Login Project

This project is a complete web platform for user, account, and data management, focused on security, role-based access control (RBAC), and a clean and sustainable software architecture.

Front-end Repository: https://github.com/felipebabel/login
Back-End Repository: https://github.com/felipebabel/login-backend

1. Architecture and Technology

The project adopts a Clean Architecture with a focus on **Hexagonal Architecture** (Ports and Adapters) in the back-end.

Architecture:

> **Hexagonal (Ports and Adapters):** Clean code is prioritized, with interfaces and separation of responsibilities to ensure that domain logic is independent of technical details (such as database or frameworks). The design focuses on Ports (interfaces) and Adapters (implementations) to isolate business rules.

Security:

> **Authentication/Authorization:** Uses JSON Web Tokens (JWT) for access control. The system implements JWT and Refresh Token (valid for 24 hours), ensuring that when the JWT expires, a new one is requested by the user.

> **Encryption:** Passwords are securely stored using **Bcrypt** for encryption and verification.

> **Access Control (RBAC):** Endpoints are protected by specific roles, ensuring that each user can only perform actions allowed by their access level.

Swagger Documentation:

> All API endpoints have interactive documentation via Swagger, facilitating development and maintenance.

Scheduler (Scheduled Tasks):

A task scheduler executes daily routines at 6 AM for system maintenance:

> **Log Cleanup:** Deletes logs older than 180 days.

> **Account Inactivation:** Accounts without access in the last 30 days are inactivated.

> **Token Cleanup:** Deletes expired 6-digit password reset tokens.

Notes

The back-end is deployed on the **Render** platform. Due to the hosting plan, if the service is in idle mode, the first request may take approximately **one minute** to be processed until the server is reactivated (cold start).

The sending of emails for account activation and password recovery is handled through **Brevo** (formerly Sendinblue). The service operates under the free plan, with a limit of **300 emails per day**.

2. User Roles

The platform supports three access levels, each with specific permissions:

ADMIN: Full access to the Administrative Dashboard and settings.

ANALYST: Read-only access to the Dashboard, with restricted permissions, including the option to access their own profile.

USER: Access to their own profile and account activity logs.

3. Admin Dashboard Features

The main Dashboard has 4 tabs, offering granular system control:

3.1 Account Management
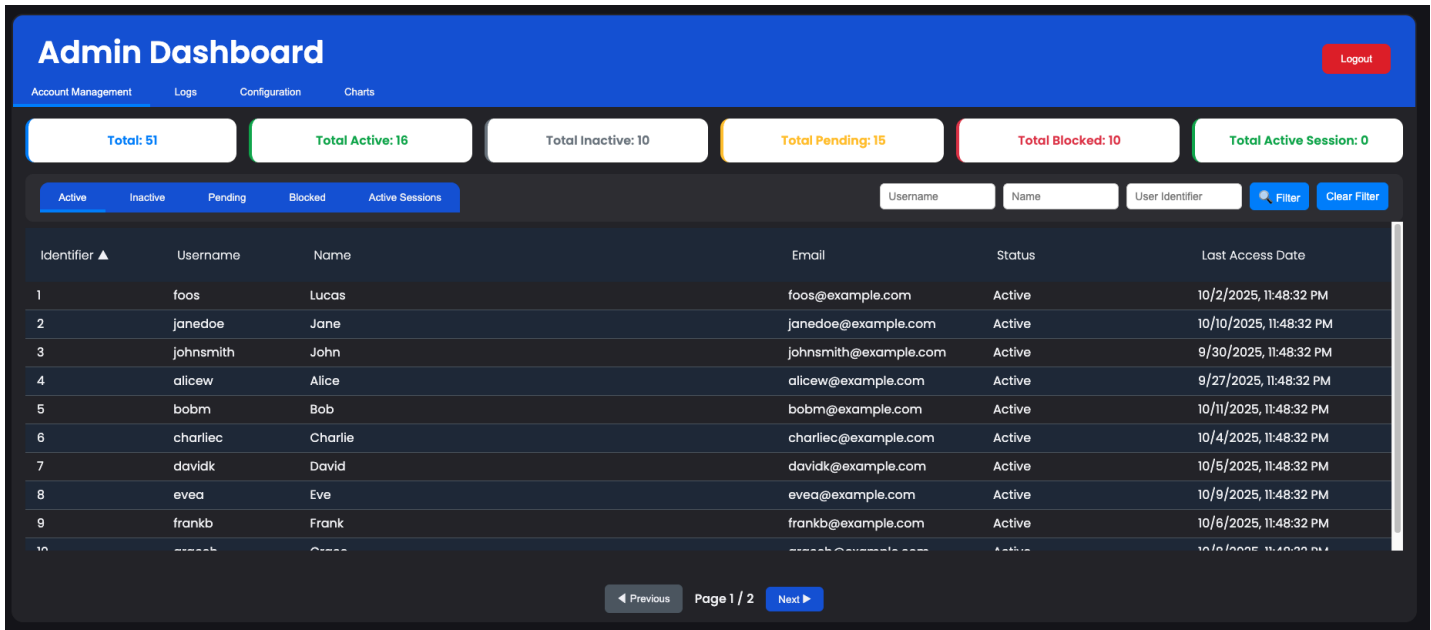
Displays total accounts (Active, Inactive, Pending, Blocked, Active Sessions).

Has 5 sub-tabs for individual list viewing and management.

- **Active**: Filter for active accounts.
- **Inactive:** Filter for inactive accounts; an account can become inactive via the ADMIN dashboard or after 30 days of inactivity.
- **Pending:** Filter for pending accounts; a pending account is one that has not yet activated the account via the email token.

- **Blocked:** Filter for blocked accounts.
- **Active Sessions:** Filter for active users; an active user is someone who performed any account action in the last 10 minutes.
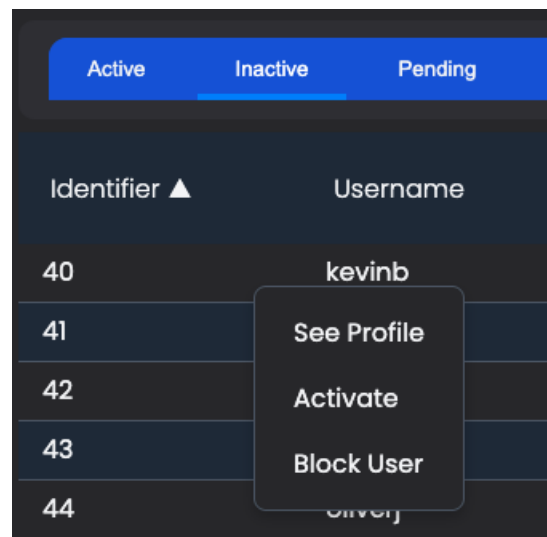
Sub-tabs include pagination (10 records) and ASC/DESC sorting. There is a search option by Username, Name, or User Identifier.

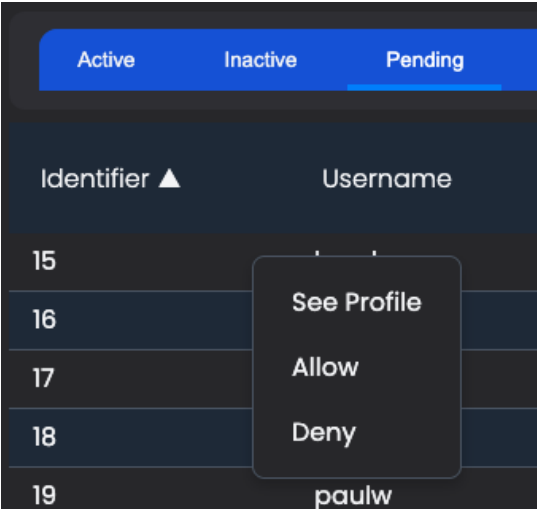Right-clicking on a record in the sub-tabs shows options:

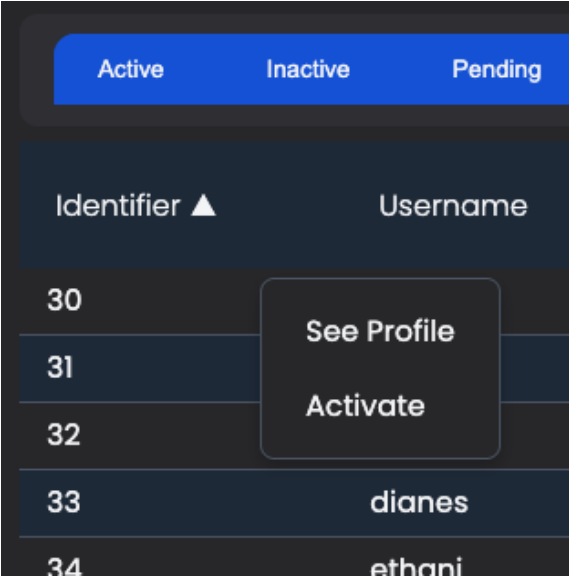**Active Tab:** Option to Inactivate, Block, Grant Analyst Privilege, and Force Password Change.
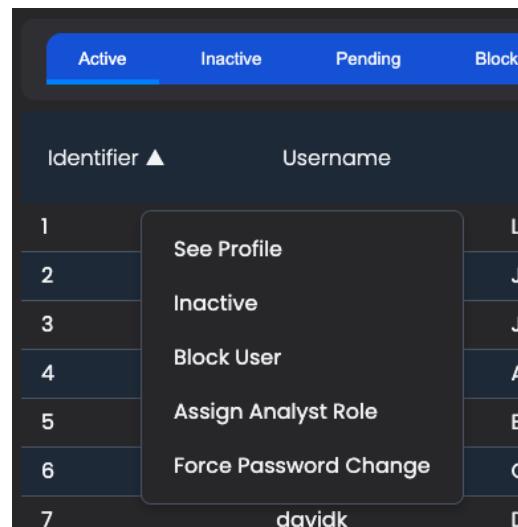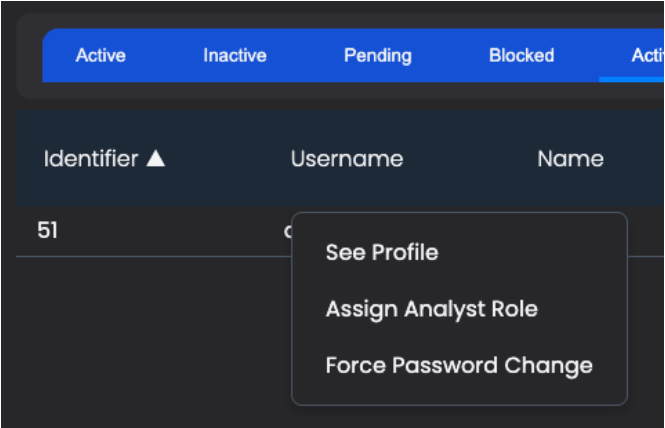

Inactive Tab: Option to Activate or Block account.

Pending Tab: Option to Approve or Decline account (deletes the record).

Blocked: Option to Activate account.

Active Session: Option to Grant Analyst Privilege and Force Password Change.

Note: The "See Profile" option to view all detailed information of an account is available in all sub-tabs.

3.2 Logs

View activity logs of all accounts. Filters: By Username and User Identifier. General: Pagination (10 records) and sorting.
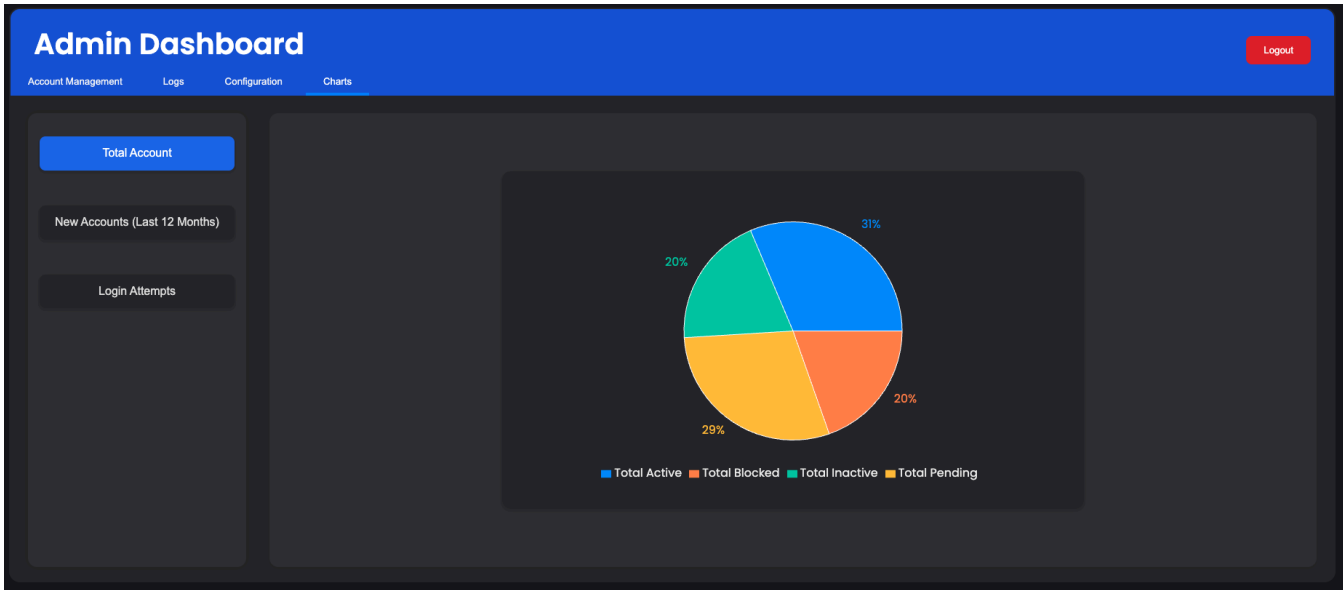
3.3 Configuration

Allows modifying global settings:

- Password Expiration (default 90 days).
- JWT Token Expiration in minutes (Refresh Token is fixed at 24h).
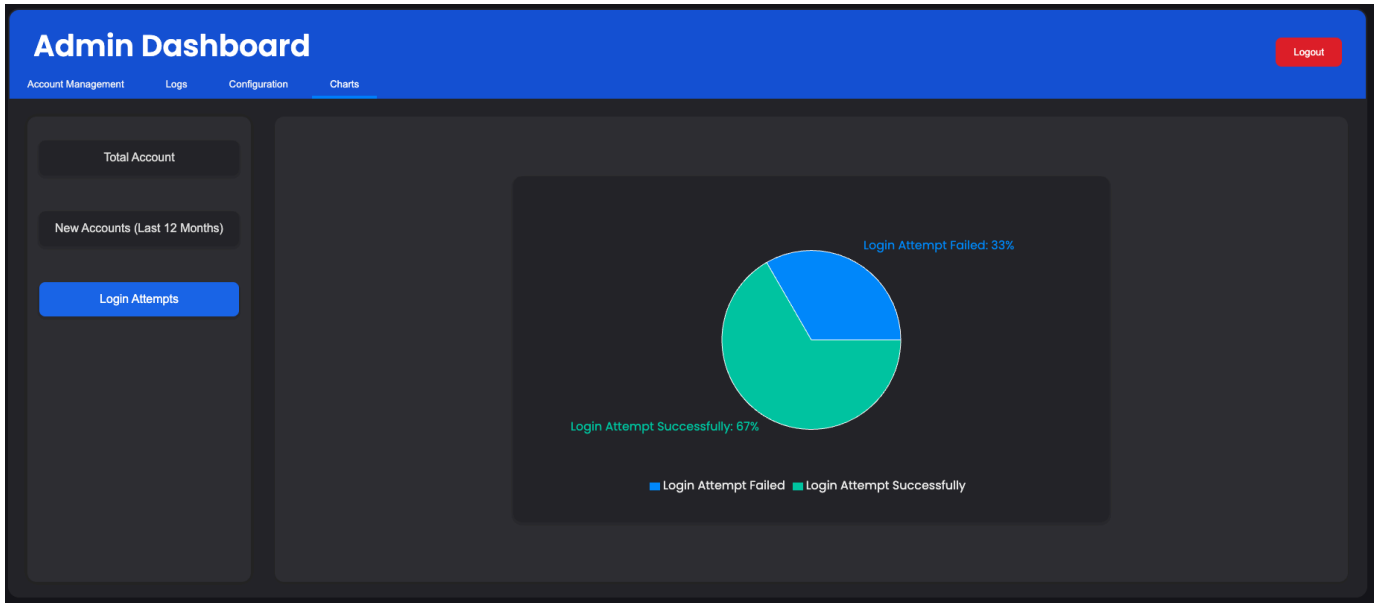
3.4 Charts

Displays 3 types of analytical charts:

● Pie Chart: Total accounts (Active, Inactive, Pending, Blocked, Active Sessions).

● Bar Chart: New accounts in the last 12 months.

● Pie Chart: Successful Login vs. Failed Login ratio.

4. Analyst Dashboard Features

The Analyst has a dashboard similar to the admin but with read-only permissions: the only action available in the Account Management tab is "See My Profile," and the Configuration tab is view-only. The Analyst Dashboard includes an additional feature: a button that directs them to their own user profile, accessing User Dashboard functionalities.
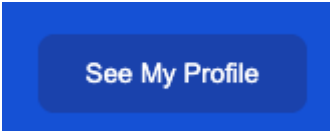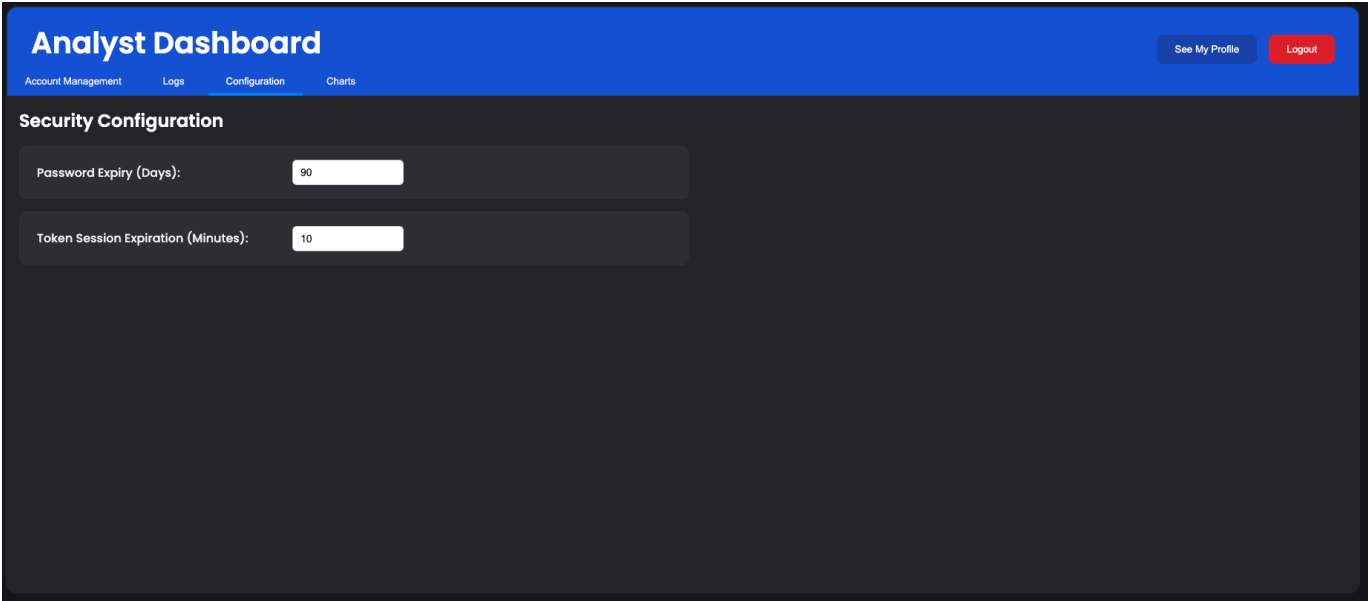
5. User Dashboard Features

Standard users have access to a personal dashboard focused on their account and security:

Tab	Features
Account Management	View: All profile data (username, name, phone, address, etc.). Edit: Can update most fields except "User Created On" and "Email". Username: Can be changed, subject to uniqueness validation.
Security Settings	Change Password: Form to update password (New Password and Confirmation) Delete Account: Irreversible action to delete the account.
Activity Log	View own account activity, with pagination and sorting.

Hello, User!

Account Management | Security Settings | Activity Log

Logout

Username
user

Name
User

User Created On
10/12/2025

Phone
+55 (99) 99999-9999

Gender
Male ▼

Birth Date
01/01/2000

City
City

State
SC

Address
My address

Address Complement
Complement

ZIP Code
999999

Email
dsadas@gmail.com

Country
Brazil ▼

Language
English ▼

Save Changes

Hello, User!

Account Management | Security Settings | Activity Log

Logout

Change Password   Update your password to keep your account secure.   Change Password

Delete Account   This action is irreversible.   Delete My Account

---

Hello, User!

Account Management | Security Settings | Activity Log

Logout

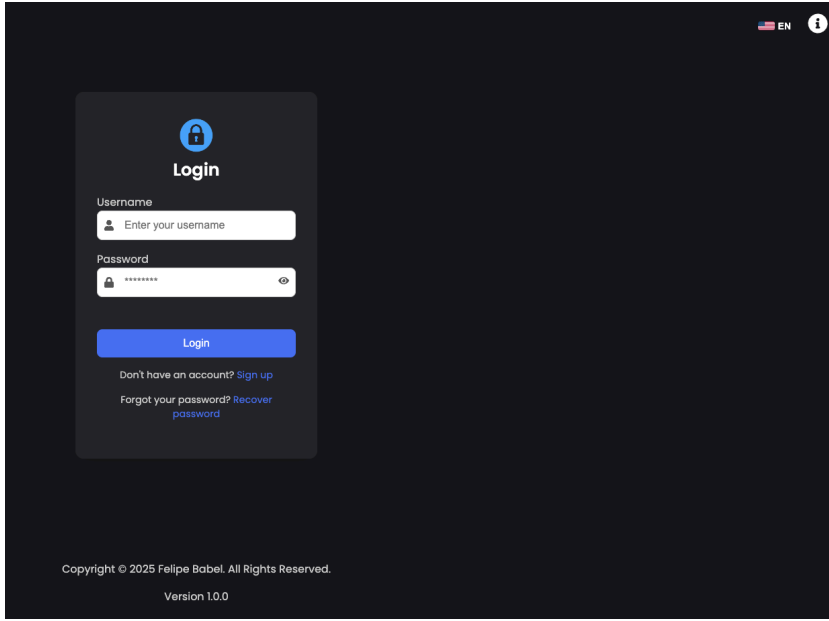| Action	IP Address	adminDashboard.deviceName	Description	Date ▼
LOGIN ACCOUNT	192.168.65.1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko…		10/13/2025, 2:14:01 AM
UPDATED LOGIN INFO…			Updated login date: 2025-10-13T0…	10/13/2025, 2:14:01 AM
LOGIN ATTEMPT OK			Login attempt: 0	10/13/2025, 2:14:01 AM
PASSWORD RESET			Password reset successfully.	10/13/2025, 2:13:56 AM
LOGIN ACCOUNT	192.168.65.1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko…		10/13/2025, 12:35:21 AM
UPDATED LOGIN INFO…			Updated login date: 2025-10-13T0…	10/13/2025, 12:35:21 AM
LOGIN ATTEMPT OK			Login attempt: 0	10/13/2025, 12:35:21 AM
LOGIN ATTEMPT FAILED			Login attempt: 1	10/13/2025, 12:35:18 AM
LOGIN ACCOUNT	192.168.65.1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko…		10/13/2025, 12:32:16 AM
UPDATED LOGIN INFO…			Updated login date: 2025-10-13T0…	10/13/2025, 12:32:16 AM

Users with the Analyst role have a shortcut button to the Analyst Dashboard.

Global Feature: All Dashboards (Admin, Analyst, and User) include a Logout button to end the session.

6. Authentication and Recovery Flows

Login

Fields for Username and Password. Includes options for:

○ View Project Documentation.
○ Change Language (English, Portuguese, Spanish, German).
○ Create Account.
○ Forgot Password.

Create Account (Sign Up)

Requires Username, Email, Name, Password, and Confirmation. Send a 6-digit code via email, valid for 15 minutes, to activate the account. Includes an option to go back to Login.

Validate Code Email

Screen to enter the activation code to activate the account.

Recover Password (Forgot Password)

Send a reset link/code to the email. Option to return to Login.
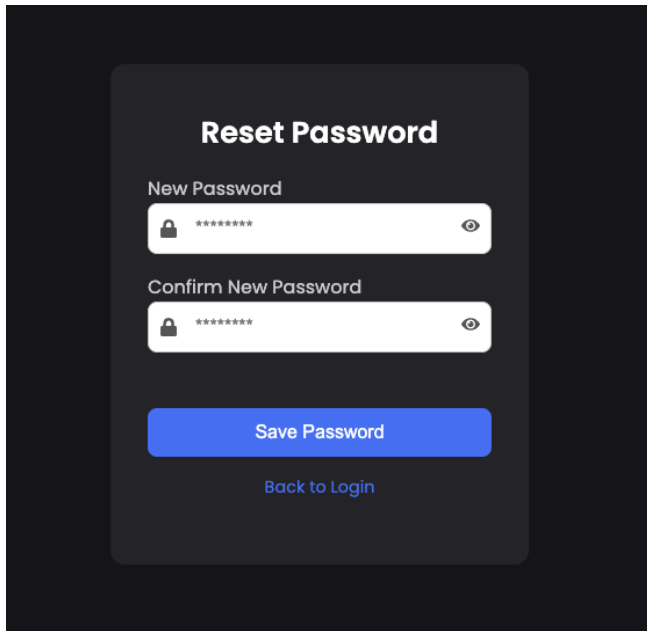
Validate Code Password

Screen to enter the 6-digit reset code (valid for 15 minutes).

Features:

Resend Code: If the user did not receive the email, they can request a resend, subject to a 2-minute cooldown between requests.

Back to Login: Option to cancel the process and return to the Login screen.

Reset Password

Accessed after validating the recovery code or when the user's password expires (due to expiration policy). Requires New Password and Confirmation, with validation to ensure the new password is different from the previous one.