2-FA

2FA – Zwei-Faktor-Authentifizierung

Was ist das?

2FA ist eine **Sicherheitsmaßnahme**, bei der **zwei verschiedene Faktoren** verwendet werden, um deine Identität zu bestätigen – nicht nur ein Passwort.

z.B. Ein Code per SMS, Code in einer App (Google Authenticator), Fingerabdruck, Gesichtsscan, ein USB-Sicherheitsschlüssel

Wozu braucht man das?

Um **Konten und Daten besser zu schützen**. Selbst wenn jemand Ihr Passwort kennt, reicht das allein nicht mehr aus.

OTP wird genutzt, um **Konten zusätzlich abzusichern**, z. B. beim Online-Banking, in E-Mail-Diensten oder bei Cloud-Logins. Es ist Teil der sogenannten **Zwei-Faktor-Authentifizierung (2FA)**

OTP – One-Time Password

Was ist das?

Ein OTP ist ein **einmalig gültiges Passwort**, das für die **Authentifizierung** verwendet wird. Es ist nur für eine kurze Zeit oder einen einzigen Login-Vorgang gültig.

TOTP - Time-based One-Time Password (benutzen wir)

ist ein Algorithmus zur Zwei-Faktor-Authentifizierung, der nur auf der aktuellen Uhrzeit basiert, um alle 15 - 30 Sekunden ein neues, einmaliges Passwort zu generieren. Die Codes werden lokal auf einem Gerät (z. B. mit einer App wie Google Authenticator) erstellt und mit dem Server verglichen, um die Identität des Nutzers zu bestätigen.

Wie funktioniert es?

- Sie geben Ihren Benutzernamen + Passwort ein
- Danach bekommen Sie ein OTP (z. B. per SMS, App oder E-Mail)
- Erst mit diesem zusätzlichen Code können sie sich einloggen

Gegen was ist man besser geschützt?

- **Phishing:** Selbst wenn jemand Ihr Passwort entwendet, bekommt der jenige ohne das OTP keinen Zugang zu ihren Account
- **Hackerangriffe:** Besonders wirksam bei gestohlenen oder schwachen Passwörtern
- **Identitätsdiebstahl:** Erschwert unbefugten Zugriff

TOTP ist ein offener Standard. Entscheiden Sie sich für eine dieser Apps - welche Sie nehmen, ist egal

App	Authy	Google Authenticator	WinOTP Authenticator
App-Logo			
Plattformen zur Installation	Android/iOS über Play Store / App Store Desktop (Windows/macOS/Linux): eigenständige Apps von authy.com	Android/iOS über Play Store / App Store (nur mobil)	Windows 10/11 via Microsoft Store (UWP-App)
Hersteller- & Anbieter-unabhängig	Unterstützt alle Dienste mit TOTP (z. B. Google, Facebook, Amazon u.v.m.)	Funktioniert mit jedem Dienst, der QR-Codes oder TOTP-Schlüssel ausgibt	Offener Standard (TOTP/RFC 6238), funktioniert überall dort, wo ein QR-Code oder Geheimschlüssel vorliegt

Besonderheiten	Multi-Device & Cloud-Backup (verschlüsselt), PIN/biometrische Sicherheit & Master-Passwort, Desktop-Variante verfügbar	Sehr schlank und einfach Keine Cloud-Backup-Funktion (lokal) Export via QR-Codes möglich, meist manuell	Open-Source, QR-Code-Import oder manueller Schlüssel Clipboard-Clearing bei Ablauf, NTP-Sync Nur für Windows geeignet

Anleitung mit Authy

1. **App Herunterladen**

1.1 Besuchen Sie zunächst Ihren **App Store** und navigieren Sie zu der „**Suchleiste**“.

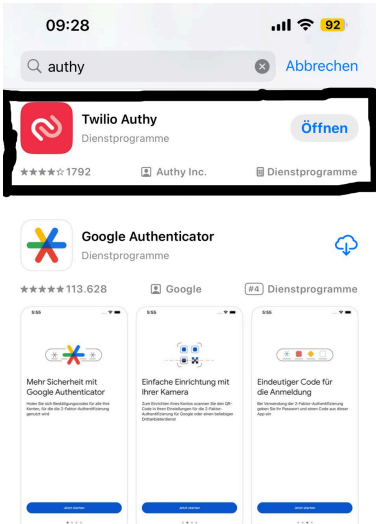
2. Suchen Sie nun in der **Suchleiste** nach „**Authy**“.

3. **Laden** Sie nun die „**Authy**“ App herunter und öffnen Sie sie danach.

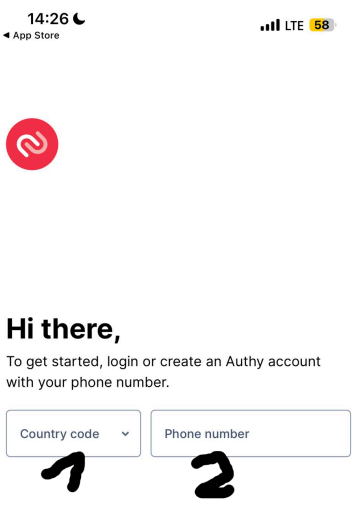
4 .1 Geben Sie nun die Vorwahl (1) an. (In Deutschland +49)

4.2 Geben Sie hier Ihre Telefonnummer an. (2)

4.3 Bestätigen Sie Ihre Eingabe und fahren Sie fort. (3)







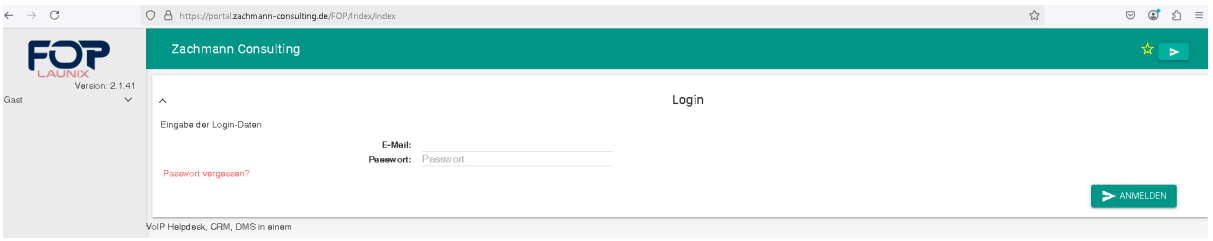
5 . Rechts unten finden Sie nun einen Knopf mit einem „**+**“ drauf.

5.1 Klicken Sie nun auf diesen Knopf.

6. **<u>Kundenportal öffen</u>**

6.1 Gehen Sie jetzt zunächst in einen **beliebigen Browser** (Edge, Firefox, Opera etc.) und rufen Sie unser **Kundenportal** auf. (https://portal.zachmann-consulting.de)

6.2. Loggen Sie sich mit ihren Zugangsdaten ein



6.3 Gehen Sie nun links oben, unter der Aufschrift „FOP Launix“ auf den **Pfeil nach unten**.

6.4 Wählen Sie nun „**2-Faktor-Authentifizierung“** im Fenster.

6.5 Geben Sie Ihr aktuelles Passwort ein und klicken Sie danach auf „**Geheimnis erneuern**“.

Der “**Geheimcode**” steht unter dem QR-Code.



7. Nun zurück in die „**Authy**“ - App.

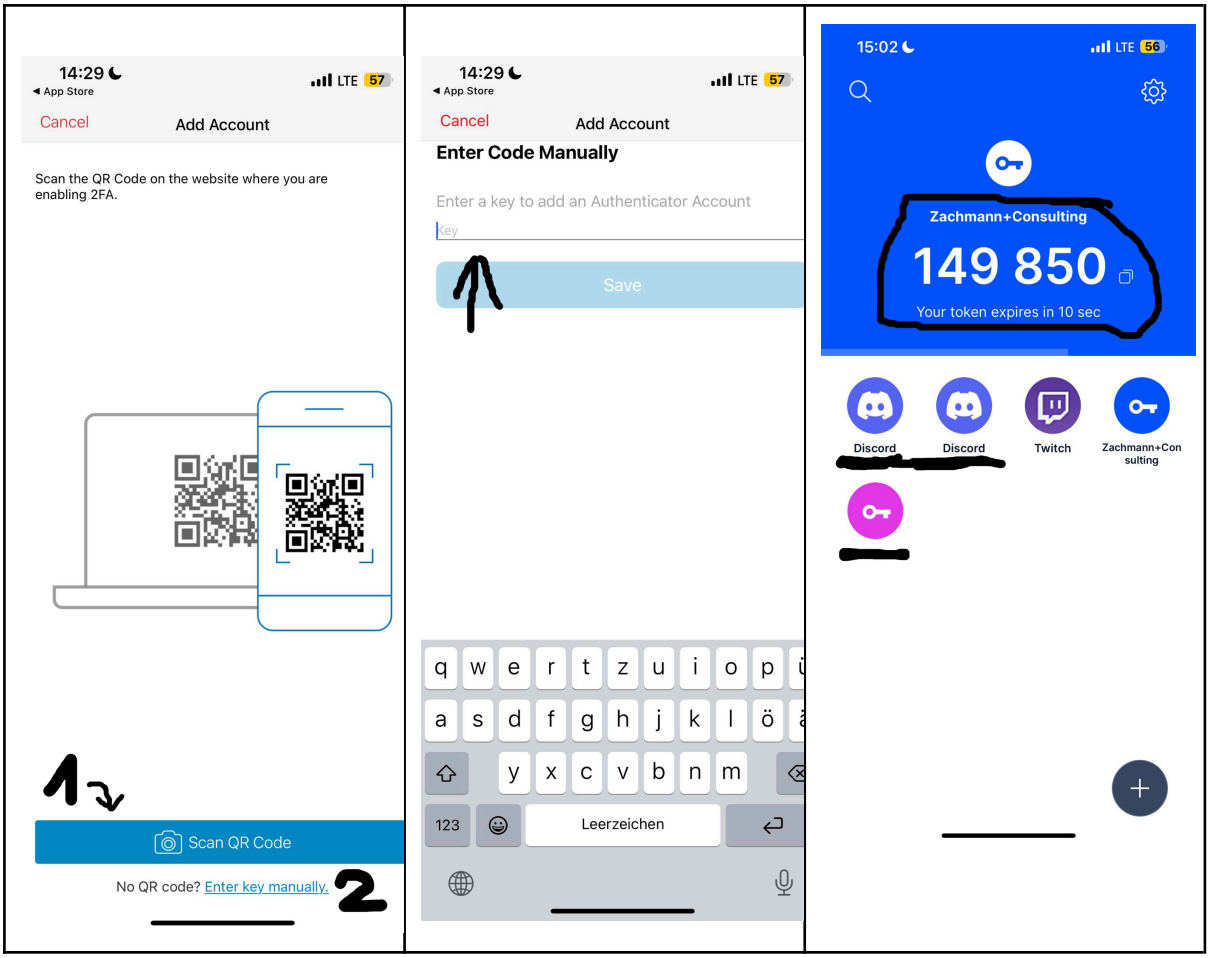
7.1 Sie können jetzt entweder den QR- Code auf unserer Seite scannen… (1)

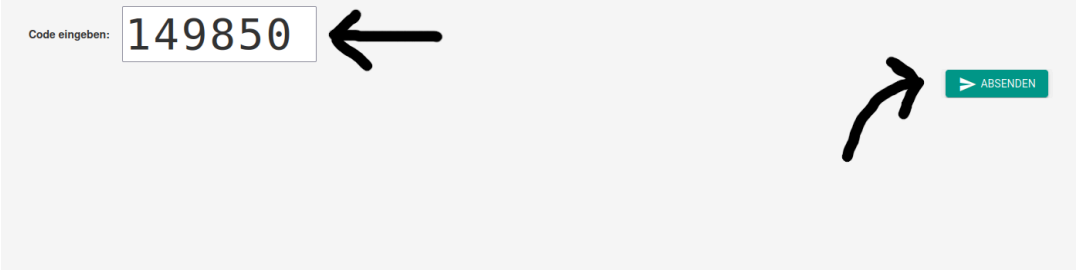
7.2 … oder sie klicken auf die andere Option und tragen den **Geheimschlüssel** manuell ein. (2)

7 .2.2 Sollten Sie sich für Option (2) entschieden haben, tragen Sie den Schlüssel in das Feld ein und bestätigen Ihre Eingabe durch klicken auf den blauen Knopf.

8. Geschafft! Sie haben erfolgreich ihren „**Einmalcode**“ eingerichtet

9 . Beachten Sie dass Sie ab nun bei **JEDER ANMELDUNG** diesen Einmalcode abrufen müssen!





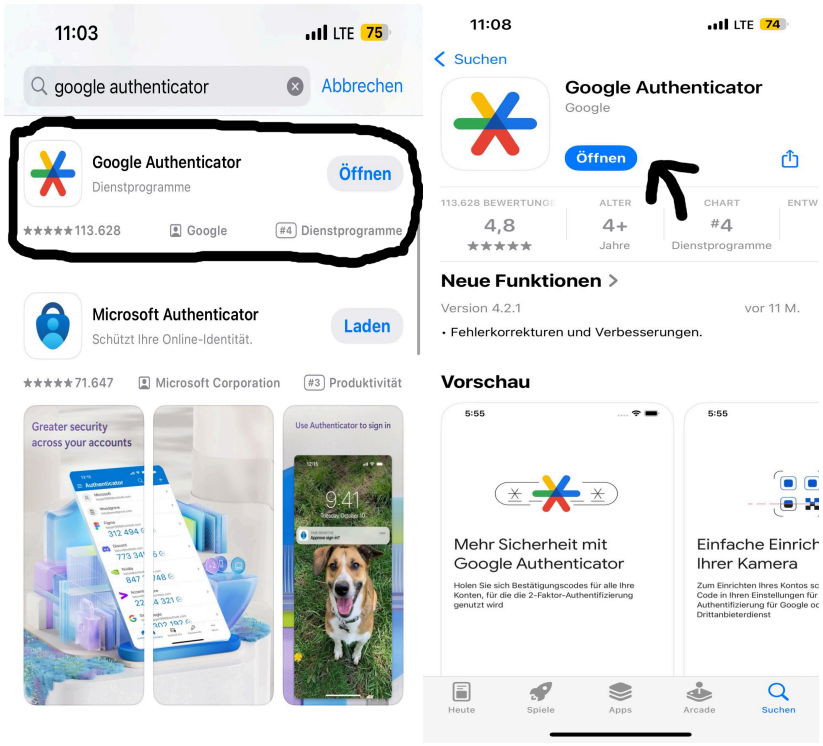
Anleitung mit Google Authenticator

1. Besuchen Sie zunächst Ihren **App Store** und navigieren Sie zur „**Suchleiste**“.

2. Suchen Sie nun in der **Suchleiste** nach „**Google Authenticator**“. (in Bild eingekreist)

3. **Laden** Sie nun die „**Google-Authenticator-App**” herunter und öffnen Sie sie danach.

4. Sobald die App geöffnet ist **klicken** sie unten den blauen Knopf mit der Aufschrift



„Jetzt starten“

5. Google wird Ihnen nun eine E-mail anbieten, die für Authenticator genutzt werden soll. Wählen Sie eine Email die genutzt werden soll

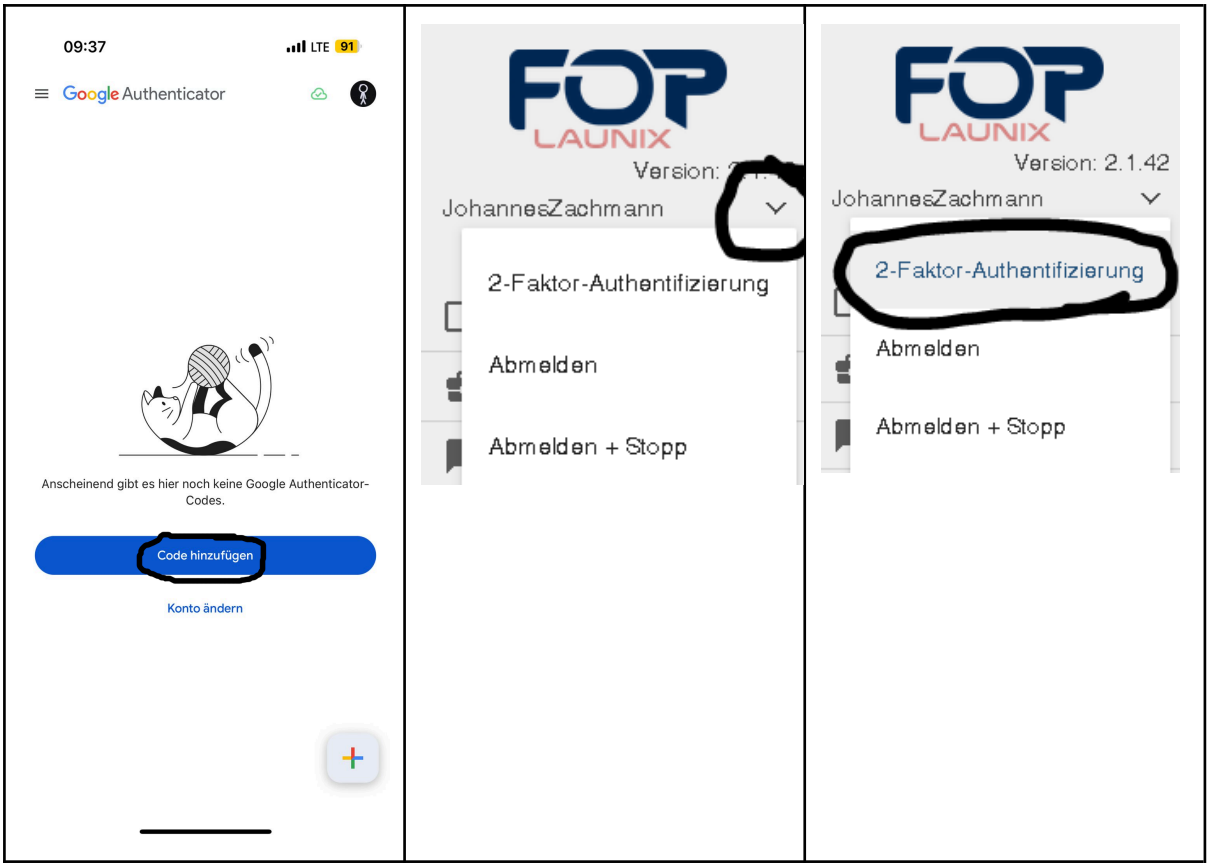
6. Nun müssen Sie den **Einmalcode** noch **hinzufügen.** Drücken sie also auf „**Code hinzufügen**“.

7. Gehen Sie jetzt zunächst in einen **beliebigen Browser** (Edge, Firefox, Oper etc.) und rufen Sie unser **Kundenportal** auf (https://portal.zachmann-consulting.de)

7.1. Loggen Sie sich mit ihren Zugangsdaten ein

7.2 Gehen Sie nun links oben, unter der Aufschrift „FOP Launix“ auf den **Pfeil nach unten**.

7.3 Wählen Sie nun „**2-Faktor-Authentifizierung“** im Fenster.



7.4 Geben Sie Ihr aktuelles Passwort ein und klicken Sie danach auf „**Geheimnis erneuern**“. Der Code unter dem QR Code ist der „**Geheimcode**“.



8. Nun zurück in den „**Google Authenticator**“.

8.1 Geben Sie einen Kontonamen (1) an. (am besten Zachmann Consulting)

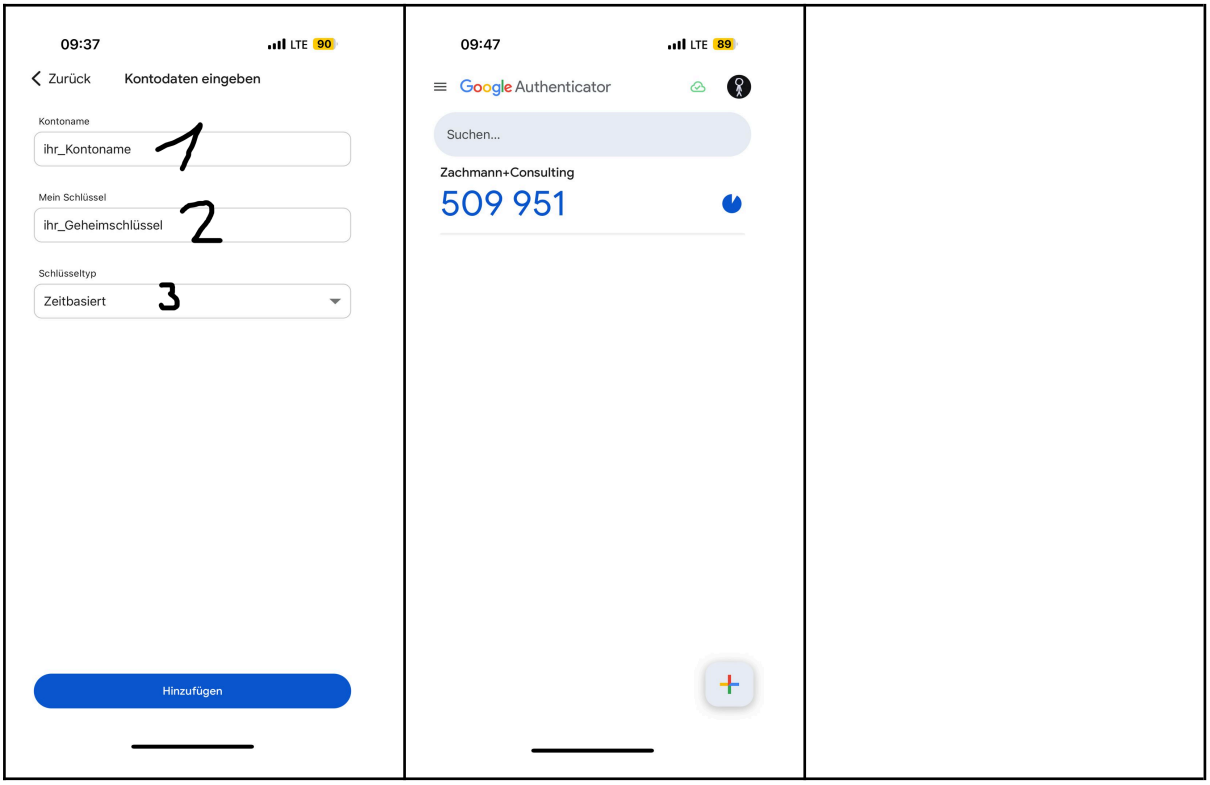
8.2 Geben Sie jetzt auch Ihren **Geheimcode** (2) ein.

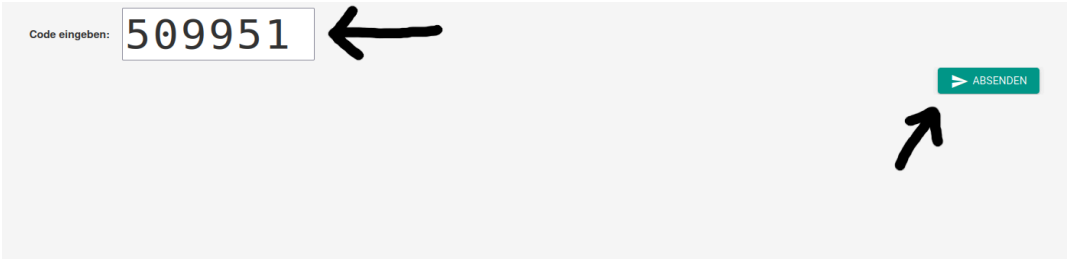
8.3 Achten sie darauf das beim **Schlüsseltyp** (3) „Zeitbasiert“ ausgewählt ist!

8.4 Klicken Sie jetzt auf „**Hinzufügen**“.

9. Geschafft! Sie haben erfolgreich ihren „**Einmalcode**“eingerichtet.

10. Beachten Sie dass Sie ab nun bei **JEDER ANMELDUNG** diesen Einmalcode abrufen müssen!



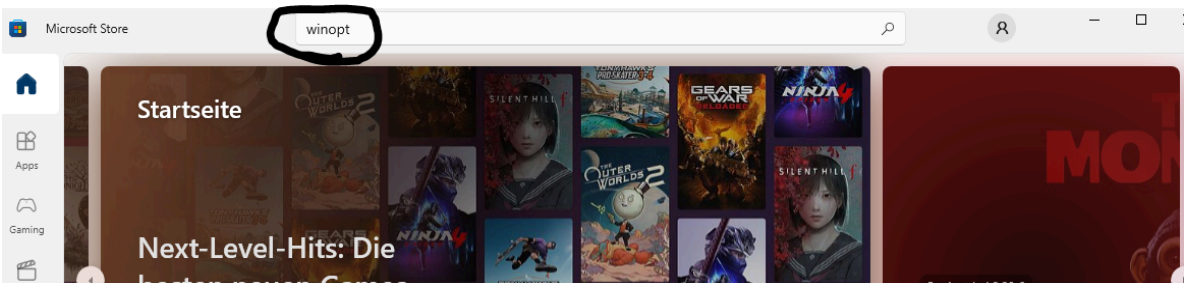


Anleitung mit WinOTP

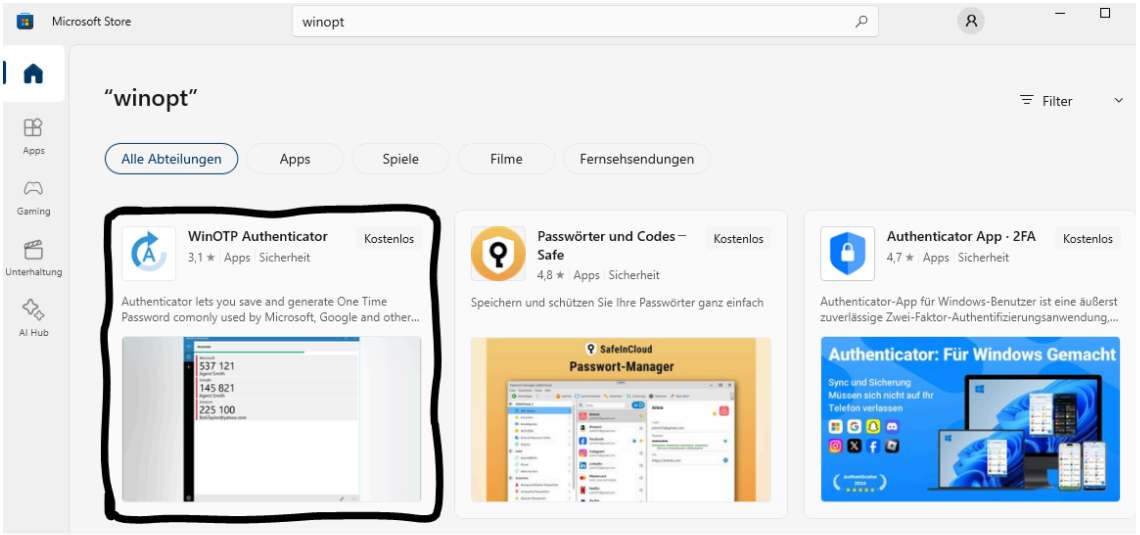
1. Öffnen Sie den **Microsoft Store**.



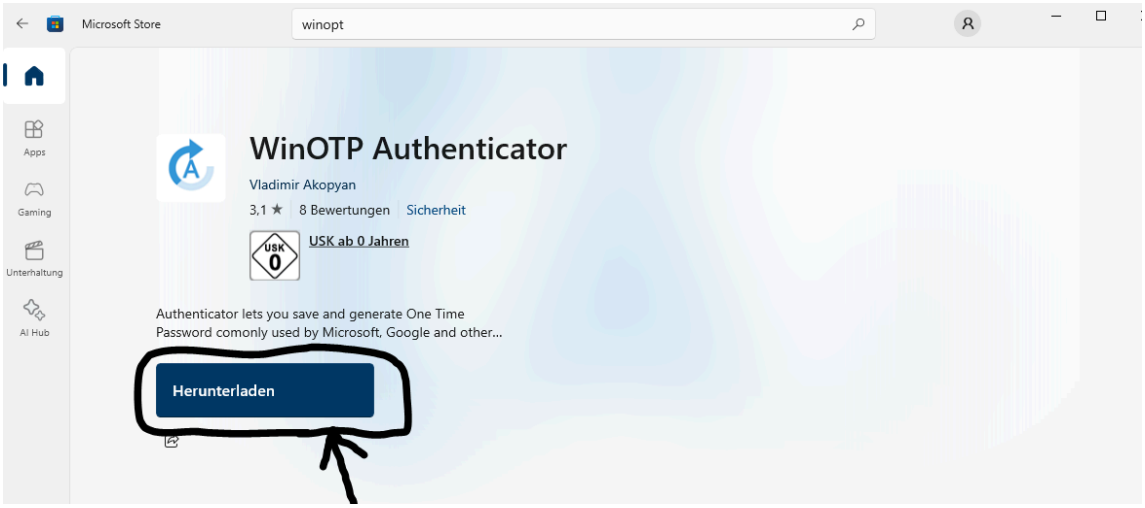
2. Suchen Sie im Suchfeld oben nach **WinOTP**.



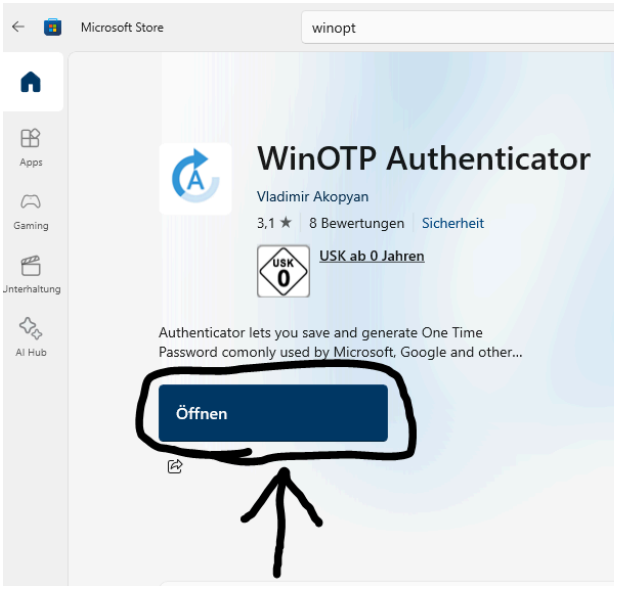
3. Tippen Sie „**WinOTP - Authenticator**“ ein. (hier schwarz eingekreist)



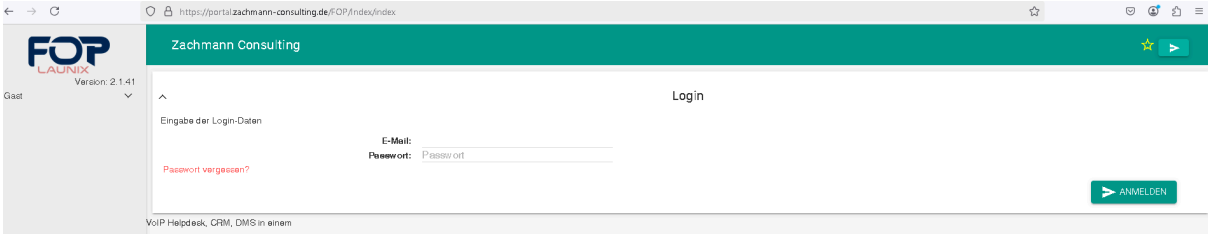
4. **Laden** Sie nun WinOTP **herunter**.



5. Nun können Sie WinOTP **öffnen**.



6. Gehen Sie jetzt zunächst in einen **beliebigen Browser** (Edge, Firefox, Opera etc.) und rufen Sie unser **Kundenportal** auf. (https://portal.zachmann-consulting.de)



6.1. Loggen Sie sich mit ihren Zugangsdaten ein

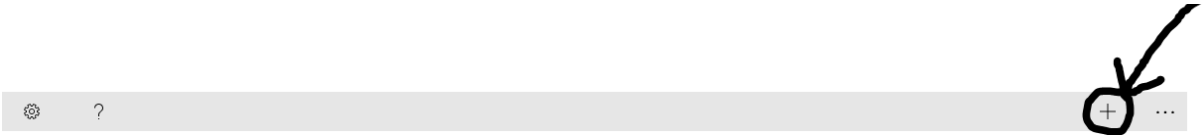
7. Gehen Sie nun links oben, unter der Aufschrift „FOP Launix“ auf den **Pfeil nach unten**.
8. Wählen Sie nun „**2-Faktor-Authentifizierung“** im Fenster.



9. Geben Sie Ihr aktuelles Passwort ein und klicken Sie danach auf „**Geheimnis erneuern**“. Der Code unter dem QR Code ist Ihr „Geheimcode

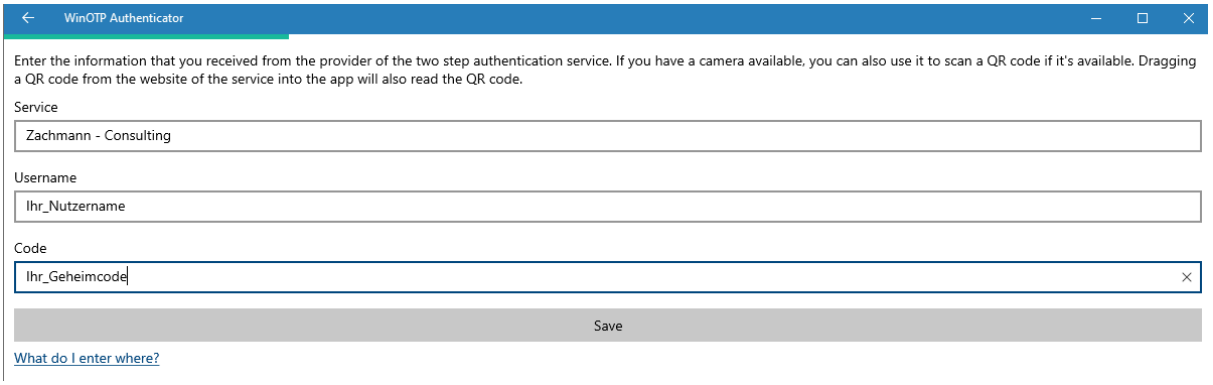


10. Navigieren Sie nun wieder zurück zu **WinOTP** und klicken sie unten rechts auf das



„+“

11. Füllen Sie die drei Felder wie im Bild beschrieben aus.



12. Sie haben erfolgreich die 2-FA eingerichtet nach der Eingabe ihres Passwortes geben sie nun immer zusätzlich den Code vom WinOTP mit ein.

