

User Manual - Directory Management with OpenLDAP, AD and SSO Integration with ADFS

Introduction

This User Manual provides a detailed guide for managing directory services and authentication integration within the platform. The system seamlessly integrates OpenLDAP, Active Directory (AD), and Active Directory Federation Services (ADFS) to enable centralized **Directory Management** and **Single Sign-On (SSO)**.

Users will interact with the platform based on their assigned roles, performing various tasks such as user management, authentication, and group actions. This guide will walk you through the platform's key features, configuration steps, and role-based actions to ensure an efficient and secure user experience.

Key Features

This application designed to streamline directory management and enhance the user authentication experience. The streamlined integration with OpenLDAP, Active Directory (AD) and Active Directory Federation System (ADFS) ensures the unified approach to managing user identities and access control.

The **centralized Directory Management** allows admin to efficiently manage users, groups with different directory services. By leveraging **Single Sign-On (SSO)**, the platform enables users to authenticate once and access multiple services and applications without the need to re-enter credentials.

Furthermore, role-based access control (RBAC) is implemented, which allows users to perform actions based on their assigned roles, with each role having different levels of permissions for directory management, and access to resources.

TABLE OF CONTENTS

<u>GLOSSARY</u>	<u>3</u>
<u>USE CASE</u>	<u>4</u>
<u>ROLES IN THE APPLICATION</u>	<u>5</u>
<u>AUTHENTICATION PROCESS</u>	<u>6</u>
<u>USER INTERFACE GUIDE</u>	<u>6</u>
LOGIN INTERFACE	
<u>OPENLDAP</u>	<u>7</u>
<u>ACTIVE DIRECTORY</u>	<u>8</u>
<u>SSO</u>	<u>9</u>
DASHBOARD INTERFACE	
<u>ADMIN DASHBOARD</u>	<u>11</u>
<u>USER DASHBOARD</u>	<u>11</u>
<u>ADMIN DASHBOARD FUNCTIONALITIES</u>	<u>11</u>
<u>USER DASHBOARD FUNCTIONALITIES</u>	<u>18</u>

GLOSSARY

AD	Active Directory
SSO	Single Sign On
ADFS	Active Directory Federation Services
RBAC	Role Based Access Control
LDAP	Light Weight Directory Access Protocol
SP	Service Provider
IDP	Identity Provider
SAML	Security Assertion Markup Language
OU	Organizational Unit
CN	Common Name
DN	Distinguish Name
UI	User Interface
RP	Relay Party

USE CASE

1. Simplified Management

- By centralized access to user accounts, OU and groups admin can able to efficiently access and manage directory.

2. Enhance Security

- Ensures users can access resources only when they are authorized through RBAC.

3. Multiple Authentication Experience

- Enable users to login in both traditional authentication and SSO based authentication for seamless login experience.
- For SSO, ADFS provides a claim contains the user employee ID, which is validated by system across directory and validating that employee ID with user data present in the directory service and proceed for appropriate dashboard.

4. Scalability

- Works seamlessly with multiple LDAP based systems like OpenLDAP, AD & ADFS.

ROLES IN APPLICATION

This application supports RBAC method, which allowing users to perform specific tasks and access resources based on the assigned roles.

Each role is defined with distinct permissions to ensure security, efficiency and proper delegation of responsibilities.

1. Admin

- Admin user has full access and responsible for managing the directory service.
- **Permissions:**
 - i. Create, update, delete user accounts.
 - ii. Manage permission to users.
 - iii. Create & manage group members.
 - iv. Reset user password.

2. User

- Regular user has limited access and can perform only related to their own account and general queries.
- **Permissions:**
 - i. Change password.
 - ii. Search users within the directory.

AUTHENTICATION PROCESS

In this application, authentication is managed via both Traditional and SSO methods.

1. Traditional Method:

- Validates authentication with using user credentials against either OpenLDAP or AD.

2. SSO Integration:

- Enables users to authenticate once via ADFS access the application without re-entering credentials.
- Authentication tokens are securely passed between the IDP and the application to maintain session validity and user access.

UI GUIDE - Overview

This section provides a detailed overview of the application's user interface, outlining the available features and actions for users based on their roles.

It includes a walkthrough of the key screens for both OpenLDAP and AD, highlighting how to navigate and use the platform effectively, along with any differences in functionality between the two directory services.

LOGIN INTERFACE

1. OpenLDAP

- User enter the login credentials, which are validated against the OpenLDAP server.
- The Dropdown value is set to “**My Ldap**” which specifies the **connection to the OpenLDAP server within the application.**
- Upon successful login, users are redirected to their role-specific dashboard.

- **Input Fields**

- Username (Text)
- Organizational Unit (Text)
- Password (Text)
- User Type (Radio button)

General Login SSO Login (SAML)

Login

My Ldap ▼

Username * Organizational Unit *

Enter username Enter Organizational Unit

Password *

Enter password

Type: ☒ User ☐ Admin

Login

Powered by Cybernexus

Figure 1: OpenLDAP Directory Login page

2. Active Directory

- The AD login screen is designed to validate the user credentials against the AD server and redirect users to their designated dashboard based on assigned roles.
- The Dropdown value is set to “**Cylock**” which specifies the **connection with AD server within the application.**

- **Input Fields**

- Email (Text)
- Password (Text)

General Login SSO Login (SAML)

Login Cylock

Email *
Enter your email

Password *
Enter password

Login

Powered by Cybernexus

Figure 2: Active Directory Login page

3. SSO

- The SSO interface enables users to authenticate once through the ADFS Identity Provider (IDP) and seamlessly access the application without the need for repeated logins.
- After successful authentication, the user is redirected to application, where they are **granted access to their respective dashboard bases on the role provided by IDP claim through SAML assertion.**
- **Input Fields**
 - Email (Text)
 - Password (Text)

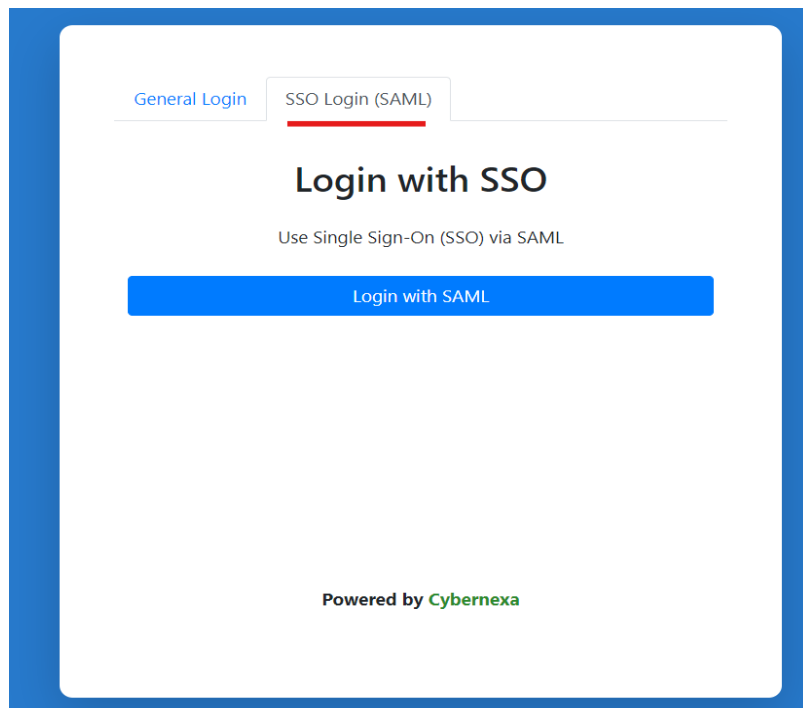


Figure 3: SSO login page (redirected to ADFS login page).



Figure 4: ADFS Login page

DASHBOARD INTERFACE

1. Admin Dashboard

- **Create User:** Able to create user across the directory.
- **Manage User Actions:** View and manage all users, performing admin-specific actions.
- **Manage Organizations:** Able to create (OU_s) in the directory.
- **Manage Group:** Create groups and manage group members associated with the group.
- **Reset User Password:** Reset the any user password at a time.

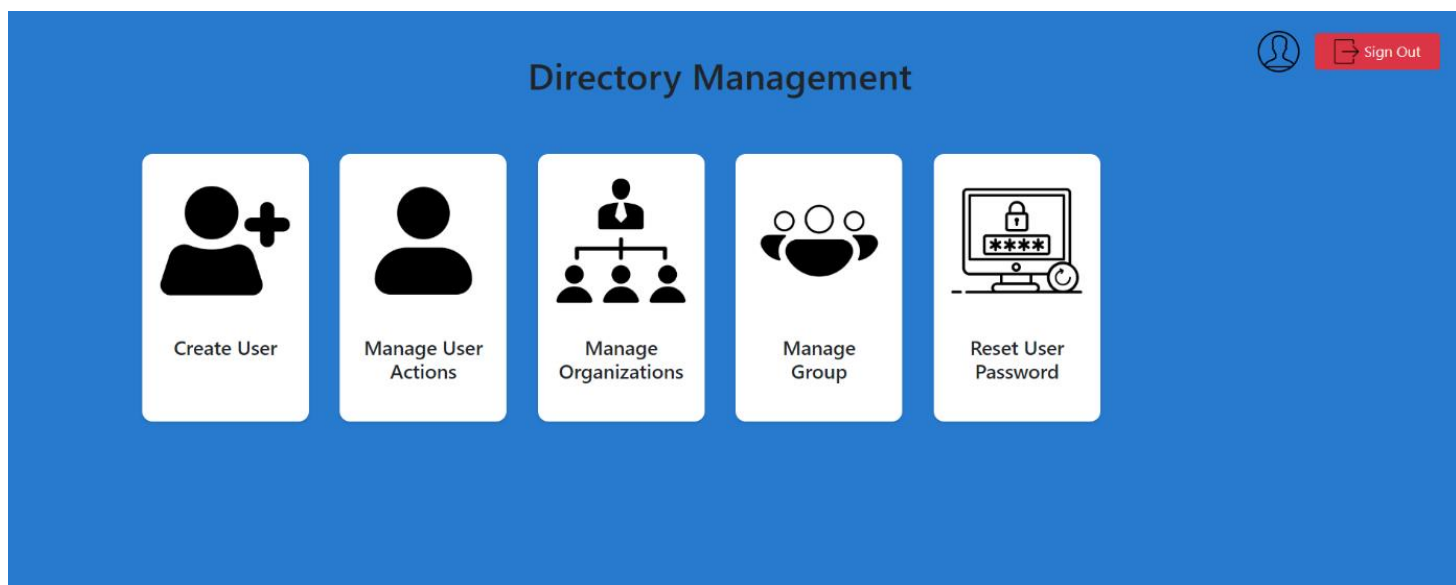


Figure 5: Admin Dashboard with Functionalities

2. User Dashboard

- **Change Password:** User can able to change their own user password.
- **Search User:** User can search any user from the directory.



Figure 6: User Dashboard with Functionalities

ADMIN DASHBOARD FUNCTIONALITIES

1. Create User

- The page which will is used to create the user inside the directory.
- Title Field is used only in OpenLDAP login to choose values (User/Admin) to determine the dashboard type and disabled in AD login.
- All fields presented in below Figure (7) is mandatory.
- Actions allowed rules while creating user.

- **Select OU where the user needs to stored.** OU options depend on the LDAP server connected during login.
- **First name, Last name & Username:** Accepts alphanumeric characters.
- **Phone number and Postal code: allow only 10 digits and 6 digits respectively** (Indian standard).
- **Address:** Supports all character types.
- **Email:** Must follow valid mail ID format.
- **Password:** Stored securely and used later for authentication.

The screenshot shows a 'Create User' form with the following fields and values:

Field	Value	Status
Title *	User	Valid
Select OU *	Users	Valid
First Name *	demo	Valid
Last Name *	user	Valid
Username *	user1	Valid
Phone Number (+91) *	9012345678	Valid
Address *	Lake view street	Valid
Postal Code *	876789	Valid
Email *	user@domain.com	Valid
User Password *	*****	Valid

The form is titled 'Create User' and has a 'Create User' button at the bottom. The background is blue with 'Back' and 'Home' links in the top left and a 'Sign Out' button in the top right.

Figure 7: User Creation Screen

2. Manage User Actions

- The Manage Users page enable admin to view, search and perform various actions on user accounts stored in the directory.

- Search users by Username, Email, Phone Number or OU by selecting a specific field and providing the search value.
- Using the dropdown to filter users based on their current status, such as active, locked or disabled.
- **Actions based on OpenLDAP**
 - **View Member:** View detailed user information (Figure 10).
 - **Delete User:** Remove the user from the directory.
 - **Lock User:** Lock a user account to prevent authentication or further actions.
 - **Unlock User:** Available only when a user is locked to restore access.
 - **Edit User:** Modify stored user details (Figures 11 & 12).
- **Actions based on AD**
 - **View Member:** View detailed user information (Figure 10).
 - **Delete User:** Remove the user from the directory.
 - **Unlock User:** Unlock a user after a lockout event.
 - **Disable User:** Prevent the user from authenticating or making changes in the directory.
 - **Enable User:** Replace the "Disable User" option when a user is disabled to restore access.
 - **Edit User:** Modify stored user details (Figures 11 & 12).

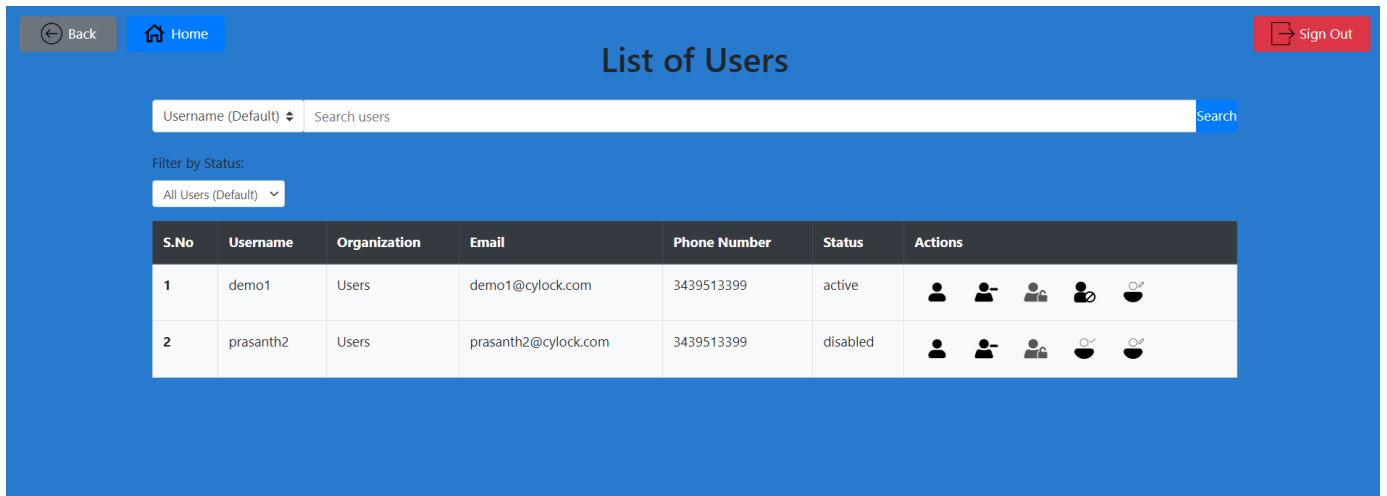


Figure 8: Manage user actions with AD server

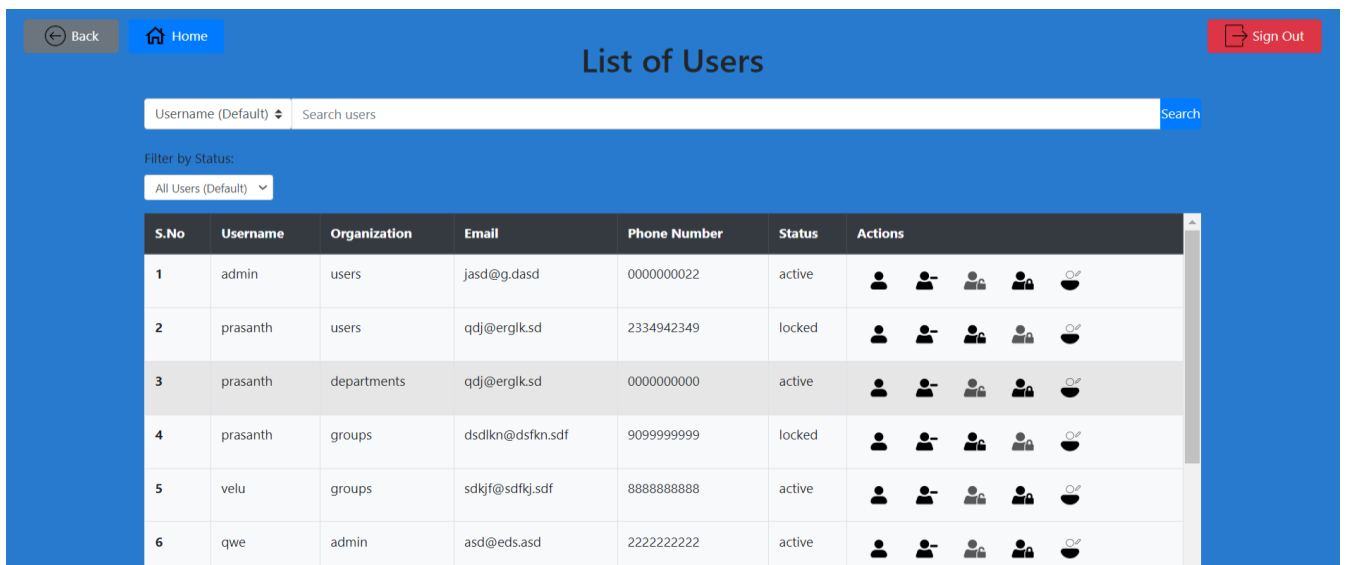


Figure 9: Manage user actions with OpenLDAP server

User Details [Close]

DN: cn=admin,ou=users,dc=myLDAP,dc=com

Username: admin

Email: jasd@g.dasd

Phone: 0000000022

Address: lvfdre

Postal Code: 232392

Status: active

User type: admin

[Close]

Figure 10: Displaying a particular user data.

Edit User Details

Choose Edit Type: General Edit

Username: prasad2 OU: Users

Phone Number (+91):

Email:

Address:

Postal Code:

[Update User]

Edit User Details

Choose Edit Type: Edit Contact Details Only

Username: prasad2 OU: Users

Phone Number (+91):

Email:

[Update User]

Figure 11 & 12: Editing user on general type and only contact details.

3. Manage Organizations

- This page is used to create and list organization across directory.
- By creating organizational unit (OU) we can create a hierarchy structure of a organization in that directory
- **Input Fields**

- Organizational Name
- Description (Optional)

The screenshot shows a web interface titled "Organization Management". At the top, there are navigation buttons for "Back" and "Home", and a "Sign Out" button. The main content area is divided into two sections:

Create Organization

This section contains a form with two input fields: "Organization Name" (required, indicated by a red asterisk) and "Description". Below the form is a blue button labeled "Create Organization".

Organization List

This section displays a table with the following data:

S.No	OU Name	DN	Description
1	groups	ou=groups,dc=myLDAP,dc=com	Organizational unit for groups
2	departments	ou=departments,dc=myLDAP,dc=com	Organizational unit for different departments
3	admin	ou=admin,dc=myLDAP,dc=com	Organizational unit for administrative accounts
4	users	ou=users,dc=myLDAP,dc=com	Organization unit for storing all users in common
5	demo	ou=demo,dc=myLDAP,dc=com	foio

Figure 13: Managing the organizational unit.

4. Manage Groups

- Manage groups page allows admin to create and manage groups across directory.
- By creating groups, admin can add users and perform different actions depending on directory service used during authentication.
- **Input Fields (AD)**
 - Group name (Text)
 - OU (Dropdown)
 - Group Type (Text)
 - Group Scope (Text)
 - Description (Text & Optional)
- **Input Fields (OpenLDAP)**
 - Group name (Text)
 - OU (Dropdown)
 - Group Type (Text)
 - Description (Text & Optional)

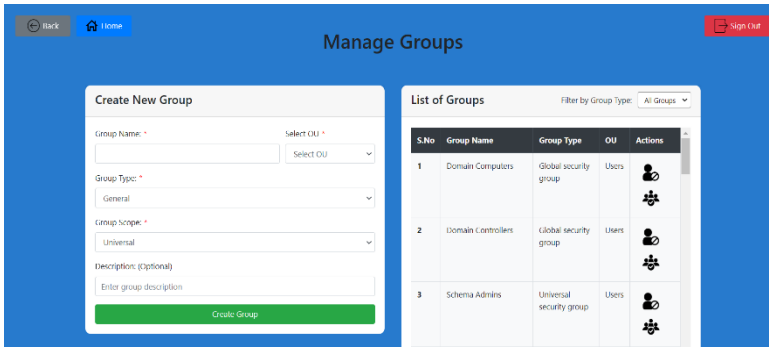


Figure 14: AD Group Page

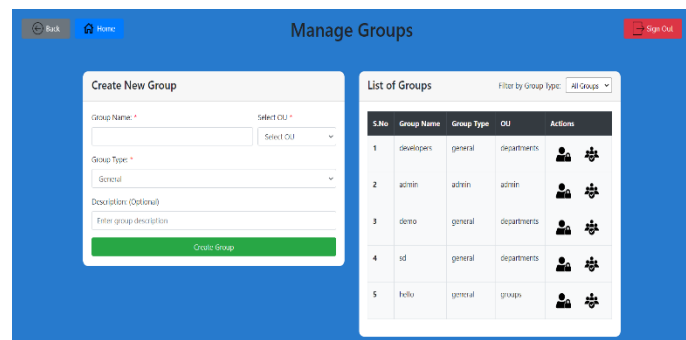


Figure 15: OpenLDAP Group Page

• Group Action in AD

- **Disabling Group:** (Figure 14) Admin can disable all users within the group, preventing them from accessing the directory.
- **Manage Group Members:** Allowing admin to view and remove from group (Figure 16).

• Group Action in OpenLDAP

- **Locking Group:** (Figure 15) Admin can lock all users within the group, preventing them from accessing the directory.
- **Manage Group Members:** Allowing admin to view and remove from group (Figure 16).

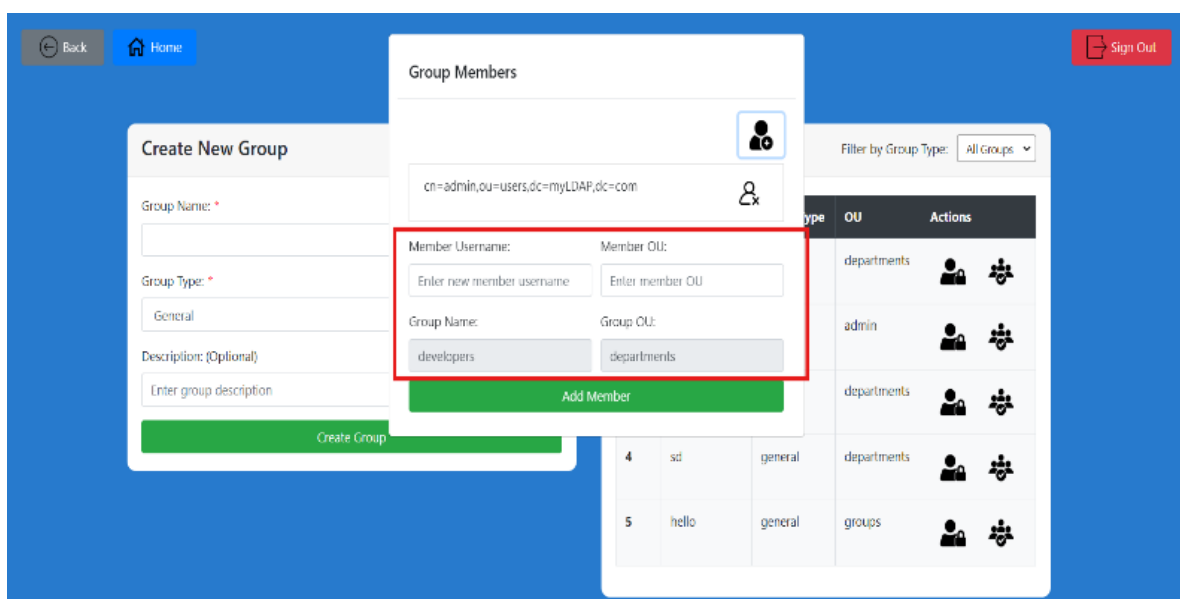


Figure 16: Managing group in OpenLdap and AD.

5. Reset Password

- Reset Password page is used by admin to reset all user password for further authentication and security purposes.
- **Input Fields (AD):**
 - Username (Text)
 - Organizational Unit (Dropdown)
 - New Password (Text)
 - Confirm Password (Text)

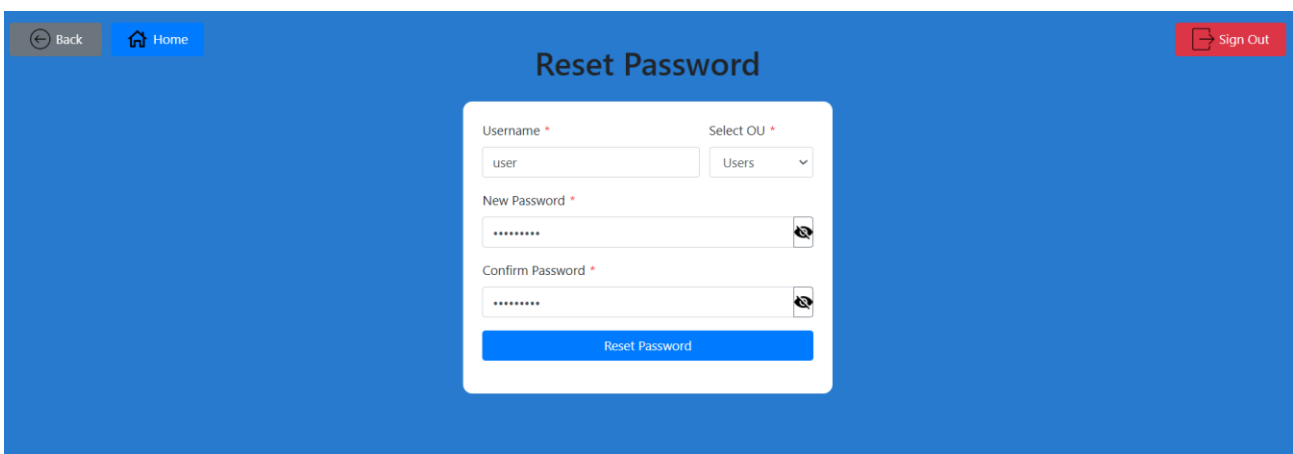
The screenshot shows a web application interface with a blue background. At the top left, there are two buttons: 'Back' with a left arrow icon and 'Home' with a house icon. At the top right, there is a 'Sign Out' button with a right arrow icon. In the center, the title 'Reset Password' is displayed. Below the title is a white form box containing four input fields: 'Username' with a red asterisk, 'Select OU' with a red asterisk, 'New Password' with a red asterisk, and 'Confirm Password' with a red asterisk. The 'Username' field contains the text 'user'. The 'Select OU' field is a dropdown menu showing 'Users'. The 'New Password' and 'Confirm Password' fields contain masked text (dots). To the right of each password field is an eye icon for toggling visibility. At the bottom of the form box is a blue button labeled 'Reset Password'.

Figure 17: Resetting password of a user

USER DASHBOARD FUNCTIONALITIES

1. Change Password

- The change password is self-service page, **where non admin users can use this page to change their own password (Figure 18).**
- **Input Fields**
 - Current Password (Text)
 - New Password (Text)
 - Confirm Password (Text)

Figure 18: Change Password page.

- As Change password is self-service page, so user details will be fetched (username and OU) directly from session once authenticated.
- Once all the details are given user new password can be used on further login.

2. Search User

- The search user is another self-service page, where non admin users can search other users from their directory (**Figure19**).
- Username should be passed for search value to get the users.

Username	First Name	Last Name	Email	Phone Number	Address	Postal Code
sgs	prasanth	ddg	qdj@erglk.sd	2334942349	qldmm	304459
ds	prasanth	fg	qdj@erglk.sd	0000000000	ABCD	563345
g	prasanth	g	dsdlkn@dsfkn.sdf	9099999999	9nn	000000

Figure 19: Search User page.