

Quarkus - Using OpenID Connect to Protect Web Applications

This guide demonstrates how to use the OpenID Connect Extension to protect your application using Quarkus, where authentication and authorization are based on tokens issued by OpenID Connect and OAuth 2.0 compliant Authorization Servers such as [Keycloak](#).

The extension allows you to easily enable authentication to your web application based on the Authorization Code Flow so that your users are redirected to a OpenID Connect Provider (e.g.: Keycloak) to authenticate and, once the authentication is complete, return back to your application.

We are going to give you a guideline on how to use OpenID Connect to authenticate users using the Quarkus OpenID Connect Extension.

Prerequisites

To complete this guide, you need:

- less than 15 minutes
- an IDE
- JDK 1.8+ installed with `JAVA_HOME` configured appropriately
- Apache Maven 3.6.3
- [jq tool](#)
- Docker

Architecture

In this example, we build a very simple web application with a single page:

- `/index.html`

This page is protected and can only be accessed by authenticated users.

Solution

We recommend that you follow the instructions in the next sections and create the application step by step. However, you can go right to the completed example.

Clone the Git repository: `git clone https://github.com/quarkusio/quarkus-quickstarts.git`, or download an [archive](#).

The solution is located in the `security-openid-connect-web-authentication-quickstart` directory.

Creating the Maven Project

First, we need a new project. Create a new project with the following command:

```
mvn io.quarkus:quarkus-maven-plugin:1.5.1.Final:create \
    -DprojectId=org.acme \
    -DprojectArtifactId=security-openid-connect-web-authentication-quickstart \
    -Dextensions="oidc"
cd security-openid-connect-web-authentication-quickstart
```

If you already have your Quarkus project configured, you can add the `oidc` extension to your project by running the following command in your project base directory:

```
./mvnw quarkus:add-extension -Dextensions="oidc"
```

This will add the following to your `pom.xml`:

```
<dependency>
  <groupId>io.quarkus</groupId>
  <artifactId>quarkus-oidc</artifactId>
</dependency>
```

Configuring the application

The OpenID Connect extension allows you to define the configuration using the `application.properties` file which should be located at the `src/main/resources` directory.

Configuring using the `application.properties` file

```
quarkus.oidc.auth-server-
url=http://localhost:8180/auth/realms/quarkus
quarkus.oidc.client-id=frontend
quarkus.oidc.application-type=web-app
quarkus.http.auth.permission.authenticated.paths=/*
quarkus.http.auth.permission.authenticated.policy=authenticated
```

This is the simplest configuration you can have when enabling authentication to your application.

The `quarkus.oidc.client-id` property references the `client_id` issued by the OpenID Connect Provider and, in this case, the application is a public client (no client secret is defined).

The `quarkus.oidc.application-type` property is set to `web-app` in order to tell Quarkus that you want to enable the OpenID Connect Authorization Code Flow, so that your users are redirected to the OpenID Connect Provider to authenticate.

For last, the `quarkus.http.auth.permission.authenticated` permission is set to tell Quarkus about the paths you want to protect. In this case, all paths are being protected by a policy that ensures that only `authenticated` users are allowed to access. For more details check [Security Guide](#).

Starting and Configuring the Keycloak Server

To start a Keycloak Server you can use Docker and just run the following command:

```
docker run --name keycloak -e KEYCLOAK_USER=admin -e  
KEYCLOAK_PASSWORD=admin -p 8180:8080  
quay.io/keycloak/keycloak:10.0.2
```

You should be able to access your Keycloak Server at localhost:8180/auth.

Log in as the `admin` user to access the Keycloak Administration Console. Username should be `admin` and password `admin`.

Import the [realm configuration file](#) to create a new realm. For more details, see the Keycloak documentation about how to [create a new realm](#).

Running and Using the Application

Running in Developer Mode

To run the microservice in dev mode, use `./mvnw clean compile quarkus:dev`.

Running in JVM Mode

When you're done playing with "dev-mode" you can run it as a standard Java application.

First compile it:

```
./mvnw package
```

Then run it:

```
java -jar ./target/security-openid-connect-web-authentication-quickstart-runner.jar
```

Running in Native Mode

This same demo can be compiled into native code: no modifications required.

This implies that you no longer need to install a JVM on your production environment, as the runtime technology is included in the produced binary, and optimized to run with minimal resource overhead.

Compilation will take a bit longer, so this step is disabled by default; let's build again by enabling the **native** profile:

```
./mvnw package -Pnative
```

After getting a cup of coffee, you'll be able to run this binary directly:

```
./target/security-openid-connect-web-authentication-quickstart-runner
```

Testing the Application

To test the application, you should open your browser and access the following URL:

- <http://localhost:8080>

If everything is working as expected, you should be redirected to the Keycloak server to authenticate.

In order to authenticate to the application you should type the following credentials when at the Keycloak login page:

- Username: **alice**
- Password: **alice**

After clicking the **Login** button you should be redirected back to the application.

Logout

By default the logout is based on the expiration time of the ID Token issued by the OpenID Connect Provider. When the ID Token expires, the current user session at the Quarkus endpoint is invalidated and the user is redirected to the OpenID Connect Provider again to authenticate. If the session at the OpenID Connect Provider is still active, users are automatically re-authenticated without having to provide their credentials again.

The current user session may be automatically extended by enabling a `quarkus.oidc.token.refresh-expired` property. If it is set to `true` then when the current ID Token expires a Refresh Token Grant will be used to refresh ID Token as well as Access and Refresh Tokens.

User-Initiated Logout

Users can request a logout by sending a request to the Quarkus endpoint logout path set with a `quarkus.oidc.logout.path` property. For example, if the endpoint address is `https://application.com/webapp` and the `quarkus.oidc.logout.path` is set to `"/logout"` then the logout request has to be sent to `https://application.com/webapp/logout`.

This logout request will start an [RP-Initiated Logout](#) and the user will be redirected to the OpenID Connect Provider to logout where a user may be asked to confirm the logout is indeed intended.

The user will be returned to the endpoint post logout page once the logout has been completed if the `quarkus.oidc.logout.post-logout-path` property is set. For example, if the endpoint address is `https://application.com/webapp` and the `quarkus.oidc.logout.post-logout-path` is set to `"/signin"` then the user will be returned to `https://application.com/webapp/signin` (note this URI must be registered as a valid `post_logout_redirect_uri` in the OpenID Connect Provider).

If the `quarkus.oidc.logout.post-logout-path` is set then a `q_post_logout` cookie will be created and a matching `state` query parameter will be added to the logout redirect URI and the OpenID Connect Provider will return this `state` once the logout has been completed. It is recommended for the Quarkus `web-app` applications to check that a `state` query parameter matches the value of the `q_post_logout` cookie which can be done for example in a JAX-RS filter.

Note that a cookie name will vary when using [OpenID Connect Multi-Tenancy](#). For example, it will be named `q_post_logout_tenant_1` for a tenant with a `tenant_1` id, etc.

Accessing ID and Access Tokens

ID Token is always a JWT token. One can access ID Token claims by injecting `JsonWebToken` with an `IdToken` qualifier:

```
import javax.inject.Inject;
import org.eclipse.microprofile.jwt.JsonWebToken;
import io.quarkus.oidc.IdToken;
import io.quarkus.security.Authenticated;

@Path("/web-app")
@Authenticated
public class ProtectedResource {

    @Inject
    @IdToken
    JsonWebToken idToken;

    @GET
    public String getUsername() {
        return idToken.getName();
    }
}
```

Access Token is usually used by the OIDC **web-app** application to access other endpoints on behalf of the currently logged in user. The raw access token can be accessed as follows:

```

import javax.inject.Inject;
import org.eclipse.microprofile.jwt.JsonWebToken;
import io.quarkus.oidc.AccessTokenCredential;
import io.quarkus.security.Authenticated;

@Path("/web-app")
@Authenticated
public class ProtectedResource {

    @Inject
    JsonWebToken accessToken;

    // or
    // @Inject
    // AccessTokenCredential accessTokenCredential;

    @GET
    public String getReservationOnBehalfOfUser() {
        String rawAccessToken = accessToken.getRawToken();
        //or
        //String rawAccessToken = accessTokenCredential.getToken();


        // Use the raw access token to access a remote endpoint
        return getReservationfromRemoteEndpoint(rawAccessToken);
    }
}


```


Note that `AccessTokenCredential` will have to be used if the Access Token issued to the Quarkus `web-app` application is opaque (binary) and can not be parsed to `JsonWebToken`. However the opaque access tokens are not currently supported by the `web-app` applications.

Injection of the `JsonWebToken` and `AccessTokenCredential` is supported in both `@RequestScoped` and `@ApplicationScoped` contexts.

Configuration Reference

 Configuration property fixed at build time - All other configuration properties are overridable at runtime



Configuration property	Type	Default
 <code>quarkus.oidc.enabled</code> If the OIDC extension is enabled.	boolean	<code>true</code>

<code>quarkus.oidc.tenant-id</code>		
A unique tenant identifier. It must be set by <code>TenantConfigResolver</code> providers which resolve the tenant configuration dynamically and is optional in all other cases.	string	
<code>quarkus.oidc.tenant-enabled</code>		
If this tenant configuration is enabled.	boolean	<code>true</code>
<code>quarkus.oidc.application-type</code>		
The application type, which can be one of the following values from enum <code>ApplicationType</code> .	<code>web-app, service</code>	<code>service</code>
<code>quarkus.oidc.connection-delay</code>		
The maximum amount of time the adapter will try connecting to the currently unavailable OIDC server for. For example, setting it to '20S' will let the adapter keep requesting the connection for up to 20 seconds.	Duration 	
<code>quarkus.oidc.auth-server-url</code>		
The base URL of the OpenID Connect (OIDC) server, for example, 'https://host:port/auth'. OIDC discovery endpoint will be called by appending a '/.well-known/openid-configuration' path segment to this URL. Note if you work with Keycloak OIDC server, make sure the base URL is in the following format: 'https://host:port/auth/realms/{realm}' where '{realm}' has to be replaced by the name of the Keycloak realm.	string	
<code>quarkus.oidc.introspection-path</code>		
Relative path of the RFC7662 introspection service.	string	
<code>quarkus.oidc.jwks-path</code>		
Relative path of the OIDC service returning a JWK set.	string	
<code>quarkus.oidc.end-session-path</code>		
Relative path of the OIDC end_session_endpoint.	string	
<code>quarkus.oidc.public-key</code>		
Public key for the local JWT token verification.	string	

<code>quarkus.oidc.client-id</code>		
The client-id of the application. Each application has a client-id that is used to identify the application	string	
<code>quarkus.oidc.roles.role-claim-path</code>		
Path to the claim containing an array of groups. It starts from the top level JWT JSON object and can contain multiple segments where each segment represents a JSON object name only, example: "realm/groups". Use double quotes with the namespace qualified claim names. This property can be used if a token has no 'groups' claim but has the groups set in a different claim.	string	
<code>quarkus.oidc.roles.role-claim-separator</code>		
Separator for splitting a string which may contain multiple group values. It will only be used if the "role-claim-path" property points to a custom claim whose value is a string. A single space will be used by default because the standard 'scope' claim may contain a space separated sequence.	string	
<code>quarkus.oidc.token.issuer</code>		
Expected issuer 'iss' claim value.	string	
<code>quarkus.oidc.token.audience</code>		
Expected audience 'aud' claim value which may be a string or an array of strings.	list of string	
<code>quarkus.oidc.token.lifespan-grace</code>		
Life span grace period in seconds. When checking token expiry, current time is allowed to be later than token expiration time by at most the configured number of seconds. When checking token issuance, current time is allowed to be sooner than token issue time by at most the configured number of seconds.	int	
<code>quarkus.oidc.token.principal-claim</code>		
Name of the claim which contains a principal name. By default, the 'upn', 'preferred_username' and sub claims are checked.	string	
<code>quarkus.oidc.token.refresh-expired</code>		
Refresh expired ID tokens. If this property is enabled then a refresh token request is performed and, if successful, the local session is updated with the new set of tokens. Otherwise, the local session is invalidated as an indication that the session at the OpenID Provider no longer exists. This option is only valid when the application is of type ApplicationType#WEB_APP .	boolean	false


<code>quarkus.oidc.credentials.secret</code>		
Client secret which is used for a 'client_secret_basic' authentication method. Note that a 'client-secret.value' can be used instead but both properties are mutually exclusive.	string	
<code>quarkus.oidc.credentials.client-secret.value</code>		
The client secret	string	
<code>quarkus.oidc.credentials.client-secret.method</code>		
Authentication method.	basic, post	
<code>quarkus.oidc.credentials.jwt.secret</code>		
client_secret_jwt: JWT which includes client id as one of its claims is signed by the client secret and is submitted as a 'client_assertion' form parameter, while 'client_assertion_type' parameter is set to "urn:ietf:params:oauth:client-assertion-type:jwt-bearer".	string	
<code>quarkus.oidc.credentials.jwt.lifespan</code>		
JWT life-span in seconds. It will be added to the time it was issued at to calculate the expiration time.	int	10
<code>quarkus.oidc.proxy.host</code>		
The host (name or IP address) of the Proxy. Note: If OIDC adapter needs to use a Proxy to talk with OIDC server (Provider), then at least the "host" config item must be configured to enable the usage of a Proxy.	string	
<code>quarkus.oidc.proxy.port</code>		
The port number of the Proxy. Default value is 80.	int	80
<code>quarkus.oidc.proxy.username</code>		
The username, if Proxy needs authentication.	string	
<code>quarkus.oidc.proxy.password</code>		
The password, if Proxy needs authentication.	string	

<code>quarkus.oidc.authentication.redirect-path</code>		
Relative path for calculating a "redirect_uri" query parameter. It has to start from a forward slash and will be appended to the request URI's host and port. For example, if the current request URI is 'https://localhost:8080/service' then a 'redirect_uri' parameter will be set to 'https://localhost:8080/' if this property is set to '/' and be the same as the request URI if this property has not been configured. Note the original request URI will be restored after the user has authenticated.	string	
<code>quarkus.oidc.authentication.restore-path-after-redirect</code>		
If this property is set to 'true' then the original request URI which was used before the authentication will be restored after the user has been redirected back to the application.	boolean	true
<code>quarkus.oidc.authentication.remove-redirect-parameters</code>		
Remove the query parameters such as 'code' and 'state' set by the OIDC server on the redirect URI after the user has authenticated by redirecting a user to the same URI but without the query parameters.	boolean	true
<code>quarkus.oidc.authentication.force-redirect-https-scheme</code>		
Force 'https' as the 'redirect_uri' parameter scheme when running behind an SSL terminating reverse proxy. This property, if enabled, will also affect the logout <code>post_logout_redirect_uri</code> and the local redirect requests.	boolean	false
<code>quarkus.oidc.authentication.scopes</code>		
List of scopes	list of string	
<code>quarkus.oidc.authentication.cookie-path</code>		
Cookie path parameter value which, if set, will be used for the session and state cookies. It may need to be set when the redirect path has a root different to that of the original request URL.	string	
<code>quarkus.oidc.tls.verification</code>		
Certificate validation and hostname verification, which can be one of the following values from enum <code>Verification</code> . Default is required.	required, none	required
<code>quarkus.oidc.logout.path</code>		
The relative path of the logout endpoint at the application. If provided, the application is able to initiate the logout through this endpoint in conformance with the OpenID Connect RP-Initiated Logout specification.	string	

<code>quarkus.oidc.logout.post-logout-path</code>		
Relative path of the application endpoint where the user should be redirected to after logging out from the OpenID Connect Provider. This endpoint URI must be properly registered at the OpenID Connect Provider as a valid redirect URI.	string	
<code>quarkus.oidc.authentication.extra-params</code>	<code>Map<String, String></code>	required 
Additional properties which will be added as the query parameters to the authentication redirect URI.		
Additional named tenants	Type	Default
<code>quarkus.oidc."tenant".tenant-id</code>		
A unique tenant identifier. It must be set by <code>TenantConfigResolver</code> providers which resolve the tenant configuration dynamically and is optional in all other cases.	string	
<code>quarkus.oidc."tenant".tenant-enabled</code>		
If this tenant configuration is enabled.	boolean	<code>true</code>
<code>quarkus.oidc."tenant".application-type</code>	<code>web-app, service</code>	<code>service</code>
The application type, which can be one of the following values from enum <code>ApplicationType</code> .		
<code>quarkus.oidc."tenant".connection-delay</code>		
The maximum amount of time the adapter will try connecting to the currently unavailable OIDC server for. For example, setting it to '20S' will let the adapter keep requesting the connection for up to 20 seconds.	<code>Duration</code> 	
<code>quarkus.oidc."tenant".auth-server-url</code>		
The base URL of the OpenID Connect (OIDC) server, for example, 'https://host:port/auth'. OIDC discovery endpoint will be called by appending a '/.well-known/openid-configuration' path segment to this URL. Note if you work with Keycloak OIDC server, make sure the base URL is in the following format: 'https://host:port/auth/realms/{realm}' where '{realm}' has to be replaced by the name of the Keycloak realm.	string	
<code>quarkus.oidc."tenant".introspection-path</code>		
Relative path of the RFC7662 introspection service.	string	

<code>quarkus.oidc."tenant".jwks-path</code>	string	
Relative path of the OIDC service returning a JWK set.		
<code>quarkus.oidc."tenant".end-session-path</code>	string	
Relative path of the OIDC end_session_endpoint.		
<code>quarkus.oidc."tenant".public-key</code>	string	
Public key for the local JWT token verification.		
<code>quarkus.oidc."tenant".client-id</code>	string	
The client-id of the application. Each application has a client-id that is used to identify the application		
<code>quarkus.oidc."tenant".roles.role-claim-path</code>	string	
Path to the claim containing an array of groups. It starts from the top level JWT JSON object and can contain multiple segments where each segment represents a JSON object name only, example: "realm/groups". Use double quotes with the namespace qualified claim names. This property can be used if a token has no 'groups' claim but has the groups set in a different claim.		
<code>quarkus.oidc."tenant".roles.role-claim-separator</code>	string	
Separator for splitting a string which may contain multiple group values. It will only be used if the "role-claim-path" property points to a custom claim whose value is a string. A single space will be used by default because the standard 'scope' claim may contain a space separated sequence.		
<code>quarkus.oidc."tenant".token.issuer</code>	string	
Expected issuer 'iss' claim value.		
<code>quarkus.oidc."tenant".token.audience</code>	list of string	
Expected audience 'aud' claim value which may be a string or an array of strings.		
<code>quarkus.oidc."tenant".token.lifespan-grace</code>	int	
Life span grace period in seconds. When checking token expiry, current time is allowed to be later than token expiration time by at most the configured number of seconds. When checking token issuance, current time is allowed to be sooner than token issue time by at most the configured number of seconds.		

<code>quarkus.oidc."tenant".token.principal-claim</code>		
Name of the claim which contains a principal name. By default, the 'upn', 'preferred_username' and sub claims are checked.	string	
<code>quarkus.oidc."tenant".token.refresh-expired</code>		
Refresh expired ID tokens. If this property is enabled then a refresh token request is performed and, if successful, the local session is updated with the new set of tokens. Otherwise, the local session is invalidated as an indication that the session at the OpenID Provider no longer exists. This option is only valid when the application is of type ApplicationType#WEB_APP .	boolean	false
<code>quarkus.oidc."tenant".credentials.secret</code>		
Client secret which is used for a 'client_secret_basic' authentication method. Note that a 'client-secret.value' can be used instead but both properties are mutually exclusive.	string	
<code>quarkus.oidc."tenant".credentials.client-secret.value</code>		
The client secret	string	
<code>quarkus.oidc."tenant".credentials.client-secret.method</code>		
Authentication method.	basic, post	
<code>quarkus.oidc."tenant".credentials.jwt.secret</code>		
client_secret_jwt: JWT which includes client id as one of its claims is signed by the client secret and is submitted as a 'client_assertion' form parameter, while 'client_assertion_type' parameter is set to "urn:ietf:params:oauth:client-assertion-type:jwt-bearer".	string	
<code>quarkus.oidc."tenant".credentials.jwt.lifespan</code>		
JWT life-span in seconds. It will be added to the time it was issued at to calculate the expiration time.	int	10
<code>quarkus.oidc."tenant".proxy.host</code>		
The host (name or IP address) of the Proxy. Note: If OIDC adapter needs to use a Proxy to talk with OIDC server (Provider), then at least the "host" config item must be configured to enable the usage of a Proxy.	string	
<code>quarkus.oidc."tenant".proxy.port</code>		
The port number of the Proxy. Default value is 80.	int	80

<code>quarkus.oidc."tenant".proxy.username</code>	string	
The username, if Proxy needs authentication.		
<code>quarkus.oidc."tenant".proxy.password</code>	string	
The password, if Proxy needs authentication.		
<code>quarkus.oidc."tenant".authentication.redirect-path</code>	string	
Relative path for calculating a "redirect_uri" query parameter. It has to start from a forward slash and will be appended to the request URI's host and port. For example, if the current request URI is 'https://localhost:8080/service' then a 'redirect_uri' parameter will be set to 'https://localhost:8080/' if this property is set to '/' and be the same as the request URI if this property has not been configured. Note the original request URI will be restored after the user has authenticated.		
<code>quarkus.oidc."tenant".authentication.restore-path-after-redirect</code>	boolean	true
If this property is set to 'true' then the original request URI which was used before the authentication will be restored after the user has been redirected back to the application.		
<code>quarkus.oidc."tenant".authentication.remove-redirect-parameters</code>	boolean	true
Remove the query parameters such as 'code' and 'state' set by the OIDC server on the redirect URI after the user has authenticated by redirecting a user to the same URI but without the query parameters.		
<code>quarkus.oidc."tenant".authentication.force-redirect-https-scheme</code>	boolean	false
Force 'https' as the 'redirect_uri' parameter scheme when running behind an SSL terminating reverse proxy. This property, if enabled, will also affect the logout <code>post_logout_redirect_uri</code> and the local redirect requests.		
<code>quarkus.oidc."tenant".authentication.scopes</code>	list of string	
List of scopes		
<code>quarkus.oidc."tenant".authentication.extra-params</code>	Map<String, String>	required 
Additional properties which will be added as the query parameters to the authentication redirect URI.		

<code>quarkus.oidc."tenant".authentication.cookie-path</code>	string	
Cookie path parameter value which, if set, will be used for the session and state cookies. It may need to be set when the redirect path has a root different to that of the original request URL.		
<code>quarkus.oidc."tenant".tls.verification</code>	required, none	required
Certificate validation and hostname verification, which can be one of the following values from enum <code>Verification</code> . Default is required.		
<code>quarkus.oidc."tenant".logout.path</code>	string	
The relative path of the logout endpoint at the application. If provided, the application is able to initiate the logout through this endpoint in conformance with the OpenID Connect RP-Initiated Logout specification.		
<code>quarkus.oidc."tenant".logout.post-logout-path</code>	string	
Relative path of the application endpoint where the user should be redirected to after logging out from the OpenID Connect Provider. This endpoint URI must be properly registered at the OpenID Connect Provider as a valid redirect URI.		



About the Duration format

The format for durations uses the standard `java.time.Duration` format. You can learn more about it in the [Duration#parse\(\) javadoc](#).

You can also provide duration values starting with a number. In this case, if the value consists only of a number, the converter treats the value as seconds. Otherwise, `PT` is implicitly prepended to the value to obtain a standard `java.time.Duration` format.

References

- [Keycloak Documentation](#)
- [OpenID Connect](#)
- [JSON Web Token](#)