

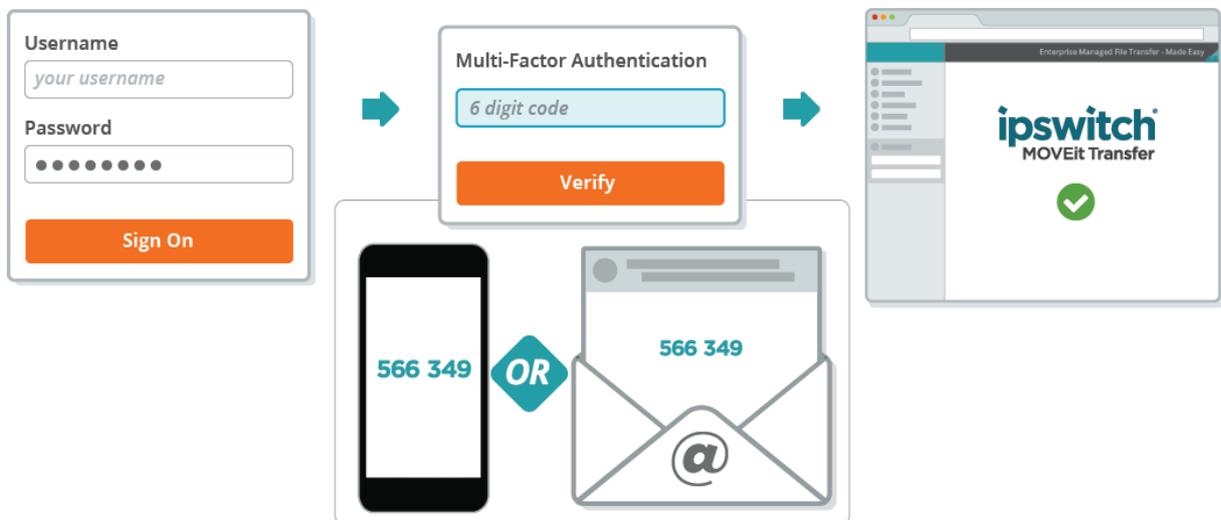
Absicherung Ihres MOVEit-Kontos mit Multi-Factor Authentication

Warum Multi-Factor Authentication?

MOVEit als aus dem Internet erreichbare Datenaustauschplattform ist grundsätzlich Angriffen auf Ihre Zugangsdaten ausgesetzt. Auch wenn Sie Ihr Kennwort regelmäßig ändern müssen, sind Ihre dort abgelegten Daten „nur“ mit Ihrem Benutzernamen und Ihrem Kennwort abgesichert. Sollte sich jemand Zugang zu Ihrem Passwort verschafft haben, kann er ohne Weiteres auf Ihre MOVEit-Daten zugreifen.

Hier kommt die Multi-Factor Authentication (kurz MFA) ins Spiel. Das Prinzip der MFA kennen Sie vielleicht aus dem Online-Banking, bei dem Sie diverse Aktionen mit einer einmal gültigen TAN bestätigen müssen. So ähnlich funktioniert auch die MFA bei MOVEit: zusätzlich zu Benutzernamen und Kennwort müssen Sie bei der Anmeldung einen einmal gültigen Zahlencode („Token“) eingeben. Diesen generieren Sie einfach über eine App, die für Ihr iOS- oder Android-Smartphone verfügbar ist.

Sollten Sie dafür kein Smartphone benutzen können oder wollen, können Sie alternativ den Token anstatt über die mobile App auch per eMail erhalten. Welche Methode Sie bevorzugen, können Sie bei der Einrichtung von MFA entsprechend auswählen. Bitte bedenken Sie: wenn Sie sich für den Versand per Mail entscheiden, können Sie sich während einer Störung des Mail-Systems nicht an MOVEit anmelden.



Ist die Einrichtung von MFA verpflichtend?

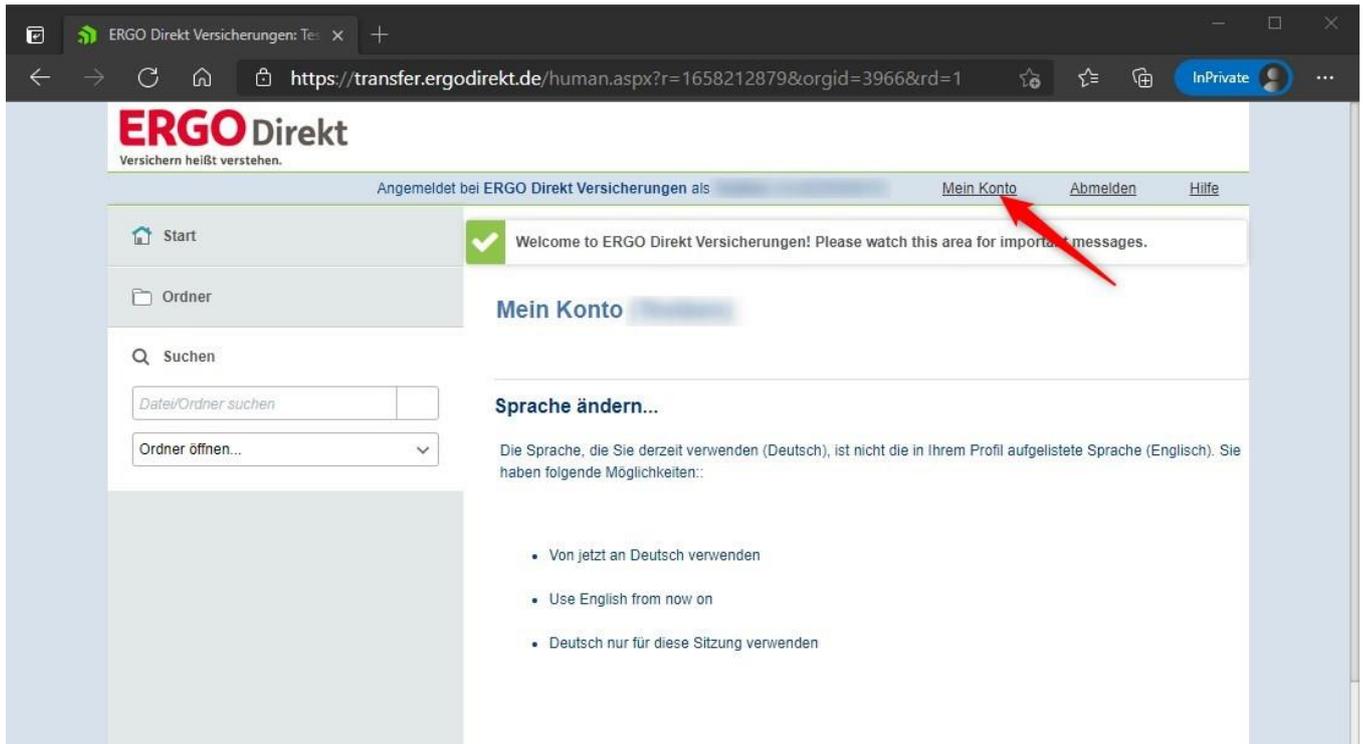
Ja, ab dem 13.09.2021 wird aufgrund einer Revisionsvorgabe MFA verpflichtend werden. Von daher lohnt es sich, bereits heute in der Übergangsphase aktiv zu werden, um erste Erfahrungen damit zu sammeln.

Technische User für automatisierte Prozesse via SFTP/FTPS sind von der Änderung nicht betroffen! Mit allen anderen Accounts wird ab dem 13.09.2021 jedoch nur noch ein Zugang mit MFA über den Browser bzw. die MOVEit Mobile App möglich sein.

So einfach richten Sie MFA ein Variante 1: Smartphone App

Zuerst benötigen Sie auf Ihrem iOS- oder Android-Smartphone eine entsprechende Authenticator App. Hier empfehlen wir Ihnen die Apps „Microsoft Authenticator“ oder „Google Authenticator“, die Sie beide in den jeweiligen App-Stores finden und kostenlos installieren können.

Melden Sie sich danach ganz normal an MOVEit an und klicken Sie rechts oben auf „Mein Konto“:



Dort finden Sie den Punkt „Mehrstufige Authentifizierung“ und darunter einen Kasten mit „Authenticator-App“. Klicken Sie in diesem auf den Button „Aktivieren...“:

Mehrstufige Authentifizierung...

Verfügbare Verfahren

Zur Verwendung der mehrstufigen Authentifizierung müssen Sie mindestens eines der Verfahren unten aktivieren. (Wenn mehrere Verfahren aktiviert werden, kann das Authentifizierungsverfahren bei der Anmeldung ausgewählt werden.)
Weitere Informationen

Authentifikator-App
Verifizierungscode über eine synchronisierte Authentifikator-App auf dem Mobilgerät erstellen **Aktivieren...**

E-Mail
Verifizierungscode an die E-Mail-Adresse senden, die für dieses Konto konfiguriert wurde **Aktivieren...**

E-Mail-Einstellungen bearbeiten...

E-Mail-Adresse(n):

Sie können mehrere E-Mail-Adressen angeben, die Sie mit einem Komma (,) voneinander trennen müssen.

Öffnen Sie nun die installierte Authenticator-App auf Ihrem Smartphone und scannen den auf dem Bildschirm angezeigten QR-Code damit:

ERGO Direkt
Versichern heißt verstehen.

Angemeldet bei ERGO Direkt Versicherungen als [Name] [Mein Konto](#) [Abmelden](#) [Hilfe](#)

Mehrstufige Authentifizierung über Authenticator-App einrichten

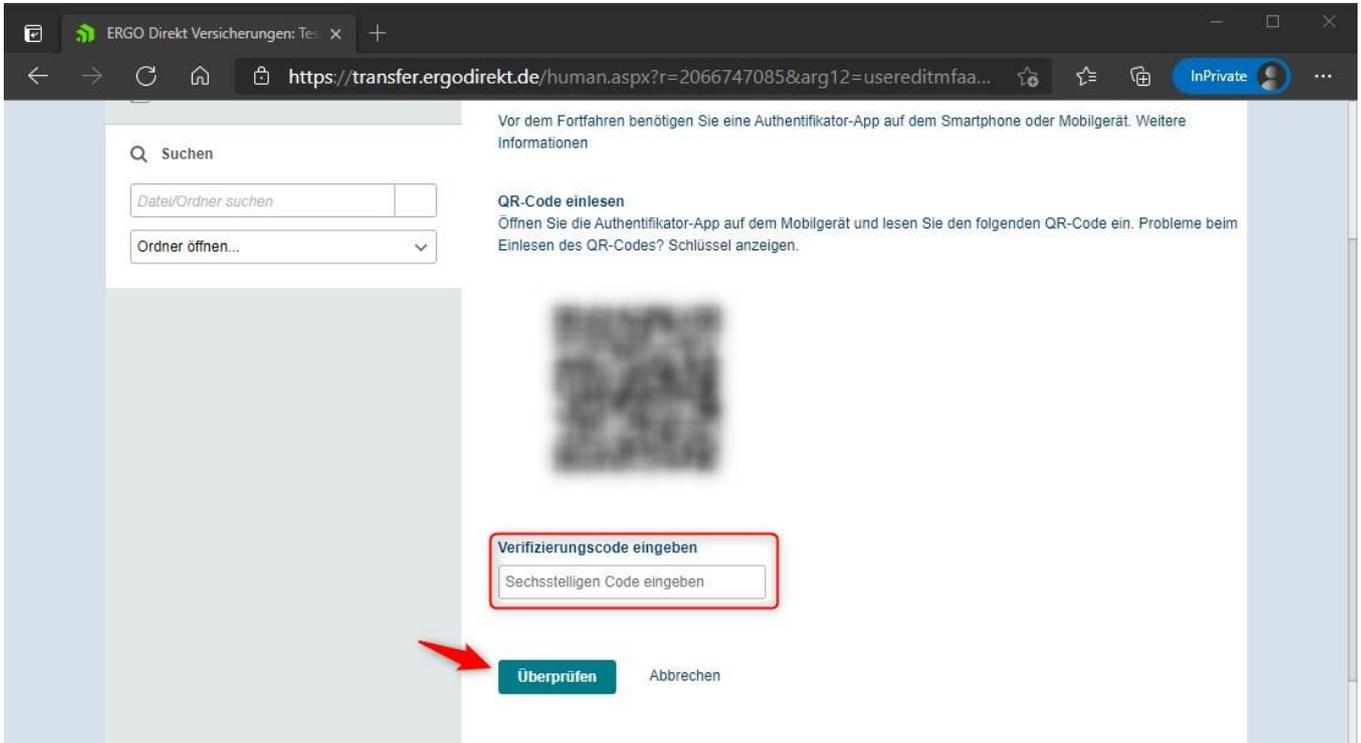
Vor dem Fortfahren benötigen Sie eine Authenticator-App auf dem Smartphone oder Mobilgerät. Weitere Informationen

QR-Code einlesen
Öffnen Sie die Authenticator-App auf dem Mobilgerät und lesen Sie den folgenden QR-Code ein. Probleme beim Einlesen des QR-Codes? Schlüssel anzeigen.

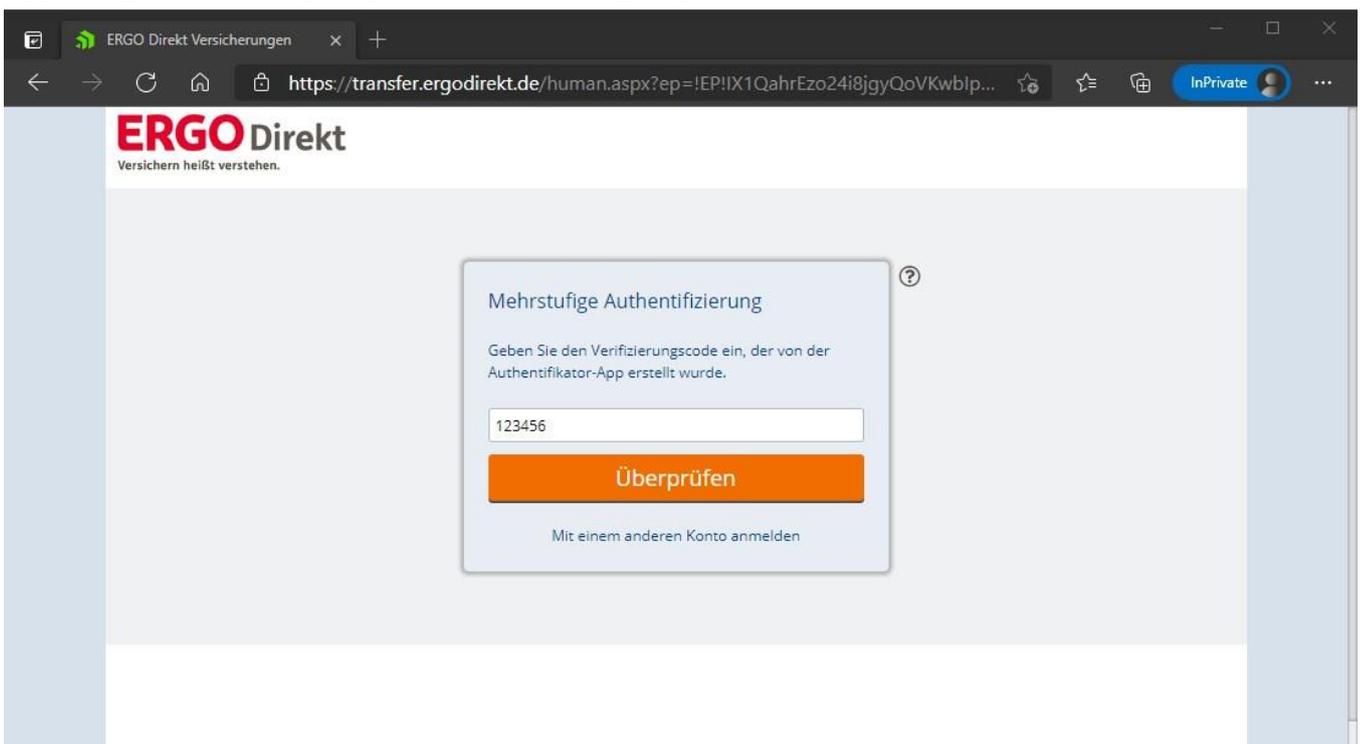


Verifizierungscode eingeben

Nachdem Sie den Code gescannt haben, zeigt Ihnen die Authenticator App auf dem Smartphone einen sechsstelligen Code. Diesen geben Sie bitte im Textfeld unter „Verifizierungscode eingeben“ ein und klicken anschließend auf „Überprüfen“:

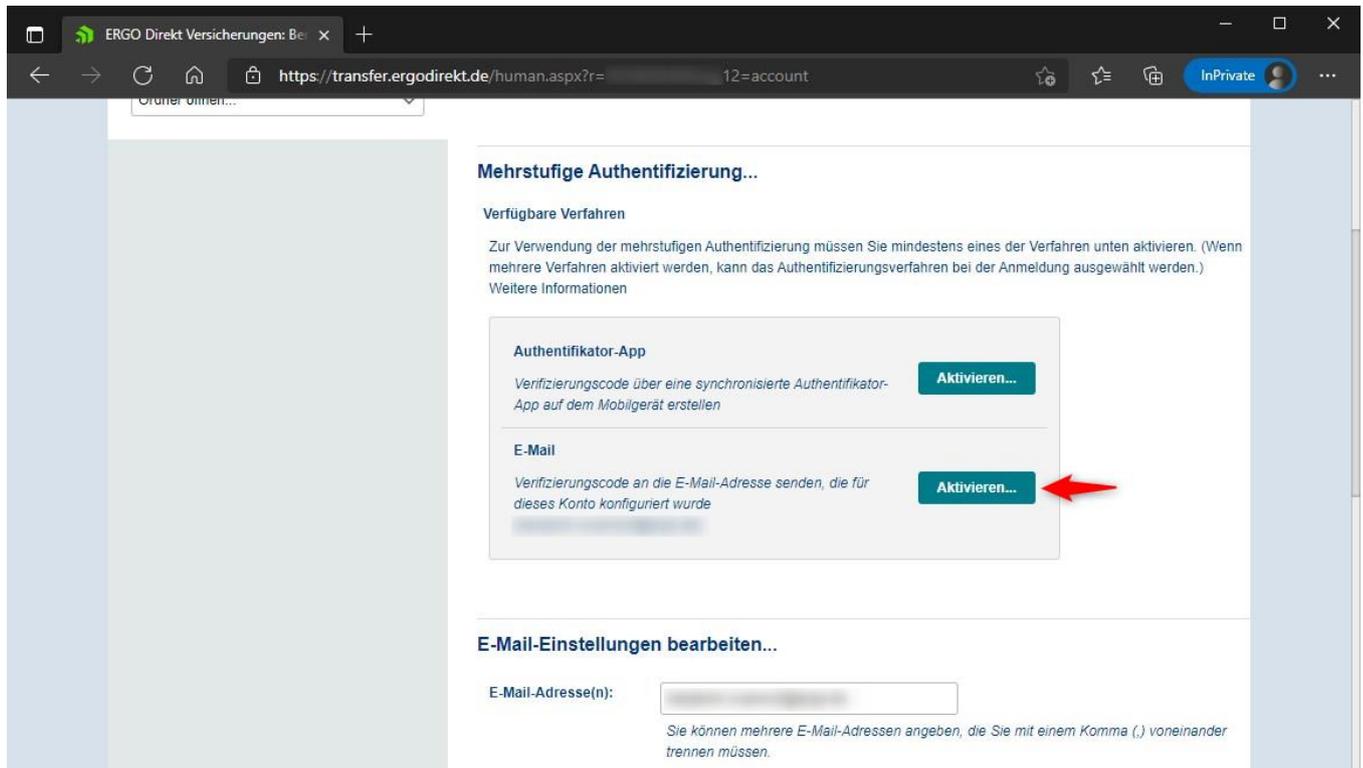


Das war schon alles! Ab der nächsten Anmeldung an MOVEit fragt das System Sie nach der Eingabe von Benutzernamen und Kennwort zusätzlich nach einem Code. Starten Sie dann einfach die Authenticator App und geben den angezeigten, 30 Sekunden gültigen, Code ein:



Danach sind Sie in MOVEit angemeldet und können wie gewohnt damit arbeiten.

So einfach richten Sie MFA ein Variante 2: eMail



Wenn Sie sich für die eMail-Variante entscheiden, wird nach dem Klick auf „Aktivieren“ automatisch eine Mail an die hinterlegte Mailadresse versandt, in der ein sechsstelliger Code zur Aktivierung enthalten ist und den Sie in MOVEit eingeben und bestätigen müssen. Sollten Sie keine Mail erhalten haben, prüfen Sie bitte Ihren SPAM-Ordner. Anschließend sind Sie in MOVEit angemeldet und MFA via eMail wurde aktiviert.

Künftig erhalten Sie dann bei jedem Login nach der Eingabe von Benutzernamen und Kennwort eine Mail mit einem (nur kurz gültigen) Token, den Sie bei der Anmeldung mit angeben müssen:

