# Instructions for Initial Login with 2-Factor Authentication (FAQ)

ONTRAS Gastransport GmbH

Verdichterstation Bobbau

- **How can I set up the two-factor authentication?**

- During the transition phase from January 8, 2024, to March 31, 2024, login to the customer portal can be done as usual (using username/email address and password).
- During this transition period, customer portal users will already have a possibility to set up two-factor authentication.
- At the end of the transition phase on April 1, 2024, setting up two-factor authentication will become mandatory upon the first login attempt.
- To open the setup interface, the link "Set Up" shall be selected or navigate to "Edit Authentication" in the personal data section (accessible via the username in the top right corner). In this section, the "Set up Authenticator Application" function can be chosen.

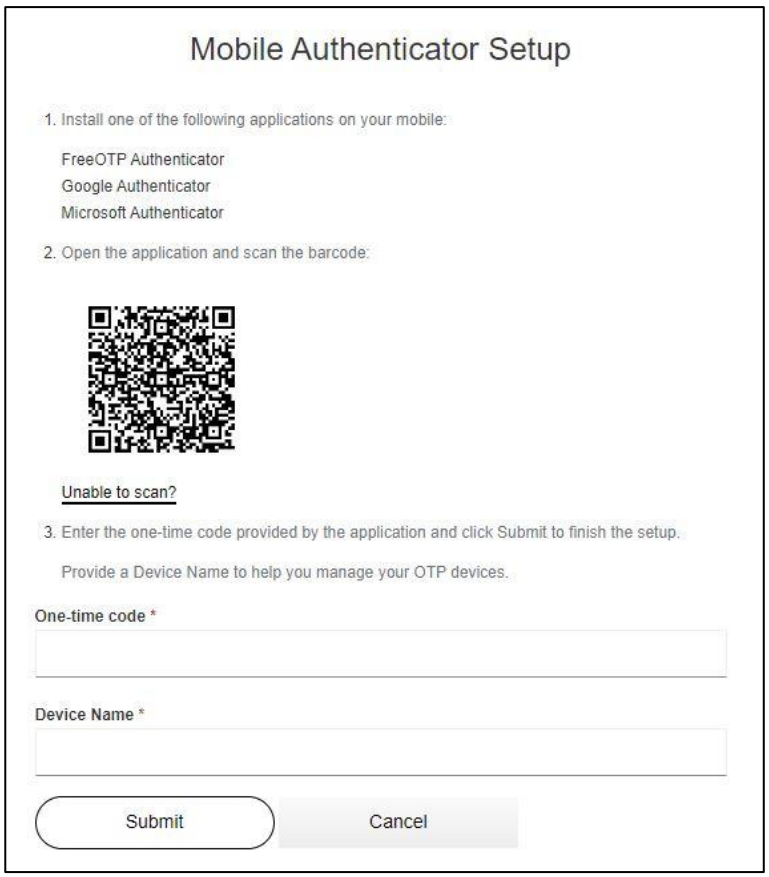


*Figure 1: Overview of possible applications and procedure*

- The second factor is set up in the following steps:

    - The first step is to install a supported application on the smartphone to set up 2-factor authentication.
    - Then open the selected application.

    - **FreeOTP Authenticator:**

        - The first step is to select "Add a token" or QR code icon.
        - Next, the QR code generated in the customer portal needs to be scanned.
        - Then, it is possible to set up an icon for the portal in the application.

- It is necessary to decide whether the smartphone always needs to be unlocked to receive a code.

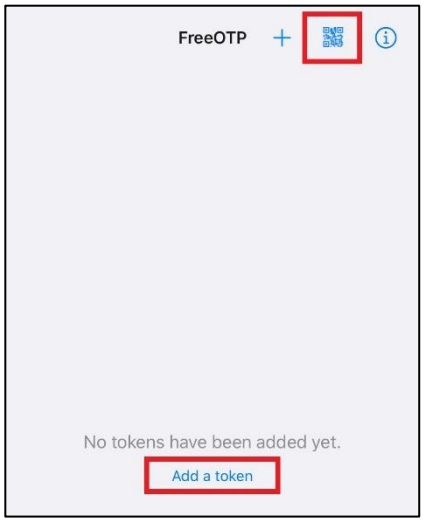


*Figure 2: Homepage of the FreeOTP Authenticator app*

- Now, the account and its corresponding one-time code are visible.

- **Google Authenticator**

  - First, please select the "Add Code" button.

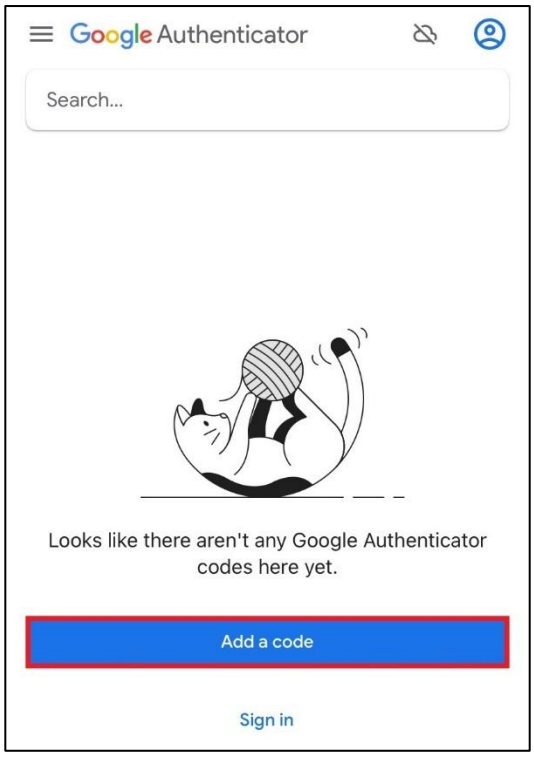


*Figure 3: Home screen of the Google Authenticator application*

  - The next step is to select the "Scan QR code" button.

- Then the QR code generated in the customer portal should be scanned with the smartphone.
- With the input of the one-time code generated in the application into the customer portal, the setup is complete.

- **Microsoft Authenticator**

  - The first step is to select the plus symbol on the home screen oft the app.


*Figure 4: Toolbar on the home page of the Microsoft Authenticator application*

  - The "Other" type of the account shall be selected.

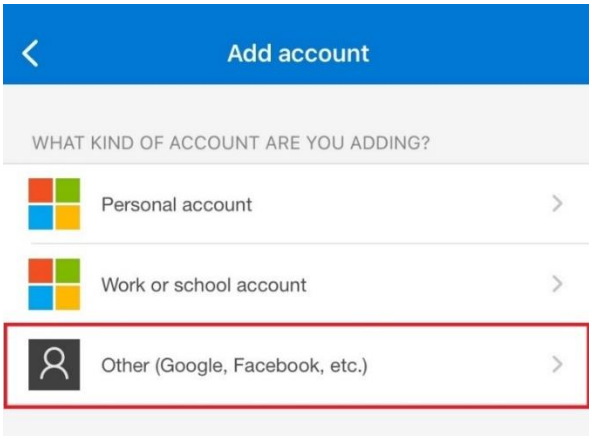


*Figure 5: Account Types in the Microsoft Authenticator Application*

  - Then, the QR code generated in the customer portal can be scanned.
  - Now, the account and its corresponding one-time code are visible.
  - Note: If the same device is registered a second time, it must first be removed when using the Microsoft Authenticator.

- **Physical Device**

  - If no mobile phone is available, there is the possibility to authenticate with a physical device such as the REINER SCT Authenticator.
  - Please do the setup according to the instructions of the physical device.

- **Recovery Codes**

  - In addition to authentication using the applications, recovery codes should be generated. These codes can be saved, printed, or copied into a password manager.
  - The codes must be kept safe.
  - With the help of these codes, it is possible to log in if, for example, access to the 2-factor device is not possible.

- **How can I set up the security keys?**
    - Prerequisite is the successful setup of two-factor authentication using an appropriate 2-factor device.
    - In the logged-in mode, you can switch to 'Edit Authentication' in the personal data section (accessible via the username in the top right corner). In this section, you can select the “Set up security key” function.

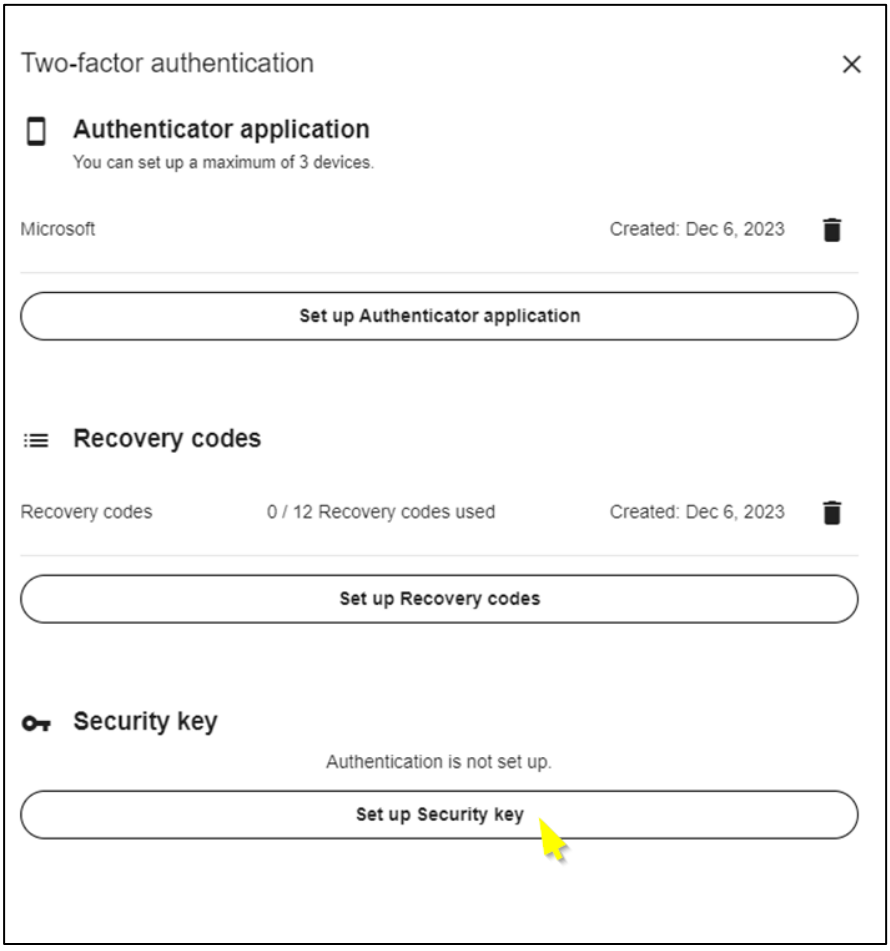


*Figure 6: 2-Factor Authentication Setup Mask*

- **Even though my device (especially a Reiner SCT) or smartphone app correctly recognized the QR code for the second factor, the setup fails, or (sometimes) the 6-digit numbers appear to be incorrect. What could be the reason for this?**
    - The generation of a valid 6-digit code depends on the exact time of your device. If the device's time is inaccurate, the portal will not accept the codes or not for the full 30 seconds when they would otherwise be valid. Please ensure that your device has the correct time down to the second. Smartphones usually handle this automatically, especially hardware devices like the Reiner SCT may need to be set manually, depending on the accuracy of their internal clock or, in the case of battery changes, possibly multiple times a year. Reiner SCT provides a website for convenient and precise time synchronization: https://www.reiner-sct.de/sync.

- **What can I do if I no longer have recovery codes and my 2-Factor-Authentication device is lost?**
    - In this case, the customer portal user cannot independently restore access. Initially, the customer support representatives of ONTRAS need to be contacted. After authenticating the caller in the customer portal, they can remove the devices associated with the user. Subsequently, the customer portal user can register a new device to perform the 2-factor authentication again (refer to the instructions “How can I set up the two-factor authentication?”).

- **I got a new device. How do I register the new device?**
    - There are two options:
        - If you still have the old device, you can use it to log in and then register a second device under your user data. To do this, you have to scan a QR code with the new device so that the one-time password can be generated there again. The procedure is the same as if you were setting up the 2FA initially. Once the setup is complete, you can remove the old device from your user data for completeness.
        - Alternatively, you can also use the recovery codes, especially if the old device is no longer available. After logging in, the procedure is identical to that of variant 1, i.e. add a new device, scan the QR code on the new device and then remove the old device for completeness.

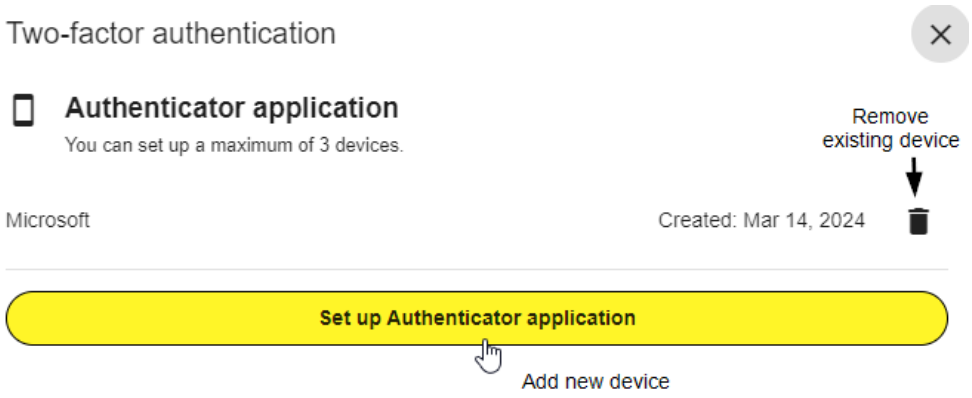


*Figure 7: Procedure for changing device*

- **How can I change my password?**
    - After logging in to the customer portal, the dialog for changing the password can be accessed via the menu area of your own data (accessible via the username in the top right corner). There, a new password can be set according to the defined password guidelines.

- **How do I proceed if I've forgotten my password?**
    - In the login interface of the customer portal, there is a link “Forgot password?” available to reset the password by entering the email address or username.

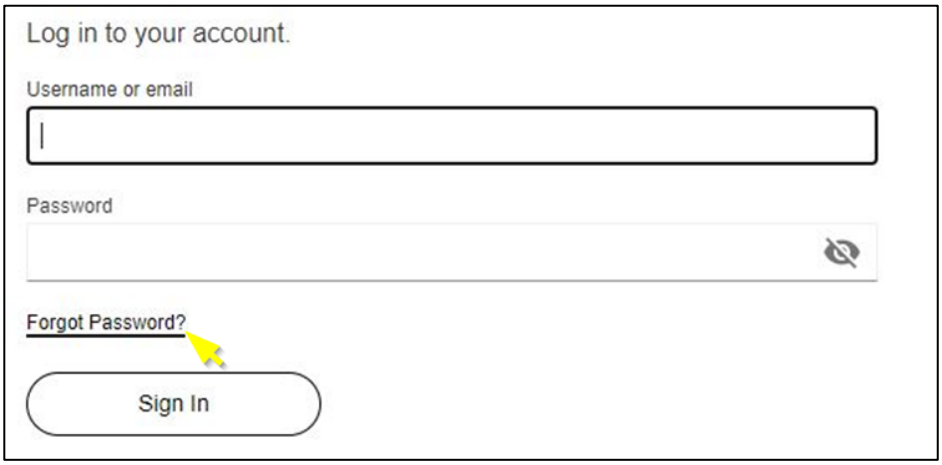


*Figure 8: Login screen of the ONTRAS customer portal*

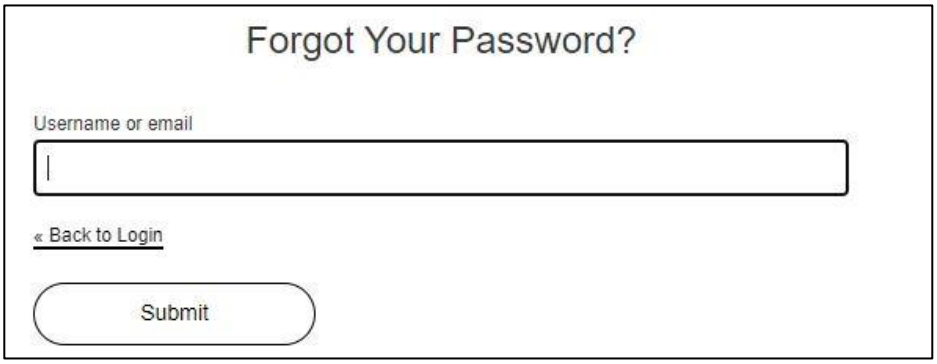


*Figure 9: Forgot Password Function*