

External Certificate

Acquire certificate

Buy a certificate from a provider. Note that the max lifetime is currently 1 year, så buying a 5 year certificate only help on pricing.

```
https://www.ssls.com/
```

After issuing the files you will have

- A private key - ex: movia.tempusserva.dk.pfx
- A certificate - ex: movia_tempusserva_dk_key.txt

Install certificate

1. Upload the files
2. Convert to a pfx file format

```
openssl pkcs12 -export -out movia.tempusserva.dk.pfx -inkey movia_tempusserva_dk_key.txt -in  
movia.tempusserva.dk.crt
```

Write the password down

Check alias if needed

```
openssl pkcs12 -nokeys -info -in movia.tempusserva.dk.pfx -passin pass:TempusServaFTW!
```

4. Install in tomcat Add the following code to <tomcat>\conf\server.xml

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" URIEncoding="UTF-8"  
scheme="https" secure="true" maxHttpHeaderSize="8192"  
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"  
enableLookups="false" acceptCount="100" disableUploadTimeout="true"
```

```
keystoreFile="/mnt/sda/certs/movia.tempusserva.dk.pfx" keystorePass="TempusServaFTW!"
keystoreType="PKCS12"
clientAuth="false" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,
        TLS_RSA_WITH_AES_128_CBC_SHA,
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
        TLS_RSA_WITH_AES_128_CBC_SHA256,
        TLS_RSA_WITH_AES_128_GCM_SHA256,
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
        TLS_RSA_WITH_AES_256_CBC_SHA,
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
        TLS_RSA_WITH_AES_256_CBC_SHA256,
        TLS_RSA_WITH_AES_256_GCM_SHA384,
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
compression="on" compressionMinSize="2048" nocompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/plain,application/xml"
/>
```

5. Restart the server

Revision #1

Created 3 April 2025 12:23:11 by Theis Villumsen

Updated 3 April 2025 12:26:52 by Theis Villumsen