The HTTP 401 Unauthorized error usually means that the **admin access token** you're using doesn't have the necessary permissions to access the API endpoint. This could be due to one or more of the following reasons:

**Possible Causes:**

1. **Incorrect Scopes**: The token may lack the correct scope to access the admin endpoints.
2. **Realm Permissions**: The token may not have permissions for the secure-realm you're trying to access.
3. **Token Expired**: The token might have expired (it has a short lifespan, typically 60 seconds).

**Steps to Troubleshoot:**

1. **Check Token Expiry**:
   * Your token has an expires\_in value of 60, which means it expires after 60 seconds. If you're seeing this error after a few seconds, the token may have expired.
   * **Fix**: Get a new token and try again promptly.
2. **Check Admin Role and Permissions**:
   * The token you used needs to have access to the **admin CLI** and permissions to manage users in the secure-realm. Make sure that:
     + The **client ID (admin-cli)** you're using for the token is correct.
     + The **user associated with the token** (e.g., admin) has the necessary roles/permissions in the Keycloak Admin Console.

**To verify user roles**:

* + Go to **Keycloak Admin Console** > **Users** > **admin** (or whichever user you used to generate the token).
  + Ensure the user has the realm-admin role assigned under **Role Mappings**.

1. **Check the Admin URL**:
   * Make sure that your Keycloak instance URL (http://localhost:8080) and the realm name (secure-realm) are correct.
   * The URL should be publicly accessible for your curl request to work.
2. **Verify Token’s Permissions**:
   * The token must include permissions for the **admin API** to query users. In your current response, the token only mentions email and profile in the **scope**.
   * You may need to request **admin** scope when obtaining the token.

**Regenerate the Token with Admin Scopes**

If you suspect the token does not have admin rights, you can request a new token with the correct scopes.

curl -X POST "http://localhost:8080/realms/master/protocol/openid-connect/token" \

-H "Content-Type: application/x-www-form-urlencoded" \

-d "username=admin" \

-d "password=your\_admin\_password" \

-d "grant\_type=password" \

-d "client\_id=admin-cli" \

-d "scope=admin"

If that still doesn’t work, let me know the next steps you want to take!