Hongkong Post e-Cert
香港郵政電子核證

e-Cert (Server) User Guide

For Microsoft IIS 10.0

Revision Date: December 2022

Contents

A. Guidelines for e-Cert (Server) Applicant

After receipt and approval of an e-Cert (Server) application, Hongkong Post Certification Authority will send an e-mail with subject "Submission of Certificate Signing Request (CSR)" to request the Authorized Representative to submit the CSR at the Hongkong Post CA web site.

This user guide is for reference by applicants of e-Cert (Server) in generating their key pair and Certificate Signing Request (CSR) using Microsoft Internet Information Server (IIS) 10.0. The CSR containing the public key will then be submitted to Hongkong Post Certification Authority for certificate signing.

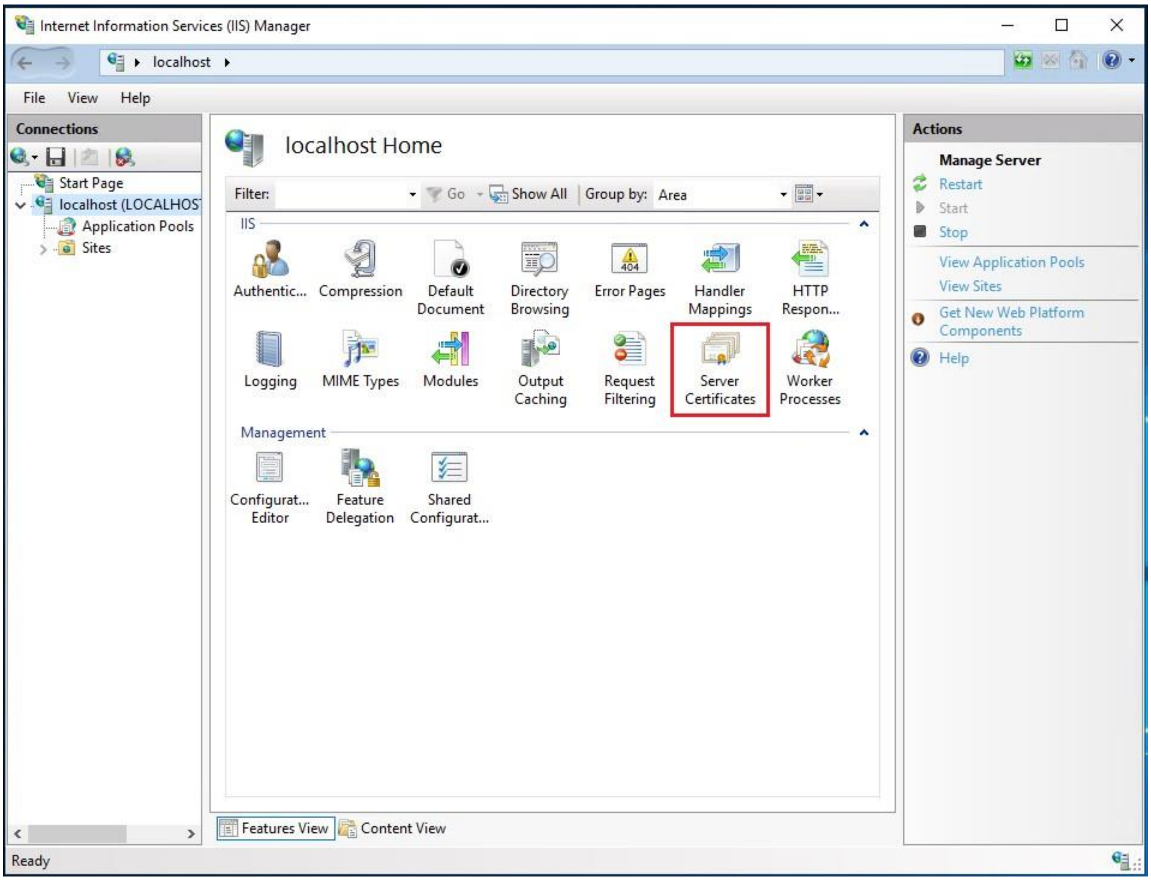
If you lose the private key after the certificate is issued, you will be unable to install or use the certificate. Therefore, it is strongly recommended that you should backup the private key **before the submission of the Certificate Signing Request (CSR)** and **after the installation of the server certificate**. To learn the backup and restore procedures of the private key, please follow the instructions as described in the following sections:

New and Renew Application

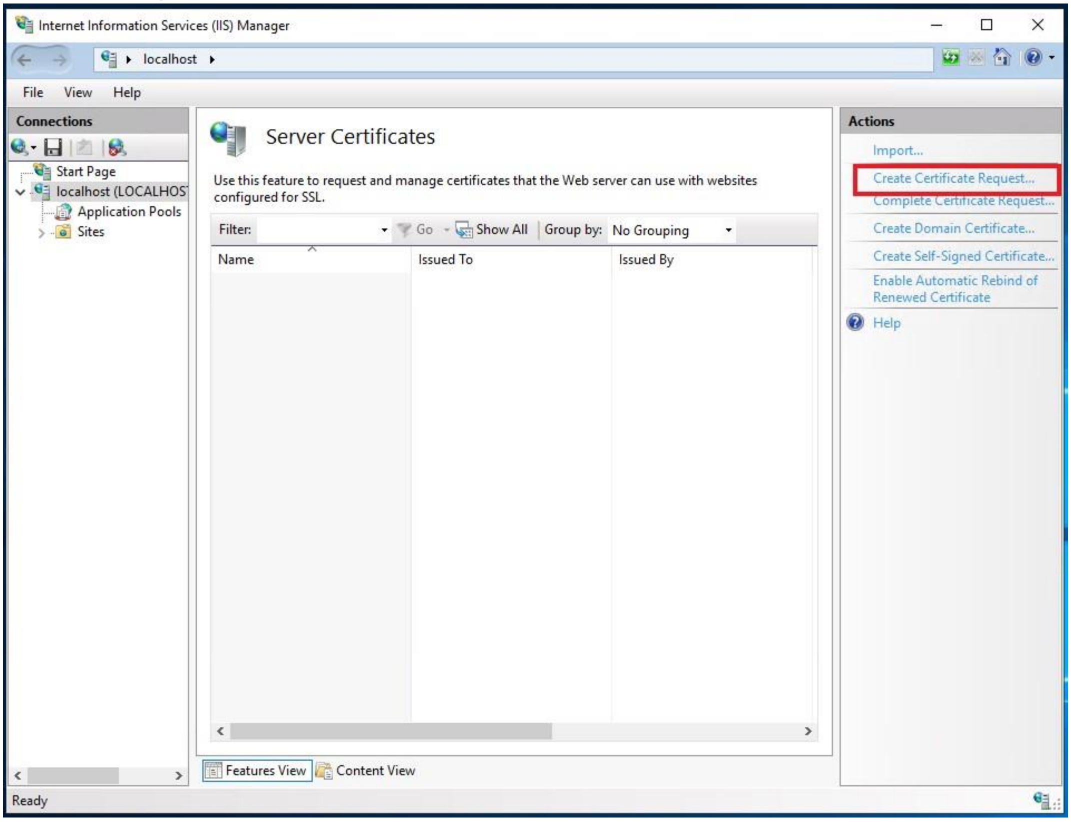
Please follow the instructions as described in the following sections for a new or renew application for e-Cert (Server):

B. Generating Certificate Signing Request (CSR)

1. Start menu, "Administrative Tools", and click on "Internet Information Services (IIS) Manager".
2. In "Internet Information Services (IIS) Manager", select your web site, and then double-click "Server Certificates".

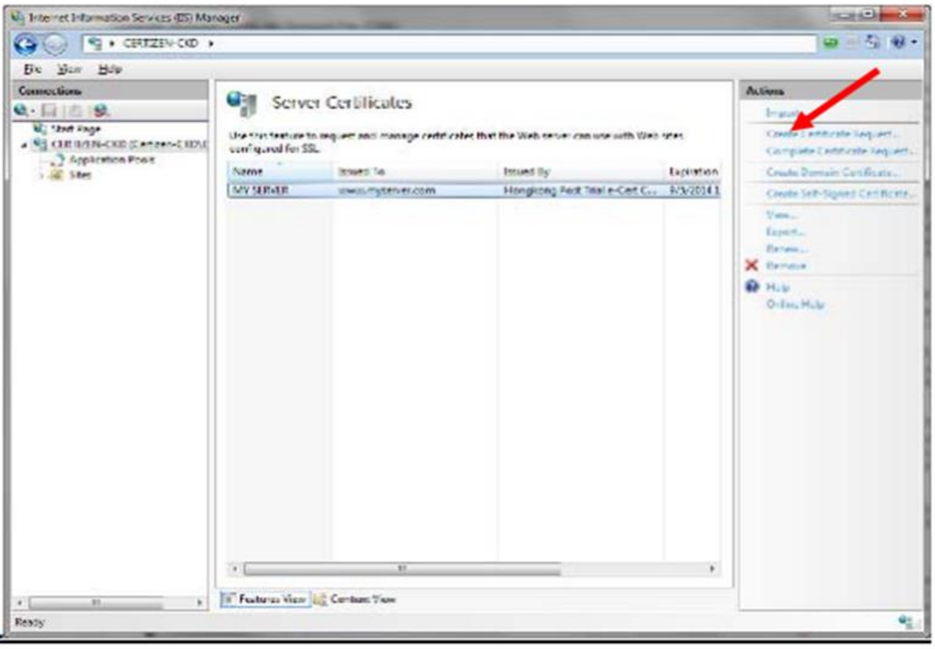


3 At the right column "**Actions**", select “**Create Certificate Request**”.



Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Note : For renew of e-Cert (Server) application, please do not click “Renew” option to renew the certificate. Please click “Create Certificate Request” as the same procedures as new application for e-Cert (Server).


Internet Information Services (IIS) Manager
Server Certificates
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Help
Online Help
Features View
Content View
Ready

4 Type the common name (i.e. server name) for your site, organization's name and your organizational unit, select "**HK**" for the "**Country/Region**". Type "**Hong Kong**" for both "**State/province**" and "**City/locality**", and then click "**Next**".

Note: Please make sure that the correct domain name (i.e. server name) is shown in the "Issued To" field and "HK" in the "Country/Region" field.

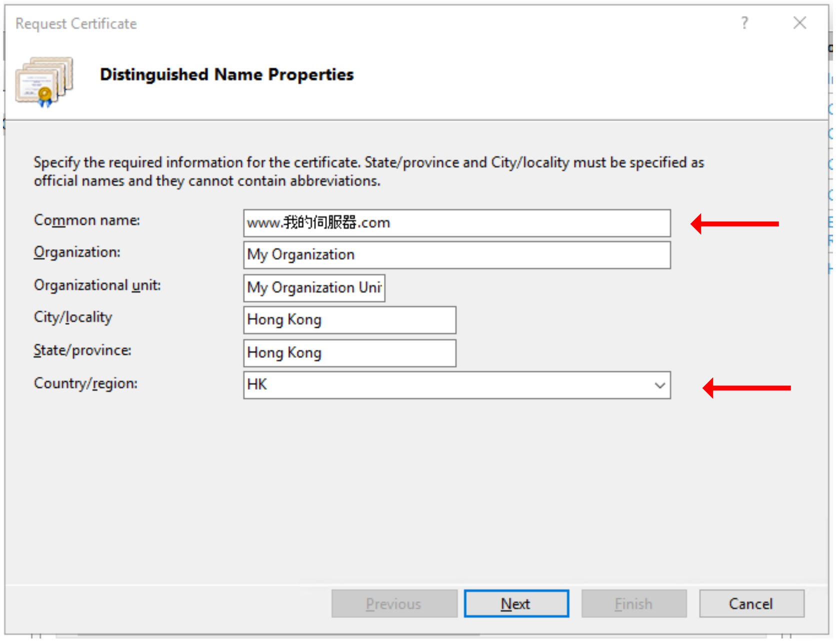
*Note: **For application of e-Cert (Server) with "Multi-domain" feature or EV e-Cert (Server) with "Multi-domain" feature,** please input the "Common Name" field with "Server name used as Subject Name in the Certificate" being filled in the application form. It is not necessary to specify any "Additional Server Name(s)" in the Subject Alternative Name of the CSR to be generated. It will be assigned by the Hongkong Post CA system automatically based on the information applied in the application form when the certificate is issued.*

***For application of e-Cert (Server) with "Wildcard" feature**, please input the "Common Name" field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk '*', in the left-most component of the server name), e.g. *.myserver.com, being filled in the application form.*

Note: For application of e-Cert (Server) with Chinese Domain Name

Option 1: please input the "Common Name" field with "Server name used as Subject Name in the Certificate" being filled in the application form.

Option 2: Use of IDN conversion tool to convert Chinese Domain Name into ASCII characters and input of the converted name in the "Common Name" field is also supported.

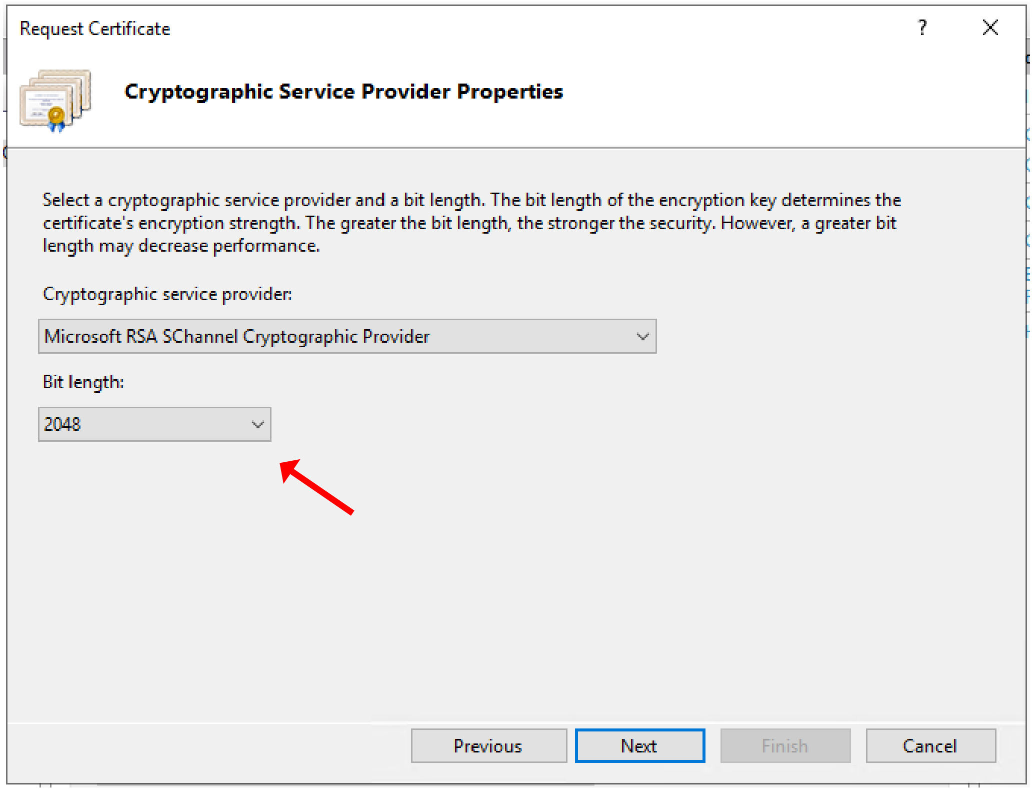


Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	www.我的伺服器.com
Organization:	My Organization
Organizational unit:	My Organization Uni
City/locality	Hong Kong
State/province:	Hong Kong
Country/region:	HK

5. Choose “**Microsoft RSA SChannel Cryptographic Provider**” for the “Cryptographic service provider”, and “**2048**” for the “Bit length”, and then click “**Next**”.

Note: Bit length smaller than 2048 may not be strong enough, while greater than 2048 may be incompatible with certain web browsers. It is recommended the bit length of the encryption key to be 2048 in order to support better security strength.



Request Certificate

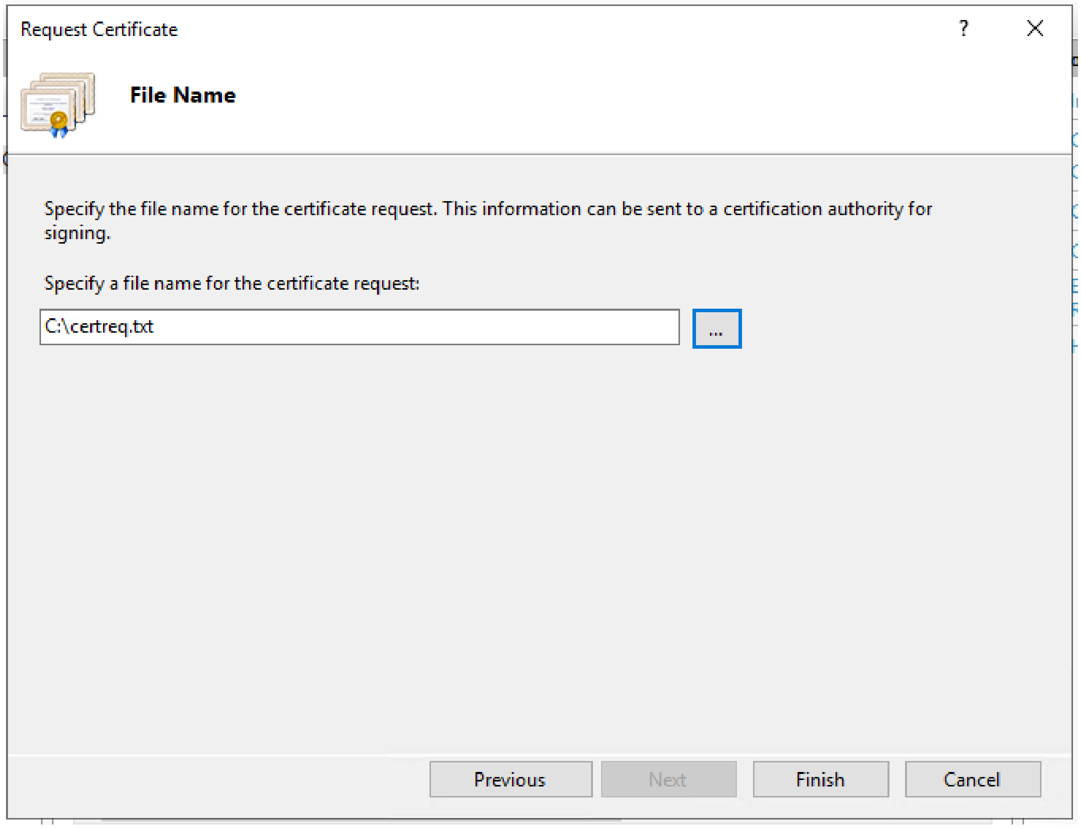
Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

6. Enter a file name for the certificate request, and then click “**Finish**”.



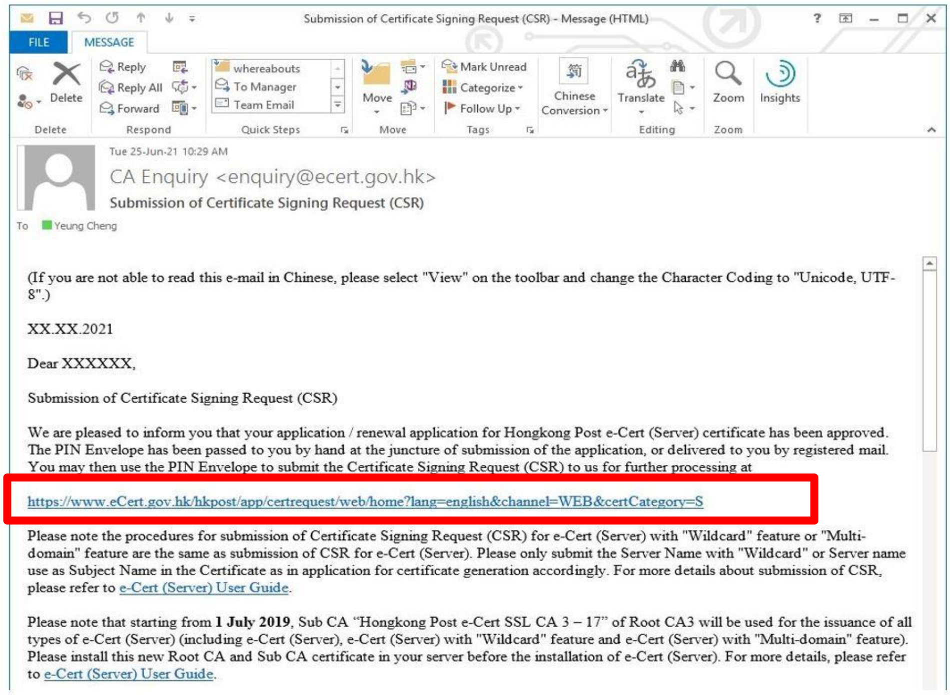
Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

C:\certreq.txt

C. Submitting Certificate Signing Request (CSR)

1. Click on the hyperlink in the e-mail with subject “**Submission of Certificate Signing Request (CSR)**” sent from Hongkong Post Certification Authority to access the Hongkong Post CA web site.



Tue 25-Jun-21 10:29 AM

CA Enquiry <enquiry@ecert.gov.hk>

Submission of Certificate Signing Request (CSR)

To Yeung Cheng

(If you are not able to read this e-mail in Chinese, please select "View" on the toolbar and change the Character Coding to "Unicode, UTF-8".)

XX.XX.2021

Dear XXXXXX,

Submission of Certificate Signing Request (CSR)

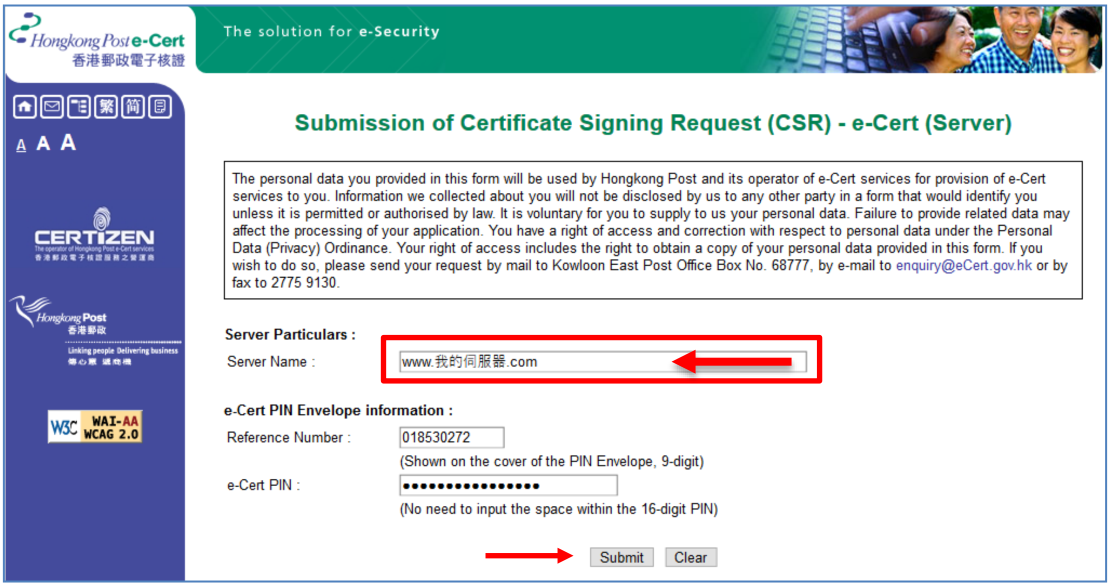
We are pleased to inform you that your application / renewal application for Hongkong Post e-Cert (Server) certificate has been approved. The PIN Envelope has been passed to you by hand at the juncture of submission of the application, or delivered to you by registered mail. You may then use the PIN Envelope to submit the Certificate Signing Request (CSR) to us for further processing at

https://www.eCert.gov.hk/hkpost/app/certrequest/web/home?lang=english&channel=WEB&certCategory=S

Please note the procedures for submission of Certificate Signing Request (CSR) for e-Cert (Server) with "Wildcard" feature or "Multi-domain" feature are the same as submission of CSR for e-Cert (Server). Please only submit the Server Name with "Wildcard" or Server name use as Subject Name in the Certificate as in application for certificate generation accordingly. For more details about submission of CSR, please refer to e-Cert (Server) User Guide.

Please note that starting from **1 July 2019**, Sub CA “Hongkong Post e-Cert SSL CA 3 – 17” of Root CA3 will be used for the issuance of all types of e-Cert (Server) (including e-Cert (Server), e-Cert (Server) with "Wildcard" feature and e-Cert (Server) with "Multi-domain" feature). Please install this new Root CA and Sub CA certificate in your server before the installation of e-Cert (Server). For more details, please refer to e-Cert (Server) User Guide.

2. Type the “**Server Name**”, the “**Reference Number**” (9-digit) as shown on the cover of the PIN Envelope and the “**e-Cert PIN**” (16-digit) as shown inside the PIN Envelope, and then click “**Submit**”.



Submission of Certificate Signing Request (CSR) - e-Cert (Server)

The personal data you provided in this form will be used by Hongkong Post and its operator of e-Cert services for provision of e-Cert services to you. Information we collected about you will not be disclosed by us to any other party in a form that would identify you unless it is permitted or authorised by law. It is voluntary for you to supply to us your personal data. Failure to provide related data may affect the processing of your application. You have a right of access and correction with respect to personal data under the Personal Data (Privacy) Ordinance. Your right of access includes the right to obtain a copy of your personal data provided in this form. If you wish to do so, please send your request by mail to Kowloon East Post Office Box No. 68777, by e-mail to enquiry@eCert.gov.hk or by fax to 2775 9130.

Server Particulars :

Server Name : www.我的伺服器.com

e-Cert PIN Envelope information :

Reference Number : 018530272

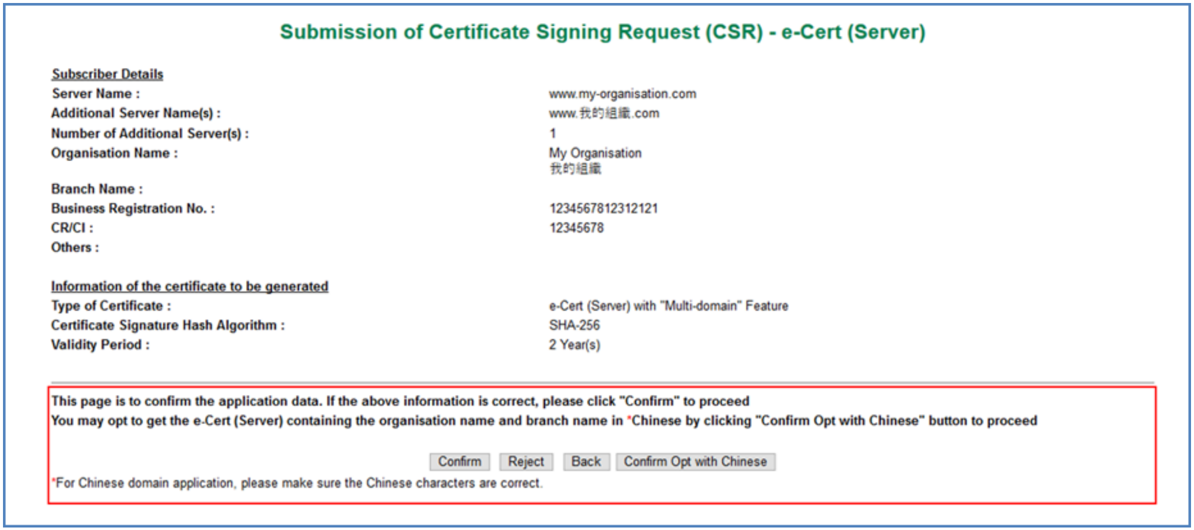
(Shown on the cover of the PIN Envelope, 9-digit)

e-Cert PIN : ●●●●●●●●●●●●●●●●

(No need to input the space within the 16-digit PIN)

Submit Clear

3. Click “**Confirm**” to confirm the application information. (If the information is incorrect, please contact Hongkong Post Certification Authority by email to enquiry@eCert.gov.hk.)



Submission of Certificate Signing Request (CSR) - e-Cert (Server)

Subscriber Details

Server Name :	www.my-organisation.com
Additional Server Name(s) :	www.我的組織.com
Number of Additional Server(s) :	1
Organisation Name :	My Organisation 我的組織
Branch Name :	
Business Registration No. :	1234567812312121
CR/CI :	12345678
Others :	

Information of the certificate to be generated

Type of Certificate :	e-Cert (Server) with "Multi-domain" Feature
Certificate Signature Hash Algorithm :	SHA-256
Validity Period :	2 Year(s)

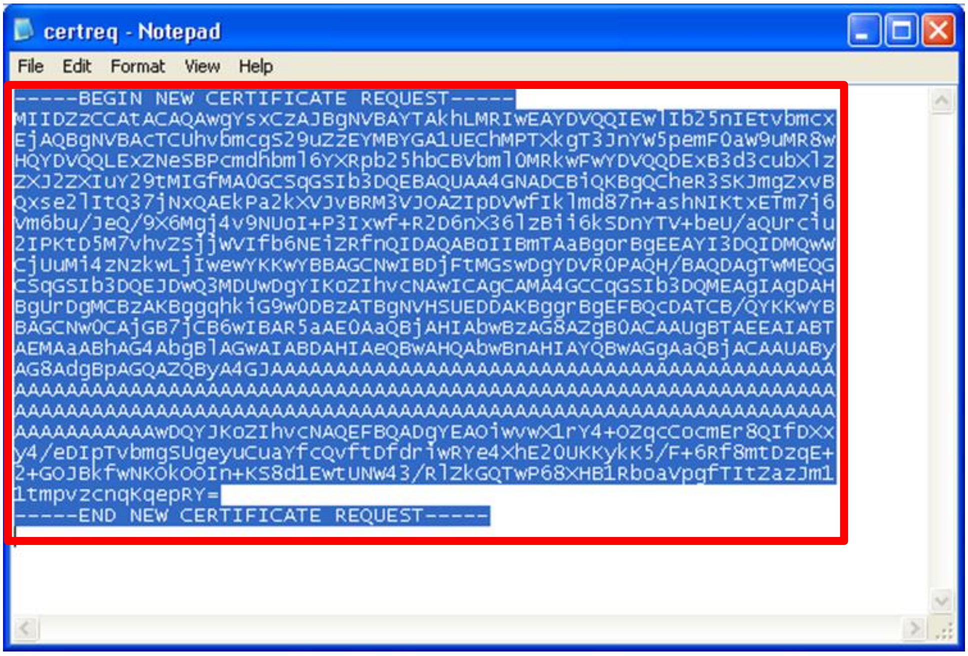
This page is to confirm the application data. If the above information is correct, please click "Confirm" to proceed

You may opt to get the e-Cert (Server) containing the organisation name and branch name in *Chinese by clicking "Confirm Opt with Chinese" button to proceed

*For Chinese domain application, please make sure the Chinese characters are correct.

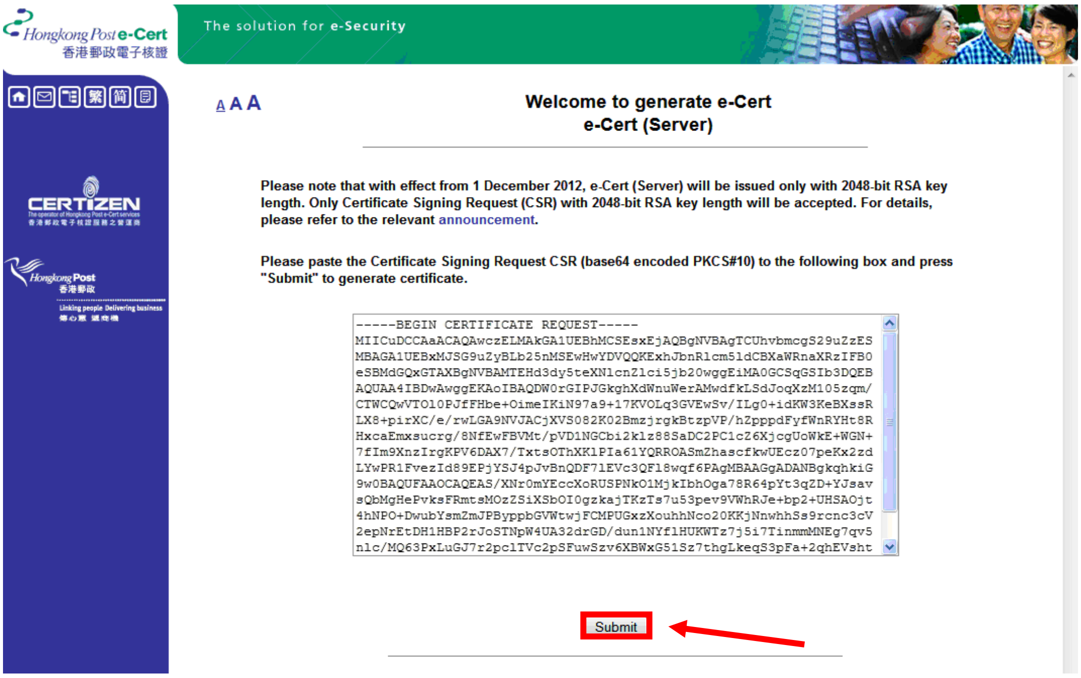
Note: If English and Chinese organisation name and/or branch name have been provided at the application form, in order to generate e-Cert (Server) with Chinese organisation name at Subject O field, click the button "Confirm Opt with Chinese" to proceed.

4. Open the previously generated **Certificate Signing Request** (CSR) with a text editor (e.g. Notepad) and copy the entire content including the "**-----BEGIN NEW CERTIFICATE REQUEST-----**" and "**-----END NEW CERTIFICATE REQUEST-----**". (You may refer to Part B Step 6 for the location of certificate request file.)



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDZzCCAtACAQAwgYsxCzAJBgNVBAYTAkhLMRIwEAYDVQQIEwlIb25nIEtvbmcx
EjAQBgNVBAcTCUhvbmcgS29uZzEYMBYGA1UEChMPTXkgT3JnYW5pemF0aW9uMR8w
HQYDVQQLExZNeSBPcmdhbml6YXRpb25hbCBVbml0MRkwFwYDVQQDExB3d3cubXlz
ZXJ2ZXIuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCheR3SKJmgZxvB
Qxse2lItQ37jNxQAEkPa2kXVJvBRM3VJOAZIpDVwfIklmd87n+ashNIKtxETm7j6
Vm6bu/JeQ/9X6Mgj4v9NUoI+P3Ixwf+R2D6nX36lzBii6kSDnYTV+beU/aQUrciu
2IPKtD5M7vhvZSjjWVIfb6NEiZRfnQIDAQABoIIBmTAaBgorBgEEAYI3DQIDMQwW
CjUuMi4zNzkwLjIwewYKKwYBBAGCNwIBDjFtMGswDgYDVR0PAQH/BAQDAgTwMEQG
CSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAH
BgUrDgMCBzAKBggqhkiG9w0DBzATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKKwYB
BAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABT
AEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUABy
AG8AdgBpAGQAZQByA4GJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAwDQYJKoZIhvcNAQEFBQADgYEAOiwvwX1rY4+OZqcCocmEr8QIfDXx
y4/eDIpTvbmgSUgeyuCuaYfcQvftDfdriwRYe4XhE20UKKykK5/F+6Rf8mtDzqE+
2+GOJBkfwNKOkOOIn+KS8d1EwtUNW43/RlZkGQTwP68XHB1RboaVpgfTItZazJm1
1tmpvzcnqKqepRY=
-----END NEW CERTIFICATE REQUEST-----
```

5. Paste the content to the text box, and then click “**Submit**”.



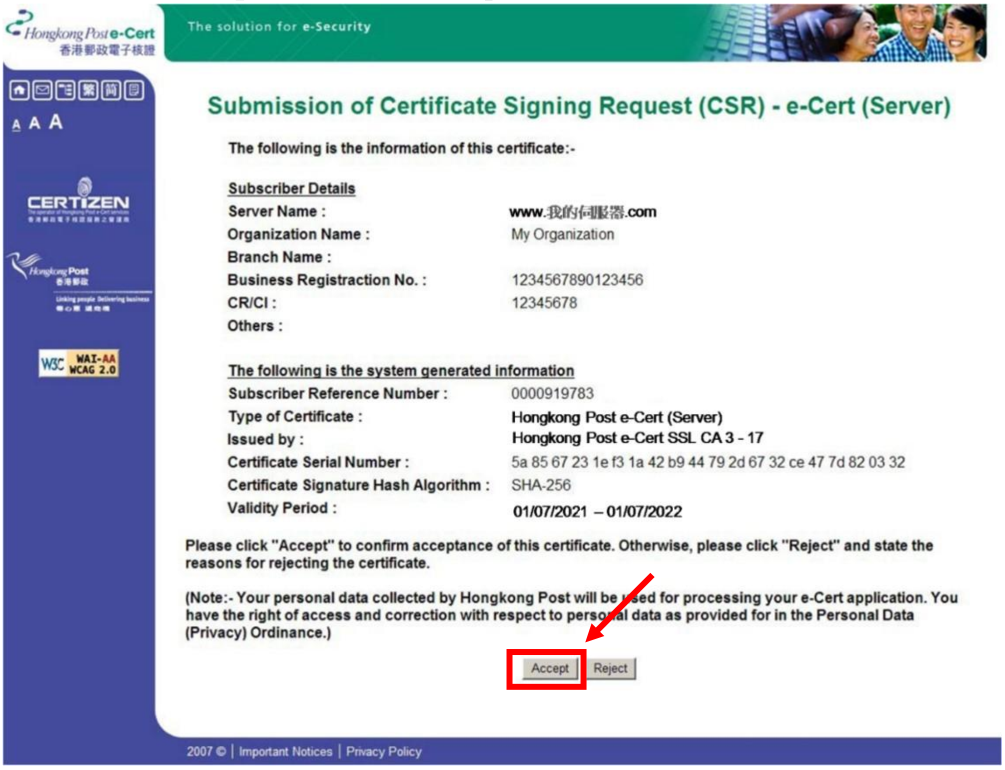
Welcome to generate e-Cert
e-Cert (Server)

Please note that with effect from 1 December 2012, e-Cert (Server) will be issued only with 2048-bit RSA key length. Only Certificate Signing Request (CSR) with 2048-bit RSA key length will be accepted. For details, please refer to the relevant announcement.

Please paste the Certificate Signing Request CSR (base64 encoded PKCS#10) to the following box and press "Submit" to generate certificate.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICuDCCAaACAQAwczELMAkGA1UEBhMCSEsxEjAQBgNVBAgTCUhvbmcgS29uZzES
MBAGA1UEBxMJSG9uZyBLb25nMSEwHwYDVQQKExhJbnRlcm5ldCBXaWRnaXRzIFB0
eSBMdGQxGTAXBgNVBAMTEHd3dy5teXNlcnZlci5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDW0rGIPJGkghXdWnuWerAMwdfkLSdJoqXzM105zqm/
CTWCQwVTOl0PJfFHbe+OimeIKiN97a9+17KVOLq3GVEwSv/ILg0+idKW3KeBXssR
LX8+pirXC/e/rwLGA9NVJACjXVS082K02BmzjrgkBtzpVP/hZpppdFyfWnRYHt8R
HxcaEmxsucrg/8NfEwFBVMt/pVD1NGCbi2klz88SaDC2PC1cZ6XjcgUoWkE+WGN+
7fIm9XnzIrgKPV6DAX7/TxtsOThXKlPIa61YQRROASmZhascfkwUEcz07peKx2zd
LYwPR1FvezId89EPjYSJ4pJvBnQDF71EVc3QF18wqf6PAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEAS/XNr0mYEccXoRUSPNkO1MjkIbhOga78R64pYt3qZD+YJsav
sQbMgHePvksFRmtsMOzZSiXSbOI0gzkajTKzTs7u53pev9VWhRJe+bp2+UHSAOjt
4hNPO+DwubYsmZmJPByppbGVWtwjFCMPUGxzXouhhNco20KKjNnwhhSs9rcnc3cV
2epNrEtDH1HBP2rJoSTNpW4UA32drGD/dun1NYflHUKWTz7j5i7TinmmMNEg7qv5
nlc/MQ63PxLuGJ7r2pclTVc2pSFuwSzv6XBWxG51Sz7thgLkeqS3pFa+2qhEVsht
```

6. Click “**Accept**” to confirm acceptance of the certificate.



Submission of Certificate Signing Request (CSR) - e-Cert (Server)

The following is the information of this certificate:-

Subscriber Details

Server Name :	www.我的伺服器.com
Organization Name :	My Organization
Branch Name :	
Business Registration No. :	1234567890123456
CR/CI :	12345678
Others :	

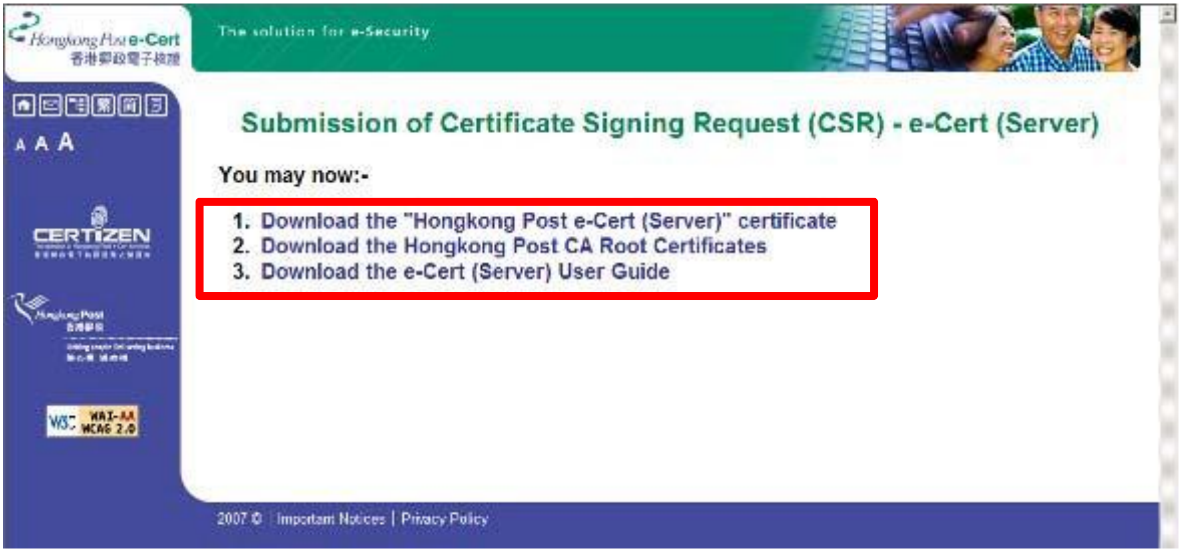
The following is the system generated information

Subscriber Reference Number :	0000919783
Type of Certificate :	Hongkong Post e-Cert (Server)
Issued by :	Hongkong Post e-Cert SSL CA 3 - 17
Certificate Serial Number :	5a 85 67 23 1e f3 1a 42 b9 44 79 2d 67 32 ce 47 7d 82 03 32
Certificate Signature Hash Algorithm :	SHA-256
Validity Period :	01/07/2021 – 01/07/2022

Please click "Accept" to confirm acceptance of this certificate. Otherwise, please click "Reject" and state the reasons for rejecting the certificate.

(Note:- Your personal data collected by Hongkong Post will be used for processing your e-Cert application. You have the right of access and correction with respect to personal data as provided for in the Personal Data (Privacy) Ordinance.)

7. Click to download the **Hongkong Post e-Cert (Server).**



Submission of Certificate Signing Request (CSR) - e-Cert (Server)

You may now:-

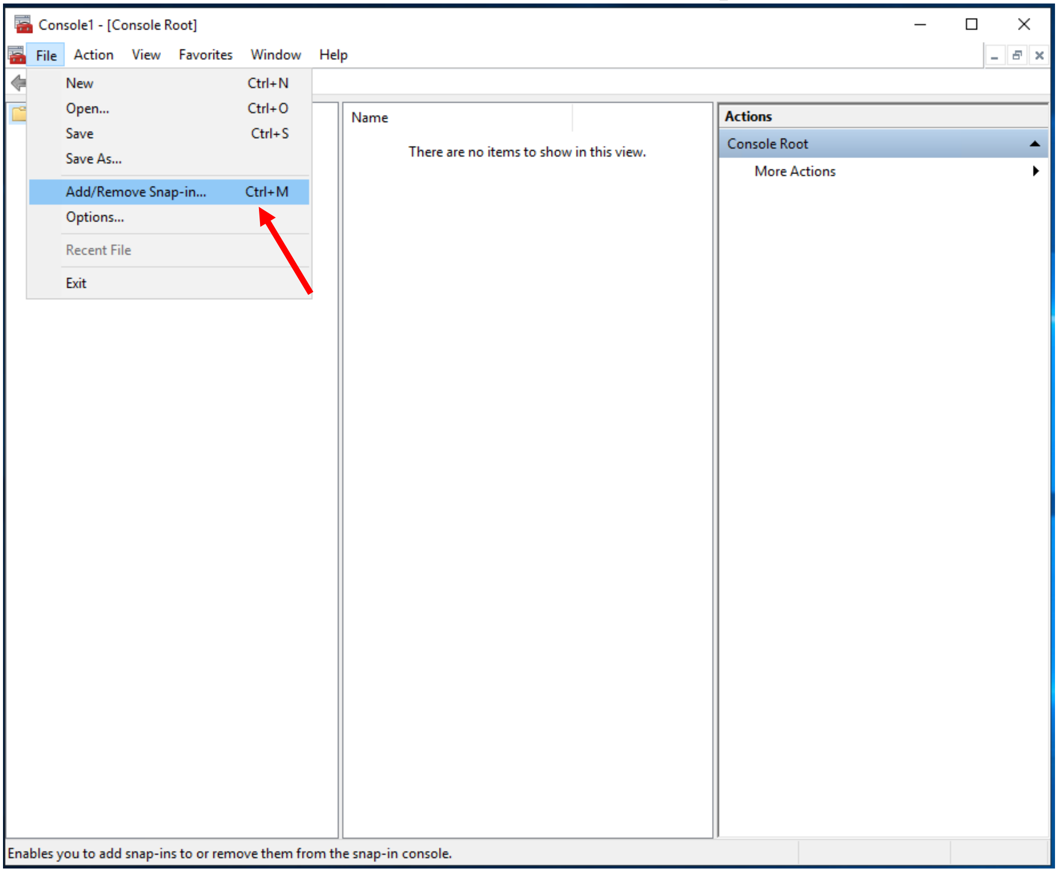
1. Download the "Hongkong Post e-Cert (Server)" certificate
2. Download the Hongkong Post CA Root Certificates
3. Download the e-Cert (Server) User Guide

Note:

1. *You can also download your e-Cert (Server) from the Search and Download Certificate web page.* *https://www.ecert.gov.hk/en/sc/index.html*
2. *For all types of e-Cert (Server):* *Install the Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" issued by Root CA3. Click the following link to download:* *http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt* *Install the cross-certificate "Hongkong Post Root CA 3 (Cross certificate 2022)". Click the following link to download:* *http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt*
3. *For all types of EV e-Cert (Server):* *Install the Sub CA "Hongkong Post e-Cert EV SSL CA 3 - 17" issued by Root CA3. Click the following link to download:* *http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt* *Install the cross-certificate "Hongkong Post Root CA 3 (Cross certificate 2022)". Click the following link to download:* *http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt*

D. Installing Sub CA / Cross Certificate

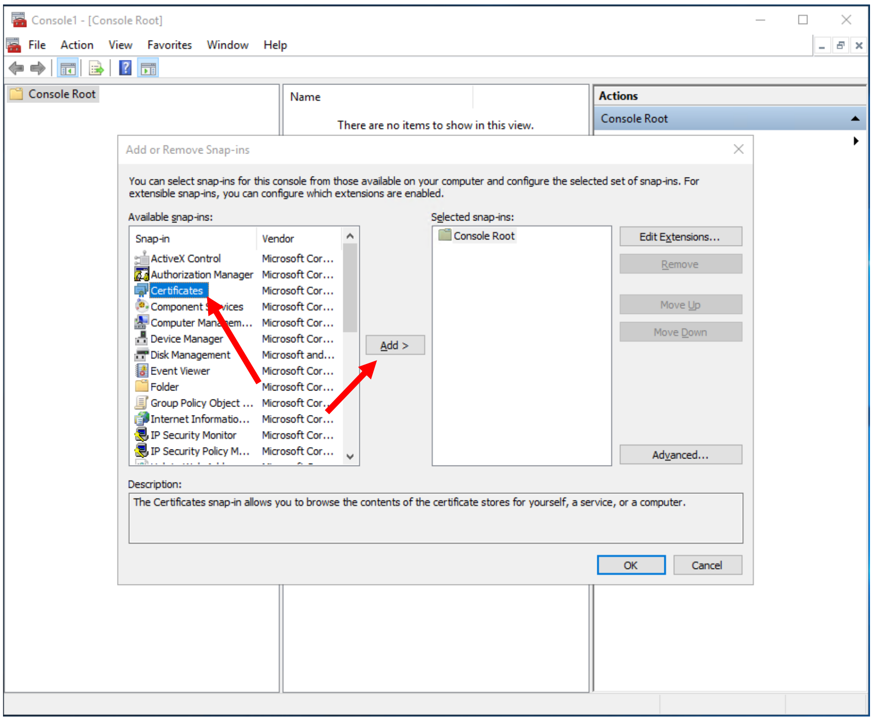
1. Start **Microsoft Management Console (MMC)** by clicking "**Start**" > "**Run**", type "**mmc**" and click **OK**, and then select "**Add/Remove Snap-in**" from the "**File**" menu.



There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

2. Select "**Certificate**" then Click "**Add**".



There are no items to show in this view.

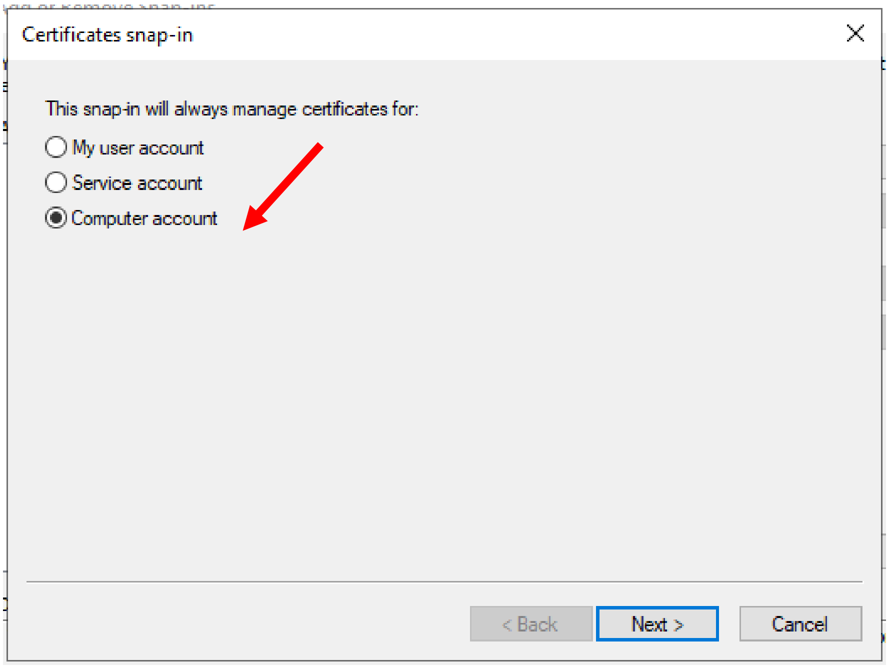
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

3. Select "**Computer account**", and then click "**Next**".



Certificates snap-in

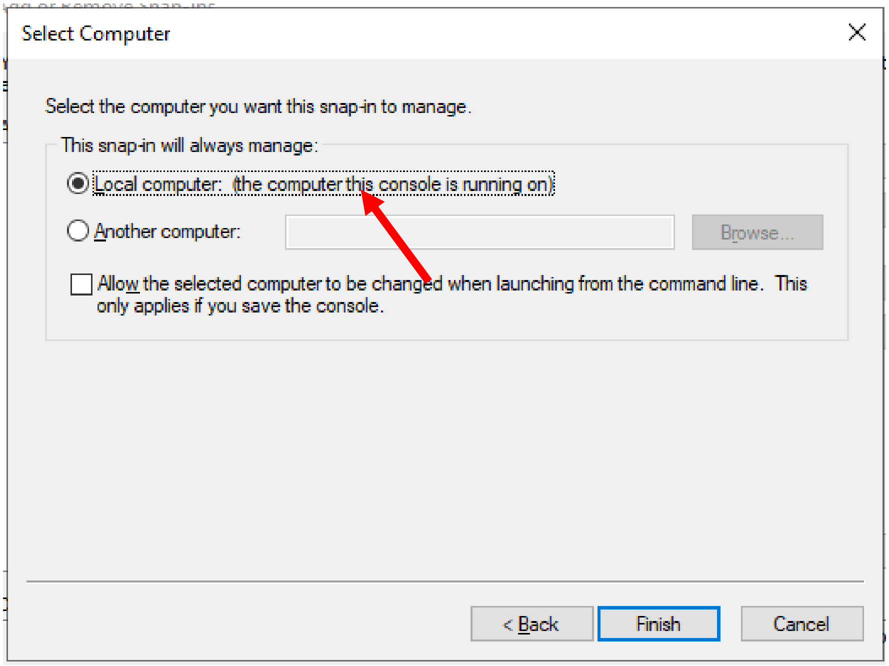
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

4. Select “**Local computer**”, and then click “**Finish**”.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

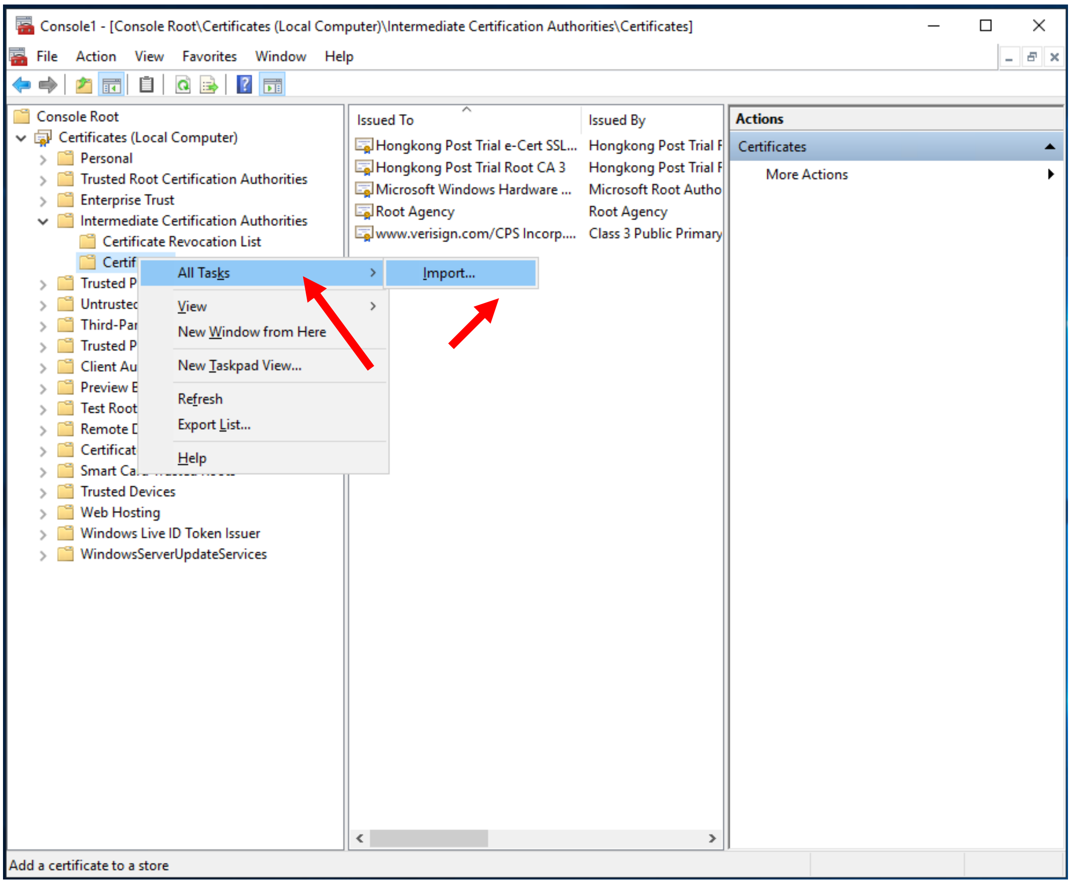
● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

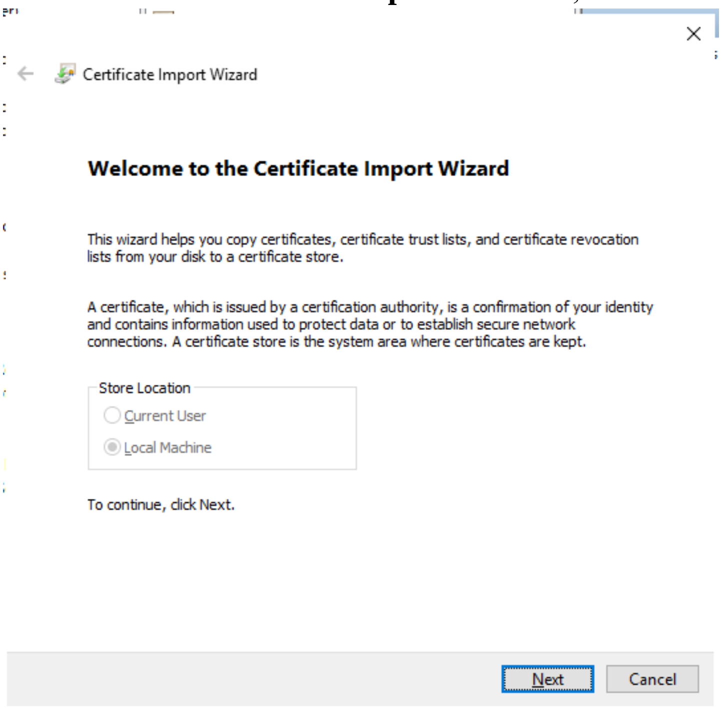
The following uses the “**Hongkong Post e-Cert SSL CA 3 - 17”** Sub CA certificate as example.

5. Expand “**Intermediate Certification Authorities**” and right-click “**Certificates**”, and then select “**All Tasks**” > “**Import**”.


Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certif
Trusted P
Untrustec
Third-Par
Trusted P
Client Au
Preview E
Test Root
Remote D
Certificat
Smart Ca
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
WindowsServerUpdateServices
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Import...
Actions
Certificates
More Actions
Add a certificate to a store

Issued To	Issued By
Hongkong Post Trial e-Cert SSL...	Hongkong Post Trial F
Hongkong Post Trial Root CA 3	Hongkong Post Trial F
Microsoft Windows Hardware ...	Microsoft Root Autho
Root Agency	Root Agency
www.verisign.com/CPS Incorp....	Class 3 Public Primary

6. In the "**Certificate Import Wizard**", click "**Next**" to continue.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

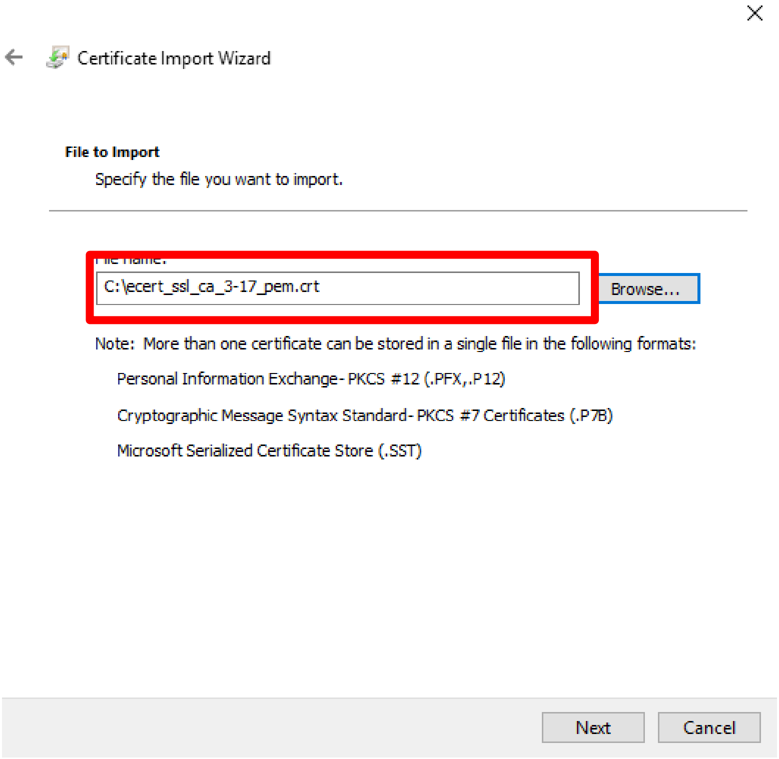
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

7. Click "**Browse**" to locate the "**Hongkong Post e-Cert SSL CA 3 - 17**" certificate that you downloaded in Part C Step 7 (ecert_ssl_ca_3-17_pem.crt), and then click "**Next**".



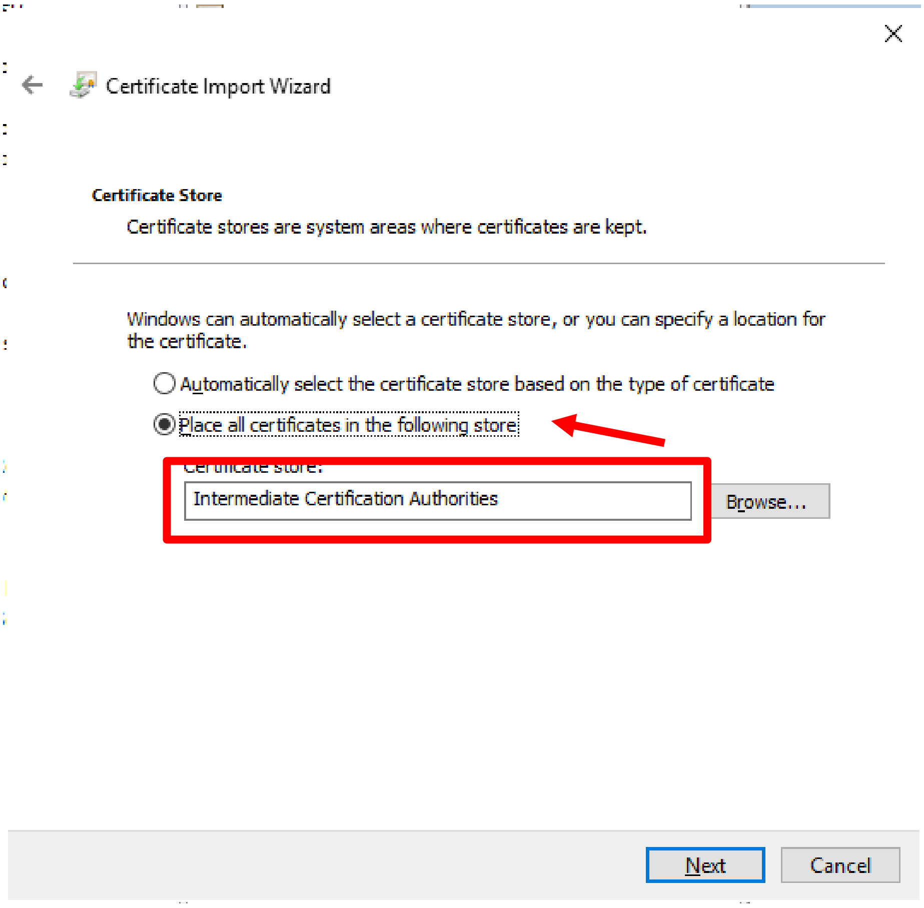
Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:
C:\ecert_ssl_ca_3-17_pem.crt

Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)

8. Select "**Place all certificates in the following store**", make sure "**Intermediate Certification Authorities**" has been selected as "Certificate store", and then click "**Next**".



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

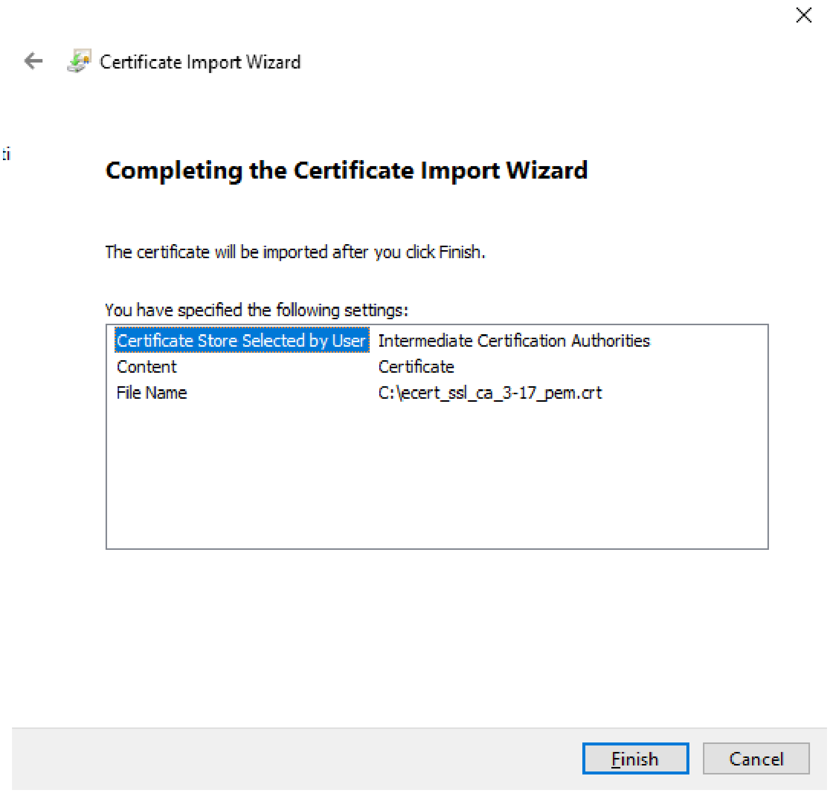
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

9. Click "**Finish**" to close the wizard.



Certificate Import Wizard

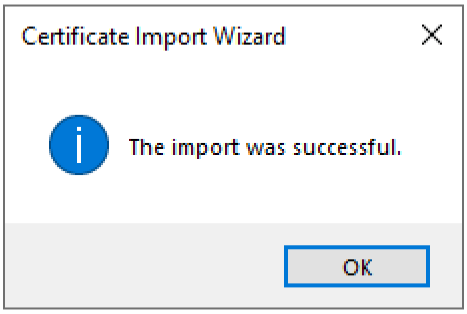
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

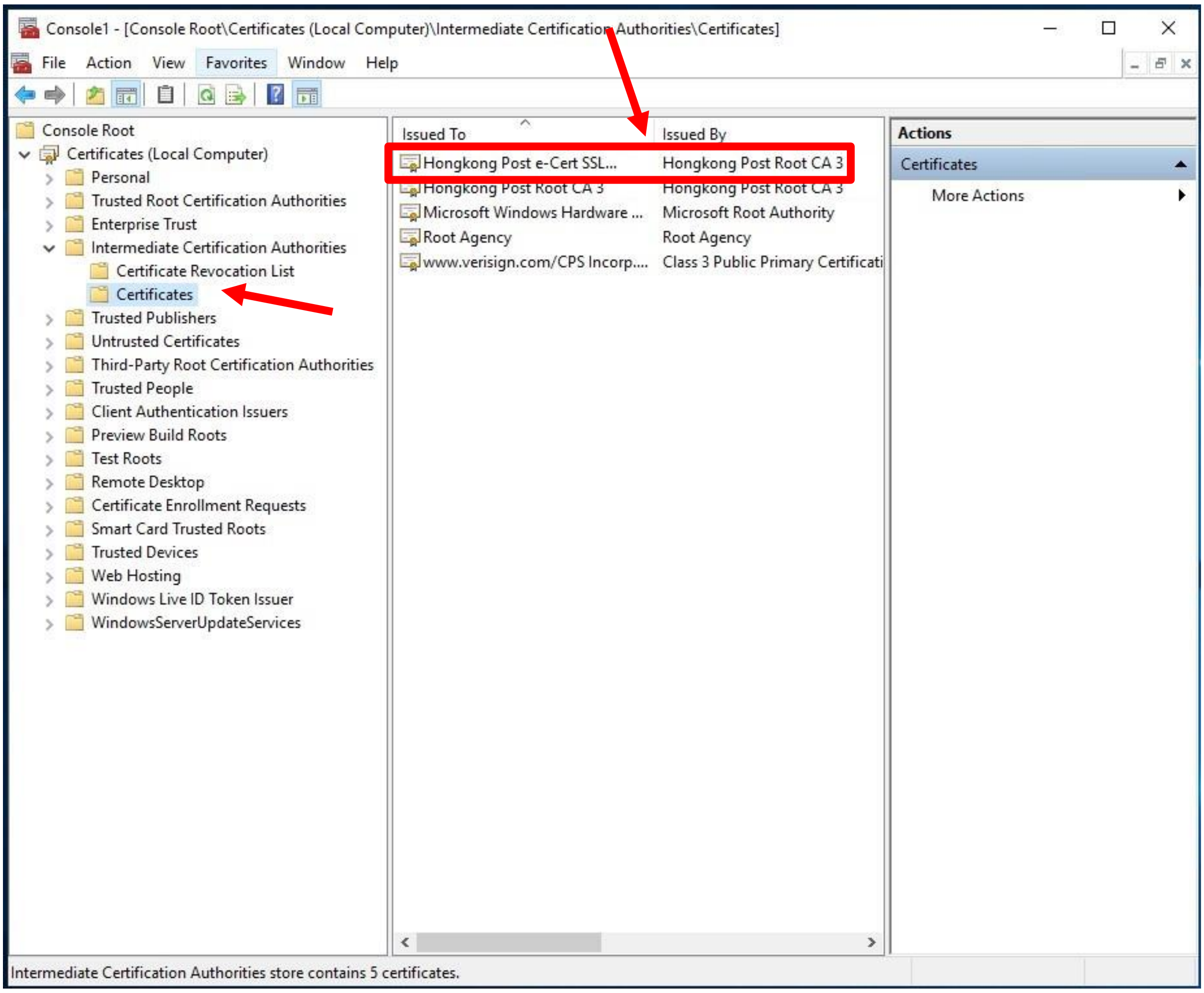
Certificate Store Selected by User	Intermediate Certification Authorities
Content	Certificate
File Name	C:\ecert_ssl_ca_3-17_pem.crt

10. Click “**OK**” to complete.



Certificate Import Wizard

The import was successful.



Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
WindowsServerUpdateServices
Actions
Certificates
More Actions

Issued To	Issued By
Hongkong Post e-Cert SSL...	Hongkong Post Root CA 3
Hongkong Post Root CA 3	Hongkong Post Root CA 3
Microsoft Windows Hardware ...	Microsoft Root Authority
Root Agency	Root Agency
www.verisign.com/CPS Incorp....	Class 3 Public Primary Certificati

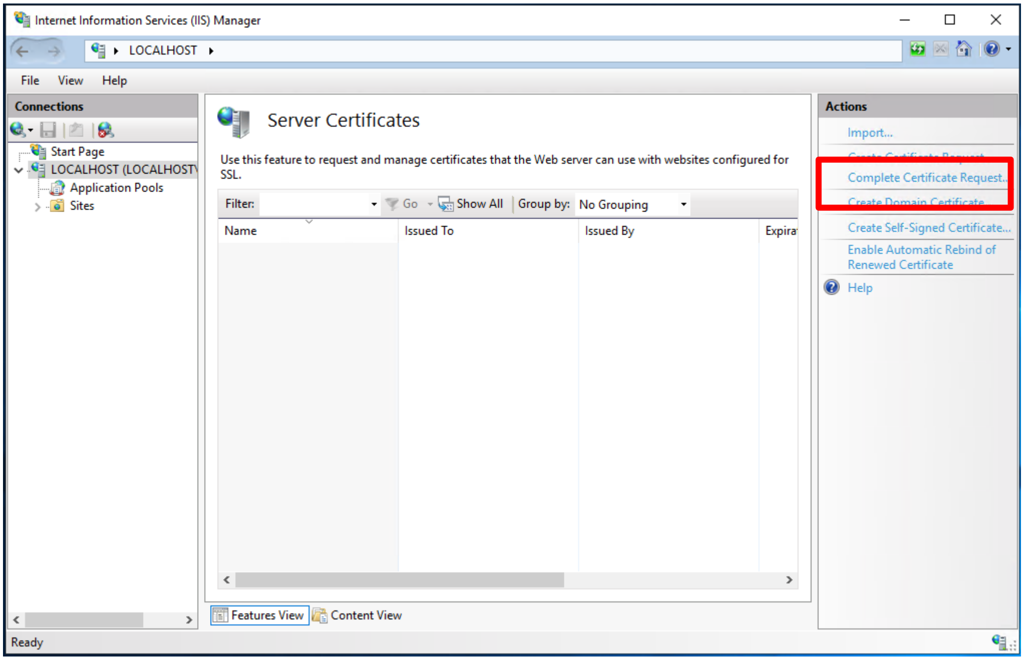
Intermediate Certification Authorities store contains 5 certificates.

Figure 1: “Hongkong Post e-Cert SSL CA 3 - 17” certificate has been successfully installed

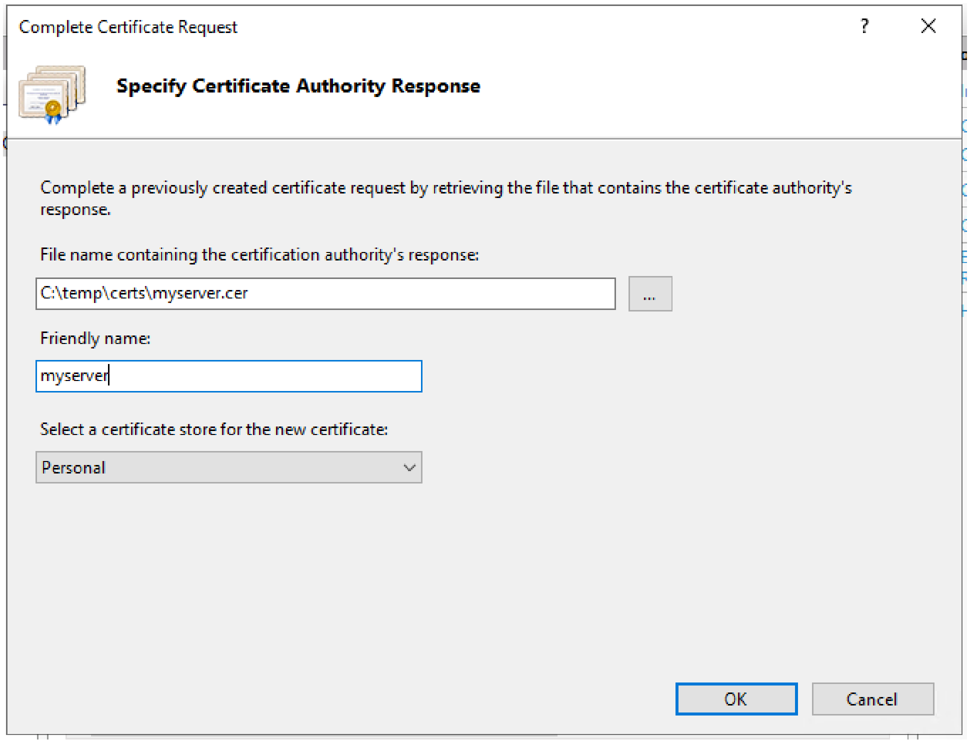
11. Repeat step 5 to step 10 for installation of cross-cert (root_ca_3_x_gsca_r3_pem.crt) which was downloaded in Section C step 7.

E. Installing Server Certificate

1. In “**Internet Information Services (IIS) Manager**”, select your web site, and then double-click “**Server Certificates**”. At the right column "**Actions**", select “**Complete Certificate Request**”.


Internet Information Services (IIS) Manager
LOCALHOST
File
View
Help
Connections
Start Page
LOCALHOST (LOCALHOST\
Application Pools
Sites
Server Certificates
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.
Filter:
Go
Show All
Group by:
No Grouping
Name
Issued To
Issued By
Expira
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

2. Click “**Browse**” to locate the “**Hongkong Post e-Cert (Server)**” certificate that you downloaded in Part C Step 7, and then input “**Friendly name**”, click “**OK**”.


Complete Certificate Request

Specify Certificate Authority Response

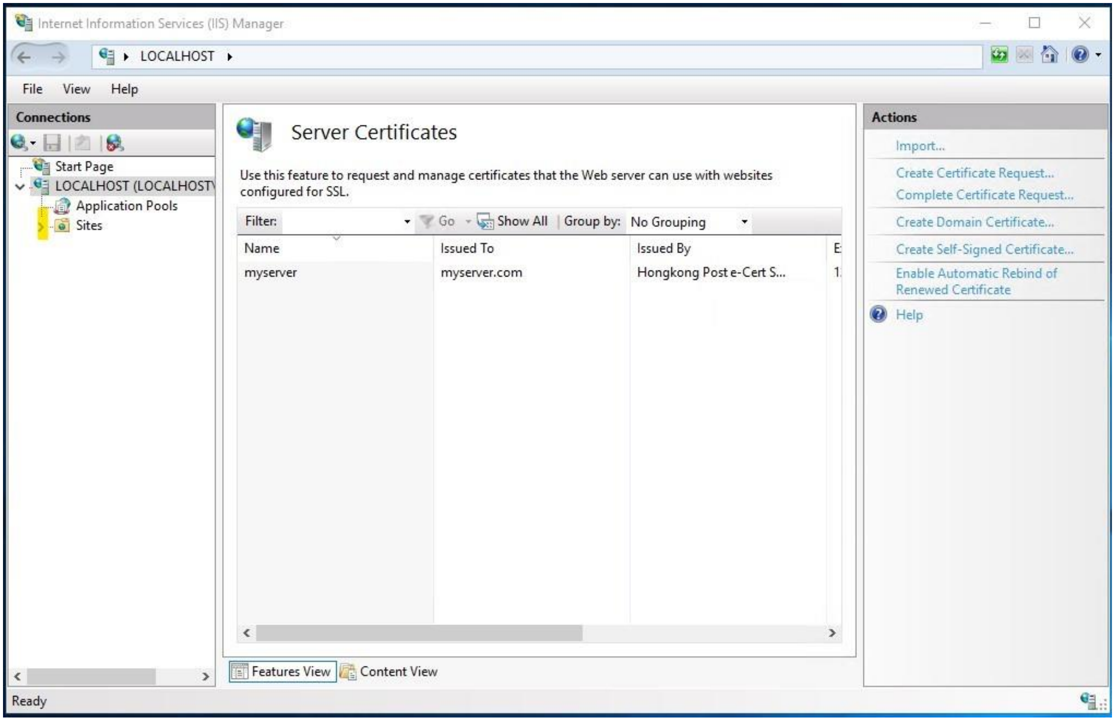
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response: C:\temp\certs\myserver.cer

Friendly name: myserver

Select a certificate store for the new certificate: Personal

3. “**Hongkong Post e-Cert (Server)**” certificate has been successfully installed.

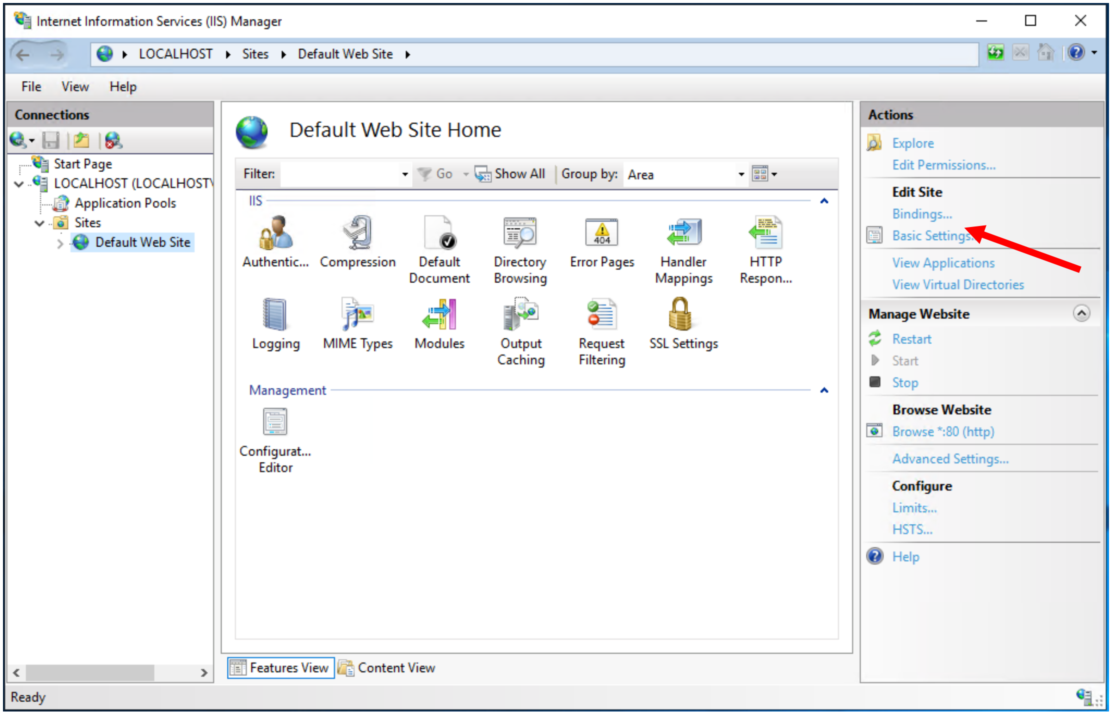


Internet Information Services (IIS) Manager
LOCALHOST
File
View
Help
Connections
Start Page
LOCALHOST (LOCALHOST\
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
No Grouping
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

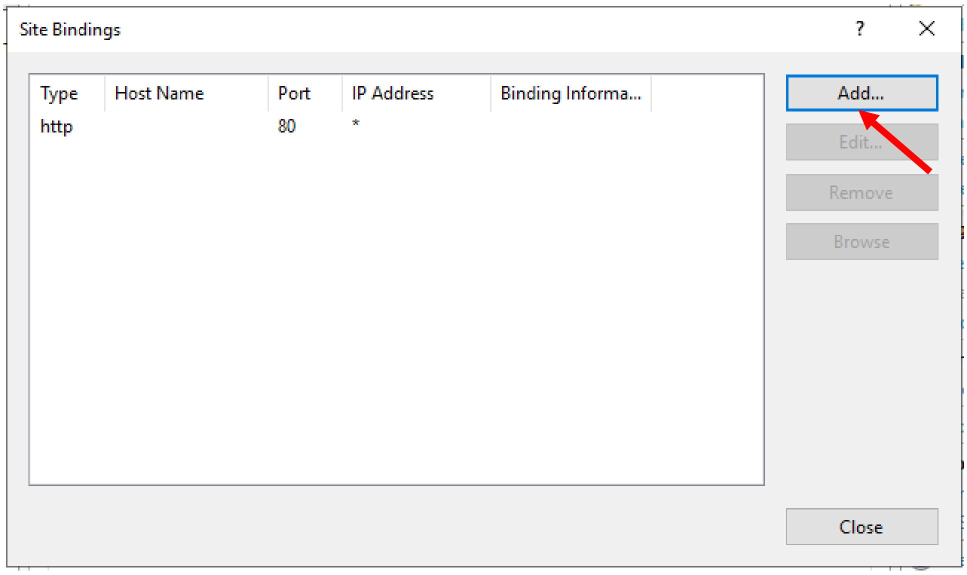
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	E
myserver	myserver.com	Hongkong Post e-Cert S...	1.

4. Click on the website that you want to bind the certificate to. Click “**Bindings**”.



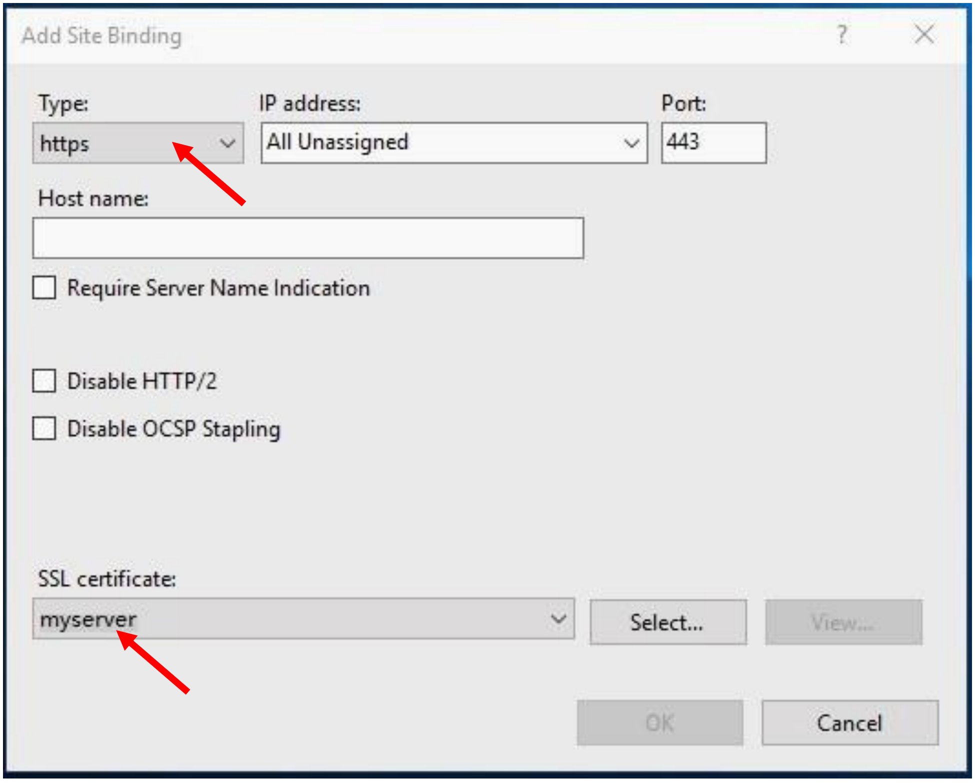
5. click “**Add…**”.



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	

6. Select “**https**” and related SSL certificate, then click “**OK**” to confirm.



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

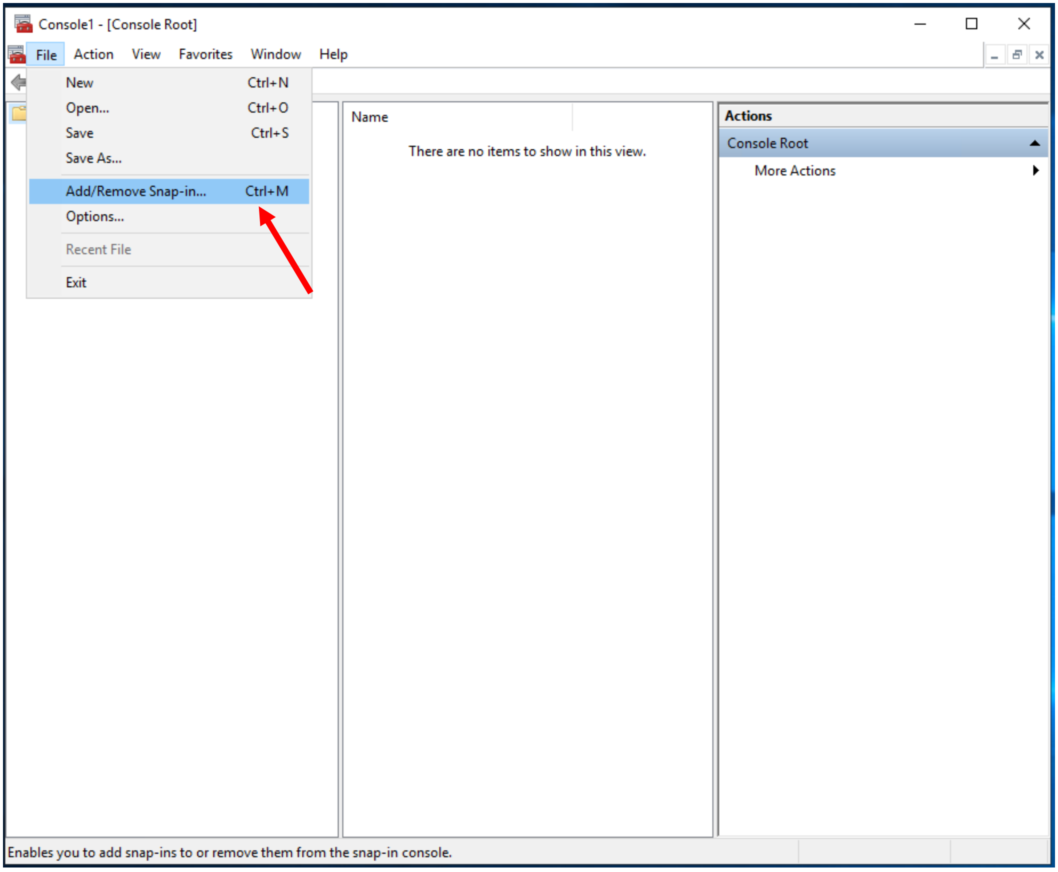
□ Disable HTTP/2

□ Disable OCSP Stapling

SSL certificate: myserver

F. Backing up the Private Key

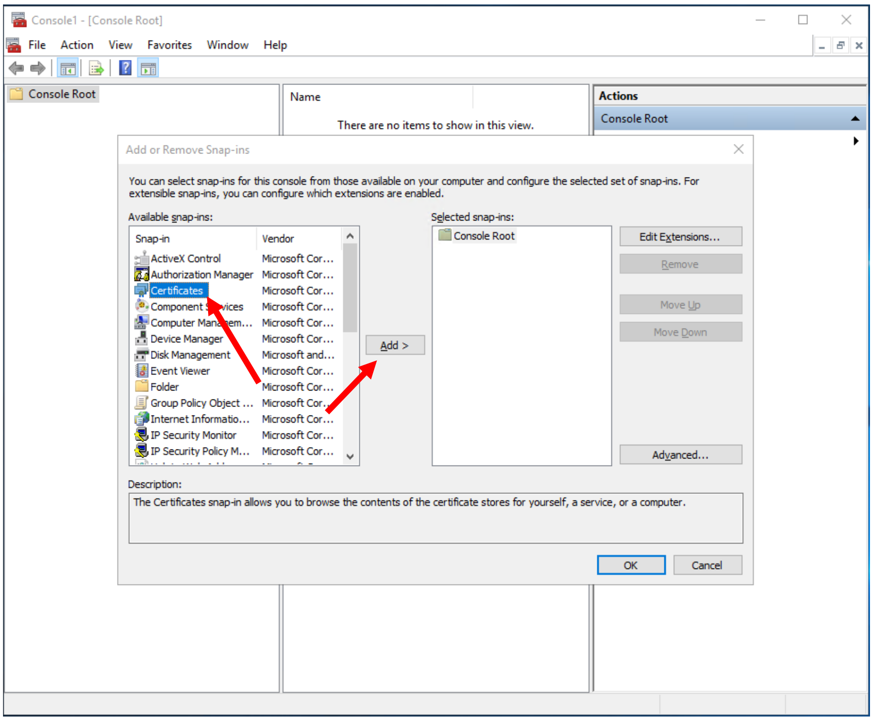
1. Start Microsoft Management Console (MMC) by clicking “**Start**” > “**Run**”, type “**mmc**” and click OK, and then select “**Add/Remove Snap-in**” from the “**File**” menu.



There are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

2. Select “**Certificate**” then Click “**Add**”.



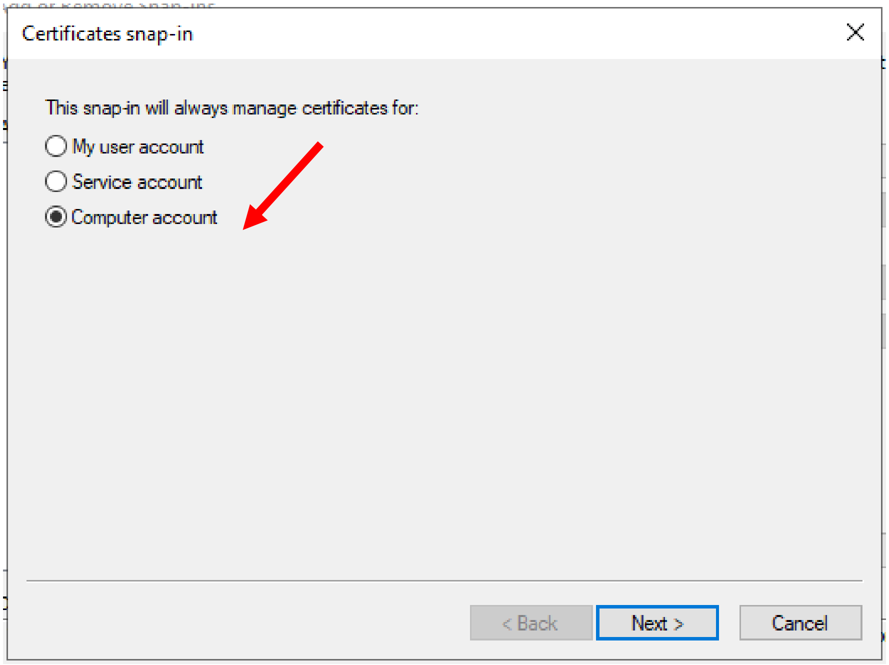
There are no items to show in this view.

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

3. Select "**Computer account**", and then click "**Next**".



Certificates snap-in

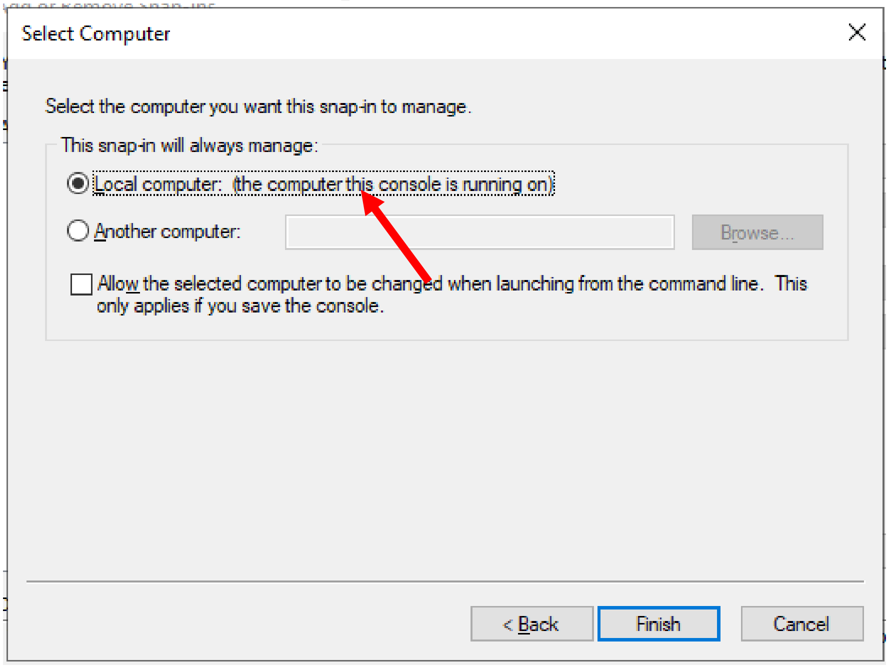
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

4. Select "**Local computer**", and then click "**Finish**".



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

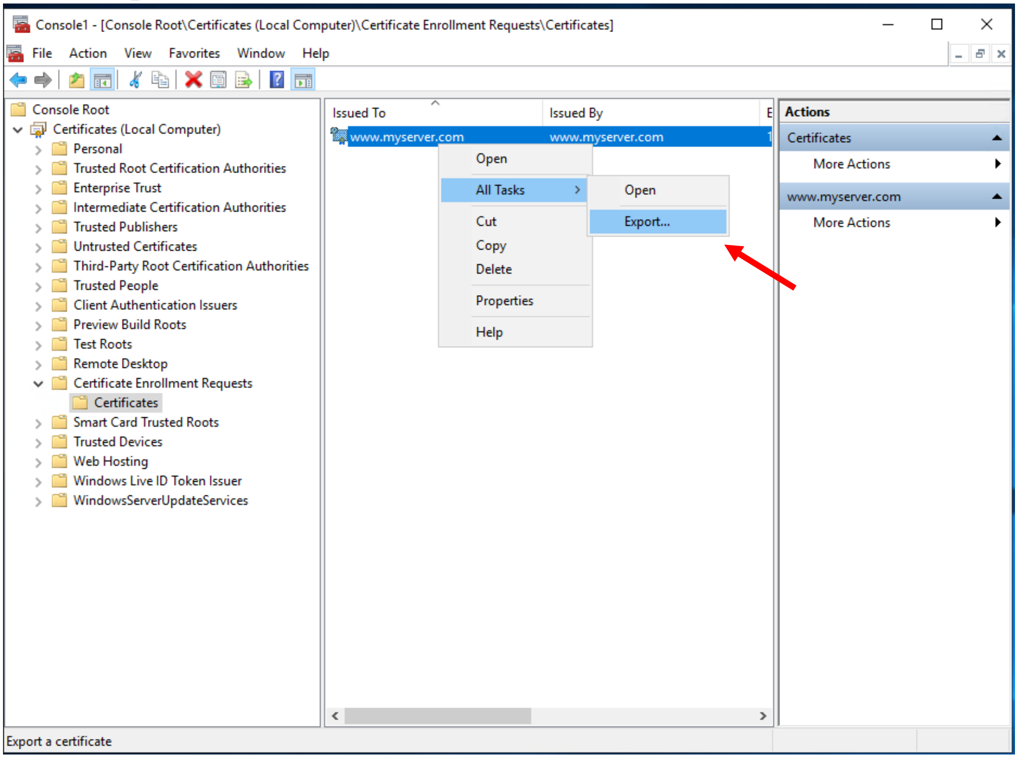
● Local computer: (the computer this console is running on)

○ Another computer:

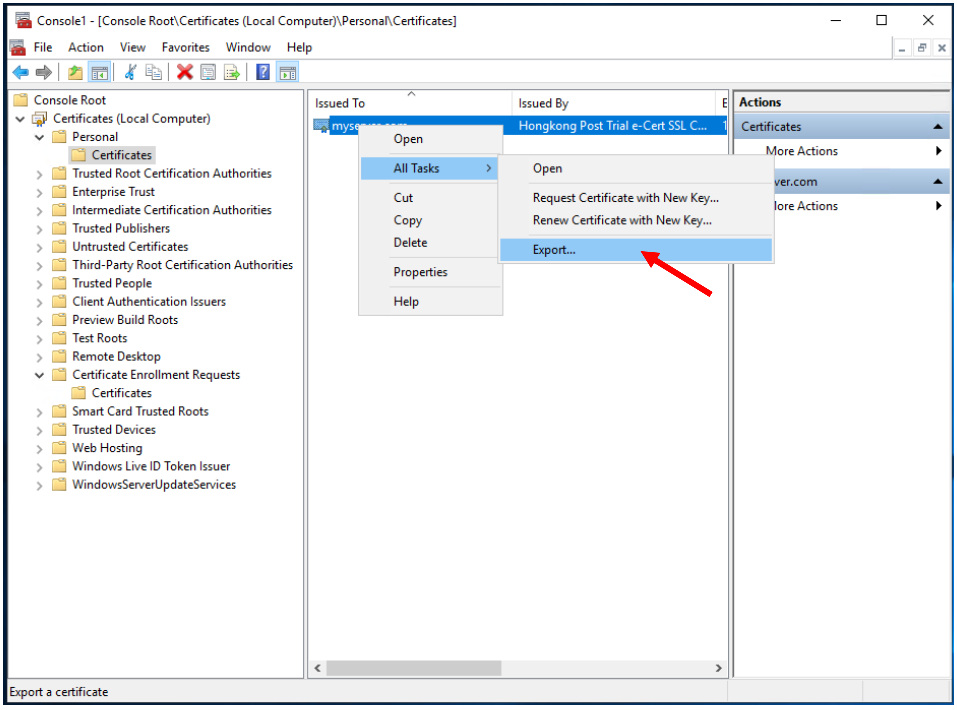
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

5. Backup the private key:

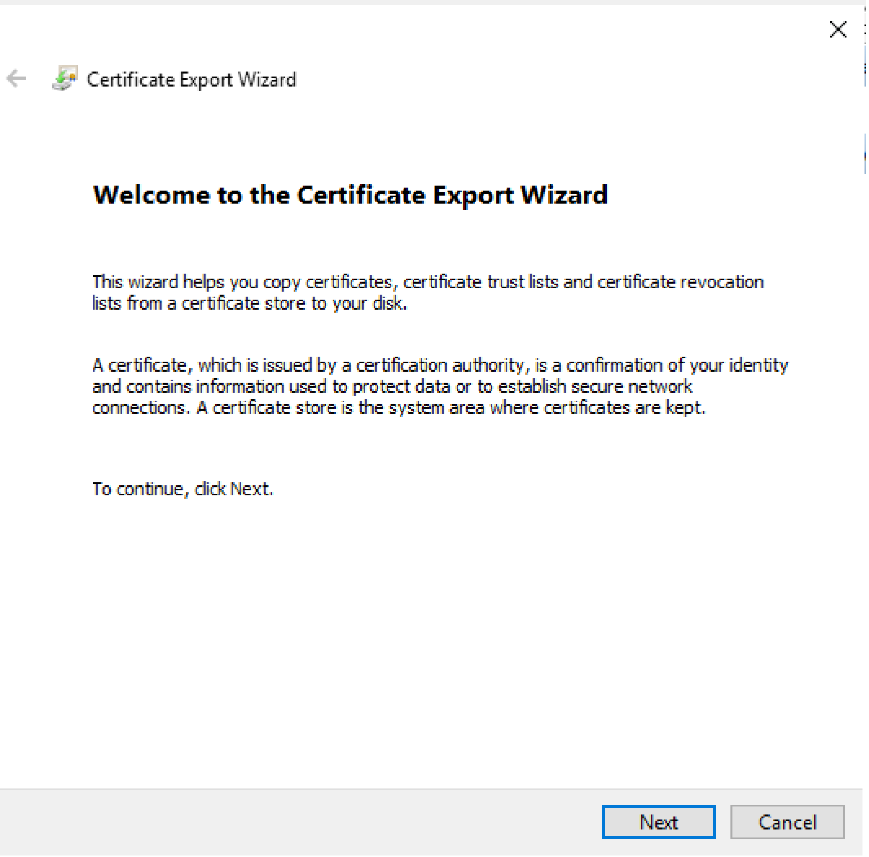
- To backup the private key of a pending request, expand “**Certificate Enrollment Requests**” (or named “**REQUESTS**” in some systems) and select “**Certificates**”, select the pending request that you just created, right-click and then select “**All Tasks**” > “**Export**”.


Console1 - [Console Root\Certificates (Local Computer)\Certificate Enrollment Requests\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Remote Desktop
Certificate Enrollment Requests
Certificates
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
WindowsServerUpdateServices
Issued To
Issued By
www.myserver.com
www.myserver.com
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Export...
Actions
Certificates
More Actions
www.myserver.com
More Actions
Export a certificate

- To backup the private key of an existing certificate, expand “**Personal**” and select “**Certificates**”, select the certificate that you would like to make a backup, right-click and then select “**All Tasks**” > “**Export**”.


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Remote Desktop
Certificate Enrollment Requests
Certificates
Smart Card Trusted Roots
Trusted Devices
Web Hosting
Windows Live ID Token Issuer
WindowsServerUpdateServices
Issued To
Issued By
Hongkong Post Trial e-Cert SSL C...
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Export...
Actions
Certificates
More Actions
ver.com
lore Actions
Export a certificate

6. In Certificate Export Wizard, choose “**Next**”.



Certificate Export Wizard

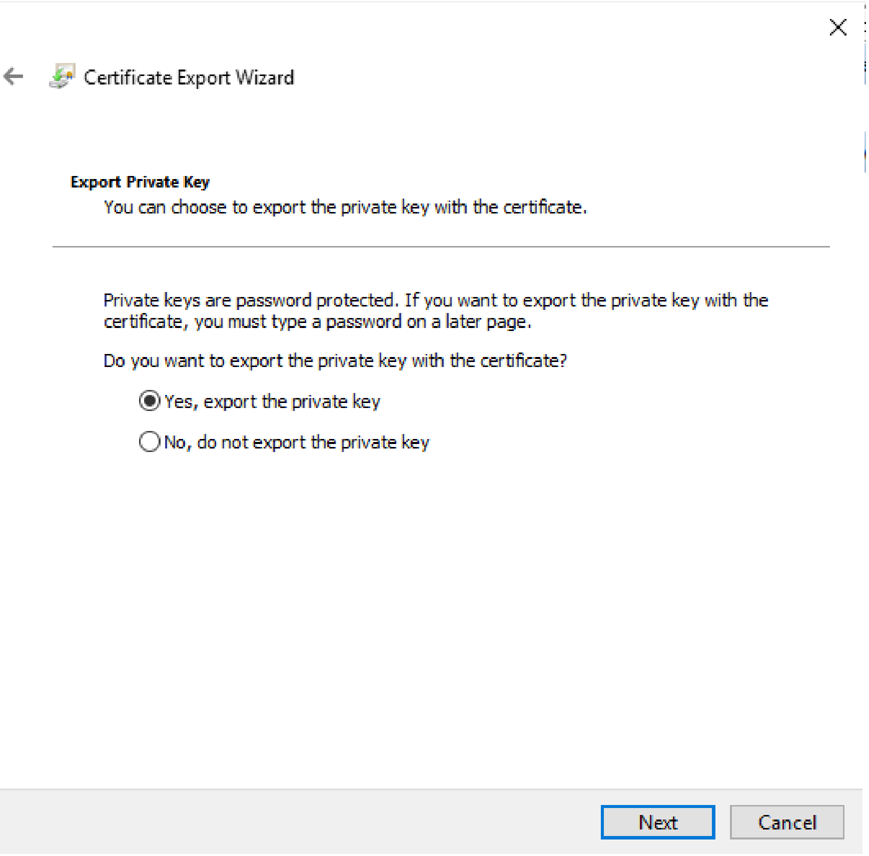
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Select “**Yes, export the private key**”, and then click “**Next**”.



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

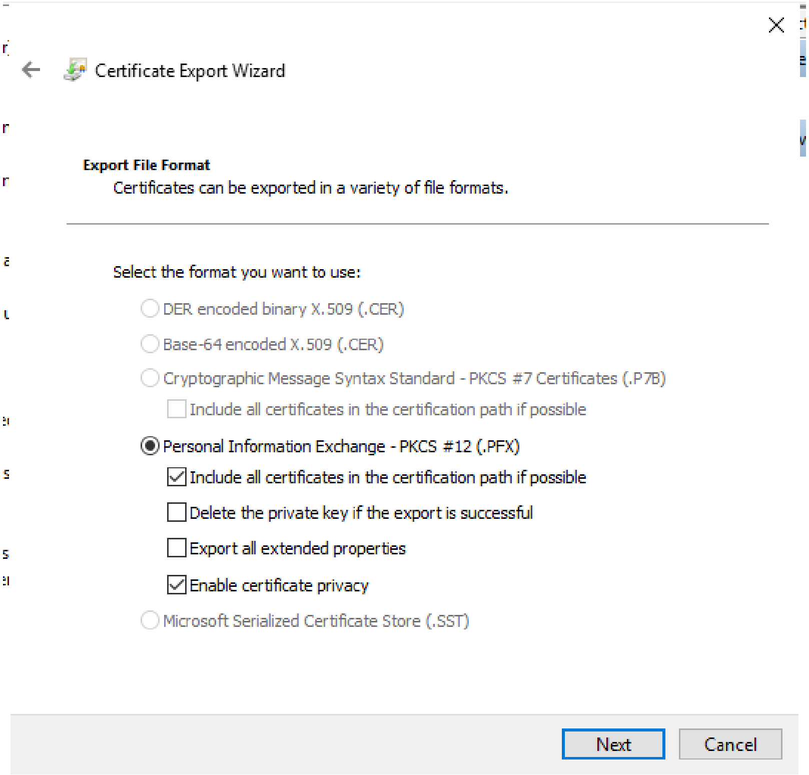
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

8. Select "**Personal Information Exchange - PKCS #12 (.PFX)**" and check the boxes "**Include all certificates in the certification path if possible**" and "**Enable certificate privacy**" while leave the other boxes unchecked, and then click "**Next**"



Certificate Export Wizard

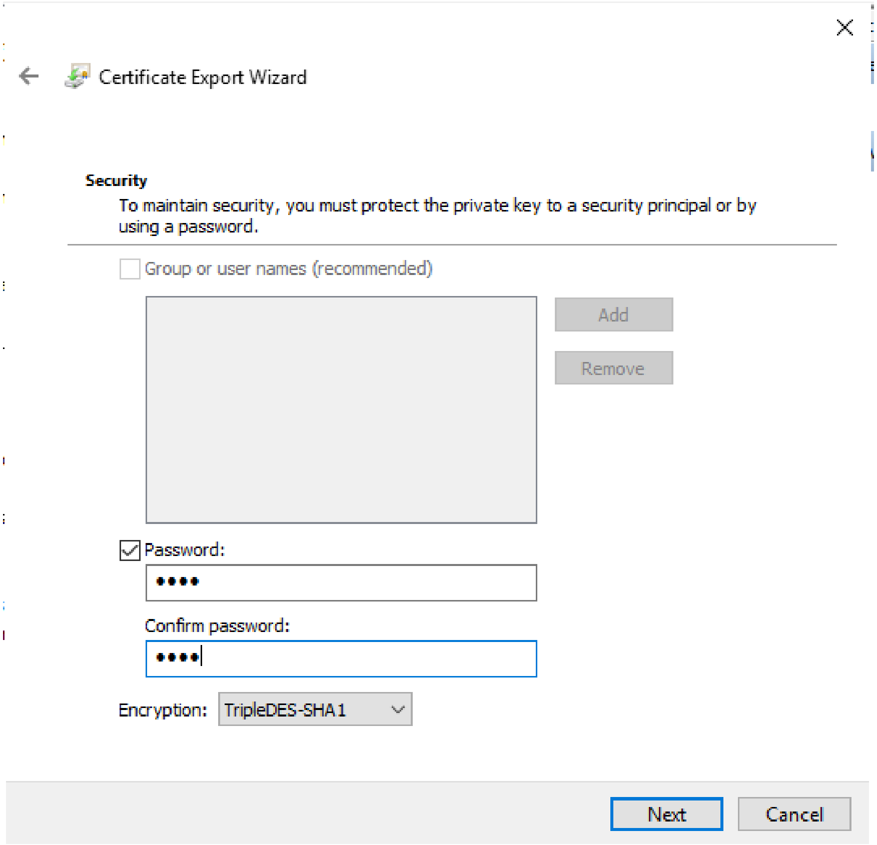
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  □ Include all certificates in the certification path if possible
● Personal Information Exchange - PKCS #12 (.PFX)
  ☑ Include all certificates in the certification path if possible
  □ Delete the private key if the export is successful
  □ Export all extended properties
  ☑ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

9. Type and confirm a password for the private key, and then click "**Next**".

Note: It is very important that you remember this password. If you forget it, you will be unable to restore your private key.



Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

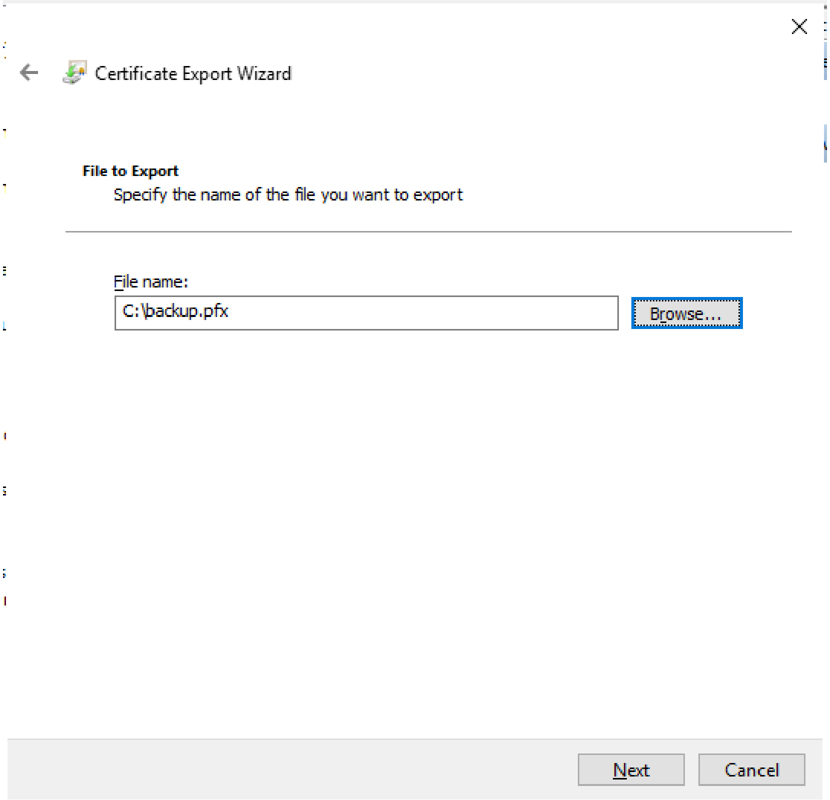
□ Group or user names (recommended)

☑ Password:
••••

Confirm password:
••••

Encryption: TripleDES-SHA1

10. Specify the name of the file you want to export, and then click “**Next**”. (By default, the file will be saved with a .PFX extension.)



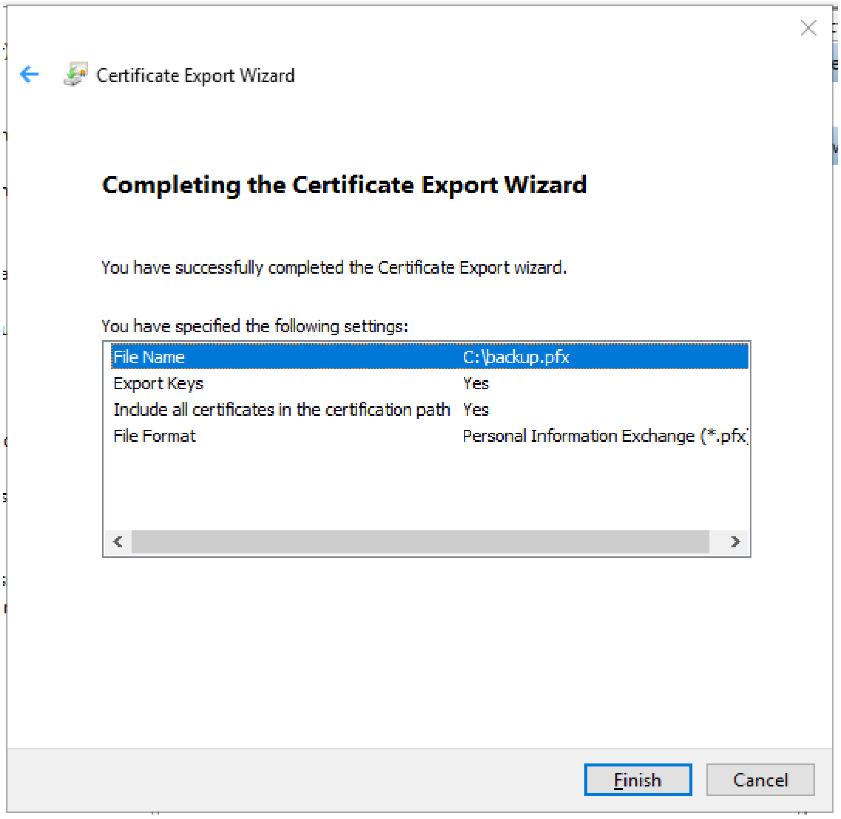
File to Export

Specify the name of the file you want to export

File name:

C:\backup.pfx

11. Click “**Finish**” to close the wizard.



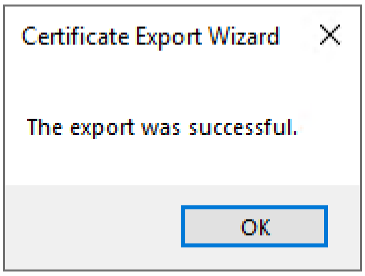
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\backup.pfx
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx

12. Click “**OK**” to complete

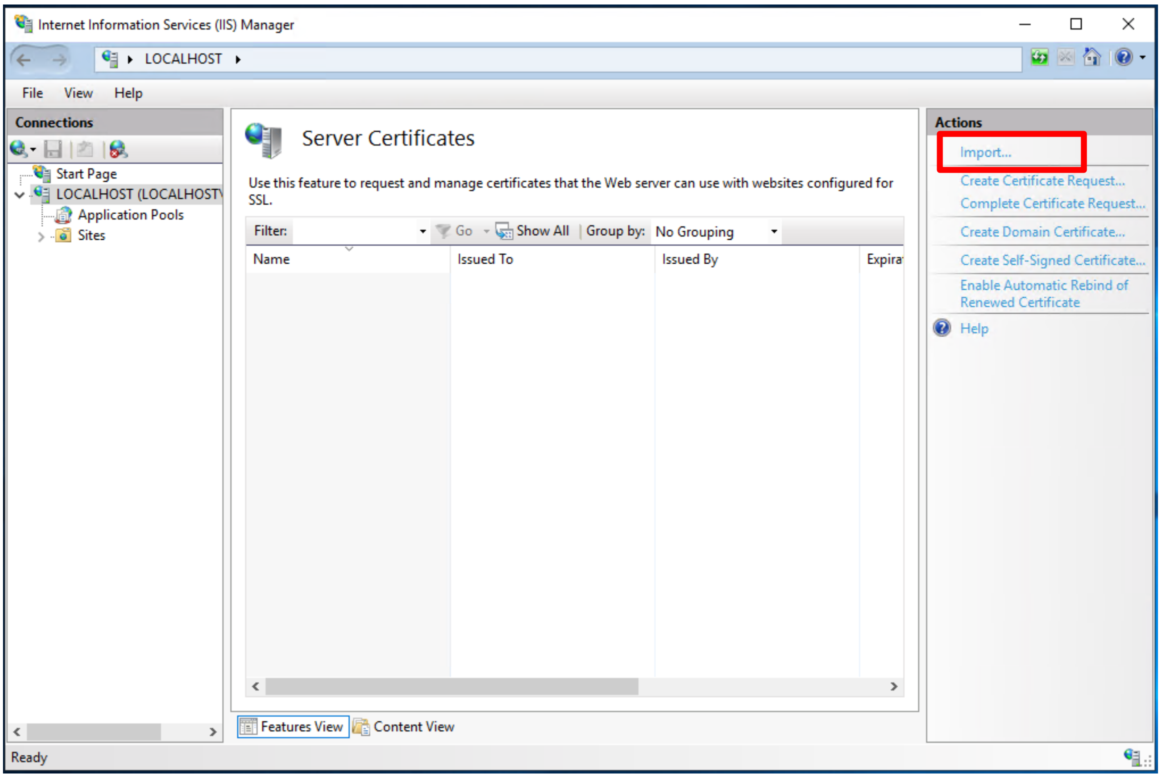


Certificate Export Wizard

The export was successful.

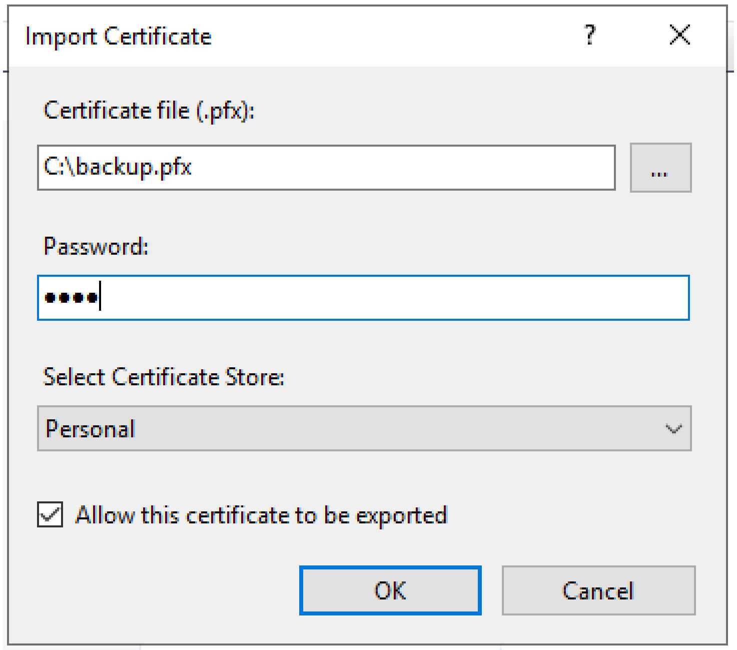
G. Restoring the Private key

1. Start menu, “**Administrative Tools**”, and click on “**Internet Information Services (IIS) Manager**”.
2. Select your web site, and then double-click “**Server Certificates**”.
3. At right column “**Actions**”, select “**Import**”


Internet Information Services (IIS) Manager
LOCALHOST
File
View
Help
Connections
Start Page
LOCALHOST (LOCALHOST\
Application Pools
Sites
Server Certificates
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.
Filter:
Go
Show All
Group by:
No Grouping
Name
Issued To
Issued By
Expira
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready

4. Enter the path and file name of the file containing the certificate, and password, then click “**OK**”.

Note: You may uncheck the box “Allow this certificate to be exported” to not allow the certificate to be exported. Or to allow you to back up or transport your certificate at a later time, you may check the box “Allow this certificate to be exported”.



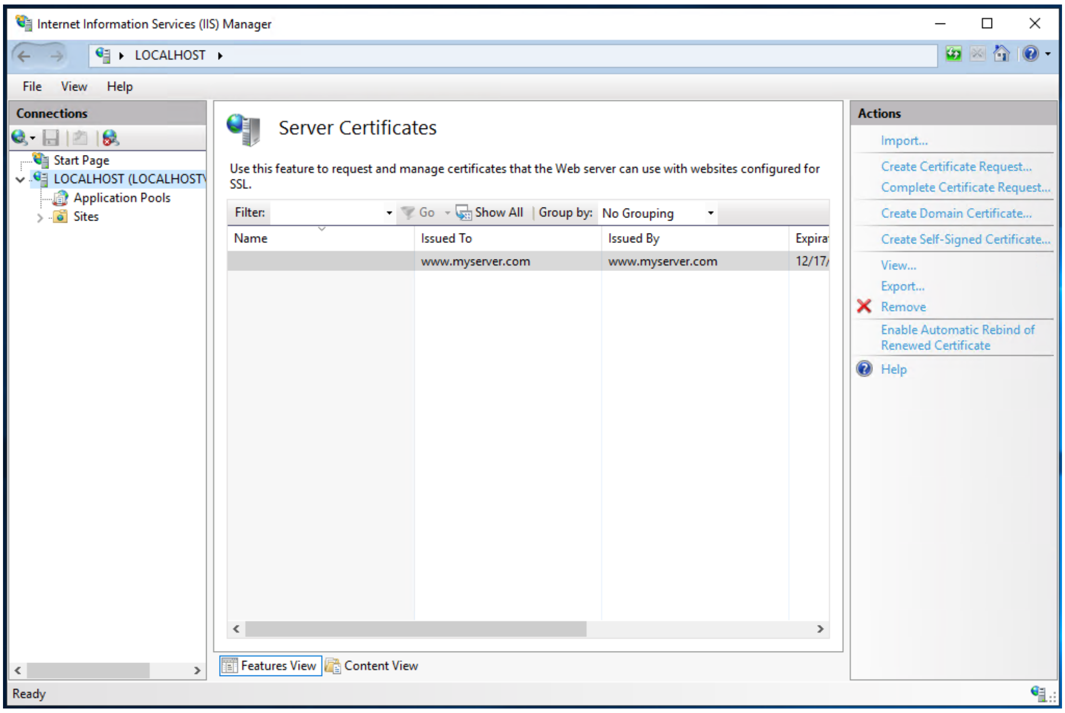
Certificate file (.pfx): C:\backup.pfx

Password: ●●●●

Select Certificate Store: Personal

☑ Allow this certificate to be exported

5. “**Hongkong Post e-Cert (Server)**” certificate has been successfully restored.


Internet Information Services (IIS) Manager
LOCALHOST
File
View
Help
Connections
Start Page
LOCALHOST (LOCALHOST)
Application Pools
Sites
Filter:
Go
Show All
Group by:
No Grouping
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expira
	www.myserver.com	www.myserver.com	12/17/