

Acceso al Portal del Bus Federal de Justicia

En el caso que no sea posible integrar el sistema del gestion del organismo con el BUS Federal a través de la capa de servicios, existe la posibilidad de acceder al portal de gestion de documentos electrónicos del BUS, este portal permite de forma simple el envío y recepción de documentos electrónicos con cualquier Organismo conectado al BUS. El único requisito a cumplir para integrar usando el portal del BUS es el de contar con una plataforma de autenticación abierta que permita federar identidad con el sistema de autenticación del BUS, de esta forma la gestion de usuarios la realiza el organismo a través del mecanismo de federación de identidad con la plataforma de AIM del BUS.

Como integrar con el sistema de autenticación del BUS Federal

El BUS Federal usa un sistema de autenticación basado en el protocolo de autenticación OpenID Connect y tenemos la posibilidad de federar identidad con cualquier plataforma compatible. Una vez que tengamos federados los sistemas de autenticación, simplemente hay que configurar el OIDC de borde para que incluye en los tokens de autenticación dos claims puntuales:

- **codigo_dependencia:** (Opcional) Debe contener el código en el BUS de la dependencia a la que pertenece el usuario. Si este claim no se encuentra disponible el portal va a permitir que los usuarios autenticados accedan a los documentos de todas las dependencias del organismo.
- **basic_access_front:** Claim indicando si el usuario tiene acceso restringido a las funcionalidades del BUS. (No puede definir dependencias)
- **full_access_front:** Claim indicando si el usuario tiene acceso completo a las funcionalidades del BUS. (Puede definir dependencias)

En este documento dejamos un enlace con un laboratorio para que puedas instalar un sistema de autenticación OIDC (Keycloak) y configurarlo para federar identidad con el sistema de autenticación del BUS Federal, configurado para la gestion de usuarios de frontend.

El instructivo que se detalla a continuación muestra de forma sencilla el despliegue de una instancia de Keycloak , un gestor de identidad de código libre y la configuración básica para la federación con el BUS Federal de Justicia incluyendo una propuesta de organización por grupos para la gestion de usuarios.

Instructivo de instalación

Requisitos previos

Contar con una distribución de Linux con docker y docker-compose instalado.

Paso 1 – Generar el archivo `compose.yaml`

Crear un archivo `compose.yaml` con el siguiente contenido

```
version: '3.9'
services:
  postgres:
    image: postgres:13.2
    restart: unless-stopped
    environment:
      POSTGRES_DB: keycloak
      POSTGRES_USER: keycloak
      POSTGRES_PASSWORD: keycloak
    networks:
      - local-keycloak

  keycloak:
    depends_on:
      - postgres
    container_name: local_keycloak
    environment:
      DB_VENDOR: postgres
      DB_ADDR: postgres
      DB_DATABASE: keycloak
      DB_USER: keycloak
      DB_PASSWORD: keycloak
    image: jboss/keycloak:15.0.2
    ports:
      - "28080:8080"
    restart: unless-stopped
    networks:
      - local-keycloak

networks:
  local-keycloak:
```

Paso 2 – Levantar el stack

Ejecutar el comando: **`docker-compose -f compose.yaml up`**

Deberá recibir una salida similar a esta con la ejecución del comando **`docker-compose ps`**:

Name	Command	State	Ports

keycloak-compose_postgres_1	docker-entrypoint.sh postgres	Up	5432/tcp
local_keycloak	/opt/jboss/tools/docker-en ...	Up	0.0.0.0:28080->8080/tcp, :::28080->8080/tcp, 8443/tcp

Paso 3 – Probar acceso a Keycloak

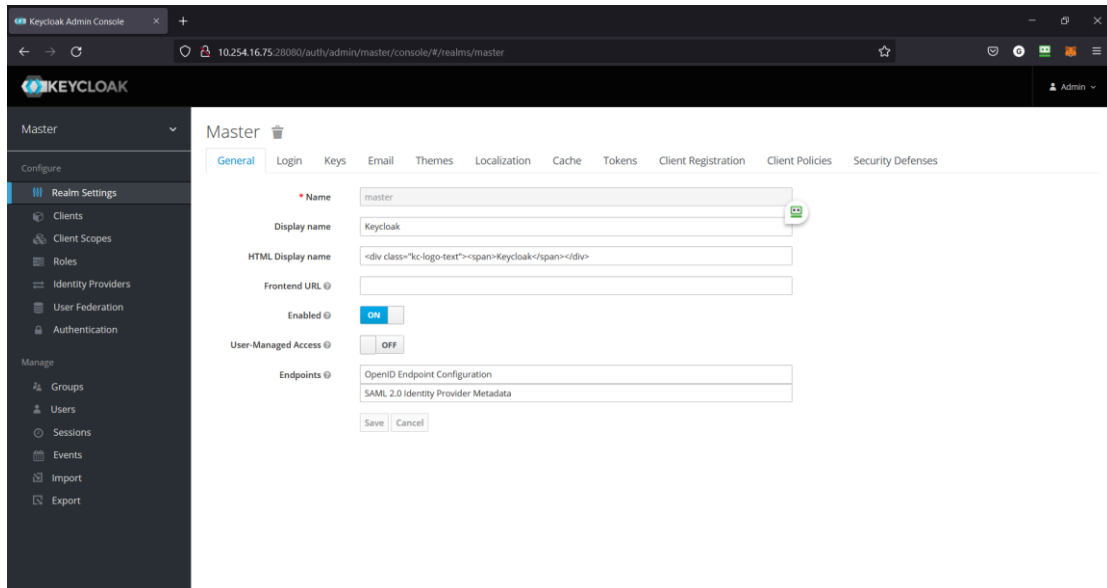
Desde un navegador deberá estar disponible el acceso a la consola web de Keycloak en el puerto 28080.

Paso 4 – Generar la cuenta de administrador

```
docker exec local_keycloak /opt/jboss/keycloak/bin/add-user-keycloak.sh -u admin -p admin && docker restart local_keycloak
```

Paso 5 – Ingresar al dashboard de keycloak

A este punto podrá ingresar a la configuración de keycloak con usuario admin y clave admin.



Configuración de Keycloak

Configuración del REALM

1. En la pantalla principal del real de administración (MASTER) posicione el mouse sobre el nombre del real y seleccione la opción **Add Realm**. Seleccione un nombre para el nuevo REALM.
2. Presione el botón **CREAR**.
3. Complete los datos básicos del nuevo REALM
 - a. Display Name: REALM Prueba Federacion BFJ
 - b. HTML Display Name: REALM Prueba Federacion BFJ
4. Del menú de la izquierda seleccione la opción **Clients** y luego presión el botón **CREATE** ubicado en el vértice superior derecho de la grilla de aplicaciones.
5. En el campo **Client ID**: Ingrese la palabra: **federación** y presione el botón **SAVE**

6. A continuación, complete los siguientes valores:
 - a. **Name:** Cliente para federación BFJ
 - b. **Description:** Cliente para federación BFJ
 - c. **Access Type:** Confidential
 - d. **Standard Flow Enabled:** OFF
 - e. **Direct Access Grant Enabled:** OFF
 - f. **Service Account Enabled:** ON
7. Presione el botón **SAVE** al pie del formulario
8. Dentro de la configuración del cliente de aplicación seleccione la solapa ROLES
9. Presione el botón **Add** y complete el nombre del rol con el valor [full_access_front](#) y presione el botón **SAVE**
10. Dentro de la configuración del cliente de aplicación seleccione la solapa ROLES
11. Presione el botón **Add** y complete el nombre del rol con el valor [basic_access_front](#) y presione el botón **SAVE**.
12. Una vez completados los datos del cliente de federación y los roles, se deberá configurar un mapeador role to claim para transportar el rol asignado al usuario en el token de federación. Para esto:
 - a. Seleccione la solapa **Mappers**
 - b. Presione el botón **Create**
 - c. Complete los datos de acuerdo a la siguiente figura:

Create Protocol Mapper

Protocol ⓘ	<input type="text" value="openid-connect"/>
Name ⓘ	<input type="text" value="federacion_role_to_claim"/>
Mapper Type ⓘ	<input type="text" value="User Client Role"/>
Client ID ⓘ	<input type="text" value="federación"/>
Client Role prefix ⓘ	<input type="text"/>
Multivalued ⓘ	<input checked="" type="checkbox"/>
Token Claim Name ⓘ	<input type="text" value="federacion_roles"/>
Claim JSON Type ⓘ	<input type="text" value="String"/>
Add to ID token ⓘ	<input checked="" type="checkbox"/>
Add to access token ⓘ	<input checked="" type="checkbox"/>
Add to userinfo ⓘ	<input checked="" type="checkbox"/>
	<input type="button" value="Save"/> <input type="button" value="Cancel"/>


13. Presione el botón **SAVE** para finalizar. Con esta configuración el IDP incluirá los roles de aplicación asignados al usuario en un claim específico dentro del token de federación.

Hasta este punto se encuentra configurado el REALM con la cuenta del servicio de federación con el IAM del BUS Federal. Para poder realizar la integración hay que enviar al equipo del BUS Federal la URL de Keycloak, el client ID y la credencial de acceso que puede ser accedida desde la solapa **Credentials**. Con estos datos ya es suficiente para establecer la federación. Hay que tener en cuenta que en un ambiente productivo el servidor keycloak debe contar un certificado SSL que coincida con la URL de acceso.

Creación de Grupos – Configuración de dependencias y permisos



El próximo paso en la configuración es el de asociar a cada grupo de usuarios los roles y dependencias que corresponda, para esto se recomienda la creación de grupos con atributos que luego serán mapeados al token de autenticación. En este caso podemos asignar el código de dependencia al grupo y el rol con los permisos de acceso a cada usuario en particular.

- a) Seleccione la opción Grupos.
- b) Presione el botón **NEW**
- c) En el nombre de grupo complete con el nombre de la dependencia (ej. BFJ - Juzgado Civil 1) y presione el botón **SAVE**.
- d) Seleccione la solapa atributos y complete:
 - a. Key:codigo_dependencia
 - b. Value: El código de la dependencia asignado por el BUS al momento del alta.
 - c. Presione el botón **ADD** y luego el botón **SAVE**
- e) Genere una cuenta de usuario y asóciela al grupo
- f) Nuevamente desde la pantalla de configuración del grupo, seleccione la opción **MEMBERS**.
- g) Haga click sobre el usuario para seleccionarlo
- h) Dentro de la pantalla de configuración del usuario seleccione la solapa **Role Mapping**
- i) Despliegue la lista **Client Roles** al final de la pantalla y seleccione el cliente de aplicación.
- j) Al seleccionar el cliente de aplicación se deberá desplegar una lista de roles disponibles en los que se encuentran los definidos en el apartado anterior (full_access_front y basic_access_front).
- k) Seleccione el rol que corresponda al usuario elegido y presione el botón **Añadir Selección**.

Pruebabus 

Details Attributes Credenciales **Role Mappings** Groups Consents Sesiones

Roles de dominio	
Roles Disponibles ⓘ	Roles Asignados ⓘ
MO-Gestion-Externos MP-Gestion-Externos NE-Gestion-Externos Netmon Users offline_access	default-roles-scba-interno
Añadir seleccionado >	< Borrar seleccionados
Roles Efectivos ⓘ	
default-roles-scba-interno offline_access uma_authorization	

Roles de Cliente		
auth-bf  		
Roles Disponibles ⓘ	Roles Asignados ⓘ	Roles Efectivos ⓘ
basic_access_front full_access_front		
Añadir seleccionado >	< Borrar seleccionados	

Al finalizar este instructivo, ya podrá integrar el sistema de autenticación al BUS Federal de Justicia para el acceso al portal.

Historial de Revisiones

04/07/2023	Se incorpora carga de mapper role to claim en definición de cliente de federación.	gperez
------------	--	--------