

Login as superadmin when SSO is enabled globally

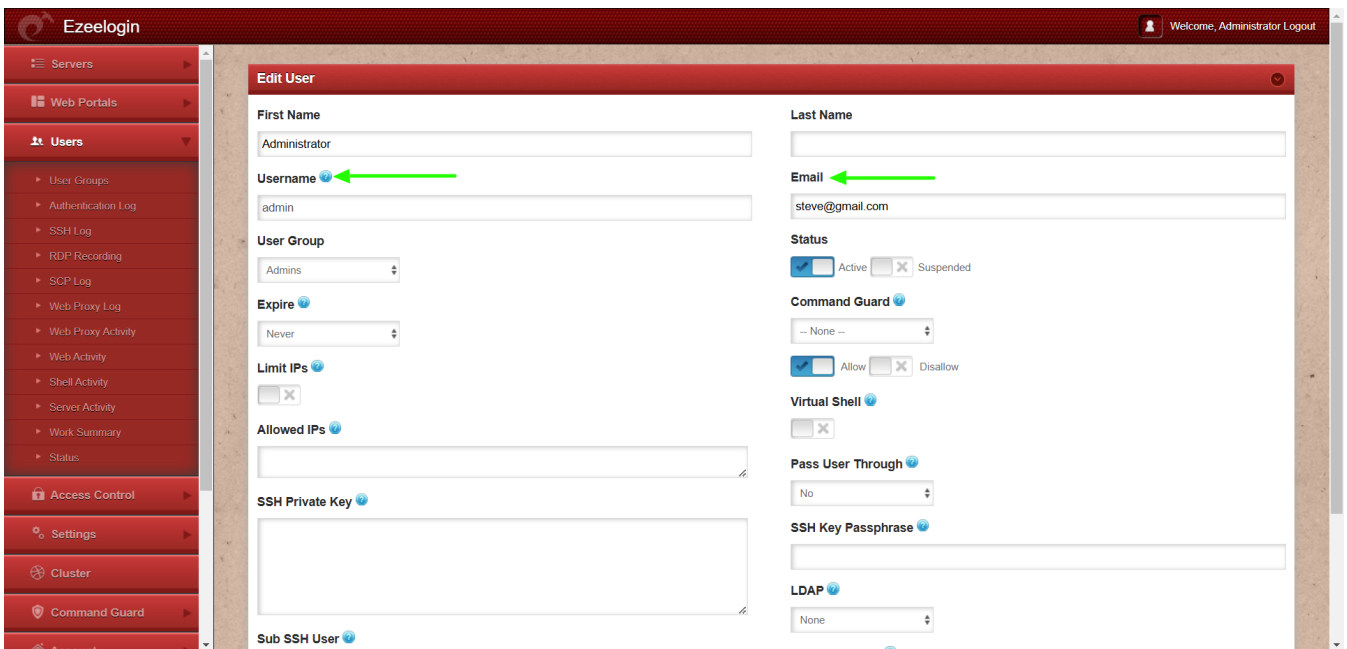
753 Jisna Joseph November 22, 2024 [Features & Functionalities](#) 527

How to login as superadmin user when SSO is enabled?

Overview: This article helps superadmin user (user account created at the time of installation) to login to GUI while using SSO.

METHOD 1

Step 1: Add the superadmin user(user account created at the time of installation) in Ezeelogin to [SSO](#) with the exact username and Email address as used in Ezeelogin.



Ensure that the superadmin user's email address in Ezeelogin matches the email used in SSO, as Ezeelogin uses email for user verification by default.

Step 2: Once the superadmin user has been added to SSO with the exact username and email address, they should be able to log in using [SSO](#).

METHOD 2

This is an alternative method where you can log in without [SAML authentication](#). We are not disabling the SAML here, instead users can login without SAML authentication with the provided url.

Step 1: Navigate to **Settings -> SAML -> Advanced option -> Enable Allow Internal Authentication**.

The screenshot shows the Ezeelogin administration interface. On the left is a navigation menu with 'Settings' and 'SAML' highlighted. The main content area is divided into sections: 'SAML Service Provider (SP) Info', 'SAML Identity Provider (IdP) Settings', and 'Azure AD Settings'. The 'Advanced' sub-section under 'SAML Identity Provider (IdP) Settings' is expanded, showing various configuration options. The 'Allow Internal Authentication' checkbox is checked, and the 'Internal Auth URL' is displayed as `https://cloudweg.com/ezelogin/index.php/auth/login/1`.

SAML Service Provider (SP) Info	
Metadata URL	<code>https://cloudweg.com/ezelogin/index.php/metadata</code>
Entity ID	<code>https://cloudweg.com/ezelogin/</code>
Assertion Consumer Service URL	<code>https://cloudweg.com/ezelogin/index.php/auth/acs</code>
Single Logout Service URL	<code>https://cloudweg.com/ezelogin/index.php/auth/slo</code>

SAML Identity Provider (IdP) Settings - Advanced

- Strict**:
- Compress Requests**:
- Encrypted Name ID**:
- Sign Logout Requests**:
- Sign Metadata**:
- Want Encrypted Assertions**:
- Want Signed Assertions**:
- Relax Destination Validation**:
- Reject Unsolicited Responses with InResponseTo**:
- Name ID Format**: `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Organization Display Name**:
- Technical Contact Name**:
- Support Contact Name**:
- Signature Algorithm**: `http://www.w3.org/2001/04/xmldsig-more#rsa-sha512`
- Service Provider Certificate**:
- New Service Provider Certificate**:
- Debug**:
- Compressed Responses**:
- Sign Authentication Requests**:
- Signed Logout Responses**:
- Want Signed Messages**:
- Want Encrypted Name ID**:
- Want XML Validation**:
- Match Destination Strictly**:
- Lowercase URL Encoding**:
- Organization Name**:
- Organization URL**:
- Technical Contact Email**:
- Support Contact Email**:
- Digest Algorithm**: `http://www.w3.org/2001/04/xmlenc#sha512`
- Service Provider Private Key**:
- Allow Internal Authentication**:
Internal Auth URL: `https://cloudweg.com/ezelogin/index.php/auth/login/1`

Step 2: After enabling **Allow Internal Authentication**, you will receive an internal auth URL from which you can log in without SAML authentication for Ezeelogin users.



Related Articles:

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

Online URL:

<https://www.ezeelogin.com/kb/article/login-as-superadmin-when-sso-is-enabled-globally-753.html>