Deutsches Biomasseforschungszentrum
gemeinnützige GmbH

Inhalt

1 Introduction

To increase security and for better protection of important project documents on our DBFZ document management system „EDMS " we are introducing two-factor authentication, or 2FA for short.

2 Why two-factor autentication

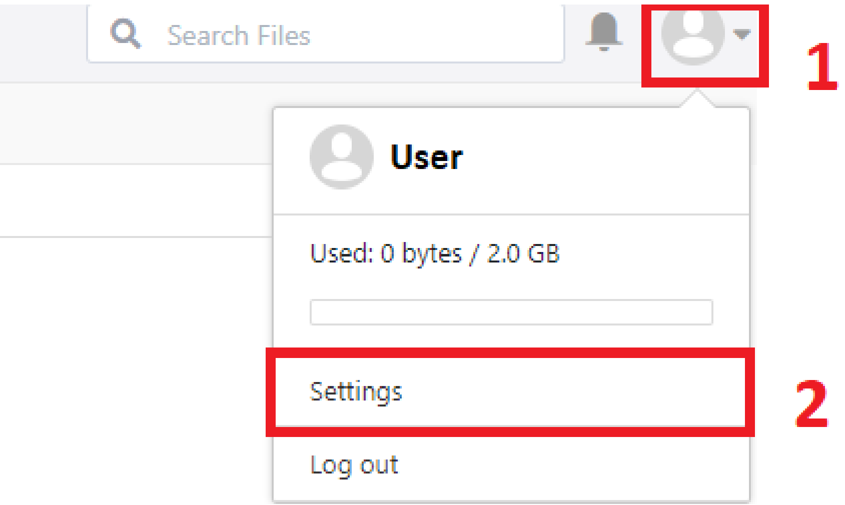
As you probably already know from other areas, e.g. online banking, an additional authentication feature is used for 2-factor authentication. This additional feature, in the form of an access token, must be generated on your smartphone in an app.
The token is additionally requested after your EDMS user name and password have been requested. This prevents a hacker from gaining unauthorized access to the project documents using only your access data. Only with additional physical access to your smartphone could an unauthorized person log in to EDMS.

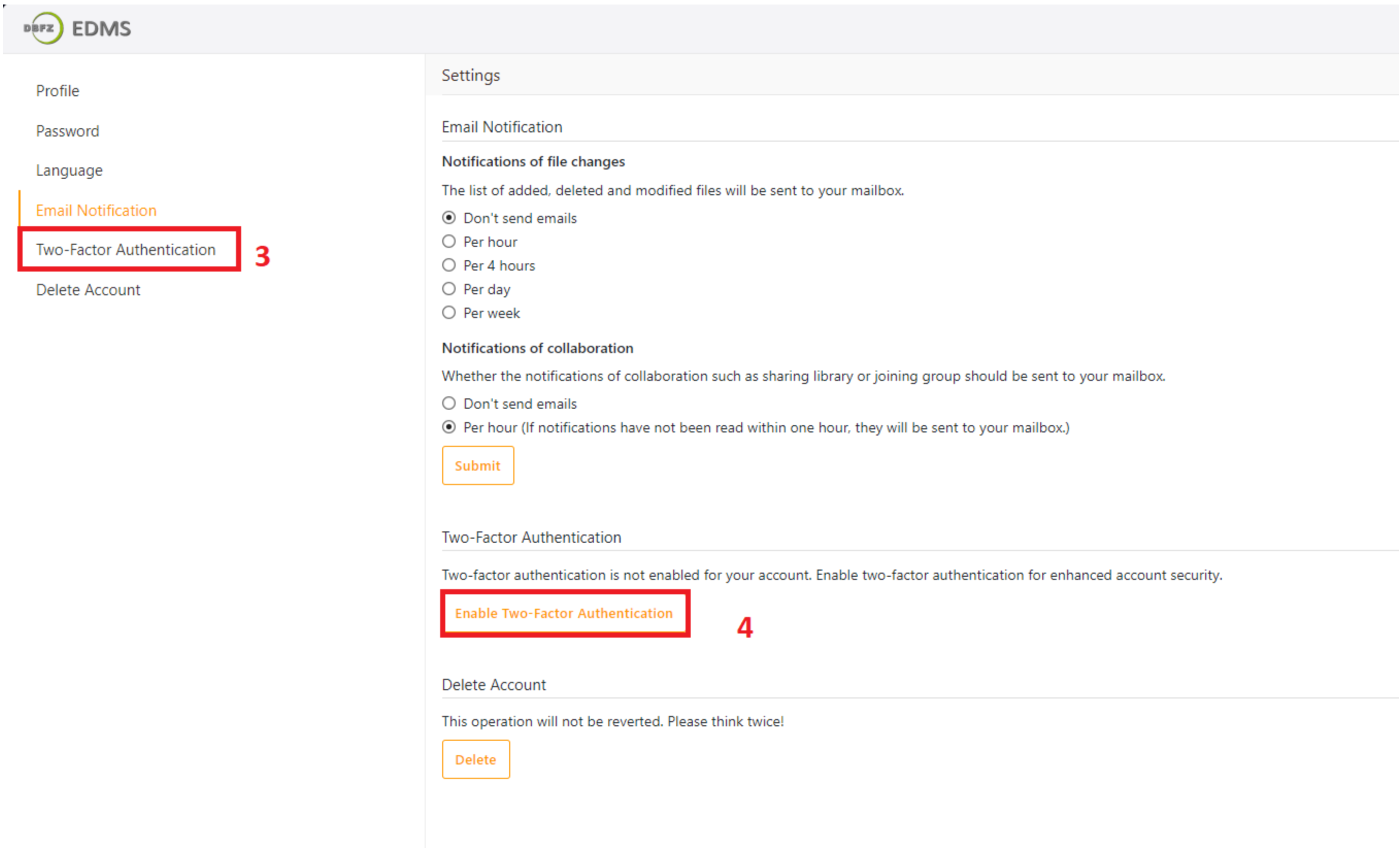
3 Apps for generating tokens

There are a couple of apps which can generate token. You could use FreeOTP, Google Authenticator or another app of your choice. Install these apps from the official app store of your smartphone.

4 Set up two-factor authentication in EDMS

You can already enable two-factor authentication in your EDMS profile and use it. For that you need to click on the user icon on the top right of the screen (1) after that go into the „settings" (2). After that you need to click on „two-factor authentication" (3) or just scroll down until you see that point. When you see the headline "two-factor authentication" you can enable it by clicking on the button beneath it (4).





Settings

Email Notification

Notifications of file changes

The list of added, deleted and modified files will be sent to your mailbox.

● Don't send emails
○ Per hour
○ Per 4 hours
○ Per day
○ Per week

Notifications of collaboration

Whether the notifications of collaboration such as sharing library or joining group should be sent to your mailbox.

○ Don't send emails
● Per hour (If notifications have not been read within one hour, they will be sent to your mailbox.)

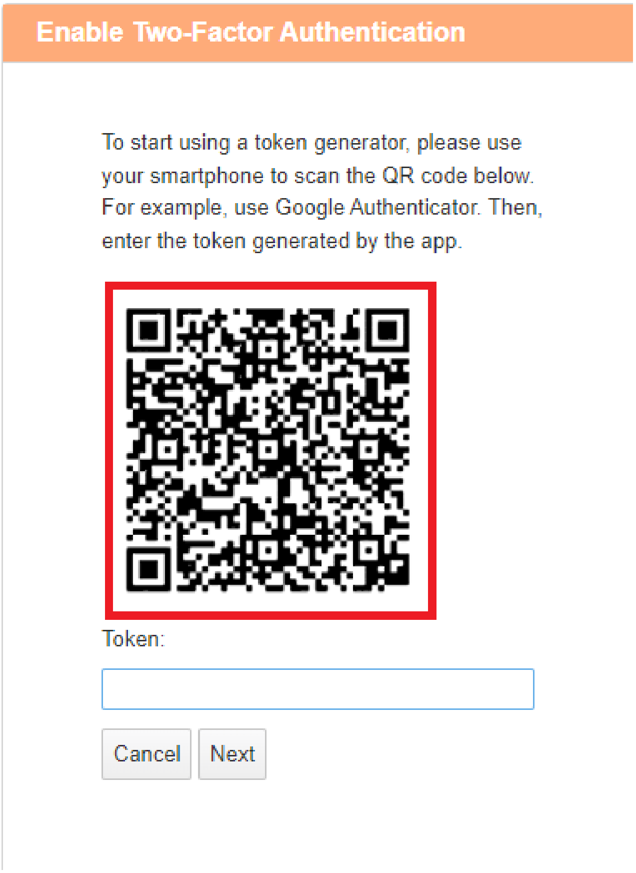
Two-Factor Authentication

Two-factor authentication is not enabled for your account. Enable two-factor authentication for enhanced account security.

Delete Account

This operation will not be reverted. Please think twice!

Now you need to scan the displayed QR-code with the token app of your choice (for example “Google authenticator” or “FreeOTP”).

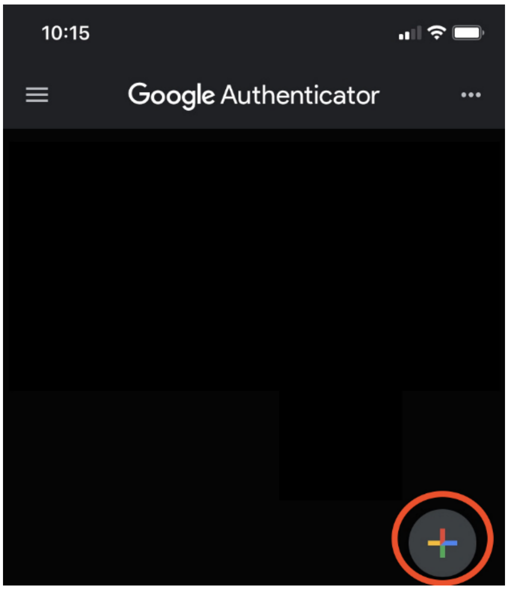


Enable Two-Factor Authentication

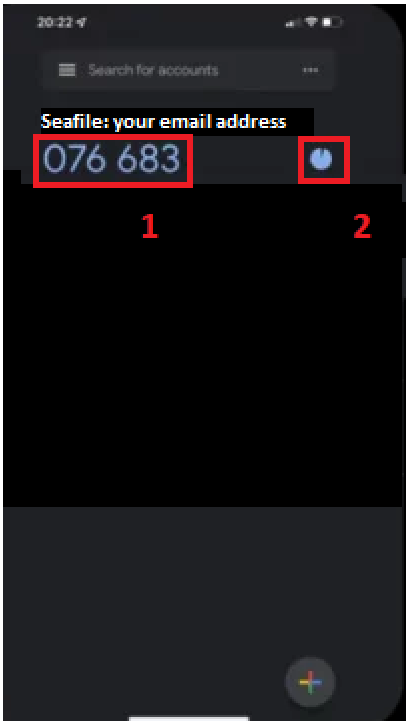
To start using a token generator, please use your smartphone to scan the QR code below. For example, use Google Authenticator. Then, enter the token generated by the app.

Token:

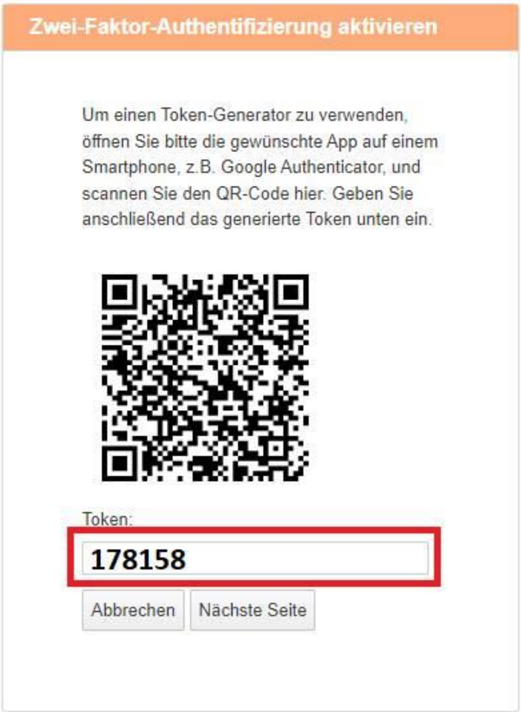
To do that open the app. We will use „Google Authenticator “in this example. Tap on the plus in the bottom right corner, then on “Scan QR-code” and point your camera at the QR-code.



Once you scanned that QR-code, a new entry will appear in the app named: Seafile: “your email address”. Right under that you will find a six-digit number combination (1) and a circle (2), which displays the valid time period for that number. After that little circle disappears, a new number will be generated and the previous one will be invalid. Once the number disappears, it will be invalid and the now displayed token will be valid.



You will need to type in that number into the “Token” space on the EDMS page and click “Next” while that token is still displayed as valid inside your token app.

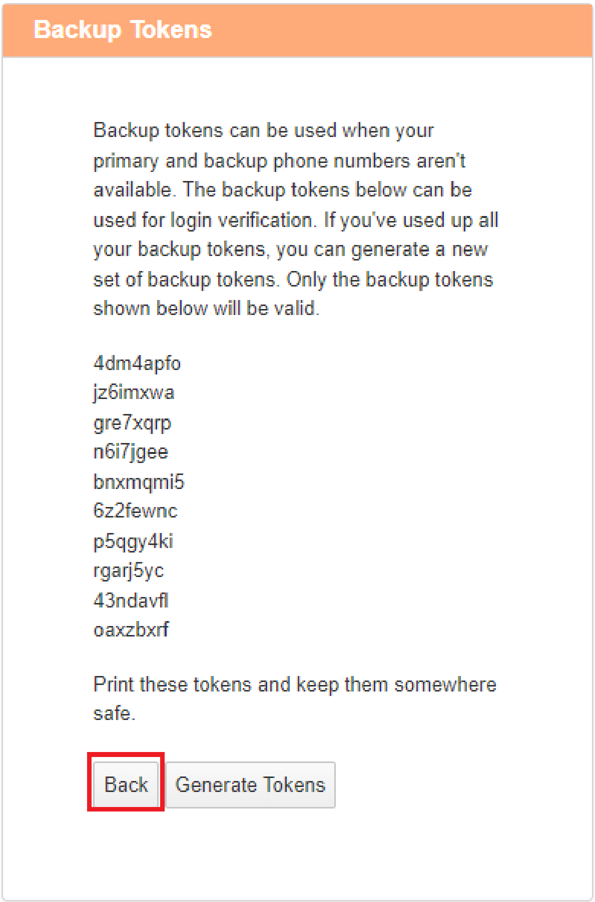


Zwei-Faktor-Authentifizierung aktivieren

Um einen Token-Generator zu verwenden, öffnen Sie bitte die gewünschte App auf einem Smartphone, z.B. Google Authenticator, und scannen Sie den QR-Code hier. Geben Sie anschließend das generierte Token unten ein.

Token: 178158

On the next page you will see a couple of backup tokens you can use in case you lose your phone or don´t have it with you and can´t generate a token because of that. Save these somewhere or print them out and click “Back”.



Backup Tokens

Backup tokens can be used when your primary and backup phone numbers aren't available. The backup tokens below can be used for login verification. If you've used up all your backup tokens, you can generate a new set of backup tokens. Only the backup tokens shown below will be valid.

4dm4apfo
jz6imxwa
gre7xqrp
n6i7jgee
bnxmqmi5
6z2fewnc
p5qgy4ki
rgarj5yc
43ndavfl
oaxzbxrf

Print these tokens and keep them somewhere safe.

5 Additional information

What is 2FA:
https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

Example video of someone activating 2FA in Seafile (but in german):
https://youtu.be/s5U9R34xMI8?t=76