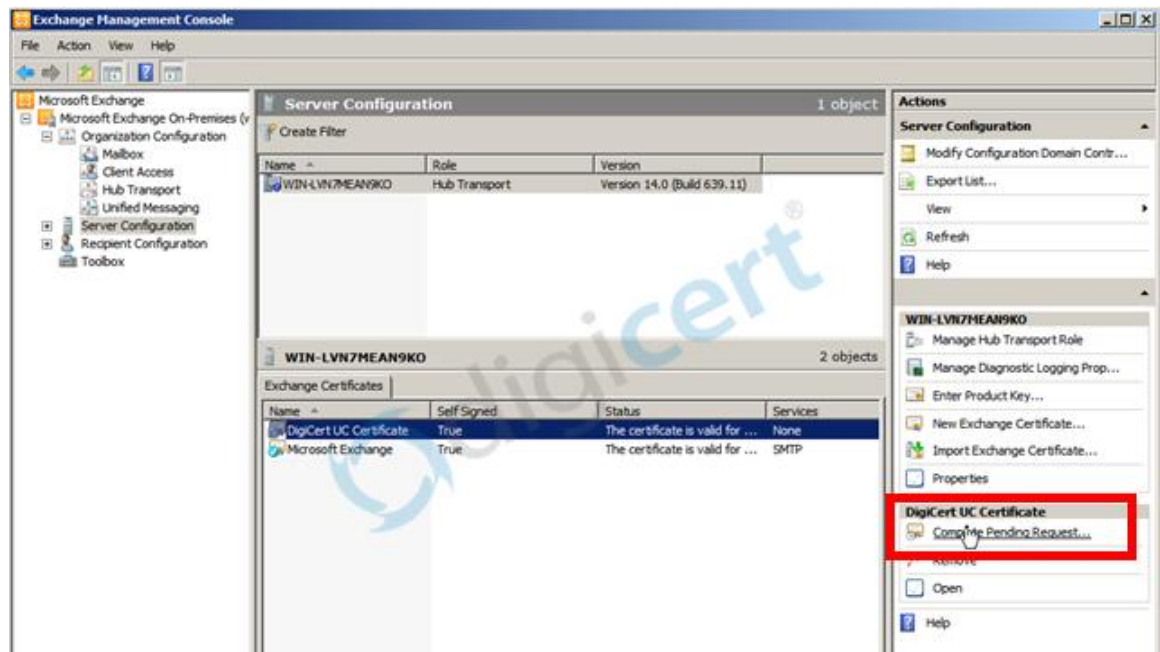
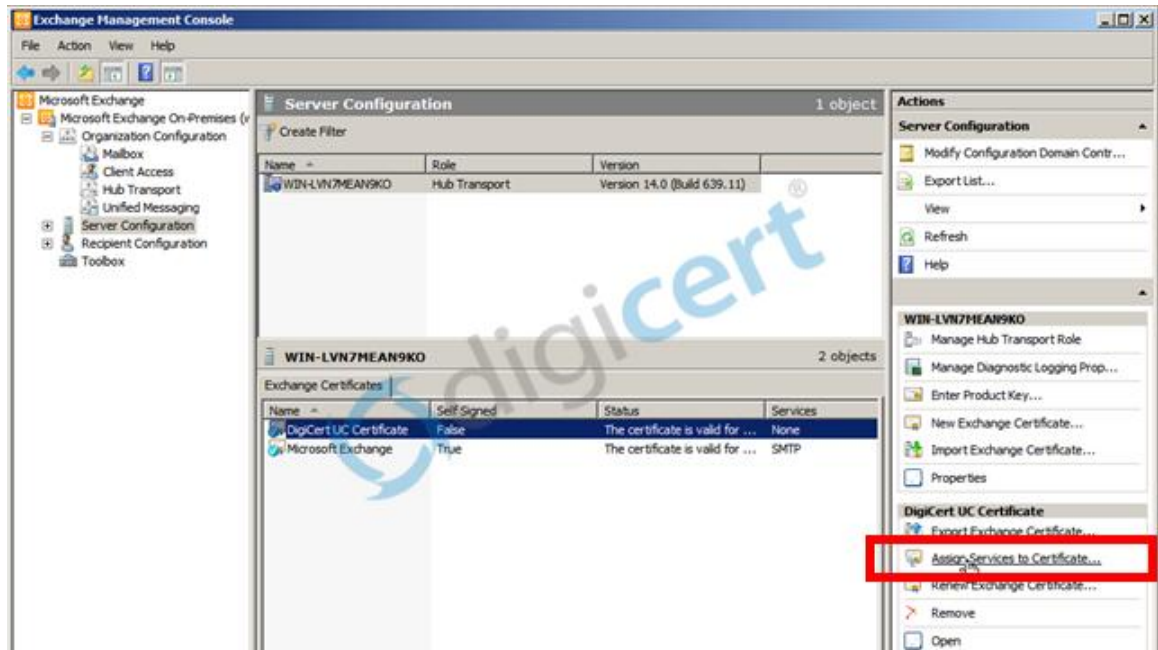


## SSL Installation Microsoft Exchange Server 2010

1. Copy the SSL.cer file to your Exchange server
2. Start the Exchange Management Console by going to **Start > Programs > Microsoft Exchange 2010 > Exchange Management Console**.
3. Click the link to "Manage Databases" and click on Server Configuration on the left-hand pane.
4. In the **Exchange Certificates** section in the middle pane, you should see the friendly name that you entered while creating the CSR. Click and highlight it and then click on **Complete Pending Request** from the action menu in the right hand pane.
5. A new window appears that resembles a Wizard with a heading of **Complete Pending Request**. Click on the **Browse** button and navigate to where you saved your Certificate file with extension \*.cer



6. Back in the **Exchange Certificates** section, click on the certificate you want to install from the list and then on the right-hand pane, click on the **Assign Services to Certificate** link.



7. A new window appears similar to the previous wizard that you had before. This window is named **Assign Services to Certificate**. In the Select Servers field, you want to click on highlight the server that you want to assign the certificate to and click on the **Next** button.
8. On the **Select Services** screen, click on the services that you would like to secure using the certificate. By default, **Internet Information Services** is selected. When you have selected the services, click on the **Next** button
9. At the **Assign Services** screen, you will see a **Configuration Summary** of the certificate. When you have read over the configuration, click on the **Assign** button.
10. The **Assign Services to Certificates** wizard will load the certificate and complete. The **Completion** screen will display that will summarize the installation of the certificate. Click on the **Finish** button at the bottom of the Wizard.
11. When you are ready, click on the **Finish** button.

- **Install Intermediate Certificate CA**
  1. Type **mmc** in the **Start search** box after pressing the Start menu to start the Microsoft Management Console (MMC).
  2. In the Management Console, select **File** then **Add/Remove Snap In**.
  3. In the **Add or Remove Snap-ins** dialog, click the **Add** button and then select **Certificates**.
  4. Choose **Computer Account** then click **Next**.
  5. Choose **Local Computer**, and then click **Finish**.
  6. Close the **Add or Remove Snap-ins** dialog and click **OK** to return to the main MMC window.
  7. If necessary, click the **+** icon to expand the Certificates folder so that the **Intermediate Certification Authorities** folder is visible.
  8. Right-click on **Intermediate Certification Authorities** and choose **All Tasks**, then click **Import**.
  9. Follow the wizard prompts to complete the installation procedure.
  10. Click **Browse** to locate the certificate file. Change the file extension filter in the bottom right corner to be able to select the file. Click **Open** after selecting the appropriate file.
  11. Click **Next** in the Certificate Import Wizard.
  12. Choose **Place all certificates in the following store**; then use the Browse function to locate Intermediate Certification Authorities. Click **Next**. Click **Finish**.

Don't forget to take Backup from the certificate

- **Taking Backup**

1. Type **mmc** in the **Start search** box after pressing the Start menu to start the Microsoft Management Console (MMC).
2. In the Management Console, select **File** then **Add/Remove Snap In**.
3. In the **Add or Remove Snap-ins** dialog, click the **Add** button and then select **Certificates**.
4. Choose **Computer Account** then click **Next**.
5. Choose **Local Computer**, and then click **Finish**.
6. Close the **Add or Remove Snap-ins** dialog and click **OK** to return to the main MMC window.
7. In the Personal certificate click the **+** icon to expand the Certificates folder so that you find your SSL certificate.
8. Right-click on **personal certificates** and chooses **All Tasks**, then click **Export**.
9. In the **Export File Format** window, ensure the option for **Personal Information Exchange - PKCS#12 (.pfx)** is selected.
10. Select **Include all certificates in the certificate path if possible** and then click **Next**. (If you do not select the Include all certificates in the certificate path if possible option, your server may not recognize the issuer of the certificate, which may result in security warnings for your clients.
11. De-select **Require Strong Encryption**. (This may cause a password prompt every time an application attempts to access the private key or it may cause IIS to fail)
12. Click **Next**.
13. Enter and confirm a password to protect the PFX file and click **Next**.

14. Choose a file name and location for the export file (do not include an extension in your file name; the wizard automatically adds the PFX extension for you).
15. Click **Next**