DIGITALHOUSE

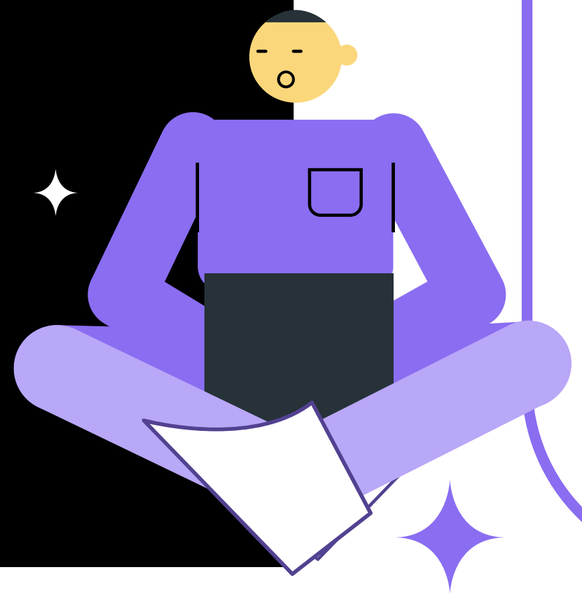
Configuración de seguridad en Keycloack

Certified Tech Developer
The Ultimate Degree

Índice

En esta instancia tenemos que configurar los siguientes ítems inicialmente:

- Realm
- Client
- User

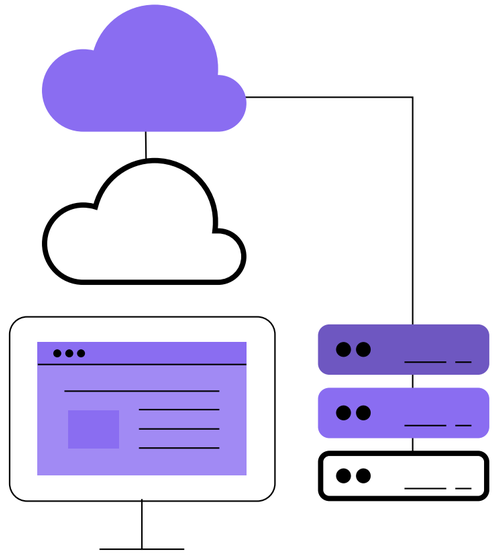


01 Realm

Realm (reino)

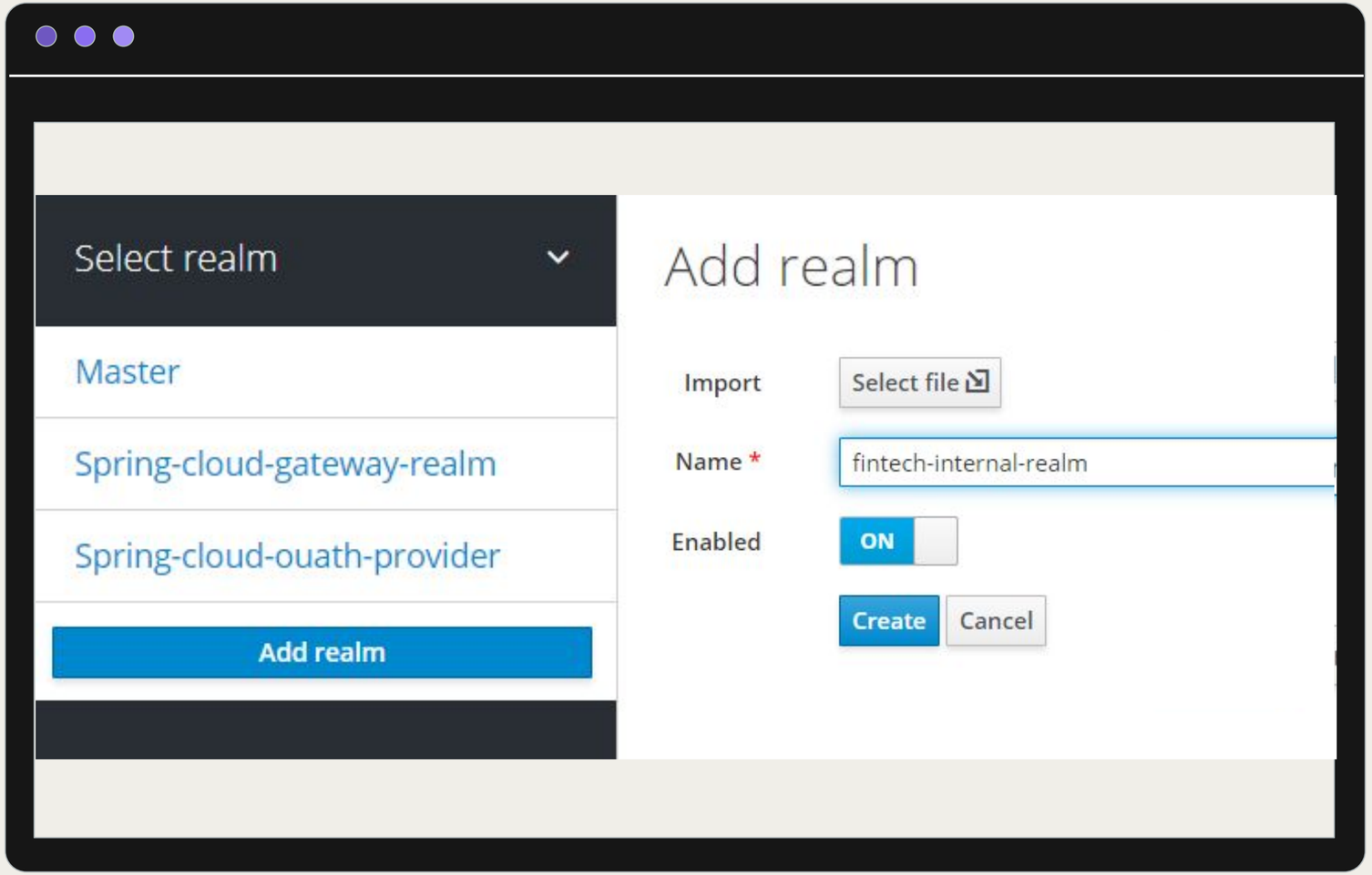
Es el dominio de configuración principal para configurar usuarios, credenciales, roles y grupos.

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.

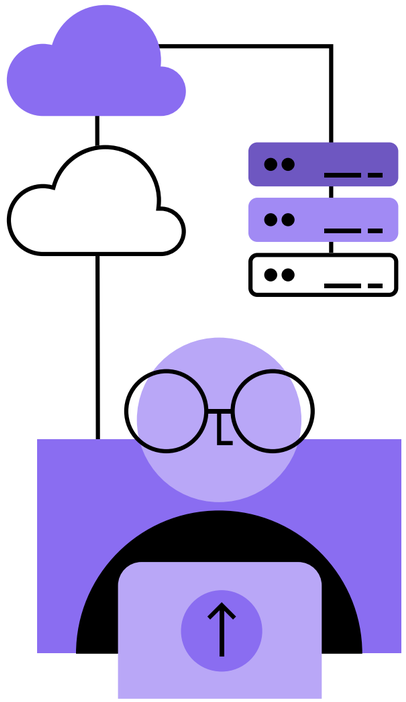


02 Client

Client

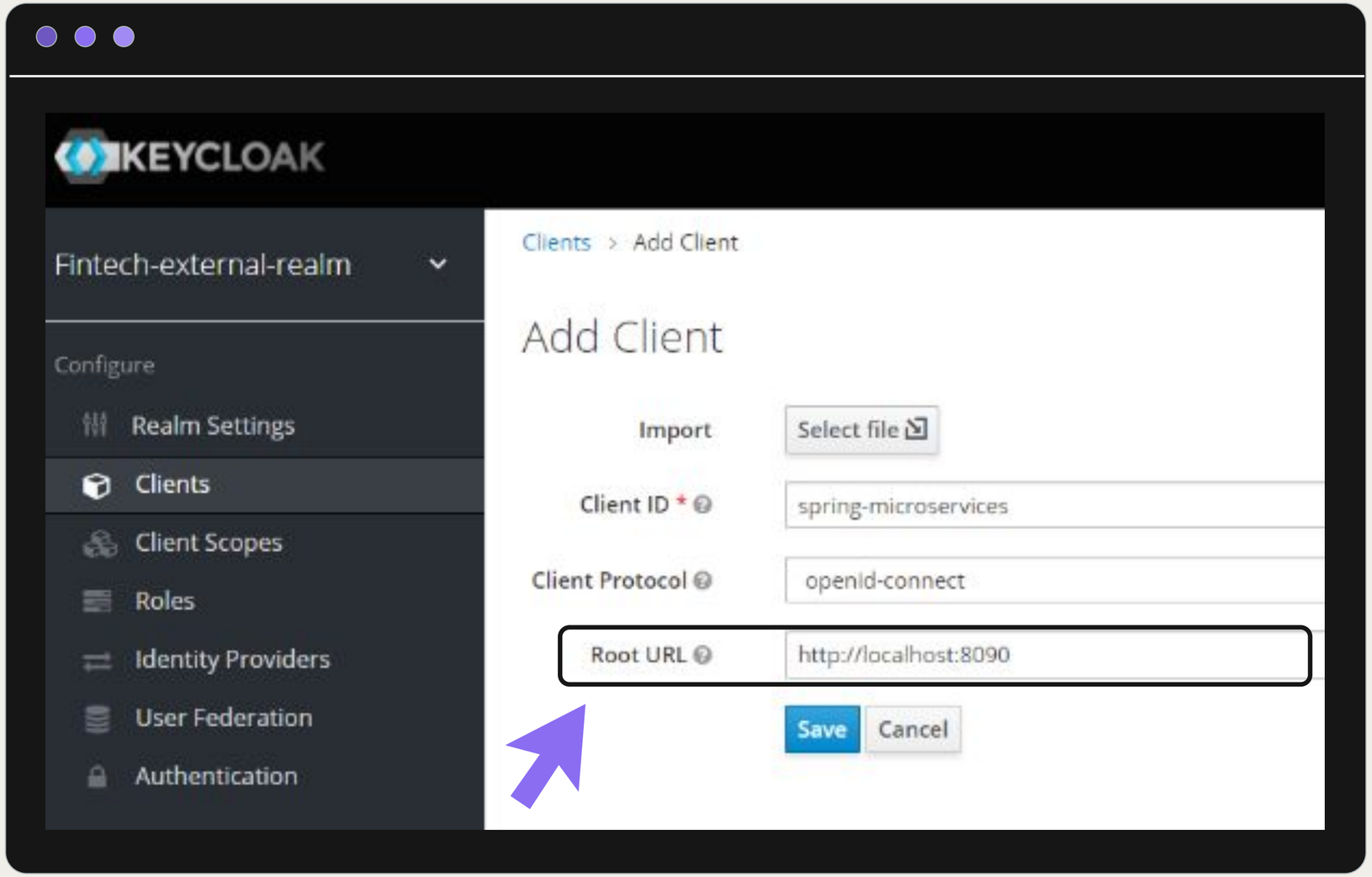
Son las **entidades** que pueden solicitar a Keycloak la autenticación de un usuario. Generalmente, son **aplicaciones y/o servicios que necesitan autenticar** vía single sign-on.

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.



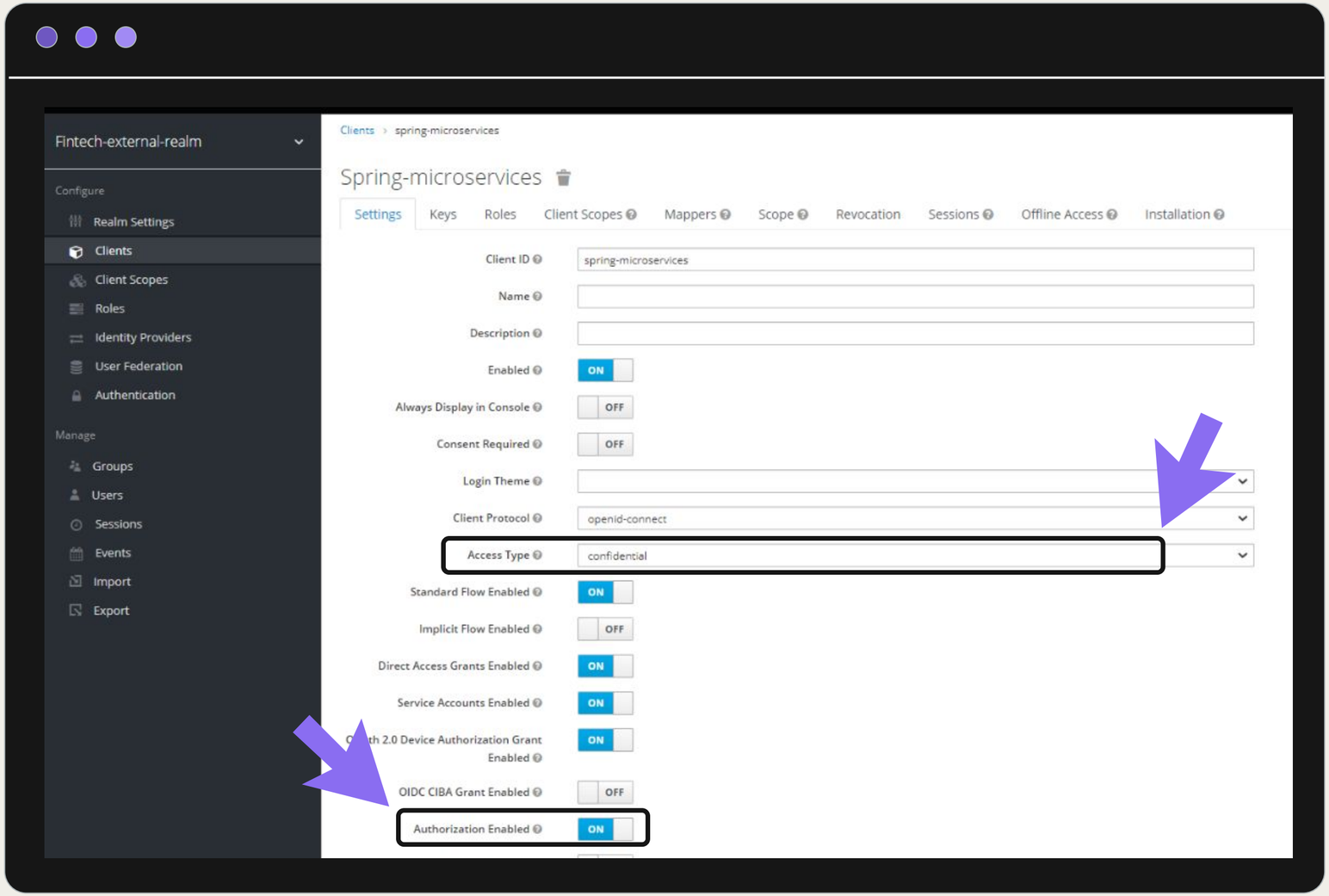
Crear un **client**

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.

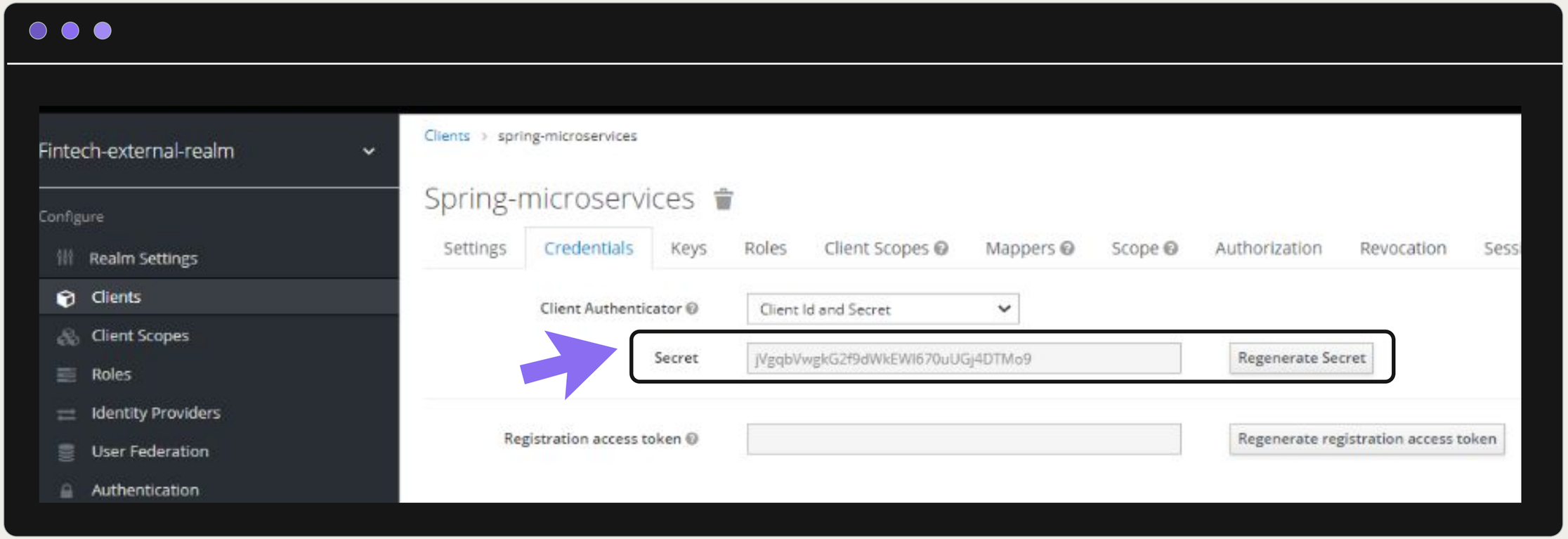


Luego, debemos hacer que nuestro cliente sea de acceso confidencial para que cada API o servicio que lo requiera deba tener un identificador y una contraseña como **secret** para poder acceder a estos servicios de Keycloak.

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



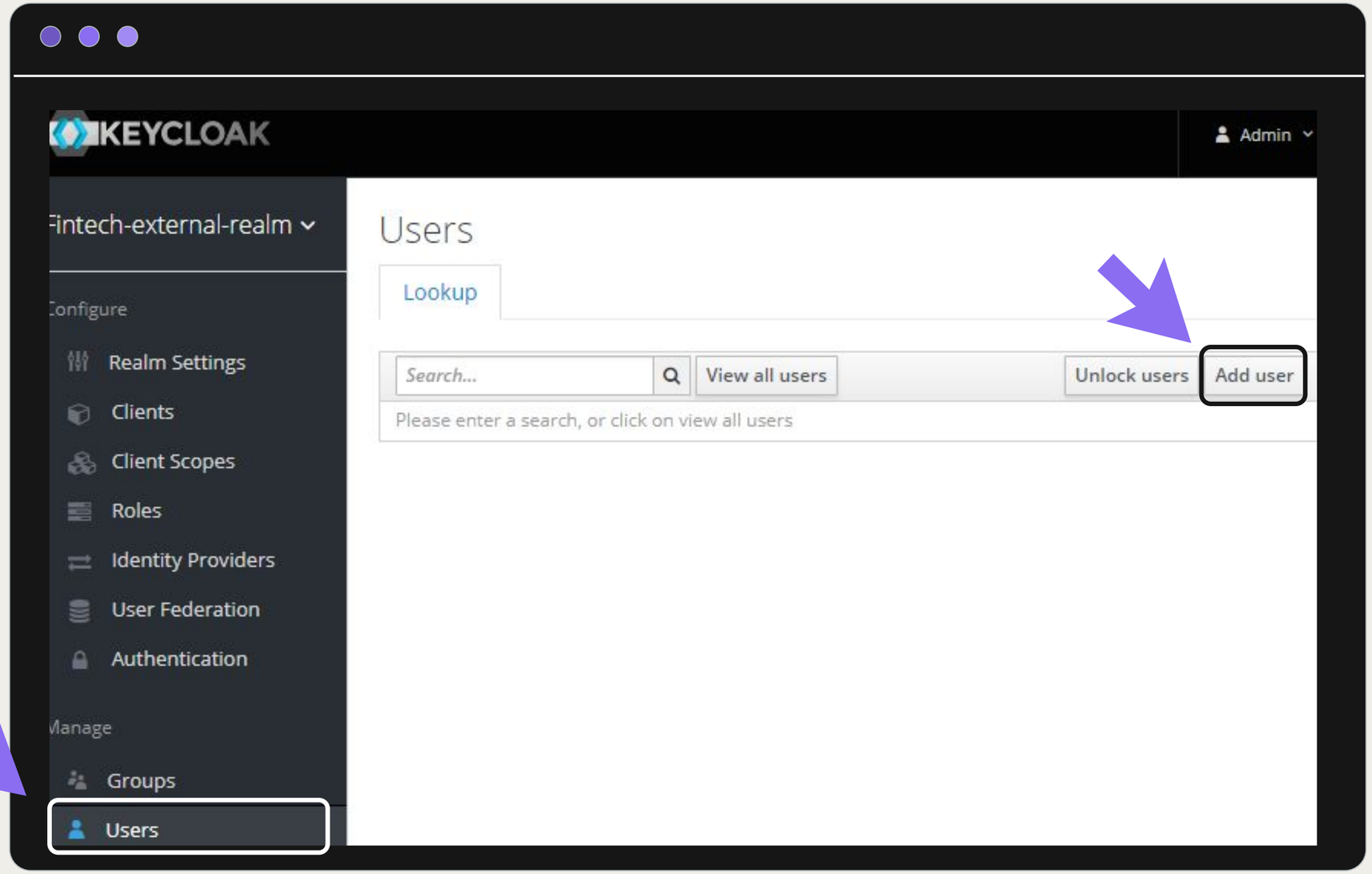
Luego de seleccionar la opción “**Save**”, en la **solapa de credenciales** podremos visualizar el secret a utilizar para conectarnos como clientes de Keycloak desde nuestro microservicio que desea autenticar a un usuario.
En este caso: **jVgqbVwgkG2f9dWkEWI670uUGj4DTMo9**.



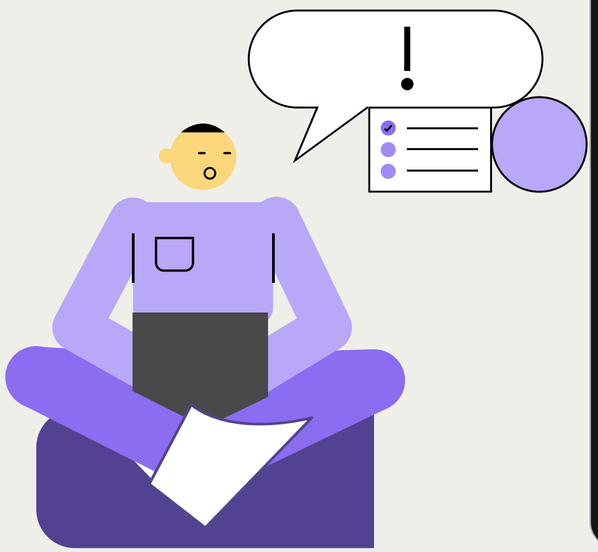
03 User

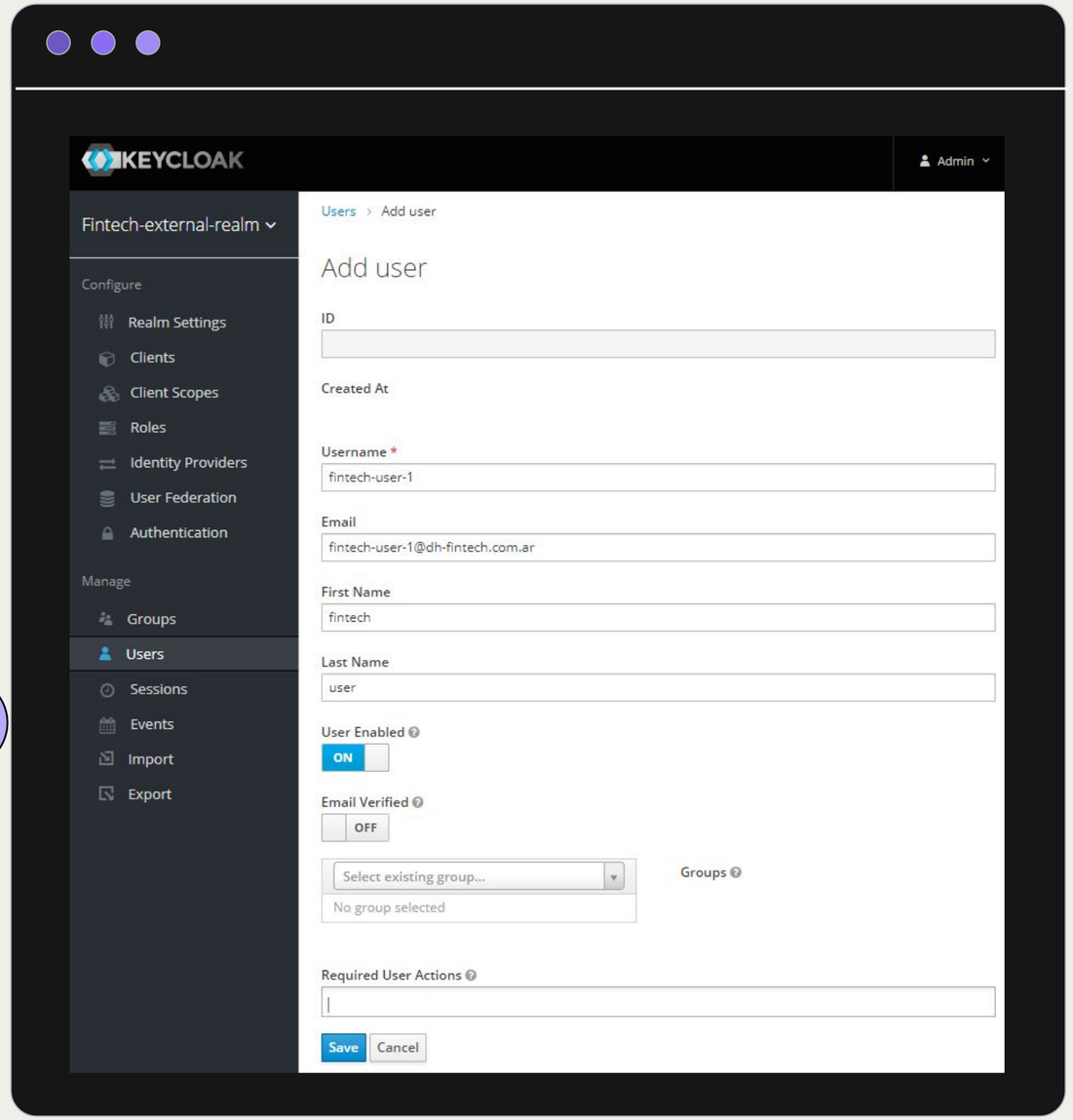
Crear un **User**

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

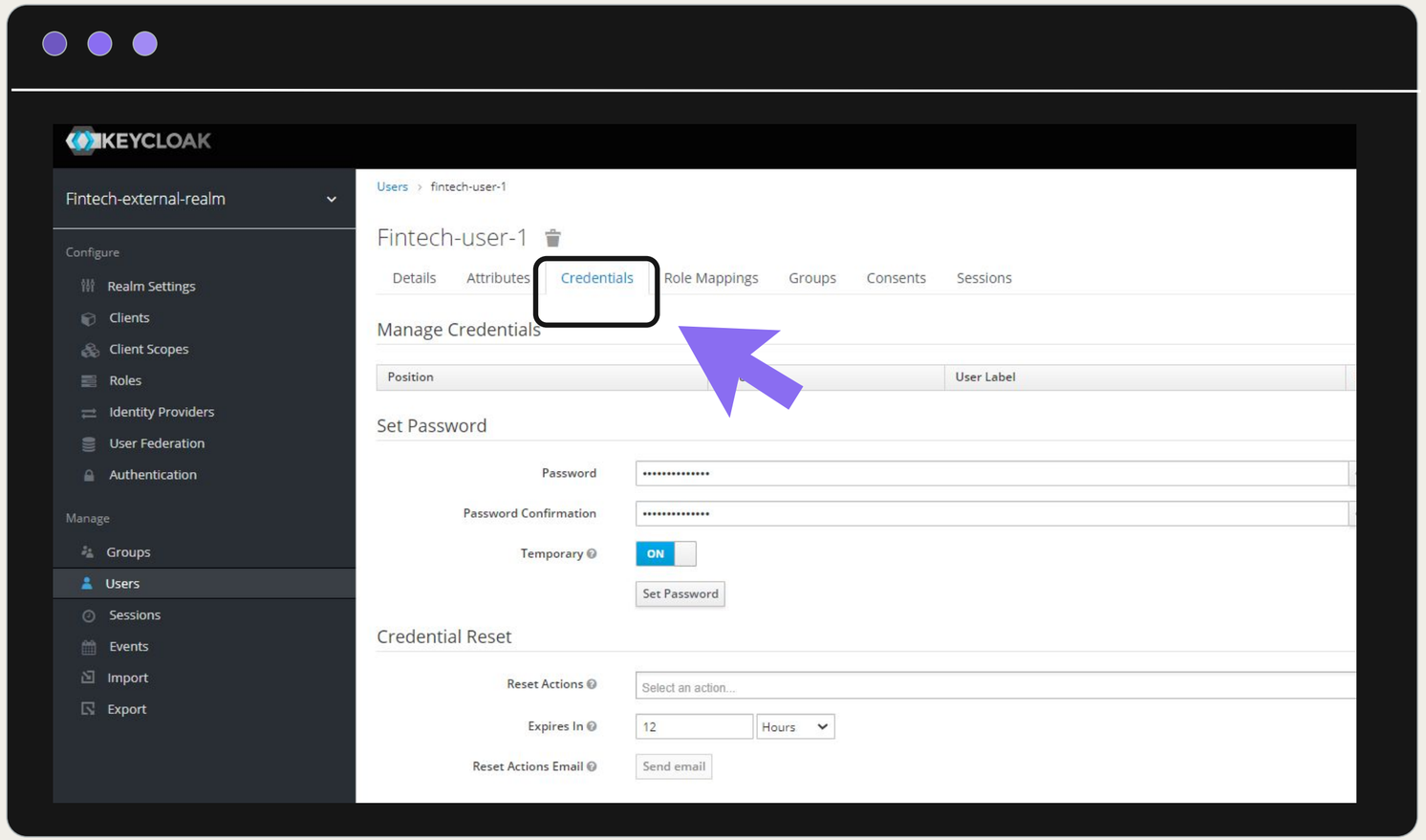


Completamos los datos de usuario y lo dejamos en esta instancia sin grupo.





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

DIGITALHOUSE

¡Muchas gracias!