Audit Log Module

User Manual - Console Interface

SONARWORKS WORKFLOW SYSTEM

Version 1.1

Table of Contents

1. Introduction

The Audit Log module provides a comprehensive record of all significant actions performed in the Sonar Workflow System. It serves as an essential tool for security monitoring, compliance, troubleshooting, and accountability.

What is Audited:

- User authentication events (login, logout, failed attempts)
- Data changes (create, update, delete operations)
- Workflow actions (submissions, approvals, rejections)
- Administrative actions (user management, settings changes)
- Security events (password changes, account locks)
- System operations (imports, exports, backups)

NOTE: Audit logs are read-only and cannot be modified or deleted by users.

[Screenshot: Audit Log Overview]

Figure: Audit Log Overview

2. Accessing Audit Logs

Steps:

Step 1: Log in with administrator credentials

Step 2: Click 'Administration' in the navigation sidebar

Step 3: Click 'Audit Log' from the sub-menu

Step 4: The Audit Log list page displays

NOTE: Only users with VIEW_AUDIT_LOG privilege can access audit logs.

[Screenshot: Navigation to Audit Log]

Figure: Navigation to Audit Log

3. Understanding Audit Entries

3.1 Audit Entry Components

Field	Description	Example
Timestamp	Date and time of action	2024-01-15 14:30:25
User	Person who performed action	john.doe

Action	Type of action performed	UPDATE, LOGIN, APPROVE
Entity Type	Type of object affected	User, Workflow, WorkflowInstance
Entity ID	Identifier of affected object	uuid-123-456
Module	System module involved	USER_MANAGEMENT, WORKFLOW
Summary	Brief description	Updated user profile
IP Address	Client IP address	192.168.1.100
User Agent	Browser/client information	Chrome 120, Windows

[Screenshot: Audit Log Entry Example]

Figure: Audit Log Entry Example

3.2 Entity Types

Entity Type	Description
User	User account operations
Role	Role and privilege changes
Workflow	Workflow template changes
WorkflowInstance	Workflow submission operations
Corporate	Corporate entity changes
SBU	SBU changes
Branch	Branch changes
Department	Department changes
Setting	System setting modifications
System	System-level operations

3.3 Change Tracking

For update actions, the audit log tracks both old and new values:

Example: Change Tracking Example

Action: UPDATE
Entity: User (john.doe)
Changes:
- email: old="john@old.com" -> new="john@new.com"
- phone: old="555-0100" -> new="555-0200"

4. Searching and Filtering

4.1 Available Filters

Filter	Type	Description

Date Range	Date Picker	Start and end date for entries
User	Text/Select	Filter by specific user
Action	Multi-Select	Filter by action types
Entity Type	Multi-Select	Filter by entity types
Module	Multi-Select	Filter by system module
IP Address	Text	Filter by client IP
Search	Text	Full-text search in summary

4.2 Using Filters

Steps:

Step 1: Click 'Filters' button to open filter panel

Step 2: Set your filter criteria

Step 3: Click 'Apply' to filter results

Step 4: Results update to show matching entries

Step 5: Click 'Clear' to reset all filters

[Screenshot: Audit Log Filter Panel]

Figure: Audit Log Filter Panel

4.3 Quick Filter Examples

Goal	Filter Settings
All logins today	Date: Today, Action: LOGIN
Failed login attempts	Action: LOGIN_FAILED
User changes by admin	Entity: User, User: admin
Workflow approvals this week	Date: This Week, Action: APPROVE
Activity from specific IP	IP Address: 192.168.1.100

4.4 Sorting

Click column headers to sort:

- Default sort: Newest first (by timestamp)
- Click column header to change sort
- Click again to reverse order

5. Audit Actions Reference

5.1 Authentication Actions

Action	Description
LOGIN	Successful user login
LOGIN_FAILED	Failed login attempt
LOGOUT	User logged out
PASSWORD_CHANGE	User changed their password
PASSWORD_RESET	Password reset via admin or email

5.2 Data Actions

Action	Description
CREATE	New entity created
READ	Entity was viewed (if configured)
UPDATE	Entity was modified
DELETE	Entity was deleted

5.3 Workflow Actions

Action	Description
SUBMIT	Workflow submitted for approval
APPROVE	Workflow approved
REJECT	Workflow rejected
ESCALATE	Workflow escalated
RECALL	Workflow recalled by initiator
CANCEL	Workflow cancelled

5.4 Administrative Actions

Action	Description
LOCK	User account locked
UNLOCK	User account unlocked
IMPORT	Data import operation
EXPORT	Data export operation
BACKUP	System backup created
RESTORE	System restore performed
SYSTEM_LOCK	System-wide lock activated
SYSTEM_UNLOCK	System-wide lock deactivated

6. Viewing Audit Details

6.1 Opening Entry Details

Steps:

Step 1: Locate the entry in the audit log list

Step 2: Click on the row or the 'View' button

Step 3: The Audit Detail dialog/page opens

6.2 Detail View Contents

Section	Information
Header	Action type, timestamp, result (success/failure)
Actor	User who performed the action, their roles
Target	Entity type, ID, and name of affected object
Changes	Old vs New values for update actions
Context	IP address, user agent, session ID
Related	Links to related entities if applicable

[Screenshot: Audit Detail View]

Figure: Audit Detail View

6.3 Navigating to Related Entities

From the audit detail view, you can often navigate to:

- The user who performed the action
- The affected entity (if it still exists)
- Related workflow instance (for approval actions)

7. Exporting Audit Data

7.1 Export Options

Format	Description	Best For
CSV	Comma-separated values	Spreadsheet analysis, data processing
Excel	Microsoft Excel format	Reporting, sharing with stakeholders
PDF	Portable Document Format	Formal reports, archival

7.2 Exporting Data

Steps:

Step 1: Apply filters to select the data range

Step 2: Click the 'Export' button

Step 3: Select the export format

Step 4: Choose columns to include (optional)

Step 5: Click 'Download'

Step 6: File is downloaded to your computer

7.3 Export Best Practices

- Filter data before export to reduce file size
- Include date range in export filename
- Secure exported files (they contain sensitive data)
- Delete exports after use if not needed for retention

> **WARNING:** Exported audit data should be handled according to your organization's data security policies.

8. Compliance and Retention

8.1 Audit Log Retention

Audit logs are retained according to system configuration:

Setting	Typical Value	Description
Retention Period	7 years	How long logs are kept
Archive Policy	After 1 year	When logs move to archive
Deletion Policy	Never (manual)	When logs are purged

8.2 Compliance Considerations

The audit log supports compliance with:

- SOX (Sarbanes-Oxley) - Financial controls
- GDPR - Data access tracking
- HIPAA - Healthcare data access
- ISO 27001 - Information security
- Internal audit requirements

8.3 Audit Log Integrity

To ensure integrity:

- Logs cannot be modified after creation
- Logs cannot be deleted by regular users
- All log entries have unique identifiers
- Timestamps are system-generated and tamper-proof

9. Best Practices

9.1 Regular Review

- Review audit logs weekly for unusual activity
- Check failed logins for potential attacks
- Monitor administrative actions
- Investigate unexpected data changes

9.2 Security Monitoring

Key patterns to watch for:

Pattern	Concern	Action
Multiple failed logins	Brute force attack	Verify account, check IP
Unusual login times	Compromised account	Verify with user
Mass data export	Data theft attempt	Review and verify
Admin actions by non-admin	Privilege escalation	Investigate immediately
Actions from unusual IP	Account compromise	Verify, consider lock

9.3 Investigation Process

1. Identify the suspicious activity in audit log
2. Note the timestamp, user, and action
3. Filter for all related actions by that user/IP
4. Determine if activity is legitimate
5. Take appropriate action (lock account, alert security)
6. Document your investigation

9.4 Reporting

- Create regular audit summary reports
- Report security incidents promptly
- Archive reports for compliance
- Include audit review in security procedures