Qvu Data Service

Getting Started

Updated: 10/13/2023

1. Ensure java 17 or higher is installed on the server that will run Qvu.
2. Download the Qvu application from http://rbtdesign.org
3. Create the server-side folder that will be house the Qvu repository.
4. Start the Qvu application by running the following command:

   ```
   java -jar qvu.jar
   ```

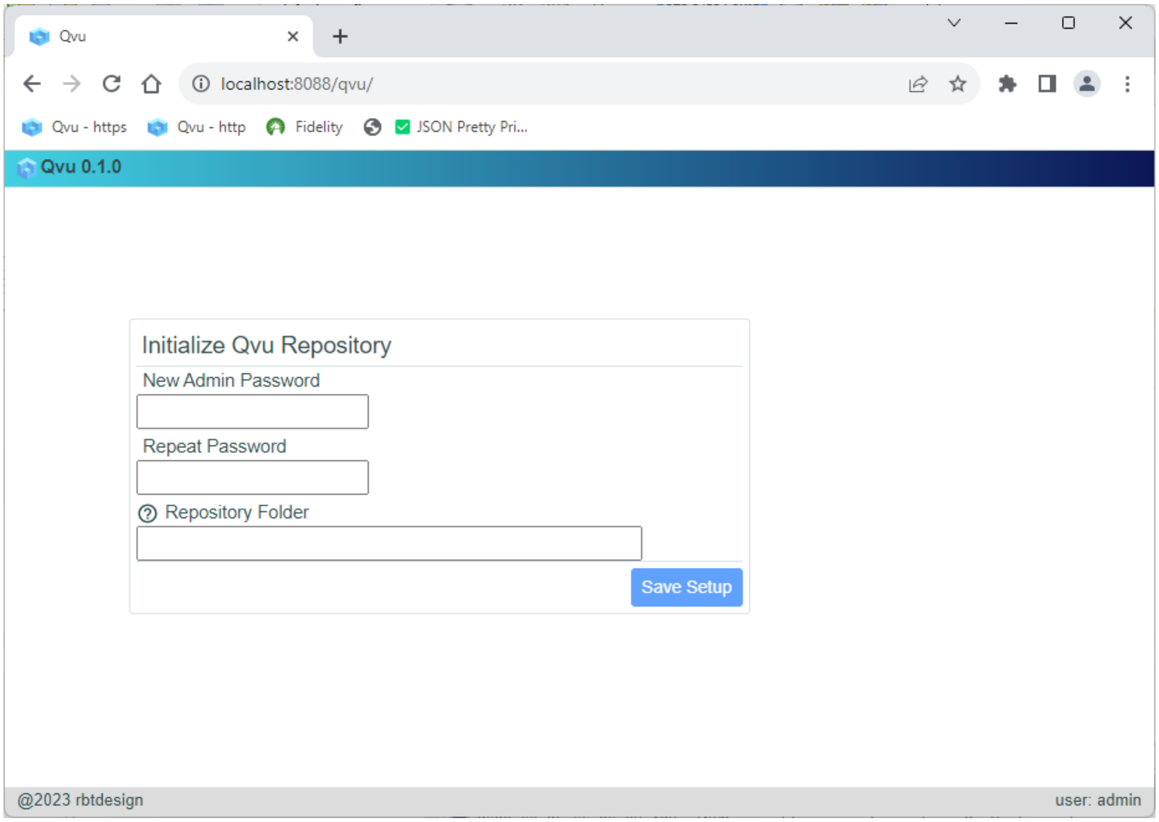
5. Once the application starts, pull up the initialization page by going to

   http://localhost:8088/qvu

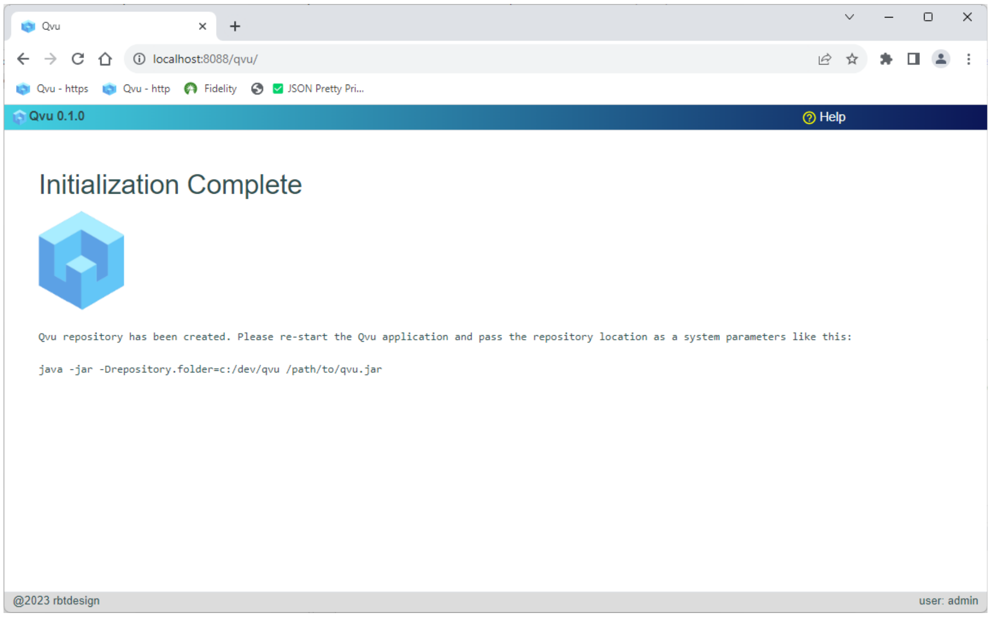
   and logging in with:

   username: admin
   password: admin

   - the initialization screen shown below should display:



6. Enter a new admin password and the repository folder created in step 3.
7. Click “Save Setup” – if Qvu was successfully initialized you should see a message similar to the following:



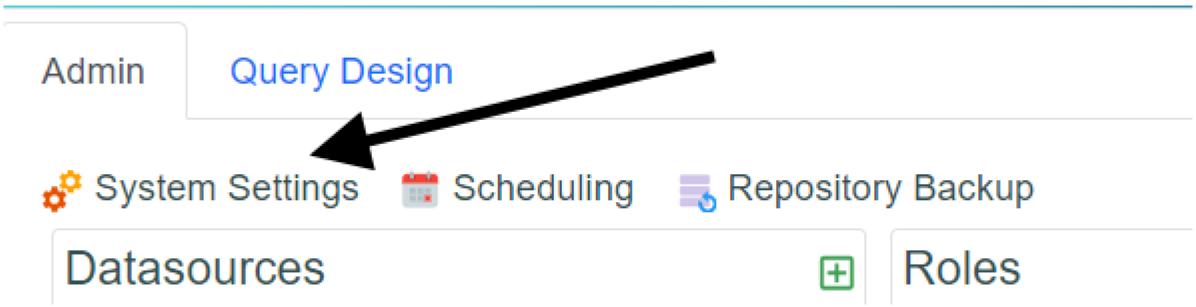
Initialization Complete

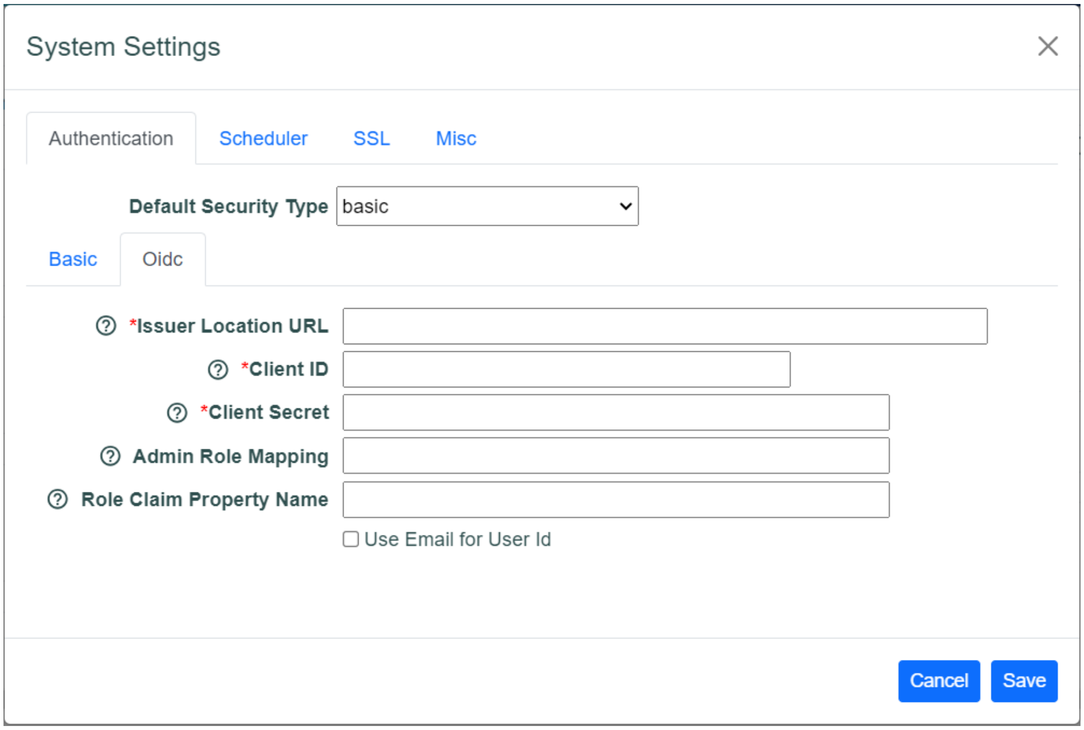
Qvu repository has been created. Please re-start the Qvu application and pass the repository location as a system parameters like this:

```
java -jar -Drepository.folder=c:/dev/qvu /path/to/qvu.jar
```

8. Once initialization is complete, stop the application and restart passing the repository folder location as a system parameter as follows:
   java -jar -Drepository.folder=/my/repository/location qvu.jar
   By default, Qvu log level is set to INFO. You can change this by passing the log level as a startup parameter -Dlog.level=<desired level> - DEBUG, WARN ERROR etc.
9. Pull up the application at http://localhost:8088/qvu, login with username=admin and password=<new password> and you should see the administration page displayed:

By default basic authentication is used and users and roles are stored as json in the file <repository.folder>/config/qvu-security.json. Qvu supports OIDC and Basic authentication. You can change this setup by clicking the System Settings icon in the admin tab.





System Settings

Default Security Type: basic

Ⓘ *Issuer Location URL:

Ⓘ *Client ID:

Ⓘ *Client Secret:

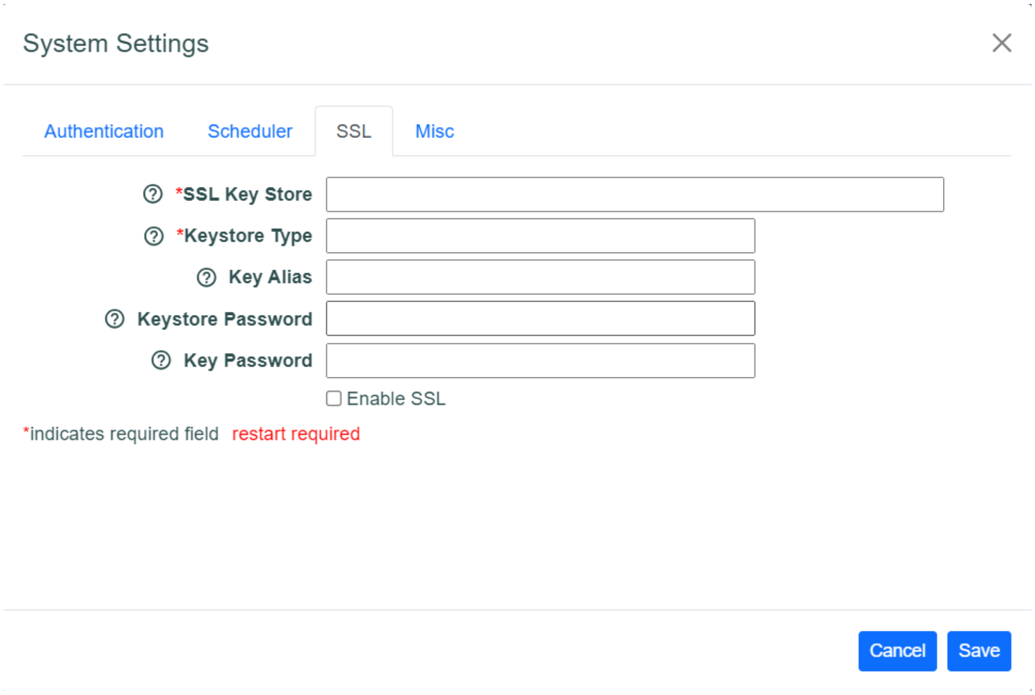
Ⓘ Admin Role Mapping:

Ⓘ Role Claim Property Name:

□ Use Email for User Id

Once changed you will have to restart the application. You can also implement your own customized security. See the help documentation for more information on this process.

If you wish to enable SSL, click the Systems Settings icon and go to the SSL tab. Enter the appropriate information then restart the application.



System Settings

*SSL Key Store

*Keystore Type

Key Alias

Keystore Password

Key Password

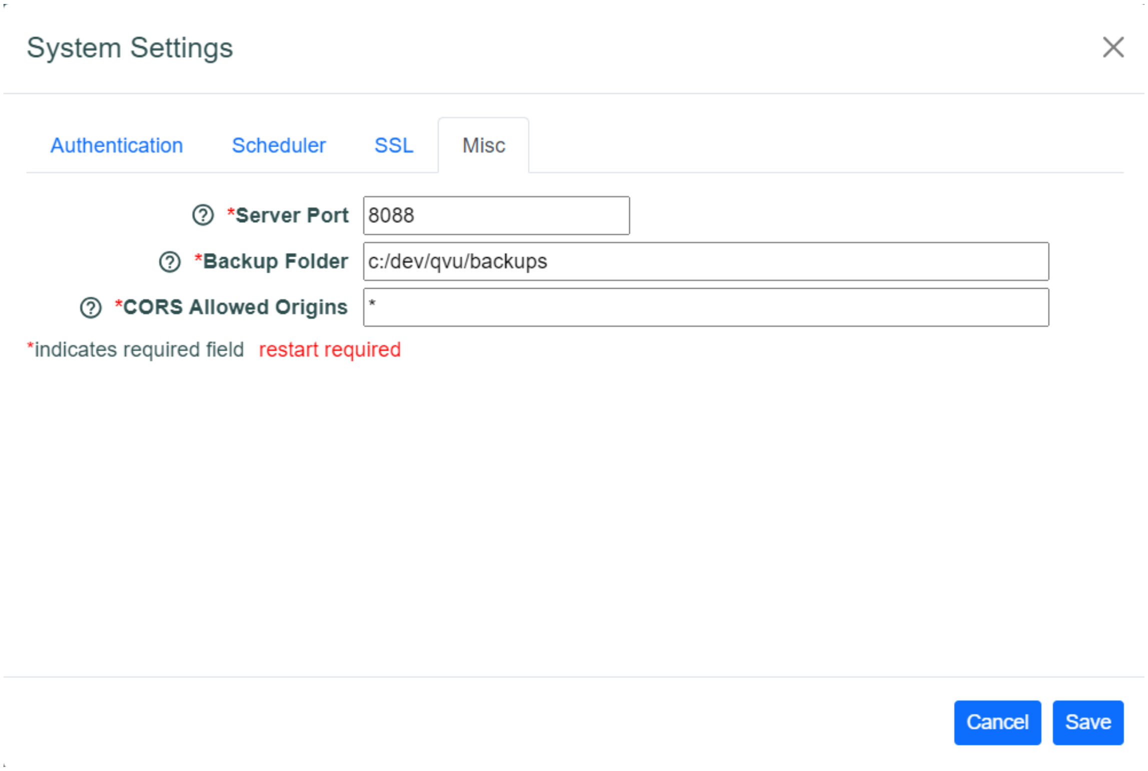
□ Enable SSL

*indicates required field restart required

The SSL entries in the SSL tab correspond to the Spring Boot application.properties for SSL shown below:

- server.ssl.enabled
- server.ssl.key-store
- server.ssl.key-store-type
- server.ssl.key-alias
- server.ssl.key-store-password
- server.ssl.key-password

You will probably also want to change the server port property at the same time – this is found on the Systems Settings Misc tab:



System Settings

*Server Port 8088

*Backup Folder c:/dev/qvu/backups

*CORS Allowed Origins *

*indicates required field restart required