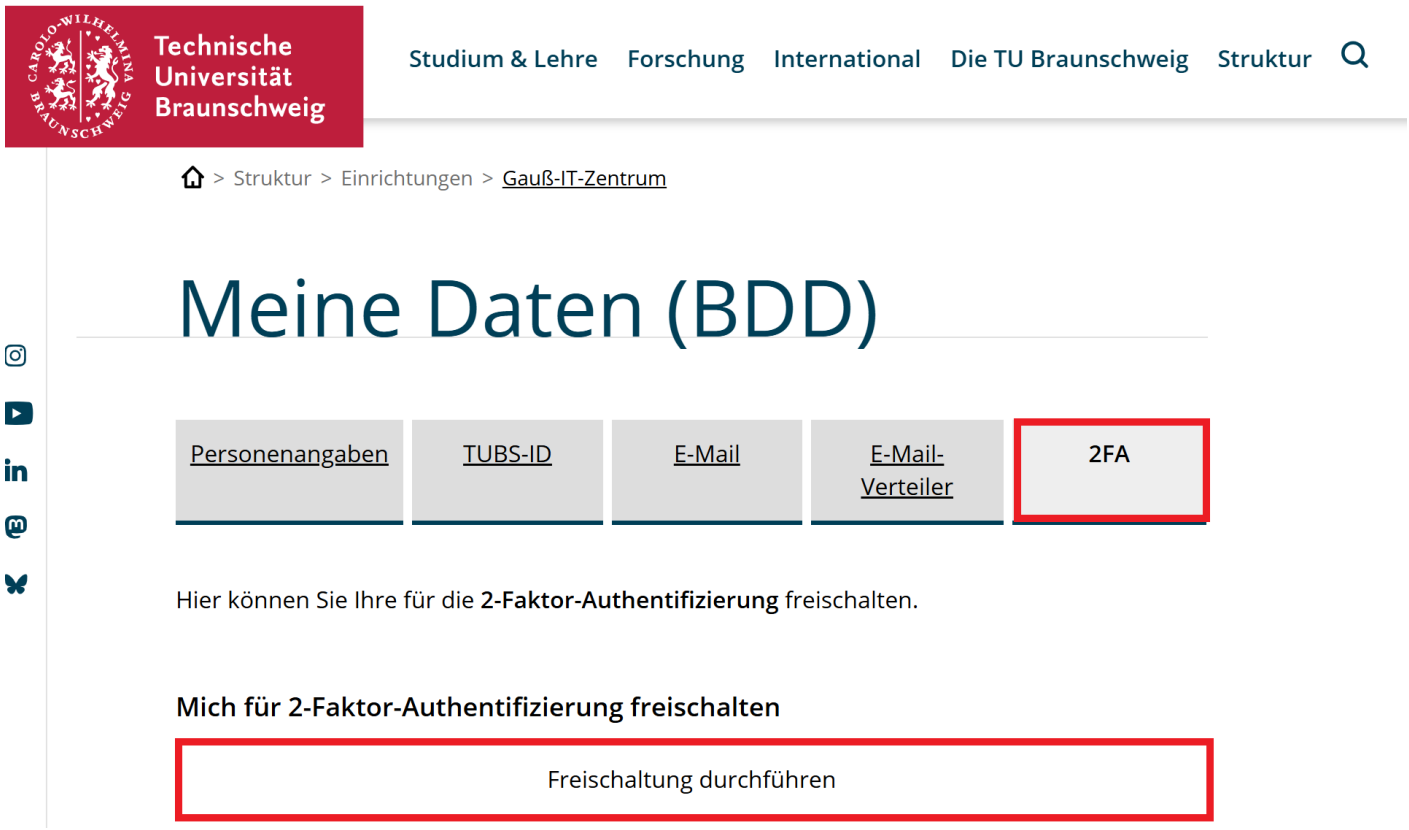
Activation of 2 FA for employees and students of TU Brunswick

To participate in the pilot phase of the 2FA project, user IDs must be activated via "My Data (BDD) ". To do this, log in to BDD with your TUBS ID and password, and then open the 2FA tab.

Here click the button "Freischaltung durchführen" (activation)



You have been unlocked for the second factor.

Meine Daten (BDD)

Hier können Sie Ihre für die **2-Faktor-Authentifizierung** freischalten.

Freischaltung erfolgreich

Ihre Freischaltung war erfolgreich. Nach ca. 45 min können Sie das Gerät registrieren, mit dem Sie die 2-Faktor-Authentifizierung nutzen wollen. Nähere Informationen finden Sie in unseren Anleitungen:

Approximately 30 to 45 minutes after activation in "Meine Daten (BDD)", an automated email will be sent to you informing you that DUO has been rolled out. The mail can arrive via Outlook, Thunderbid or the Mail Apps on a mobil device.

> If the Mail won't arrive in an hour, sign in on the OWA or the SSO and follow the instructions for the setup of the DUO Desktop Application or the DUO Mobile App. It is not mandatory for the second Factor to use the mail.

To add your device, please follow the instructions in the email or also the other instructions in this book.

Currently, two-factor authentication is active when using OWA (Outlook Web Access), VPN, and SSO. For VPN, please use the VPN gateway, vpngate.tu-braunschweig.de. If you want to use the DUO Desktop Application to login to the VPN you have to use this gateway: vpngate.tu-braunschweig.de/saml

The second factor can be generated via the DUO Desktop application, a hardware token (if applicable), or a mobile app. If you have a centrally managed device, please email it-service-desk@tu-braunschweig.de for the desktop application, and it will be made available to you. The DUO Desktop application is the most practical option, as it runs in the background of your work device (which you should have with you for work or studies anyway) and is therefore always available and cannot be forgotten (unlike the token or mobile device). For this reason, we

recommend using the DUO Desktop application on Windows or Mac devices for TU Braunschweig employees (the application is not yet available for Linux). For students, we recommend the DUO Mobile App for their mobile devices, as logins often occur on other devices, and the DUO Desktop application would not work because it is activated for the device and not the account. Here are the instructions for setting up the DUO Desktop application, and here are the instructions for the DUO Mobile App.

> If you have a company mobile phone, you can use it as a second factor without any problems, which is why you will not be provided with a hardware token.

You also have the option of requesting a token. To do so, please send an email to 2fa@tu-braunschweig.de. We will add and issue these hardware tokens directly after registration. Between registering for 2FA and receiving the token, login via OWA, SSO, or the VPN gateway vpngate.tu-braunschweig.de will not be possible. Furthermore, these tokens are not sustainable and you must carry them with you at all times, otherwise login is not possible. Additionally, the tokens are very environmentally harmful because they cannot be repaired, nor can the batteries be replaced. Therefore, they become electronic waste and are not recommended by us.

> Other FIDO keys (e.g., YubiKeys) are also possible. We will set them up if possbile but we will not further support them and neither will we explain them further in our Instructions.

Further documentation on the various procedures can be found at: https://guide.duo.com/?ljs=de

---

Revision #10
Created 2026-01-29 10:30:48 UTC by Lenny Naumann
Updated 2026-05-22 08:22:20 UTC by Timo Nitschke