# Prerequisites

A valid certificate in .pfx format and password

# Update SSL Certificate in Tomcat

* Navigate to C:\Program Files\Apache Software Foundation\Tomcat 9.0\conf
* Open file – server.xml
* Change **keystoreFile** and **keystorePass**

**Eg -**

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

keystoreFile="<.pfx file path>"

keystorePass="<password>"

clientAuth="false" acceptCount="100"/>

# Update SSL certificate in java keystore

## Convert .pfx certificate to .cer format

### Import

* Open Internet Explorer
* Tools >> Internet Option >> ‘Content’ tab >> ‘Certificates’ Button >> import
* Click next >> Select the .pfx file >> Follow the wizard

### Export as .cer file

* Open Internet Explorer
* Tools >> Internet Option >> ‘Content’ tab >> ‘Certificates’ Button
* Select your certificate >> Click on ‘Export’
* Click Next >> Select format – ‘DER encoded binary X.509 (.CER)’
* Click Next >> Select file path >> Finish

### Import to Java Keystore

1. Open CMD in admin mode
2. Go to:\Program Files\Java\jdk1.8.0\_211\bin
3. Run keytool command –

|  |
| --- |
| keytool -importcert -keystore cacerts -storepass changeit -file <.cer file oath> -alias "<certificate alias>" |

# How to Verify??

* Login to IIQ
* Click on the Lock icon, next to refresh button
* Click on “Connection is secure”
* Click on ‘Certificate is valid/invalid’
* Verify the date

# Java Keystore location??

* JDK path\jre\lib\security
* 