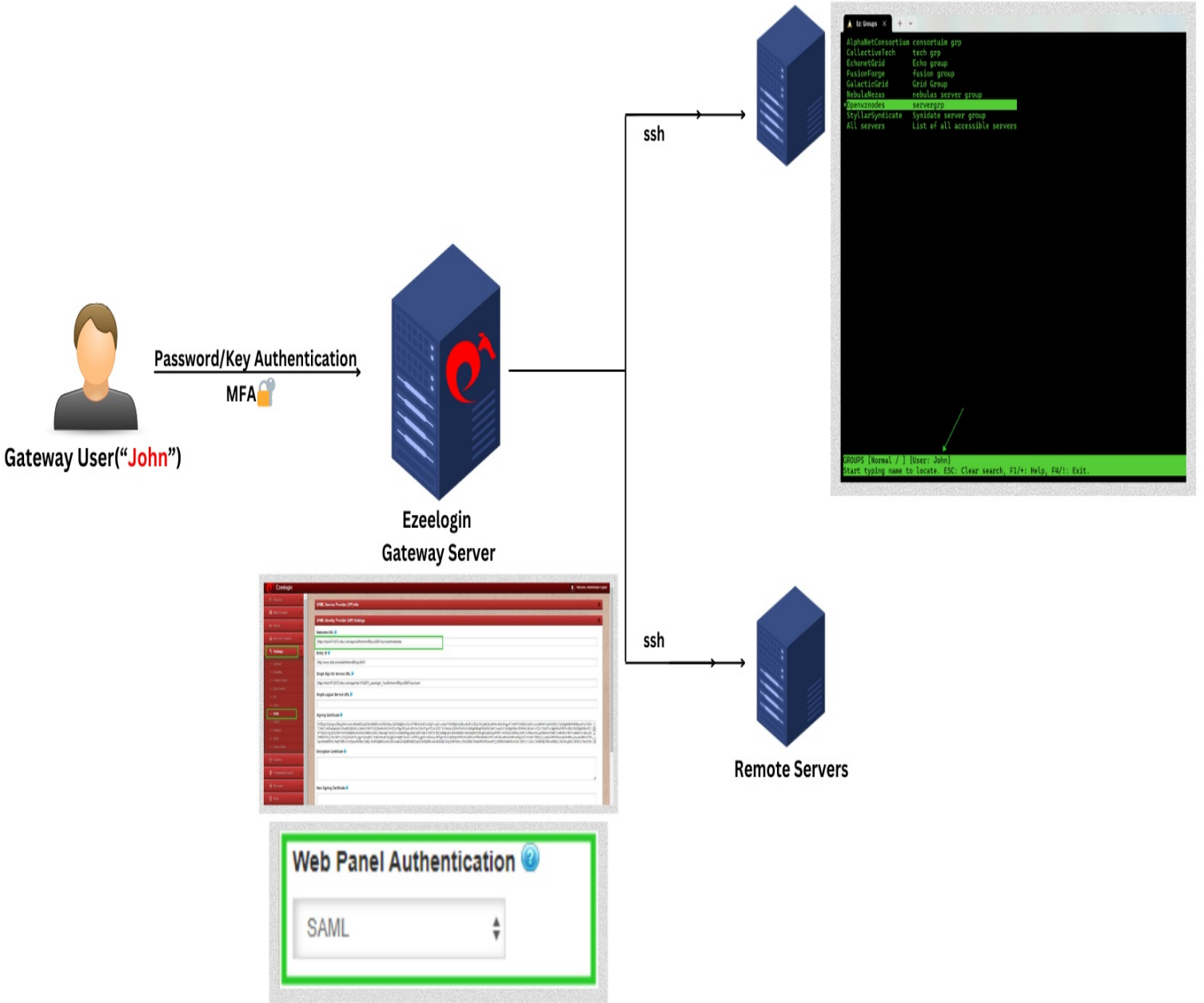


Integrate Okta SSO with jumpserver

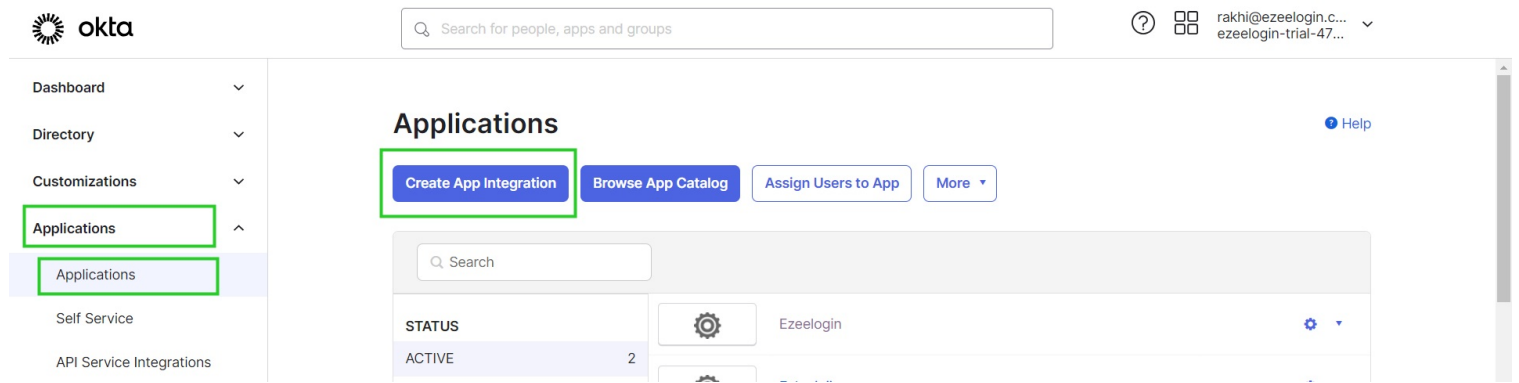
Integrating Okta Single Sign-On (SSO) with Jumpserver

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.

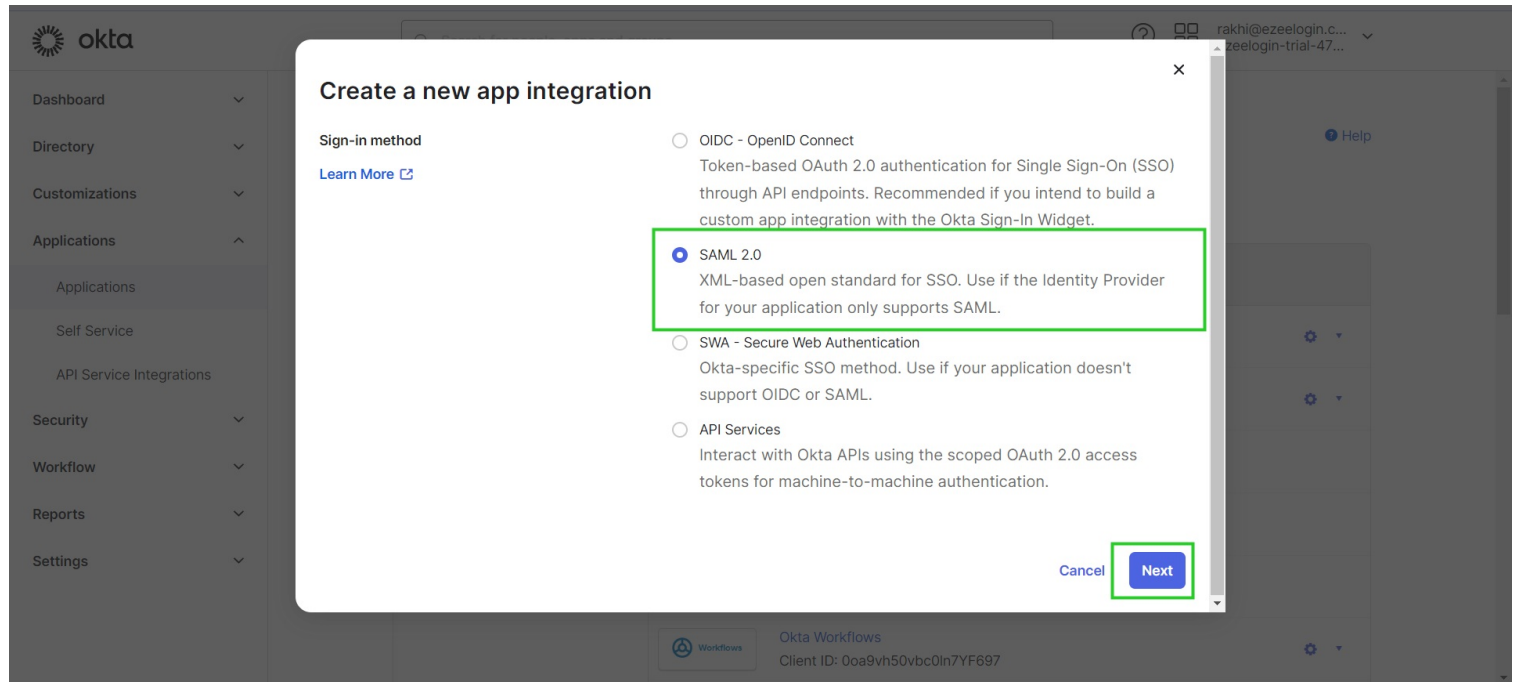
SAML is an authentication mechanism for web applications. It's based on web protocols and it cannot be used for user authentication over SSH.



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**.

1 General Settings

App name

App logo (optional)

App visibility ☐ Do not display application icon to users

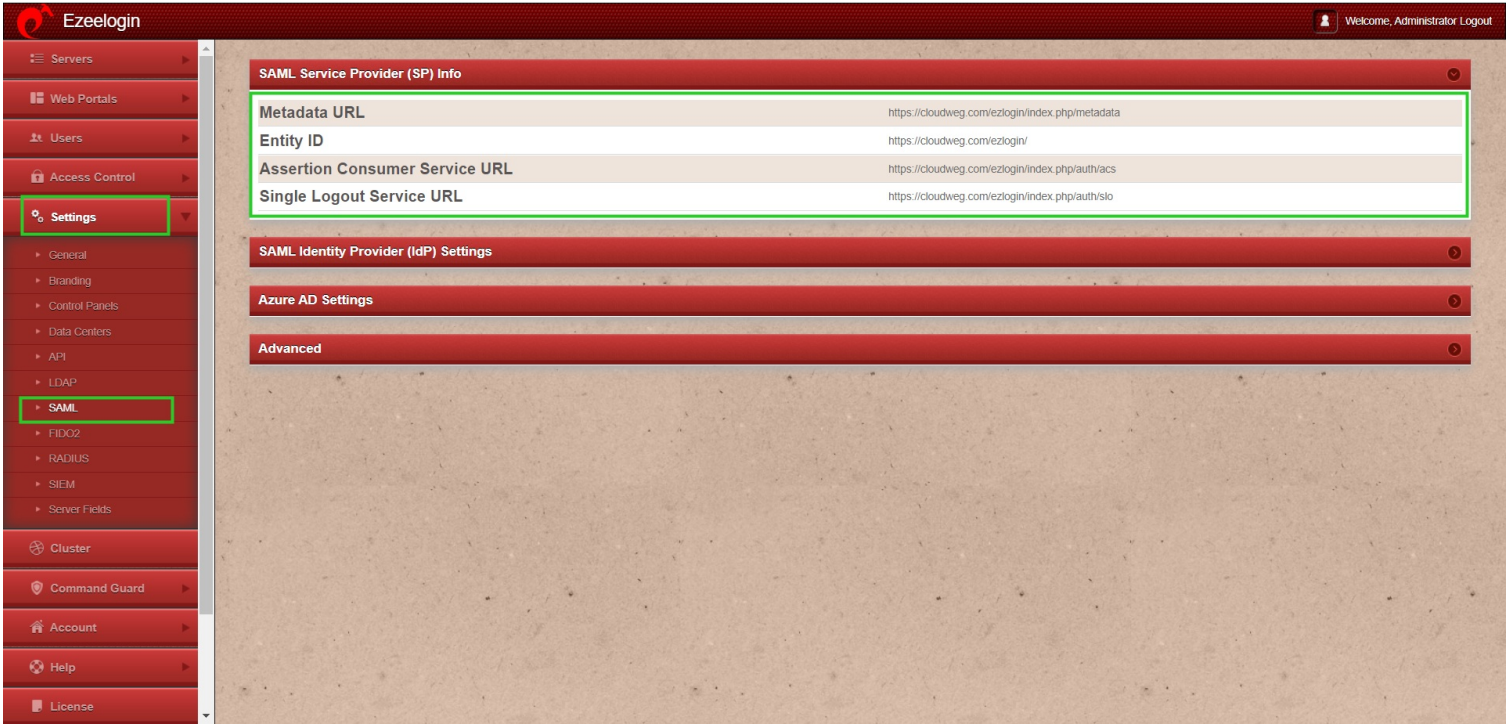
[Cancel](#) [Next](#)

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**)



Dashboard

Directory

Customizations

Applications

Security

Workflow

Reports

Settings

Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

A SAML Settings

General

Single sign-on URL

https://cloudweg.com/ezlogin/index.php/auth/acs

Audience URI (SP Entity ID)

https://cloudweg.com/ezlogin/

Default RelayState

If no value is set, a blank RelayState is sent

Name ID format

Unspecified

Application username

Okta username

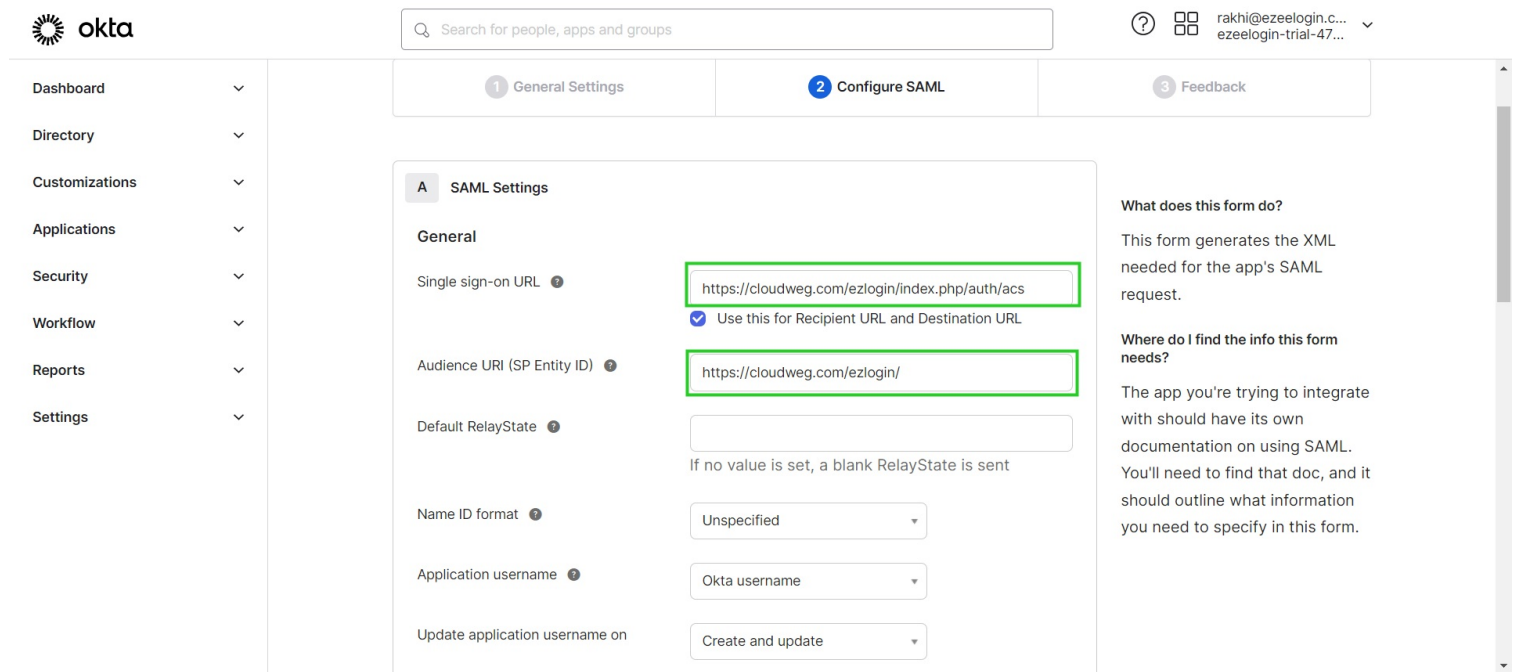
What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

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



The image shows the 'Configure SAML' step in the Okta application setup process. The left sidebar contains navigation links: Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'SAML Settings' and includes a 'General' section with the following fields: 'Single sign-on URL' (https://cloudweg.com/ezlogin/index.php/auth/acs), 'Audience URI (SP Entity ID)' (https://cloudweg.com/ezlogin/), 'Default RelayState' (empty), 'Name ID format' (Unspecified), 'Application username' (Okta username), and 'Update application username on' (Create and update). A checkbox 'Use this for Recipient URL and Destination URL' is checked. A right-hand panel provides explanatory text about the form's purpose and where to find necessary information. The top navigation bar includes the Okta logo, a search bar, and user information.

Okta

Search for people, apps and groups

1 General Settings 2 Configure SAML 3 Feedback

A SAML Settings

General

Single sign-on URL  https://cloudweg.com/ezlogin/index.php/auth/acs

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID)  https://cloudweg.com/ezlogin/

Default RelayState 

If no value is set, a blank RelayState is sent

Name ID format  Unspecified

Application username  Okta username

Update application username on Create and update

What does this form do?

This form generates the XML needed for the app's SAML request.

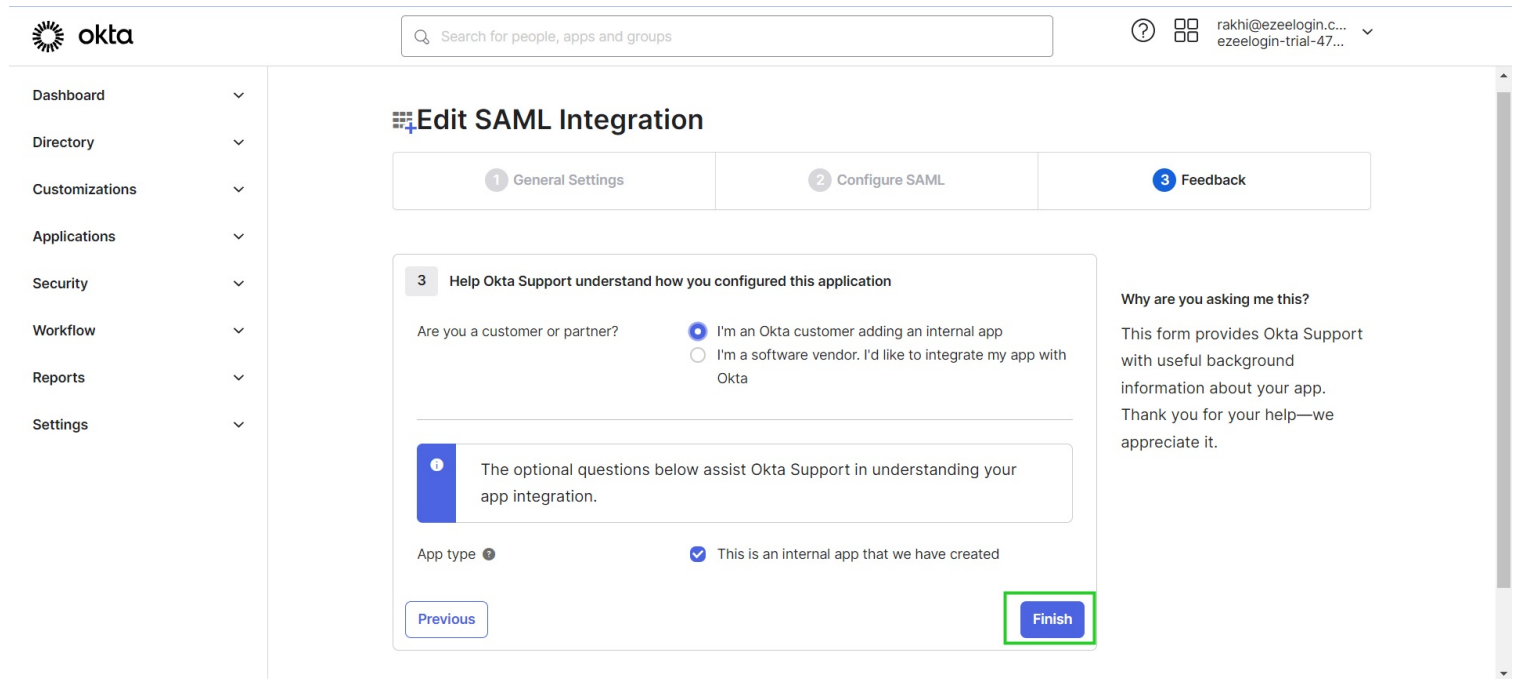
Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

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.



The image shows the 'Edit SAML Integration' page in the Okta application setup process. The left sidebar contains navigation links: Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Edit SAML Integration' and includes a 'Help Okta Support understand how you configured this application' section. This section contains two radio buttons for 'Are you a customer or partner?' (selected: 'I'm an Okta customer adding an internal app'), a text box for 'The optional questions below assist Okta Support in understanding your app integration.', and a checkbox 'This is an internal app that we have created' which is checked. At the bottom, there are 'Previous' and 'Finish' buttons. A right-hand panel provides explanatory text about the form's purpose. The top navigation bar includes the Okta logo, a search bar, and user information.

Okta

Search for people, apps and groups

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner? ☒ I'm an Okta customer adding an internal app ☐ I'm a software vendor. I'd like to integrate my app with Okta

 The optional questions below assist Okta Support in understanding your app integration.

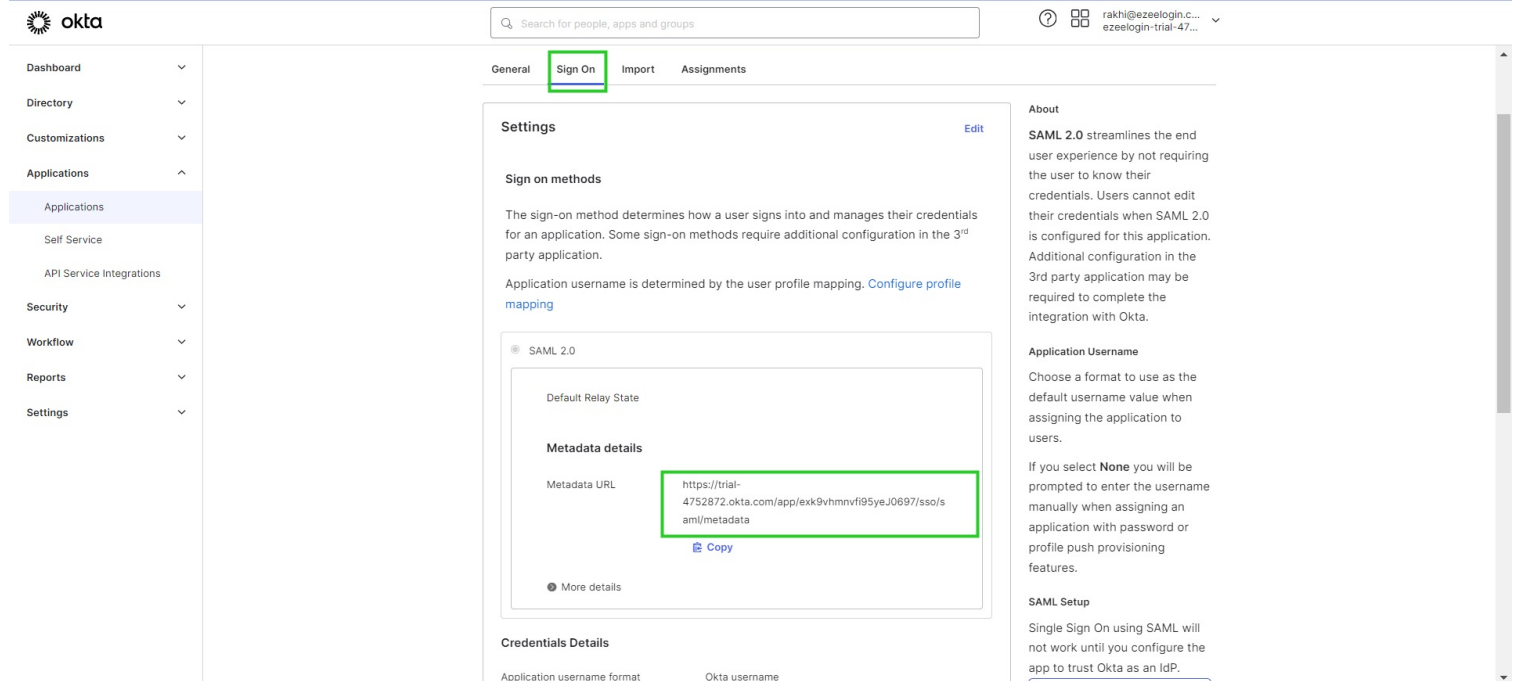
App type  ☒ This is an internal app that we have created

Why are you asking me this?

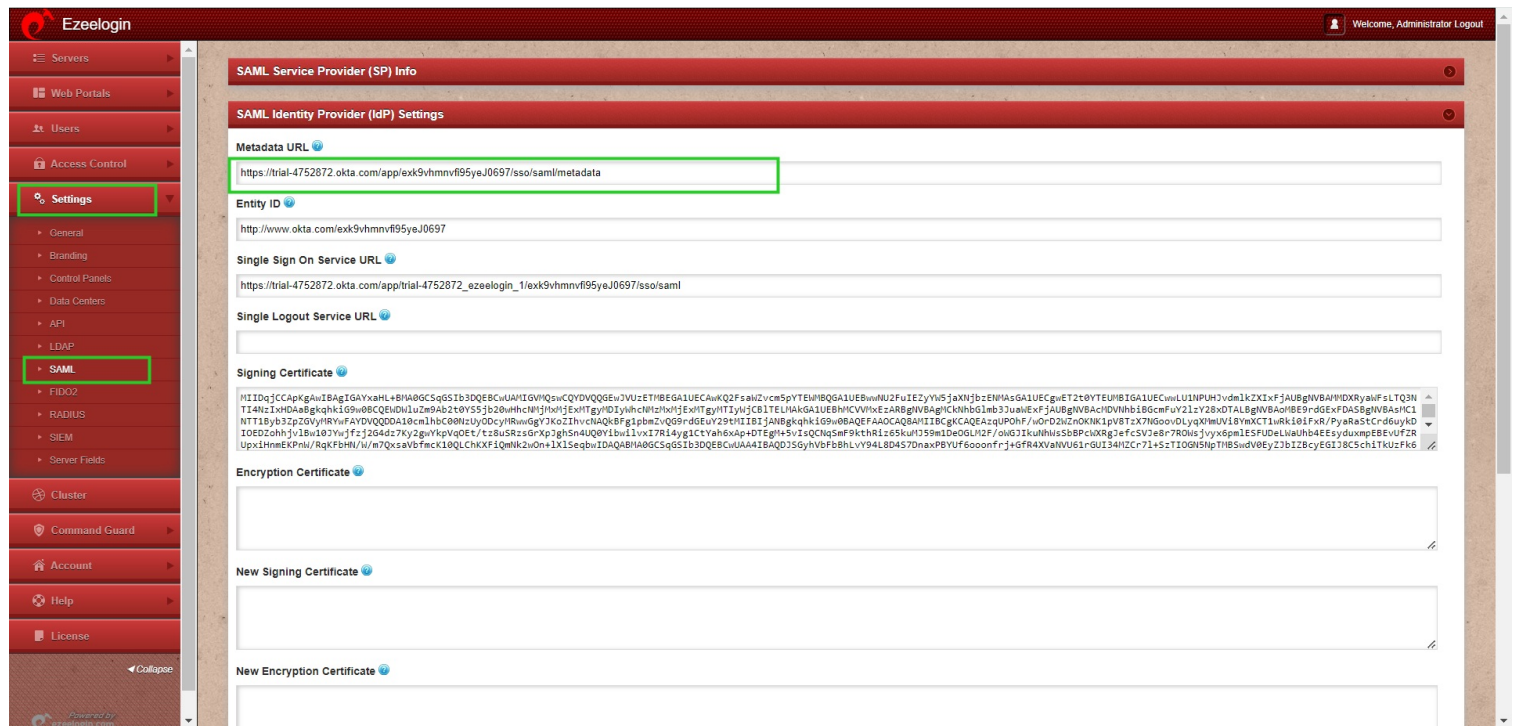
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

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.

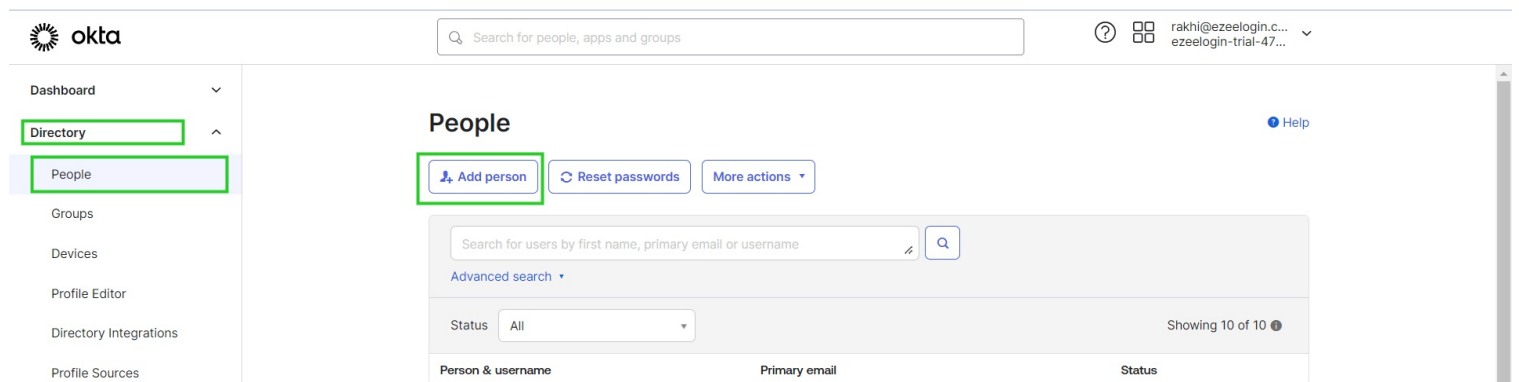


Step 7(B): Copy the URL of the page and paste it to the Metadata URL on **Ezeelogin GUI -> Settings -> SAML Metadata URL** and click on the **Fetch** button, it will autofill the SAML settings and Save it.



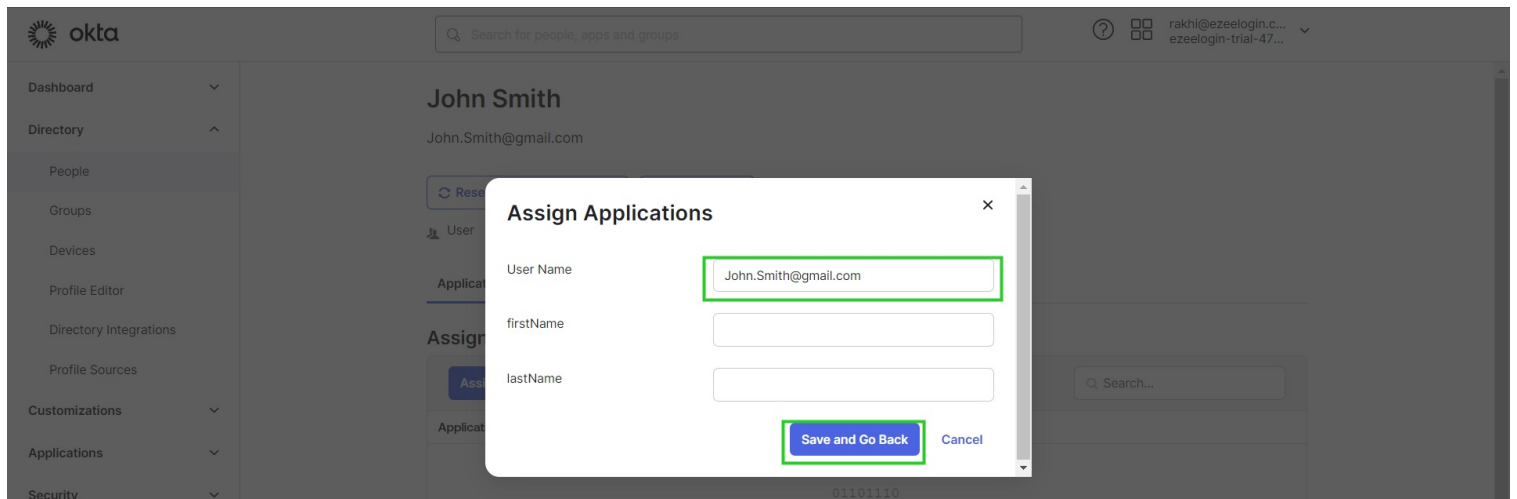
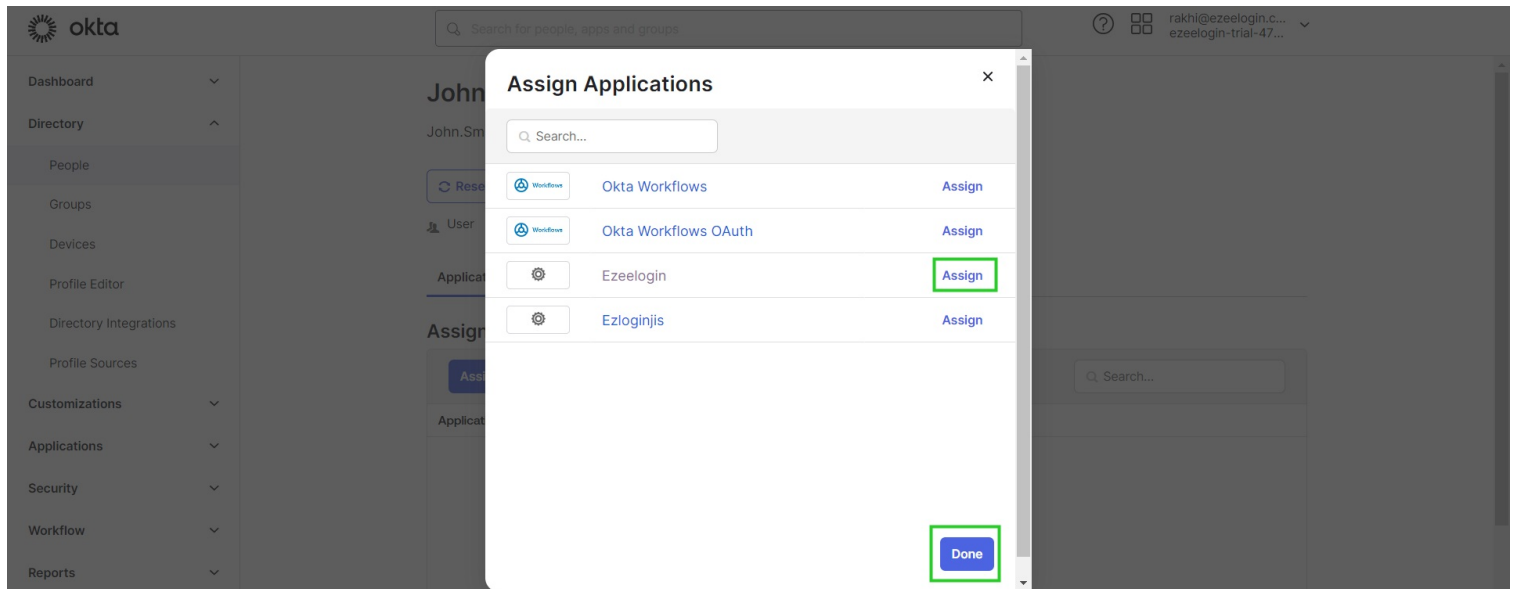
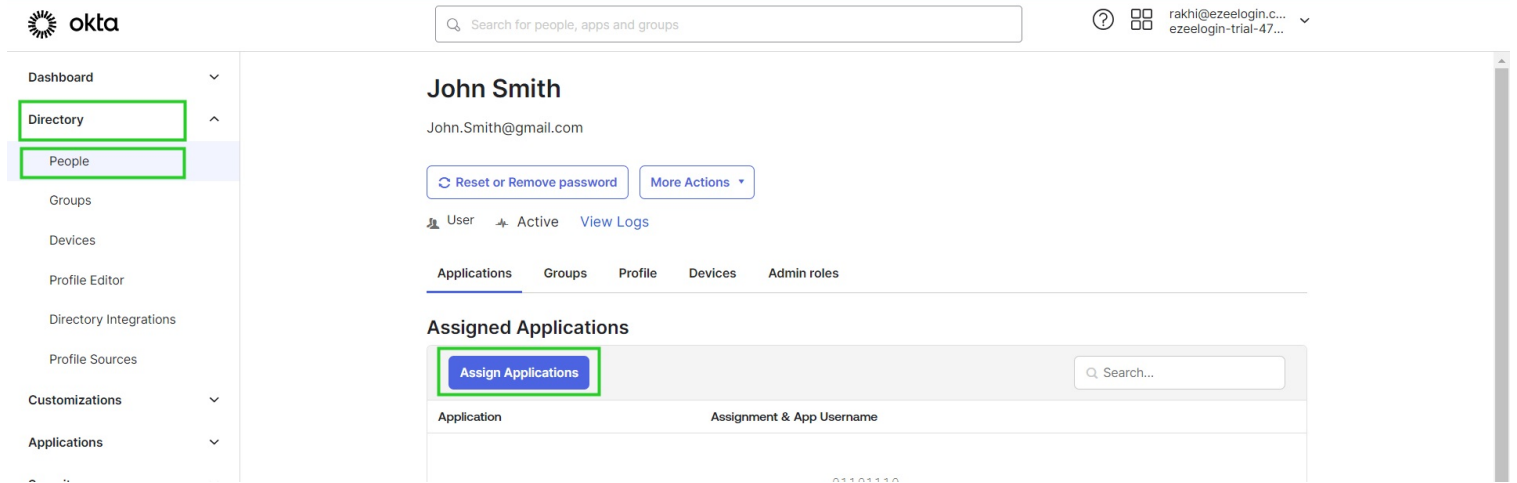
Step 8: Add Users.

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



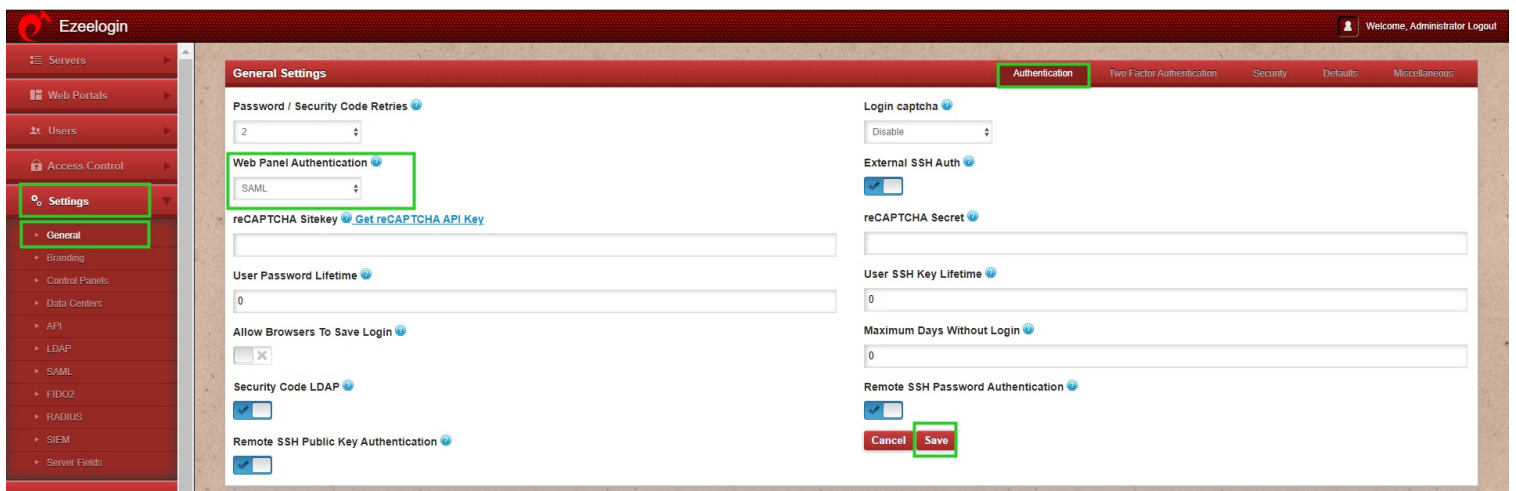
Step 9: Assign users to the application.

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

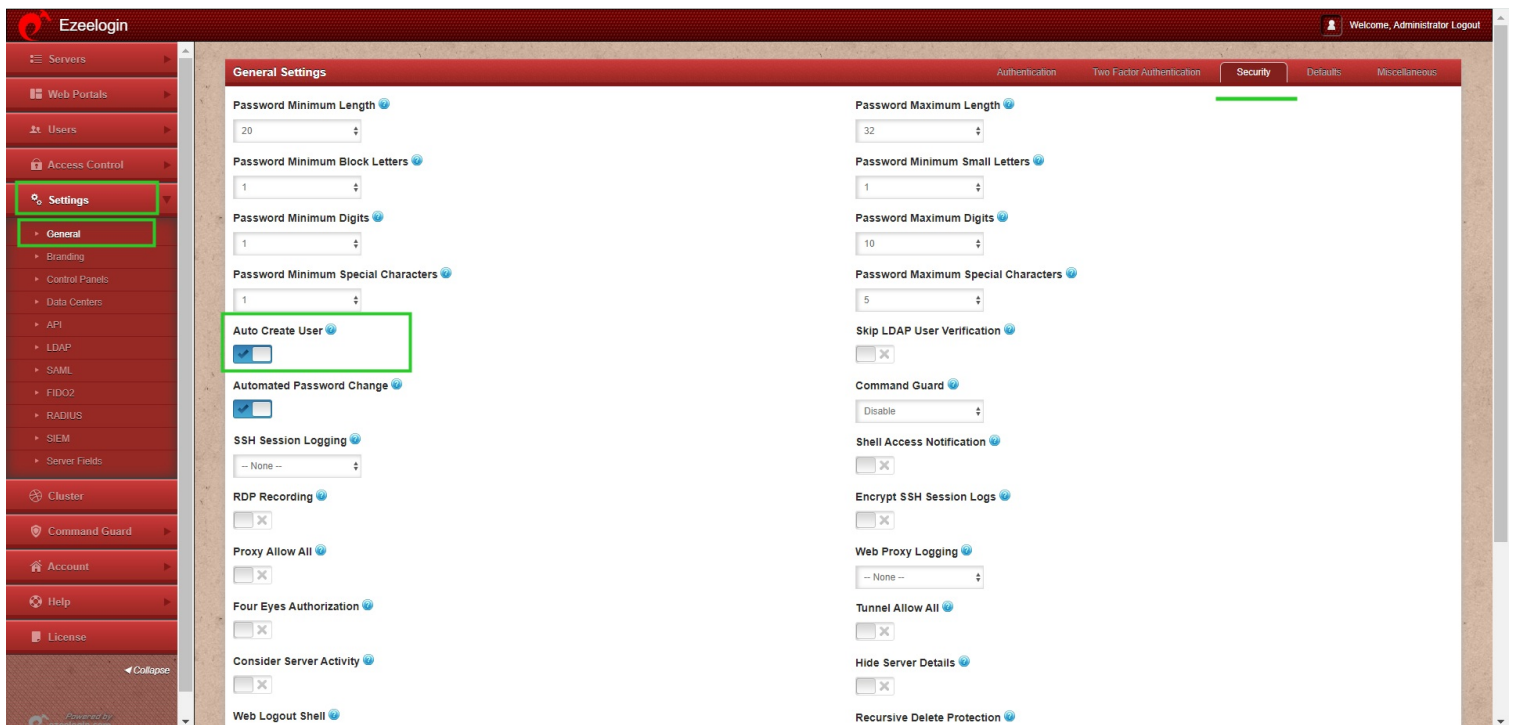


Step 10:Configure JumpServer.

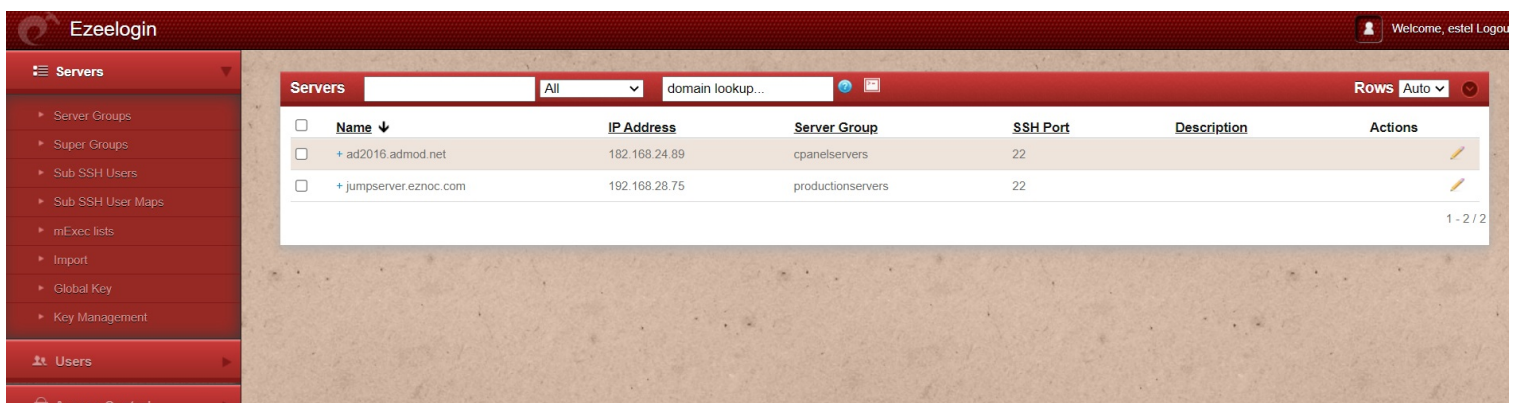
Step 10(A): Change **Web panel Authentication** to **SAML** from **Ezeelogin GUI** -> **Settings** -> **General** -> **Authentication** -> **Web Panel Authentication**.



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.

Name	IP Address	Open Web SSH Console	SSH Port	Description	Actions
+ Alphaserver	192.168.0.111	CollectiveTech	22		
+ CosmosNetServers	192.168.0.105	CollectiveTech	22		
+ Deltasystem	192.168.0.112	Openvznodes	22		

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.

```
AlphaNetConsortium consortium grp
CollectiveTech tech grp
EchonetGrid Echo group
FusionForge fusion group
GalacticGrid Grid Group
NebulaNezas nebula server group
*Openvznodes servergrp
StyllarSyndicate Synidate server group
All servers List of all accessible servers
```

```
GROUPS [Normal / ] (User: John)
Start typing name to locate. ESC: Clear search, F1/+: Help, F4/!: Exit.
```

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**.

```
root@AD-LAPLEN-11:~# ssh John@192.168.0.110
John@192.168.0.110's password: |
```

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**.

The screenshot shows the Ezeelogin web interface. On the left is a sidebar menu with options like Servers, Web Portals, Users, Access Control, Settings, Cluster, Command Guard, and Account. The 'Settings' menu is expanded, showing sub-options like General, Branding, Control Panels, Data Centers, API, LDAP, SAML, RADIUS, and Server Fields. The main content area is titled 'General Settings' and has tabs for 'Authentication', 'Two Factor Authentication', 'Security', 'Defaults', and 'Miscellaneous'. The 'Two Factor Authentication' tab is active. It contains various settings for enabling/disabling authentication methods like Google Authenticator, Duo, Radius, Yubikey, and Access Keyword. At the bottom of this tab, the 'Skip Two Factor Authentication For SAML' option is checked and highlighted with a green rectangular box. There are also input fields for Yubico Client ID, Yubico Secret Key, DUO Integration key, and DUO API hostname, along with buttons for 'Cancel' and 'Save'.

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>