Inhaltsverzeichnis

1Docker setup..2
2Test JWT access..6

1 Docker setup

- Clone from git@github.com:GilbertHofstaetter/spring-boot-oauth2-resource-server-client.git
- Add **127.0.0.1 keycloak** to your hosts file
  - Linux/Max **/etc/hosts**
  - Windows 10 **c:\Windows\System32\Drivers\etc\hosts**

```
127.0.0.1       keycloak
```

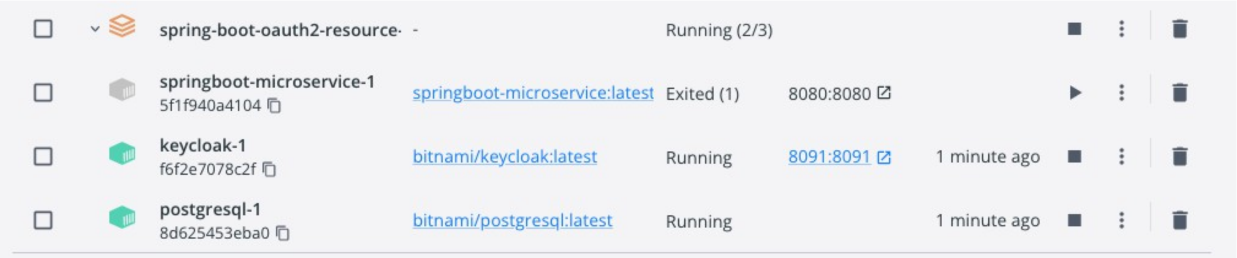
- Change to directory to project root directory

```
spring-boot-oauth2-resource-server-client %
```

- Run **`docker-compose -f docker-compose-bitnami-custom.yml up`**

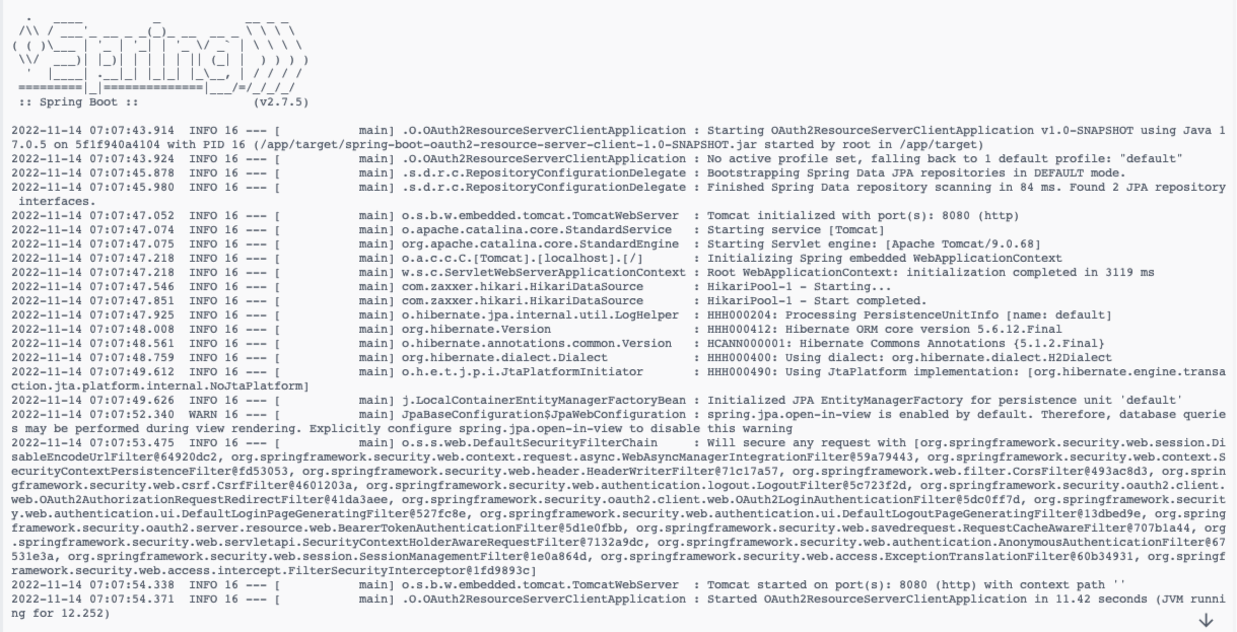
```
spring-boot-oauth2-resource-server-client % docker-compose -f docker-compose-bitnami-custom.yml up
```

- Postgres, keycloak and springboot-microservice are starting → keycloak imports Demo-Realm from file ./realms/Demo-Realm-realm.json
- springboot-microservice fails on startup (Docker Desktop) → don't mind



□ spring-boot-oauth2-resource-	-	Running (2/3)			
□ springboot-microservice-1 5f1f940a4104	springboot-microservice:latest	Exited (1)	8080:8080		
□ keycloak-1 f6f2e7078c2f	bitnami/keycloak:latest	Running	8091:8091	1 minute ago	
□ postgresql-1 8d625453eba0	bitnami/postgresql:latest	Running		1 minute ago	

- Restart springboot-microservice-1

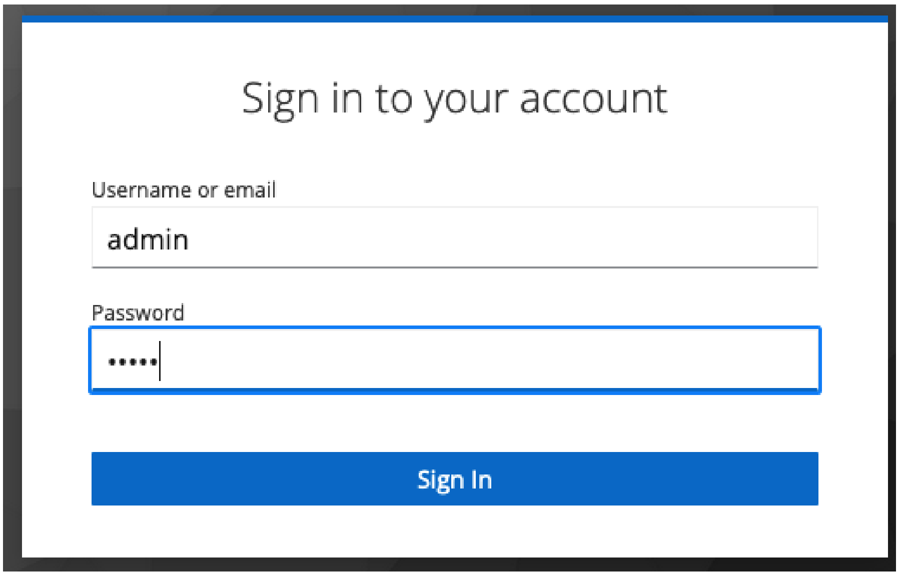


```
  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.7.5)

2022-11-14 07:07:43.914  INFO 16 --- [           main] .O.OAuth2ResourceServerClientApplication : Starting OAuth2ResourceServerClientApplication v1.0-SNAPSHOT using Java 1
7.0.5 on 5f1f940a4104 with PID 16 (/app/target/spring-boot-oauth2-resource-server-client-1.0-SNAPSHOT.jar started by root in /app/target)
2022-11-14 07:07:43.924  INFO 16 --- [           main] .O.OAuth2ResourceServerClientApplication : No active profile set, falling back to 1 default profile: "default"
2022-11-14 07:07:45.878  INFO 16 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2022-11-14 07:07:45.980  INFO 16 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 84 ms. Found 2 JPA repository
 interfaces.
2022-11-14 07:07:47.052  INFO 16 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8080 (http)
2022-11-14 07:07:47.074  INFO 16 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2022-11-14 07:07:47.075  INFO 16 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache Tomcat/9.0.68]
2022-11-14 07:07:47.218  INFO 16 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
2022-11-14 07:07:47.218  INFO 16 --- [           main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in 3119 ms
2022-11-14 07:07:47.546  INFO 16 --- [           main] com.zaxxer.hikari.HikariDataSource       : HikariPool-1 - Starting...
2022-11-14 07:07:47.851  INFO 16 --- [           main] com.zaxxer.hikari.HikariDataSource       : HikariPool-1 - Start completed.
2022-11-14 07:07:47.925  INFO 16 --- [           main] o.hibernate.jpa.internal.util.LogHelper  : HHH000204: Processing PersistenceUnitInfo [name: default]
2022-11-14 07:07:48.008  INFO 16 --- [           main] org.hibernate.Version                    : HHH000412: Hibernate ORM core version 5.6.12.Final
2022-11-14 07:07:48.561  INFO 16 --- [           main] o.hibernate.annotations.common.Version   : HCANN000001: Hibernate Commons Annotations {5.1.2.Final}
2022-11-14 07:07:48.759  INFO 16 --- [           main] org.hibernate.dialect.Dialect            : HHH000400: Using dialect: org.hibernate.dialect.H2Dialect
2022-11-14 07:07:49.612  INFO 16 --- [           main] o.h.e.t.j.p.i.JtaPlatformInitiator       : HHH000490: Using JtaPlatform implementation: [org.hibernate.engine.transa
ction.jta.platform.internal.NoJtaPlatform]
2022-11-14 07:07:49.626  INFO 16 --- [           main] j.LocalContainerEntityManagerFactoryBean : Initialized JPA EntityManagerFactory for persistence unit 'default'
2022-11-14 07:07:52.340  WARN 16 --- [           main] JpaBaseConfiguration$JpaWebConfiguration : spring.jpa.open-in-view is enabled by default. Therefore, database querie
s may be performed during view rendering. Explicitly configure spring.jpa.open-in-view to disable this warning
2022-11-14 07:07:53.475  INFO 16 --- [           main] o.s.s.web.DefaultSecurityFilterChain     : Will secure any request with [org.springframework.security.web.session.Di
sableEncodeUrlFilter@64920dc2, org.springframework.security.web.context.request.async.WebAsyncManagerIntegrationFilter@59a79443, org.springframework.security.web.context.S
ecurityContextPersistenceFilter@fd53053, org.springframework.security.web.header.HeaderWriterFilter@71c17a57, org.springframework.web.filter.CorsFilter@493ac8d3, org.sprin
gframework.security.web.csrf.CsrfFilter@4601203a, org.springframework.security.web.authentication.logout.LogoutFilter@5c723f2d, org.springframework.security.oauth2.client.
web.OAuth2AuthorizationRequestRedirectFilter@41da3aee, org.springframework.security.oauth2.client.web.OAuth2LoginAuthenticationFilter@5dc0ff7d, org.springframework.securit
y.web.authentication.ui.DefaultLoginPageGeneratingFilter@527fc8e, org.springframework.security.web.authentication.ui.DefaultLogoutPageGeneratingFilter@13dbed9e, org.spring
framework.security.oauth2.server.resource.web.BearerTokenAuthenticationFilter@5d1e0fbb, org.springframework.security.web.savedrequest.RequestCacheAwareFilter@707b1a44, org
.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@7132a9dc, org.springframework.security.web.authentication.AnonymousAuthenticationFilter@67
531e3a, org.springframework.security.web.session.SessionManagementFilter@1e0a864d, org.springframework.security.web.access.ExceptionTranslationFilter@60b34931, org.springf
ramework.security.web.access.intercept.FilterSecurityInterceptor@1fd9893c]
2022-11-14 07:07:54.338  INFO 16 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8080 (http) with context path ''
2022-11-14 07:07:54.371  INFO 16 --- [           main] .O.OAuth2ResourceServerClientApplication : Started OAuth2ResourceServerClientApplication in 11.42 seconds (JVM runni
ng for 12.252)
```

- springboot-microservice is up and running
- keycloak has imported Demo-Realm-realm.json at startup → Realm, springboot-microservice, scope read, Userroles (app-user, app-admin, admin, user) are now present
- Create 3 Users through keycloak admin console → localhost:8091

- User: admin, Pwd: admin

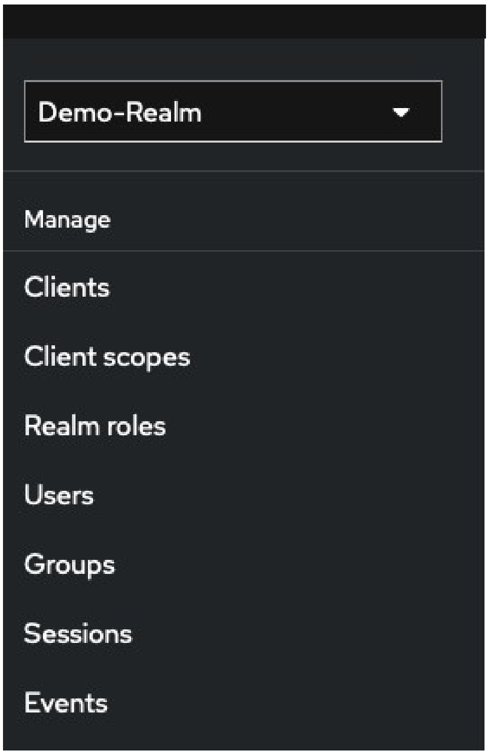


Sign in to your account

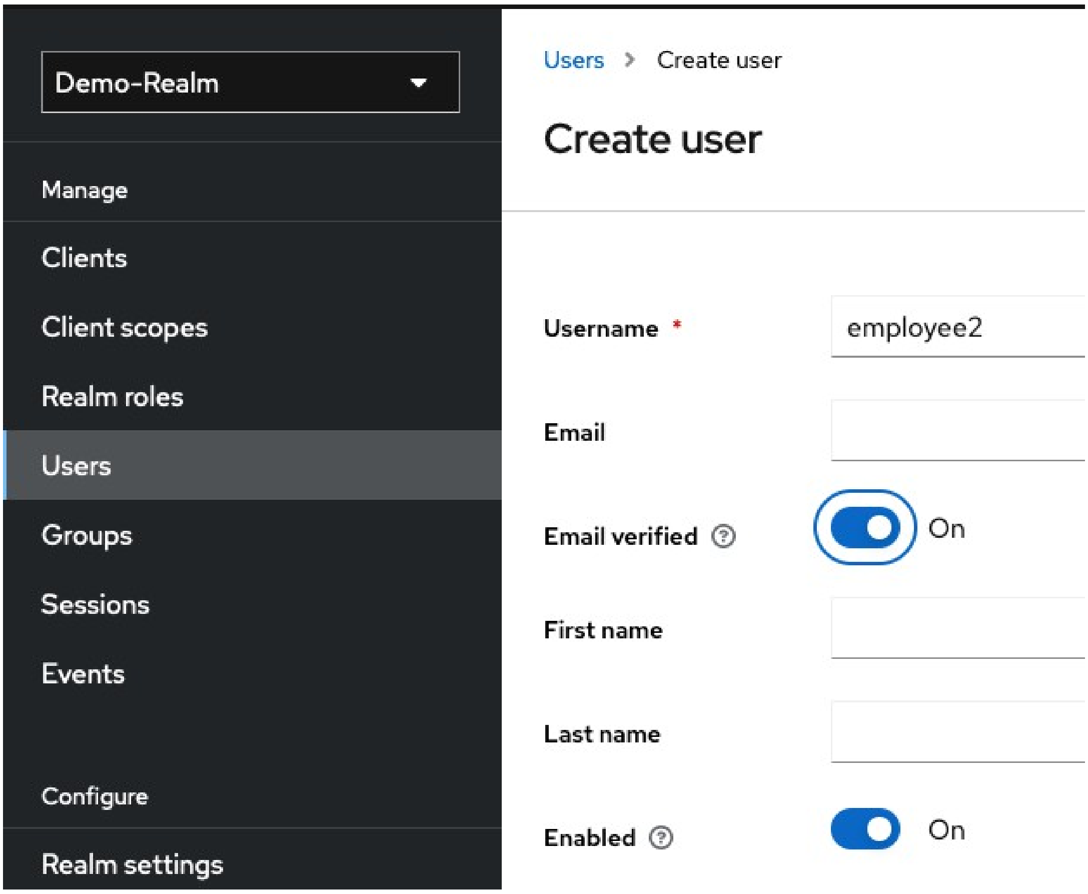
Username or email: admin

Password: •••••

- Open realm „**`Demo-Realm`**“



- Create 3 Users
  - employee1 → Assign Role app-user, set Email verified to on, set credential switch „Temporary“ to off
  - employee2 → Assign Role app-admin, set Email verified to on, set credential switch „Temporary“ to off
  - employee3 → Assign Role app-user, app-admin, set Email verified to on, set credential switch „Temporary“ to off



Users > Create user

Create user

Username * employee2

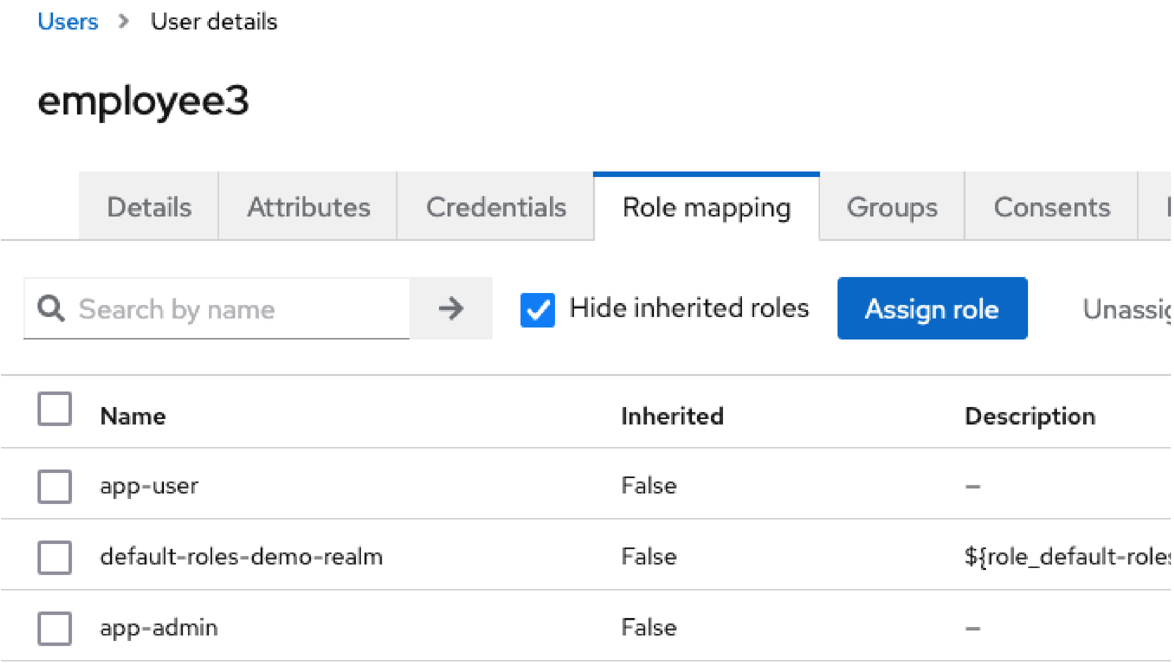
Email

Email verified On

First name

Last name

Enabled On

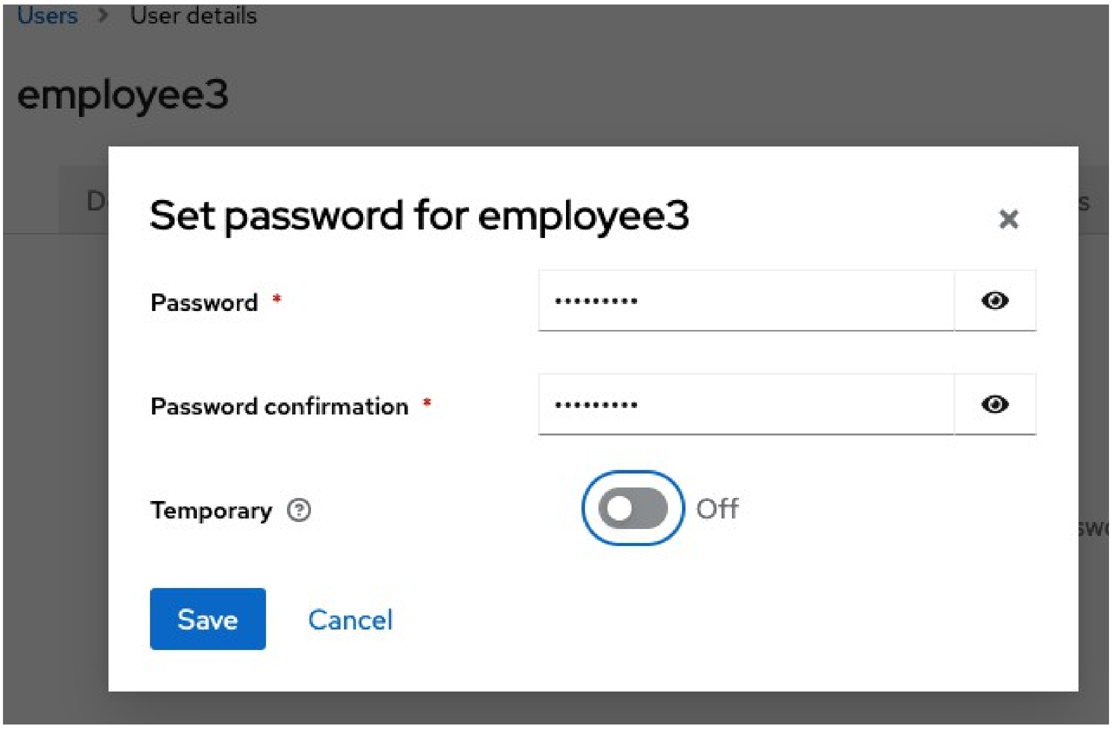


Users > User details

employee3

☑ Hide inherited roles

□	Name	Inherited	Description
□	app-user	False	–
□	default-roles-demo-realm	False	${role_default-role
□	app-admin	False	–



Users > User details

employee3

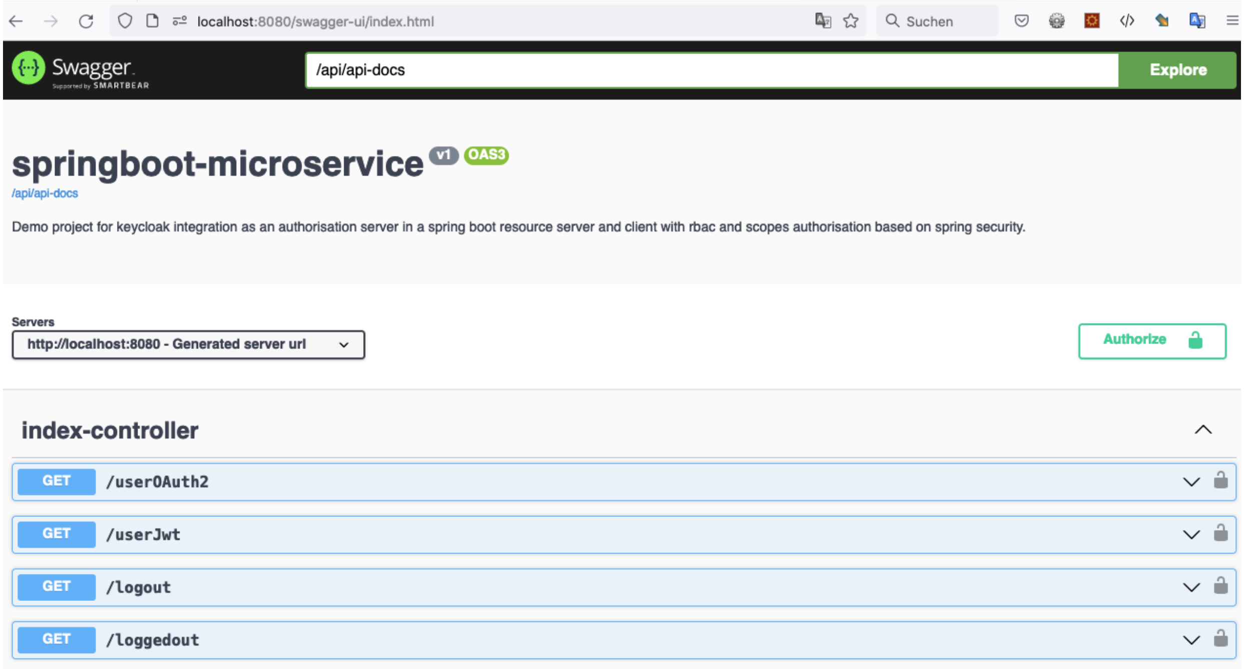
Set password for employee3

Password * ••••••••••

Password confirmation * ••••••••••

Temporary ⓘ ○ Off

- Open http://localhost:8080/swagger-ui.html
- Sign in with employee3



localhost:8080/swagger-ui/index.html

/api/api-docs

springboot-microservice v1 OAS3

/api/api-docs

Demo project for keycloak integration as an authorisation server in a spring boot resource server and client with rbac and scopes authorisation based on spring security.

Servers: http://localhost:8080 - Generated server url

index-controller

GET /userOAuth2

GET /userJwt

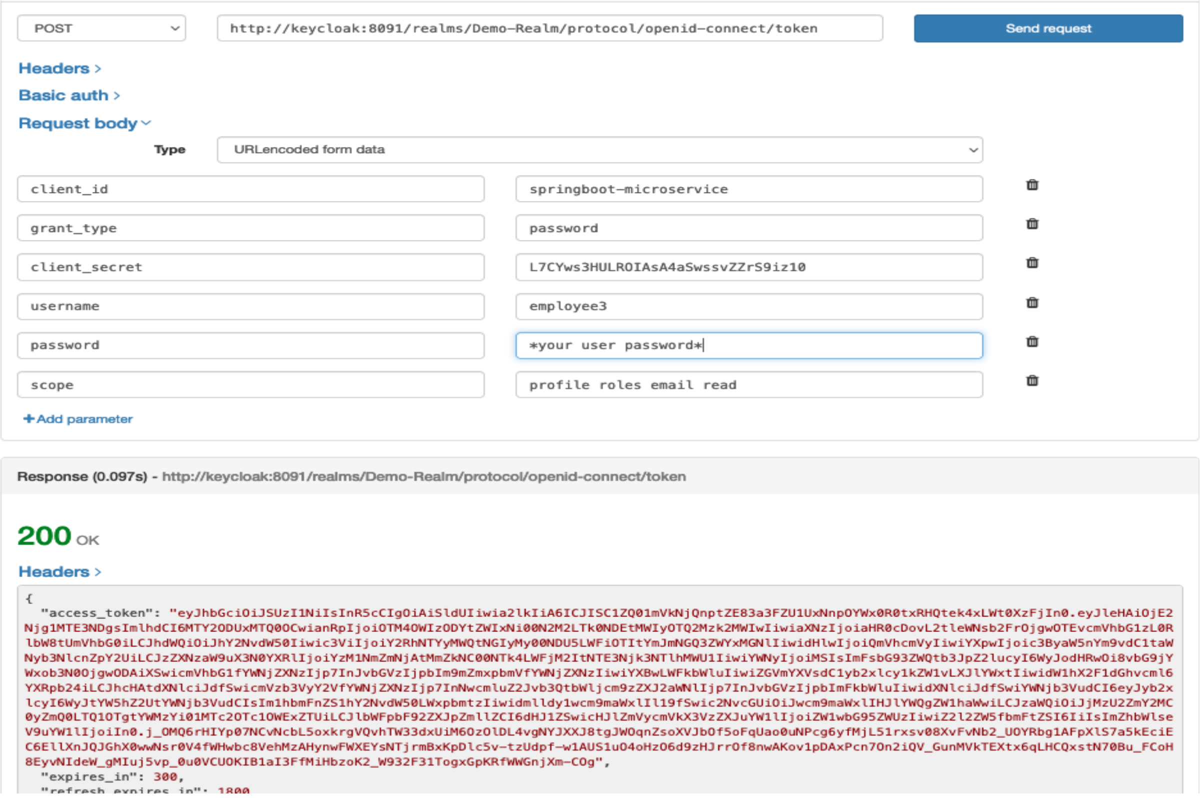
GET /logout

GET /loggedout

- Try out
    - http://localhost:8080/api/customer/list
    - http://localhost:8080/api/employee/list
    - http://localhost:8080/userJwt
    - http://localhost:8080/userOAuth2
    - http://localhost:8080/logout

2 Test JWT access

- With Docker the Keycloak host changed from localhost to „keycloak“
- Use http://keycloak:8091/realms/Demo-Realm/protocol/openid-connect/token to request an access token from Keycloak. A request with host localhost:8091 delivers an invalid token



http://keycloak:8091/realms/Demo-Realm/protocol/openid-connect/token

Type: URLencoded form data

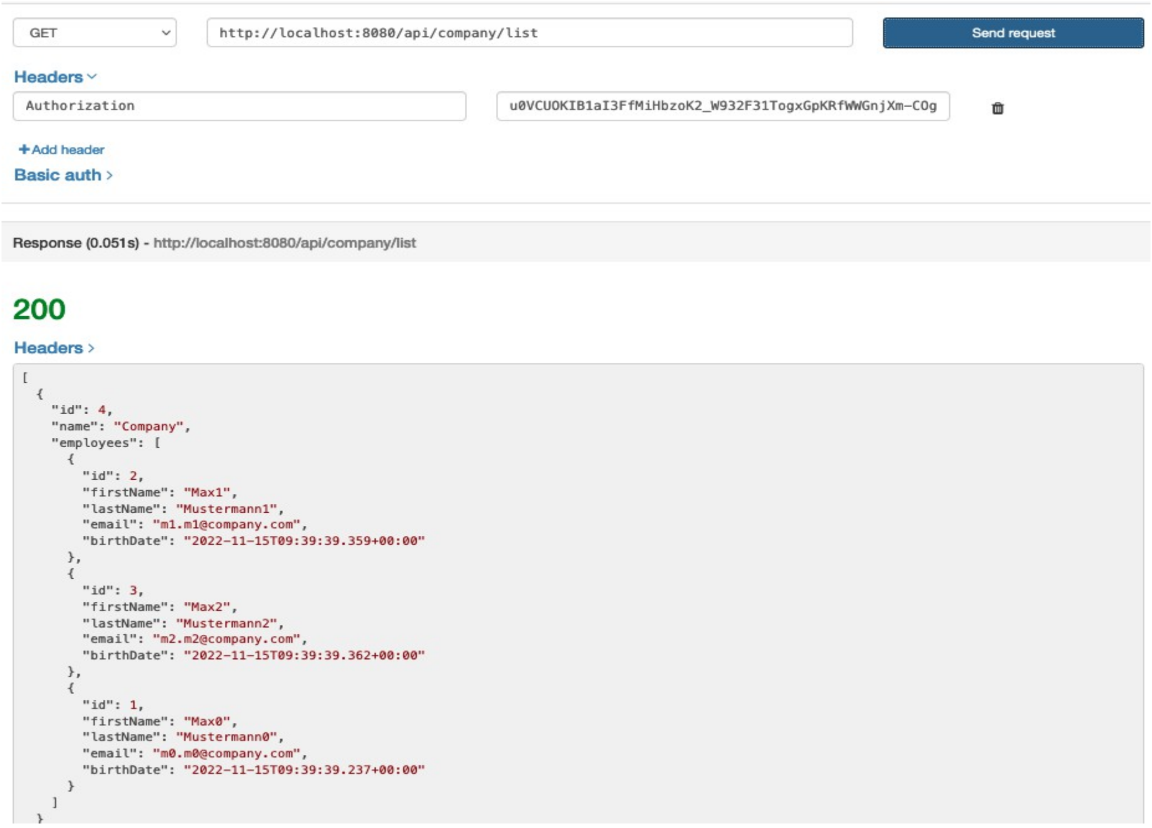
client_id	springboot-microservice
grant_type	password
client_secret	L7CYws3HULROIAsA4aSwssvZZrS9iz10
username	employee3
password	*your user password*
scope	profile roles email read

Response (0.097s) - http://keycloak:8091/realms/Demo-Realm/protocol/openid-connect/token

200 OK

```
{
  "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJISC1ZQ01mVkNjQnptZE83a3FZU1UxNnpOYWx0R0txRHQtek4xLWt0XzFjIn0.eyJleHAiOjE2
Njg1MTE3NDgsImlhdCI6MTY2ODUxMTQ0OCwianRpIjoiOTM4OWIzODYtZWIxNi00N2M2LTk0NDEtMWIyOTQ2Mzk2MWIwIiwiaXNzIjoiaHR0cDovL2tleWNsb2FrOjgwOTEvcmVhbG1zL0R
lbW8tUmVhbG0iLCJhdWQiOiJhY2NvdW50Iiwic3ViIjoiY2RhNTYyMWQtNGIyMy00NDU5LWFiOTItYmJmNGQ3ZWYxMGNlIiwidHlwIjoiQmVhcmVyIiwiYXpwIjoic3ByaW5nYm9vdC1taW
Nyb3NlcnZpY2UiLCJzZXNzaW9uX3N0YXRlIjoiYzM1NmZmNjAtMmZkNC00NTk4LWFjM2ItNTE3Njk3NTlhMWU1IiwiYWNyIjoiMSIsImFsbG93ZWQtb3JpZ2lucyI6WyJodHRwOi8vbG9jY
Wxob3N0OjgwODAiXSwicmVhbG1fYWNjZXNzIjp7InJvbGVzIjpbIm9mZmxpbmVfYWNjZXNzIiwiYXBwLWFkbWluIiwiZGVmYXVsdC1yb2xlcy1kZW1vLXJlYWxtIiwidW1hX2F1dGhvcml6
YXRpb24iLCJhcHAtdXNlciJdfSwicmVzb3VyY2VfYWNjZXNzIjp7InNwcmluZ2Jvb3QtbWljcm9zZXJ2aWNlIjp7InJvbGVzIjpbImFkbWluIiwidXNlciJdfSwiYWNjb3VudCI6eyJyb2x
lcyI6WyJtYW5hZ2UtYWNjb3VudCIsIm1hbmFnZS1hY2NvdW50LWxpbmtzIiwidmlldy1wcm9maWxlIl19fSwic2NvcGUiOiJwcm9maWxlIHJlYWQgZW1haWwiLCJzaWQiOiJjMzU2ZmY2MC
0yZmQ0LTQ1OTgtYWMzYi01MTc2OTc1OWExZTUiLCJlbWFpbF92ZXJpZmllZCI6dHJ1ZSwicHJlZmVycmVkX3VzZXJuYW1lIjoiZW1wbG95ZWUzIiwiZ2l2ZW5fbmFtZSI6IiIsImZhbWlse
V9uYW1lIjoiIn0.j_OMQ6rHIYp07NCvNcbL5oxkrgVQvhTW33dxUiM6OzOlDL4vgNYJXXJ8tgJWOqnZsoXVJbOf5oFqUao0uNPcg6yfMjL51rxsv08XvFvNb2_UOYRbg1AFpXlS7a5kEciE
C6EllXnJQJGhX0wwNsr0V4fWHwbc8VehMzAHynwFWXEYsNTjrmBxKpDlc5v-tzUdpf-w1AUS1uO4oHzO6d9zHJrrOf8nwAKov1pDAxPcn7On2iQV_GunMVkTEXtx6qLHCQxstN70Bu_FCoH
8EyvNIdeW_gMIuj5vp_0u0VCUOKIB1aI3FfMiHbzoK2_W932F31TogxGpKRfWWGnjXm-COg",
  "expires_in": 300,
  "refresh_expires_in": 1800
```

- Request http://localhost:8080/api/company/list from resource server



http://localhost:8080/api/company/list

Authorization	u0VCUOKIB1aI3FfMiHbzoK2_W932F31TogxGpKRfWWGnjXm-COg

Response (0.051s) - http://localhost:8080/api/company/list

200

```
[
  {
    "id": 4,
    "name": "Company",
    "employees": [
      {
        "id": 2,
        "firstName": "Max1",
        "lastName": "Mustermann1",
        "email": "m1.m1@company.com",
        "birthDate": "2022-11-15T09:39:39.359+00:00"
      },
      {
        "id": 3,
        "firstName": "Max2",
        "lastName": "Mustermann2",
        "email": "m2.m2@company.com",
        "birthDate": "2022-11-15T09:39:39.362+00:00"
      },
      {
        "id": 1,
        "firstName": "Max0",
        "lastName": "Mustermann0",
        "email": "m0.m0@company.com",
        "birthDate": "2022-11-15T09:39:39.237+00:00"
      }
    ]
  }
```