Role Management Module

User Manual - Console Interface

SONARWORKS WORKFLOW SYSTEM

Version 1.1

Table of Contents

1. Introduction

The Role Management module allows administrators to define and manage roles, which are collections of privileges (permissions) that control what users can do in the Sonar Workflow System. Effective role management is crucial for system security and proper access control.

Key Functions:

- Create custom roles for different job functions
- Define privilege sets for each role
- Manage system and custom roles
- Control access to features and data

NOTE: Only administrators can access Role Management.

[Screenshot: Role Management Overview]

Figure: Role Management Overview

2. Understanding Roles and Privileges

2.1 What is a Role?

A Role is a named collection of privileges that can be assigned to users. Roles represent job functions or access levels within the organization.

Example: Role Concept

Role: "Finance Approver"
Description: Approves financial workflow requests

Contains Privileges:
- View Workflows
- View Approvals
- Approve/Reject Workflows
- View Reports (Financial)

2.2 What is a Privilege?

A Privilege is a specific permission that allows a particular action in the system. Privileges are atomic units of access control.

Privilege Category	Example Privileges
Workflow	Create Workflow, Edit Workflow, Delete Workflow, Publish Workflow

Approval	View Approvals, Approve, Reject, Escalate
User Management	Create User, Edit User, Delete User, Reset Password
Administration	Manage Settings, View Audit Log, Manage Roles
Reports	View Reports, Export Reports, Create Reports

2.3 How Roles Work

1. Administrator creates roles with specific privileges
2. Roles are assigned to users
3. Users inherit all privileges from their assigned roles
4. Multiple roles can be assigned to one user
5. Privileges are additive (combined) across all roles

[Screenshot: Role and Privilege Relationship Diagram]

Figure: Role and Privilege Relationship Diagram

3. Accessing Role Management

Steps:

Step 1: Log in with administrator credentials

Step 2: Click 'Administration' in the navigation sidebar

Step 3: Click 'Roles' from the sub-menu

Step 4: The Role List page displays all available roles

[Screenshot: Navigation to Role Management]

Figure: Navigation to Role Management

4. Viewing Roles

4.1 Role List

Column	Description
Role Name	Display name of the role
Description	Brief explanation of the role's purpose
System Role	Indicator if this is a built-in system role
Users	Count of users assigned to this role
Privileges	Number of privileges assigned
Actions	Edit, Delete (custom roles only)

4.2 Viewing Role Details

Steps:

Step 1: Click on a role name in the list

Step 2: Or click the 'View' action button

Step 3: The Role Detail panel shows all assigned privileges

5. Creating New Roles

5.1 When to Create a New Role

- New job function needs specific access
- Existing roles are too broad or too restrictive
- Department-specific access is required
- Temporary project-based access is needed

5.2 Creating a Role

Steps:

Step 1: Click the '+ New Role' button

Step 2: Enter a Role Name (unique, descriptive)

Step 3: Enter a Description explaining the role's purpose

Step 4: Select privileges from the available list

Step 5: Click 'Save' to create the role

5.3 Role Form Fields

Field	Required	Description
Role Name	Yes	Unique identifier (e.g., 'Finance Reviewer')
Description	No	Explanation of role purpose and usage
Privileges	Yes	List of permissions to include in this role

[Screenshot: Create Role Form]

Figure: Create Role Form

5.4 Selecting Privileges

In the privilege selection area:

- Privileges are organized by category/module

- Check individual privileges to include them
- Use 'Select All' within a category for quick selection
- Search for specific privileges by name

Example: Creating a Custom Role

Role Name: "Department Head"
Description: "Review and approve department workflows"

Selected Privileges:
[x] View Workflows
[x] View Approvals
[x] Approve Workflow
[x] Reject Workflow
[x] View Department Reports
[ ] Create Workflow (not needed)
[ ] Manage Users (not needed)

6. Editing Roles

6.1 Editing Custom Roles

Steps:

Step 1: Locate the role in the Role List

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

Step 3: Modify the role name, description, or privileges

Step 4: Click 'Save' to apply changes

6.2 Impact of Role Changes

When you modify a role:

- All users with that role are affected
- Changes take effect immediately
- Users may need to log out and back in
- Audit log records the change

WARNING: Be careful when removing privileges from widely-used roles. Consider the impact on all affected users.

6.3 Deleting Roles

Steps:

Step 1: Locate the custom role in the list

Step 2: Click the 'Delete' action button (trash icon)

Step 3: Confirm the deletion

> **NOTE:** You cannot delete a role that has users assigned. Remove users from the role first.

> **NOTE:** System roles cannot be deleted.

7. Privilege Reference

7.1 Workflow Privileges

Privilege	Description
VIEW_WORKFLOWS	View workflow list and details
CREATE_WORKFLOW	Create new workflow definitions
EDIT_WORKFLOW	Modify existing workflows
DELETE_WORKFLOW	Remove workflow definitions
PUBLISH_WORKFLOW	Publish/unpublish workflows
SUBMIT_WORKFLOW	Submit workflow instances

7.2 Approval Privileges

Privilege	Description
VIEW_APPROVALS	See pending approval queue
APPROVE_WORKFLOW	Approve workflow instances
REJECT_WORKFLOW	Reject workflow instances
ESCALATE_WORKFLOW	Escalate to higher authority
REASSIGN_WORKFLOW	Reassign to different approver

7.3 User Management Privileges

Privilege	Description
VIEW_USERS	View user list and details
CREATE_USER	Create new user accounts
EDIT_USER	Modify user information
DELETE_USER	Remove user accounts
LOCK_USER	Lock/unlock user accounts
RESET_PASSWORD	Reset user passwords

7.4 Administration Privileges

Privilege	Description
MANAGE_ROLES	Create and edit roles
MANAGE_SETTINGS	Modify system settings
VIEW_AUDIT_LOG	Access audit trail
MANAGE_ORGANIZATION	Manage corporates, SBUs, branches

7.5 Report Privileges

Privilege	Description
VIEW_REPORTS	Access reports module
EXPORT_REPORTS	Export report data
CREATE_REPORTS	Create custom reports

8. System Roles

System roles are pre-defined roles that come with the system. They provide baseline access levels and cannot be deleted.

8.1 Default System Roles

Role	Purpose	Key Privileges
Super Administrator	Full system access	All privileges
Administrator	System administration	User, role, settings management
Workflow Administrator	Manage workflows	Create, edit, publish workflows
Approver	Process approvals	View and process approvals
Initiator	Submit workflows	Submit and track workflows
Viewer	Read-only access	View workflows and reports

8.2 Modifying System Roles

System roles may be:

- Viewed - See the privileges assigned
- Limited editing - Some systems allow adding privileges
- Cannot be deleted - They are protected

TIP: It's recommended to create custom roles rather than modifying system roles for specific needs.

9. Best Practices

9.1 Role Design Principles

- Create roles based on job functions, not individuals
- Follow principle of least privilege
- Use descriptive names that indicate purpose
- Document each role's intended use
- Keep roles focused - avoid too many privileges in one role

9.2 Role Naming Convention

Suggested naming patterns:

Pattern	Example	Use For
[Department] [Function]	Finance Approver	Department-specific access
[Level] [Area]	Senior Workflow Manager	Hierarchical access
[Project] [Role]	Project X Viewer	Temporary project access

9.3 Maintenance Recommendations

6. Review roles quarterly for relevance
7. Audit role assignments when employees change positions
8. Remove unused custom roles
9. Document changes to role privileges
10. Test role changes before wide deployment

9.4 Common Mistakes to Avoid

- Creating too many similar roles (consolidate instead)
- Assigning admin privileges unnecessarily
- Forgetting to remove privileges when scope changes
- Using roles for temporary access (use time-limited assignments)
- Not documenting custom role purposes