

Instructions for activating two-factor authentication (2FA)

Enable two-factor authentication

Logging in to 2FA management

Open the 2FA management page in a browser at <https://login.tu-darmstadt.de/2fa>. You can also find this link in the [IDM portal](#) (under 'Personal Account Management' - 'Account / Password') and under '2FA-management' to the right of the SSO (Single Sign-On) login screen. Log in with your TU ID and the corresponding password.

After opening 2FA management, you will be taken to a **welcome page** (Figure 1). Click on **Continue** to receive a brief introduction (Figure 2).

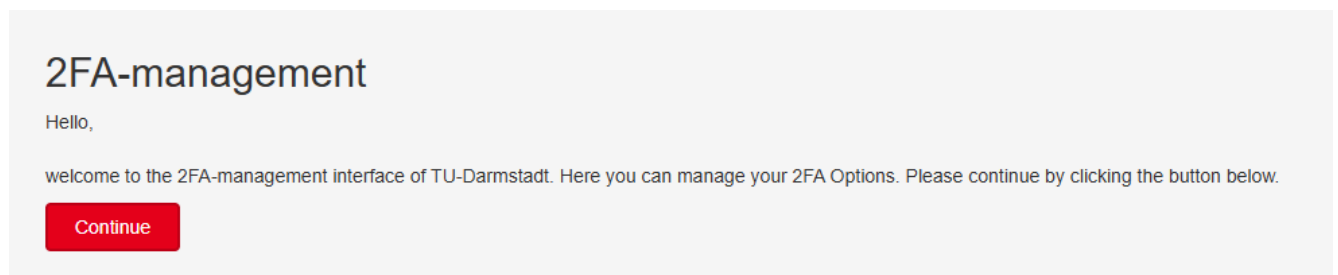


Figure 1: Welcome page

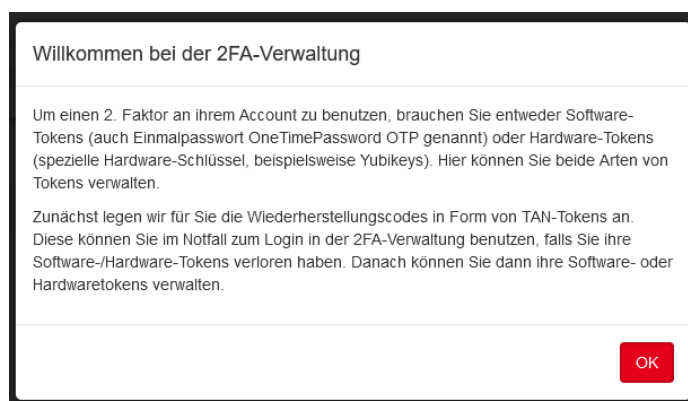


Figure 2: Brief introduction

Creation of the recovery code

After clicking **OK**, you will first be taken to another information page to create your recovery codes (Figure 3).

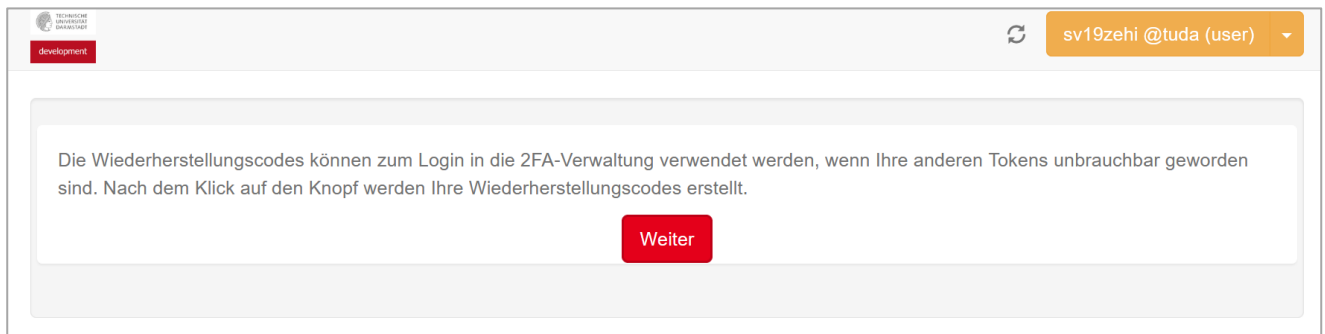


Figure 3: Information page

Important: Be sure to save or print your recovery codes!

If your other tokens are defective or lost – whether due to loss or damage to a hardware token or loss of a device or resetting of the operating system in the case of a software token – you will need these codes to log in to 2FA management. Without the recovery codes, access is no longer possible, and you could be permanently locked out.

What should I do if I lose my token?

If you lose your token despite taking the utmost care, you can proceed as follows:

- Log in to 2FA management with the recovery code you created during registration.
- Delete the lost or invalid token there.
- You can then set up a new token in 2FA management.

After clicking **Continue**, a numbered list of exactly 5 recovery codes will be generated, which are displayed in the form of a one-time password (OTP). Each one-time password consists of 6 consecutive digits (Figure 4).

The recovery codes can only be used to log in to the 2FA administration.

To print the list, click on the **Print OTP list** button.

Es ist wichtig, die Wiederherstellungscodes (OTP) auszudrucken oder sicher zu speichern. Wenn Sie die Wiederherstellungscodes und alle anderen Tokens verlieren kann ausschließlich der HRZ-Service Ihren Account zurücksetzen.

OTP-Werte

#	OTP	#	OTP	#	OTP	#	OTP	#	OTP
0	276058	1	155337	2	986197	3	587607	4	838252

OTP-Liste drucken

Ihr Account ist jetzt durch die Wiederherstellungscodes vorbereitet und damit 2FA aktiviert. Um sich mit einem zweiten Faktor auch am SSO anmelden zu können, müssen Sie sich jetzt Ihren ersten Token erstellen. Klicken Sie dafür zunächst auf "Weiter" und dann auf der nächsten Seite auf "Token ausrollen". Alternativ können Sie jetzt einen Hardware-Token vom HRZ zuweisen lassen.

Weiter

Figure 4: List of generated recovery codes

Once you have completed this step, 2FA will be automatically activated for you. **It is therefore particularly important that you keep the recovery codes in a safe place so that you can use them in an emergency.**

You will also receive an email confirming the activation.

Note:

If you have not created any tokens other than the recovery codes, two-factor authentication is only enabled in the 2FA management itself.

This means that if you exit 2FA management now, you will only be able to log in again with a recovery code.