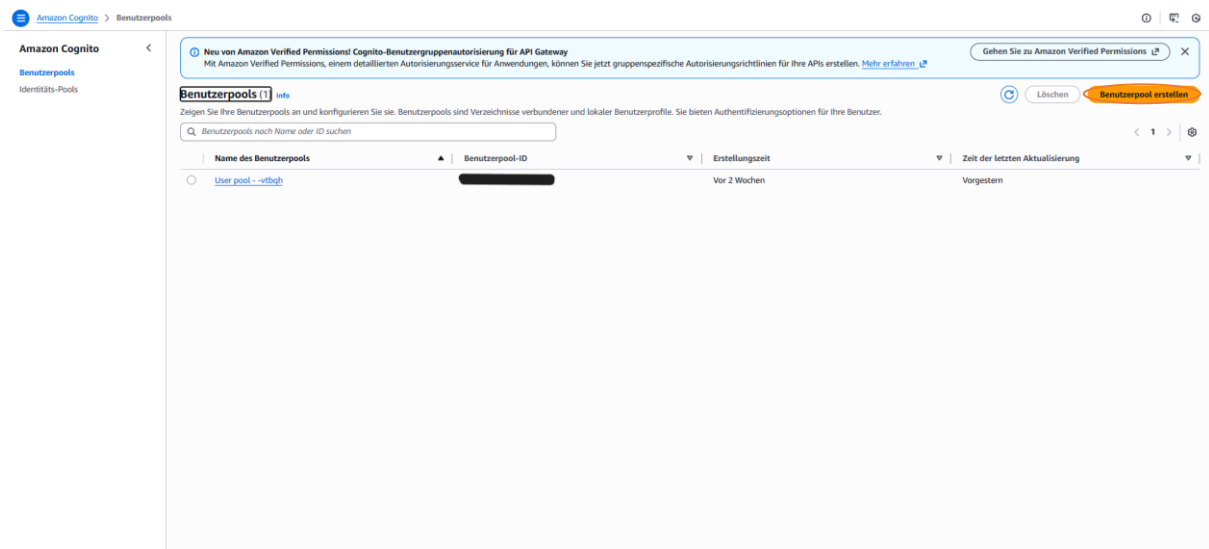


AWS Cognito

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.

Definieren Sie Ihre Anwendung

Wählen Sie einen Anwendungstyp und geben Sie ihm einen Namen.

Anwendungstyp | [Info](#)

Wählen Sie die Art der Anwendung, die Sie entwickeln. Wir zeigen Beispiel-Code für Anwendungen wie Ihre.

☐ Herkömmliche Webanwendung
Eine Anwendung, die auf einem Webserver gehostet wird. Verwendet Weiterleitungen und separate Seiten, um Informationen anzuzeigen. Beispiele sind Java, Python, nodeJS.

☒ Anwendung auf einer Seite (SPA)
Eine Website mit einer einzigen URL, die Inhalte basierend auf Benutzerinteraktionen aktualisiert. Beispiele sind JavaScript, Angular und React.

☐ App für Mobilgeräte
Eine App, die mit einem mobilen SDK erstellt wurde. Beispiele sind Android oder iOS.

☐ Maschine-zu-Maschine-Anwendung
Plattformunabhängige Server-zu-Server-Kommunikation ohne Benutzerinteraktion. Autorisiert den API-Zugriff mit OAuth 2.0-Scopes.

Benennen Sie Ihre Anwendung | [Info](#)

My SPA app - rgmxx

Namen sind auf 128 Zeichen oder weniger beschränkt. Namen dürfen nur alphanumerische Zeichen, Leerzeichen und die folgenden Sonderzeichen enthalten: * . , @ -

Optionen konfigurieren

Sie müssen zunächst einige Entscheidungen über den Benutzerpool treffen, der Ihre Anwendung unterstützt. Um diese Einstellungen später zu ändern, müssen Sie einen neuen Benutzerpool erstellen.

Optionen für Anmeldekennungen | [Info](#)

Wählen Sie Anmeldeattribute. Benutzername können eine E-Mail-Adresse, eine Telefonnummer oder ein vom Benutzer ausgewählter Benutzername sein. Wenn Sie nur E-Mail und Telefon auswählen, müssen die Benutzer entweder E-Mail oder Telefon als Benutzernamen auswählen. Wenn der Benutzername eine Option ist, können sich die Benutzer mit jeder von Ihnen gewählten Option anmelden, wenn sie einen Wert für diese Option angegeben haben.

☒ E-Mail
☐ Telefonnummer
☐ Benutzername

[Möchten Sie eine Social-, SAML- oder OIDC-Anmeldung einrichten?](#)

Selbstregistrierung | [Info](#)

Wenn Sie die Benutzerregistrierung in Ihrem Benutzerpool aktivieren, kann jeder Internetnutzer ein Konto anlegen und sich bei Ihren Apps anmelden. Aktivieren Sie die Selbstregistrierung in Ihrem Benutzerpool erst, wenn Sie Ihre App für die öffentliche Anmeldung öffnen möchten. [Weitere Informationen](#)

☐ Aktivieren der Selbstregistrierung
Zeigen Sie auf der Anmeldeseite in der gehosteten Benutzeroberfläche einen Link "Anmelden" an und erlauben Sie die Verwendung von öffentlichen APIs zur Erstellung neuer Benutzerkonten. Wenn diese Funktion nicht aktiviert ist, werden Benutzerprofile durch Verbindungs- und administrative API-Vorgänge erstellt.

Erforderliche Attribute für die Anmeldung | [Info](#)

Wählen Sie alle Attribute aus, die Benutzer angeben müssen. Wenn Sie nur den Benutzernamen verwenden, müssen Sie die E-Mail-Adresse oder Telefonnummer als erforderliches Attribut festlegen.

Attribute auswählen

email
Die bevorzugte E-Mail-Adresse des Benutzers.

family_name
Nachname(n) des Benutzers.

given_name
Rufname(n) oder Vorname(n) des Benutzers.

⚠ Die Optionen für Anmeldekennungen und erforderliche Attribute können nicht mehr geändert werden, nachdem die App erstellt wurde.

Eine Rückgabe-URL hinzufügen – optional

Wählen Sie eine Rückgabe-URL. Cognito leitet nach erfolgreicher Anmeldung über die verwalteten Anmeldeseiten auf Ihrer Benutzerpool-Domain zu dieser URL weiter. Ihre Anwendung kann dann die resultierenden Token verarbeiten.

Rückgabe-URL | [Info](#)

https://

Die Länge der Rückgabe-URL muss zwischen 1 und 1.024 Zeichen lang sein. Gültige Zeichen sind Buchstaben, Markierungen, Zahlen, Symbole und Satzzeichen. Amazon Cognito erfordert HTTPS über HTTP; mit Ausnahme von http://localhost nur für Testzwecke. App-Rückgabe-URLs wie myapp://example werden ebenfalls unterstützt. Darf kein Fragment enthalten.

[Abbrechen](#)
[Benutzerverzeichnis erstellen](#)

5. Überblick über den Benutzerpool

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

Amazon Cognito

Benutzerpools

User pool --vtbqh

Überblick

Aktueller Benutzerpool

Alles anzeigen

User pool --vtbqh

Überblick

Anwendungen

Benutzermanagement

Authentifizierung

Sicherheit

Branding

Überblick: User pool --vtbqh

Umbenennen

Benutzerpool löschen

Informationen zum Benutzerpool

Name des Benutzerpools

User pool --vtbqh

URL des Token-Signaturschlüssels

Erstellungszeit

31. Dezember 2025 um 10:03 MEZ

Benutzerpool-ID

Geschätzte Anzahl der Benutzer

4

Zeit der letzten Aktualisierung

13. Januar 2026 um 11:01 MEZ

ARN

Feature-Plan

Essentials

Empfehlungen

Richten Sie Ihre App ein: Gym2.0

Möchten Sie Ihre Anwendung für Amazon Cognito einrichten? Mithilfe unserer Quick-Setup-Anleitungen können Sie sofort loslegen.

[Quick-Setup-Anleitung anzeigen](#)

Branding auf Ihre Seiten von Managed Login anwenden

Jetzt, da Sie Anmeldeseiten haben, können Sie die Logobilder und das Erscheinungsbild Ihres Authentifizierungsservices anpassen.

[Anmeldeseite anzeigen](#) [Stile konfigurieren](#)

Risiken erkennen und Benutzer schützen

Aktivieren Sie den Bedrohungsschutz und erhalten Sie eine Laufzeitanalyse der Risikofaktoren, wenn Benutzer eine Verbindung zu Ihrer Anwendung herstellen.

[Bedrohungsschutz hinzufügen](#)

Passwortlose Anmeldung einrichten

Unterstützen Sie die passwortlose Anmeldung bei Ihrer Anwendung mit Einmalcodes aus E-Mail- und SMS-Nachrichten. Unterstützt die Anmeldung per Passwort mit biometrischen Geräten und Hardware-Sicherheitsschlüsseln.

[Konfigurieren](#)

MFA einrichten

Anmeldung bei sozialen Anbietern hinzufügen

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.

The screenshot shows the 'Registrieren' (Registration) page in the Amazon Cognito console. The left sidebar contains navigation links for 'Amazon Cognito', 'Benutzerpools', 'User pool - <id>', and 'Registrieren'. The main content area is titled 'Registrieren' and includes sections for 'Attributverifizierung und Bestätigung des Benutzerkontos', 'Von Cognito unterstützte Verifizierung und Bestätigung', 'Überprüfen von Attributänderungen', 'Erforderliche Attribute', 'Benutzerdefinierte Attribute (4)', and 'Self-Service-Registrierung'. A red circle highlights the link 'Benutzerdefinierte Attribute hinzufügen' in the 'Benutzerdefinierte Attribute' section.

Name	Typ	Min. Wert/Länge	Max. Wert/Länge	Veränderbar
customCity	String	0	2048	true
customHouse-number	String	0	2048	true
customPostal-Code	String	0	2048	true
customStreet	String	0	2048	true

7. Lambda-Auslöser (Triggers) konfigurieren

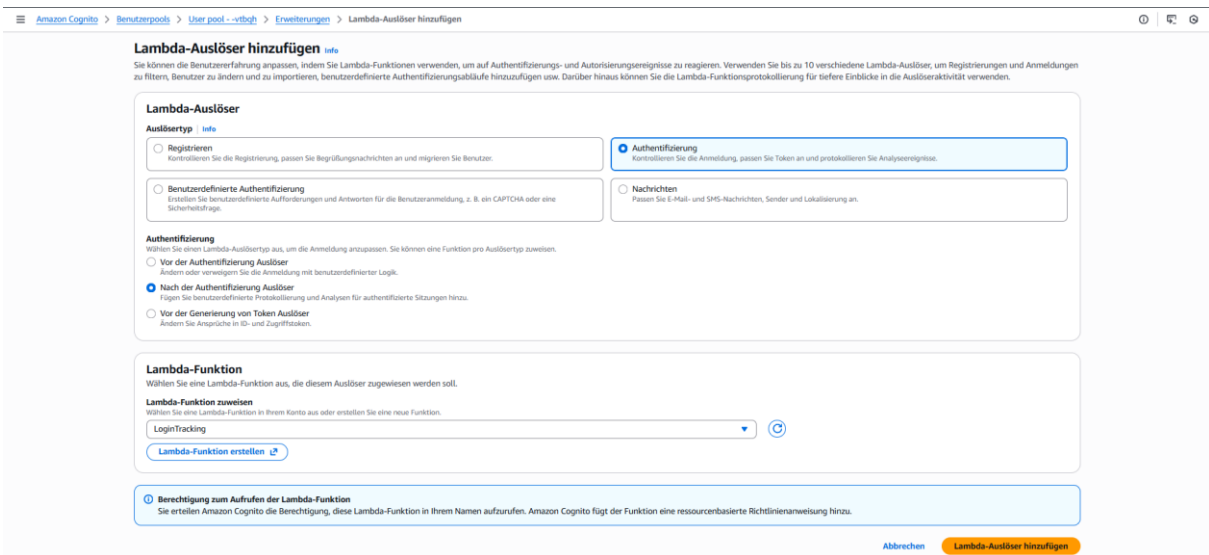
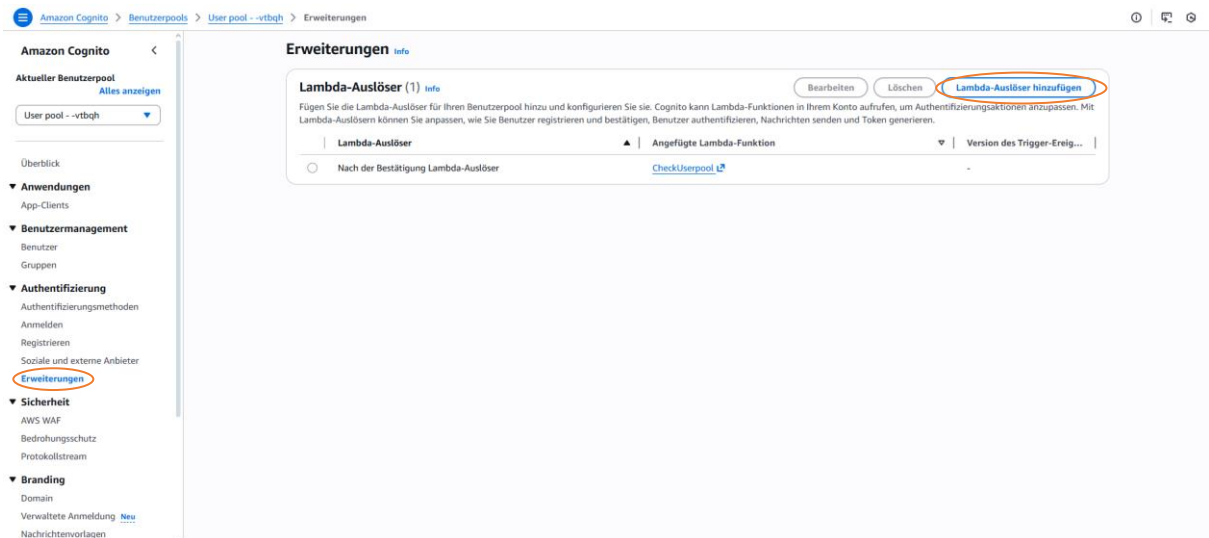
Im Tab „**Erweiterungen**“ können **Lambda-Triggers** hinzugefügt werden.

Diese Lambda-Funktionen werden automatisch bei bestimmten Ereignissen ausgeführt.

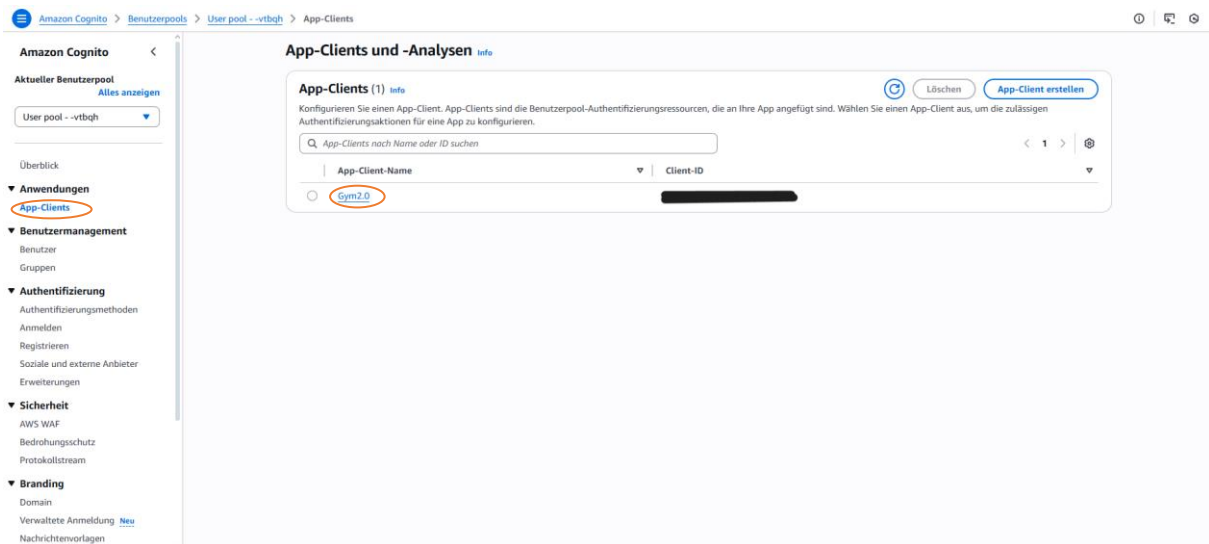
Vorgehen:

- 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.

The screenshot shows the Amazon Cognito console interface. On the left is a navigation menu with categories like 'Anwendungen', 'Benutzermanagement', 'Authentifizierung', 'Sicherheit', and 'Branding'. The main area is titled 'App-Client: Gym2.0' and contains two tabs: 'Anmeldeseiten' (selected) and 'Bedrohungsschutz'. The 'Anmeldeseiten' tab shows the 'Konfiguration verwalteter Anmeldeseiten' (Configure managed sign-in pages) section. It includes fields for 'Erlaubte Callback-URLs' (Allowed callback URLs) and 'Standard-Umleitungs-URL' (Default redirect URL). The 'Status' is 'Verfügbar' (Available). The 'Identitätsanbieter' (Identity provider) is 'Cognito-Benutzerpool-Verzeichnis' (Cognito User Pool Directory). The 'OAuth-Erteilungstypen' (OAuth grant types) are 'Autorisierungscode erteilen' (Authorize code grant) and 'OpenID-Connect-Bereiche' (OpenID Connect scopes) which include 'email', 'openid', and 'profile'.

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.

Konfiguration verwalteter Anmeldeseiten bearbeiten [info](#)

Die verwaltete Anmeldung ist eine praktische Schnittstelle, um Ihrer App eine Anmelde- und Registrierungsfunktion hinzuzufügen. Die interaktiven verwalteten Anmeldeseiten sind ein sofort einsatzbereiter Service für die Authentifizierung und ein Autorisierungsserver für Ihren Benutzerpool und Drittanbieter.

Verwaltete Anmeldeseiten

Konfigurieren Sie die verwalteten Anmeldeseiten für diesen App-Client.

Erlaubte Callback-URLs [info](#)

Geben Sie mindestens eine Callback-URL ein, zu der der Benutzer nach der Authentifizierung zurückgeleitet wird. Dies ist in der Regel die URL für die App, die den von Cognito ausgegebenen Autorisierungscode erhält. Sie können HTTPS-URLs sowie benutzerdefinierte URL-Schemata verwenden.

URL

Entfernen

Entfernen

Die Länge der Callback-URLs muss zwischen 1 und 1024 Zeichen lang sein. Gültige Zeichen sind Buchstaben, Markierungen, Zahlen, Symbole und Satzzeichen. Amazon Cognito erfordert HTTPS über HTTP, mit Ausnahme von http://localhost nur für Testzwecke. App-Callback-URLs wie myapp://example werden ebenfalls unterstützt. Darf kein Fragment enthalten.

[Weitere URL hinzufügen](#)

Sie können 98 weitere URLs hinzufügen.

Standard-Umleitungs-URL

Die Standard-Umleitungs-URL. Ersetzt in App-Clients mit einem zugeordneten IDP „redirect_uri“ in Authentifizierungsanfragen. Muss in der Liste der erlaubten Callback-URLs enthalten sein.

Erlaubte Abmelde-URLs – optional [info](#)

Geben Sie mindestens eine Abmelde-URL ein. Die Abmelde-URL ist eine Umleitungsseite, die von Cognito gerufen wird, wenn Ihre Anwendung Benutzer abmeldet. Dies ist nur erforderlich, wenn Sie möchten, dass Cognito abgemeldete Benutzer auf eine andere Seite als die Rückruf-URL weiterleitet.

URL

Entfernen

Die Länge der Abmelde-URLs muss zwischen 1 und 1024 Zeichen lang sein. Gültige Zeichen sind Buchstaben, Markierungen, Zahlen, Symbole und Satzzeichen. Amazon Cognito erfordert HTTPS über HTTP, mit Ausnahme von http://localhost nur für Testzwecke. App-Abmelde-URLs wie myapp://example werden ebenfalls unterstützt. Darf kein Fragment enthalten.

[Weitere URL hinzufügen](#)

Sie können 99 weitere URLs hinzufügen.

Identitätsanbieter [info](#)

Wählen Sie die Identitätsanbieter aus, die diesem App-Client zur Verfügung stehen.

Cognito-Benutzerpool

Benutzer können sich mit einer E-Mail, Telefonnummer oder Benutzername bei Cognito anmelden.

OAuth 2.0-Erteilungstypen [info](#)

Wählen Sie mindestens einen OAuth 2.0-Erteilungstyp aus, um zu konfigurieren, wie Cognito Token an diese App liefert. Wir haben die empfohlenen Optionen basierend auf dem ausgewählten App-Typ ausgefüllt.

Autorisierungscode erteilen

Stellt einen Autorisierungscode als Antwort bereit.

OpenID-Connect-Bereiche [info](#)

Wählen Sie mindestens einen OpenID Connect (OIDC) Bereich aus, um die Attribute anzugeben, die dieser App-Client für Zugriffstoken abrufen kann. Wir haben die empfohlenen Optionen basierend auf dem Anwendungstyp und den erforderlichen Attributen, die Sie ausgewählt haben, ausgefüllt.

E-Mail-Adresse

Erfordert die Auswahl von OpenID

OpenID

Profil

Erfordert die Auswahl von OpenID

Benutzerdefinierte Bereiche [info](#)

Wählen Sie benutzerdefinierte Bereiche aus, die Sie für diese App autorisieren. Benutzerdefinierte Bereiche werden mit Ressourcenverwaltern konfiguriert.

Abbrechen
Änderungen speichern

12. App-Client bearbeiten

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

Amazon Cognito

Benutzerpools

User pool - vrbqh

App-Clients

App-Client: Gym2.0

🔍
🔧
🔗

Aktueller Benutzerpool

Alles anzeigen

User pool - vrbqh

Überblick

Anwendungen

App-Clients

Benutzermanagement

Benutzer

Gruppen

Authentifizierung

Authentifizierungsmethoden

Anmelden

Registrieren

Soziale und externe Anbieter

Erweiterungen

Sicherheit

AWS WAF

Bedrohungsschutz

Protokollstream

Branding

Domain

Verwaltete Anmeldung

Neu

Nachrichtenvorlagen

App-Client: Gym2.0 [info](#)

Löschen
Anmeldeseite anzeigen
Bearbeiten

App-Client-Informationen

App-Client-Name

Gym2.0

Dauer der Authentifizierungsablaufzeit

3 Minuten

Erstellungszeit

31. Dezember 2025 um 10:03 MEZ

Client-ID

[REDACTED]

Ablauf des Aktualisierungs-Tokens

5 Tage

Zeit der letzten Aktualisierung

7. Januar 2026 um 18:10 MEZ

Client-Geheimnis

-

Ablauf des Zugriffs-Tokens

60 Minuten

Ablauf des ID-Tokens

60 Minuten

Erweiterte Authentifizierungseinstellungen

Token-Aufhebung aktivieren

„Fehler bei vorhandenen Benutzern verhindern“ aktivieren

Authentifizierungsabläufe

Wahlbasierte Anmeldung

Benutzername und Passwort

Quick-Setup-Anleitung

Attributberechtigungen

Anmeldeseiten

Bedrohungsschutz

Konfiguration verwalteter Anmeldeseiten [info](#)

Konfigurieren Sie die verwalteten Anmeldeseiten für diesen App-Client.

Status

🟢 Verfügbar

Identitätsanbieter

Cognito-Benutzerpool-Verzeichnis

Erlaubte Callback-URLs

https://amplifyv2.d2r89bauoj5mo.amplifyapp.com

https://amplifyv2.d2r89bauoj5mo.amplifyapp.com/callback.html

OAuth-Erteilungstypen

Autorisierungscode erteilen

Standard-Umleitungs-URL

-

OpenID-Connect-Bereiche

email

openid

profile

Bearbeiten
Anmeldeseite anzeigen

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.

App-Client-Informationen bearbeiten Info

App-Clients erstellen eine Integration zwischen Ihrer App und Ihrem Benutzerpool. App-Clients können Ihre eigene Teilmenge der Authentifizierungsabläufe, Token-Merkmale und Sicherheit aus Ihrem Benutzerpool verwenden.

App-Client

Konfigurieren von App-Clients. App-Clients sind die Benutzerpool-Authentifizierungsressourcen, die an Ihre App angefügt sind. Wählen Sie einen App-Client aus, um die zulässigen Authentifizierungsaktionen für eine App zu konfigurieren.

App-Client-Name Info

Geben Sie einen Anzeigenamen für Ihren App-Client ein.

Gym2.0

App-Client-Namen sind auf 128 Zeichen oder weniger beschränkt. Namen dürfen nur alphanumerische Zeichen, Leerzeichen und die folgenden Sonderzeichen enthalten: +, -, @.

Authentifizierungsabläufe Info

Wählen Sie Authentifizierungsabläufe aus, die Ihre App unterstützt. Die Aktualisierungs-Token-Authentifizierung ist immer aktiviert. Wir haben Optionen basierend auf Ihrem App-Typ ausgefällt.

☒ Wahlbasierte Anmeldung: ALLOW_USER_AUTH

Ihre Benutzer können sich mit einer Wahlbasierten Anmeldung anmelden. Benutzer können Optionen wie Einmalpasswörter, biometrische Geräte und Sicherheitschlüssel sowie die passwortbasierte Anmeldung mit MFA wählen.

☒ Mit Benutzername und Passwort anmelden: ALLOW_USER_PASSWORD_AUTH

Benutzer können sich mit einem Benutzernamen und einem Passwort anmelden. Einmal ein Passwort eingetippt, wird der Benutzername und das Passwort direkt an Ihren Benutzerpool.

☐ Anmeldung mit einem sicheren Remote-Passwort (SRP) anmelden: ALLOW_USER_SRP_AUTH

Benutzer können sich mit Benutzername und Passwort anmelden. Ihre Anwendung verwendet SRP-Bibliotheken bei serverseitigen oder clientseitigen Anmeldevorgängen, um einen Passwort-Hash und einen Verifier zu übergeben.

☐ Anmeldung mit serverseitigen administrativen Anmeldeinformationen: ALLOW_ADMIN_USER_PASSWORD_AUTH

Benutzer können sich bei serverseitigen Authentifizierungsvorgängen mit Benutzername und Passwort anmelden. Dieses Feature wird in HostedUI nicht unterstützt.

☐ Anmeldung mit benutzerdefinierten Authentifizierungsabläufen von Lambda-Auslösern: ALLOW_CUSTOM_AUTH

Benutzer können sich anmelden, optional mit Benutzername und Passwort, und auf benutzerdefinierte Herausforderungen antworten, die Sie in Lambda-Funktionen entwerfen.

☐ Neue Benutzertoken aus vorhandenen authentifizierten Sitzungen abrufen: ALLOW_REFRESH_TOKEN_AUTH

Ihre Anwendung kann ein Aktualisierungstoken mit längerer Lebensdauer speichern, das Benutzersitzungen ohne zusätzliche Benutzer-Prompts erneuert.

Dauer der Authentifizierungsablaufsitzung Info

Minuten

Muss zwischen 5 und 15 Minuten liegen.

Ablauf des Aktualisierungstokens Info

Tage Minuten

Muss zwischen 60 Minuten und 10 Jahren liegen.

Ablauf des Zugriffstokens Info

Tage Minuten

Muss zwischen 5 Minuten und 1 Tag liegen. Wert darf nicht größer als der Ablauf des Aktualisierungstokens sein.

Ablauf des ID-Tokens Info

Tage Minuten

Muss zwischen 5 Minuten und 1 Tag liegen. Wert darf nicht größer als der Ablauf des Aktualisierungstokens sein.

Erweiterte Sicherheitskonfigurationen – optional

☒ Token-Aufhebung aktivieren Info

Amazon Cognito fügt neue Ansprüche für Zugriffstoken und ID-Token hinzu, um den Widerruf zu aktivieren. Dies erhöht die Größe der Token.

☒ Fehler bei vorhandenen Benutzern verhindern Info

Amazon-Cognito-Authentifizierungs-APIs geben eine generische Fehlerantwort zurück, die angibt, dass der Benutzername oder das Passwort falsch ist, anstatt anzugeben, dass der Benutzer nicht gefunden wurde.

☐ Aktualisierungstoken Tread-Token zulassen Info

Senden Sie Aktualisierungstoken und erhalten Sie neue ID-, Zugriffstoken und Aktualisierungstoken für Benutzer. Mithilfe dieser Option können Sie Aktualisierungstoken notieren, bevor der Ablaufzeitraum abgelaufen ist.

Aktualisierungswert für Refresh-Token aktualisieren für das Aktualisieren des Tokens ermöglichen

Konfigurieren Sie den Zeitraum nach dem Token „Rotation Aktualisierung“, in dem das ursprüngliche Aktualisierungstoken gültig bleibt.

Sekunden

Muss zwischen 0 und 60 Sekunden liegen

[Abbrechen](#)
[Änderungen speichern](#)

14. Authentifizierungsmethoden und Passwortregeln

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

Authentifizierungsmethoden Info

Konfigurieren Sie, wie Ihr Benutzerpool E-Mail-Nachrichten an Benutzer sendet.

E-Mail-Adresse Info

E-Mail-Absender

Senden von E-Mails mit Cognito

SENDER-E-Mail-Adresse

no-reply@amazon.com

SENDER-E-Mail-Adresse

no-reply@amazon.com

SMS Info

Konfigurieren Sie, wie Ihr Benutzerpool SMS-Nachrichten an Ihre Benutzer sendet. Es gelten die Tarife für den Empfang von Nachrichten und Daten.

IAM-Rollen-ARN

-

SMS-Region

-

⚠ AWS Service-Abhängigkeiten konfigurieren, um die Einrichtung Ihrer SMS-Nachrichten abzuschließen

Um SMS-Nachrichten von diesem Benutzerpool zu senden, müssen Sie die folgenden zusätzlichen Schritte ausführen, falls Sie dies noch nicht getan haben. [Weitere Informationen](#)

Die folgenden Service-Links können Sie zu einer anderen AWS-Region umleiten.

- Anforderen einer Erlaubnis der Amazon SNS-Konfigurationsrolle
- Wechsel zur Amazon SNS-Produktionsumgebung
- Einrichten einer Ursprungsidentität von Amazon Pinpoint

Passwortrichtlinien Info

Erstellen Sie eine Passwortrichtlinie, um die Länge und Komplexität der Passwörter zu definieren, die Ihre Benutzer festlegen können.

Mindestlänge des Passworts

8 Zeichen

Mindestalter des Passworts

7 Tage

Wiederverwendung früherer Passwörter zulassen

-

Passwortanforderungen

Enthält mindestens 1 Zahl

Enthält mindestens 1 Sonderzeichen

Enthält mindestens 1 Großbuchstaben

Enthält mindestens 1 Kleinbuchstaben

Passkey Info

Konfigurieren Sie die Anmeldung mit Biometrie, Hardwarechlüsseln und Authentifizierungs-Apps.

Verifizierung durch den Benutzer

Benötigt

Domain für die ID der vertrauenswürdigen Instanz

Cognito-Prüfdomäne

Cognito-Prüfdomäne

eu-north-1::auth.eu-north-1.amazonaws.com

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