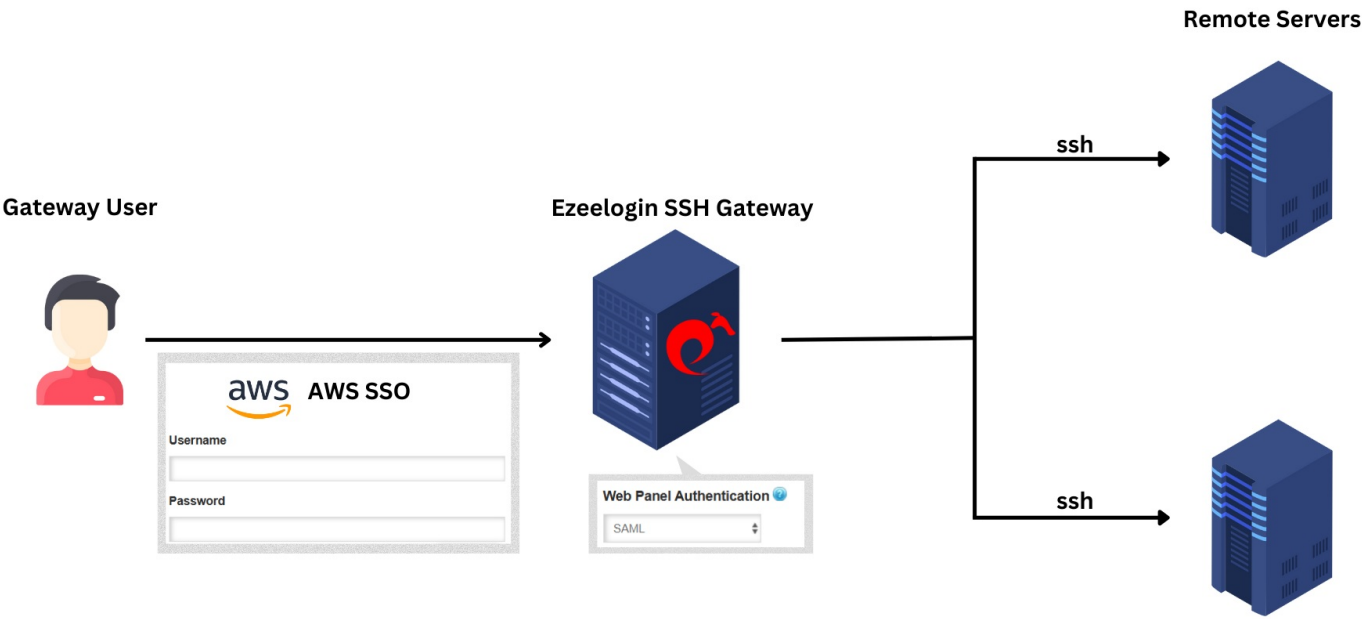


Integrate AWS SSO with Jumpserver

Integrate AWS SSO in Ezeelogin SSH Gateway

Overview: This article provides a comprehensive guide to integrating AWS SSO with Ezeelogin SSH Gateway. It covers the steps to configure a custom SAML 2.0 application in AWS, map user attributes, add and assign users, configure SAML Identity Provider settings in Ezeelogin, and enable SAML authentication. Additionally, it explains how to log into the Ezeelogin GUI and shell using SAML credentials, manage 2FA settings, and emphasizes the convenience of using the web SSH shell for SAML authentication.



Step 1: Login to AWS console > select AWS Single Sign-On and click on Applications



Step 2: Click on Add Application

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S] oktaez ▾ Ohio ▾ Support ▾

Dashboard
AWS accounts
Applications
Users
Groups
Settings

AWS SSO > Applications

Applications

Configure single sign-on (SSO) access to multiple cloud applications and any custom applications that support identity federation with SAML 2.0. [Learn more](#)

Add a new application Actions ▾

Application name ▾	Status	Certificate expiration
☐ ezeelogin	Configured	✓ May 10, 2026

Step 3. Click on Add a custom SAML 2.0 application

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S] oktaez ▾ Ohio ▾ Support ▾

Add New Application

Choose an application from our catalog of preintegrated cloud applications or choose to add a custom SAML 2.0 application. Each application comes with detailed instructions to help you set up the trust between AWS SSO and the application's service provider. [Learn more](#)

AWS SSO Application Catalog

Type the name of an application

☒ Add a custom SAML 2.0 application
You can add SSO integration to your custom SAML 2.0-enabled applications

10,000ft

4me

7Geese

Abstract

Accredible

Adobe Connect

Adobe Creative Cloud

Adobe Experience Manager

Cancel Add application

Step 4: Configure Custom SAML 2.0 application. Add **Display name & Description**

aws Services ▾ Search for services, features, marketplace products, and docs [Alt+S] oktaez ▾ Ohio ▾ Support ▾

Configure Ezeelogin

AWS SSO works as an identity provider (IdP) for any SAML 2.0-compliant cloud applications. To configure this application for SSO access, you must establish a trust relationship between AWS SSO and your cloud application (service provider) through a SAML metadata exchange. You can view instructions on this page and find metadata details for your provider. [View instructions](#)

Details

Display name* Ezeelogin

Description Ezeelogin SAML 2.0 application

The description you type here does not appear in the user portal. However, it will be visible in the AWS SSO console and when using the AWS SSO APIs.

AWS SSO metadata

Your cloud application may require the following certificate and metadata details to recognize AWS SSO as the identity provider.

AWS SSO SAML metadata file	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	Download
AWS SSO sign-in URL	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	
AWS SSO sign-out URL	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	
AWS SSO issuer URL	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	
AWS SSO certificate	Download certificate		

Step 5: Add Application properties & Application metadata

Step 5.a: Fill the Application start URL . You can find it from **Ezeelogin GUI > Settings > SAML> Entity ID**

Step 5.b: Fill the **Application start URL** & Click on **If you don't have a metadata file, you can manually type your metadata values.**

Fill the **Application ACS URL & Application SAML audience**

Application ACS URL - Assertion Consumer Service URL (you can find it from Ezeelogin GUI > Settings > SAML> Assertion Consumer Service URL)

Application SAML audience - Entity ID (you can find it from Ezeelogin GUI > Settings > SAML> Entity ID)

Application properties

Your cloud application may optionally take additional settings to configure your user experience. [Learn more](#)

Application start URL ⓘ	https://192.168.1.7/ezlogin/
Relay state	
Session duration	1 hour

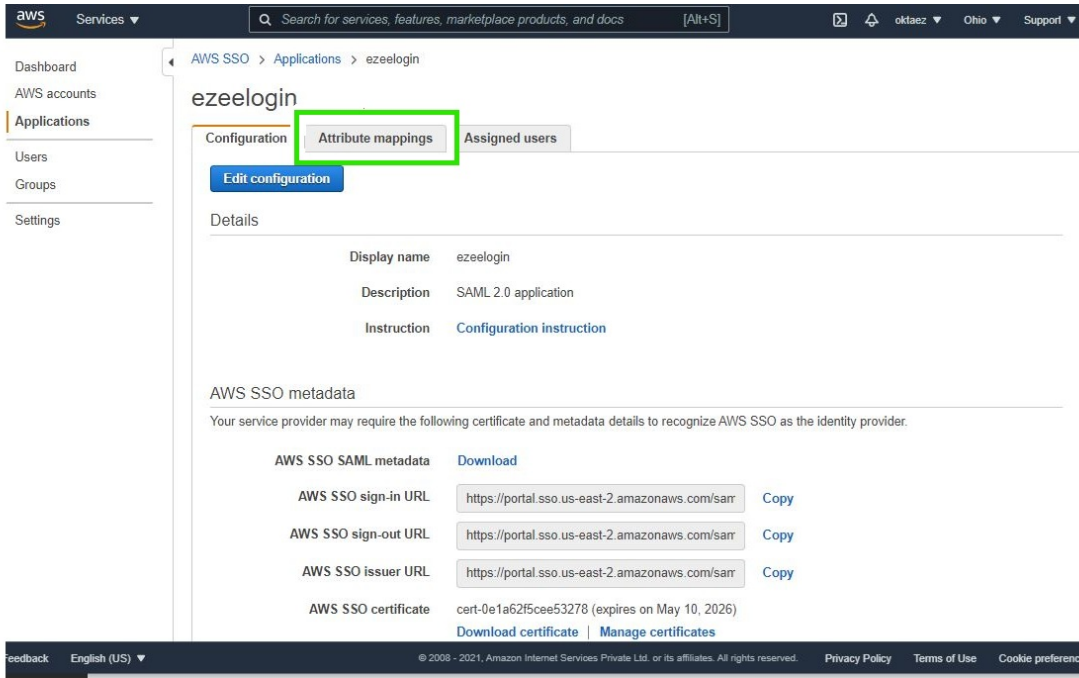
Application metadata

AWS SSO requires specific metadata about your SAML service provider before it can trust this application. You can tune this metadata manually or upload a metadata exchange file.

Application ACS URL ⓘ	https://192.168.1.7/ezlogin/index.php/auth/acs
Application SAML audience	https://192.168.1.7/ezlogin/

Click on save changes.

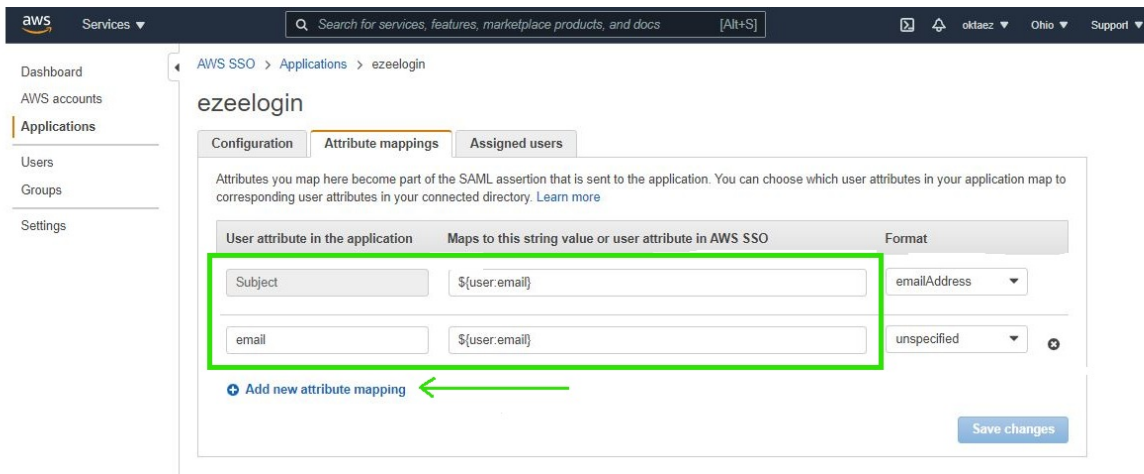
Step 6: Click on Attribute Mappings and Add attributes as follows.



Add attributes

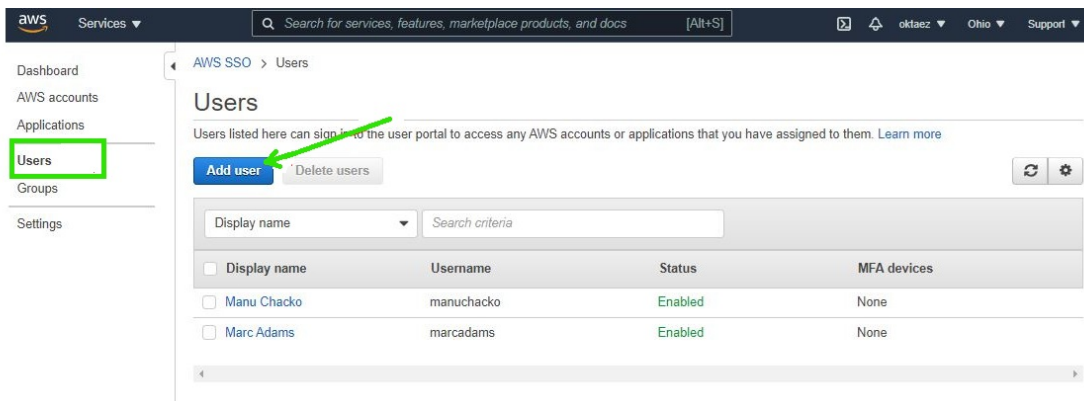
Step 6.a: Add `${user:email}` and select **emailAddress** Format

Step 6.b: Click on **Add new attribute mapping** and add **email** to first column, `${user:email}` to next column & select **unspecified** Format and **save**.



Step 7: Add and assign users to access our application.

Step 7.a: Add user : Click on **Add user** in **Users** tab in aws sso console



Step 7.b: Add **Username, Password, Email address, First name, Last name & Display name** and Click **Next**. Assign to a **usergroup** and **Save**.

You need to add different email address for each users. By default ezeelogin uses email address for creating

users. You should an email address for superadministrator in ezeelogin(It will be empty by default)
If you want to add an existing user in ezeelogin into SSO, Add the user with exact username, email address as follows. (Ezeelogin will verify with the email address of the users by default)

Ezeelogin Welcome, Administrator Logout

Users

Edit User

First Name: Administrator

Last Name:

Username: **steve**

Email: **steve@ezeelogin.com**

User Group: Admins

Status: ☒ Active ☐ Suspended

Command Guard: -- None --

Limit IPs: ☐ ☒ X

Allowed IPs:

Add user

1 Details 2 Groups

User details

Username*: steve

This username will be required to sign in to the user portal. It cannot be changed later.

Password: ☒ Send an email to the user with password setup instructions. [Learn more](#)
☐ Generate a one-time password that you can share with the user. [Learn more](#)

Email address*: steve@ezeelogin.com

Confirm email address*: steve@ezeelogin.com

First name*: Steve

Last name*: Irvin

Display name*: Steve Irvin

▶ Contact methods (optional)

▶ Job-related information (optional)

▶ Address (optional)

Cancel **Next: Groups**

Step 7.c: Click on **Assigned users** tab and click on **Assign users** button to assign users to this application.

Assigned users

The following users and groups from your connected directory can access this application. [Learn more](#)

Assign users

User/group	
manuchacko	Remove access
marcadams	Remove access

Step 8: Add **SAML Identity Provider (IdP) Settings** on Ezeelogin.

Copy the **AWS SSO SAML metadata url** and paste it to Metadata URL on Ezeelogin GUI > Settings > SAML Metadata URL and click on the fetch button ,It will autofill the SAMLsettings and Save it.

Configure Ezeelogin

AWS SSO works as an identity provider (IdP) for any SAML 2.0-compliant cloud applications. To configure this application for SSO access, you must establish a trust relationship between AWS SSO and your cloud application (service provider) through a SAML metadata exchange. You can view instructions on this page and find metadata details for your provider.

[View instructions](#)

Details

Display name*

Ezeelogin

Description

Ezeelogin SAML 2.0 application

The description you type here does not appear in the user portal. However, it will be visible in the AWS SSO console and when using the AWS SSO APIs.

AWS SSO metadata

Your cloud application may require the following certificate and metadata details to recognize AWS SSO as the identity provider.

AWS SSO SAML metadata file	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	Download
AWS SSO sign-in URL	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	
AWS SSO sign-out URL	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	
AWS SSO issuer URL	https://portal.sso.us-east-2.amazonaws.com/saml	Copy URL	
AWS SSO certificate	Download certificate		

Paste the **Metadata URL** on **Ezeelogin GUI > Settings > SAML Metadata URL** and click on the **Fetch** button & **save** it.

Ezeelogin Welcome, Administrator Logout

Settings

- General
- Branding
- Control Panels
- Data Centers
- API
- LDAP
- SAML**
- RADIUS
- Server Fields

Cluster

Command Guard

Account

Help

License

⏏ Collapse

Powered by  Ezeelogin.com

SAML Identity Provider (IdP) Settings

Metadata URL 

<https://portal.sso.us-east-2.amazonaws.com/saml/metadata/MzY3ODExMjU2OTUwX2lucy1jMWM3MDQxNjFkYWUxZGE5>

Entity ID 

<https://portal.sso.us-east-2.amazonaws.com/saml/assertion/MzY3ODExMjU2OTUwX2lucy1jMWM3MDQxNjFkYWUxZGE5>

Single Sign On Service URL 

<https://portal.sso.us-east-2.amazonaws.com/saml/assertion/MzY3ODExMjU2OTUwX2lucy1jMWM3MDQxNjFkYWUxZGE5>

Single Logout Service URL 

<https://portal.sso.us-east-2.amazonaws.com/saml/logout/MzY3ODExMjU2OTUwX2lucy1jMWM3MDQxNjFkYWUxZGE5>

Signing Certificate 

MIIDAzCCAeugAwIBAgIBATANBqkqhkiG9w0BAQsFADBFMRywFAYDVQDDA1hbmF6b25hd3MuY29tMQ0wCwYDVQQLDARJREFTMQ8wDQYDVQQKDAZBbWV6b24xZCzAJBgNVBAYTA1VTMB4XDTE1MDUxMDEwMjUxM1oXDTE1MDUxMDEwMjUxM1owRTEwMBQGA1UEAwM1hem9uYXZzLmNvbTENCMAAGA1UECwwESURBUzEPMA0GA1UECgwGQW1hem9uMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJ2yi18Y6wyueCuhXpeMYGjAZcxV/5b8403niqgrCFF+T2pcDX/ch1t8fIkacqxKFqx37CxKpn1RmuJEbCKED/tKN1pyPxNw9c8LV95FAP8Ye20htd9qeAmc6sCgo+Pf/xsEUEpHb1Erp2YJKVJBRS5m9PfTpPgn0wis/+GzUSWJ1B3rq/aS2sG/TV9LDQNDerahz23i4fM7w2jdp/4niuh+dgEBgb

Encryption Certificate 

New Signing Certificate 

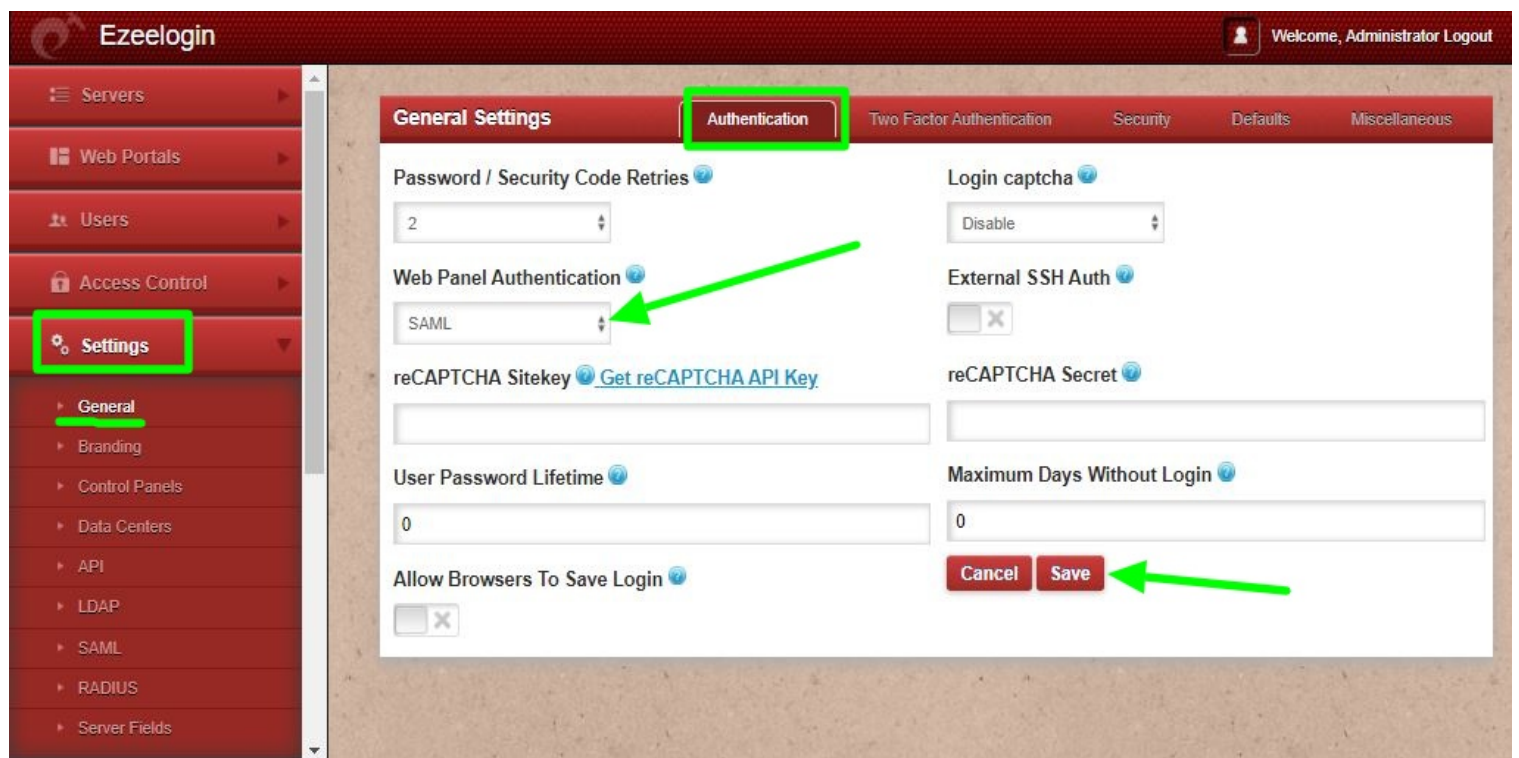
New Encryption Certificate 

Username Attribute Name 

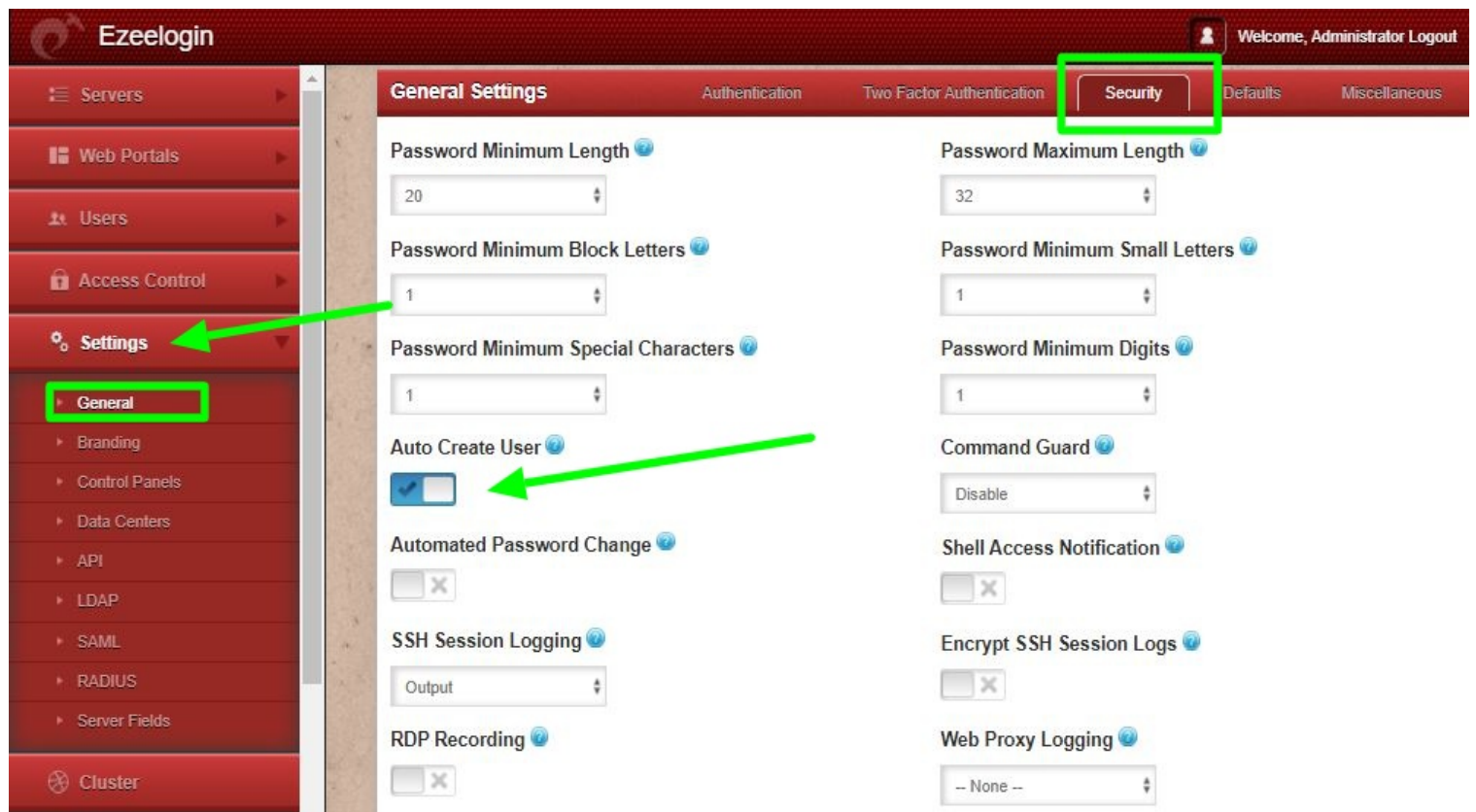
Group Attribute Name 

Cancel **Fetch** **Save**

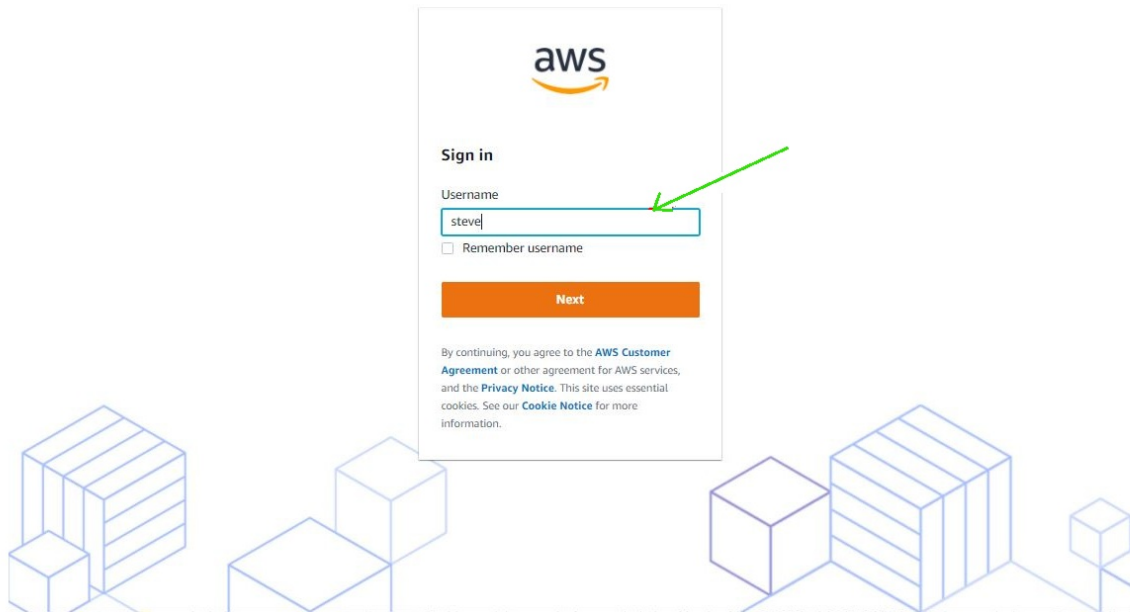
Step 9: Change **Web panel Authentication** to **SAML** from **Ezeelogin GUI > Settings > General > Web Panel Authentication > SAML**



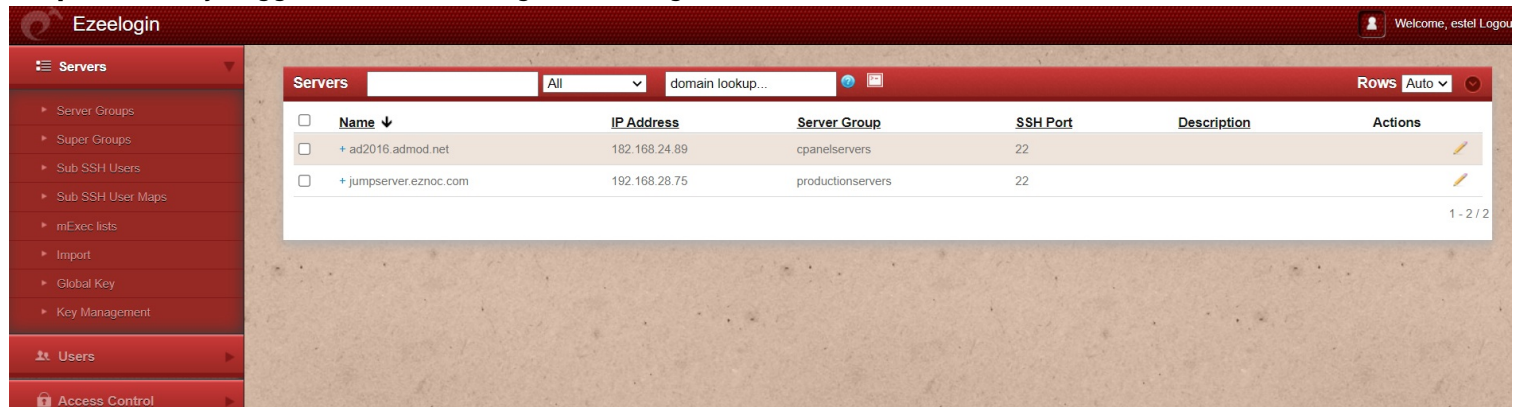
Step 10: Enable **Autocreate user** from **Ezeelogin GUI > Settings > General > Security > Enable Auto create user**



You can now login to ezeelogin GUI with ezeelogin URL and it will redirect to aws sso page. You must log in with aws sso credentials and it will redirect and log in to ezeelogin gui after successful authentication.



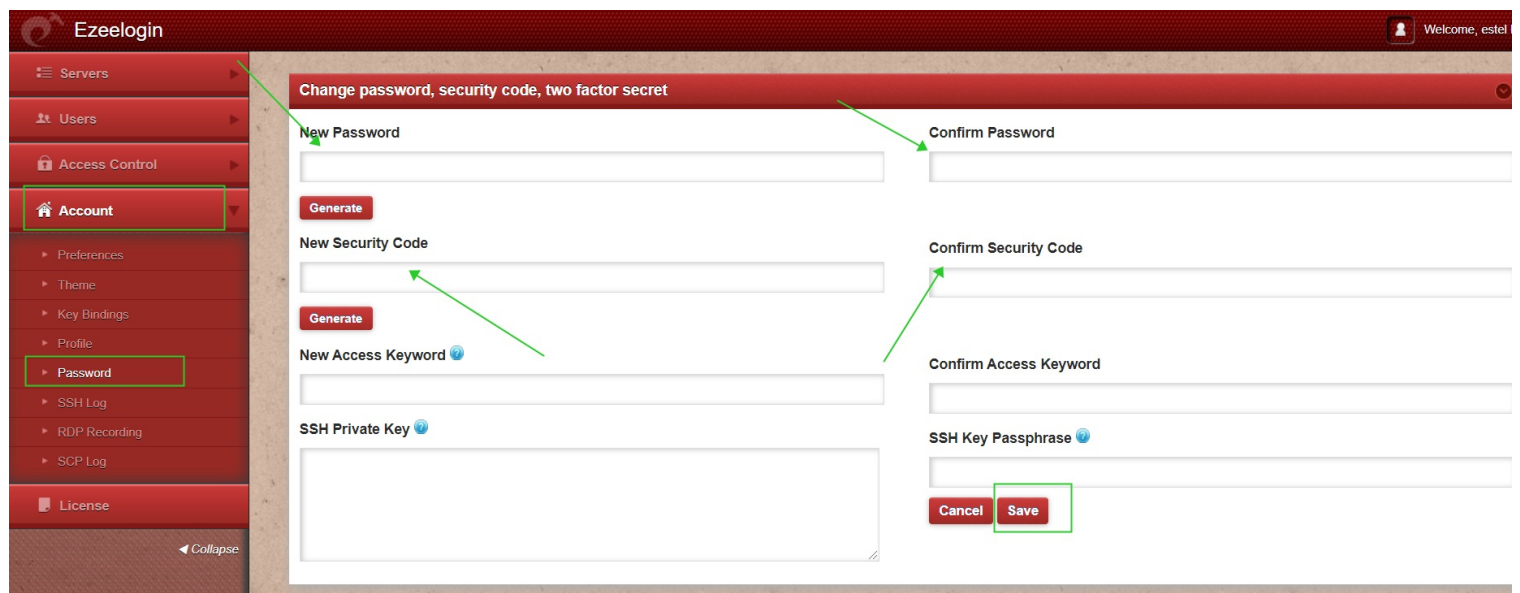
Step 11: Finally, logged into the Ezeelogin GUI using SAML Authentication.



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

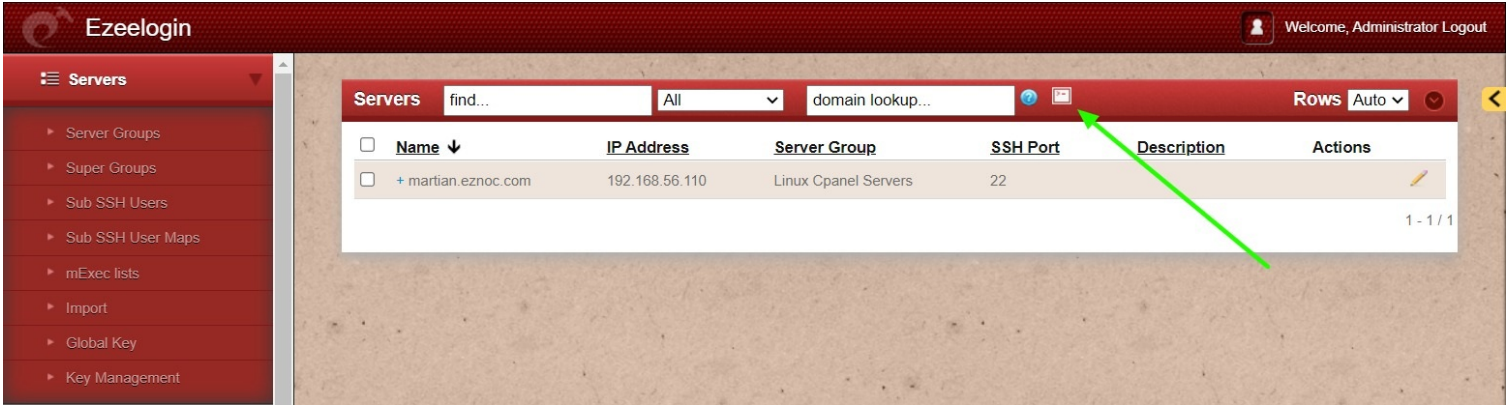
Error: Invalid password

Step 12: After logging into the GUI, you need to reset the password and security code of the saml user under **Account>Password** in order to ssh to the Ezsh shell

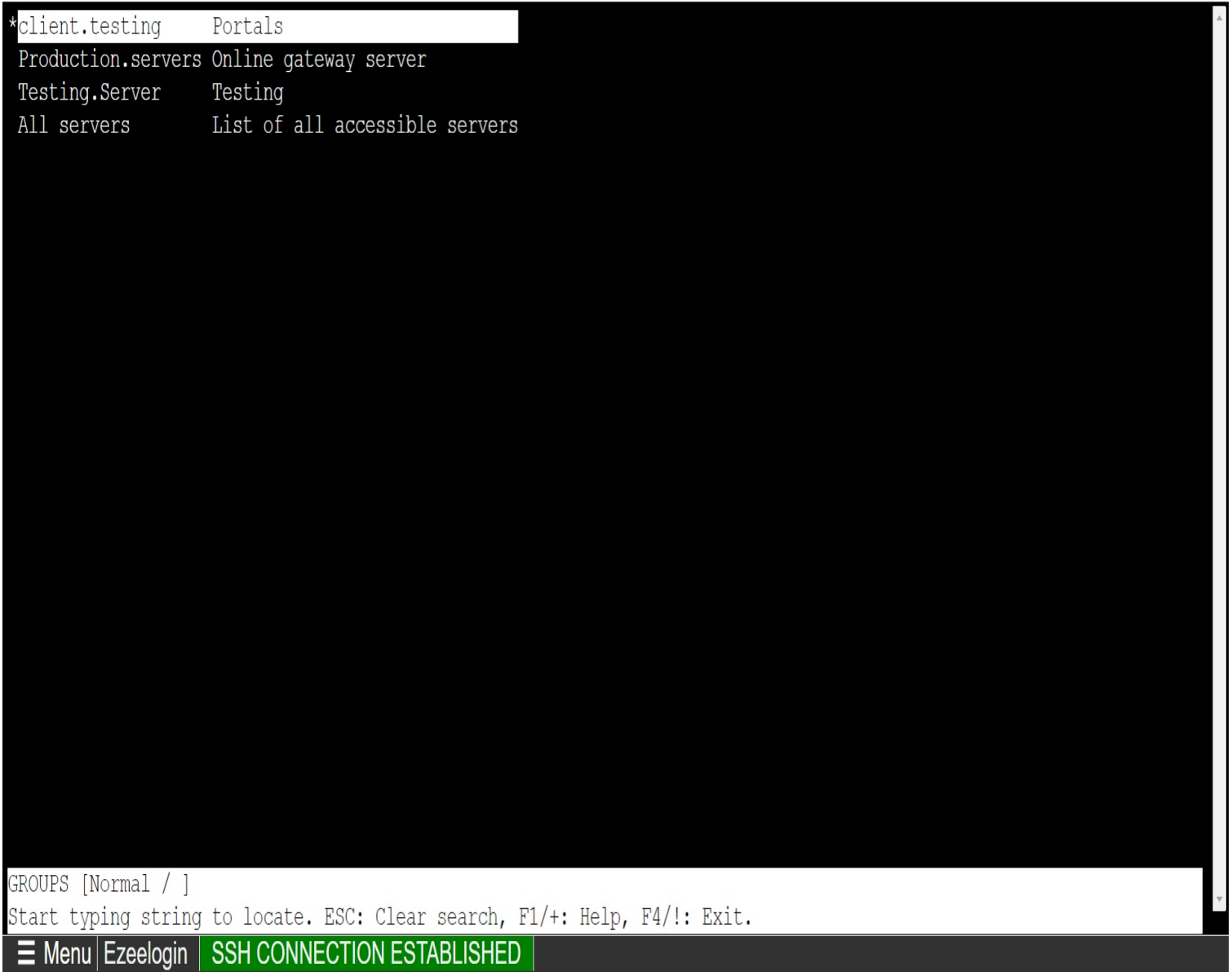


Step 13: You can log in to **Ezeelogin shell** via **Webssh** shell or using any **SSH client** such as Putty or terminal etc.

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.**



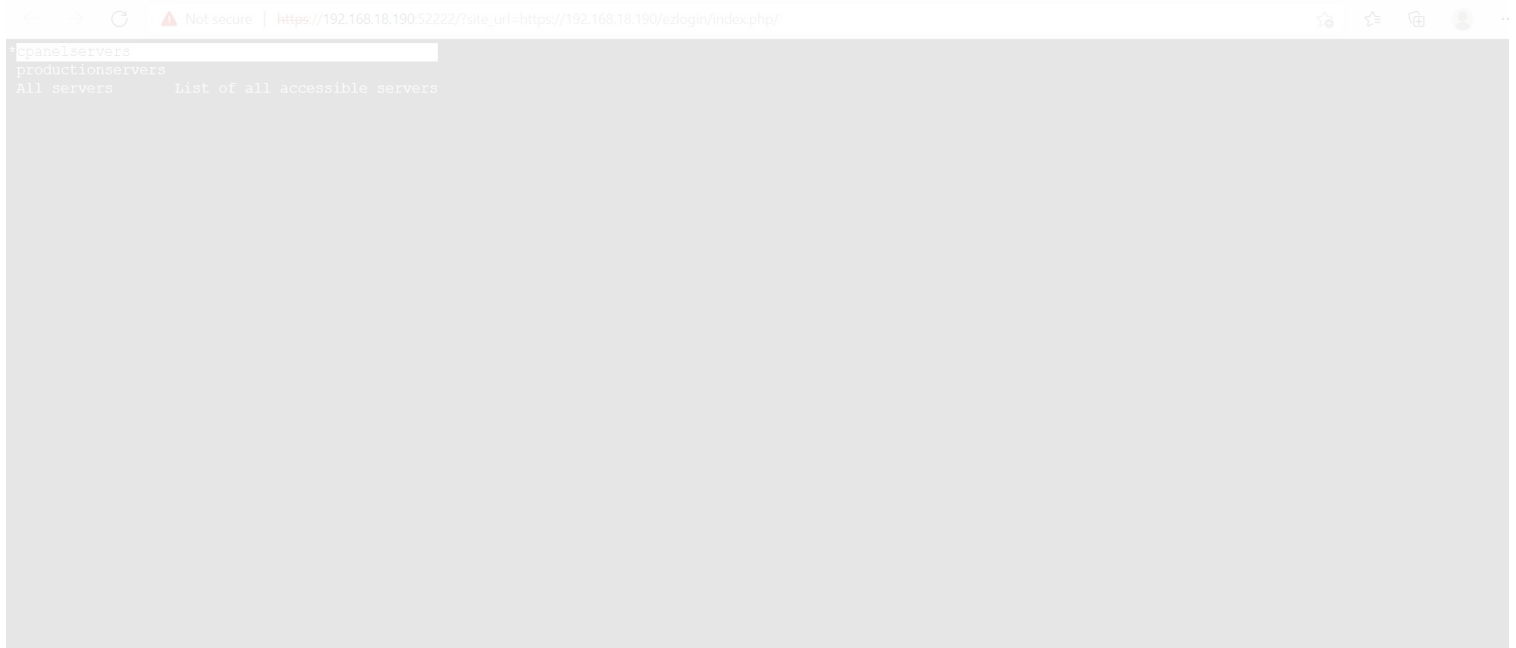
Native SSH Client: After resetting the password and security code you can **SSH to the Ezsh shell** (using Terminal or Putty) with the **SAML username**.

```
amadmin@ADMOD-LAPLEN-012:~$ ssh estel@192.168.18.190
estel@192.168.18.190's password: |
```

Step 14: If you are SSHing with 2FA enabled using Putty or Terminal it would prompt you 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 webpanel, otherwise if the user is not logged into the webpanel it would prompt for the 2FA codes.

The screenshot shows the Ezeelogin web interface. On the left is a sidebar menu with options: Servers, Web Portals, Users, Access Control, Settings (selected), Cluster, Command Guard, and Account. The 'Settings' menu is expanded, showing sub-options: General, Branding, Control Panels, Data Centers, API, LDAP, SAML, RADIUS, and Server Fields. The 'General' sub-option is selected. 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 different authentication methods (Google Authenticator, Duo, Radius, Yubikey, Access Keyword) and fields for Yubico Client ID, Yubico Secret Key, DUO Integration key, and DUO API hostname. At the bottom left, the option 'Skip Two Factor Authentication For SAML' is checked, highlighted with a green box. At the bottom right, there are 'Cancel' and 'Save' buttons. The top right of the interface shows a user profile icon and the text 'Welcome, Administrator'.

Step 15: It is recommended to use the webssh shell for the SAML authentication. The webssh shell is more convenient as the user would not have to open an ssh client such as putty/terminal and enter the username/password and 2FA codes. Using the webssh, the user can ssh from the webpanel itself and 2fa will not be prompted if you have enabled the Skip Two factor Authentication for SAML.



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

Related Articles:

[Login as superadmin when SSO is enabled globally](#)

[Integrate OneLogin SSO with jumpserver](#)

[Integrate Jumpcloud SSO with Ezeelogin](#)

[Integrate GSuite SSO with Jumpserver](#)

[Integrate Okta SSO with jumpserver](#)

[Disable SAML /SSO Authentication on ezeelogin](#)

[Integrate SAML Authentication in Ezeelogin GUI using Microsoft Azure SSO and Azure Active Directory](#)

[Map existing user group from SAML provider to ezeelogin.](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-aws-sso-with-jumpserver-402.html>