User Management Portal

User Manual

Version 11.0

09-Jan-2025

Document Release Note

Notice No. : NA
Customer : National Health Authority, India
Project : PMJAY 2.0

Document Details

Name	Version Number	Description
User Manual	11.0	This document describes the processes and steps to use the UMP Application

Revision Details

Action Taken (Add/Del/Change)	Previous Page Number	New Page Number	Revision Description
Add	1-40	1-40	Document Updated

Review By

Name of the Reviewer	Review Date	Description
Dhananjay Saini	09-01-2025	Document reviewed

Document Revision List

Customer : National Health Authority, India
Project : PMJAY 2.0
Document Name : User Manual

Release Notice Reference (for release)

Revision Date	Version Details	Revision Description
18 Sept 22	Version 1	Document Created
15 Nov 22	Version 2	Document Updated
26 Apr 23	Version 3	Document Updated
03 May 23	Version 4	Document Updated
09 May 23	Version 5	Document Enhanced
30 May 23	Version 6	Document Enhanced
11 July 23	Version 7	Application updates incorporated
19 July 23	Version 8	Added hierarchy table
08 Jan 24	Version 9	Document Updated based on new requirements
30 Sept 24	Version 10	Document Updated based on new requirements
09 Jan 25	Version 11	Document Updated based on new requirements

Table of Contents

ABBREVIATIONS

Abbreviation	Expansion
ABDM	Ayushman Bharat Digital Mission
AB-PMJAY	Ayushman Bharat Pradhan Mantri Jan Arogya Yojana
CGRMS	Centralized Grievance Redressal Management System
DEC	District Empanelment Committee
ISA	Implementation Support Agency
NHA	National Health Authority
OTP	One Time Password
PMAM	Pradhan Mantri Arogya Mitra
SEC	State Empanelment Committee
SHA	State Health Agency
SMS	Short Message Service
SSO	Single-Sign-On
TMS	Transaction Management System
TPA	Third Party Agency
UHC	Universal Health Coverage
UMP	User Management Portal

1. INTRODUCTION

1.1. Purpose

User Management Portal (UMP) is aimed to facilitate the users to access the various PMJAY application through the single ID and password. User will no longer be required to create separate credentials. It will also provide the single sign-on facility such that user will be required to login once and all the authorised applications will be accessible under the same screen.
UMP facilitates users to create Aadhaar mapped unique User ID and Password that can be used across the PMJAY IT platform.

1.2. Features

1. Users will login into the UMP application which enables the following features for them:

- User role allocation based on entity and application.
- Tracking of the activities through Activity Log
- Updating Mobile number, Email Id, Photo
- Deletion of existing roles
- Account Deactivation
- Change Email ID, Mobile number, User ID, Password

2. Users will be able to login into the respective applications such as TMS-Payer, TMS-Provider, HEM, etc using their User ID.

1.3. UMP Roles

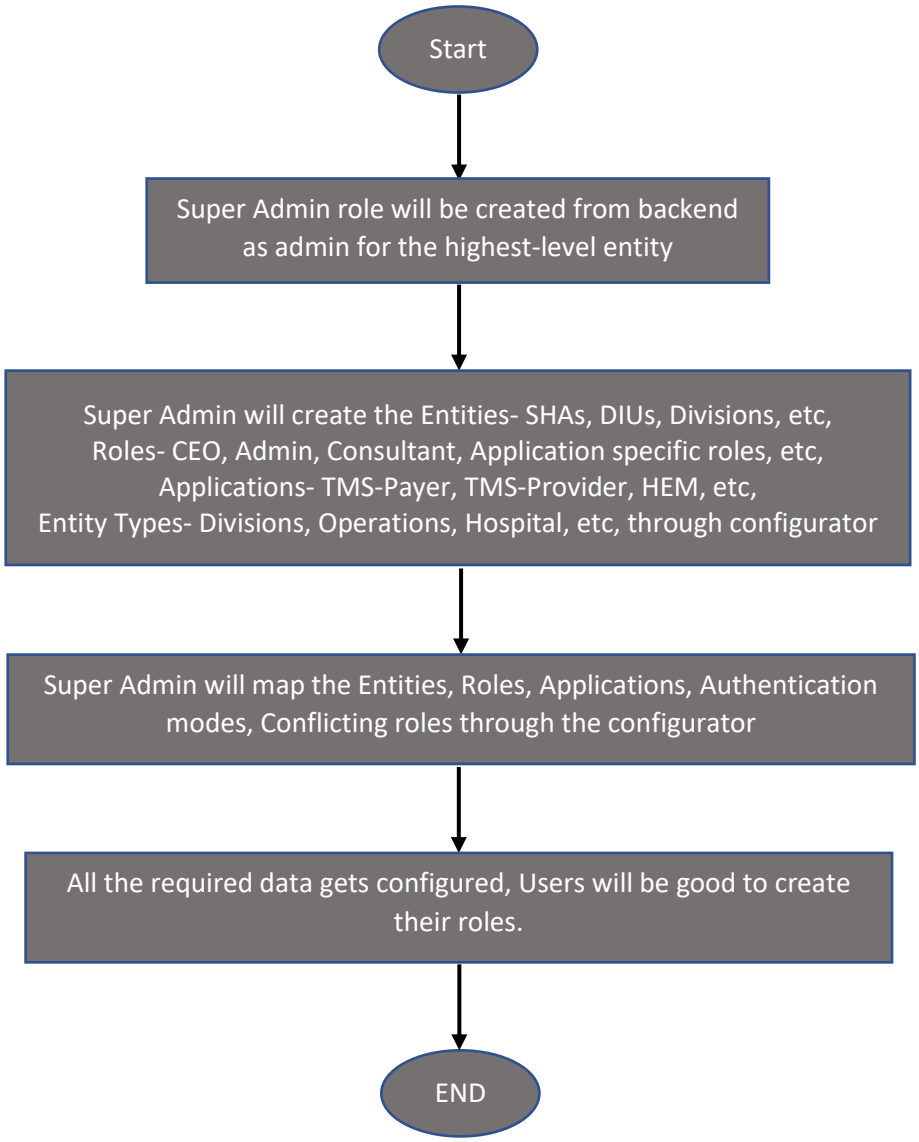
1. **Application User**: The user who are going to access the various applications such as TMS-Payer, TMS-Provider, HEM etc, the role will be requested to access the various applications and perform the assigned activities in the respective applications. Example: PPD, CPD, Medco, PMAM, etc
2. **Admin**: The role will be requested to perform all the admin related activities such as actions on request of roles raised, view the active users, and take the actions like blacklist/unblock them, deactivate or activate their roles. Every entity will have at least 1 admin to run the process flow for the user.

- Admin user will have all the feature that a normal user has, addition to that admin can see the necessary cards (My roles, Pending roles for approval, Active users, Deactivated Users, Blacklisted users, Self-deleted users).
- Admin can see the profile, history and take necessary actions for the users under his authority.

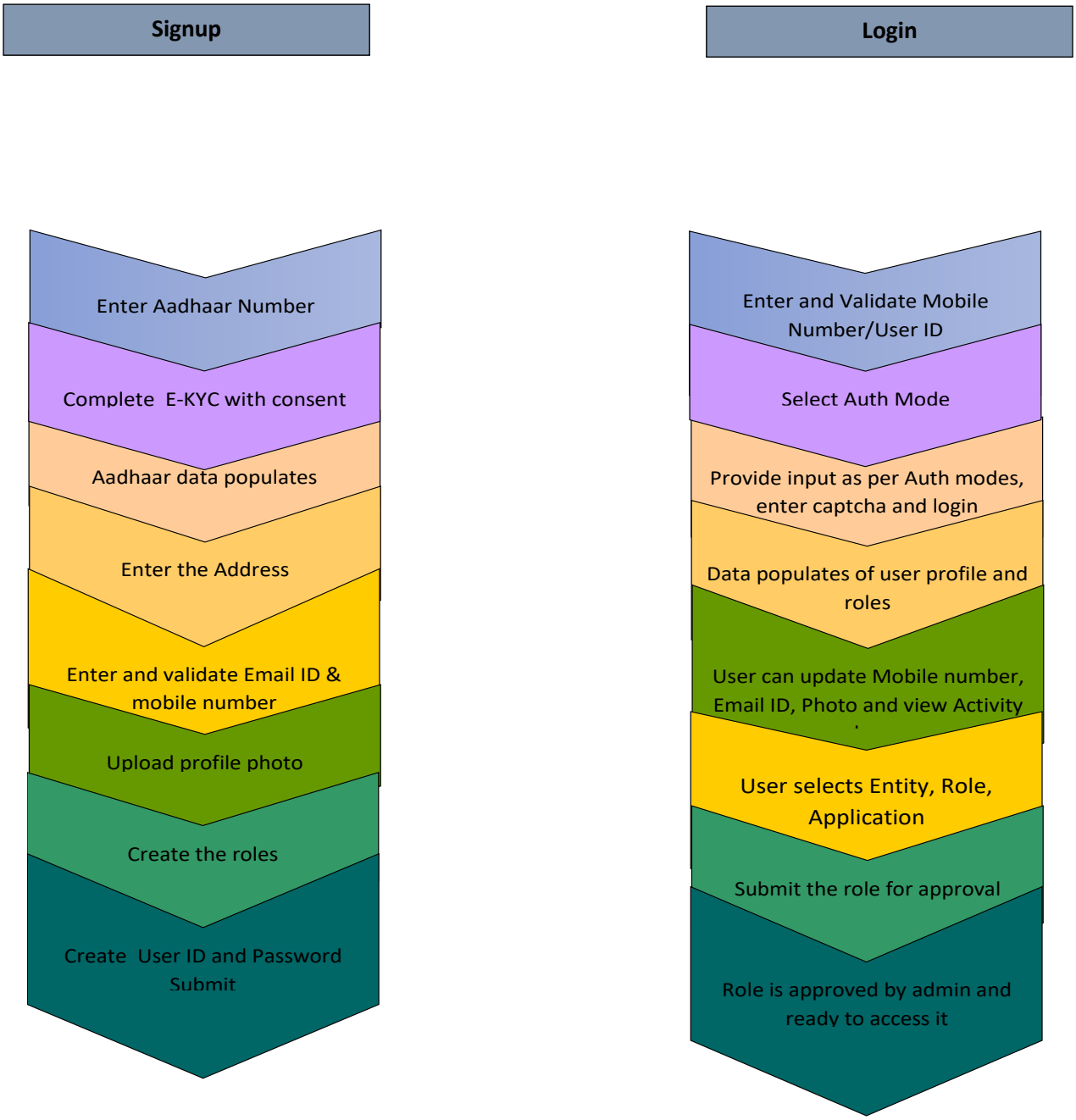
3. **Super Admin**: The role is a system created role to perform all the admin activities for the highest-level parent entities like NHA, SHAs, etc and monitor their activities on the system through dashboard. Along with that super admin will be able to configure the application through configurator for the users.

- Super admin has the authority to create new entities, roles, applications, conflicting roles.
- Super admin will be able to view the reports of the user on the user dashboard.

2. Application Configuration Process Flow



3. UMP User/Role Creation Process Flow



4. User Hierarchy Table for ROLE Creation

S. no	Parent Entity	Entity Type	Entity	Role	Application
National Health Authority					
1	Global	Operations	NHA	Admin,Addl. CEO	UMP
2	NHA	Divisions	IT	Admin, Consultant	UMP
3	NHA	Divisions	HPQA	Admin, Consultant	UMP
4	NHA	Divisions	ABDM-Divisions	Admin, Consultant	UMP
5	NHA	Divisions	Finance	Admin, Consultant	UMP
6	NHA	Divisions	IEC	Admin, Consultant	UMP
7	NHA	Divisions	SPC	Admin, Consultant	UMP
8	NHA	Grievance	NHA-Grievance	ADMIN	UMP
9	NHA	Grievance	NHA-Grievance	National Grievance Nodal Officer	CGRMS
10	NHA	Grievance	NHA-Grievance	National Grievance Redressal Committee	CGRMS
11	NHA	Grievance	NHA-Grievance	National Hysterectomy Monitoring committee	CGRMS
12	NHA	Grievance	NHA-Grievance	National Call Center	CGRMS
State Health Authority					
1	Global	Operations	SHA State	Admin	UMP
2	SHA (State)	Divisions	IT	ADMIN, Consultant	UMP, Samvaad
3	SHA (State)	Divisions	HPQA	ADMIN, Consultant	UMP, Samvaad
4	SHA (State)	Divisions	CEO-office	ADMIN, Consultant	UMP, Samvaad
5	SHA (State)	Divisions	Finance	ADMIN, Consultant	UMP, Samvaad
6	SHA (State)	DIU	District Implementation Unit	District Nodal Officer	UMP, Samvaad, HEM
7	SHA (State)	DIU	District Implementation Unit	District Programme Coordinator	BIS, UMP, Samvaad
8	SHA (State)	DIU	District Implementation Unit	ADMIN, Consultant	UMP, Samvaad
9	SHA (State)	TPA	TPA Name	PPD, CPD, CEX, SHA ISA Auditor login	TMS-Payer, UMP, Samvaad
10	SHA (State)	IC	Insurance Company	ACO Insurer, SHA Insurer, Project Manager, IC BIS Auditor, IC TMS Auditor	TMS-Payer, UMP, Samvaad
11	SHA (State)	IC	Insurance Company	ADMIN, Consultant	UMP, Samvaad
12	SHA (State)	Division	SHA Operation	CEO SHA	UMP, Samvaad
13	SHA (State)	Division	SHA Operation	Addl. CEO	UMP, Samvaad
14	SHA (State)	Division	SHA Operation	Medical Auditors	TMS-Payer, UMP, Samvaad

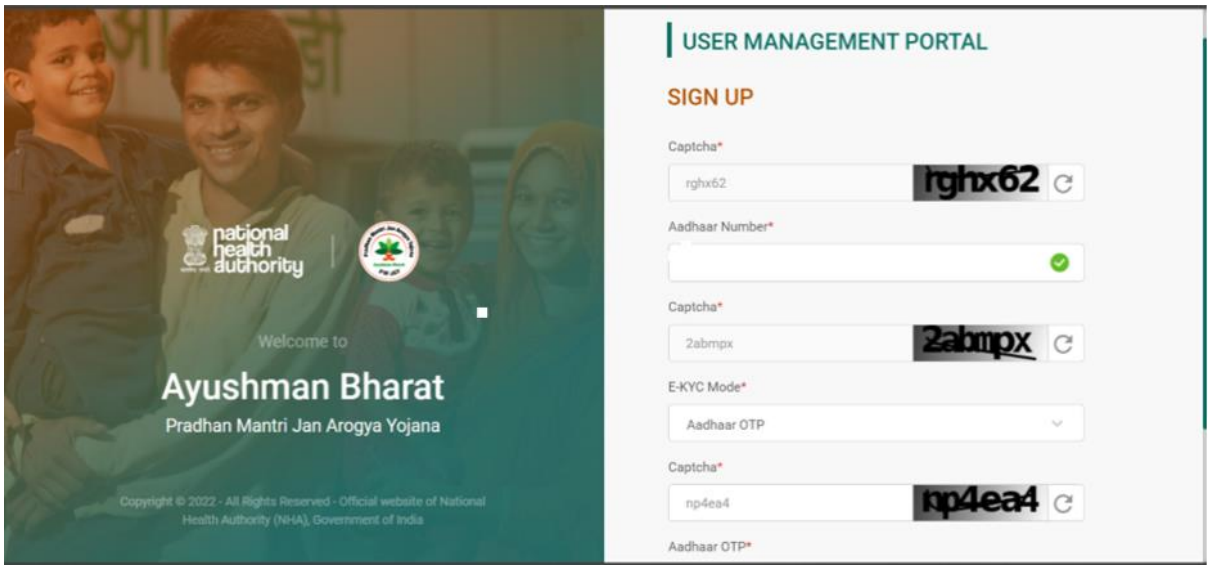
15	SHA (State)	Division	SHA Operation	SHA Approver (final level approver)	BIS, UMP, Samvaad
16	SHA (State)	Division	SHA Operation	SHA Verifier	TMS-Payer, UMP, Samvaad
17	SHA (State)	Division	SHA Operation	State Head BFA	TMS-Payer, UMP, Samvaad
18	SHA (State)	Division	SHA Operation	ACO Approver	TMS-Payer, UMP, Samvaad
19	SHA (State)	Division	SHA Operation	SHA Approver	TMS-Payer, UMP, Samvaad
20	SHA (State)	Division	SHA Operation	Medical committee	TMS-Payer, UMP, Samvaad
21	SHA (State)	Division	SHA Operation	Unspecified approver ACS	TMS-Payer, UMP, Samvaad
22	SHA (State)	Division	SHA Operation	Unspecified approver ACS	TMS-Payer, UMP, Samvaad
23	SHA (State)	Division	SHA Operation	AFO Login	TMS-Payer, UMP, Samvaad
24	SHA (State)	Division	SHA Operation	SAFU Doctor Login	TMS-Payer, UMP, Samvaad
25	SHA (State)	Grievance	SHA Grievance	ADMIN	UMP
26	SHA (State)	Grievance	SHA Grievance	State Grievance Nodal Officer	CGRMS
27	SHA (State)	Grievance	SHA Grievance	State Grievance Redressal Committee	CGRMS
28	SHA (State)	Grievance	SHA Grievance	State Appellate Authority	CGRMS
29	SHA (State)	Grievance	SHA Grievance	District Grievance Nodal Officer	CGRMS
30	SHA (State)	Grievance	SHA Grievance	District Grievance Redressal Committee	CGRMS
31	SHA (State)	Division	SHA Operation	ADMIN, Consultant	UMP, Samvaad
32	SHA (State)	Hospital	Hospital Name	Admin, MEDCO, Medical Superintendent	UMP, TMS-Payer
33	SHA (State)	Hospital	Hospital Name	PMAM	BIS, Samvaad
34	SHA (State)	Hospital	Hospital Name/ Hospital Onboarding Entity	ADMIN	HEM
35	SHA (State)	Division	District Empanelment Committee	ADMIN, DEC Officer	UMP, HEM
36	SHA (State)	Division	District Empanelment Committee	Physical Verifier	HEM

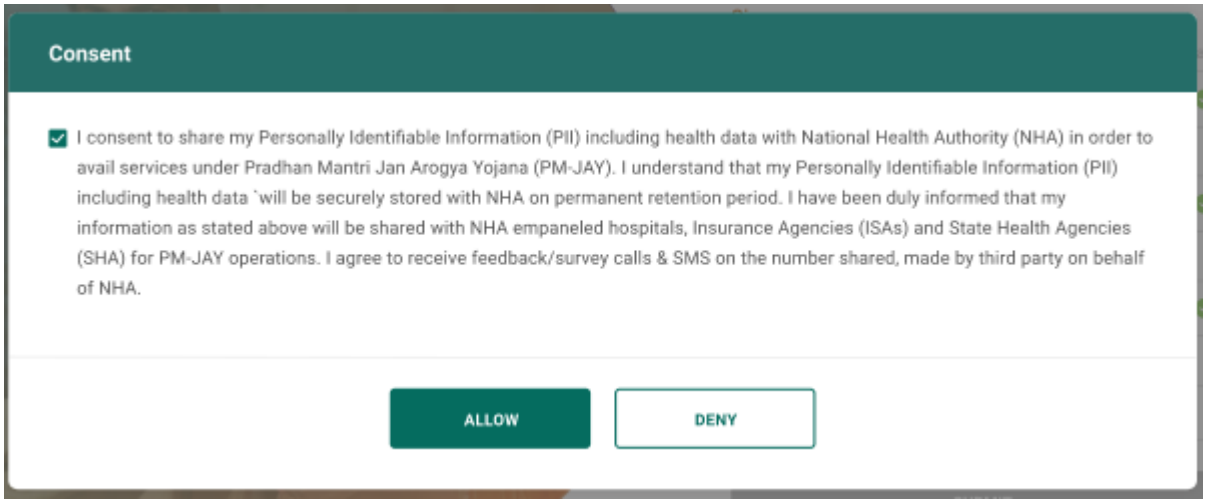
37	SHA (State)	Division	State Empanelment Committee	ADMIN, SEC Officer	UMP, HEM
38	SHA (State)	Division	State Empanelment Committee	Physical Verifier	HEM
39	National Health Authority	Division	Convergence	Additional Director	HEM
40	National Health Authority	Division	Convergence	Dealing Hand	HEM
41	SHA (State)	TPA	Agency Name	Physical Verifier	HEM
42	National Health Authority	Division	SPE	ADMIN	HEM
43	Global	Operations	NHA Hospitals	ADMIN	UMP
44	Global	Operations	NHA Hospitals	NHA Officer	HEM
45	Global	Operations	NHA Hospitals	Physical Verifier	HEM
46	NHA	Grievance	Convergence-Grievance	ADMIN	UMP
47	NHA	Grievance	Convergence-Grievance	BOCW-Central Grievance Nodal Office	CGRMS
48	NHA	Grievance	Convergence-Grievance	ESIC-Central Grievance Nodal Office	CGRMS
49	NHA	Grievance	Convergence-Grievance	PMCARES-Central Grievance Nodal Office	CGRMS
50	NHA	Grievance	Convergence-Grievance	CAPF Level 1	CGRMS
51	NHA	Grievance	Convergence-Grievance	CAPF Level 2	CGRMS
52	SHA (State)	Division	SHA Operation	SHA-BIS	BIS
53	SHA (State)	Card Processing Agency	Agency Name	ISA-BIS	BIS

5. UMP: SIGNUP PROCESS

5.1. E-KYC

PMJAY Users shall be able to sign up through UMP, as shown below. User enters the Aadhaar number, validates it and selects the E-KYC modes (Aadhaar OTP/Fingerprint/Face Auth). Post validating Aadhaar number, user will allow consent and click on the submit button thus completing the E-KYC and system will take the user to the signup dashboard.





5.2. Signup Dashboard

User is asked to enter and verify the details mentioned on the signup dashboard such as Aadhaar linked mobile number, email ID, address. User can upload new profile photo for the dashboard such that it should match with the Aadhaar photo. Once it is done, user is required to create required roles to perform the required actions and duties, post which new username and password based on certain criteria will be created that can be viewed under 'i' button and the credentials will be used to login into the various applications based on the role allocation.

User ID Criteria:

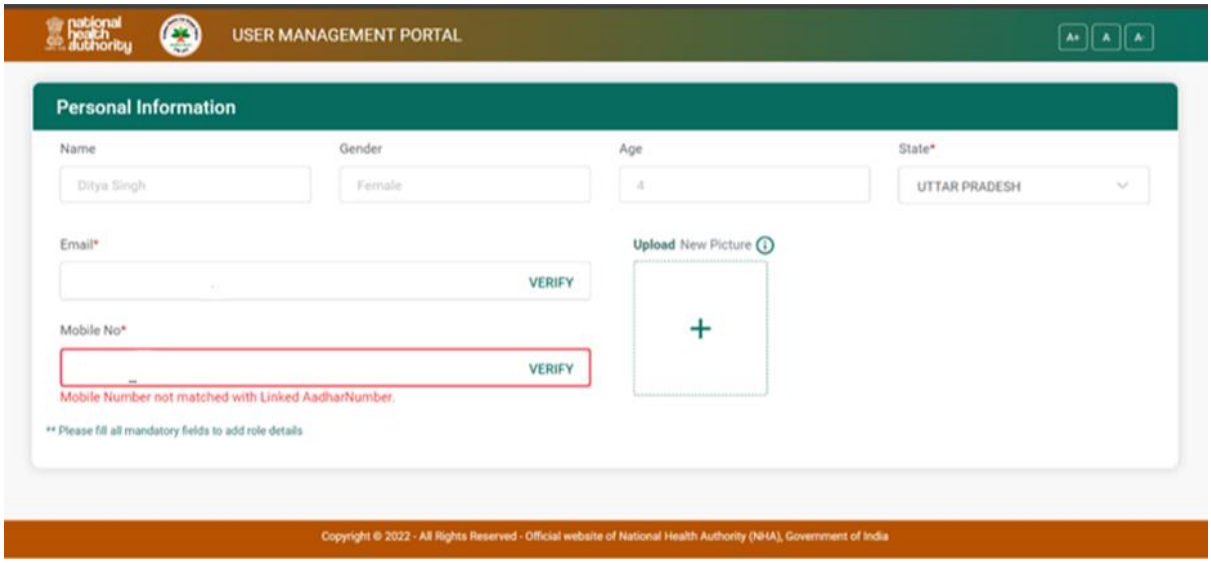
1. It should consist of minimum 8 variables which can be combination of alphabets, numbers and special characters ('@' '-' '_' '.').
2. It should not start with a number.
3. It should not consist of consecutive special characters.
4. It should not end with a special character.

Password Criteria:

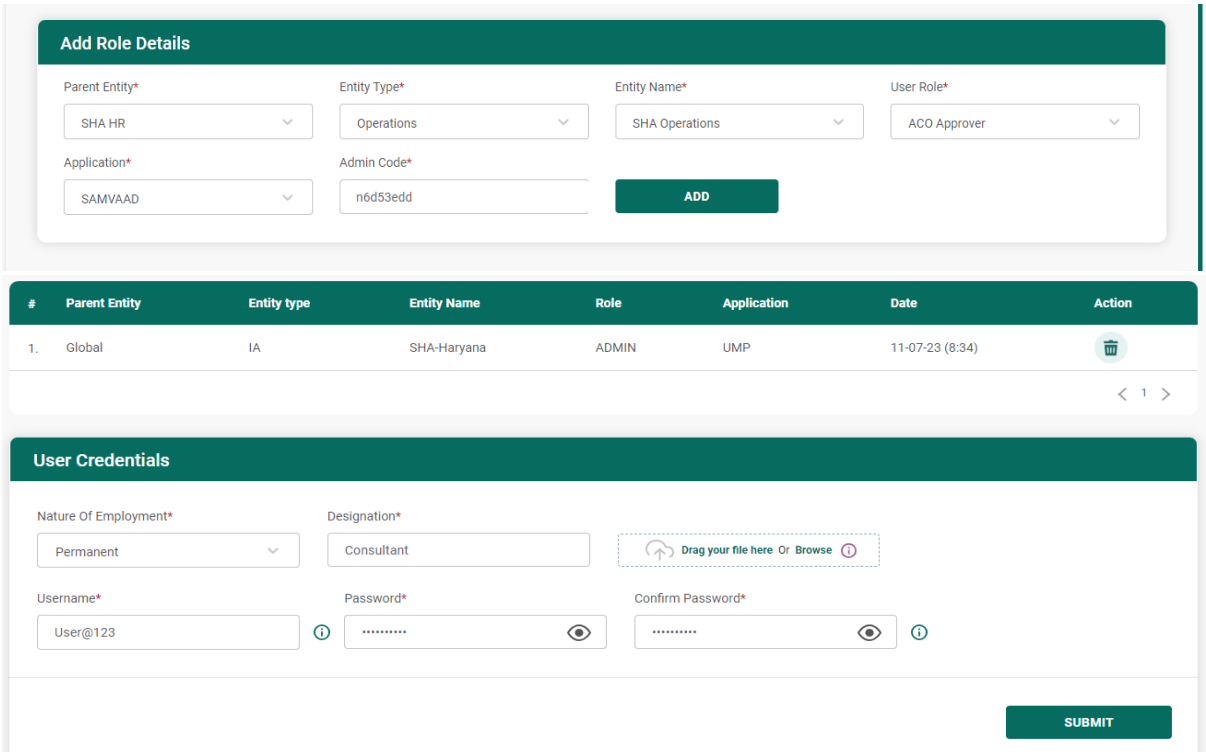
1. It should follow the criteria mention in the 'i' button.
2. It should not consist of consecutive special characters. Eg: User@@name
3. It should not end with a special character. Eg: Username@

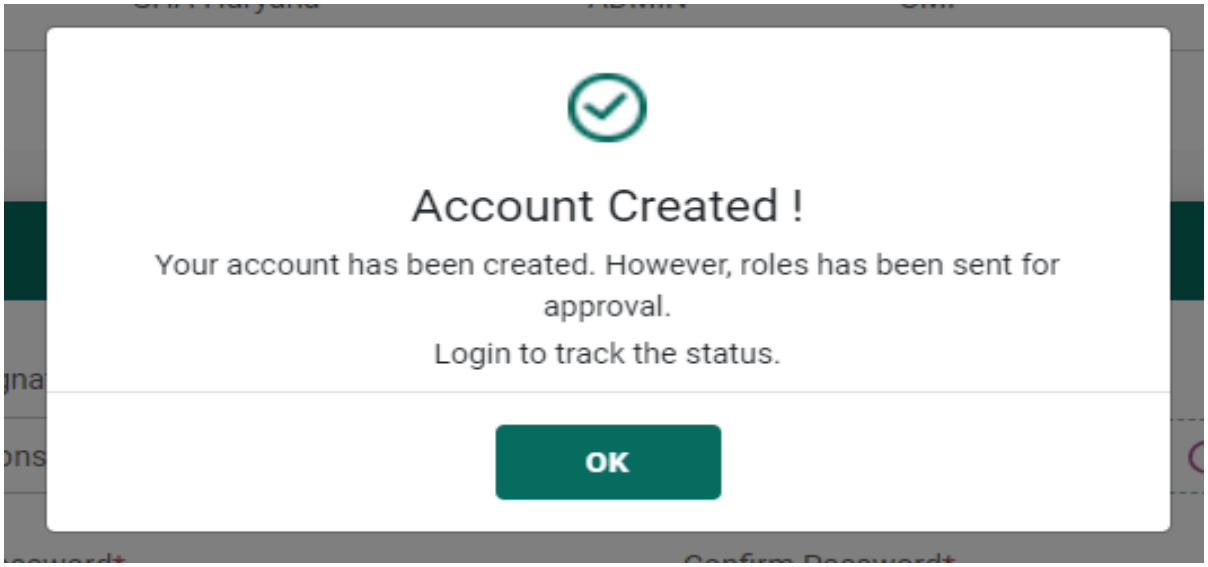
Once the mandatory details are filled in the respective fields, user will submit it and receive the success for the same.

Note: In order to verify the email ID, a link will be sent to the entered email ID and user will be required to click on the link to verify it. However, the email ID can be verified up to a period of 7 days while user will be given required access on the application post its verification.



User can enter the address details or select the check box in case the current address is same as that of Aadhaar address. User Will enter Email id and Mobile number and verify them through a link sent on mail and Mobile OTP respectively. Then user will be required to select their entities, roles, application based on the required access and then enters the nature of employment, designation, document (as suggested by user's admin) as a mandate for any entity admin. Finally, user creates ID, password and click on submit button.

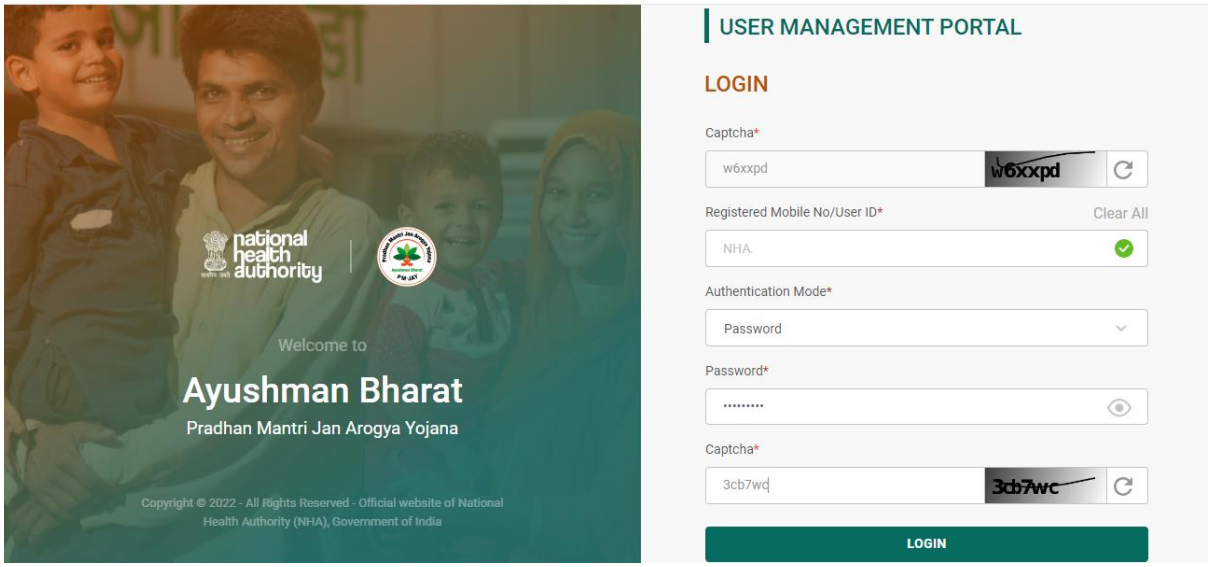




6. UMP: User Portal

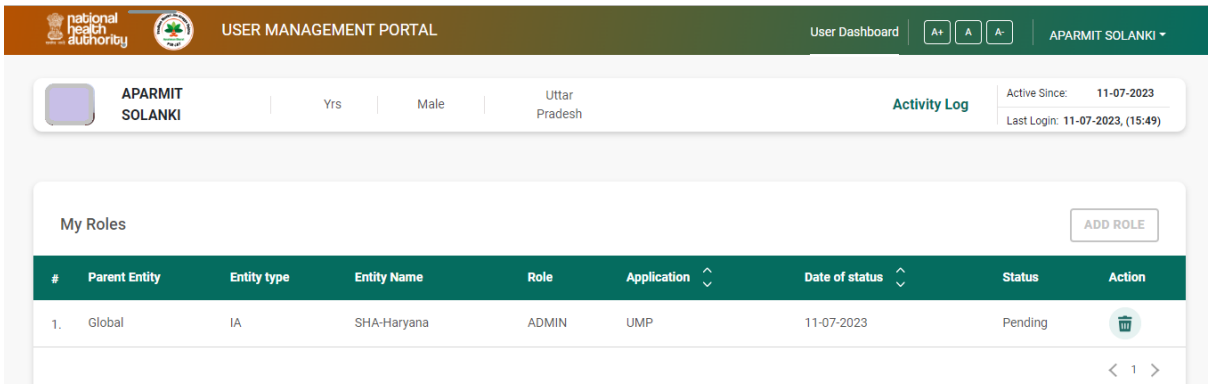
6.1. User Login

PMJAY user logs into the UMP application in order to create role as per the entity and application. User enters user ID/mobile number and click on verify button such that system check its correctness, post which user will be required to select authentication mode (Mobile OTP, Aadhaar OTP, Password, Fingerprint, Face Auth, Iris Auth) based on the one allowed for the user's allocated role. After selecting the authentication mode, user provides input depending upon the selected auth mode. Finally, user enters captcha and click on the 'Login' button.



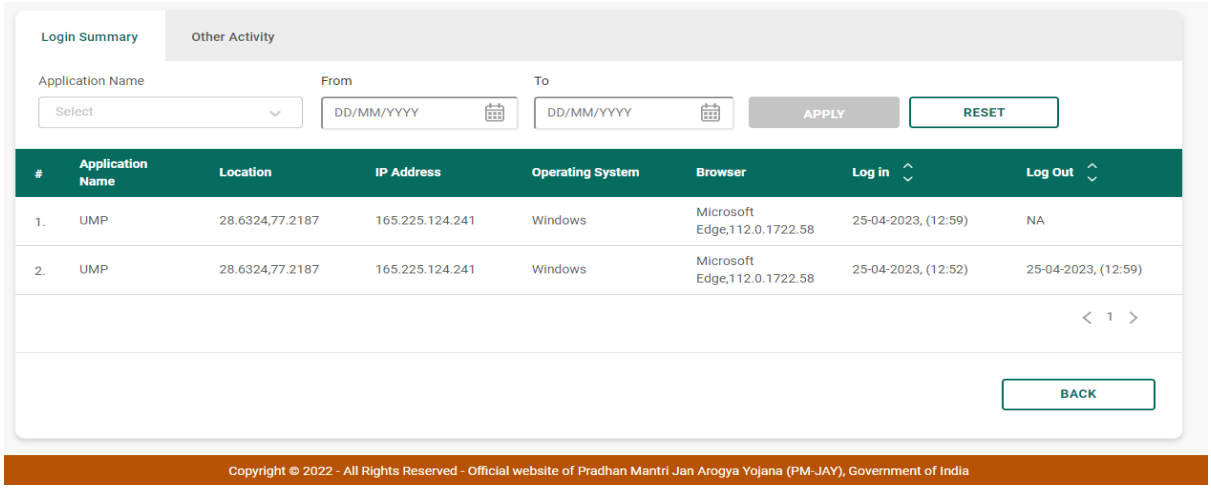
6.2. User Portal

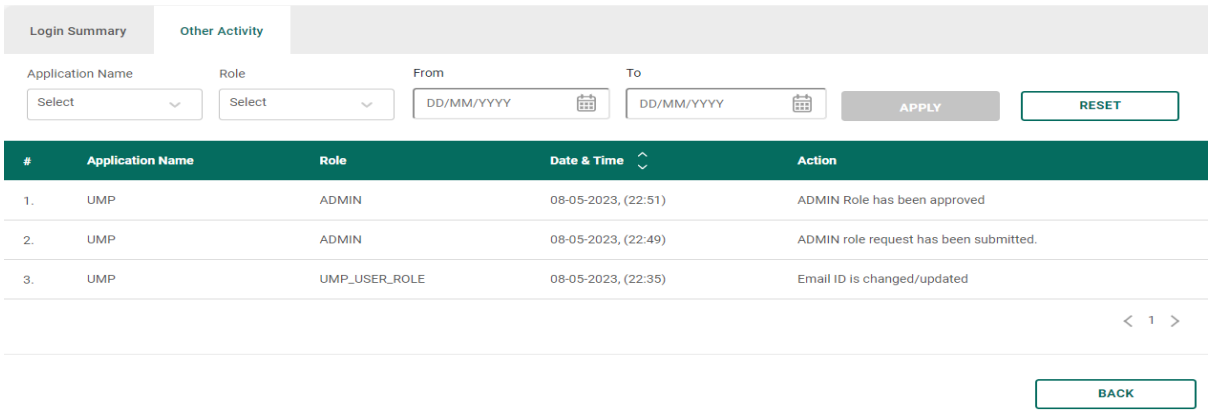
When user logs into the system, user dashboard will appear on the screen which displays user's profile details, Activity log, Active Since date, Last login details. On the top right corner, when user click on the name, a drop down will appear which consists of (Change password, Update details, Delete account, Logout). Apart from this user can click on activity log in which user will be able to see the activities performed on the applications. In order to create any role user will be required to click on the add role button and user will be required to select the values in dropdown and submit the request for approval.



6.3. Activity Log

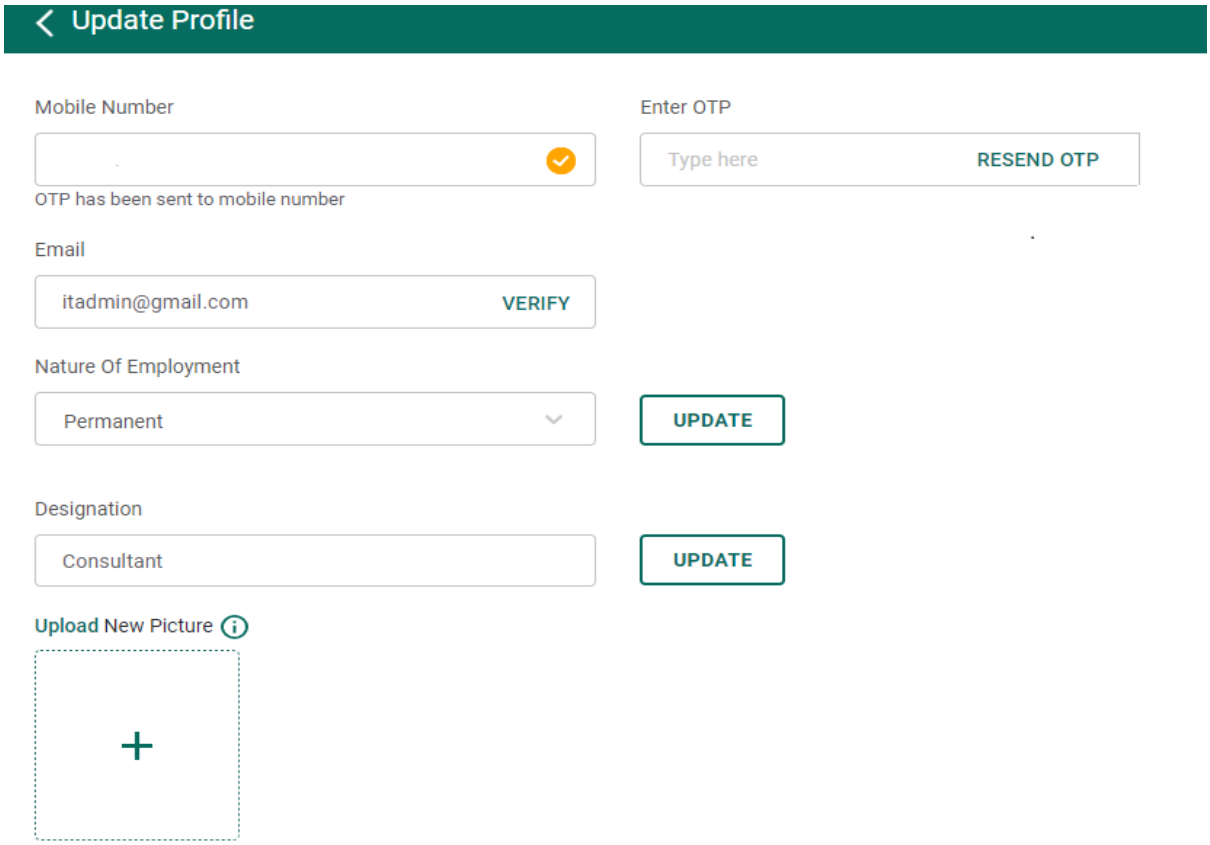
Users click on the activity log on the user portal, they will be able to view the activities performed by them under this section as mentioned in the images. Here users will be able to view the details of Login details and other activities. User will be able to view the activities by filtering them based on the required criteria. In order to go back to the dashboard, user is required to click on the back button at the right bottom corner.





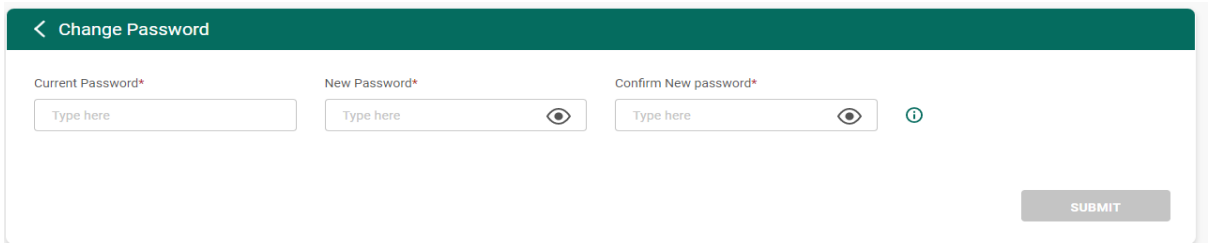
6.4. Update Details

Users will be able to update the mobile number using the mobile OTP considering the number is not tagged with another user. Similarly, user will be able to update email ID which needs to be verified by clicking on the link received on the entered mail ID. Also, the photo can be updated, considering it matching with Aadhaar photo of the user else the system wouldn't allow to update it. Apart from this, users can also update designation and employment type. In order to move back to the user portal, Users can click on the back arrow in the header beside update profile heading.



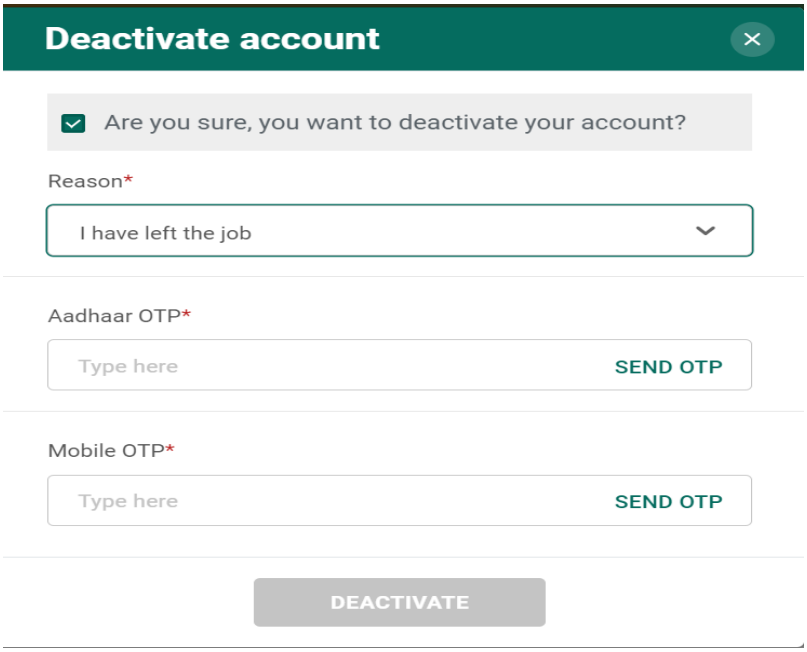
6.5. Change Password

Users will be able to change their password under this section by entering the current and new password based on its criteria that can be viewed from the 'i' button.



6.6. Deactivate Account

The facility is provided to the users such that they would be able to deactivate their account. User will click on the Self deactivate account button, a popup will appear to generate and enter the Reason along with Aadhaar OTP and Mobile OTP. Once the account is deactivated, they will no longer be able to access their account. In order to access the applications, User should request the admin to activate the account under the deactivated user card.



6.7. Role Creation

Users once login, will be able to see pre-assigned roles if any, above which a button named 'Add Role' has been given, user click on the button and they will be able to see the necessary fields (Parent Entity, Entity type, Sub Entity, User Role, Application). User selects the details from the respective drop downs and click on the add button. The role will be added and visible on the list below, which can be deleted by the delete button if added mistakenly, similarly user can create multiple roles and submit them all in one click of submit button. The roles will appear in the pending list of the respective entity admin, where admin can take necessary action on the user role application.

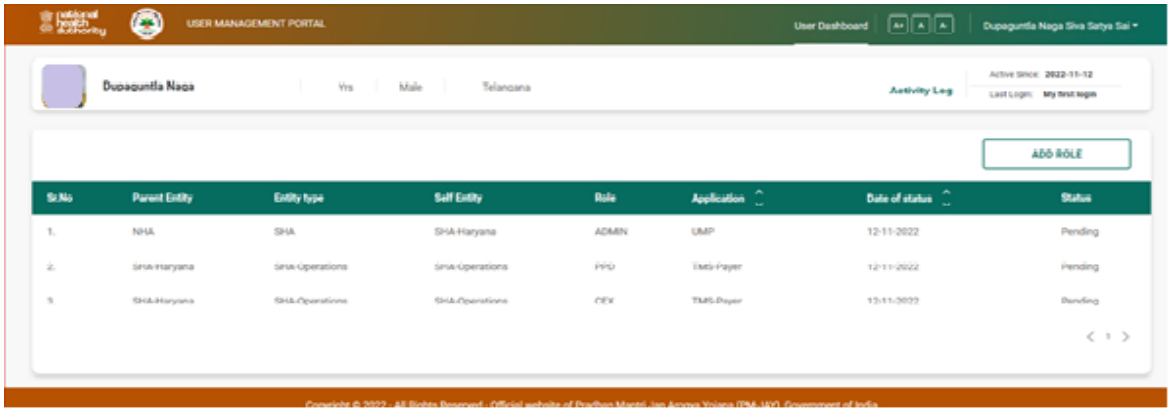
Entity Name: It represents the entity the user is currently working under, such as SHA-State, Division name, Hospital Name, etc.

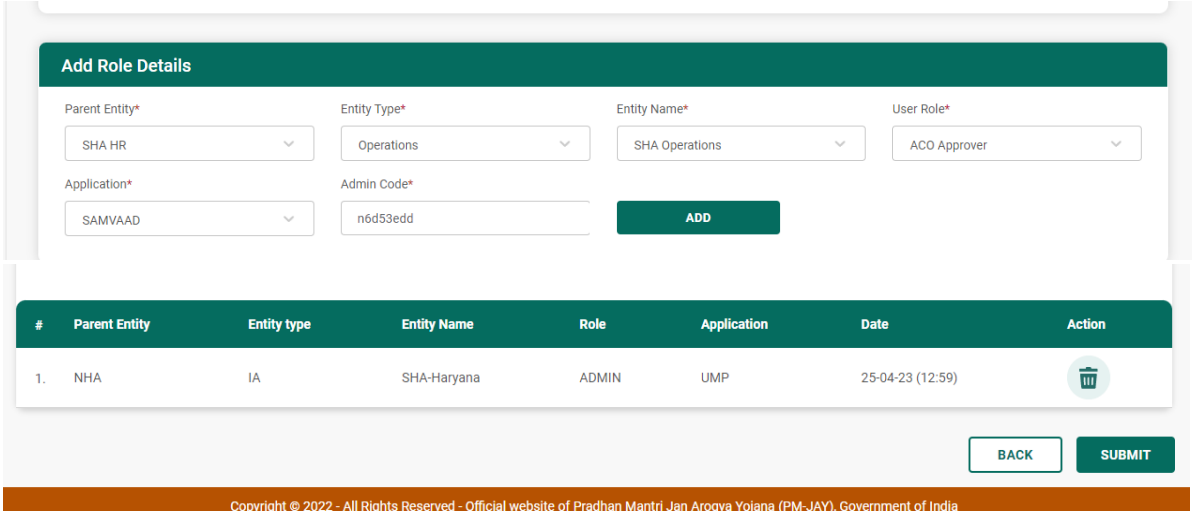
Entity Type: It represents the type of entity the user is currently working under, such as Operations, Hospital, ISA, etc.

Parent Entity: It represents the entity which is parent to that of the user's entity, such as Global, SHA-State, NHA, etc.

User Role: It represents the role the user is having under the entity which is required to impart the duties by the user, such as Admin role, PPD, CPD, ACO, CEX, etc.

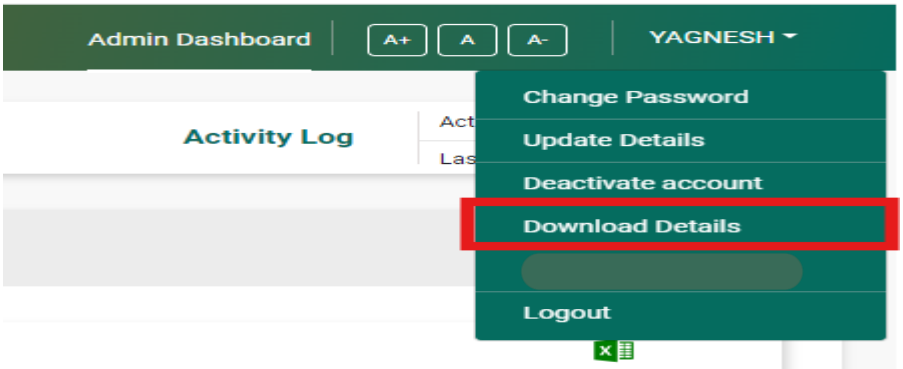
Application: It represents the application on which user is going to perform the required actions thus will be selected by the user to get the access for the same.





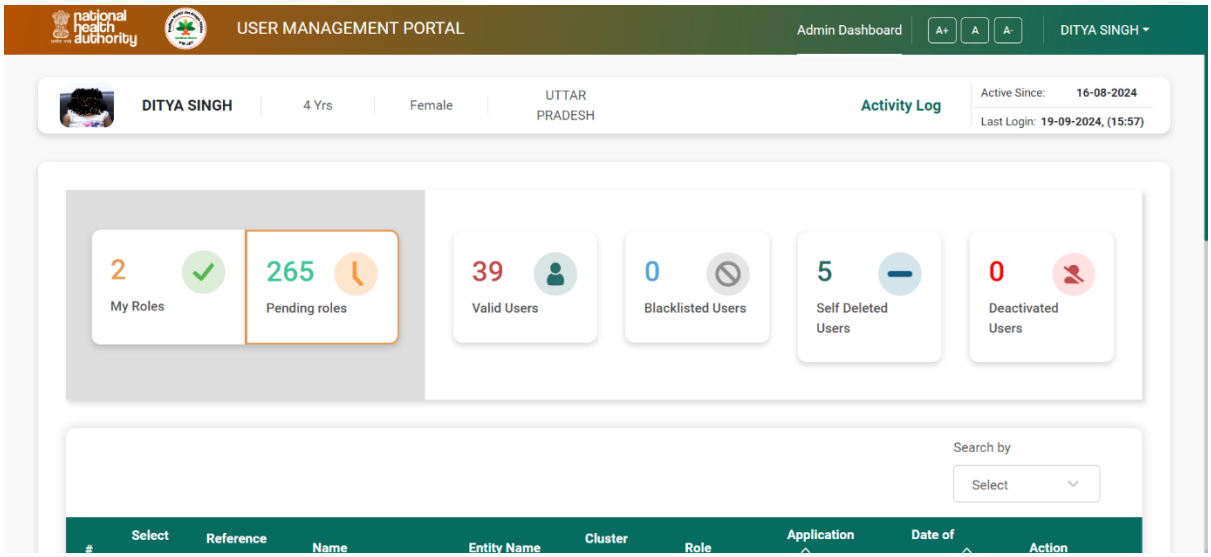
6.8. Download Details

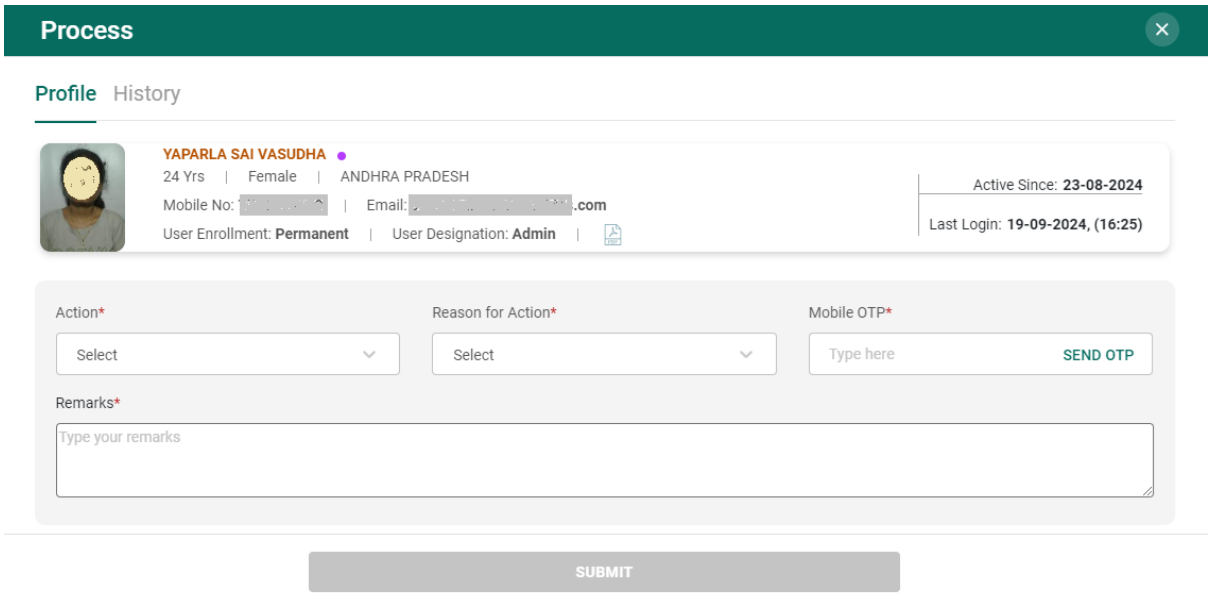
User will be able to download the details which was entered during the signup process. User can refer the User ID, reference ID and other account related details from the downloaded file.



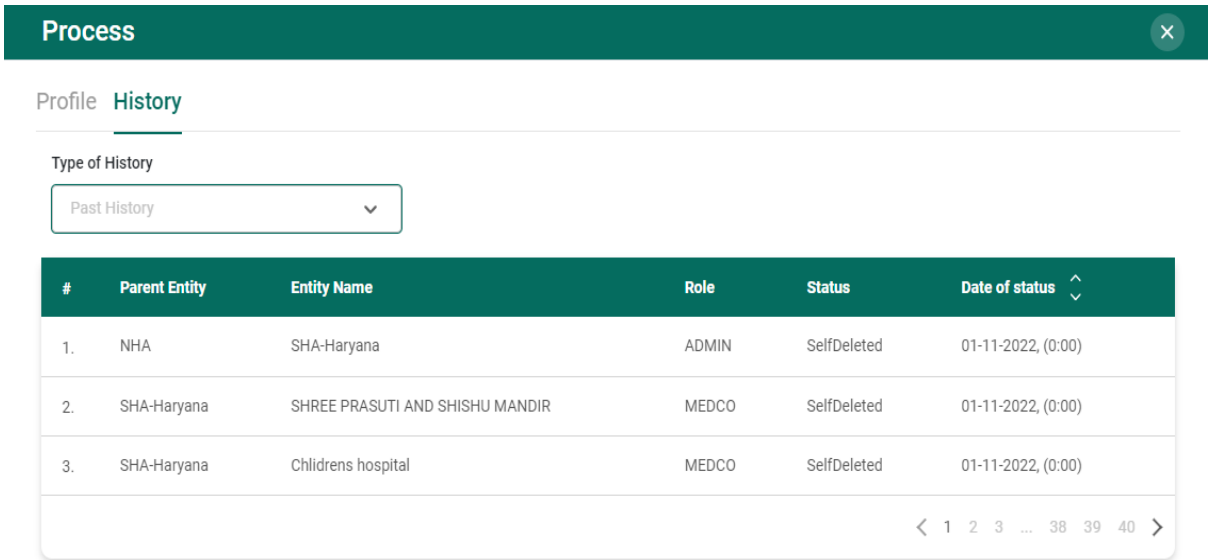
7. UMP: ADMIN DASHBOARD

Every entity needs to create an admin login in the user management portal.
STEP-1: Creation of admin role should also follow above mentioned self-registration process to initiate a request. This request shall be approved by the competent authority as per the hierarchy.
STEP-2: Once the Admin request is approved by the higher hierarchy admin/super admin, the admin will be able to view the dashboard which consists of various features. Apart from the features mentioned for the normal user, an admin user will be able to see the following tabs (Profile, Pending, Active, Deactivated, Blacklisted, Self-Deleted.
In the mentioned tabs user will be able to see the list of users/roles depending upon the tab name and admin could perform necessary actions by clicking on the 'Process' button which will open-up a popup in which admin will be able to view user 'Profile' and 'History' section where admin can take necessary action (Approve/Reject/Activate/Deactivate/Blacklist) for the user. On the State admin and global admin dashboard, self and ecosystem radio button has been provided such that self shows the user's data under the parent entity only while the ecosystem shows the user's data of parent entity along with the entities under it.



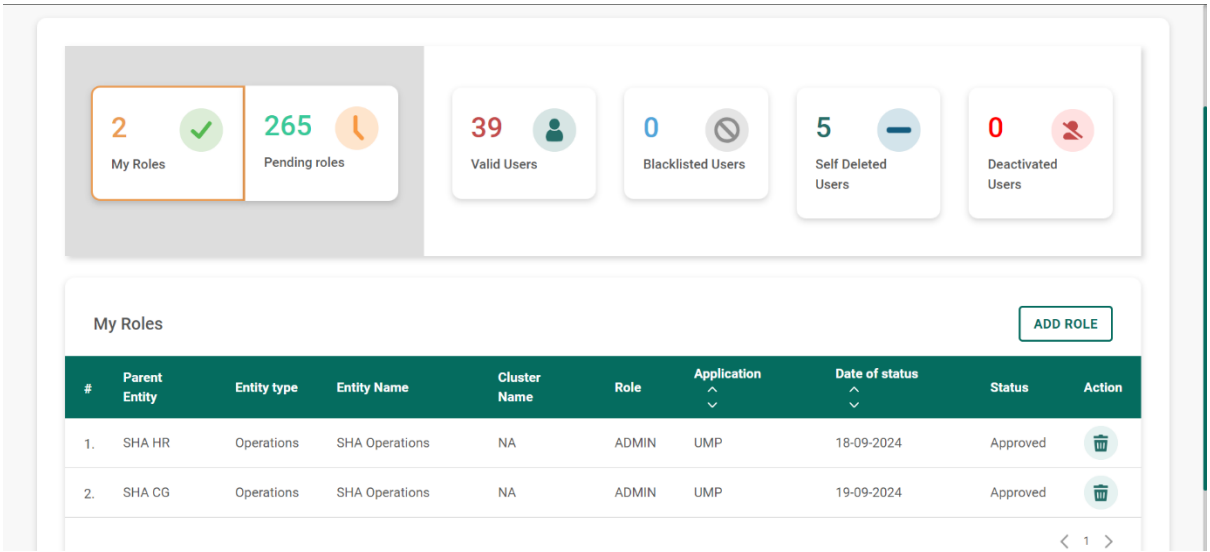


There are two types of histories that has been provide to the admin to be shown i.e. Present history showing the current status of roles which had been raised by user and past history that shows the role details of the user before the user's account got deleted and blacklisted.



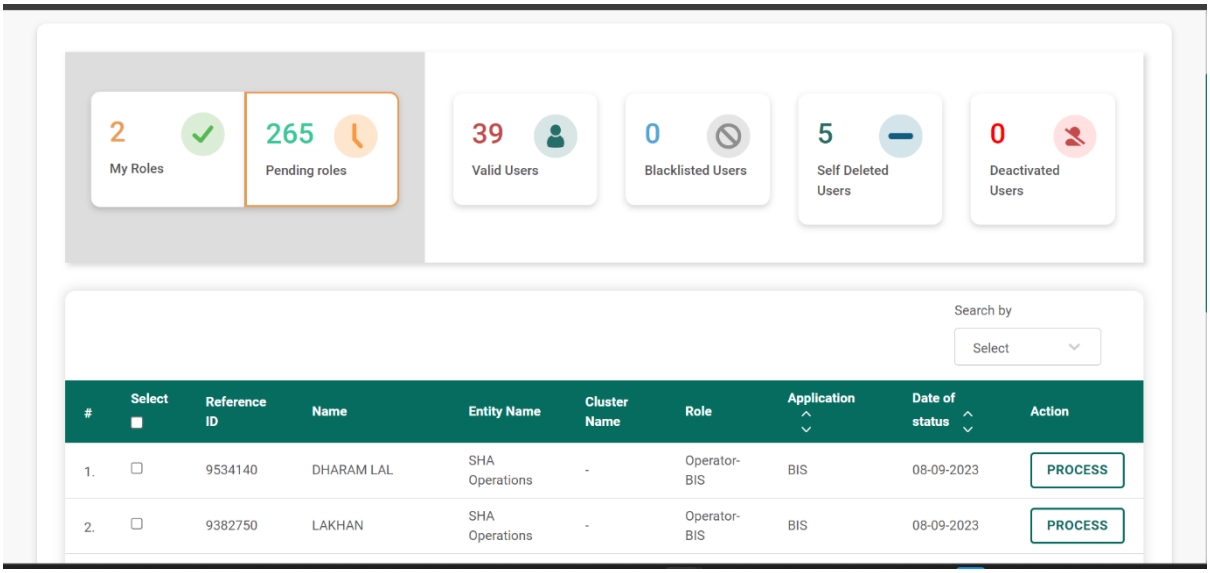
7.1. My Roles

Admin will be able to view the roles that is allocated to him/her and will be able to raise the request for new roles under the tab through 'Add role' button. All the roles with approved, rejected, pending, deactivated status will appear here under the section.



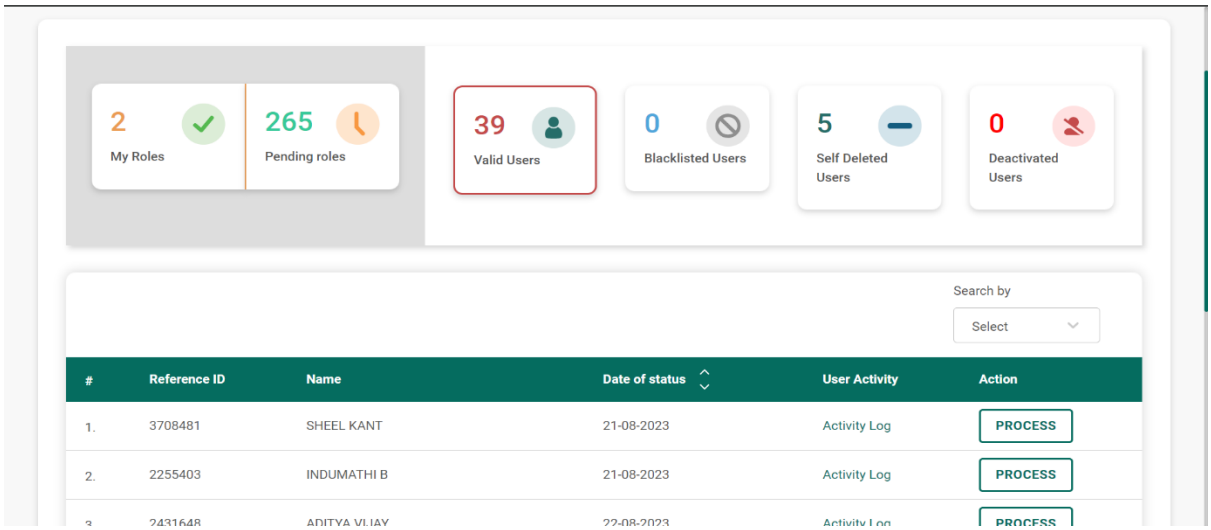
7.2. Pending Roles

The roles which have been raised for approval by will be visible under this tab to the admin. Admin will be required to click on the process button for the required user and a popup will appear in which admin can view the user's profile, history (Present-current roles, Past-roles before user gets self-deleted/blacklisted and take necessary actions on the user's request.



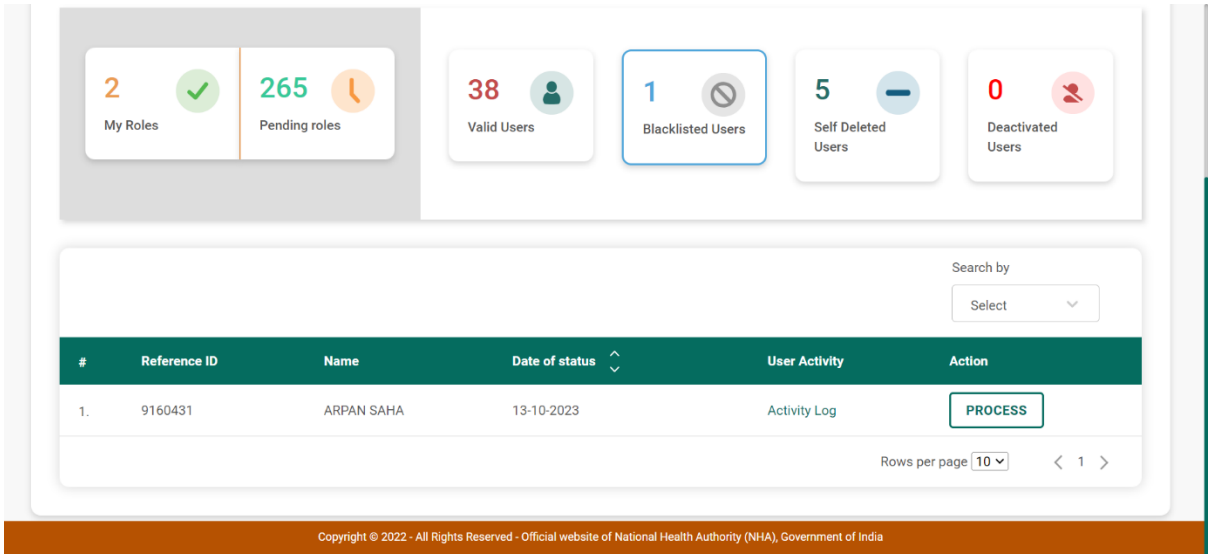
7.3. Valid Users

Admin will be able to view the users under their entity/hierarchy. The admin will be able to take the required actions (Deactivate role, Activate role, Blacklist) for the users under the process button.



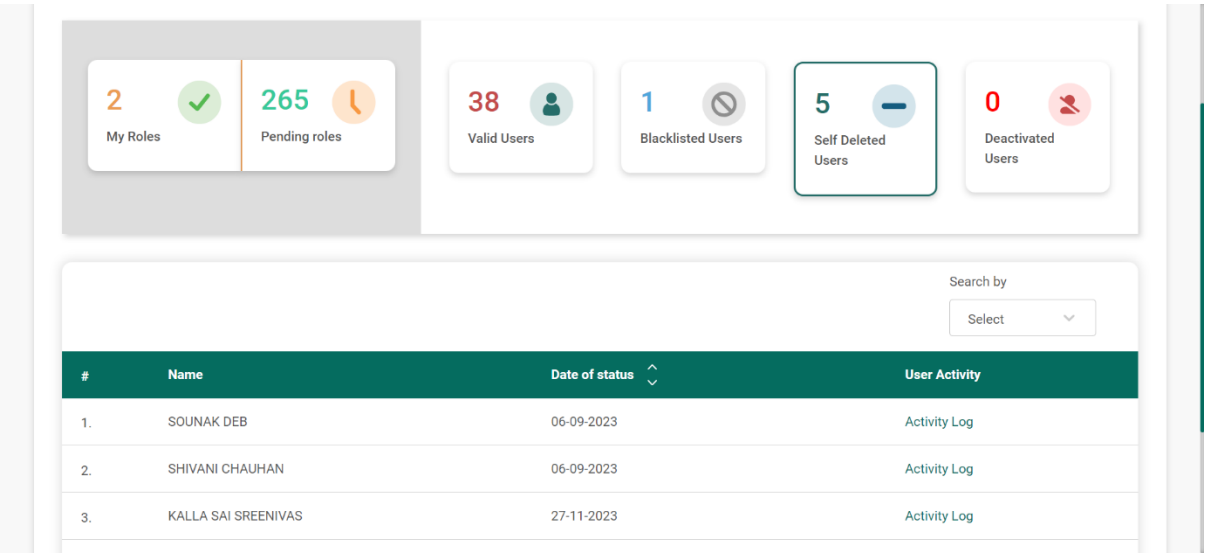
7.4. Blacklisted Users

Admin will be able to view the blacklisted users under the tab such that admin can unblock them under the tab through process button.



7.5. Self Deleted Users

Admin will be able to view the users who have self deleted themselves. The user's details along with the activity log will be visible to admin under the tab.

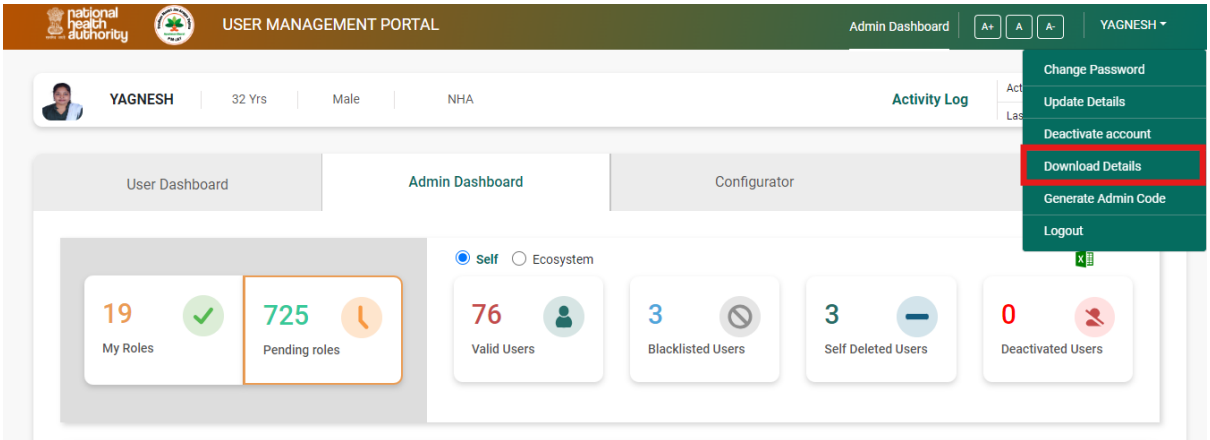


7.6. Deactivated Users

Admin will be able to view the users who have self deactivated their account from the

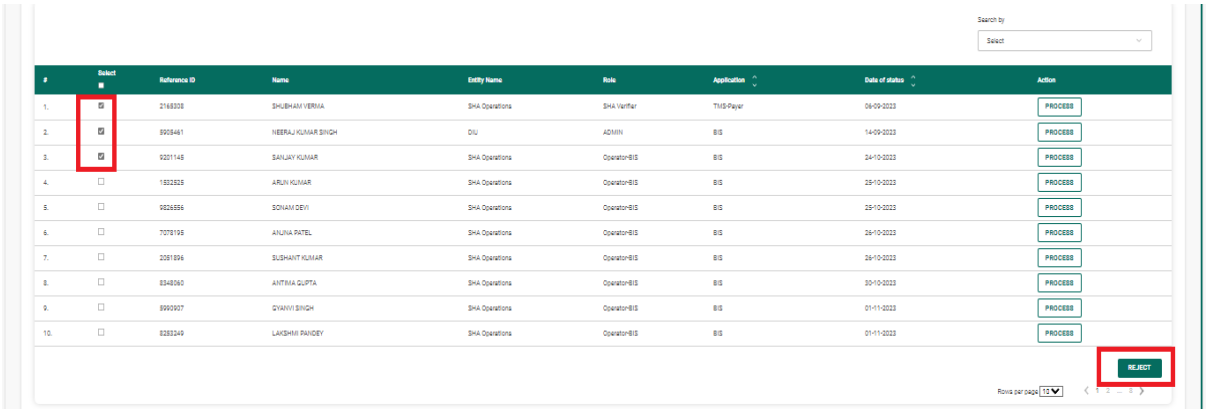
7.7. Download Details

Ump users can download their details present on the signup page along with their reference number such that they could refer the details afterwards and also can be shared with admin if required for approving the roles.



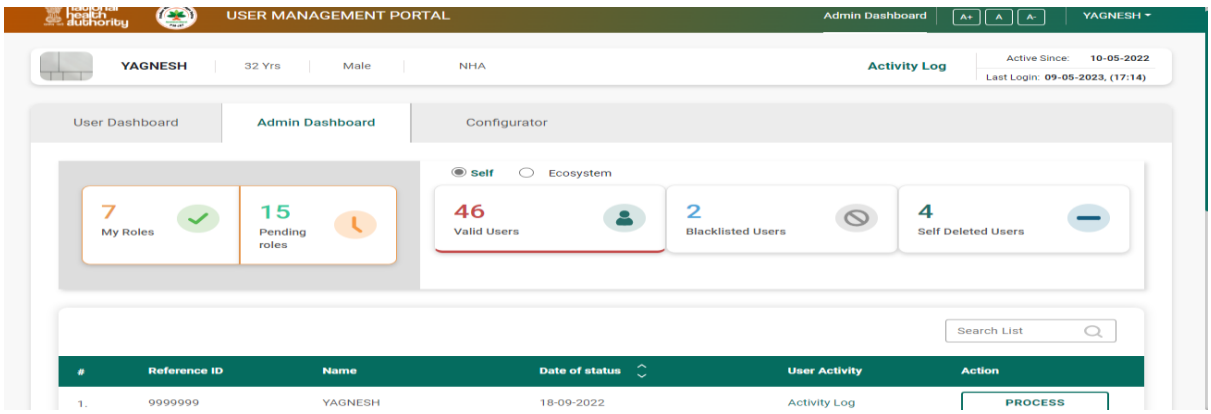
7.8. Bulk Rejection of roles

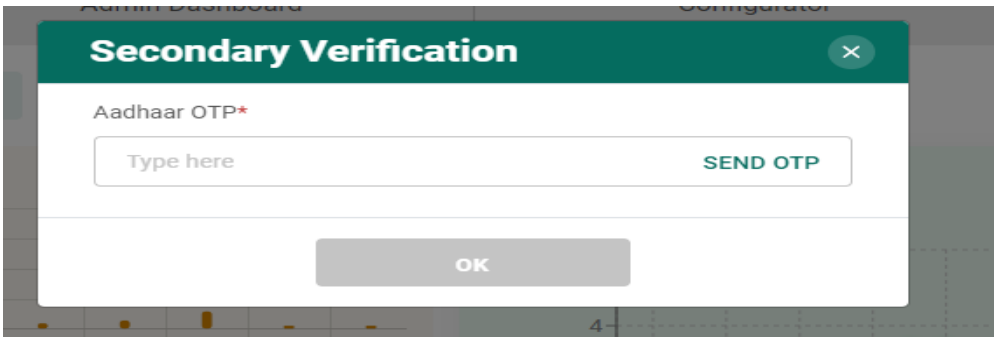
Admin can reject the roles in bulk from the Reject button given at bottom right corner on the pending roles list. Admin will select the roles from the check box given on the screen, Once done admin can reject them by entering the remarks for them.



8. UMP: SUPER ADMIN DASHBOARD

Super admin will be a role which will be provided with special privileges of application configuration and Dashboard to monitor the platform users under the
Super admin as per the hierarchy and the same approval process will be followed for Admin as that for normal user, where their respective admin/ Super admin can take the necessary actions on the requests.
Super admin will be created from backend which will be used as overall approver for highest level parent entity admin-State admin. Super admin user will have all the access and features that an entity admin has, apart from that super admin will have the access for the UMP configurator in which admin will be able to make the necessary configurations for the application. User reports dashboard in which admin will be able to view the roles, user's details under their hierarchy in the tabular as well as graphical format. The account has also been made more secure by providing the dual authentication criteria for login the super admin account.



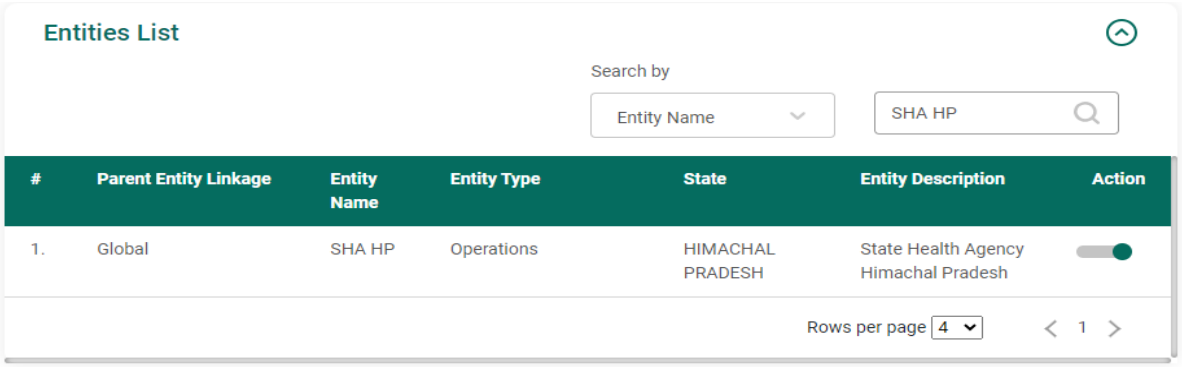


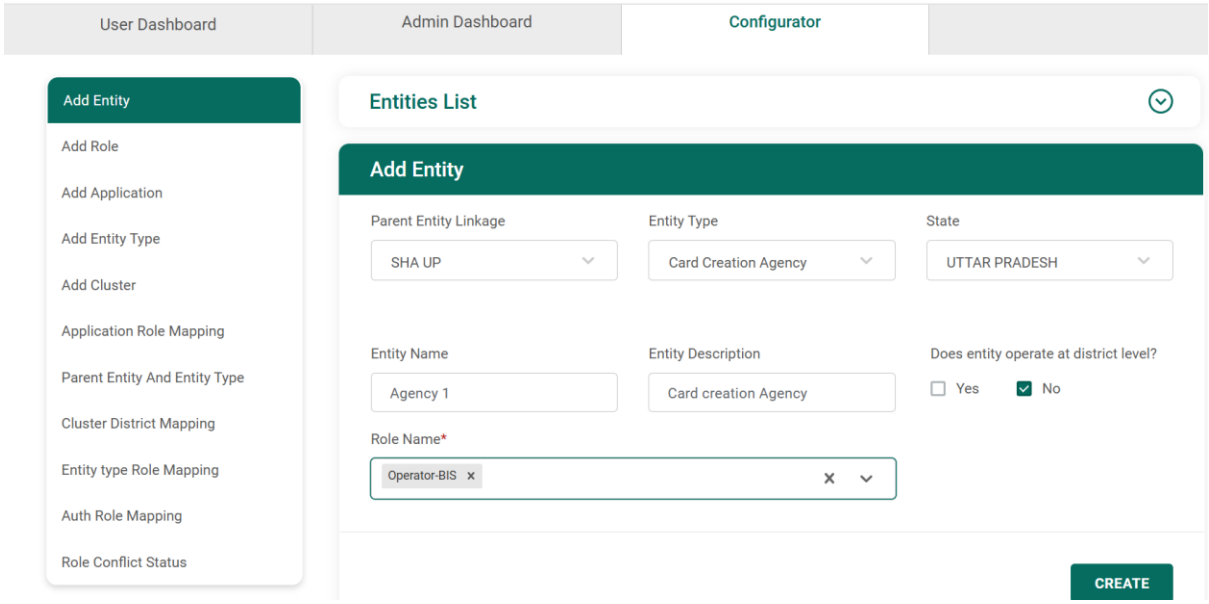
9. UMP: CONFIGURATOR

Configurator is a tool by which super admin can make the required configuration for the application which will be used by all the users in the application. It consists of Entity creation, Role creation, Application creation, Entity type creation, Application role mapping, Entity role mapping, Authentication mode role mapping, Conflicting role mapping. Already made configuration will be visible from the list at the top of the section. Admin can search the required parameters through the search bar and activate/deactivate it using the toggle button in the list.

9.1. Add Entity

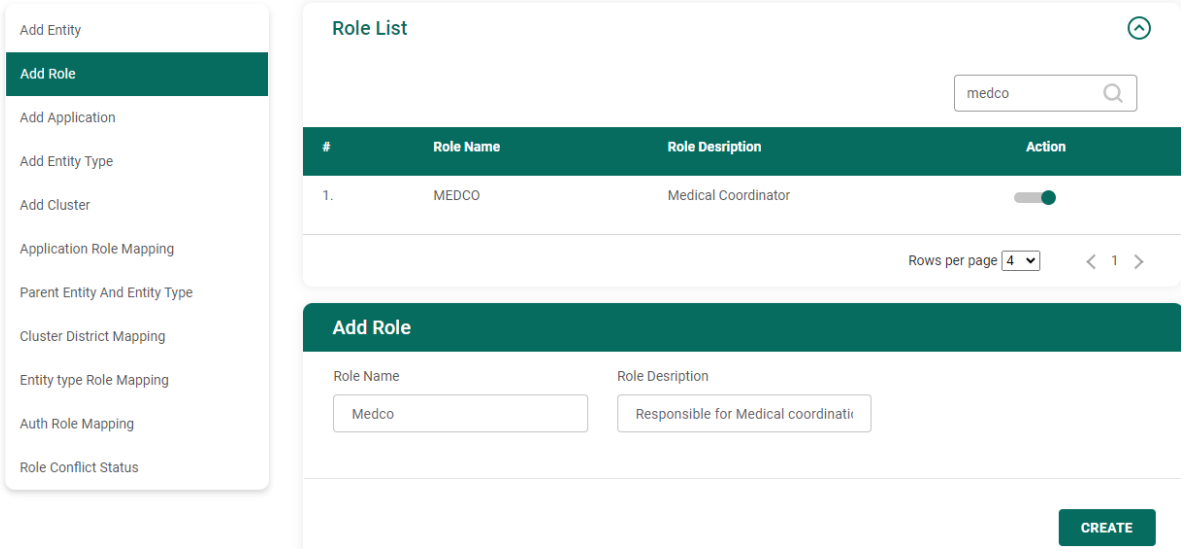
Admin will be able to create new entity under a parent entity in the application by selecting the required details and click on create button, the created entity will reflect in the list at the top along with the required search bars. The bottom of the page there is check box to select the level the entity is operating at such that admin will select 'Yes' in case the created entity is operating at district level. Admin can also disable the selected entity by the radio button provided against each item in the list. In order to disable, admin will be asked for the Aadhaar OTP. Now roles can also be mapped during the creation of entity itself. Thus, the same will be visible in the role drop down against the entity while performing the 'Add Role'.





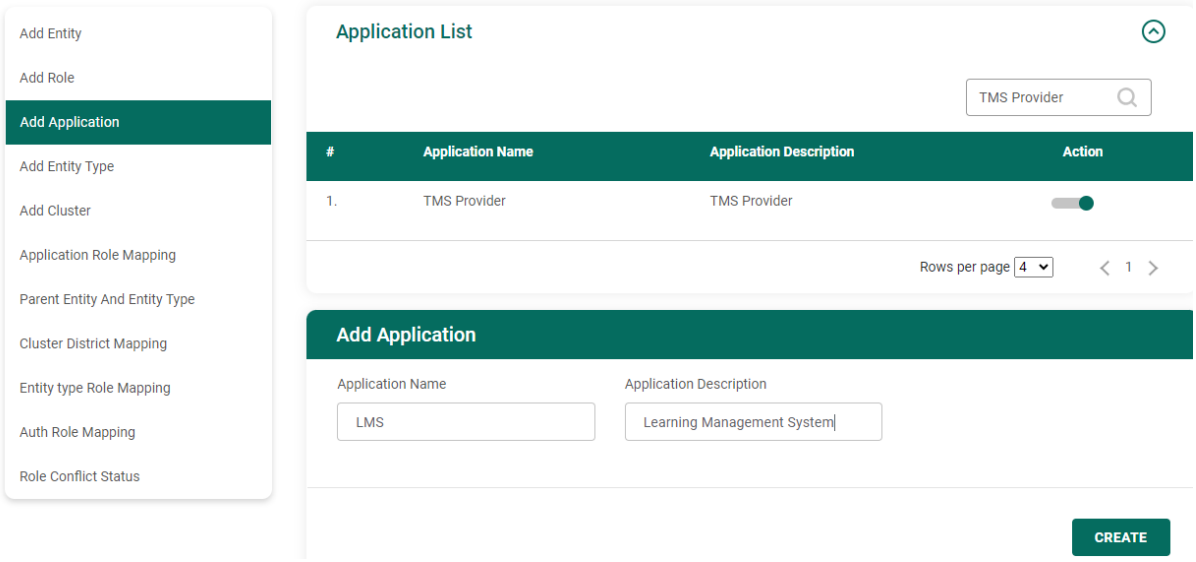
9.2. Add Role

Admin will be able to create new role for the users to get allocated to them, Admin has to enter role and description detail and click on create button. The role will get reflected in the role list. Admin can search and disable the role as well by entering the Aadhaar OTP.



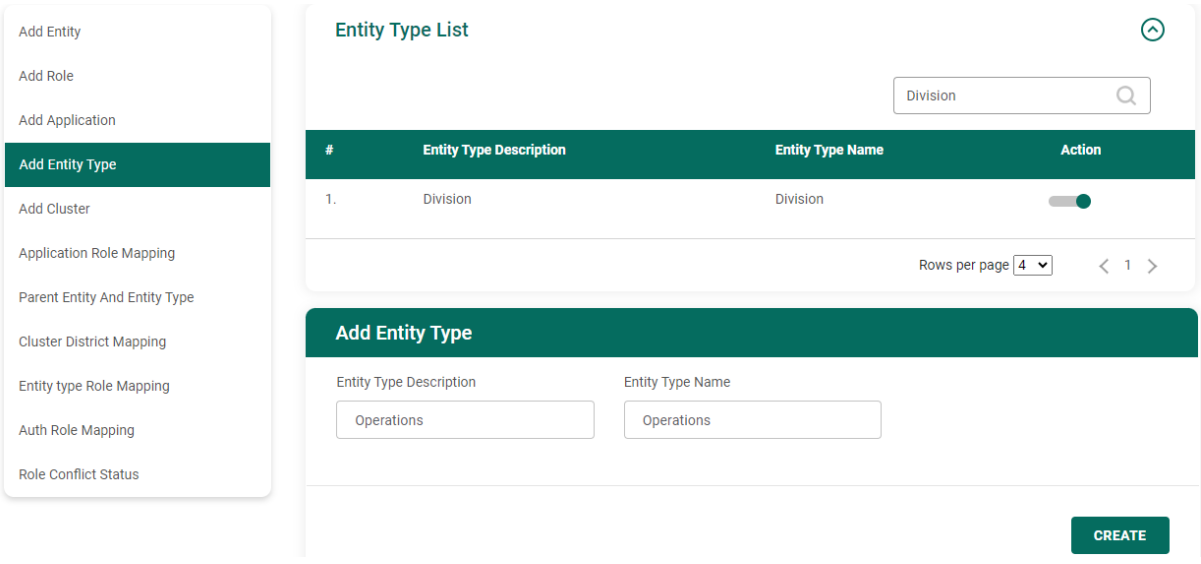
9.3. Add Application

Admin will be able to create new application through it, the naming convention created here will be used by the respective applications. Admin can search the application and disable it using the radio button.



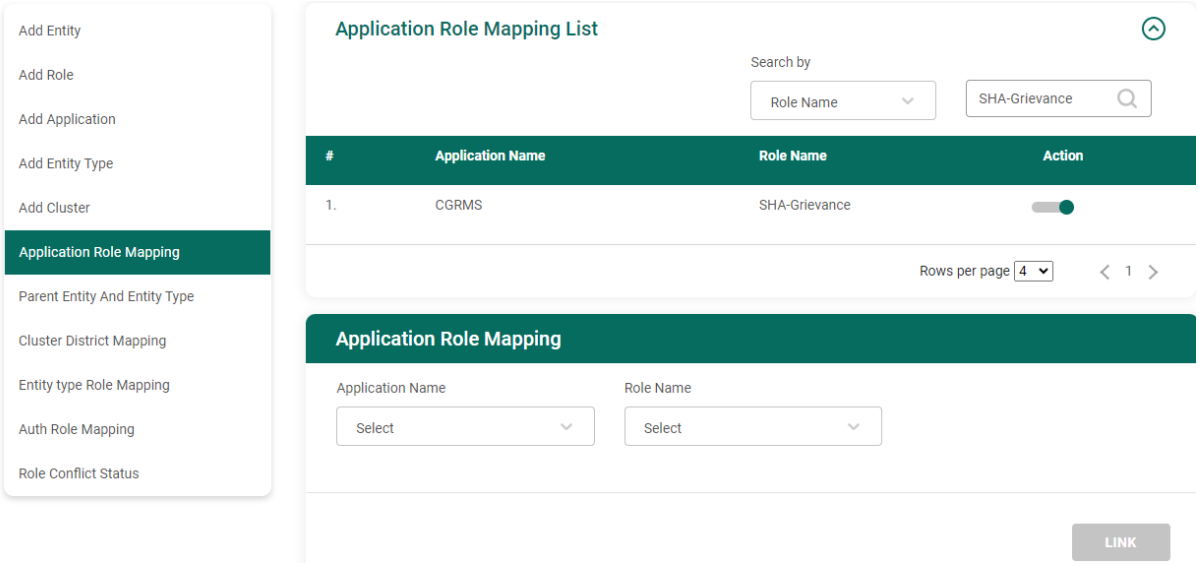
9.4. Add Entity Type

Admin will be able to create the entity type for the entity for its configuration during the entity creation.



9.5. Application Role Mapping

Admin will be able to perform the mapping of application and role such that when user will select the role then accordingly the mapped application will get populate in the dropdown.



9.6. Entity Type Role Mapping

Admin will be able to perform the mapping of entity type and role such that when user will select the entity type and role from the dropdown, then the respective mapping gets done. Thus all the entities under the entity type will get mapped with role. Now the mapping can be state wise by selecting the parent entity and role can be mapped specific to a particular entity in a entity type segment. Admin can also configure the role count for the configuration created, Thus restricting the no. of users for the entity in the state.

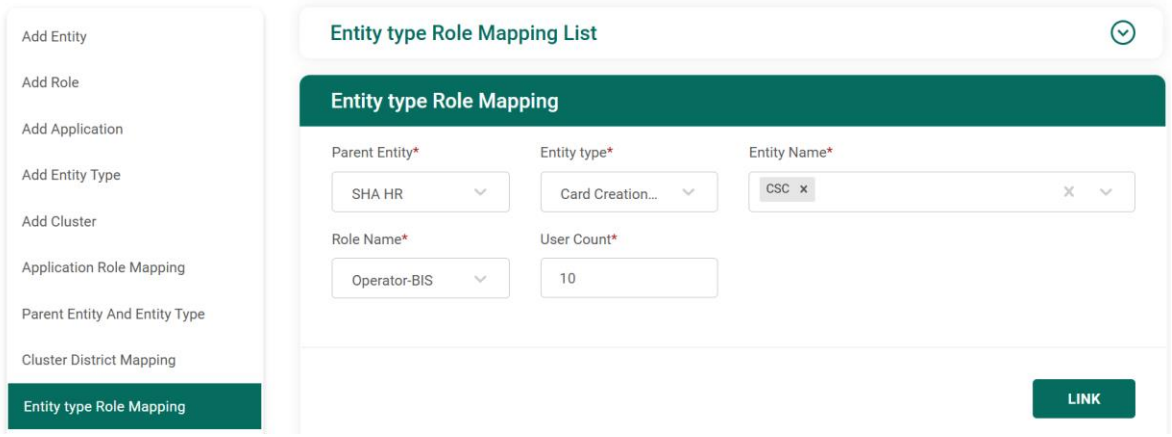
Entity type Role Mapping List

Search by

Select

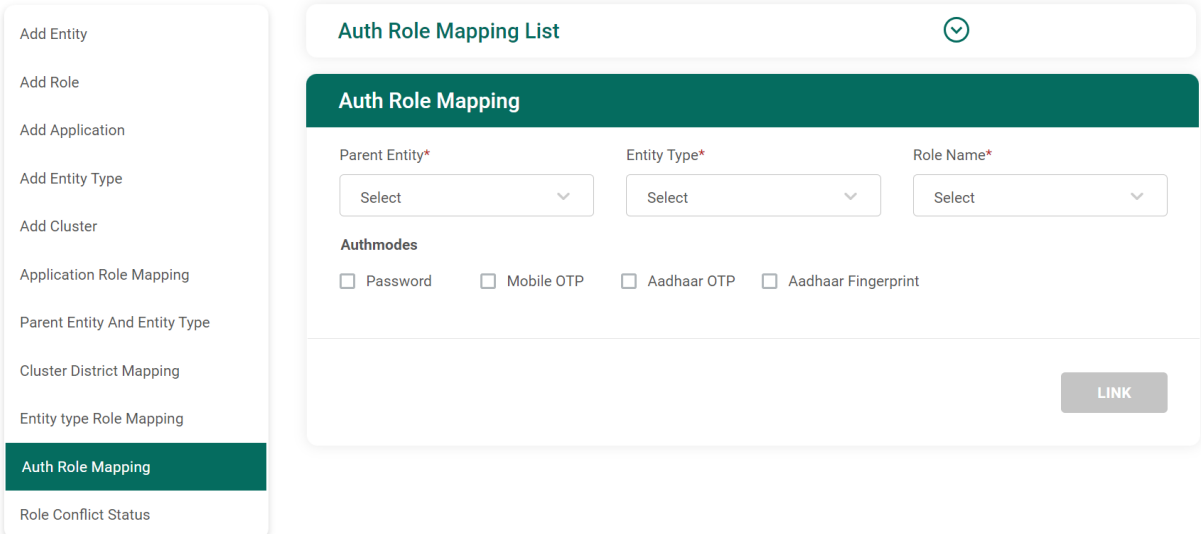
#	Parent Entity	Entity Type Name	Role Name	User Count	Edit	Action
14721.	SHA HR	Grievance	District Grievance Nodal Officer	10		
14722.	SHA HR	Grievance	District Grievance Redressal Committee	10		
14723.	NHA	Grievance	ADMIN	10		
14724.	SHA HR	Grievance	National Call Center	10		

Rows per page 4 1 ... 3680 3681 3682 3683



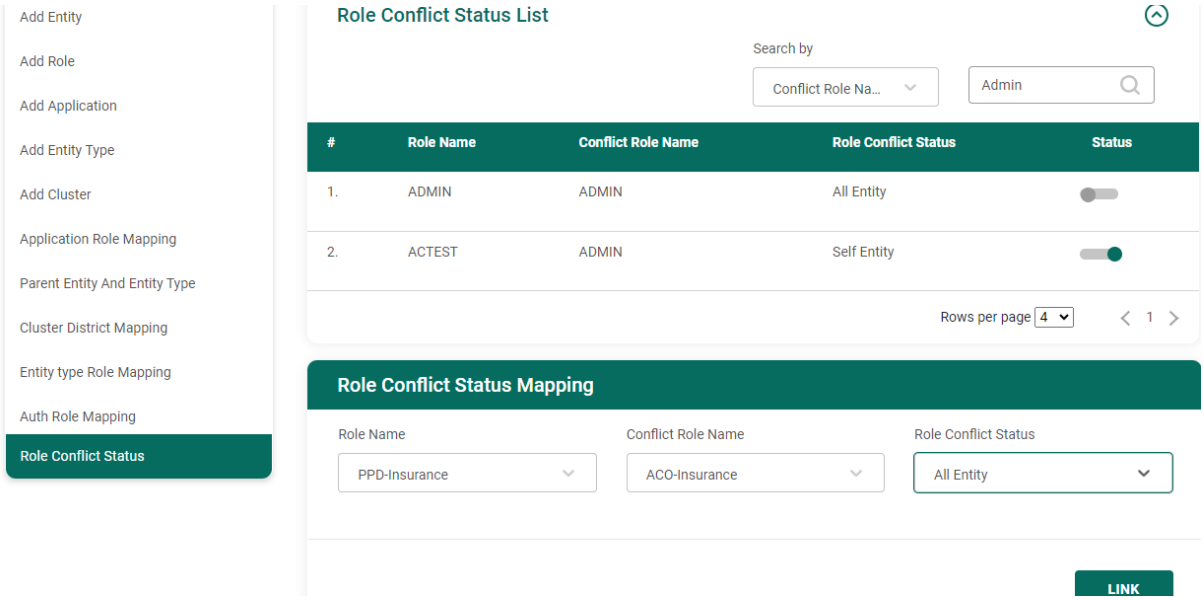
9.7. Auth Role Mapping

Admin will be able to perform the authentication mode and role mapping such that when user logs into the application then required authentication mode will populate based on the allocated role to the user. In case of multiple roles union of auth roles will get reflect for the users. Now the mapping can be done based on the parent entity.



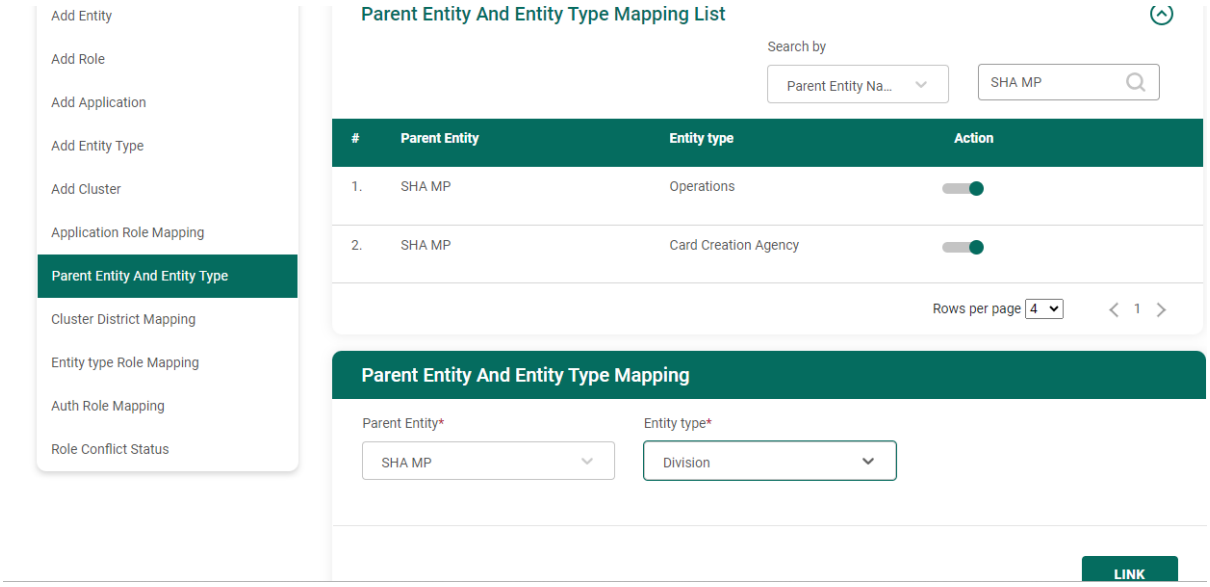
9.8. Conflicting Role Mapping

Admin will be able to create conflicting roles such that if role 1 and role 2 are conflicting then user will be able to request either of the roles at a time i.e. user cannot have both the roles at a time, If user raises the request for 1 role thus the request for conflicted role cannot be raised. Such as if CPD and CEX are conflicted roles then user cannot have both the roles at the same time.



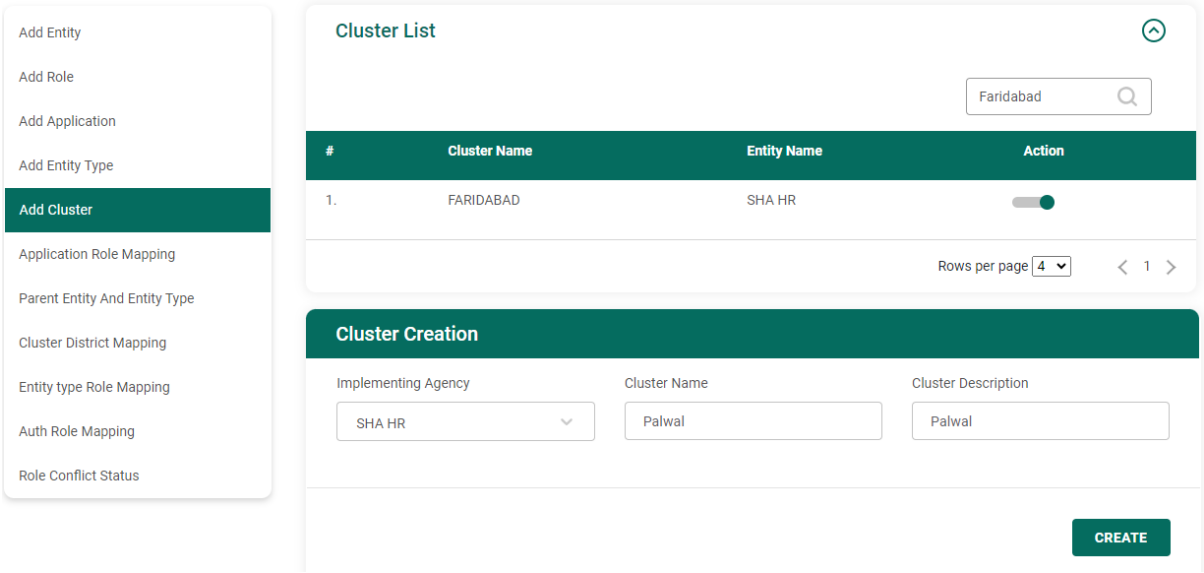
9.9. Parent Entity and Entity Type Mapping

Admin will be required to map the parent entity with entity type such that while role allocation only required entity types gets reflected in the dropdown.



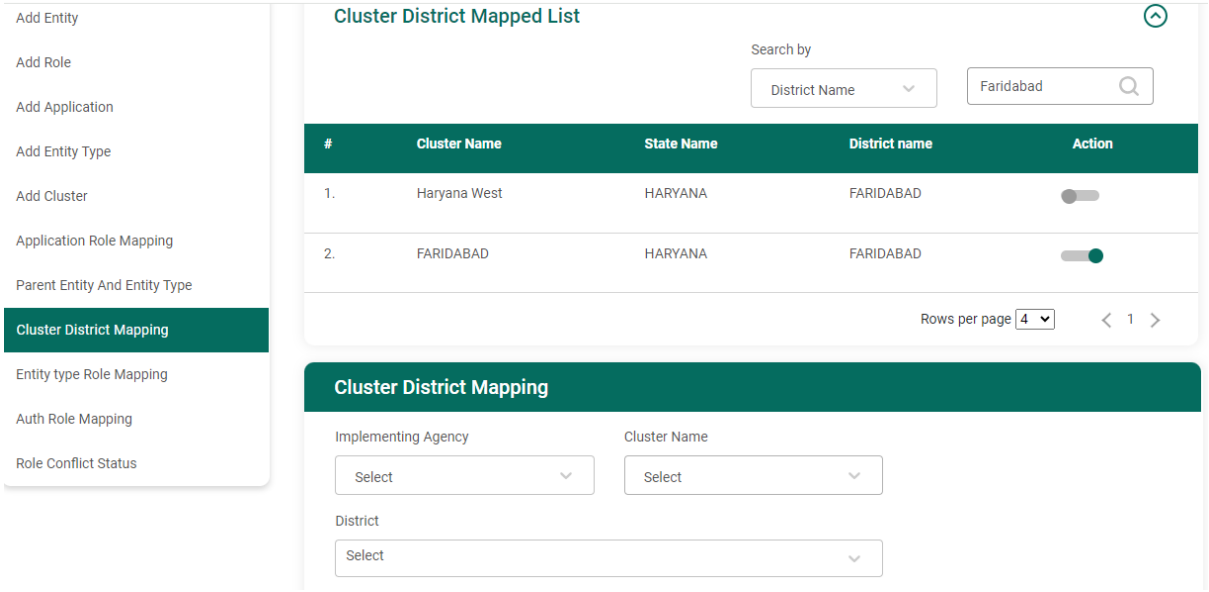
9.10. Add Cluster

Admin will be able to create the cluster by entering the implementation agency i.e. parent entity, cluster name and description. Once created , it will be visible in the above list.



9.11. Cluster District mapping

Admin will be required to map the cluster with the required district or number of district as per the implementation requirement. Once created, the mapping will be visible in the above mentioned list which can searched and disabled as per the requirement.



10. UMP: User Dashboard-Reports

Admin will have the facility to view the reports of the users in the graphical format to track the users and the ongoing activities. Admin will be able to view the Total Valid users, Pending roles for approval, Live users, Active user graph, Users hierarchy table, Entity search.

10.1. Total Valid Users

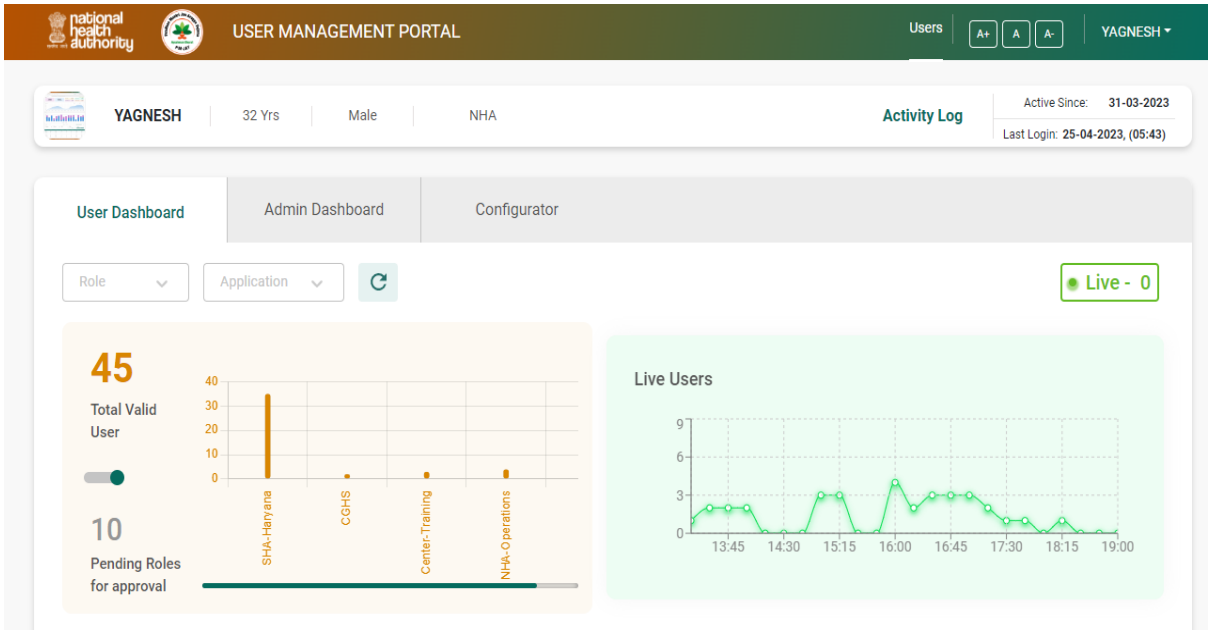
The graph facilitates admin to view the users based on the parent entities in the form of bar, when admin click on the bar, it will show the respective entity type under the parent entity. If admin once again click on the bar it will get back to the initial stage of the graph.

10.2. Pending Roles

The graph shows the roles which are required to be actioned upon i.e. Approve/Reject based on the parent entity and entity types in the ecosystem under the user role. The count on the left will show the cumulative count while the graph will show it entity wise.

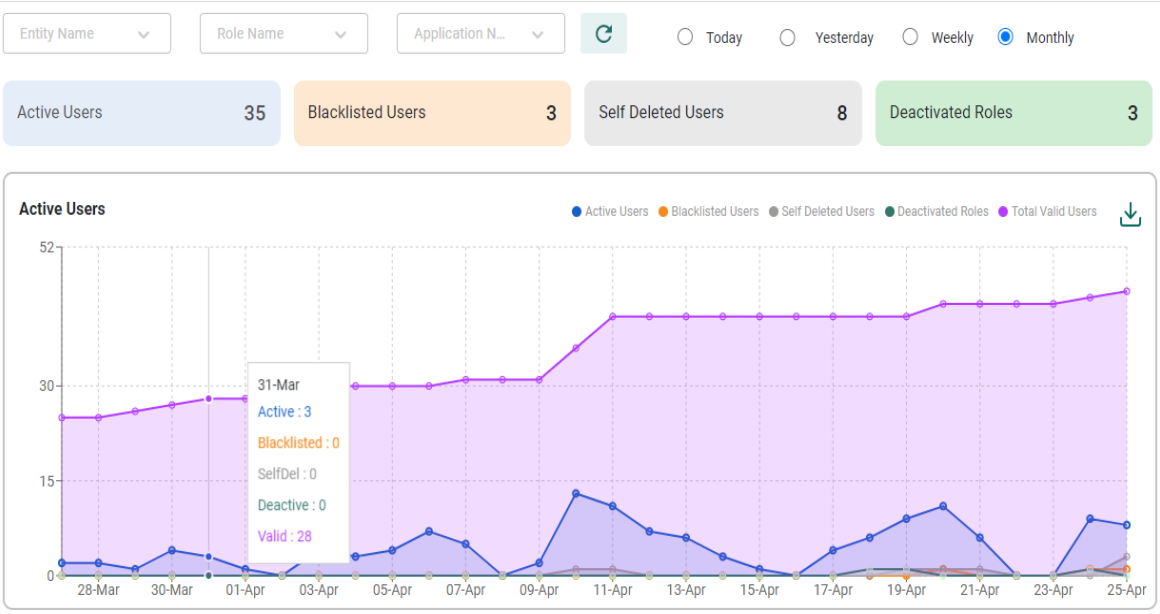
10.3. Live Users

The graph represents the data of live users for the last six hours from the system time at the time interval of 15 minutes. Such that the users logging in the application at any point of time will be shown at the next interval of 15 minutes. Here the x-axis represents the time while the y-axis represents the count of user.



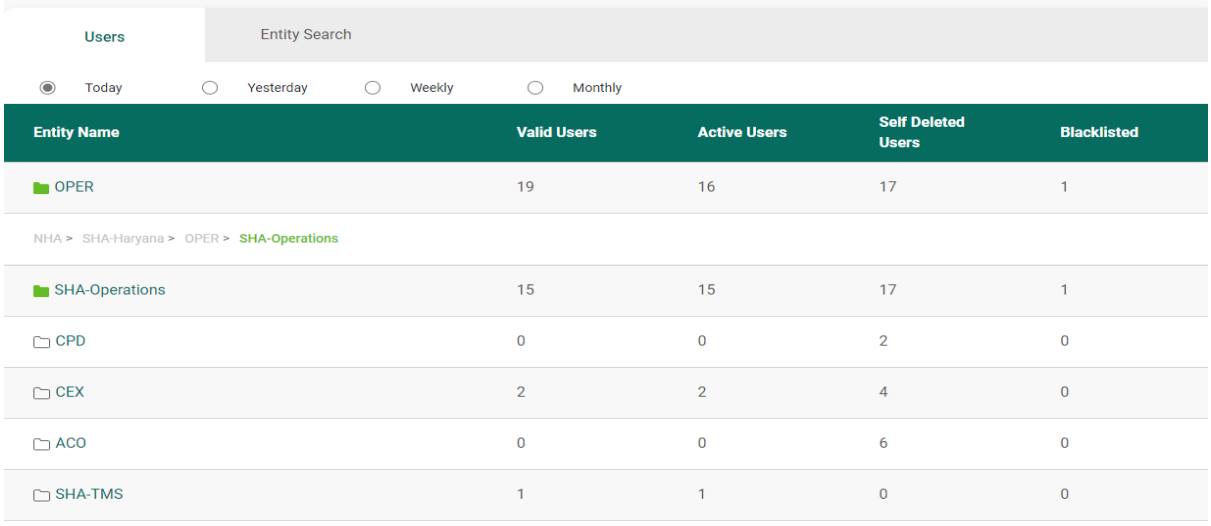
10.4. Active Users Graph

The graph represents the status of Valid users, Active users, Blacklisted users, self-deleted users, Deactivated roles that can be viewed on monthly for last 1 month, weekly for last 1 week, yesterday and today basis. Tab mentioned at the top of the graph is clickable and once clicked, the graph will show the data of the clicked tab based on the filter. In order to remove any filter or to move the graph to the initial stage, user will be required to click the reset button beside the application name filter at the top of the graph.



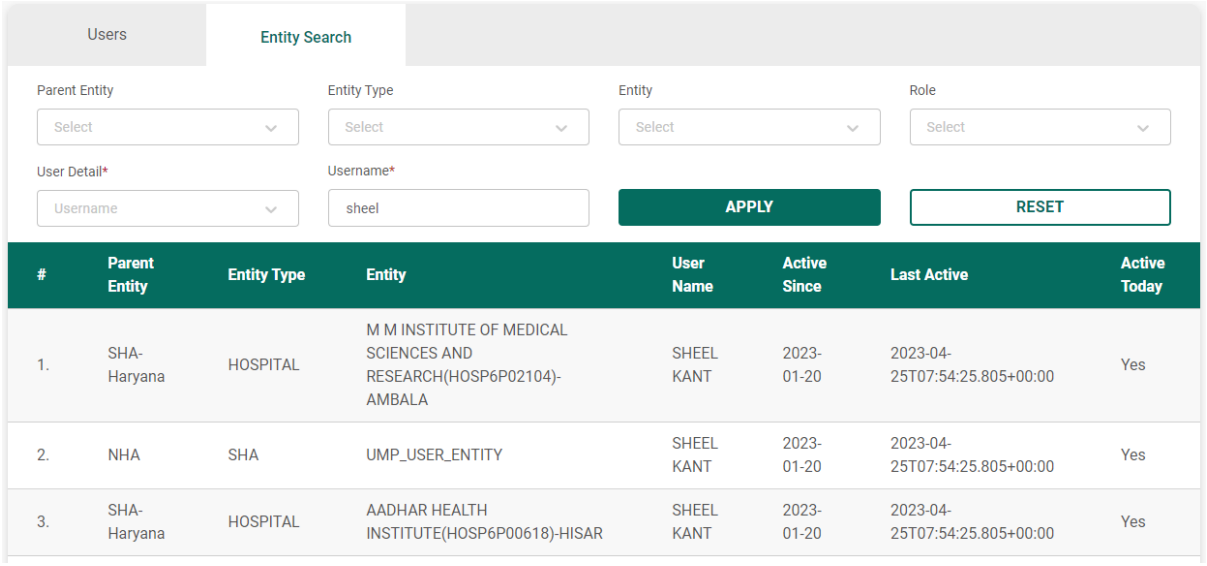
10.5. Hierarchy Table

The table represents the complete level of user hierarchy based on parent entity, entity type, entity name, role. At the end of table admin will be able to view the users details along with their profile while clicking the username. Admin can view the data based on the filter given at the top of the table.

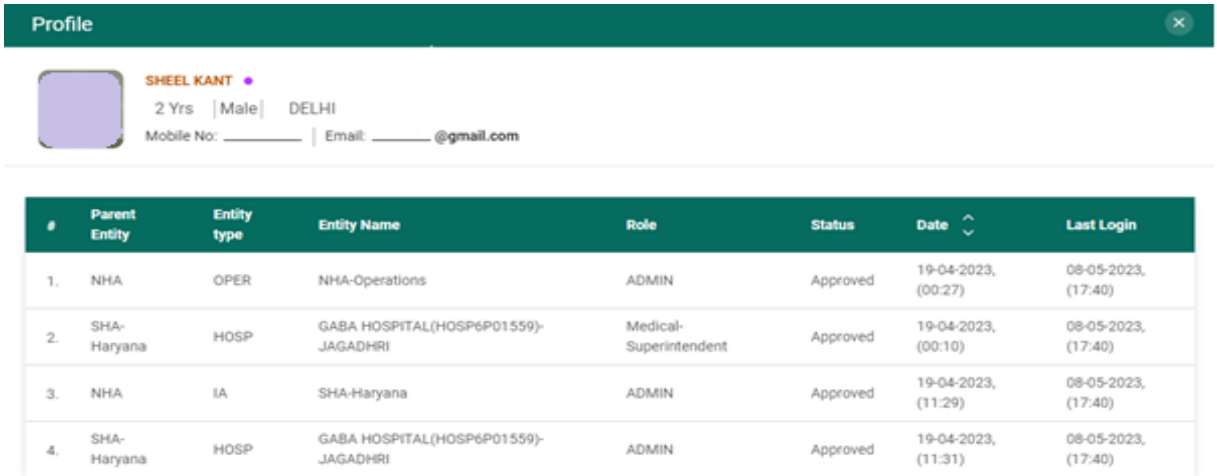


10.6. Entity Search

Admin will be able to search the user based on the user name, Aadhaar number, mobile number. User may or may not apply the filter at the top while the fields marked with star are mandatory to search the details. System will show the users details and while clicking the details, system will show the profile of the user.



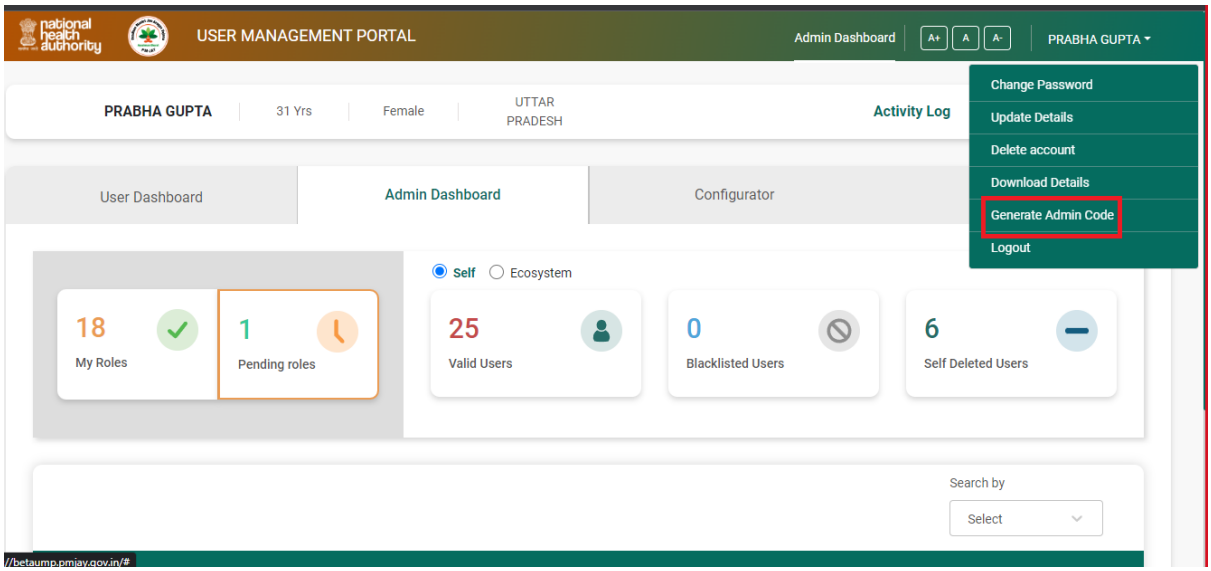
#	Parent Entity	Entity Type	Entity	User Name	Active Since	Last Active	Active Today
1.	SHA-Haryana	HOSPITAL	M M INSTITUTE OF MEDICAL SCIENCES AND RESEARCH(HOSP6P02104)-AMBALA	SHEEL KANT	2023-01-20	2023-04-25T07:54:25.805+00:00	Yes
2.	NHA	SHA	UMP_USER_ENTITY	SHEEL KANT	2023-01-20	2023-04-25T07:54:25.805+00:00	Yes
3.	SHA-Haryana	HOSPITAL	AADHAR HEALTH INSTITUTE(HOSP6P00618)-HISAR	SHEEL KANT	2023-01-20	2023-04-25T07:54:25.805+00:00	Yes



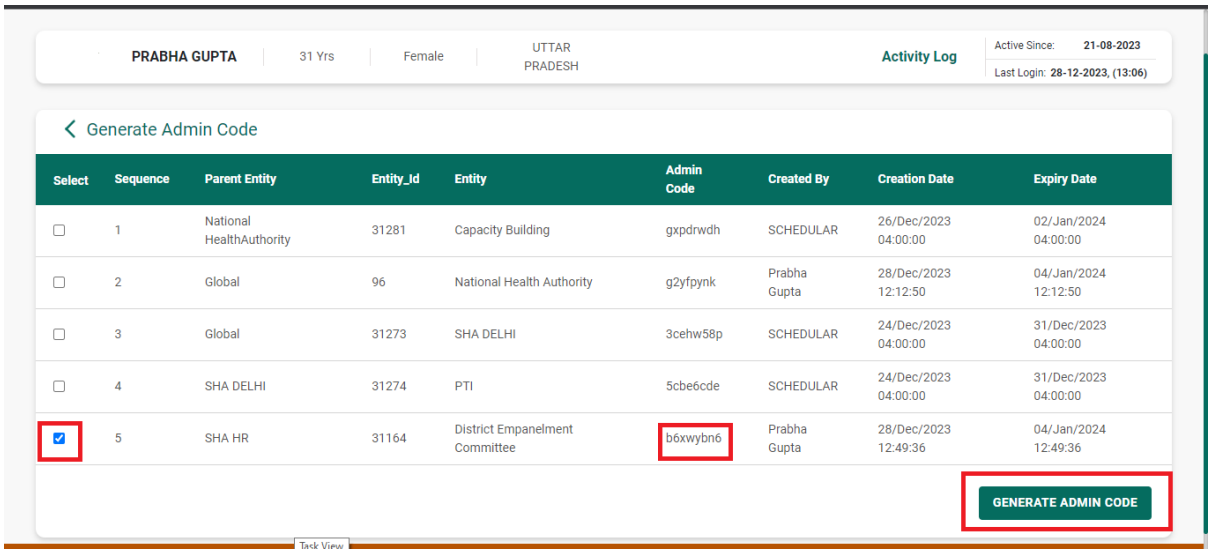
#	Parent Entity	Entity type	Entity Name	Role	Status	Date	Last Login
1.	NHA	OPER	NHA-Operations	ADMIN	Approved	19-04-2023, (00:27)	08-05-2023, (17:40)
2.	SHA-Haryana	HOSP	GABA HOSPITAL(HOSP6P01559)-JAGADHRI	Medical-Superintendent	Approved	19-04-2023, (00:10)	08-05-2023, (17:40)
3.	NHA	IA	SHA-Haryana	ADMIN	Approved	19-04-2023, (11:29)	08-05-2023, (17:40)
4.	SHA-Haryana	HOSP	GABA HOSPITAL(HOSP6P01559)-JAGADHRI	ADMIN	Approved	19-04-2023, (11:31)	08-05-2023, (17:40)

11. ADMIN CODE

UMP has the facility to allow the users to create their roles only under the authorised entity by taking the admin code for the required entity from their admin. In order to generate the admin code, admin is required to click on the name mentioned in the top right corner, A dropdown gets opened from where 'Generate Admin code' button is clicked.

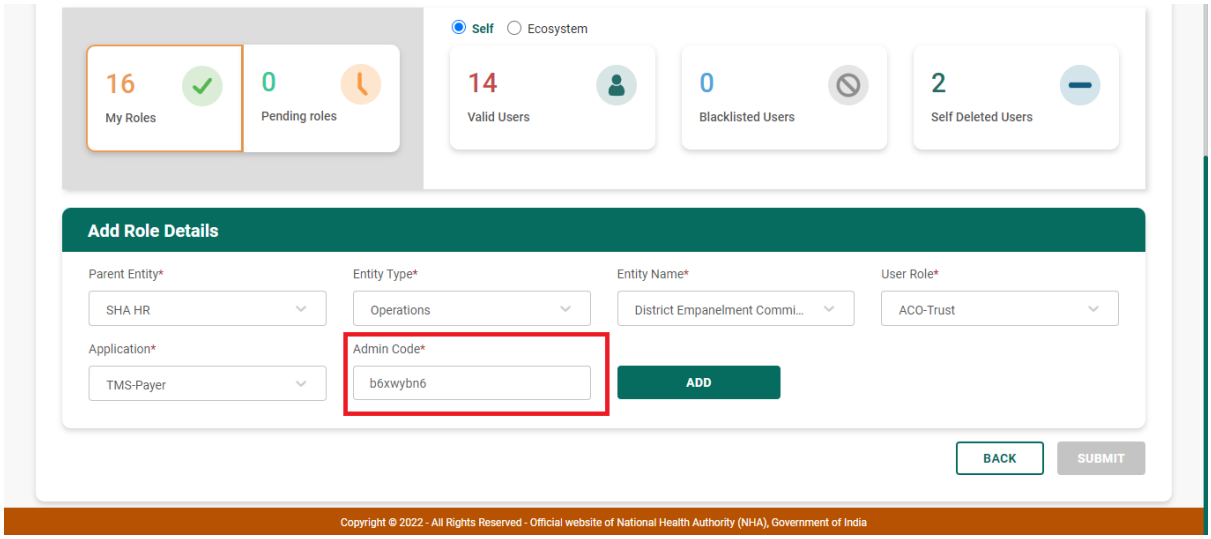


A new window gets opened to generate the code, admin is required to select the entity from the checkbox and click on the Generate Admin Code button. The code once generated will appear in the table and will be sent to the mobile. Admin can regenerate the code once every 24 hours while the system will auto generate the code every 7 days of last generated code.



Select	Sequence	Parent Entity	Entity_Id	Entity	Admin Code	Created By	Creation Date	Expiry Date
☐	1	National HealthAuthority	31281	Capacity Building	gxpdrwdh	SCHEDULAR	26/Dec/2023 04:00:00	02/Jan/2024 04:00:00
☐	2	Global	96	National Health Authority	g2yfpynk	Prabha Gupta	28/Dec/2023 12:12:50	04/Jan/2024 12:12:50
☐	3	Global	31273	SHA DELHI	3cehw58p	SCHEDULAR	24/Dec/2023 04:00:00	31/Dec/2023 04:00:00
☐	4	SHA DELHI	31274	PTI	5cbe6cde	SCHEDULAR	24/Dec/2023 04:00:00	31/Dec/2023 04:00:00
☑	5	SHA HR	31164	District Empanelment Committee	b6xwybn6	Prabha Gupta	28/Dec/2023 12:49:36	04/Jan/2024 12:49:36

Once the admin code is generated, admin is requested to share the code with their valid users to allow them to create their roles in the application.



12. IMPORTANT POINTS

1) The Admin login should be approved by the parent entity admin/Super admin as per the hierarchy.
2) All other users shall self-register for their respective role and there by the request will be approved by the respective Admin.
3) Each entity needs to have “Admin Role” in the User Management Portal.
4) Super Admin logins will be created from backend.
5) Currently, all the SHA admin logins will be approved by super admin Login
6) All other entity admin within the state will be approved by SHA.
7) All the self-registration will be approved by the respective entity admin.
8) Same Aadhar number cannot be used for multiple signup.

13. FAQ

Ques1 What is User Management Portal?
Ans. UMP is an application which has the following features:

- To Create users and their roles.
- To keep track of the users by viewing their activities, profile and history.
- To take necessary actions for the user by admin.
- To configure the application by super admin

Ques2 How to use UMP?
Ans. User will be required to sign-up on the portal using the Aadhaar number. Once the signup is done, user will be required to login the application and user can perform required actions.

Ques3 How to Sign-up in UMP?
Ans. User will be required to go to signup page. Now user will be required to perform e-KYC through Aadhaar number, once it is done user will be required to enter necessary details (Address, email ID, mobile number, user ID, password). Once the details are submitted the signup process is considered as completed.

Ques4 What can I do If I have forgotten my credentials?
Ans. User will be required to click on the forgot credential option on the login page, a new page will appear where the user will be required to perform Aadhaar e-KYC and post which user will be able to view and change the credential.

Ques5 How to reset user ID/password?
Ans. User will be required to click on the forgot credential option on the login page, a new page will appear where the user will be required to perform Aadhaar e-KYC and post which user will be able to view and change the credential.

Ques6 How to create role?
Ans. User will be required to login, now user will be able to view the add role on the portal (In case of admin dashboard under My role). User will be required to click on the add role and select the required parent entity, entity type, entity name, role, application and submit it for approval. Once the role is approved by admin user will be able to access the roles and perform the required action.

Ques7 What is parent entity?
Ans. Parent entity could be any entity which has a child entity under it. Such as SHA-State is the parent entity for hospital while Global/NHA is the parent entity for SHA-State.

Ques8 What is entity?
Ans. It is the body/organisation the user belongs to.

Ques9 What is entity type?
Ans. It represents the type of the entity user is working under.

Ques10 How to self-delete account?
Ans. User will be able to self-delete account by clicking on the name at the op right corner, a dropdown will appear with the self-delete as an option, once user click on it, a popup will appear on which user will be required to select the appropriate reason and generate both Aadhaar and mobile OTP by clicking the send OTP button once user enters correct OTP and click on Delete button, the account will get deleted.

Ques11 How to approve/reject a role?
Ans. Admin will be able to approve/reject a role from their dashboard under pending roles tab. User will be required to click on process button and a popup will appear to view profile, history and take the necessary action for the user.

Ques12 How to blacklist users?
Ans. Admin will be required to login on their dashboard. Under Valid Users tab, Admin will be able to view the list of users, click on the process button for whom the action will be required to be taken and a popup will appear to view profile, history and take necessary action for the user.

Ques13 How to activate/ deactivate a role?
Ans. Admin will be required to login on their dashboard. Under Valid Users tab, Admin will be able to view the list of users, click on the process button for whom the action will be required to be taken and a popup will appear to view profile, history and take necessary action for the user.

Ques14 How to unblock user?
Ans. Admin will be required to login on their dashboard. Under Blacklisted Uses tab, Admin will be able to view the list of users, click on the process button for whom the action will be required to be taken and a popup will appear to view profile, history and take necessary action for the user.

Ques15 What Should we do if the account gets lock due to wrong password in multiple attempts?
Ans. The account will get unlocked itself on the next day.