

Especialización en Back End II

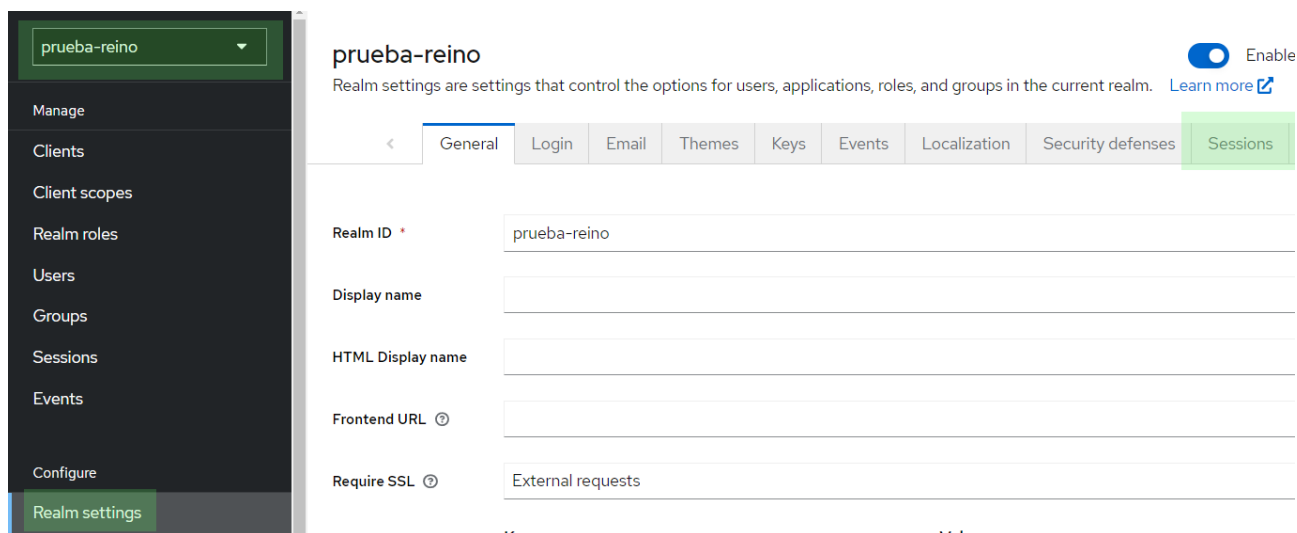
Configurando el tiempo de expiración y de inactividad

Para poder configurar las especificaciones de tiempo de expiración y/o inactividad, debemos seguir los siguientes pasos.

Configurando Sesiones de usuarios

En el contexto de las aplicaciones web y los sistemas de autenticación, una sesión de usuario se refiere a la sesión que se crea cuando un usuario se autentica en una aplicación o servicio en línea. En esta primera parte veremos cómo se configuran los tiempos de expiración e inactividad de una **Sesión de Usuario**.

Paso 1: Seleccionar el reino al que deseamos acceder y luego dirigirnos al apartado **Realm Settings**. Una vez allí, nos dirigimos a la pestaña **Sessions**.



Paso 2: Una vez en Sessions 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.

Recordá que SSO significa Single Sign-on que se refiere a la capacidad de un usuario para autenticarse una sola vez y luego acceder a múltiples aplicaciones o servicios protegidos por Keycloak sin tener que volver a autenticarse en cada uno de ellos.

prueba-reino 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 Sessions Tokens

SSO Session Settings

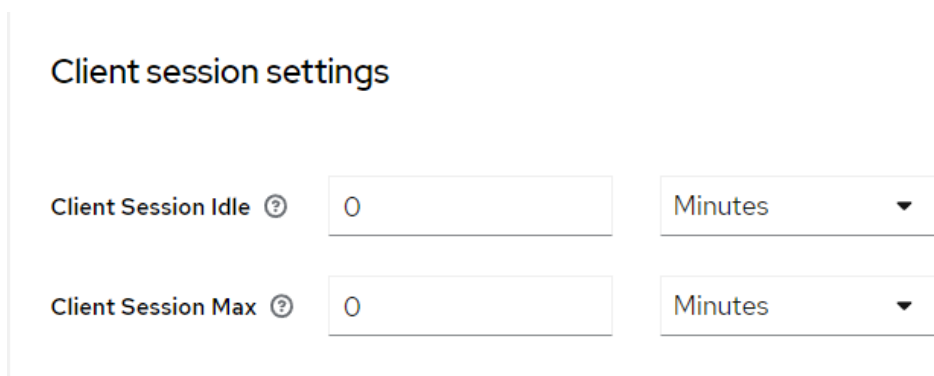
SSO Session Idle ?	30	Minutes
SSO Session Max ?	10	Hours
SSO Session Idle Remember Me ?	0	Minutes
SSO Session Max Remember Me ?	0	Minutes

Si un usuario se autentica y se aleja del teclado y el cliente no actualiza sus tokens durante este período configurado, 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.

Configurando Sesiones de Clientes

Una sesión de cliente se refiere a la sesión que se crea cuando una aplicación o servicio (cliente) se comunica con un servidor de autenticación en nombre del usuario. En esta segunda parte veremos cómo se configuran los tiempos de expiración e inactividad de una Sesión de Cliente

Paso 1: Dentro de la pestaña Session además del apartado SSO Session Settings, contamos con otro apartado llamado Client Session Settings donde también tenemos dos campos: “**Client Session Idle**” y “**Client Session Max**”.



The screenshot shows a configuration panel titled "Client session settings". It contains two rows of settings. The first row is for "Client Session Idle" with a value of "0" and a unit of "Minutes". The second row is for "Client Session Max" with a value of "0" and a unit of "Minutes". Both settings have a question mark icon next to the label.

Client session settings		
Client Session Idle ?	0	Minutes
Client Session Max ?	0	Minutes

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**”.

En **resumen**, la principal diferencia entre una sesión de usuario y una sesión de cliente es que la sesión de usuario está asociada con el usuario que está interactuando directamente con la aplicación o servicio, mientras que la sesión de cliente está asociada con la aplicación o servicio que está interactuando con el servidor de autenticación en nombre del usuario.

¿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.