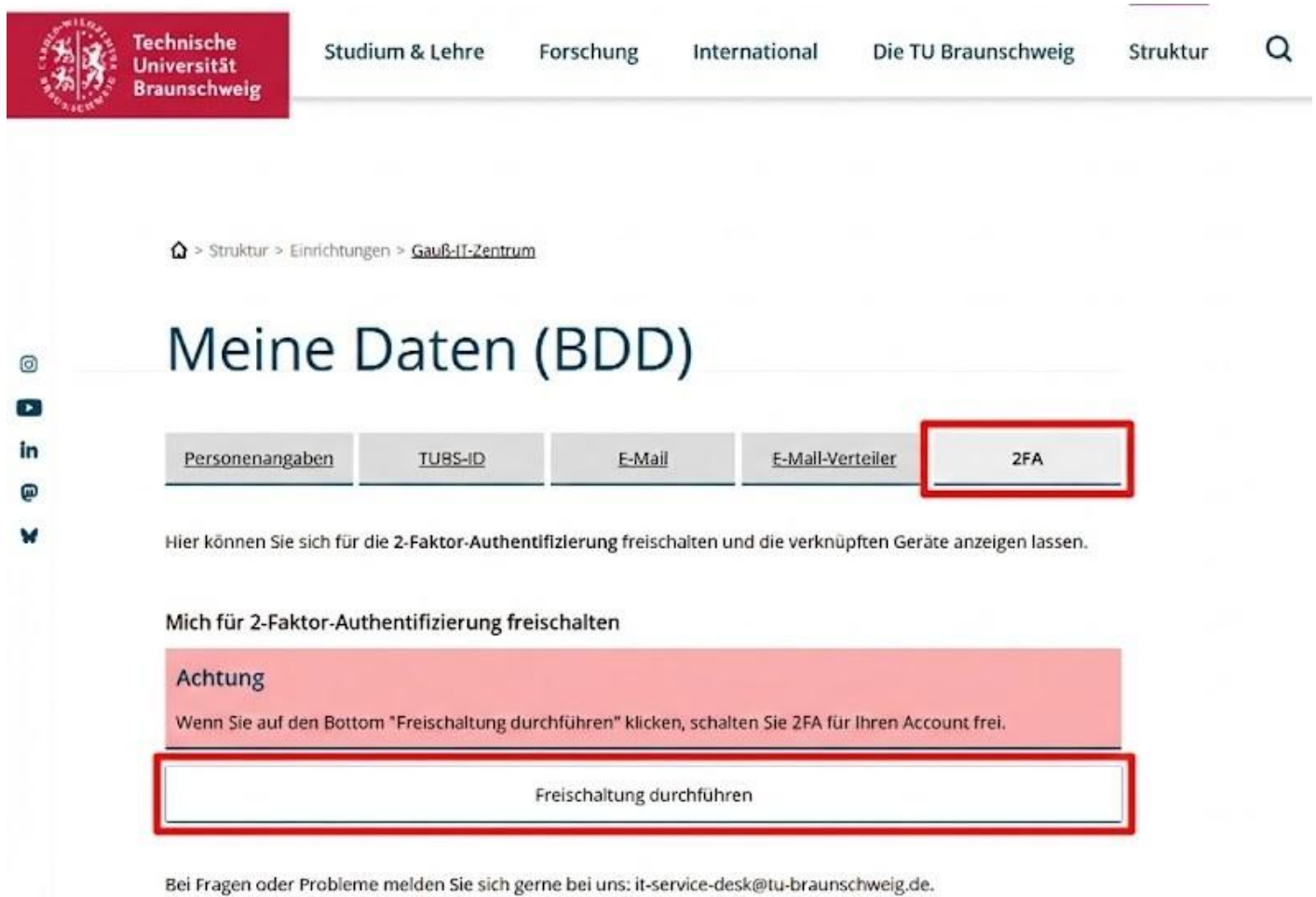


# Freischaltung von 2FA für Mitarbeitende und Studierende der TU Braunschweig

There is also an english version available. Click [Here](#).


Um an der Pilotphase für das Projekt 2FA teilzunehmen, müssen die Benutzerkennungen über "[Meine Daten \(BDD\)](#)" freigeschaltet werden. Dafür melden Sie sich beim BDD mit der eigenen TUBS-ID und dem zugehörigen Passwort an und öffnen dann den Reiter 2FA.

Hier klicken Sie auf den Button "Freischaltung durchführen".



The screenshot shows the TU Braunschweig website header with the logo and navigation menu. The breadcrumb trail is: [Struktur](#) > [Einrichtungen](#) > [Gauß-IT-Zentrum](#). The main heading is "Meine Daten (BDD)". Below it, there are five tabs: "Personenangaben", "TUBS-ID", "E-Mail", "E-Mail-Verteiler", and "2FA". The "2FA" tab is highlighted with a red border. Below the tabs, the text reads: "Hier können Sie sich für die 2-Faktor-Authentifizierung freischalten und die verknüpften Geräte anzeigen lassen." Underneath, there is a section titled "Mich für 2-Faktor-Authentifizierung freischalten" with a red warning box containing the text: "Achtung Wenn Sie auf den Button 'Freischaltung durchführen' klicken, schalten Sie 2FA für Ihren Account frei." Below the warning box, the button "Freischaltung durchführen" is highlighted with a red border. At the bottom, there is a footer note: "Bei Fragen oder Probleme melden Sie sich gerne bei uns: [it-service-desk@tu-braunschweig.de](mailto:it-service-desk@tu-braunschweig.de)."

Sie wurden für den zweiten Faktor freigeschaltet.

 > [Struktur](#) > [Einrichtungen](#) > [Gauß-IT-Zentrum](#)

# Meine Daten (BDD)

<a href="#">Personenangaben</a>	<a href="#">TUBS-ID</a>	<a href="#">E-Mail</a>	<a href="#">E-Mail-Verteiler</a>	2FA
---------------------------------	-------------------------	------------------------	----------------------------------	-----

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:

Nach ungefähr 30 bis 45 Minuten nach der Freischaltung in "Meine Daten (BDD)" wird eine automatisierte Mail an Sie versendet mit dem Hinweis, dass DUO ausgerollt wurde. Die Mail kann über Outlook, Thunderbird oder Mail-Apps auf Mobilgeräten aufgerufen werden.

Sollten Sie keine der genannten alternativen Zugriffsmöglichkeiten auf Ihr Mail-Postfach eingerichtet haben, ist es ratsam sich innerhalb der 30 Minuten beim OWA anzumelden und die Session nicht zu beenden, bis die Einrichtung abgeschlossen ist. Aber keine Sorge, auch wenn der Zugang zu den Mails nicht möglich ist wird der Einrichtungsprozess beim nächsten Loginversuch automatisch für das Gerät angestoßen, an dem der Anmeldeversuch stattfindet.

Falls die Mail nach einer Stunde nicht angekommen ist, melden Sie sich bei OWA oder dem SSO an und folgen Sie den Anleitungen zur Einrichtung der DUO Desktop Anwendung oder der DUO Mobile App. Es ist nicht zwingend notwendig für das Hinzufügen des zweiten Faktors die Mail zu verwenden.

Um Ihr Device hinzuzufügen, folgen Sie bitte der Anleitung in der E-Mail. Ansonsten finden Sie hier auch weitere Anleitungen.

Zurzeit ist der zweite Faktor bei der Nutzung von OWA (Outlook-Web-Access), VPN und SSO aktiv. Für VPN nutzen sie bitte das VPN Gateway, [vpngate.tu-braunschweig.de](https://vpngate.tu-braunschweig.de). Bei der Verbindung der VPN mit der DUO Desktop Anwendung brauchen sie das Gateway: [vpngate.tu-braunschweig.de/saml](https://vpngate.tu-braunschweig.de/saml)

Der zweite Faktor kann über eine App auf dem Mobilgerät, die Duo Desktop Anwendung, Passkeys oder ggf. einen HW Token erzeugt werden. Die Duo Desktop Anwendung ist am praktikabelsten, da diese im Hintergrund ihres Arbeitsgeräts läuft (welches Sie für die Arbeit oder das Studium sowieso dabei haben sollten) und ist somit immer dabei und kann nicht vergessen werden (wie der Token oder das mobile Endgerät). Deswegen empfehlen wir die Nutzung der Duo Desktop Anwendung auf Windows oder Mac Geräten für Mitarbeiter der TU Braunschweig (die Anwendung ist unter Linux derzeit noch nicht anwendbar). Bei Studenten empfehlen wir DUO Mobile App für das Mobilgerät, da oft Anmeldungen an anderen Geräten stattfinden wobei die DUO Desktop Anwendung nicht funktionieren würde, weil diese für das Gerät und nicht den Account aktiviert wird. [Hier](#) finden Sie die Anleitung zur Einrichtung der DUO Desktop Anwendung und [hier](#) die Anleitung für die DUO Mobile App.

Wenn sie ein Diensthandy besitzen, können Sie Dieses ohne Probleme als zweiten Faktor nutzen, weswegen Sie keinen Hardware Token zur Verfügung gestellt bekommen.

Sie haben auch die Option eines Hardware-Tokens zu beantragen. Dieser Hardware-Token ist nicht Nachhaltig, da die Batterie nicht ausgetauscht werden kann und somit Elektroschrott ist. Daher muss dann wieder ein neuer Token ausgestellt werden. Wir empfehlen daher als ersten die Duo App und Passkey, an zweiter Stelle die Desktop Anwendung und als letzte Möglichkeit erst die Hardware Token. Senden Sie zur Beantragung des Hardware-Tokens bitte eine E-Mail mit einer Begründung, wieso der Token erforderlich ist an [2fa@tu-braunschweig.de](mailto:2fa@tu-braunschweig.de). Diese Hardware-Token tragen wir nach Genehmigung direkt ein ins System und geben Sie im IT-Service-Desk aus. Zwischen der Anmeldung für 2FA und der Ausgabe des Tokens ist dann keine Anmeldung über OWA, SSO oder das VPN-Gateway [vpngate.tu-braunschweig.de](https://vpngate.tu-braunschweig.de) möglich. Die Token sind aber nicht beste Option für einen zweiten Faktor und werden von uns auch nicht empfohlen. Die Geräte sind nicht sehr nachhaltig und müssen (sofern sie als einziger Faktor genutzt werden) immer mit in der Tasche sein. Sollte man einen Token verlieren oder dieser kaputt gehen benötigen Sie einen Neuen, was dazu führt, dass der Alte Token auf dem Elektroschrott landet und damit der Umwelt schadet. Außerdem passiert dies auch, wenn die Batterien leer gehen da diese nicht getauscht werden können.

Es sind auch andere FIDO-Keys (z.B. yubikeys) möglich. Diese werden zwar sofern möglich von uns eingerichtet aber nicht weiter unterstützt oder aktiv in den Anleitungen erklärt.

Weitere Dokumentation zu den verschiedenen Verfahren finden Sie unter:

<https://guide.duo.com/?ljs=de>

---

Revision #45

Created 2024-02-10 05:02:54 UTC by Matthias Hentschel

Updated 2026-06-23 04:31:32 UTC by Marius Kannicht