

Generate QA Insights

✓ Story Analysis Complete

User Story

US-1024: As a registered user, I want to reset my password so that I can regain access to my account.

Description

Users who have forgotten their password can request a password reset link via email and create a new password to access their account.

Acceptance Criteria

1. User can request a password reset from the 'Forgot Password' page.
2. System sends a password reset email to the registered email address.
3. Email contains a secure, time-limited link (valid for 30 minutes).
4. User is taken to a secure page to create a new password.
5. New password must meet complexity requirements.
6. On successful reset, user is redirected to the sign-in page with a confirmation message.
7. If the link is expired or already used, an appropriate error message is shown.
8. User can request a new reset link after the previous one expires.

Notes

- Applicable to all registered users.
- Rate limit reset requests to prevent abuse.
- Follow security and email templates as per standards.

Story ID
US-1024

Epic
Account Management

Feature
Password Recovery

Story Points
5

Priority
High

Status
In Review

Created By
Product Team

Created On
May 14, 2024

Last Updated
May 14, 2024

⚠ Risks

- Account enumeration risk if email exists check is exposed.
- Reset link interception if email is compromised.
- Weak password policy may lead to unauthorized access.
- No rate limiting may lead to abuse.

💬 Questions

- Should the reset link work for multiple devices?
- What message should be shown after successful password reset?
- Is two-factor authentication required after reset?
- Should users be notified of password reset activity?

📋 Business Rules

- Password reset link is valid for 30 minutes.
- New password must meet complexity requirements.
- Rate limit reset requests to prevent abuse.
- Follow security and email templates as per standards.

❓ Missing Information

- What are the password complexity rules?
- Is there a limit on the number of reset requests per user?
- What is the expected email template and sender?
- Should the user be logged out from other active sessions?