Authentication Module

User Manual - Console Interface

SONARWORKS WORKFLOW SYSTEM

Version 1.1

Table of Contents

1. Introduction

The Authentication Module is the gateway to the Sonar Workflow System. It provides secure access control to ensure only authorized users can access the system and its features. This module handles user login, password management, and session security.

Key Features:

- Secure username and password authentication
- JWT (JSON Web Token) based session management
- Self-service password reset via email
- Password change functionality
- Account lockout protection
- Session timeout for security

[Screenshot: Login Page Overview]

Figure: Login Page Overview

2. System Access Requirements

2.1 Browser Requirements

The Sonar Workflow System is a web-based application accessible through modern web browsers:

Browser	Minimum Version	Recommended
Google Chrome	90+	Latest
Mozilla Firefox	88+	Latest
Microsoft Edge	90+	Latest
Safari	14+	Latest

2.2 User Account Requirements

To access the system, you need:

- A valid username assigned by the system administrator
- An active password (not expired)
- An active account (not locked or disabled)
- Appropriate role and privileges assigned

NOTE: Contact your system administrator if you don't have login credentials or your account is locked.

3. Login Process

3.1 Accessing the Login Page

Open your web browser and navigate to the Sonar Workflow System URL provided by your organization. The login page will be displayed automatically.

[Screenshot: Login Page with Username and Password Fields]

Figure: Login Page with Username and Password Fields

3.2 Login Fields

Field	Description	Required
Username	Your unique system identifier (case-sensitive)	Yes
Password	Your secret authentication key	Yes
Remember Me	Keep session active for extended period	No

3.3 Step-by-Step Login Instructions

Steps:

Step 1: Open your web browser and navigate to the system URL

Step 2: Enter your username in the 'Username' field

Step 3: Enter your password in the 'Password' field

Step 4: Optionally, check 'Remember Me' to stay logged in longer

Step 5: Click the 'Login' button or press Enter

Step 6: Wait for authentication - you will be redirected to the Dashboard upon success

[Screenshot: Successful Login - Dashboard Redirect]

Figure: Successful Login - Dashboard Redirect

3.4 Login Errors

Error Message	Cause	Solution
Invalid credentials	Wrong username or password	Verify your credentials and try again
Account locked	Too many failed login attempts	Contact system administrator
Account disabled	Account deactivated by admin	Contact system administrator
Password expired	Password validity period exceeded	Use 'Forgot Password' to reset

Session expired	Previous session timed out	Log in again

Example: Successful Login Flow

1. User enters: admin / password123
2. System validates credentials
3. JWT token is generated
4. User is redirected to Dashboard
5. Navigation menu shows based on user roles

4. Forgot Password

If you forget your password, you can request a password reset link via email. This is a self-service feature that allows you to regain access without administrator intervention.

4.1 Accessing Forgot Password

Steps:

Step 1: On the Login page, click the 'Forgot Password?' link

Step 2: The Forgot Password form will be displayed

Step 3: Enter your registered email address

Step 4: Click 'Send Reset Link'

[Screenshot: Forgot Password Form]

Figure: Forgot Password Form

4.2 Forgot Password Fields

Field	Description	Validation
Email Address	Your registered email in the system	Must be a valid email format and registered in system

4.3 What Happens Next

1. System verifies the email exists in the database
2. A unique password reset token is generated (valid for 24 hours)
3. An email is sent with a secure reset link
4. You receive the email with instructions

TIP: If you don't receive the email within 5 minutes, check your spam folder or verify your email address is correct.

WARNING: The reset link expires after 24 hours for security reasons. Request a new link if needed.

5. Reset Password

After clicking the reset link in your email, you will be directed to the password reset page where you can set a new password.

5.1 Reset Password Form

Field	Description	Requirements
New Password	Your new password	Minimum 8 characters, must include uppercase, lowercase, number
Confirm Password	Re-enter new password	Must exactly match New Password

[Screenshot: Reset Password Form]

Figure: Reset Password Form

5.2 Password Requirements

Your new password must meet the following security requirements:

- Minimum 8 characters in length
- At least one uppercase letter (A-Z)
- At least one lowercase letter (a-z)
- At least one number (0-9)
- Optionally include special characters (!@#$%^&*)
- Cannot be the same as your last 3 passwords

5.3 Reset Process

Steps:

Step 1: Click the reset link in your email

Step 2: Enter your new password in the 'New Password' field

Step 3: Re-enter the password in the 'Confirm Password' field

Step 4: Click 'Reset Password'

Step 5: Upon success, you'll see a confirmation message

Step 6: Click 'Go to Login' to log in with your new password

6. Change Password

Once logged in, you can change your password at any time through your profile settings. Regular password changes are recommended for security.

6.1 Accessing Change Password

Steps:

Step 1: Log in to the system

Step 2: Click on your profile icon/name in the top-right corner

Step 3: Select 'Change Password' from the dropdown menu

Step 4: The Change Password dialog will appear

[Screenshot: Change Password Dialog]

Figure: Change Password Dialog

6.2 Change Password Fields

Field	Description	Required
Current Password	Your existing/current password	Yes
New Password	The new password you want to set	Yes
Confirm New Password	Re-enter the new password	Yes

6.3 Step-by-Step Instructions

Steps:

Step 1: Enter your current password to verify your identity

Step 2: Enter your new password (following password requirements)

Step 3: Confirm the new password by entering it again

Step 4: Click 'Change Password'

Step 5: A success message confirms the password change

Step 6: Your session remains active - no need to log in again

NOTE: If you're forced to change your password on first login, you cannot skip this step.

7. Session Management

7.1 Session Overview

The system uses JWT (JSON Web Token) based authentication to manage your session. This provides secure, stateless authentication across all system features.

7.2 Session Duration

Session Type	Duration	Description
Standard Session	8 hours	Default session length after login
Remember Me Session	7 days	Extended session when 'Remember Me' is checked
Idle Timeout	30 minutes	Session expires after 30 minutes of inactivity

7.3 Session Indicators

The system provides visual indicators of your session status:

- User icon in the top-right shows your username
- Session warning appears 5 minutes before expiry
- Automatic redirect to login page when session expires

7.4 Logging Out

Always log out properly when you're done using the system:

Steps:

Step 1: Click your profile icon/name in the top-right corner

Step 2: Select 'Logout' from the dropdown menu

Step 3: You will be redirected to the login page

Step 4: Your session token is invalidated for security

> **WARNING:** Always log out when using shared or public computers to protect your account.

8. Security Features

8.1 Account Lockout Protection

To protect against brute-force attacks, accounts are temporarily locked after multiple failed login attempts.

Security Feature	Setting	Description
Failed Login Threshold	5 attempts	Account locks after 5 failed attempts
Lockout Duration	30 minutes	Account automatically unlocks after 30 minutes
IP Tracking	Enabled	Failed attempts are logged with IP address

8.2 Password Security

- Passwords are encrypted using industry-standard hashing (bcrypt)
- Passwords are never stored in plain text
- Password history prevents reuse of recent passwords
- Reset tokens are single-use and time-limited

8.3 Audit Logging

All authentication events are logged for security auditing:

- Successful and failed login attempts
- Password changes and resets
- Session creation and termination
- IP address and browser information

9. Troubleshooting

9.1 Common Issues and Solutions

Issue	Possible Cause	Solution
Can't access login page	Network/URL issue	Verify URL, check internet connection
'Invalid credentials' error	Wrong username/password	Verify credentials, check caps lock
Account locked	Too many failed attempts	Wait 30 minutes or contact admin
Not receiving reset email	Wrong email or spam filter	Check spam folder, verify email address
Reset link doesn't work	Link expired or used	Request a new reset link
Session keeps expiring	Idle timeout	Stay active or check 'Remember Me'
Can't change password	Current password wrong	Verify current password is correct

9.2 Getting Help

If you continue to experience issues:

5. Note the exact error message displayed

6. Record the time the issue occurred
7. Take a screenshot if possible
8. Contact your system administrator with these details

9.3 Contact Information

For authentication issues, contact:

- System Administrator: [Your Admin Email]
- IT Help Desk: [Your Help Desk Number]
- Support Portal: [Your Support URL]