

# Quarkus - HTTP Reference

This document explains various HTTP features that you can use in Quarkus.

HTTP is provided using Eclipse Vert.x as the base HTTP layer. Servlet's are supported using a modified version of Undertow that runs on top of Vert.x, and RESTEasy is used to provide JAX-RS support. If Undertow is present RESTEasy will run as a Servlet filter, otherwise it will run directly on top of Vert.x with no Servlet involvement.

## 1. Serving Static Resources

To serve static resources you must place them in the `META-INF/resources` directory of your application. This location was chosen as it is the standard location for resources in `jar` files as defined by the Servlet spec. Even though Quarkus can be used without Servlet following this convention allows existing code that places its resources in this location to function correctly.

### 1.1. WebJar Locator Support

If you are using webjars, like the following JQuery one

```
<dependency>
  <groupId>org.webjars</groupId>
  <artifactId>jquery</artifactId>
  <version>3.1.1</version>
</dependency>
```

and rather write `/webjars/jquery/jquery.min.js` instead of `/webjars/jquery/3.1.1/jquery.min.js` in your HTML files, you can add the `quarkus-webjars-locator` extension to your project. To use it, add the following to your project's dependencies:

```
<dependency>
  <groupId>io.quarkus</groupId>
  <artifactId>quarkus-webjars-locator</artifactId>
</dependency>
```

## 2. Configuring the Context path

By default Quarkus will serve content from under the root context. If you want to change this you can use the `quarkus.http.root-path` config key to set the context path.

If you are using Servlet you can control the Servlet context path via `quarkus.servlet.context-path`. This item is relative to the http root above, and will only affect Servlet and things that run on top of Servlet. Most applications will want to use the HTTP root as this affects everything that Quarkus

serves.

If both are specified then all non-Servlet web endpoints will be relative to `quarkus.http.root-path`, while Servlet's will be served relative to `{quarkus.http.root-path}/{quarkus.servlet.context-path}`.

If REST Assured is used for testing and `quarkus.http.root-path` is set then Quarkus will automatically configure the base URL for use in Quarkus tests, so test URL's should not include the root path.

## 3. Supporting secure connections with SSL

In order to have Quarkus support secure connections, you must either provide a certificate and associated key file, or supply a keystore.

In both cases, a password must be provided. See the designated paragraph for a detailed description of how to provide it.



To enable SSL support with native executables, please refer to our [Using SSL With Native Executables guide](#).

### 3.1. Providing a certificate and key file

If the certificate has not been loaded into a keystore, it can be provided directly using the properties listed below. Quarkus will first try to load the given files as resources, and uses the filesystem as a fallback. The certificate / key pair will be loaded into a newly created keystore on startup.

Your `application.properties` would then look like this:

```
quarkus.http.ssl.certificate.file=/path/to/certificate
quarkus.http.ssl.certificate.key-file=/path/to/key
```

### 3.2. Providing a keystore

An alternate solution is to directly provide a keystore which already contains a default entry with a certificate. You will need to at least provide the file and a password.

As with the certificate/key file combination, Quarkus will first try to resolve the given path as a resource, before attempting to read it from the filesystem.

Add the following property to your `application.properties`:

```
quarkus.http.ssl.certificate.key-store-file=/path/to/keystore
```

As an optional hint, the type of keystore can be provided as one of the options listed. If the type is not provided, Quarkus will try to deduce it from the file extensions, defaulting to type JKS.

```
quarkus.http.ssl.certificate.key-store-file-type=[one of JKS,
JCEKS, P12, PKCS12, PFX]
```

### 3.3. Setting the password

In both aforementioned scenarios, a password needs to be provided to create/load the keystore with. The password can be set in your `application.properties` (in plain-text) using the following property:

```
quarkus.http.ssl.certificate.key-store-password=your-password
```

However, instead of providing the password as plain-text in the configuration file (which is considered bad practice), it can instead be supplied (using [MicroProfile config](#)) as the environment variable `QUARKUS_HTTP_SSL_CERTIFICATE_KEY_STORE_PASSWORD`. This will also work in tandem with [Kubernetes secrets](#).

*Note: in order to remain compatible with earlier versions of Quarkus (before 0.16) the default password is set to "password". It is therefore not a mandatory parameter!*

### 3.4. Disable the HTTP port

It is possible to disable the HTTP port and only support secure requests. This is done via the `quarkus.http.insecure-requests` property in `application.properties`. There are three possible values:

#### **enabled**

The default, HTTP works as normal

#### **redirect**

HTTP requests will be redirected to the HTTPS port

#### **disabled**

The HTTP port will not be opened.



if you use `redirect` or `disabled` and have not added a SSL certificate or keystore, your server will not start!

## 4. HTTP/2 Support

HTTP/2 is enabled by default, and will be used by browsers if SSL is in use on JDK11 or higher. JDK8 does not support ALPN so cannot be used to run HTTP/2 over SSL. Even if SSL is not in use HTTP/2 via cleartext upgrade is supported, and may be used by non-browser clients.

If you want to disable HTTP/2 you can set:

```
quarkus.http.http2=false
```

## 5. CORS filter

[Cross-origin resource sharing](#) (CORS) is a mechanism that allows restricted resources on a web page to be requested from another domain outside the domain from which the first resource was served.

Quarkus comes with a CORS filter which implements the `javax.servlet.Filter` interface and intercepts all incoming HTTP requests. It can be enabled in the Quarkus configuration file, `src/main/resources/application.properties`:

```
quarkus.http.cors=true
```

If the filter is enabled and an HTTP request is identified as cross-origin, the CORS policy and headers defined using the following properties will be applied before passing the request on to its actual target (servlet, JAX-RS resource, etc.):

| Property Name   | Default | Description  |
|---|---------|--|
| <code>quarkus.http.cors.origins</code>                          |         | The comma-separated list of origins allowed for CORS. The filter allows any origin if this is not set.   |
| <code>quarkus.http.cors.methods</code>                          |         | The comma-separated list of HTTP methods allowed for CORS. The filter allows any method if this is not set.  |
| <code>quarkus.http.cors.headers</code>                          |         | The comma-separated list of HTTP headers allowed for CORS. The filter allows any header if this is not set.  |
| <code>quarkus.http.cors.exposed-headers</code>                  |         | The comma-separated list of HTTP headers exposed in CORS.  |
| <code>quarkus.http.cors.access-control-max-age</code>           |         | The duration (see note below) indicating how long the results of a pre-flight request can be cached. This value will be returned in a <code>Access-Control-Max-Age</code> response header. |
| <code>quarkus.http.cors.access-control-allow-credentials</code> |         | Boolean value to tell the browsers to expose the response to front-end JavaScript code when the request's credentials mode <code>Request.credentials</code> is "include"                   |

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.

Here's what a full CORS filter configuration could look like:

```
quarkus.http.cors=true
quarkus.http.cors.origins=http://foo.com,http://www.bar.io
quarkus.http.cors.methods=GET,PUT,POST
quarkus.http.cors.headers=X-Custom
quarkus.http.cors.exposed-headers=Content-Disposition
quarkus.http.cors.access-control-max-age=24H
quarkus.http.cors.access-control-allow-credentials=true
```

## 6. HTTP Limits Configuration

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

| Configuration property  | Type        | Default |
|---|-------------|---------|
| <code>quarkus.http.limits.max-header-size</code><br>The maximum length of all headers.                                      | Memory Size | 20K     |
| <code>quarkus.http.limits.max-body-size</code><br>The maximum size of a request body.                                       | Memory Size | 10240K  |
| <code>quarkus.http.limits.max-chunk-size</code><br>The max HTTP chunk size  | Memory Size | 8192    |
| <code>quarkus.http.limits.max-initial-line-length</code><br>The maximum length of the initial line (e.g. "GET / HTTP/1.0"). | int         | 4096    |



*About the MemorySize format*

A size configuration option recognises string in this format (shown as a regular expression): `[0-9]+[KkMmGgTtPpEeZzYy]?`. If no suffix is given, assume bytes.

## 7. Configuring HTTP Access Logs

You can add HTTP request logging by configuring it in `application.properties`. There are two options for logging, either logging to the standard JBoss logging output, or logging to a dedicated file.

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

| Configuration property  | Type    | Default                                 |
|---|---------|---|
| <code>quarkus.http.access-log.enabled</code><br>If access logging is enabled. By default this will log via the standard logging facility  | boolean | <code>false</code>                      |
| <code>quarkus.http.access-log.pattern</code><br>The access log pattern: If this is the string 'common', 'combined' or 'long' then this will use one of the specified named formats: - common: %h %l %u %t "%r" %s %b - combined: %h %l %u %t "%r" %s %b "%{i,Referer}" "%{i,User-Agent}" - long: %r %{ALL_REQUEST_HEADERS} Otherwise consult the Quarkus documentation for the full list of variables that can be used. | string  | <code>common</code>                     |
| <code>quarkus.http.access-log.log-to-file</code><br>If logging should be done to a separate file.   | boolean | <code>false</code>                      |
| <code>quarkus.http.access-log.base-file-name</code><br>The access log file base name, defaults to 'quarkus' which will give a log file name of 'quarkus.log'.   | string  | <code>quarkus</code>                    |
| <code>quarkus.http.access-log.log-directory</code><br>The log directory to use when logging access to a file If this is not set then the current working directory is used.   | string  |   |
| <code>quarkus.http.access-log.log-suffix</code><br>The log file suffix  | string  | <code>.log</code>                       |
| <code>quarkus.http.access-log.category</code><br>The log category to use if logging is being done via the standard log mechanism (i.e. if base-file-name is empty).   | string  | <code>io.quarkus.http.access-log</code> |

|   |         |                   |
|---|---------|-------------------|
| <code>quarkus.http.access-log.rotate</code> |         |                   |
| If the log should be rotated daily          | boolean | <code>true</code> |

| Attribute   | Short Form      | Long Form                            |
|---|-----------------|--------------------------------------|
| Remote IP address   | <code>%a</code> | <code>%{REMOTE_IP}</code>            |
| Local IP address  | <code>%A</code> | <code>%{LOCAL_IP}</code>             |
| Bytes sent, excluding HTTP headers, or '-' if no bytes were sent            | <code>%b</code> |                                      |
| Bytes sent, excluding HTTP headers  | <code>%B</code> | <code>%{BYTES_SENT}</code>           |
| Remote host name  | <code>%h</code> | <code>%{REMOTE_HOST}</code>          |
| Request protocol  | <code>%H</code> | <code>%{PROTOCOL}</code>             |
| Request method  | <code>%m</code> | <code>%{METHOD}</code>               |
| Local port  | <code>%p</code> | <code>%{LOCAL_PORT}</code>           |
| Query string (prepended with a '?' if it exists, otherwise an empty string) | <code>%q</code> | <code>%{QUERY_STRING}</code>         |
| First line of the request   | <code>%r</code> | <code>%{REQUEST_LINE}</code>         |
| HTTP status code of the response  | <code>%s</code> | <code>%{RESPONSE_CODE}</code>        |
| Date and time, in Common Log Format format                                  | <code>%t</code> | <code>%{DATE_TIME}</code>            |
| Remote user that was authenticated  | <code>%u</code> | <code>%{REMOTE_USER}</code>          |
| Requested URL path  | <code>%U</code> | <code>%{REQUEST_URL}</code>          |
| Request relative path   | <code>%R</code> | <code>%{RELATIVE_PATH}</code>        |
| Local server name   | <code>%v</code> | <code>%{LOCAL_SERVER_NAME}</code>    |
| Time taken to process the request, in millis                                | <code>%D</code> | <code>%{RESPONSE_TIME}</code>        |
| Time taken to process the request, in seconds                               | <code>%T</code> |                                      |
| Time taken to process the request, in micros                                |                 | <code>%{RESPONSE_TIME_MICROS}</code> |

| Attribute                                   | Short Form      | Long Form   |
|---|-----------------|---|
| Time taken to process the request, in nanos |                 | <code>%{RESPONSE_TIME_NANOS}</code>                       |
| Current request thread name                 | <code>%I</code> | <code>%{THREAD_NAME}</code>                               |
| SSL cypher                                  |                 | <code>%{SSL_CIPHER}</code>                                |
| SSL client certificate                      |                 | <code>%{SSL_CLIENT_CERT}</code>                           |
| SSL session id                              |                 | <code>%{SSL_SESSION_ID}</code>                            |
| All request headers                         |                 | <code>%{ALL_REQUEST_HEADERS}</code>                       |
| Cookie value                                |                 | <code>%{c, cookie_name}</code>                            |
| Query parameter                             |                 | <code>%{q, query_param_name}</code>                       |
| Request header                              |                 | <code>%{i, request_header_name}</code><br><code>}</code>  |
| Response header                             |                 | <code>%{o, response_header_name}</code><br><code>}</code> |

## 8. Servlet Config

To use Servlet you need to explicitly include `quarkus-undertow`:

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

### 8.1. undertow-handlers.conf

You can make use of the Undertow predicate language using an `undertow-handlers.conf` file. This file should be placed in the `META-INF` directory of your application jar. This file contains handlers defined using the [Undertow predicate language](#).

### 8.2. web.xml

If you are using a `web.xml` file as your configuration file, you can place it in the `src/main/resources/META-INF` directory.