

Poems Desktop
User Guide for Two Factor Authentication

Contents

User Manual	1
Part 1: 2FA Activation.....	1
Step 1: Login to the Poems Desktop	1
Step 2: Choose to activate the 2FA	2
Step 3: Enter SMS token to verify user identity	3
Step 4: Start 2FA registration process	4
Step 5: 2FA Activation had been completed successfully.....	6
Part 2: 2FA Authentication	7
Step 1: Login to the Poems Desktop	7
Step 2: Authenticate with the code you have from your linked device.	7
Step 3: Login successfully to the Poems Desktop system.....	8
Part 3: De-link and Re-link	9
Step 1: Login to the Poems Desktop	9
Step 2: Select 'Relink' button to switch to new device	9
Step 3: Confirmation to unlink from Google Authenticator, click on 'OK' to proceed.....	10
Step 4: Enter SMS token to verify user identity	11
Step 5: Delink successfully from the device, click on 'Activate' to proceed	12
Step 6: Relink to new device.....	12
Step 7: 2FA Activation had been completed successfully.....	14
FAQ	15
Client User	18
Part 1: 2FA Activation.....	18
Step 1: Login to the Poems Mobile	18
Step 2: Choose to setup and activate the 2FA	19
Step 3: Read the Terms and Conditions of Digital Token	19
Step 4: Confirmation on the registered mobile number	20
Step 5: Enter SMS token to verify user identity	20
Step 6: Start 2FA registration process, by installing the Google Authenticator app.....	22
Step 7: Once Installation is successful, tap on QRCode/Copy the text code line.....	23
Step 8: Upon tap on CQCode, will redirect to Google Authenticator.....	23
Step 9: Input/Paste the OTP from Google Authenticator	24

Step 10: Login Successful.....	25
Part 2: 2FA Login.....	26
Step 1: Login to the Poems Mobile	26
Step 2: Authenticate with the code you have from your linked device	26
Step 3: Login successful	27
Part 3: De-link and Re-link	28
Step 1: Login to the Poems Mobile	28
Step 2: Select 'Relink' button to switch to new device	28
Step 3: Read the Terms and Conditions of Digital Token	29
Step 6: Start 2FA registration process, by installing the Google Authenticator app.....	32
Step 7: Once Installation successful, tap on QRCode/Copy the code line	33
Step 8: Upon scanning, will redirect to Google Authenticator	33
Step 9: Input/Paste the OTP from Google Authenticator.....	34
Step 10: Login Successful.....	32
FAQ	33

The primary objective of two factor authentication is to secure the user authentication process and to protect online user accounts against unauthorized access. When implemented properly, 2FA offers much greater protection against hacking than single-factor password authentication and helps to safeguard online user accounts from unauthorized access even when the passwords have been compromised.

For Poems Desktop trading platform users, we will implement 2 factors below to fulfill the requirement of 2FA:

1. Something you know (User Password) – Already in used
2. Something you have (One-time password) – New

In order to get the one-time password (OTP), users will need to register their device to our system with the authenticator. There are lot of software-based authenticators online, among the most well-known is Google Authenticator. We will use Google authenticator as the OTP generator for our Poems Dekstop system.

This document is intended to guide end client users on the 2FA setup and login to the system with 2FA.

User Manual

Part 1: 2FA Activation

Step 1: Login to the Poems Desktop

Enter login ID and password, then Click 'Login'.



POEMS Global MY Login

poems MY
GLOBAL 20 v. 1.0.303.307-D10

User Name

Password

☒ Remember this Username

Login

[Forgot your Username or Password?](#)

By clicking on the Login button, you acknowledge that you have read, understood and accepted the following:

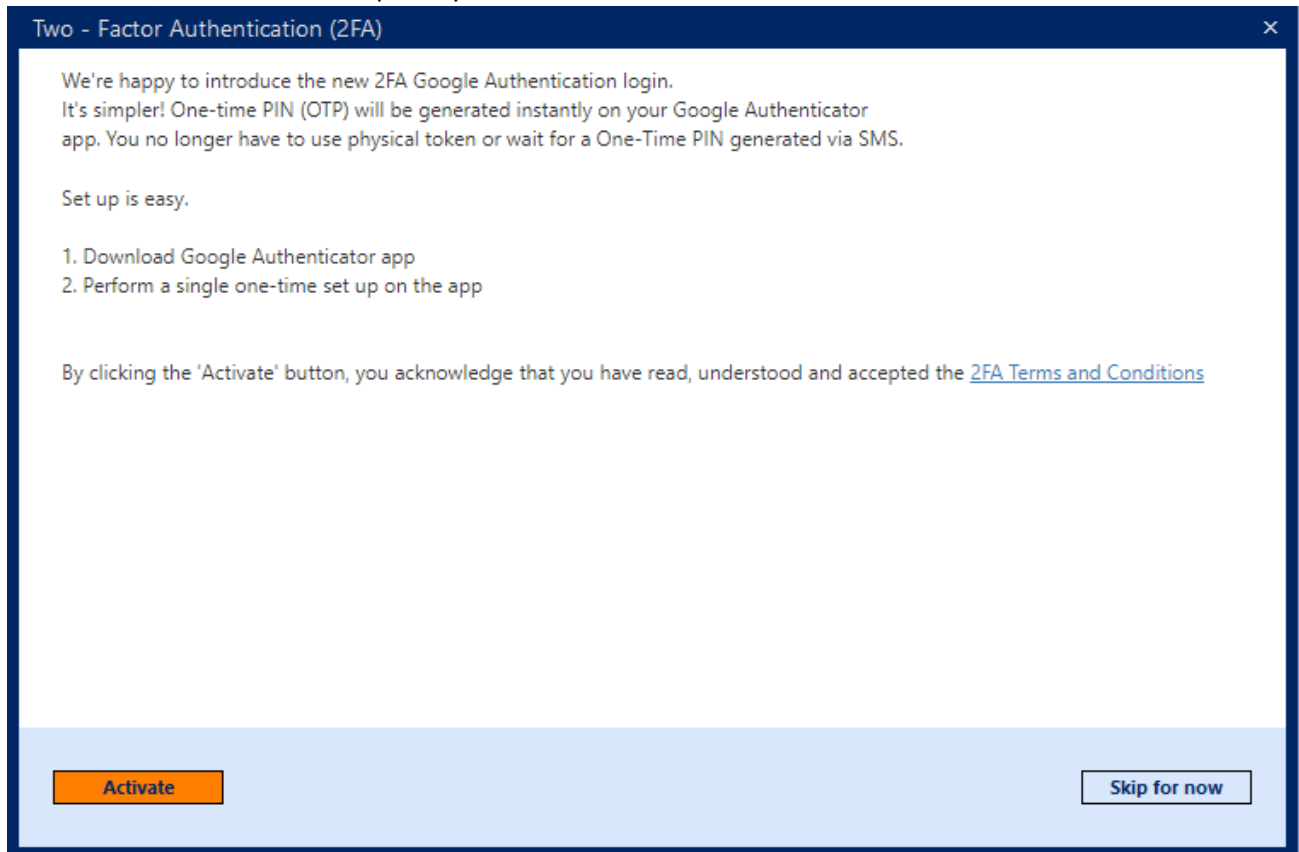
[Terms and Conditions](#) [Privacy and Security](#)

☐ Dealer Login

? i

Step 2: Choose to activate the 2FA

Select 'Activate' to enable the 2FA authentication to your account. Users may choose to 'Skip for now' as well for now, but it will be compulsory to enable 2FA in future.



It will open 2FA Terms and Conditions page by clicking the "[2FA Terms and Conditions](#)" link

Step 3: Enter SMS token to verify user identity

A GFO System token will be sent to the user's registered mobile number via SMS. User will need to key in the token and activate within 2 mins before the token expired.

The screenshot shows a window titled "Two - Factor Authentication (2FA)". Inside, the section "User Confirmation - SMS Token Verification" contains the following text: "A verification token has been sent to your registered number. Please key in the token stated in the SMS". Below this is a text input field labeled "Enter OTP:" with the placeholder text "Enter OTP". To the right of the input field is a "Verify" button. Below the input field, it says "Resend Code in 49 sec" and "Having problem with receiving token? Please contact your administrator." in red text. At the bottom right of the window is a "Sign Out" button.

If users enter wrong SMS, OTP will display Invalid Token message. Please note that the user account will be suspended after more than 4 incorrect token attempts during verification.

This screenshot shows the same "Two - Factor Authentication (2FA)" window as above, but with an error message displayed. The "Enter OTP:" field now contains the text "123456". An error dialog box is overlaid in the center of the screen with the title "Invalid Token", a close button (X), and the message "Your OTP is invalid." with an "OK" button. The background of the main window is dimmed. The "Sign Out" button remains at the bottom right.

Step 4: Start 2FA registration process

Please follow provided steps to complete the 2FA registration by linking your login account to your device.

Two - Factor Authentication (2FA)

Protect your account by enabling two-factor authentication in 3 simple steps

1) Install Google Authenticator App
Download and install "Google Authenticator" on your mobile phone by searching for it in Google PlayStore or Apple AppStore.



2) Scan the QR Code
Open the Google Authenticator App and press the (+) button to scan this QR Code:



[Sign Out](#)

Two - Factor Authentication (2FA)



If scanning fails, you can also enter this code manually:

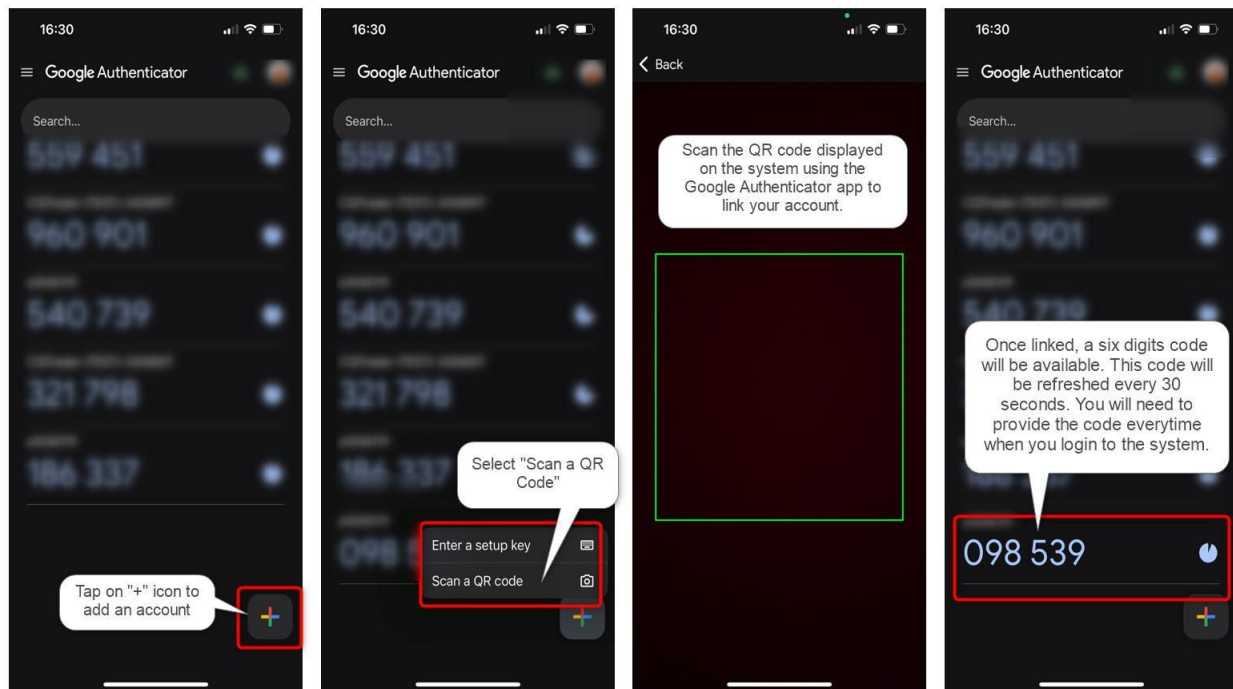
[Copy text](#)

3) Enter the 6-Digit Code
You're almost done! Enter the current 6-digit code shown in your authenticator app:

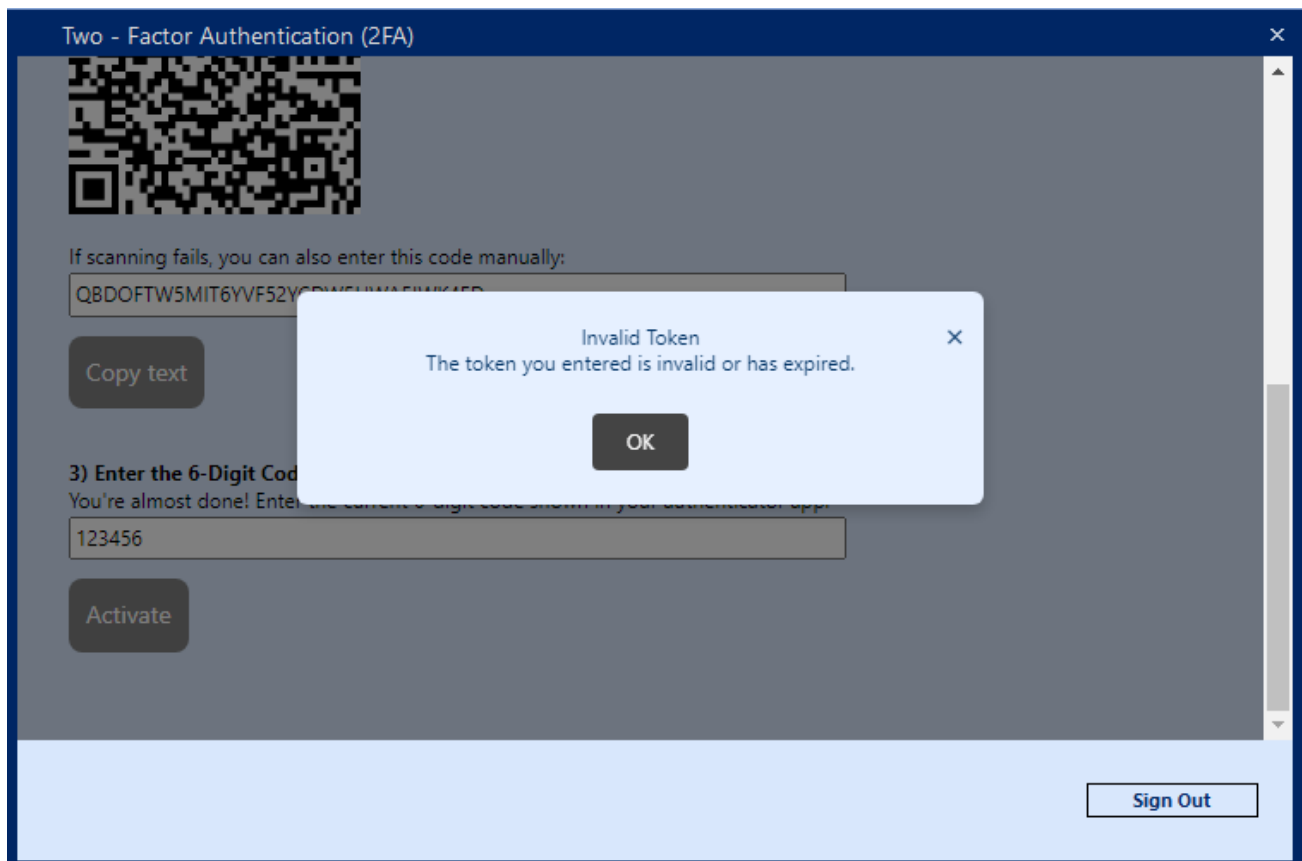
[Activate](#)

[Sign Out](#)

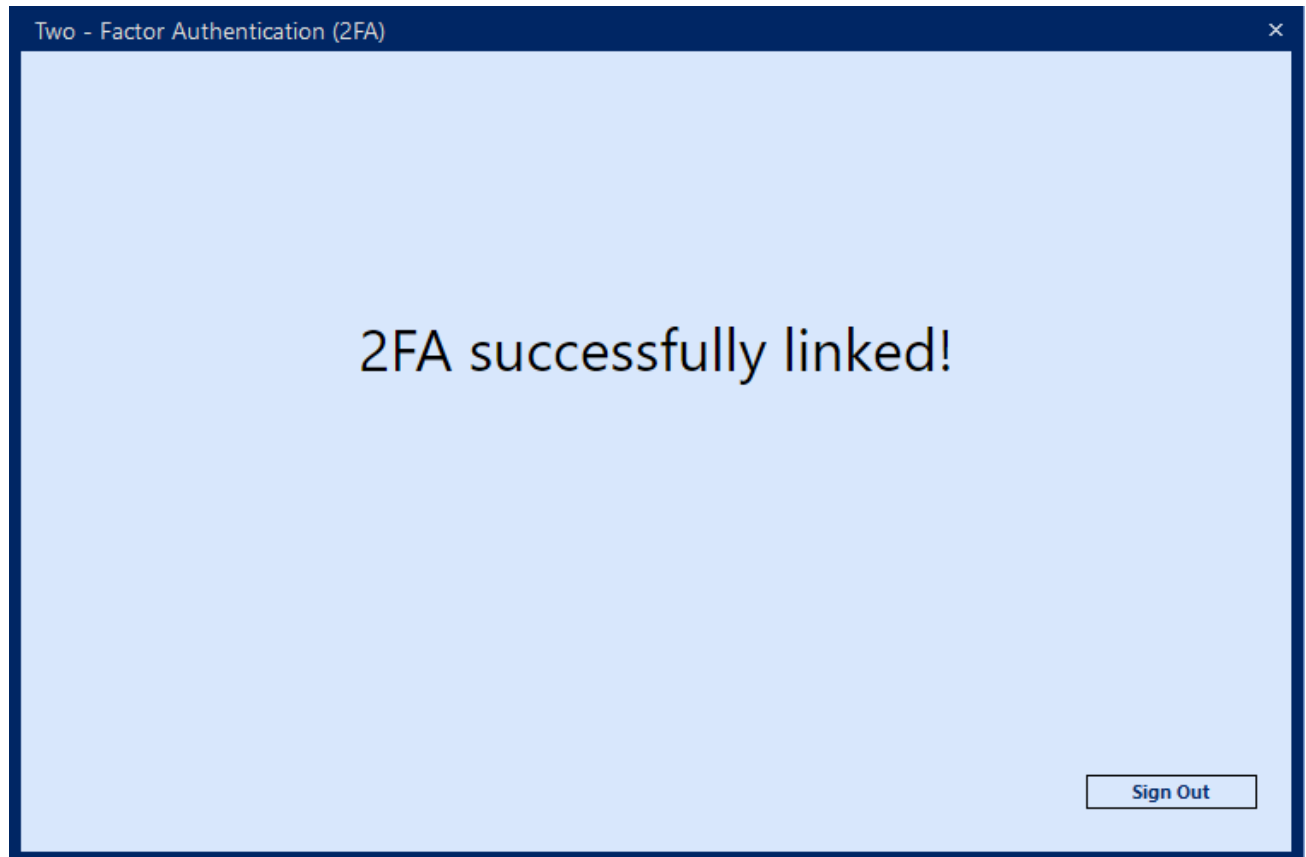
Users will need to install the Google Authenticator on their device and scan the QR code to link up the device and login account. Once linked up successfully, a 6 digits code will be displayed, user will need to key in the code into the system to complete the activation process.



If users enter the wrong 6-digit Google Auth pin will display an Invalid Token message. Please note that the user account will be suspended after more than 10 incorrect attempts during verification.



Step 5: 2FA Activation had been completed successfully



Part 2: 2FA Authentication

Step 1: Login to the Poems Desktop

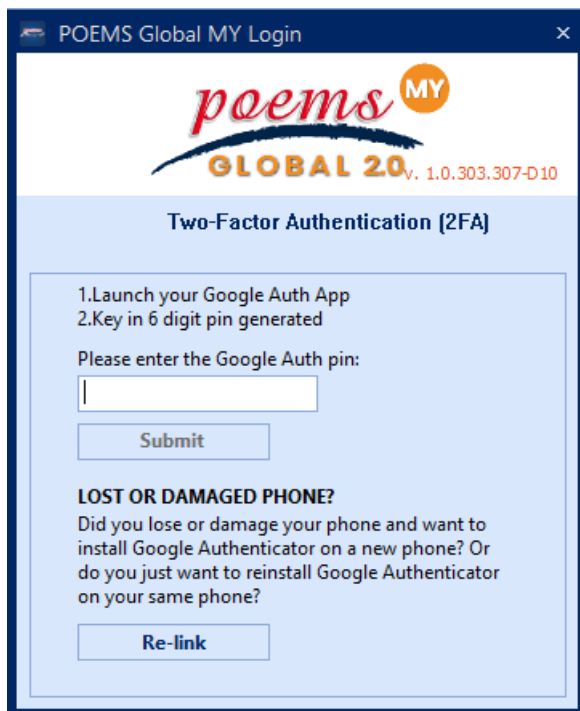
Enter login ID and password, then Click 'Login'.



The screenshot shows the 'POEMS Global MY Login' window. At the top is the 'poems MY GLOBAL 20' logo with version 'v. 1.0.303.307-D10'. Below the logo are two input fields: 'User Name' and 'Password'. A checkbox labeled 'Remember this Username' is checked. A 'Login' button is to the right of the password field. Below the inputs is a link: 'Forgot your Username or Password?'. A paragraph of text states: 'By clicking on the Login button, you acknowledge that you have read, understood and accepted the following:'. Below this are two links: 'Terms and Conditions' and 'Privacy and Security'. At the bottom left is a checkbox labeled 'Dealer Login'. At the bottom right are question mark and information icons.

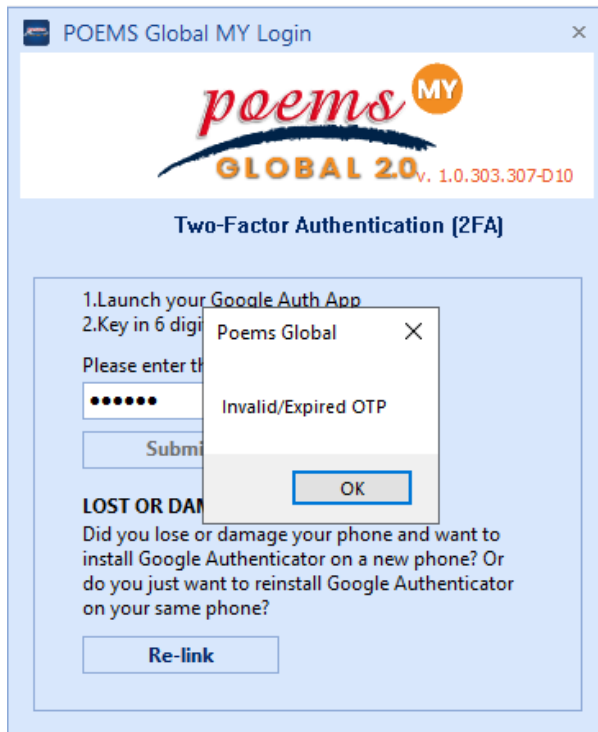
Step 2: Authenticate with the code you have from your linked device.

Enter the 6 digits code from Google Authenticator and click on 'Submit'.

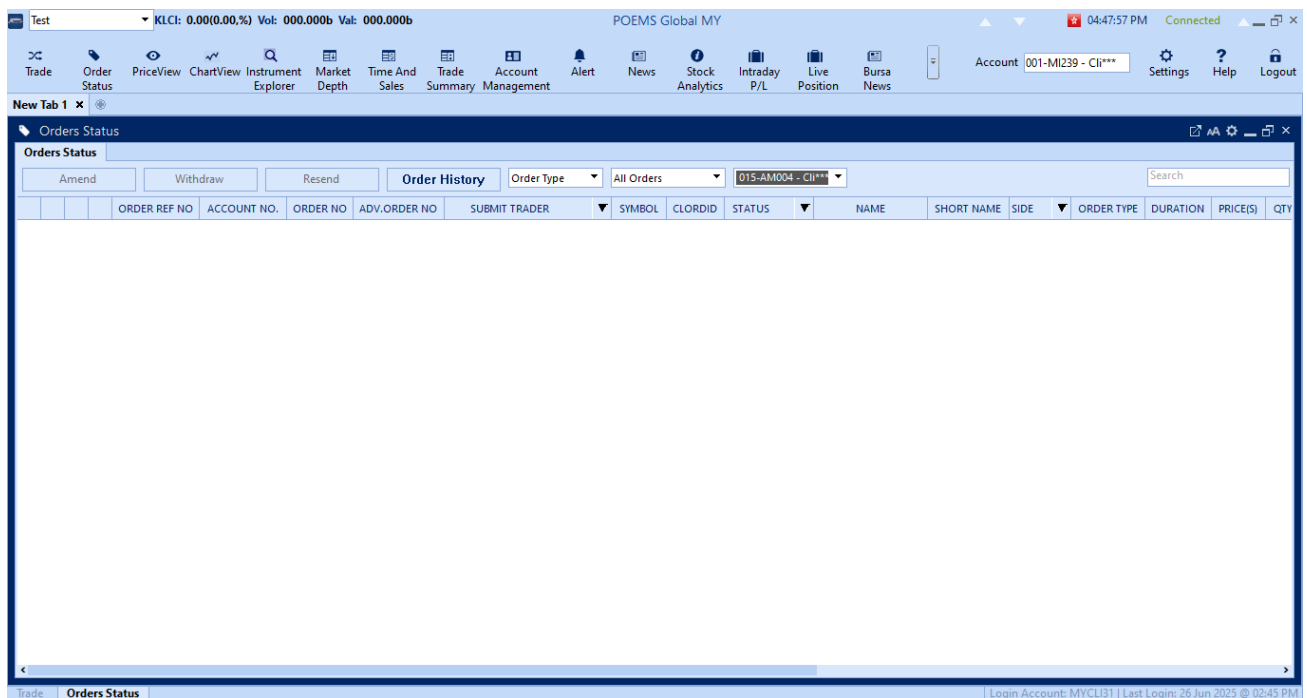


The screenshot shows the 'POEMS Global MY Login' window with the title 'Two-Factor Authentication (2FA)'. It lists two steps: '1. Launch your Google Auth App' and '2. Key in 6 digit pin generated'. Below this is the text 'Please enter the Google Auth pin:' followed by a single-character input field. A 'Submit' button is below the input field. Further down is the section 'LOST OR DAMAGED PHONE?' with the text: 'Did you lose or damage your phone and want to install Google Authenticator on a new phone? Or do you just want to reinstall Google Authenticator on your same phone?'. A 'Re-link' button is at the bottom.

If users enter the wrong Google Auth pin will display “Invalid/Expired” or “User was suspended.” message.



Step 3: Login successfully to the Poems Desktop system.



Part 3: De-link and Re-link

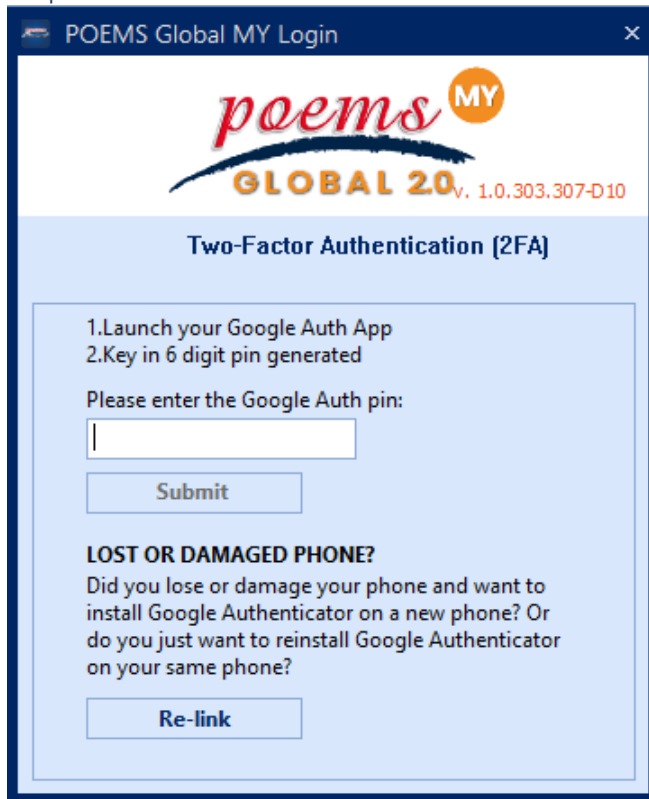
Step 1: Login to the Poems Desktop

Enter login ID and password, then Click 'Login'.



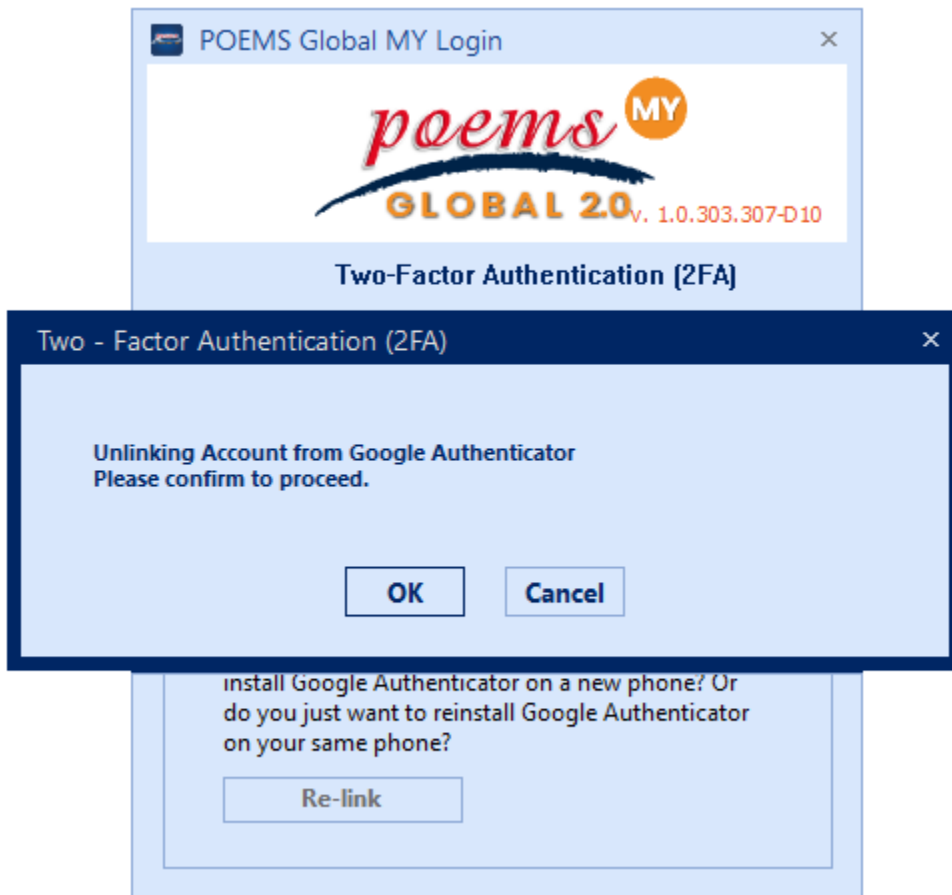
The screenshot shows a web browser window titled "POEMS Global MY Login". The page features the "poems MY GLOBAL 20" logo with the version number "v. 1.0.303.307-D10". Below the logo, there are two input fields for "User Name" and "Password". A checkbox labeled "Remember this Username" is checked. A "Login" button is positioned to the right of the password field. Below the login fields, there is a link that says "Forgot your Username or Password?". A disclaimer states: "By clicking on the Login button, you acknowledge that you have read, understood and accepted the following:". Below this, there are two links: "Terms and Conditions" and "Privacy and Security". At the bottom left, there is a checkbox for "Dealer Login". At the bottom right, there are icons for help (?) and information (i).

Step 2: Select 'Relink' button to switch to new device



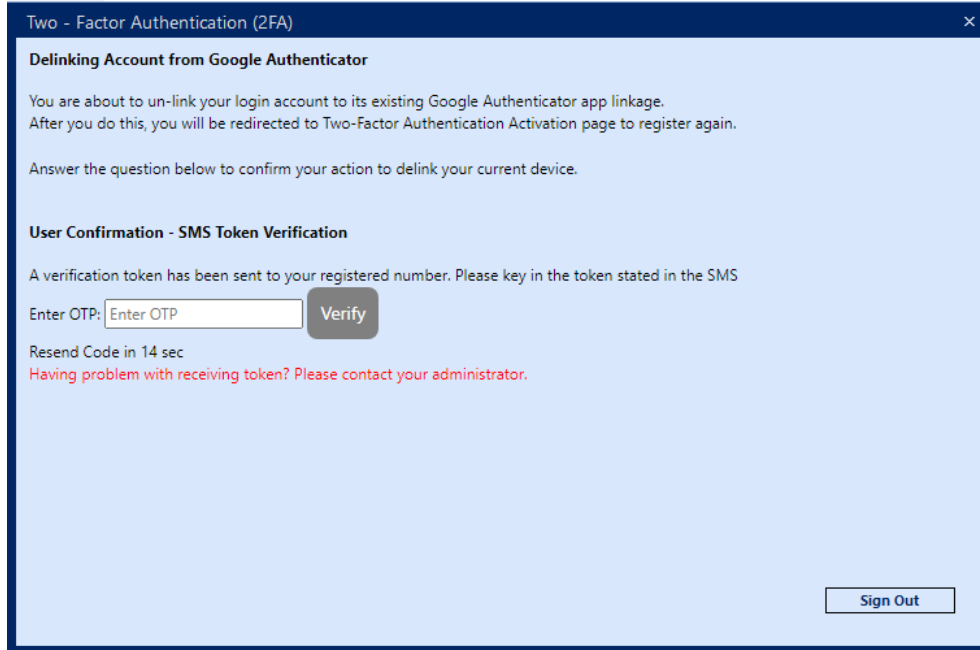
The screenshot shows the same "POEMS Global MY Login" window, but now it displays the "Two-Factor Authentication (2FA)" section. It lists two steps: "1. Launch your Google Auth App" and "2. Key in 6 digit pin generated". Below these steps, it says "Please enter the Google Auth pin:" followed by a text input field. A "Submit" button is located below the input field. Further down, there is a section titled "LOST OR DAMAGED PHONE?" with the text: "Did you lose or damage your phone and want to install Google Authenticator on a new phone? Or do you just want to reinstall Google Authenticator on your same phone?". A "Re-link" button is positioned at the bottom of this section.

Step 3: Confirmation to unlink from Google Authenticator, click on 'OK' to proceed.



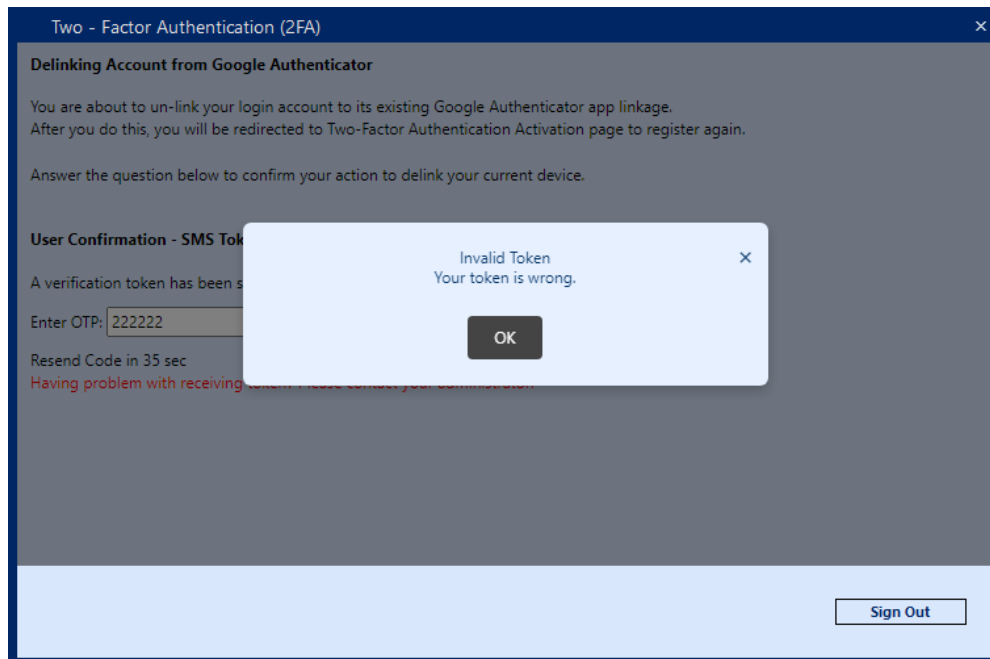
Step 4: Enter SMS token to verify user identity

A GFO System token will be sent to the user registered mobile number via SMS, user will need to key in the token and activate within 2 mins before token expired. Please note that the user account will be suspended after more than 4 incorrect token attempts during verification.



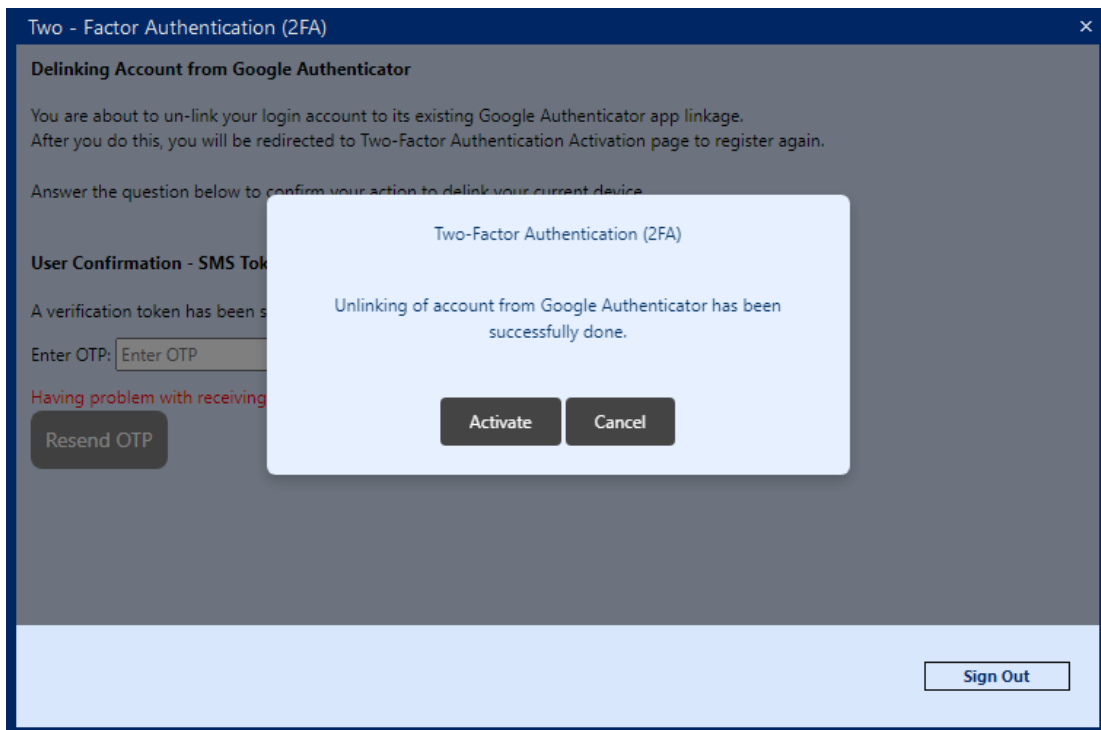
The screenshot shows a window titled "Two - Factor Authentication (2FA)". It contains two main sections. The first section, "Delinking Account from Google Authenticator", explains that the user is about to un-link their login account from its existing Google Authenticator app linkage and that they will be redirected to the Two-Factor Authentication Activation page to register again. It asks the user to answer a question below to confirm their action to delink their current device. The second section, "User Confirmation - SMS Token Verification", states that a verification token has been sent to the user's registered number and asks them to key in the token. It includes a text input field labeled "Enter OTP:" with a "Verify" button next to it. Below the input field, it says "Resend Code in 14 sec" and "Having problem with receiving token? Please contact your administrator." A "Sign Out" button is located at the bottom right of the window.

If users enter wrong SMS, OTP will display Invalid Token message. Please note that the user account will be suspended after more than 4 incorrect token attempts during verification.



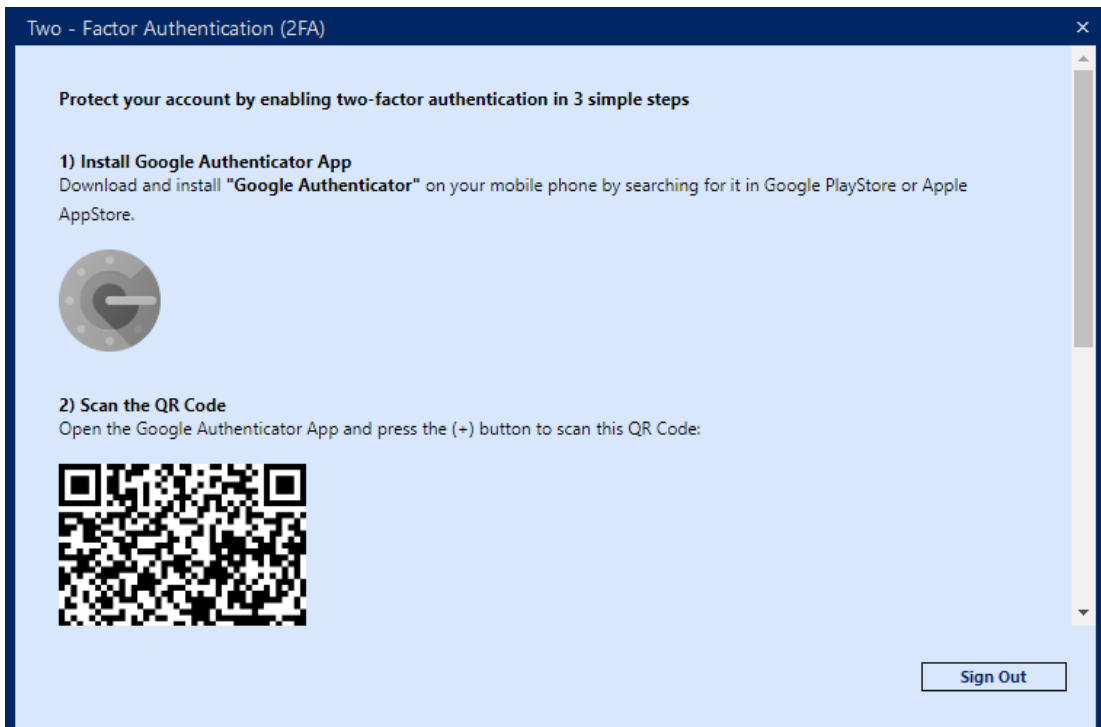
The screenshot shows the same "Two - Factor Authentication (2FA)" window as before, but with an "Invalid Token" error message displayed in a modal dialog box. The dialog box has a title bar with "Invalid Token" and a close button (X). The message inside says "Your token is wrong." and there is an "OK" button. In the background, the "User Confirmation - SMS Token Verification" section is visible, showing the "Enter OTP:" field with the value "222222" and the "Verify" button. The "Resend Code in 35 sec" and "Having problem with receiving token? Please contact your administrator." text are also visible. The "Sign Out" button is at the bottom right of the window.

Step 5: Delink successfully from the device, click on 'Activate' to proceed

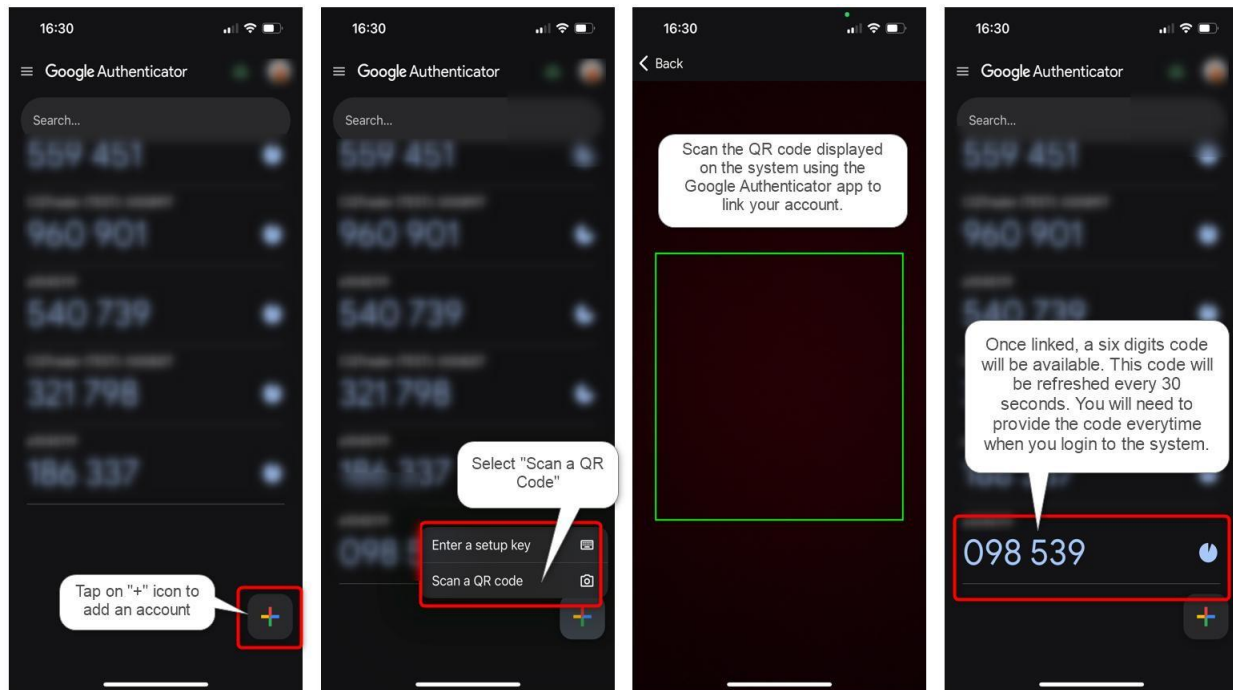


Step 6: Relink to new device

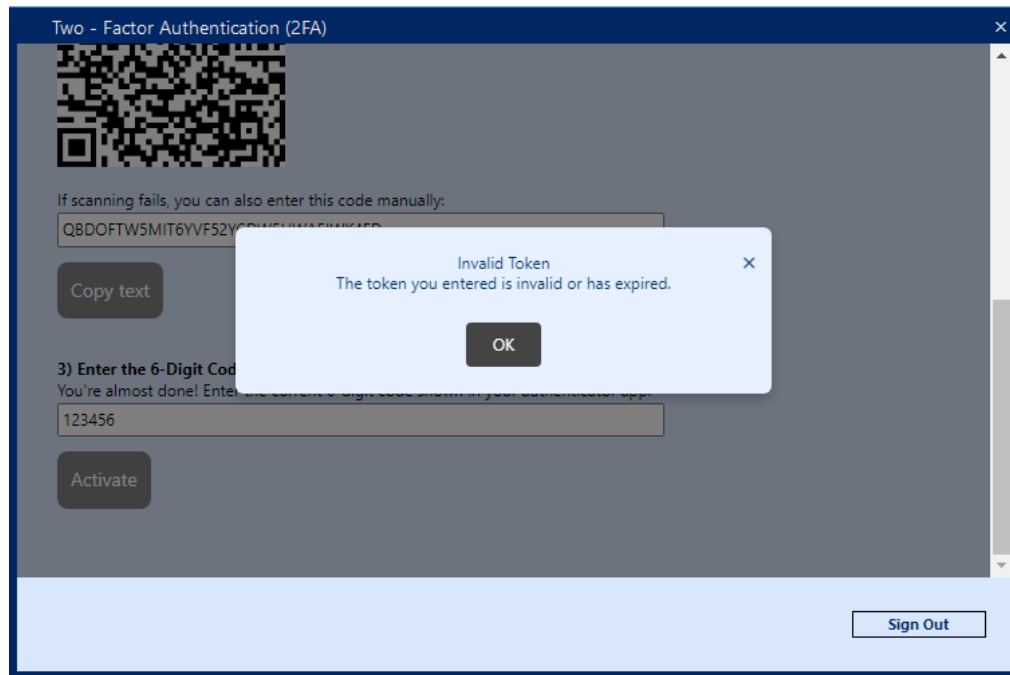
User will need to relink/activate the 2FA again on the new device. Please refer to Part 1, steps 4 and 5.



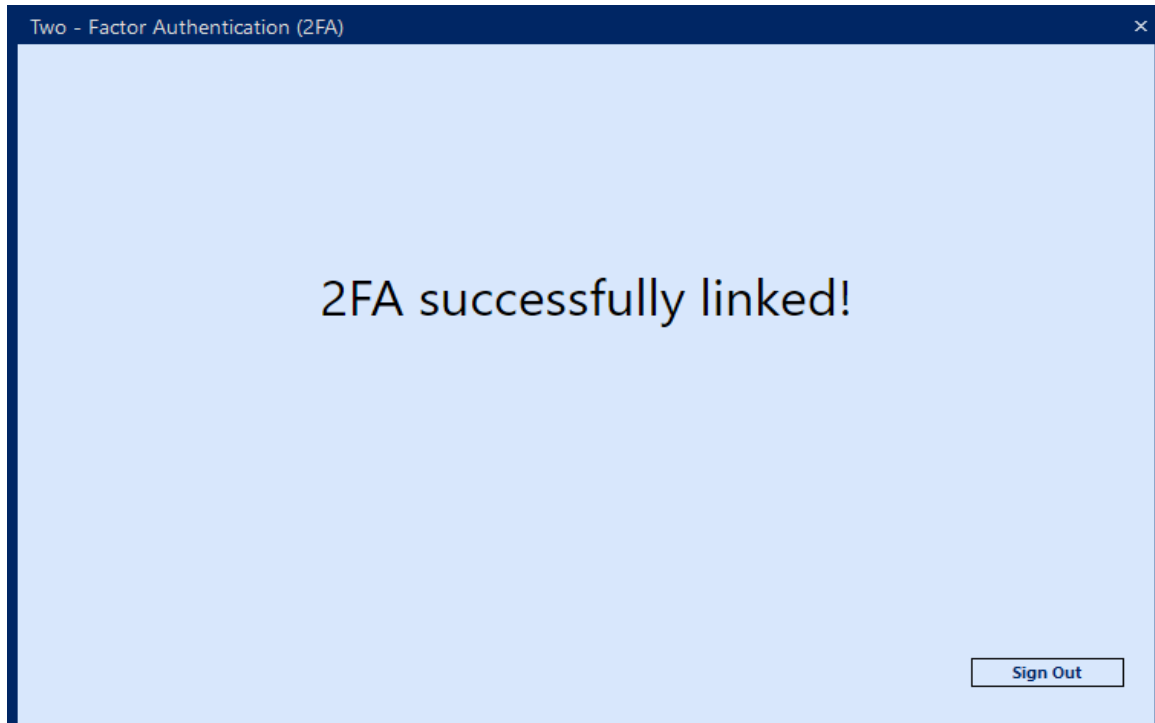
Users will need to install Google Authenticator on their device and scan the QR code to link up the device and login account. Once linked up successfully, a 6 digits code will be displayed, user will need to key in the code into the system to complete the activation process.



If users enter the wrong 6-digit Google Auth pin will display an Invalid Token message. Please note that the user account will be suspended after more than 10 incorrect attempts during verification.



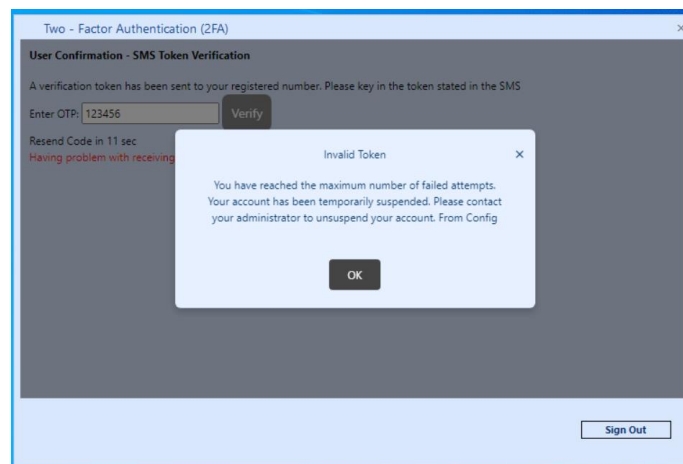
Step 7: 2FA Activation had been completed successfully



FAQ

What happens after more than 4 incorrect SMS token attempts during verification for 2FA setup?

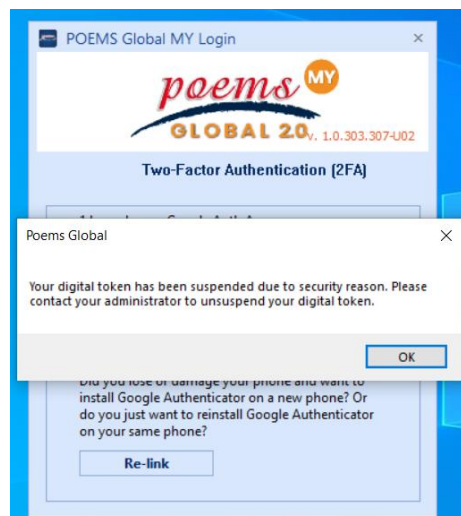
The user account will be suspended after more than 4 incorrect SMS token attempts during verification for the 2FA setup as displayed below.

**What can I do to unsuspend the account after 4 incorrect SMS token attempts during verification for 2FA setup?**

Please contact your Administrator / Hotline to unsuspend your account to proceed with the 2FA setup.

How many wrong attempts is allowed when you key in the Google Authenticator code after keying in your password?

On your 10th attempt keying in the wrong Google Authenticator code, your digital token will be suspended.

**What can I do to unsuspend the digital token after 10 incorrect Google Authenticator code attempts?**

Please contact your Administrator / Hotline to unsuspend your digital token. After unsuspend, you can proceed to login with the Google Authenticator code.

What should I do in the event that even when I input the correct Google Authenticator code from Google Authenticator apps, but error message “Invalid OTP” appear?

Please first ensure that “Date & Time” and “Time Zone” on your phone has been set automatically and correctly to Malaysia time zone. After the done setting the “Date & Time” and “Time Zone” correctly, please try to key-in the Google Authenticator code again in our POEMS Apps

Poems Mobile

User Guide for Two Factor Authentication

The primary objective of two factor authentication is to secure the user authentication process and to protect online user accounts against unauthorized access. When implemented properly, 2FA offers much greater protection against hacking than single-factor password authentication, and helps to safeguard online user accounts from unauthorized access even when the passwords have been compromised.

For Poems Mobile trading platform users, we will implement 2 factors below to fulfill the requirement of 2FA:

1. Something you know (User Password) – Already in used
2. Something you have (One-time password) – New

To obtain the one-time password (OTP), users must register their device with our system using the authenticator. There is lot of software-based authenticators online, among the most well-known is Google Authenticator. We will use Google authenticator as the OTP generator for our Poems Mobile system.

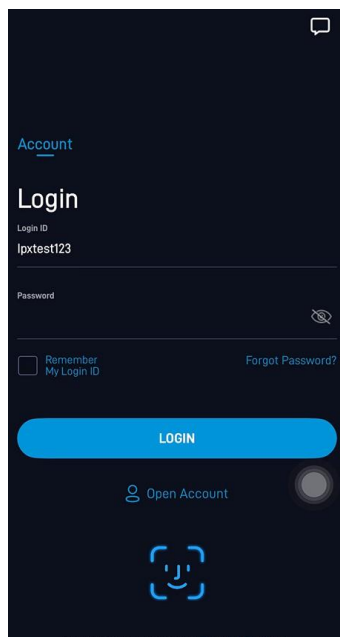
This document is intended to guide end client users on the 2FA setup and login to system with 2FA.

Client User

Part 1: 2FA Activation

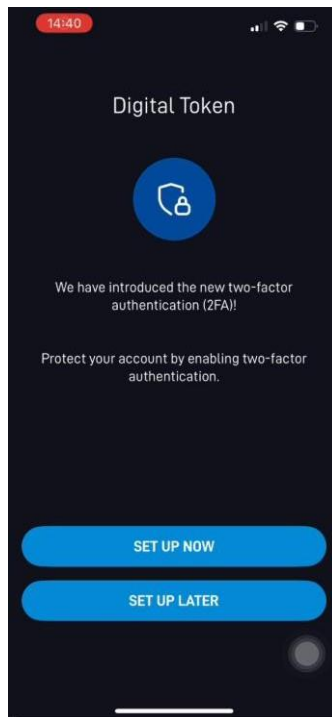
Step 1: Login to the Poems Mobile

Enter login ID and password, then Tap 'Login' or may login with FaceID/Fingerprint.



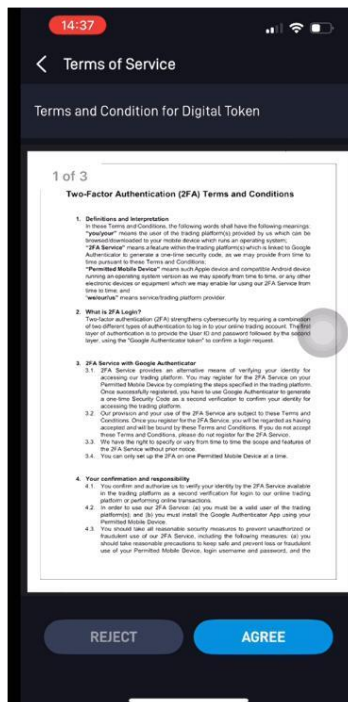
Step 2: Choose to setup and activate the 2FA

Select 'Set Up Now' to enable the 2FA authentication to your account. User may choose to skip as well for now, but it will be compulsory to enable 2FA in future.

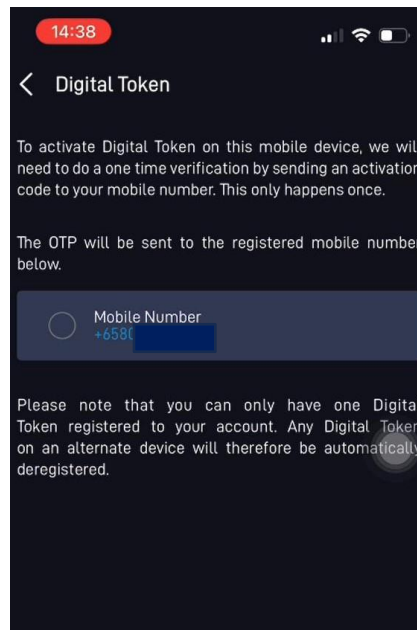


Step 3: Read the Terms and Conditions of Digital Token

The user will need to read the Terms and Conditions for Digital Token and Agree to proceed.

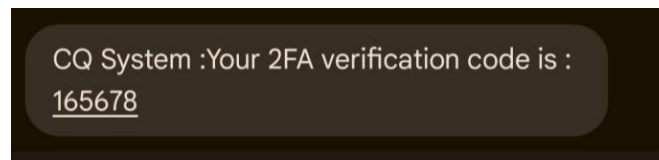


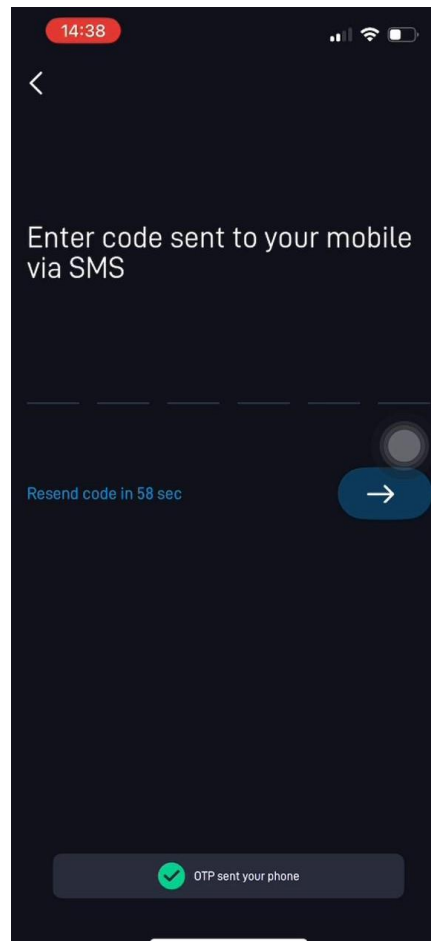
Step 4: Confirmation on the registered mobile number



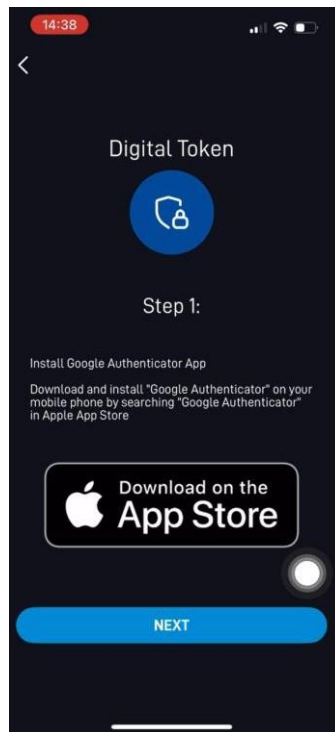
Step 5: Enter SMS token to verify user identity

A CQ System token will be sent to user registered mobile number via SMS, user will need to key in the token and activate within 2 mins before token expired. Please note that the user account will be suspended after more than 4 incorrect token attempts during verification.

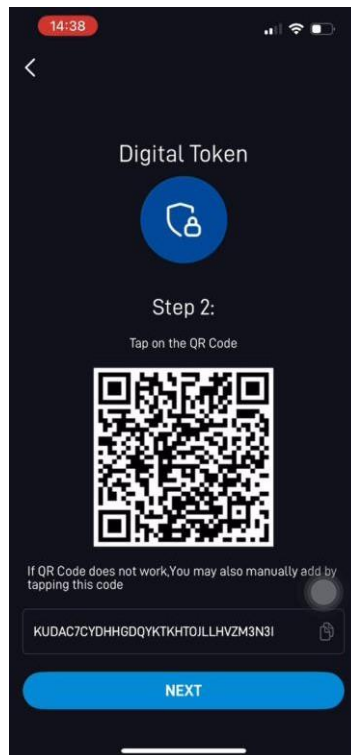




Step 6: Start 2FA registration process, by installing the Google Authenticator app

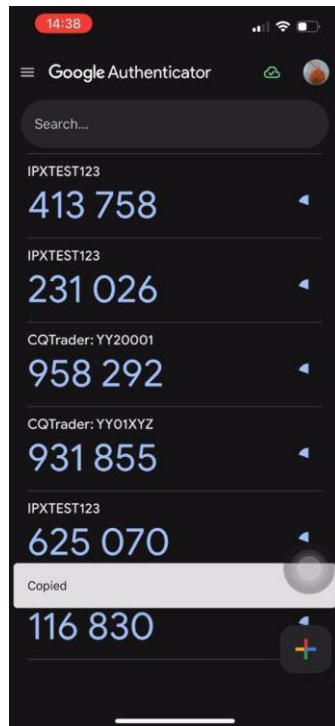


Step 7: Once Installation is successful, tap on QRCode/Copy the text code line

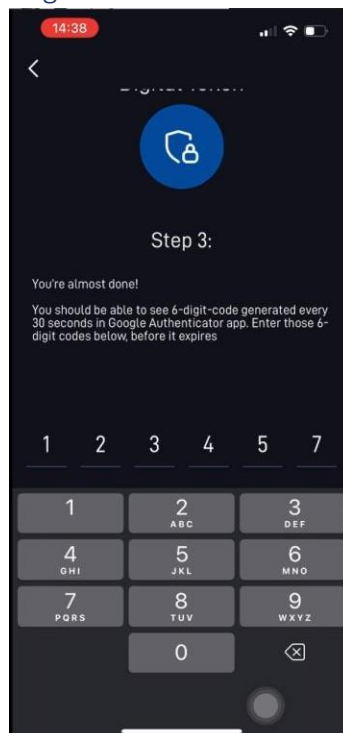


Step 8: Upon tap on CQCode, will redirect to Google Authenticator

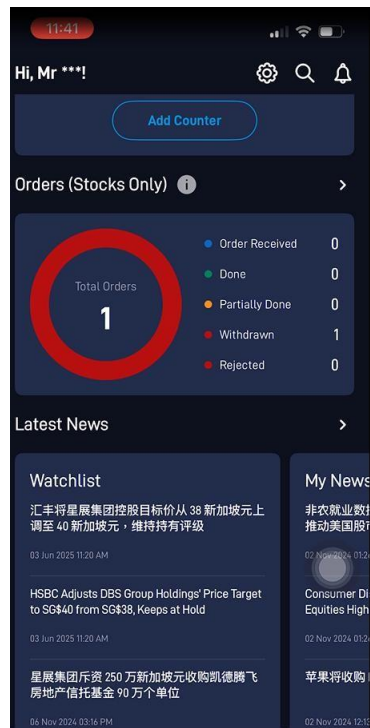
User will need to redirect to Google Authenticator, and may copy the 6 digit of OTP password



Step 9: Input/Paste the OTP from Google Authenticator



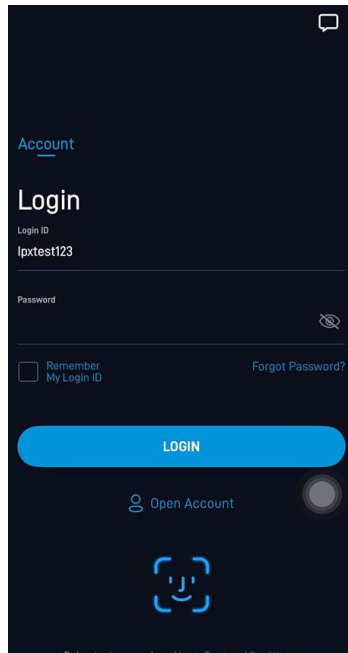
Step 10: Login Successful



Part 2: 2FA Login

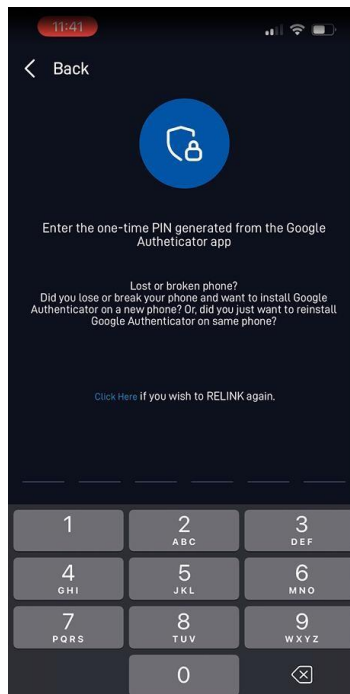
Step 1: Login to the Poems Mobile

Enter login ID and password, then Tap 'Login' or may login with FaceID/Fingerprint.

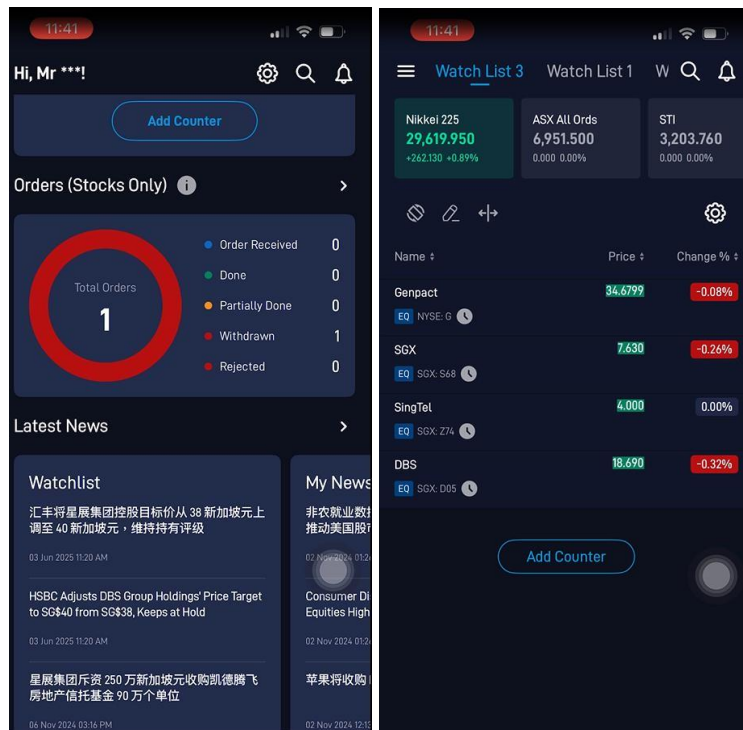


Step 2: Authenticate with the code you have from your linked device

Enter the 6 digits code from Google Authenticator and click on 'Login'.



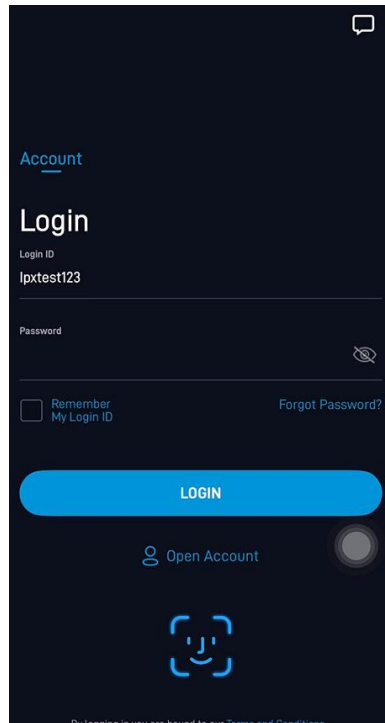
Step 3: Login successful



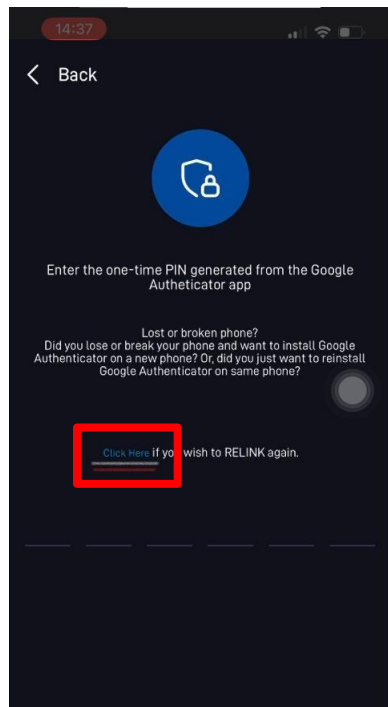
Part 3: De-link and Re-link

Step 1: Login to the Poems Mobile

Enter login ID and password, then Tap 'Login' or may login with FaceID/Fingerprint.

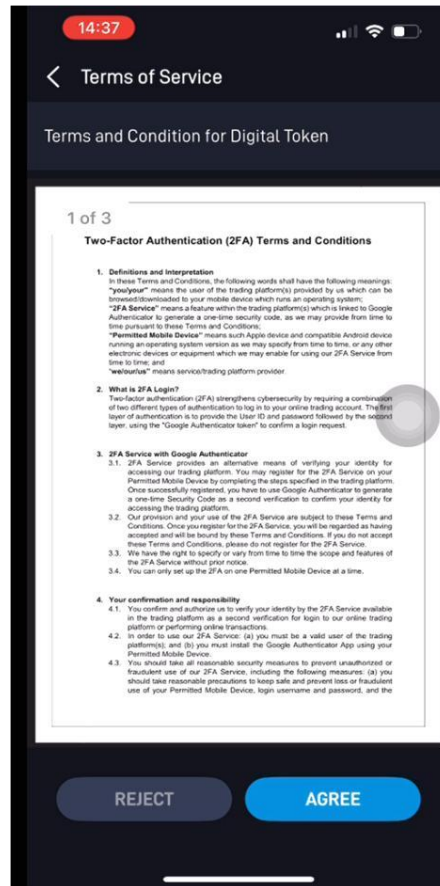


Step 2: Select 'Relink' button to switch to new device

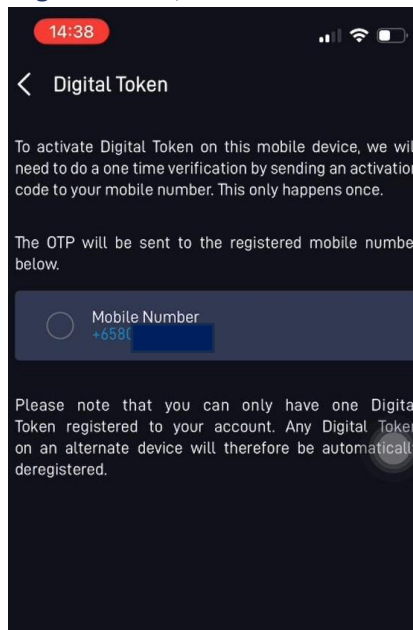


Step 3: Read the Terms and Conditions of Digital Token

The user will need to read the Terms and Conditions for Digital Token and Agree/Disagree to proceed. .

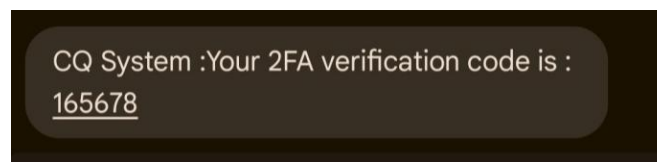


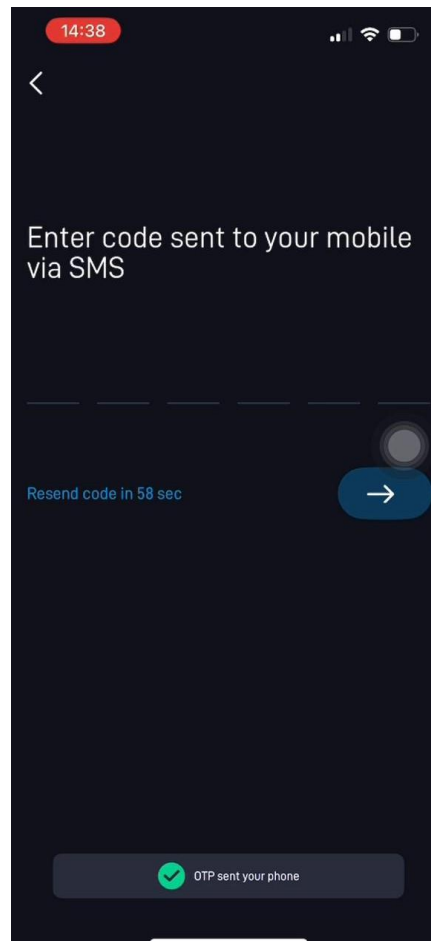
Step 4: Confirmation to activate Digital Token, OTP will be sent to the registered mobile number



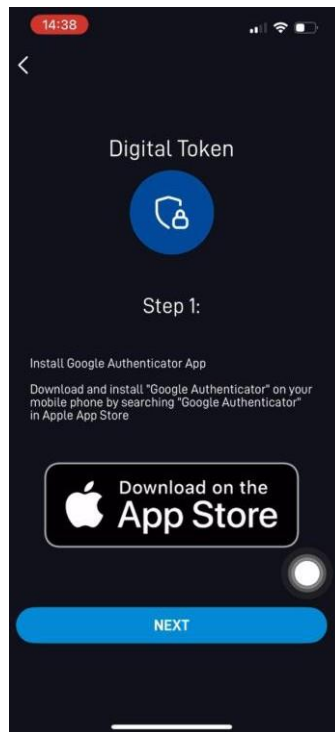
Step 5: Enter SMS token to verify user identity

A CQ System token will be sent to user registered mobile number via SMS, user will need to key in the token and activate within 2 mins before token expired. Please note that the user account will be suspended after more than 4 incorrect token attempts during verification.

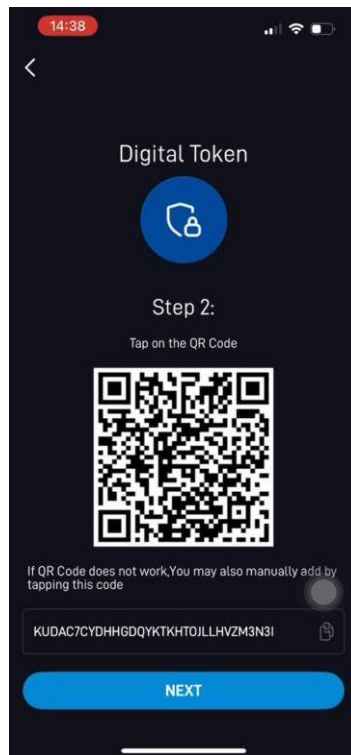




Step 6: Start 2FA registration process, by installing the Google Authenticator app

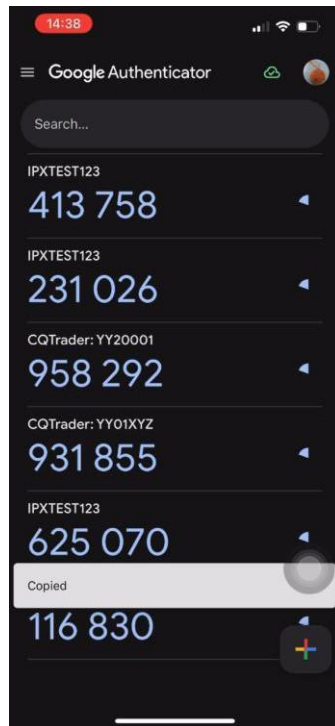


Step 7: Once Installation successful, tap on QRCode/Copy the code line

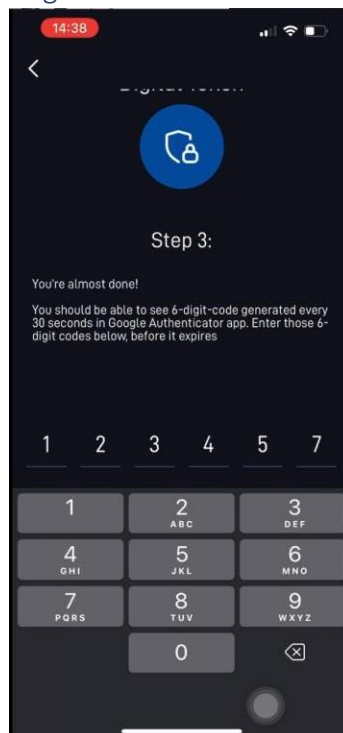


Step 8: Upon scanning, will redirect to Google Authenticator

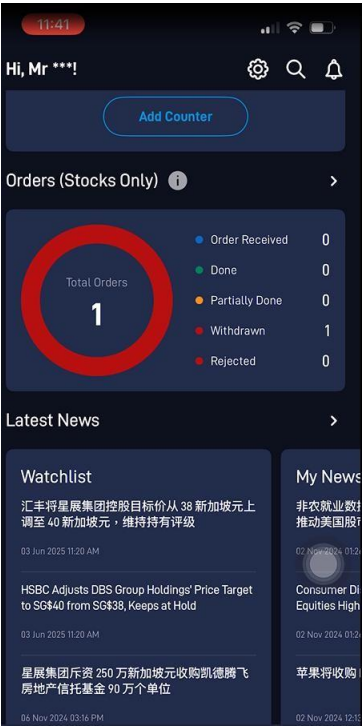
User will need to redirect to Google Authenticator, and may copy the OTP password



Step 9: Input/Paste the OTP from Google Authenticator



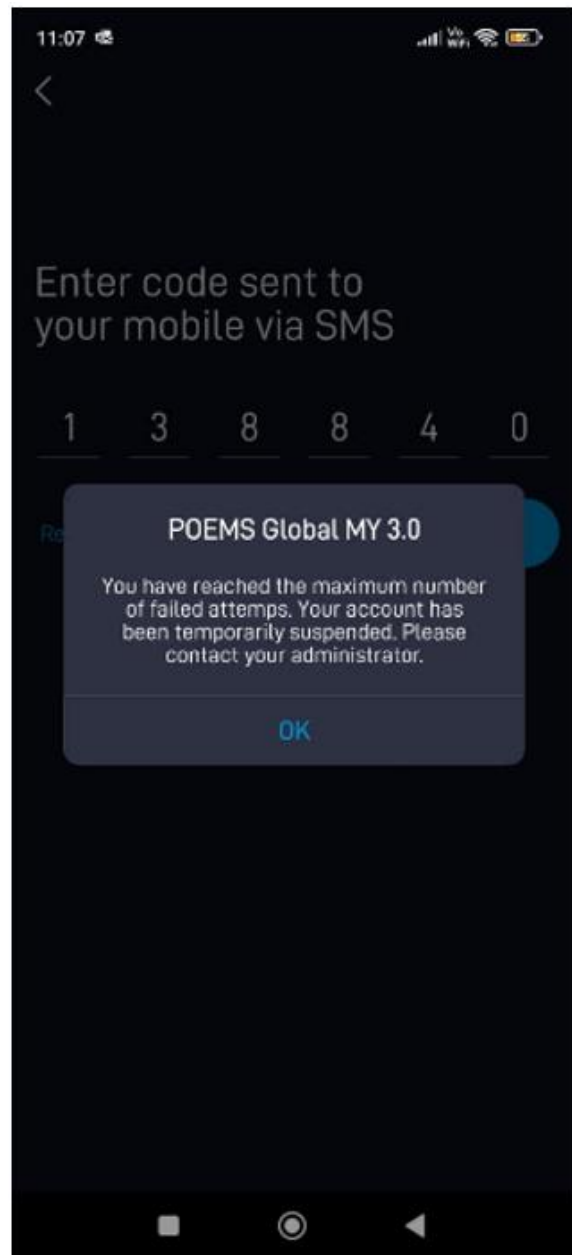
Step 10: Login Successful



FAQ

What happens after more than 4 incorrect SMS token attempts during verification for 2FA setup?

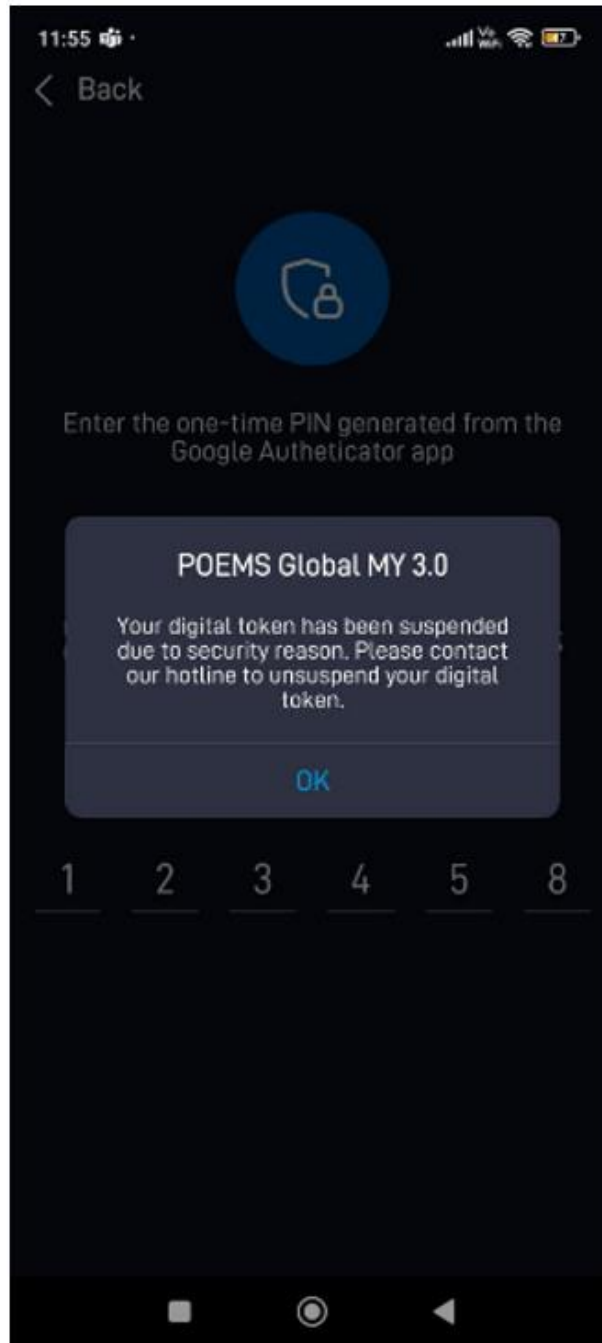
The user account will be suspended after more than 4 incorrect SMS token attempts during verification for the 2FA setup as displayed below.

**What can I do to unsuspend the account after 4 incorrect SMS token attempts during verification for 2FA setup?**

Please contact your Administrator / Hotline to unsuspend your account to proceed with the 2FA setup.

How many wrong attempts is allowed when you key in the Google Authenticator code after keying in your password?

On your 10th attempt keying in the wrong Google Authenticator code, your digital token will be suspended.



What can I do to unsuspend the digital token after 10 incorrect Google Authenticator code attempts?

Please contact your Administrator / Hotline to unsuspend your digital token. After unsuspend, you can proceed to login with the Google Authenticator code

What should I do in the event that even when I input the correct Google Authenticator code from Google Authenticator apps, but error message “Invalid OTP” appear?

Please first ensure that “Date & Time” and “Time Zone” on your phone has been set automatically and correctly to Malaysia time zone. After the done setting the “Date & Time” and “Time Zone” correctly, please try to key-in the Google Authenticator code again in our POEMS Apps.

This page is intentionally left blank