Login mit 2-Faktor-Authentifizierung

22.04.2025 - Grundeinstellungen

Je nach Einstellungen durch die Administratoren ist Ihr Login mit einer Zwei-Faktor-Authentifizierung geschützt. Diese zusätzliche Sicherheitsebene stellt sicher, dass selbst wenn jemand Ihr Passwort kennt, er ohne den einmaligen Code nicht auf Ihr Konto zugreifen kann. Als 2. Faktor stehen E-Mail und Authenticator-App (Time-based one-time password, TOTP) zur Auswahl. Je nach Einstellungen durch die Administratoren stehen eine oder beide dieser Optionen zur Verfügung.

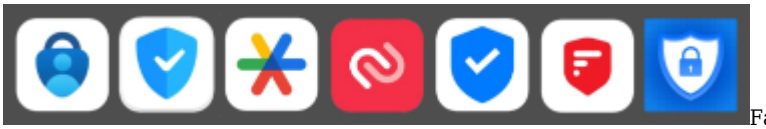
2FA mit E-Mail verwenden

Wenn Sie 2FA per E-Mail verwenden, brauchen Sie nichts einzurichten. Nach dem Login erhalten Sie den einmaligen Code auf Ihre E-Mail-Adresse zugestellt. Fügen Sie diesen in das verfügbare Feld, um den Login-Prozess abzuschliessen. Falls Sie keine solche E-Mail erhalten, prüfen Sie bitte auch den Spam-Ordner.

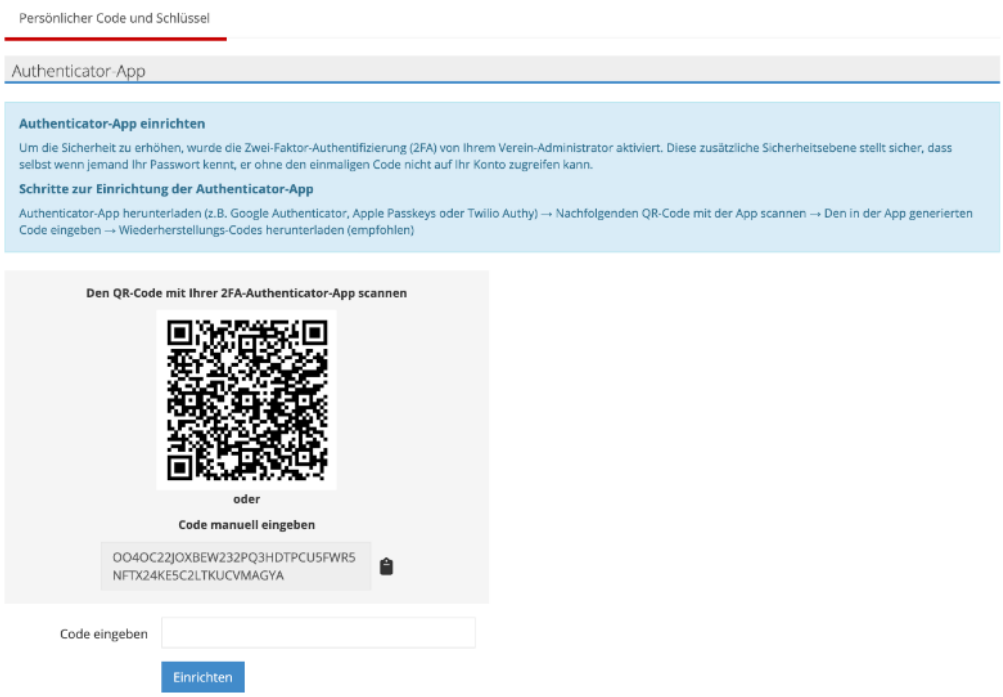
Wenn Sie den Haken bei “Ich bin auf vertrauenswürdigem Gerät” setzen, werden Sie beim nächsten Login vom gleichen Gerät diesen Schritt überspringen können.

2FA mit Authenicator-App einrichten

Für die Verwendung der Authenticator-App als 2. Faktor müssen Sie diese einmalig einrichten. Gehen Sie wie folgt vor:

1.  Falls Sie auf Ihrem Mobiltelefon noch keine Authenticator-App installiert haben, laden Sie sich eine solche herunter. Verbreitete Authenticator-Apps sind zum Beispiel Google Authenticator, Apple Keypass, Microsoft Authenticator und Twilio Authy.

2. Nach Ihrem Login bei Fairgate erscheint ein QR-Code. Die Authenticator-App enthalten eine Scan-Funktion, mit der Sie den QR-Code scannen und so das Konto hinzufügen können.

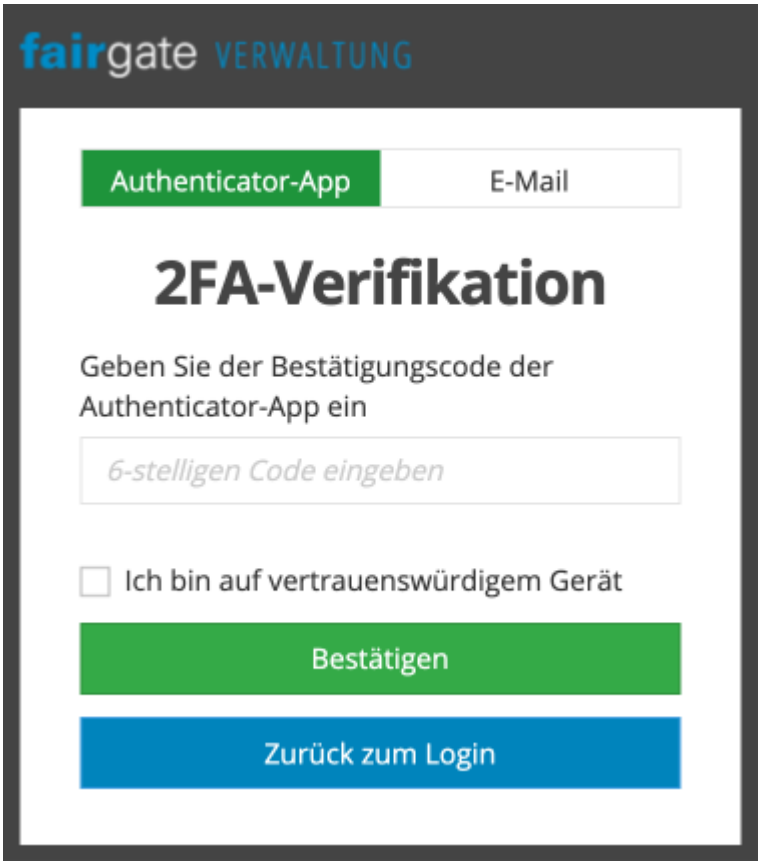


3. Die Authenticator-App generiert nun alle 30 Sekunden einen neuen 6-stelligen Code, der nach Ablauf der 30 Sekunden ungültig wird. Um die Einrichtung abzuschliessen, fügen Sie den aktuellen Code einmalig in das entsprechende Feld bei Fairgate.

4. Um sicherzustellen, dass Sie den Zugang zu Fairgate nicht verlieren, können Sie eine Datei mit Wiederherstellungs-Codes generieren und herunterladen. Speichern Sie diese an einem sicheren Ort, idealerweise in einem Passwort-Manager.

Einloggen mit Authenticator-App

Nach dem Login erhalten Sie ein Feld für den einmaligen Code angezeigt. Öffnen Sie Ihre Authenticator-App und rufen Sie den Code für das Konto für Ihre Organisation ab. Tippen Sie diesen in das Feld beim Fairgate-Login. Falls der Code ungültig ist, ist vermutlich die Gültigkeitsdauer von 30 Sekunden schon abgelaufen. Versuchen Sie es einfach mit dem nächsten Code nochmals.



Wenn Sie den Haken bei “Ich bin auf vertrauenswürdigem Gerät” setzen, werden Sie beim nächsten Login vom gleichen Gerät diesen Schritt überspringen können.

Wiederherstellungs-Codes verwenden

Haben Sie den Zugang zu Ihrer Authenticator-App verloren? In diesem Fall können Sie stattdessen einen bei der Einrichtung gespeicherten Wiederherstellungs-Code verwenden. Geben Sie diesen in das Feld der Fairgate 2FA-Verifikation ein. Jeder Wiederherstellungs-Code ist nur einmal verwendbar.