

Configuración de seguridad en Keycloak

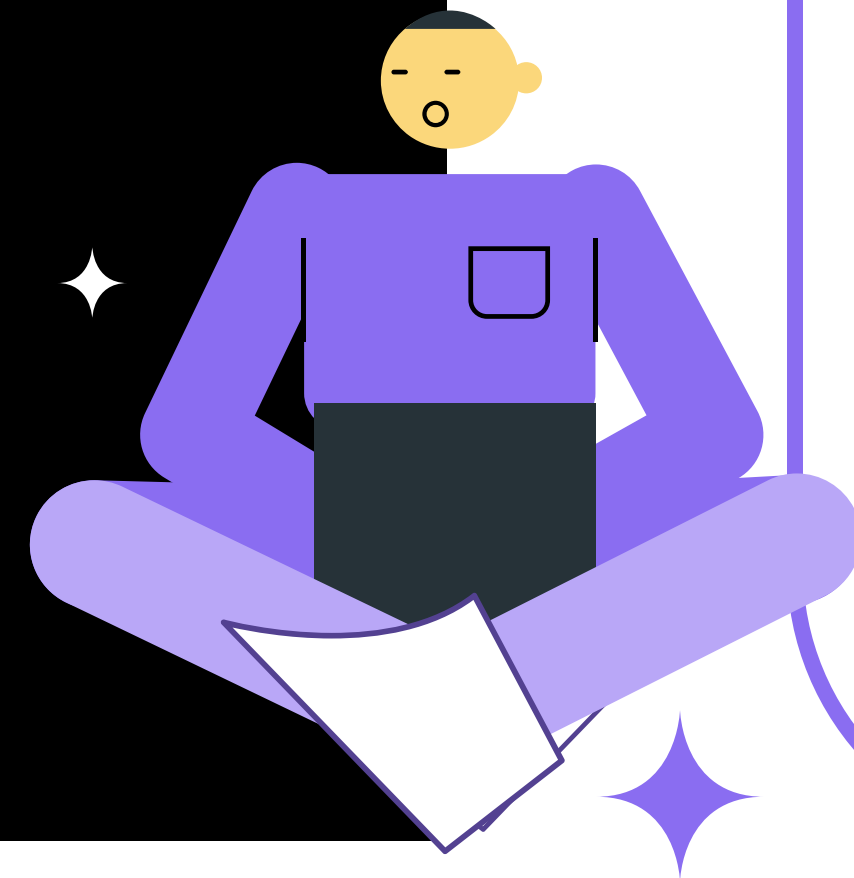
Índice

- 01 [Realm](#)
- 02 [Client](#)
- 03 [User](#)



En esta instancia tenemos
que configurar los siguientes
ítems inicialmente:

- Realm
- Client
- User



01

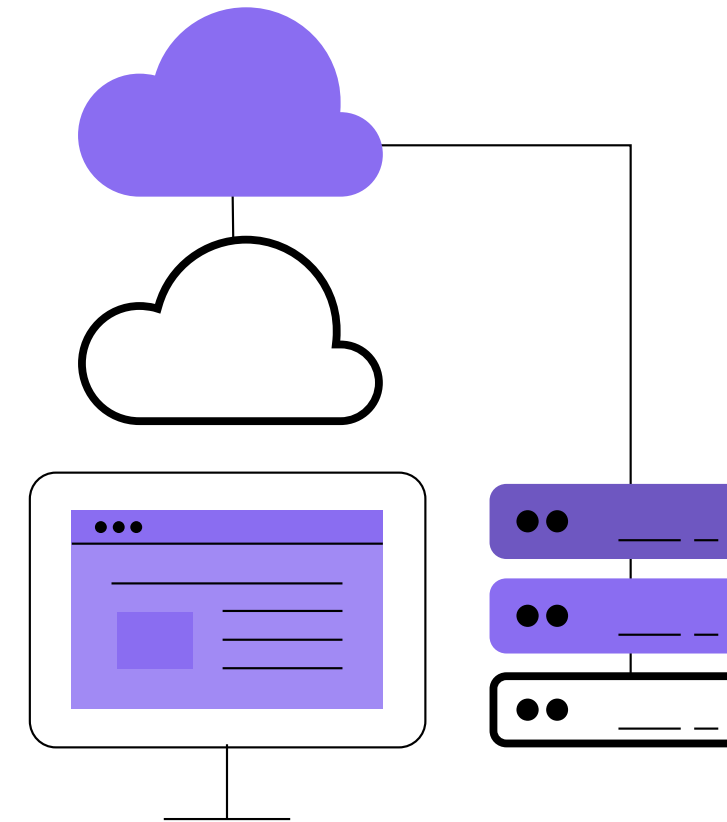
Realm



Realm (reino)

Es el dominio de configuración principal para configurar usuarios, credenciales, roles y grupos.

Está totalmente aislado de otros reinos y solo maneja lo que se haya definido en su dominio. Existirá, por ejemplo, uno por cada aplicación interna para empleados y otro para aplicaciones externas para clientes.





Crear un realm

Para crear un **realm** debemos entrar a nuestra URL root de Keycloak y seleccionar la opción de creación desde el menú izquierdo.

Select realm ▼

- Master
- Spring-cloud-gateway-realm
- Spring-cloud-ouath-provider

Add realm

Add realm

Add realm

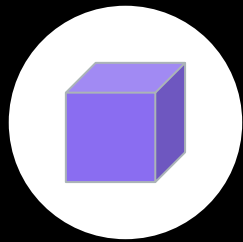
Import

Name *

Enabled ☒ ON

02

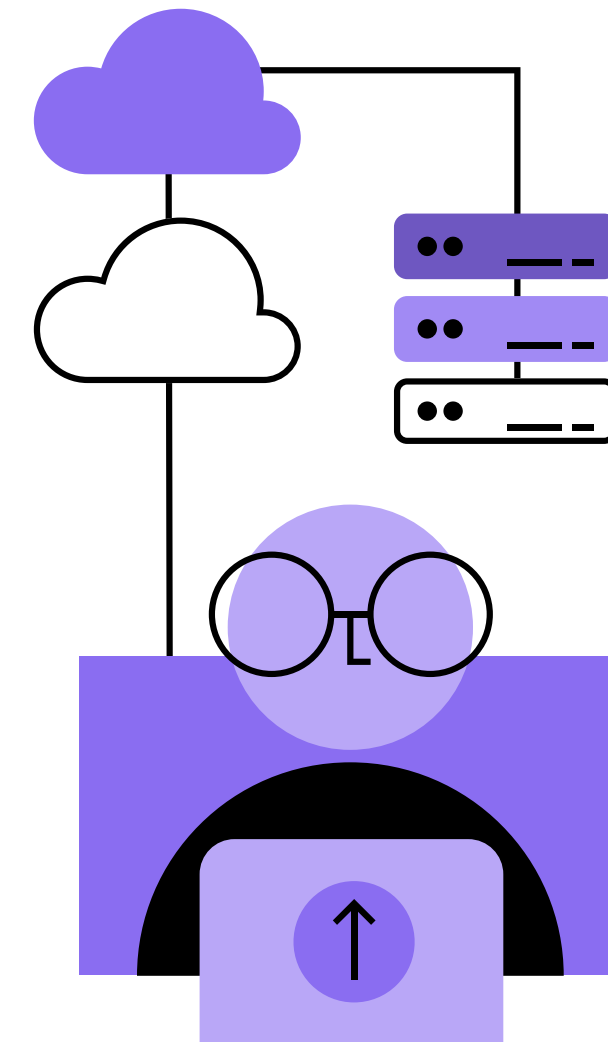
Client

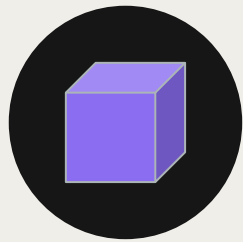


Client

Son las **entidades** que pueden solicitar a Keycloak la autenticación de un usuario. Generalmente, son **aplicaciones y/o servicios que necesitan autenticar** vía single sign-on.

También pueden ser entidades que requieren **información del usuario** autenticado previamente, o un token relacionado con ellos, para poder invocar a otros servicios de la solución que también usen Keycloak.





Crear un client

Para crear un cliente, dentro del apartado “**Clients**”, seleccionamos la opción “**Create**” y en “**Root URL**” debemos especificar la URL root de nuestra aplicación o servicio.

KEYCLOAK

Fintech-external-realm

Configure

- Realm Settings
- Clients**
- Client Scopes
- Roles
- Identity Providers
- User Federation
- Authentication

Clients > Add Client

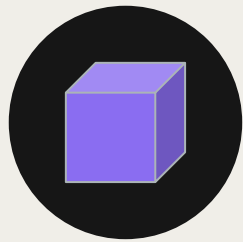
Add Client

Import

Client ID

Client Protocol

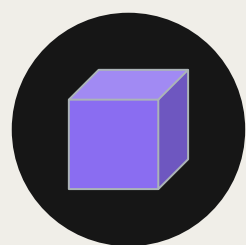
Root URL



Luego, debemos hacer que nuestro cliente sea de acceso confidencial para que cada API o servicio que lo requiera deba tener un identificador y una contraseña como **secret** para poder acceder a estos servicios de Keycloak.

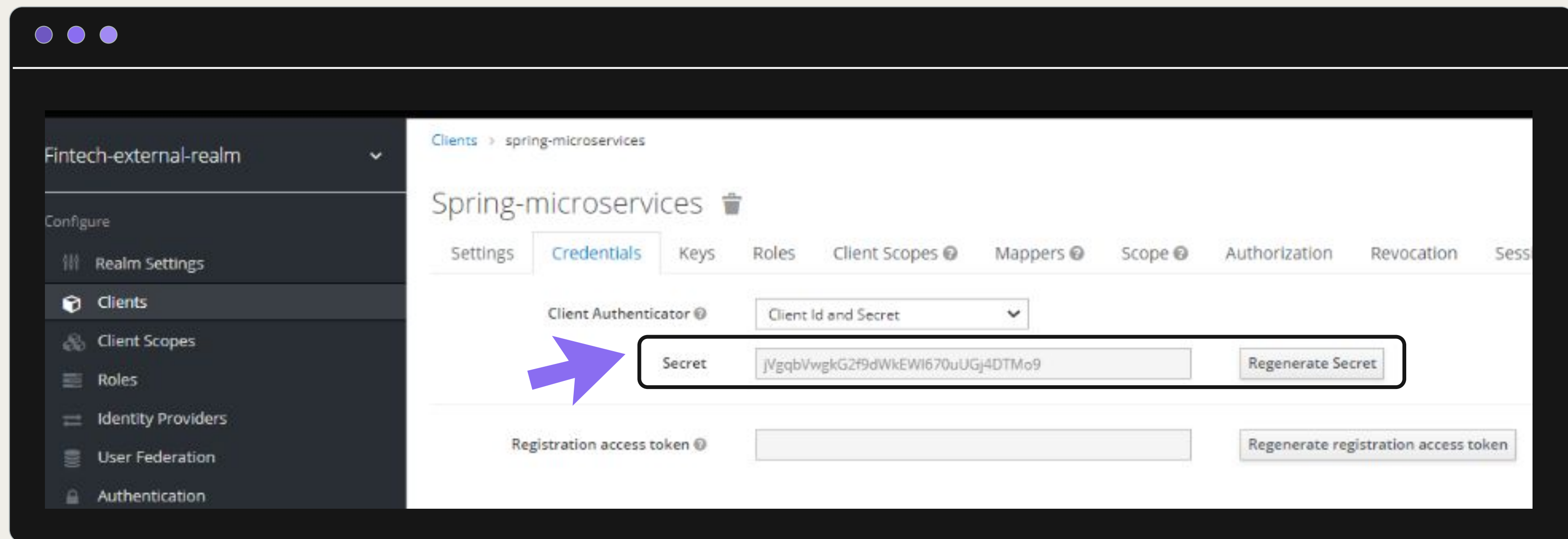
Con esta opción habilitada, también tendremos que activar la opción “**Authorization Enabled**”.

The screenshot shows the Keycloak Admin Console interface for the 'Fintech-external-realm'. The left sidebar contains navigation options under 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions, Events, Import, Export). The main panel displays the configuration for the 'Spring-microservices' client. The 'Settings' tab is active, showing fields for Client ID (spring-microservices), Name, Description, Enabled (ON), Always Display in Console (OFF), Consent Required (OFF), Login Theme, Client Protocol (openid-connect), Access Type (confidential), Standard Flow Enabled (ON), Implicit Flow Enabled (OFF), Direct Access Grants Enabled (ON), Service Accounts Enabled (ON), OAuth 2.0 Device Authorization Grant Enabled (ON), and OIDC CIBA Grant Enabled (OFF). The 'Access Type' dropdown is highlighted with a blue arrow, and the 'Authorization Enabled' toggle is also highlighted with a blue arrow.



Luego de seleccionar la opción “**Save**”, en la **solapa de credenciales** podremos visualizar el secret a utilizar para conectarnos como clientes de Keycloak desde nuestro microservicio que desea autenticar a un usuario.

En este caso: **jVgqbVwgkG2f9dWkEWI670uUGj4DTMo9**.



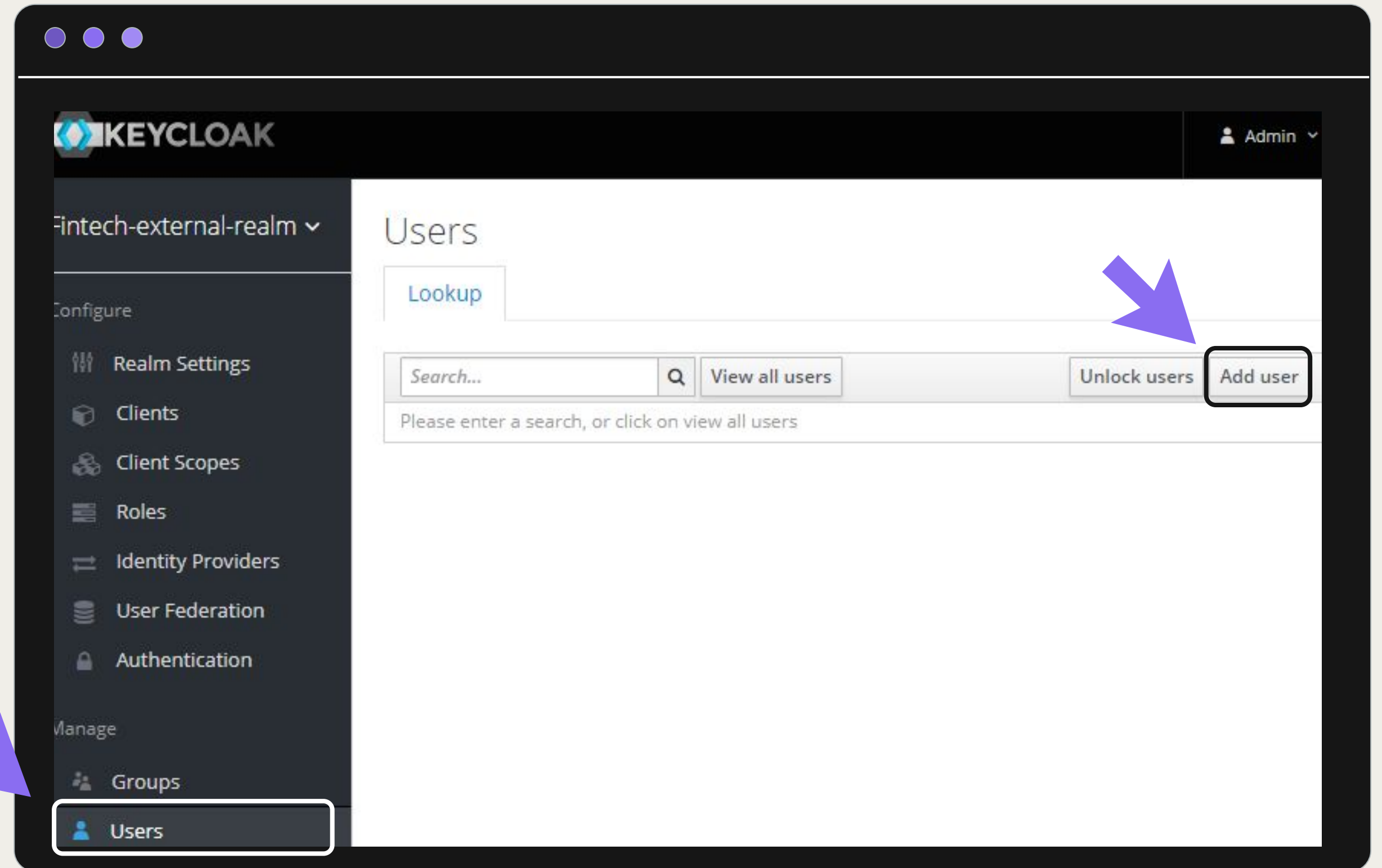
03

User



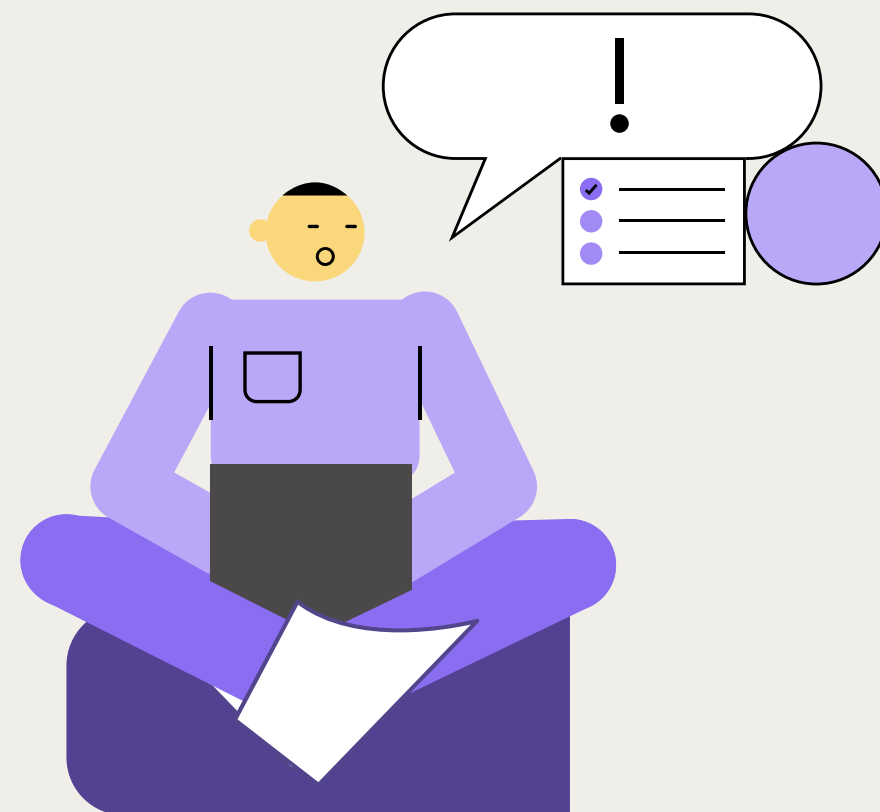
Crear un User

Por último, creamos un usuario para poder autenticar. Para esto, desde el apartado **“Manage > Users”**, seleccionamos el botón **“Add user”**.





Completamos los datos de usuario y lo dejamos en esta instancia sin grupo.



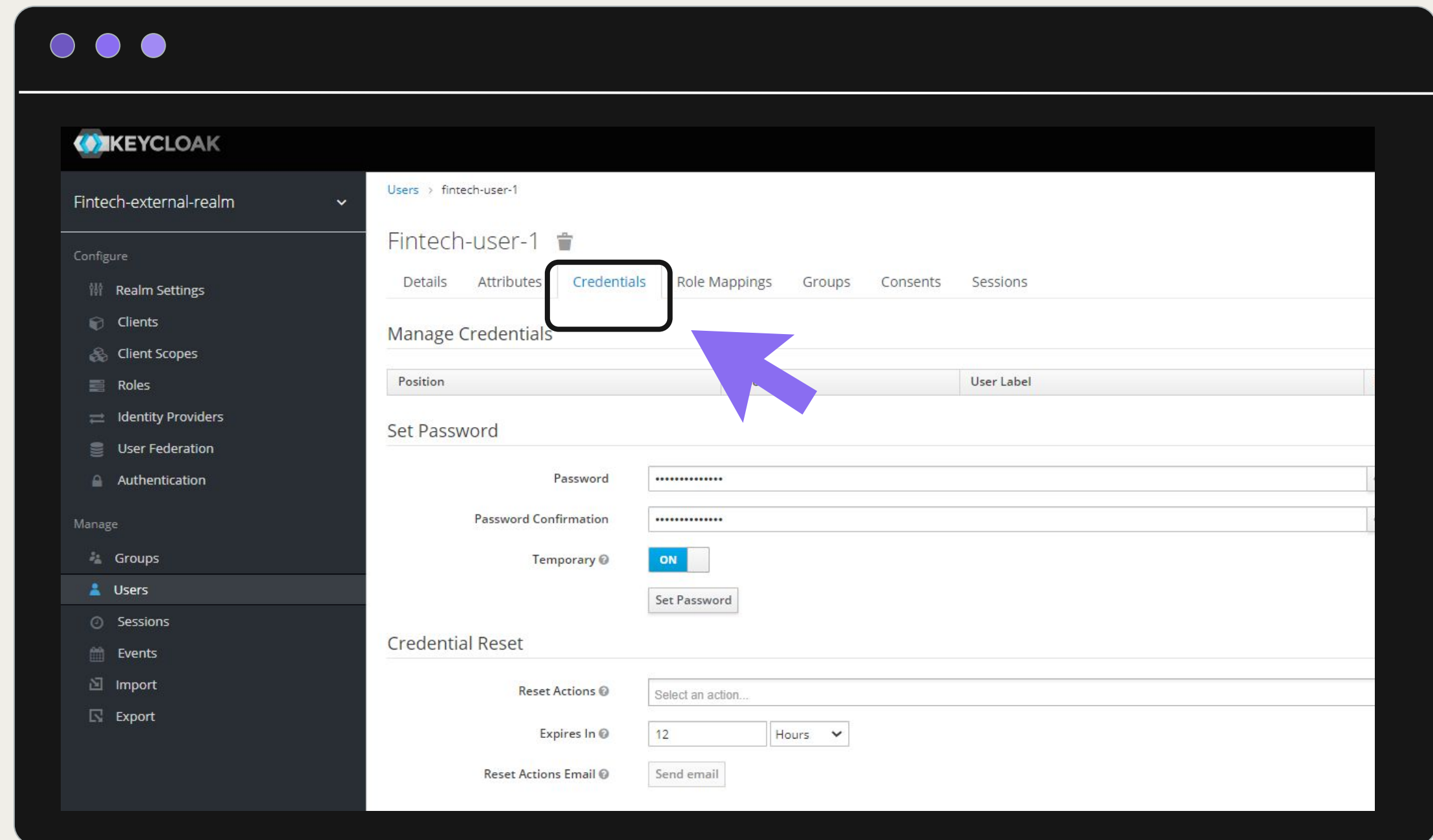
The image shows a screenshot of the Keycloak Admin Console interface. The top navigation bar includes the Keycloak logo and the text "Fintech-external-realm". The left sidebar contains a "Configure" section with links to Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, and Authentication, and a "Manage" section with links to Groups, Users, Sessions, Events, Import, and Export. The "Users" link is highlighted. The main content area is titled "Add user" and contains the following fields and controls:

- ID**: A text input field.
- Created At**: A text input field.
- Username ***: A text input field containing "fintech-user-1".
- Email**: A text input field containing "fintech-user-1@dh-fintech.com.ar".
- First Name**: A text input field containing "fintech".
- Last Name**: A text input field containing "user".
- User Enabled ?**: A toggle switch set to "ON".
- Email Verified ?**: A toggle switch set to "OFF".
- Groups ?**: A dropdown menu with the text "Select existing group..." and "No group selected".
- Required User Actions ?**: A text input field.
- Buttons**: "Save" and "Cancel" buttons at the bottom.



Luego de guardarlo, vamos a la solapa “**Credentials**” para asignarle un password.

Si queremos revisar nuestra configuración en formato JSON, podemos ingresar a la siguiente URL:



<http://localhost:9091/realms/fintech-external-realm/well-known/openid-configuration>

¡Muchas gracias!