



PSW
PAKISTAN SINGLE WINDOW



USER MANUAL FOR MULTIFACTOR AUTHENTICATION

Confidential Information:

The information provided in this document is intended solely for the use of PSW. The contents of this document may not be reproduced or divulged outside the intended organizations without the express written permission of PSW.



TABLE OF CONTENTS

1. Introduction	3
2. Background.....	4
3. Salient Features of Multi-Factor Authentication Feature	5
4. System Requirements	5
5. Step by Step Business Process	6
5.1 User Login.....	6
5.2 Activation of Multi-Factor Authentication	7
5.3 Login with Authentication Code	9
5.4 Adding Trusted Device	13
6. Installation of Authenticator Application	15
6.1 Authenticator Application.....	15
6.2 Adding Account.....	16
7. Contact Information.....	20



1. Introduction

Pakistan Single Window (PSW) is an electronic portal that allows parties involved in cross border trade and transport to lodge standardized information and documents using a single-entry point to fulfill all import, export, and transit related regulatory requirements. The information is transmitted electronically and individual data elements for clearance and regulatory approvals need only to be submitted once. Use of the PSW portal is allowed to authorize users who have completed the subscription process. Once subscribed and registered with PSW, you can access the PSW to perform cross border trade and transit related activities including online payment of taxes and Other Government Agencies (OGA) fees.

The PSW aims to simplify your cross-border trade and transport experience. This new platform will facilitate the traders to apply for the Export Permit from the Drug Regulatory Authority of Pakistan (DRAP). The application for the same shall be received and processed through the PSW portal. Similarly, the sharing of messages and documents required for processing of regulatory approval requests shall be enabled by the PSW.

This new platform will automate all trade-related business processes of DRAP (phase-wise), including registrations. With the PSW system going live, there will be no DRAP office visits and manual submission of applications for the issuance of regulatory approvals. The processing of the application will be done online, where you can have a clear visibility of the action being performed on the same.



2. Background

Background As a signatory to the WTO's Trade Facilitation Agreement (2015), Pakistan has notified the establishment of a 'National Single Window' (NSW) as a 'Category C' commitment with effect from 22nd February 2017. To implement NSW the Government of Pakistan has promulgated the Pakistan Single Window Act, 2021 while declaring Pakistan Customs as the Lead Agency. Pakistan Customs has established a dedicated PSW Company (PSWC), as a not-for-profit Company under the Companies Act, 2017, to implement the PSW program. The PSWC has been designated as the Operating Entity under the PSW Act for developing and maintaining the PSW portal in collaboration with 77 different public sector entities involved in the regulation of cross border trade in Pakistan. The PSWC will digitize the processes of public sector entities, related to the regulation of international trade. This will not only reduce the time and costs but also increase compliance and immensely benefit economic operators like importers, exporters, freight forwarders, clearing agents, shipping companies, transporters, etc. The implementation of the PSW program will also enhance government controls and transparency. By creating a national electronic trade and logistics platform the PSW will help Pakistan integrate better into the regional and global single window systems. It will facilitate integration into global value chains and enable Pakistan to become a hub for regional and international transit and trade.



3. Salient Features of Multi-Factor Authentication Feature

- A robust security solution that adds an additional layer of authentication to safeguard user access to the PSW system.
- It ensures secure login by verifying user identity through multiple authentication factors, reducing the risk of unauthorized access.
- The configurable MFA management framework will enable users, enforce security controls, and monitor system access in line with approved security standards.
- User verification prompts and authentication alerts will be delivered to ensure secure and timely access confirmation.

4. System Requirements

- To use PSW Portal on Windows®, the subscriber will require:
 - a. Google Chrome Browser.
 - b. Windows 7, Windows 8, Windows 8.1, Windows 10 or later
 - c. An Intel Pentium 4 processor or later that's SSE3 capable.
- To use PSW Portal on Mac®, the subscriber will need:
 - d. Google Chrome Browser
 - e. OS X El Capital 10.11 or later.



5. Step by Step Business Process

5.1 User Login

- i. Please visit "www.psw.gov.pk" and click on the 'Login' button.

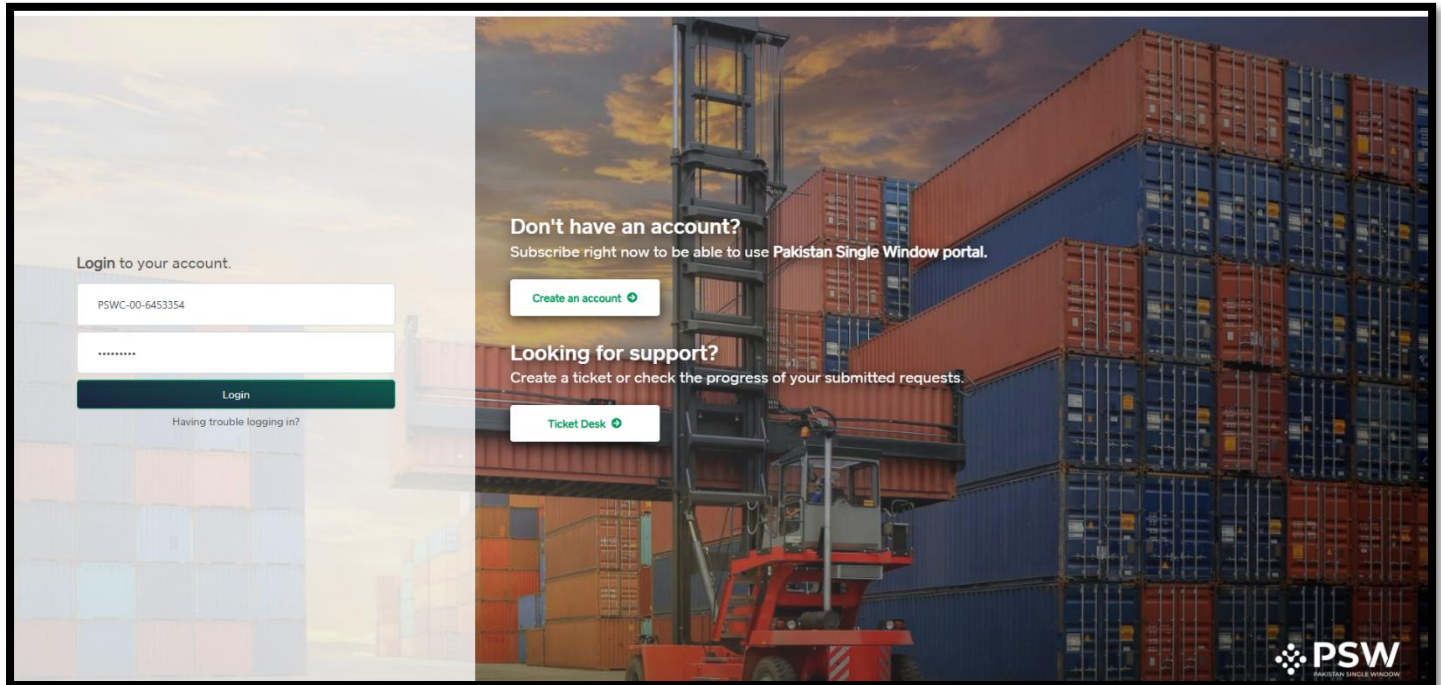


Figure 1

- ii. Multi-factor Authentication (MFA) is required pop-up will appear. To setup MFA, User shall click on 'Continue' button.

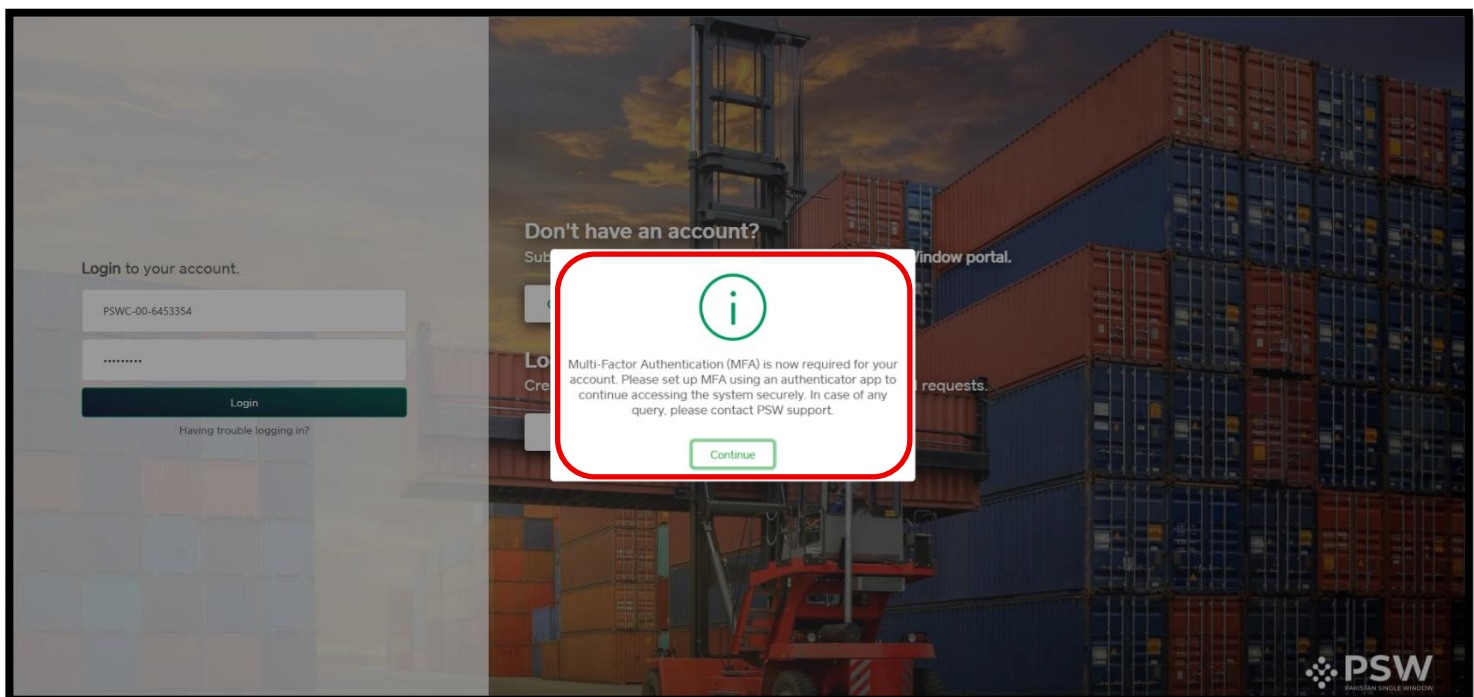


Figure 2



5.2 Activation of Multi-Factor Authentication

- i. MFA definition and the instructions will appear. User shall open the Authentication App (e.g Google Authenticator, Microsoft Authenticator) on your phone, Scan the code displayed at the screen. Enter the 6-digit code appears on the authentication app.

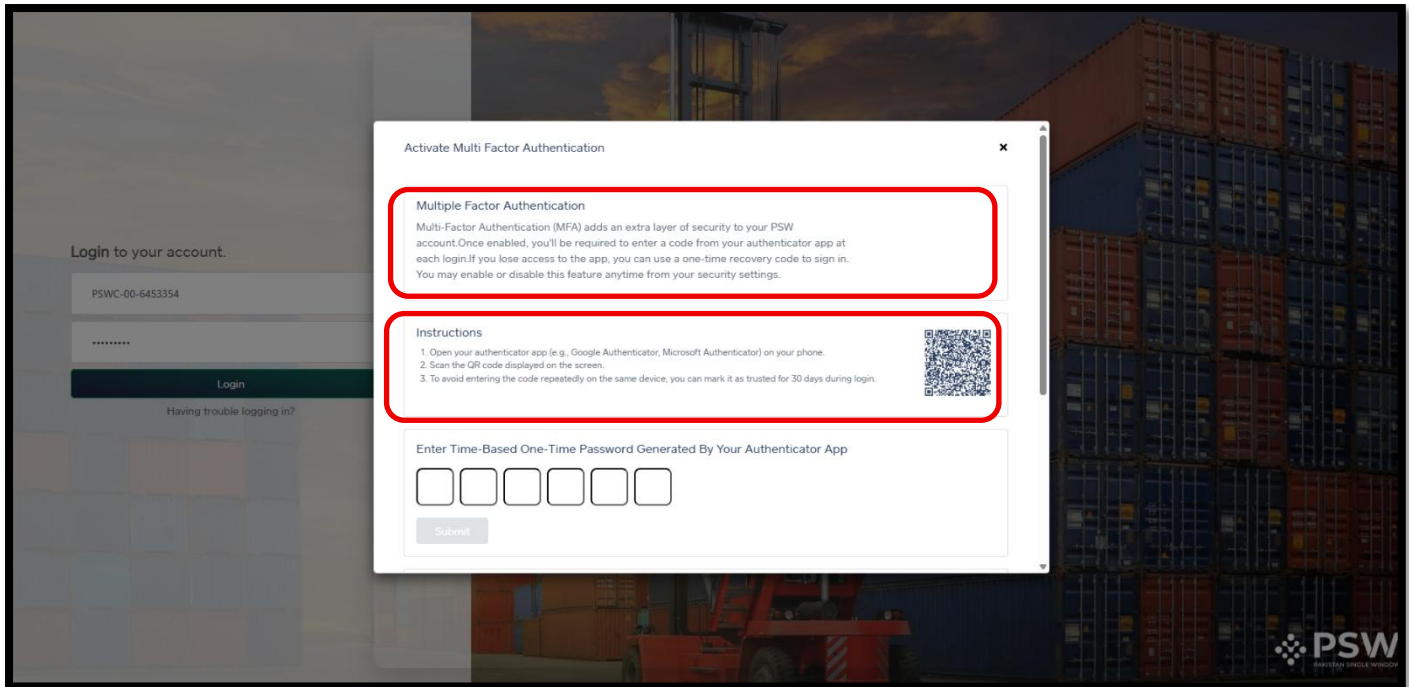


Figure 3

P.S To avoid entering the code repeatedly on the same device, User can mark it as trusted device, it will allow User to login on the same device for next 30 days

- ii. After entering the code, User shall press 'Submit' button to proceed further.

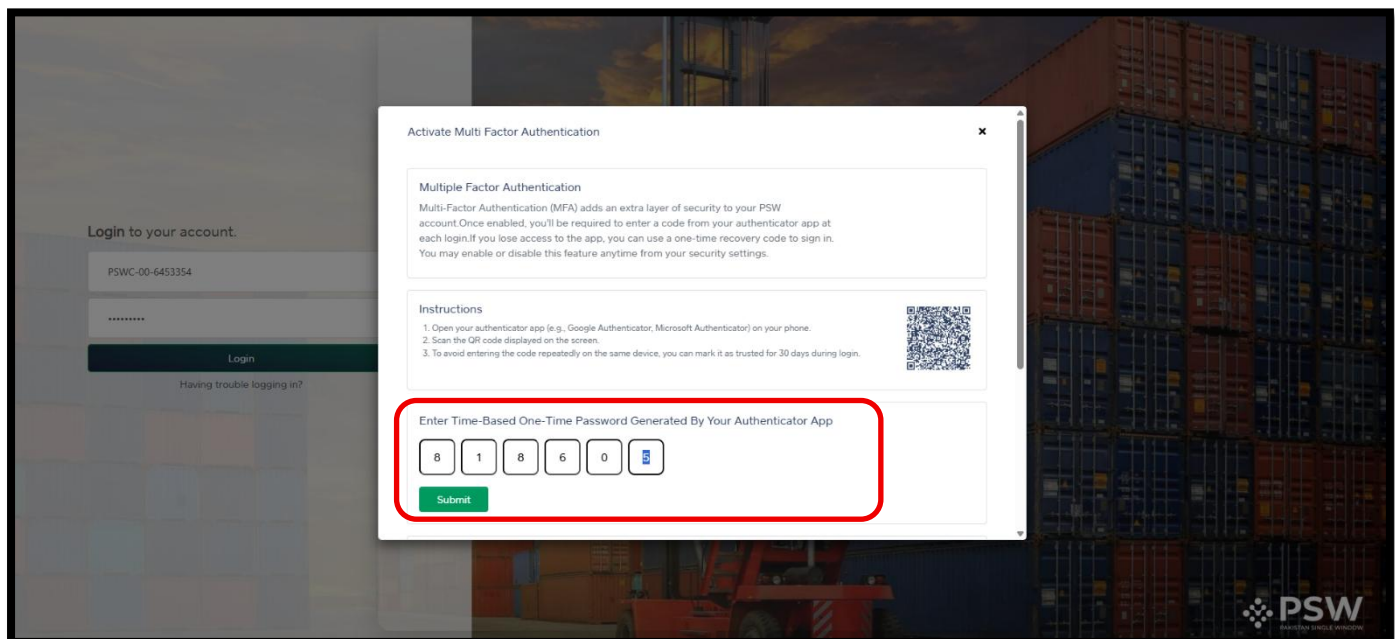


Figure 4



- iii. Upon scroll down list of recovery codes will appear; User shall press the 'Copy Code' button and save the codes on the safe and secure sheet. These one-time recovery codes can be used if you lose access to your authenticator app – each code can be used only once; a new set of codes can be generated by clicking on 'Regenerate Codes'.

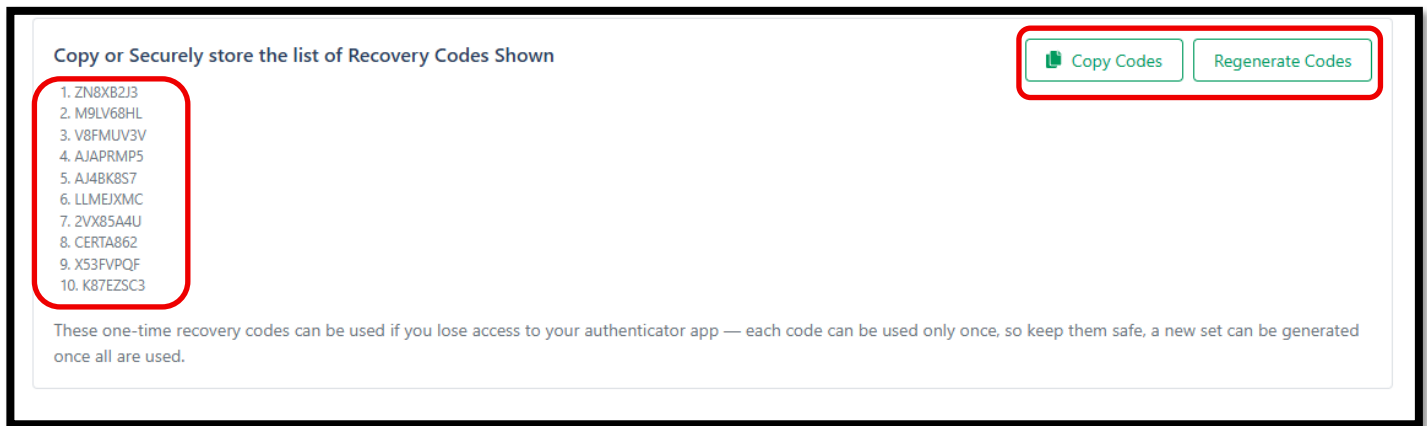


Figure 5

- iv. 'Multi-Factor Authentication (MFA) configured successfully' message will appear. User shall click 'Continue' button.

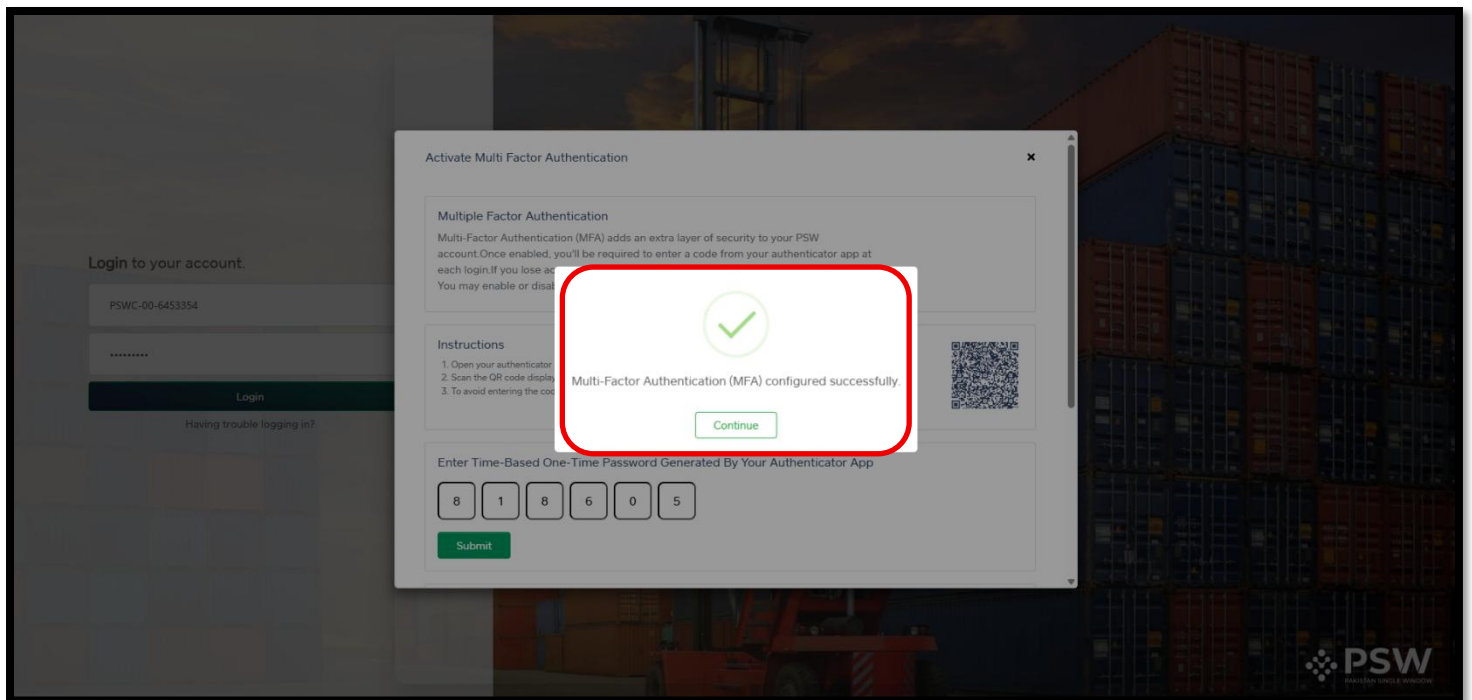


Figure 6



5.3 Login with Authentication Code

- i. User shall login with his ID and Password and click on the 'Login' button.

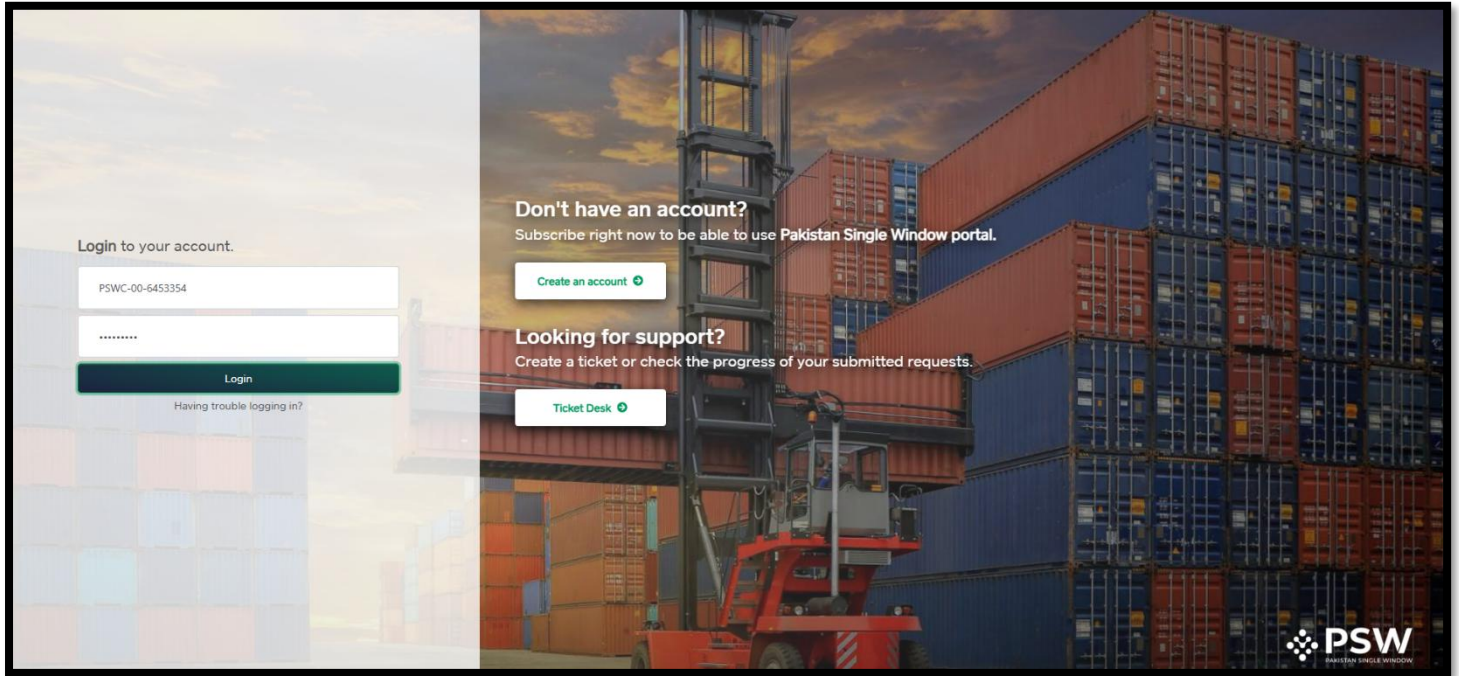


Figure 7

- ii. User shall enter 6-digit code appear on the authenticator app.

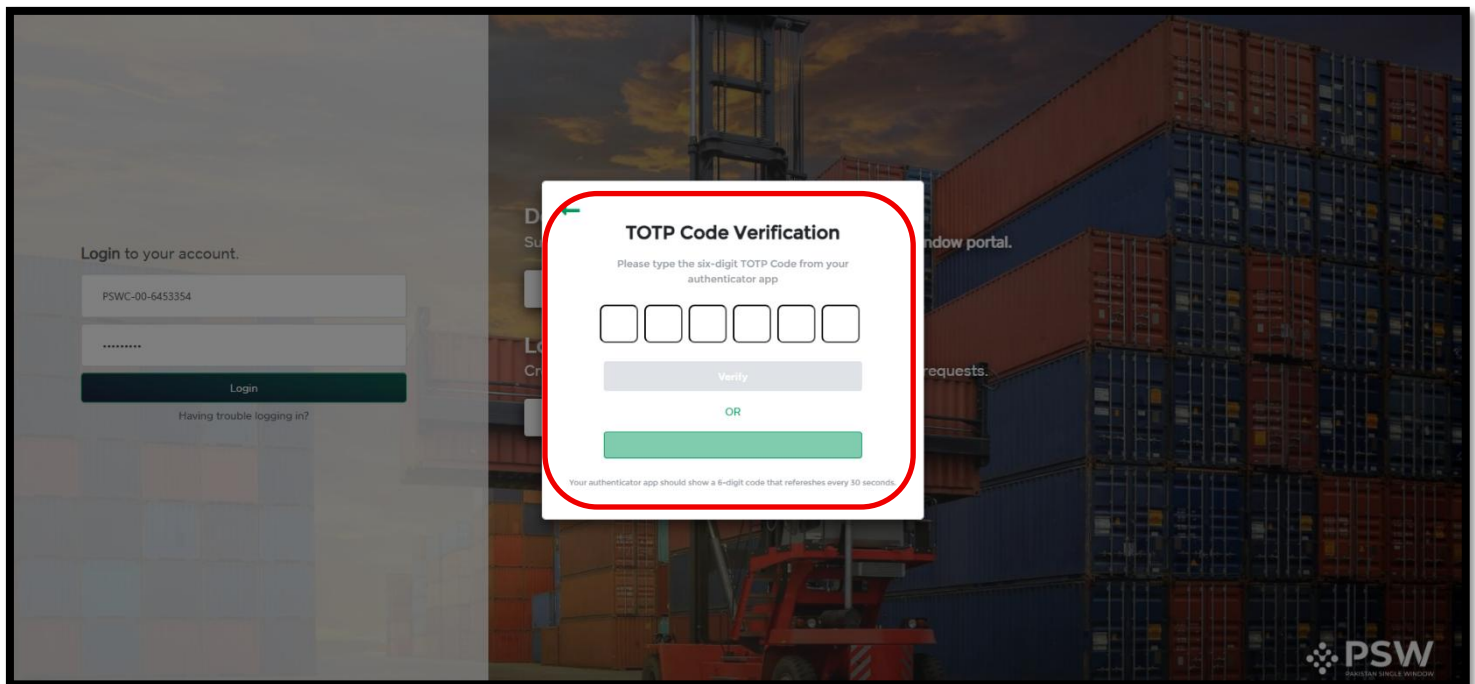


Figure 8



- iii. User shall enter TOTP verification code, appear on the authenticator app and click on 'Verify' button.²

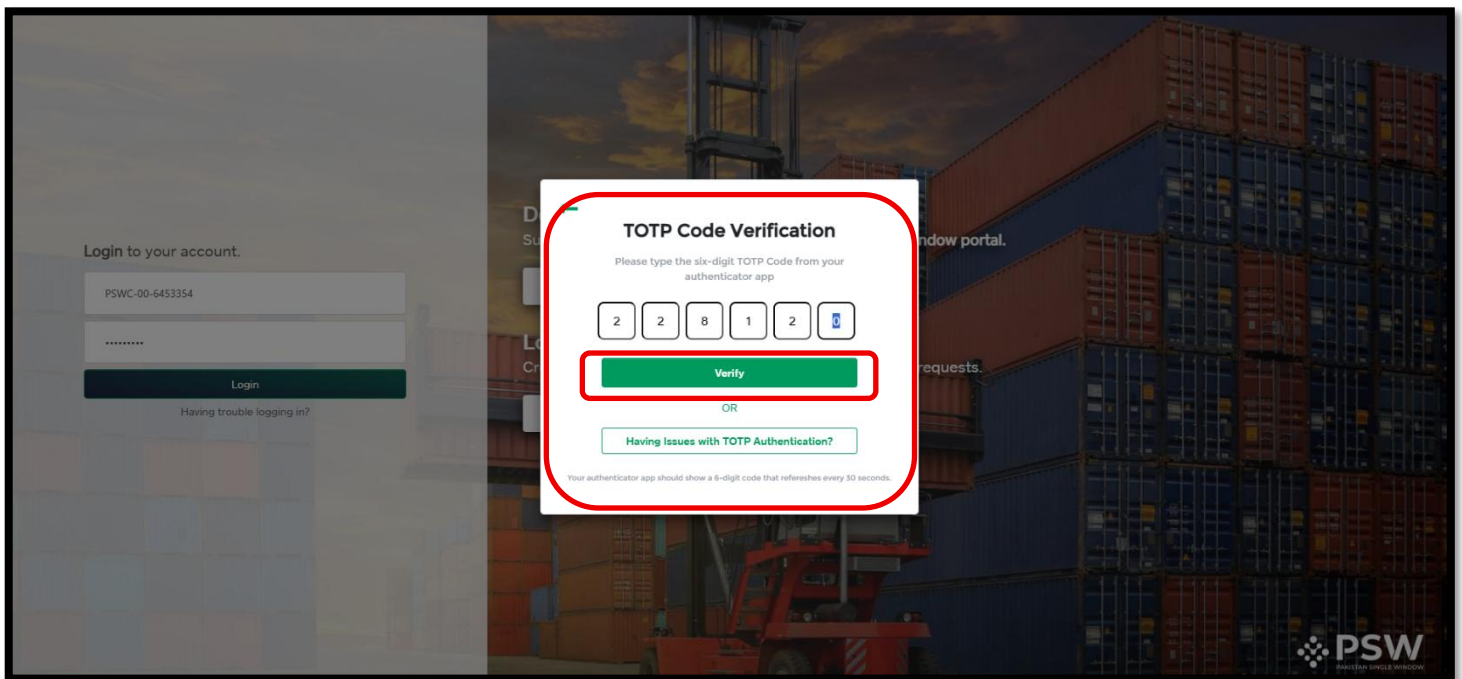


Figure 9

- iv. If the user facing difficulty in getting TOTP Code, User shall click on 'Having Issues with TOTP Authentication' tab.

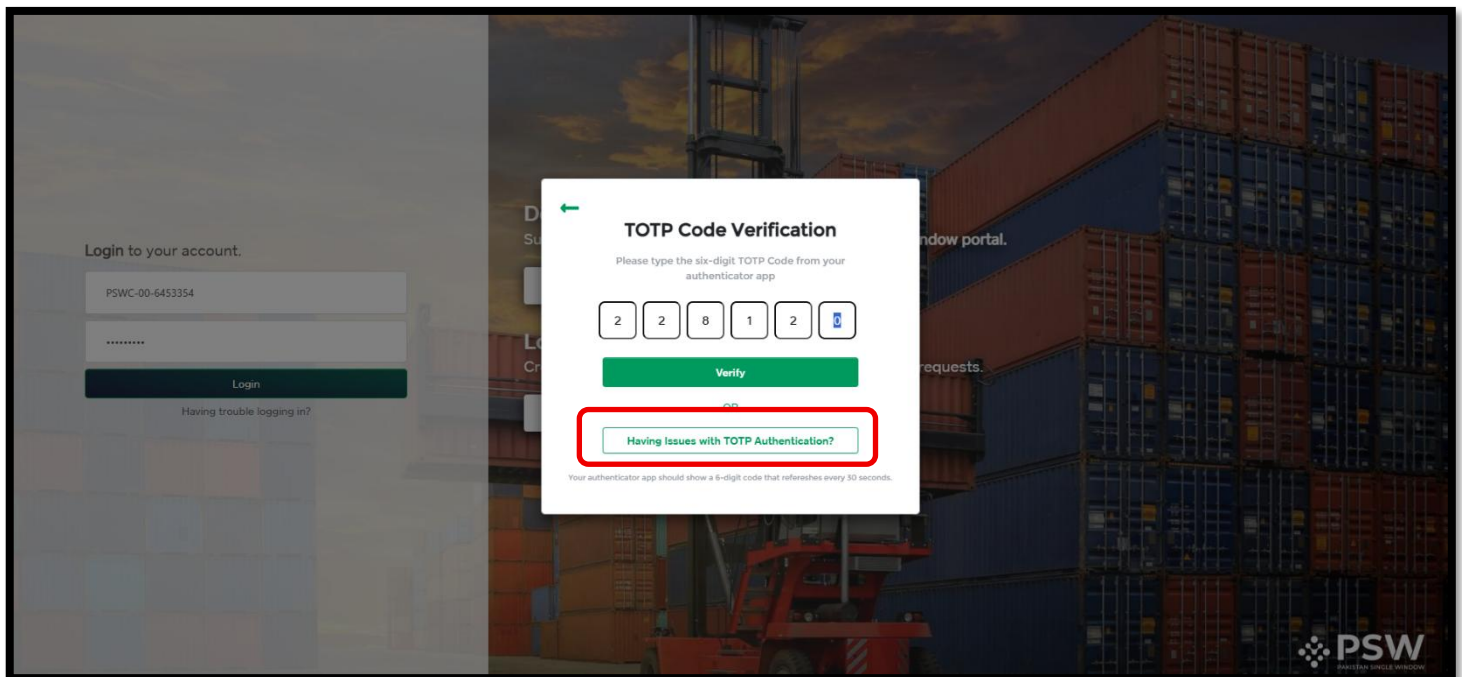


Figure 10



- v. Here User will have option to login with Recovery Code or User can select 'Receive OTP via SMS & Email'. Then click on continue button.

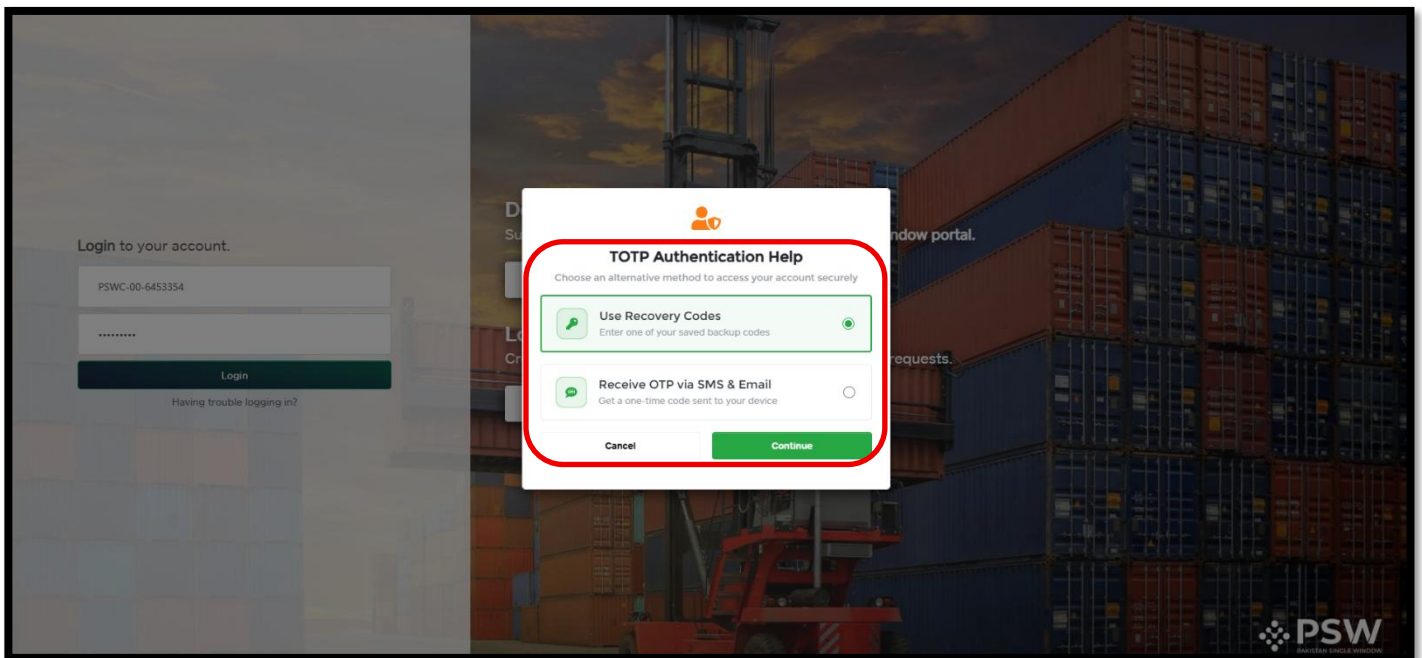


Figure 11

- vi. User shall enter verification codes receive on SMS & Email and click on 'Verify' button.

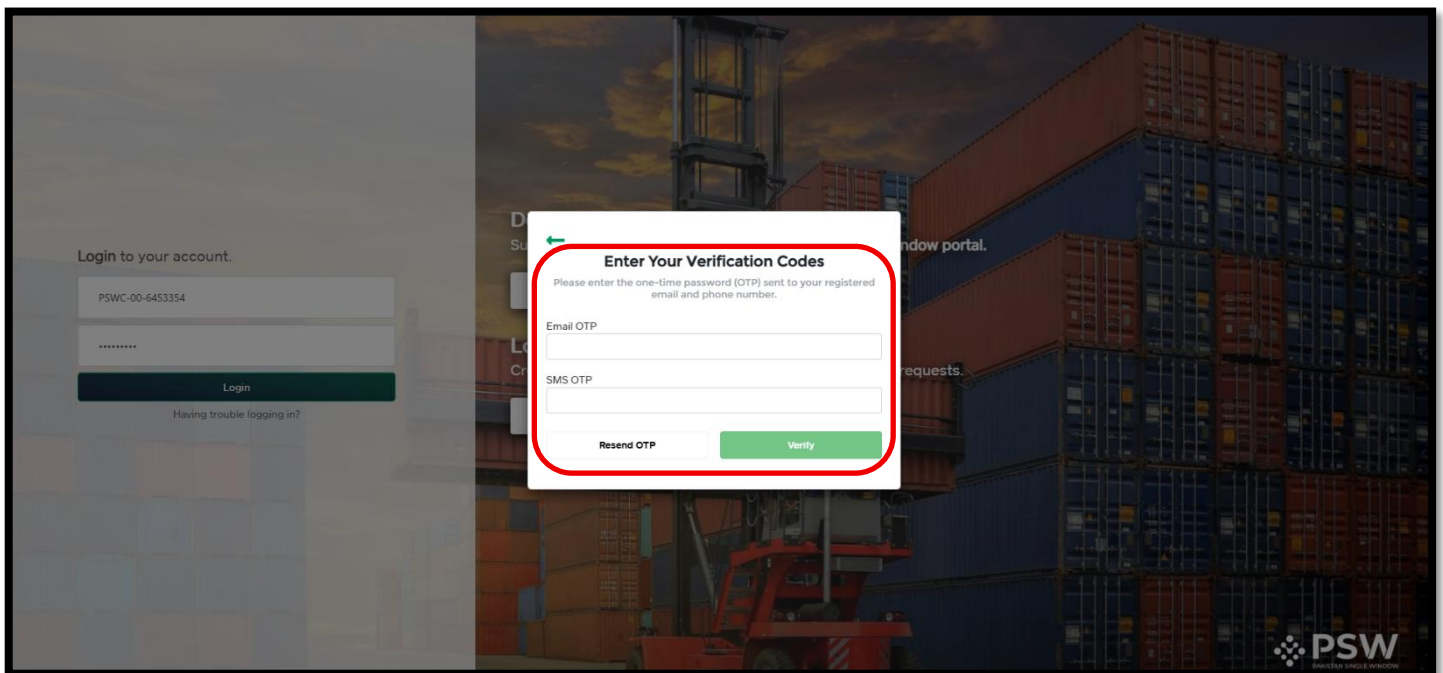


Figure 12



- vii. Upon verification, TOTP code will generate the authenticator app, User shall enter the 6-digit code and click on verify button.

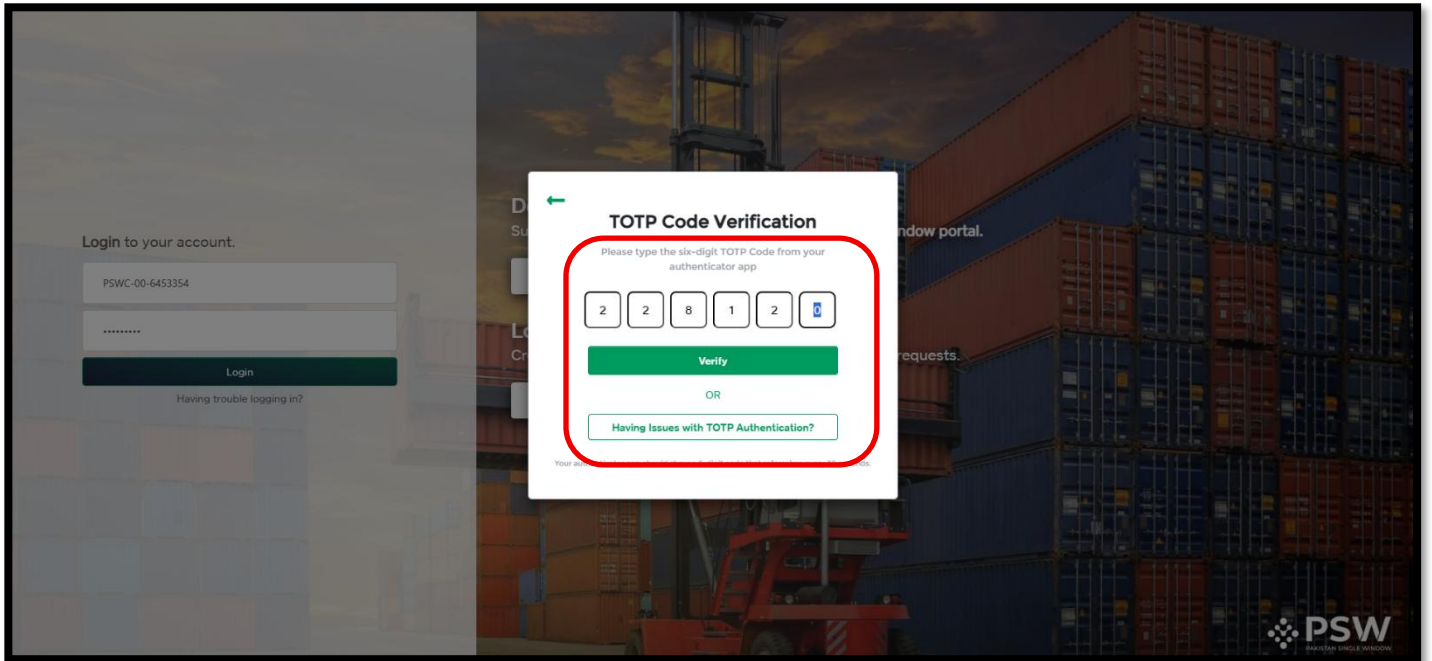


Figure 13

5.4 Adding Trusted Device

- i. After entering TOTP, User shall be able to login in the system, a pop-up will appear on the right corner of the screen showing 'Make your device Trusted for 30 Days'. Upon clicking 'Yes', the device will be added as an trusted device and User will be able to login with his/her credential without TOTP

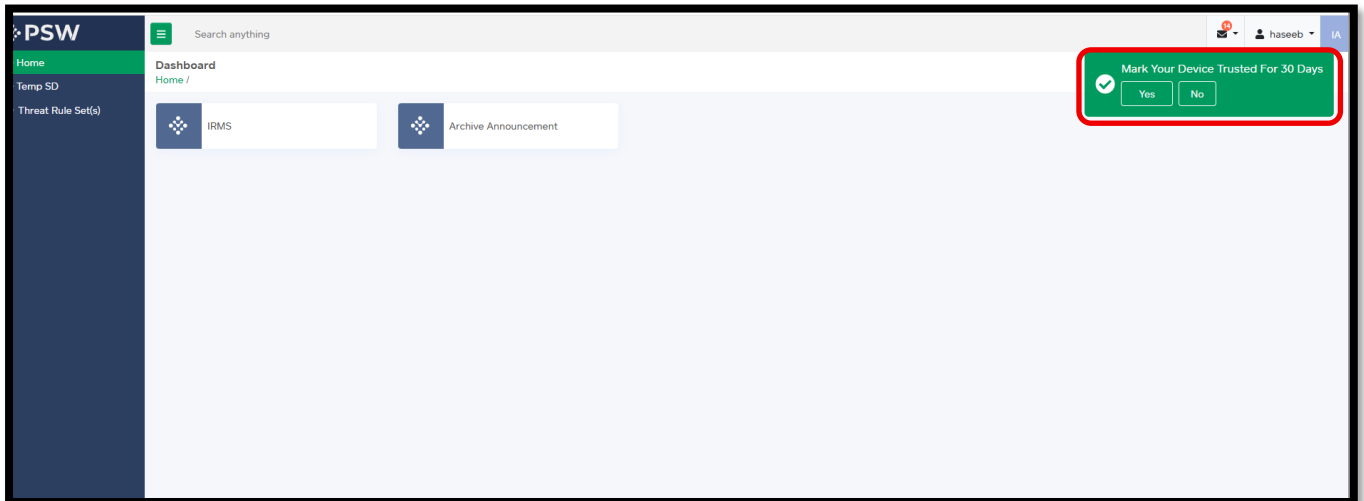


Figure 14

- ii. Upon login, User shall click on the username on the top right corner of the screen and select 'Security Setting'.

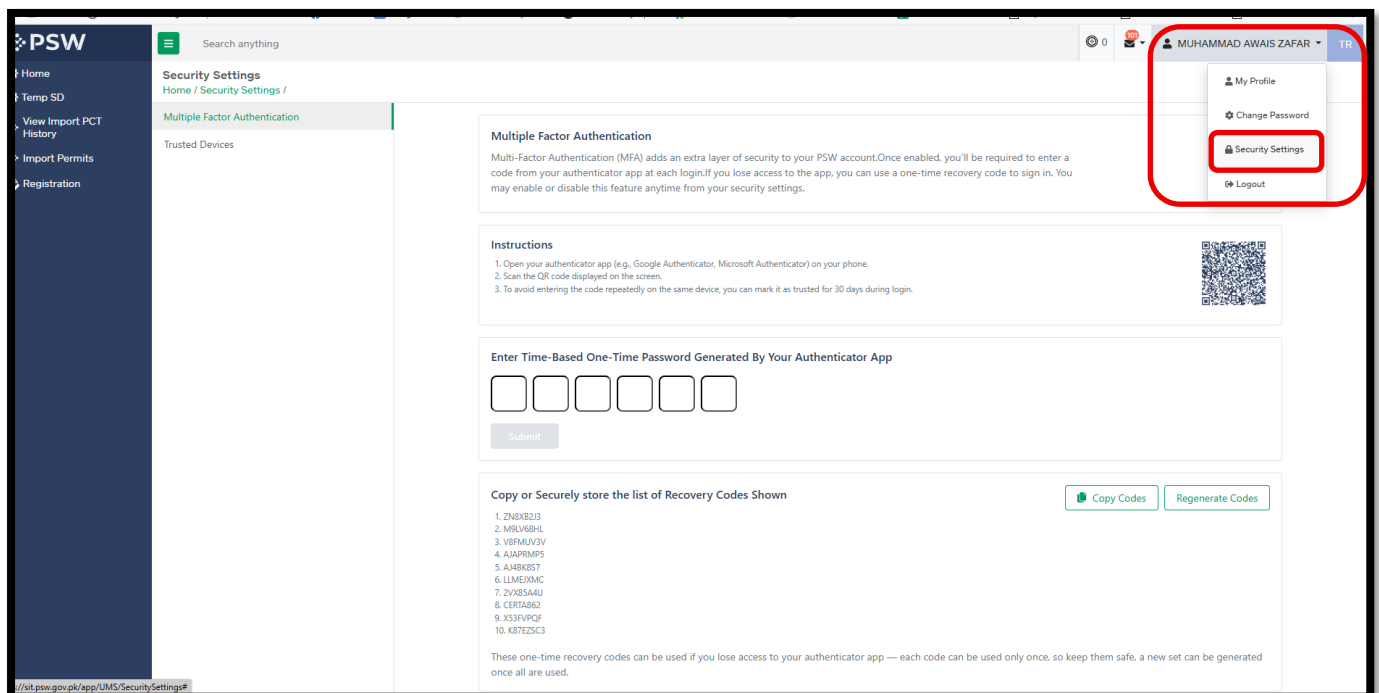


Figure 15



- iii. User shall click on 'Trusted Device' and the detail of the trusted device will be shown.

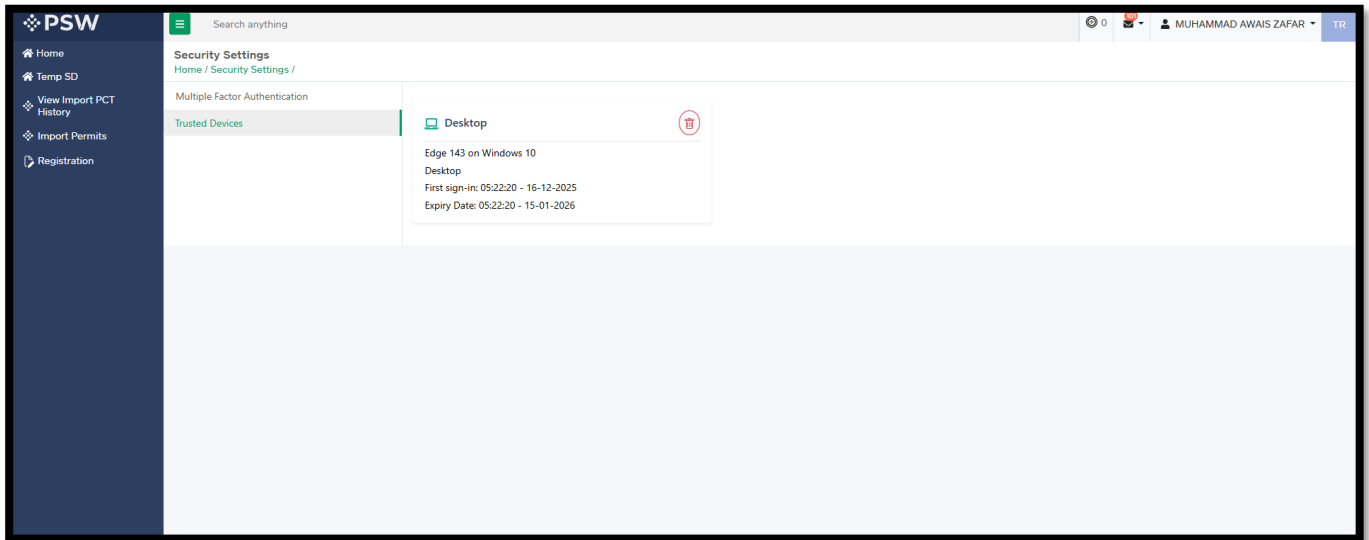


Figure 16



6. Installation of Authenticator Application

6.1 Authenticator Application

i. Choose one of the following apps (both work the same way):

- **Google Authenticator**
- **Microsoft Authenticator**

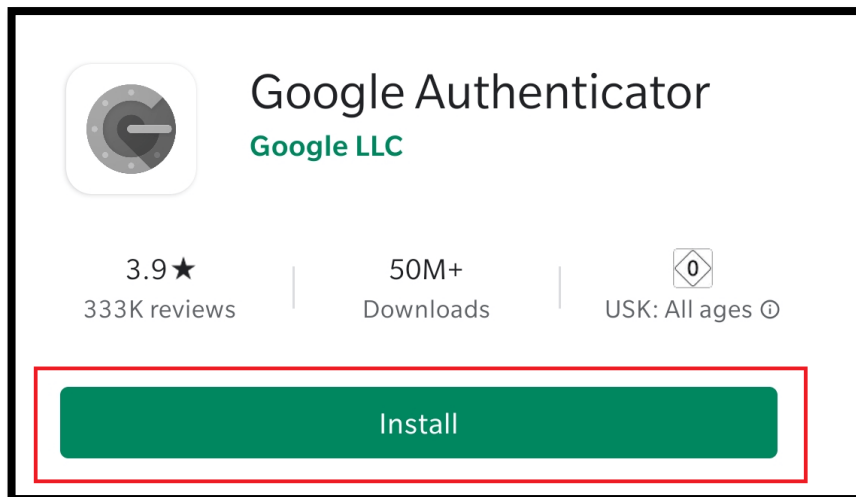


Figure 17

ii. Open Authentication App, press skip on the top right corner.

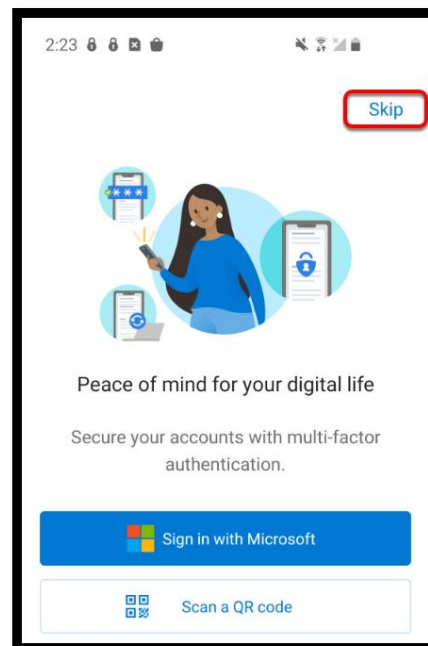


Figure 18



6.2 Adding Account

- i. User shall click on the '+' sign available at the right bottom of the application.

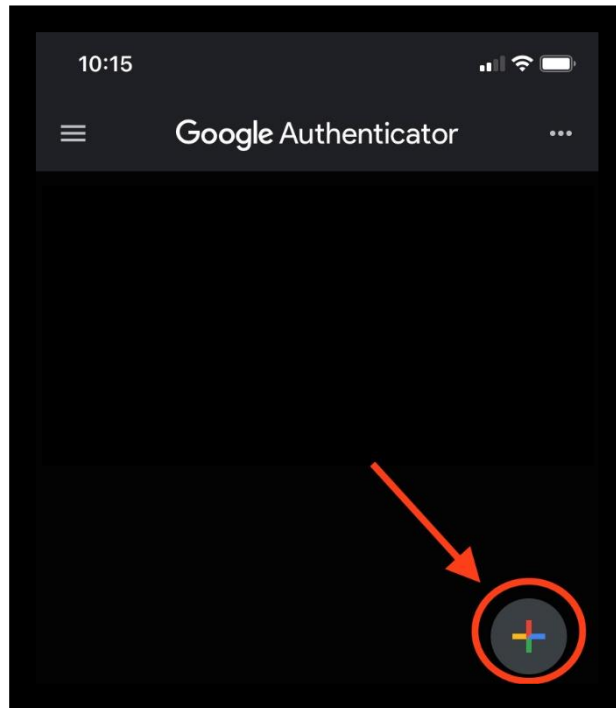


Figure 19

- ii. For Microsoft Authenticator '+' sign or add account

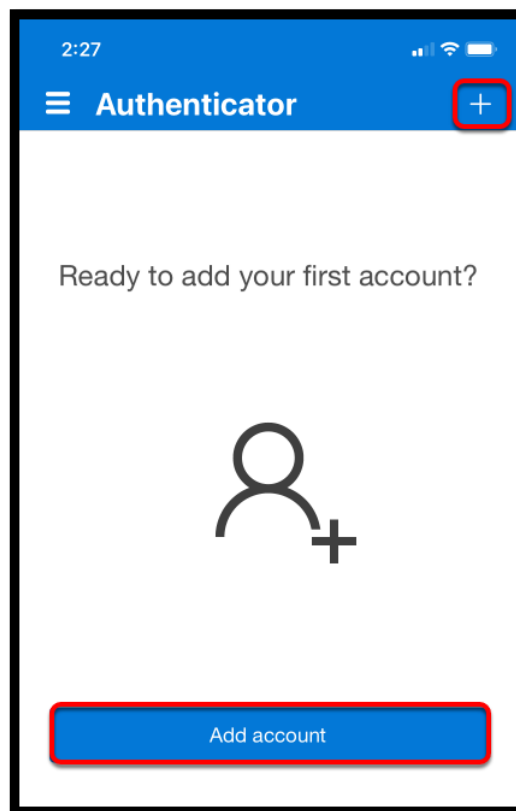


Figure 20



- iii. Select 'Scan a QR Code', choose **Enter a Setup Key Manually** only if QR code is not available.

Set up 2-factor authentication

1. Scan the QR code with an authenticator app ⓘ

Unable to scan?

2. Enter the one-time code provided by your authenticator app

One-time code

One-time code

Submit

Figure 21

- iv. Log in to the system/portal where 2FA is required
 - 1. Go to **Security / Two-Factor Authentication**
 - 2. Click **Enable Authenticator App**
 - 3. A **QR code** will appear on the screen

TWO-FACTOR AUTHENTICATION (2FA)

SETUP TWO-FACTOR AUTHENTICATION

1. Install the Google Authenticator app on your phone.

2. Scan the QR code below with your app.

3. Enter the 6-digit Google Authenticator code from the app once the scan is complete.

###-###

ENABLE 2FA CANCEL

Figure 22



- v. Select 'Scan the QR Code' and point the camera towards the QR appearing on the laptop/Computer screen. The account will be added automatically. A 6-digit code will appear and refresh after every 30 seconds. After entering the code click on 'Verify/Confirm'. Two-factor authentication will be successfully enabled.

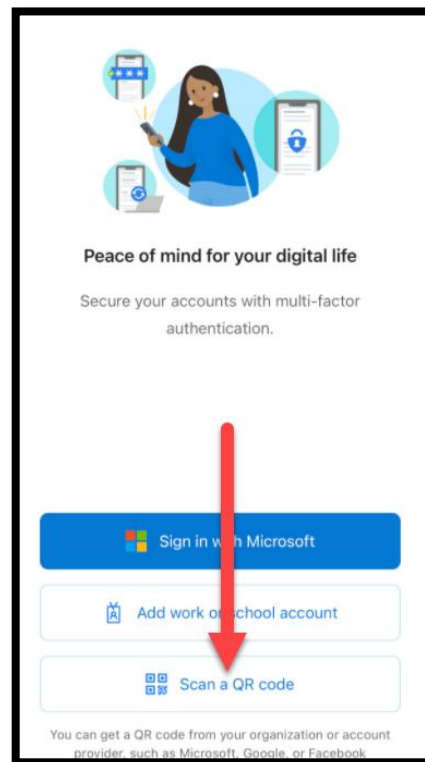


Figure 23

- vi. Save backup codes, The system may show **backup/recovery codes**. **Save or download** them securely. These codes help if: Phone is lost, App is deleted, Device is changed

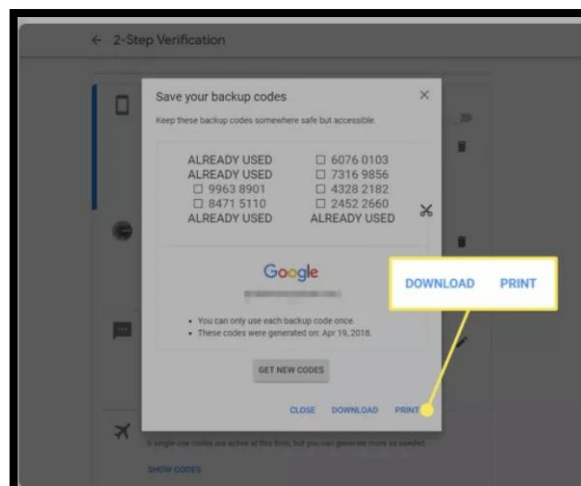




Figure 24

- viii. Enter username and password, open the authenticator app. Enter the current 6-digit code and you will be able to login to the system.

Log in using your authenticator app

To continue, please enter the 6-digit verification code generated by your authenticator app.

-

⚠ Incorrect verification code.

[Continue](#)

[Sign in another way](#)

Figure 25

Two-Factor authentication

Enter the 6-digit code generated by your app to confirm your action.

[Verify](#)

Can't find your device? [Use backup code.](#)

[Return to site](#)

Figure 26



7. Contact Information

If you require any assistance, please feel

free to contact us as:

Email: support@psw.gov.pk

Phone: 021-111-111-779



+92-51-9245605



info@psw.gov.pk



www.psw.gov.pk