# Admin Logs Documentation

### Overview

The Admin Logs system is a comprehensive audit trail mechanism that tracks and records all administrative actions performed within the Sundaram Portal. It provides detailed insights into who made changes, what changes were made, when they occurred, and from where they originated.

### Purpose

- Maintain accountability for administrative actions
- Track system changes over time
- Provide audit trails for compliance purposes
- Enable troubleshooting of configuration changes
- Support system security through activity monitoring

### Key Features

### 1. Action Tracking Categories

The system tracks several types of administrative actions:

- User Management
- Group Management
- Column Permissions
- Validation Configurations
- Dropdown Management
- Column Renaming
- Table Configuration

### 2. Tracked Information

For each administrative action, the system records:

- Action Type (CREATE, UPDATE, DELETE)
- Section/Category of the action
- Admin user details (email, name)
- IP address of the admin

- Timestamp of the action
- Target table/entity affected
- Detailed before/after states
- Success/failure status
- Additional context-specific information

**3. Filtering and Search Capabilities**

Users can filter and search logs using:

- Date range selection
- Section/category filters
- Action type filters
- Text-based search
- Advanced filters for:
    - Group names
    - Table names
    - Column names
    - Action types

**Detailed Section Breakdown**

**1. User Management Logs**

Tracks changes related to user accounts:

- User creation
- Role modifications
- Account activation/deactivation
- Profile updates
- Password changes

**2. Group Management Logs**

Records changes to table groupings:

- Group creation
- Adding/removing tables from groups

- Group activation/deactivation
- Group deletion
- Table reassignment between groups

**3. Column Permission Logs**

Monitors changes to column-level permissions:

- Setting columns as editable/non-editable
- Bulk permission updates
- Permission scheme modifications
- Column access control changes

**4. Validation Configuration Logs**

Tracks changes to data validation rules:

- Data type restrictions
- Value range limits
- Format requirements
- Custom validation rules
- Validation rule activation/deactivation

**5. Dropdown Management Logs**

Records changes to dropdown configurations:

- Regular dropdown options
- Dependent dropdown relationships
- Option additions/removals
- Parent-child relationship changes
- Dropdown value modifications

**6. Column Rename Logs**

Tracks column display name changes:

- Original column name
- New display names

- Affected tables
- Rename history

**7. Table Configuration Logs**

Monitors table-level configuration changes:

- Display name modifications
- Description updates
- Table metadata changes
- Configuration activation/deactivation

## User Guide

### Accessing Admin Logs

1. Navigate to the Admin section
2. Select the "Admin Logs" option
3. View the comprehensive log listing

### Using Filters

1. Date Range Filter
   - Select start and end dates
   - View actions within specific timeframes

2. Section Filters
   - Click section tabs to filter by category
   - View all sections or specific ones

3. Advanced Filters
   - Use the "Advanced Filters" button
   - Filter by specific criteria:
     - Action types
     - Group names
     - Table names

  - Column names

4. Search Functionality
   - Use the search bar for text-based searches
   - Search across multiple fields
   - Find specific actions or changes

**Viewing Log Details**

1. Click "See Details" for comprehensive information
2. Review:
   - Action summary
   - Before/after states
   - Technical details
   - Related changes
   - Context-specific information

**Understanding Log Entries**

1. Action Type Indicators
   - Green: Creation actions
   - Blue: Update actions
   - Red: Deletion actions

2. Status Information
   - Completed actions
   - Failed actions
   - Pending changes

3. Change Details
   - What was modified
   - Previous values
   - New values

- Related impacts

**Best Practices**

1. Regular Review

- Schedule periodic log reviews
- Monitor critical changes
- Track unusual activities
- Maintain system security

2. Documentation

- Note significant changes
- Document reason for changes
- Maintain change history
- Track impact of changes

3. Troubleshooting

- Use logs for issue investigation
- Track change patterns
- Identify problem sources
- Verify configuration changes

**Security Considerations**

1. Access Control

- Limited to administrative users
- Role-based access control
- Secure log viewing
- Protected sensitive information

2. Data Protection

- Encrypted sensitive data
- Protected user information

- Secure transmission

- Controlled access