Digital Newspaper Website
Use-Case Specification: Recover Password

Version 1.0

Revision History

Date	Version	Description	Author
18/07/2025	1.0	Specific about the Recover Password use case	Thạch Ngọc Hân

Table of Contents

Use-Case Specification: Recover Password

1.   Use-Case Name: Recover Password

1.1   Brief Description

This use case describes how a user can recover access to their account in case they forget their password. It involves requesting a password reset link via email and setting a new password using a secure recovery token.

2.   Flow of Events

2.1   Basic Flow

1.   The use case starts when the user clicks on the "Forgot Password?" link on the login page.
2.   The user is directed to the Password Recovery page.
3.   The user enters their registered email address and submits the form.
4.   The System validates the email format and checks if it exists in the database.
5.   If the email is valid, the system generates a secure, time-limited password reset token
6.   The system sends a recovery email with a reset link to the user's email address.
7.   The user clicks the link and is redirected to the Reset Password page.
8.   The user enters a new password and confirms it.
9.   The system validates the token and the new password, updates the password in the database, and notifies the user of success.
10. The use case ends.

2.2   Alternative Flows

2.2.1   Invalid Email Address

At step 4 of the Basic Flow, if the email address is not associated with any account:

a.   The system shows an error message: "This email is not registered."
b.   The user may try a different email or return to the login page.

2.2.2   Expired or Invalid Token

At step 9 of the Basic Flow, if the token is expired or tampered with:

a.   The system displays a message: "This reset link is invalid or has expired."
b.   The user is prompted to request a new password reset link.
c.   The flow returns to step 1 of the Basic Flow.

3.   Special Requirements

3.1   Security & Privacy

1.   The reset token must be encrypted, unique, and expire within 15 minutes.
2.   The new password must meet system-defined complexity requirements.

4.   Preconditions

4.1   The user is on the login page and selects the option to recover their password.

4.2   The system is online and email services are operational.
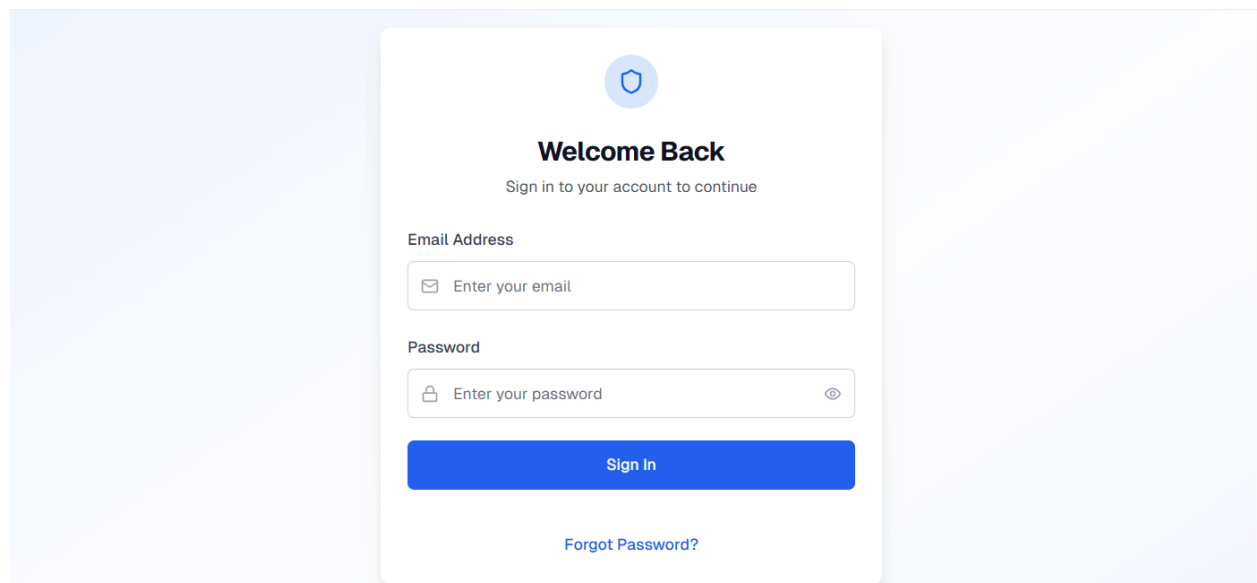
5. Postconditions

5.1   The user's password has been securely changed.

5.2   The reset token is invalidated.

5.3   The user may now log in with the new password.

6. Extension Points

6.1   Redirect to Login

- Location: After step 9 of the Basic Flow.
- Description: The system redirects the user to the login page with a success message: "Your password has been updated. Please log in."

Original interface

When you click "Forgot Password?"

When you enter an invalid email

When the email is valid