



FinLedger

User Manual

Financial management system

Generated: 2026-02-12 21:32:48 UTC



Contents

- [1. Manual Framework](#)
- [2. Overview and Roles](#)
- [3. Login and Security](#)
- [4. User Administration](#)
- [5. Navigation and UI](#)

FinLedger User Manual

This manual describes how to use the FinLedger web application. Each section lives in its own folder so it can be authored independently and later compiled into a single PDF.

Structure

- Each section has its own folder under docs/User Manual/.
- Each section should include a README.md with the actual content.
- Use todo.md while a section is in progress; remove it after the section is complete.
- Section folders are numbered to preserve the final document order.
- Shared writing standards are in docs/User Manual/STYLE_GUIDE.md.
- Section drafting template is in docs/User Manual/templates/SECTION_TEMPLATE.md.
- Screenshot and figure standards are in docs/User Manual/assets/README.md.

Section Order

1. docs/User Manual/01Overviewand_Roles/README.md
2. docs/User Manual/02Loginand_Security/README.md
3. docs/User Manual/03UserAdministration/README.md
4. docs/User Manual/04Navigationand_UI/README.md
5. docs/User Manual/05Chartof_Accounts/README.md
6. docs/User Manual/06JournalEntries/README.md
7. docs/User Manual/07_Ledger/README.md
8. docs/User Manual/08AdjustingEntries/README.md
9. docs/User Manual/09FinancialReports/README.md
- 10.docs/User Manual/10Dashboardsand_Ratios/README.md
- 11.docs/User Manual/11Documentsand_Attachments/README.md
- 12.docs/User Manual/12Notificationsand_Email/README.md
- 13.docs/User Manual/13AuditandEventLogs/README.md

PDF Generation

- Generate the PDF with the project script:

```
npm run manual:pdf
```

- Default output path: docs/User Manual/FinLedgerUserManual.pdf
- Optional custom output path:

```
node scripts/build-user-manual-pdf.js --out "docs/User Manual/  
FinLedger_User_Manual_custom.pdf"
```

- The generator includes: - docs/User Manual/README.md - Any numbered section folder that

contains README.md

- Numbered folders without README.md are skipped with a warning.



Overview and Roles

System Overview

FinLedger is a web-based financial management system that supports core accounting workflows, including user administration, chart of accounts, journal entries, ledger review, adjusting entries, and financial reporting. The application is organized into modules that align with the sprint feature lists and is accessed through a single-page web interface.

UI Landmarks

Use these landmarks when navigating the application or referencing UI elements:

- **Header and branding:** The top-left header area shows the FinLedger logo, application name, and a logged-in user banner. The banner reads “You are logged in as ...” when authenticated.
- **Main navigation:** The top navigation bar includes Dashboard, Accounts, Transactions, Reports, Help, and a Login/Logout link depending on session state.
- **Profile menu:** The top-right profile button shows the current user name and avatar. It opens a small menu with Go to profile and Logout.
- **Calendar popup:** A calendar icon in the header opens a pop-up calendar for quick date reference.
- **Main content area:** Page content loads into the central area below the header. This is where module screens (Dashboard, Chart of Accounts, Ledger, Reports, etc.) appear.
- **Loading overlay:** A full-page loading overlay appears during page loads or long actions.

Role Summary

FinLedger supports three roles. The UI exposes or hides controls based on the user’s role.

- **Administrator:** Manages users (create, update, approve/reject registrations, suspend/reinstate, reset passwords) and manages the Chart of Accounts (add/edit/deactivate accounts, manage categories and subcategories). Administrators also access user and system reports and can email users from within the application.
- **Manager:** Creates and approves journal entries, reviews pending approvals, and runs financial reports (trial balance, income statement, balance sheet, retained earnings). Managers can also view ledgers and account event logs.
- **Accountant:** Prepares journal entries and adjusting entries, attaches source documents, and tracks approval status. Accountants can view ledgers and account details but do not approve entries.

Module Map (High Level)

- **Dashboard:** Landing page that summarizes key metrics, alerts, and role-specific information.
- **Accounts:** Chart of Accounts management and navigation to ledgers.
- **Transactions:** Ledger and journal entry access.
-

Reports: Financial reporting (trial balance, income statement, balance sheet, retained earnings).

- Help: In-app help content organized by topic.
- Profile: User profile management, password changes, and security questions.

For login details and security rules, see [docs/User Manual/02LoginandSecurity/README.md](#). For user administration tasks, see [docs/User Manual/03User_Administration/README.md](#).



Login and Security

This section explains how users sign in, manage passwords, recover access, and how FinLedger enforces session and password security.

Login Screen

The login screen is available from the top navigation link Login.

The sign-in form includes:

- Username
- Password
- Log In
- New User
- Forgot Password

After successful sign-in:

- The header shows You are logged in as
- The top-right profile control shows your display name and profile image.
- The navigation link changes from Login to Logout.

Sign-In Process

1. Open the Login page.
2. Enter your username and password.
3. Select Log In.

On success, FinLedger creates a signed session token and redirects to the dashboard.

If credentials are invalid, the page shows a login failure message.

Session and Access Control

FinLedger uses authenticated requests for protected pages and APIs.

- Protected requests include Authorization: Bearer <token> and X-User-Id headers.
- Session expiration is tracked server-side and extended while users remain active.
- If a session is missing or expired, protected routes return an authentication error and the UI redirects to sign-in.

Logout

Users can sign out in either of these ways:

- Select Logout in the top navigation.
- Open the profile menu and select Logout.

Logout invalidates the active server session and clears local session data in the browser.

Password Rules

Password validation is enforced during password changes and resets.

Current enforcement requires:

- Minimum length of 8 characters.
- At least one uppercase letter.
- At least one lowercase letter.
- At least one number.
- At least one special character.

Password reuse protection is enabled.

- New passwords cannot match previously used passwords stored in password history.

Failed Login Attempts and Suspension

FinLedger tracks failed login attempts.

- After 3 failed attempts, login is blocked for that user.
- The user receives an account suspended message and must contact an administrator.
- On successful login, failed-attempt counters are reset.

Forgot Password Flow

Use Forgot Password when you cannot log in.

1. Open Forgot Password from the login page.
2. Enter your email and user ID.
3. Select Reset Password.
4. Check your email for the reset link.
5. Open the link and answer your three security questions.
6. Enter and confirm a new password.
7. Submit to complete reset.

Important behavior:

- Reset tokens expire.
-

Security answers must match what is stored for the account.

- Password complexity and password-history rules still apply.

Temporary Password and Forced Change

Some accounts are issued temporary passwords.

When logging in with a temporary password:

- The user is redirected to the Change Password screen.
- Most routes are blocked until password change is completed.
- The user must set three security questions and answers, then set a new password.

After successful completion:

- Temporary password mode is cleared.
- The user can access normal application pages.

Password Expiration and Warnings

FinLedger enforces password expiration.

- Standard passwords are set to expire after 90 days.
- Warning emails are sent in the 3-day window before expiration.
- Expired-password accounts can be suspended automatically by background jobs.

Security Storage and Encryption

FinLedger stores security credentials in hashed form.

- Passwords are hashed before storage.
- Security answers are hashed before storage.
- Password history hashes are stored to enforce reuse restrictions.
- Reset links use time-limited reset tokens.

Common Security Messages

Users may see these messages during authentication flows:

- Invalid username or password
- Account is suspended due to multiple failed login attempts
- Invalid or expired reset token
- Security answers verification failed
- TEMPPASSWORDCHANGE_REQUIRED

If access remains blocked after valid inputs, contact an administrator.

User Administration

This section documents administrator-only user management features in FinLedger.

Access and Scope

User administration is available from Dashboard for users with the administrator role.

Manager and accountant users do not see the admin user-management cards and cannot call admin user-management APIs.

Admin Workspace (Dashboard)

On the dashboard, the User Management area includes:

- User Approvals
- Users with Expired Passwords
- Suspended Users
- Currently Logged-in Users
- All Users table
- Create User
- Delete User
- Reset User Password
- Suspend User Account
- Email User

Registration Request Workflow

New users can request access from the login page using New User.

Registration behavior:

1. The requester submits profile details, role, password, and security questions.
2. FinLedger creates the account with pending status.
3. The requester receives a registration confirmation email.
4. An administrator reviews the request in User Approvals.
5. The admin selects Approve or Reject.

Approval behavior:

- Status is updated to active.
- An approval email is sent to the user.

Rejection behavior:

- Status is updated to rejected.

Create User (Administrator)

Use the Create User form to create accounts directly.

Fields in the form:

- First Name
- Last Name
- Address
- Date of Birth
- Email
- Role (administrator, manager, accountant)
- Profile Image

Implementation notes:

- Username is generated automatically from first initial + last name + month/year stamp.
- If no password is provided by the flow, a temporary password is generated by the system.
- New accounts are created in pending status and then approved in User Approvals.
- Profile images are limited to common image file types and size limits enforced by upload middleware.

View and Edit Users

The All Users table provides a report of users and supports inline editing.

Table capabilities:

- Pagination (5, 10, 25, 50, 100 per page)
- Editable fields from the table cells
- Updates to fields such as name, role, status, dates, email, and address

Use this table to maintain role changes and status changes as part of user lifecycle operations.

Suspend and Reinstate Users

Manual suspension:

1. Open Suspend User Account.
2. Select an eligible active user.
3. Enter suspension start and end date/time.
- 4.

Submit the form.

Reinstatement:

- In Suspended Users, select Reinstatement.

Additional behavior:

- Expired suspension windows are automatically unsuspended by background jobs.
- Suspensions can also occur from security policy events (for example failed login limits or expired passwords).

Delete User

Use Delete User to permanently remove an account.

Behavior:

- Admin selects a username.
- Confirmation prompt appears before deletion.
- The UI prevents an admin from deleting their own account.

Reset User Password

Use Reset User Password when a user cannot access their account.

Behavior:

1. Select the username.
2. Submit reset.
3. System generates a temporary password.
4. Temporary password is emailed to the user.

Security behavior after reset:

- Account is marked as temporary-password mode.
- Temporary passwords use a short expiry window.
- User must complete forced password change and security-question setup at next login.

Email User

Use Email User to send direct messages from inside the system.

Required fields:

- Recipient username
- Subject
-

Message

This is useful for approval follow-ups, suspension notices, and operational communication.

Logged-In Users and Expired Password Reporting

Currently Logged-in Users card:

- Shows active sessions visible to administrators.

Users with Expired Passwords card:

- Highlights users with expired passwords.
- Works with password-expiration automation that sends warnings and can suspend expired accounts.

Operational Notes

- Most user-administration actions are API-enforced as admin-only, even if a user attempts direct calls.
- For password policy details and self-service recovery, see [docs/User Manual/02Loginand_Security/README.md](#).

Navigation and UI

This section explains how users move through FinLedger and what UI patterns are used consistently across pages.

Navigation Model

FinLedger uses a single-page application (SPA) pattern.

- The page frame (header and navigation) stays on screen.
- Main content is loaded into the center content area.
- URL hash routes control which page appears (for example `#/dashboard`).

Default route:

- If no route is provided, FinLedger loads Dashboard.

Header Layout

The global header includes:

- FinLedger logo and product name
- Logged-in user label (You are logged in as ...)
- Calendar icon (opens pop-up calendar)
- Main navigation links
- Profile button with user name and avatar

Logo behavior:

- Selecting the logo returns the user to Dashboard.

Main Navigation

Primary navigation links:

- Dashboard
- Accounts
- Transactions
- Reports
- Help
- Login or Logout (depends on session state)

Active-page behavior:

-

The current route is highlighted in the navigation bar.

- Browser title updates to FinLedger - <Page Name>.

Route Access and Redirect Behavior

Common route outcomes:

- Valid route: requested page loads into the main content area.
- Unknown route: user is shown the Not Found page.
- Not logged in or expired session: user is redirected to Not Logged In or Login depending on context.
- Insufficient permission: user is redirected to Not Authorized.
- Temporary password required: user is redirected to Change Password.

Profile Menu

The top-right profile control opens a menu with:

- Go to profile
- Logout

Interaction behavior:

- Opens on hover/focus.
- Closes on mouse leave, route change, or Esc.

Help and Tooltips

Help:

- Help is a top-level navigation item.
- The Help page is organized as expandable accordion topics.
- Topics cover account access, profile/security, admin tools, reports, and support.

Tooltips:

- Many interactive controls use hover text (title) for quick guidance.
- Examples include page actions, table controls, and form inputs.

Calendar Widget

The header calendar icon opens a pop-up calendar.

Calendar controls:

- Previous month
-

Today

- Next month
- Month dropdown
- Year dropdown

Display behavior:

- Shows a month grid with the current day highlighted.
- Closes when clicking outside the calendar popup.

Loading and Page Transition Behavior

FinLedger uses a global loading overlay for page changes and long-running actions.

Behavior:

- Overlay appears during route/page loads.
- Overlay hides after content finishes loading.
- A short minimum display time is applied to prevent flashing.

Layout Consistency Standards

UI consistency expectations across pages:

- Shared header/navigation frame
- Consistent page title and subtitle pattern
- Reusable card, table, form, and button styles
- Consistent placement for notices and status feedback
- Unified role-aware navigation behavior

These patterns support predictable navigation and reduce training time for end users.