**SSL Certificate Installation and Binding**

**SSL Certificate:**

**Verifying** an **SSL certificate** is the process of ensuring the **certificate** the site holds is valid and identifying it correctly.

**Pre-requisites:**

* SSL Certificate
* PowerShell
* Internet Information Services(IIS) Manager
* Microsoft Management Console(MMC)

**SSL Certificate Installation and Binding:**

Follow the below steps to install SSL certificate and to add certificate binding to the web app.

**Step 1:**

Open PowerShell and Use the following commands to get the content of the SSL certificate.

Command 1:

**$fileContentBytes = get-content ‘C:\Desktop\Certificates\<certificate name>.pfx’ -Encoding Byte**

Note: Use certificate location path in above specified path.

Command 2:

**[System.Convert]::ToBase64String($fileContentBytes) | Out-File -Encoding ASCII ‘<Certificate name >.pfx.txt’**

**Step 2:**

Open the converted SSL certificate text file and **copy the content** in it (Note: remove unnecessary spaces at the last)

**Step 3:**

Login to VM of respective environment and create a text file and paste the content of SSL certificate text and click on **save as** and save the file name (file name will **be certificateName +.pfx**, save as type will be **‘All’**, Encoding will be **‘ANSI’**).

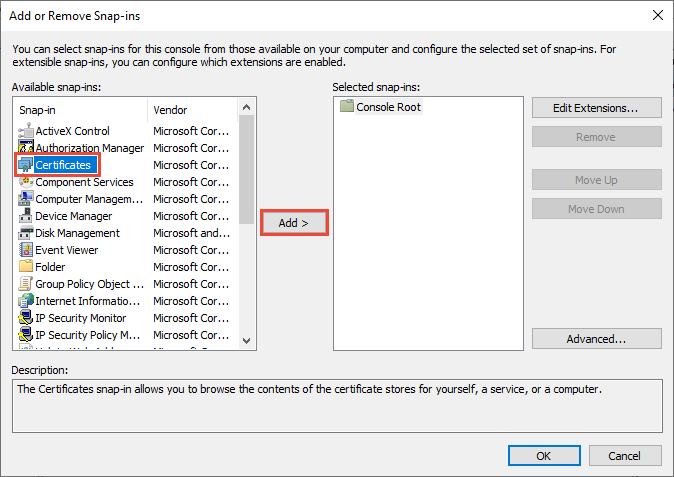
**Step 4:**

The next step is to import certificate using MMC Snap-In.

Open Microsoft Management Console(MMC), From the **File** menu, select **Add/Remove Snap In**. From the **Available snap-ins** list, choose **Certificates**, then select **Add**.

**Note:** Refer the below figure **Add or Remove Snap-ins**

In the **Certificates snap-in** window, select **Computer account and Select Next.** In the **Select Computer** window, leave **Local computer** selected, and then select **Finish**.



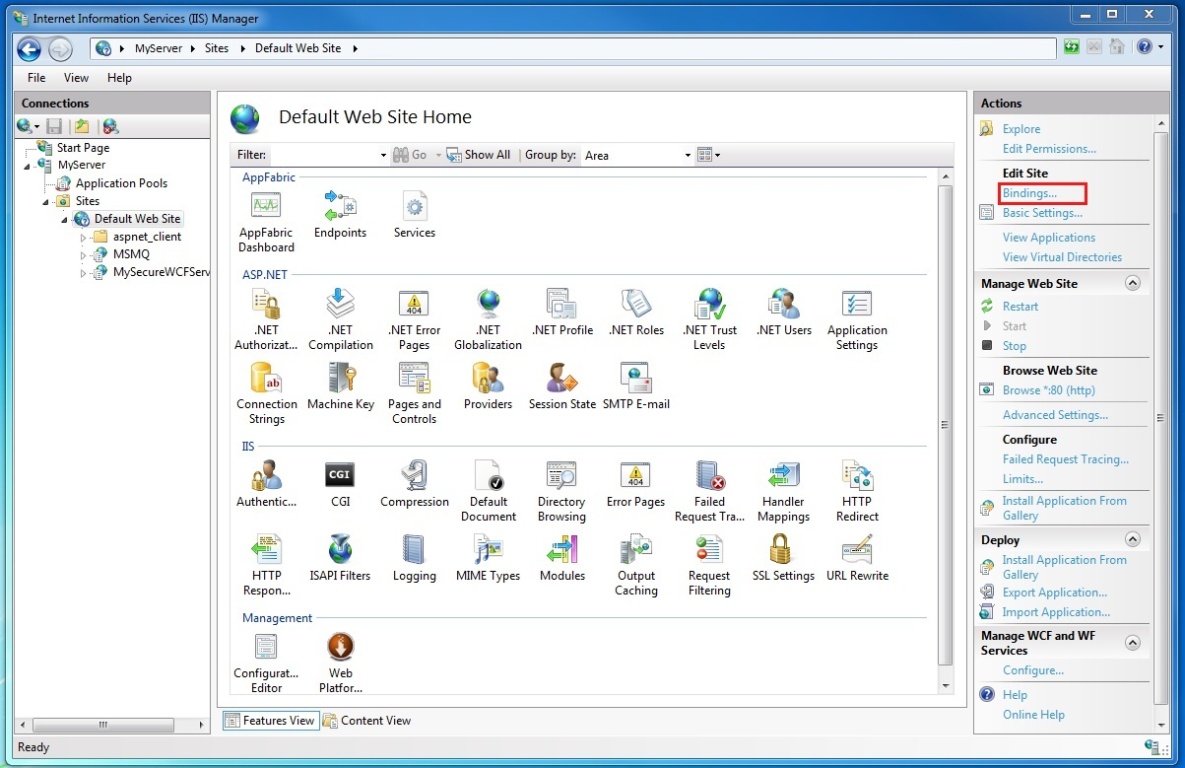
Note: This image is taken from Microsoft Website

**Step 5:**

The next step is to bind the SSL Certificate to HTTPS port 443. Binding refers to the process of configuring the certificate to use port 443 on the web application.

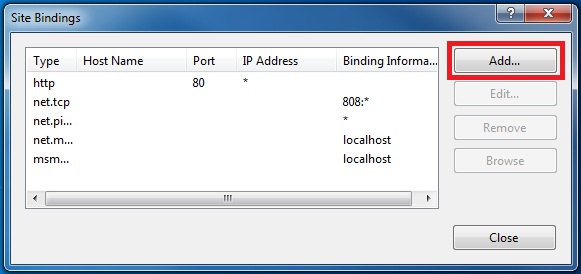
Open **Internet Information Services(IIS) Manager** for mapping the imported SSL Certificate and follow the below steps to add binding:

Click the **Bindings….** Link in the **Actions** section in the upper right hand portion of the window.



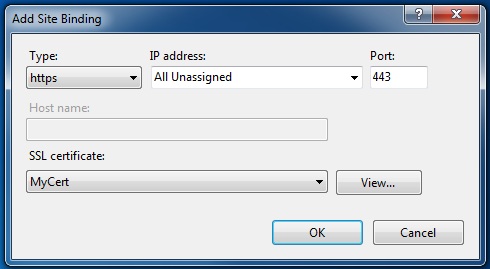
Note: This image is taken from Microsoft Website

In the Site Bindings window click the **Add** button.



Note: This image is taken from Microsoft Website

In the **Add Site Binding** dialog, select https for the type and configure port to 443 and the friendly name of the certificate. From SSL Certificate drop down box select imported certificate and click on ok to add.



Note: This image is taken from Microsoft Website

**Step 6:**

After binding the certificate to the web app, restart the web app.

In the IIS Manager, Click the **Restart** Link in the **Actions** section in the upper right hand portion of the window under Manage Web Site to restart the application.

**Step 7:**

The final step is to **test** the application.

Test the web application page using an **HTTPS URL** such as https://<domain-name>.com/<app-name>  
  
**For example:**   
Dev URL: <https://dev-google-app.com/Tulip-AI>  
INT URL: <https://int-google-app.com/Tulip-AI>  
QA URL: <https://qa-google-app.com/Tulip-AI>  
PROD URL: <https://google-app.com/Tulip-AI>

Note: These are the sample url’s, it doesn’t refer to any of the website url’s.

\*\*\* THE END \*\*\*