

Integrate Jumpcloud SSO with Ezeelogin

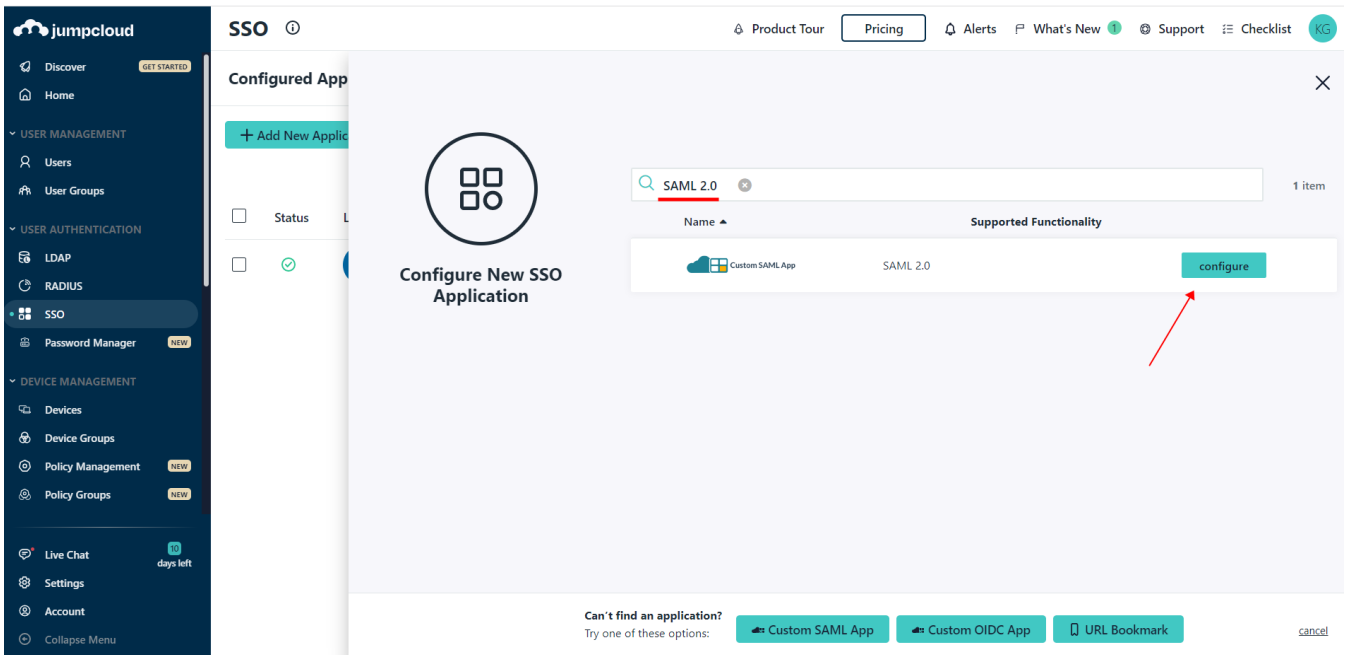
599 admin October 25, 2024 [Features & Functionalities](#) 2672

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.

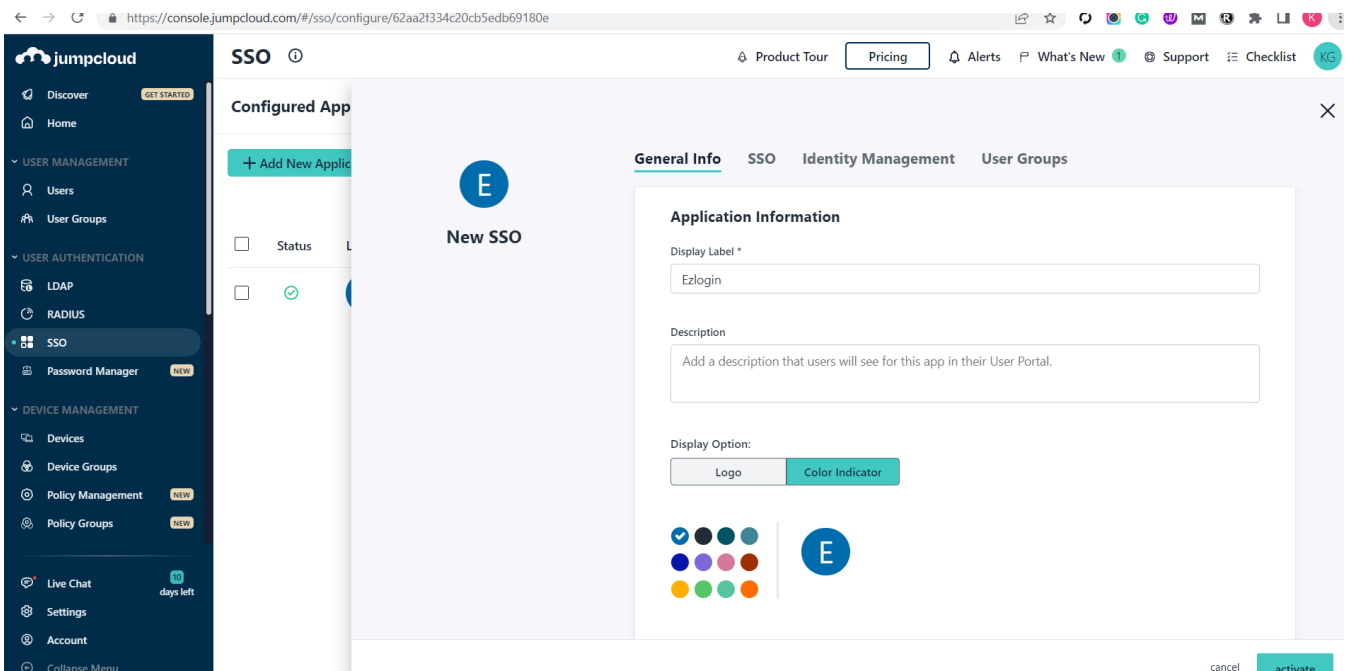
1. Login to Jumpcloud and Add the Application

The screenshot displays the Jumpcloud SSO configuration interface. On the left, a dark sidebar contains navigation options: Discover (GET STARTED), Home, USER MANAGEMENT (Users, User Groups), USER AUTHENTICATION (LDAP, RADIUS, SSO, Password Manager), and DEVICE MANAGEMENT (Devices, Device Groups, Policy Management, Policy Groups). The 'SSO' option is highlighted with a red box. The main content area is titled 'SSO' and 'Configured Applications'. It features a '+ Add New Application' button (highlighted with a red box and a red arrow), a search bar, and a table with one application. The table has columns for Status, Logo, Display Label, Show In User Portal, Supported Functionality, and IdP Certificate Status. The application listed has a status of 'On', a logo with the letter 'E', and an expiration date of 'Expires 03-29-2028'. Additional options like 'Export Metadata' and 'Delete' are visible for the application.

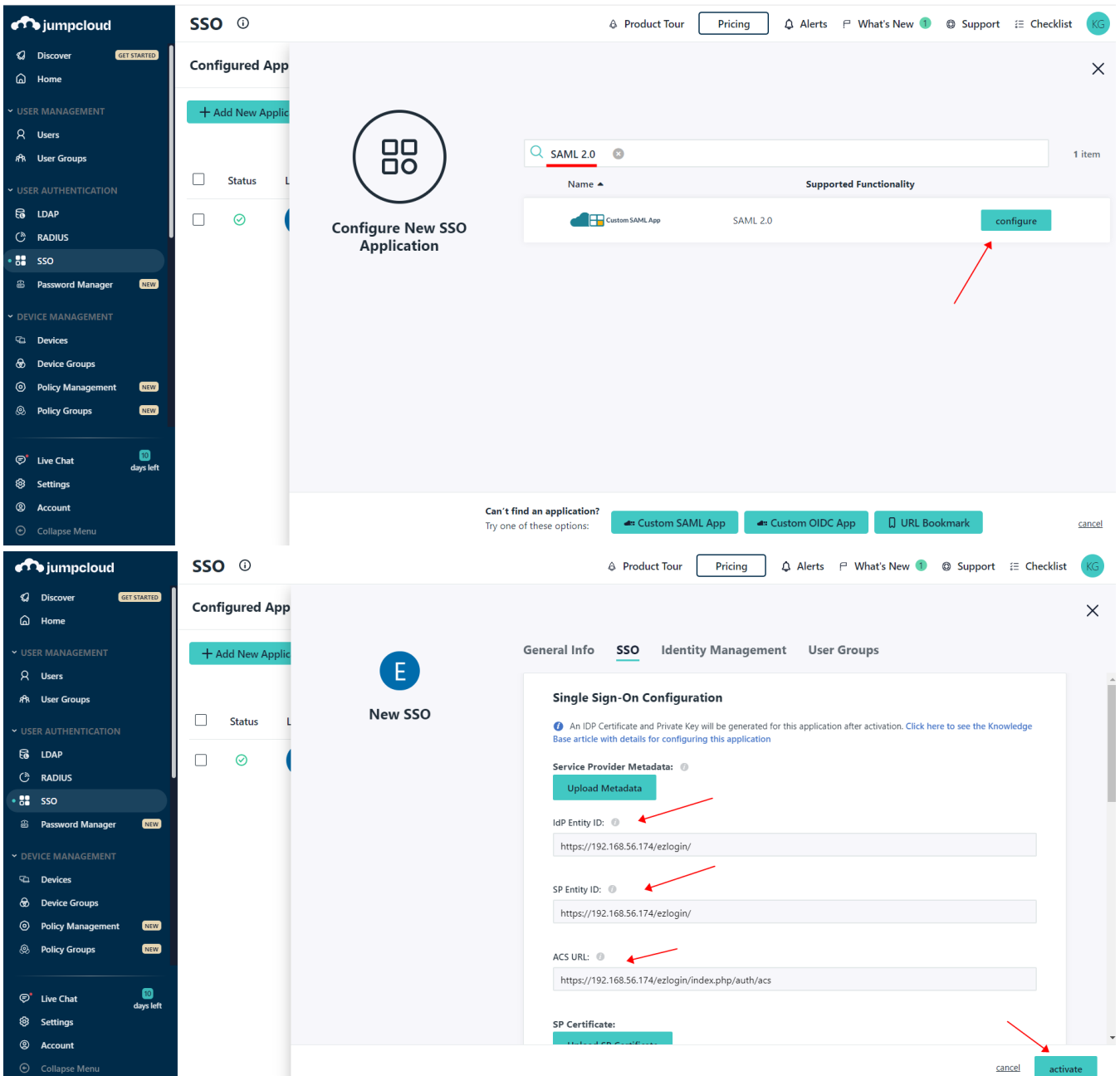
2. Search for SAML 2.0



3. Change the Display Label and save



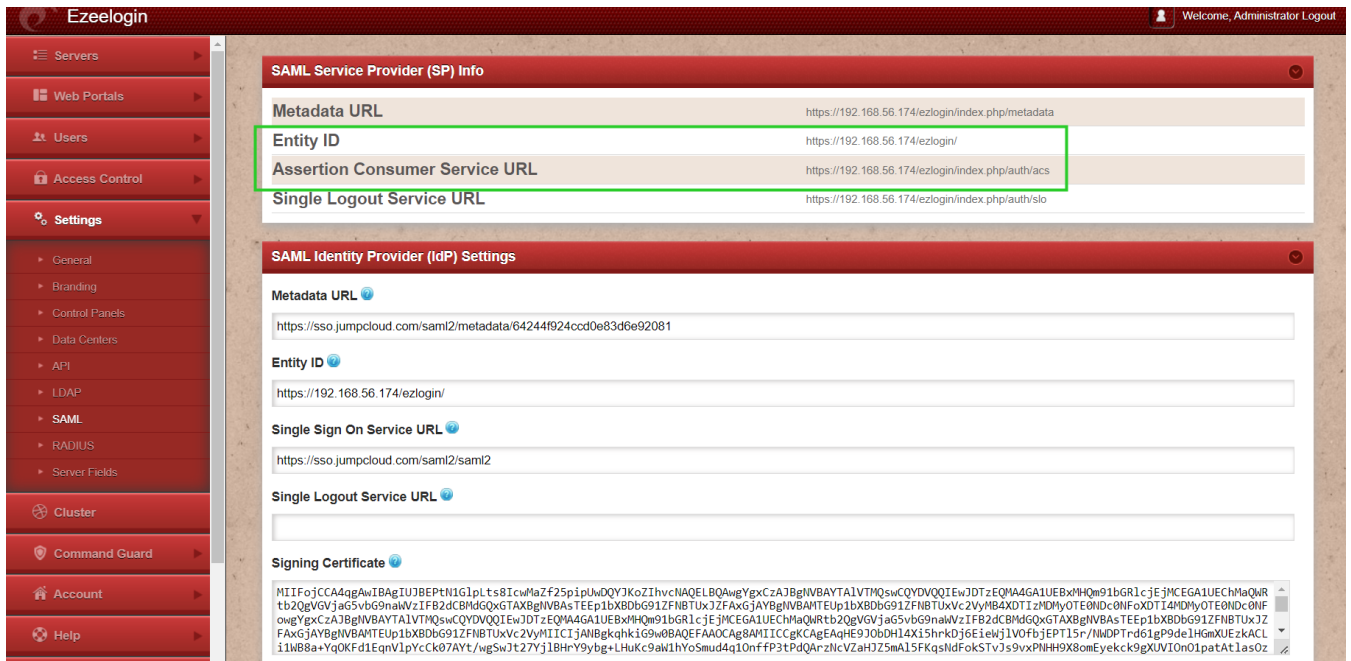
4. Select the configure tab and fill in the Application details and activate



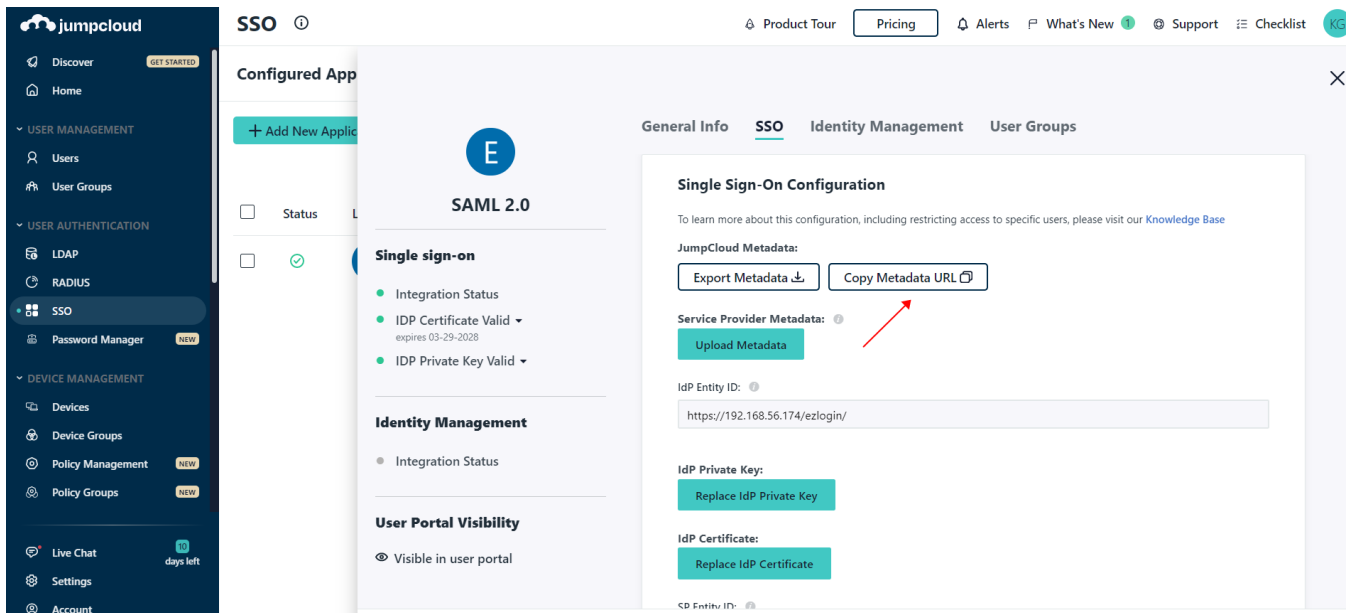
IdP Entity ID - Entity ID (you can find it from ezeelogin **GU > Settings > SAML**)

SP Entity ID -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**)



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



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

- Servers
- Web Portals
- Users**
- User Groups
- Authentication Log
- SSH Log
- RDP Recording
- SCP Log
- Web Proxy Log
- Web Proxy Activity
- Web Activity
- Shell Activity
- Server Activity**
- Work Summary
- Status
- Access Control
- Settings
- Cluster
- Command Guard

Search

User

-- All --

Servers

-- All --

From

2023-09-25 12:13

To

2023-09-30 12:13

Rows Per Page

10

Note: Logs are local to the node. Search the other node as well if cluster is configured.

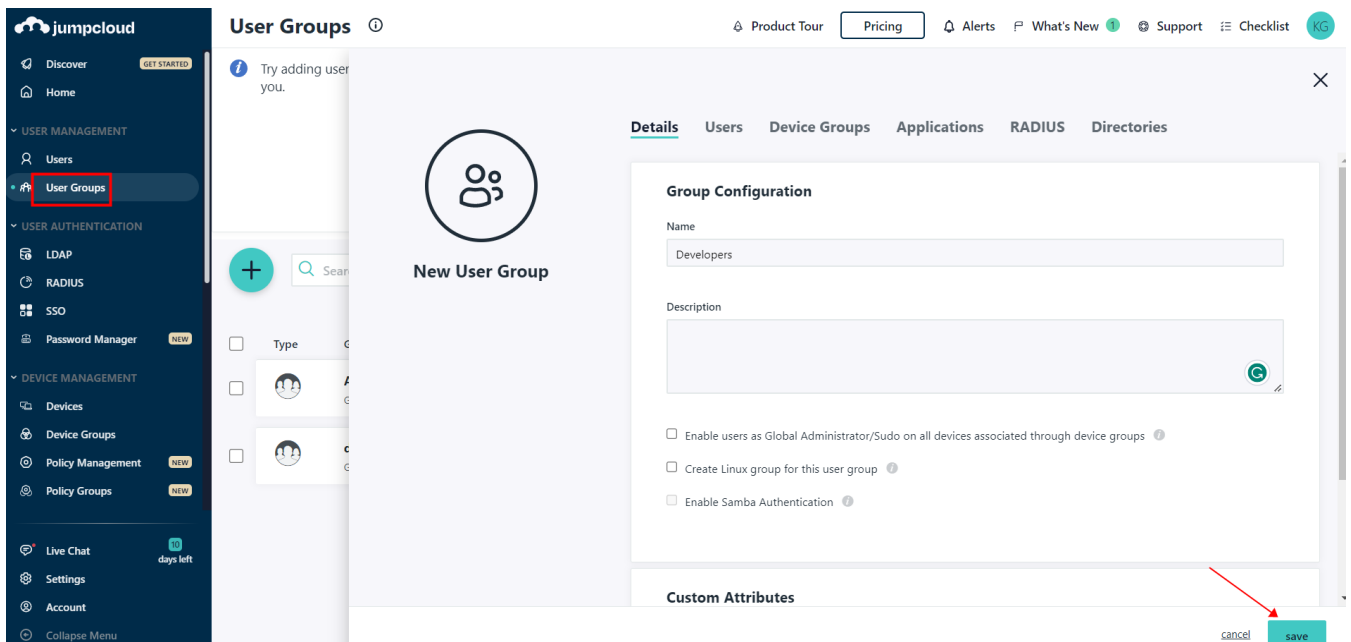
Export Reset Find

Server Activity Logs Clear all

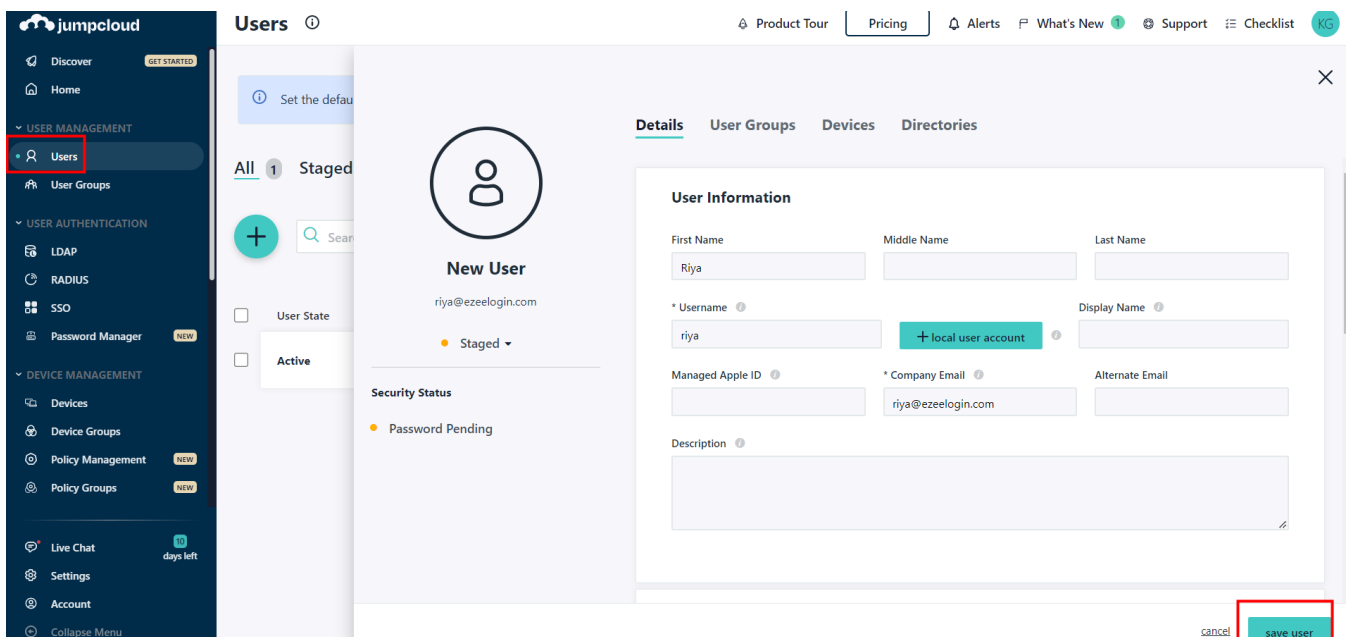
<input type="checkbox"/>	Username	Server Name	Status	IP Address	Login Time	Logout Time	Input Idle Time	Output Idle Time	Actions
<input type="checkbox"/>	admin	ubuntu.mysql	FAILED: Could not connect	192.168.1.5	2023-09-29 19:57:51	2023-09-29 19:57:52	0s	0s	
<input type="checkbox"/>	admin	ubuntu.mysql	FAILED: Could not connect	192.168.1.5	2023-09-29 19:59:16	2023-09-29 19:59:17	0s	0s	
<input type="checkbox"/>	admin	ubuntu.mysql	SUCCESS	192.168.1.5	2023-09-29 19:59:53	2023-09-29 23:12:39	3h 11m 49s	3h 11m 49s	

1 - 3 / 3

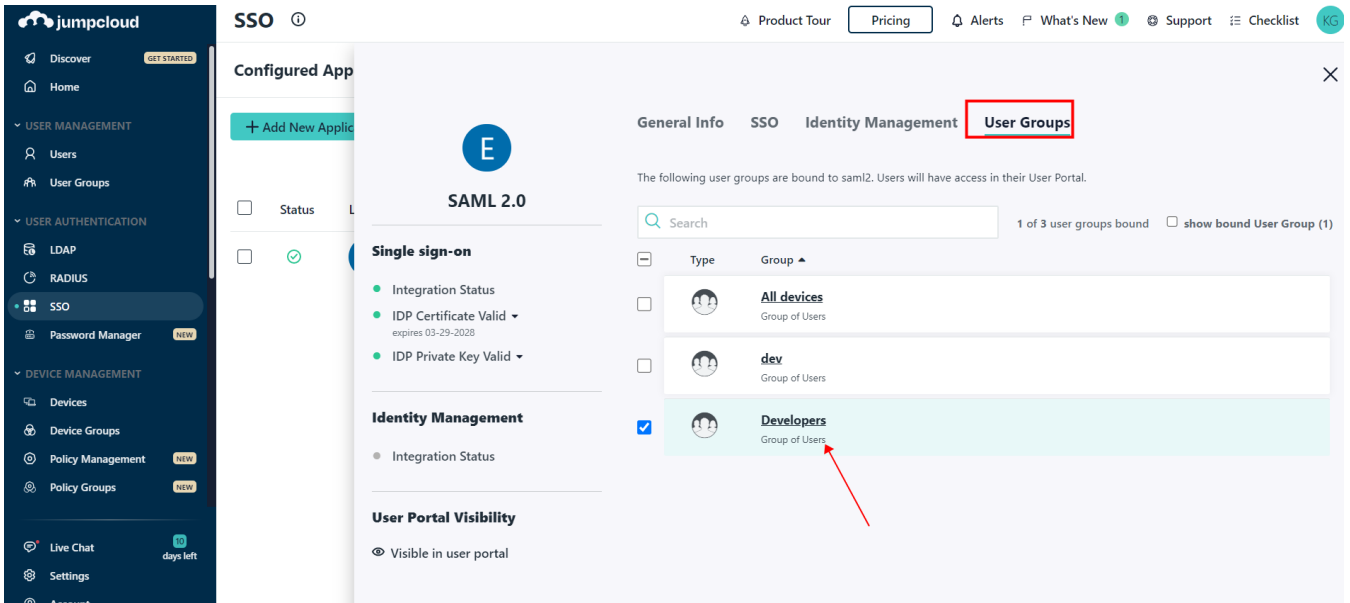
7. Select the user group tab from the left panel, add the user group name, and save it.



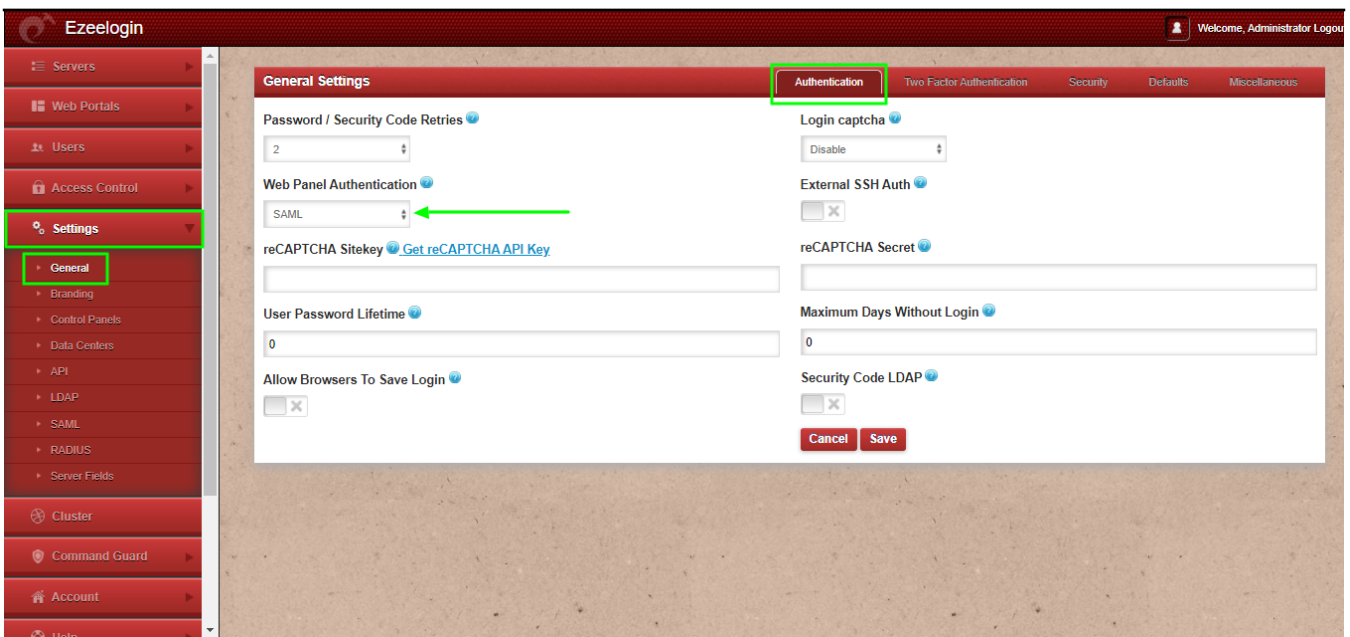
8. Add the user by selecting the users tab.



9. Select the SSO applications from left panel and assign the user group to that application



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



Enable Auth: Create User from Ezeelogin GUI -> Settings -> General -> Security ->

- Servers
- Web Portals
- Users
- Access Control
- Settings**
- General
- Branding
- Control Panels
- Data Centers
- API
- LDAP
- SAML
- RADIUS
- Server Fields
- Cluster
- Command Guard
- Account

General Settings

Authentication Two Factor Authentication **Security** Defaults Miscellaneous

Password Minimum Length

Password Minimum Block Letters

Password Minimum Special Characters

Auto Create User

Automated Password Change

SSH Session Logging

RDP Recording

Proxy Allow All

Password Maximum Length

Password Minimum Small Letters

Password Minimum Digits

Command Guard

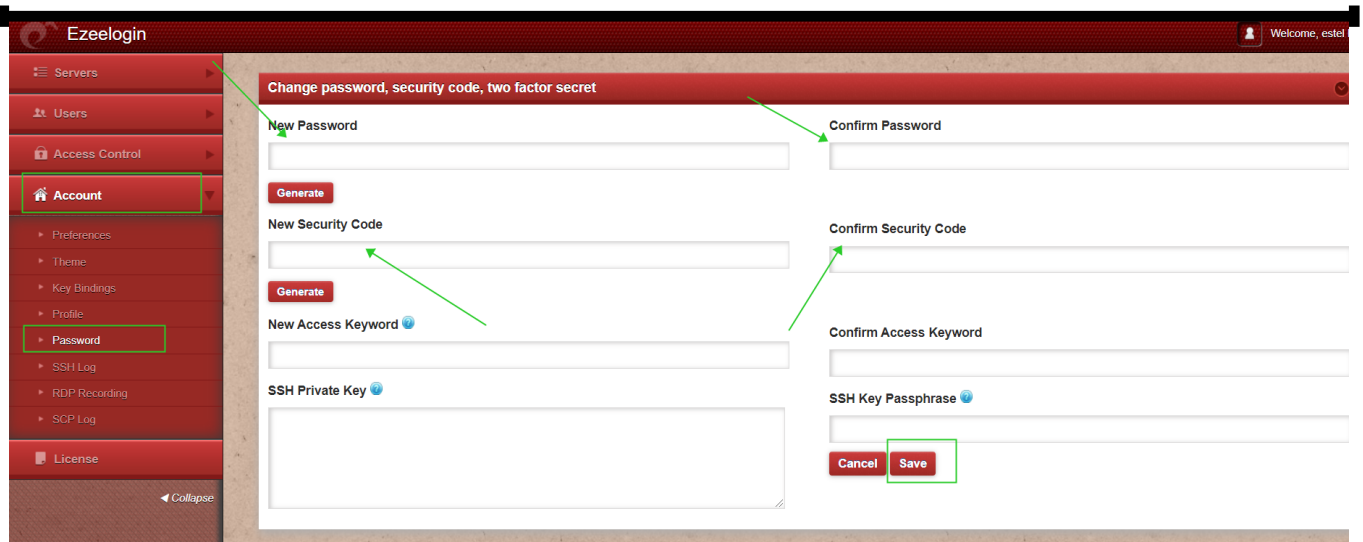
Shell Access Notification

Encrypt SSH Session Logs

Web Proxy Logging

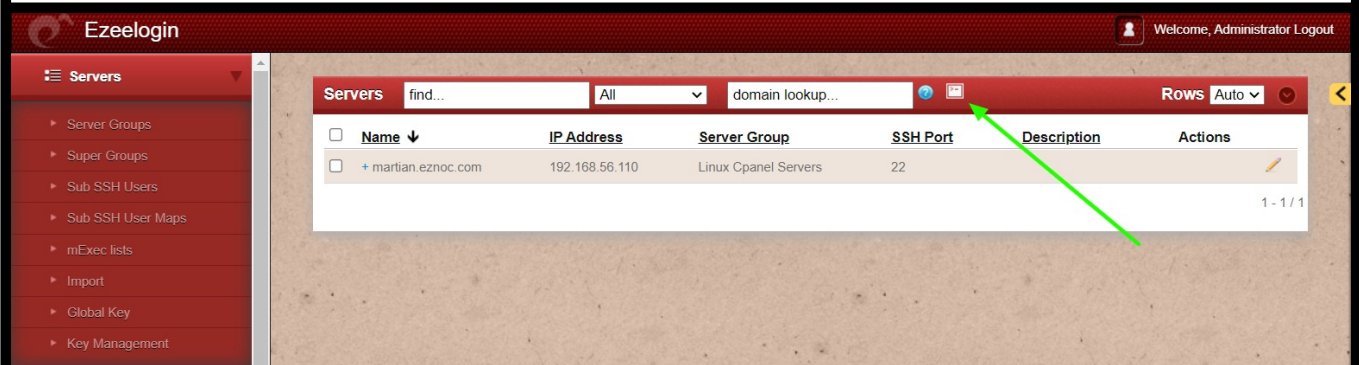
Tunnel Allow All

4.2e. **Accounting** - In the **General Settings** tab, under the **Security** section, check the **Auto Create User** checkbox to automatically create users for the SAMI



14. 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.**



```
*client.testing Portals
Production.servers Online gateway server
Testing.Server Testing
All servers List of all accessible servers
```

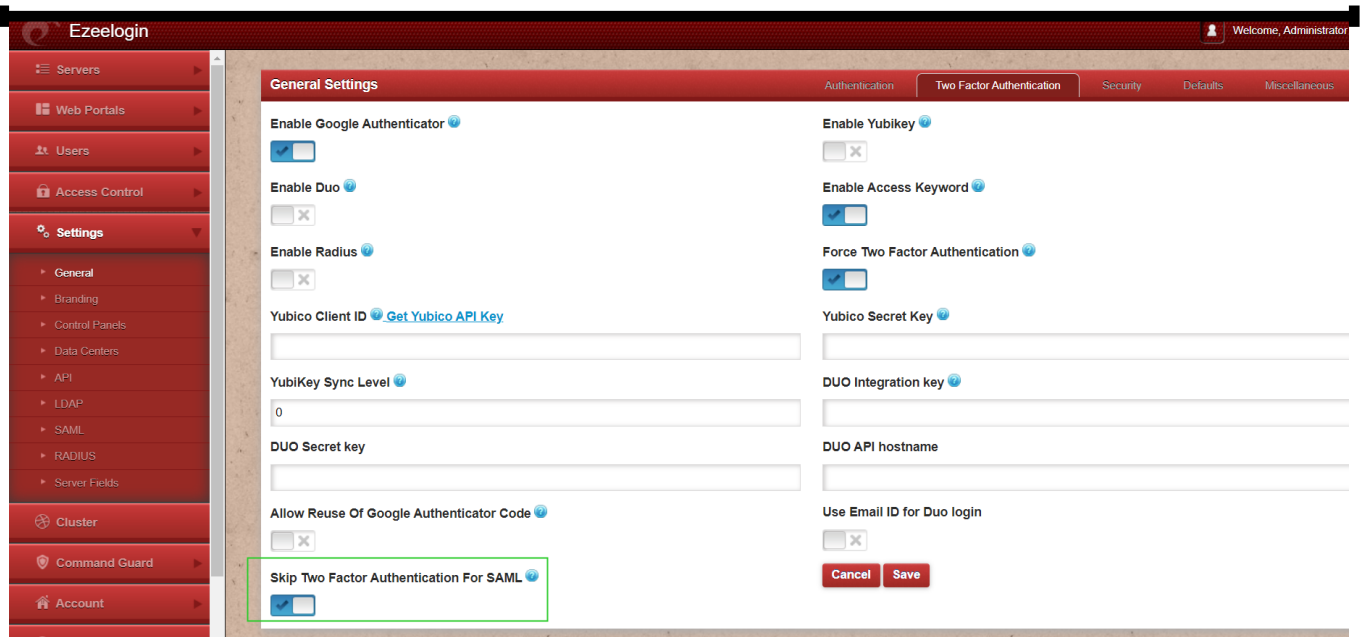
GROUPS [Normal /]

Start typing string to locate. ESC: Clear search, F1/+: Help, F4/!: Exit.

Menu Ezeelogin SSH CONNECTION ESTABLISHED

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**.

```
amadmin@ADMOD-LAPHP-6:~$ ssh riya@192.168.56.174
riya@192.168.56.174's password:
```



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.

- 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.

Online URL: <https://www.ezeelogin.com/kb/article/integrate-jumpcloud-sso-with-ezeelogin-599.html>