**SSL Setup for CHO instances.**

To perform this setup, you need to have CA access, if you don’t have CA access ( as most of the clients will not be ready to provide CA access ) you can follow below steps.

SSL will be binded to IIS automatically by running the script given in security operations guide in DSS and HIUI servers. Below steps mention about the manual binding as well, if the binding is failed while running the script.

When it comes to HQ server, as we are not using IIS, we use apache tomcat, binding will be automatically done when we run activatebase.cmd there are manual steps which needs to be done to import the root certificate.

**DSS and HIUI Server**

**Ask the client to generate the SSL certificate and copy it to some location in the server to where installer account has the access**

**Step1:**

Unzip the HIUTL package to C drive and launch the command prompt to .\Utils\SSL Cert Request Scripting

**Step2:**

Run the below command

**CreateCert-CHO.cmd -app *<Application>* -folder *<Certificate Path>* and -certificatename**

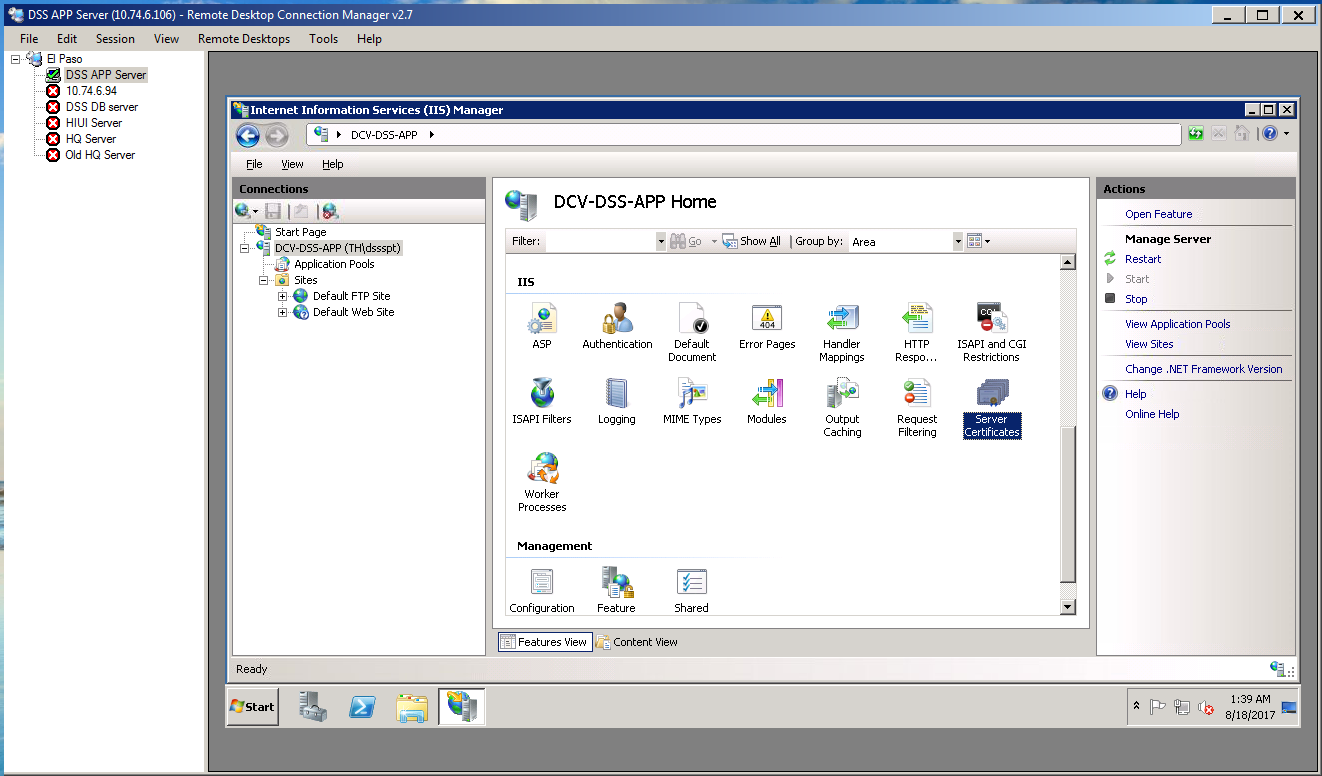
Where app can be **HI or HQ**

Folder is the certificate path where the client has copied the certificate

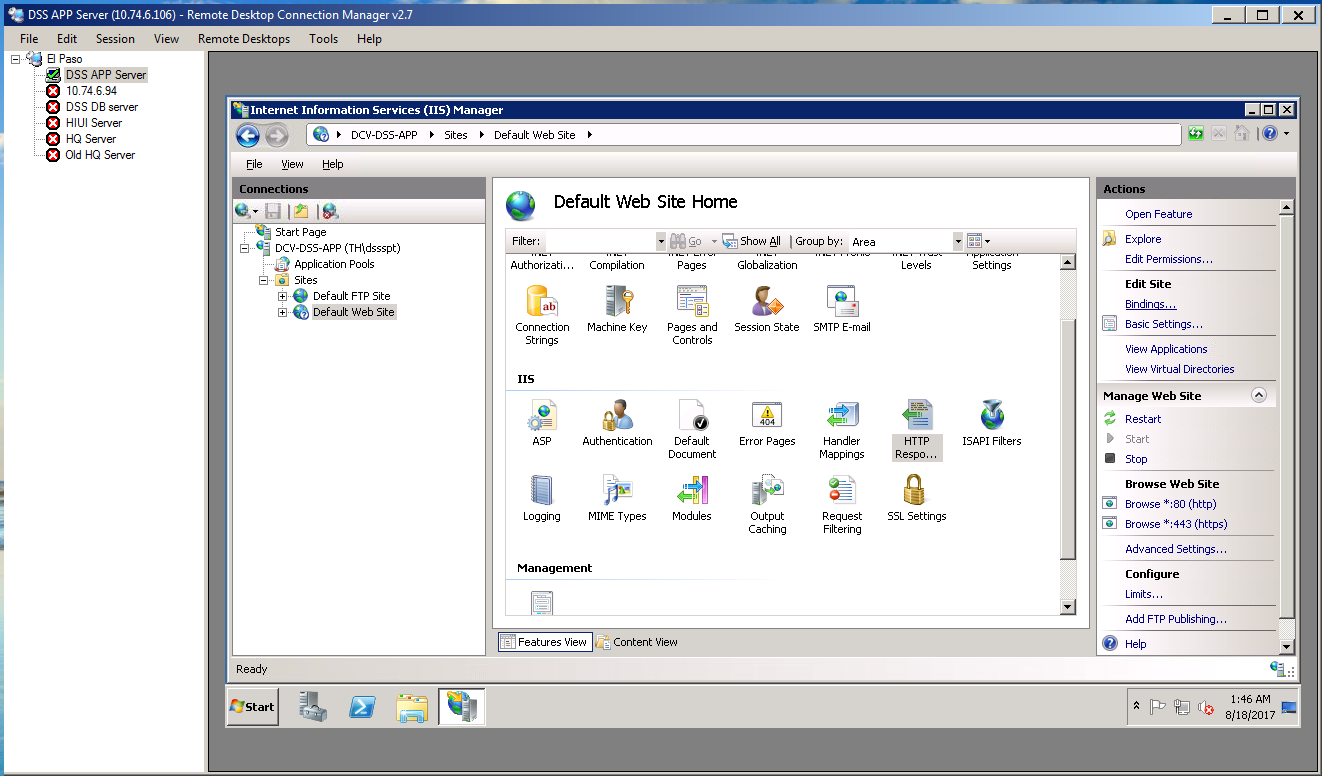
Certificate name is the SSL certificate name without the extension i.e. **.cer**

**Most of the times running the above script would complete the SSL setup, if the bindings are failed please follow below steps.**

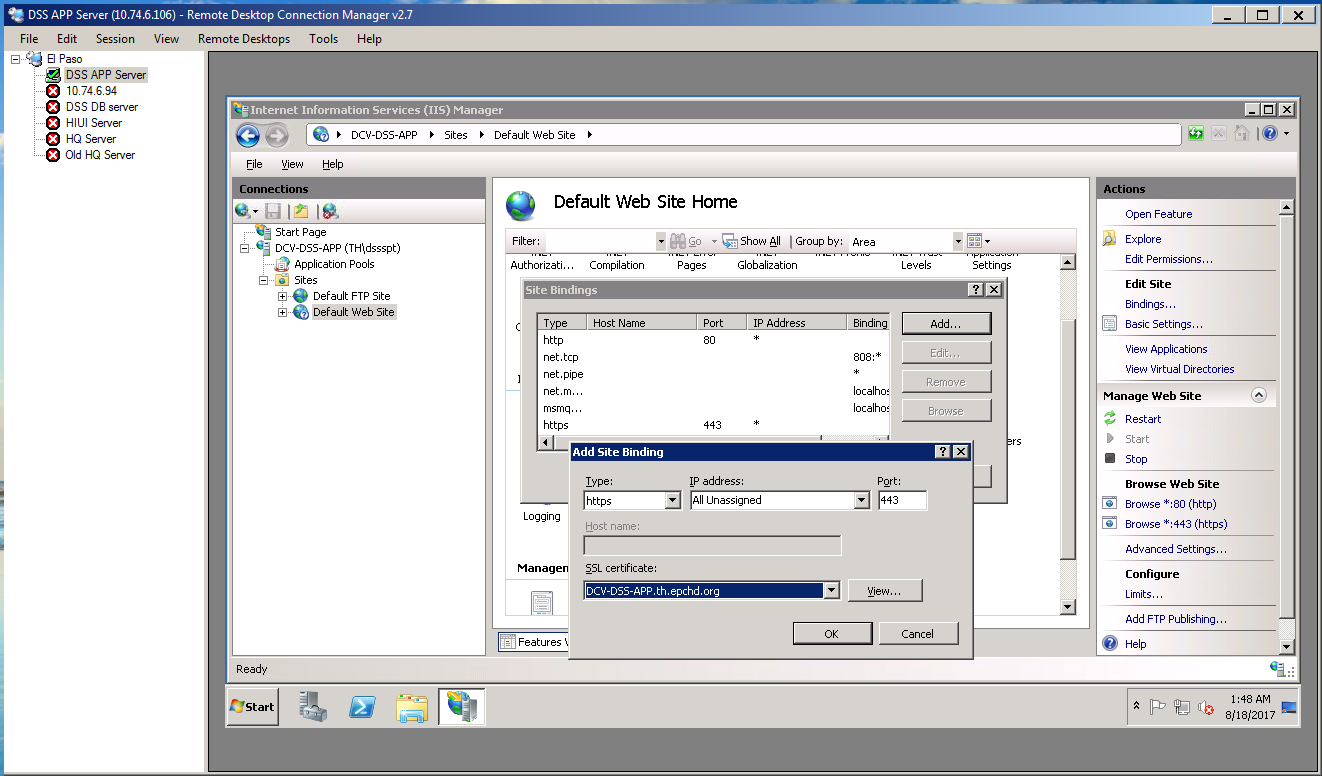
**Step1:** Go to IIS and click on **server name** and double click on **Server Certificates check for the certificate here**



**Step2: Select default website and select bindings under actions**



**Step3:** Click add on site bindings, select https as type this will automatically select the port number as 443 select the certificate from SSL certificate dropdown and select the certificate and hit ok



Repeat the same steps for HIUI server

This would complete the SSL certificate work on DSS and HIUI server

**HQ server:**

**Step1:** Create the SSL folder under C drive

**Step2:**  Run the below script to generate the java keystore file

"%JAVA\_HOME%\bin\keytool" -genkey -noprompt -alias tomcat -keyalg RSA -dname "CN=DCV-DSS.BOE.th.epchd.org, OU=Health Services, O=Cerner, L=El Paso, S=Texas, C=US" -keystore C:\SSL\Certs.jks -storepass changeit -keypass changeit

**-dname is fully qualified domain name**

**OU and O are standard**

**L= City name where the hospital is residing**

**S= State of the hospital**

**-storepass and -keypass can be anything in the above script password is mentioned as changeit we can use the same**

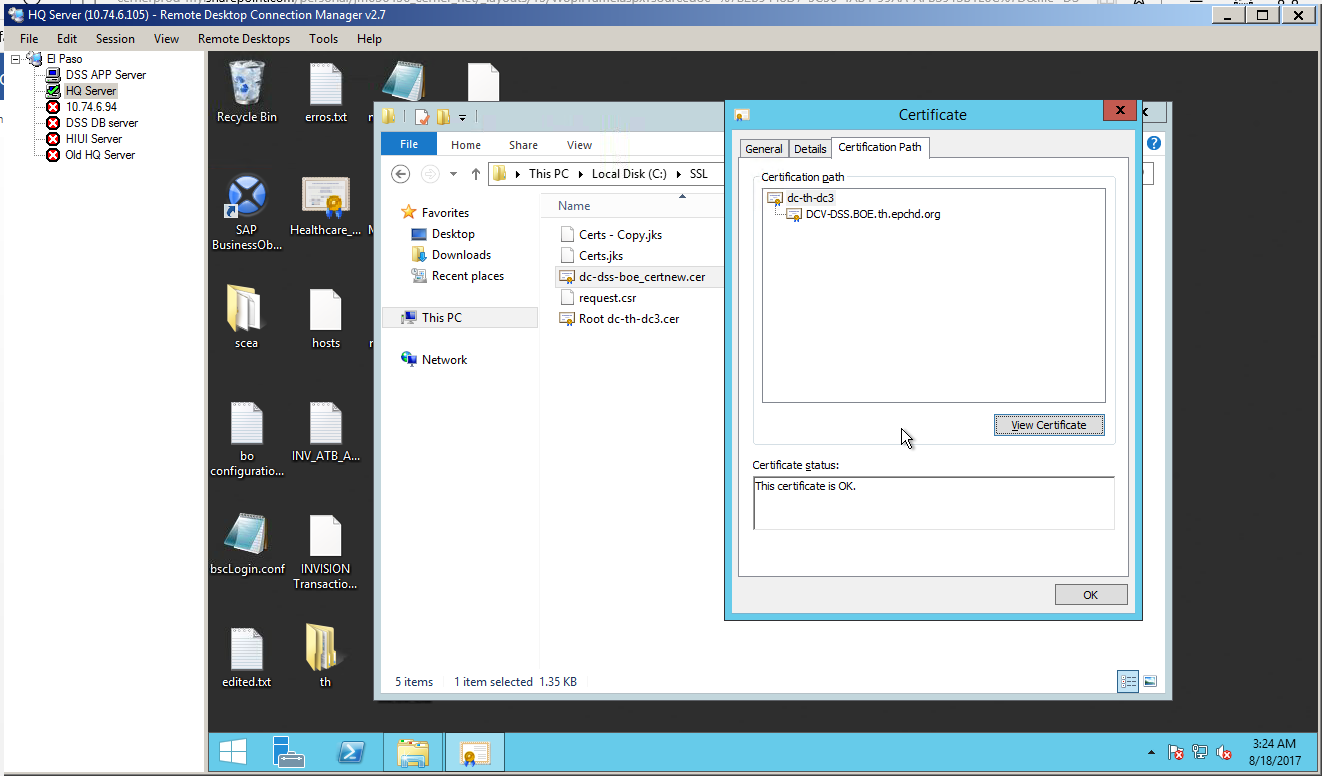
**Step3:** Use the below script to generate the request.csr

**"%JAVA\_HOME%\bin\keytool" -certreq -keyalg RSA -alias tomcat -file C:\SSL\request.csr -keystore c:\ssl\Certs.jks -storepass changeit**

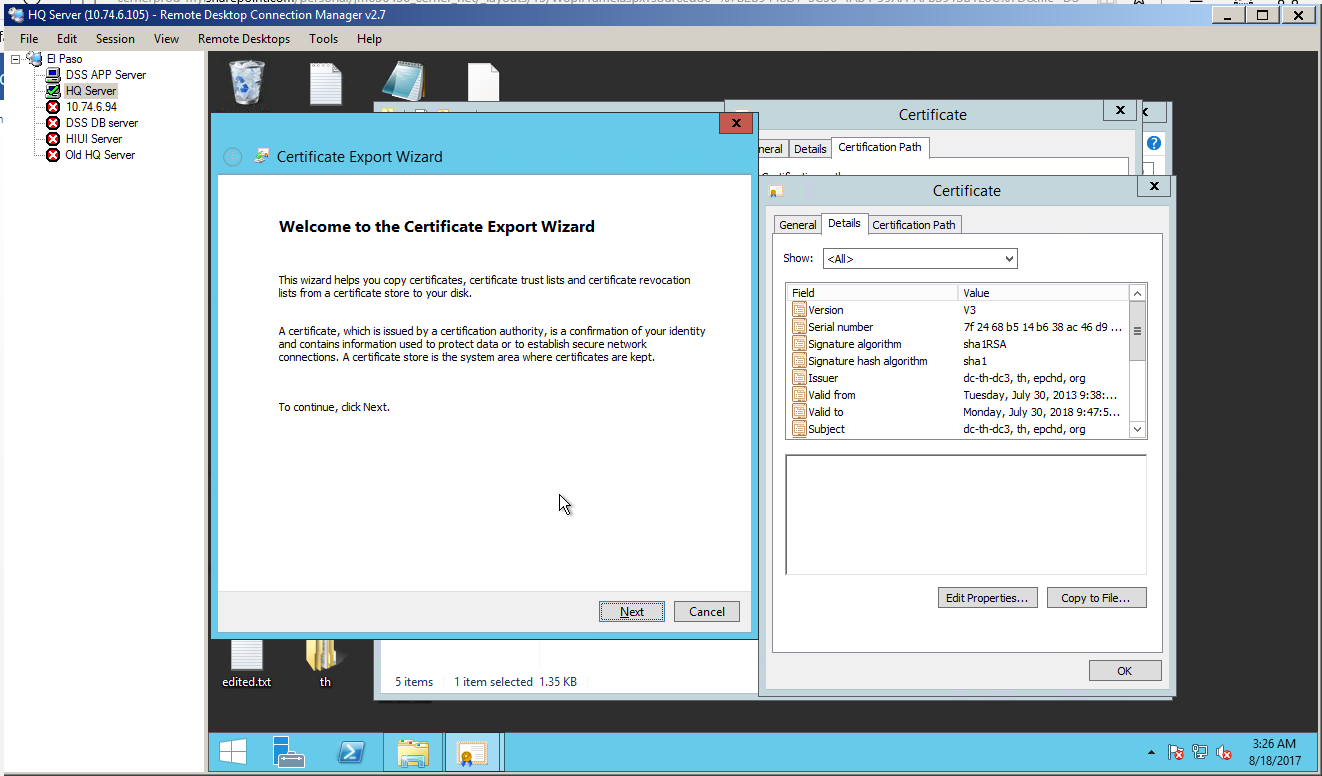
Once the request.csr is created, ask the client to use that and create the SSL Certificate.

**Step4: Import the root certificate by following below steps**

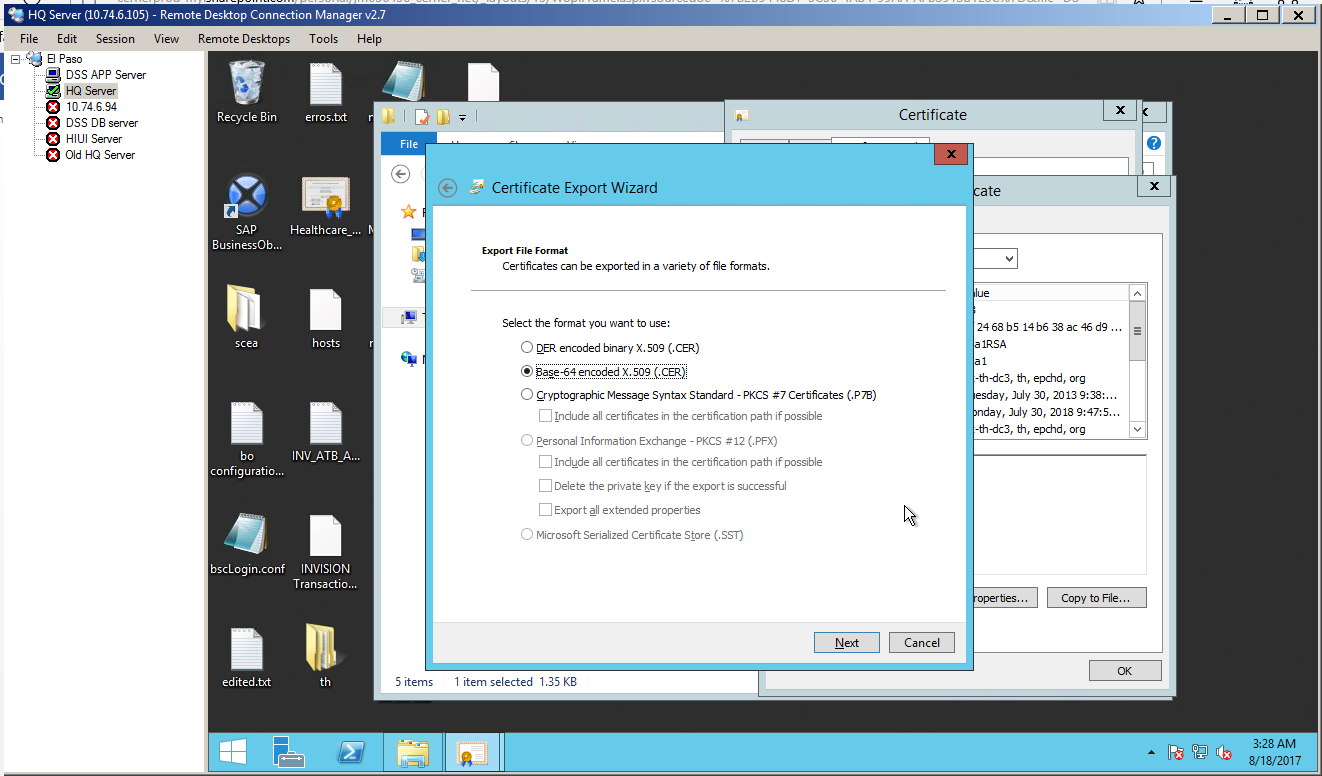
1. Right click and open the SSL certificate provided by client go to Certificate Path and select the root certificate and hit view certificate



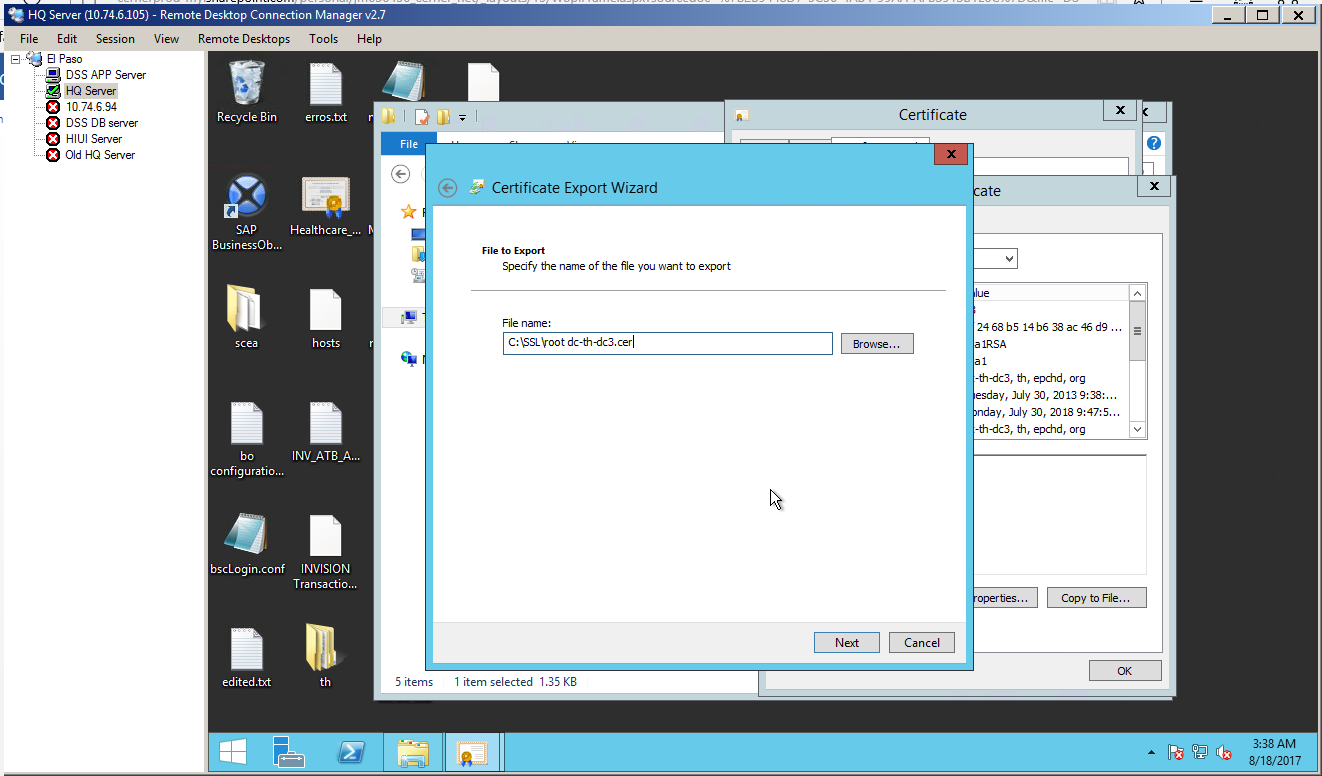
1. Go to details on root certificate window and select copy to File



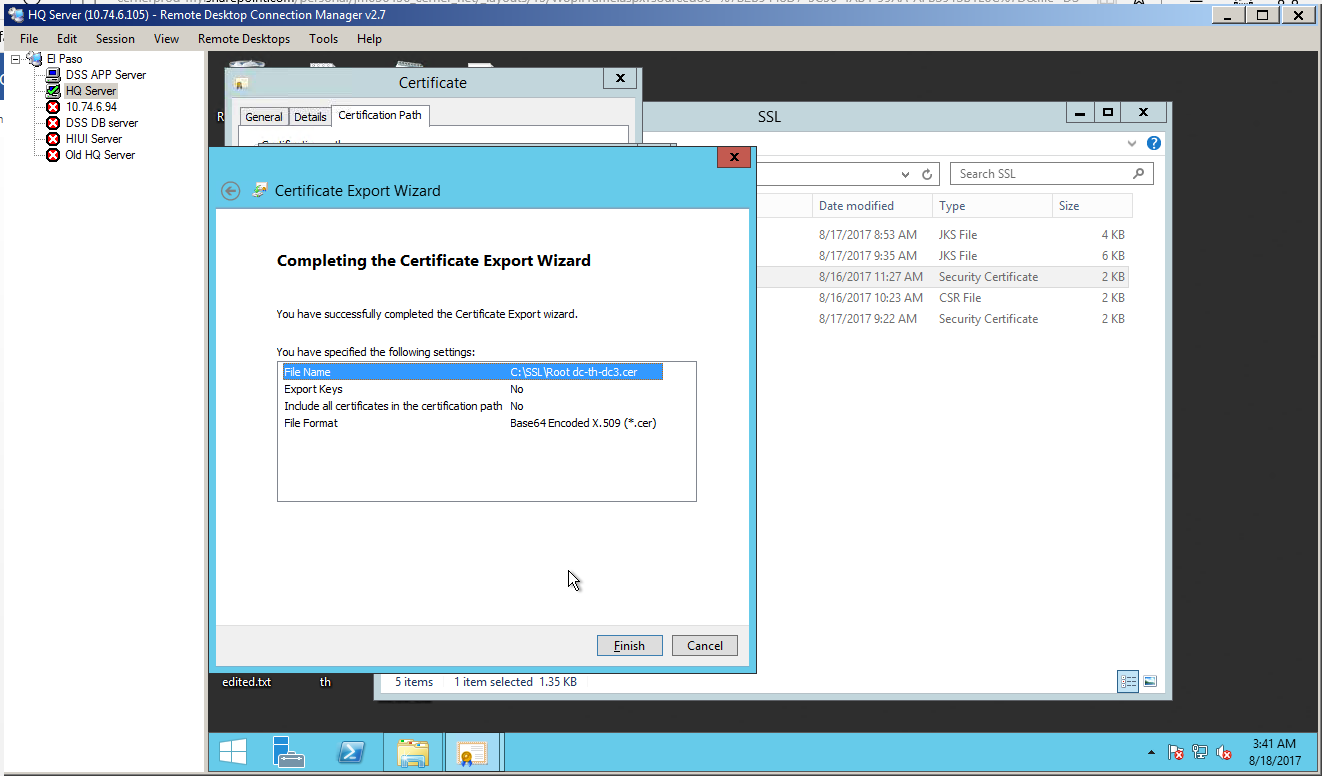
1. Hit next on the welcome to certificate wizard screen select Base-64 encoded X.509 (.CER) on the Certificate Export Wizard screen



1. Give a certificate name with same location used for storing SSL Certificate use root in front of the root certificate name



1. Hit finish at the Completing the Certificate Export Wizard



**Step5:** Run the java commands as below

1. "%JAVA\_HOME%\bin\keytool" -import -alias root -keystore c:\ssl\Certs.jks -trustcacerts -file "c:\ssl\**dc-dss-boe\_certnew.cer**" -storepass changeit -noprompt

**Run the below command replacing the certificate value with root certificate**

1. "%JAVA\_HOME%\bin\keytool" -import -alias tomcat -keystore c:\ssl\Certs.jks -trustcacerts -file "c:\ssl\**root dc-dss-boe\_certnew.cer**" -storepass changeit -noprompt

