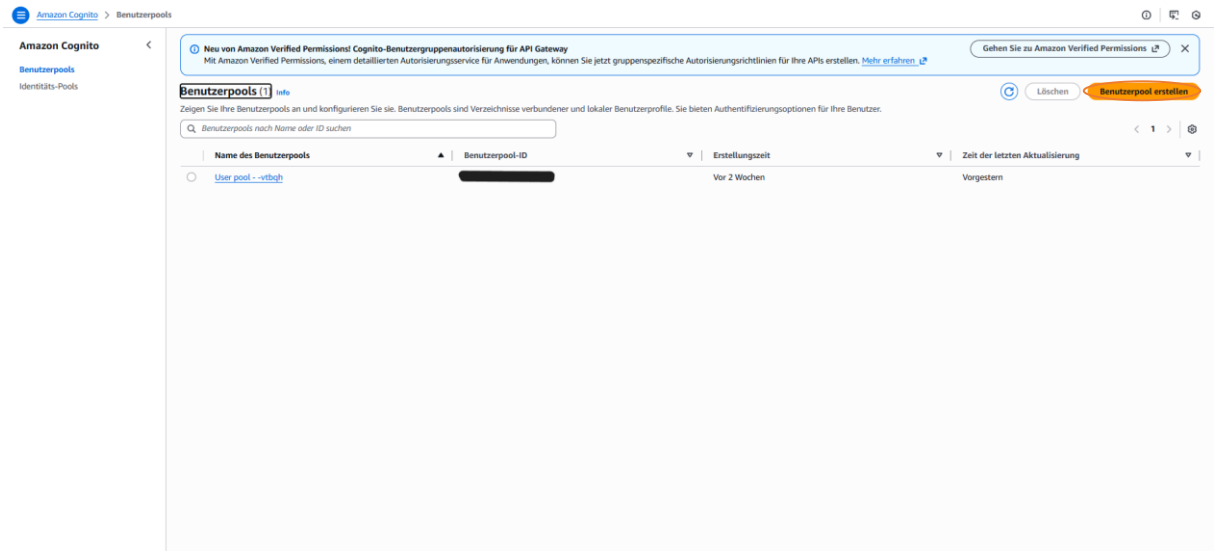
AWS Cognito

Dieses Dokument dient als einfache Anleitung zum Erstellen eines AWS Cognito Benutzerpools für die Gym2.0 Anwendung

1. Anmeldung bei AWS
   Melden sie sich bei AWS an.

2. AWS Cognito öffnen
   Suchen Sie in der AWS-Suchleiste nach „Cognito“ und öffnen Sie den Dienst.

3. Benutzerpool erstellen
   Wählen sie „Benutzerpool erstellen“

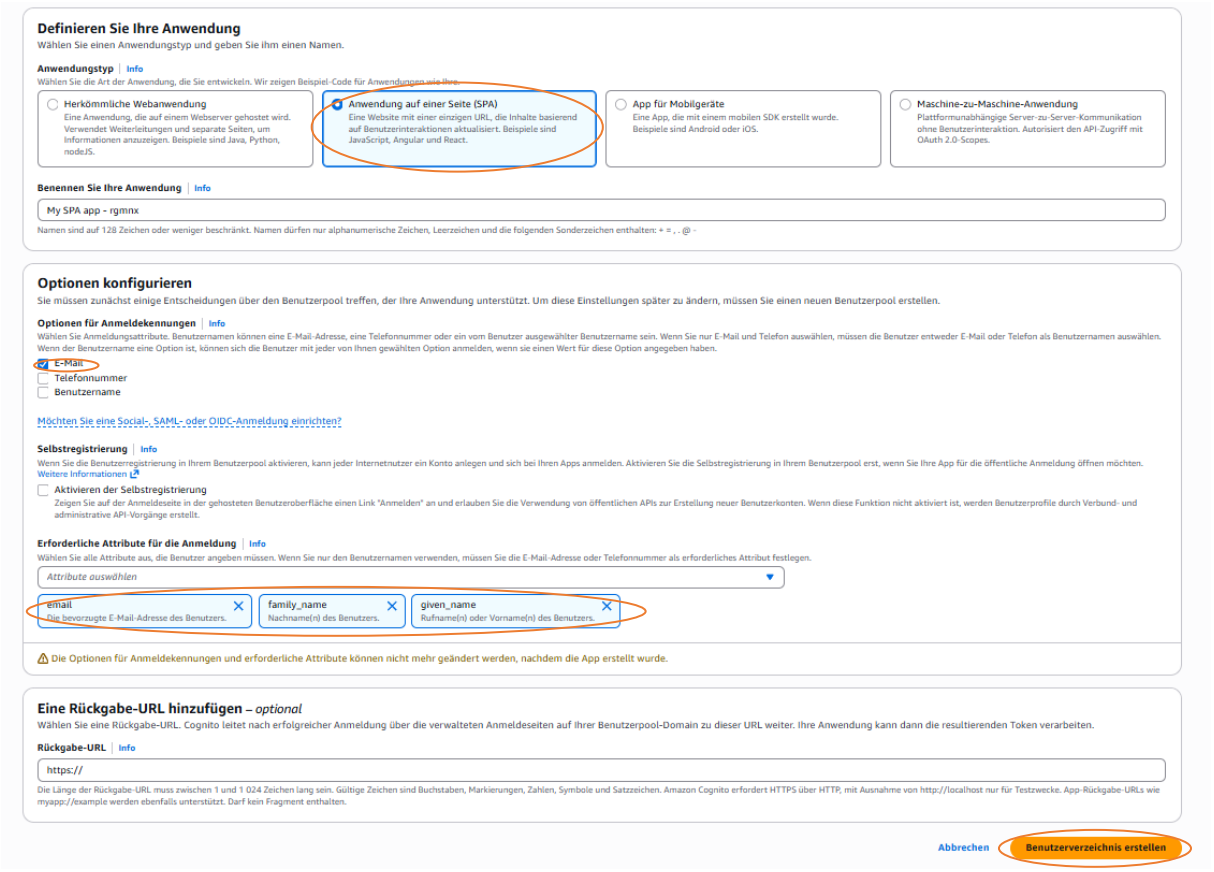


4. Benutzerpool einrichten
   - Wählen sie als Anwendungstypen **Single Page Application** (SPA)
   - Legen sie fest, dass sich Benutzer **ausschließlich mit ihrer E-Mail-Adresse anmelden** können.
   - Deaktivieren sie **Selbstregistrierung zunächst**, um den Benutzerpool kontrolliert einzurichten
   - Definieren sie die **erforderlichen Standardattribute** für die Registrierung (email, family_name, given_name)

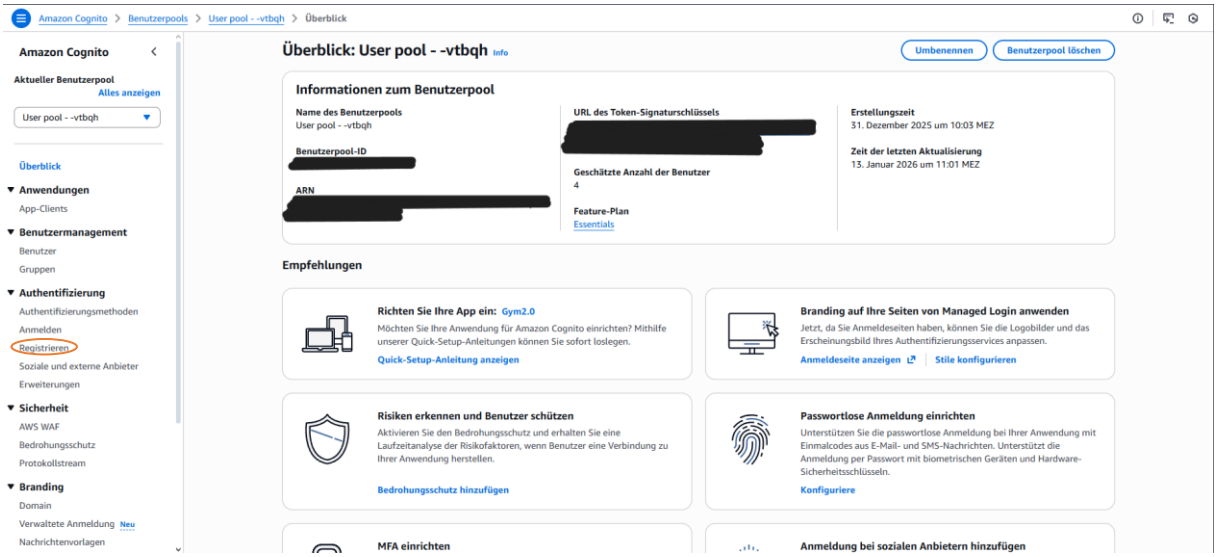
Hinweis:

Die von der **Cognito Hosted UI** unterstützten Attribute sind begrenzt.
Da im Projekt **zusätzliche Custom Attribute** benötigt werden (z. B. City), wird später ein **eigenes Registrierungsformular** verwendet.

- Schließen Sie die Konfiguration ab, indem Sie **„Benutzerverzeichnis erstellen“** auswählen.



5. Überblick über den Benutzerpool
   Nach der Erstellung befinden Sie sich im **Übersicht-Tab** des Benutzerpools. Navigieren Sie nun zum Tab **„Registrieren“**.

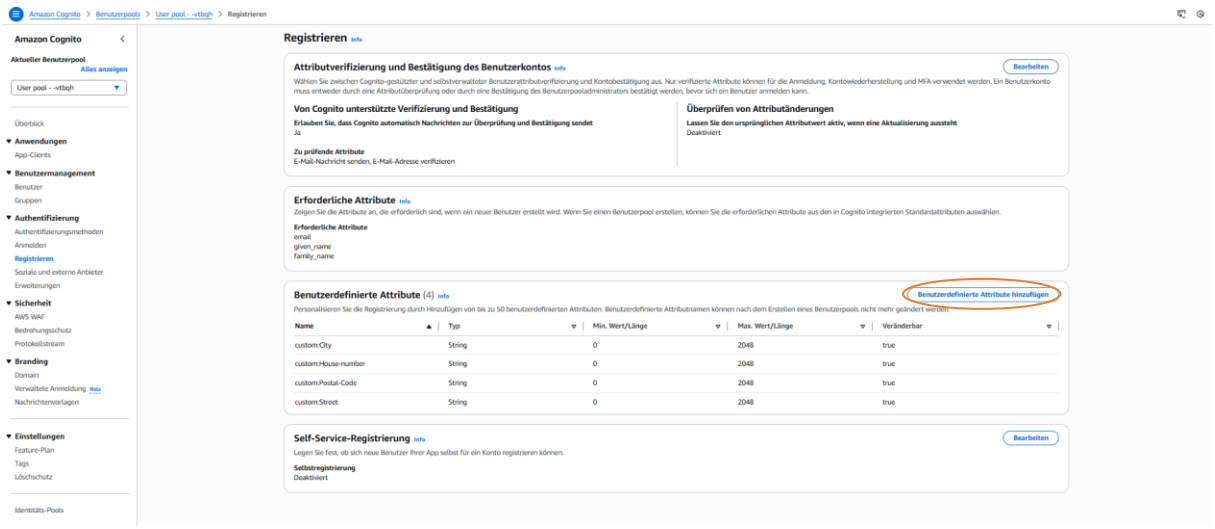


6. Custom Attribute und Selbstregistrierung
   - Fügen Sie im Registrierungsbereich die benötigten **Custom Attribute** hinzu (z. B. Straße, Hausnummer, PLZ, Ort)

Wichtig:
Die **Selbstregistrierung sollte erst ganz am Ende aktiviert werden**, nachdem:

- alle Standard- und Custom Attribute korrekt angelegt wurden,
- alle Lambda-Triggers konfiguriert sind,
- und die App-Client-Einstellungen vollständig abgeschlossen wurden.

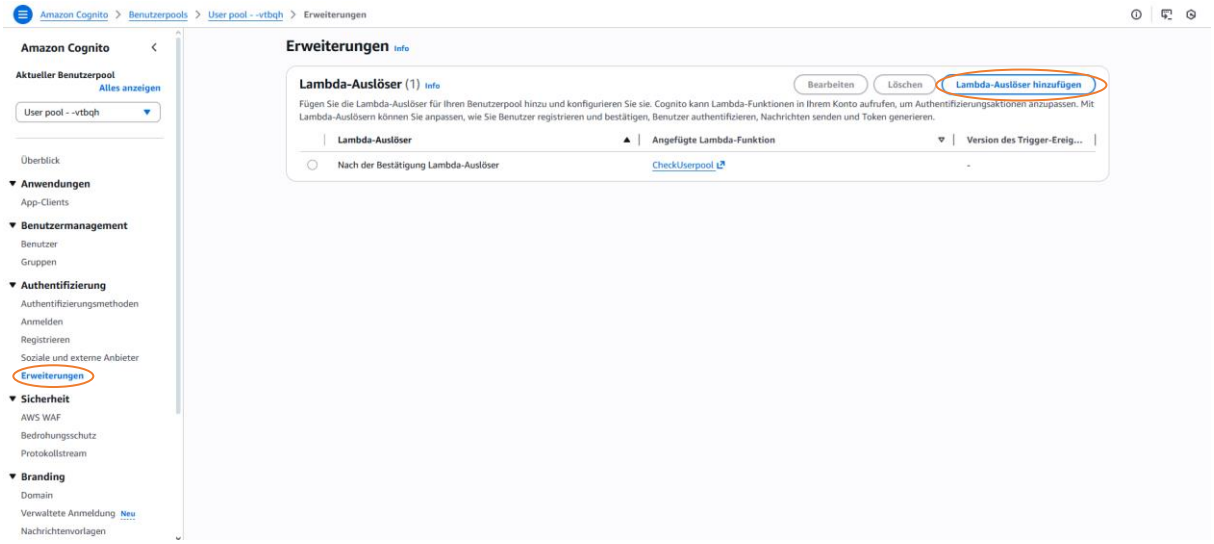
Dies verhindert fehlerhafte oder unvollständige Benutzerregistrierungen während der Konfigurationsphase.

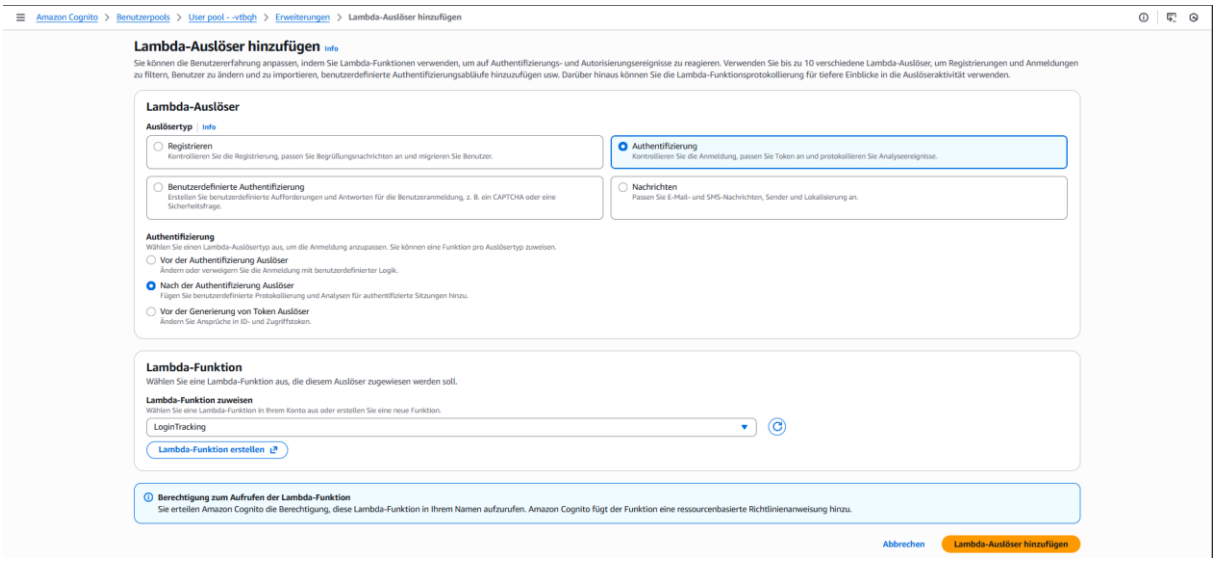


7. Lambda-Auslöser (Triggers) konfigurieren
   Im Tab **„Erweiterungen“** können **Lambda-Triggers** hinzugefügt werden.
   Diese Lambda-Funktionen werden automatisch bei bestimmten Ereignissen ausgeführt.

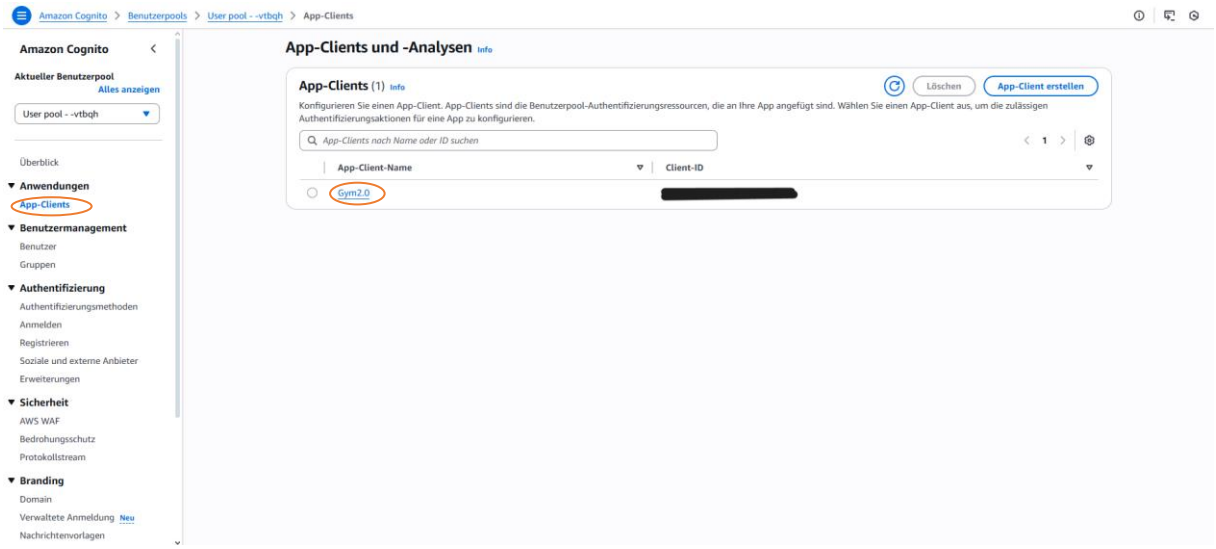
   Vorgehen:
   - Wählen Sie **„Lambda-Auslöser hinzufügen“**
   - Definieren Sie den Auslösertyp (z. B. Registrierung oder Anmeldung)
   - Legen Sie fest, ob die Funktion **vor oder nach der Authentifizierung** ausgeführt werden soll
   - Verknüpfen Sie die entsprechende Lambda-Funktion

Diese Trigger werden im Projekt genutzt, um z. B. Benutzerdaten in DynamoDB anzulegen oder Login-Ereignisse zu protokollieren.

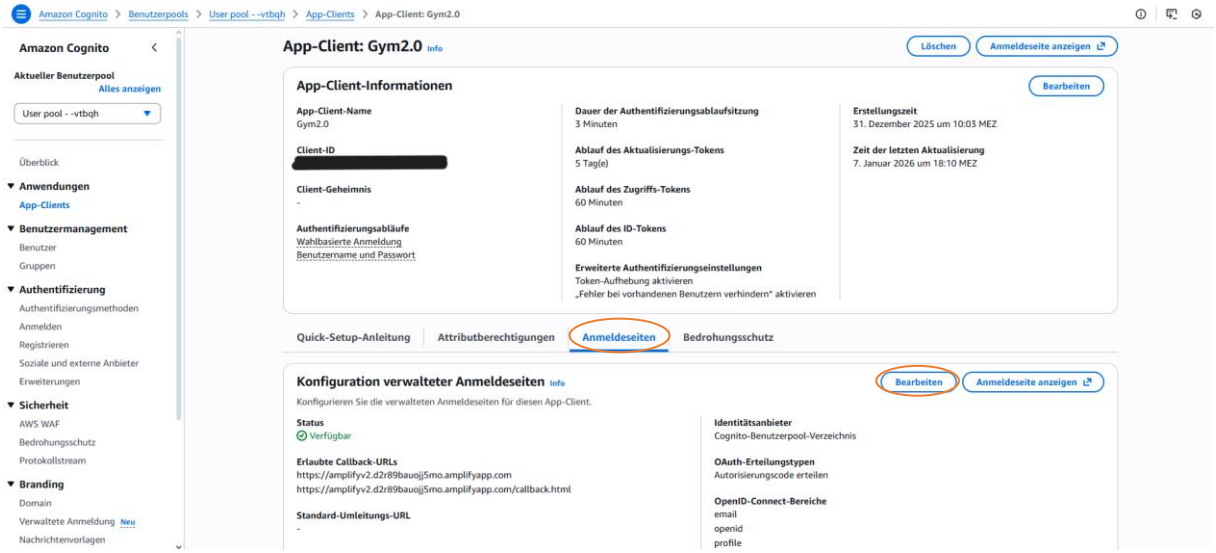




8. App-Client auswählen
   Navigieren Sie in der Benutzerpool-Übersicht zum **App-Client**.



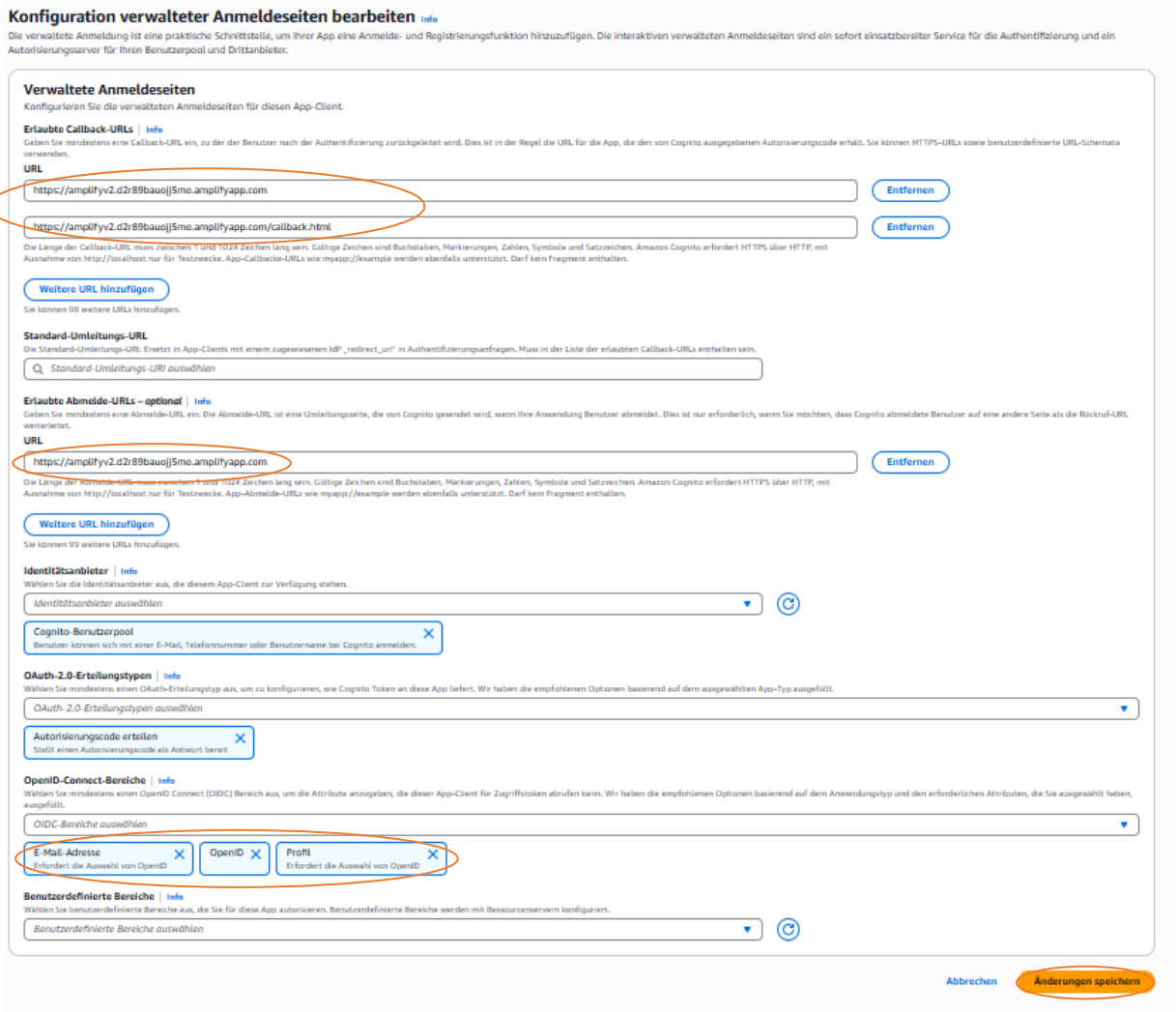
9. Anmeldeseiten konfigurieren
   Wählen Sie im App-Client den Bereich **„Anmeldeseiten“** aus.



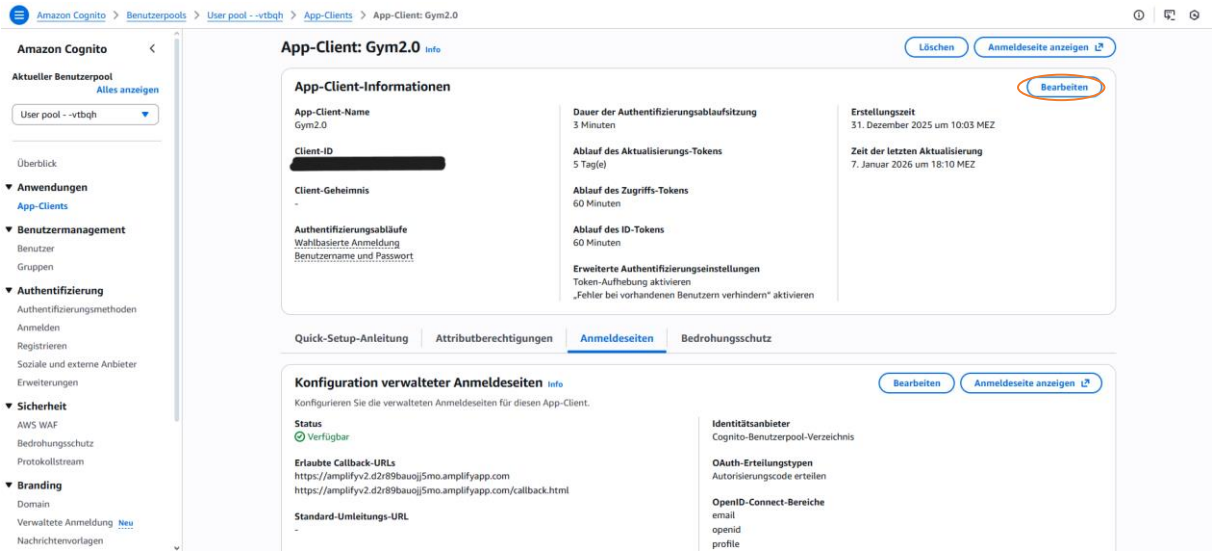
10. Callback- und Logout-URLs festlegen
    Tragen Sie hier die **erlaubten Callback-URLs** und **Abmelde-URLs** ein.

    Diese URLs ermöglichen es AWS Cognito, Benutzer nach erfolgreicher Anmeldung oder Abmeldung wieder auf die **über AWS Amplify gehostete Webanwendung** weiterzuleiten.

11. OpenID-Connect (OIDC) konfigurieren
    Wählen Sie im **OpenID-Connect-Bereich** ausschließlich die Attribute aus, die im Projekt benötigt werden (email, openid, profile).
    Speichern Sie anschließend die Änderungen.



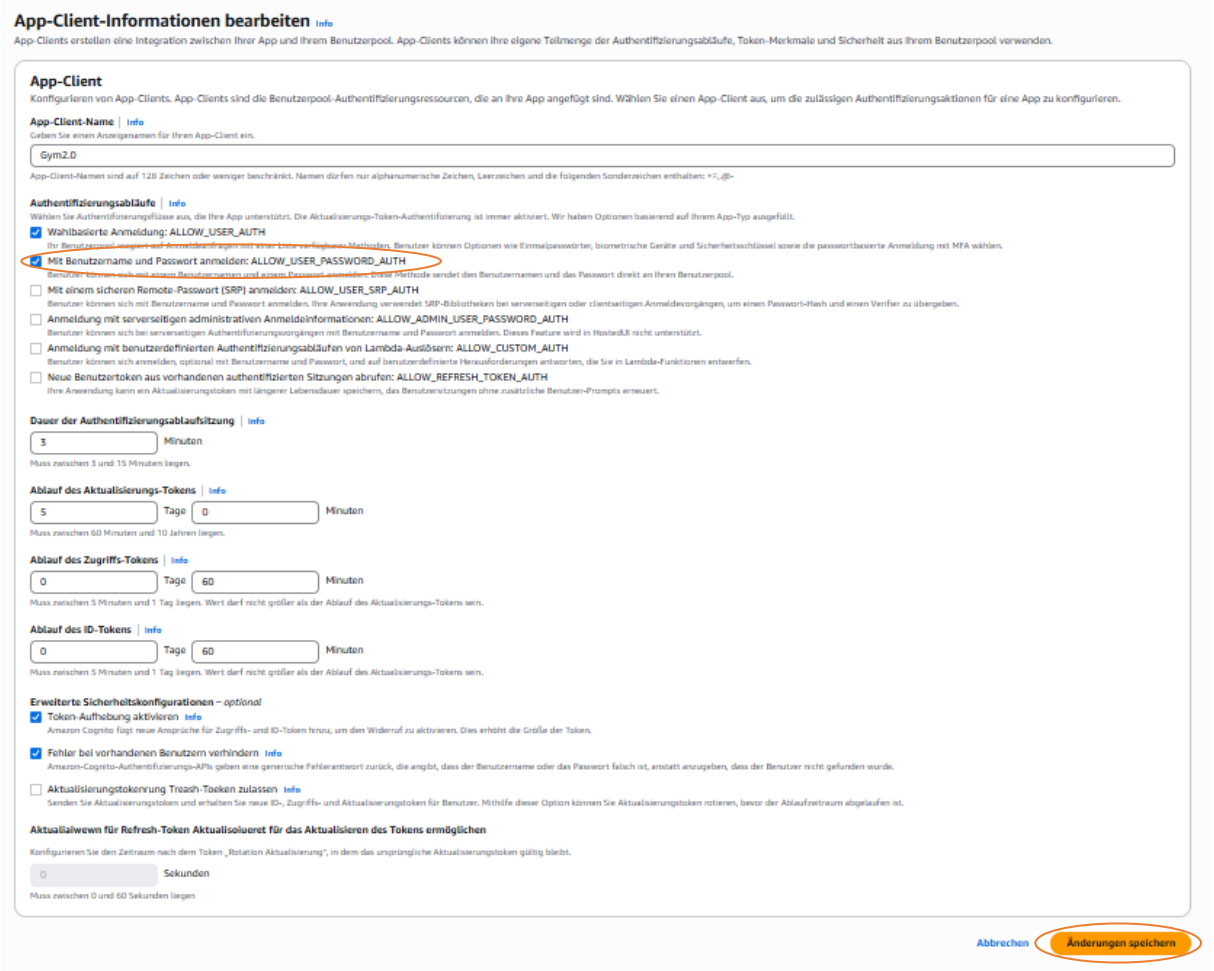
12. App-Client bearbeiten
    Wechseln Sie in die **App-Client-Übersicht** und klicken Sie auf **„Bearbeiten“**.



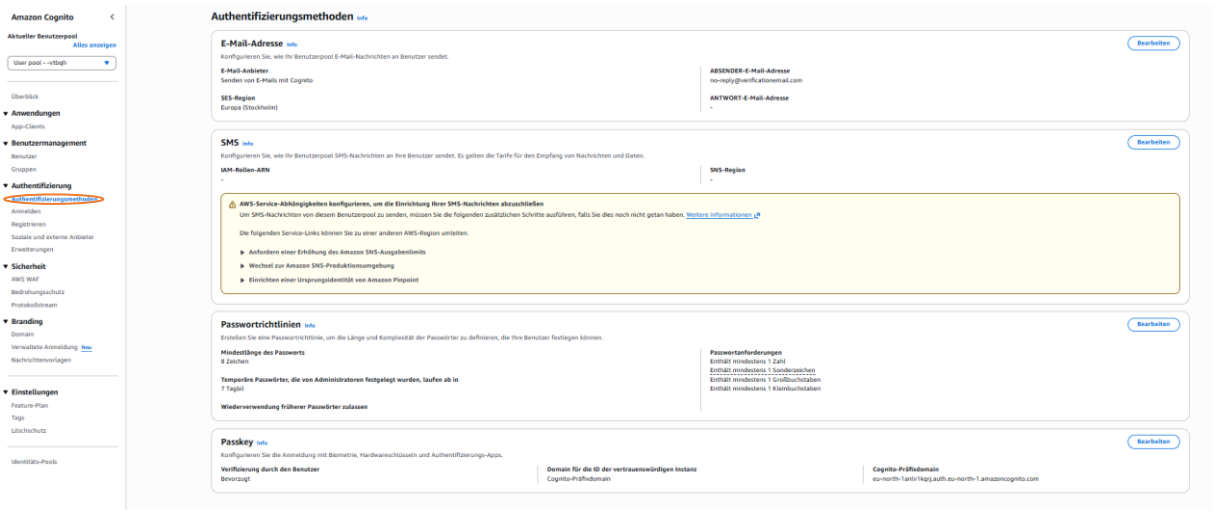
13. Authentifizierungsabläufe festlegen
    Für das Projekt GYM2.0 sind folgende Einstellungen erforderlich:
    - **ALLOW_USER_PASSWORD_AUTH → aktiviert**

- **ALLOW_USER_SRP_AUTH → deaktiviert**

Diese Konfiguration stellt sicher, dass die Authentifizierung korrekt über das eigene Frontend erfolgt.



14. Authentifizierungsmethoden und Passwortregeln
    - Legen Sie fest, wie sich Benutzer authentifizieren (z. B. E-Mail)
    - Definieren Sie Passwort-Richtlinien (Länge, Sonderzeichen, etc.)



Abschluss

Nach Durchführung aller Schritte ist AWS Cognito vollständig eingerichtet und in der Lage, Benutzer für das Projekt GYM2.0 sicher zu registrieren und zu authentifizieren.

Häufige Fehlerquellen

Falls Registrierung oder Anmeldung nicht funktionieren, überprüfen Sie:

- Funktion und Berechtigungen der verknüpften Lambda-Triggers
- Ob die Selbstregistrierung aktiviert ist
- Ob im OIDC-Bereich **nur tatsächlich verwendete Attribute** ausgewählt sind
- Ob die Callback-URLs korrekt eingetragen wurden
- Ob **ALLOW_USER_SRP_AUTH deaktiviert** ist