Installing SSL Certificate for GeoServer/Jetty

Monica Mohan · Follow
3 min read · Jun 17, 2021

Listen Share

GeoServer

Here’s a short tutorial on installing SSL Certificate for Jetty Server that comes bundled with GeoServer.

Disclaimer: The following steps are performed and tested in Windows OS

Generate PFX Certificate

You can create self-signed certificate and export it as a pfx file in Powershell as administrator. For this, run the following command:

```
$cert = New-SelfSignedCertificate -certstorelocation cert:\localmachine\my -dnsname <domain name>

$pwd = ConvertTo-SecureString -String ‘password’ -Force -AsPlainText

$path = ‘cert:\localMachine\my\’ + $cert.thumbprint

Export-PfxCertificate -cert $path -FilePath m:\certs\powershellcert.pfx -Password $pwd
```

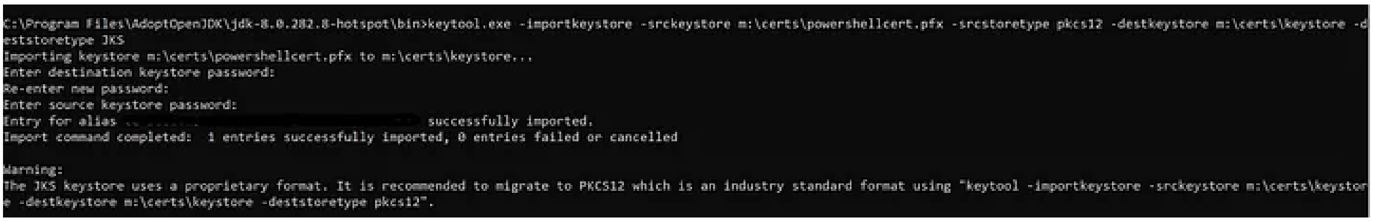
Install the certificate by simply double-clicking the newly generated pfx file.

Generate KEYSTORE file

Keystore file is required by Jetty for SSL configuration. Hence, convert the PFX file to JKS Keystore and then install it on the Jetty Server that comes with GeoServer.

- Go to ‘bin’ folder of JDK and run the following command in cmd:

```
keytool -importkeystore -srckeystore m:\certs\powershellcert.pfx -srcstoretype pkcs12 -destkeystore m:\certs\keystore -deststoretype JKS
```



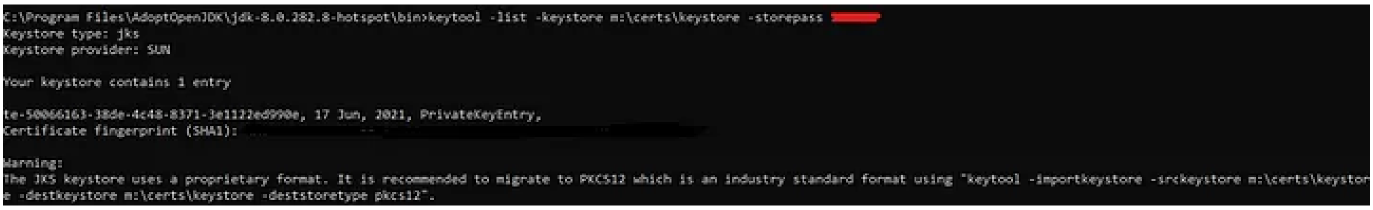
```
C:\Program Files\AdoptOpenJDK\jdk-8.0.282.8-hotspot\bin>keytool.exe -importkeystore -srckeystore m:\certs\powershellcert.pfx -srcstoretype pkcs12 -destkeystore m:\certs\keystore -d
eststoretype JKS
Importing keystore m:\certs\powershellcert.pfx to m:\certs\keystore...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias [redacted] successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore m:\certs\keystor
e -destkeystore m:\certs\keystore -deststoretype pkcs12".
```

Import keystore from PFX certificate file

**Tip: Use the same password that you used to generate the pfx file

- Now, execute the following command to verify if the created keystore is a PrivateKeyEntry.

> *keytool -list -keystore m:\certs\keystore -storepass password*



```
C:\Program Files\AdoptOpenJDK\jdk-8.0.282.8-hotspot\bin>keytool -list -keystore m:\certs\keystore -storepass [redacted]
Keystore type: jks
Keystore provider: SUN

Your keystore contains 1 entry

te-50066163-38de-4c48-8371-3e1122ed990e, 17 Jun, 2021, PrivateKeyEntry,
Certificate fingerprint (SHA1): [redacted]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format using "keytool -importkeystore -srckeystore m:\certs\keystor
e -destkeystore m:\certs\keystore -deststoretype pkcs12".
```

List Keystore

- Copy the generated keystore to %GEOSERVER_HOME%\etc\keystore (make a backup of the existing keystore)

Configure Jetty Server

- Open the start.ini in %GEOSERVER_HOME% and copy the following to after — module=http

> *#SSL*
>
> *— module=ssl*
>
> *jetty.ssl.port=8443*
>
> *jetty.sslContext.keyStorePath=etc/keystore*
>
> *jetty.sslContext.trustStorePath=etc/keystore*
>
> *jetty.sslContext.keyStorePassword=password*
>
> *jetty.sslContext.keyManagerPassword=password*
>
> *jetty.sslContext.trustStorePassword=password*
>
> *— module=https*
>
> *jetty.httpConfig.securePort=8443*

- Download the jetty-distribution file (it must be the same version as in the geoserver — geoserver 2.21 uses jetty 9.4.48) from maven eclipse site and extract the contents.

Central Repository: org/eclipse/jetty/jetty-distribution/9.4.48.v20220622 (maven.org)

**Tip: You can cross check the jetty version in %GEOSERVER_HOME%/lib

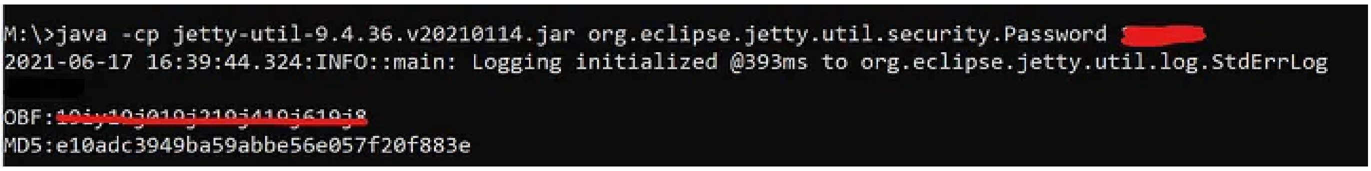
(3 files are required — ssl.mod, jetty-ssl-context.xml and jetty-util-xx.jar)

- Copy ssl.mod from /modules to %GEOSERVER_HOME%\modules
- Copy jetty-ssl-context.xml from /etc to %GEOSERVER_HOME%\etc
- Copy jetty-util-x.x.xx.jar to any path on the machine and navigate to this path in cmd

Run this command:

> *java -cp jetty-util-<JettyVersion>.jar org.eclipse.jetty.util.security.Password password*

and obtain the obfuscated password (OBF:….)



```
M:\>java -cp jetty-util-9.4.36.v20210114.jar org.eclipse.jetty.util.security.Password [redacted]
2021-06-17 16:39:44.324:INFO::main: Logging initialized @393ms to org.eclipse.jetty.util.log.StdErrLog

OBF:[redacted]
MD5:e10adc3949ba59abbe56e057f20f883e
```

Generating obfuscated password

- Copy the OBF password and replace the existing OBF password in jetty-ssl-context.xml

**Tip: If port needs to be changed, make changes in jetty-ssl.xml (secure.port) and in start.ini

- Restart the GeoServer service in Services.msc or Restart using start.bat in %GEOSERVER_HOME%

Now, you will be able to access secure GeoServer using https://<domain>:<port>/geoserver/web

Cheers!

Geoserver Jetty Ssl Https Security

Follow

Written by Monica Mohan

16 Followers · 12 Following

I'm a Geospatial Application Developer. ESRI Certified. I'm passionate about employing GIS and developing geospatial applications, esp in Earth Observation.

Open in app ↗ Sign up Sign in

Medium Search

Responses (6)

Write a response

What are your thoughts?