

3.Import SSL certificate

3.1 Get SSL certificate

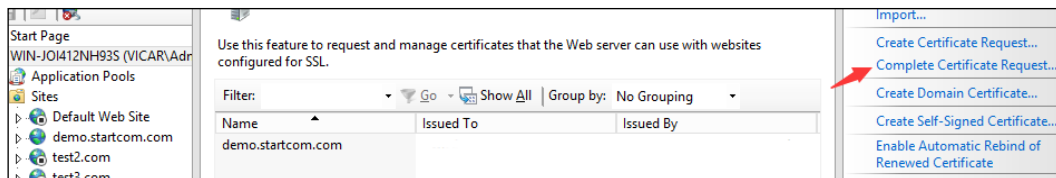
You will get a zip file after you apply the certificate from StartCom successfully. Then you extract the file, you will get 4 files. After we extra the IIS Server.zip, we can get 2 certificates.

 Apache Server.zip	2016/1/7 10:27	Compressed (zipp...	4 KB
 IIS Server.zip	2016/1/7 10:27	Compressed (zipp...	4 KB
 Nginx Server.zip	2016/1/7 10:27	Compressed (zipp...	3 KB
 Other Server.zip	2016/1/7 10:27	Compressed (zipp...	4 KB

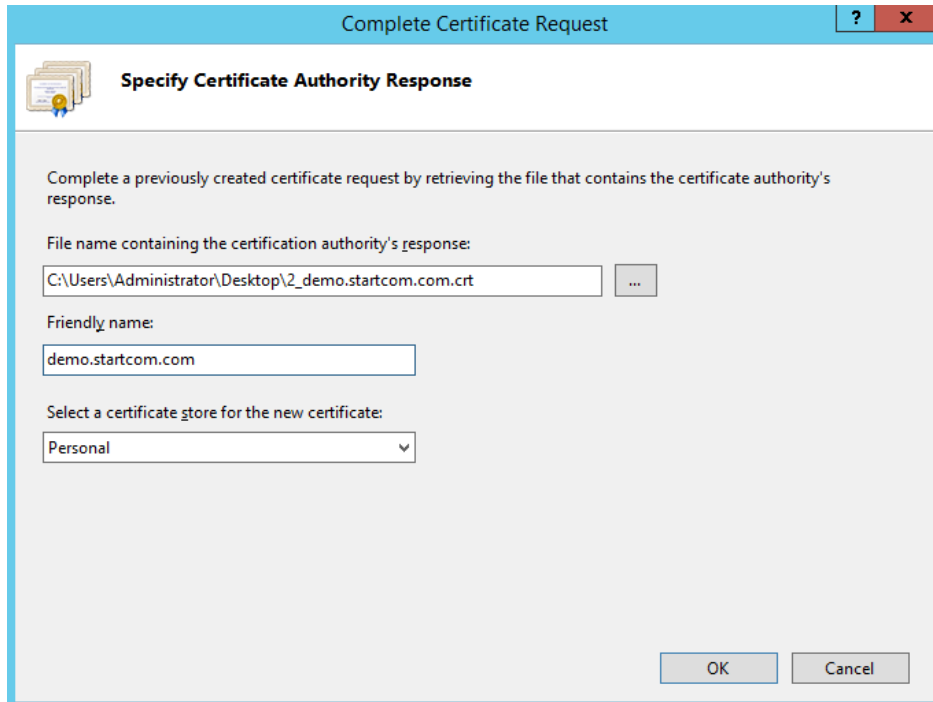
 1_Intermediate.crt	2016/1/7 10:27	Security Certificate	3 KB
 2_demo.startcom.com.crt	2016/1/7 10:27	Security Certificate	3 KB

3.2 Import SSL certificate

Back to server certificate, click Complete Certificate Request.



Upload 2_domian.com.crt to your server. Click "Browse" to select the Certificate and set a Friendly name for the certificate, complete the import of the certificate.



Import the intermediate certificate in your local mmc.

Start → Run → MMC, Start console → Select menu file → Add / remove management unit” → Select the certificate in the list → click “add” → choose “Computer account” → Click Finish. On the left side of the console display certificate tree list, choose “Personal” → “certificate”. Right click, choose “All tasks → Import”.

Import “1_Intermediate.crt” and the following g3 cert into the ‘Intermediate Certification Authorities’.

-----BEGIN CERTIFICATE-----

```
MIIGXjCCBEagAwIBAgIQMhHgbC2MmjmGj0BgeDy2ATANBgkqhkiG9w0BAQsFADB9MQswCQYDVQQGEwJJTDEWMBQGA1UEChMNU3RhcncnRDb20gTHRkLjErMCKGA1UECxMiU2VjdXJlIERpZ2l0YWwgQ2VydGlmaWNhdGUgU2lnbmluZzEpMCCcGA1UEAxMgU3RhcncnRDb20gQ2VydGlmaWNhdGlvbiBBdXR0b3JpdHkwHhcNMTcwNDExMDczMDAxWhcNMjIwNDExMDczMDAxWjBRMQswCQYDVQQGEwJFUzEUMBIGA1UECgwL
```

U3RhcnRDb20g
Q0ExLDAqBgNVBAMMI1N0YXJ0Q29tIENlcnRpZmljYXRpb24gQXV0aG9yaX
R5IEcz
MIICljANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA6itwI0q4m0+q8L1
Nyjjk
gUWnCAgogaXI6Wn7Kvg9in7zgnVSEuLdiWbBuNxyECYi17gaWlqo0PepYN/
+orOK
xCbUjmhYRcDiUpglHWi5Lkpf8nPHB+jWe/BdumRkldOwULDCDgwMpkPn/O
2eHhbK
XgWGOy0Rs7/1NGfPIZykLiJxSgwij21z4HrRnfyC+1vAhm8qf0DgpNLCLoLgE
AfW
MdxjZiCx37U4N3M3qn4b9dd4h98+ZxR6fjlmjhKcAb1TkUnx52ADLkcMlf978u
8N
QL6MG7frrH2m7tQhm6xXBhKNZwoDR3yZAP2Wu8cDP374+NPUXt7eXXAH
CBE+CypM
FQAtq3gB5uvwPNhSBUgVLO+6BGcS+n/1eZxZYQTnVel5O4rxW3+s4vNZ0k
sos4Yn
557nnmyJjPWnPqnQT1hCtubKCSZ62JO/r8+VF1Koj0AWE9WSWW4DDSF
B1P6vmfxY
BhmdC6uw7kLi/jinPO1MUkf75tuUFD0NXkOKqL7abFLWAqUpfEZ1E7bjH8fq
U/Ap
DqwnP8Yn2F6KIWnzCwQ6gX1IWEc9+A5MUSfrl/DwsDvqmu9QfXhoRci44Yq
AyRYY
JQ1N3u3nPHRSVxLRrHI+wE+GLaJrY1JYvToxuf7Pp+sBdSHjaXdBsyTXb/fTT
uEH
JDbT9m6R3TifWbRjyJ15Oa0CAwEAAaOCAQQwggEAMA4GA1UdDwEB/wQ
EAwIBBjAS
BgNVHRMBAf8ECDAGAQH/AgECMDIGA1UdHwQrMCkwJ6AloCOGIWh0dH
A6Ly9jcmwu
c3RhcnRzc2wuY29tL3Nmc2NhLmNybDBmBggrBgEFBQcBAQRaMFgwJAYI

KwYBBQUH

MAGGGGh0dHA6Ly9vY3NwLnN0YXJ0c3NsLmNvbTAwBggrBgEFBQcwAoY
kaHR0cDov

L2FpYS5zdGFydHNzbC5jb20vY2VydHMvY2EuY3J0MBOGA1UdDgQWBTL
EK0sRt0m

Rd+uF9YbH73ymmCqFDAfBgNVHSMEGDAWgBROC+8apEBbpRdphzDKN
GhD0EGu8jAN

BgkqhkiG9w0BAQsFAAOCAgEAZ1zbnAOD3Xlg2Q/tN/Z7J/0H7xdqA9kqmEo
3K01

K5KgmYFVblc+kq1XyYt9qX0/OCnpKTo/rBTHr70bXofGT0i/X1JwICXSEF4GL
9gc

vDTPEbXaVpFSvPpJgXg+GIJhdg5CUiGOFF1yK0d7DxIIAAUvhPNIu8ZF0go
w16Ae

EXPFG4E7ay4mTRaXc2nAO9dVnnH6wxqruVMc/AEwGIKw+xKHjbHCdnY5k
B13cGpJ

0pxrBGcduS7AL3tU1pYPIpNFwfHnnlBEWa6+9/fQHxFMcr0L8GPhLx/k2pur
4gm

NDYqd8mqAReVYhqCMFrB5RoGMW19r80OyDd4jVDn9drdcXtKIJ2X9ppiEfX
GbKWz

B4UZUwwrZr582ZbShWdilVOfGW9QnaIYoAisq89IP3PpDYAI5Afz3IQN0EUs
TbN3

ydiGN7+xG52b+yL9fQMBpur6ymPD5AAAd7Fyfbb1YBvdR9L0qjZBstLrfkBiRlc
h

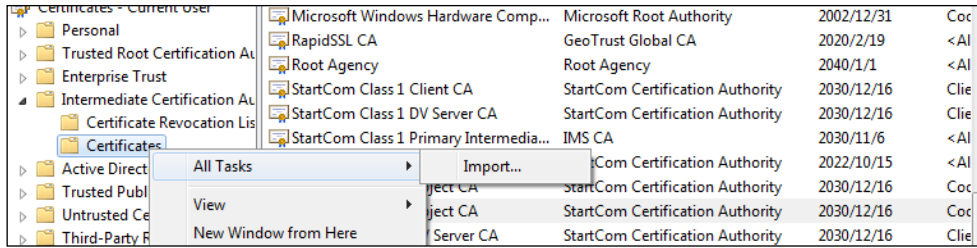
zOC06vVFXkw/tC5VaDhoBrgRU6CsD2Dz8tNUb/SPRloVrsC7HXjWCIUeyR9g
KgEJ

vEjYQJOKTsmEQntrA3/mhTfkD2d7+eK+kSpcASd9wkA32bOoeRve+mxUAAtC
FFYMg

o3AgMaMBBnr9cy1bfchq5RBparix43pKEZ/JIDfkUJFkMAjXNWrLixzWT+dg
WCt

eXA=

-----END CERTIFICATE-----



3.3 Binding server certificate

Open the IIS manager panel, find the site to be deployed certificate, click on the "binding".

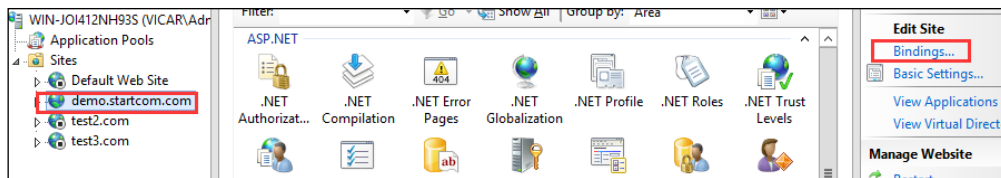
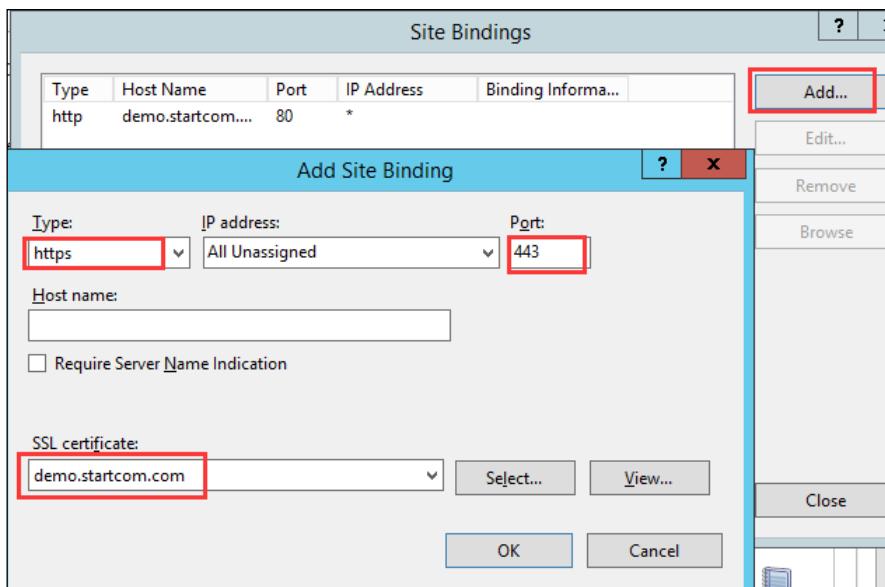


Figure 3

Setting parameters

Select "binding" → "add" → "Type selection HTTPS" → "Port 443" → "SSL certificate the name of the imported certificate" → "Determine", SSL default port 443 port.

(Please don't make any changes. If you use other ports such as: 8443, you must enter the <https://www.domain.com:8443>.)



3.4 Test the SSL certificate.

Input the address in browser address bar: `https://domain.com` (the domain of the applied SSL certificate) Test your SSL certificate is installed successfully or not. If successful, the browser address bar will display a safety lock sign.

You could test your website's certificate and configuration by

<https://www.ssllabs.com/ssltest/>.

4.Backup of SSL certificate

When you have finished installing the certificate, please backup your certificate as follow.

1. Back to Console1, go Certificates (Local Computer)→Personal→Certificates, choose your certificate just you have installed. Right click → All Tasks → Export.

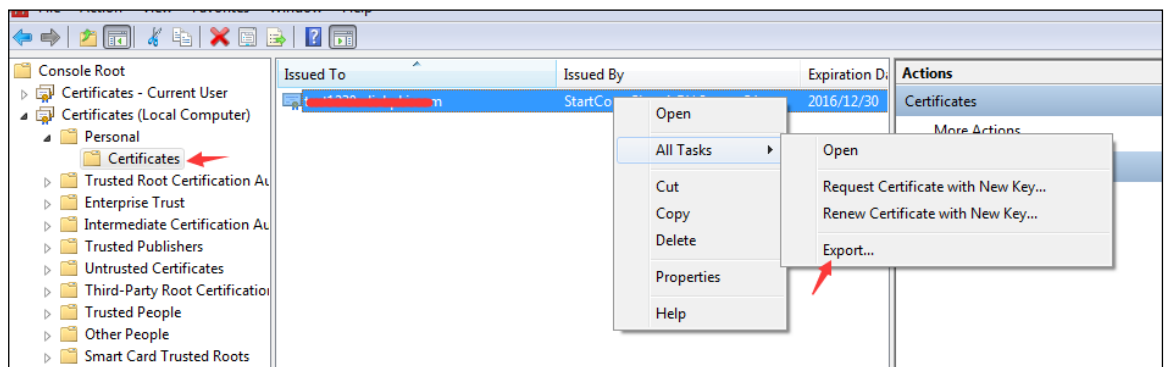
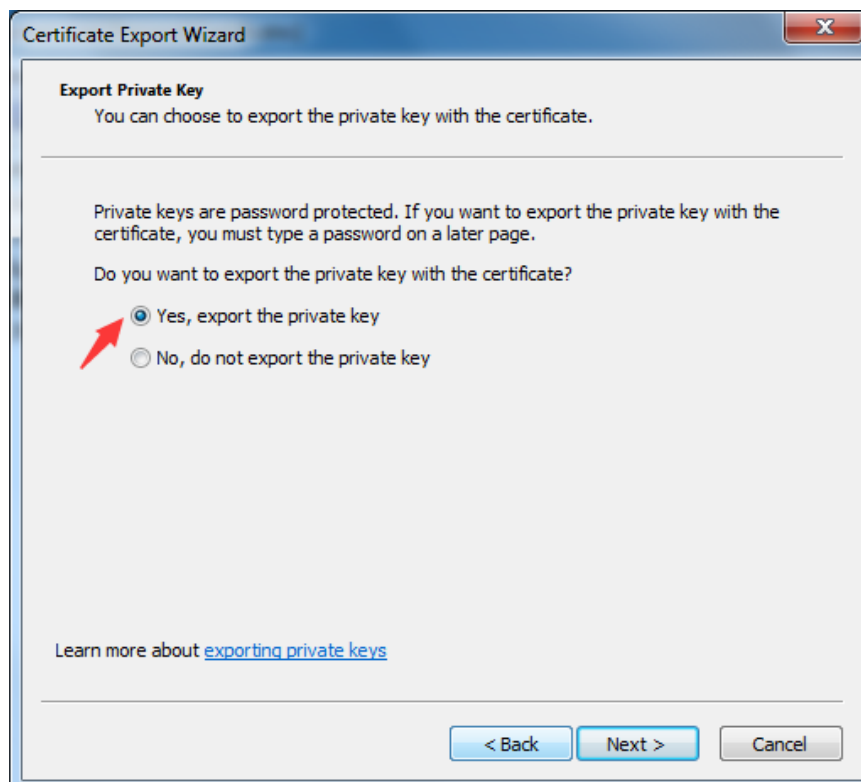
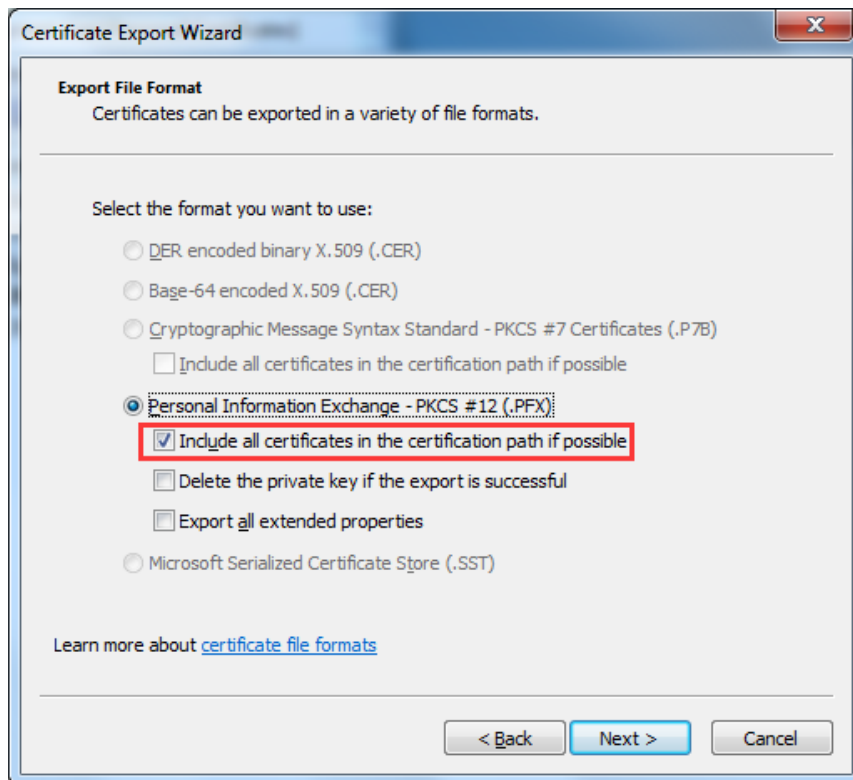


Figure 12

2. Then attend to check 'Yes, export the private key', click next.



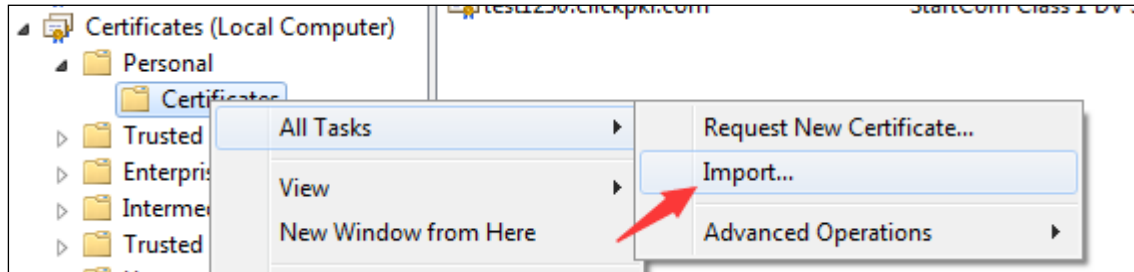
3. Check 'Include all certificates in the certification path if possible', click next.



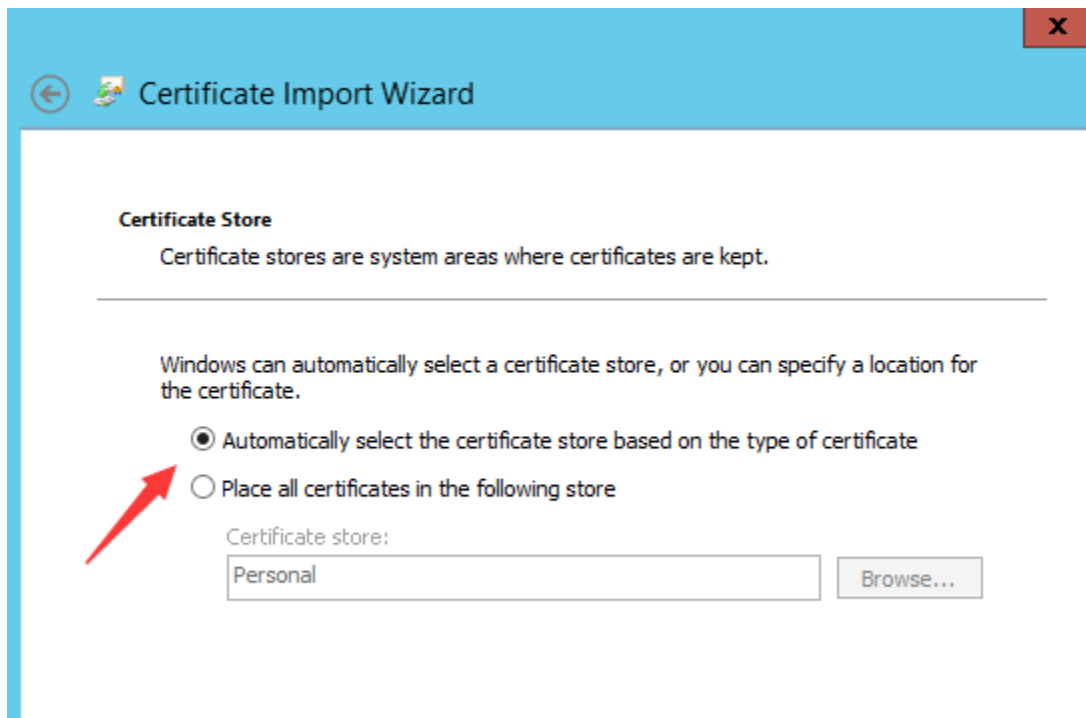
4. Type and confirm your password, Specify a name and path of this file, you will get a certificate PFX format, keep these in mind.

5.Restore of SSL certificate

1. Go Certificates (Local Computer) → Personal → Certificates, right click Certificate select Import as follow.



2. According to the certificate Import Wizard, import the PFX format certificate to “Automatically select the certificate store based on the type of certificate”, type your password of certificate, finish import certificate.



3. Open the IIS manager panel, Binding certificate again.