FIAU Financial Intelligence Analysis Unit Malta

CASPAR: Two-Factor Authentication (2FA) End-User Guide

November 2025

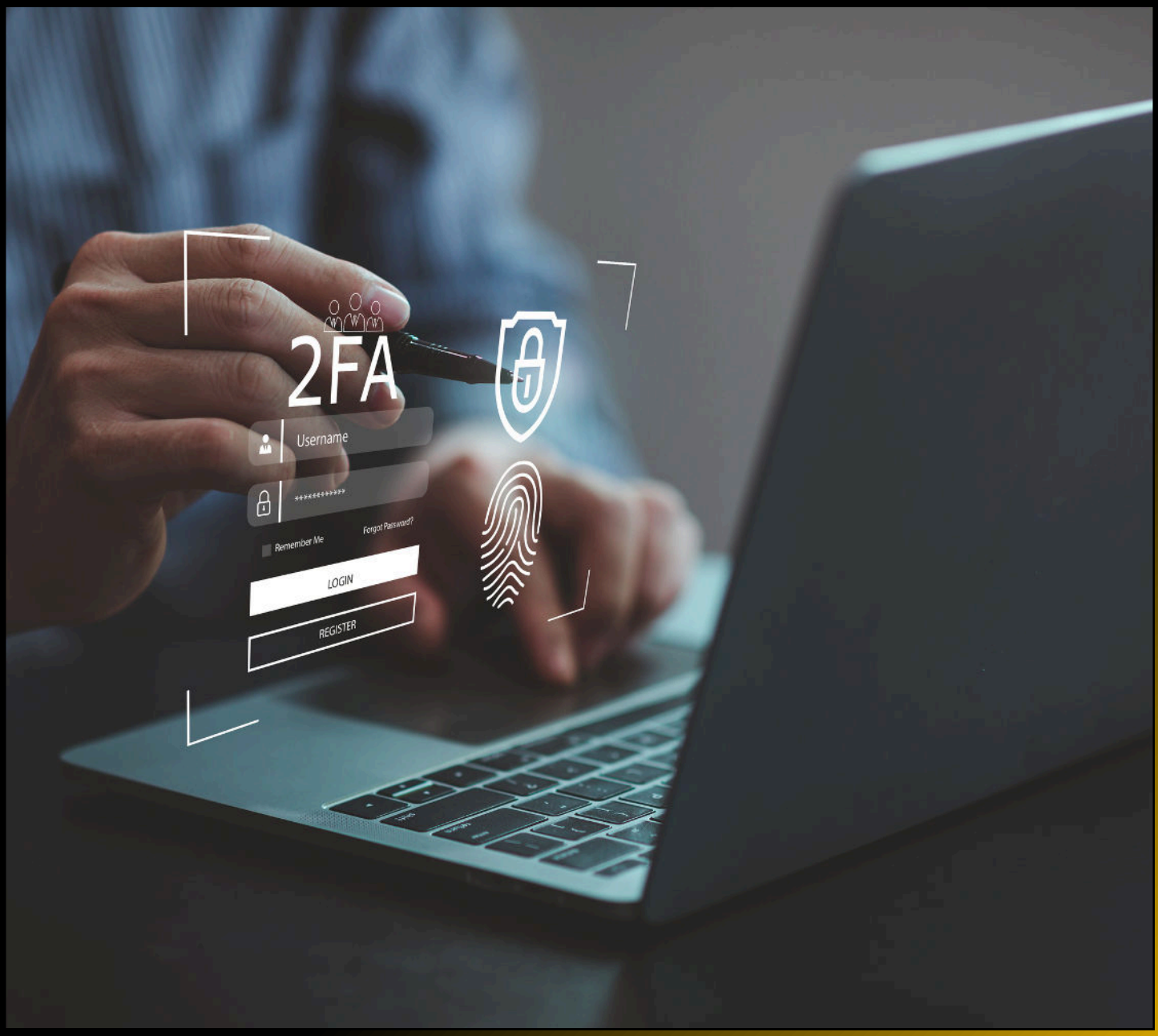


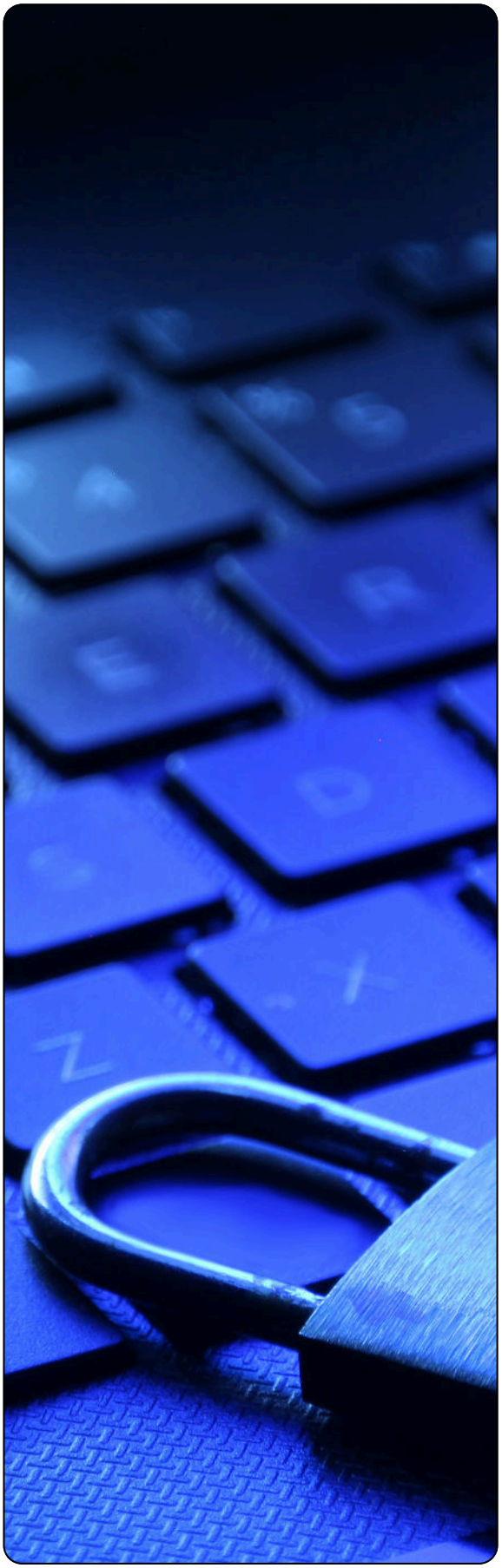
Table Of Contents

Overview

Two-Factor Authentication (2FA) adds an extra layer of security to your account by requiring two forms of verification:

1. Your password.
2. Time-based, one-time passcode generated by an application.

Even if your password is compromised, 2FA helps ensure that only you can access your account.



How It Works

When 2FA is enabled, accessing your account involves two steps:

1. Entering your username and password as usual.
2. Entering a verification code, which can be:
    - Generated by an authenticator app on your mobile device (Time-based One-Time Password or TOTP).

Each time you log in, a new, unique code is required, ensuring enhanced protection against unauthorised access.

Benefits

Enhanced Security:
Prevents unauthorised access, even if your password is stolen.

Protection Against Phishing:
Reduces the risk of credential-based attacks.

User-Friendly:
Simple to set up and quick to use daily.

Requirements

Before enabling 2FA, ensure the following:

- You have access to a mobile device (smartphone or tablet).
- You have downloaded and installed an authenticator app that supports TOTP (Time-based One-Time Password).

Recommended Authenticator Apps

You can download any of the following free authenticator apps from the Google Play Store (Android) or the Apple App Store (iOS):

Authenticator App	Play Store Link	Apple App Store Link
Microsoft Authenticator	Download for Android	Download for iOS
Google Authenticator	Download for Android	Download for iOS

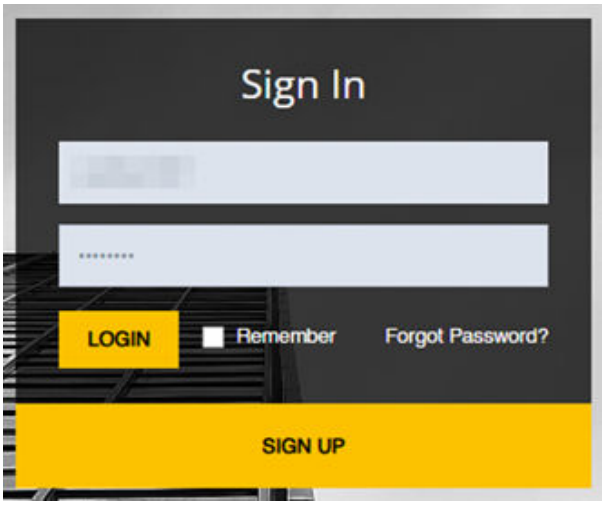
These apps generate a secure, rotating six-digit code that you will use as your second step during login.

Setup Instructions

One time set up

To enable Two-Factor Authentication (2FA) for your account, follow these steps:

Step 1: Log in to your account using your **username and password**.

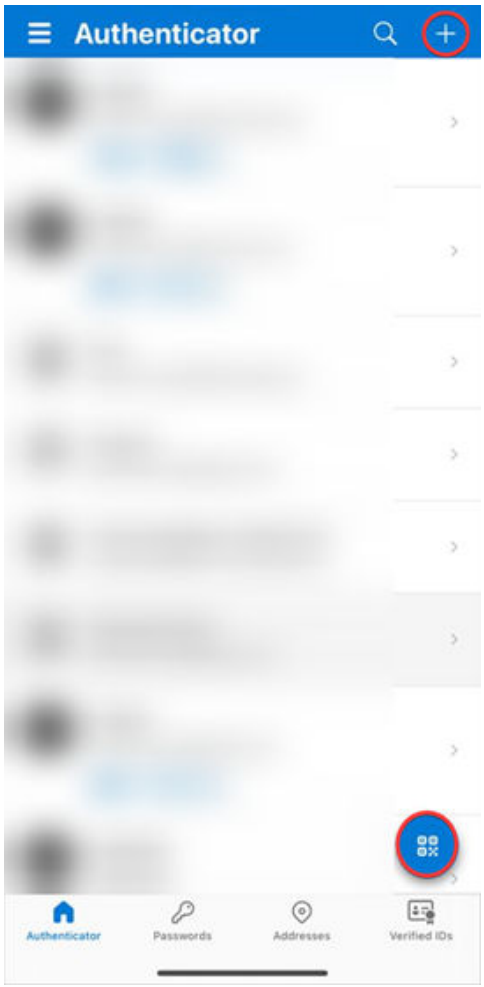


Step 2: After successful login, you will be redirected to a page displaying a **QR code** for 2FA setup.

Step 3: On your mobile device, **open your chosen authenticator app** (e.g., Microsoft Authenticator, or Google Authenticator).

Step 4: In the app, choose **"Add Account"** or tap the **"+" icon**, then **scan the QR code** shown on your screen *(in step 3)*.

- This step links your account to the authenticator app by securely sharing a secret key.

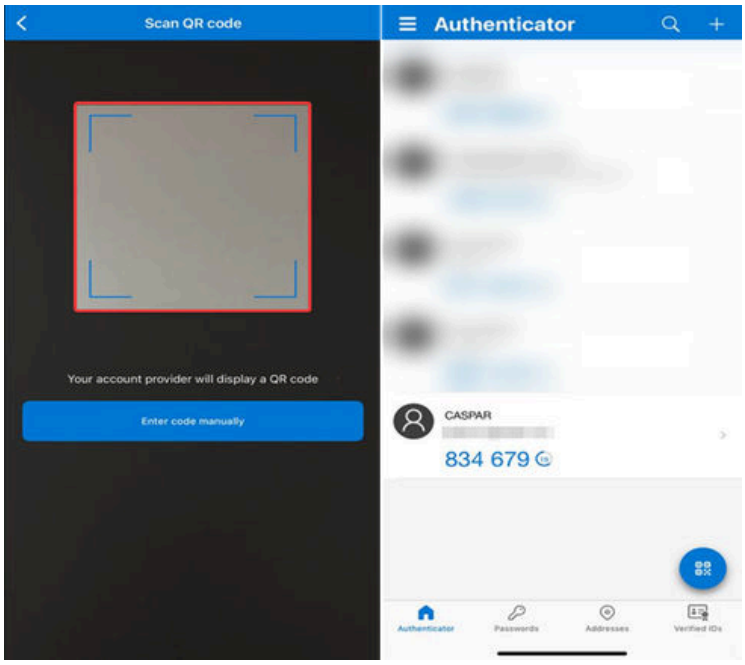


Important Note: When using a single account as a shared group email, all team members must scan the QR code *together* during the initial setup.

This ensures that the same six-digit authentication code - generated from the shared QR code - can be used across multiple devices (e.g., each team member's personal device).

This allows the code to be registered and accessed by everyone in the team.

Step 5: Once scanned, the app will generate a **6-digit time-based code** for your account.



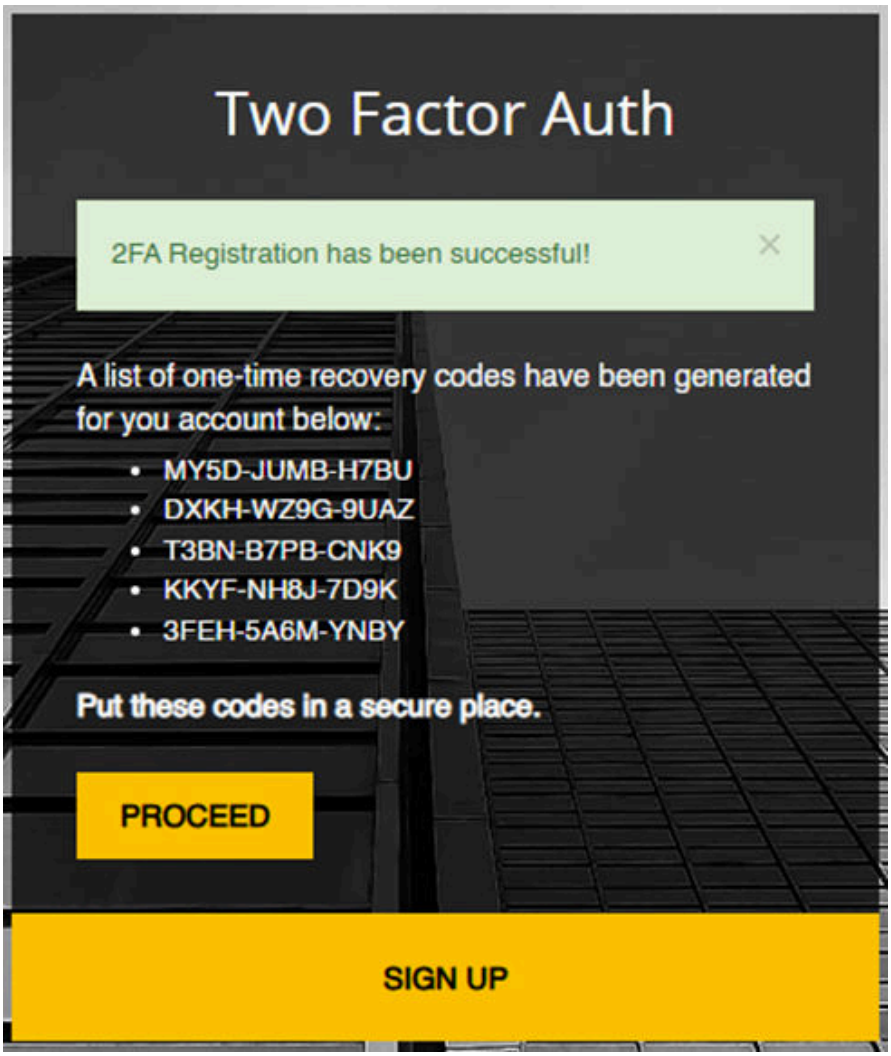
Step 6: Enter the **6-digit code** displayed in the app into the field below the QR code on the website and click **"Validate 2FA"** to complete the 2FA setup process.

Once set up, every login attempt will require the 2FA code in addition to your password.

Step 7: Upon validating the Two-Factor Authentication (2FA) for the first time, **five recovery codes** are automatically generated. These codes are displayed once only during the initial QR code validation process.

Please ensure you securely note down these codes, as they are intended for one-time use only in case you do not have access to your 2FA application (e.g., due to device loss or app issues).

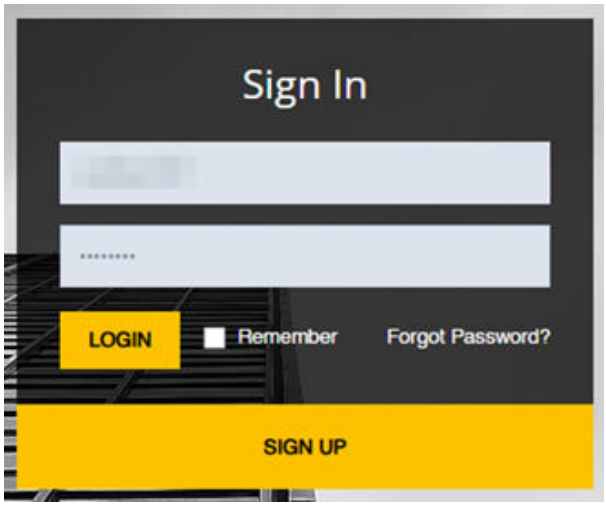
Failure to retain these codes will result in difficulty accessing your account without administrative assistance.



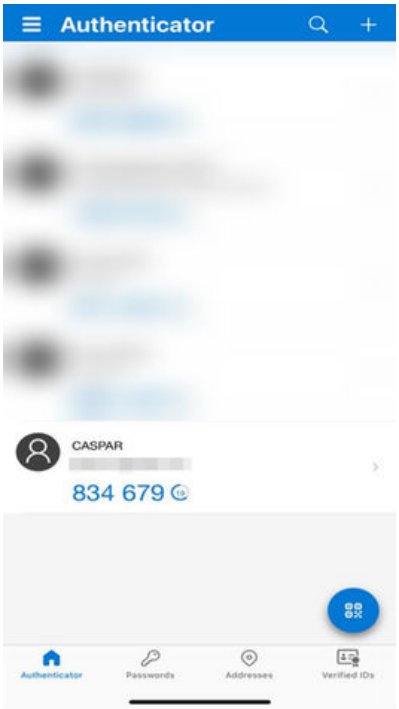
Logging In with Two-Factor Authentication (2FA)

Once 2FA is successfully set up:

Step 1: Log in using your username and password.



Step 2: You will be prompted to enter the **6-digit code** generated by your authenticator app.

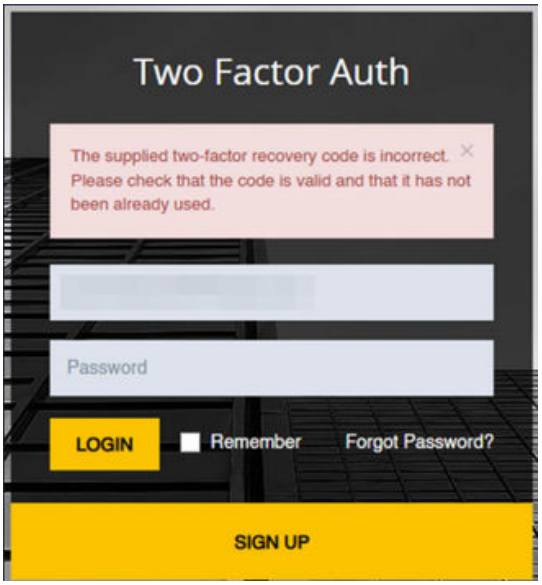


Step 3: When logging in, you will be prompted to enter a verification code after providing your username and password. At this stage, you have two options:

- **Option 1 – Using the 2FA Application:**
  - If you have access to your authenticator app, enter the **6-digit code** it generates to gain access to the system.

- **Option 2 – Using Recovery Codes:**
  - If you **do not** have access to the 2FA application (e.g., due to device loss or technical issues), you may use **one of the recovery codes (refer to point 7)** that were generated during the initial QR code setup.

Each recovery code is valid for **one-time use only.**



Once used, it cannot be reused. Please refer to the screenshot below for an example of how this is displayed.

Questions on this document may be sent to:
compliance@fiaumalta.org

Financial Intelligence Analysis Unit
Trident Park, No. 5, Triq l-Mdina,
Central Business District Birkirkara, CBD 2010

Telephone: (+356) 21 231 333
Fax: (+356) 21 231 090
E-mail: info@fiaumalta.org
Website: www.fiaumalta.org