

Especialización en Back End II

Mapear membresías de groups dentro del token

Empecemos creando un cliente con “**client id: myclient**”. Luego, creamos un usuario en Keycloak, por ejemplo, un usuario con “**username: Carlos**”. Una vez tenemos estos datos, navegamos al client **myclient** y hacemos clic en la pestaña “**Mappers**”. En esta pestaña, crearemos un mapper haciendo clic en el botón “**Create**”.

En esta página crearemos un mapper con los siguientes atributos:

- Name: groups
- Mapper Type: Group Membership
- Token Claim Name: groups

[Clients](#) > [myclient](#) > [Mappers](#) > Create Protocol Mappers

Create Protocol Mapper


Protocol ?	<input type="text" value="openid-connect"/>
Name ?	<input type="text" value="groups"/>
Mapper Type ?	<input type="text" value="Group Membership"/>
Token Claim Name ?	<input type="text" value="groups"/>
Full group path ?	<input checked="" type="checkbox"/>
Add to ID token ?	<input checked="" type="checkbox"/>
Add to access token ?	<input checked="" type="checkbox"/>
Add to userinfo ?	<input checked="" type="checkbox"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>

Hacemos clic en el botón **“Save”** y se creará nuestro mapper para el client **myclient**.

Clients > myclient

Myclient

Settings Roles Client Scopes **Mappers** Scope Revocation Sessions Offline Access Installation





Create Add Builtin

Name	Category	Type	Priority Order	Actions	
groups	Token mapper	Group Membership	0	Edit	Delete

Ahora debemos crear un grupo para este usuario. Para eso hacemos clic en el link **“Groups”**.


User Groups

Groups Default Groups 



View all groups

New Edit Cut Paste Delete

 Groups

Luego, hacemos clic en **“New”** y crearemos un grupo que se llamará **“Project Management Office”**. Escribimos el nombre dentro de **“Name”** y hacemos clic en **“Save”**.

Create group

Name *

Project Management Office


Save Cancel

Ahora debemos añadir a **Carlos** al grupo, para esto vamos a la página de usuarios y, en el detalle del usuario, vamos a la pestaña “**Groups**”.

[Users](#) > carlos

Carlos 

[Details](#) [Attributes](#) [Credentials](#) [Role Mappings](#) [Groups](#) [Consents](#) [Sessions](#)



Group Membership ?	Available Groups ?
<input type="text" value="Search..."/> <input type="button" value="Q"/>	<input type="text" value="Search..."/> <input type="button" value="Q"/>
<input type="button" value="View all groups"/> <input type="button" value="Leave"/>	<input type="button" value="View all groups"/> <input type="button" value="Join"/>
	 Project Management Office

Para ingresar al grupo hacemos clic en el nombre del grupo en el recuadro “**Available Groups**” y luego en “**Join**”. Ahora, el grupo nos deberá aparecer dentro de “**Group Membership**”.

[Users](#) > carlos


Carlos 

[Details](#) [Attributes](#) [Credentials](#) [Role Mappings](#) [Groups](#) [Consents](#) [Sessions](#)

Group Membership ?	Available Groups ?
<input type="text" value="Search..."/> <input type="button" value="Q"/>	<input type="text" value="Search..."/> <input type="button" value="Q"/>
<input type="button" value="View all groups"/> <input type="button" value="Leave"/>	<input type="button" value="View all groups"/> <input type="button" value="Join"/>
 /Project Management Office	 Project Management Office

El usuario **Carlos** es ahora miembro del grupo **Project Management Office**. Volvamos a la pantalla del cliente, dentro de la pestaña “**Client Scopes**” vamos al apartado “**Evaluate**”. Una vez allí, donde dice “user”, escribimos el nombre del usuario y lo seleccionamos.

Clients > myclient

Myclient 

Settings Keys Roles **Client Scopes** Mappers Scope Revocation Sessions Offline Access Installation

Setup **Evaluate**

Scope Parameter openid

Client Scopes

Available Optional Client Scopes

address
microprofile-jwt
offline_access
phone

Add selected >

Selected Optional Client Scopes

<< Remove selected

Effective Client Scopes

acr
email
profile
roles
web-origins

User carlos

Evaluate

Una vez tenemos el usuario, hacemos clic en el botón “**Evaluate**” y veremos lo siguiente:

Effective Protocol Mappers Effective Role Scope Mappings Generated Access Token Generated ID Token Generated User Info

Name	Parent Client Scope	Category	Type	Priority Order
allowed web origins	web-origins	Token mapper	Allowed Web Origins	0
acr loa level	acr	Token mapper	Authentication Context Class Reference (ACR)	0
profile	profile	Token mapper	User Attribute	0
family name	profile	Token mapper	User Property	0
given name	profile	Token mapper	User Property	0
nickname	profile	Token mapper	User Attribute	0
updated at	profile	Token mapper	User Attribute	0
locale	profile	Token mapper	User Attribute	0
full name	profile	Token mapper	User's full name	0
zoneinfo	profile	Token mapper	User Attribute	0
gender	profile	Token mapper	User Attribute	0

Hacemos clic en la pestaña **“Generated Access Token”** para ver que nuestro token posea la información sobre el grupo del usuario.



```

{
  "uma_authorization":
  },
  "resource_access": {
    "account": {
      "roles": [
        "manage-account",
        "manage-account-links",
        "view-profile"
      ]
    }
  },
  "scope": "openid profile email",
  "sid": "4c8deec8-7c06-4466-b731-91af230635a0",
  "email_verified": false,
  "groups": [
    "/Project Management Office"
  ],
  "preferred_username": "carlos"
}
```

Como se puede observar, se tiene el atributo **“groups”:[“/Project Management Office”]**, indicándonos que nuestro token ahora devuelve la información sobre los grupos a los que pertenece un usuario.