Especialización en Back End II

Configuraciones adicionales de Keycloak para un Refresh Token

A continuación, veremos una serie de configuraciones extras/adicionales que podemos tener en cuenta a la hora de utilizar Refresh Token. ¡Veamos!

Prevenir generación no deseada de un **Refresh Token**

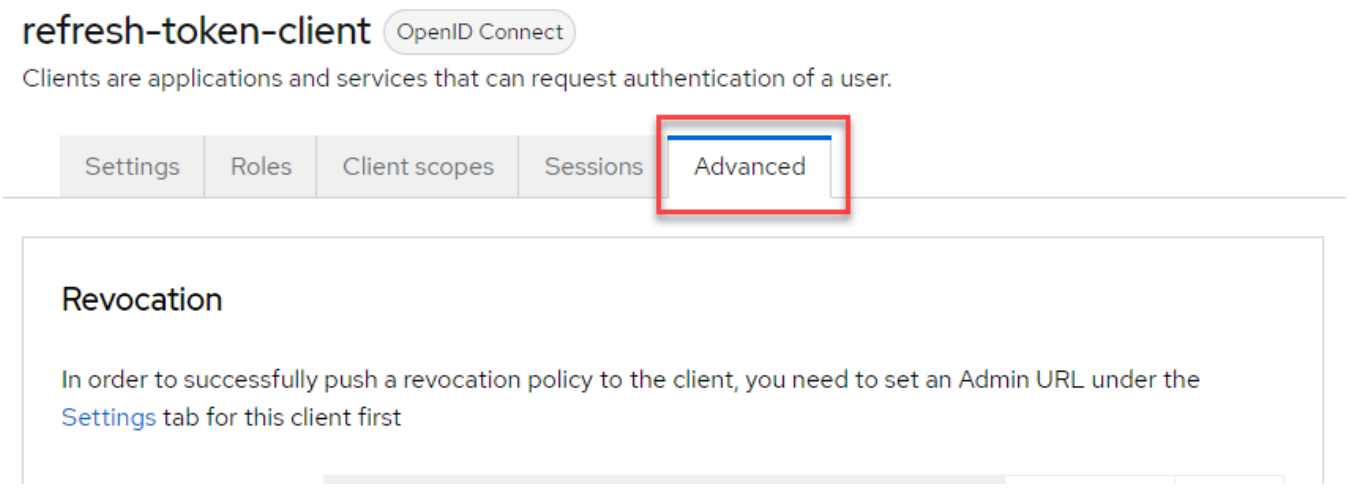
Ya sabemos que, cuando un **access token** expira, se utiliza un **refresh token** para obtener un nuevo access token sin que el usuario tenga que volver a autenticarse.

Sin embargo, es importante **prevenir la generación de un refresh token no autorizado** porque si un atacante obtiene acceso a un refresh token válido, puede utilizarlo para generar nuevos access tokens y acceder a recursos protegidos por el sistema, incluso después de que el access token original haya expirado. Esto podría permitirle acceder a información confidencial, realizar acciones maliciosas o comprometer la seguridad del sistema en general.

Es por ello que, veamos a continuación el paso a paso de cómo prevenir esta situación.

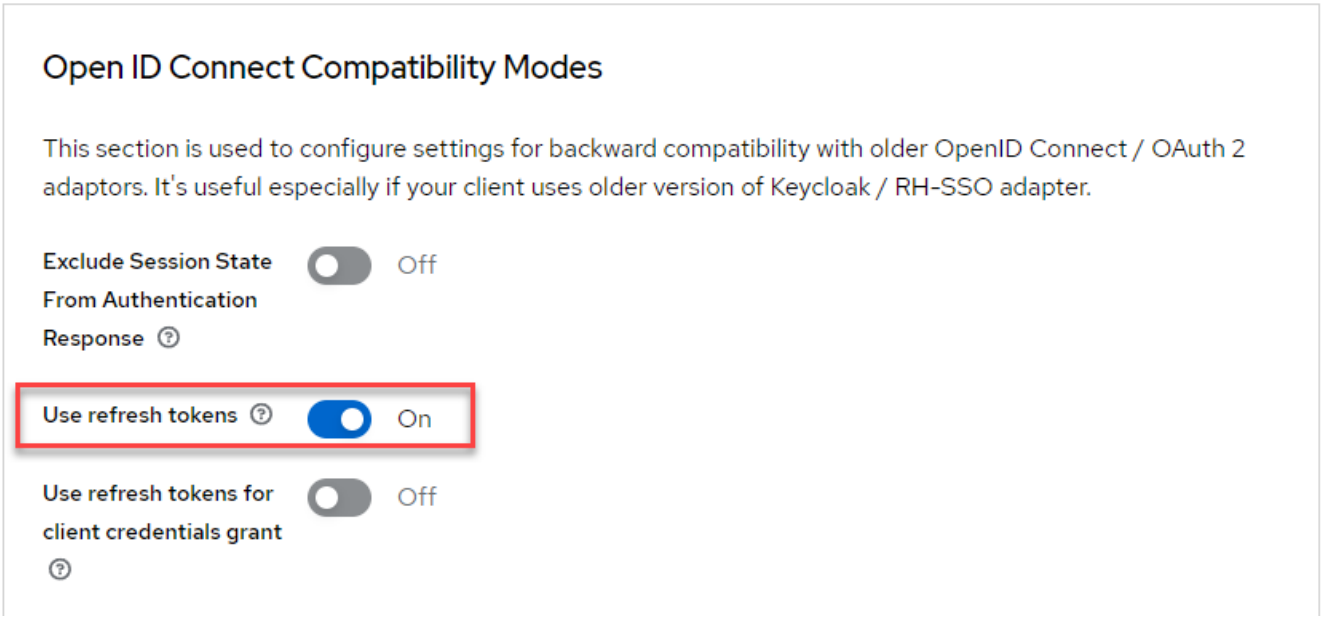
Paso 1

Vamos a dirigirnos al cliente que generamos anteriormente (**refresh-token-client**) y a ingresar a la pestaña **Advanced**.



Paso 2:

Vamos a scrollear hasta la parte inferior de las configuraciones, hasta llegar al apartado **Open ID Connect Compatibility Modes**, allí desactivaremos la opción “Use refresh tokens”. Por defecto esta opción siempre está activa (en azul), en nuestro caso, vamos a dejarla desactivada (en gris), tal como se ve en la siguiente imagen:



y luego guardamos los cambios con el botón **Save**. De esta manera, estaremos frenando la utilización de refresh tokens para este cliente en particular.

Restringir la cantidad de **Refresh Token** que pueden ser creados

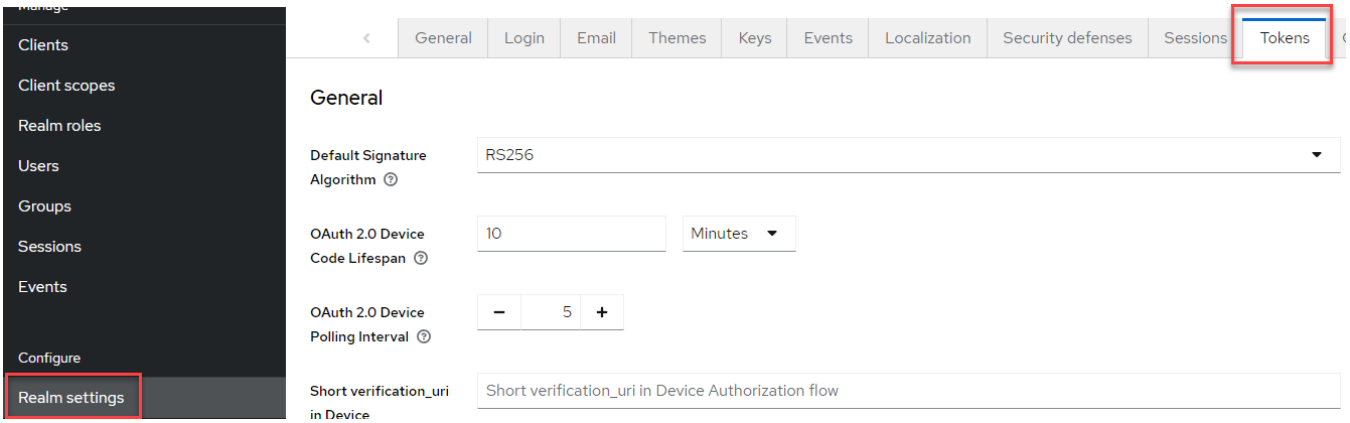
Como otra configuración adicional, es importante controlar la cantidad de refresh tokens que se pueden crear para el acceso a la aplicación que estemos configurando. Esto se debe a varios motivos, entre ellos:

- **Seguridad:** Si se permiten demasiados refresh tokens, esto aumenta el riesgo de que un token sea robado o comprometido.
- **Control de acceso:** Controlar la cantidad de refresh tokens también ayuda a garantizar que sólo se otorguen tokens a los usuarios autorizados y que el sistema tenga un registro completo de quién está accediendo a la cuenta y cuándo.
- **Gestión de recursos:** Permitir una cantidad ilimitada de refresh tokens puede poner una carga innecesaria en el sistema y afectar su rendimiento.

Dicho esto, veamos el paso a paso para poder **limitar/restringir la cantidad de Refresh Tokens** que pueden ser creados con **Keycloak**.

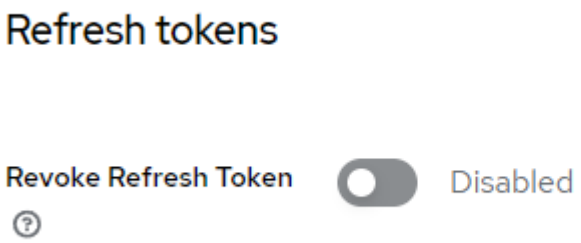
Paso 1

Vamos a dirigirnos a la sección Realm Settings del reino en el que estemos en este momento (vamos a suponer el reino por defecto master) y luego a la pestaña Tokens.



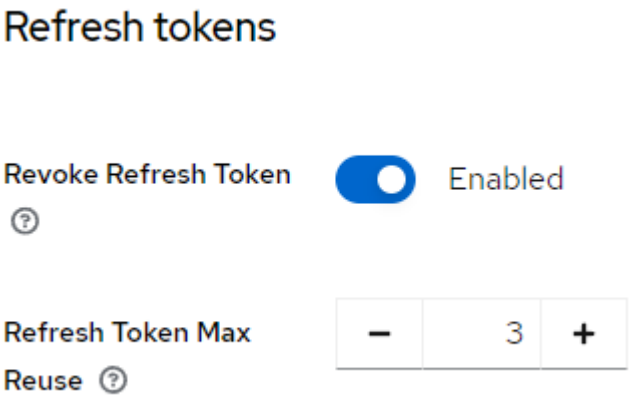
Paso 2

Luego, scrolleamos hacia abajo y nos encontraremos con una sección llamada **“Refresh tokens”** donde veremos la opción **“Revoke Refresh Token”** que por defecto estará deshabilitada.



Paso 3

Vamos a habilitar la opción **“Revoke Refresh Token”** deslizando hacia la derecha y veremos que se nos presenta un nuevo campo llamado **“Refresh Token Max Reuse”** donde podemos establecer la cantidad de **Refresh Token** que permitimos que sean creados. Pongamos por ejemplo, 3.



Una vez hecho esto, scrolleamos hasta el final de la página, guardamos las configuraciones mediante el botón **Save** y ¡Listo! Configuramos correctamente la cantidad de refresh tokens que pueden ser creados.