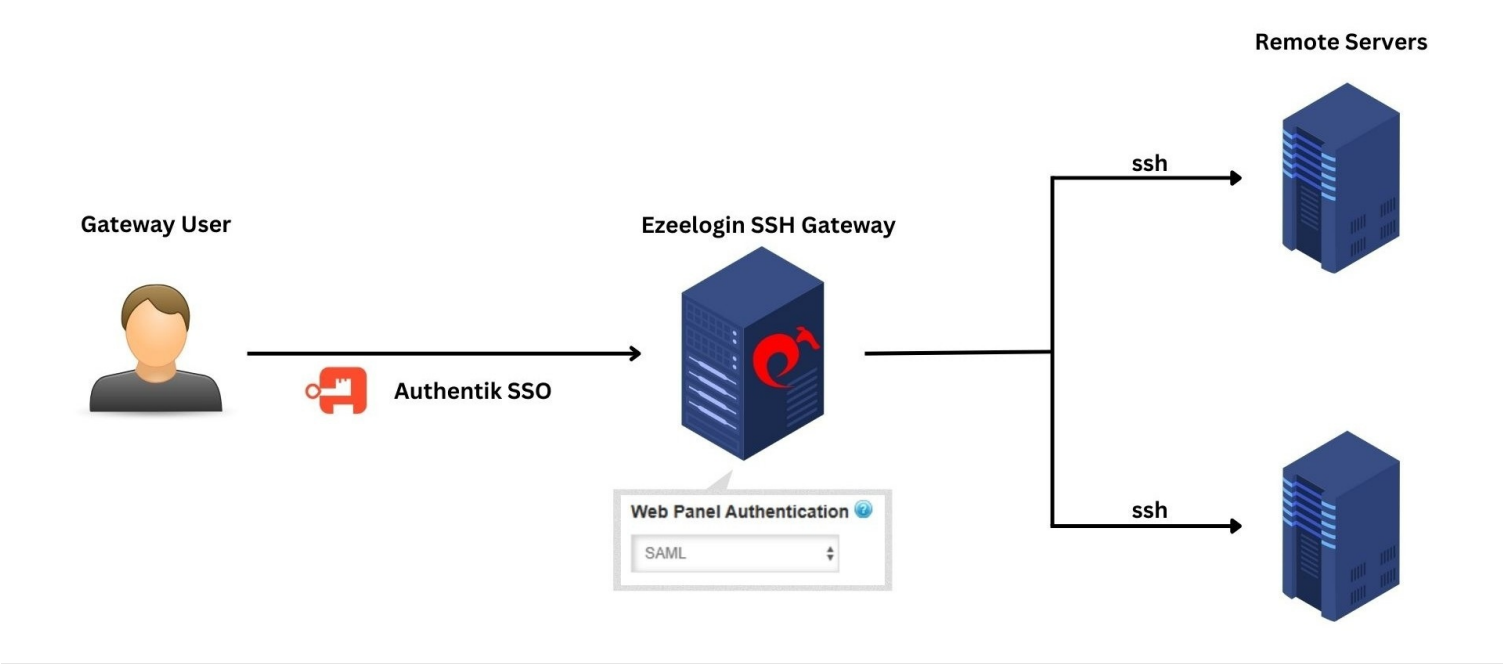


Integrate Authentik SSO with Jumpserver

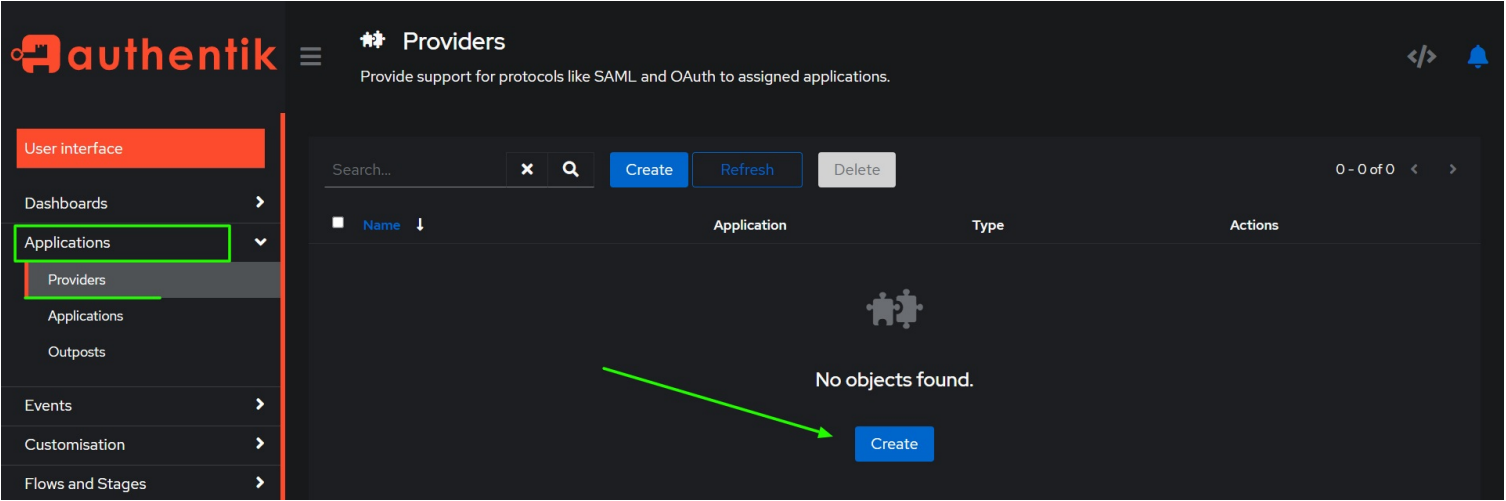
Integrate Authentik SSO with Ezeelogin SSH Gateway

Overview: This article will help Ezeelogin admin users to integrate Authentik SSO with Ezeelogin gateway server.

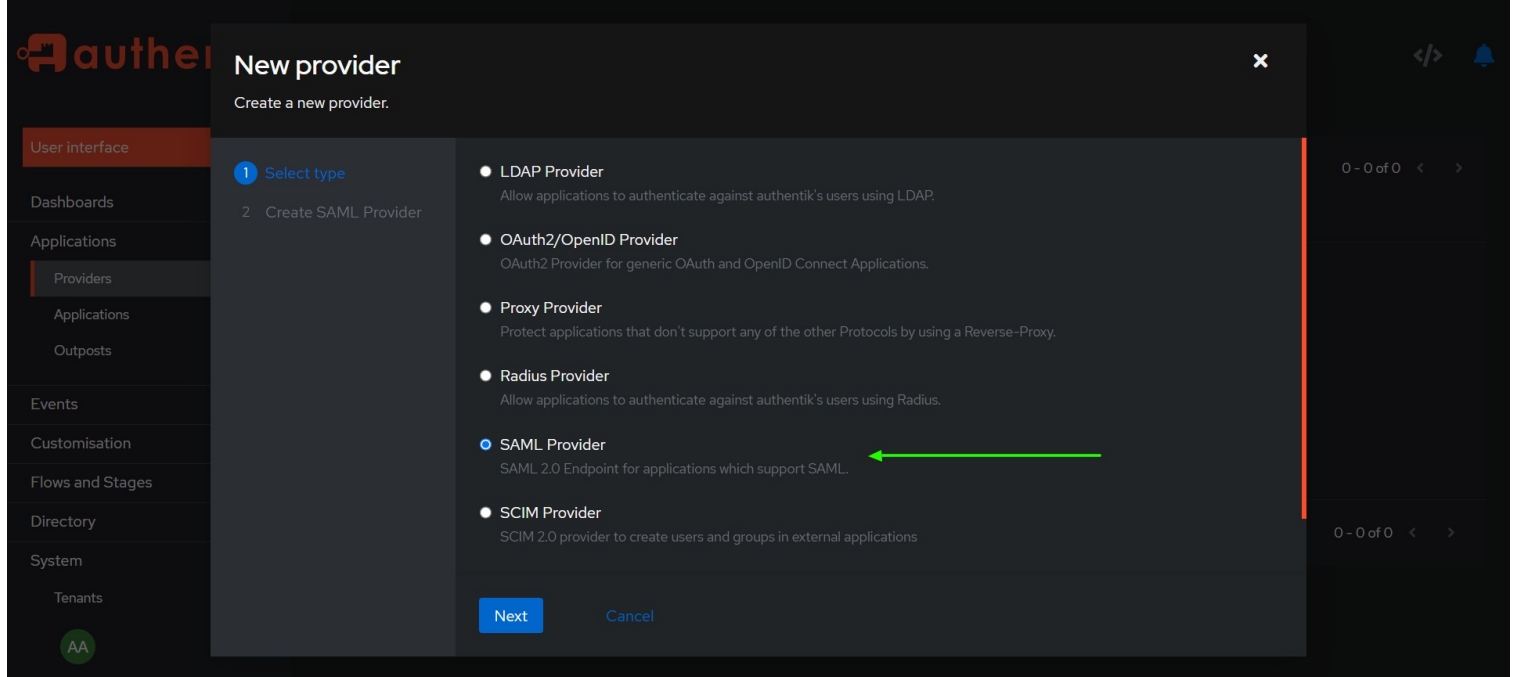
SAML is an authentication mechanism for web applications.
It's based on web protocols and it cannot be used for user authentication over SSH.



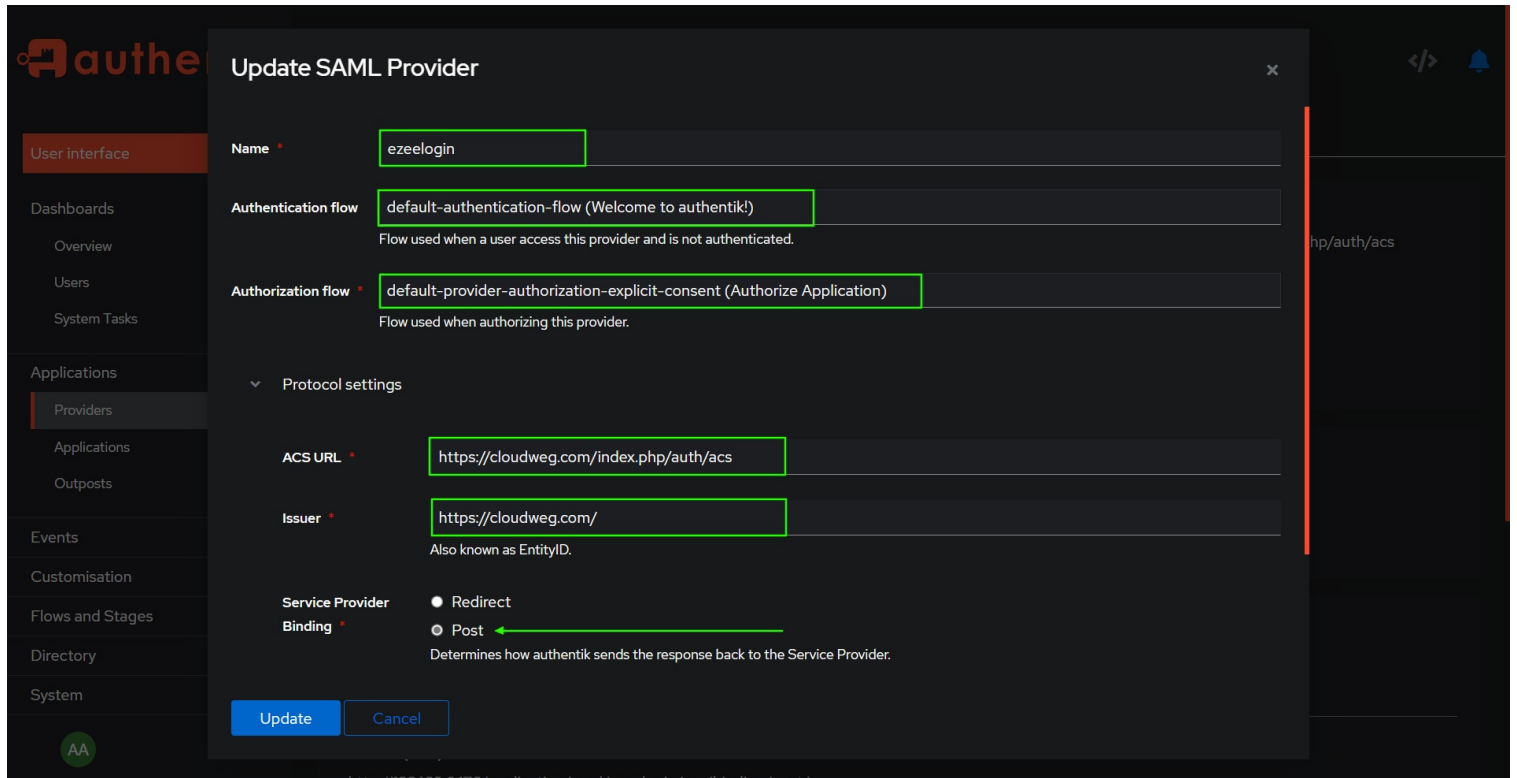
Step 1: Login to **Authentik** administrator dashboard and add **Providers** under **Application** tab.



Step 2: Select **SAML Provider** and click **next**.



Step 3: Provide a **name for the SAML provider** and set both the **Authentication Flow** and **Authorization Flow** to **default**. Under **Protocol Settings**, paste the **ACS URL** and **Entity ID** from the **Ezeelogin SAML settings in the GUI**, select **POST** then click **Finish**.



Ezeelogin Welcome, Administrator Logout

- Servers
- Web Portals
- Users
- Access Control
- Settings**
 - General
 - Branding
 - Control Panels
 - Data Centers
 - API
 - LDAP
 - SAML**
 - FIDO2
 - RADIUS
 - SIEM
 - Server Fields
- Cluster
- Command Guard

SAML Service Provider (SP) Info

Metadata URL	https://cloudweg.com/index.php/metadata
Entity ID	https://cloudweg.com/
Assertion Consumer Service URL	https://cloudweg.com/index.php/auth/acs
Single Logout Service URL	https://cloudweg.com/index.php/auth/slo

SAML Identity Provider (IdP) Settings

Metadata URL

Entity ID

Single Sign On Service URL

Single Logout Service URL

Signing Certificate

Step 4: After successfully creating the SAML provider, it will be listed under the Providers tab and display a warning message stating, "**Provider not assigned to any application.**"

authentik Providers

Provide support for protocols like SAML and OAuth to assigned applications.

Search... Create Refresh Delete 1 - 1 of 1

Name	Application	Type	Actions
ezeelogin	Warning: Provider not assigned to any application.	SAML Provider	

1 - 1 of 1

Step 5: Add an **Application** under the **Applications** tab.

authentik Applications

External Applications which use authentik as Identity-Provider, utilizing protocols like OAuth2 and SAML. All applications are shown here, even ones you cannot access

Search... Create Refresh Delete 0 - 0 of 0

Name	Group	Provider	Provider ...	Actions
No objects found.				

Create

Applications

Applications in authentik are the other half of providers. They exist in a 1-to-1 relationship, each application needs a provider and every provider can be used with one application. Starting with authentik 2023.5, applications can use multiple providers, to augment the functionality of the main provider. For more information, see [Backchannel providers](#).

Applications are used to configure and separate the authorization / access control and the appearance in the *My applications* page.

Authorization

Step 6: Provide a **name for the application**, select the **provider** using the **drop-down box**, and **create the application**.

Create Application

Name *
Application's display Name.

Slug *
Internal application name, used in URLs.

Group
Optionally enter a group name. Applications with identical groups are shown grouped together.

Provider
Select a provider that this application should use.

Backchannel providers
Select backchannel providers which augment the functionality of the main provider.

Policy engine mode * ☒ any

Step 7: After the successful creation of the application, it will be listed under the Applications tab. Also, **check the Providers tab to see if the previous warning message has disappeared.**

Applications

External Applications which use authentik as Identity-Provider, utilizing protocols like OAuth2 and SAML. All applications are shown here, even ones you cannot access.

Search...

1 - 1 of 1 < >

Name	Group	Provider	Provider Type	Actions
ezeelogin	-	ezeelogin	SAML Provider	edit delete

1 - 1 of 1 < >

Applications

Applications in authentik are the other half of providers. They exist in a 1-to-1 relationship, each application needs a provider and every provider can be used with one application. Starting with authentik 2023.5, applications can use multiple providers, to augment the functionality of the main provider. For more information, see [Backchannel providers](#).

Applications are used to configure and separate the authorization / access control and the appearance in the *My applications* page.

Authorization

Providers

Provide support for protocols like SAML and OAuth to assigned applications.

Search...

Name	Application	Type
ezeelogin	Assigned to application ezeelogin	SAML Provider

Step 8: Generate new **Certificate-Key Pair** for Ezeelogin and provide a name for certificate and click **generate**.

authentik  **Certificate-Key Pairs**  

Import certificates of external providers or create certificates to sign requests with.

Search...   [Create](#) [Generate](#) [Refresh](#) [Delete](#) 1 - 2 of 2  

 Name ↓	Private key available?	Expiry date	Actions
 > authentik Self-signed Certificate	✓ Yes (RSA)	✓ 9/12/2025, 9:57:22 am	
 > ezeelogin	✓ Yes (RSA)	✓ 10/12/2025, 11:29:19 am	

1 - 2 of 2  

User interface

- Dashboards >
- Applications >
- Events >
- Customisation >
- Flows and Stages >
- Directory >
- System** ▾
 - Tenants
 - Certificates**
 - Outpost Integrations
- Enterprise >

authentik  **Certificate-Key Pairs**  

Import certificates of external providers or create certificates to sign requests with.

Search...   [Create](#) [Generate](#) [Refresh](#) [Delete](#) 1 - 2 of 2  

Generate Certificate-Key Pair 

Common Name *

Subject-alt name
Optional, comma-separated SubjectAlt Names.

Validity days *

[Generate](#) [Cancel](#)

User interface

- Dashboards >
- Applications >
- Events >
- Customisation >
- Flows and Stages >
- Directory >
- System** ▾
 - Tenants
 - Certificates**
 - Outpost Integrations
- Enterprise >

Step 9: Edit the **Application provider**, map the certificate, and **configure the NameID property mapping**, then click **Update**.

authentik  **ezeelogin**  

SAML Provider

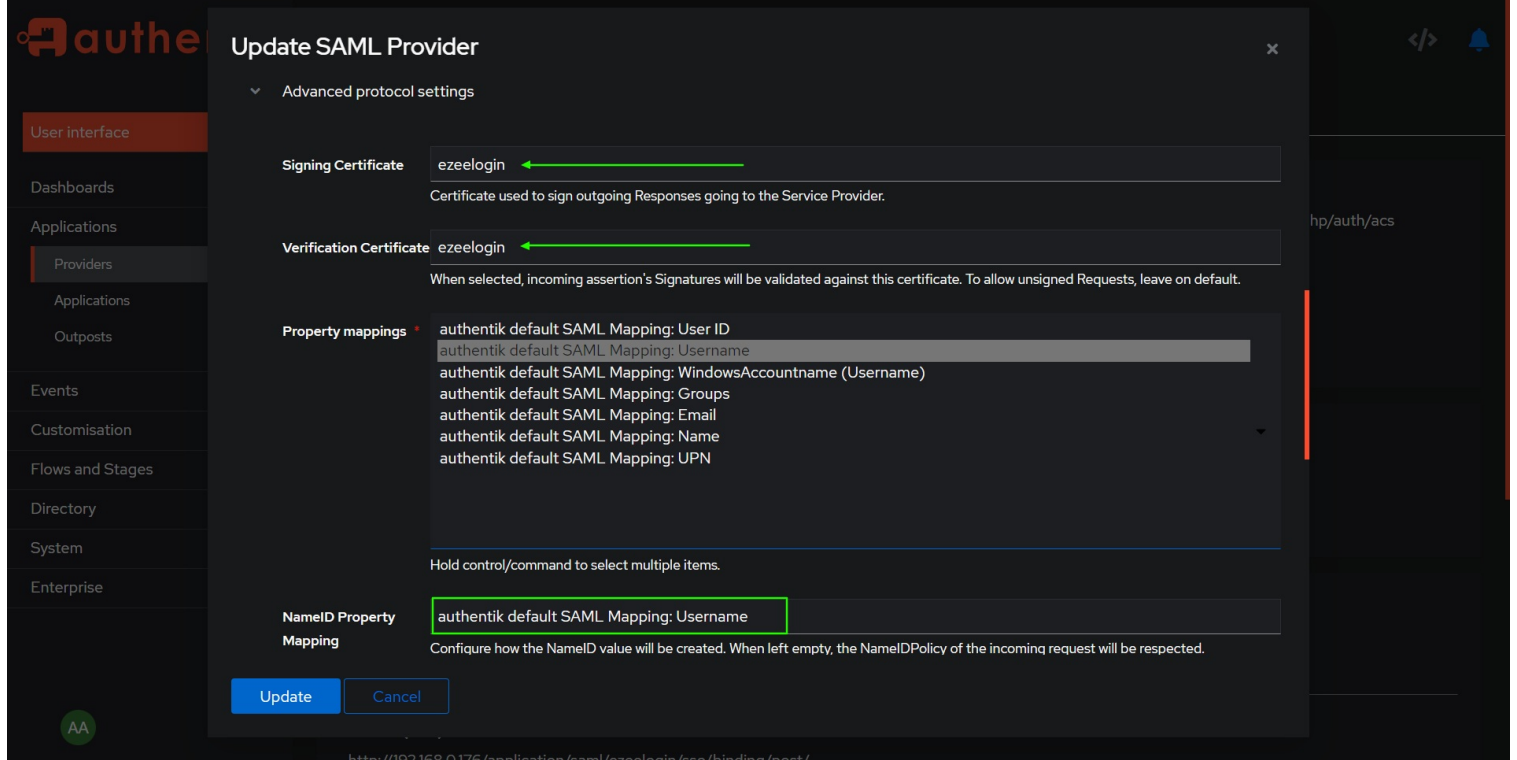
[Overview](#) [Metadata](#) [Preview](#) [Changelog](#)

Name	Assigned to application	ACS URL
ezeelogin	ezeelogin	https://cloudweg.com/index.php/auth/acs
Audience	Issuer	
-	https://cloudweg.com/	

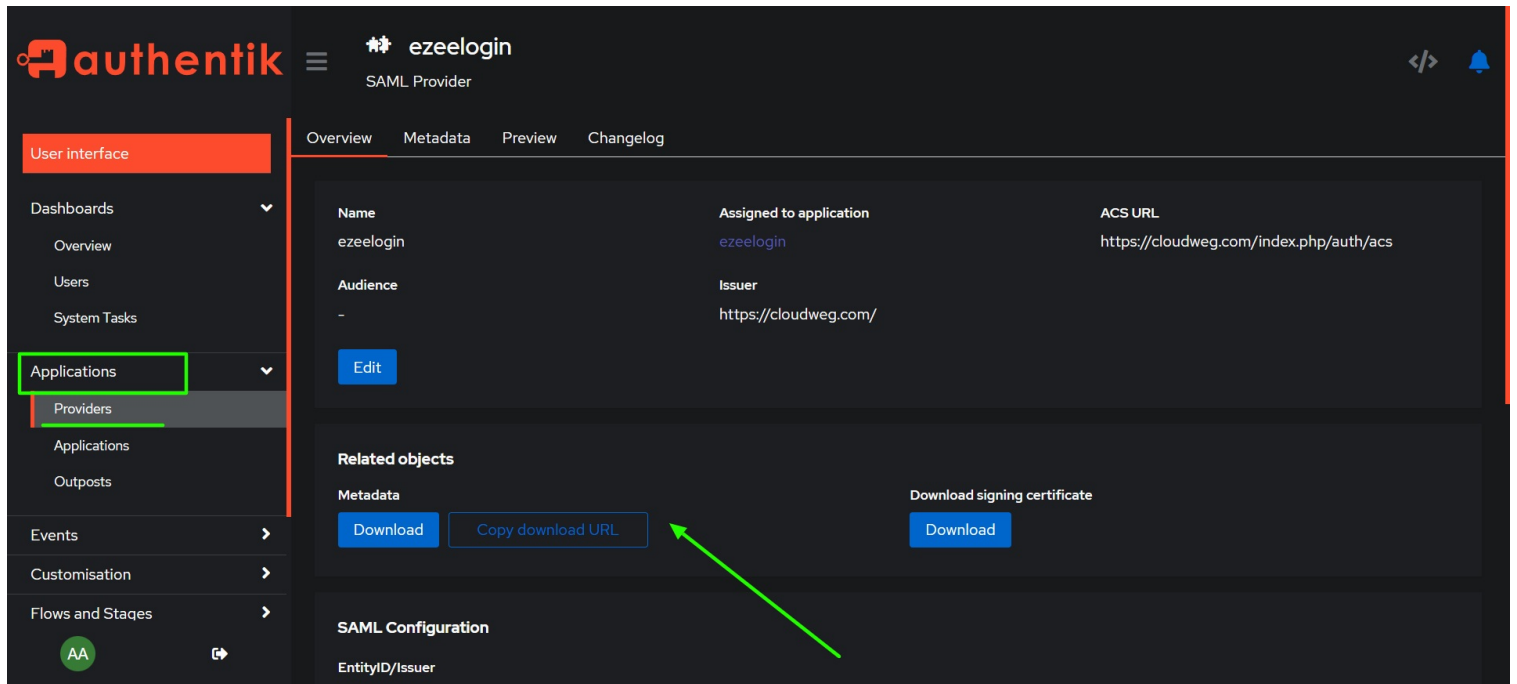
[Edit](#)

User interface

- Dashboards >
- Applications** ▾
 - Providers**
 - Applications
 - Outposts
- Events >



Step 10: Click on the provider name, **copy the download URL**, paste it into the Ezeelogin GUI, and click "**Fetch**" to automatically populate the data and save the settings.



Ezeelogin Welcome, Administrator Logout

SAML Service Provider (SP) Info

Metadata URL	https://cloudweg.com/index.php/metadata
Entity ID	https://cloudweg.com/
Assertion Consumer Service URL	https://cloudweg.com/index.php/auth/acs
Single Logout Service URL	https://cloudweg.com/index.php/auth/slo

SAML Identity Provider (IdP) Settings

Metadata URL [?](#)

Entity ID [?](#)

Single Sign On Service URL [?](#)

Single Logout Service URL [?](#)

Signing Certificate [?](#)

Username Attribute Name [?](#)

Group Attribute Name [?](#)

Firstname Attribute Name [?](#)

Lastname Attribute Name [?](#)

Azure AD Settings

Advanced

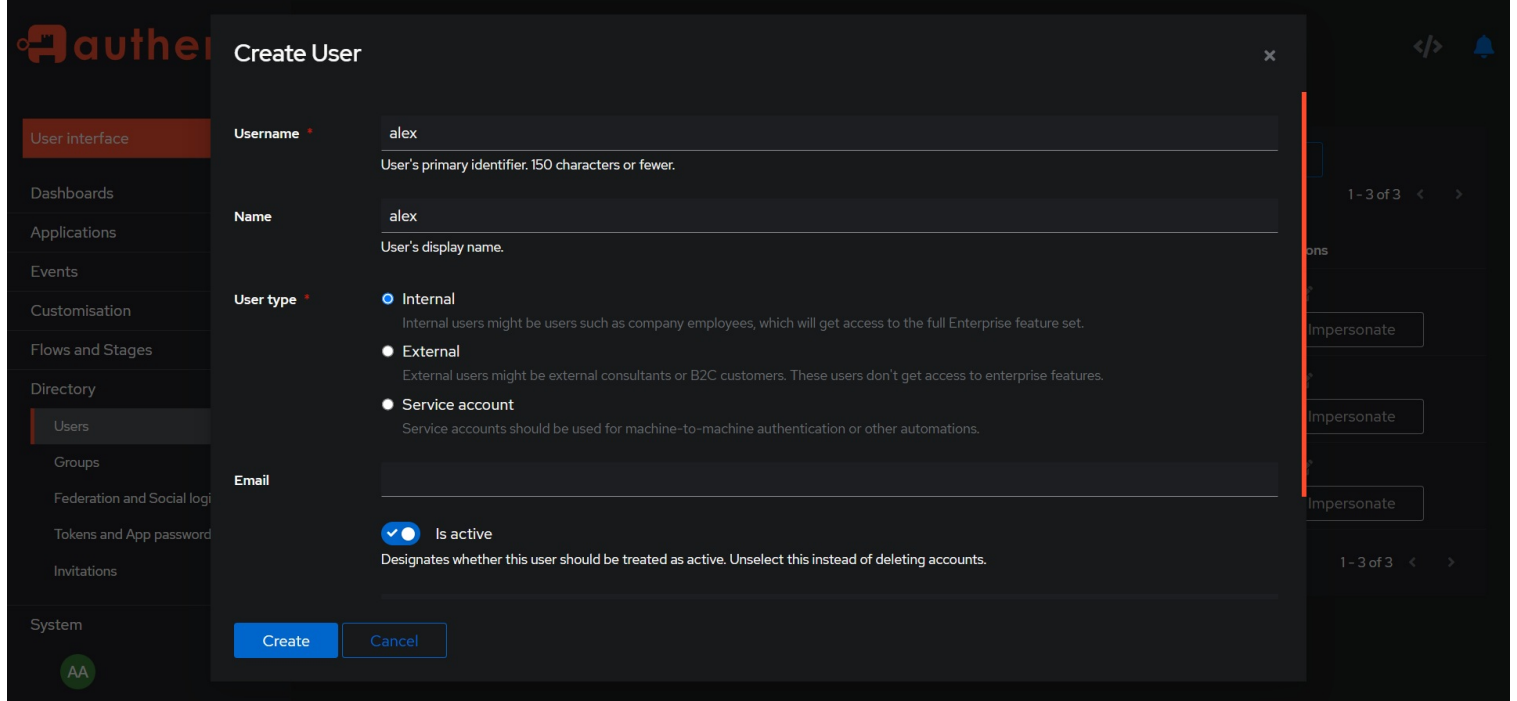
Step 11: Edit the **SAML settings** in the Ezeelogin GUI, and in the **advanced section**, enable **Sign Authentication Requests**.

Ezeelogin Welcome, Administrator Logout

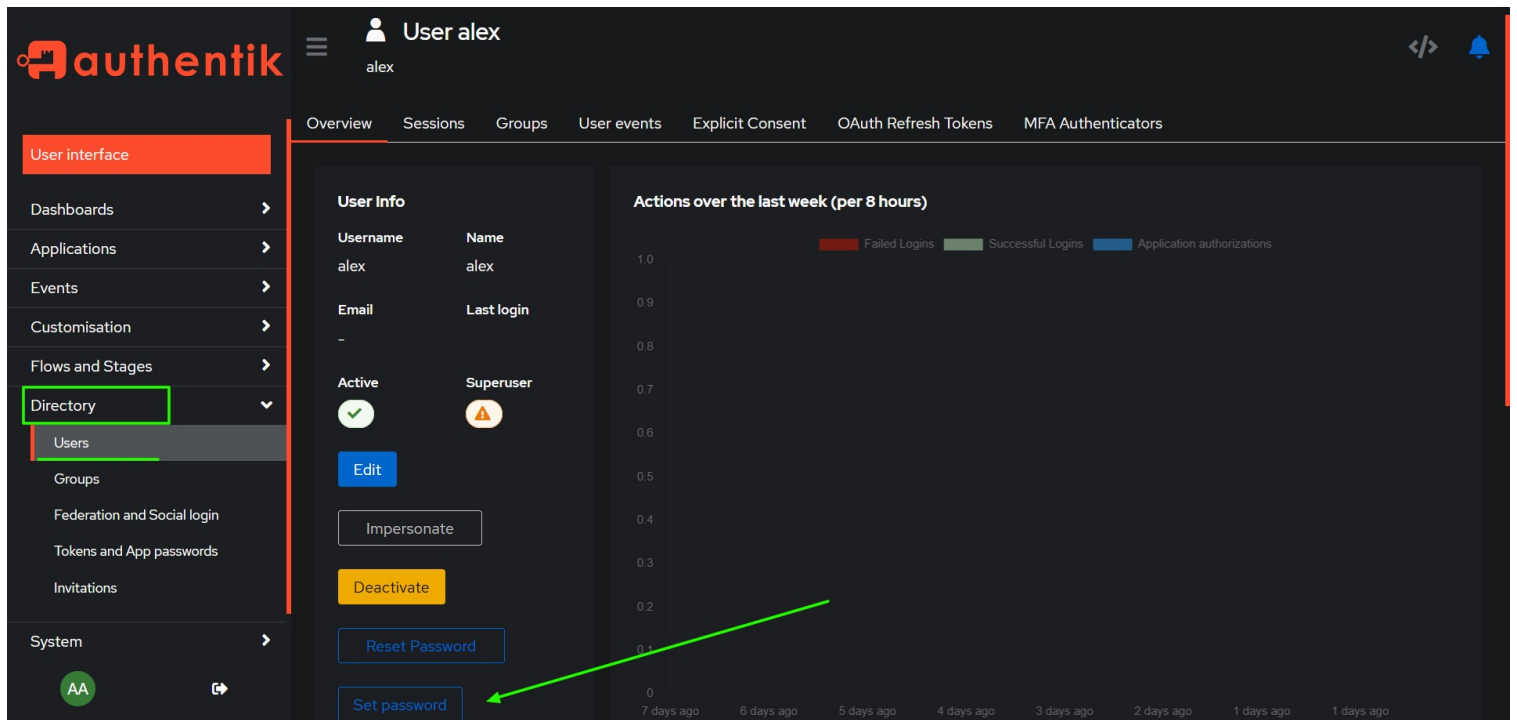
Advanced

Strict ? ☒	Debug ? ☐
Compress Requests ? ☒	Compressed Responses ? ☒
Encrypted Name ID ? ☐	Sign Authentication Requests ? ☒
Sign Logout Requests ? ☐	Signed Logout Responses ? ☐
Sign Metadata ? ☐	Want Signed Messages ? ☐
Want Encrypted Assertions ? ☐	Want Encrypted Name ID ? ☐
Want Signed Assertions ? ☐	Want XML Validation ? ☒

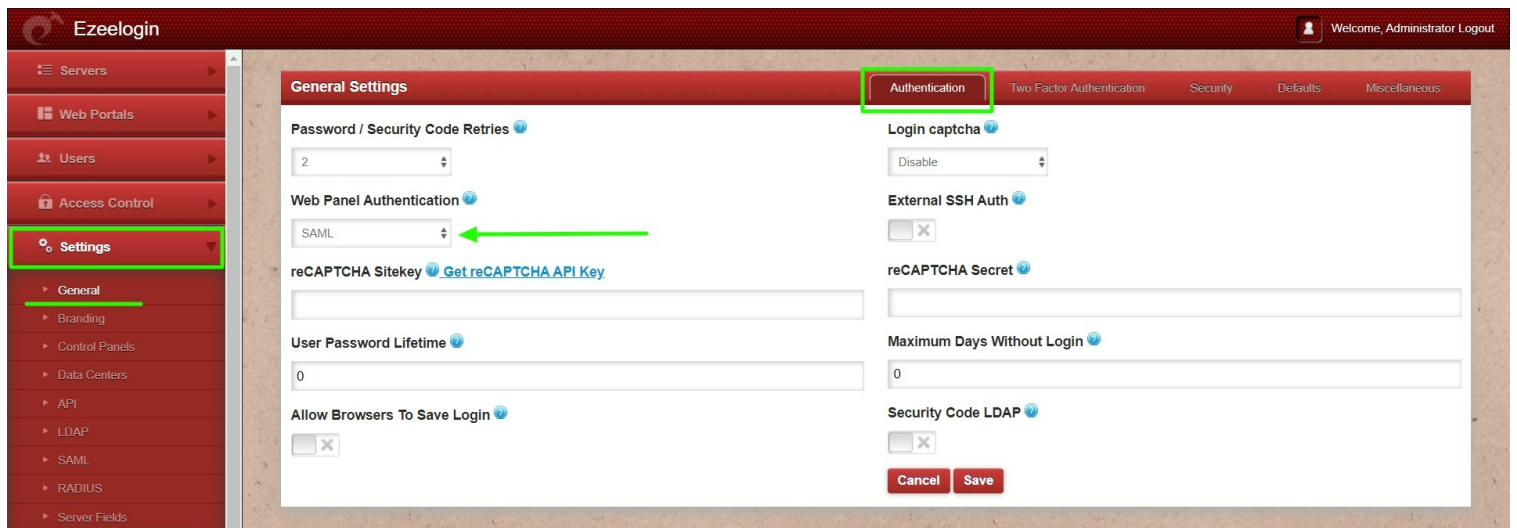
Step 12: Download the certificate and private key, and paste them into the **Ezeelogin SAML settings**.



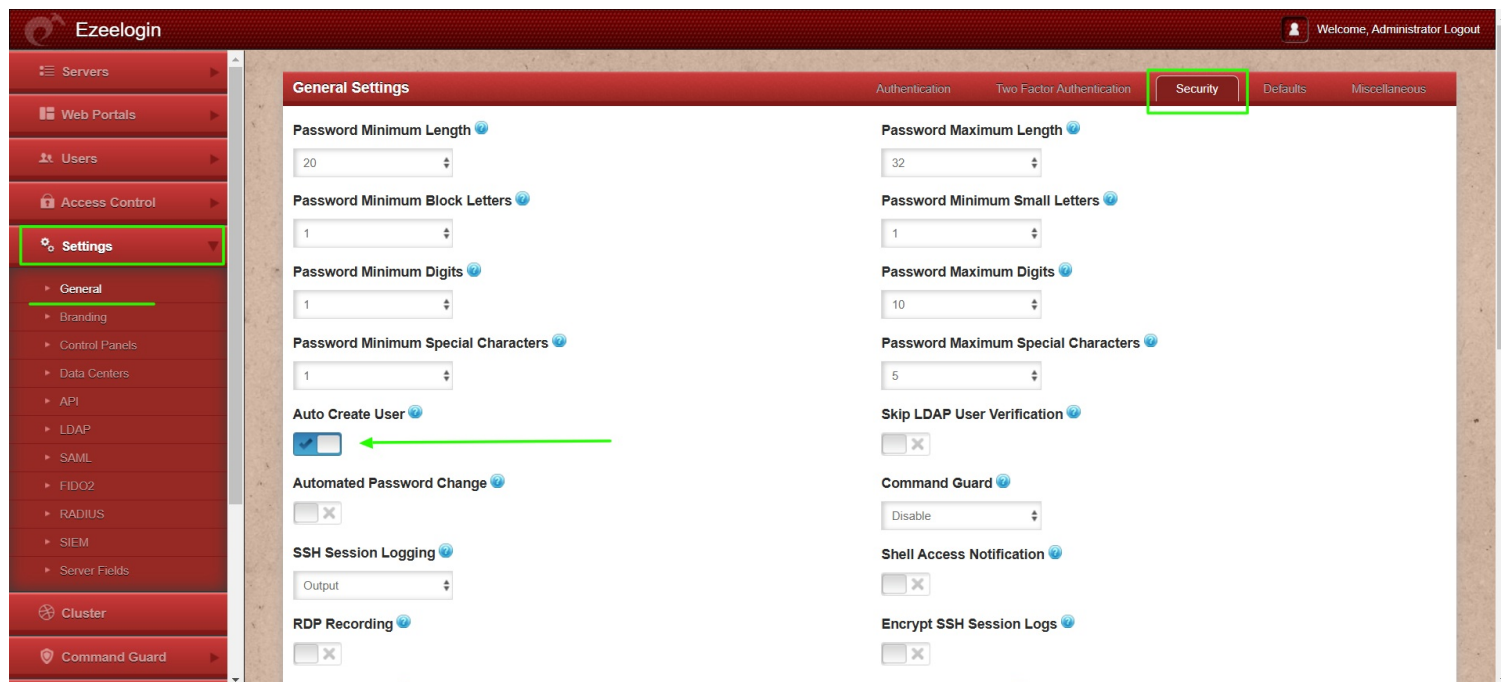
Step 15: Edit the user and set password for the new user.



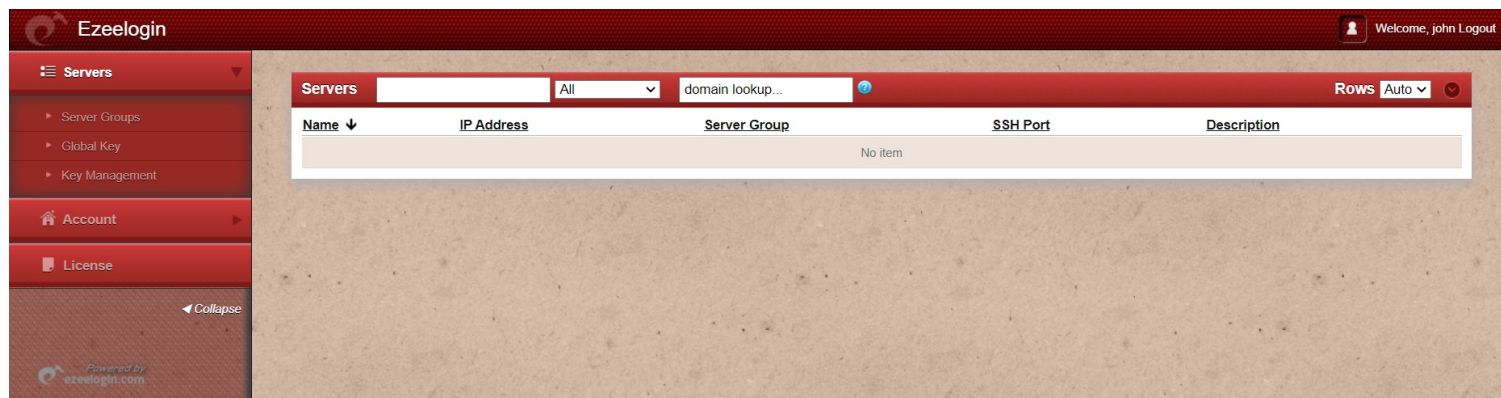
Step 16: Change Web panel Authentication to SAML from Ezeelogin GUI > Settings > General > Authentication



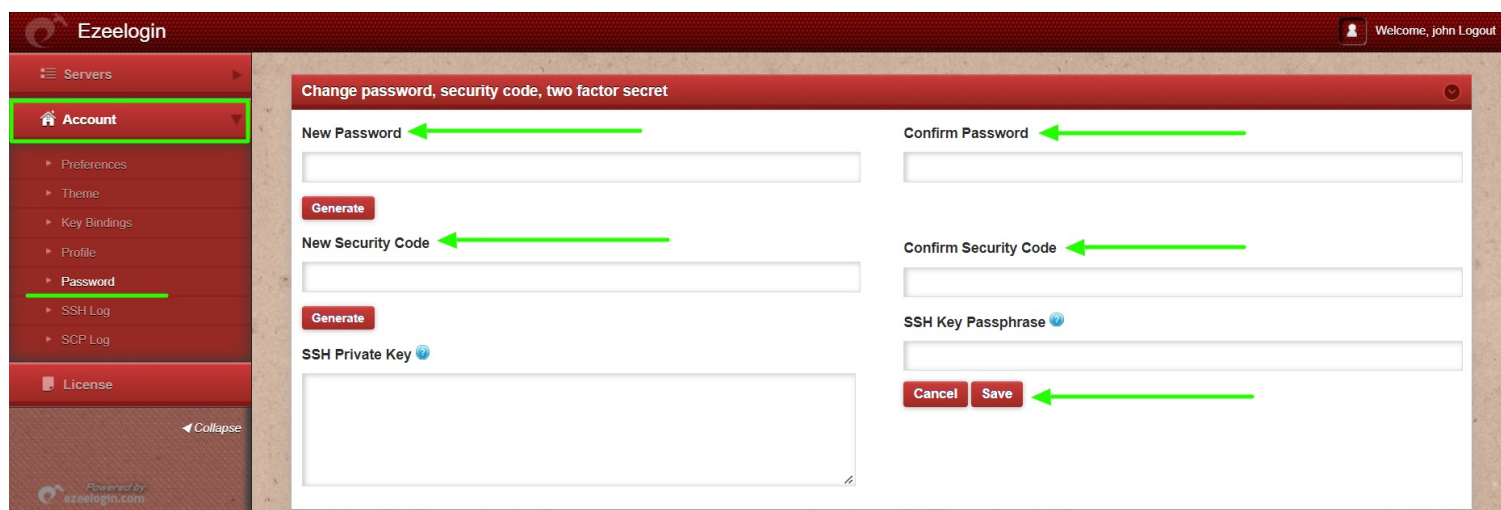
Step 17: Enable **Auto Create** User from **Ezeelogin GUI -> Settings -> General -> Security -> Enable Auto Create User**.



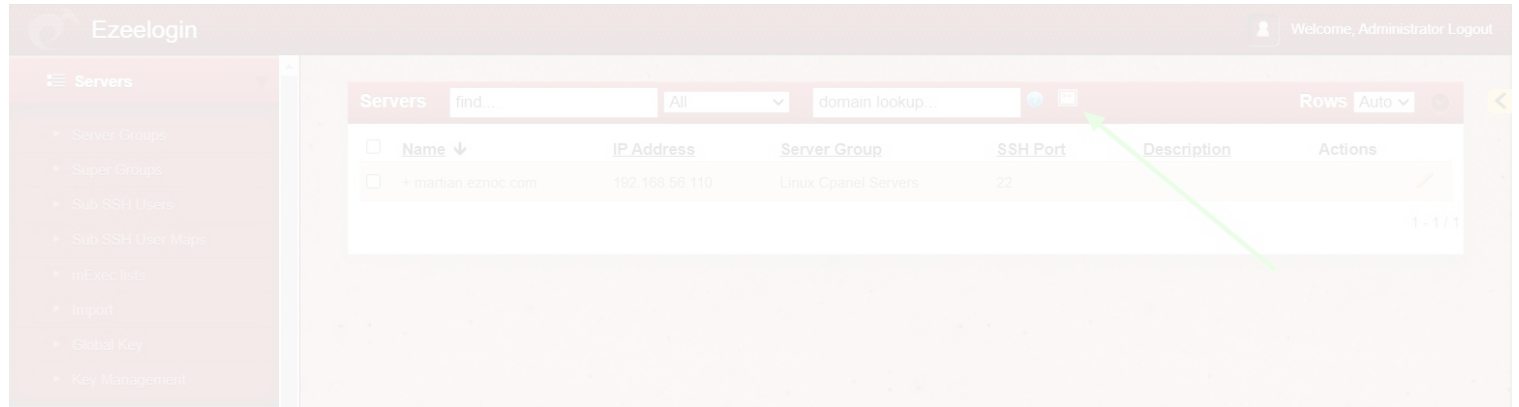
Step 18: Login to Ezeelogin GUI with SAML authentication.



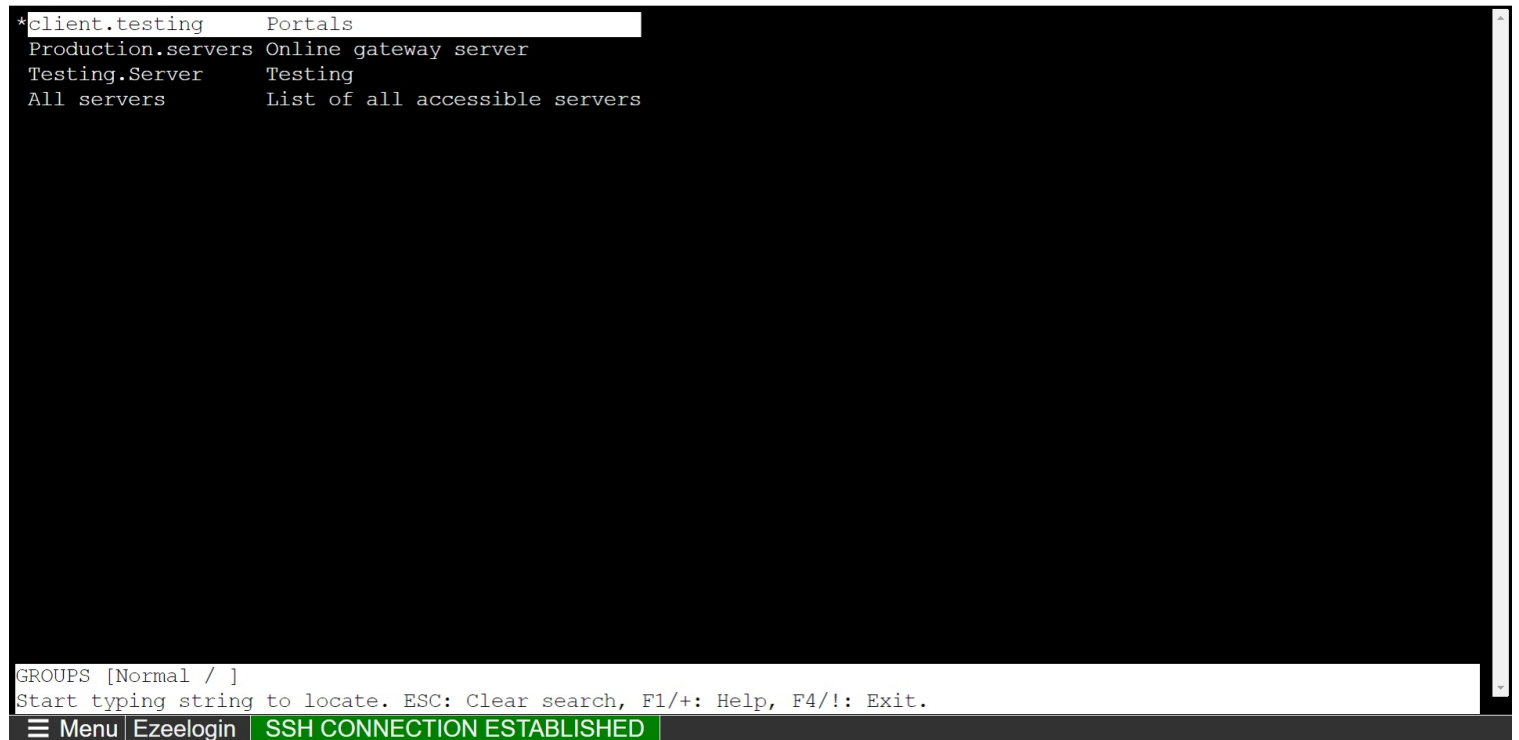
Step 19: After logging into GUI, you need to **reset the password and security code of the SAML user** under **Account -> Password** in order to SSH to the EZSH shell.



Step 15: Login 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.

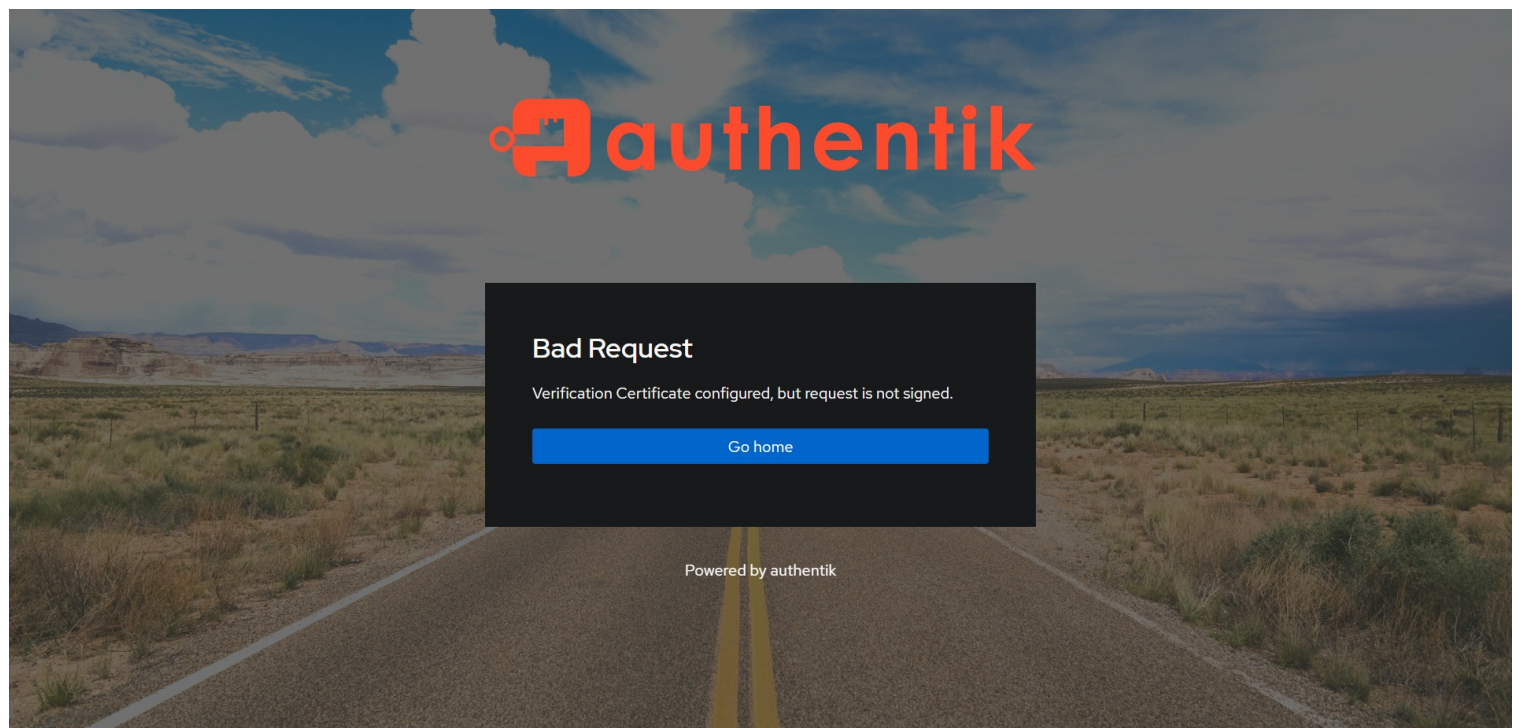


WebSSH terminal will open like below. Users can navigate the server group with the Up and Down arrow buttons and enter to login into the server.



Common error while accessing Ezeelogin with Authentik SSO login.

Bad Request Verification Certificate configured, but request is not signed.



Verify Ezeelogin settings with step 11 and 12 from above steps to fix the above error.

Related Articles:

[Integrating SSO/SAML with Ezeelogin PAM](#)

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

Online URL: <https://www.ezeelogin.com/kb/article/integrate-authentik-sso-with-jumpserver-759.html>