

Directory Management – OpenLdap, AD and SSO Integration with ADFS

A platform integrates with OpenLdap and Active Directory (AD) and Active Directory Federation System (ADFS) to provide centralized Directory Management and enabled SP-initiated Single Sign-On (SSO).

This platform will have different types of actions to be performed based on authenticated user assigned roles.

Architectural Design Explanation:

a. Synchronous Engine:

- a. This application will provide a **synchronously connection between Active Directory (AD) and OpenLDAP**.
- b. A bidirectional approach process keeps user and group information uniform across both directory services.

b. Traditional Authentication and SSO Module:

- a. **Traditional authentication:** will be performed in both Ldap protocols (OpenLdap and AD).
- b. **SP-Initiated Single Sign-On:** Leverages ADFS to enable users to authenticate through a centralized system, ensuring a seamless login experience across multiple services.

c. Directory Management Layer:

- a. **RBAC UI Interface:** Dynamically assigns the role to users and unique user dashboard based on role based:
 - i. **Role – 1 (Admin):** This role has access across all major actions.
 - 1. **User Creation, Updates, Deletion.**
 - 2. **Manging permission to all users across directory.**
 - 3. **Adding user to multiple groups and OU's.**
 - ii. **Role – 2 (User):** This role has actions directly related to their account.
 - 1. **Authentication**
 - 2. **Change Password**
 - 3. **Search users across Directory.**

Login Page:

1. OpenLdap Login Page:

While login it will connect to OpenLDAP server check user credentials are valid and then redirect to user dashboard (based on user type role).

Input Fields:

- a. Username (Text)
- b. Organizational Unit (Text)
- c. Password (Text)
- d. 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

Image 1: OpenLdap Directory Login page

(My Ldap refers to the Openldap server for naming purpose)

2. Active Directory Login Page:

While login it will connect to Active Directory server check user credentials are valid and then redirect to user dashboard (based on user role).

Input Fields:

- a. Email (Text)
- b. Password (Text)


General Login SSO Login (SAML)

Login

Cylock ▼

Email *

Password *

Login

Powered by Cybernixa

Image 2: Active Directory Login page
(Cylock refers to the AD server for naming purpose)

3. Single Sign on (SSO) Login Page:

This login allow user to login once via ADFS with AD seamlessly.

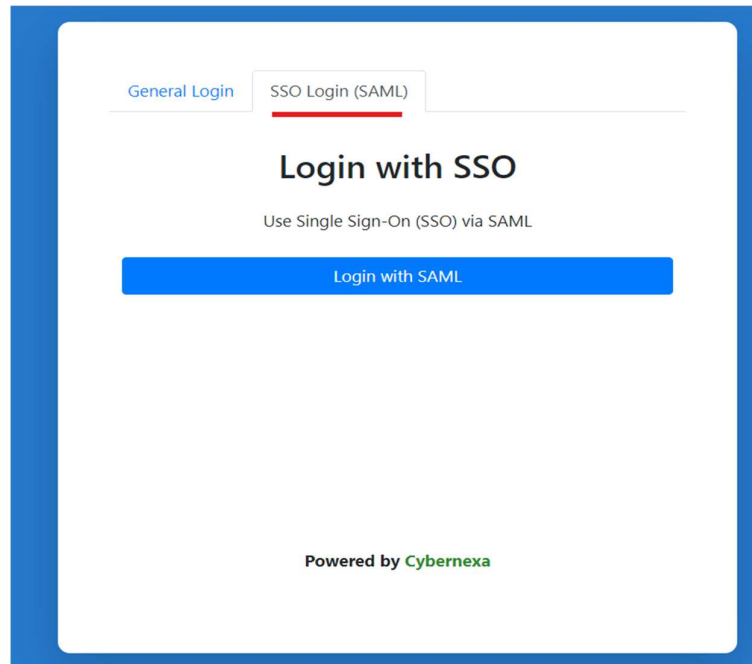


Image 3: SSO login page (SP – initiated).

This UI will redirect to ADFS official login page with assigned Relay Party (RP) uniquely assigned for this AD.

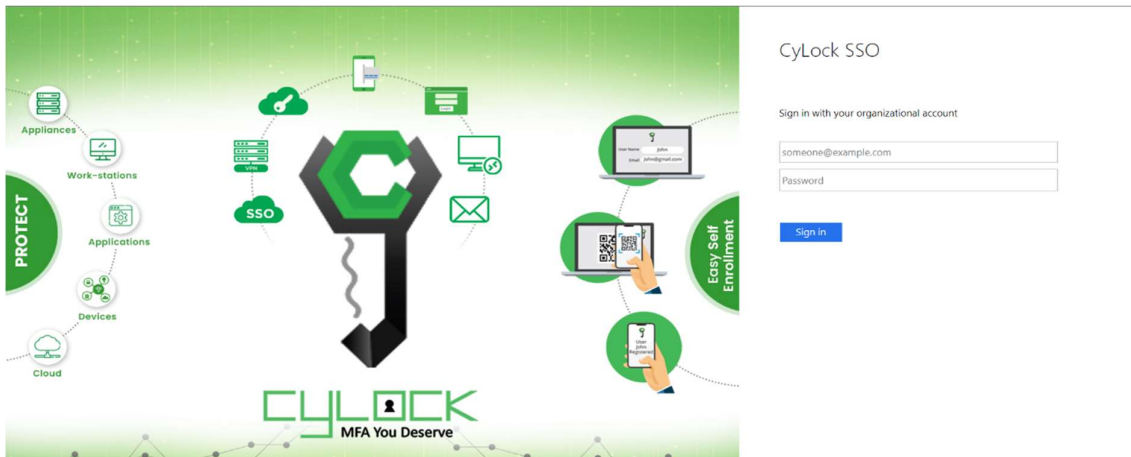


Image 4: ADFS Login page

Once email and password are given it will check and redirect to Directory (AD) application dashboard.

4. Dashboard View:

4.1 Admin Dashboard:

- a. **Create User:** Able to create user over the directory.
- b. **Manage User Actions:** Listing users all users from a ldap server and able to do actions to individual users.
- c. **Manage Organizations:** Able to create OU across directory.
- d. **Manage Group:** Able to create group and group actions which will reflect to users associated to the group.
- e. **Reset User Password:** Reset the any user password at a time.

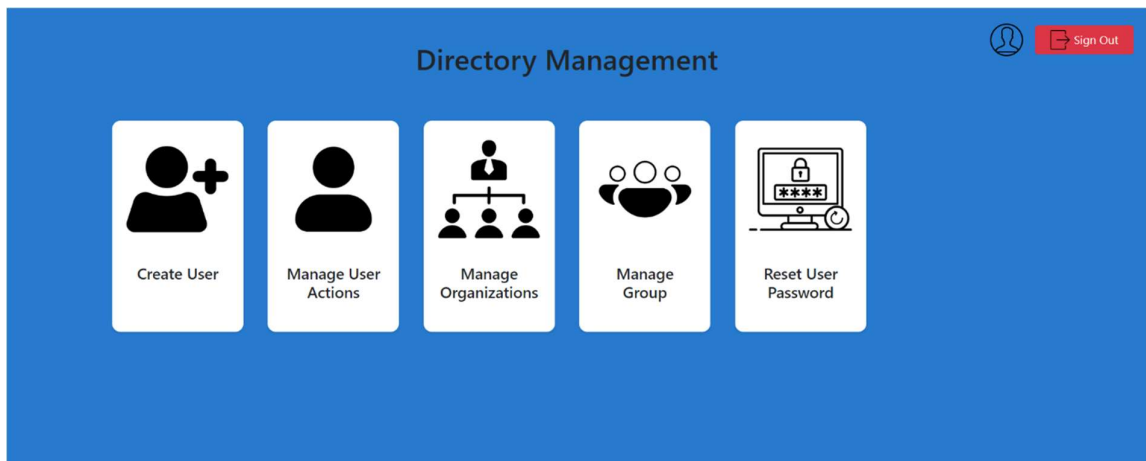


Image 5: Admin Dashboard and Functionalities

4.2 User Dashboard:

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

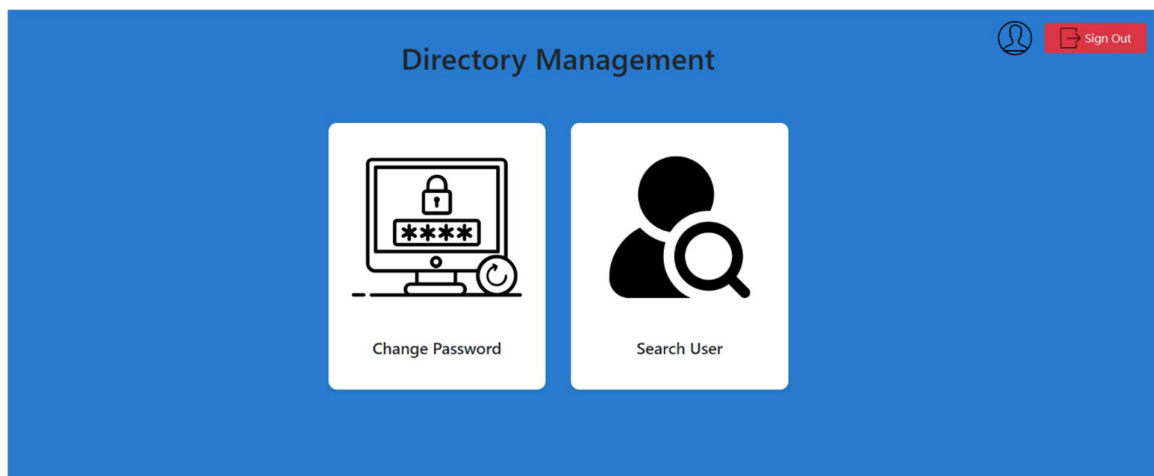


Image 6: User Dashboard and it's Functionalities

5. Admin Dashboard Pages:

5.1 Create User:

- Title Field is used only with OpenLdap login to choose values User / Admin to decide the dashboard, same in AD it will be disabled.
- The page which will be used to create the user inside the directory.
- All fields presented in below image (**Image 7**) are mandatory.
- Actions allowed rules while creating user:
 - **Select OU where the user needs to be stored** (also the OU values will be displayed according to the Ldap server connected while user connected initially).
 - **First name & Last name are allowed only alphabets.**
 - **Username is allowed with alphanumeric characters.**
 - **Phone number and Postal code field will allow only 10 digits and 6 digits respectively** (as per Indian standard).
 - Address is free to add all types of characters.
 - Email value should be maintained as per mail id structure.
 - User Password is stored and used later to authenticate for that with those credentials.

The screenshot shows a 'Create User' form within an admin dashboard. The form is titled 'Create User' and contains the following fields:

- Title ***: A dropdown menu with 'User' selected.
- Select OU ***: A dropdown menu with 'Users' selected.
- First Name ***: A text input field containing 'demo' with a green checkmark.
- Last Name ***: A text input field containing 'user' with a green checkmark.
- Username ***: A text input field containing 'user1' with a green checkmark.
- Phone Number (+91) ***: A text input field containing '9012345678' with a green checkmark.
- Address ***: A text input field containing 'Lake view street'.
- Postal Code ***: A text input field containing '876789' with a green checkmark.
- Email ***: A text input field containing 'user@domain.com' with a green checkmark.
- User Password ***: A password input field with masked characters (dots).

A blue 'Create User' button is located at the bottom of the form. The form is set against a blue background. In the top left corner, there are 'Back' and 'Home' links. In the top right corner, there is a 'Sign Out' link.

Image 7: User Creation Screen

5.2 Manage User Actions:

- a. The page to list the user from the directory with user details and user actions will be shown under actions section.
- b. Search can be operated with username / email / Phone number / Organization, by selecting the either one option and passing the value the search with the field will occur.
- c. Filtering by status, can be done by selecting the dropdown value and users will fetched accordingly.
- d. Actions on manage user page varies slightly based on ldap server selected when authenticated.
 - AD (Image 8):
 1. **View Member:** It is used to view details of a particular user (Image 10).
 2. **Delete User:** This will use to delete the user from directory.
 3. **Unlock User:** This is enabled and used to unlock user from lock state after getting into lockout policy.
 4. **Disable User:** This feature is used to disable user to authenticate and make changes across directory.
 5. **Enable User:** This icon is replaced by disable user logo after the particular user been disabled.
 6. **Edit User:** This will help admin to edit the user details from been stored in directory (Image 11 & 12).
 - OpenLdap (Image 9):
 1. **View Member:** It is used to view details of a particular user (Image 10).
 2. **Delete User:** This will use to delete the user from directory.
 3. **Lock User:** This is used to lock user from directory and stops to from authenticate and make other actions.
 4. **Unlock User:** This icon is enabled to use only when user is locked and make the user free to access and authenticate.
 5. **Edit User:** This will help admin to edit the user details from been stored in directory (Image 11 & 12).

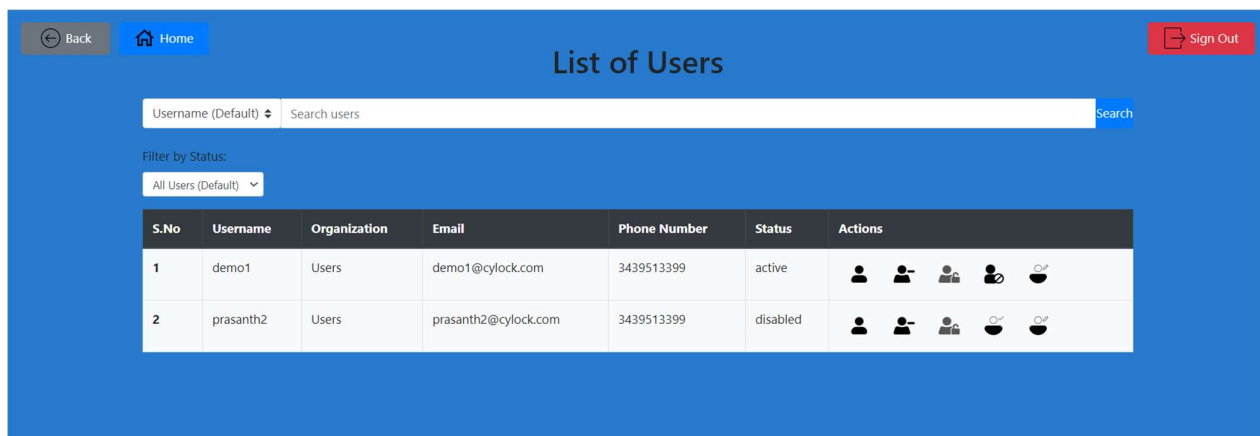


Image 8: Manage user actions with AD server

Back

Home

List of Users

Sign Out

Username (Default)

Search users

Search

Filter by Status:

All Users (Default)































S.No	Username	Organization	Email	Phone Number	Status	Actions
1	admin	users	jasd@g.dasd	0000000022	active	    
2	prasanth	users	qdj@erglk.sd	2334942349	locked	    
3	prasanth	departments	qdj@erglk.sd	0000000000	active	    
4	prasanth	groups	dsdlkn@dsfkn.sdf	9099999999	locked	    
5	velu	groups	sdkjf@sdfkj.sdf	8888888888	active	    
6	qwe	admin	asd@eds.asd	2222222222	active	    

Image 9: Manage user actions with OpenLdap server

User Details

×

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

Image 10: Displaying a particular user data (read only).

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

5.3 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)

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

Image 13: Adding and displaying the organizational unit from OpenLdap server.

5.4 Manage Groups:

- This page admin page is used to create groups across directory.
- By creating groups, admin can add user's and perform different actions based on ldap protocol opted when authenticated.

c. Input Fields (AD):

- Group name (Text)
- Organizational Unit (Dropdown)
- Group Type (Text)
- Group Scope (Text)
- Description (Text & Optional)

d. Input Fields (OpenLdap):

- Group name (Text)
- Organizational Unit (Dropdown)
- Group Type (Text)
- Description (Text & Optional)

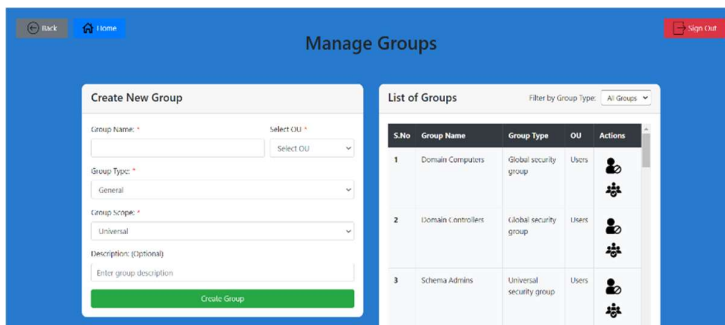


Image 14: Group UI from AD

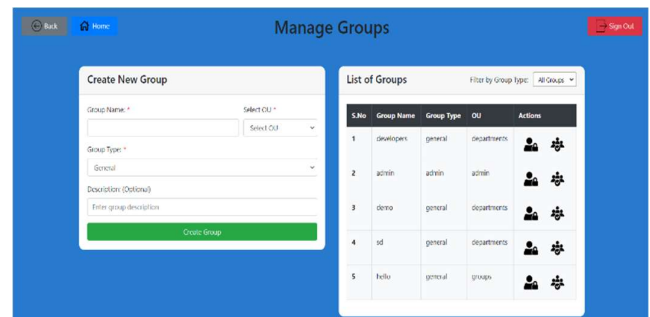


Image 15: Group UI from OpenLdap

- e. From (image 14), the group details of AD can be disabled. Which will disable all users present in that group & view member icon is used to view the members and also has access to update the group by adding new members and delete existing users from that group (image 16).
- f. From (image 15), the group details of OpenLdap can be locked. Which will lock all the users present in that group & view member icon is used to view the members and also access to update the group by adding new members and delete the existing users from that group (image 17).

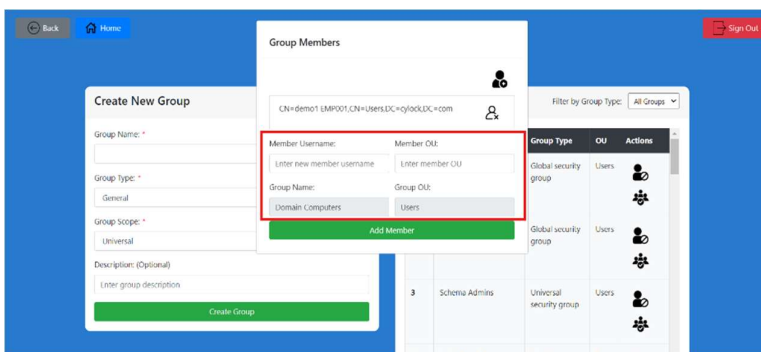


Image 16: Updating group in AD

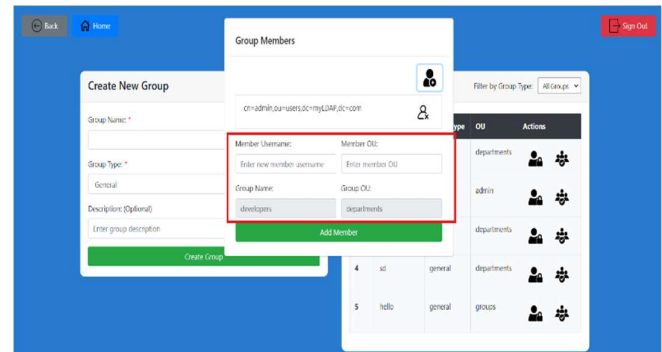


Image 17: Updating group in OpenLdap

5.5 Reset Password:

- a. The reset page will be same for both ldap protocols, which is used to reset any user password by admin (**Image 18**).

- b. **Input Fields (AD):**

- Username (Text)
- Organizational Unit (Dropdown)
- New Password (Text)
- Confirm Password (Text)

- c. **Input Fields (OpenLdap):**

- Username (Text)
- Organizational Unit (Dropdown)
- New Password (Text)
- Confirm Password (Text)

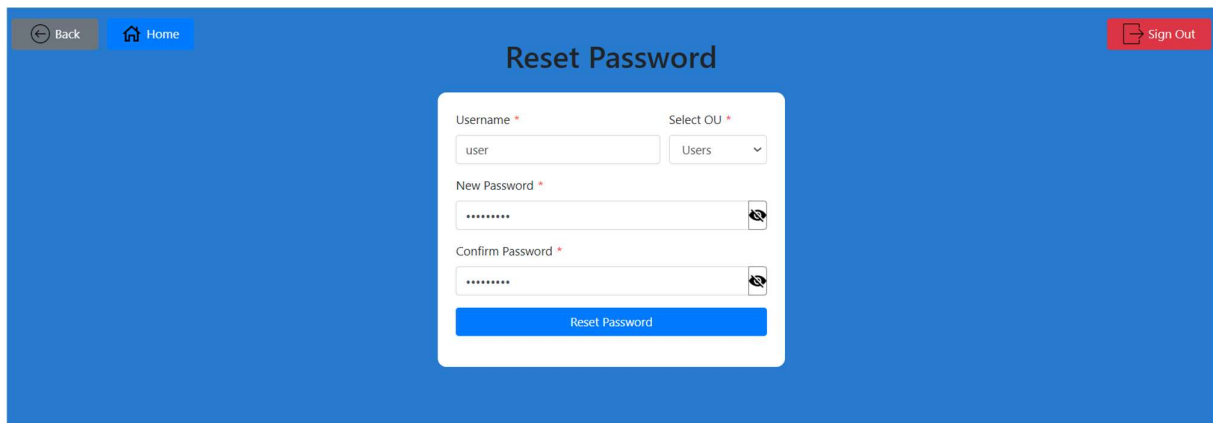
The image shows a web application interface for resetting a password. The background is a solid blue color. At the top left, there are two buttons: 'Back' with a left arrow icon and 'Home' with a house icon. At the top right, there is a 'Sign Out' button with a right arrow icon. In the center, the title 'Reset Password' is displayed in white. Below the title is a white form with a blue 'Reset Password' button at the bottom. The form contains four input fields: 'Username *' with the text 'user', 'Select OU *' with a dropdown menu showing 'Users', 'New Password *' with masked characters and a toggle icon, and 'Confirm Password *' with masked characters and a toggle icon.

Image 18: Resetting password of a user

6. User Dashboard Pages:

6.1 Change Password:

- a. The change password is self service page, where non admin users can use this page to change their own password (**Image 19**).

b. **Input Fields (AD / OpenLdap):**

- Current Password (Text)
- New Password (Text)
- Confirm Password (Text)

Change Password

Username: prasanth2 OU: Users

Current Password: [password field]

New Password: [password field]

Confirm Password: [password field]

Reset Password

Image 19: Change Password page.

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

6.2 Search User:

- a. The search user is another self-service page, where non admin users can search other users from their directory (**Image 20**).
- b. Username should be passed for search value to get the users.

Select OU: [dropdown] prasanth Search

User Details

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	dsdln@dsfkn.sdf	9099999999	9nn	000000

Image 20: Search User page.

7. Use Case:

7.1 Objective:

- To streamline directory management application with access control and directory synchronization across OpenLDAP and Active Directory while providing a seamless Single Sign-On (SSO) experience.

7.2 User Authentication:

- A user logs in through either the **Active Directory Login Page** (direct AD credential validation) or the **Single Sign-On Login Page** (via ADFS for federated authentication).
- For SSO, ADFS provides a claim containing the user's employee ID, which is validated by system across directory and determine the user role and proceed for appropriate dashboard.

7.3 Role-Based Access Control (RBAC):

Based on the user's role, the platform provides access to specific features:

- Admin: Full control over directory operations (user creation, updates, deletions).
- User: Limited access, including authentication, password changes, and directory searches.