User Story 1: Enabling MFA During Sign-Up

Title:

New users must configure Multi-Factor Authentication after email verification.

User Roles:

- Newly registered user
- System Admin (making MFA compulsory)

Story Description:

As a newly registered user, I want to be prompted to configure multi-factor authentication (MFA) immediately after I verify my email address, So that my account is protected with an additional layer of security before my first login session.

This helps prevent unauthorized access even if someone else gains access to my email and password.

Preconditions:

- User has completed account creation with valid name, email, and password.
- User has verified their email via a verification link or code.
- MFA is made compulsory by System Administrator.

Acceptance Criteria:

1. After successful email verification, user is redirected to MFA setup.
2. User is prompted to submit a valid mobile number.
3. Till a valid mobile number is inputted step 2 is repeated.
4. A verification code is sent to the input valid mobile number.
5. The user is prompted to enter the OTP sent.
6. On correct OTP input:
    - MFA is marked as “enabled” for the user.
    - A “recovery key” is optionally shown.
    - The system logs in the user and sets up session tokens.
7. If OTP is incorrect, the user is prompted again with error messaging (max 3 attempts before redirect to login).
8. Optionally, the user may request to resubmit mobile number or re-generate OTP in case of technical issues.
9. In case use user closes window abruptly without completing process, MFA is set to inactive by default

Error States & Messages:

Condition	**Message**
OTP field left empty	"Please enter the verification code to continue."
OTP entered is incorrect	"Invalid code. Please check OTP and try again."
OTP expired	"This code has expired. Please generate a new one."

Condition	Message
Too many failed attempts	"Too many failed attempts. Please restart setup."

Postconditions:

- MFA is marked active/inactive according to user preference and saved database.
- Access and refresh tokens are issued.
- User is redirected to the main dashboard.

Open Questions:

- Should we allow skipping MFA setup during signup and allow it to be setup once user logs in?
- Should admins be able to reset MFA for users?

User Story 2: MFA Challenge During Login

Title:

Returning users must pass MFA challenge after correct login credentials

User Roles:

- Existing user with MFA enabled
- System Admin (monitoring login attempts)

Story Description:

As a returning user with MFA enabled, I want to be challenged with a verification code that should be received at the registered mobile number, after entering my username and password, So that even if my primary credentials are compromised, no one else can access my account.

Preconditions:

- User exists and has completed MFA setup in a prior session.
- User enters valid email/username and password.
- MFA is still activated for the user.
- The current device is not a trusted device.

Flow & Acceptance Criteria:

1. User submits valid login credentials.
2. System detects that MFA is enabled and that the device is not trusted.
3. User is prompted to enter OTP received at registered mobile number.
4. If the OTP is correct:
    - Access and refresh tokens are generated.
    - If the user checks "Remember this device", a trusted device token is stored.
    - The user is redirected to the dashboard.
5. If OTP is incorrect:
    - Show error message.
    - Allow up to 3 attempts before session is terminated.
    - Regenerate OTP.
6. If MFA is not enabled, skip this step and directly issue tokens.
7. If the window is closed abruptly without completing process, user is not logged in.

Error States & Messages:

Condition	Message
OTP left blank	"Verification code is required to continue."
Incorrect OTP entered	"The code you entered is incorrect. Please try again."

Condition	Message
Expired OTP	"Your verification code has expired. Use a new one."
3 Failed attempts	"Too many failed attempts. Please try logging in again."

Postconditions:

- If OTP is correct, the user is logged in and session is active.
- If "Remember this device" is selected:
    - A secure cookie is stored to skip MFA next time.
- If OTP fails repeatedly, user is logged out or redirected to login.

Open Questions:

- What is the expiration time of tokens for trusted devices?
- Should trusted device be invalidated on password reset or account recovery?
- Can users view/manage their trusted devices?