

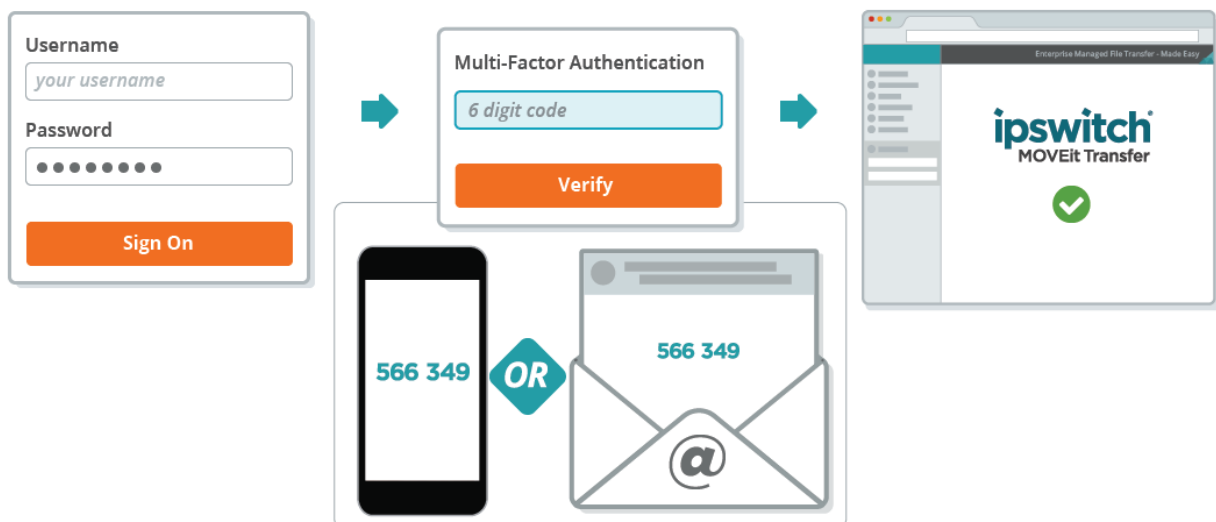
Protect your MOVEit account with Multi-Factor Authentication

Why should I use Multi-Factor Authentication?

Since MOVEit is a platform for exchanging data over the Internet, it is vulnerable to attacks on your credentials. Although you have to regularly change your password, your stored data is „only“ protected by username and password. If someone got access to your password, he could access your data on MOVEit.

This is where Multi-Factor Authentication (MFA) can help. Perhaps you already know the concept of MFA from online banking where you have to approve certain transactions with a one time code (TAN). MOVEit uses a similar concept during the login process: in addition to your username and password every sign on has to be authenticated using a one time code. This code (‘‘token’’) is simply generated with an app, which is available for your iOS- or Android smartphone.

If you can not use a smartphone or do not wish to do so, you can receive the token via eMail instead of an app. You can choose your preferred method when you set up MFA. Please keep in mind: if you choose to receive your token by eMail you won't be able to sign in to MOVEit during technical malfunctions of the eMail-System.



Is using MFA mandatory?

Due to an internal policy using MFA will be mandatory starting 13.09.2021. So activating it already now in the transitional period to gain experience will pay off.

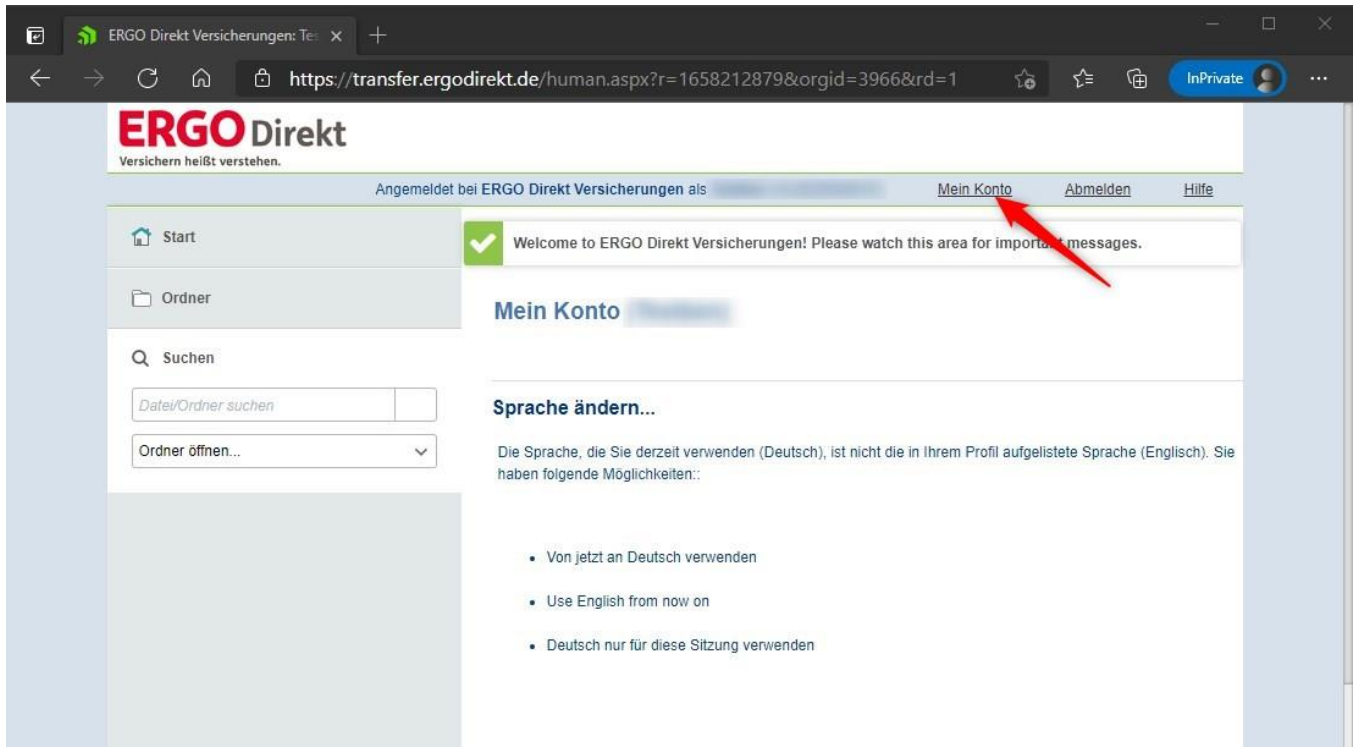
Technical accounts which are used for automated processes using SFTP/FTPS are not affected from this policy! All other accounts will be able to access MOVEit using MFA only via the Browser and the MOVEit Mobile App starting 13.09.2021.

Activating MFA is that easy!

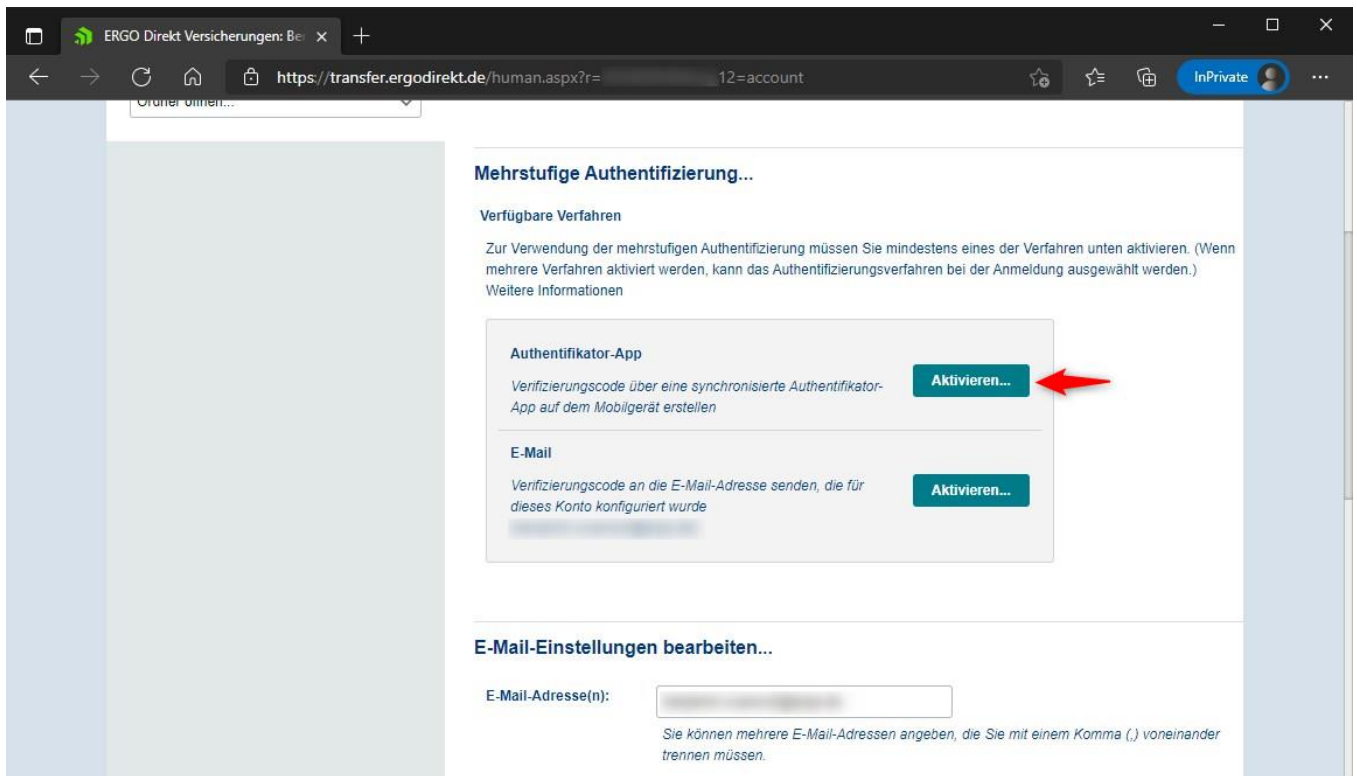
Option 1: Smartphone App

First of all you need an authenticator app on your iOS- or Android smartphone. We recommend using „Microsoft Authenticator“ or „Google Authenticator“, which can be found in the respective app stores and can be installed for free.

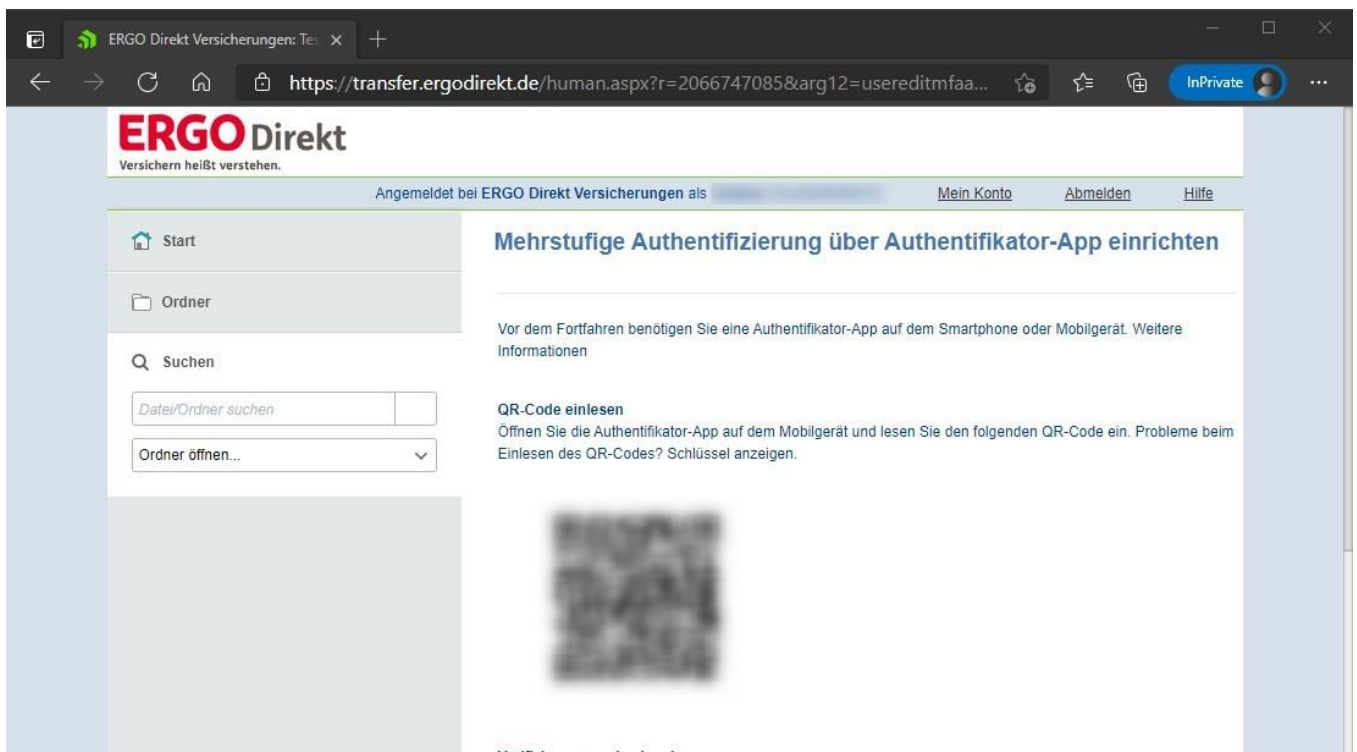
After you have installed the app, just log in to MOVEit and go to „My Account“ / „Mein Konto“:



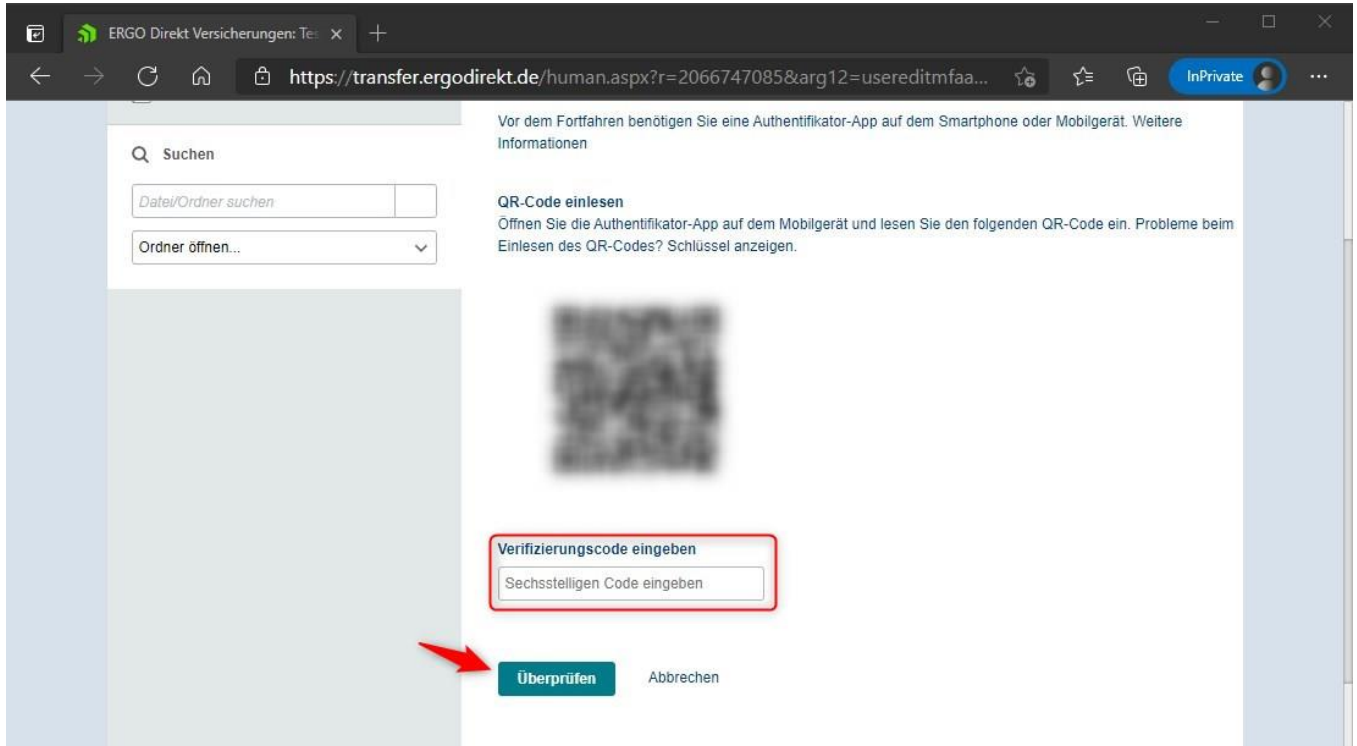
You will find the section „Multi-Factor Authentication“ / „Mehrstufige Authentifizierung“ and inside a box „Authenticator App“. Click „Enable“ / „Aktivieren...“:



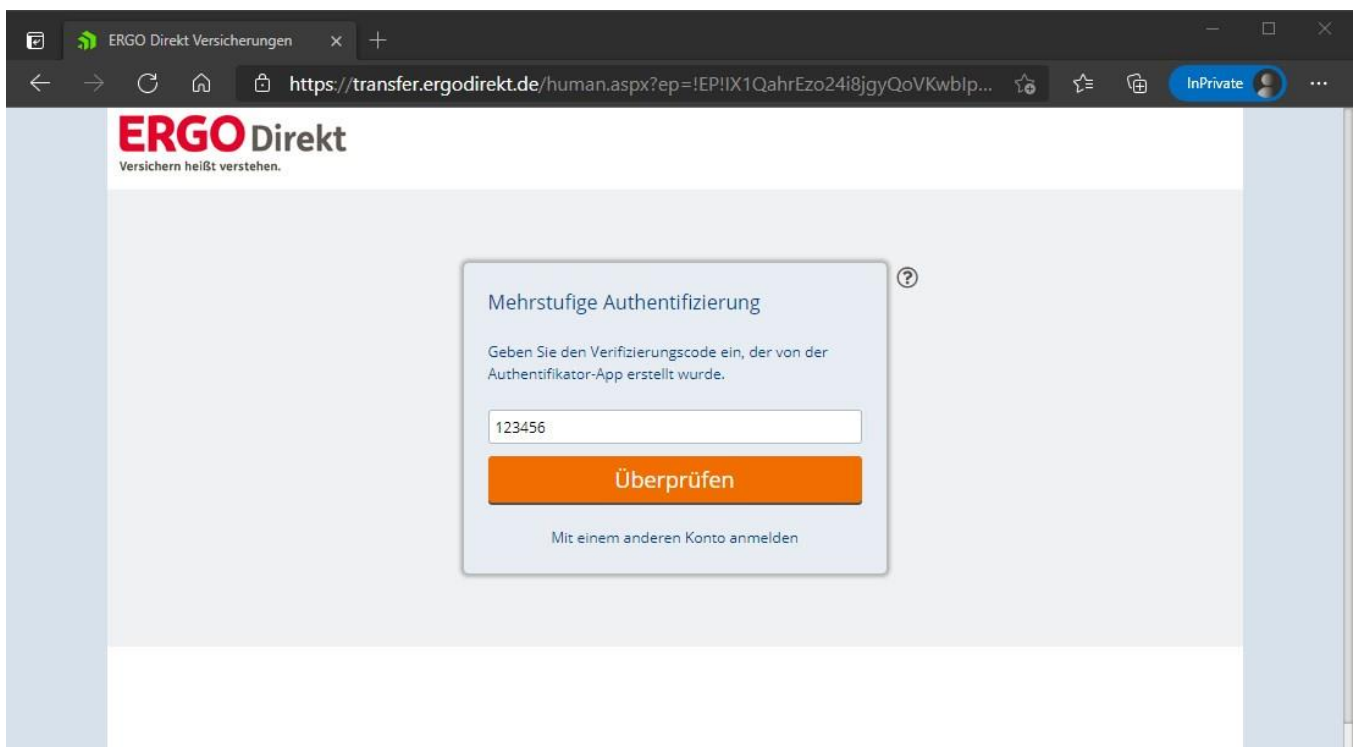
Now open your previously installed authenticator app on your smartphone and scan the QR code that is displayed on your screen:



After you scanned the code the authenticator app on your smartphone shows a 6-digit code. Please enter that code in the text field „Enter Verification Code“ / „Verifizierungscode eingeben“ and click on „Verify“ / „Überprüfen“:

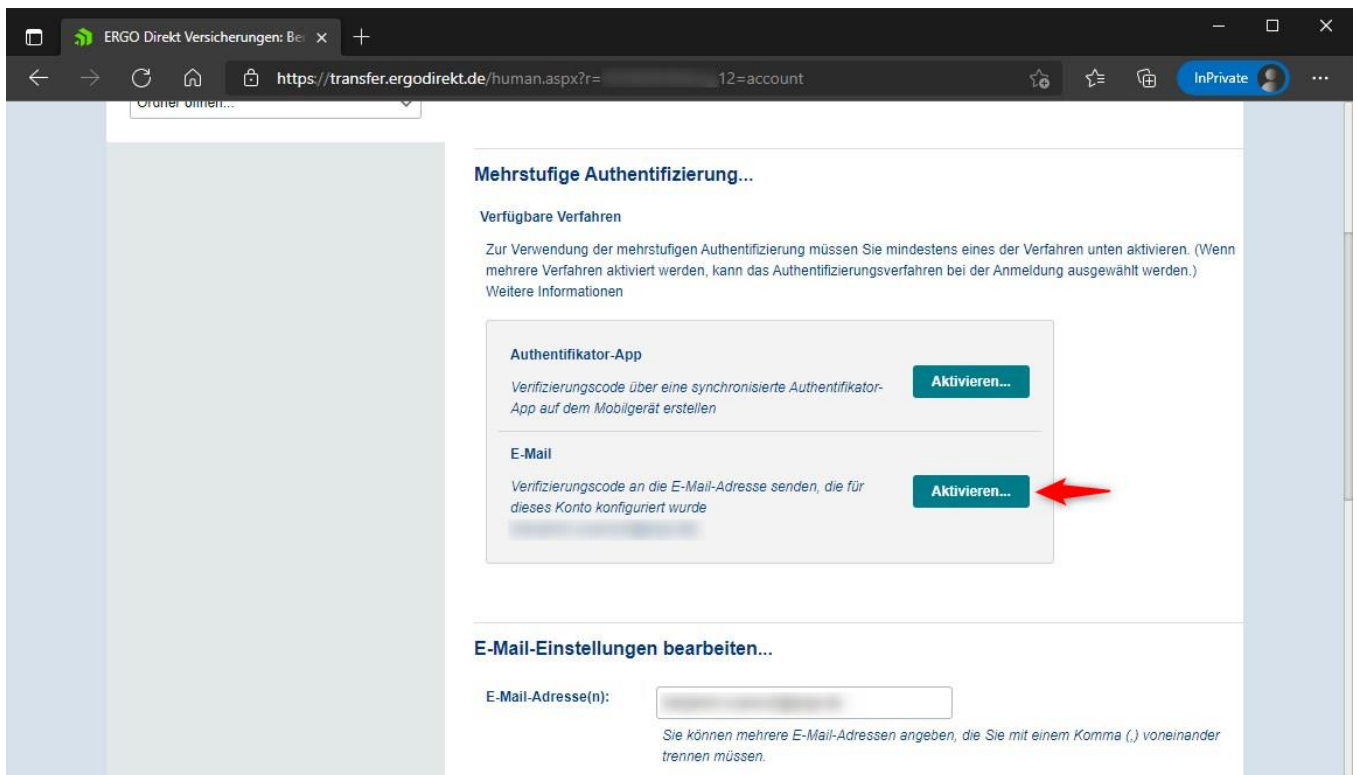


That's it! When you sign in to MOVEit the next time the system will ask you for an additional code after entering your username and password. Just start your authenticator app and enter the generated code to the text field:



Now you are logged in to MOVEit and can work as you are used to.

Activating MFA is that easy! Option 2: eMail



If you choose eMail, after clicking „Enable“ / „Aktivieren...“ you automatically will receive an eMail containing a six-digit activation code that you have to enter in MOVEit. If you did not receive the Mail please check your SPAM-Folder. After you confirm the activation code, you are logged in to MOVEit and MFA by eMail has been enabled.

In the future you will receive an eMail every time you log in with your Username and Password containing a token (which will be only valid for a very limited amount of time).

