How to Update ProjectDox SSL Cert

Purpose:

This document outlines the steps for creating the required JKS file for use with Apache Tomcat when SSL cert has been installed in IIS.

**Export .pfx file**

\*\*The cert must be installed with the option to be exportable

1. Log into your web server
2. Open IIS
3. Click on the server name
4. Select Server Certificates



1. Highlight the valid certificate
2. Right click or click on the export link in the right margin





1. You will be prompted to enter a password, name for the file and the location to place the new .pfx file.
	1. Export to – Find your ProjectDox Installation root folder. Enter the drive location and a name for the .pfx file. Example below (your drive location may be different)
	2. Create password. You will need this password again in a later step



**Export .p7b file**

1. Open MMC
2. Go to file > Add/Remove Snap in
3. Choose Certificates
4. Click add with the arrow between the sections



1. Click OK
2. This will open a window with three radio buttons – select the third button for Computer Account



1. Click Next
2. Click the radio button for the option Local Computer



1. Click Finish – this will bring you back to the MMC window
2. Expand the Personal folder > Certificates
3. Right click on the Cert and select the option All Tasks > Export. This will open an export wizard window
4. Select the option to ***Do Not Export Private Key***
5. Click the radio button - ***Cryptographic Message Syntax Standard for PKCS #7 Certificates (.P7B)*** and ***Include all certificates in the certain path if possible***



1. Navigate to the root folder where ProjectDox is installed. This is the same location where you exported the .pfx file to. You will see a .pfx and .p7b file in the folder after export.
2. You can name this what you prefer. It can be easier to name it similar to the .pfx file



1. The next window will show the settings that were selected.



1. Click finish

**Run the following DOS commands**

**Convert .pfx to .jks file**

1. Verify if there is an existing JKS file in the Java bin folder. You will want to rename it to .old if one already exists



1. Open Command Prompt window
2. Navigate to the Java bin folder (your path may be different depending on Java location and installation
	1. cd c:\Program Files\Java\jrex.x.x\_xxx\bin
3. Run below command
	1. keytool -importkeystore -srckeystore e:\certificate.pfx -srcstoretype pkcs12 -destkeystore pdtomcert.jks -deststoretype JKS -storepass <yourpassword>
	2. Update the file location. This is the location of the .pfx file, which should be the root folder of ProjectDox from the .pfx export steps
	3. Your password – This is the password that was created when the .pfx file was created
4. This will generate an alias. Copy this alias – you will need this in the next step.
5. This is the response you should see after running the command

Entry for alias le-c5a08b67-625c-4184-8769-59eca73b6b55 successfully imported.

Import command completed: 1 entries successfully imported, 0 entries failed or

cancelled

\*\* The path was not determined in the command, so the .jks file will be in the Java bin folder

**Import the Certificate into the .jks file**

1. Copy the .p7b file into the Java bin folder
2. Run the following command in Command Window – this is still in the bin folder for Java
3. **keytool -import -trustcacerts -alias alias\_from\_jks\_file -file your\_p7b\_file.p7b -keystore pdtomcert.jks -storepass <yourpassword>**
	1. ***file -file your\_p7b\_file.p7b:*** Insert the name of the .p7b file as it was named during the export step. Should look like this: -file ssl\_certificate.p7b (the name of the file will need to match what you created)
	2. **-alias alias\_from\_jks\_file:** Insert the alias from above. It will look like this: -alias le-c5a08b67-625c-4184-8769-59eca73b6b55 (the alias will be different from this example)
	3. **-storepass <yourpassword>:** This is the password that was created during the .pfx export step
4. This is what should show in the command window after the script is completed



**Edit Server.xml file**

1. Copy the .jks file from the Java bin folder to the conf file of Program Files > Apache Software Foundation > Tomcat x.x > conf (the file path can differ depending on installation and version of Tomcat)
2. Make a copy of the server.xml file (this will create a back up with the old information in case you need to roll back the changes)
3. Open the server.xml file – you will need to update the alias and password to the new values created with the above scripts
	1. Scroll down to the section showing in screenshot below



1. Update the password to what was created in the .pfx export
2. Update the alias from the script
3. If the following section is commented you will need to uncomment

<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"

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

 clientAuth="false" sslProtocol="TLS" />

1. Update Tomcat to use newer TLS protocols
	1. replace *sslProtocol=”TLS”* with
	 *sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2"*
2. Turn off the logs if enabled by commenting out the line –

<Valve className=”org.apache.catalina.valves.AccessLogValve”  directory=”logs” prefix=”localhost\_access\_log.” Suffix=”.txt” pattern=”%h %l %u %t &quot;%r&quot; %s %b” />

1. Save .xml file

**\*\*Final Step - Delete DLCache and restart Apache/JP services\*\***