

# User Management Module

User Manual - Console Interface

SONARWORKS WORKFLOW SYSTEM

Version 1.1

# Table of Contents

1. Introduction
2. Accessing User Management
3. User List Overview
4. Creating New Users
5. Editing User Information
6. User Roles and Permissions
7. Organization Assignment
8. Password Management
9. Locking and Unlocking Users
10. User Types
11. Best Practices

# 1. Introduction

The User Management module enables administrators to manage user accounts, assign roles and permissions, and control access to the Sonar Workflow System. Proper user management is essential for system security and effective workflow operations.

**Key Functions:**

- Create and maintain user accounts
- Assign roles and privileges
- Map users to organizational units
- Manage passwords and security
- Lock/unlock user accounts
- Track user login activity

**NOTE:** User Management is only accessible to users with administrative privileges.

*[Screenshot: User Management Overview]*

*Figure: User Management Overview*

# 2. Accessing User Management

**Steps:**

- Step 1:** Log in with administrator credentials
- Step 2:** Click 'Administration' in the navigation sidebar
- Step 3:** Click 'Users' from the sub-menu
- Step 4:** The User List page displays

*[Screenshot: Navigation to User Management]*

*Figure: Navigation to User Management*

# 3. User List Overview

## 3.1 List Columns

Column	Description
Username	Unique login identifier
Full Name	User's display name (first and last name)
Email	Email address for notifications
User Type	Category: SYSTEM, STAFF, MANAGER, EXTERNAL

Roles	Assigned roles (comma-separated)
Status	Active/Inactive/Locked indicator
Last Login	Date and time of last successful login
Actions	Edit, Lock/Unlock, Reset Password, Delete

*[Screenshot: User List Table]*

*Figure: User List Table*

## 3.2 User Status Indicators

Status	Indicator	Meaning
Active	Green badge	User can log in normally
Inactive	Gray badge	User account is disabled
Locked	Red badge	User is locked out (failed logins or manual lock)

## 3.3 Filtering Users

Use filters to find specific users:

Filter	Options
Search	Search by username, name, or email
User Type	SYSTEM, STAFF, MANAGER, EXTERNAL, All
Status	Active, Inactive, Locked, All
Role	Filter by specific role assignment
Corporate/SBU	Filter by organizational unit

# 4. Creating New Users

## 4.1 Starting User Creation

**Steps:**

**Step 1:** Navigate to Administration > Users

**Step 2:** Click the '+ New User' button

**Step 3:** The User Form opens in creation mode

## 4.2 User Form Fields

**Basic Information:**

Field	Required	Description
Username	Yes	Unique login ID (no spaces, alphanumeric)
Email	Yes	Valid email address for notifications

First Name	Yes	User's first name
Last Name	Yes	User's last name
Phone	No	Contact phone number
Staff ID	No	Employee/staff identification number
User Type	Yes	Category of user (STAFF, MANAGER, etc.)
Password	Yes (new)	Initial password (or auto-generate)
Must Change Password	No	Force password change on first login

*[Screenshot: User Creation Form - Basic Info]*

*Figure: User Creation Form - Basic Info*

### 4.3 Role Assignment

In the Roles section:

**Steps:**

**Step 1:** View available roles in the list

**Step 2:** Check the checkbox for each role to assign

**Step 3:** Multiple roles can be assigned to one user

**Step 4:** Roles determine user permissions and access

### 4.4 Organization Assignment

Assign user to organizational units:

- Corporates: Which corporate entities user belongs to
- SBUs: Strategic Business Units
- Branches: Physical branch locations
- Departments: Departmental assignment

### 4.5 Saving the User

**Steps:**

**Step 1:** Fill in all required fields

**Step 2:** Assign appropriate roles

**Step 3:** Set organization mappings

**Step 4:** Click 'Save' button

**Step 5:** User is created and can now log in

**TIP:** The initial password should be communicated securely to the user. Consider enabling 'Must Change Password' for security.

## 5. Editing User Information

### 5.1 Opening User for Edit

**Steps:**

**Step 1:** Locate the user in the User List

**Step 2:** Click the 'Edit' button (pencil icon)

**Step 3:** The User Form opens with existing data

### 5.2 Editable Fields

Most fields can be edited:

- Basic information (name, email, phone)
- User type
- Role assignments
- Organization mappings
- Active status

**NOTE:** Username typically cannot be changed after creation. Contact system support if username change is needed.

### 5.3 Saving Changes

**Steps:**

**Step 1:** Make necessary modifications

**Step 2:** Click 'Save' to update the user

**Step 3:** Changes take effect immediately

**Step 4:** User may need to log out and back in for role changes to apply

## 6. User Roles and Permissions

### 6.1 Understanding Roles

Roles are collections of permissions that define what a user can do in the system. Each role has specific privileges that grant access to features and functions.

## 6.2 Common System Roles

Role	Description	Typical Permissions
Administrator	Full system access	All features, user management, settings
Workflow Manager	Manage workflows	Create/edit workflows, view all instances
Approver	Process approvals	View/approve assigned workflows
Initiator	Submit workflows	Submit workflows, view own submissions
Viewer	Read-only access	View workflows and reports only
Report User	Access reports	View and export reports

## 6.3 Assigning Multiple Roles

Users can have multiple roles. Permissions are additive:

### Example: Multiple Role Assignment

*User: John Smith*

*Assigned Roles:*

- Initiator (can submit workflows)
- Approver (can approve workflows)

*Result: John can both submit and approve workflows*

*(Note: Users typically cannot approve their own submissions)*

## 6.4 Role Best Practices

- Assign minimum necessary roles (principle of least privilege)
- Review role assignments periodically
- Use role-based rather than individual permissions
- Document role purposes and permissions
- Create custom roles for specific job functions

# 7. Organization Assignment

Organization assignment controls which workflows and data a user can access based on their organizational unit membership.

## 7.1 Organization Hierarchy

Level	Description	Example
Corporate	Top-level organization	Holding Company, Subsidiary A
SBU	Strategic Business Unit	Finance, Operations, HR

Branch	Physical location	Head Office, Regional Office
Department	Functional department	IT, Accounting, Legal

## 7.2 Assigning Organizations

### Steps:

**Step 1:** In the User Form, locate the Organization section

**Step 2:** Select appropriate Corporates from the multi-select

**Step 3:** Select applicable SBUs

**Step 4:** Select Branches if applicable

**Step 5:** Select Departments if applicable

## 7.3 Organization Impact

Organization assignment affects:

- Which workflows the user can see and submit
- Which approval requests are routed to the user
- What data appears in reports
- Access to SBU-specific features

*[Screenshot: Organization Assignment Section]*

*Figure: Organization Assignment Section*

# 8. Password Management

## 8.1 Setting Initial Password

When creating a user, you can:

- Enter a specific password manually
- Generate a random password (if feature available)
- Enable 'Must Change Password' to force reset on first login

## 8.2 Admin Password Reset

### Steps:

**Step 1:** Locate the user in the User List

**Step 2:** Click 'Reset Password' action button

**Step 3:** Enter a new temporary password

**Step 4:** Check 'Must Change Password' (recommended)

**Step 5:** Click 'Reset' to confirm

**Step 6:** Communicate new password to user securely

### 8.3 Password Security Guidelines

- Never share passwords via email or chat
- Use secure channels to communicate initial passwords
- Enforce password complexity requirements
- Set password expiry policies
- Enable multi-factor authentication if available

**WARNING:** Users should change their password immediately after receiving it from an administrator.

## 9. Locking and Unlocking Users

### 9.1 Why Lock a User?

- Security concern or suspicious activity
- Employee termination or leave
- Temporary access restriction
- Policy violation
- Automatic lock after failed login attempts

### 9.2 Manually Locking a User

**Steps:**

**Step 1:** Locate the user in the User List

**Step 2:** Click the 'Lock' action button (padlock icon)

**Step 3:** Enter a lock reason (required for audit)

**Step 4:** Click 'Confirm' to lock the account

**Step 5:** User immediately loses access

### 9.3 Unlocking a User

**Steps:**

**Step 1:** Find the locked user (red badge indicator)

**Step 2:** Click the 'Unlock' action button

**Step 3:** Confirm the unlock action

**Step 4:** User can now log in again

**Step 5:** Consider resetting password if lock was security-related

## 9.4 Automatic vs Manual Lock

Lock Type	Cause	Resolution
Automatic	Too many failed login attempts	Wait for timeout or admin unlock
Manual	Administrator action	Admin must unlock

# 10. User Types

User Types categorize users by their relationship to the organization and typical access patterns.

## 10.1 User Type Definitions

User Type	Description	Typical Use
SYSTEM	System/service accounts	Automated processes, integrations
STAFF	Regular employees	Day-to-day workflow users
MANAGER	Management personnel	Approvers, team leads, supervisors
EXTERNAL	External parties	Vendors, contractors, partners

## 10.2 Selecting User Type

Choose the user type based on:

- User's relationship to the organization
- Level of access and trust
- Workflow participation role
- Reporting and audit requirements

# 11. Best Practices

## 11.1 User Creation Guidelines

- Use consistent username format (e.g., firstname.lastname)
- Verify email addresses for notification delivery
- Assign roles based on job function, not individual
- Document the purpose for external user accounts
- Enable 'Must Change Password' for new users

## 11.2 Access Control

- Follow principle of least privilege
- Review user access periodically (quarterly recommended)
- Remove access promptly when users leave
- Audit privileged account usage
- Maintain documentation of role assignments

## 11.3 Security Practices

- Lock accounts immediately upon termination
- Review failed login attempts regularly
- Investigate locked accounts for security issues
- Use strong password policies
- Keep user contact information current

## 11.4 Troubleshooting

Issue	Cause	Solution
User can't log in	Wrong password, locked, inactive	Reset password, unlock, activate
User can't see workflow	Missing role or org assignment	Assign appropriate role/organization
User can't approve	Not assigned as approver	Assign approver role, configure workflow
Duplicate user error	Username already exists	Use different username
Email not received	Invalid email or spam filter	Verify email, check spam folder