

# Secure Communication

## Okta Updates



# Okta Updates

- Since Angular app is running on a different protocol
  - `https://localhost:4200`
- Need to update Okta configs for Redirect URIs

# Development Process

*Step-By-Step*

1. Update Redirect URI in Angular App
2. Update Redirect URIs in Okta Dashboard
3. Update API Trusted Origins in Okta Dashboard

# Step 1: Update Redirect URI in Angular App

File: my-app-config.ts

```
export default {  
  
  oidc: {  
    clientId: '<><>your-client-id<>>',  
    issuer: 'https://<><>your-dev-domain>>/oauth2/default',  
    redirectUri: 'https://localhost:4200/login/callback',  
    scopes: ['openid', 'profile', 'email']  
  }  
}
```

*Note the https*

*Since our Angular app will run using https*

# Step 2: Update Redirect URIs in Okta Dashboard

- Update redirect URIs

The image shows two overlapping screenshots from the Okta Dashboard. The left screenshot shows the 'General' tab of the 'Demo 5' application, displaying the Client ID (Ooa3c41kh6ZiUcvqX5d6) and the 'Use PKCE (for public clients)' option selected. The right screenshot shows the 'LOGIN' section where the 'Sign-in redirect URIs' and 'Sign-out redirect URIs' fields are both set to `https://localhost:4200/login/callback`. Below these fields, the 'Login initiated by' dropdown is set to 'App Only'. A green callout box with the text 'Note the https' has red arrows pointing to both the sign-in and sign-out redirect URI fields.

**Demo 5**

Client Credentials

Client ID: Ooa3c41kh6ZiUcvqX5d6

Client authentication: Use PKCE (for public clients)

Sign-in redirect URIs: https://localhost:4200/login/callback

Sign-out redirect URIs: https://localhost:4200

Login initiated by: App Only

Initiate login URI:

Note the https

# Step 3: Update API Trusted Origins in Okta Dashboard

The screenshot shows the Okta API Trusted Origins page. At the top, there are three tabs: Authorization Servers, Tokens, and Trusted Origins. A red arrow points to the Trusted Origins tab. Below the tabs, there's a section titled "Add Origins" with a note about adding Origin URLs for CORS access. A blue "Add Origin" button is visible. To the right, there's a search bar and a table with columns for Filters, Name, Origin URL, and Type. The table has one row: "All Origins" under Filters, "My SPA 200" under Name, "https://localhost:4200" under Origin URL, and "CORS Redirect" under Type. A red arrow points to the "Origin URL" column. A green callout box with white text says "Note the https".

| Filters     | Name       | Origin URL             | Type             |
|-------------|------------|------------------------|------------------|
| All Origins | My SPA 200 | https://localhost:4200 | CORS<br>Redirect |