SARANGSoft

Setting up HTTPS in IIS

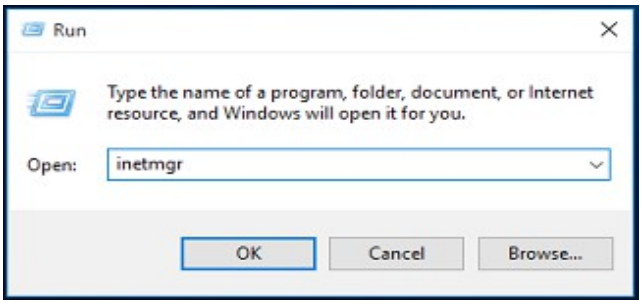
(June 2019)

Here are the steps for setting up a https server with IIS (version 7.0 and above) on Windows Server Operating System. This document has been created for setup of various SARANGSoft software products, viz., SysExpertez, WinBackup Business, and digipaper (Server component).

1. Steps to Get Your Common Name / Subject Name
2. How to Bind a Web Site with https
3. Scenarios Where a Trusted Certificate is Needed from a Certificate Authority

1. Steps to Get Your Server's Common Name / Subject Name

1. Open IIS (for that go to *Start → Run...*, type *inetmgr*, and press *Enter*).



2. In the left-pane, go to the *Web Site* (e.g., *Default Web Site*).
3. Right-click on the *Web Site* and select *Edit Bindings...*
4. The *Site Bindings* dialog will open. In this dialog, see if you have https under the *Type* column.
5. If so, select the column corresponding to https and click on *Edit*.
   If not, please refer to the ***How to bind a Web Site with https*** section below.
6. The *Edit Site Bindings* dialog will open. Under *SSL certificate* section, click on the *View...* button.
7. The *Certificate* dialog will open. Under the *General* tab, note down the value for *Issued to*.
8. This value is your server's ***Common Name / Subject Name***.

2. How to Bind a Web Site with https

Before binding a *Web Site* with *https*, please do the following steps.

1. Import a security certificate to IIS (SSL / TLS certificate).
2. Bind the security certificate to the web site to enable *https*.

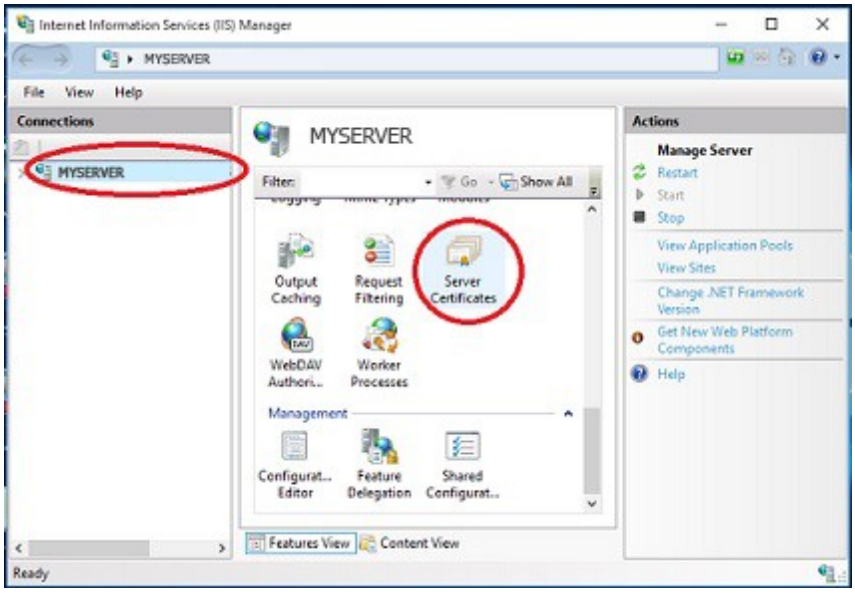
2.1. Importing a Security Certificate to IIS

A security certificate can be imported in two ways.

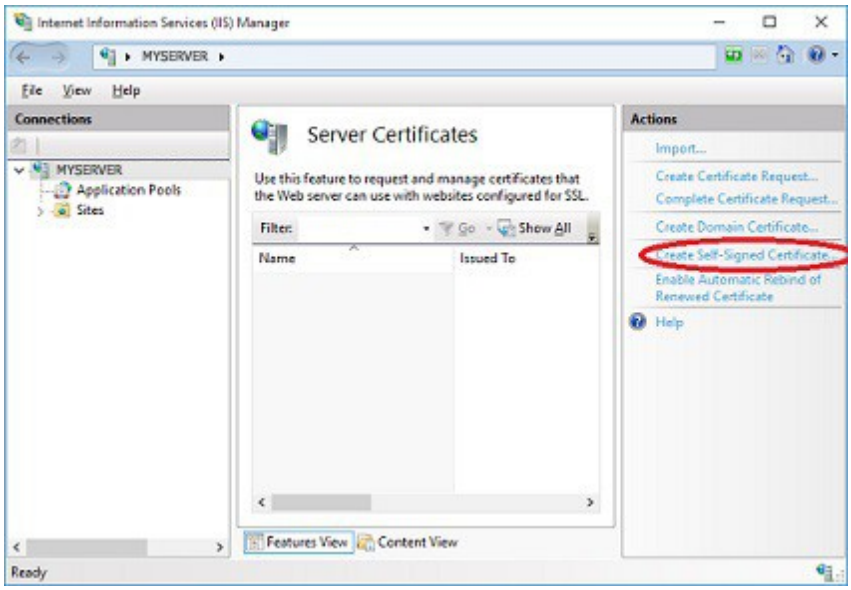
2.1.1. Option A: Creating a *Self-Signed Certificate* in IIS.

1. Open IIS (go to *Start → Run...,* type in *inetmgr,* and press *Enter*).

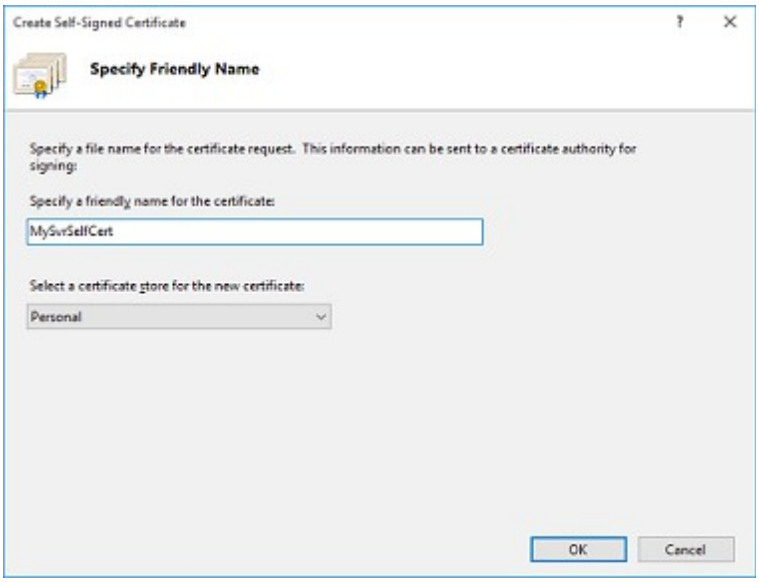
2. In the left-pane, select the server name.



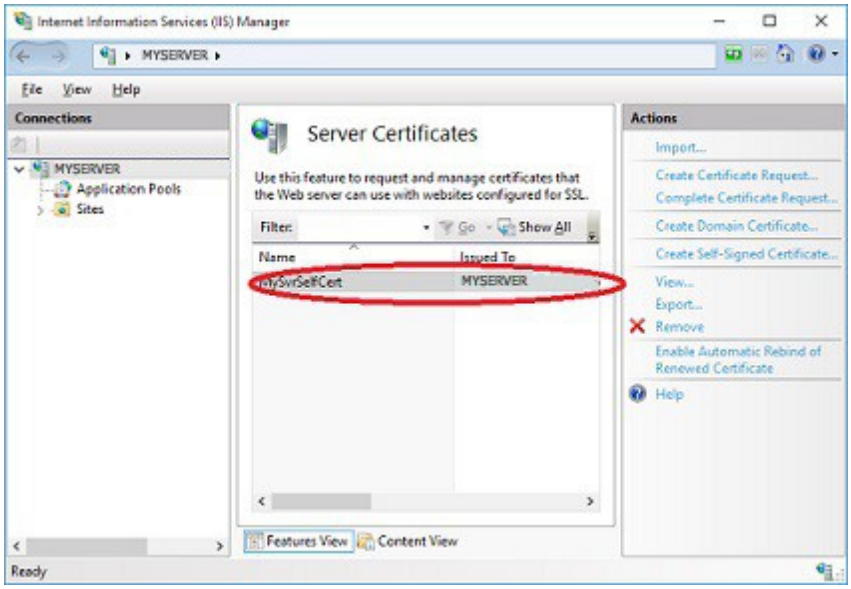
3. In the middle-pane, double-click on the *Server Certificates* icon.
4. In the *Actions* section, click on *Create Self-Signed Certificate...* in the right-pane.



5. In the *Create Self-Signed Certificate* dialog, specify a *Friendly Name* for the certificate, and click *OK .*



6. You will see your new certificate in the *Server Certificates* list.



2.1.2. Option B: Importing a Third-party Certificate from a Certificate Authority.

1. Purchase the certificate from a Certificate Authority. They will instruct you on how to get the certificate file (.PFX, .CER, or .CRT file) from their store / server.
2. After getting the certificate file, you will need to install the certificate file in your server. In general, just double-clicking on the certificate file will install it.
3. Once installed, you will need to import the certificate in IIS as follows.

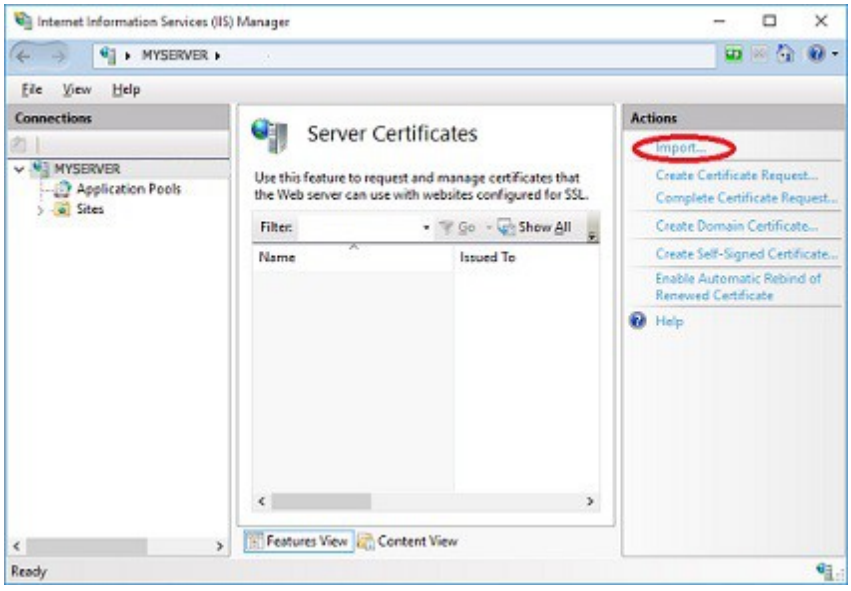
2.1.2.1. If the Certificate is a **PFX file**:

a) Open *IIS* (go to *Start → Run...,* type in *inetmgr,* and press *Enter*).

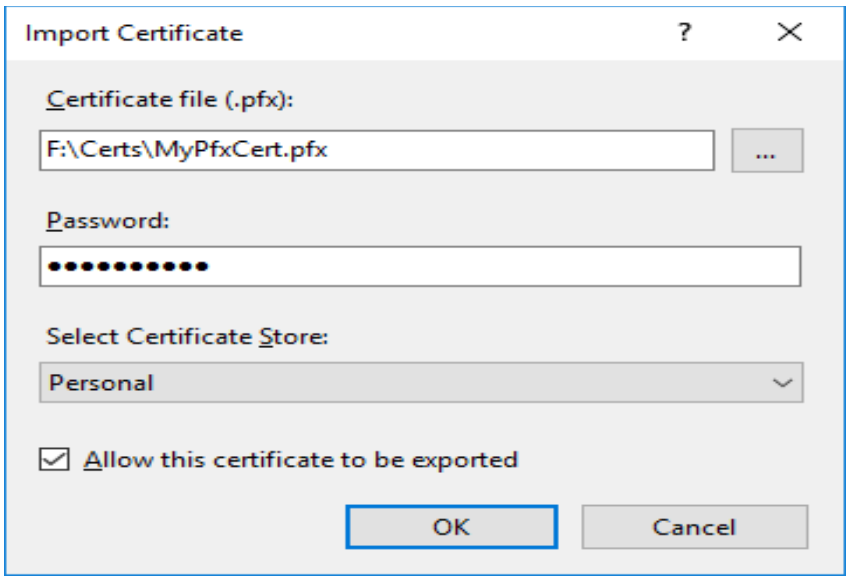
b) In the left-pane, select the required server name.

c) In the middle-pane, double-click on the *Server Certificates* icon.

d) In the *Actions* section, click on *Import...* in the right-pane.



e) In the *Import Certificate* dialog, browse to your PFX file, and put it in the *Certificate file (.pfx)* edit box.



f) Enter your PFX *Password* and click on *OK.* Your certificate will get imported in IIS.

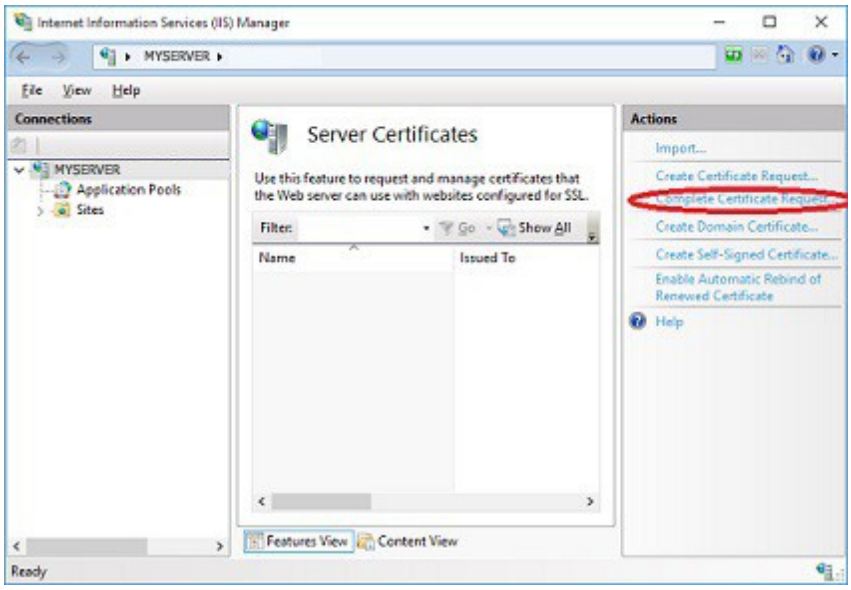
2.1.2.2. If the Certificate File is a **CER or CRT file**:

a) Open IIS (go to *Start → Run...*, type in *inetmgr*, and press *Enter*).

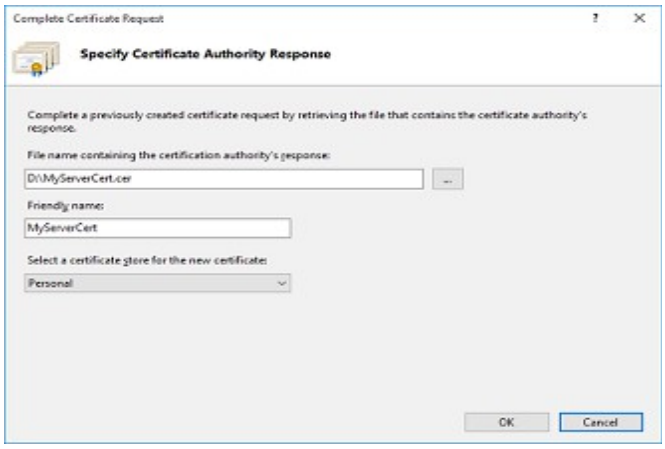
b) In the left-pane, select the required server name.

c) In the middle-pane, double-click on the *Server Certificates* icon.

d) In the *Actions* section, click on *Complete Certificate Request...* in the right-pane.



e) In *Complete Certificate Request* dialog, browse to the CER file, and put it in the *File name* edit box.

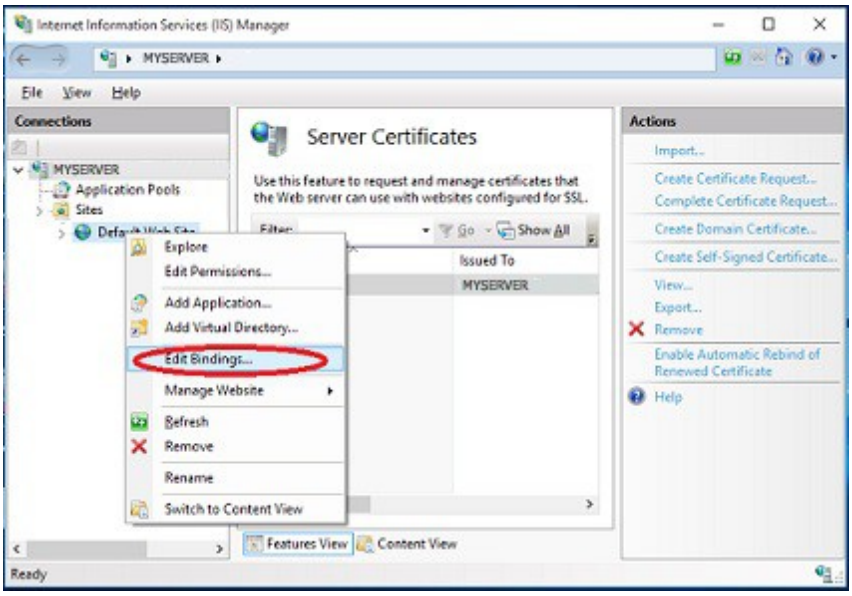


f) Next enter the *Friendly name,* and click *OK*. Your certificate will get imported in IIS.

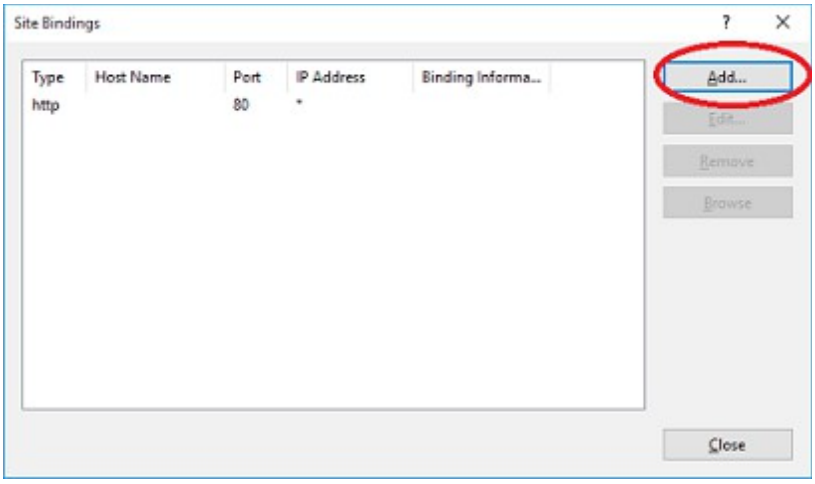
2.2. Bind the Security Certificate to the Web Site to Enable https

After your (SSL / TLS) certificate gets imported in IIS (either a Self-Signed Certificate or importing a Third-Party Certificate), the next step is to bind the certificate with the web site as follows.

1. Open IIS (go to *Start → Run...*, type in *inetmgr*, and press *Enter*).
2. Go to Web site (e.g., *Default Web Site*) in the left-pane.
3. Right-click on the *Web Site* and select *Edit Bindings...*



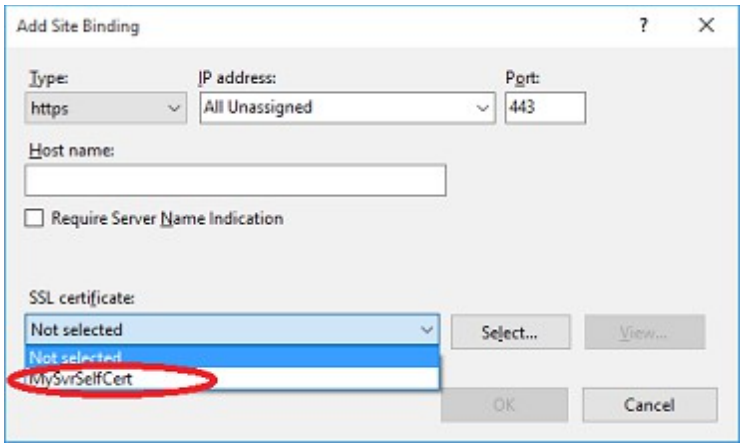
4. In the *Site Bindings...* dialog, click on *Add...*



5. In the *Add Site Binding* dialog, select *'https'* from the *Type* dropdown list.

6. The *Host name* is optional, but if you need to put the host name, it must be same as the certificate's *Common Name / Subject Name.*

7. Next select your certificate from the *SSL certificate* dropdown list.



8. Click *OK* and your certificate will be bound to the web site.

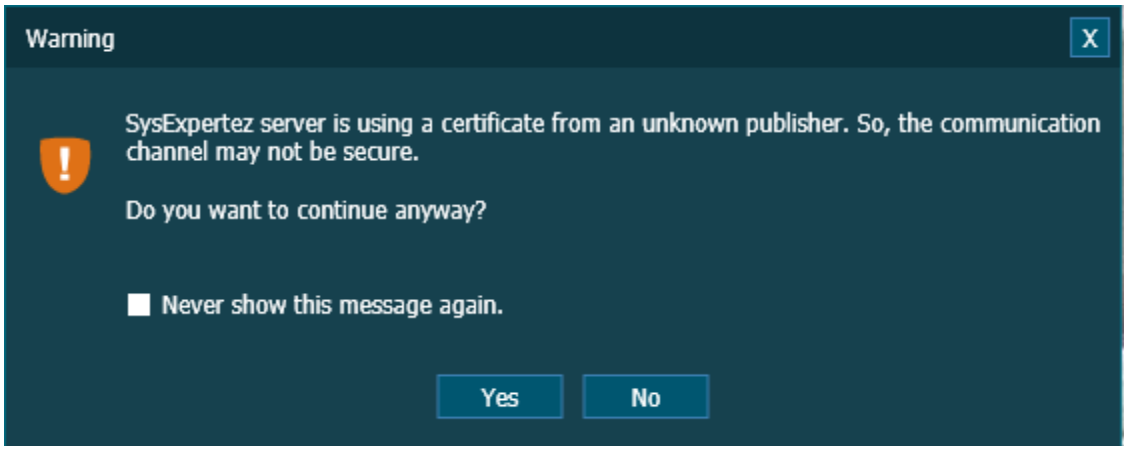
3. Scenarios Where a Trusted Certificate is Needed from a Certificate Authority

A Trusted Certificate from a Certificate Authority (CA) is highly recommended for the following cases. In this case, *SARANGSoft SysExpertez* has been used as an example to show / explain how this works.

a) For Deployment in Cloud: If '*SysExpertez Web Service and Database*' is installed in a cloud server (e.g., AWS or Azure) and the '*SysExpertez Agents*' and/or the *'SysExperetez Admin Console'* are installed on-premise and/or in cloud server instances.

b) If '*SysExpertez Agents*' or '*SysExpertez Admin Console*' are installed in different Active Directory domain(s) or workgroup(s) than '*SysExpertez Web Service*'.

In such cases, if a self-signed certificate binds with the IIS where 'SysExpertez Web Service' is hosted, the following security warning will be shown by SysExpertez.



If *SysExpertez Server* and *SysExpertez Admin Console* both belong to the same domain in different PCs / servers or within a Trusted Domain, the security warning about the self-signed certificate can be resolved as follows.

1. Export the Self-Signed Certificate from the *SysExpertez Server*.
2. Install the certificate in the '*Trusted Certificate Authority*' store of the server running *SysExpertez Admin Console*.

3.1. Export the Self-Signed Certificate from the *SysExpertez Server* computer.

a) On the computer hosting '*SysExpertez Web Service*', open IIS (go to *Start → Run...*, type in *inetmgr*, and press *Enter*).

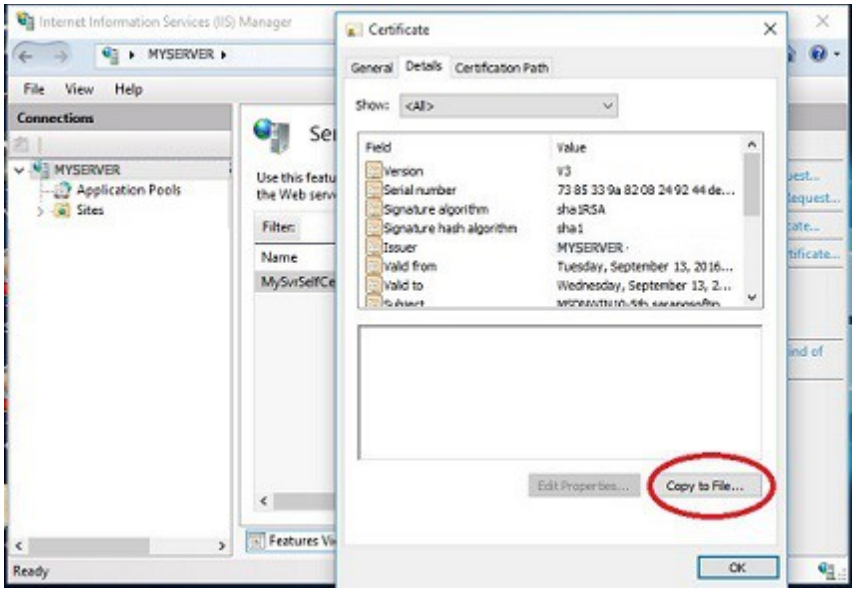
b) In the left-pane, select the server name.

c) In the middle-pane, double-click on the *Server Certificates* icon.

d) Double-click on the certificate, which binds to the Web Site.

e) The *'Certificate'* property sheet will appear. Click on the *'Details'* tab.

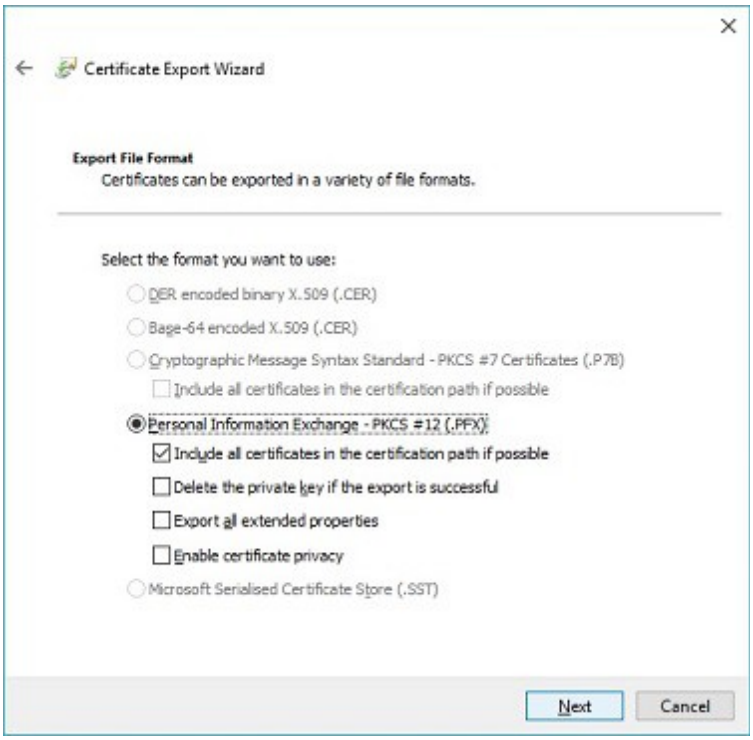
f) Click on the *'Copy to File...'* button.



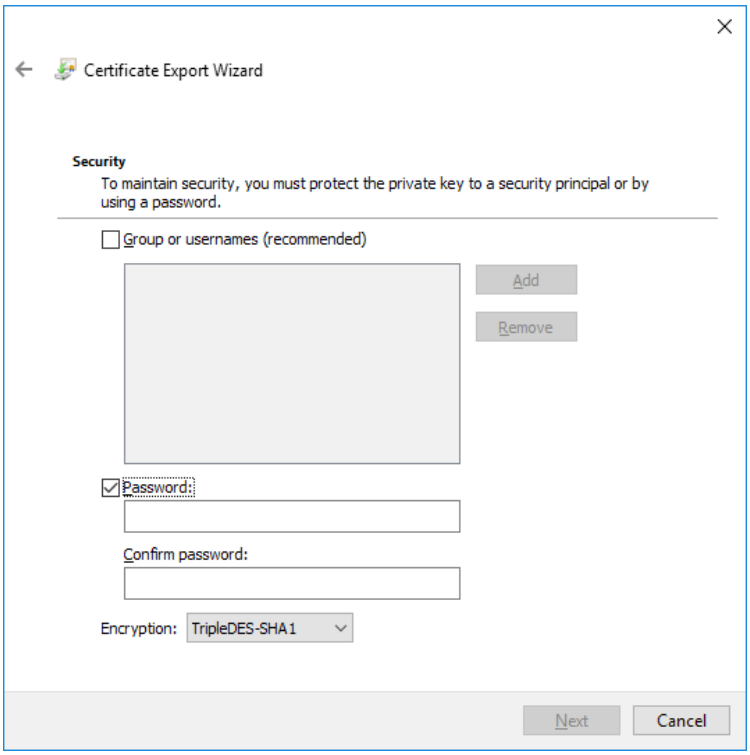
g) Click on *Next* in *'Certificate Export Wizard'.*

h) In the *Export Private Key* page, select the '*Yes, export the private key'* radio button.

i) In the *'Export File Format'* page, select the *'Personal Information Exchange – PKCS#12 (.PFX)'* radio button.



j) In the *'Security'* page of *'Certificate Export Wizard'*, select the *'Password'* checkbox, type in the password of your choice in both the '*Password'* edit box and the '*Confirm password'* edit box.

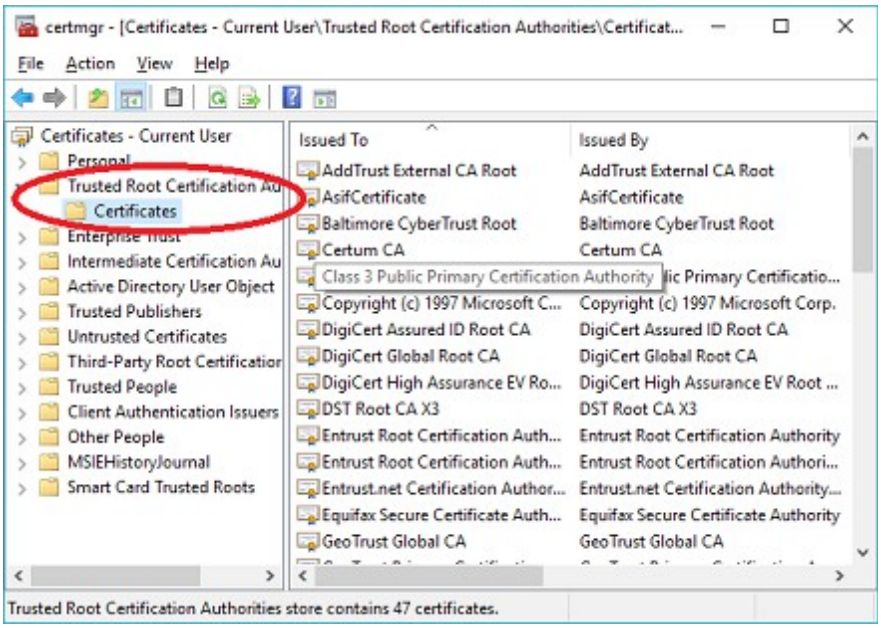


k) In the *'File to Export'* page, specify '*File name'* (e.g., F:\MyCert.pfx) of the exported file.

l) In *'Completing the Certificate Export Wizard'* page, click on the *'Finish'* button.

3.2. Install the Certificate in the 'Trusted Certificate Authority' Store of the computer running '*SysExpertez Admin Console*'.

a) Go to *Start → Run...,* type in *certmgr.msc*, and press *Enter*. It will open the *Certificate Store* of the current user.

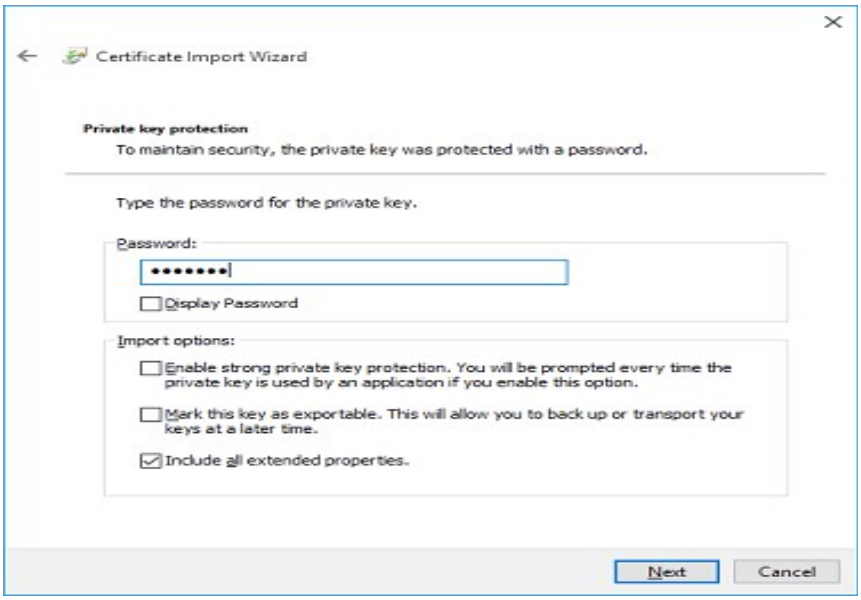


b) Select the *'Certificates'* sub-item under *'Trusted Root Certification Authorities'.*

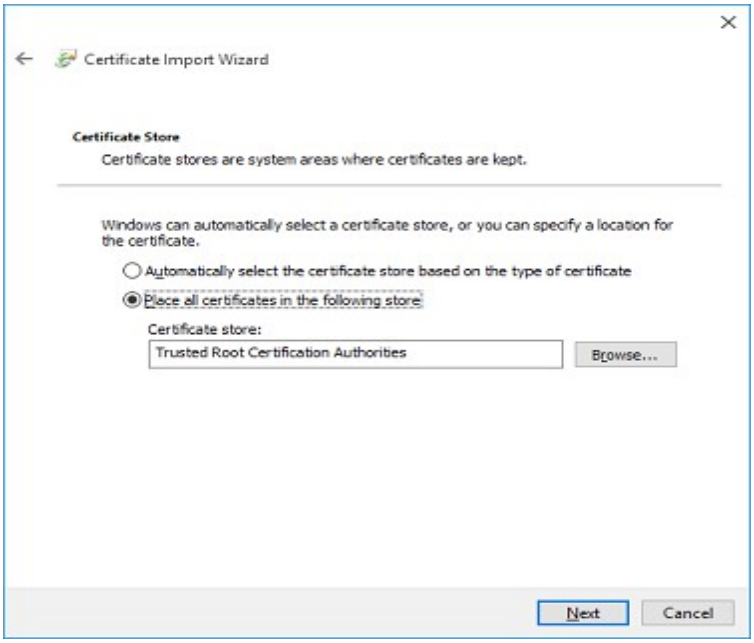
c) Go to *'Action'* menu option, and click on *'Import'* sub-menu under *'All Tasks'*. It will open the *'Certificate Import Wizard'*. Click on the '*Next'* button.

d) In the *'File to Import'* page, browse to the certificate file path (e.g., F:\MyCert.pfx) exported in the previous section.

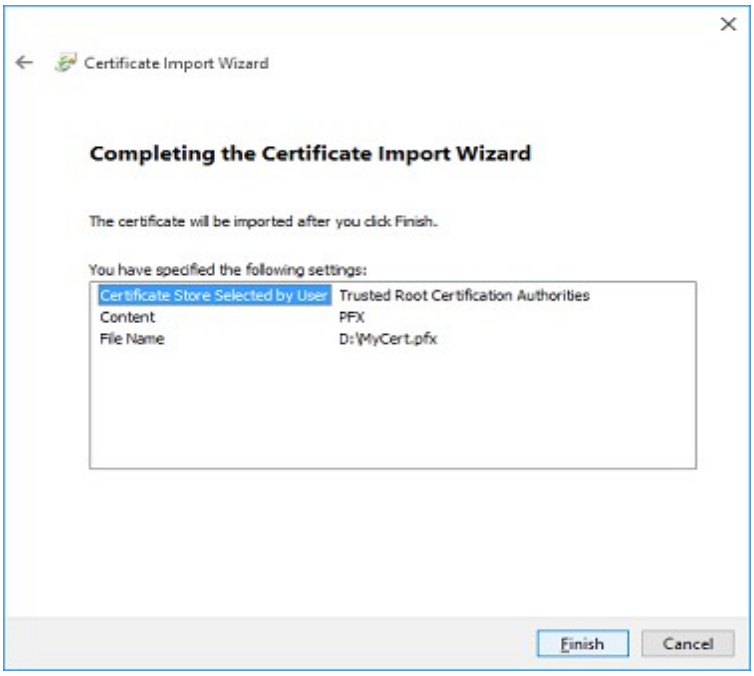
e) Type password of the certificate in the *Password* edit box, which was set while exporting the certificate (refer to the previous section – 3.1).



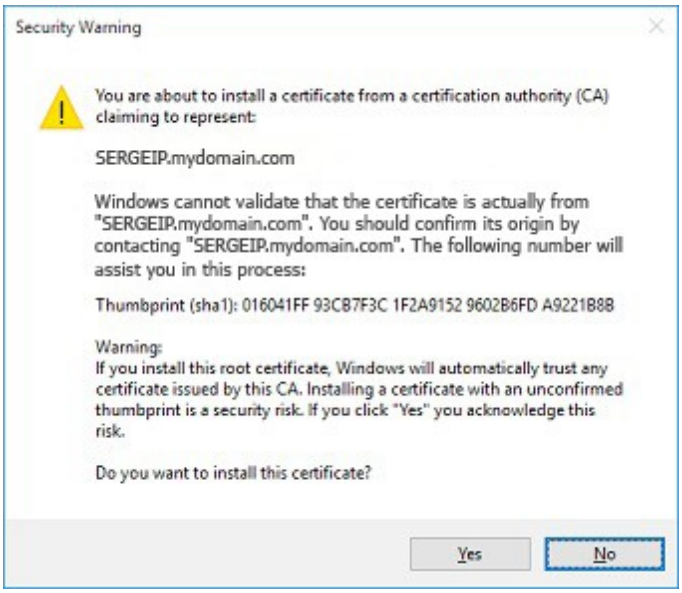
f) In the *'Certificate Store'* page, select the radio button option *'Place all certificates in the following store'* and browse to the *'Trusted Root Certification Authorities'* store.



g) In *'Completing the Certificate Import Wizard'* page, click on the *'Finish'* button.



h) A security warning dialog may be shown. Just click *'Yes'* to complete the import.



NOTE: A certificate issued by Certificate Authority (CA) is always recommended. A Self-signed certificate cannot be an alternative to a CA-issued certificate in terms of security. Self-signed certificate does not provide adequate security and poses security risks while using it in production environment.