Benutzerkonto und Multi-Faktor-Authentisierung (MFA) – Anleitung zur Einrichtung

vom Juli 2025

1. Einleitung

Im Benutzerkonto oder Kundenportal melden Sie sich als Benutzer/-in zunächst mit ihrer E-Mail-Adresse und einem Passwort an. Im Fall eines Passwortdiebstahls besteht das Risiko, dass Dritte auf das Benutzerkonto zugreifen. Die Multi-Faktor-Authentisierung (**MFA**) bietet eine zusätzliche Sicherheitsebene für Ihr Benutzerkonto. Wer im Benutzerkonto oder Kundenportal persönliche Dienste nutzt (z.B. Steuerkonto, persönliche Online-Schalter-Geschäfte, Reservationen usw.), kann dieses Konto durch die Multi-Faktor-Authentisierung besser vor Drittzugriffen schützen.

Mit der Multi-Faktor-Authentisierung erzeugen Sie sich als zweiten Sicherheitsfaktor in einer Smartphone-App mit einem geheimen Schlüssel für jedes Login einen sicheren zeitbasierten Einmal-Code (einen sogenannten *Time Based OTP* oder *TOTP*). Viele Anbieter nutzen TOTP, um ihren Kunden mehr Sicherheit für ihr Benutzerkonto zu bieten.

Sie entscheiden frei, ob Sie die Multi-Faktor-Authentisierung nutzen möchten. Wir empfehlen Ihnen jedoch dringend, diese Funktion zu aktivieren und zu nutzen! Der Service lässt sich direkt im Benutzerkonto aktivieren.

2. Benötigtes Hilfsmittel: Authenticator-App

Um die Multi-Faktor-Authentisierung zu nutzen, brauchen Sie eine Authenticator-App. Sie können diese App frei wählen. Es gibt viele kostenlose und kostenpflichtige Lösungen, als Beispiele seien genannt: FreeOTP, Google Authenticator, Microsoft Authenticator, Apple Schlüsselbund, 1Password, LastPass. Meist wird die Authenticator-App auf dem eigenen Smartphone installiert.

Die gleiche Authenticator-App lässt sich für viele verschiedene Plattformen (kommerzielle Shops, Gemeinde-Website, ePortale etc.) nutzen. Wenn Sie bereits eine solche App benutzen, müssen Sie also keine weitere mehr installieren, um die Multi-Faktor-Authentisierung für das Benutzerkonto der Stadt Affoltern am Albis zu nutzen.

3. Benutzerkonto erstellen

Um MFA zu nutzen, benötigen Sie ein persönliches Benutzerkonto. Falls Sie noch kein Benutzerkonto haben, klicken Sie auf den Link "**Login**" im Kopfbereich des Webauftritts/Kundenportals (siehe Bild 1). So gelangen Sie zur Login-Maske, wo im unteren Bereich auch der Link "**Benutzerkonto erstellen**" zu finden ist (siehe Bild 2). Auf der folgenden Seite können Sie Ihr Konto anlegen, indem Sie Ihre E-Mail-Adresse angeben und ein sicheres Passwort setzen (siehe Bild 3).

Das Benutzerkonto lautet auf Ihre persönliche E-Mail-Adresse. Mit einem per E-Mail zugestellten Link bestätigen Sie, dass Sie tatsächlich Inhaber/-in des E-Mail-Kontos sind. Das Bestätigungsmail erhalten Sie kurz nach Erstellung Ihres Benutzerkontos.

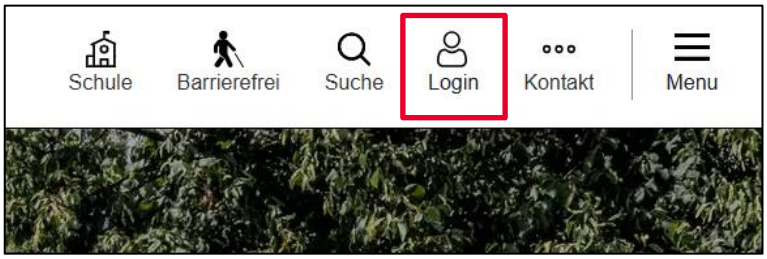

*Bild 1: Mit Klick auf **Login** gelangen Sie zur Login-Maske.*

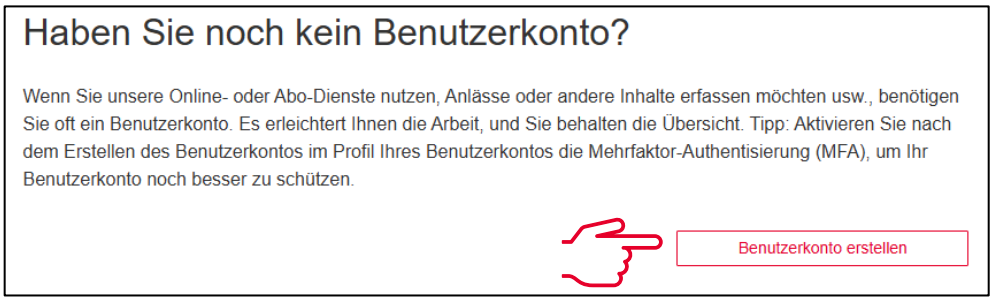

*Bild 2: Klicken Sie auf **Benutzerkonto erstellen**, um ein neues Konto anzulegen.*

Bild 3: Tragen Sie Ihre E-Mail-Adresse ein und wählen Sie ein sicheres Passwort.

4. Erstanmeldung

Sobald Sie ein Benutzerkonto erstellt und bestätigt haben, melden Sie sich über den Login-Link im Benutzerkonto an. Die Login-Maske erreichen Sie über denselben Link, den Sie auch für die Erstellung des Kontos benutzt haben (siehe Bild 1 im obigen Abschnitt).

Nach der ersten Anmeldung können Sie die Multi-Faktor-Authentisierung aktivieren (siehe Abschnitt 6).

5. Menü Benutzerkonto

Auch später besteht jederzeit die Möglichkeit, in Ihrem Konto die MFA zu aktivieren: Sobald Sie angemeldet sind, erscheint im Kopfbereich anstelle des Login-Links ein Personensymbol mit dem Textteil "**Konto**". Beim Anklicken oder Antippen erscheint das Menü mit den Funktionen Ihres Benutzerkontos.

Wählen Sie "**Benutzerkonto**" (siehe Bild 4 rechts).

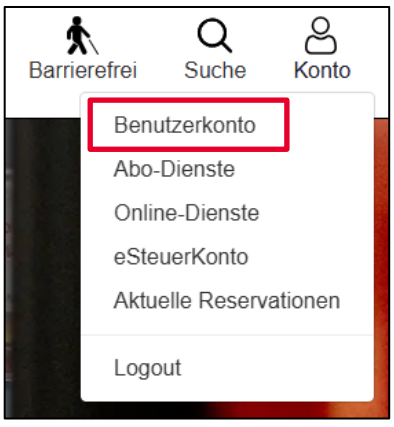

Bild 4: Benutzerkonto öffnen

Auf der Profil-Seite klicken Sie unten im Abschnitt "**Multi-Faktor-Authentisierung**" auf den Knopf "**MFA aktivieren**" (siehe Bild 5). Nun gelangen Sie auf die Seite zur Aktivierung der Multi-Faktor-Authentisierung.

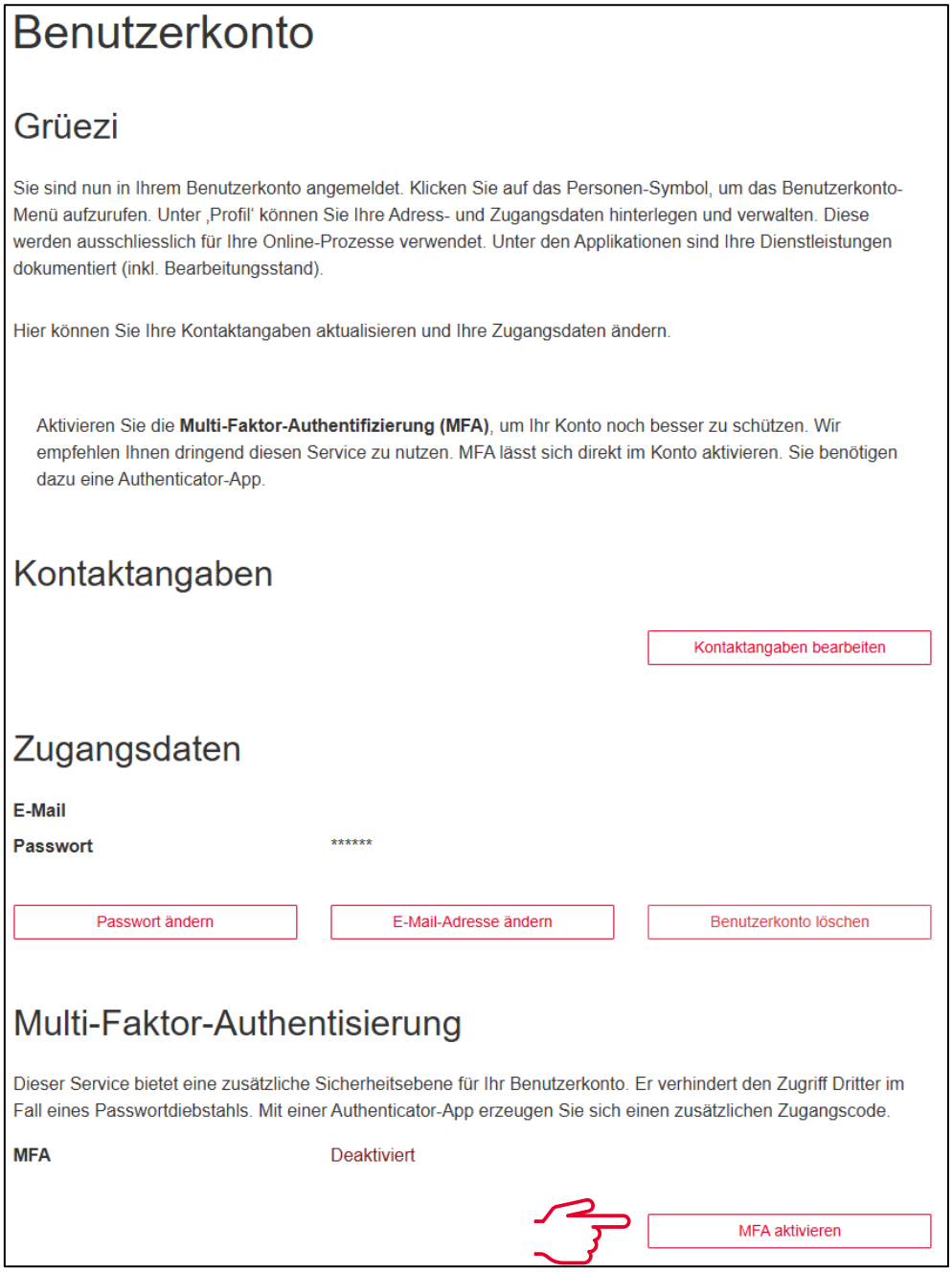

*Bild 5: Klicken Sie im unteren Bereich auf **MFA aktivieren**.*

6. Multi-Faktor-Authentisierung aktivieren

Auf der Seite zur Aktivierung der Multi-Faktor-Authentisierung werden Sie zur Eingabe eines Codes aufgefordert (siehe Bild 6). Um diesen Code zu erhalten, benötigen Sie Ihre Authenticator-App. Das weitere Vorgehen wird in Abschnitt 7 unten erläutert.

Bild 6: In das rot umrahmte Feld müssen Sie den Code aus der Authenticator-App eingeben, nachdem Sie diese eingerichtet haben (siehe Abschnitt 7 unten).

7. Zugangscode generieren

Für jede Plattform richten Sie sich in Ihrer Authenticator-App einen Zugangscode-Generator ein. Benennen Sie in der Authenticator-App jeweils das hinzugefügte Konto mit einer eindeutigen Plattform-Bezeichnung, falls dies nicht automatisch geschieht (im vorliegenden Fall zum Beispiel "Stadt Affoltern am Albis"). Einige Authenticator-Apps erzeugen automatisch eindeutige Bezeichnungen.

Der Zugangscode-Generator für Ihr Benutzerkonto benötigt den persönlichen QR-Code oder Sicherheitsschlüssel, den das Benutzerkonto Ihnen anzeigt (siehe Bild 6 oben; QR-Code und Sicherheitsschlüssel sind in dieser Anleitung verdeckt). Beim Aktivieren der Multi-Faktor-Authentisierung scannen Sie deshalb diesen QR-Code in Ihre Authenticator-App ein oder erfassen Sie dort den Sicherheitsschlüssel.

Nach erfolgreicher Erfassung des QR-Codes oder des Sicherheitsschlüssels erzeugt die Authenticator-App nun einen ersten Code. Diesen tragen Sie im Aktivierungsfenster des Benutzerkontos im Abschnitt "Zugangscode" ein. Klicken Sie danach auf "Bestätigen", um die Aktivierung der Multi-Faktor-Authentisierung abzuschliessen (siehe Bild 6 oben).

8. Backup-Codes

In einem nächsten Schritt werden Ihnen im Benutzerkonto Backup-Codes angezeigt. Diese Backup-Codes sind für den Fall gedacht, dass das Smartphone mit der Authenticator-App verloren geht oder entwendet wird. Am besten drucken Sie die Liste dieser Codes und bewahren sie an einem sicheren Ort auf (siehe Bild 7).

Wichtig: Beachten Sie bitte, dass jeder Code nur einmal verwendet werden kann. Die Codes müssen in der richtigen Reihenfolge verwendet werden. Im Benutzerkonto können Sie bei Bedarf weitere Codes erstellen.

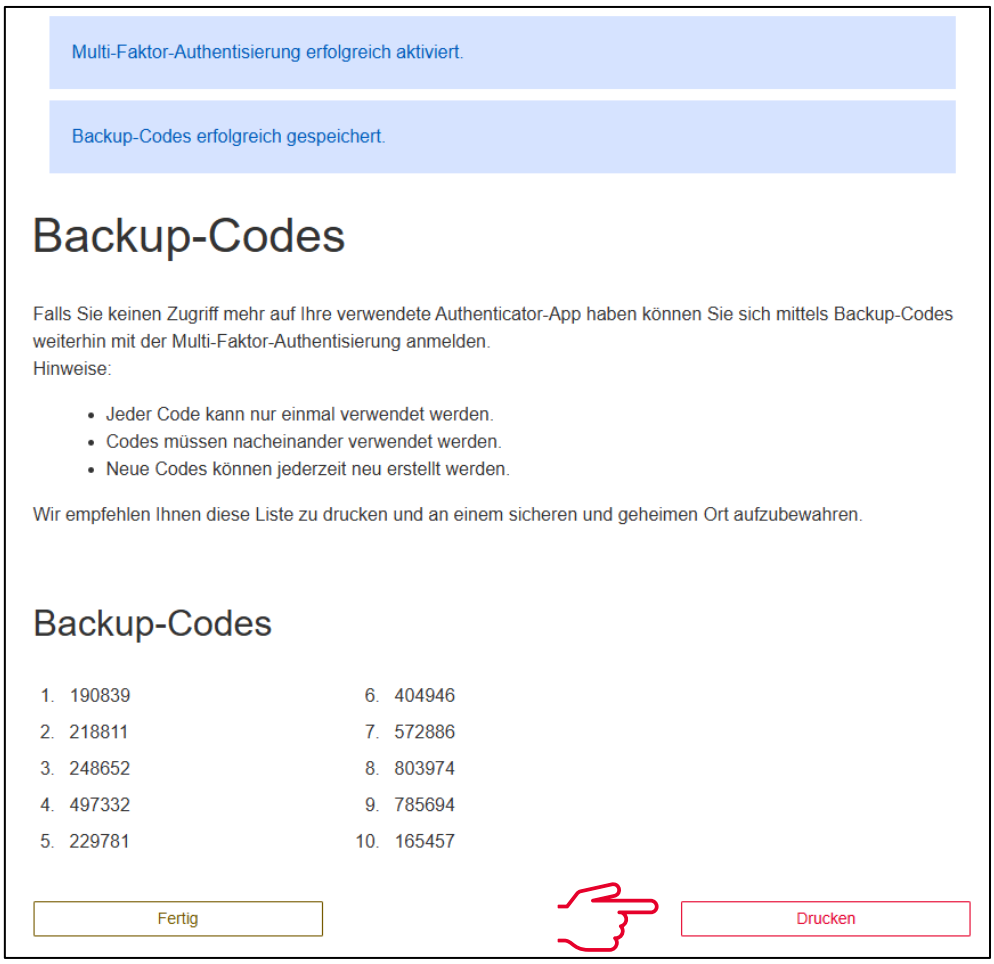

*Bild 7: Notieren oder speichern Sie alle Backup-Codes oder drucken Sie sie mit dem Knopf **Drucken** aus. Bewahren Sie diese Codes an einem sicheren Ort auf.*

9. Abmelden

Melden Sie sich immer ab, wenn Sie das Benutzerkonto oder den Webauftritt verlassen. Klicken Sie zu diesem Zweck auf das Personensymbol im Kopfbereich des Webauftritts und wählen Sie den Logout-Link (siehe Bild 8 rechts).

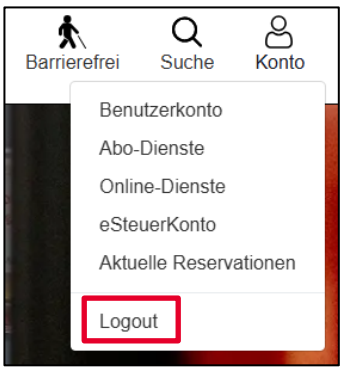

Bild 8: Abmelde-Link

10. Nächster Zugriff aufs Benutzerkonto: Zugangscode erzeugen

Wer im Benutzerkonto die Multi-Faktor-Authentisierung aktiviert hat, benötigt für jede Anmeldung im Benutzerkonto zusätzlich zur E-Mail-Adresse und zum persönlichen Passwort einen einmaligen Zugangscode.

Die Authenticator-App erzeugt diesen Zugangscode mithilfe des für Ihr Benutzerkonto hinterlegten Einrichtungsschlüssels. Wählen Sie also in der Authenticator-App die Plattform bzw. den Eintrag, der zum Benutzerkonto gehört (um beim Beispiel dieser Anleitung zu bleiben: "Stadt Affoltern am Albis"). Die App zeigt Ihnen nun einen Code an. Übertragen Sie den Code ins Feld „Zugangscode“ und klicken Sie auf „Prüfen“ (siehe Bild 9).

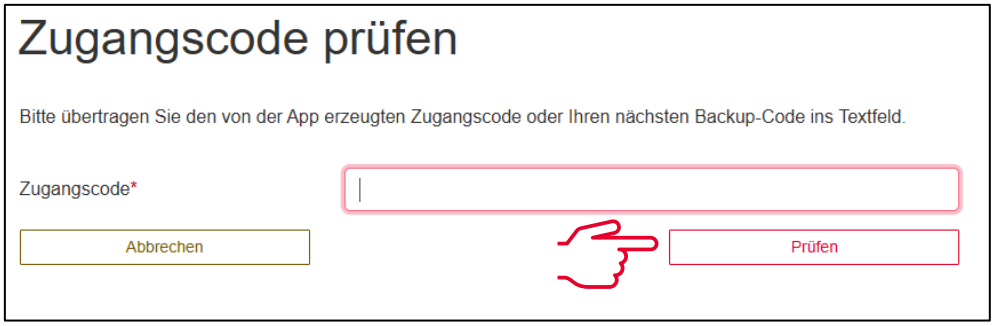

*Bild 9: Übertragen Sie den Code aus der Authenticator-App in das rot umrahmte Feld und klicken/tippen Sie dann auf **Prüfen**.*

Hinweis: Die Authenticator-App erzeugt Codes, die jeweils 30 Sekunden gültig sind. Läuft ein Code ab, wird sofort ein neuer generiert, der wiederum 30 Sekunden gültig ist. Meist sehen Sie in der App, ob ein Code in wenigen Sekunden abläuft. Warten Sie in diesem Fall, bis ein neuer Code angezeigt wird. Diesen können Sie dann übertragen und sich im Benutzerkonto anmelden.