

Sunward Portal Management System

DOCUMENT INFORMATION

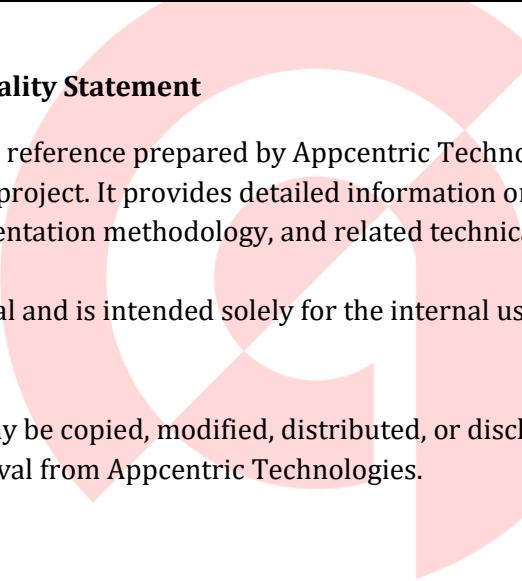
Prepared by	Appcentric Technologies
Client	Sunward
Project Name	Sunward Portal Management System
Prepared by	Vijayakumar
Module Name	Users, User Group, User Permissions Module
Pages	9

Disclaimer and Confidentiality Statement

This document is a technical reference prepared by Appcentric Technologies for the Sunward Portal Management System project. It provides detailed information on the system architecture, technical approach, implementation methodology, and related technical specifications.

This document is confidential and is intended solely for the internal use of the authorized technical team of Sunward.

No part of this document may be copied, modified, distributed, or disclosed to any third party without prior written approval from Appcentric Technologies.



AppCentric
Technologies

Table of Contents

Sunward Portal Management System.....	1
1. Project Overview	3
2. Objectives	3
3. System Modules & Key Functions	3
3.1 Users Module — Key Features.....	3
3.2 Users Module — Key Features.....	3
3.3 User Permissions by Roles — Key Features.....	4
3.4 Transfer Permissions – Key Features	4
4. Functional Components.....	4
4.1 Users.....	4
4.2 User Permissions by Roles	5
4.3 User Group	6
4.4 Transfer Permissions.....	7
5. Database Structure (Detailed Explanation).....	7
5.1 User → UserRoleAssign → UserRole	7
5.2 Role → RolePermission.....	7
5.3 User → UserGroupMembers → UserGroup	7
6. Business Logic.....	8
6.1 Users - Business Logic	8
6.2 User Permissions by Roles – Business Logic.....	8
6.3 User Group – Business Logic.....	9
6.4 Transfer Execution Logic – Business Logic.....	9
7. Summary.....	10

1. Project Overview

The **Users & User Permissions Module** manages all system user accounts, access control, and role-based permissions across the Sunward Portal. This module ensures that each user has appropriate system access according to their role, department, and responsibilities while maintaining strong audit and security compliance.

It consists of two major components:

1. **Users** – Manages user identity, login details, status, and account controls.
2. **User Group** - Logical organization of teams across the organization, multiple users in bulk
3. **User Permissions by Roles** – Controls system access based on predefined roles.
4. **Transfer Permissions** - To simplify reassignment of data such as conversations, form data.

2. Objectives

- Maintain a centralized repository of all active and inactive system users.
- Streamline the user onboarding and offboarding process.
- To organize users into meaningful functional groups.
- Provide secure and structured role-based access control.
- Ensure that each module, screen, and action is permission-controlled.
- Support audit requirements by providing traceability for all user changes.
- Reduce administrative overhead by using reusable permission roles.
- Prevent unauthorized access and strengthen system security.

3. System Modules & Key Functions

3.1 Users Module — Key Features

- View full list of users with paging, filtering, and search.
- Add new users (Sage ID, Full Name, Nick Name).
- Edit existing user information.
- Activate / Deactivate / Lock accounts.
- Reset Password & Sync user data.
- Track modification history (Modified By, Modified Date).
- Assign User Roles.

3.2 Users Module — Key Features

- Create and manage user groups for department/functional grouping.
- Add or remove multiple users using multi-select.
- Edit group name, description, and status.
- Track added/modified details for audit purposes.
- Use groups for workflow routing and shared access logic.

- Activate or deactivate groups based on operational needs.

3.3 User Permissions by Roles — Key Features

- Define system roles (e.g., Admin, HR, QC, Store, General, PA, Production Supervisor).
- Assign application modules and submodules to each role.
- Permission tree structure with nested items and checkboxes.
- “Check All” feature to grant full access.
- Save Permission to apply changes to selected role.
- Automatic integration with Users module (users inherit role permissions).

3.4 Transfer Permissions – Key Features

- Select "From User" and "To User".
- Transfer operational data including:
 - User Groups
 - File Profile Type Security
 - Email Conversations
 - Dynamic Form Master
 - Dynamic Form Data
- Bulk selection supported.
- Filtering, grouping, and searching available.
- Auto-audit of previous owner (Previous User column).
- Ensures smooth role transition without data loss.

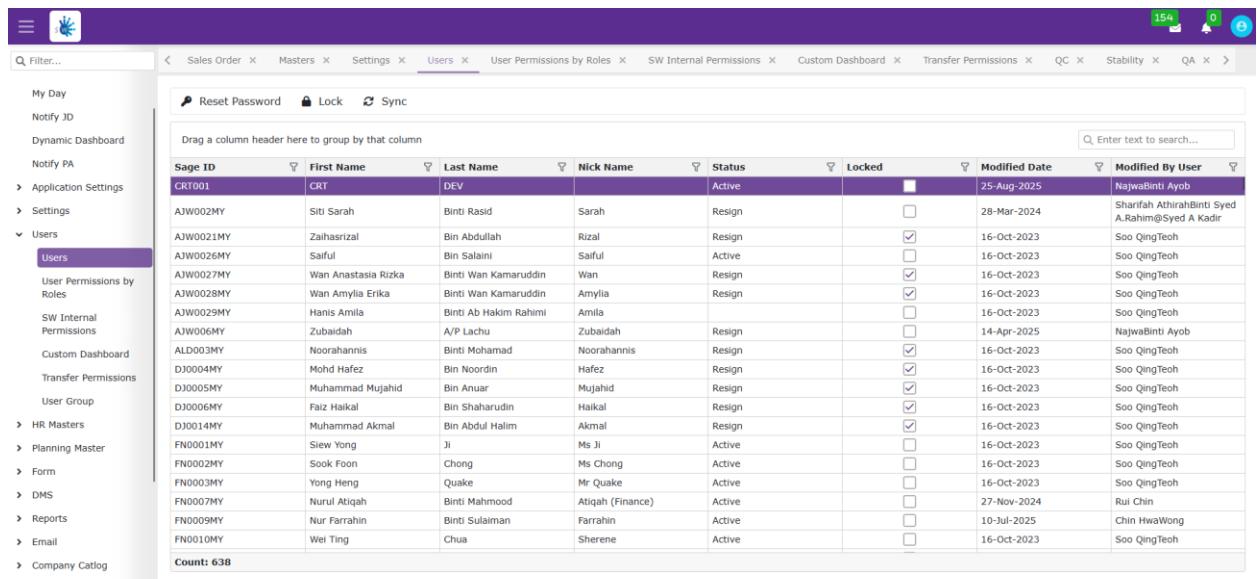
4. Functional Components

4.1 Users

This component manages all system user accounts and controls the basic identity information stored in the portal.

Key Functionalities

- Maintain complete list of users with paging, filtering, and searching.
- Create new users with Sage ID, Full Name, Nick Name, and Employment details.
- Edit user details and update status (Active / Resign / On Hold).
- Lock or unlock user accounts.
- Reset password and Sync user data with external systems.
- View modification history such as “Modified By” and “Modified Date”.



Sage ID	First Name	Last Name	Nick Name	Status	Locked	Modified Date	Modified By User
CRT001	CRT	DEV		Active	<input type="checkbox"/>	25-Aug-2025	NajwaBinti Ayob
AJW002MY	Siti Sarah	Binti Radid	Sarah	Resign	<input type="checkbox"/>	28-Mar-2024	Sharifah AthirahBinti Syed A.Rahim@Syed A Kadir
AJW0021MY	Zaiharizal	Bin Abdullah	Rizal	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
AJW0026MY	Saiful	Bin Salaini	Saiful	Active	<input type="checkbox"/>	16-Oct-2023	Soo QingTech
AJW0027MY	Wan Anastasia Rizka	Binti Wan Kamaruddin	Wan	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
AJW0028MY	Wan Amylia Erika	Binti Wan Kamaruddin	Amylia	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
AJW0029MY	Hanis Amila	Binti Ab Hakim Rahimi	Amila		<input type="checkbox"/>	16-Oct-2023	Soo QingTech
AJW006MY	Zubaidah	A/P Lachu	Zubaidah	Resign	<input type="checkbox"/>	14-Apr-2025	NajwaBinti Ayob
ALD003MY	Noorahannis	Binti Mohamad	Noorahannis	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
DJ0004MY	Mohd Hafez	Bin Noordin	Hafez	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
DJ0005MY	Muhammad Mujahid	Bin Anuar	Mujahid	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
DJ0006MY	Faiz Halikal	Bin Shaharudin	Halikal	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
DJ0014MY	Muhammad Akmal	Bin Abdul Halim	Akmal	Resign	<input checked="" type="checkbox"/>	16-Oct-2023	Soo QingTech
FN0001MY	Siew Yong	Ji	Ms Ji	Active	<input type="checkbox"/>	16-Oct-2023	Soo QingTech
FN0002MY	Sook Foon	Chong	Ms Chong	Active	<input type="checkbox"/>	16-Oct-2023	Soo QingTech
FN0003MY	Yong Heng	Quake	Mr Quake	Active	<input type="checkbox"/>	16-Oct-2023	Soo QingTech
FN0007MY	Nurul Atiqah	Binti Mahmood	Atiqah (Finance)	Active	<input type="checkbox"/>	27-Nov-2024	Rui Chin
FN0009MY	Nur Farrahin	Binti Sulaiman	Farrahin	Active	<input type="checkbox"/>	10-Jul-2025	Chin Hwa Wong
FN0010MY	Wei Ting	Chua	Sherene	Active	<input type="checkbox"/>	16-Oct-2023	Soo QingTech

4.2 User Permissions by Roles

This component defines system access rights based on predefined roles.

Key Functionalities

- Display full list of system roles (e.g., HR, Store, QC, Sales, Supervisor, Contractor).
- Assign application permissions module-wise (Dashboard, Application Settings, HR Masters, Sales Order, etc.).
- Enable “Check All” to assign full system access quickly.
- Grant or revoke specific menu/submenu access using hierarchical view.
- Save and update role-based permissions centrally.
- Ensure consistent access control for all users under the same role.

User Permissions by Roles	
SW Internal Permissions	<input type="checkbox"/> Check All
Custom Dashboard	<input type="checkbox"/> Item Card - HPLC Column
Transfer Permissions	<input type="checkbox"/> Stability Calendar
User Group	<input type="checkbox"/> Stability Outstock
HR Masters	<input checked="" type="checkbox"/> Dynamic Dashboard
Planning Master	<input checked="" type="checkbox"/> My Day
Form	<input checked="" type="checkbox"/> Dashboard
DMS	<input checked="" type="checkbox"/> Notify JD
Reports	<input checked="" type="checkbox"/> Notify PA
Email	<input checked="" type="checkbox"/> Dynamic Dashboard
Company Catalog	<input checked="" type="checkbox"/> Application Settings
Sales Order	<input checked="" type="checkbox"/> Application Master
	<input checked="" type="checkbox"/> Application Master Parent
	<input checked="" type="checkbox"/> Settings
	<input checked="" type="checkbox"/> Users
	<input checked="" type="checkbox"/> HR Masters
	<input checked="" type="checkbox"/> Planning Master
	<input checked="" type="checkbox"/> Form
	<input checked="" type="checkbox"/> DMS

4.3 User Group

This component allows grouping users for organizational, departmental, or workflow needs.

Key Functionalities

- Create and maintain user groups (e.g., SWMAL ENG, SWMAL FIN, SWMAL HR).
 - Add or remove multiple users using multi-selection.
 - Edit group name, description, and status.
 - Track added/modified information for audit purposes.
 - Use groups for workflow approvals, routing, and shared access logic.
 - Provide consistent item information across pricing and ordering workflows.

The screenshot shows the HRMIS software interface with the following details:

- Header:** Employee, SW Internal Permissions, Custom Dashboard, Transfer Permissions, User Group.
- Left Sidebar:** My Day, Notify JD, Dynamic Dashboard, Notify PA, Application Settings, Settings, Users, Users, User Permissions by Roles, SW Internal Permissions, Custom Dashboard, Transfer Permissions, User Group (selected).
- Top Bar Buttons:** + Add, Edit, Delete, Export.
- Search Bar:** Enter text to search...
- Table Headers:** Name, Description, Added By, Added Date, Modified By, Modified Date, Status Code.
- Table Data:**
 - Name: SWMAL ENG, Description: (empty), Status: Active.
 - Users: Kam Wai-Low-Maintenance Manager, Saifuddin Bin Abdul Jallil-Bin Abdul Jallil-Maintenance Engineer, Mohd Razali-Bin Mustapha-Maintenance Technician, Muhammad Faris-Bin Md Anuar-Maintenance Technician, Zainul Zikry-Bin Shahrol Ismail-Maintenance Engineer, Maizatul Hamira-Binti Mohamed-Maintenance Admin, NURNADIA JASMIN-BINTI KAMARUL Bahrin-Maintenance Admin, MUHAMMAD AMAR-BIN MOHD ALI-Maintenance Technician, NOORLIANA-BINTI KHOIRI-Maintenance Admin.
- Bottom Table:**

<input type="checkbox"/>	SWMAL FIN	Soo QingTeho	08-Jun-2023	Soo QingTeho	08-Jun-2023	Active
<input type="checkbox"/>	SWMAL HR	Soo QingTeho	08-Jun-2023	Soo QingTeho	21-Feb-2024	Active
<input type="checkbox"/>	SWMAL ICT	Soo QingTeho	08-Jun-2023	Soo QingTeho	31-Jan-2024	Active
- Buttons:** Save, Cancel.

4.4 Transfer Permissions

- **User Groups**
 - Transfer all group memberships from one user to another.
 - Ensures new user inherits group-based visibility and routing logic.
- File Profile Type Security
 - Transfers file access settings (security clearance, profile types).
 - Maintains attached document permissions.
- Email Conversations
 - Displays all conversation records belonging to the selected "From User".
 - Allows selection of single or multiple conversations.
 - Transfers ownership to the selected "To User".
- Dynamic Form Master
 - Transfers all user-created dynamic forms.
 - Ensures continuity of form management.
- Dynamic Form Data
 - Transfers form entries and submission records linked to the user.

5. Database Structure (Detailed Explanation)

The Users Module is supported by several relational tables responsible for storing user profiles, group assignments, role permissions, and audit information. Below is the detailed breakdown of these database components.

5.1 User → UserRoleAssign → UserRole

Users (1) ----- (∞) UserRoleAssign (∞) ----- (1) UserRole

- One user can have multiple roles.
- Each role can apply to many users through mapping.

5.2 Role → RolePermission

UserRole (1) ----- (∞) RolePermission

- Each role can have multiple module permissions.
- Permissions define visibility and action scope.

5.3 User → UserGroupMembers → UserGroup

Users (1) ----- (∞) UserGroupMembers (∞) ----- (1) UserGroup

- Users can belong to multiple groups.

- Groups can contain multiple users.
- Groups are separate from roles and do not impact login permissions.

6. Business Logic

This section explains how the **Users**, **User Permissions**, and **User Group** modules operate behind the scenes, including validation rules, logic, and system behavior.

6.1 Users - Business Logic

6.1.1 User Creation Logic

- A new user must have a **unique Sage ID**.
- System checks if the Sage ID already exists before allowing creation.
- Mandatory fields: Sage ID, First Name, Last Name, Status.
- Default values assigned:
- Status → Active
- Locked → False

6.1.2 User Modification Logic

- Any changes update:
- **Modified By**
- **Modified Date**
- Locked users cannot perform login until unlocked by admin.
- Status “Resign/Inactive” automatically removes the user from active permission lists.

6.1.3 Password Reset Logic

- Reset triggers:
- Temporary password generation.
- Force password change on next login.
- “Sync” updates the user’s basic profile fetched from HR/Sage system.

6.2 User Permissions by Roles – Business Logic

6.2.1 Role-Based Access Control (RBAC)

- Each user belongs to **one or more roles**.
- Each role includes **a set of application permissions**.
- When user logs in:
- System loads all menus allowed under assigned roles.
- Restricted menus are hidden.

6.2.2 Permission Assignment Rules

- Selecting a parent menu auto-selects child menus.
- Removing access from a top menu revokes all nested menus.
- “Check All” grants full permission to a role instantly.

6.2.3 Save Permission Logic

When admin clicks **Save Permission**:

- System clears old permissions for that role.
- Inserts new permission list.
- Updates audit logs.

6.3 User Group – Business Logic

6.3.1 Group Creation Logic

- Group name must be unique.
- Mandatory fields: Group Name, Status.
- Users can be added using multi-select dropdown.

6.3.2 Group User Assignment Logic

- When users are added:
- Entries stored in UserGroupMembers table.
- When users are removed:
- Records are deleted automatically.

6.3.3 Group Behavior in Other Modules

Groups may be used for:

- Assignment routing
- Notification targeting
- Departmental segmentation

6.4 Transfer Execution Logic – Business Logic

For each selected item:

- Update owner column (UserID) to “To User”.
- Save previous owner in “Previous User”.
- Update audit fields:
 - Modified By
 - Modified Date

Email Conversation Transfer Logic

- Reassign Conversations.OwnerUserID.
- Log PreviousUserID.
- Update ModifiedDate.

Group Transfer Logic

- Add “To User” to same groups as “From User”.
- Option to remove old user (optional depending on business rules).

7. Summary

The **Users, User Permissions, and User Group Modules** collectively form the core of system security, access control, and user management within the Sunward Portal. These modules ensure that every user is properly identified, assigned with appropriate privileges, and organized into functional groups for workflow and operational needs.

The **Users module** provides centralized control over user identity, account status, login permissions, and audit tracking. Administrators can manage new and existing users efficiently using features such as account locking, password reset, synchronization, and modification history.

The **User Permissions by Roles module** enables fine-grained access control through predefined roles. Each role determines which modules, menus, and screens users can access. This role-based permission structure ensures consistent, secure, and scalable access management across all departments.

The **User Group module** complements roles by allowing users to be grouped based on department, function, or workflow requirements. These groups support operational processes such as approval routing, task assignments, and departmental segmentation without affecting system access rights.