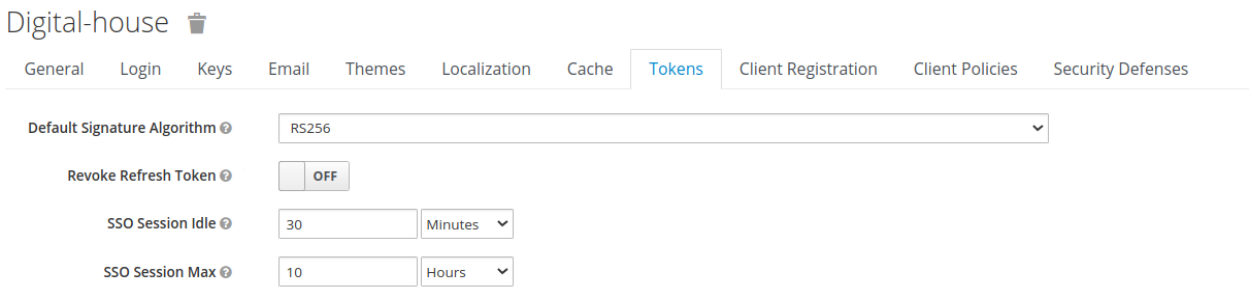
Especialización en Back End II

Configurando el tiempo de expiración y de inactividad

En **sesiones de usuario**, para modificar la configuración por defecto, tenemos que entrar en el reino y luego en "**Tokens**". En esa pestaña podemos ver los campos "**SSO Session Idle**" y "**SSO Session Max**", en donde el primero corresponde al tiempo de inactividad que vamos a permitir antes de invalidar la sesión y el segundo corresponde al tiempo máximo de una sesión antes de invalidarla.



El contador de tiempo de inactividad de una sesión se reiniciará cada vez que los usuarios interactúen con Keycloak, ya sea directamente a través del endpoint de autorización —cuando se usa un navegador— o indirectamente cuando los clientes actualizan los tokens. Si un usuario se autentica y se aleja del teclado —y el cliente no actualiza sus tokens durante este período—, la sesión del usuario se destruirá en 30 minutos. Sin embargo, si el usuario interactúa constantemente con Keycloak usando el navegador —o si el cliente actualiza constantemente sus tokens—, la sesión del usuario puede durar hasta 10 horas.

En **sesiones de clientes** podemos realizar la misma configuración utilizando los campos "**Client Session Idle**" y "**Client Session Max**".

Esta configuración permite **tener un control más detallado de la duración de las sesiones de los clientes**, definiendo límites estrictos sobre por cuánto tiempo son válidos los tokens y obligar a los clientes a volver a autenticarse cada vez que intentan actualizarlos. En otras palabras, los tokens emitidos a cualquier cliente en un reino solo son válidos hasta el tiempo máximo que se establezca, con la posibilidad de caducar prematuramente las sesiones del cliente e invalidar los tokens si el cliente no los actualiza dentro del período de inactividad.

Sin embargo, y a diferencia de las sesiones de usuario, cuando se invalida una sesión de cliente, los usuarios no están necesariamente obligados a volver a autenticarse si sus sesiones de SSO no expiraron, pero obligará a los clientes a volver a autenticarse para obtener un nuevo conjunto de tokens. De forma predeterminada, Keycloak define el mismo conjunto de configuración para las sesiones de usuario y para las sesiones de cliente. Por este motivo vemos en cero los valores para los campos "**Client Session Idle**" y "**Client Session Max**".

¿Qué configuración utilizar?

Como regla general, la duración de la sesión debe ser **lo más corta posible, teniendo en cuenta los aspectos de seguridad, rendimiento y experiencia del usuario**. Usar una vida útil corta, permite reducir el impacto de los ataques de secuestro de sesión o cuando se filtran o roban tokens. También evita sobrecargar el servidor con sesiones que no muestran ninguna actividad del usuario y, por lo tanto, ayuda a ahorrar recursos del servidor, como memoria y CPU. Sin embargo, una breve duración de la sesión tiene un **impacto directo en la experiencia del usuario** y en la frecuencia con la que los usuarios necesitan volver a autenticarse. En un enfoque centrado en el usuario, probablemente será mejor comenzar con lo que es mejor para los usuarios y luego ajustar la duración de la sesión de acuerdo con los requisitos de seguridad y las limitaciones que tengamos en recursos como la memoria y la CPU.