Unimus HTTPS with a self-signed cert

If you want to connect to Unimus using HTTPS with a self-signed cert, you can use these instructions.

On Windows

Generate self-signed cert:

```
set JAVA_HOME=C:\Program Files\Unimus\jre8
set KEYTOOL=%JAVA_HOME%\bin\keytool

cd "C:\Program Files\Unimus"
"%KEYTOOL%" -genkey -alias unimus -storetype PKCS12 -keyalg RSA -keysize
2048 -keystore unimus.keystore.p12 -validity 3650
```

Change *JAVA_HOME* to properly reflect the path to your JRE.
The default value will work for Oracle JRE, but for OpenJDK JRE it will be different.

During the cert generation, you will be asked for the keystore password.
Input the password you wish to use (the keystore will be generated with such password) - you will need it in the next step.

After the cert was generated, you will need to configure Unimus to use it.

For portable:
Create a file named **Unimus.l4j.ini** in the same directory as the Unimus executable.
Change **Unimus** in the above file name to exactly match the name of the Unimus executable.

For installer:
Add the below lines to **Unimus.l4j.ini** in 'C:\Program Files\Unimus\'.

Inside of this configuration file, please add the following lines:

```
-Dserver.ssl.key-store="C:\\Program Files\\Unimus\\unimus.keystore.p12"
-Dserver.ssl.keyStoreType=PKCS12
-Dserver.ssl.keyAlias=unimus
-Dserver.ssl.key-store-password=[insert password here]
```

Please make sure to place each argument into its own line.

Replace '*[insert password here]*' with the password you used for keystore creation.

Restart the Unimus service, and it should be available only over HTTPS.

On Linux

Generate self-signed cert:

```
JAVA_HOME=/usr/lib/jvm/java-11-openjdk-amd64
KEYTOOL=$JAVA_HOME/bin/keytool

cd /opt/unimus
$KEYTOOL -genkey -alias unimus -storetype PKCS12 -keyalg RSA -keysize 2048
-keystore unimus.keystore.p12 -validity 3650
```

Change *JAVA_HOME* to properly reflect the path to your JRE.
The default value will work for Oracle JRE, but for OpenJDK JRE it will be different.

During the cert generation, you will be asked for the keystore password.
Input the password you with to use (the keystore will be generated with such password) - you will need it in the next step.

After the cert was generated, you will need to configure Unimus to use it.

Edit '**/etc/default/unimus**', and add the following commands:

```
-Dserver.ssl.key-store=/opt/unimus/unimus.keystore.p12
-Dserver.ssl.keyStoreType=PKCS12 -Dserver.ssl.keyAlias=unimus
-Dserver.ssl.key-store-password=[insert password here]
```

Replace '*[insert password here]*' with the password you used for keystore creation.

Restart the Unimus service, and it should be available only over HTTPS.

Notes and tips

Important note: please be careful if the keystore password contains the # character.

is used as a comment, so a password containing it will not be fully read from the configuration.
You can enclose the password in **"** (double quotes) if you wish to use # as a part of the password.