



iQ.Suite KeyManager

Configuration of a Remote H2 Database

Document Version 1.3

Contents

1	System Requirements	3
2	Procedure in case of a new KeyManager Installation	4
2.1	First Steps	4
2.2	Creating the H2 Database	5
2.2.1	Procedure with the H2 Console	5
2.2.2	Procedure with a Command Line.....	6
2.3	Procedure in case of an existing KeyManager Installation	9
3	About GBS.....	12

1 System Requirements

For information about the system requirements of iQ.Suite KeyManager and the supported versions of the H2 database, please refer to the KeyManager manual.

2 Procedure in case of a new KeyManager Installation

In the following description, the following applies:

- iQ.Suite KeyManager Version 6 or higher is installed under:
C:\Program Files\GBS\KeyManager.
- The database is located on the same computer than KeyManager. The database can also be created locally and copied to another computer, or it can be created directly on another computer.

For example 1, a directory C:\H2 containing the database program and the database has been created.

For example 2, a directory C:\H2 with the sub-directory bin for the database program and the sub-directory data for the database has been created.

- The user 'kms-user' with the database password 'dbpass' and the encryption password 'encpass' is used for the database.
- The default port for the database program is '9092'.

Note: All H2 program calls should be made from the directory in which the database is located. In other cases, all paths to the database must be specified relatively to the call directory. Especially note that the database is always started from the directory which was used when the database was set up in KeyManager. Otherwise, it must be reconfigured in KeyManager.

2.1 First Steps

1. Run the KeyManager setup.

Note: If possible, do not start the KeyManager server at the end of the installation. Otherwise, the default database would be created.

For the database name, you can keep the default setting. It can be changed later.

2. Stop the iQ.Suite KeyManager Service.
3. Unpack the **km.backend.war** file located under
C:\Program Files\GBS\KeyManager\keymanager\km-base\webapps\ and copy the **WEB-INF\lib\h2-1.4.199.jar** to the target directory.

Note: The JAR file version can differ. It could be, for example, *h2-1.4.202.jar* or other.

Example 1: Copy *h2-1.4.199.jar* to C:\H2.

Example 2: Copy *h2-1.4.199.jar* to `C:\H2\bin`.

4. Delete or rename the **kms.fe.preconfigured.conf** file under
`C:\Program Files\GBS\KeyManager\etc\`

This is required to get the Database Configuration dialog after starting the KeyManager server.
Otherwise, the default database will be created.

5. Create the database.

2.2 Creating the H2 Database

You have two possibilities to create the H2 database:

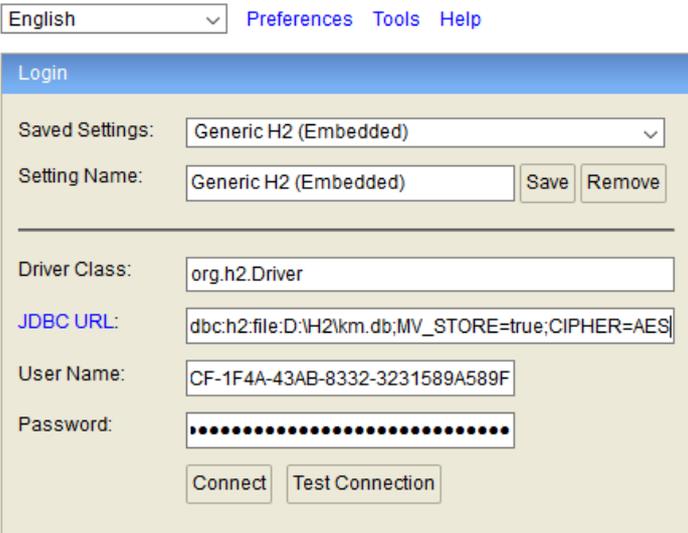
- Using the H2 Console
- Using a command line

2.2.1 Procedure with the H2 Console

1. In the command prompt, enter the following command line:

```
"C:\Program Files\GBS\KeyManager\openjdk\bin\java.exe" -cp "h2-1.4.199.jar"  
org.h2.tools.Console
```

The H2 Console will open.



Examples for **JDBC URL**:

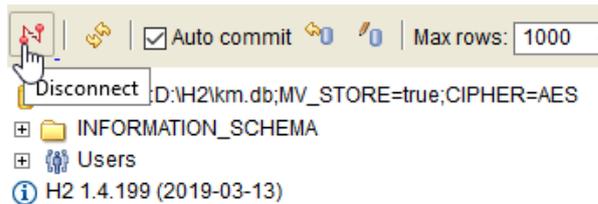
Example 1: `jdbc:h2:file:C:\H2\km.db_mv;CIPHER=AES`

Example 2: jdbc:h2:file:C:\H2\data\km.db_mv;CIPHER=AES

2. Enter the database **username** 'kms-user' and **password** 'dbpass encpass'.
3. Click CONNECT.

The database will be created.

4. In the H2 Console, disconnect and close the H2 Console:



5. In the Task Manager, stop the **javaw.exe** task if it is still running.

2.2.2 Procedure with a Command Line

Example 1:

```
cd \H2
```

```
"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -cp "h2-1.4.199.jar"
org.h2.tools.Shell -url "jdbc:h2:file:./km.db_mv;CIPHER=AES" -user "kms-user"
-password "dbpass encpass"
```

Example 2:

```
cd \H2\data
```

```
"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -cp "C:\H2\bin\
h2-1.4.199.jar" org.h2.tools.Shell -url "jdbc:h2:file:./km.db_mv;CIPHER=AES" -user
"kms-user" -password "dbpass encpass"
```

```
c:\H2>cd \h2\data
c:\H2\data>"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -cp "C:\H2\bin\h2-1.4.199.jar" org.h2.tools.Shell -url
"jdbc:h2:file:./km.db_mv;CIPHER=AES" -user "kms-user" -password "dbpass encpass"
Welcome to H2 Shell 1.4.199 (2019-03-13)
Exit with Ctrl+C
Commands are case insensitive; SQL statements end with ';'
help or ?      Display this help
list           Toggle result list / stack trace mode
maxwidth       Set maximum column width (default is 100)
autocommit     Enable or disable autocommit
history        Show the last 20 statements
quit or exit   Close the connection and exit

sql> exit
Connection closed
```

1. Start the H2 database program:

Example 1:

```
cd \H2
```

```
"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -Xmx1024M -Xms256M  
-jar h2-1.4.199.jar -web -webAllowOthers -tcp -tcpAllowOthers
```

Example 2:

```
cd \H2\data
```

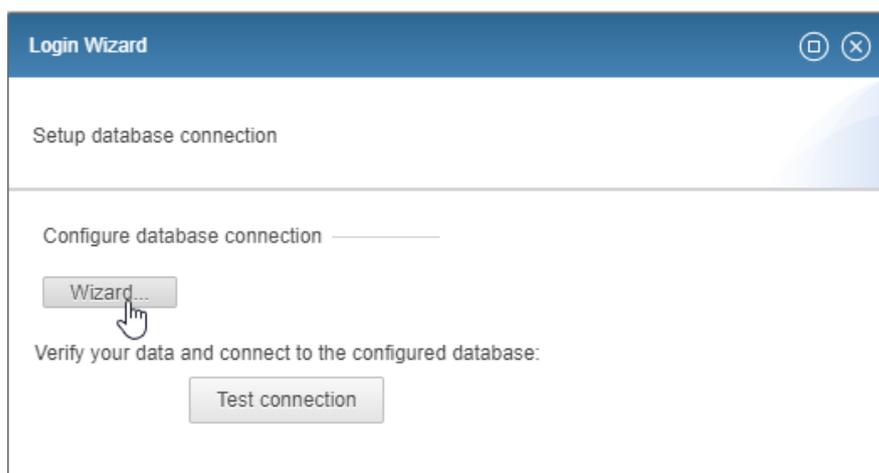
```
"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -Xmx1024M -Xms256M  
-jar ..\bin\h2-1.4.199.jar -web -webAllowOthers -tcp -tcpAllowOthers
```

```
c:\H2\data>"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -Xmx1024M -Xms256M -jar ..\bin\h2-1.4.199.jar -web -w  
ebAllowOthers -tcp -tcpAllowOthers  
Web Console server running at http://172.30.200.53:8082 (others can connect)  
TCP server running at tcp://172.30.200.53:9092 (others can connect)
```

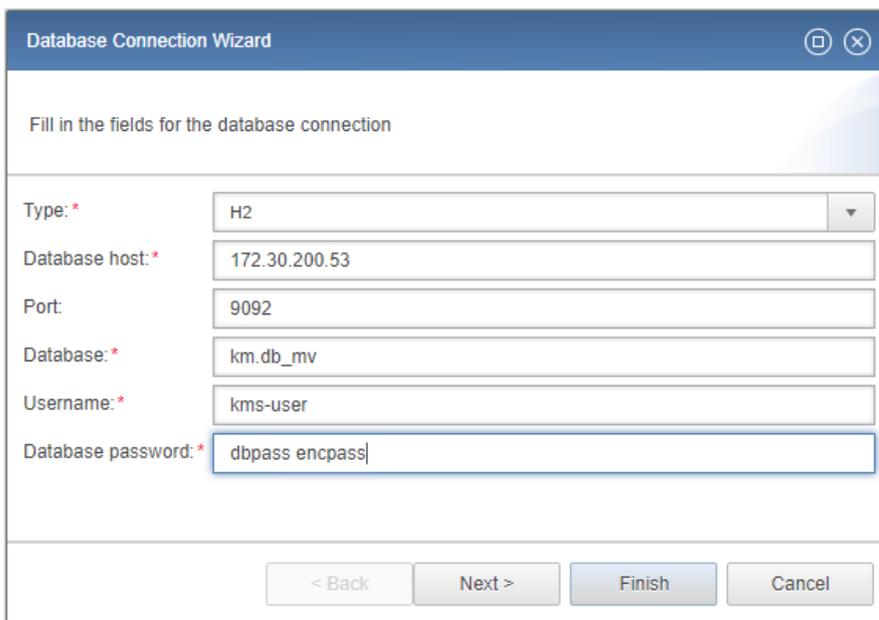
2. In the file `C:\Program Files\GBS\KeyManager\etc\kms.be.finetuning.conf`, set `kms.configuration.db.createBackup = false`.

Backups must be made manually: refer to <http://www.h2database.com/h2.pdf> for further reference.

3. Start the iQ.Suite KeyManager Service.
4. Open the KeyManager web interface (e.g.: <http://localhost/km.admin/kms>) and click LOGIN.
5. Click the WIZARD button:



6. Configure the database connection:



Database Connection Wizard

Fill in the fields for the database connection

Type: * H2

Database host: * 172.30.200.53

Port: 9092

Database: * km.db_mv

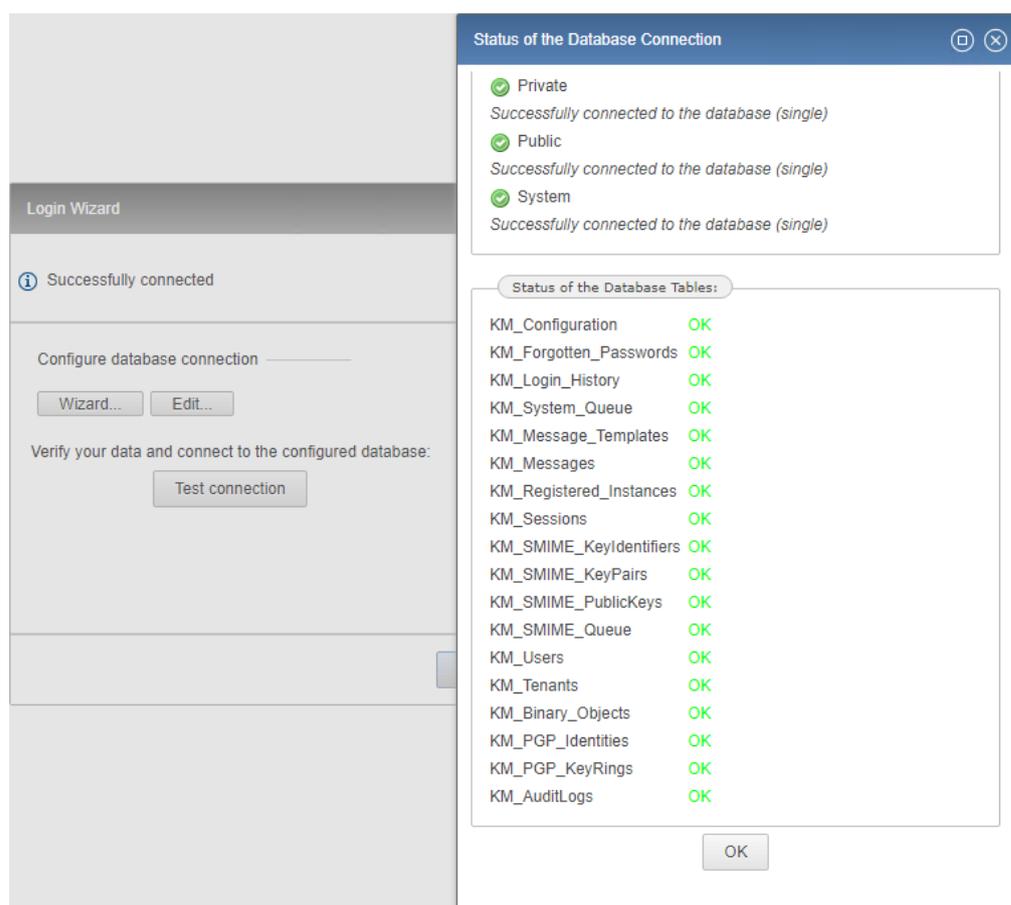
Username: * kms-user

Database password: * dbpass encpass

< Back Next > Finish Cancel

- Database host:** Enter the IP which was displayed when the H2 database was started.
 - Port:** The default port is '9092'.
 - Database:** Specify the path to the database relatively to the copied *h2-1.4.199.jar* file.
 - Username:** Enter the username used for the database creation (see above).
 - Database password:** Enter the password used for the database creation (see above).
7. Click FINISH.
 8. Click TEST CONNECTION.

All database tables should be created:



9. Click FINISH.
10. Configure the business administrator. To do this, refer to the KeyManager Installation and Administration manual.

2.3 Procedure in case of an existing KeyManager Installation

1. Stop the iQ.Suite KeyManager Service.
2. Unpack the **km.backend.war** file located under `C:\Program Files\GBS\KeyManager\keymanager\km-base\webapps\` and copy the **WEB-INF\lib\h2-1.4.199.jar** to the target directory.

Note: The JAR file version can differ. It could be, for example, *h2-1.4.202.jar* or other.

Example 1: Copy *h2-1.4.199.jar* to `C:\H2`.

Example 2: Copy *h2-1.4.199.jar* to `C:\H2\bin`.

3. Copy the database and the database program to the target machine.

Note: Do not delete the existing database!

4. Start the H2 database program:

Example:

```
cd \H2\data
```

```
"c:\Program Files\GBS\KeyManager\OpenJDK\bin\java.exe" -Xmx1024M -Xms256M  
-jar h2-1.4.199.jar -web -webAllowOthers -tcp -tcpAllowOthers
```

5. Edit the following fine-tuning parameters in order to access the database configuration:

```
C:\Program Files\GBS\KeyManager\etc\kms.be.finetuning.conf:
```

```
kms.configuration.db.createBackup = false
```

```
C:\Program Files\GBS\KeyManager\etc\kms.fe.finetuning.conf:
```

```
kms.configuration.showAdvancedSettings = true
```

6. Start the iQ.Suite KeyManager Service.
7. Login to the KeyManager web interface.
8. Open the Database Wizard and make the configuration as described under [2.2.2](#).
9. Click TEST CONNECTION.
10. If the connection test was successful, save the settings. The previous settings are kept until the new settings are saved.

If the connection test failed, edit the configuration accordingly.

11. Stop the iQ.Suite KeyManager Service.
12. Optionally, you can remove the previously used database.
13. Delete or rename the **kms.fe.preconfigured.conf** file under
C:\Program Files\GBS\KeyManager\etc\.

This is required to get the Database Configuration dialog after starting the KeyManager server. Otherwise, the default database will be created.

14. Start the iQ.Suite KeyManager Service.

Trouble-Shooting

If the connection to the database cannot be created, the session may be stopped. In this case, the login page is displayed again.

Typing errors in the configuration or firewall setting are a possible reason for this behavior.

Since the configuration has not been saved in this case, the procedure can simply be repeated.

If a wrong configuration was saved, stop the KeyManager Service and delete the files

kms.hibernate.xml and **kms.hibernate.conf.backup.xml** under:

C:\Program Files\GBS\KeyManager\etc\.

Then, the Database Configuration dialog opens when the KeyManager server is started, like in case of a new installation.

3 About GBS

GBS Europa GmbH is a leading vendor of solutions and services in the fields of messaging security and workflow for the Domino and Microsoft collaboration platforms. Over 5,000 customers and more than 4 million users worldwide trust in GBS expertise. The company operates in Europe, North America and Asia.

© 2020 GBS Europa GmbH

Our product descriptions are of a general and descriptive nature only. They do not stipulate any specific features nor do they represent any form of warranty or guarantee. We reserve the right to change the specifications and design of our products without notice at any time, in particular in order to keep abreast of technical developments.

The information contained in this document presents the topics from the viewpoint of GBS Europa GmbH (hereafter 'GBS') at the time of publishing. Since GBS needs to be able to react to changing market requirements, this is not an obligation for GBS and GBS cannot guarantee that the information presented in it is accurate after the publication date.

This document is intended for information purposes only. GBS does not extend warranty for this document, in either explicit or implied form. This also applies to quality, execution, standard commercial practice or suitability for a particular purpose.

All the product and company names that appear in this document may be trademarks of their respective owners.

Web site: www.gbs.com

Email address: info@gbs.com

Locations: www.gbs.com/en/locations

