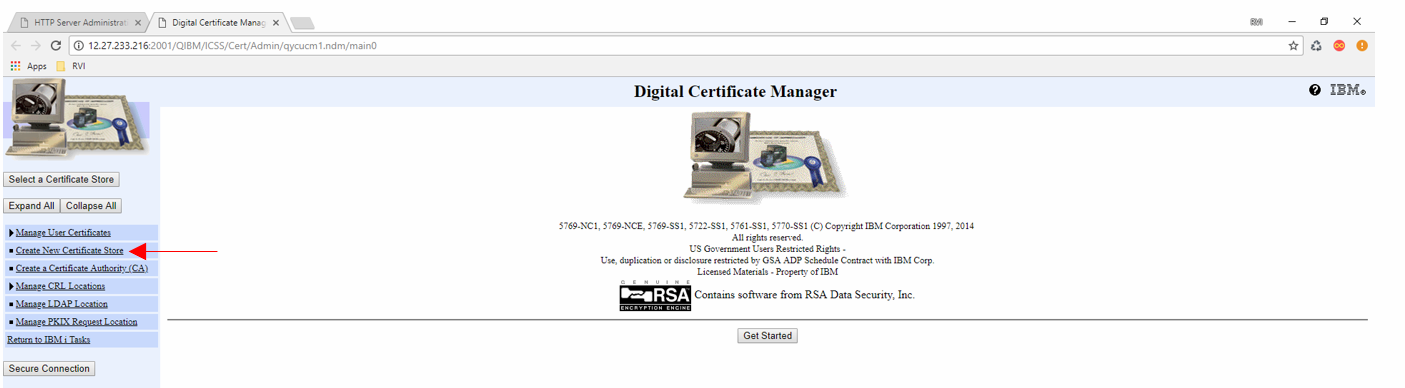
**HTTP SSL CONFIGURATION FOR IBM I**

Step 1 - Go to your Hosts DCM (Digital Certificate Manager)

Ex. <http://12.27.233.216:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0>

Step - 2 Click **Create New Certificate Store**.

Select **\*SYSTEM** store. (*This is if the \*SYSTEM store has not been created.*) Click Continue.



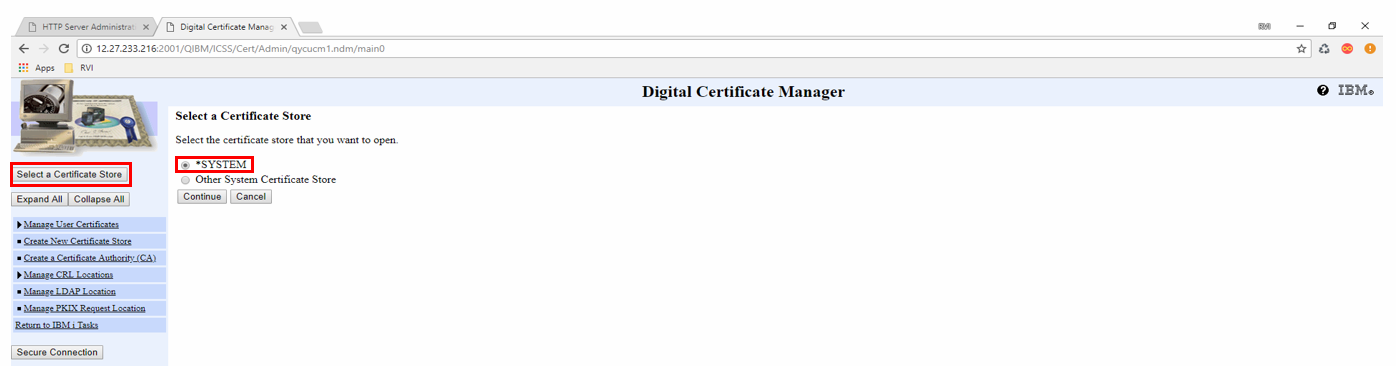
Step - 3 When prompted to create a new certificate, choose **Do not Create a certificate in the certificate store**. Click Continue.

Step - 4 Create a password for the certificate store when prompted. Click Continue.

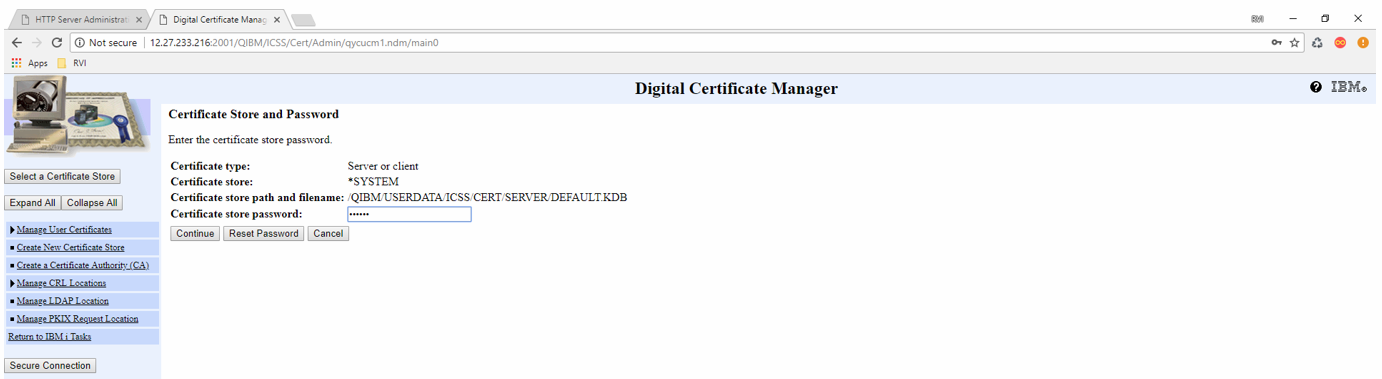
Step - 5 Fill out the information necessary for the \*SYSTEM store. Click Continue. *(\*SYSTEM store should now be created.*)

Step - 6 In the left pane, click **Select a Certificate Store**.

Step - 7 Select **\*SYSTEM**. Click Continue.

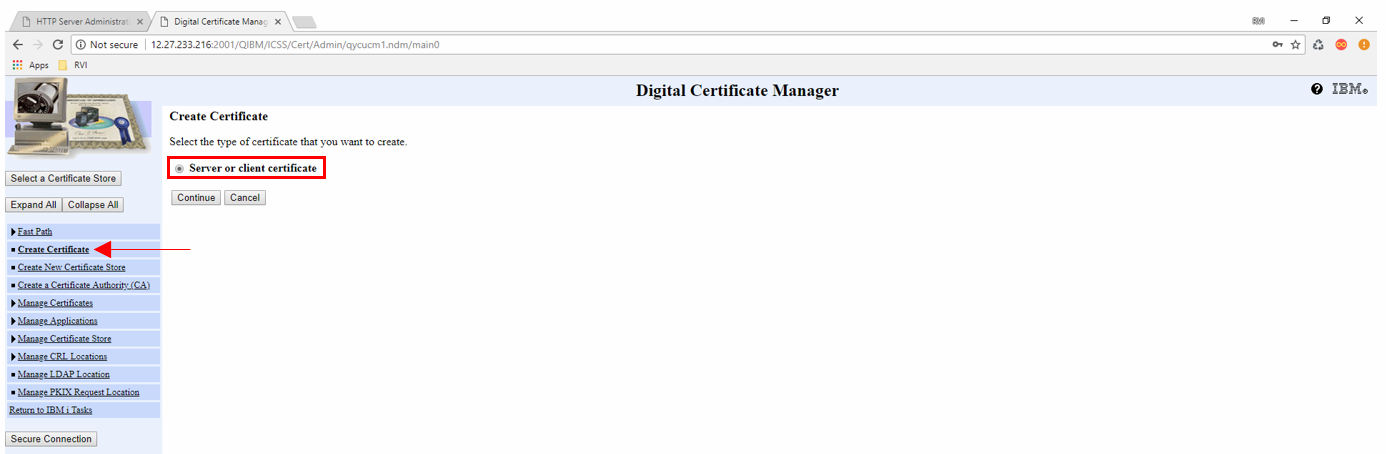


Step - 8 Enter your password. Click Continue.



Step - 9 Create a certificate key to send to the public certificate authority. On the left, select **Create Certificate**.

Step - 10 Select **Server or client certificate**. Click Continue.



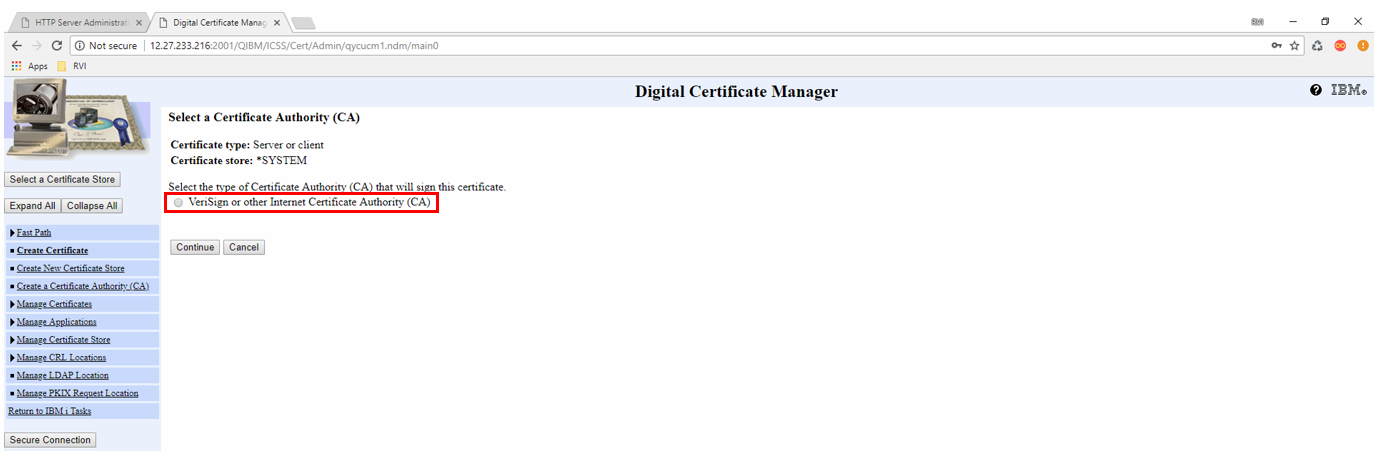
Step - 11 Select **Verisign or other Internet Certificate Authority** **(CA)**. Click Continue.

Fill out the information accordingly. Once finished, this process will produce a Base64 key.

Make sure to save the key data in a text file named **SSLKEY** for later use.

Include “-----BEGIN NEW CERTIFICATE REQUEST-----” and “-----END NEW CERTIFICATE REQUEST-----" in the file.

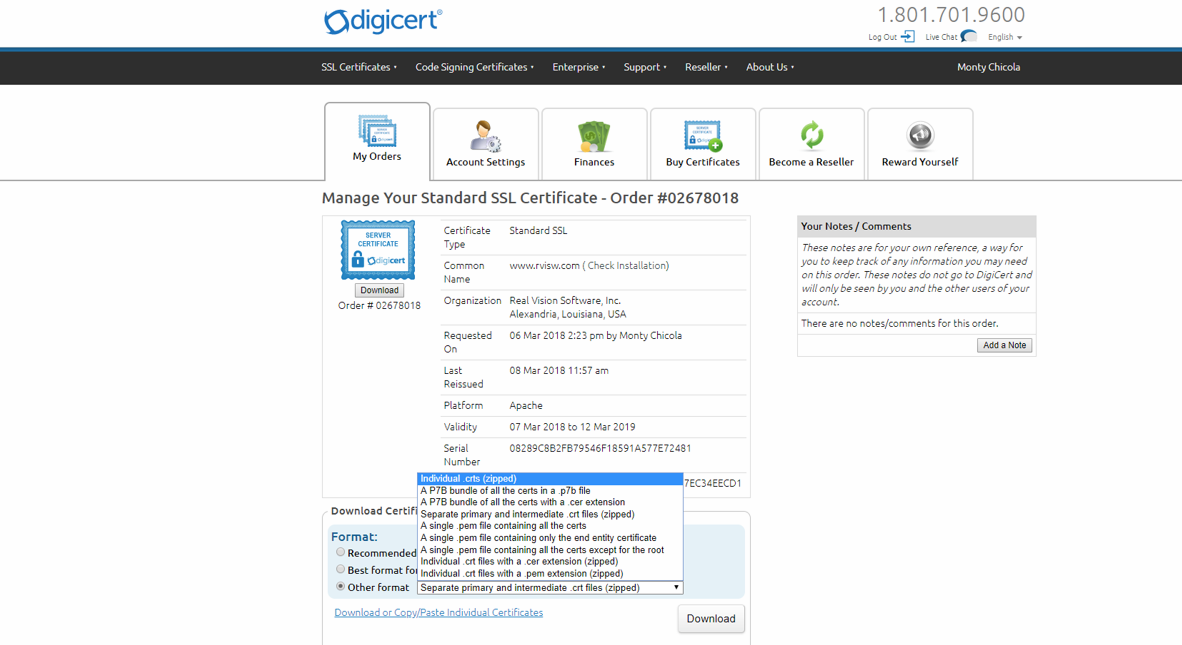
When you buy an SSL certificate, you will use this key as your “CSR” which is the key used to generate your certificate.



Step - 12 Take the key and go to [www.digicert.com](http://www.digicert.com) to download your certificates.

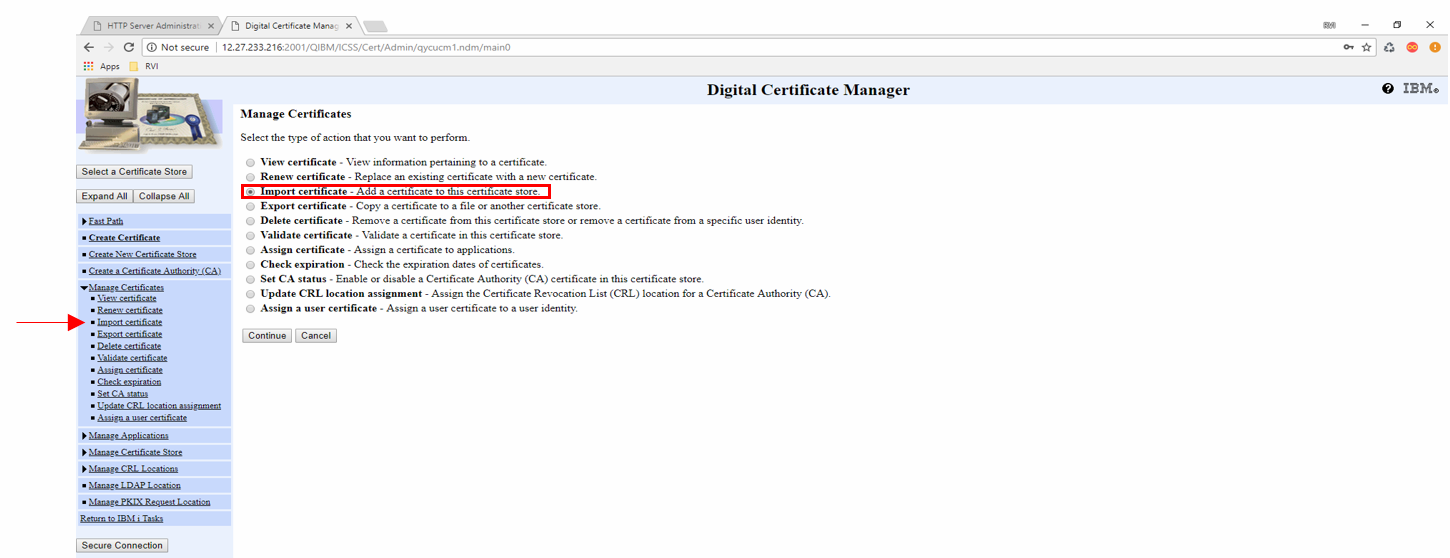
Select the options:

**Individual .crt files with a .cer extension (zipped)** and **A single .pem file containing all the certs**



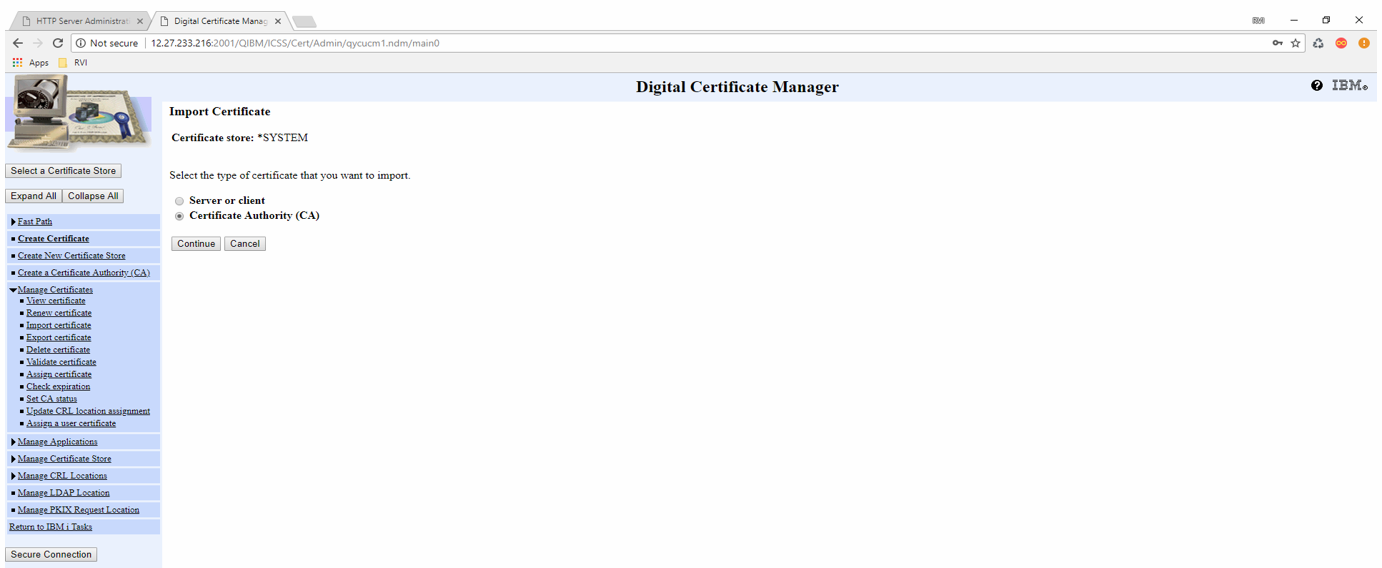
Step - 13 Now we are ready to import our certificates into the \*SYSTEM store.

In the Digital Certificate Manager, choose **Manage Certificates**. Select **Import Certificate**. Click Continue.



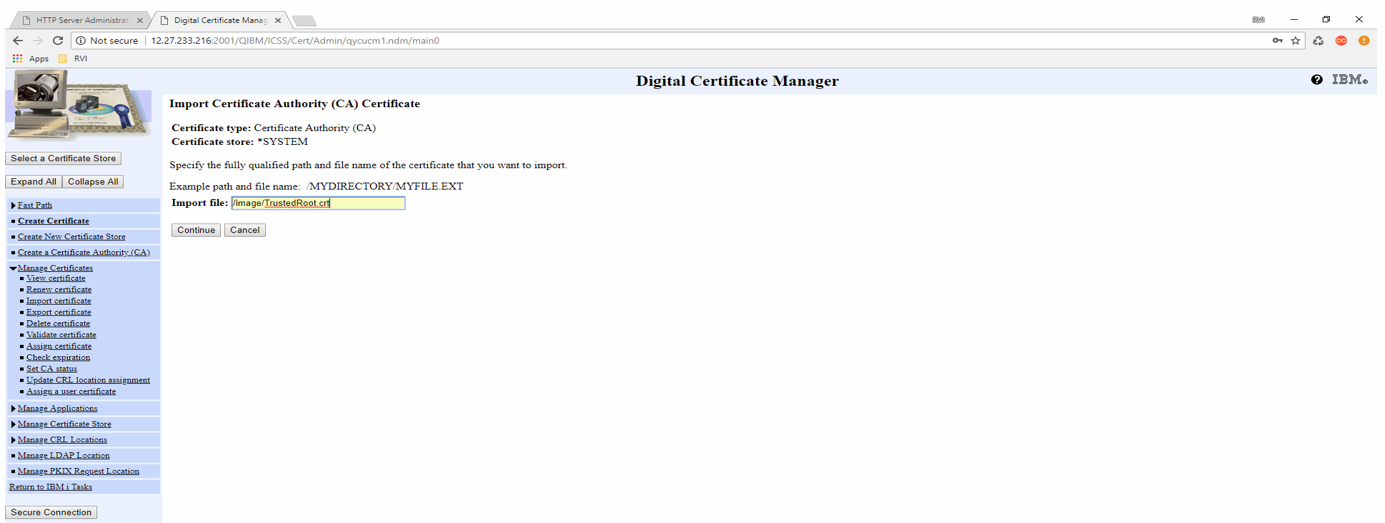
Step - 14 Select **Certificate Authority (CA)**. Click Continue.

*The Certificate Authority (CA) is the first certificate that needs to be imported in the TrustedRoot.cer.*



Step - 15 Put the path to the file in the text field. Click Continue.

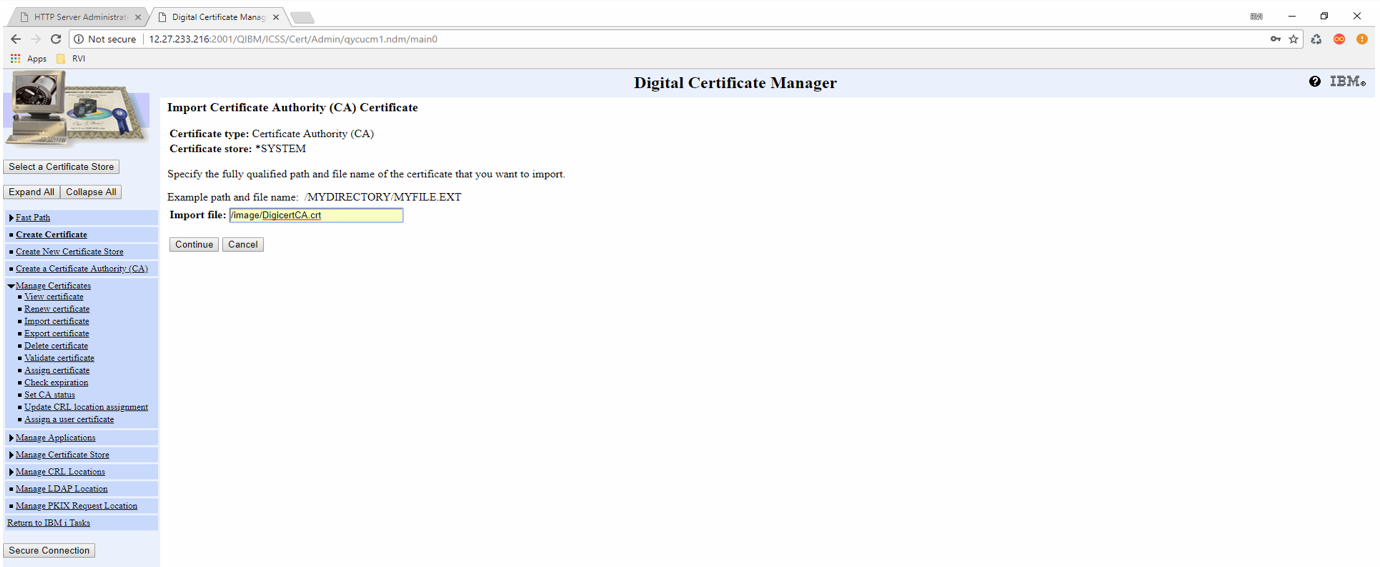
You will be prompted to assign a label to the certificate. (*You can name it anything*.) Click Continue.



This should show a successful import. Click Continue.

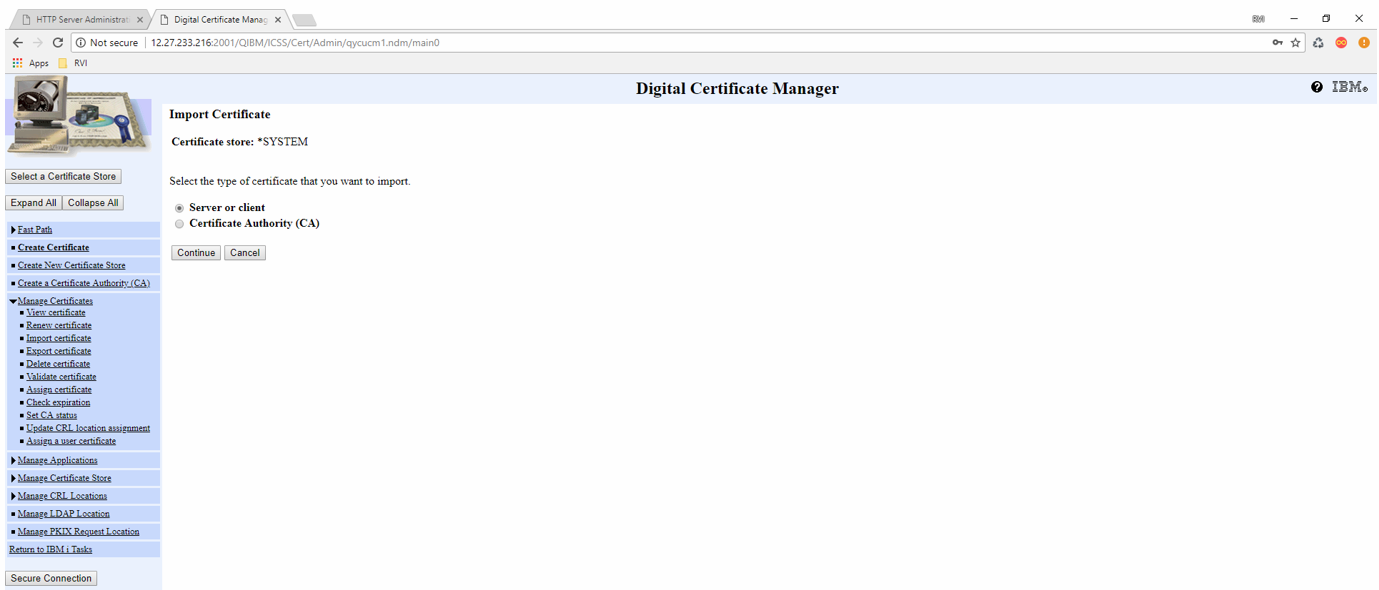
Step - 16 Import the **DigicertCA.cer**.

Put the path to the file in the text field. Click Continue. Assign a label to the certificate. Click Continue until you return to the “Manage Certificate Screen”.



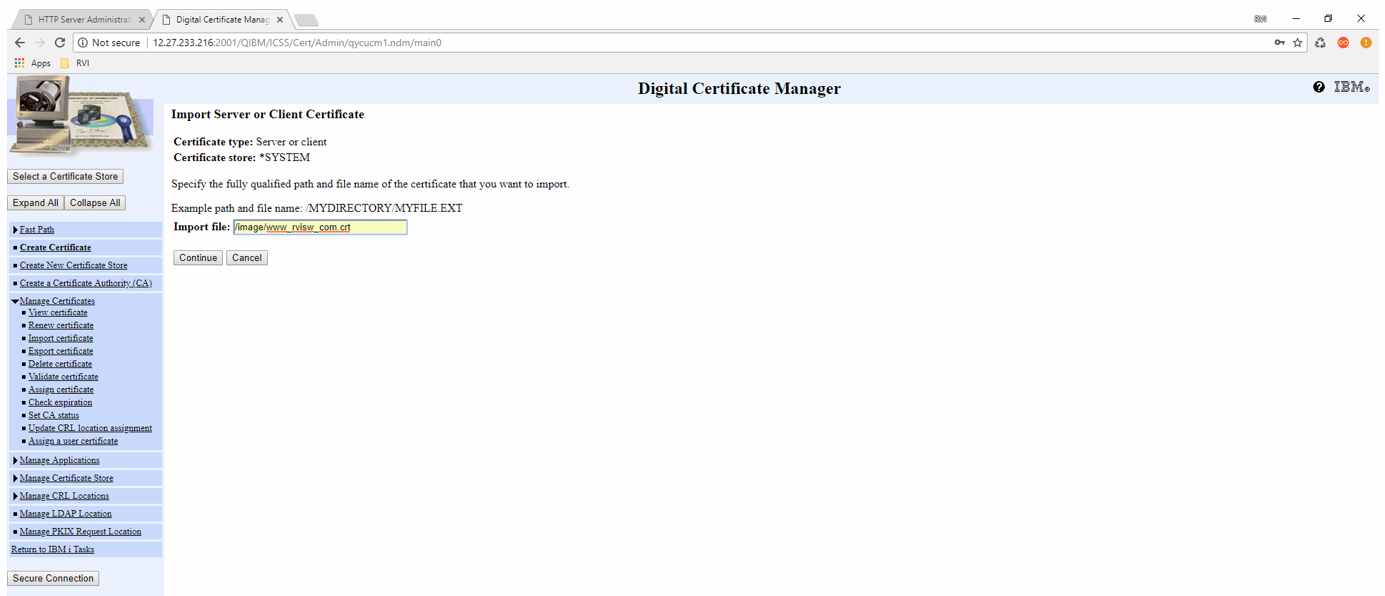
Step - 17 Import the 3rd certificate which will be used to authenticate the server.

Under **Manage Certificates**, select **Import certificate.** Select **Server or Client.** Click Continue.



Step - 18 Put the path to the final certificate which in this case is named www\_rvisw\_com.cer

Click Continue. This should show a confirmation screen if done correctly.



Step - 19 Make sure the RVIWEB web server instance has been created before proceeding.

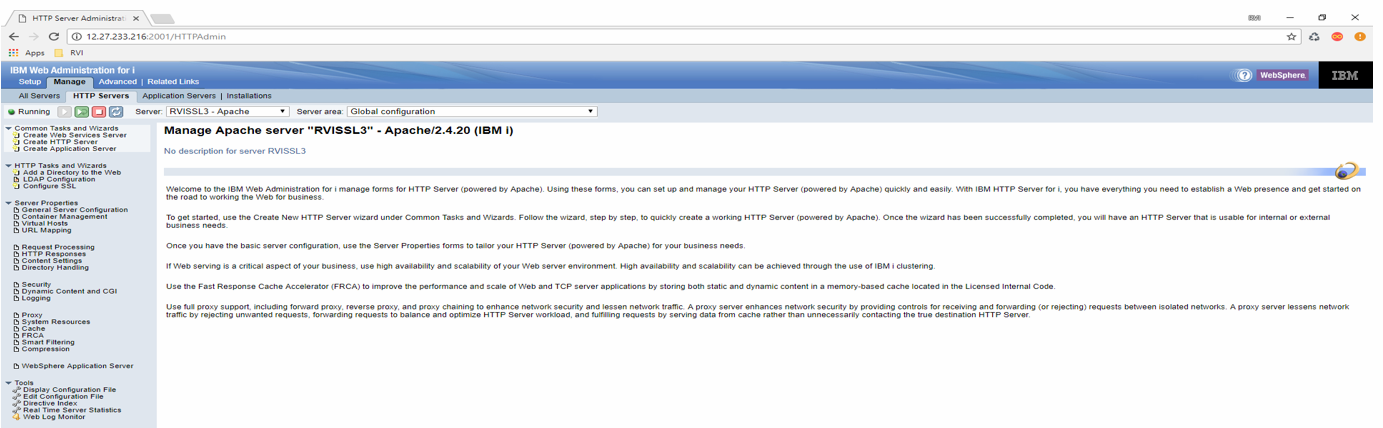
For instructions on creating the RVIWEB server instance use this link: (*Note: create the standard instance using F5. You do not need a secure instance since you are using SSL.*)

<https://www.manula.com/manuals/real-vision-software-inc/rvi-one-look/2/en/topic/how-to-setup-the-rviweb-server-on-the-ibmi>

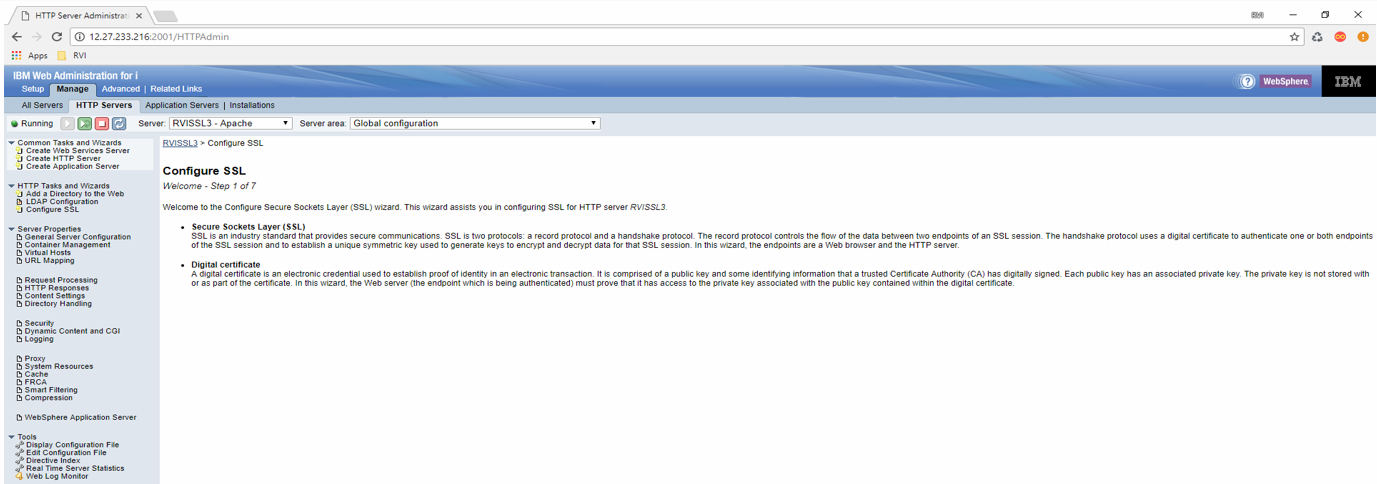
Once the web server instance is created, continue to the IBM HTTPADMIN in the browser.

Ex. <http://12.27.233.216:2001/HTTPAdmin>

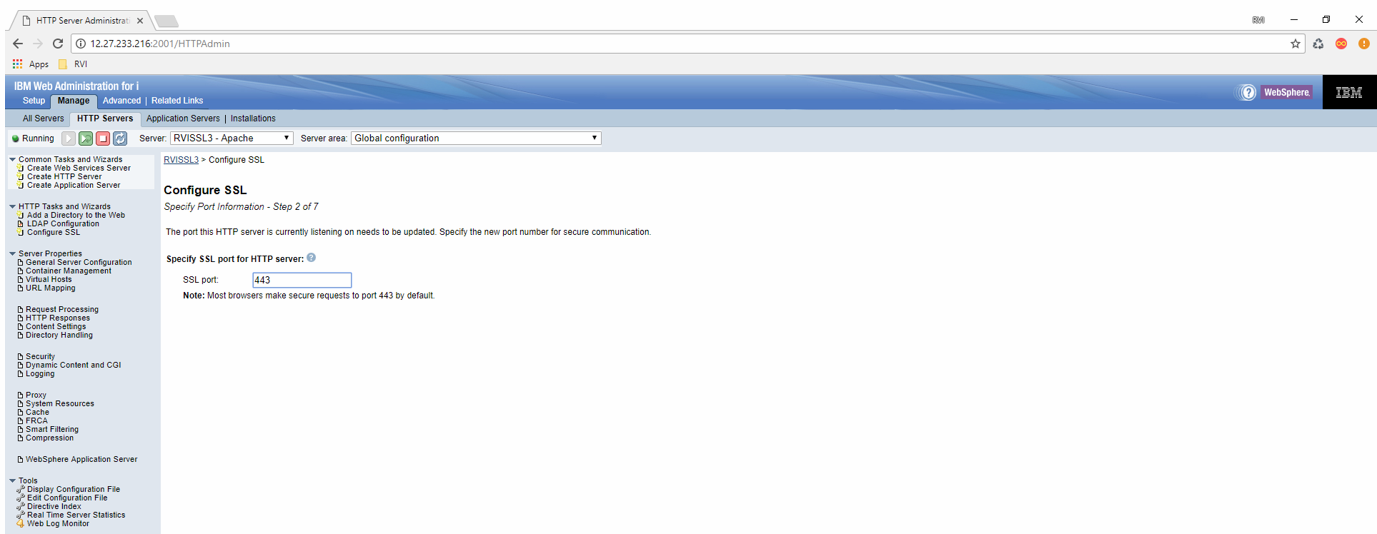
Step - 20 Select the **HTTP Servers** tab. Select the instance you just created. (For this example, it is RVISSL3)



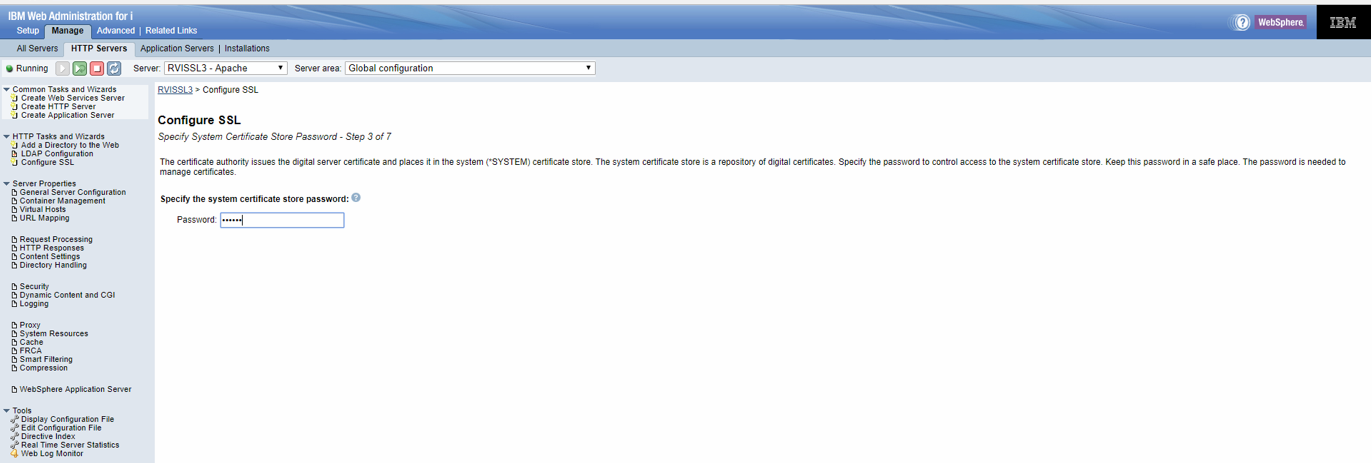
Step - 21 In the left pane under **HTTP Tasks and Wizards**, select **Configure SSL**.



Step - 22 Click Next. Keep the default port **443** and then click Next.

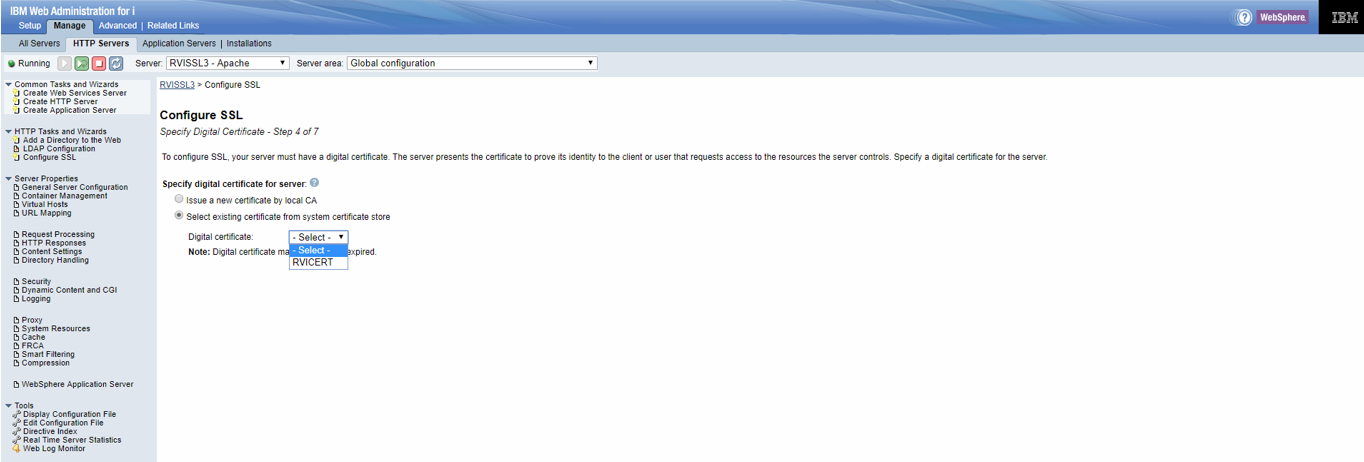


Step - 23 Enter the password that you created for the \*SYSTEM store. Click Next.

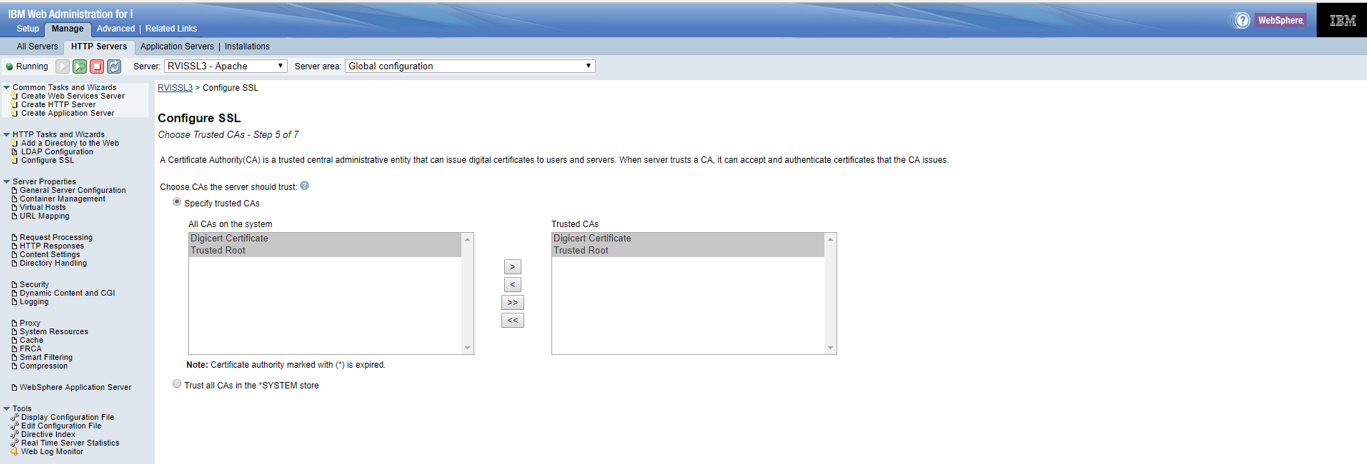


Step - 24 Choose **Select existing certificate from systems certificate store**.

You should see the certificate that you created and imported. Select that certificate. Click Next.

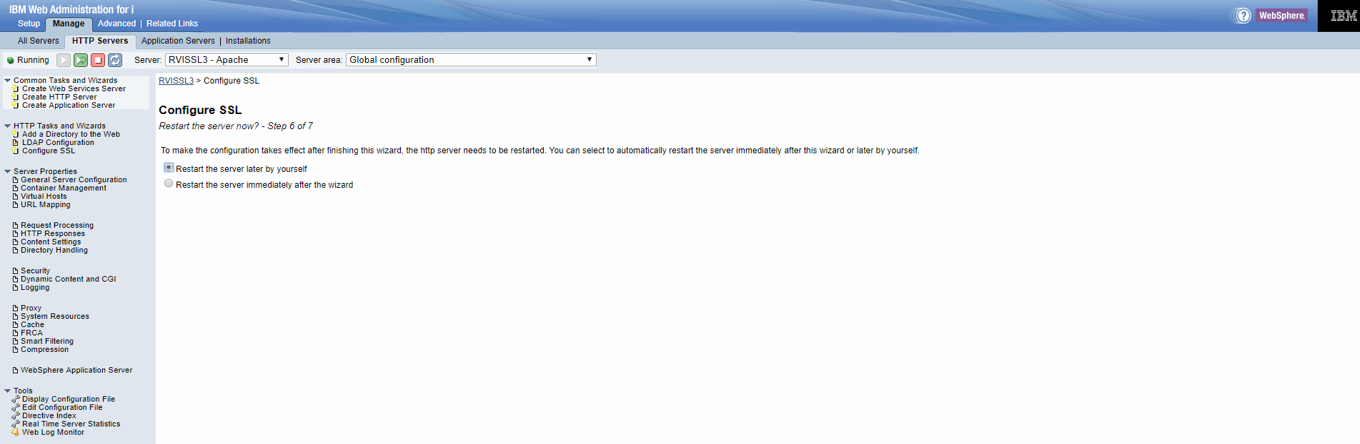


Step - 25 You will be prompted to select the Trusted CA’s. Select both **Digicert Certificate** and **Trusted Root** certificate. Click Next.

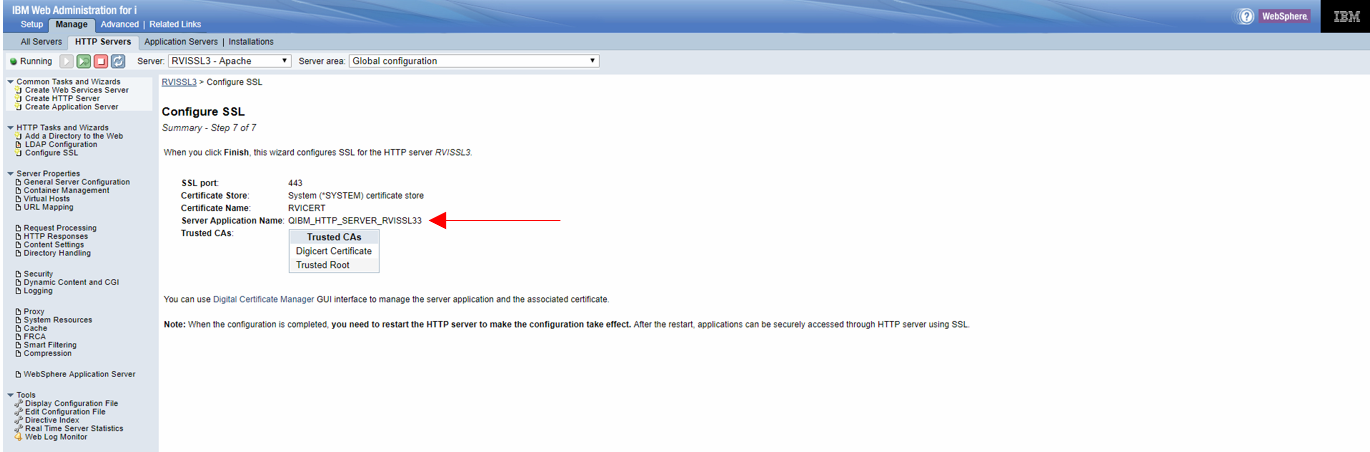


Step - 26 You will be asked to **Restart the server later by yourself** or **Restart the server immediately after the wizard**.

For this example, we selected *Restart the server later by yourself*.



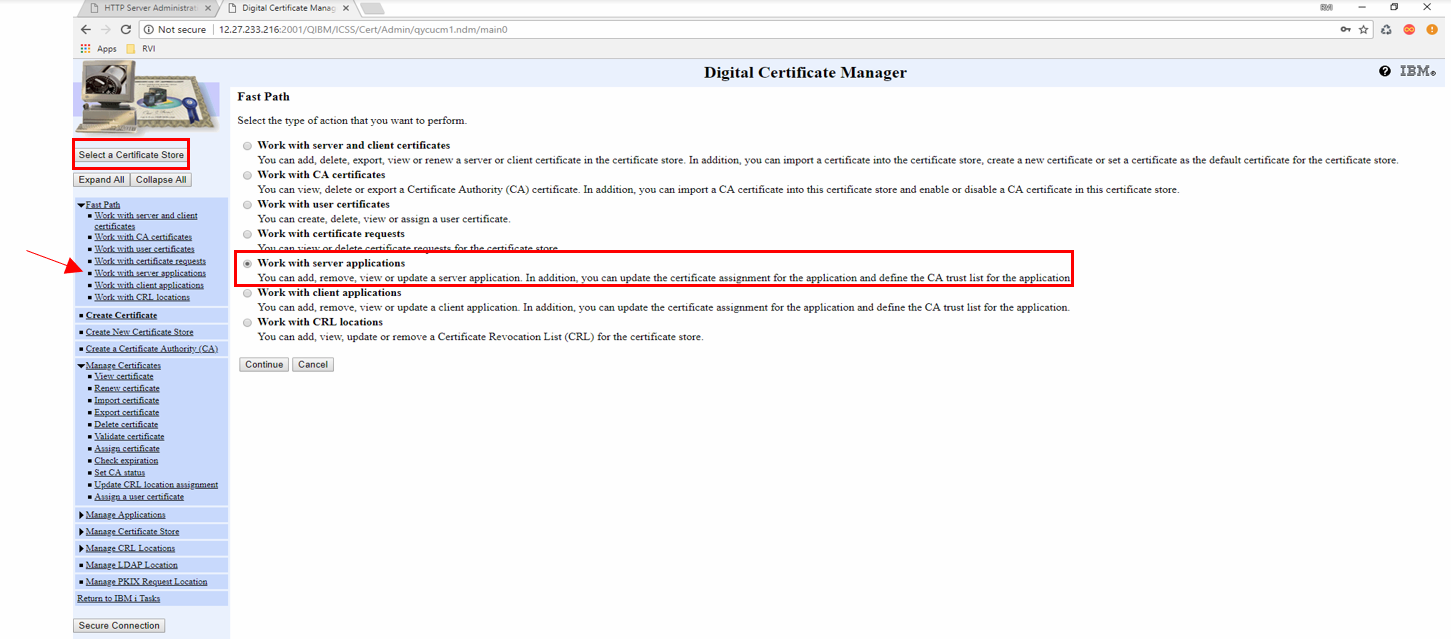
Step - 27 Once finished with the SSL wizard, you will see the final product of your SSL configuration. Make note of the **Server Application Name**. It will be used in the next steps. Click Finish.



Step - 28 Return to the Digital Certificate Manager. If not already in the \*SYSTEM store, click **Select a Certificate Store**, select the \*SYSTEM store and sign in.

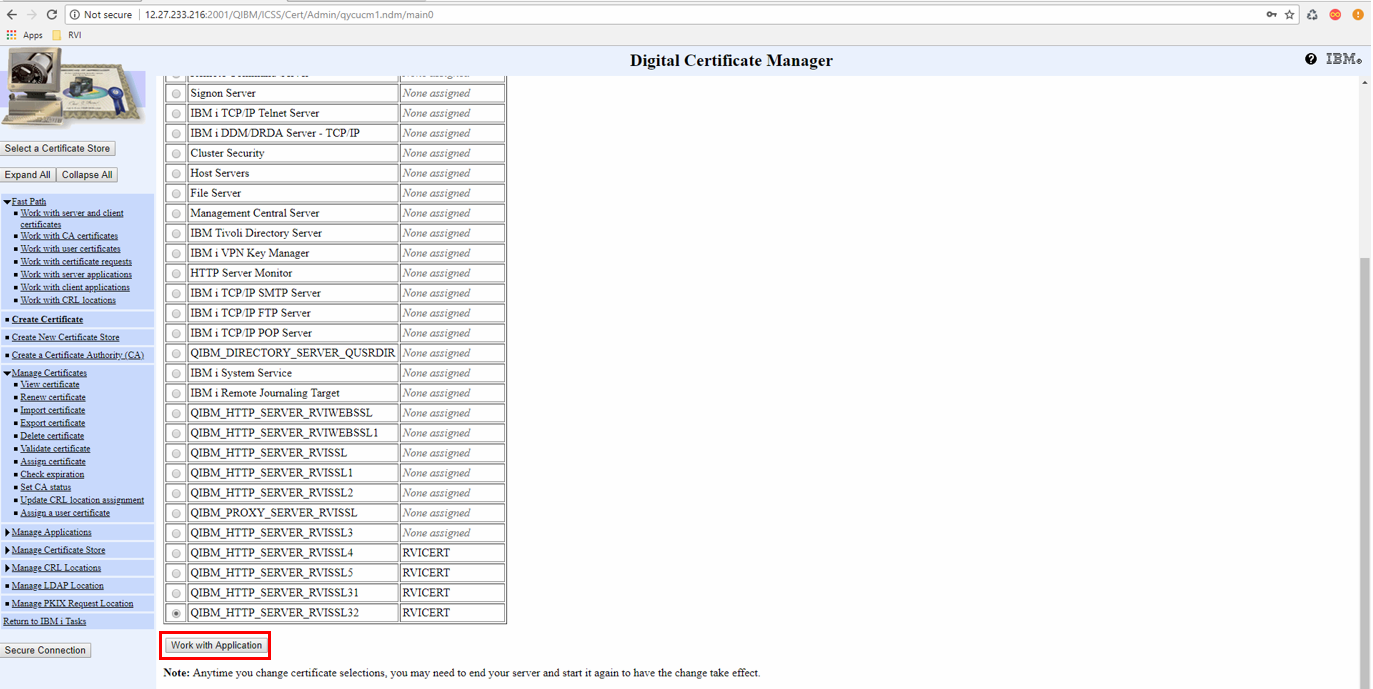
In the left pane, click **Fast Path**.

Select **Work with server applications**. Click Continue.

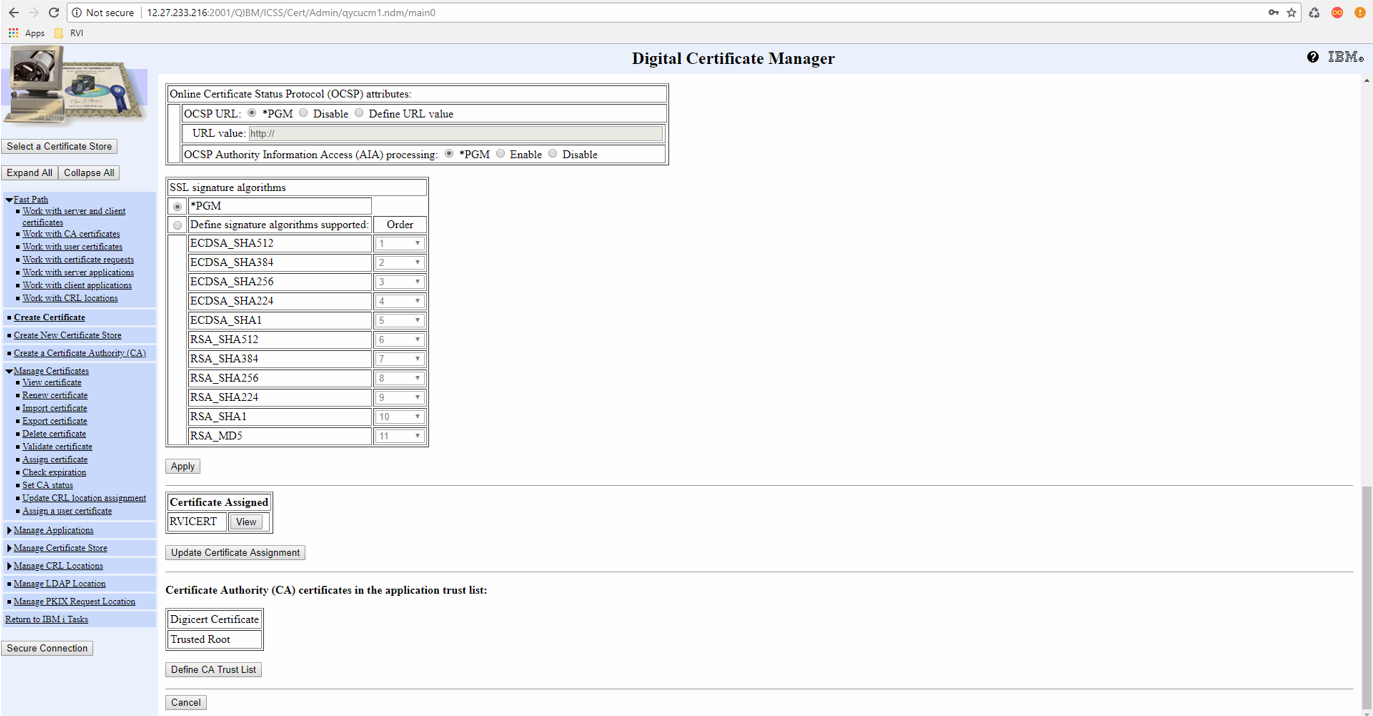


Step - 29 Select the server application name that was created from the SSL configuration wizard.

Click **Work with Application**.

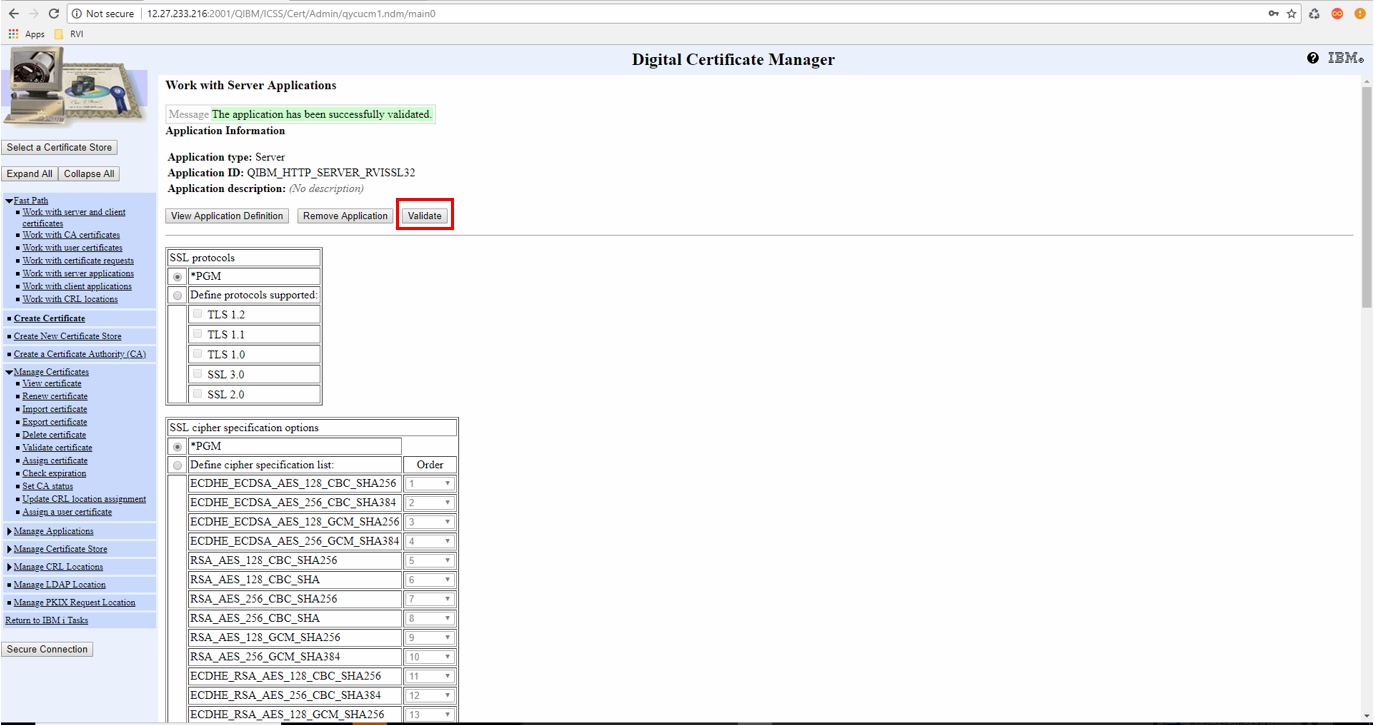


Step - 30 Scroll to the bottom. You will see the certificate that you assigned to the HTTP server program and the two trusted CA certificates underneath it.



Step - 31 To check and make sure everything is correct, scroll to the top and click on the **Validate** button.

You should get a confirmation that everything is set up correctly.



Step - 32 Start up the HTTPS server instance and test out the SSL configuration.

If you need to install RVI’s Secured WebSocket please refer to WSS SSL Configuration for IBM I.docx.

For more information on your certificate and to test your domain address go to <https://www.digicert.com/help/>