# Willis Towers Watson Information Service Portal (TWISP)

## Introduction to: Two-factor authentication (2FA)

September 2023

# The starting point
## Overview

- For transfering personal and / or confidential information we use the WTW data exchange portal. This also and applies in particular to the transfer of large quantities of this information. Therefore a higher need of protection is assumed to be neccesary. According to information, the portal is used for a large number of customers.
- The access security of the portal has increased by the introduction of the two-factor authentication (2FA).
- In the following we will explain what the two-factor authentication is and how we can implement 2FA in the portal ourselves.

# What is the 2FA and how did we implement it in TWISP?

- 2FA is based on two different authenitification methods that are combined with different authentification categories or factors (like knowledge, possession and biometrics), which increase security. Examples for authentification methods of the named categories are:
  - Category knowledge: username and password
  - Category possession: credit card, TAN-list
  - Category biometrics: Iris scan, fingerprint

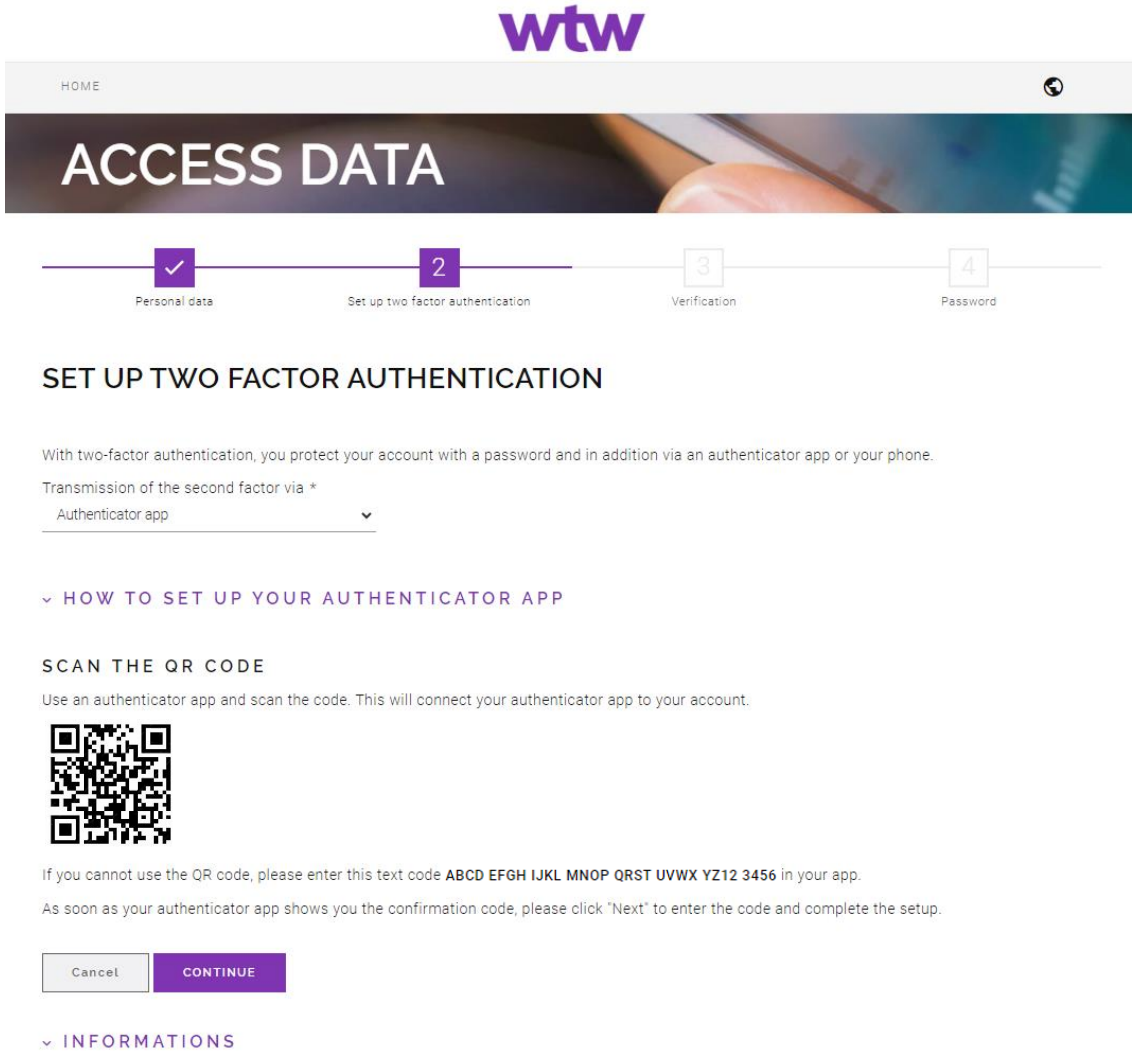
- When using TWISP more than just the username and password (category: knowledge) is required, you will need an additional authentification method from the category possession, since authentification procedures from the category biometrics are not universally applicable.
- One-time passwords with limited validity can be provided via an authenticator app, SMS or phonecalls. The authenticator app is recommended.

# Sending a one-time password with limited validity

- The portal user automatically adds an additional security level with the two-factor-authentication. After the set up, you will login with two steps:
  - User name and personal password
  - A one-time password (= verification code) which you receive via the selected 2FA method
- If the portal user has opted for an authenticator app, he will be prompted to enter the verification code from the linked authenticator app to verify his identity at the Login. Instructions for setting up Microsoft Authenticator and Google Authenticator can be found in this document.
- If the portal user has opted for telephone dispatch, WTW sends a six digit verification code to the registered phone number. The user can choose if they prefer to receive the verification code via SMS or over a voice call. He then simply enters the code during registration to confirm his identity. The verification codes are valid only once!

# What will change in the future?

## The initial login after the 2FA is activated

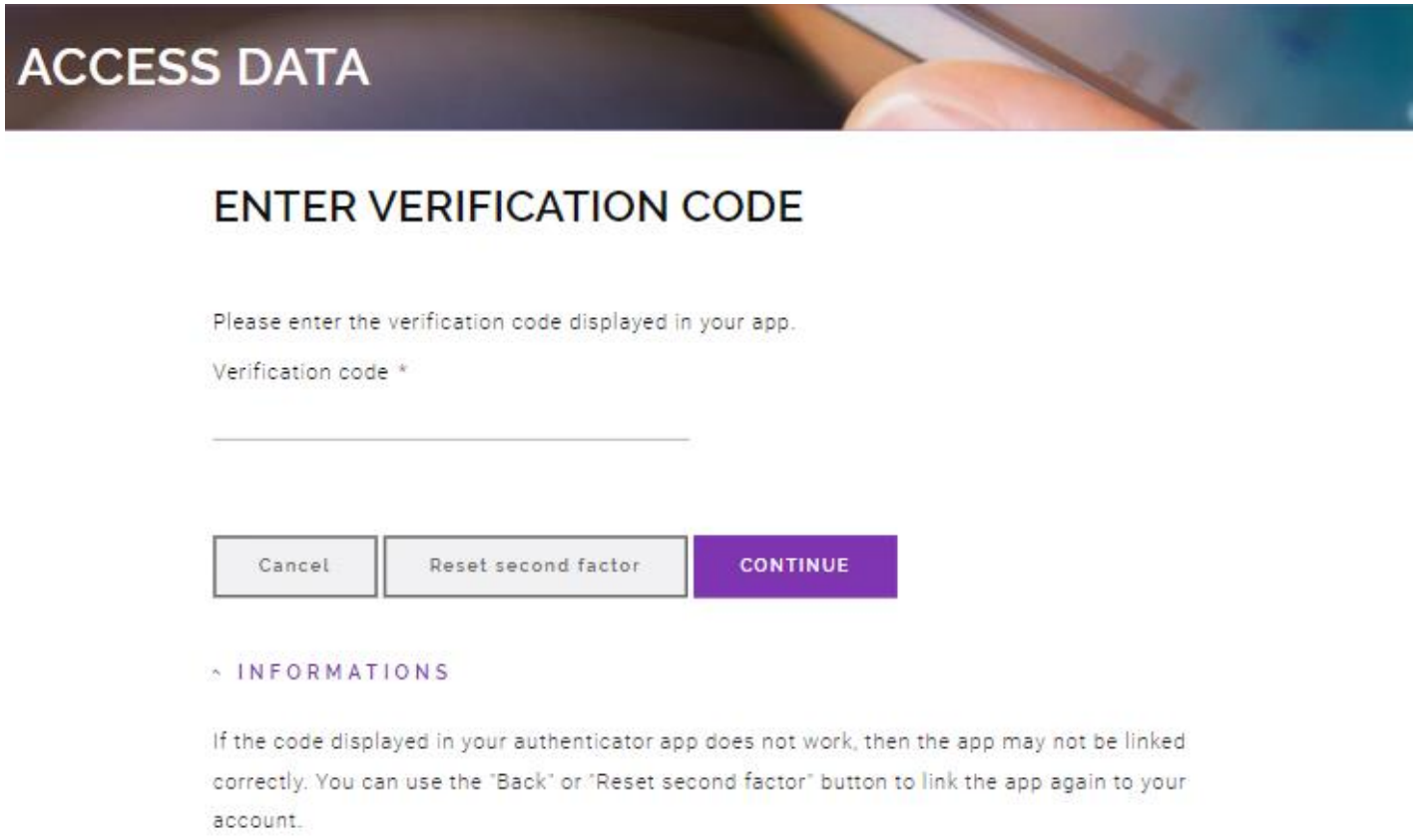



Users who login for the first time have to set-up everything as follows:

- Sign into the portal through the regular login page
- Setting up the 2FA (Authenticator app or telephone number with notification type of the verification code.)
- Enter the verification code
- Use the portal as usual

# What will change in the future?

## Regular login at the portal after setting up the 2FA




After a portal user has set up 2FA, the new login process will be as follows:

- Log in to the portal via the regular login page
- Enter the verification code
- Use the portal as usual

# What will change in the future?

## INFORMATIONS

With two-factor authentication, you add an additional layer of security to your account. Once set up, you can log in to your account in two steps:

- With something you know (your password).
- With something you have (like your smartphone).

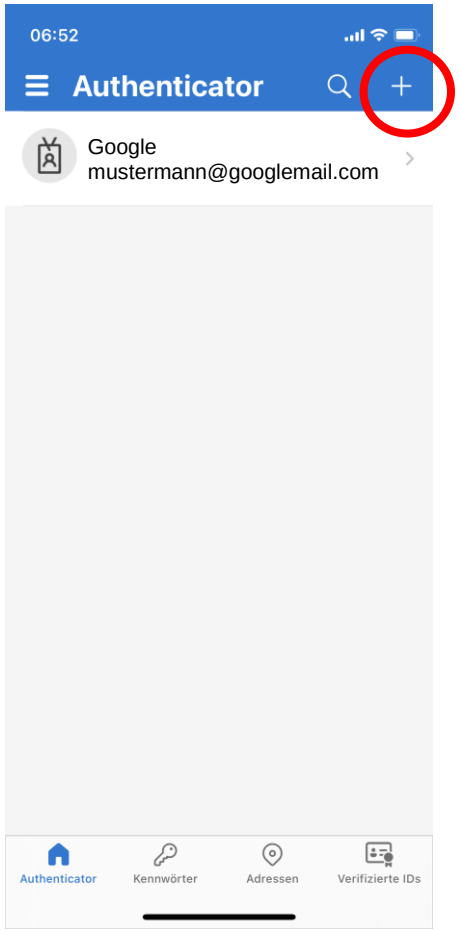
The recommended method for obtaining the second factor is the use of an authenticator app. The Microsoft Authenticator or Google Authenticator are the most suitable, but any authenticator app can be used.

If you do not have the option of authenticating via an authenticator app, you can also authenticate via SMS or voice message. To do this, select "Phone" in the selection field. Once you have set up the authenticator app, you can no longer switch to Phone.

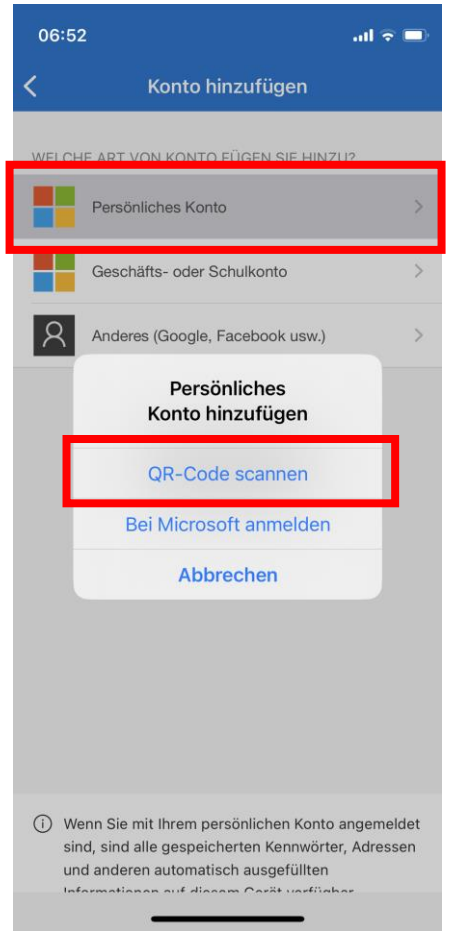
When you're done with the setup, click "Next" and enter your confirmation code on the following page.

If you have problems logging in, please contact Portal Support.

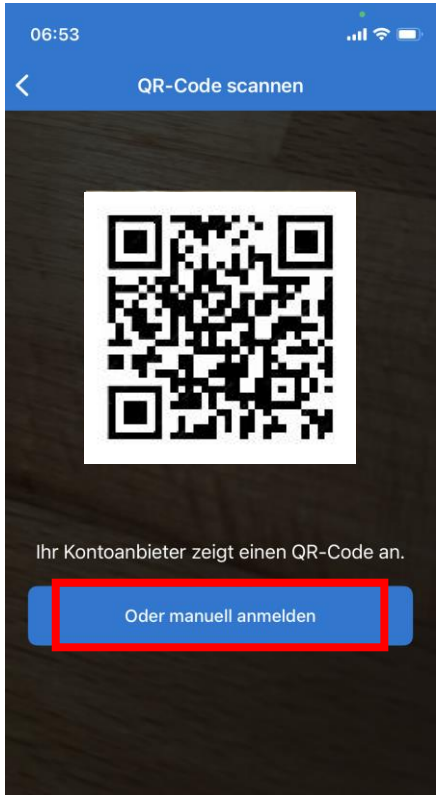
# Setup Microsoft Authenticator



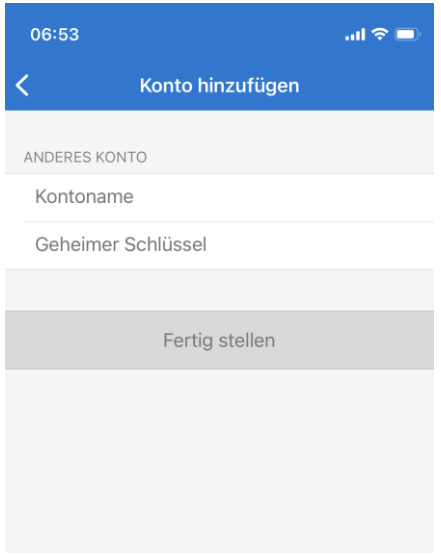

Select "Add account" in the app or the "+" in the upper right corner.



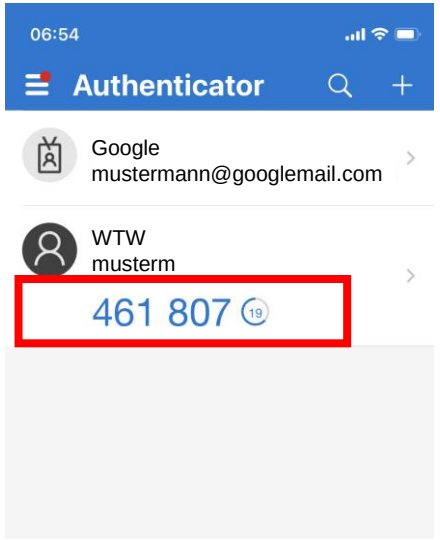

Select "Personal Account" and then "Scan QR-Code".




Scan the QR code that is displayed in the portal. If that doesn't work, you can select "Sign in manually" in the app.



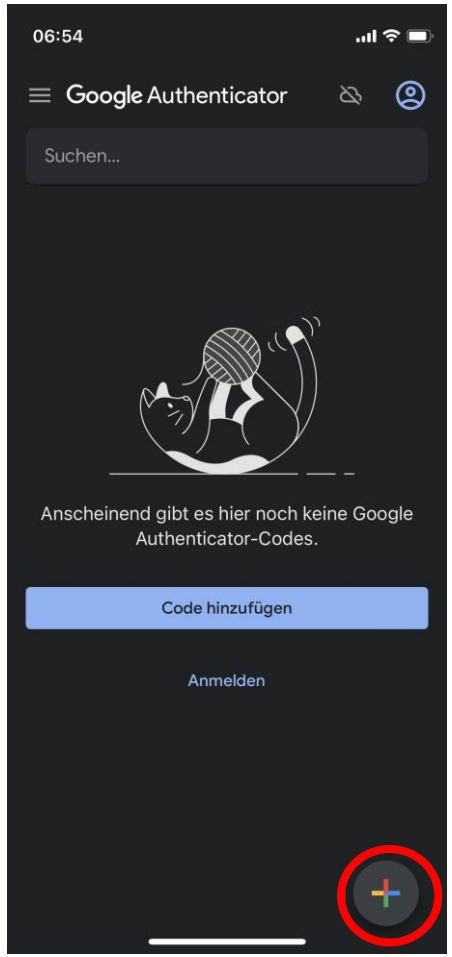

Select an account name (for example, your user name in the portal) and enter the code displayed in the portal at "Secret key".



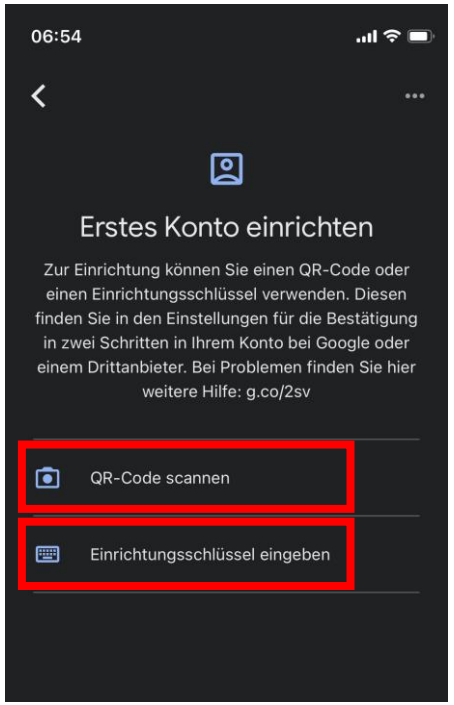

In your account overview you will now see an entry with the name "WTW" and your user name. Here you will see the six-digit one-time code. This is only valid for a limited time and will be automatically replaced by a new code after the time has expired.

Note: The screenshots shown may vary depending on the app version.

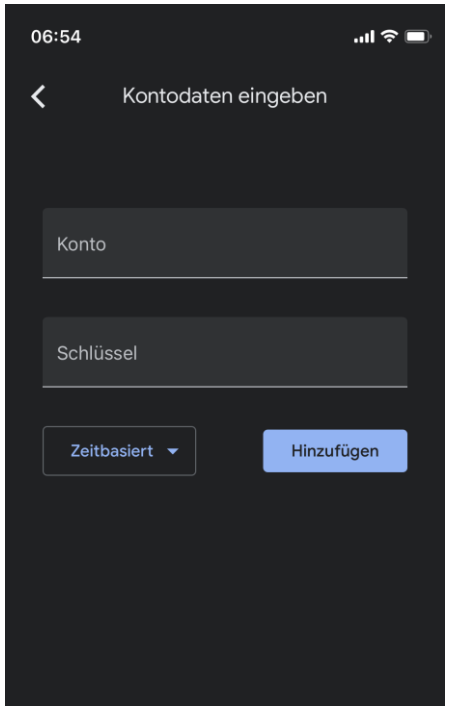
# Setup Google Authenticator



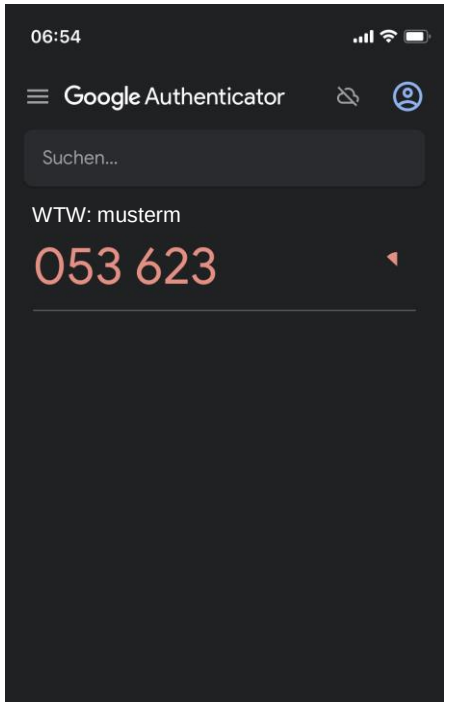

Select "Add account" in the app or the "+" at the bottom right.




Select "Scan QR code". Scan the QR code that is displayed in the portal. If this does not work, select "Enter a setup key.




Select an account name (for example, your user name in the portal) and enter the code displayed in the portal at “Key".




In your account overview you will now see an entry with the name "WTW" and your user name. On this page you will see the six-digit one-time code. This is only valid for a limited time and will be automatically replaced by a new code after the time has expired.

Note: The screenshots shown may vary depending on the app version.

# Contact

**If you have any questions or problems please contact support.twisp@willistowerswatson.com or your regular contact person for data exchange.**

# For reference

- The content of this presentation and the materials provided by WTW are general in nature. They do not represent an assessment of specific individual cases, nor can one be derived from them. They are based on our company's subjective assessments and current trends. The transfer of the content and documents don’t constitute any liability on the part of WTW towards the recipients or towards third parties.
- All contents of this presentation and all documents are the intellectual property of WTW. Any other use, content-like presentation or disclosure to third parties, in whatever form, requires the prior express consent of WTW.