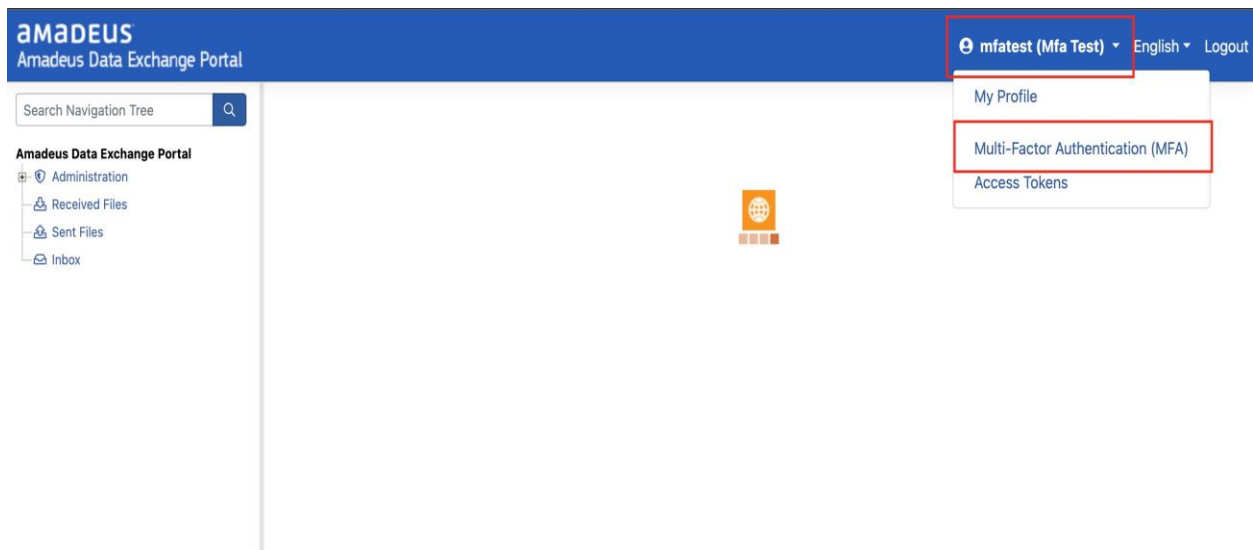


# Multi-Factor Authentication (MFA) in ADEP

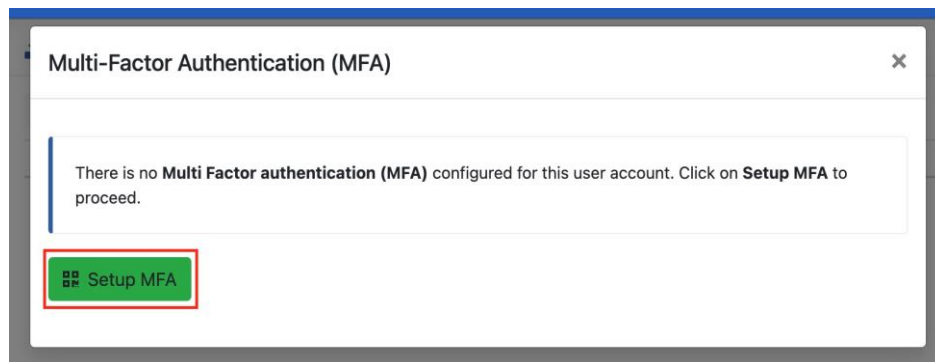
ADEP allows usage of Multi-factor authentication when login to it.

In order to set it up, follow next steps:

1. Go to the upper right corner and click on your user profile.
2. In the drop down that appears, click on Multi-Factor Authentication (MFA).



3. In the window that appears, click on Setup MFA.



4. Follow the instructions that appear, enter the code from your device and click Confirm. But you need first to download one of the applications and use it to scan the code:
  - a. Microsoft Authenticator
  - b. Google Authenticator


### Multi-Factor Authentication (MFA)

Scan the **Quick Response(QR) Code** with your phone and one of the MFA authenticator. You can use one of the popular applications like *Microsoft Authenticator* or *Google Authenticator* for example.

Once you scanned it, a code will be presented to you. Copy that value and enter it in the field below labeled **MFA Code** then click on **Confirm**.

Alternatively, you can copy the secret with the copy button at the end of the line and paste it in a password manager that supports Authenticator Key (TOTP) configuration.

If you are using an external authentication method that already works with an MFA configuration, the one you configure here will not be used for this authentication method.



Secret of the QR code  
JAANITS4YFZCILBFQHJ5A2AJ6B26LD7H

MFA Code

Enter the value presented in the MFA authenticator application

5. The window below confirms successful set up of MFA. Click on the cross in the right upper corner to exit.

### Multi-Factor Authentication (MFA)

Multi Factor Authentication (MFA) enabled. If you wish to revoke this configuration, click on **Revoke**. If you want to replace this configuration with a new one, click on **Replace**.

Your MFA configuration is confirmed.

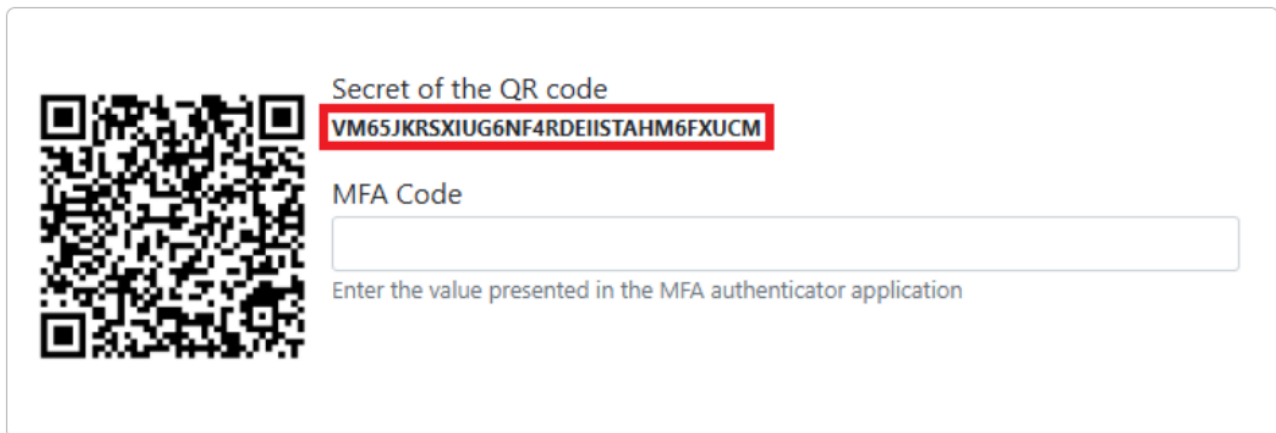
- The MFA configuration was created a **few seconds ago** (7/21/2023, 9:29:53 AM)
- It has not been used yet.

## Using MFA without a mobile device

It is possible to configure MFA without using a mobile device. An example of this type of application is *BitWarden* (<https://bitwarden.com/>) or KeePassXC (<https://keepassxc.org/>). These are password managers that can also display a TOTP (Time based One Time Password) code to the user.

The process is similar to using a mobile device, but rather than scanning a QR code, you need to enter the TOTP secret and insert it in the **Authentication Key** field.

When the S-Filer Portal authentication page is displayed, copy the secret that is shown under the label **QR Code Secret**.



The screenshot shows a QR code on the left. To its right, the text "Secret of the QR code" is displayed above a red-bordered box containing the alphanumeric string "VM65JKRSXIUG6NF4RDEIISTAHM6FXUCM". Below this, the text "MFA Code" is shown above an empty input field. A note below the input field reads "Enter the value presented in the MFA authenticator application".

## Bitwarden

1. Open the *BitWarden* application and click the **+ New** button in the top right corner of the screen.
2. Choose the **Login** option.
3. Enter the various information requested by the application and copy the TOTP secret into the **Authentication Key** field.
4. Click the **Save** button.



The screenshot shows a single input field with the label "Authenticator key" and a question mark icon. The field is empty and has a toggle icon (an eye) on the right side.

Once the TOTP secret is inserted in *BitWarden*, rather than displaying the secret value on screen, it's the TOTP code that is presented to the user. You simply need to enter this code in the **MFA Code** field on the S-Filer Portal authentication page.

## KeePassXC

Please follow [https://keepassxc.org/docs/KeePassXC\\_GettingStarted](https://keepassxc.org/docs/KeePassXC_GettingStarted) documentation