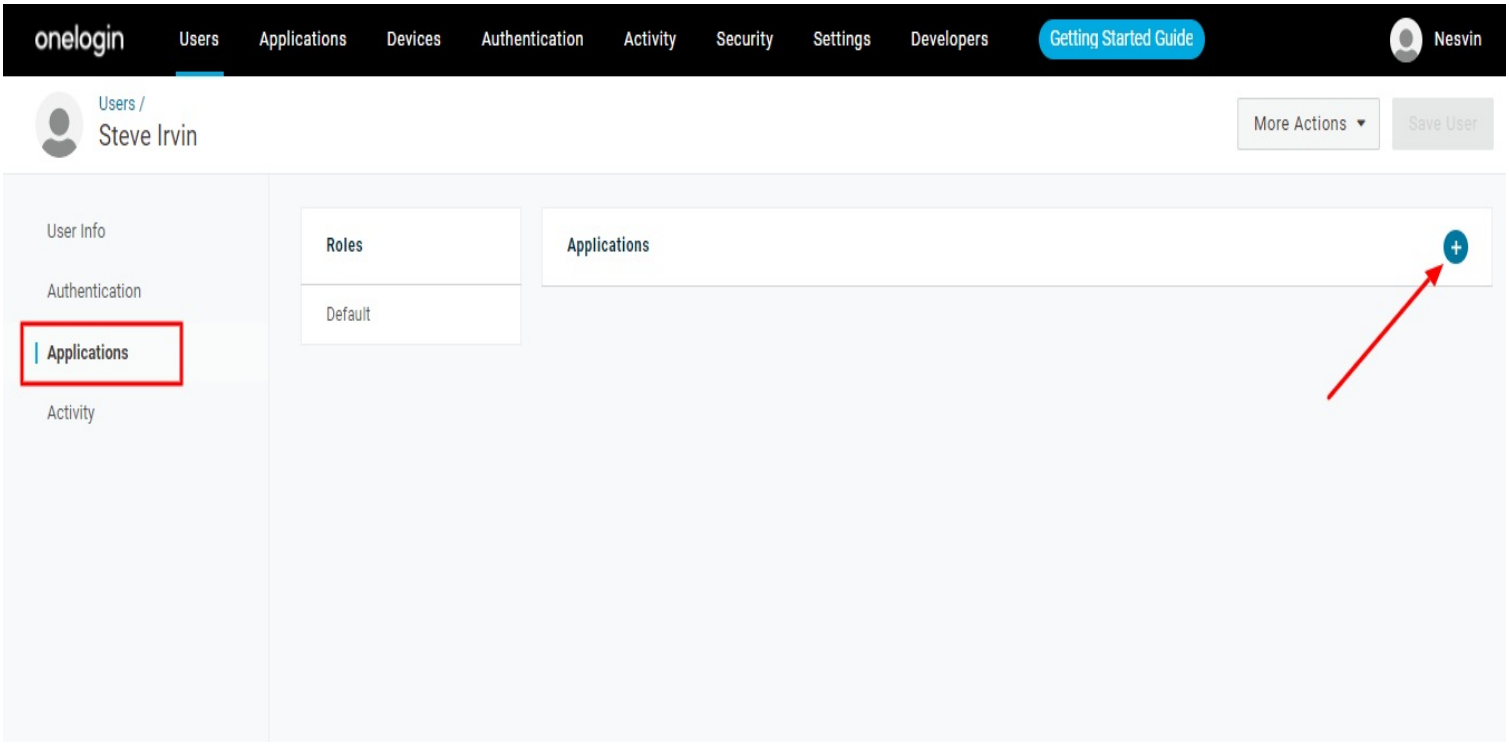


Step 7: Select the **users tab** from the left panel and click on the **new user** then provide **first name**, **last name**, and **email** to save the user.

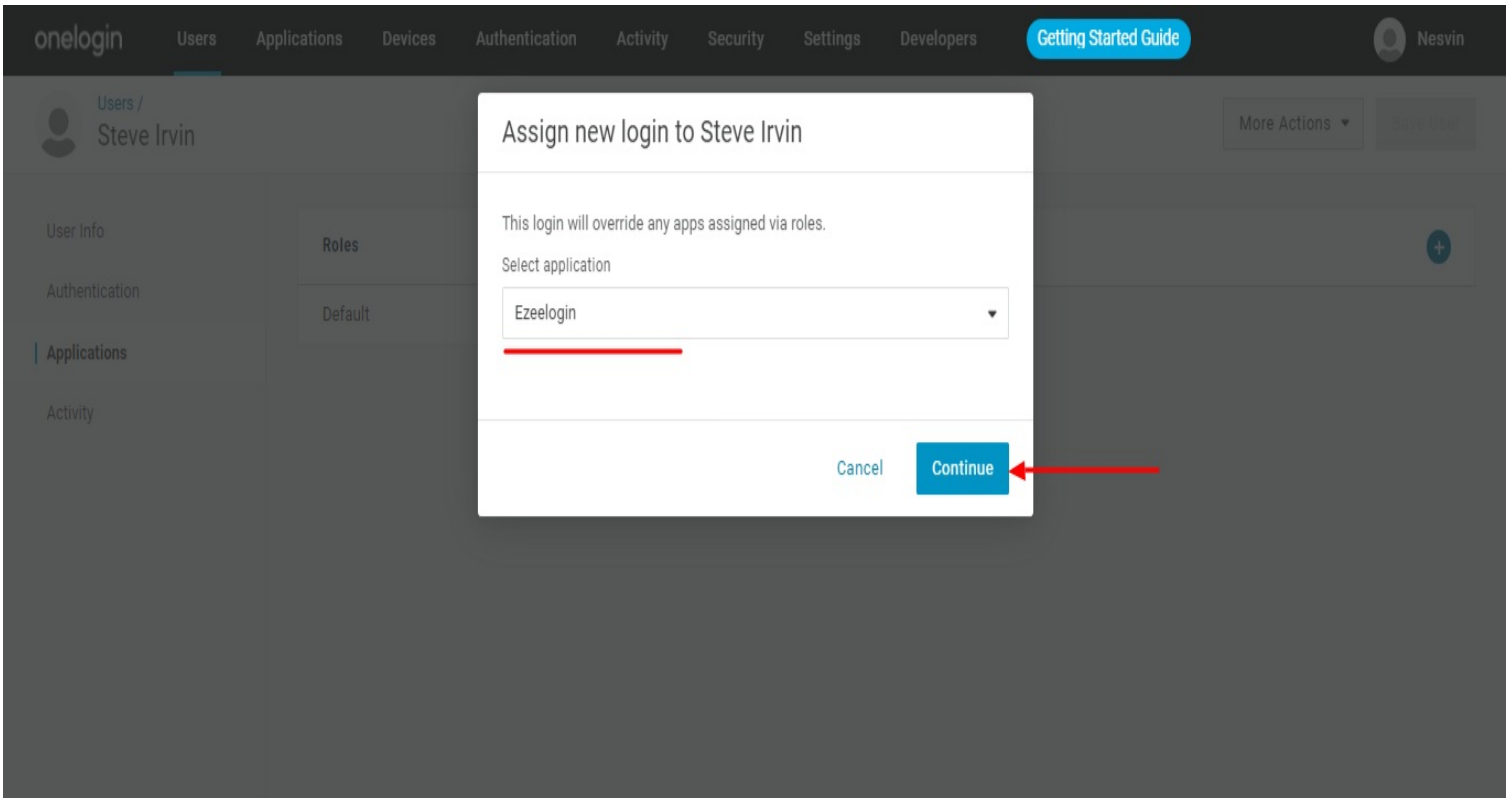


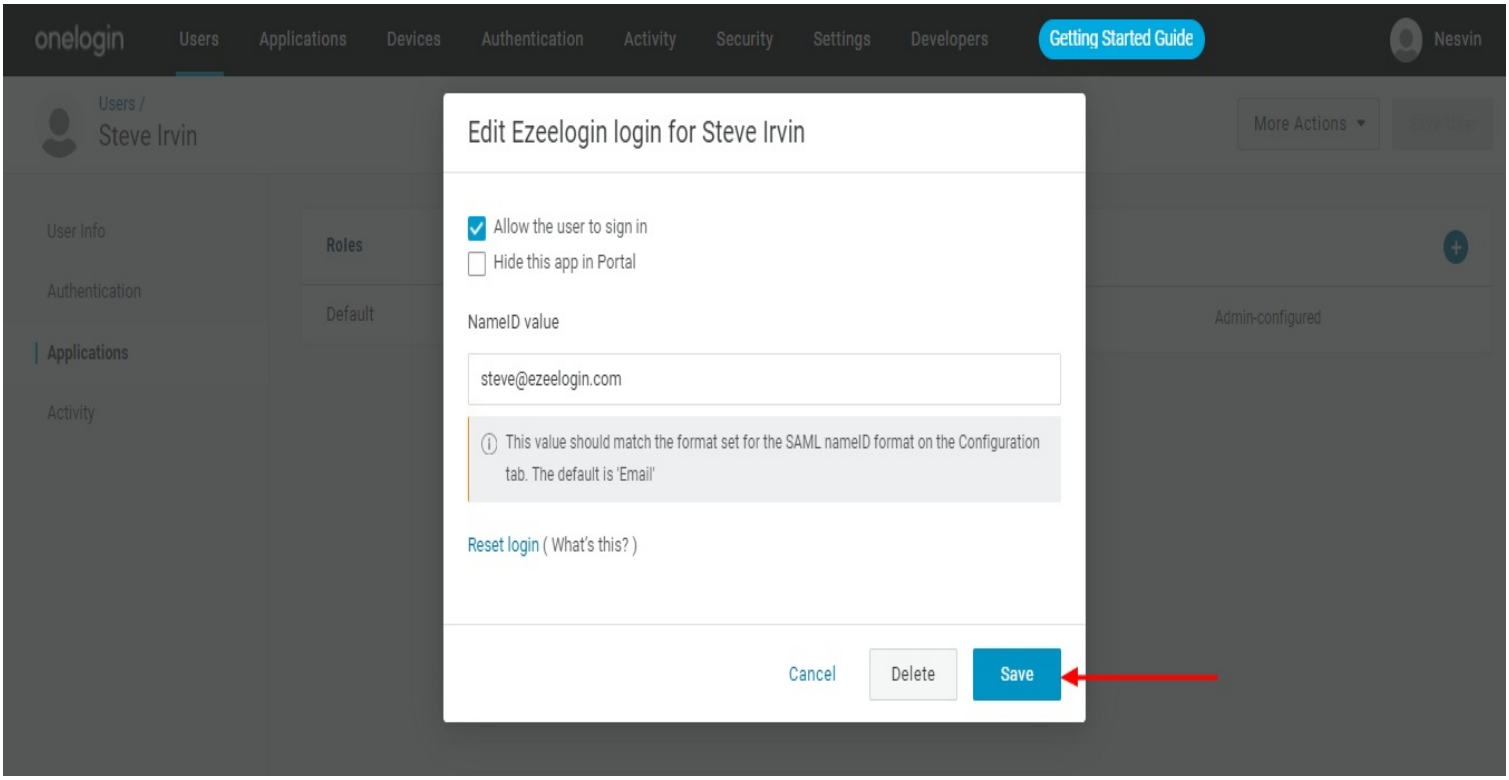


Step 8: Select **applications** from the left panel and click on the **add** icon to **map** the application to the user.

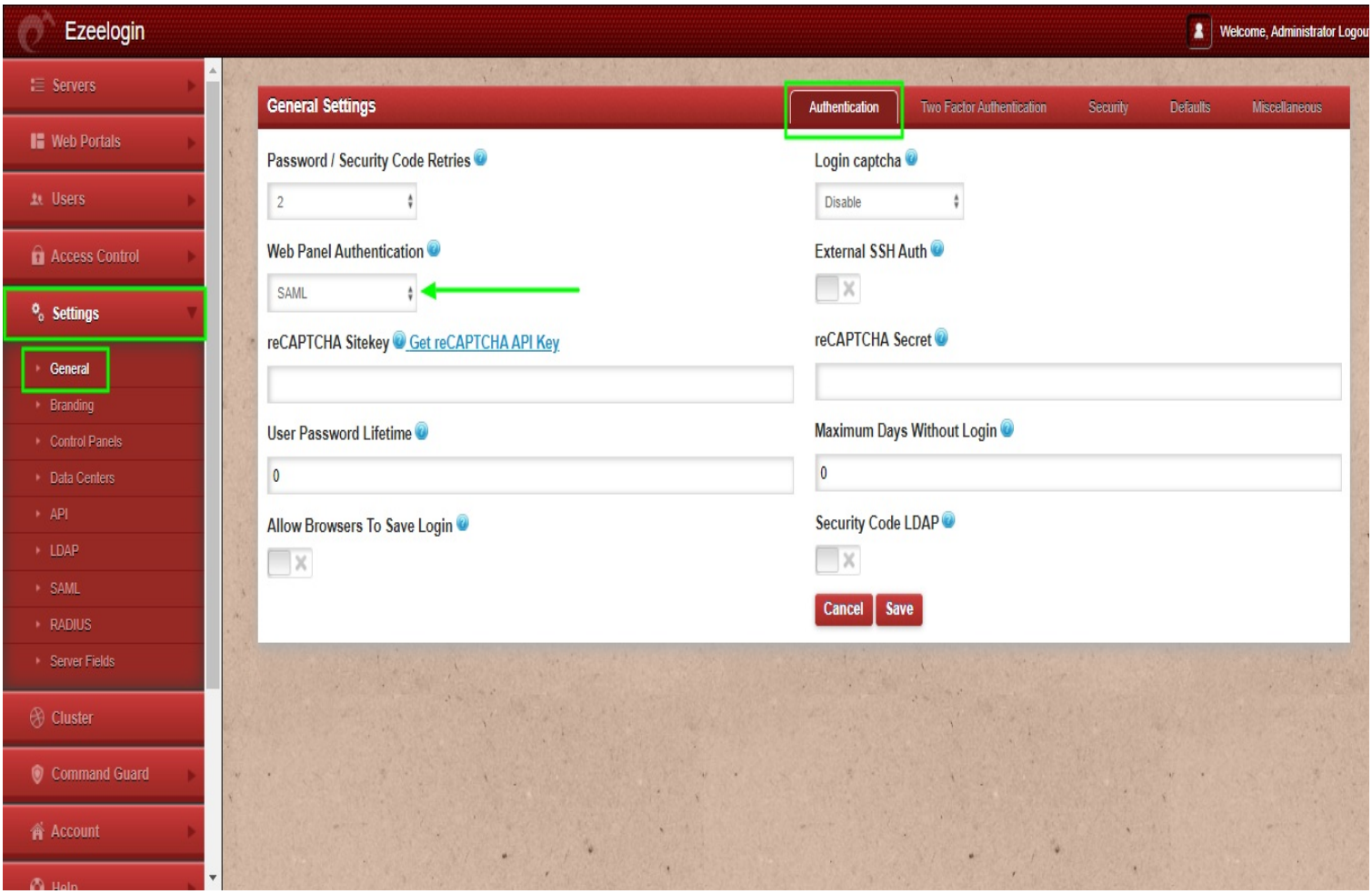


Step 9: Select the **application** from drop-down and then **save** the application.

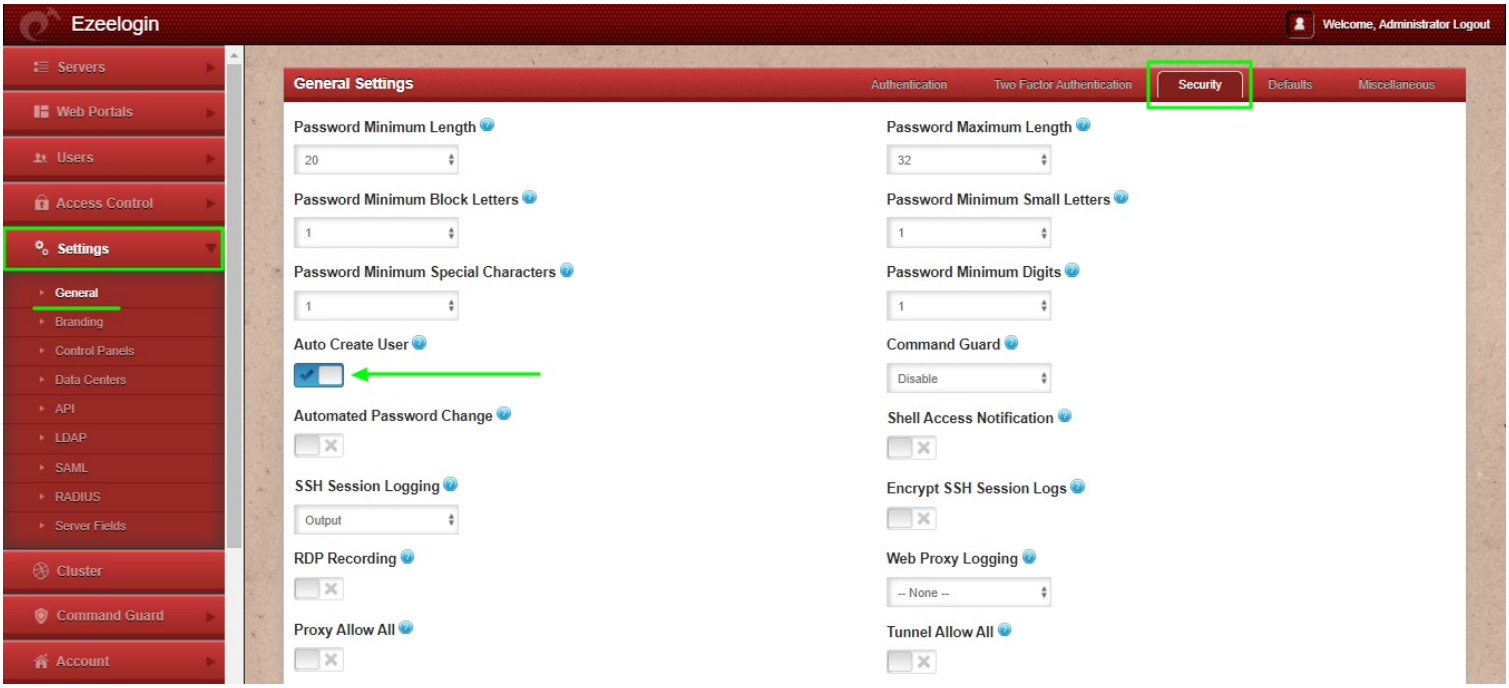




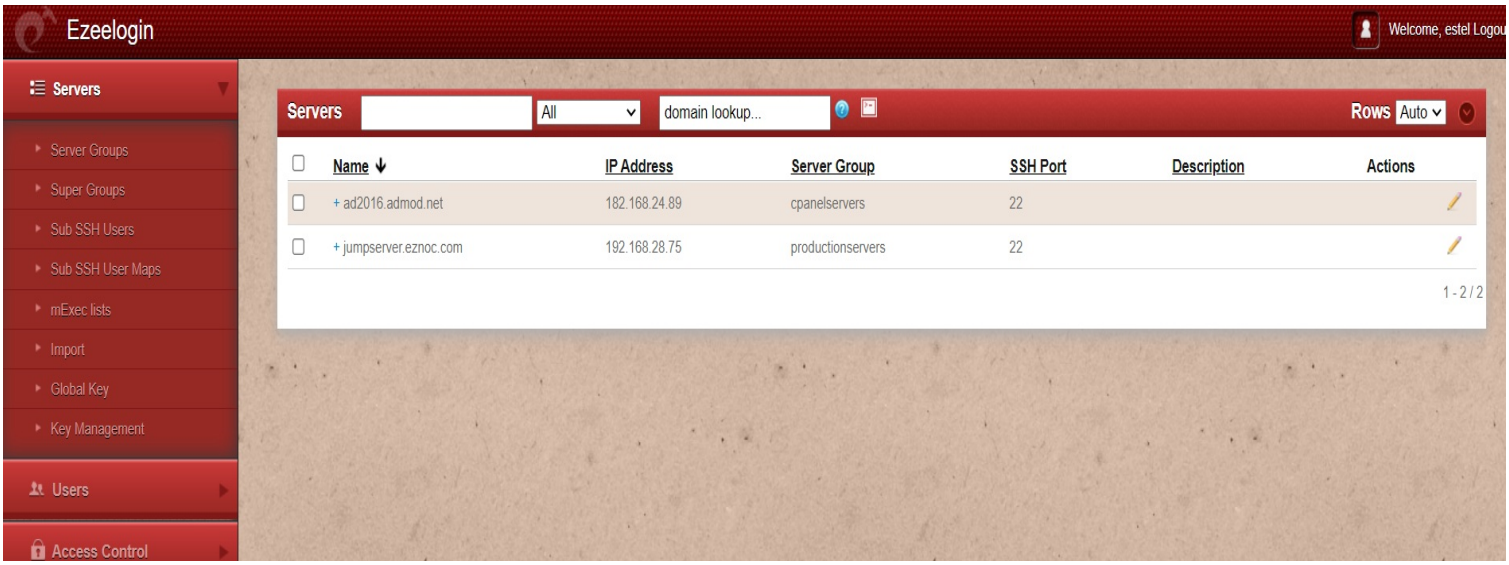
Step 10: Change **Web panel Authentication** to SAML from **Ezeelogin GUI -> Settings -> General ->Authentication.**



Step 11: Enable Auto Create User from **Ezeelogin GUI -> Settings -> General -> Security -> Enable Auto Create User.**



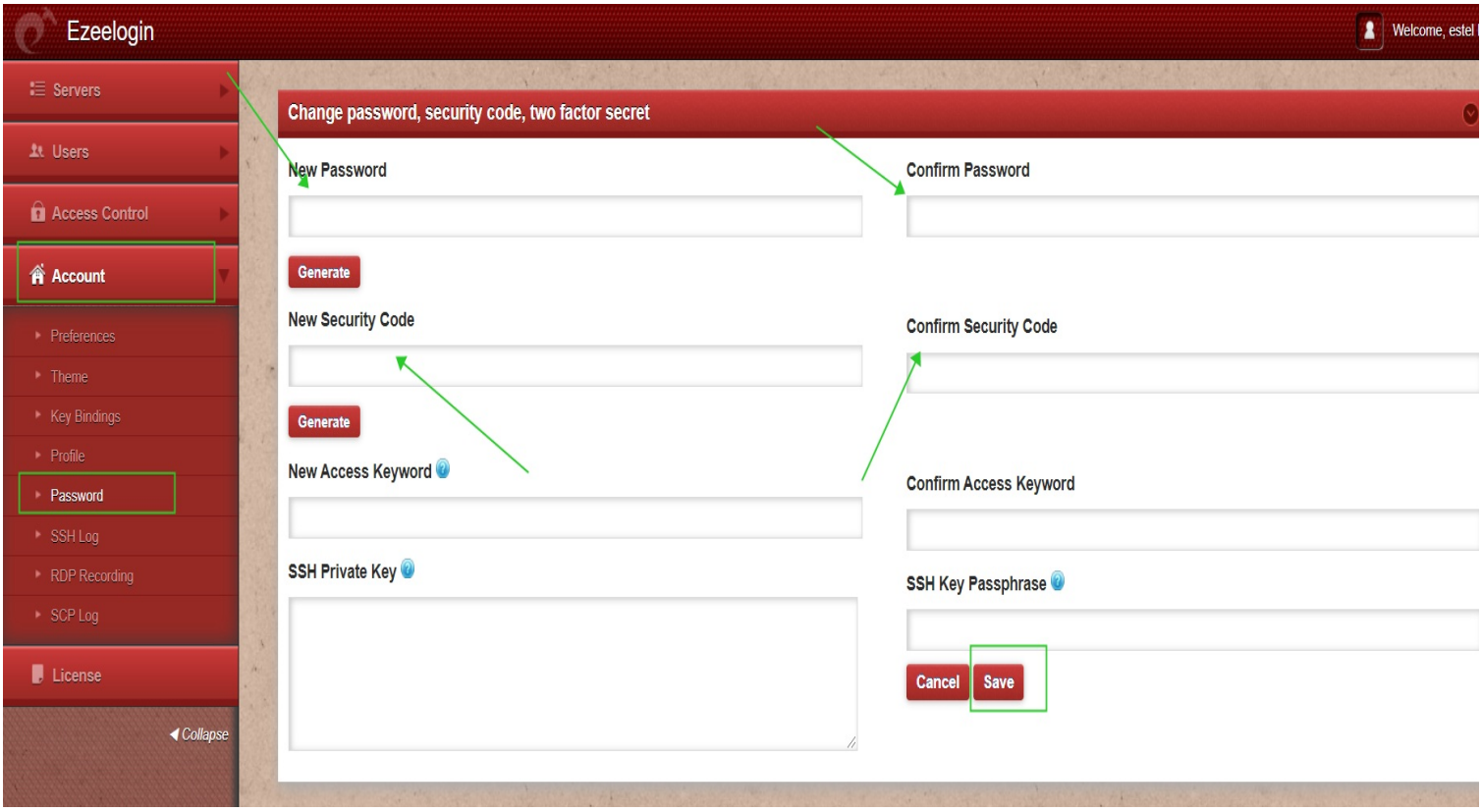
Step 12: Log in to Ezeelogin GUI with **SAML authentication**.



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

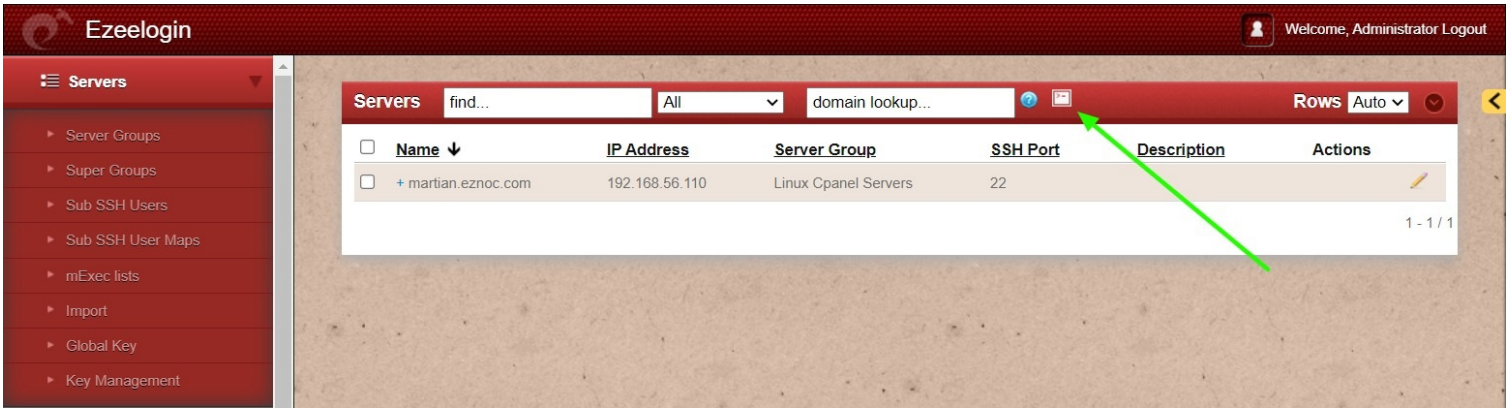
Error: Invalid password

Step 13: After logging into GUI, you need to **reset the password** and **security code** of the SAML user under **Account -> Password** in order to SSH to Ezeelogin backend(ezsh).

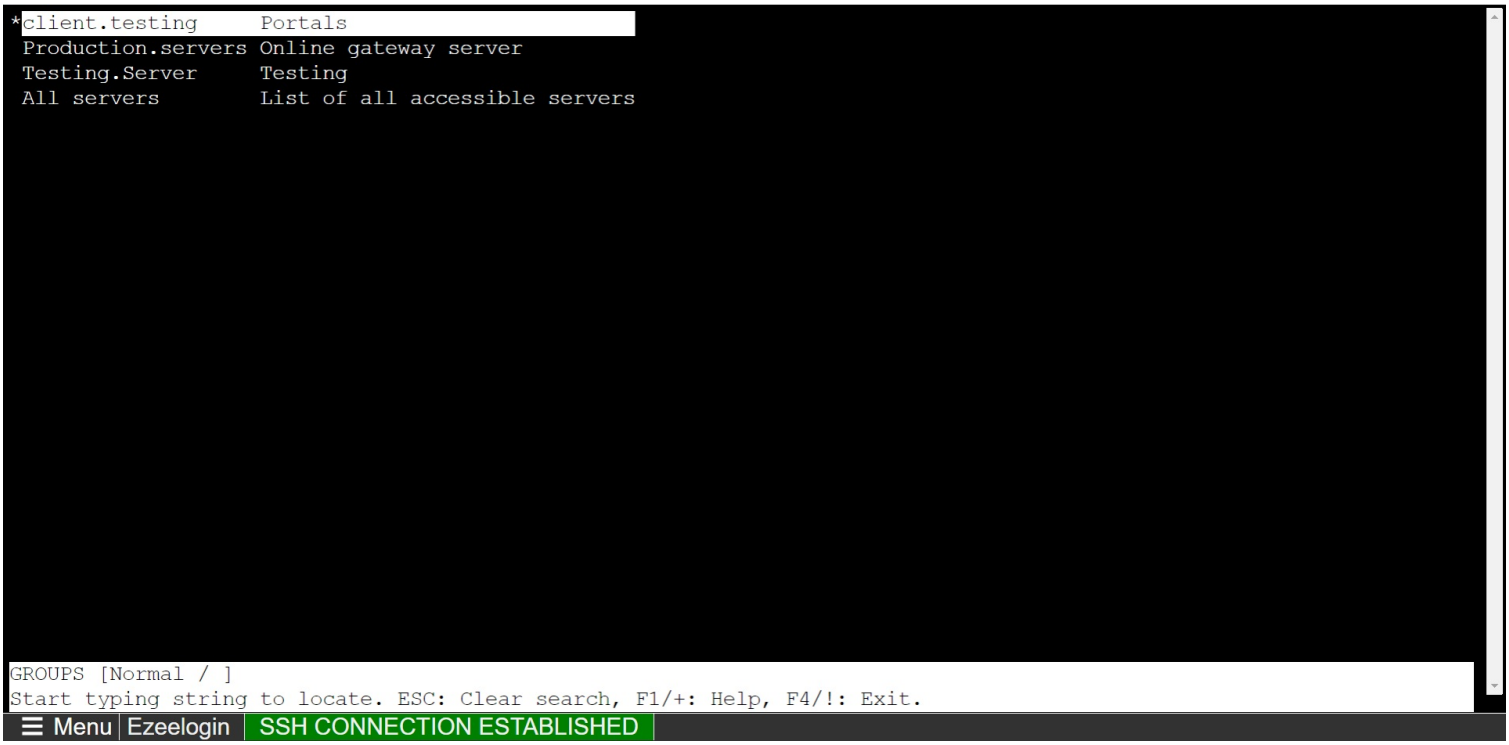


Step 14: You can log in to **Ezeelogin shell** via **Webssh** or using any **SSH client** such as Putty or terminal etc.

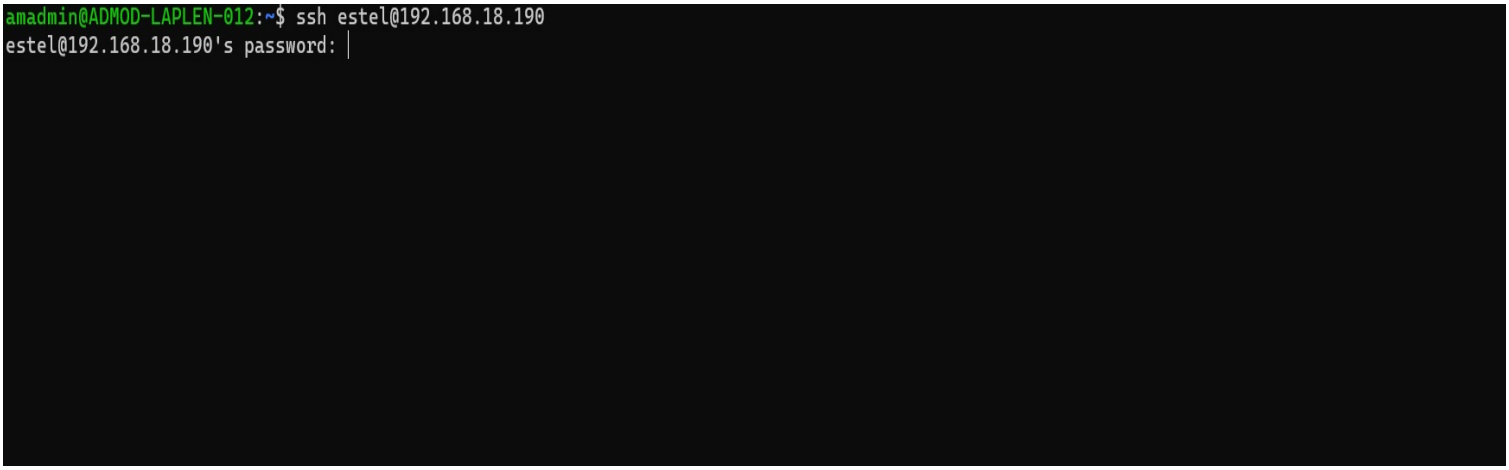
Step 14(A): Click on the '**Open Web SSH Console**' icon to SSH via the browser.



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.



Step 14(B): Native SSH Client: After resetting the password and security code you can SSH to the Ezeelogin backend(ezsh) using Terminal or Putty with the SAML username.



Step 15: When SSH with **2FA enabled** using Putty or Terminal it would prompt you to enter the 2FA codes. You can disable this for SAML Authentication by **enabling skip two factor authentication for SAML** under **Settings** -> **Two Factor Authentication** -> S**kip Two Factor Authentication for SAML**.

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.

You need to 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:

Map existing user group from SAML provider.

Login as superadmin when SSO is enabled globally

Online URL: https://www.ezeelogin.com/kb/article/integrate-onelogin-sso-with-jumpserver-273.html