1)Attempt to sign up or login using the 2FAuth app.

2)Ensure that the OTP is successfully sent to the registered device.

3)Verify that the OTP is of the correct length and format.

4)Enter the correct OTP and validate that the operation (sign up, login, password change) is successful.

5)Enter an invalid OTP (e.g., an empty field, incorrect format, incorrect length, or expired OTP).

6)Validate that the operation is unsuccessful and an appropriate error message is displayed.

7)If the OTP is incorrect, validate that the app provides an option to resend the OTP.

8)When prompted, enter the backup code.

9)Validate that the operation is successful.

10)Wait for the OTP to expire.

11)Enter the expired OTP and validate that the operation is unsuccessful and an appropriate error message is displayed.

12)Repeat steps 1-3 with different devices and different lengths of OTPs.

13)These test cases should provide comprehensive coverage of the OTP operation using the 2FAuth app