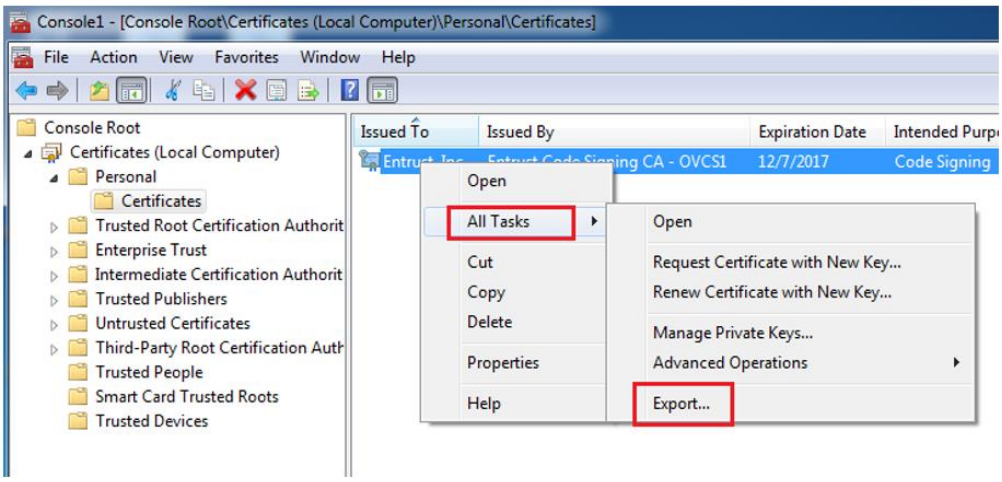
How to export an SSL/TLS certificate from Microsoft Management Console

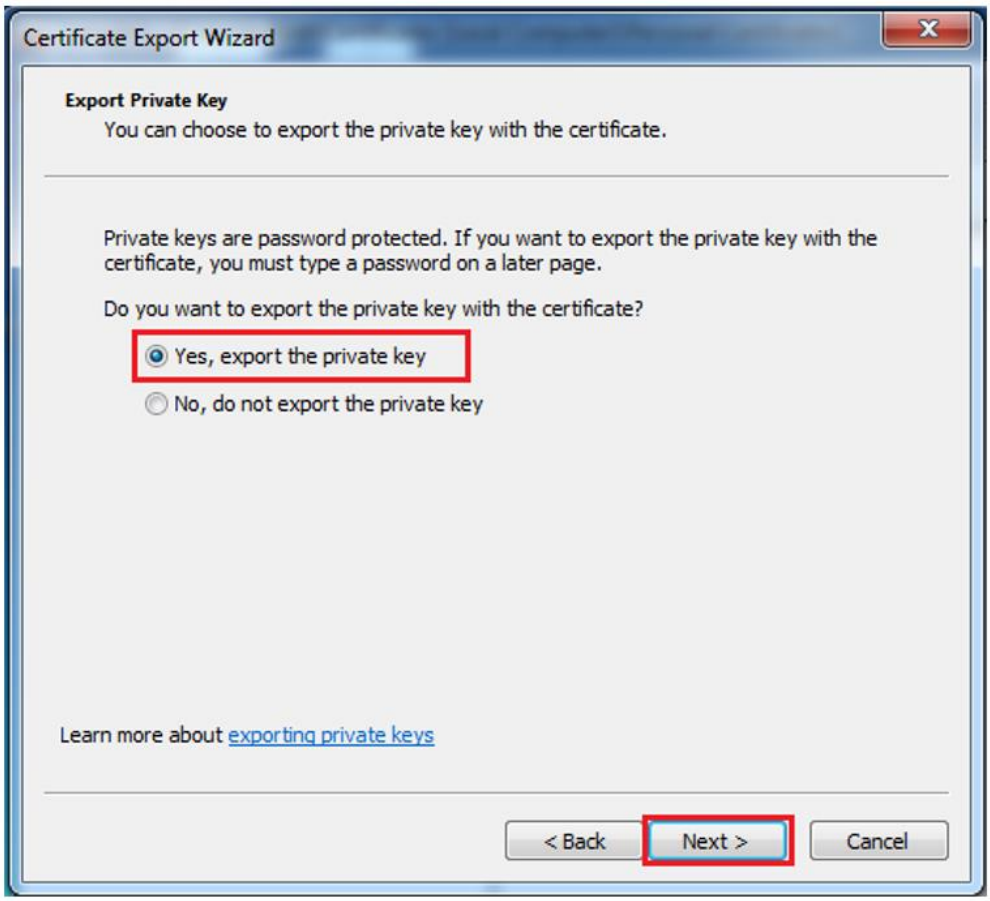
How to export an SSL/TLS certificate from Microsoft Management Console as a PFX file.

If needed, you can export an SSL/TLS certificate with its private key as a PFX file.

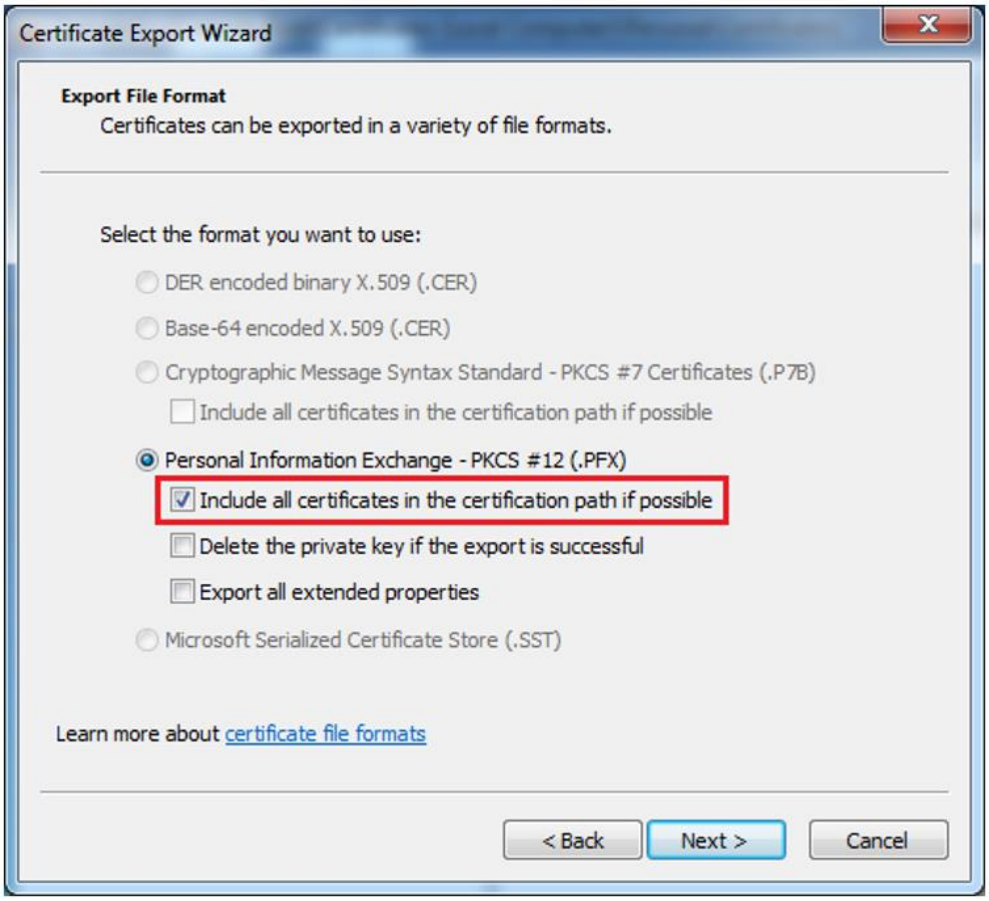
1. Right click on the certificate, select “All Tasks” and click on “Export…”.



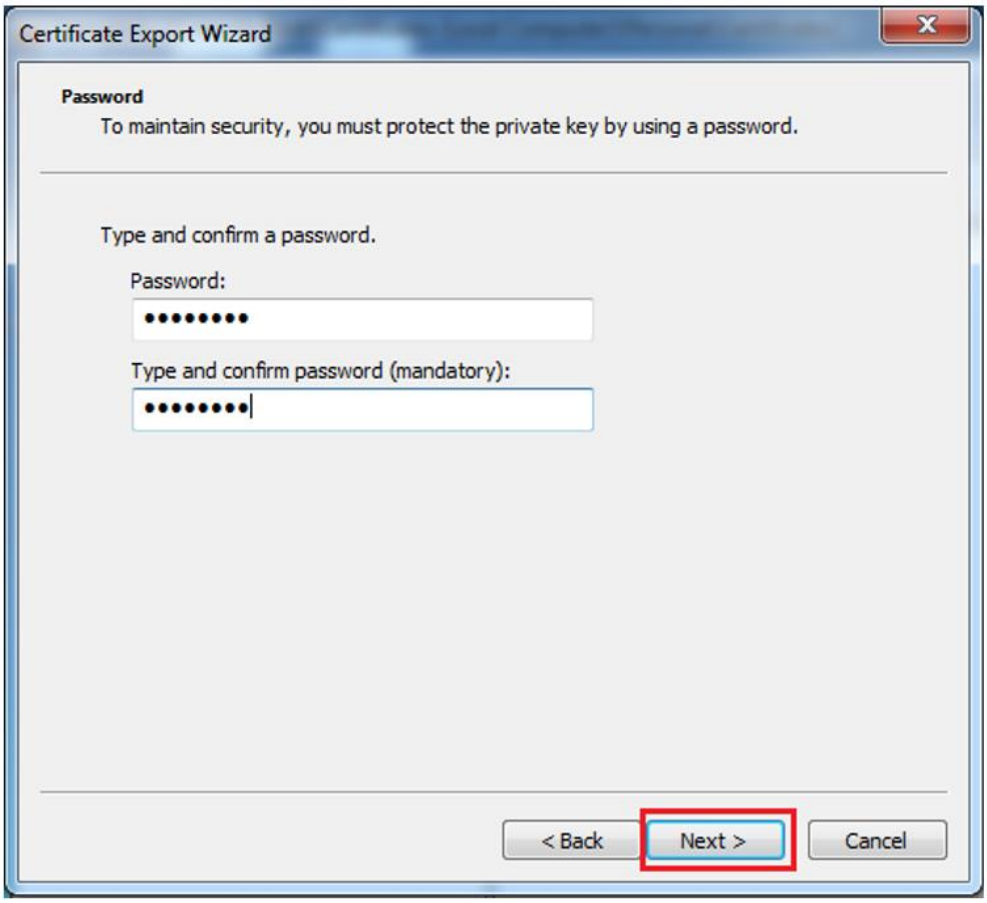
2. Click Next on the welcome screen. In the “Export Private Key” section, you must select “Yes, Export the private key” to create a PFX/PKCS12 file.



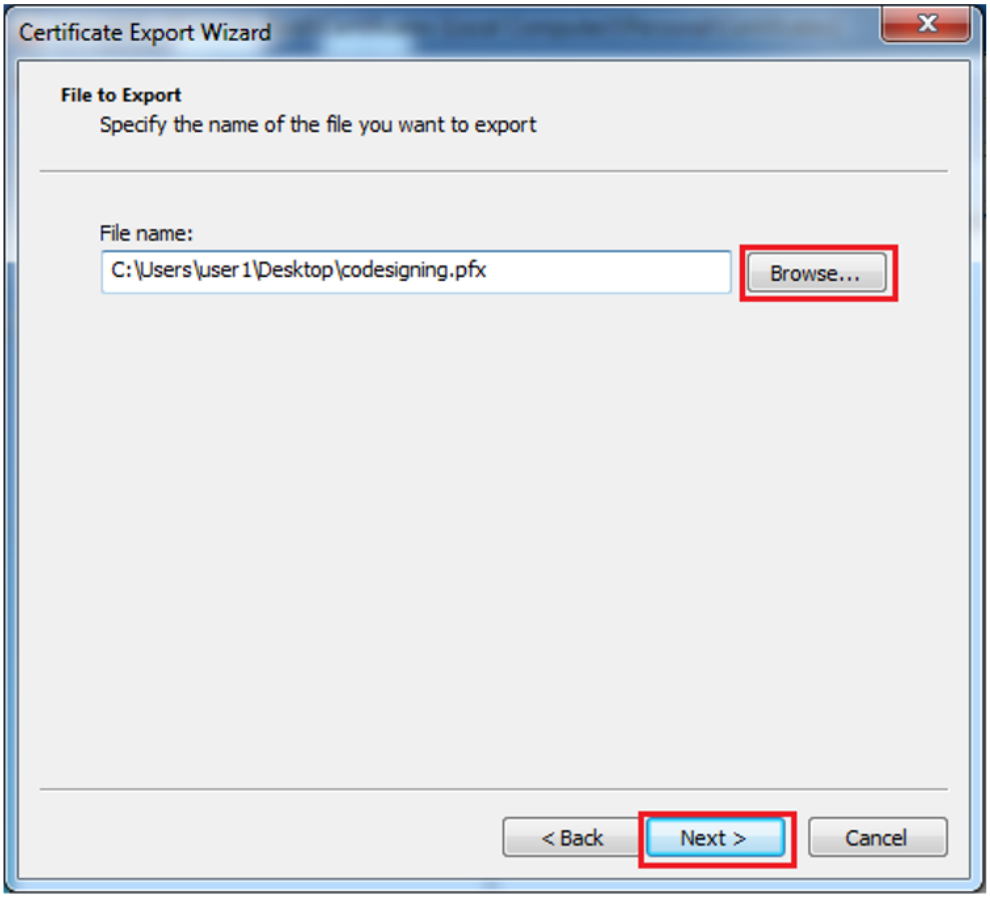
3. In the “Export File Format” section check the option for “Include all the certificates in the certification path if possible". This is very important as you may have trust errors with files if the intermediate and root certificate is not included. Click Next.



4. A password is mandatory for create a PFX file. Enter a password and click “Next”.



5. In the next screen, click “Browse” to choose a folder and a name for the PFX file.



6. Confirm the settings and click “Finish”.

7. Locate the server.xml file under the conf folder of the installed location of Tomcat server and look for the SSL connector definition. Typically, this will be commented as the stock offering. Manually change that to have sometning like below:

```
<Connector SSLEnabled="true" acceptCount="100" clientAuth="false"
    disableUploadTimeout="true" enableLookups="false" maxThreads="550"
    port="443" keystoreFile="<path to the PFX file>" keystorePass="<password
provided during export>" keystoreType="PKCS12"
    protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https"
    secure="true" sslProtocol="TLS" />
```

Note: The above setting is assumed that the FootPrints server doesn’t have the Microsoft IIS running, since we are using the default HTTPS port