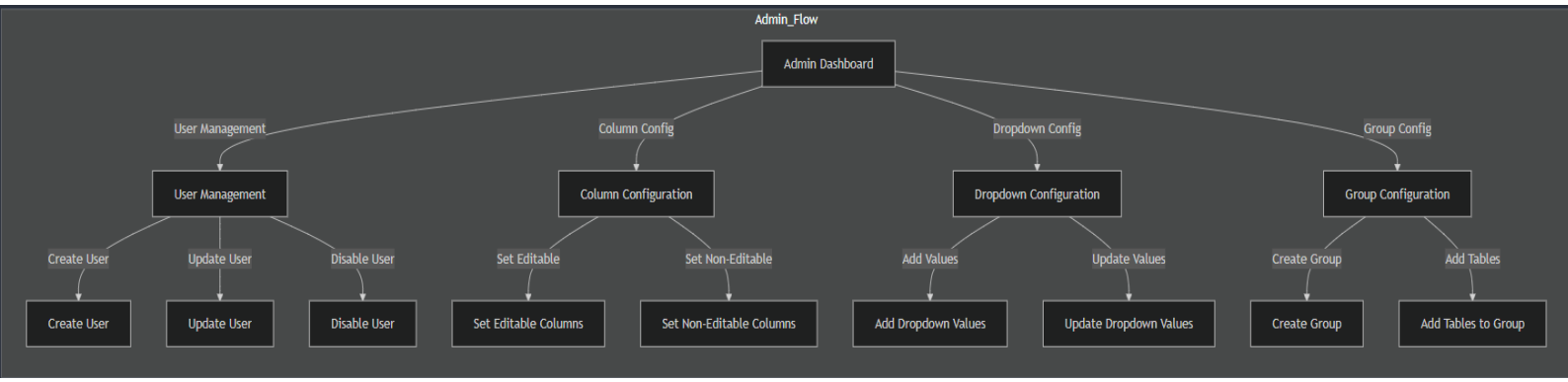
Sundaram Portal – Admin Doc



1. Overview

The Admin role in Sundaram Portal is the highest level of access, responsible for system configuration, user management, and maintaining data integrity. Admins have full control over the portal's configuration while maintaining audit trails for all changes.

Key Responsibilities

- User account management
- System configuration
- Permission management
- Data integrity maintenance
- Audit trail monitoring

2. Core Features

2.1 User Management

User Creation

- Create new users with specific roles (maker, checker, admin)
- Assign initial permissions
- Set up email notifications
- Generate temporary passwords

User Maintenance

- Update user details
- Enable/disable accounts

- Reset passwords
- Monitor user activity

Activity Monitoring

- View user login history
- Track data modifications
- Monitor permission changes
- Review audit logs

2.2 Column Permission Management

Permission Configuration

- Set column-level access controls
- Configure editable/non-editable status
- Manage data validation rules
- Set up field dependencies

Permission Types

- Read-only access
- Edit access
- Hidden fields
- Required fields

2.3 Table Management

Table Configuration

- Create/modify table structures
- Set up relationships
- Configure validation rules
- Manage table metadata

Group Management

- Create table groups

- Assign tables to groups
- Set group-level permissions
- Manage group hierarchies

3. Workflows

3.1 User Creation Workflow

1. Initiation

- Admin accesses user management interface
- Selects "Create New User"

2. User Details Entry

- Enters basic information
- Selects user role
- Sets initial permissions

3. Account Activation

- System generates temporary password
- Sends email notification
- Sets up initial access restrictions

4. First Login Process

- User receives credentials
- Forces password change
- Sets up security preferences

3.2 Permission Management Workflow

1. Access Control Setup

- Select target table/group
- Review current permissions
- Plan permission changes

2. Implementation

- Apply permission changes
- Set validation rules
- Configure dependencies

3. Verification

- Test new permissions
- Verify access levels
- Document changes

4. Security Considerations

4.1 Access Control

- Role-based access control (RBAC)
- Principle of least privilege
- Regular permission audits
- Session management

4.2 Data Protection

- Encryption at rest
- Secure transmission
- Audit logging
- Backup procedures

4.3 Compliance

- Data privacy regulations
- Industry standards
- Internal policies
- Audit requirements

5. Best Practices

5.1 User Management

- Regular account reviews
- Strong password policies
- Clear role definitions
- Proper documentation

5.2 Permission Management

- Regular permission audits
- Clear permission hierarchy
- Documented changes
- Testing procedures