

SSO OAuth2

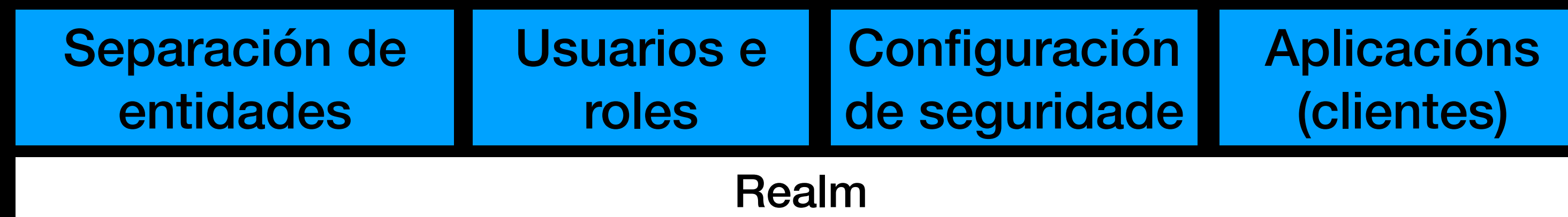
Empregando Keycloak

Contextos de autenticación (Realms)

Concepto de “Realm”

Relativo ó software Keycloak

- Partición illada que contén usuarios, aplicacións, configuracións de seguridade e políticas de acceso.
- Actúa como un espazo illado onde podes configurar a autenticación, autorización e outros aspectos de seguridade de maneira independente.



localhost

Keycloak Administration UI

localhost:8080/realms/master/.well-known/openid-configuration

KEYCLOAK

admin

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

master

Enabled

Action

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General Login Email Themes Keys Events Localization Security defenses Sessi

Realm ID * master

Display name Keycloak

HTML Display name <div class="kc-logo-text">Keycloak</div>

Frontend URL

Require SSL External requests

ACR to LoA Mapping

No attributes have been defined yet. Click the below button to add attributes, key and value are required for a key pair.

+ Add an attribute

Endpoints

[OpenID Endpoint Configuration](#)

[SAML 2.0 Identity Provider Metadata](#)

Save Revert

Clientes

Definición de cliente

- Aplicación ou servizo que solicita acceso a recursos protexidos en nome dun usuario.
- Pode ser calquera cousa:
 - Unha aplicación de teléfono móbil,
 - Unha aplicación web,
 - Un cliente de liña de comandos,
 - ...
- O cliente non só solicita o acceso a recursos, senón que tamén obtén un "token de acceso" co cal pode acceder aos recursos protexidos sen necesidade de solicitar as credenciais do usuario en cada solicitude.

Listado de clientes en Keycloak

The screenshot shows the Keycloak administration interface. The left sidebar contains a navigation menu with the following items: Manage, Clients, Client scopes, Realm roles, Users, Groups, Sessions, Events, Configure, Realm settings, Authentication, Identity providers, and User federation. The 'Clients' menu item is highlighted, and a yellow arrow points to it with the text '1. Menú de clientes'. The main content area shows the 'Clients' page with a sub-header 'Clients' and a description: 'Clients are applications and services that can request authentication of a user. Learn more'. Below this are tabs for 'Initial access token' and 'Client registration'. A search bar labeled 'Search for client' is followed by a 'Create client' button, which is highlighted with a yellow arrow and the text '2. Crear novo cliente'. Below the button is a table of clients.

Client ID	Name	Type	Description	Home URL
account	<code>#{client_account}</code>	OpenID Connect	–	http://localhost:8080/realms/master/account/
account-console	<code>#{client_account...}</code>	OpenID Connect	–	http://localhost:8080/realms/master/account/
admin-cli	<code>#{client_admin-...}</code>	OpenID Connect	–	–
broker	<code>#{client_broker}</code>	OpenID Connect	–	–
master-realm	master Realm	OpenID Connect	–	–
security-admin-console	<code>#{client_security...}</code>	OpenID Connect	–	http://localhost:8080/admin/master/console/

Definición dun novo cliente

localhost

KEYCLOAK

admin

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Clients > Create client

Create client

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

- 1 General Settings
- 2 Capability config
- 3 Login settings

Client type [?] OpenID Connect

Client ID * [?] prueba123

Name [?] Aplicación de Prueba

Description [?] Prueba de concepto

Always display in UI [?] Off

Next Back Cancel

Indicar datos identificativos

Obtención de credenciales de cliente

The image shows a browser window displaying the Keycloak Administration UI. The page title is "Keycloak Administration UI" and the URL is "localhost". The user is logged in as "admin". The left sidebar shows the navigation menu with "Clients" selected. The main content area shows the "Client details" for "prueba123" (OpenID Connect). The "Credentials" tab is active, showing the "Client Authenticator" set to "Client Id and Secret". Below this, there is a "Client secret" field with a masked value and a "Save" button. A yellow arrow points to the "Client secret" field with the text "Chave segreda". At the bottom, there is a "Registration access token" field with a "Regenerate" button.

Keycloak Administration UI

admin

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Clients > Client details

prueba123 OpenID Connect

Enabled Action

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

Settings Keys Credentials Roles Client scopes Authorization Service accounts roles

Client Authenticator Client Id and Secret

Save

Client secret

Chave segreda

Registration access token Regenerate

Ajustes do cliente

Clients > Create client

Create client

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

- 1 General Settings
- 2 **Capability config**
- 3 Login settings


Client authentication On

Authorization On

Authentication flow

- Standard flow
- Direct access grants
- Implicit flow
- Service accounts roles
- OAuth 2.0 Device Authorization Grant
- OIDC CIBA Grant

[Next](#) [Back](#) [Cancel](#)



Clients > Create client

Create client

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

- 1 General Settings
- 2 Capability config
- 3 **Login settings**


Root URL

Home URL

Valid redirect URIs [+ Add valid redirect URIs](#)

Valid post logout redirect URIs [+ Add valid post logout redirect URIs](#)

Web origins [+ Add web origins](#)



Usuarios

Creación de novos usuários

Keycloak Administration UI

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Users

Users are the users in the current realm. [Learn more](#)

User list

Default search Search

Engadir usuarios Add user Delete user

<input type="checkbox"/>	Username	Email	Last name	First name	Status
<input type="checkbox"/>	admin	!	-	-	-

Users > Create user

Create user

Required user actions

Username *

Email

Email verified Yes

First name

Last name

Groups

Credenciais de usuario

Keycloak Administration UI

master

Manage

Clients

Client scopes

Realm roles

Users

Groups

Sessions

Events

Configure

Realm settings

Authentication

Identity providers

User federation

Users

Users are the users in the current realm. [Learn more](#)

User list

Default search Search user Add user

Username	Email	Last name
admin	!	-

1. Seleccionar usuario da lista

Keycloak Administration UI

admin

Users > User details

johndoe

Enabled Action

Details Attributes Credentials Role mapping Groups Consents Identity provider links Sessions

No credentials

This user does not have any credentials. You can set password for this user.

2. Definir contrasinal (provisional)

Set password

Credential Reset

f49-b448edde0079/credentials de esta página en una pestaña nueva

Aplicación de ejemplo

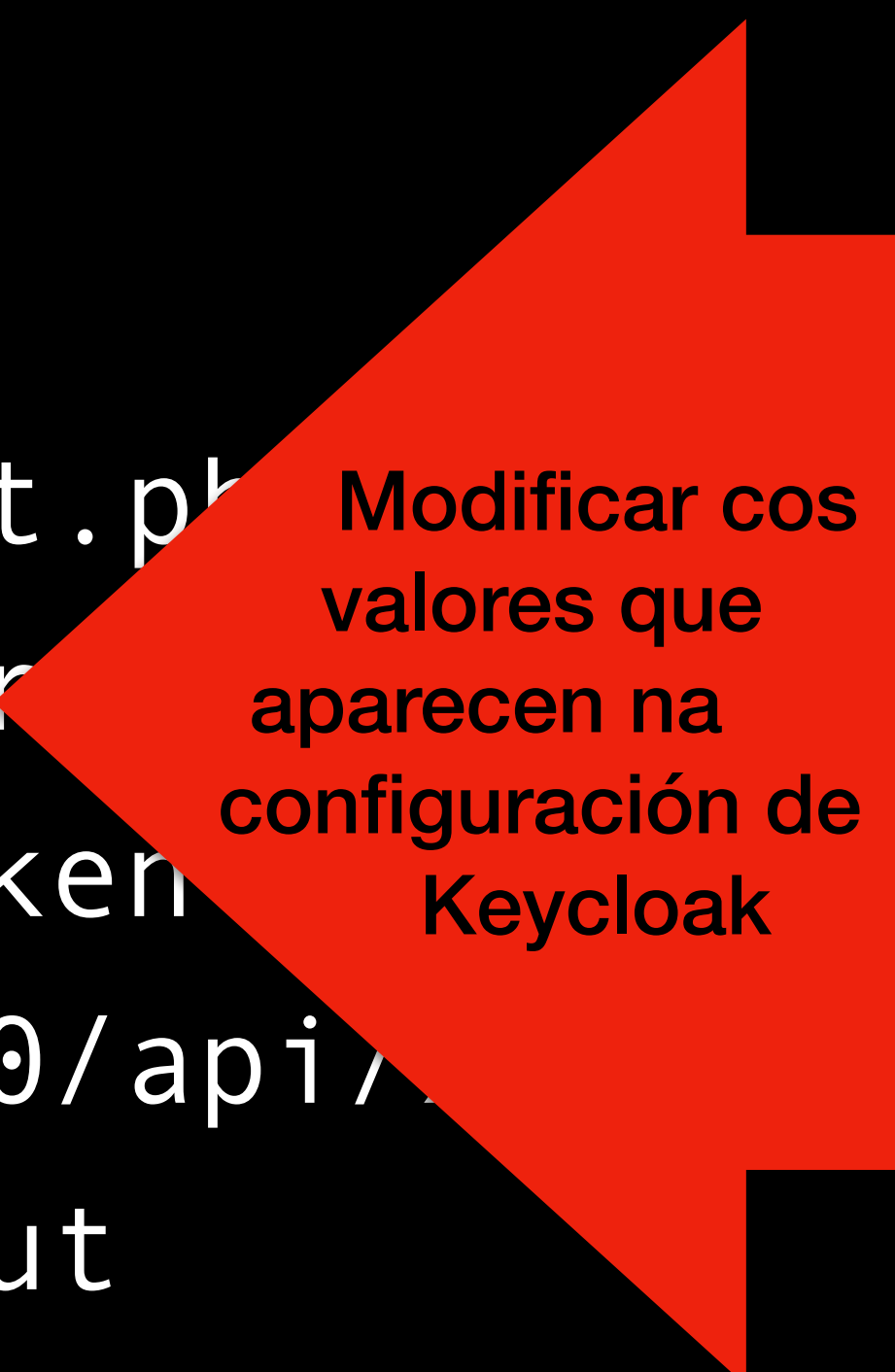
Código da aplicación

<https://github.com/jairochapela/oauth2-client-php-example>

Configuración

1. Copiar ficheiro: .env.example a .env
2. Editar ficheiro .env modificando as variables

```
CLIENT_ID=prueba123
CLIENT_SECRET=xxxxxxxxxxxxxxxxxxxxxxxxxxxx
REDIRECT_URI=http://localhost:8000/callback.php
LOGOUT_REDIRECT_URI=http://localhost:8000/logout.php
URL_AUTHORIZE=http://localhost:8080/oauth/authorize
URL_ACCESS_TOKEN=http://localhost:8080/oauth/token
URL_RESOURCE_OWNER_DETAILS=http://localhost:8080/api/v1/
URL_SSO_LOGOUT=http://localhost:8080/oauth/logout
```



Modificar cos valores que aparecen na configuración de Keycloak