Sumário

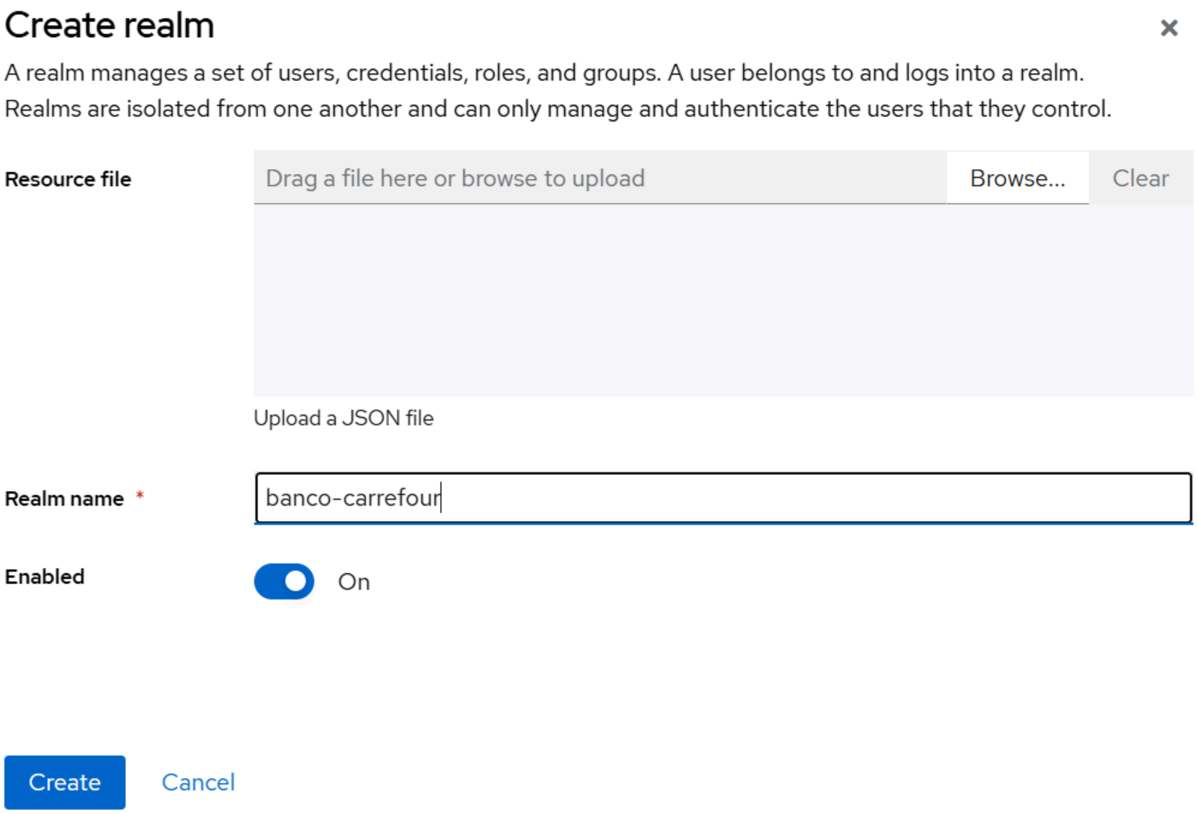
1 Criar Realm

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: Drag a file here or browse to upload

Upload a JSON file

Realm name *: banco-carrefour

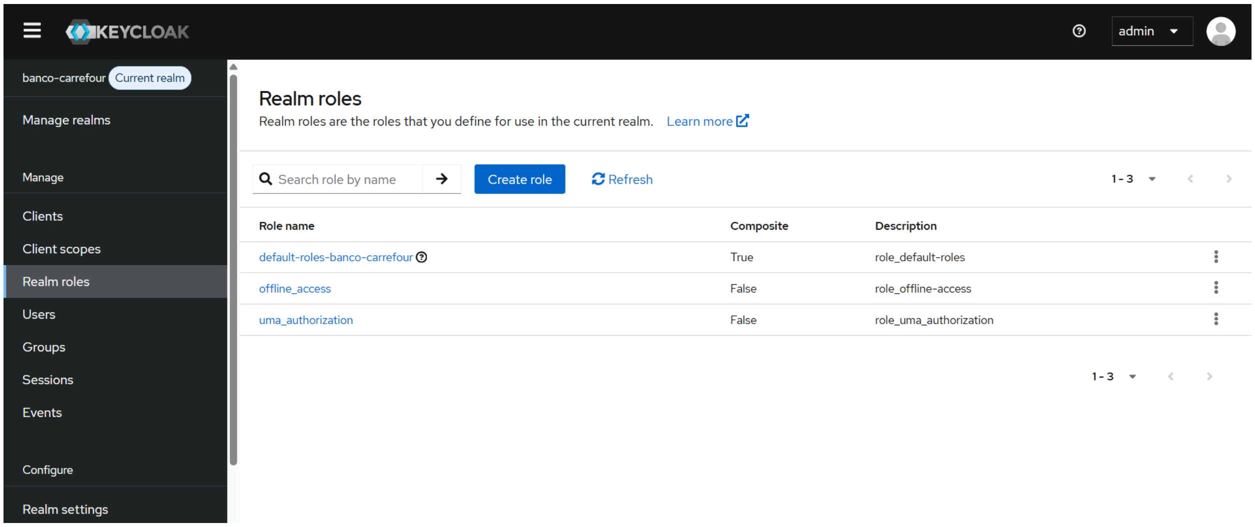
Enabled: On

Create

2 Criar Roles (Realm Roles)

Menu lateral:

```
Realm: banco-carrefour
→ Realm roles
→ Create role
```



Realm roles

Realm roles are the roles that you define for use in the current realm. Learn more

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

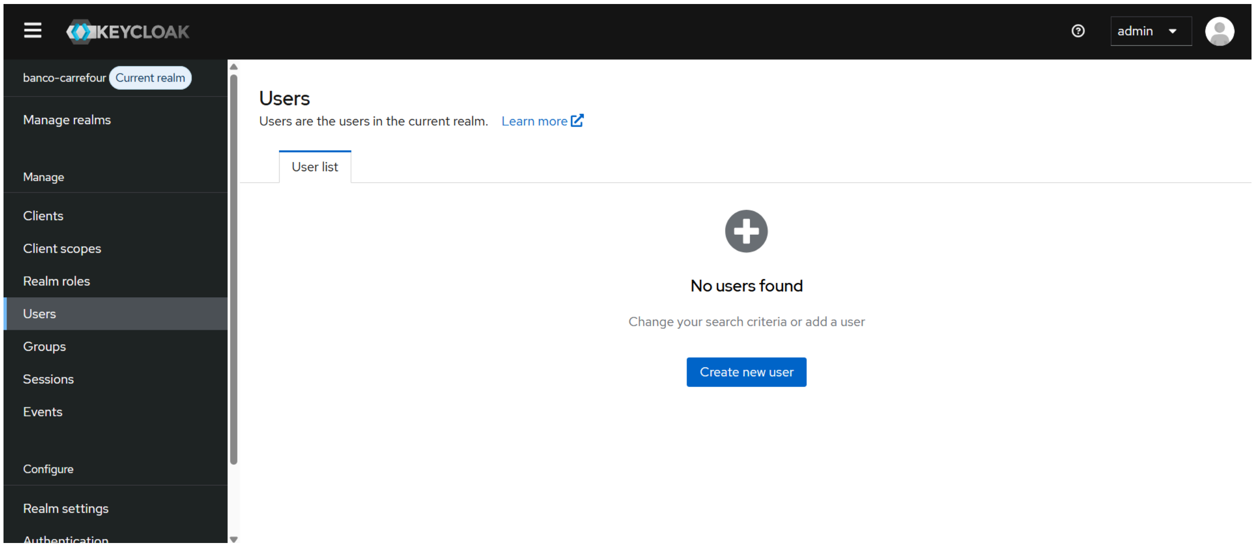
✔ Essas roles serão usadas **pelas DUAS APIs**

3 Criar Usuários

Usuário Admin

Caminho:

```
Users
→ Create new user
```



Users

Users are the users in the current realm.

No users found

Change your search criteria or add a user

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

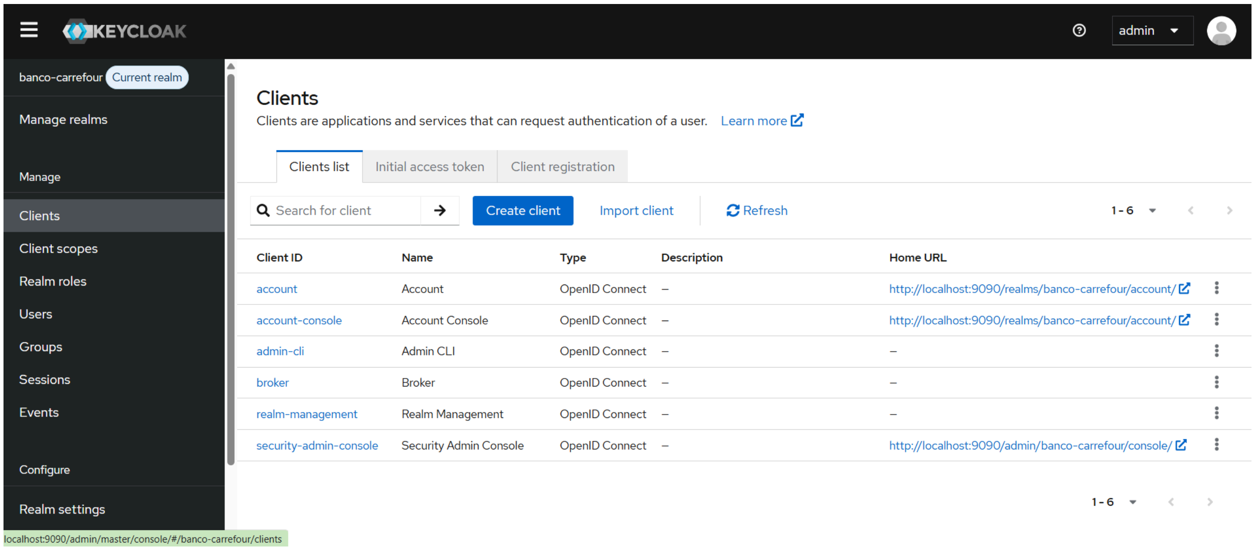
Assign

4 Criar Clients (DUAS APIs)

Client 1 — transaction-api

Caminho REAL:

```
Clients
→ Create client
```



Clients

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

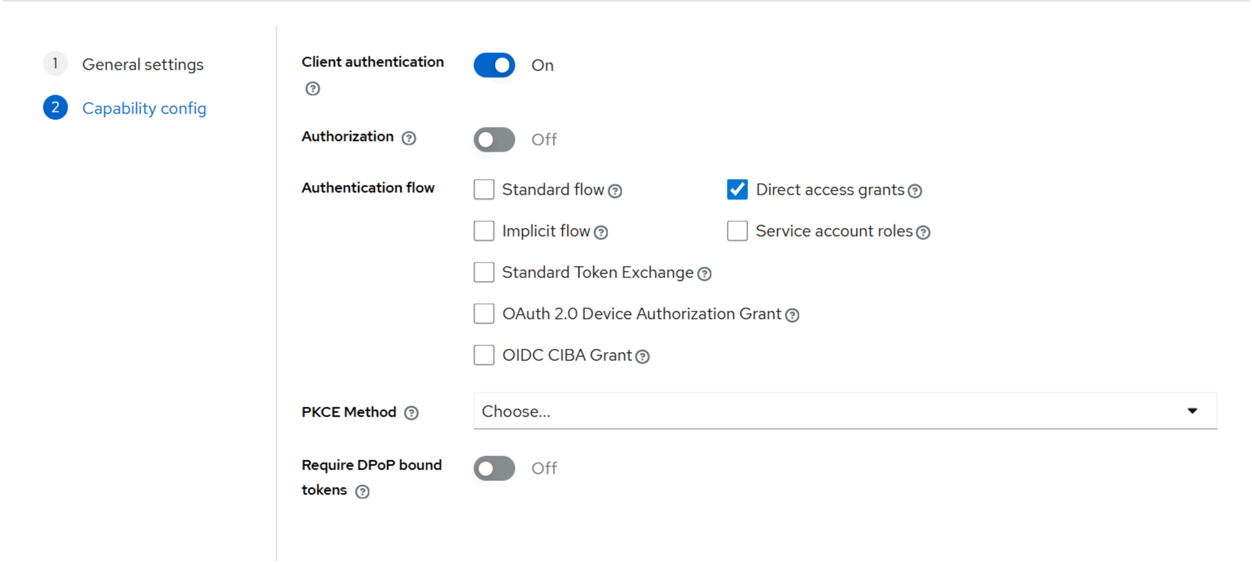
Client ID	Name	Type	Description	Home URL
account	Account	OpenID Connect	–	http://localhost:9090/realms/banco-carrefour/account/
account-console	Account Console	OpenID Connect	–	http://localhost:9090/realms/banco-carrefour/account/
admin-cli	Admin CLI	OpenID Connect	–	–
broker	Broker	OpenID Connect	–	–
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



1 General settings

2 Capability config

Client authentication: On

Authorization: Off

Authentication flow:

- □ Standard flow
- ☑ Direct access grants
- □ Implicit flow
- □ Service account roles
- □ Standard Token Exchange
- □ OAuth 2.0 Device Authorization Grant
- □ OIDC CIBA Grant

PKCE Method: Choose...

Require DPoP bound tokens: Off

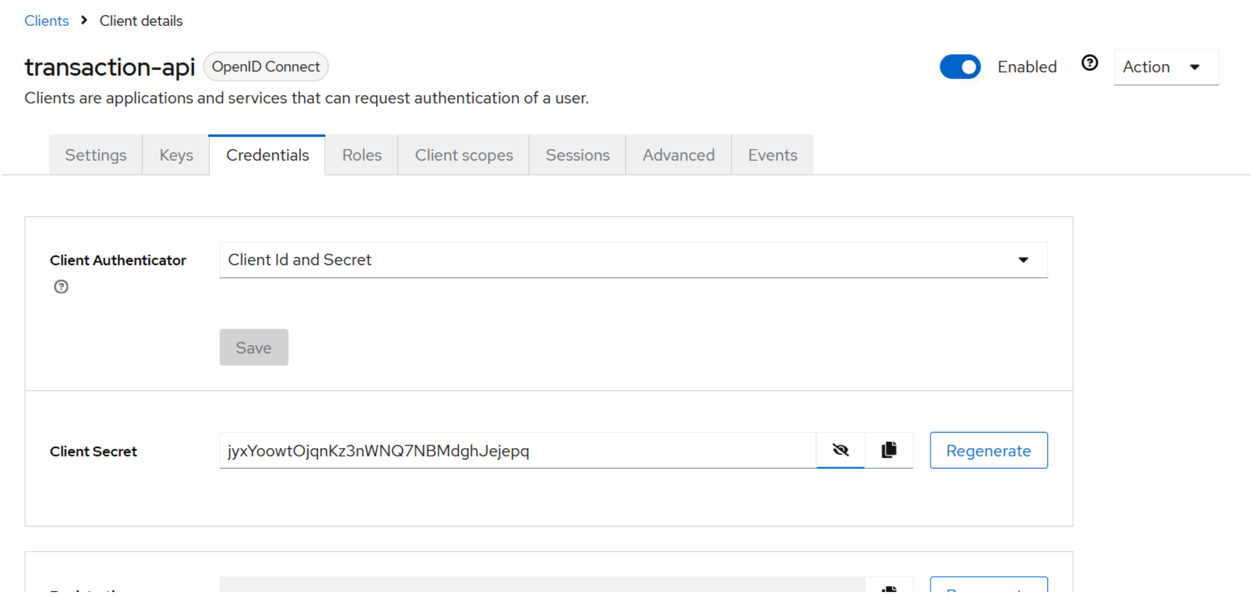
Save

Step 3 – Credentials

Caminho:

`Clients → transaction-api → Credentials`

Copie o Client Secret



transaction-api OpenID Connect

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

Client Authenticator: Client Id and Secret

Client Secret: jyxYoowtOjqnKz3nWNQ7NBMdghJejepq

Client 2 — report-api

Repita EXATAMENTE os mesmos passos:

```
Clients → Create client
```

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

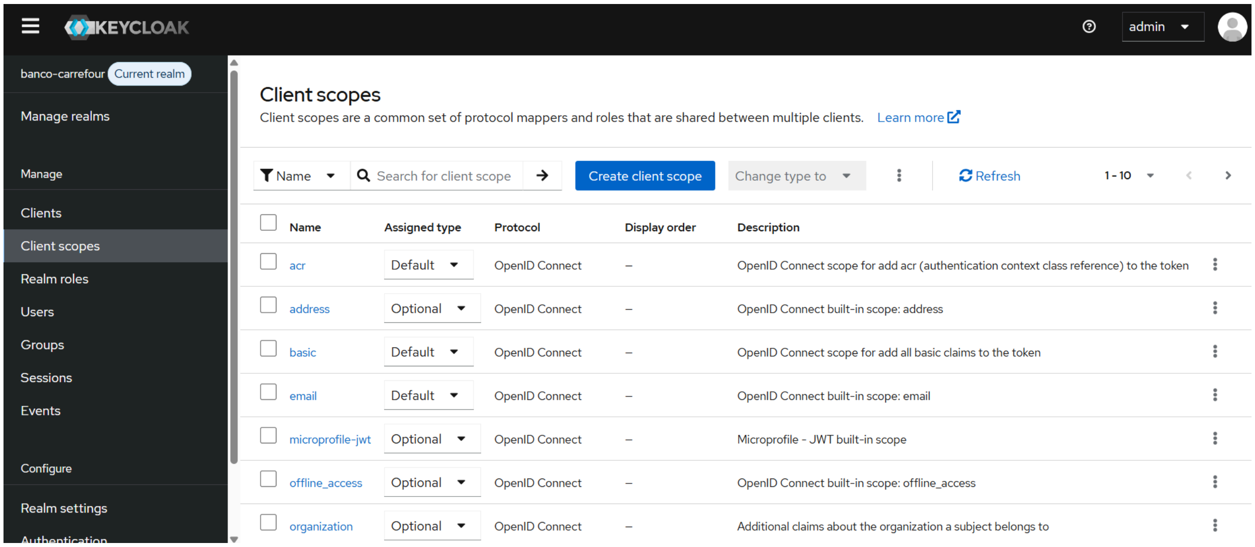
Copie o Client Secret

5 Criar Client Scope para Audience

Criar Client Scope

Caminho REAL:

```
Client scopes
→ Create client scope
```



Client scopes

Client scopes are a common set of protocol mappers and roles that are shared between multiple clients. Learn more

☐	Name	Assigned type	Protocol	Display order	Description
☐	acr	Default	OpenID Connect	–	OpenID Connect scope for add acr (authentication context class reference) to the token
☐	address	Optional	OpenID Connect	–	OpenID Connect built-in scope: address
☐	basic	Default	OpenID Connect	–	OpenID Connect scope for add all basic claims to the token
☐	email	Default	OpenID Connect	–	OpenID Connect built-in scope: email
☐	microprofile-jwt	Optional	OpenID Connect	–	Microprofile - JWT built-in scope
☐	offline_access	Optional	OpenID Connect	–	OpenID Connect built-in scope: offline_access
☐	organization	Optional	OpenID Connect	–	Additional claims about the organization a subject belongs to

Preencha:

- Name: `aud-banco-carrefour-apis`
- Type: Default
- Protocol: `openid-connect`
- `Incluide 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/realms/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/realms/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)