# References

Code at : https://github.com/Ajay-Nallanagula/epampdp/tree/master/AUTH\_AUTORIZATION

* [Basic Auth, OAuth, OpenID Connect, Scopes & Refresh Tokens](https://www.youtube.com/watch?v=x6jUDfpESmA&list=PLP_rkG1reBjrCKy2Pb1bvjJKbKfantijk&index=3)
* \*\*\* Oauth+React+Node : <https://www.youtube.com/watch?v=GGGjnBkN8xk>
* [OAuth using React and Node](https://youtu.be/dyZmsz6usWk?feature=shared)
* <https://medium.com/strapi/protected-routes-and-authentication-with-react-and-node-js-d31d234644cd>
* Using JWT AUTH : <https://www.youtube.com/watch?v=nI8PYZNFtac>
* <https://auth0.com/blog/complete-guide-to-react-user-authentication/>

**🡪**  Get access Token: <https://auth0.com/docs/quickstart/spa/react/02-calling-an-api>

* <https://auth0.github.io/auth0-react/interfaces/GetTokenWithPopupOptions.html>

# Basic Authentication

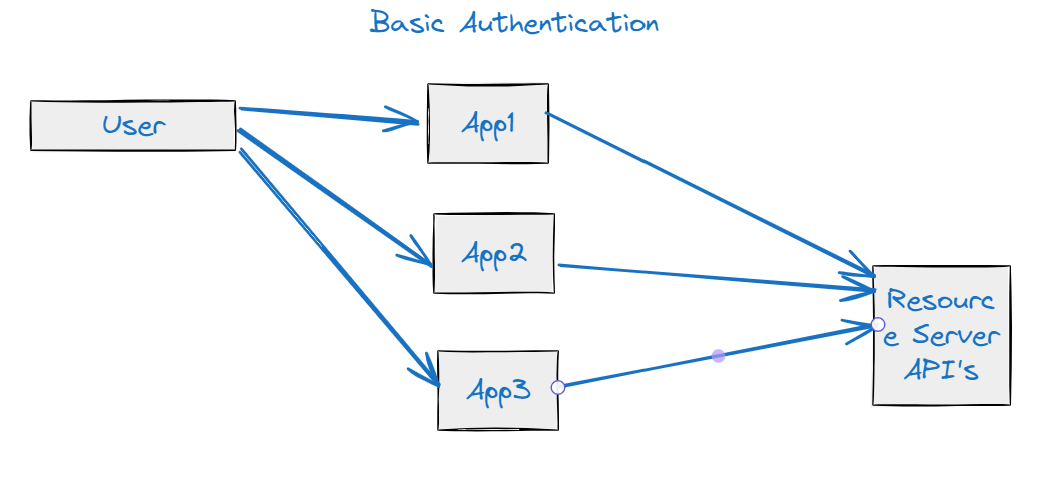
**Basic Authentication** : Where the username and password are encoded and sent on every request. The resource server, which is giving API’s sends the response . This is very naïve way of Authentication and certain dis advantages of it .

A diagram of a line

Description automatically generated

Disadvantages of Basic Authentication

1. The username and password is sent on every request this is risky. Password-Sharing is risky.
2. Now assume the resource server that offers API’s have grown popular and there are application(App1,App2,App3) that want to build on top of the API the resource server is providing … In that case as a user you will have to share the credentials with App1,App2,App3 these APPS will send the credentials to resource server on every request, Now regarding the access … consider resouce server is Twitter API, the user via App1,App2,App3 want to post a tweet and do no more.. In that case we will not have any control because App1,App2,App3 have the username and password, they can read time lines, direct-messages of our profile in Resource Server even though we didn’t give permissions … permission was only to write the messages .



1. There is no way to revoke access to an application, change in password will revoke access of all the three applications .

# OAUTH

OAUTH is limititing access to resources

1. OAUTH is granting access to applications without sharing the password to applications .
2. Ecah application should register with the API, so we can revoke access independently

## Authorization Code flow

A diagram of a software process

Description automatically generated

Assumptions:

1. There is an APP which want to talk to Resource server on Behalf of User.
2. That APP is APP1 Which has front Channel APP1(FC-APP1) and Back Channel APP1 (BC-APP1)
3. Auth-Server can be built from scratch or we can use AUTH0 Servers like OKTA, GOOGLE WORKSPACES , PingFederate etc.

Step 1: User access Front Channel of APP1,

Step 2: FC-APP1 sends a request to Authorization Server with following payload

Redirection URL: After auth flow success where to go the URL

Response Type: Code, the code here indicates this “Authorization Code Flow”.

Scope: FC-APP1 request for permissions, read/write/read-write etc

Step 3: Auth server prompts the User for his consent

Step 4: Assuming users give consent for the Prompt

Step 5: **Authorization code** is shared to FC-APP1

Step 6: Back channel communication , this happens backside cannot see these calls in the browser. These are internal calls , BC-APP1 takes the Authorization Code from FC-APP1 (Back Channel Communication)

Step 7: BC-APP1 sends **Authorization Code + SALT KEY** to Auth-Server .

Step 8: Auth-Server validates the Authorization Code and as response sends **Access Token** with required information **.**

Step 9: Using this Access Token, APP1 can communicate with Resource Server.

Step 10: Resorce server once recieves the access token, this will send to Authorization server for verification and recieves claims and user data

**How is Autorization Code Misused?**

**-----------------------------------------------------**

Authorization Code is Opaque key, without much information , BC-APP1 Shares Authorization Code + SALT Value with Auth-Server , Even If the Authorization Code is leaked , the salt value is known only to BC-APP1 and Authorization Server.

\*\*When OAUTH was introduced , It was mistakenly used for Authentication rather than delegated Authorization .

OAUTH was used to identify the user rather than focussing on access rights which is NOT CORRECT.

OAUTH at the nd gives us an access token which doesn’t contain any user/profile information like name, email,phone etc It contains only permissions for accessing the resources .

Everyone started writing hacks to authenticate using access token which is not the purpose of OAUTH this is not standarized way of OAUTH.

So to handle the authentication along with Authorization using OAUTH , **OPENID CONNECT was introduced.**

## OAUTH + OPENID CONNECT

**What is OpenID Connect?**

* Allows client to Verify the identity of end-users and get basic profile information about.
* OpenID Connect is a simple identity layer on top of OAUTH which tackles the identity problems i.e Authentication. OpenID Connect is not a separate protocol , Its meant to work along with OAUTH for authentication and Authorization.

Flow With OpenID Connect + OAUTH is as below shown

A diagram of a software process

Description automatically generated

Assumptions:

1. There is an APP which want to talk to Resource server on Behalf of User.
2. That APP is APP1 Which has front Channel APP1(FC-APP1) and Back Channel APP1 (BC-APP1)

Step 1: User access Front Channel of APP1,

Step 2: FC-APP1 sends a request to Authorization Server with following payload

Redirection URL: After auth flow success where to go the URL

Response Type: Code, the code here indicates this “Authorization Code Flow”.

Scope: FC-APP1 request for permissions, read/write/read-write and **“openid”**

Step 3: Auth server prompts the User for his consent

Step 4: Assuming users give consent for the Prompt

Step 5: **Authorization code** is shared to FC-APP1

Step 6: Back channel communication , this happens backside cannot see these calls in the browser. These are internal calls , BC-APP1 takes the Authorization Code from FC-APP1 (Back Channel Communication)

Step 7: BC-APP1 sends **Authorization Code + SALT KEY** to Auth-Server .

Step 8: Auth-Server validates the Authorization Code and as response sends **Access Token and ID TOKEN** with required information **.**

[Id Token is used for authentication Purposes and Access Token is used for Authorization purposes](https://auth0.com/blog/id-token-access-token-what-is-the-difference/)

Step 9:Using theses tokens, APP1 can communicate with Resource Server.

Step 10: Resorce server once recieves the access token, this will send to Authorization server for verification and recieves claims and user data

## Scopes

**What are Scopes?**

Scopes are used to limit access to user data

During Authorization Request , Auth-Provider will list down all the available scopes to the user, so that he understands what rights is he giving to the 3rd Party Application . This is Step-4 Typically where the scopes are listed.

Scopes should be more specific and not generic like read/write/read-write

Lets say you have to access Twitter API, which has resources like Timeline, Followers Messages, Tweets

If the scopes are generic , like say read.. the 3rd Party Application can read all the resources so rather than generic read we can give scopes like

Read-Timeline, Read-Tweets ,Read-Messages etc

Similarly for other writes etc …. We can use mix and match..

## Refresh Tokens

**What are Refresh Tokens**

------------------------------------------

Allows access tokens to be renewed

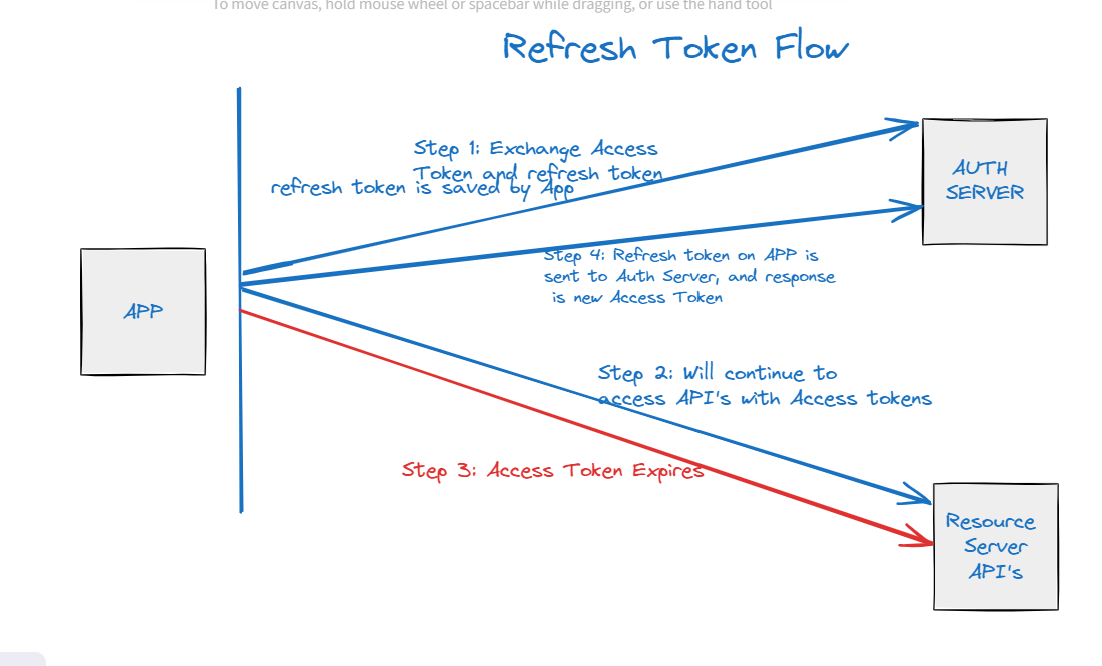
Access Tokens have a shelf life, even when compromised will not cause a devastating effect.

We can limit the Access token by providing a time periods , after a set time period 10mins or 30mins or an hour the access tokens are renewed . This provides another layer of security to our resources

Its Not a good idea to allow the access tokens live eternal…

The renew token is issued without the involvement of end user, the application(FC+BC) can provide its clientId and secret are passed to get new Access Token , It happens in back Channel only its risky to be on front channel.

ClientId is the unique Id using which the 3rd partyApplication registers with the Authorization Server



Step 1: Exchange Access Token and refresh token are sent by Auth Server. Refresh token is saved by Application user is accessing.

Step 2: Application will continue to access the Resource Server API with the access token that is provided by Auth Server.

Step 3: The Access token time elapsed and is expired .

Step 4: In that case the Application will send the refresh token to Auth server , Auth server in return will send the renewed Access Token

# WORKING OF CODE

## React Frontend

* \*\*\* Oauth+React+Node : <https://www.youtube.com/watch?v=GGGjnBkN8xk>
* Follow the example at C:\Ajay\_EPAM\PDP\_PRACTICSE\epampdp\AUTH\_AUTORIZATION\oAuth\auth-code-flow-demo on GitHub
* React Auth0 Packages Usage: <https://auth0.com/blog/complete-guide-to-react-user-authentication/>

Auth0 provides a package to work with authentication and Authorization with React

npm install @auth0/auth0-react

This @auth0/auth-react gives use few convenient methods like

 useAuth0, withAuthenticationRequired,Auth0Provider, useAuth0()

In short the auth0-react package will encapsulate all the logic that you have to do with Frontend-Channel and Backend-Channel and it will provide you with

Authorization-Code: getAccessTokenSilently or getAccessTokenWithPopup

Id Token: getIdTokenClaims

## NodeJs Backend

For NodeJs we need a package to be installed “npm i express-oauth2-jwt-bearer”

The auth method in the package will retrieve the bearer token and Id token and will give access to protected resources. All this is encapsulated

# Refresh Token Implementation

1. **Enable Refresh Token Rotation**: In the Auth0 dashboard, go to your application settings and enable "Refresh Token Rotation" under the "Advanced Settings" section.
2. **Set up API Scopes**: Ensure your API in Auth0 has the necessary scopes. You might need a scope like **offline\_access** for refresh tokens.

import createAuth0Client from '@auth0/auth0-spa-js';

const auth0 = await createAuth0Client({

domain: 'YOUR\_DOMAIN',

client\_id: 'YOUR\_CLIENT\_ID',

redirect\_uri: window.location.origin,

audience: 'YOUR\_API\_IDENTIFIER',

scope: 'openid profile email offline\_access',

});

// Log in the user and get the tokens

await auth0.loginWithRedirect();

const token = await auth0.getTokenSilently();

const refreshToken = auth0.getRefreshToken(); // Store this securely

Set up Axios Instance:

import axios from 'axios';

import createAuth0Client from '@auth0/auth0-spa-js';

// Create an axios instance

const api = axios.create({

baseURL: 'https://your-api-url.com',

});

// Function to get access token from Auth0

const getAccessToken = async () => {

return await auth0.getTokenSilently();

};

// Function to refresh access token

const refreshAccessToken = async () => {

const refreshToken = localStorage.getItem('refresh\_token'); // or from other secure storage

const { data } = await axios.post('https://your-domain/oauth/token', {

grant\_type: 'refresh\_token',

client\_id: 'YOUR\_CLIENT\_ID',

refresh\_token: refreshToken,

});

// Store new access token and refresh token

localStorage.setItem('access\_token', data.access\_token);

if (data.refresh\_token) {

localStorage.setItem('refresh\_token', data.refresh\_token);

}

return data.access\_token;

};

// Add a request interceptor

api.interceptors.request.use(

async (config) => {

const token = await getAccessToken();

if (token) {

config.headers['Authorization'] = `Bearer ${token}`;

}

return config;

},

(error) => {

return Promise.reject(error);

}

);

// Add a response interceptor

api.interceptors.response.use(

(response) => {

return response;

},

async (error) => {

const originalRequest = error.config;

// Check if the error is due to expired token

if (error.response.status === 401 && !originalRequest.\_retry) {

originalRequest.\_retry = true;

try {

// Attempt to refresh the token

const newAccessToken = await refreshAccessToken();

api.defaults.headers.common['Authorization'] = `Bearer ${newAccessToken}`;

originalRequest.headers['Authorization'] = `Bearer ${newAccessToken}`;

// Retry the original request

return api(originalRequest);

} catch (refreshError) {

// Handle refresh token failure (e.g., logout the user)

console.error('Token refresh failed:', refreshError);

// Redirect to login or logout user

}

}

return Promise.reject(error);

}

);

export default api;

### Complete Flow

1. **User logs in** and receives an access token and a refresh token.
2. **Access token is used** for API requests via Axios.
3. If an API request returns **401 Unauthorized**:
   * **Axios interceptor** catches this and uses the refresh token to get a new access token.
   * **New access token** is used to retry the failed request.

### Security Considerations

* **Token Storage**: Storing tokens in localStorage can expose them to XSS attacks. Consider more secure storage methods.
* **Token Rotation**: Regularly rotate refresh tokens to reduce the risk of token leakage.
* **Error Handling**: Ensure your application gracefully handles token refresh failures, potentially redirecting users to login.