import { HttpClient, HttpHeaders } from '@angular/common/http';

import { Injectable } from '@angular/core';

import { UserAuthService } from './user-auth.service';

@Injectable({

providedIn: 'root'

})

export class UserService {

PATH\_API = "http://localhost:8080";

requestHeader = new HttpHeaders(

{ "No-Auth": "True" }

);

//httpclient will help calling /authenticate api at the backend

constructor(

private httpClient: HttpClient,

private userAuthService: UserAuthService

) { }

//this.httpClient.post(here url to api be called)

public login(LoginData) {

return this.httpClient.post(this.PATH\_API + "/authenticate", LoginData, { headers: this.requestHeader });

}

public forUser(){

return this.httpClient.get(this.PATH\_API + '/forUser', {responseType:'text'});

}

public forAdmin(){

return this.httpClient.get(this.PATH\_API + '/forAdmin', {responseType:'text'});

}

//roleMatch(allowedRoles) allowedRoles(roles specified to user in db)--> will be matched with actual roles-->stored in datastorage if matched-->return isMatch true

public roleMatch(allowedRoles): boolean {

let isMatch = false;

const userRoles: any = this.userAuthService.getRoles();

if (userRoles != null && userRoles) {

for (let i = 0; i < userRoles.length; i++) {

for (let j = 0; j < allowedRoles.length; j++) {

if (userRoles[i].roleName == allowedRoles[j]) {

isMatch = true;

return isMatch;

}

else {

return isMatch;

}

}

}

}

}

public userRegister(registerData){

return this.httpClient.post(this.PATH\_API+'/registerNewUser', registerData);

}

//backend-->JwtFilter-->Request.getHeader-->"Authorization"

//-->/authenticate /userRegistration -->does not require any token or authentication

}