

AWS Cognito

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

1. Anmeldung bei AWS

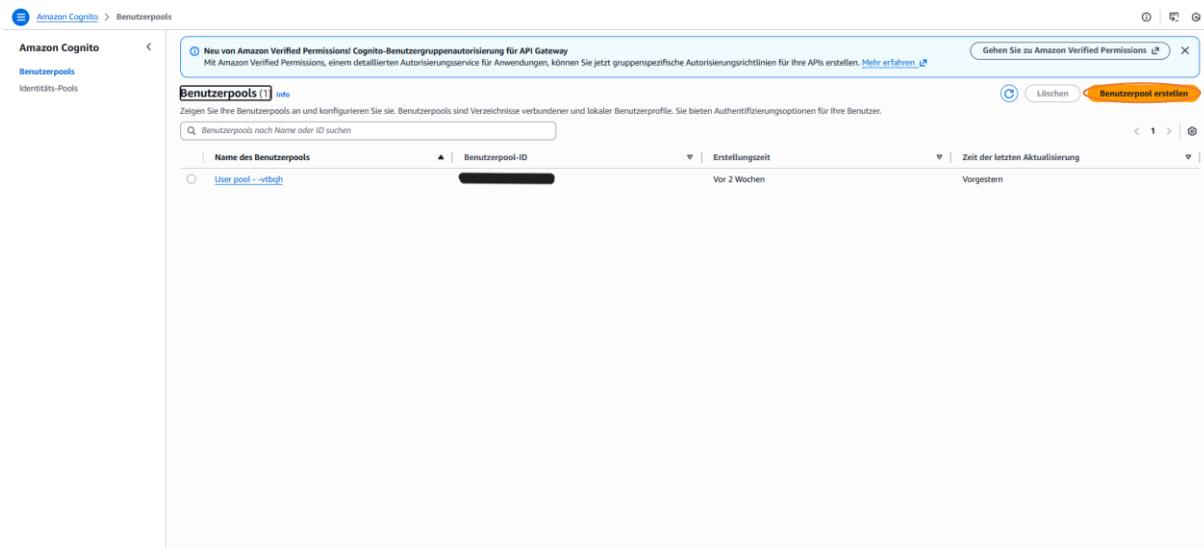
Melden sie sich bei AWS an.

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 basierend auf dem gewählten Typ.

Herkommliche Webanwendung
Eine Anwendung, die auf einem Webserver gehostet wird. Verwendet Weiterleitungen und separate Seiten, um Informationen anzuzeigen. Beispiele sind Java, Python, node.js.

Anwendung auf einer SPA (SPA)
Eine Website mit einer einzigen URL, die Inhalte basierend auf Benutzerinteraktion 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 - rgmx

Namen sind auf 120 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 Anmeldedatenmethoden | Info
Wählen Sie Anmeldedatenattribute. Benutzernamen 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 Benutzernamen 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

Benutzernname

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 Verbund- 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
Vorname(n) oder Vornam(e)n des Benutzers.

⚠ Die Optionen für Anmeldedatenmethoden 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 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

Überblick: User pool - vtbqh

Informationen zum Benutzerpool

Name des Benutzerpools
User pool - vtbqh

URL des Token-Signaturschlüssels
[redacted]

Erstellungszeit
31. Dezember 2025 um 10:03 MEZ

Zeit der letzten Aktualisierung
13. Januar 2026 um 11:01 MEZ

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 AWS Cognito User Pools configuration interface. On the left, there's a sidebar with navigation links like 'User pools', 'App Clients', 'User management', 'Authentication', 'Security', 'Branding', and 'Einstellungen'. The main panel is titled 'Registrieren' and contains several sections:

- Attributverifizierung und Bestätigung des Benutzerkontos**: Describes the verification process using Cognito or email.
- Zu prüfende Attribute**: Shows 'E-Mail-Nachricht senden, E-Mail-Adresse verifizieren'.
- Erforderliche Attribute**: Lists 'email', 'given_name', and 'family_name'.
- Benutzerdefinierte Attribute (4)**: A table showing four custom attributes: 'customCity', 'customHouse-number', 'customPostal-Code', and 'customStreet'. The 'Name' column has a circled 'Bearbeiten' button. The 'Type' column shows 'String' for all. 'Min. Wert/Länge' and 'Max. Wert/Länge' are both set to 2048. 'Veränderbar' is checked for all.
- Self-Service-Registrierung**: A section about letting users register themselves.

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.

The screenshot shows the 'Erweiterungen' (Extensions) section of the Cognito User Pool configuration. Under the 'Lambda-Auslöser' (Lambda Triggers) heading, there is a table with one entry: 'Nach der Bestätigung Lambda-Auslöser' (CheckUserpool). The 'Lambda-Auslöser hinzufügen' button at the top right of the table is circled in red.

This screenshot shows the 'Lambda-Auslöser hinzufügen' (Add Lambda Trigger) dialog. It includes sections for selecting the trigger type (Authentifizierung is selected), choosing a Lambda function (LoginTracking is selected), and granting permissions (Berechtigung zum Aufrufen der Lambda-Funktion is selected). The 'Lambda-Auslöser hinzufügen' button at the bottom right is circled in red.

8. App-Client auswählen

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

The screenshot shows the 'App-Clients und -Analysen' (App Clients and Analyses) section of the Cognito User Pool configuration. It lists one app client named 'Gym2.0'. The 'App-Client erstellen' (Create App Client) button at the top right is circled in red.

9. Anmeldeseiten konfigurieren

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

The screenshot shows the AWS Cognito console interface. On the left, there's a navigation sidebar with categories like Anwendungen, Benutzermanagement, Authentifizierung, Sicherheit, Branding, and more. The main area is titled "App-Client: Gym2.0" and contains sections for "App-Client-Informationen" and "Konfiguration verwalteter Anmeldeseiten". The "Anmeldeseiten" tab is highlighted with a red circle. In the "Konfiguration" section, there are tabs for "Quick-Setup-Anleitung", "Attributberechtigungen", "Anmeldeseiten" (which is active), and "Bedrohungsschutz". There are also buttons for "Bearbeiten" and "Anmeldeseite anzeigen".

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 ausgetragenen Autorisierungscode erhält. Sie können HTTPS-URLs sowie benutzerdefinierte URL-Schemata verwenden.

URL

 Entfernen

Entfernen

Die Länge der Callback-URL 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 99 weitere URLs hinzufügen.

Standard-Umlenkungs-URL
Der Standard-Umlenkungs-URL wird in App-Clients mit einem zugewiesenen IDP „`redirect_ur`“ 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 Umlenkungsseite, die von Cognito gesendet 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-URL 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.

Entfernen

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-Erteilungstyp aus, um zu konfigurieren, wie Cognito Tokens an diese App liefert. Wir haben die empfohlenen Optionen basierend auf dem ausgewählten App-Typ ausgewählt.

OAuth-2.0-Erteilungstypen auswählen

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, ausgewählt.

OIDC-Bereiche auswählen

E-Mail-Adresse Entfernen OpenID Entfernen Profil Entfernen

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

Entfernen

Abbrechen Änderungen speichern

12. App-Client bearbeiten

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

Amazon Cognito > Benutzerpools > User pool ->vtbh > App-Clients > App-Client: Gym2.0 Info

App-Client: Gym2.0

Bearbeiten Anmeldeseite anzeigen

App-Client-Informationen

App-Client-Name	Gym2.0	Dauer der Authentifizierungsablaufsituation	3 Minuten
Client-ID	[REDACTED]	Ablauf des Aktualisierungs-Tokens	5 Tag(e)
Client-Geheimnis	-	Ablauf des Zugriffs-Tokens	60 Minuten
Authentifizierungsabläufe	Wahlbasierte Anmeldung Benutzername und Passwort	Ablauf des ID-Tokens	60 Minuten
		Erweiterte Authentifizierungseinstellungen	Tokens-Aufhebung aktivieren „Fehler bei vorhandenen Benutzern verhindern“ aktivieren

Quick-Setup-Anleitung **Attributberechtigungen** **Anmeldeseite** **Bedrohungsschutz**

Konfiguration verwalteter Anmeldeseiten Info

Konfigurieren Sie die verwalteten Anmeldeseiten für diesen App-Client.

Status Verfügbar

Erlaubte Callback-URLs
<https://amplifyv2.d2r89bauoj5mo.amplifyapp.com>
<https://amplifyv2.d2r89bauoj5mo.amplifyapp.com/callback.html>

Standard-Umlenkungs-URL
-

Identitätsanbieter
Cognito-Benutzerpool-Verzeichnis

OAuth-Erteilungstypen
Autorisierungscode erteilen

OpenID-Connect-Bereiche
email
openid
profile

13. Authentifizierungsabläufe festlegen

Für das Projekt GYM2.0 sind folgende Einstellungen erforderlich:

- **ALLOW_USER_PASSWORD_AUTH → aktiviert**

- **ALLOW_USER_SR_P_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 an.

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 ausgewählt.

Wahlbasierte Anmeldung: ALLOW_USER_AUTH
Ihr Benutzerpool unterstützt die Wahlbasierte Anmeldung mit einer Liste von möglichst Methoden. Benutzer können Optionen wie Email/Passwort, biometrische Geräte und Sicherheitsschlüssel sowie die passwortbasierte Anmeldung mit MFA wählen.

Mit Benutzernamen und Passwort anmelden: ALLOW_USER_PASSWORD_AUTH
Benutzer anmelden sich mit einem Benutzernamen und einem Passwort. Diese Methode sendet den Benutzernamen und das Passwort direkt an Ihren Benutzerpool.

Mit einem sicheren Remote-Passwort (SRP) anmelden: ALLOW_USER_SR_P_AUTH
Benutzer können sich mit Benutzernamen 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 Authentifizierungsabläufen mit Benutzernamen und Passwort anmelden. Dieses Feature wird in HostedUI nicht unterstützt.

Anmeldung mit benutzerdefinierten Authentifizierungsabläufen von Lambda-Ausführen: ALLOW_CUSTOM_AUTH
Benutzer können sich anmelden, optional mit Benutzernamen und Passwort, und auf benutzerdefinierte Herausforderungen antworten, die Sie in Lambda-Funktionen entwerfen.

Neue Beutztokens aus vorhandenen authentifizierten Sitzungen abrufen: ALLOW_REFRESH_TOKEN_AUTH
Ihre Anwendung kann Aktualisierungstoken mit längerer Lebensdauer speichern, das Benutzersitzungen ohne zusätzliche Benutzen-Prompts erneuert.

Dauer der Authentifizierungsablaufzeit | Info
 Minuten
Muss zwischen 3 und 15 Minuten liegen.

Ablauf des Aktualisierungs-Tokens | Info
 Tage Minuten
Muss zwischen 50 Minuten und 10 Jahren liegen.

Ablauf des Zugriffs-Tokens | Info
 Tage Minuten
Muss zwischen 5 Minuten und 1 Tag liegen. Wert darf nicht größer als der Ablauf des Aktualisierungs-Tokens sein.

Ablauf des ID-Tokens | Info
 Tage Minuten
Muss zwischen 5 Minuten und 1 Tag liegen. Wert darf nicht größer als der Ablauf des Aktualisierungs-Tokens sein.

Erweiterte Sicherheitskonfigurationen – optional
 Token-Aufhebung aktivieren | Info
Amazon Cognito fügt neue Ansprüche für Zugriffs- und ID-Toknen hinzu, um den Wiederaufzug zu aktivieren. Das erhöht die Größe der Toknen.

Fehler bei vorhandenen Benutzern verhindern | Info
Amazon-Cognito-Authentifizierungs-APIs geben eine generische Fehlerantwort zurück, die angibt, dass der Benutzernname oder das Passwort falsch ist, anstatt anzugeben, dass der Benutzer nicht gefunden wurde.

Aktualisierungstokennung Treach-Toknen zulassen | Info
Senden Sie Aktualisierungstoken und erhalten Sie neue ID-, Zugriffs- und Aktualisierungstoken für Benutzer. Mithilfe dieser Option können Sie Aktualisierungstoken rotieren, bevor der Ablaufzeitraum abgelaufen ist.

Aktualisierungswen für Refresh-Token Aktualisiert für das Aktualisieren des Toknen 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.)

Amazon Cognito

Aktueller Benutzerpool [Aktion anzeigen](#)

Übersicht

Anwendungen

App-Clients

Benutzermanagement

Benutzer

Gruppen

Authentifizierung

Authentifizierungsmethoden

Annehmen

Registrieren

Soziale und externe Anbieter

Erweiterungen

Sicherheit

AWS WAF

Bildungsschutz

Protokolldaten

Branding

Domain

Verwaltete Anmeldung [Info](#)

Nachrichtenverlagen

Einstellungen

Feature-Plan

Tags

Löschnschutz

Identitäts-Pools

Authentifizierungsmethoden [Info](#)

E-Mail-Adresse [Info](#)
Konfigurieren Sie, wie Ihr Benutzerpool E-Mail-Nachrichten an Benutzer sendet.

E-Mail-Anbieter
Senden von E-Mails mit Cognito

SES-Region
Europa (Stockholm)

ABSENDER-E-Mail-Adresse
no-reply@verificationemail.com

ANTWORT-E-Mail-Adresse

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

SNS-Region

AWS-Service-Abhängigkeiten konfigurieren, um die Einrichtung Ihrer SMS-Ausgabenlimits 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:

- Anfordern einer Erhöhung des Amazon SMS-Ausgabenlimits
- Wechsel zur Amazon SNS-Produktionsumgebung
- Einrichten einer Ursprungsendlichkeit 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

Temporelle Passwörter, die von Administratoren festgelegt wurden, laufen ab
7 Tagen

Wiederherstellung früherer Passwörter zulassen

Passkey [Info](#)
Konfigurieren Sie die Anmeldung mit Biometrie, Handcheinchlüssel und Authentifizierungs-Apps.

Verifizierung durch den Benutzer
Bevorzugt

Domain für die ID der vertrauenswürdigen Instanz
Cognito-Prüfdomäne

Cognito-Prüfdomäne
eu-north-1cognitoauth.eu-north-1.amazoncognito.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