Manual testing task

Test case 1. Happy valid test case for the TFA activation
Title: Verify Two-Factor Authentication (TFA) process in the application works as expected
Description: Positive test case scenario to verify that Two-Factor Authentication (TFA) process works as expected with **valid input**
Preconditions: Google Authenticator app is successfully installed on device that is used for the test below

Test step action	Expected Result
Go navigate to Two-Factor Authentication (TFA) option of your app	Two-Factor Authentication (TFA) option of your app is shown on the screen. Two-Factor Authentication (TFA) is not enabled (**You have not enabled two factor authentication message** is displayed)
Click **Enable** button	**Finish enabling two factor authentication** message is displayed QR code and Setup Key are generated on the screen successfully
Follow the instructions on the page **Option 1.** Add account via QR code Scan the QR code on the screen using your phone's Google Authenticator app **Option 2.** Add account by using setup key Enter the **Setup Key** placed under the QR code on your phone's Google Authenticator app	**Account added** message is displayed on your phone's Google Authenticator app Random 6-digit code is generated on your phone's Google Authenticator app
Enter the generated OTP code (Random 6-digit code) from your phone's Google Authenticator app in the Code field and click CONFIRM button	You will be prompt to **Confirm Password** screen

Enter your password and click CONFIRM button	**You have enabled two factor authentication** message is displayed Random Recovery codes are generated Red button DISABLE is displayed also (click if you want to disable Two-Factor Authentication (TFA) option)

Test case 2. Negative, edge test case for the TFA activation
Title: Verify Two-Factor Authentication (TFA) process in the application works as expected when OTP code is **expired**
Description: Negative test case scenario to verify that Two-Factor Authentication (TFA) process works as expected with **expired code**
Preconditions: Google Authenticator app is successfully installed on device that is used for the test below

Test step action	Expected Result
Go navigate to Two-Factor Authentication (TFA) option of your app	Two-Factor Authentication (TFA) option of your app is shown on the screen. Two-Factor Authentication (TFA) is not enabled (**You have not enabled two factor authentication message** is displayed)
Click **Enable** button	**Finish enabling two factor authentication** message is displayed QR code and Setup Key are generated on the screen successfully
Follow the instructions on the page **Option 1.** Add account via QR code Scan the QR code on the screen using your phone's Google Authenticator app **Option 2.** Add account by using setup key Enter the **Setup Key** placed under the QR code on your phone's Google Authenticator	**Account added** message is displayed on your phone's Google Authenticator app Random 6-digit code is generated on your phone's Google Authenticator app

app	
Wait for the generated OTP code (Random 6-digit code) from your phone's Google Authenticator app to **expire**. (OTP code is temporary and expire after certain time) Enter the **expired** OTP code in the Code field and click CONFIRM button	Message that **invalid or expired** code is used is displayed on the screen

Test case 3. Negative, edge test case for the TFA activation

Title: Verify Two-Factor Authentication (TFA) process in the application works as expected when OTP code is **invalid**
Description: Negative test case scenario to verify that Two-Factor Authentication (TFA) process works as expected with **invalid input**
Preconditions: Google Authenticator app is successfully installed on device that is used for the test below

Test step action	Expected Result
Go navigate to Two-Factor Authentication (TFA) option of your app	Two-Factor Authentication (TFA) option of your app is shown on the screen. Two-Factor Authentication (TFA) is not enabled (**You have not enabled two factor authentication message** is displayed)
Click **Enable** button	**Finish enabling two factor authentication** message is displayed QR code and Setup Key are generated on the screen successfully
Follow the instructions on the page **Option 1.** Add account via QR code Scan the QR code on the screen using your	**Account added** message is displayed on your phone's Google Authenticator app

phone's Google Authenticator app **Option 2.** Add account by using setup key Enter the **Setup Key** placed under the QR code on your phone's Google Authenticator app	Random 6-digit code is generated on your phone's Google Authenticator app
Replace one digit of the valid OTP code (Random 6-digit code) from your phone's Google Authenticator app with another random digit (to make OTP code **invalid**) Enter the **invalid** OTP code in the Code field and click CONFIRM button	Message that **invalid** code is used is displayed on the screen

Test case 4. Negative, edge test case for the TFA activation

Title: Verify Two-Factor Authentication (TFA) process in the application works as expected when **two accounts** are added to Google Authenticator app
Description: Negative test case scenario to verify that Two-Factor Authentication (TFA) process works as expected with **two accounts** added to Google Authenticator app
Preconditions: Google Authenticator app is successfully installed on device that is used for the test below

Test step action	Expected Result
Go navigate to Two-Factor Authentication (TFA) option of your app	Two-Factor Authentication (TFA) option of your app is shown on the screen. Two-Factor Authentication (TFA) is not enabled (**You have not enabled two factor authentication message** is displayed)
Click **Enable** button	**Finish enabling two factor authentication** message is displayed QR code and Setup Key are generated on the screen successfully

Follow the instructions on the page **Option 1.** Add account via QR code Scan the QR code on the screen using your phone's Google Authenticator app **Option 2.** Add account by using setup key Enter the **Setup Key** placed under the QR code on your phone's Google Authenticator app	**Account added** message is displayed on your phone's Google Authenticator app Random 6-digit code is generated on your phone's Google Authenticator app That is **account 1** with **OTP code 1**
Repeat step above for either **Option 1**. Or **Option 2**.	Separate, second account is created on your phone's Google Authenticator app Random 6-digit code is generated on your phone's Google Authenticator app for that second account That is **account 2** with **OTP code 2**
Enter the generated **OTP code 1 from account 1** (Random 6-digit code) from your phone's Google Authenticator app in the Code field and click CONFIRM button	Message that **invalid** code is used is displayed on the screen
Enter the generated **OTP code 2 from account 2** (Random 6-digit code) from your phone's Google Authenticator app in the Code field and click CONFIRM button	You will be prompt to **Confirm Password** screen
Enter your password and click CONFIRM button	**You have enabled two factor authentication** message is displayed Random Recovery codes are generated Red button DISABLE is displayed also (click if you want to disable Two-Factor Authentication (TFA) option)