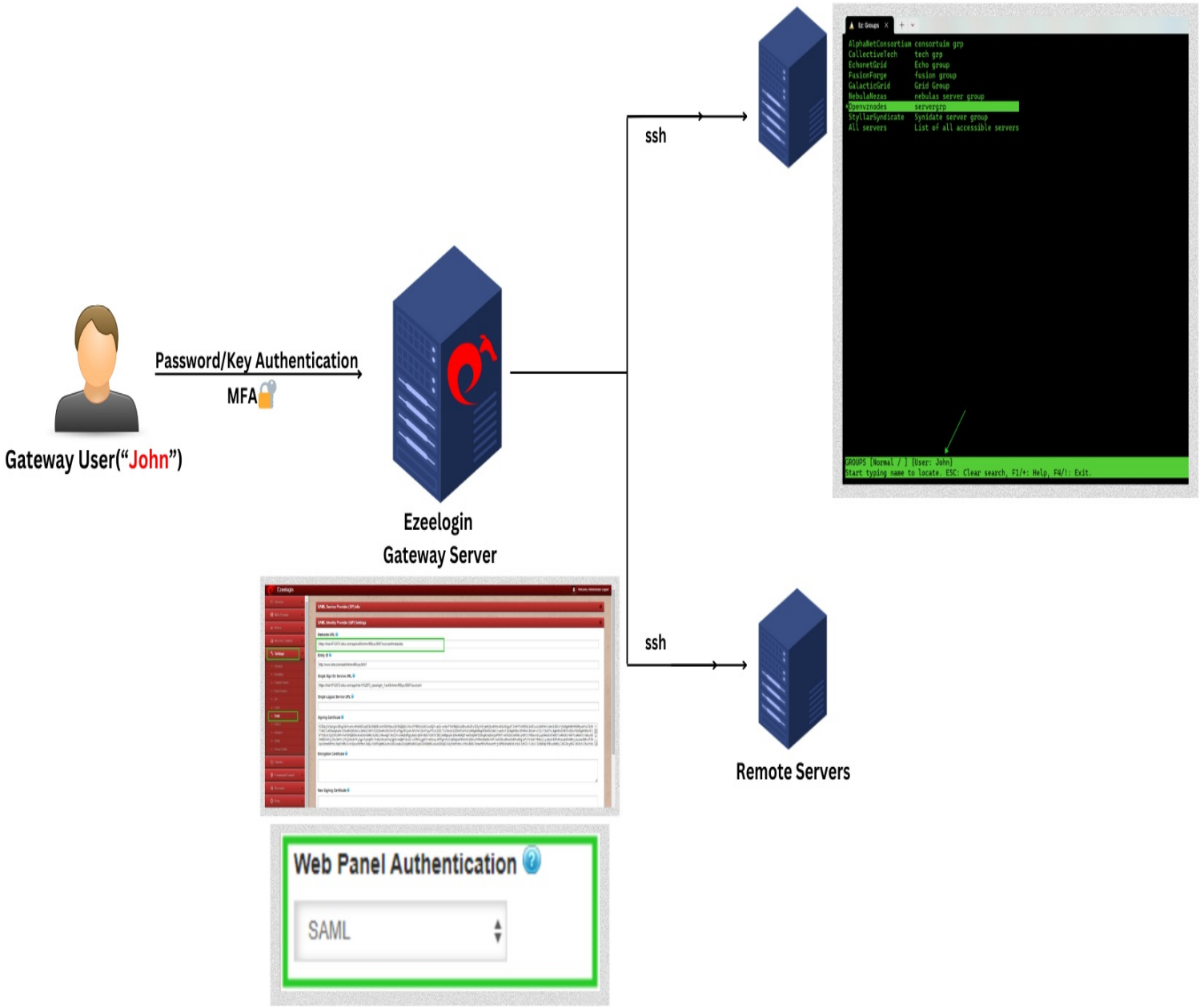
Integrate Okta SSO with jumpserver

272 Manu Chacko July 14, 2026 Tweaks & Configuration 9573

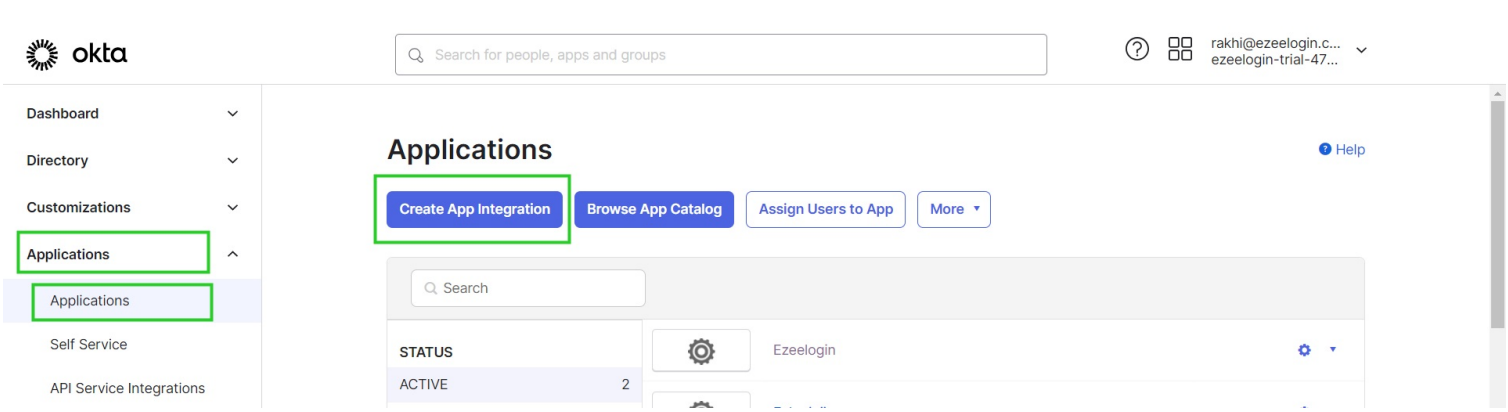
Integrating Okta Single Sign-On (SSO) with Jumpserver

Overview: This article describes integrating Okta Single Sign-On (SSO) with Jumpserver, including steps to configure Okta application settings, map SAML attributes, and enable SAML authentication in the Jumpserver GUI.

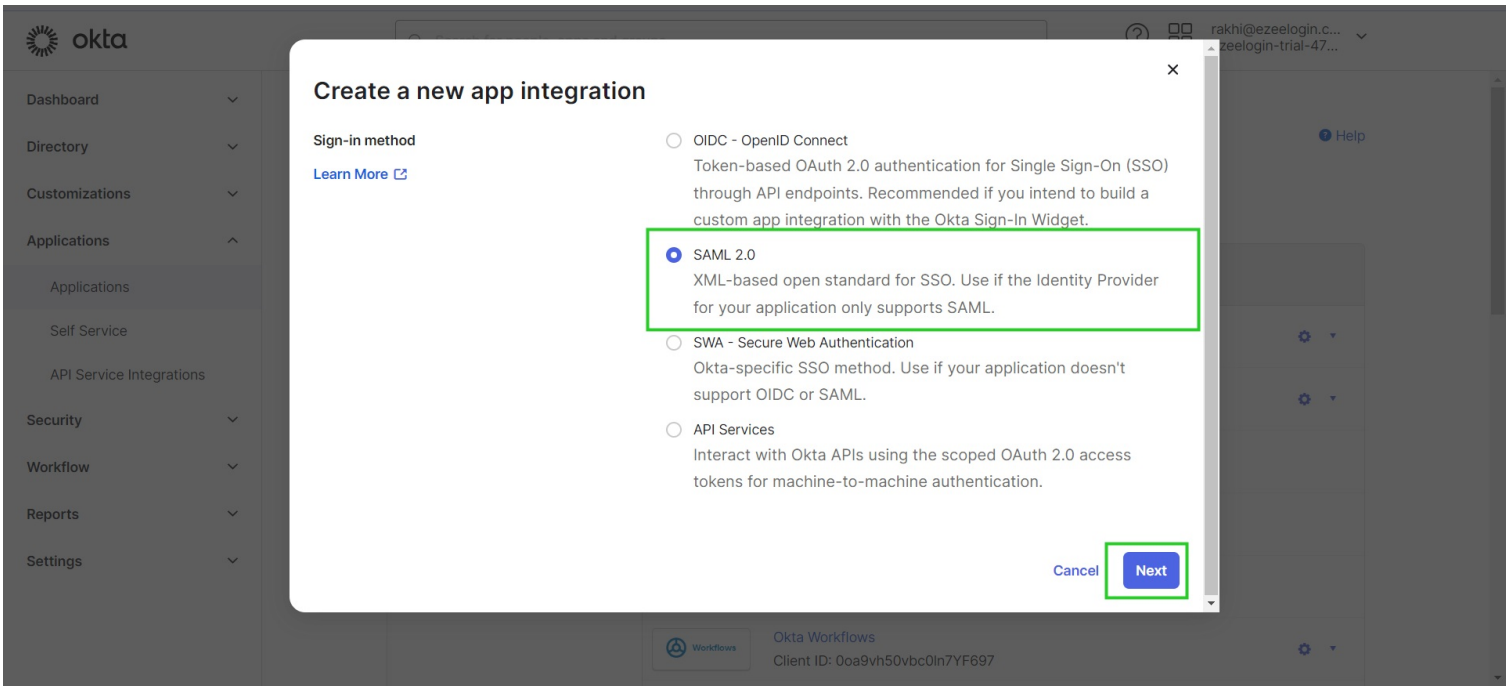
SAML is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



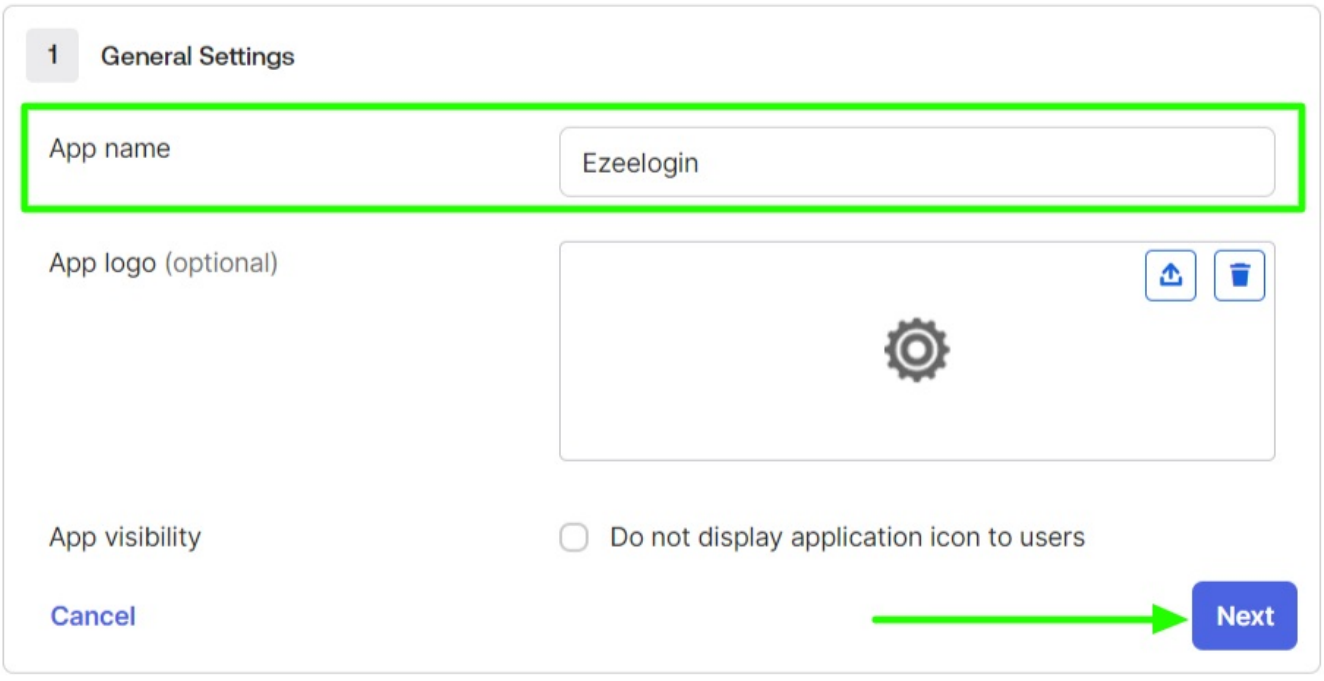
Step 1: Log in to Okta and add the Application and navigate to **Applications** -> Click on **Create App Integration**.



Step 2: Select the applications. Choose **SAML 2.0** and click **Next**.



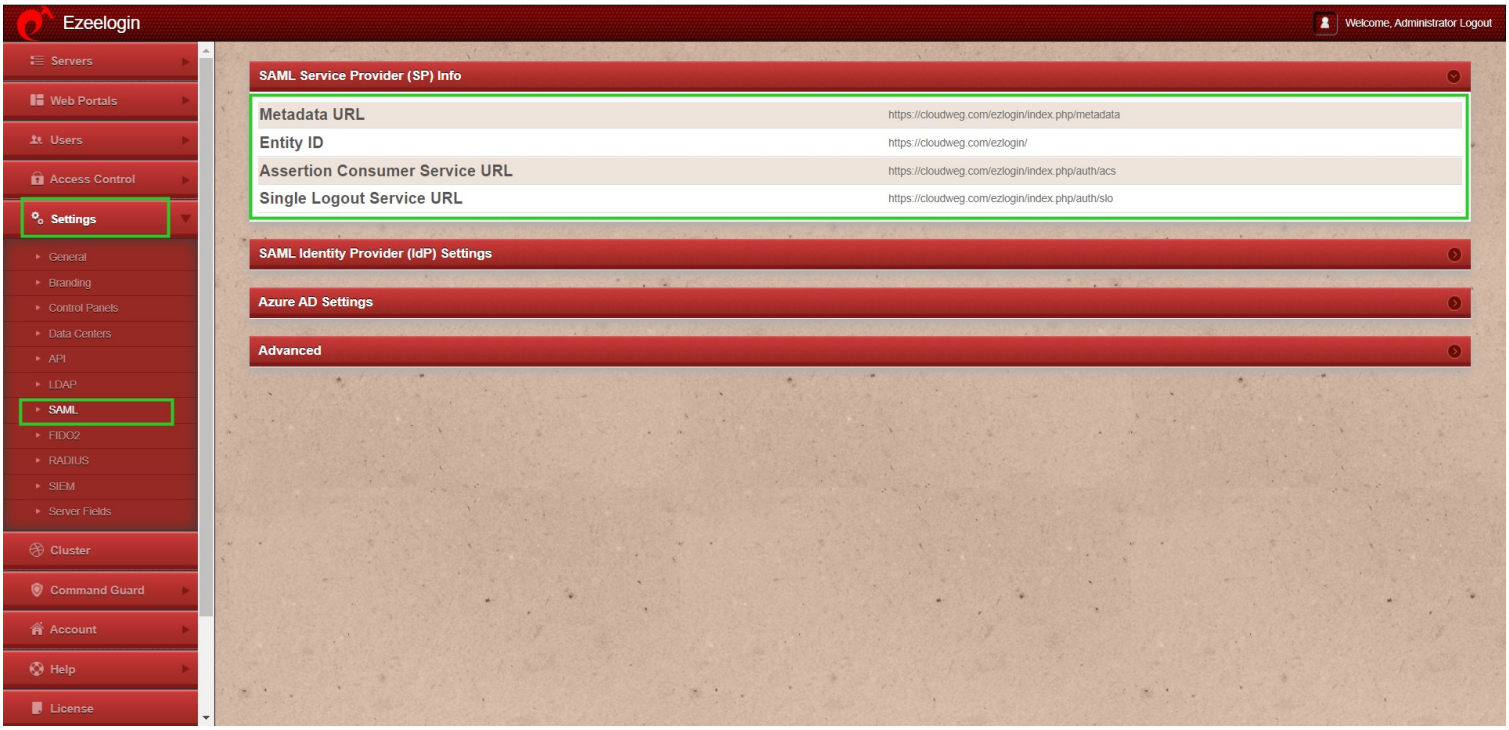
Step 3: Create SAML integration**.** Fill in the **App name** and click **Next**.

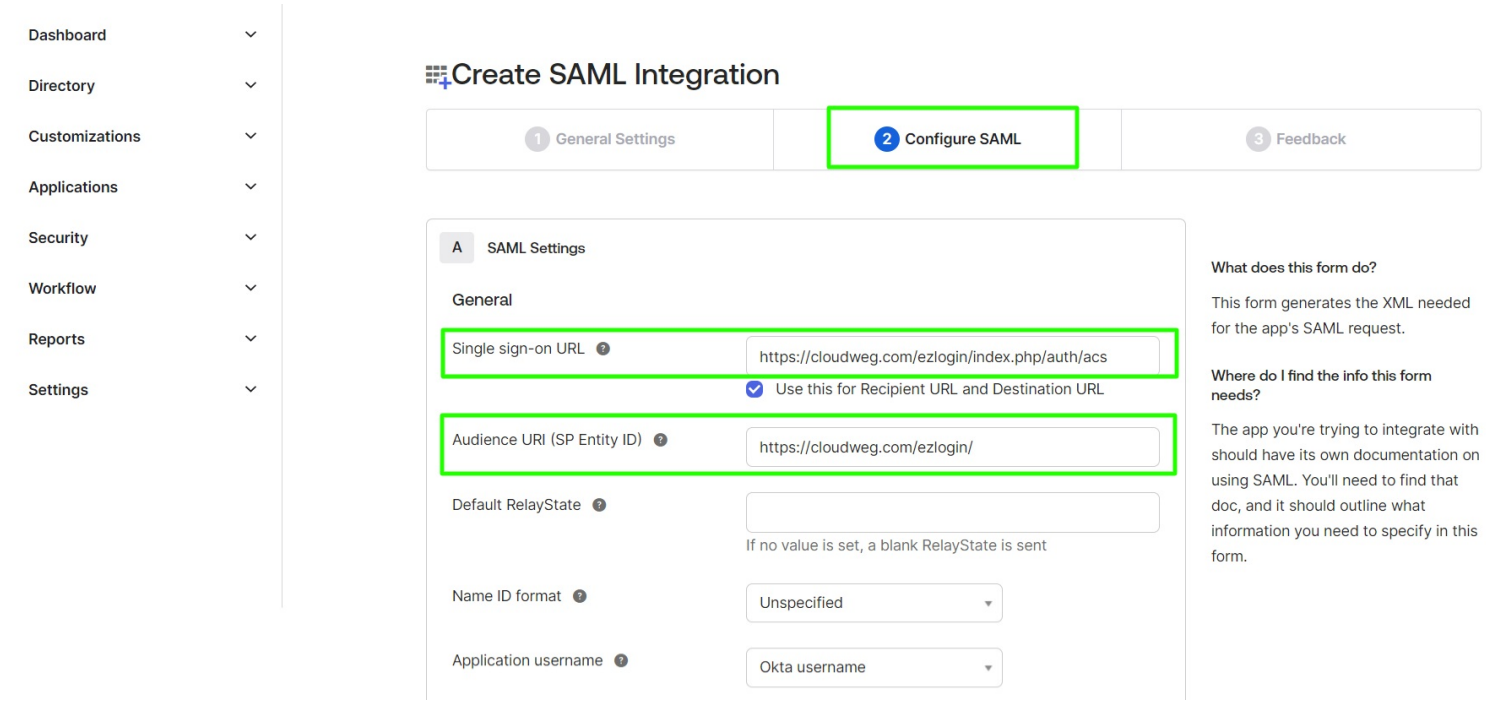


Step 4: Fill in the **SAML** setting from Ezeelogin GUI.

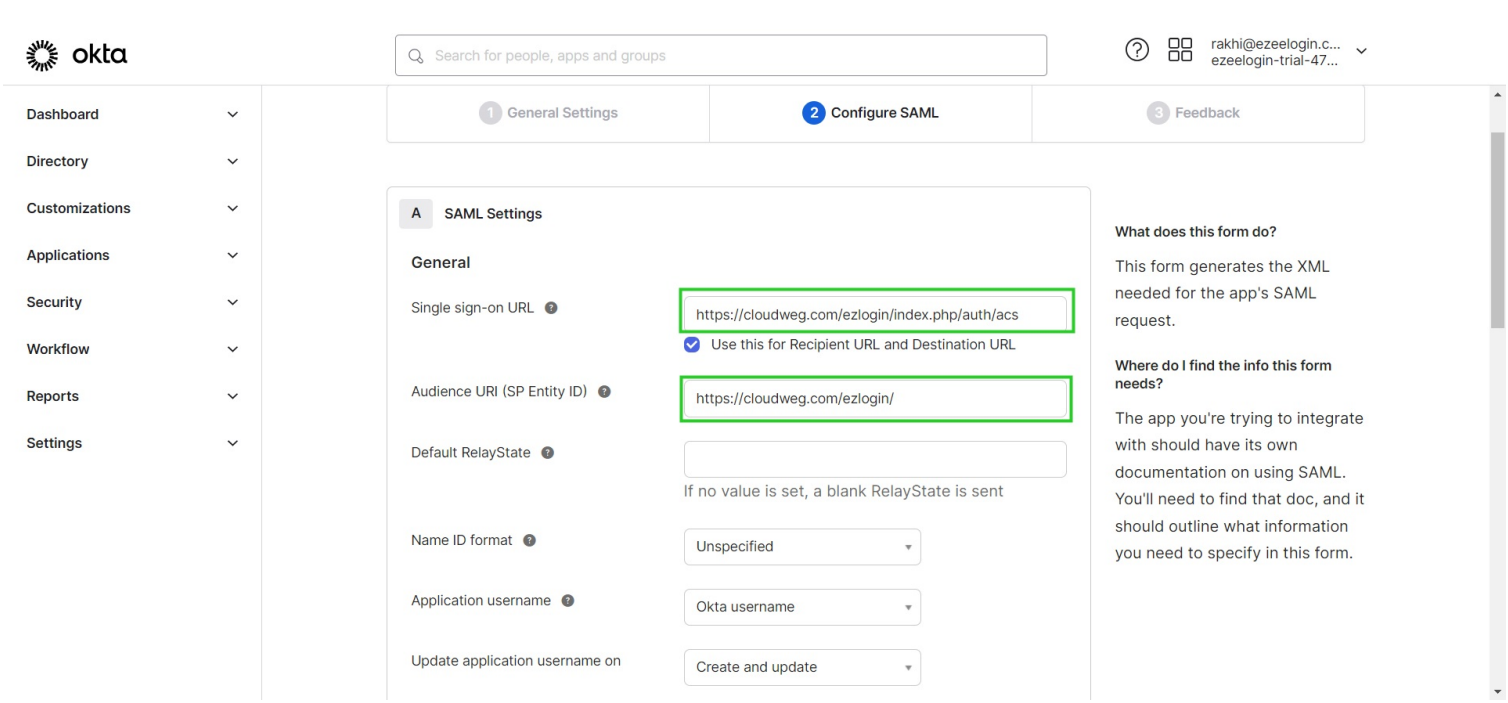
Step 4(A): Navigate to **settings** -> **SAML**. Copy **single sign-on** and **entity ID** from Ezeelogin GUI and **paste** it in the configure SAML section.

Single sign-on URL - Assertion Consumer Service URL(Find it from **Ezeelogin GUI** -> **Settings** -> **SAML** -> **Assertion Consumer Service URL**)
Audience URI (SP Entity ID) - Entity ID (Find it from **Ezeelogin GUI** -> **Settings** -> **SAML** -> **Entity ID**)





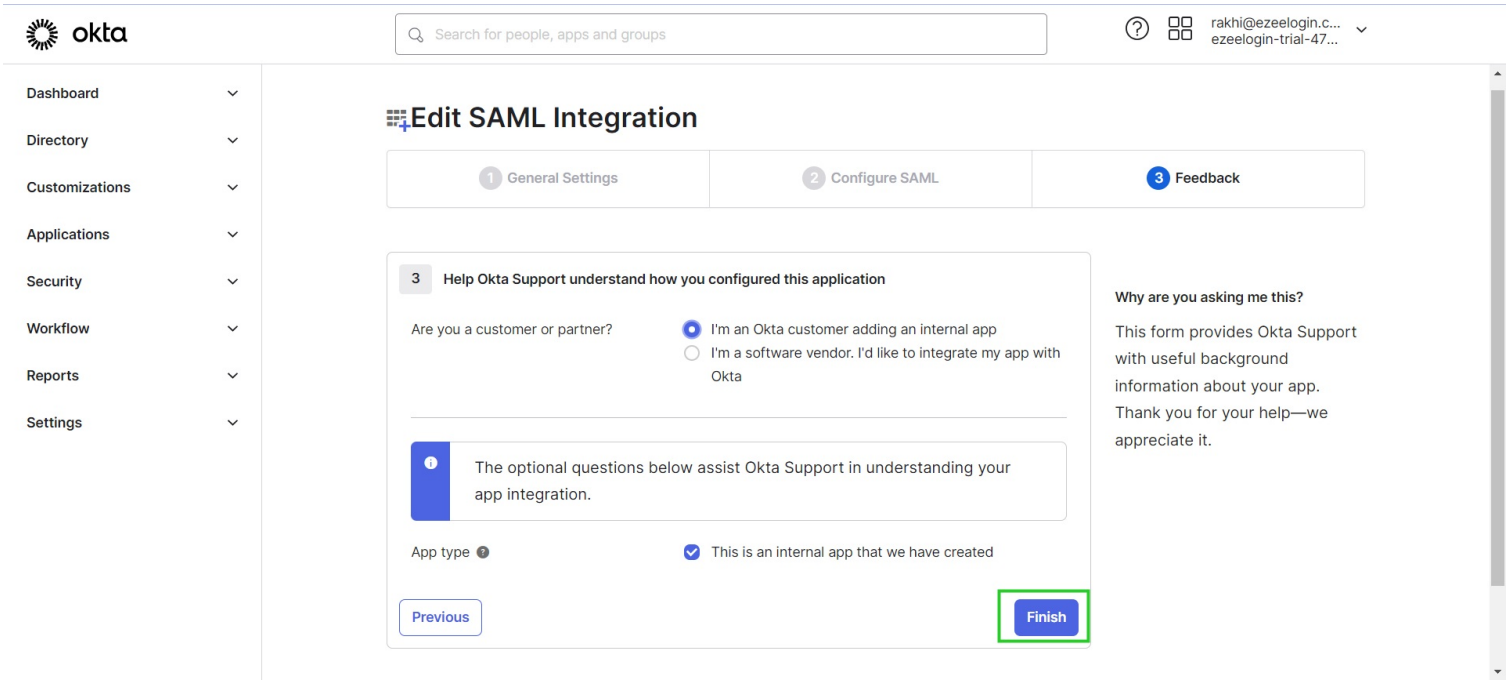
Step 5: Click on **Next** after providing the Single sign-on URL and entity ID in the SAML settings.



Step 6: Complete Okta Application Setup.

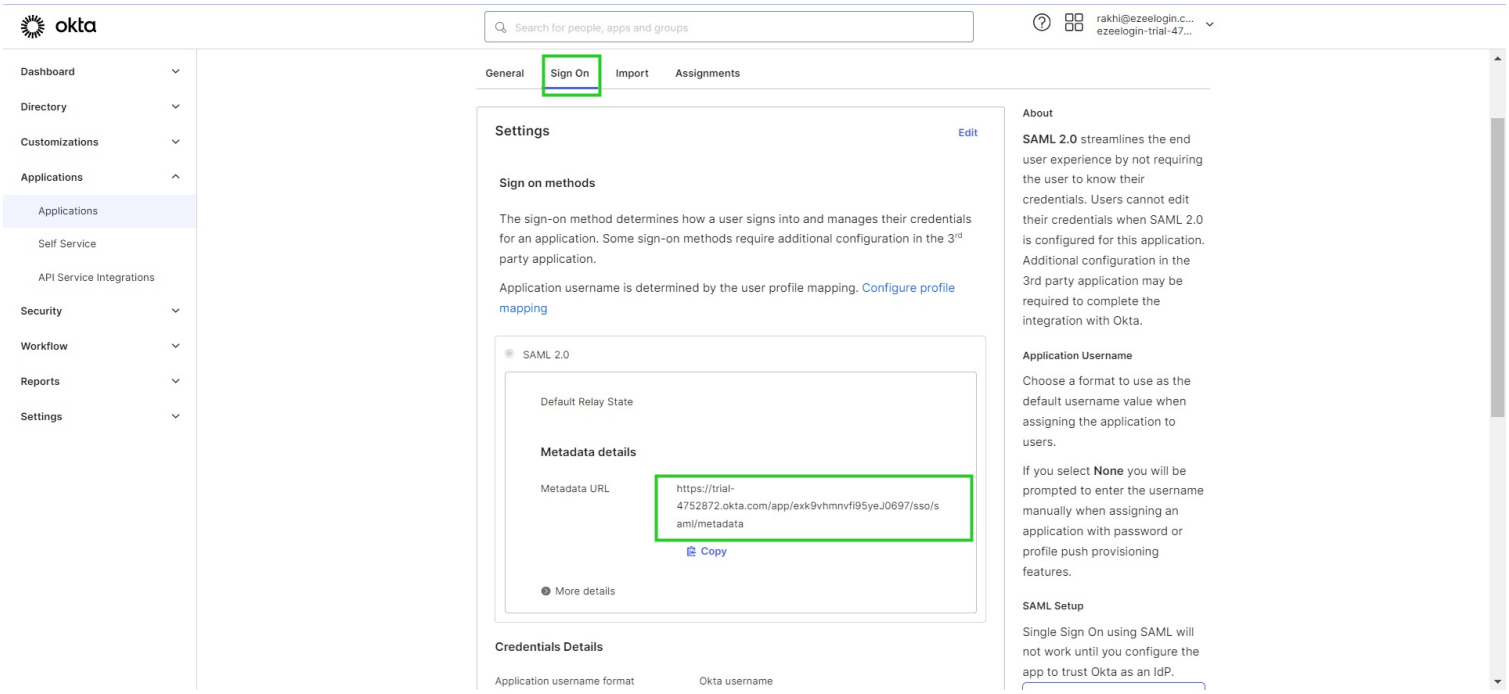
Step 6(A): Check "**I'm an Okta customer adding an internal app**" & "**This is an internal app that we have created**" and click **Finish**.

Step 6(B): On the next page, you can see the setup instructions.

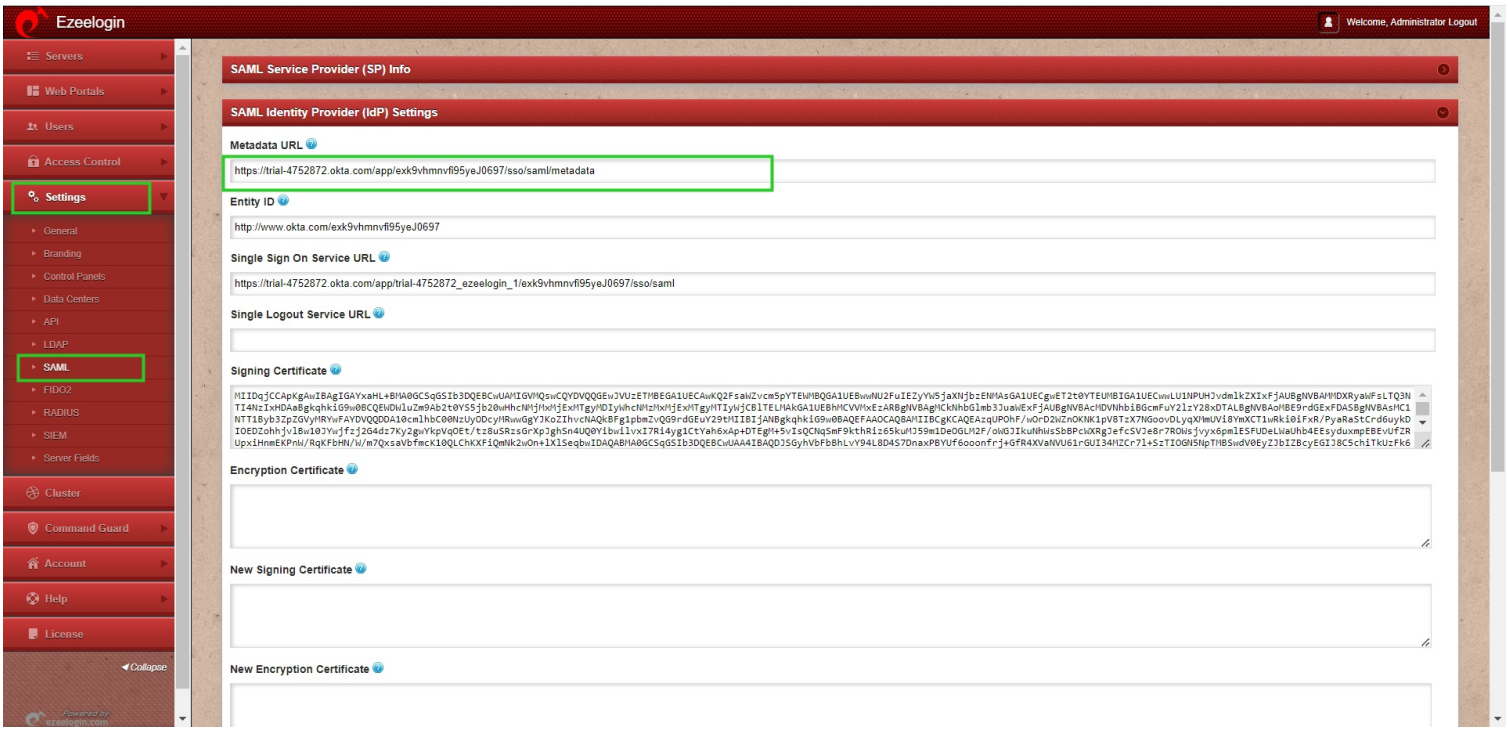


Step 7: Copy Metadata URL.

Step 7(A): Under the Sign On option, you can find the **metadata URL** which you can copy and paste into Ezeelogin GUI.

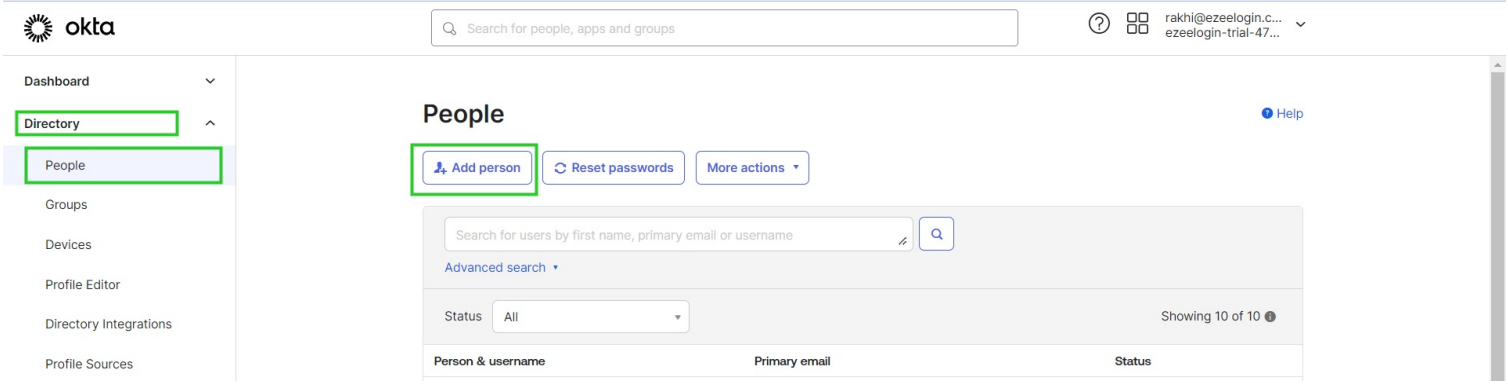


Step 7(B): Copy the URL of the page and paste it to the Metadata URL on **Ezeelogin GUI** -> **Settings** -> **SAML Metadata URL** and click on the **Fetch** button, it will autofill the SAML settings and Save it.



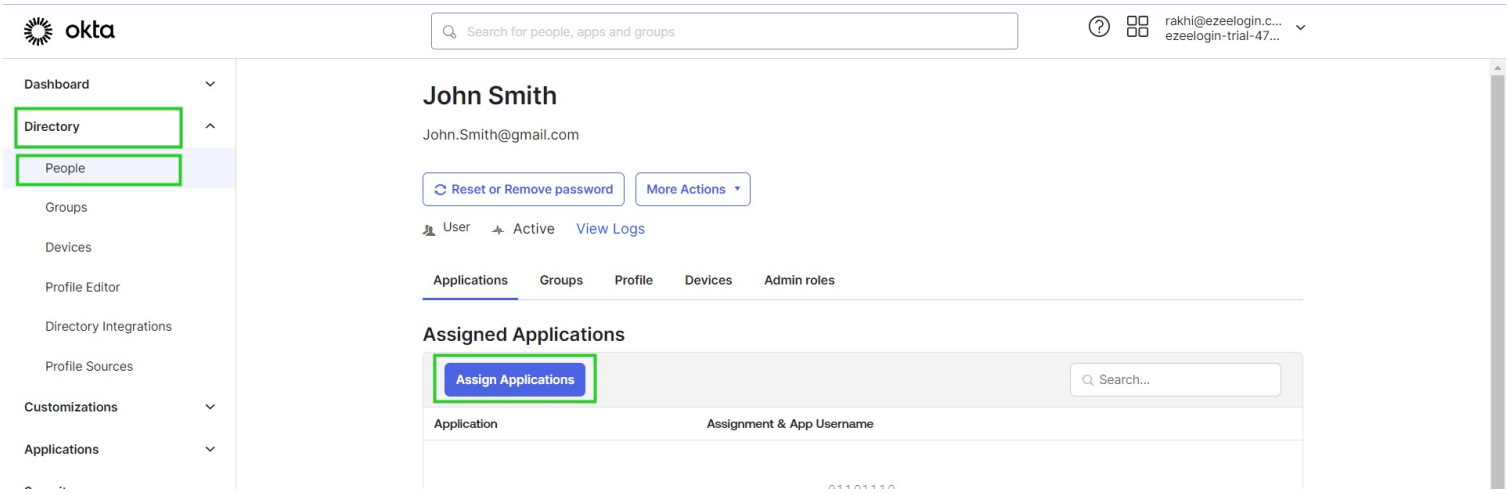
Step 8: Add Users.

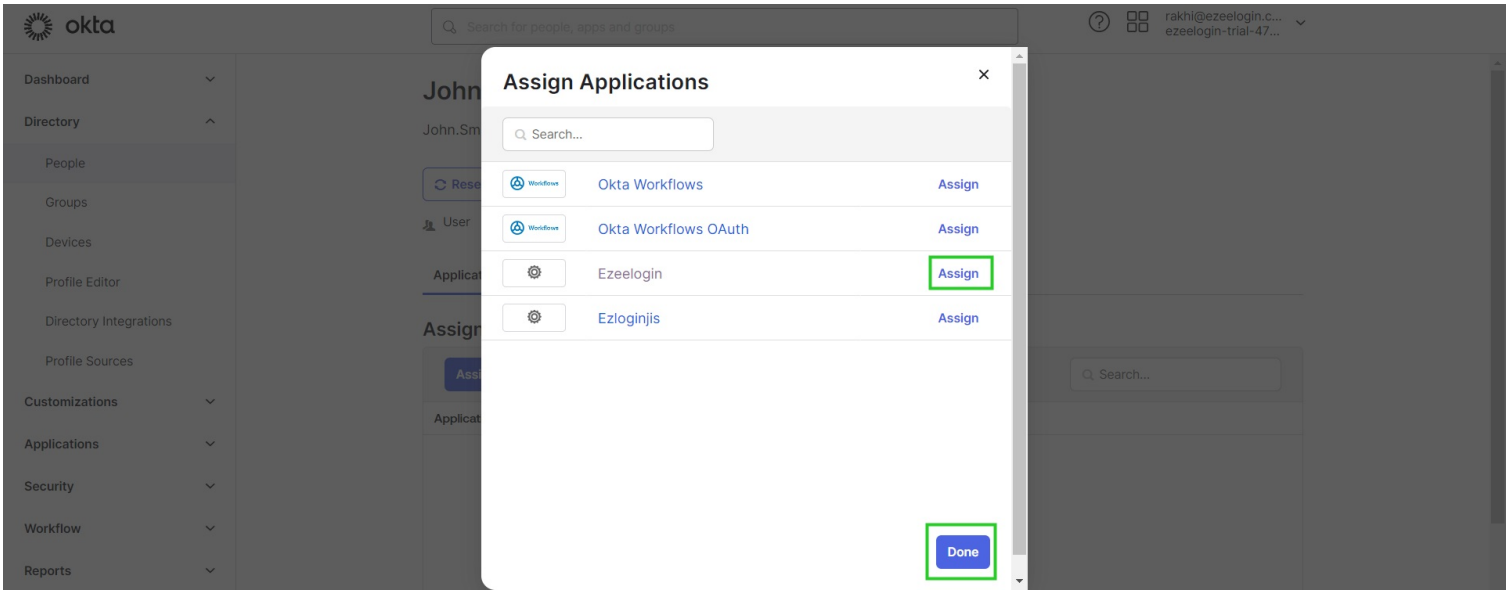
Step 8(A): In Okta Go to **Directory** -> **People** from the left panel and select **Add Person** to add a user in OKTA.

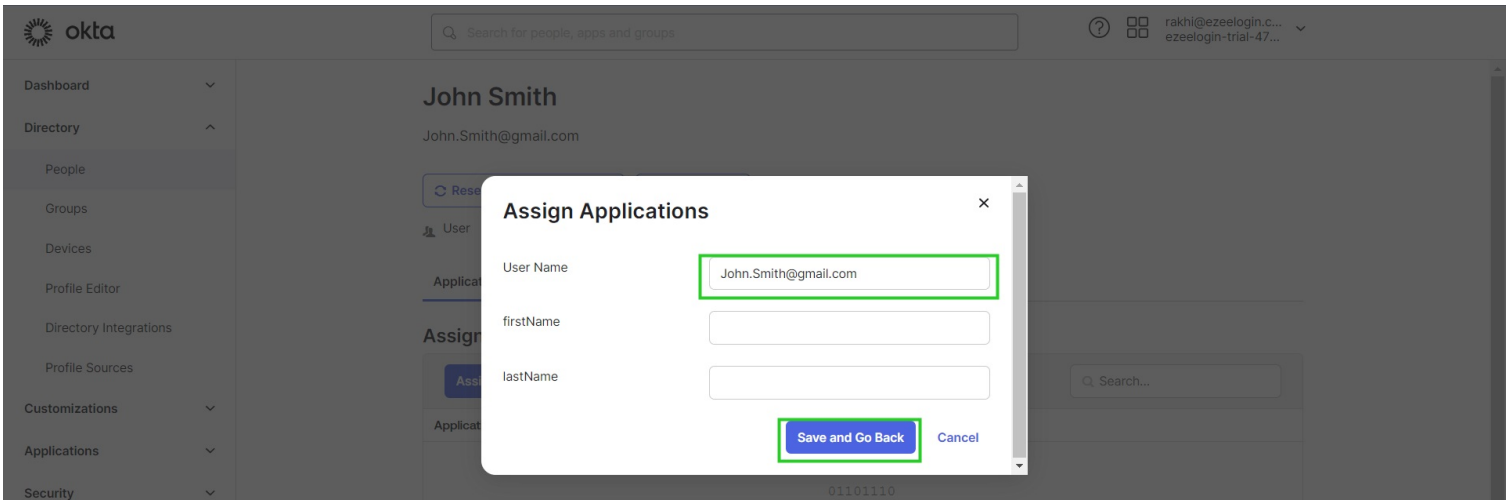


Step 9: Assign users to the application.

Step 9(A): Assign the user to the application by clicking the user in the **people tab**.

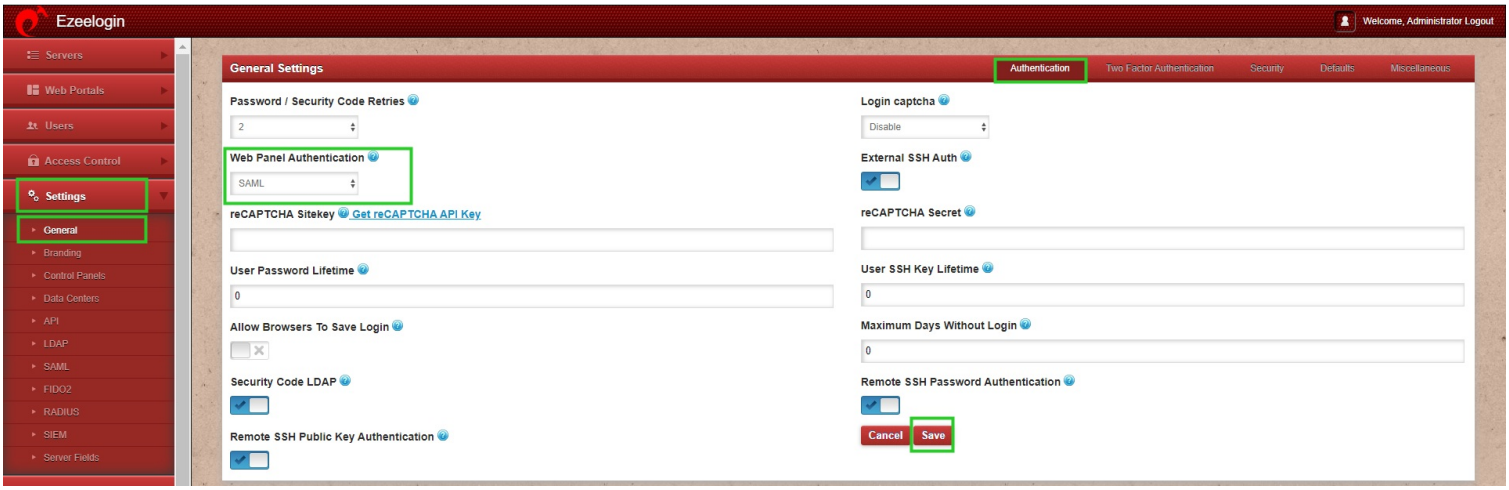




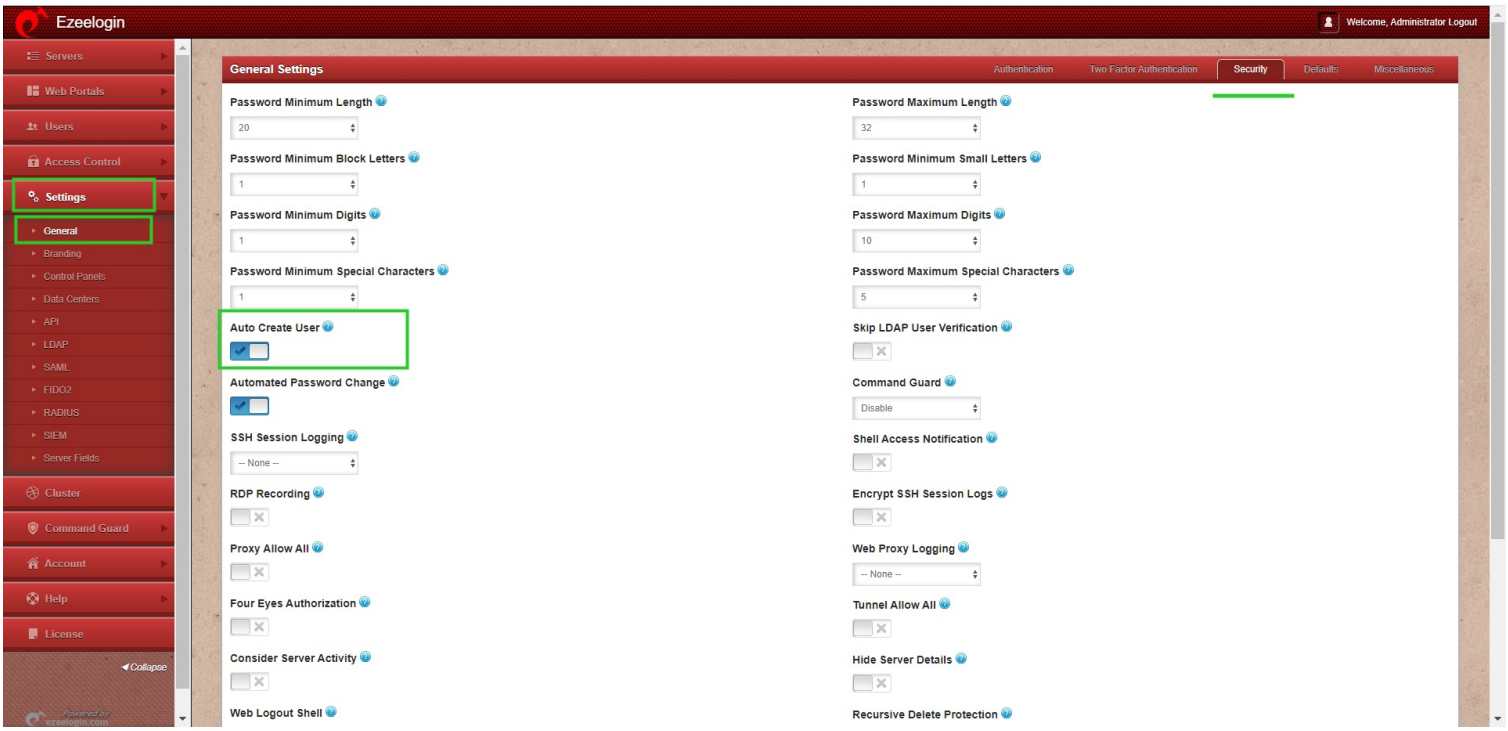


Step 10: Configure JumpServer.

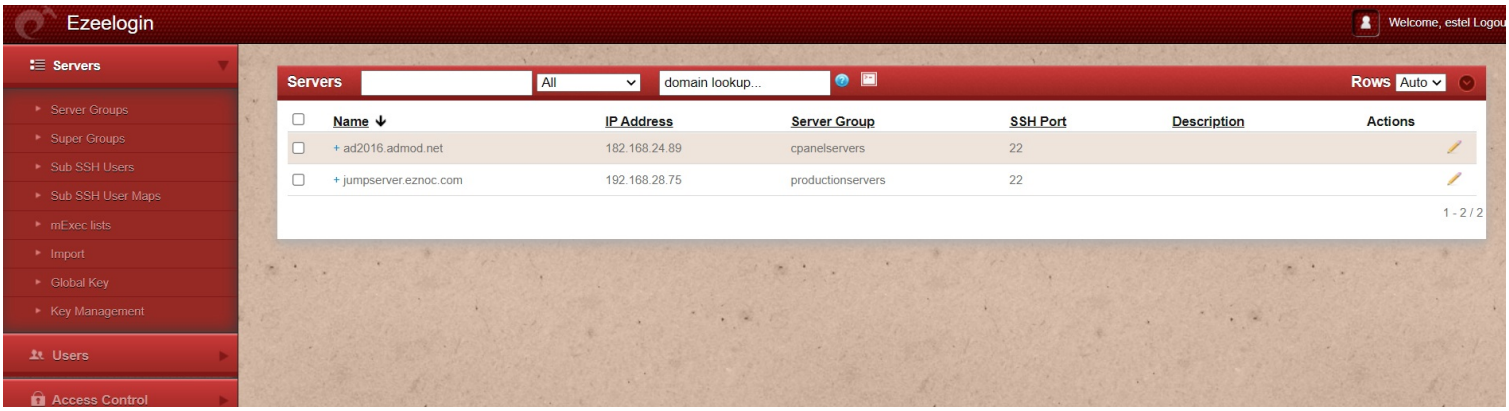
Step 10(A): Change **Web panel Authentication** to **SAML** from **Ezeelogin GUI** -> **Settings** -> **General** -> **Authentication** -> **Web Panel Authentication.**



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



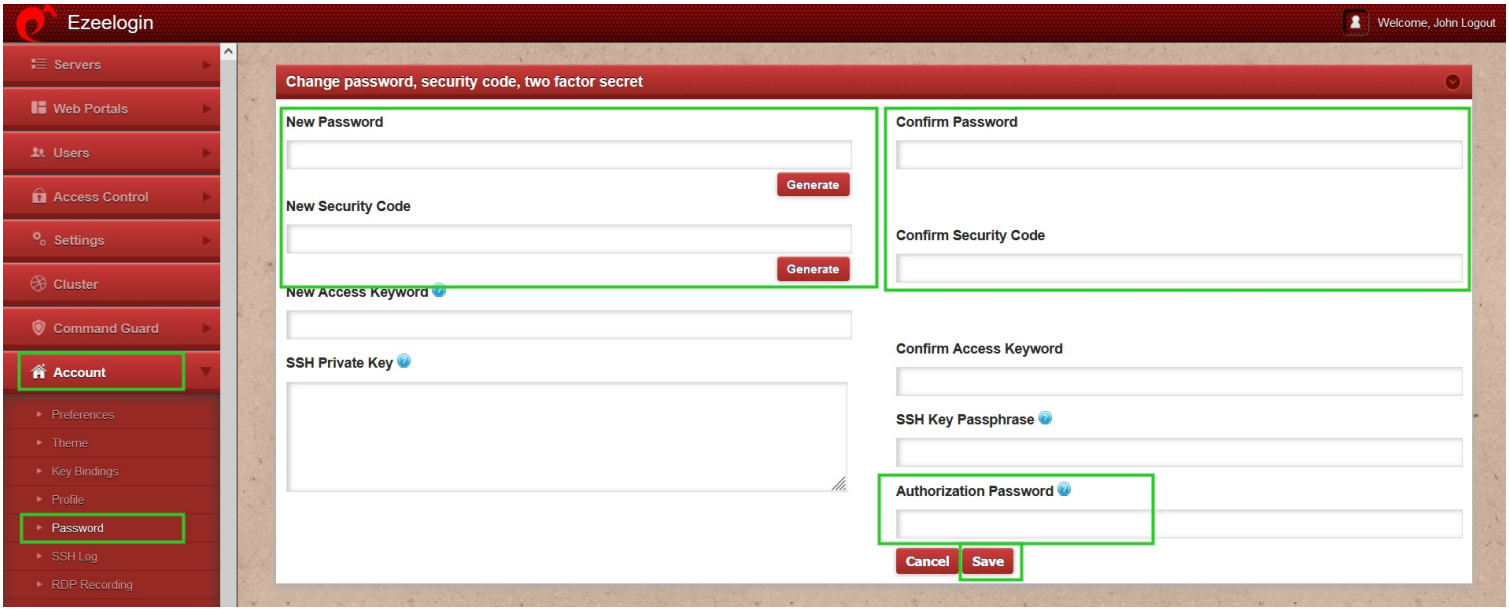
Step 12: Log in to Ezeelogin GUI with **SAML** authentication.



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

Error: Invalid password

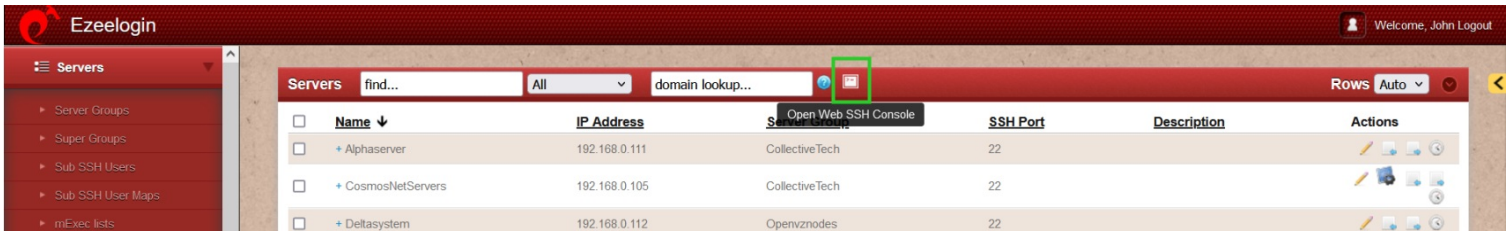
Step 13: After logging into GUI, you need to **reset** the **password** and **security code** of the SAML user under **Account** -> **Password** in order to SSH to Ezeelogin backend(ezsh).



Step 14: SSH access.

Step 14(A): Log in to Ezeelogin shell via Webssh shell or using any SSH client such as Putty or terminal etc.

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

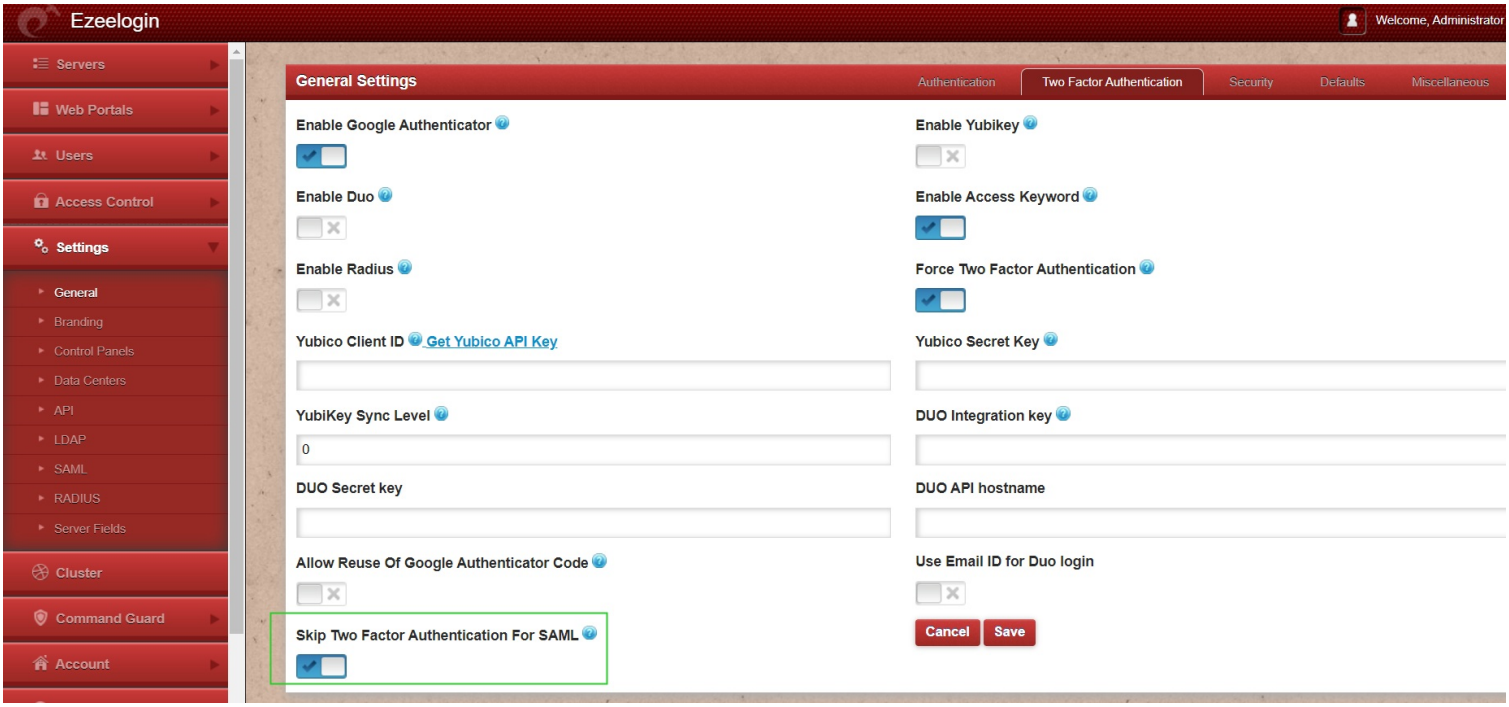


WebSSH terminal will open like below. Users can navigate the server group with the **Up and Down** arrow buttons and **enter** to log into the server.

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

Step 15: Managing 2fa.

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** -> **Skip 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.

Refer article to map Okta attribute to Ezeelogin:

Map Okta attributes to Ezeelogin

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

Related Articles:

Map Okta attributes to Ezeelogin.

Login as superadmin when SSO is enabled globally

Map existing user group from SAML provider to ezeelogin.

Online URL: https://www.ezeelogin.com/kb/article/integrate-okta-sso-with-jumpserver-272.html