# Finanzas Authentication Validation Guide

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

January 25, 2026

# 1 Finanzas Authentication Validation Guide

## 1.1 Overview

This document provides step-by-step manual validation procedures for the Finanzas Cognito Hosted UI authentication flow. Use this guide to verify that the authentication system is working correctly after deployment.

## 1.2 Architecture Summary

### 1.2.1 Authentication Flow (Cognito Hosted UI + Implicit Grant)

1. **User initiates login**: Clicks "Sign in with Cognito Hosted UI" in the Finanzas application

2. **Redirect to Cognito**: Browser redirects to Cognito Hosted UI domain (`us-east-2fyhltohiy.a`

3. **User authenticates**: Enters credentials on Cognito-hosted login page

4. **Cognito redirects with tokens**: After successful auth, Cognito redirects back to callback URL with tokens in URL hash:

   `https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.html#id_token=...&`

5. **Callback processes tokens**: Static `callback.html` file:

   - Parses tokens from URL hash fragment
   - Validates `id_token` is present
   - Stores tokens in localStorage (keys: `cv.jwt`, `finz_jwt`, `idToken`, `cognitoIdToken`)
   - Determines user's module access from token claims (Cognito groups)
   - Redirects to appropriate module (`/finanzas/` or `/`)

6. **React app loads**: AuthProvider detects stored tokens and initializes authenticated session

### 1.2.2 Key Configuration

- **User Pool ID**: `us-east-2_FyHLtOhiY`
- **App Client ID**: `dshos5iou44tuach7ta3ici5m`
- **Cognito Domain**: `us-east-2fyhltohiy.auth.us-east-2.amazoncognito.com` (no hyphen after region)
- **CloudFront URL**: `https://d7t9x3j66yd8k.cloudfront.net`
- **Callback URL**: `https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.html`
- **OAuth Flow**: Implicit grant (response_type=token)
- **OAuth Scopes**: openid, email, profile

### 1.3 Manual Validation Procedure

### 1.3.1 Prerequisites

- Access to test Cognito user account (e.g., `christian.valencia@ikusi.com`)
- Modern web browser with Developer Tools
- Network connectivity to CloudFront and Cognito

### 1.3.2 Step-by-Step Validation

**1. Clear Browser State**   Before testing, ensure a clean state:

```
[] // Open browser console and run: localStorage.clear(); sessionStorage.clear();
```

Then refresh the page or navigate to: `https://d7t9x3j66yd8k.cloudfront.net/finanzas/`

**2. Initiate Hosted UI Login**

1. Navigate to: `https://d7t9x3j66yd8k.cloudfront.net/finanzas/`

2. You should see the login page

3. Click the **"Sign in with Cognito Hosted UI"** button

4. **Expected**: Browser redirects to Cognito Hosted UI domain

5. **Verify URL** contains:

   `https://us-east-2fyhltohiy.auth.us-east-2.amazoncognito.com/oauth2/authorize?.`

**3. Authenticate with Cognito**

1. On the Cognito login page, enter test credentials:
   - **Email**: `christian.valencia@ikusi.com`
   - **Password**: (use the configured test password)

2. Click **Sign In**
3. **Expected**: After successful authentication, browser redirects back to callback URL

**4. Verify Callback Processing**   This is the most critical step.  Open browser Dev-Tools (F12) **before** starting the login flow to capture all logs.
   **What to observe**:

1. **URL should briefly show**:

   ```
   https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.html#id_token=eyJ.
   ```

2. **Console logs should show** (search for [Callback] prefix):

   ```
   [Callback] Starting authentication callback processing
   [Callback] href: https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.h
   [Callback] id_token present: true
   [Callback] access_token present: true
   [Callback] □ id_token successfully extracted from hash
   [Callback] Token claims decoded successfully
   [Callback] User: christian.valencia@ikusi.com
   [Callback] Storing tokens in localStorage...
   [Callback] □ Stored both id_token and access_token
   [Callback] User groups: ["SDT"]
   [Callback] Routing: SDT-only user → /finanzas/
   [Callback] Final redirect target: /finanzas/
   [Callback] Executing redirect to: /finanzas/
   ```

3. **Page should show** "Signing you in…" briefly before redirecting

4. **After ~50ms**: Browser redirects to /finanzas/ and loads the dashboard

**5. Verify Token Storage**   After successful login, check localStorage:

```
   [] // In browser console:  console.log('cv.jwt:', localStorage.getItem('cv.jwt')); con-
sole.log('finz_jwt:', localStorage.getItem('finz_jwt')); console.log('idToken:', localStor-
age.getItem('idToken')); console.log('cognitoIdToken:', localStorage.getItem('cognitoIdToken'));
console.log('finz_access_token:', localStorage.getItem('finz_access_token'));
```

   **Expected**: All five keys should contain JWT tokens (long base64-encoded strings)

**6. Verify Authenticated Session**

1. **Dashboard loads**: You should see the Finanzas dashboard with navigation
2. **No redirect loop**: Page should not redirect back to login
3. **User menu**: Click on user avatar/menu in top-right corner
4. **Profile displays**: Should show user information from token

**7. Verify Role-Based Access** Based on user's Cognito groups, verify appropriate sections are accessible:

- **SDT/FIN/AUD groups**: Can access Finanzas module (`/finanzas/`)
- **PMO/EXEC_RO groups**: Can access PMO module (`/`)
- **Dual-role users**: Can switch between modules

Navigate to different sections to ensure no authentication errors: - `/finanzas/catalog/rubros` - Rubros catalog - `/finanzas/projects` - Projects manager - `/finanzas/adjustments` - Adjustments

**8. Verify Logout**

1. Click logout button (usually in user menu)
2. **Expected**:

   - Tokens cleared from localStorage
   - Browser redirects to Cognito logout endpoint
   - Then redirects to `/finanzas/` (or login page)

3. **Verify**: Attempting to access `/finanzas/` after logout should show login page

## 1.4 Troubleshooting Common Issues

### 1.4.1 Issue 1: "No id_token present" Error

**Symptoms**: - Callback page shows error: "No id_token present" - Console shows: `[Callback] ▯ MISSING id_token in URL hash`

**Possible Causes**: 1. **OAuth configuration mismatch**: - Verify `response_type=token` in `src/config/aws.ts` - Verify `scope` includes `openid` 2. **Cognito App Client configuration**: - Check that "Implicit grant" is enabled - Verify callback URL is whitelisted exactly: `https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.html` 3. **Incorrect domain**: - Verify VITE_COGNITO_DOMAIN is set to: `us-east-2fyhltohiy.auth.us-east-`

**Fix**: - Review and correct configuration in `src/config/aws.ts` - Verify Cognito console settings match expected values - Redeploy if configuration changes were made

### 1.4.2 Issue 2: Infinite Login Loop

**Symptoms**: - After callback, page redirects back to login - Login → Cognito → Callback → Login (repeats)

**Possible Causes**: 1. **Tokens not being stored**: Callback.html failing to write to localStorage 2. **React intercepting callback route**: App.tsx rendering before callback completes 3. **CloudFront serving wrong file**: index.html served instead of callback.html

**Diagnosis**: 1. Check console for `[Callback]` logs - if missing, React is loading instead 2. Check Network tab - verify response body for `/finanzas/auth/callback.html` contains "Signing you in" 3. Check localStorage after redirect - if empty, tokens weren't stored

**Fix**: - Verify `src/App.tsx` has callback route exception (returns null for `/auth/callback` paths) - Verify post-deploy script confirms callback.html is being served (not index.html) - Check CloudFront configuration for `/finanzas/auth/*` behavior

### 1.4.3 Issue 3: CloudFront Returns index.html for Callback

**Symptoms**: - Network tab shows index.html content for `/finanzas/auth/callback.html` - No `[Callback]` logs in console - React app loads on callback URL instead of static HTML

**Diagnosis**:

```
[] # Test from command line: curl -I https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.
# Check response body contains callback markers: curl -s https://d7t9x3j66yd8k.cloudfront.net/fi
| grep "Signing you in"
```

**Possible Causes**: 1. **File not uploaded to S3**: Build artifact missing callback.html 2. **CloudFront caching**: Old cached version before callback.html existed 3. **CloudFront error handling**: SPA error handling (404 → index.html) intercepting callback

**Fix**: 1. Verify build output: `dist-finanzas/auth/callback.html` exists 2. Verify S3: `aws s3 ls s3://ukusi-ui-finanzas-prod/finanzas/auth/` 3. Invalidate CloudFront: `aws cloudfront create-invalidation --distribution-id EPQU7PVDLQXUA --paths "/finanzas/auth/*"` 4. Check CloudFront distribution configuration for custom error responses

### 1.4.4 Issue 4: CORS Errors on API Calls

**Symptoms**: - Login successful, dashboard loads - API calls fail with CORS errors - Console shows: "Access to fetch at '…' has been blocked by CORS policy"

**Possible Causes**: - API Gateway CORS not configured for CloudFront origin - Token not being sent in Authorization header

**Fix**: - Verify API Gateway has CORS enabled for CloudFront domain - Check that API calls include: `Authorization: Bearer ${token}` - Verify token is not expired

## 1.5 Known Limitations

1. **Implicit Grant Flow**: Currently using OAuth 2.0 implicit grant for simplicity

   - Tokens visible in URL (browser history)

- No refresh token capability
- **Future**: Migrate to Authorization Code Flow with PKCE for enhanced security

2. **Token Refresh**: No automatic token refresh implemented

- Users must re-login when token expires (typically 1 hour)
- **Future**: Implement refresh token flow

3. **Multi-Tab Behavior**: Token state not synchronized across browser tabs

- Logging out in one tab doesn't affect other tabs
- Tokens stored per-origin (shared across tabs), but state updates require page refresh

4. **Mobile Safari Quirks**: Some older iOS versions may have issues with hash-based token delivery

- URL hash may be stripped before callback.html executes
- Consider fallback to Authorization Code flow for mobile

## 1.6 Automated Testing

### 1.6.1 CI/CD Verification

The deployment pipeline includes automated checks in `scripts/post-deploy-verify.sh`:

```
[] # Run post-deployment verification: ./scripts/post-deploy-verify.sh
```

**What it checks**: 1. □ CloudFront UI accessible at `/finanzas/` 2. □ Auth callback accessible at `/finanzas/auth/callback.html` 3. □ Callback.html is actual file (not index.html) 4. □ SPA routing works for nested routes 5. □ Static assets load correctly 6. □ API endpoints respond

### 1.6.2 Pre-Build Validation

Before building, run:

```
[] npm run validate:pre-build
```

**What it checks**: - □ VITE_API_BASE_URL is set and valid - □ URL format is correct (https://...) - □ Optional: API connectivity (if VALIDATE_API_CONNECTIVITY=true)

## 1.7 Reference Configuration Files

### 1.7.1 Key Files for Authentication

1. **src/config/aws.ts**: Cognito configuration, OAuth settings, login/logout helpers
2. **src/components/AuthProvider.tsx**: Authentication state management, token validation
3. **src/hooks/useAuth.ts**: Hook for accessing auth context
4. **src/App.tsx**: Route guard, callback route exception
5. **public/finanzas/auth/callback.html**: OAuth callback handler (static file)
6. **public/auth/callback.html**: Duplicate callback for root path (legacy support)

### 1.7.2 Environment Variables

Required for production deployment:

```
[] # Cognito Configuration VITE_COGNITO_REGION=us-east-2 VITE_COGNITO_USER_POOL_ID=us-east-2_FyHLtOhiY VITE_COGNITO_CLIENT_ID=dshos5iou44tuach7ta3ici5m VITE_COGNITO_DOMAIN=
east-2fyhltohiy.auth.us-east-2.amazoncognito.com
    # CloudFront VITE_CLOUDFRONT_URL=https://d7t9x3j66yd8k.cloudfront.net
    # API VITE_API_BASE_URL=https://pyorjw6lbe.execute-api.us-east-2.amazonaws.com/dev
```

## 1.8 Support and Escalation

If issues persist after following this guide:

1. **Check recent PRs**: Review recent authentication-related PRs for known issues
2. **Review logs**: Check CloudWatch logs for API errors
3. **Cognito Console**: Verify user exists and is in correct groups
4. **CloudFront Console**: Check distribution configuration and cache behavior
5. **GitHub Issues**: Search for similar issues or create new one with validation results

---

**Last Updated**: 2025-11-22
**Maintained By**: Platform Engineering Team
**Related Docs**: AUTHENTICATION_FLOW.md, FINANZAS_AUTH_FIX_SUMMARY.md