

CVDex

COGNITO_HOSTED_UI_CONFIG

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

November 10, 2025

1 Cognito Hosted UI Configuration - Manual Steps

Last Updated: November 8, 2025

Status: Required for Hosted UI login to work

1.1 Quick Summary

The error "**Login pages unavailable**" means the Cognito App Client is not configured for Hosted UI. This guide walks through the AWS Console steps to enable it.

Time Required: 5-10 minutes

Difficulty: Easy

Prerequisites: AWS Account with Cognito admin access

1.2 Step-by-Step Instructions

1.2.1 Step 1: Open AWS Cognito Console

1. Go to: <https://console.aws.amazon.com/cognito/>
 2. Make sure you're in region **us-east-2** (top-right dropdown)
 3. Select **User pools** on the left sidebar
 4. Click on: **us-east-2_FyHLtOhY** (the Finanzas user pool)
-

1.2.2 Step 2: Navigate to App Client Settings

1. In the left sidebar, expand **App integration**
 2. Click **App clients and analytics**
 3. You should see a list of clients
 4. Look for and click on the row with Client ID: dshos5iou44tuach7ta3ici5m
 - (The name might be "Finanzas-SDT" or similar)
-

1.2.3 Step 3: Edit Authentication Flows Configuration

In the **Authentication flows configuration** section:

1. Under "Authentication flows":

- Check: **User password-based authentication (ALLOW_USER_PASSWORD_AUTH)**

- Check: **Allow refresh token based authentication (ALLOW_REFRESH_TOKEN_AUTH)**
- Check: **Allow implicit OAuth authFlow (ALLOW_IMPLICIT_OAUTH_AUTH_FLOW)**

(These enable both internal login and Hosted UI flows)

2. Click "Save changes" at the bottom of the page
-

1.2.4 Step 4: Configure Hosted UI Settings

Scroll down to the "Hosted UI settings" section:

4a. Allowed Callback URLs

1. Find the field: **Allowed callback URLs**
2. Click the **Edit** button or clear existing values
3. Add all three URLs (one per line or comma-separated):

`https://d7t9x3j66yd8k.cloudfront.net/auth/callback.html`
`https://d7t9x3j66yd8k.cloudfront.net/finanzas/`
`https://d7t9x3j66yd8k.cloudfront.net/`

1.2.5 Step 5: Configure OAuth 2.0 Settings

Under "OAuth 2.0 settings":

5a. Allowed OAuth Flows

 Check both:

- **Implicit code**
- **Authorization code**

(*Implicit is what we're using; Authorization code is for future PKCE flow*)

5b. Allowed OAuth Scopes

 Check all three:

- **openid**
- **email**
- **profile**

These scopes allow us to read user email and group information from the ID token.

1.2.6 Step 6: Save All Changes

1. **Scroll to the bottom** of the page
 2. Click the large "**Save changes**" button
 3. Wait for confirmation: "App client updated successfully"
-

1.2.7 Step 7: Wait for Propagation

- AWS Cognito changes typically propagate within **30 seconds to 2 minutes**
 - If you see errors immediately, **wait 2 minutes** and try again
-

1.2.8 Step 8: Test the Hosted UI Link

Once saved, test the login flow:

Paste this URL into a new incognito browser window:

https://us-east-2fyhltohiy.auth.us-east-2.amazoncognito.com/login?client_id=dshos5i...

Expected Result:

- See Cognito login form (username/password fields)
- Log in with test credentials
- Redirect to <https://d7t9x3j66yd8k.cloudfront.net/auth/callback.html> (briefly)
- Land at /finanzas/ (FinanzasHome page)
- localStorage contains cv.jwt and finz_jwt

If still seeing "Login pages unavailable":

1. Clear browser cache: Cmd+Shift+Delete
 2. Wait another minute
 3. Try the URL again
-

1.3 Configuration Summary Table

Setting	Value	Purpose
Client ID	dshos5iou44tuach7ta3ici5m	Identifies the app to Cognito
Auth Flows	USER_PASSWORD_AUTH, IMPLICIT_OAUTH	Enable internal + Hosted UI login

Setting	Value	Purpose
Callback URLs	/auth/callback.html, /finanzas/, /	Where Cognito redirects after login
OAuth Flows	Implicit, Code	Support both implicit (Hosted UI) and
Scopes	openid, email, profile	What user data we can read

1.4 Troubleshooting

1.4.1 Error: "Login pages unavailable"

Cause: Implicit OAuth flow not enabled or callback URL not added.

Fix:

- Verify "Allow implicit OAuth authFlow" is checked
- Verify callback URL <https://d7t9x3j66yd8k.cloudfront.net/auth/callback.html> is in the list
- Save and wait 2 minutes

1.4.2 Error: "Invalid redirect_uri"

Cause: The redirect URL in the login link doesn't match the allowed callback URLs.

Fix:

- Ensure the callback URL is spelled exactly:
<https://d7t9x3j66yd8k.cloudfront.net/auth/callback.html>
- No trailing slash
- Lowercase domain

1.4.3 Form appears but login fails

Cause: User credentials wrong or Cognito user not created.

Fix:

- Verify the user exists in Cognito → Users
- Verify the password is correct
- Check CloudWatch Logs (Cognito → CloudWatch Logs) for error details

1.4.4 Tokens stored but user sees LoginPage after redirect

Cause: AuthProvider not reading the tokens correctly.

Fix:

- Open DevTools → Application → localStorage
 - Verify cv.jwt exists and is not empty
 - Reload the page; AuthProvider should initialize from localStorage
-

1.5 Next Steps

Once Hosted UI is working:

1. Test all three user types:

- SDT-only → should land at /finanzas/
- PMO-only → should land at /
- Dual-role → should land at /finanzas/ by default

2. Verify token content:

- Open DevTools → Application → localStorage
- Find cv.jwt value
- Paste into <https://jwt.io> to decode and verify groups are present

3. Share the Hosted UI link with team:

- Copy the login URL from Step 8 above
 - Teams/Slack/email it to users
 - Users click the link, log in, and land in the correct app
-

1.6 Reference URLs

- **AWS Cognito Console:** https://console.aws.amazon.com/cognito/v2/idp/user-pools/us-east-2_FyHLtOhiY/clients?region=us-east-2
- **User Pool ID:** us-east-2_FyHLtOhiY
- **Client ID:** dshos5iou44tuach7ta3ici5m
- **Cognito Domain:** us-east-2fyltohiy.auth.us-east-2.amazoncognito.com
- **Finanzas App:** <https://d7t9x3j66yd8k.cloudfront.net/finanzas/>
- **PMO App:** <https://d7t9x3j66yd8k.cloudfront.net/>

Questions? Check the troubleshooting section above or review the Finanzas Routing Verification guide.