

Sumário

1. Criar Realm
2. Criar Roles
3. Criar Usuários
4. Criar Clients (2 APIs)
5. Criar Client Scope para Audience
6. Associar Client Scope aos Clients
7. Validar token para as duas APIs
8. Obter Token
9. Erro Account is not fully set up

1 Criar Realm

Menu lateral:

Manage realms
→ Create realm

Preencha:

- Realm name: banco-carrefour

Create realm ×

A realm manages a set of users, credentials, roles, and groups. A user belongs to and logs into a realm. Realms are isolated from one another and can only manage and authenticate the users that they control.

Resource file [Browse...](#) [Clear](#)

Upload a JSON file

Realm name *

Enabled On

Create [Cancel](#)

Create

2 Criar Roles (Realm Roles)

Menu lateral:

Realm: banco-carrefour

- Realm roles
- Create role

The screenshot shows the Keycloak administration interface. The top navigation bar has the realm name 'banco-carrefour' and the status 'Current realm'. On the far right, there is a user icon labeled 'admin'. The left sidebar contains a navigation menu with the following items: 'Manage realms', 'Manage', 'Clients', 'Client scopes', 'Realm roles' (which is highlighted), 'Users', 'Groups', 'Sessions', 'Events', 'Configure', and 'Realm settings'. The main content area is titled 'Realm roles' and contains a sub-header: 'Realm roles are the roles that you define for use in the current realm.' with a 'Learn more' link. Below this is a search bar with placeholder 'Search role by name' and a blue 'Create role' button. To the right of the search bar is a 'Refresh' button. At the bottom of the table are two pagination controls: '1 - 3' and '< >'.

Role name	Composite	Description	⋮
default-roles-banco-carrefour	True	role_default-roles	⋮
offline_access	False	role_offline-access	⋮
uma_authorization	False	role_uma_authorization	⋮

Role 1

- Role name: admin
- Save

Role 2

- Role name: transaction-api-access
- Save

Role 3

- Role name: report-api-access
- Save

✓ Essas roles serão usadas pelas DUAS APIs

3 Criar Usuários

Usuário Admin

Caminho:

Users
→ Create new user

The screenshot shows the Keycloak administration interface. The top bar includes the Keycloak logo, a search icon, the realm name 'banco-carrefour Current realm', and a user dropdown for 'admin'. The left sidebar has a dark theme with white text and includes options like 'Manage realms', 'Manage', 'Clients', 'Client scopes', 'Realm roles', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings', and 'Authentication'. The 'Users' option is highlighted with a blue selection bar. The main content area has a light background. It displays the heading 'Users' and a sub-instruction 'Users are the users in the current realm.' followed by a link 'Learn more'. Below this is a 'User list' section with a large grey plus sign icon. A message 'No users found' is centered. At the bottom of this section is a placeholder 'Change your search criteria or add a user'. A prominent blue rectangular button labeled 'Create new user' is located at the bottom right of this section.

Dados:

- Username: usuario-admin
- Email Verified: ON
- Email: email@email.com
- First Name: Usuario
- Last Name: Usuario

Create

Definir senha:

usuario-admin
→ Credentials
→ Set password

- Temporary: OFF

- Password: usuario-admin

Atribuir role:

usuario-admin

- Role mapping
- Assign role
- Realm roles

Selecione:

- admin

 **Assign**

Usuário Report

Caminho:

Users
→ Create new user

Dados:

- Username: usuario-report
- Email Verified: ON
- Email: email-report@email.com
- First Name: Usuario
- Last Name: Usuario

Create

Senha:

Credentials → Set password

- Temporary: OFF
- Password: usuario-report

Role:

Role mapping
→ Assign role
→ Realm roles

Selecione:

- report-api-access

Assign

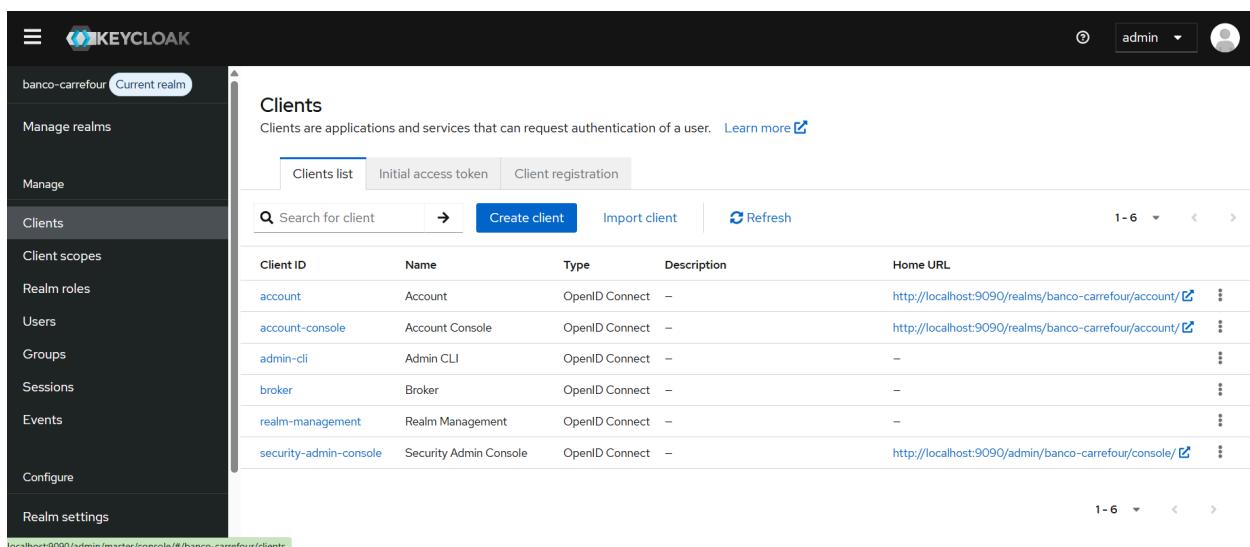
4 Criar Clients (DUAS APIs)

Client 1 — transaction-api

Caminho REAL:

Clients

→ Create client



The screenshot shows the Keycloak admin interface for the 'banco-carrefour' realm. The left sidebar has 'Clients' selected. The main page title is 'Clients' with a subtitle 'Clients are applications and services that can request authentication of a user.' Below this are tabs for 'Clients list', 'Initial access token', and 'Client registration'. A search bar and buttons for 'Create client' and 'Import client' are present. The table lists seven clients:

Client ID	Name	Type	Description	Home URL
account	Account	OpenID Connect	—	http://localhost:9090/realm/banco-carrefour/account/
account-console	Account Console	OpenID Connect	—	http://localhost:9090/realm/banco-carrefour/account-console/
admin-cli	Admin CLI	OpenID Connect	—	—
broker	Broker	OpenID Connect	—	—
realm-management	Realm Management	OpenID Connect	—	—
security-admin-console	Security Admin Console	OpenID Connect	—	http://localhost:9090/admin/banco-carrefour/console/

Step 1 – General settings

- Client type: **OpenID Connect**
- Client ID: **transaction-api**

Next

Step 2 – Capability config

The screenshot shows the 'Capability config' page for a client application. On the left, there's a navigation bar with 'General settings' (step 1) and 'Capability config' (step 2, highlighted in blue). The main area contains the following configuration:

- Client authentication:** A toggle switch is set to **On**.
- Authorization:** A toggle switch is set to **Off**.
- Authentication flow:** A list of options with checkboxes:
 - Standard flow (disabled)
 - Direct access grants (selected)
 - Implicit flow (disabled)
 - Service account roles (disabled)
 - Standard Token Exchange (disabled)
 - OAuth 2.0 Device Authorization Grant (disabled)
 - OIDC CIBA Grant (disabled)
- PKCE Method:** A dropdown menu showing 'Choose...'.
- Require DPoP bound tokens:** A toggle switch is set to **Off**.

Save

Step 3 – Credentials

Caminho:

Clients → transaction-api → Credentials

Copie o Client Secret

Clients > Client details

transaction-api OpenID Connect

Clients are applications and services that can request authentication of a user.

Enabled ? Action ▾

Settings

Keys

Credentials

Roles

Client scopes

Sessions

Advanced

Events

Client Authenticator	Client Id and Secret
<small>?</small>	
<input type="button" value="Save"/>	
Client Secret	jyxYoowtOjqnKz3nWNQ7NBMdghJejepq
<small>?</small> <input type="button" value="Regenerate"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>	
<small>...</small> <input type="button" value="Add"/>	

Client 2 — report-api

Repita EXATAMENTE os mesmos passos:

Clients → Create client

- Client ID: report-api
- Client authentication: ON
- Direct access grants: ON

Copie o Client Secret

5 Criar Client Scope para Audience

Criar Client Scope

Caminho REAL:

Client scopes

→ Create client scope

The screenshot shows the Keycloak administration interface for managing client scopes. The left sidebar is dark-themed and includes options like 'Manage realms', 'Clients', 'Client scopes' (which is selected and highlighted in blue), 'Realm roles', 'Users', 'Groups', 'Sessions', 'Events', 'Configure', 'Realm settings', and 'Authentication'. The main content area has a light background and displays a table titled 'Client scopes'. The table has columns for 'Name', 'Assigned type', 'Protocol', 'Display order', and 'Description'. It lists several built-in scopes: 'acr', 'address', 'basic', 'email', 'micropattern-jwt', 'offline_access', and 'organization'. Each row includes a small icon, a dropdown menu, and a three-dot ellipsis button. At the top of the table, there are filters ('Name', 'Search for client scope'), a 'Create client scope' button, and other navigation controls.

Preencha:

- Name: aud-banco-carrefour-apis
- Type: Default
- Protocol: openid-connect
- Incluiude in token scope: ON

Save

Criar Audience Mappers

Caminho:

Client scopes

→ aud-banco-carrefour-apis
→ Mappers
→ Configure a new mapper
→ Audience

Mapper 1

Campo	Valor
Name	aud-transaction-api
Mapper Type	Audience
Included Client Audience	transaction-api
Add to access token	
Add to ID token	

Save

Mapper 2 (no MESMO client scope)

- Add mapper
- By configuration
- Audience

Campo	Valor
Name	aud-report-api
Mapper Type	Audience
Included Client Audience	report-api
Add to access token	

Save

6 Associar Client Scope aos DOIS Clients

transaction-api

Caminho:

Clients

- transaction-api
- Client scopes
- Add client scope

- Client scope: aud-banco-carrefour-apis
- Type: **Default**

Add

report-api

Mesmo caminho:

Clients

- report-api
- Client scopes
- Add client scope

- Client scope: aud-banco-carrefour-apis
- Type: **Default**

Add

7 Resultado esperado no TOKEN

Qualquer token emitido por **QUALQUER client** terá:

```
"aud": [  
    "transaction-api",  
    "report-api",  
    "account"  
,
```

```
"realm_access": {
  "roles": [
    "admin" OU "report-api-acesss"
  ]
}
```

8 Obter Token

transaction-api

```
POST
http://localhost:8080/realmns/banco-carrefour/protocol/openid-connect/token
Content-Type: application/x-www-form-urlencoded

grant_type=password
&client_id=transaction-api
&client_secret=SECRET_TRANSACTION
&username=usuario-admin
&password=usuario-admin
```

report-api

```
POST
http://localhost:8080/realmns/banco-carrefour/protocol/openid-connect/token
Content-Type: application/x-www-form-urlencoded

grant_type=password
&client_id=report-api
&client_secret=SECRET_REPORT
&username=usuario-report
&password=usuario-report
```

9 Erro “Account is not fully set up”

Verifique se não existe nenhum item pendente, como validar email, nome/sobrenome não preenchido etc. Em último caso, redefina a senha novamente (e não esqueça de desligar como temporária)