政府伺服器數位憑證管理中心(GTLSCA)

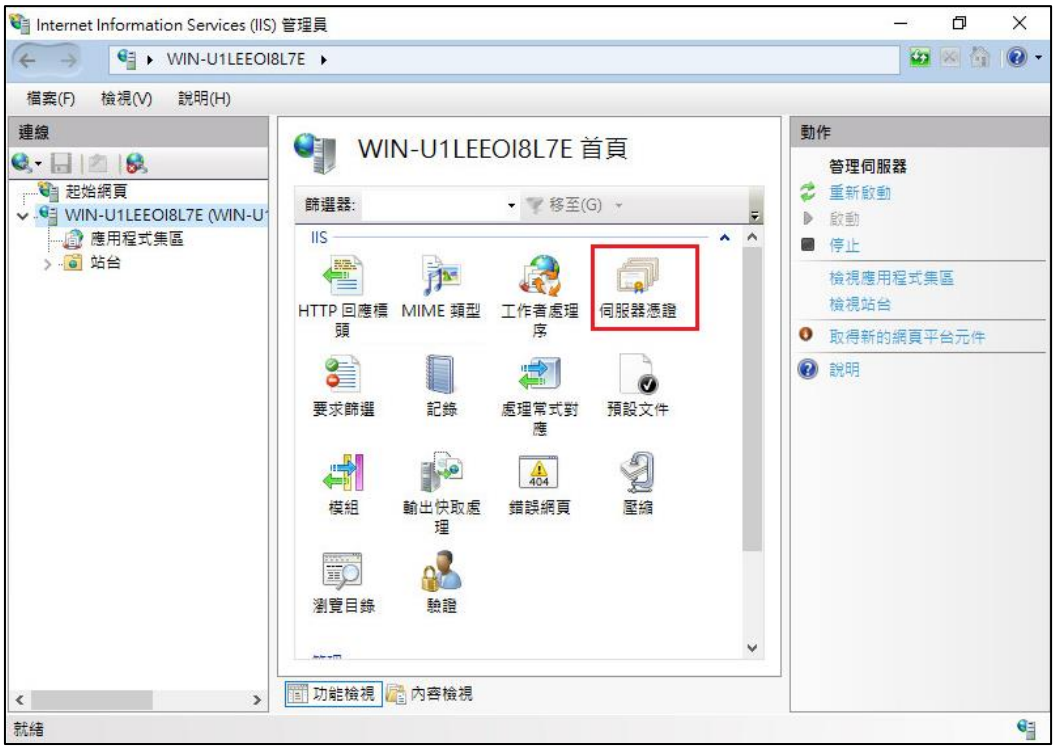
金鑰對未改變，僅更換 TLS 憑證操作手冊

中華民國 113 年 5 月

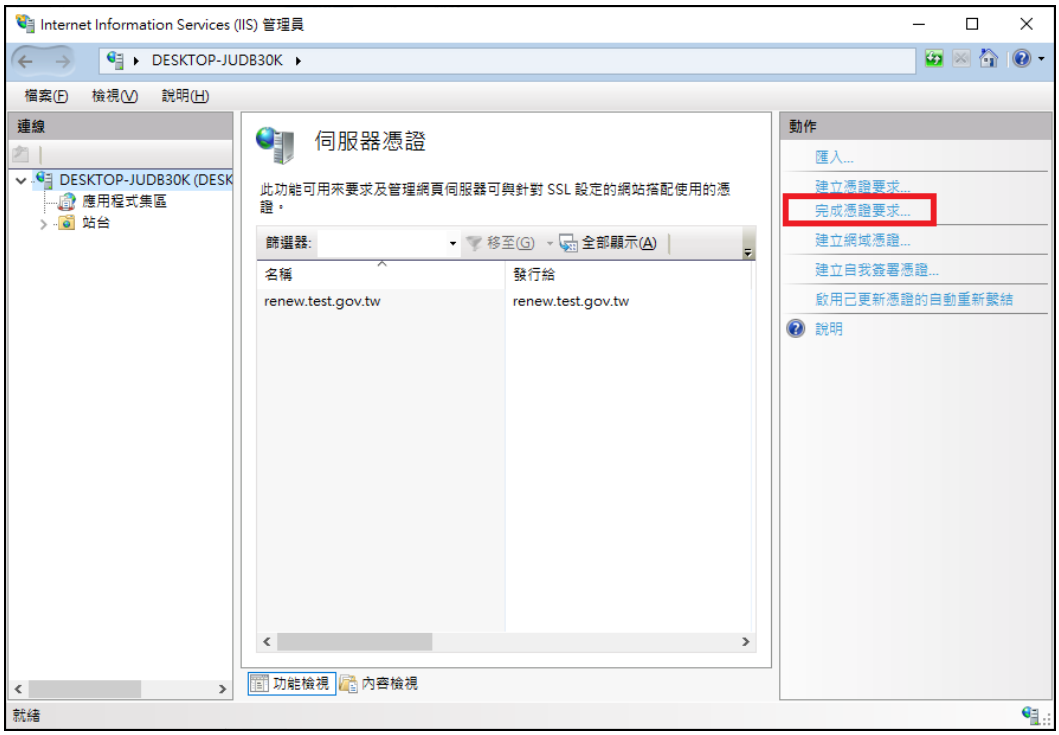
目錄

網站伺服器：IIS

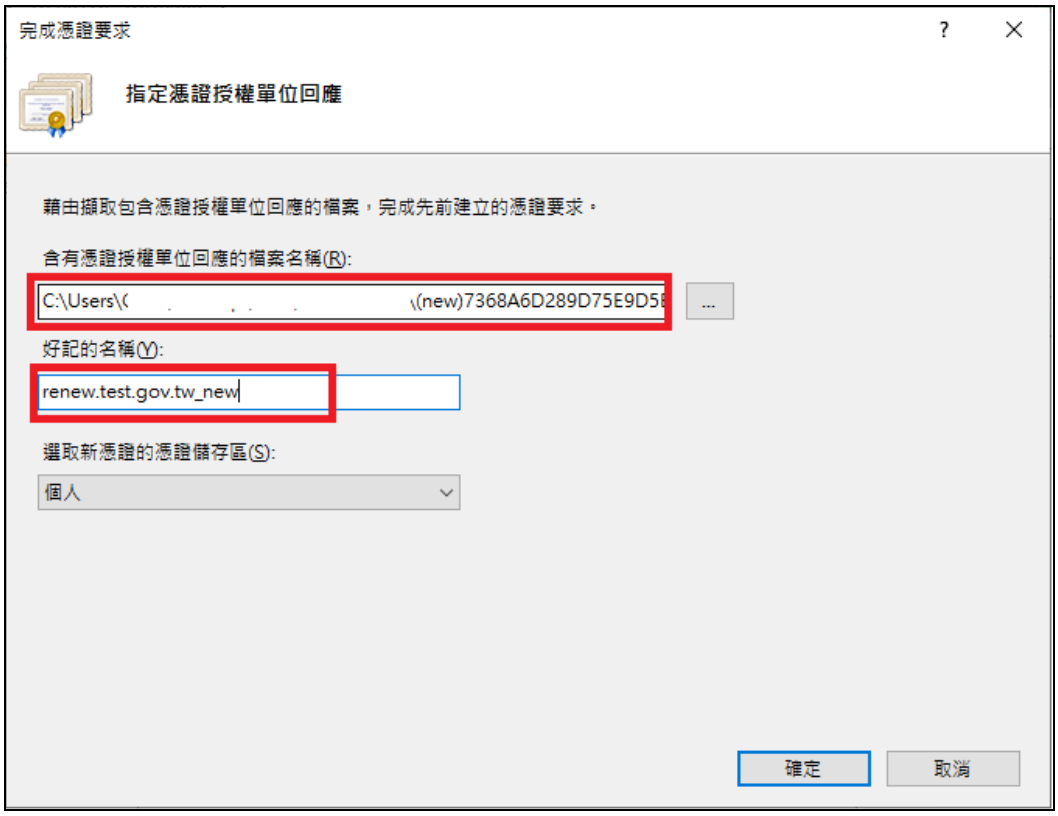
1. 開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



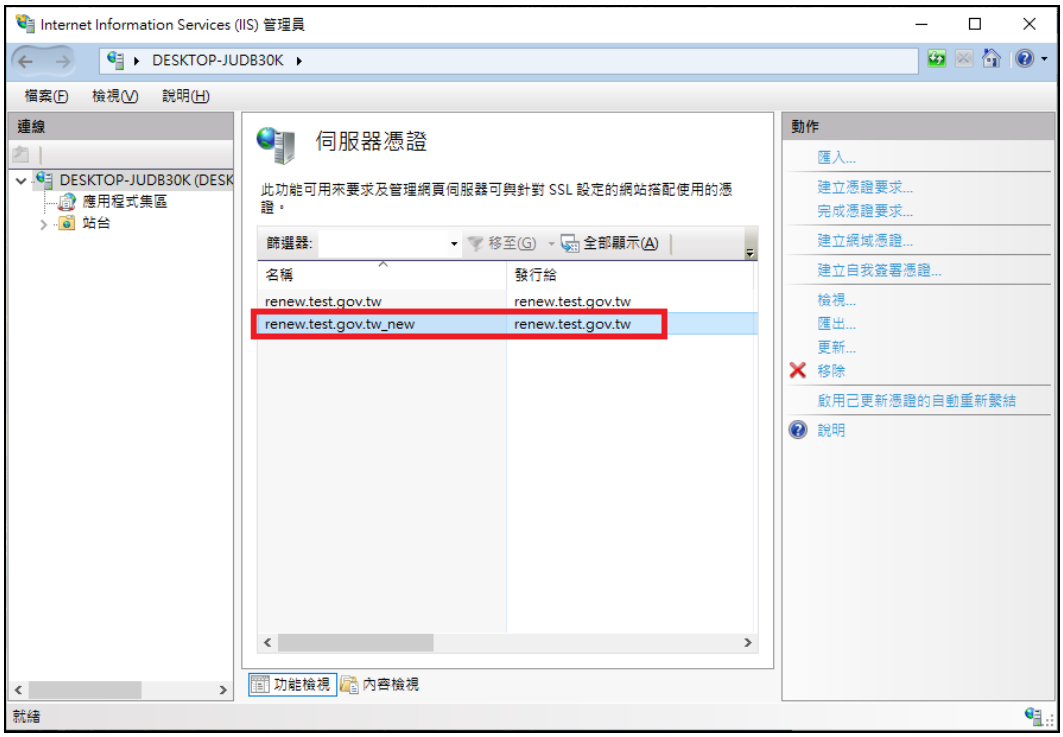
2. 點選「完成憑證要求」。(請確認原憑證是否已安裝於同一台伺服器裡。)



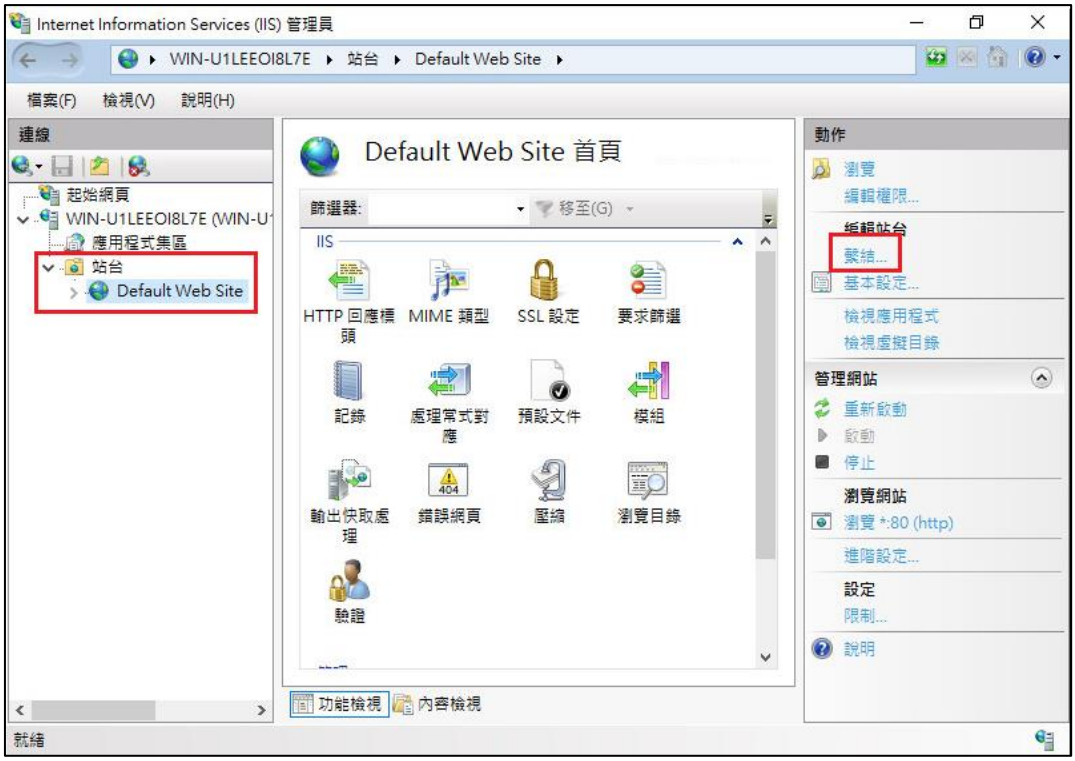
3. 選擇新的 TLS 憑證，並輸入好記的名稱。



4. 按「確定」，出現完成憑證要求的畫面，多一條新憑證列表。

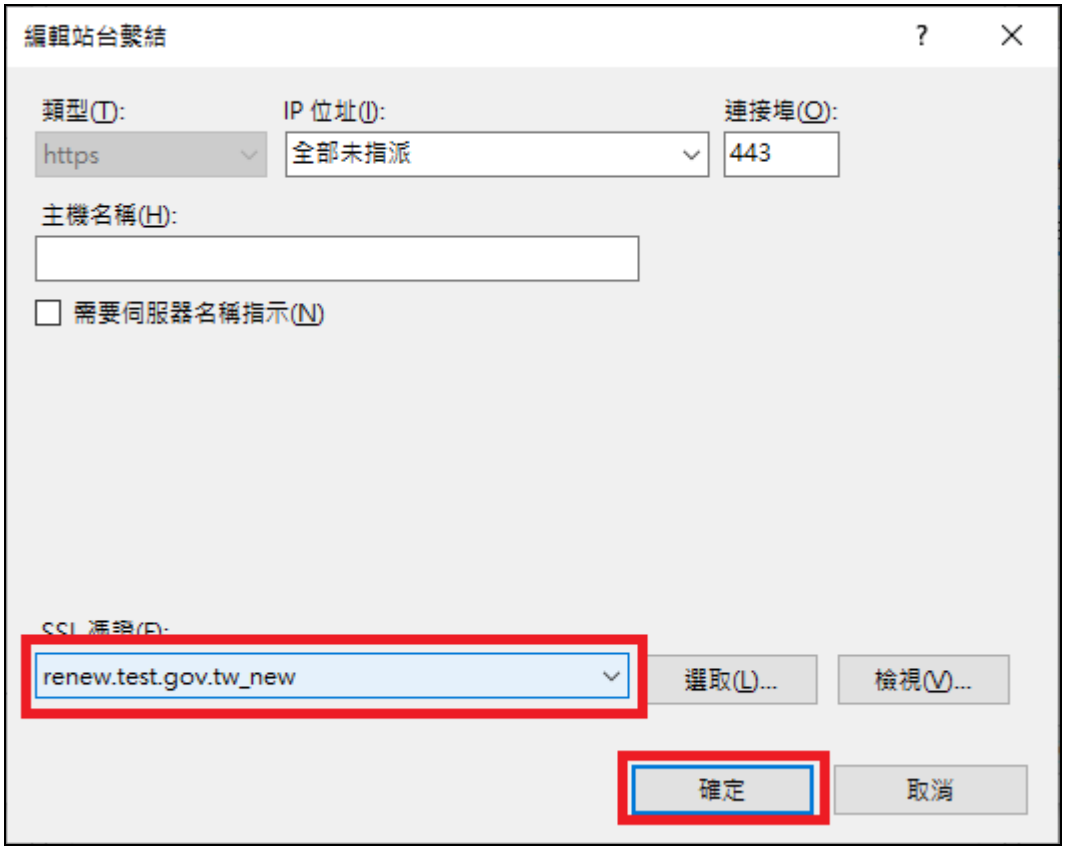


5. 點選要安裝的站台，本手冊以(Default Web Site)進行說明，選擇「繫結」。



6. 選擇已存在的 https 443 連接埠，點選「編輯」。

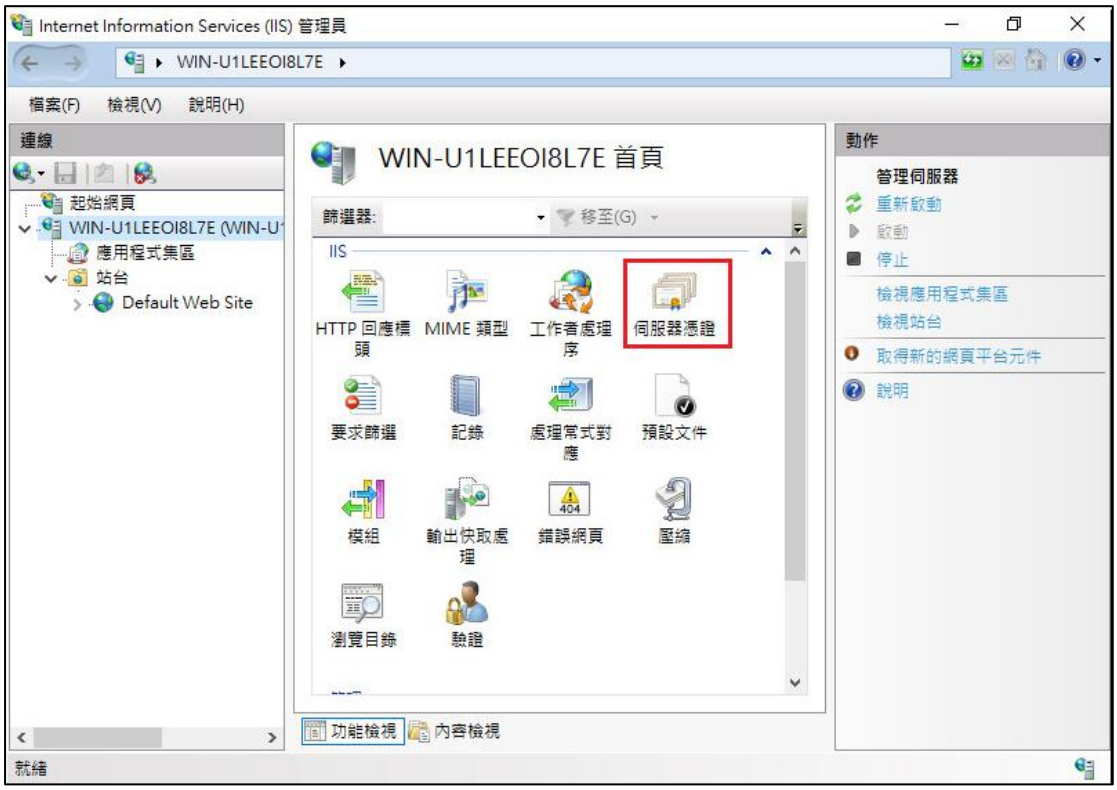
7. 重新選擇要安裝在此站台新的 TLS 憑證。(其餘設定皆不需變動)



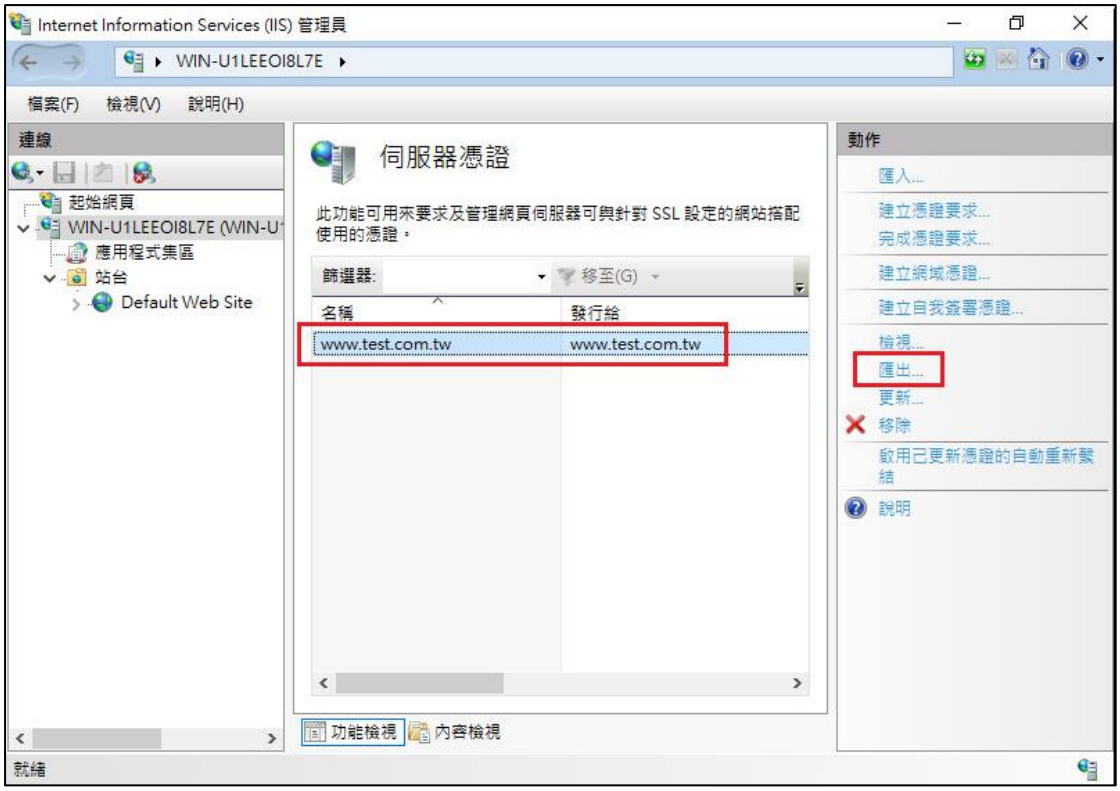
◆ 若因遠端連線匯入無法成功，可改下方操作方式。

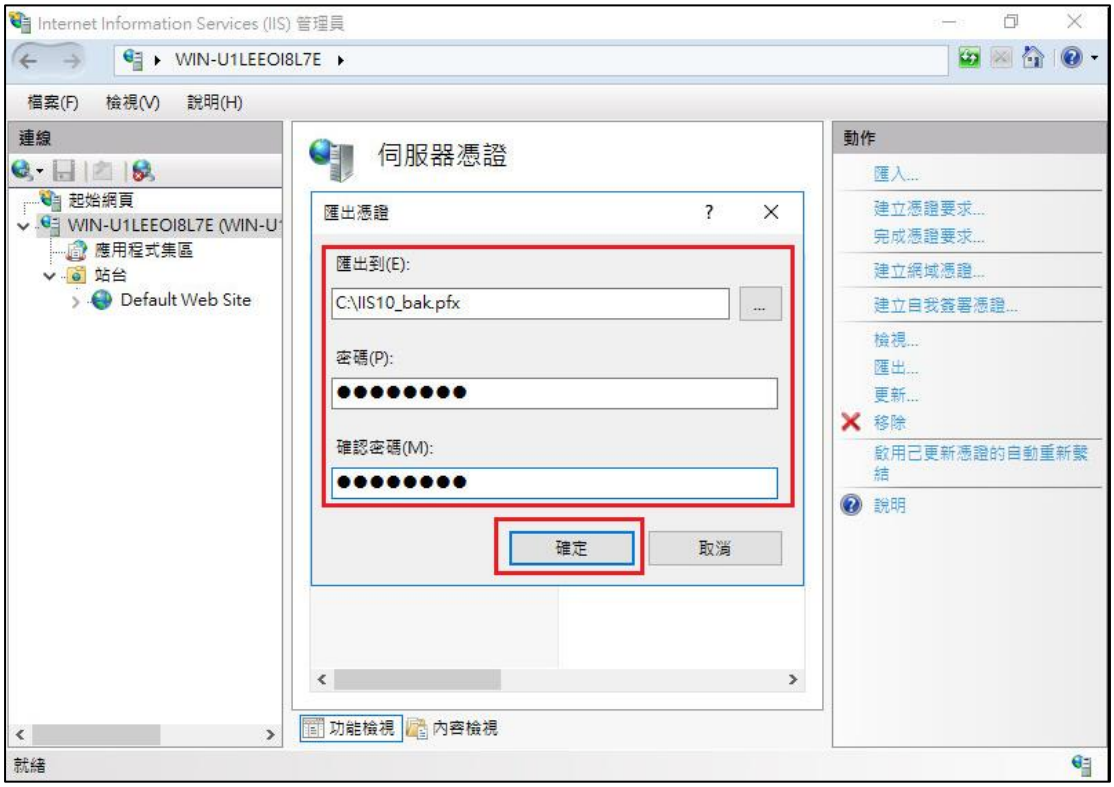
1. 請將原憑證備份匯出。

(1) 開啟「Internet Information Services (IIS)管理員」。
在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



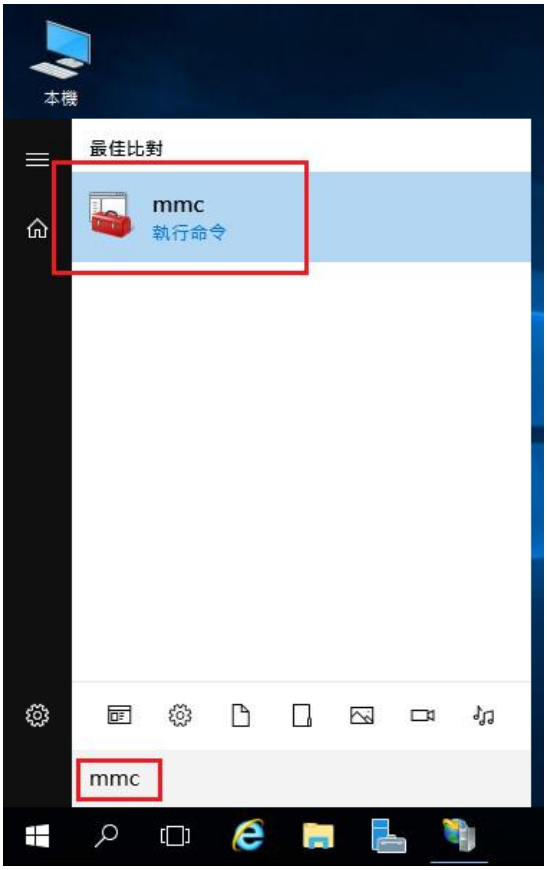
(2) 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。


Internet Information Services (IIS) 管理員
WIN-U1LEEOI8L7E
檔案(F)
檢視(V)
說明(H)
連線
起始網頁
WIN-U1LEEOI8L7E (WIN-U
應用程式集區
站台
Default Web Site
伺服器憑證
此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站搭配使用的憑證。
篩選器:
移至(G)
名稱
發行給
www.test.com.tw
www.test.com.tw
功能檢視
內容檢視
就緒
動作
匯入...
建立憑證要求...
完成憑證要求...
建立網域憑證...
建立自我簽署憑證...
檢視...
匯出...
更新...
移除
啟用已更新憑證的自動重新繫結
說明

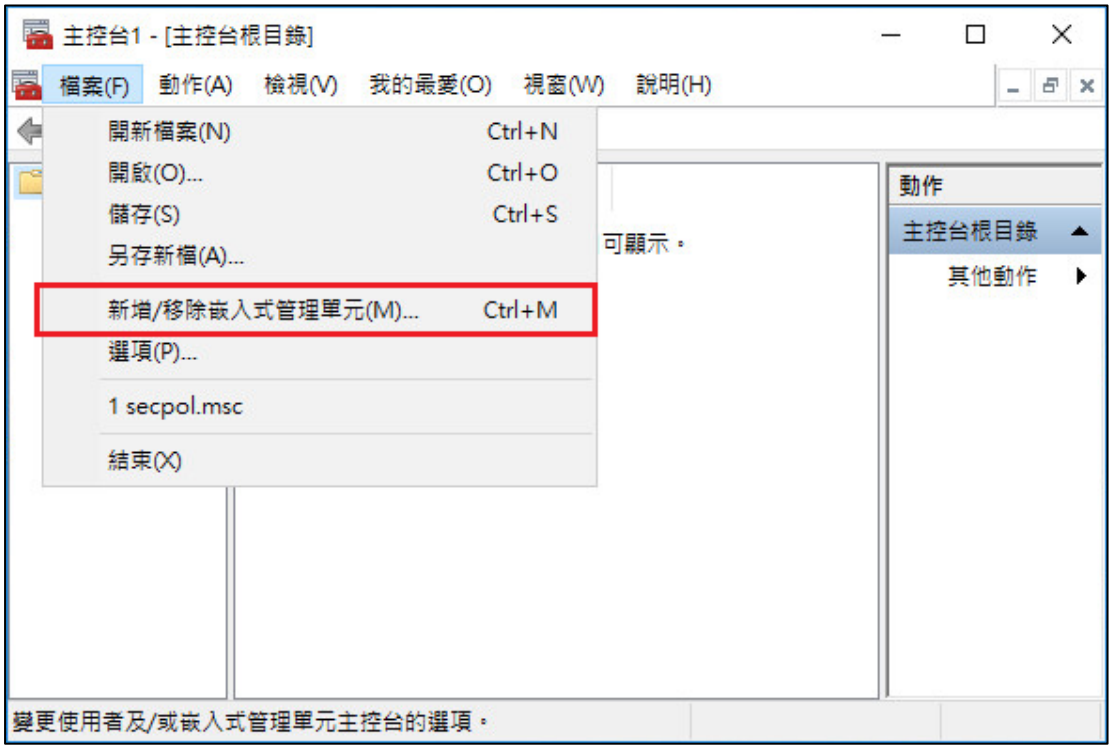

Internet Information Services (IIS) 管理員
WIN-U1LEEOI8L7E
檔案(F)
檢視(V)
說明(H)
連線
起始網頁
WIN-U1LEEOI8L7E (WIN-U
應用程式集區
站台
Default Web Site
伺服器憑證
匯出憑證
匯出到(E):
C:\IIS10_bak.pfx
密碼(P):
確認密碼(M):
確定
取消
功能檢視
內容檢視
就緒
動作
匯入...
建立憑證要求...
完成憑證要求...
建立網域憑證...
建立自我簽署憑證...
檢視...
匯出...
更新...
移除
啟用已更新憑證的自動重新繫結
說明

2. 將匯出的 PFX 檔匯入至其他有安裝 IIS 的電腦(請利用 mmc 匯入方式)。

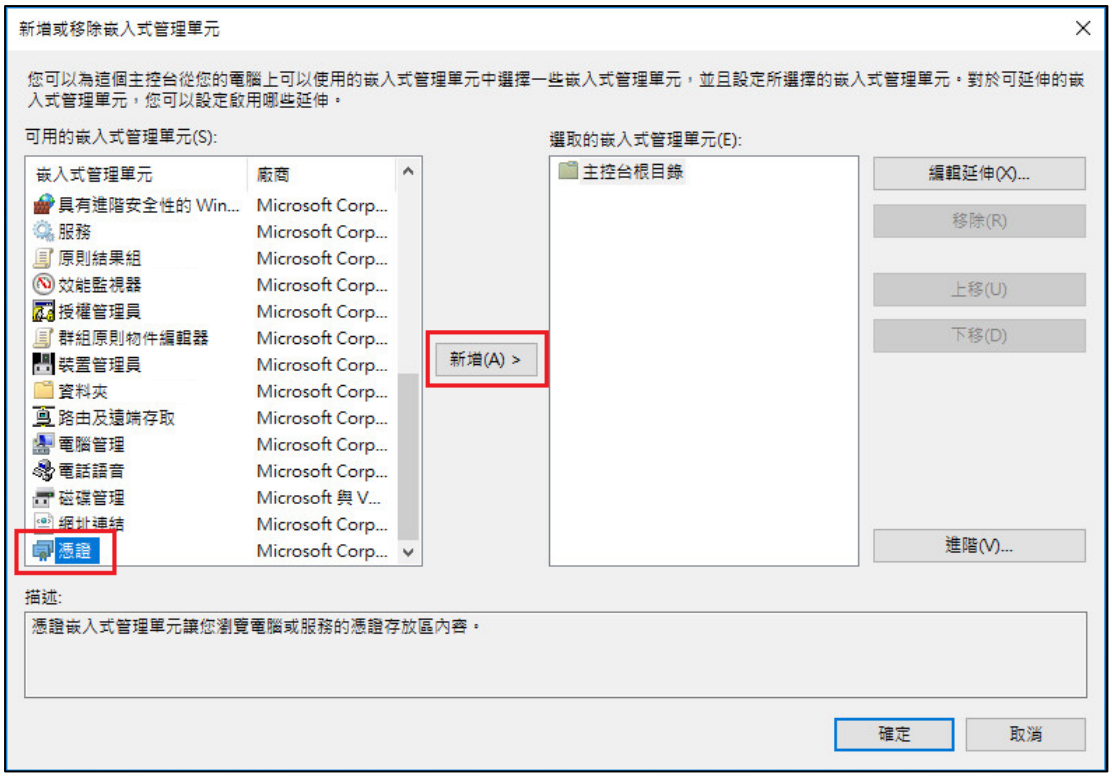
(1) 「開始」→「輸入 mmc」，按下「Enter」。



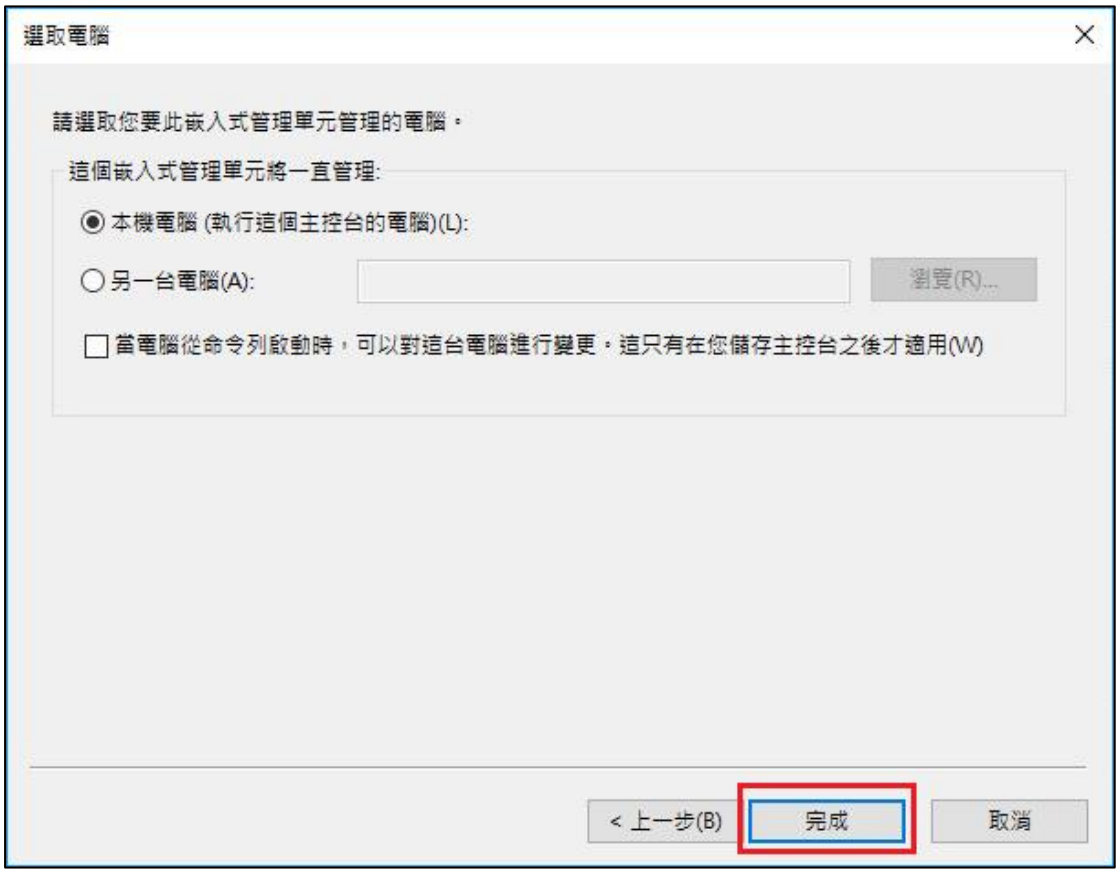
(2) 選擇「檔案」→「新增/移除嵌入式管理單元」。



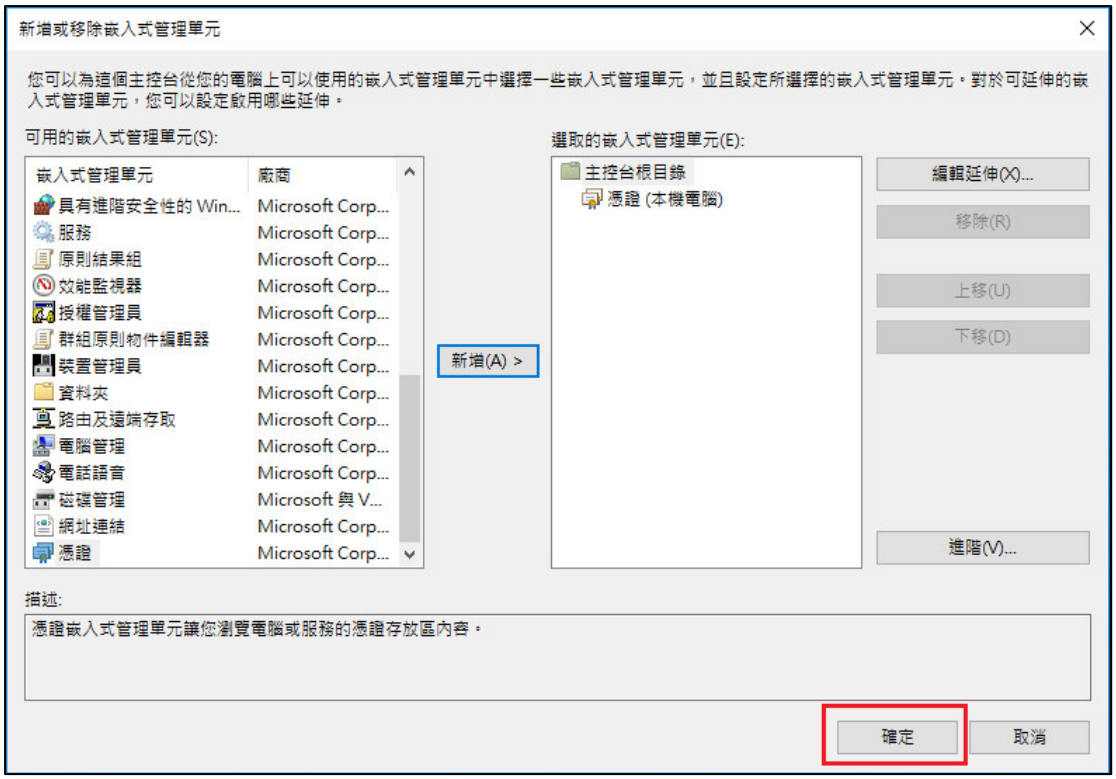
(3) 點選「憑證」→「新增」



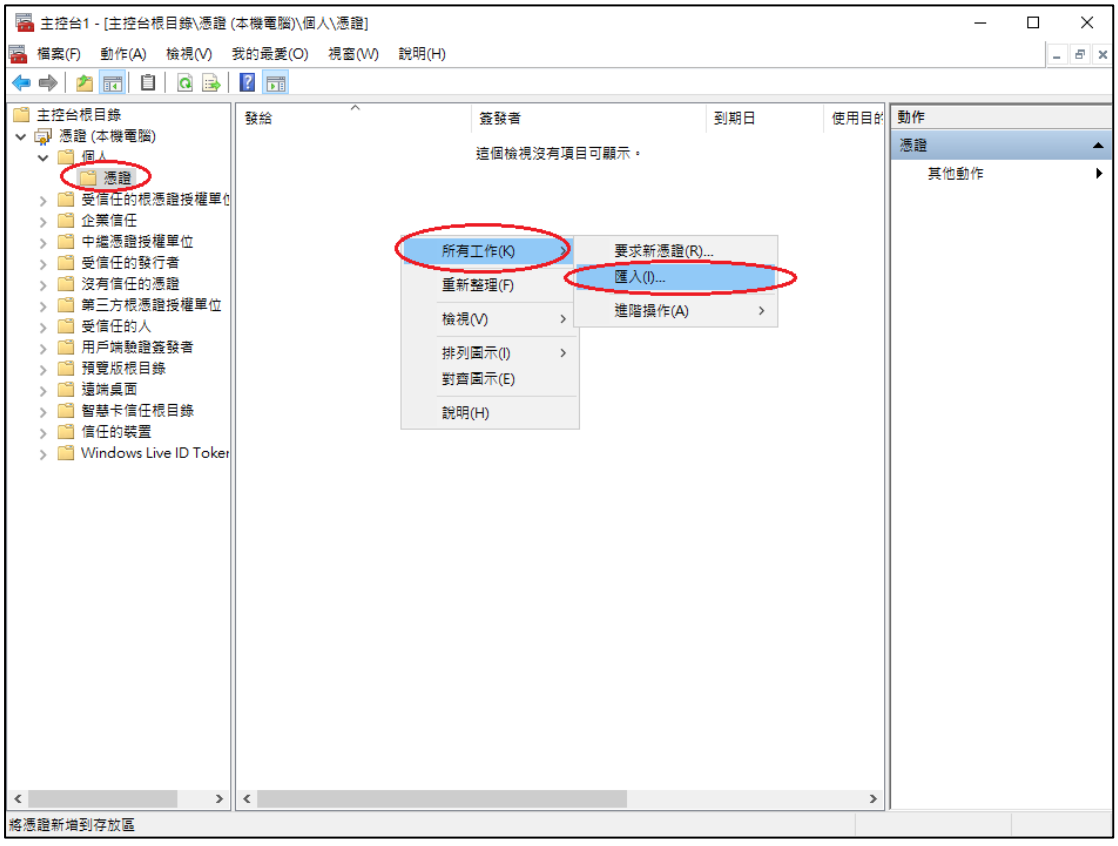
(4) 「電腦帳戶」→「下一步」→「完成」。



(5) 「確定」。

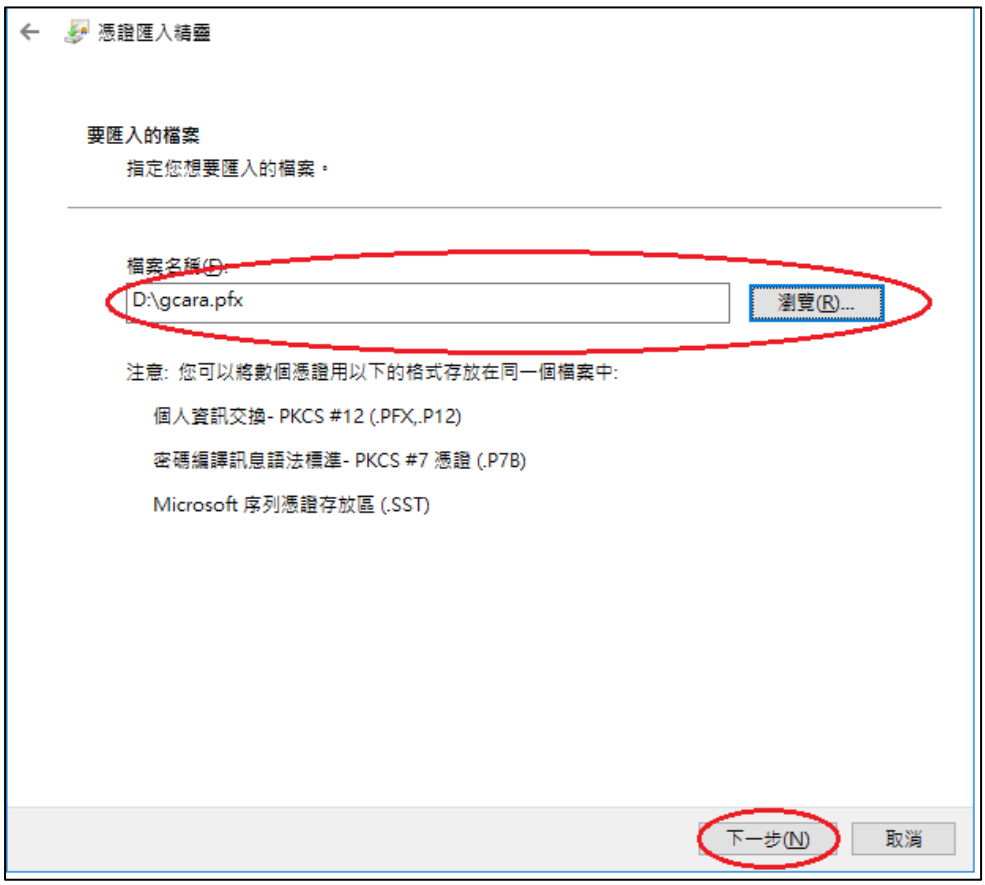


(6) 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

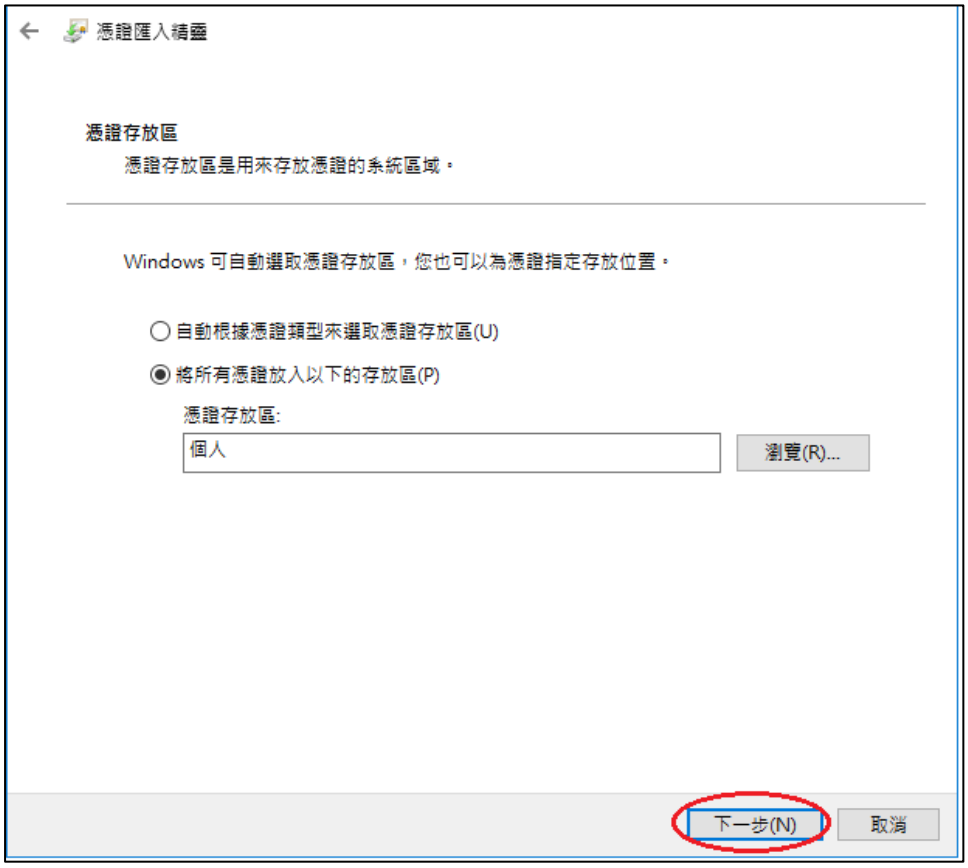


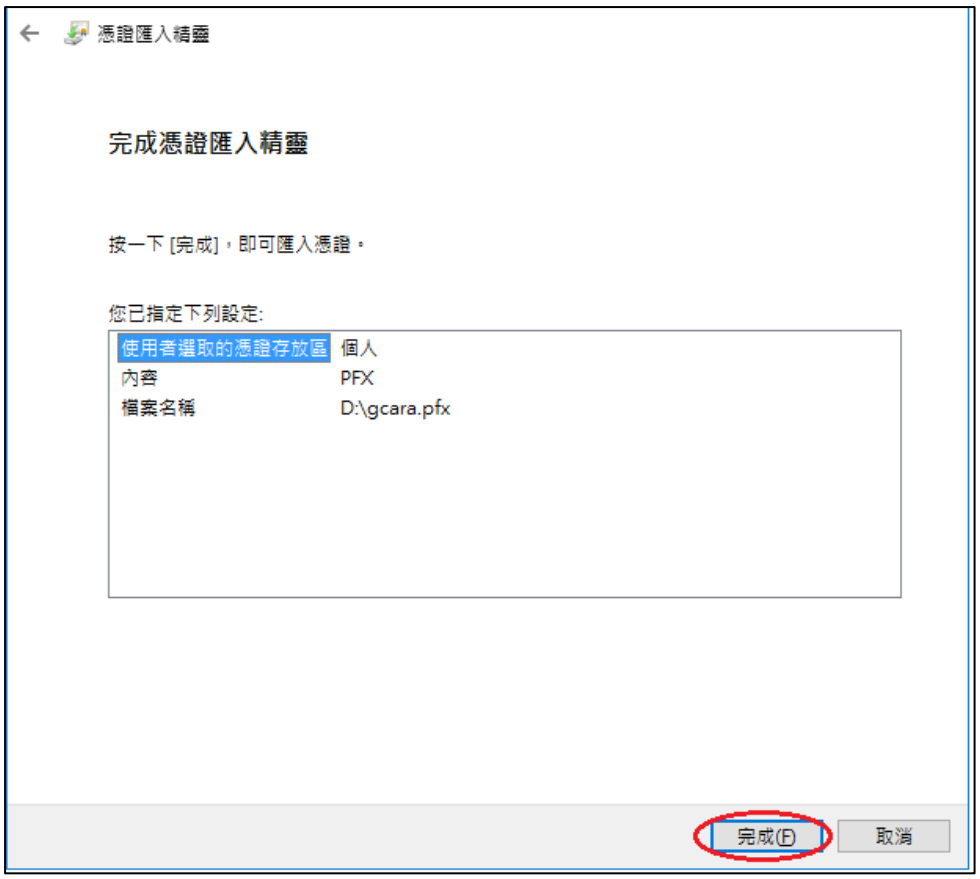
(7) 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

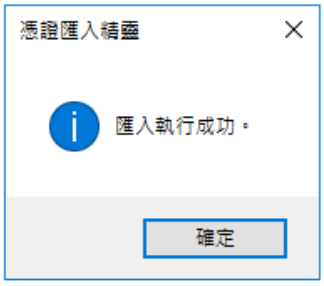

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消


憑證匯入精靈
要匯入的檔案
指定您想要匯入的檔案。
檔案名稱(F):
D:\gcara.pfx
瀏覽(R)...
注意: 您可以將數個憑證用以下的格式存放在同一個檔案中:
個人資訊交換- PKCS #12 (.PFX,.P12)
密碼編譯訊息語法標準- PKCS #7 憑證 (.P7B)
Microsoft 序列憑證存放區 (.SST)
下一步(N)
取消

(8) 輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。

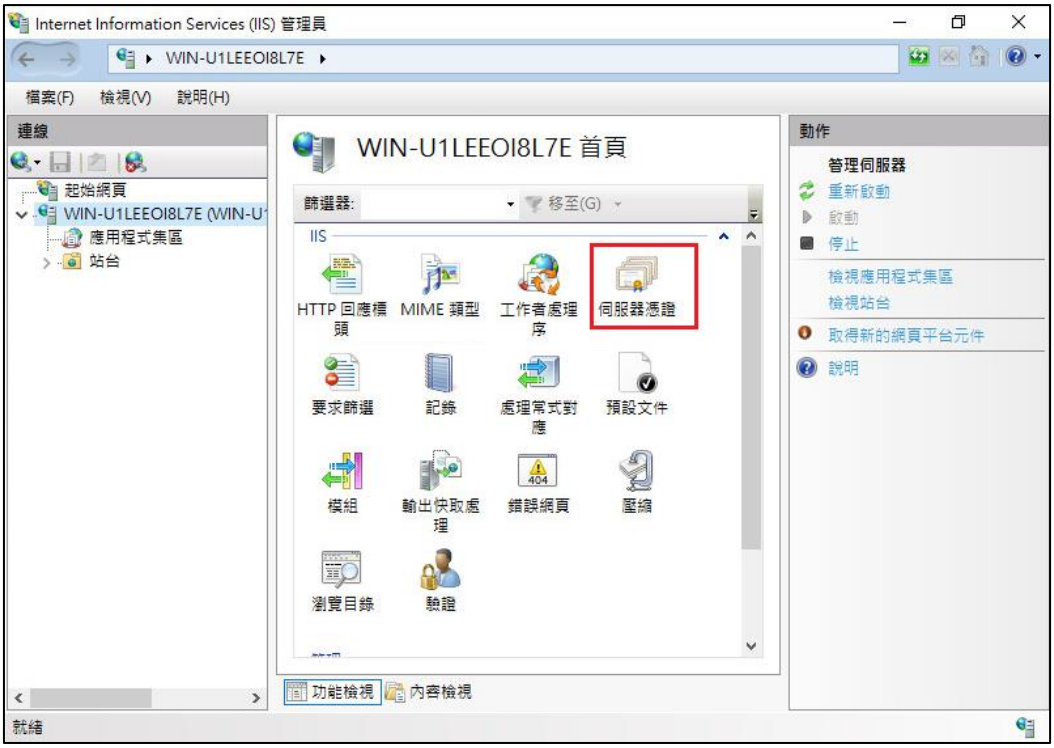




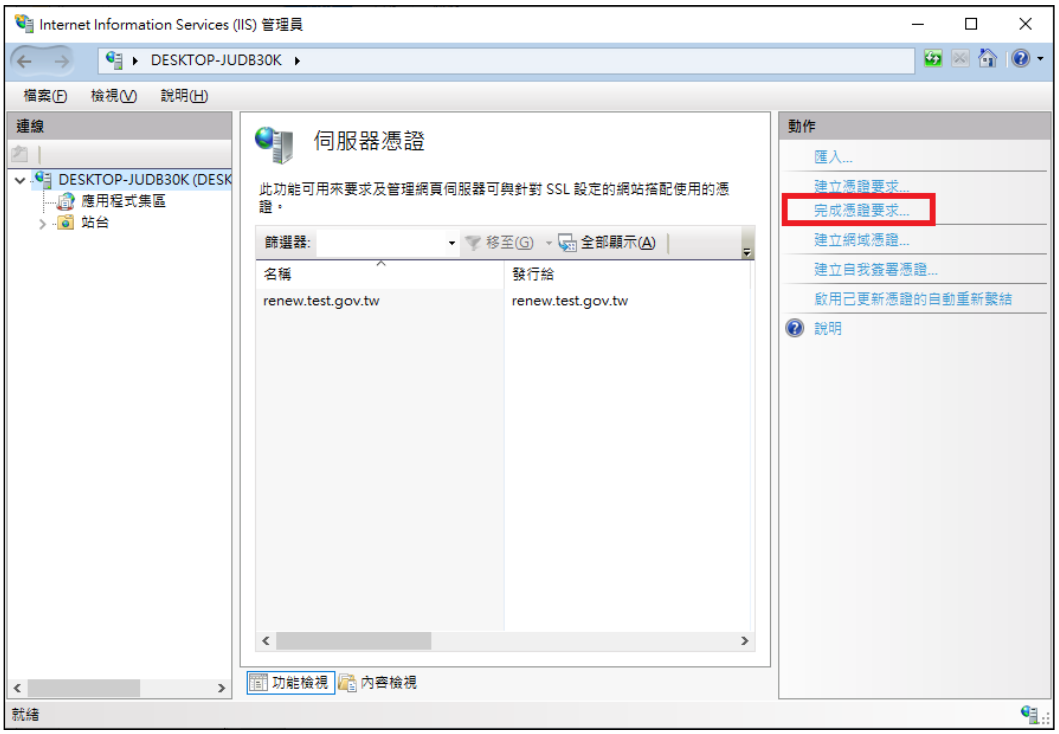


3. 於 IIS 完成註冊要求，匯入新憑證。

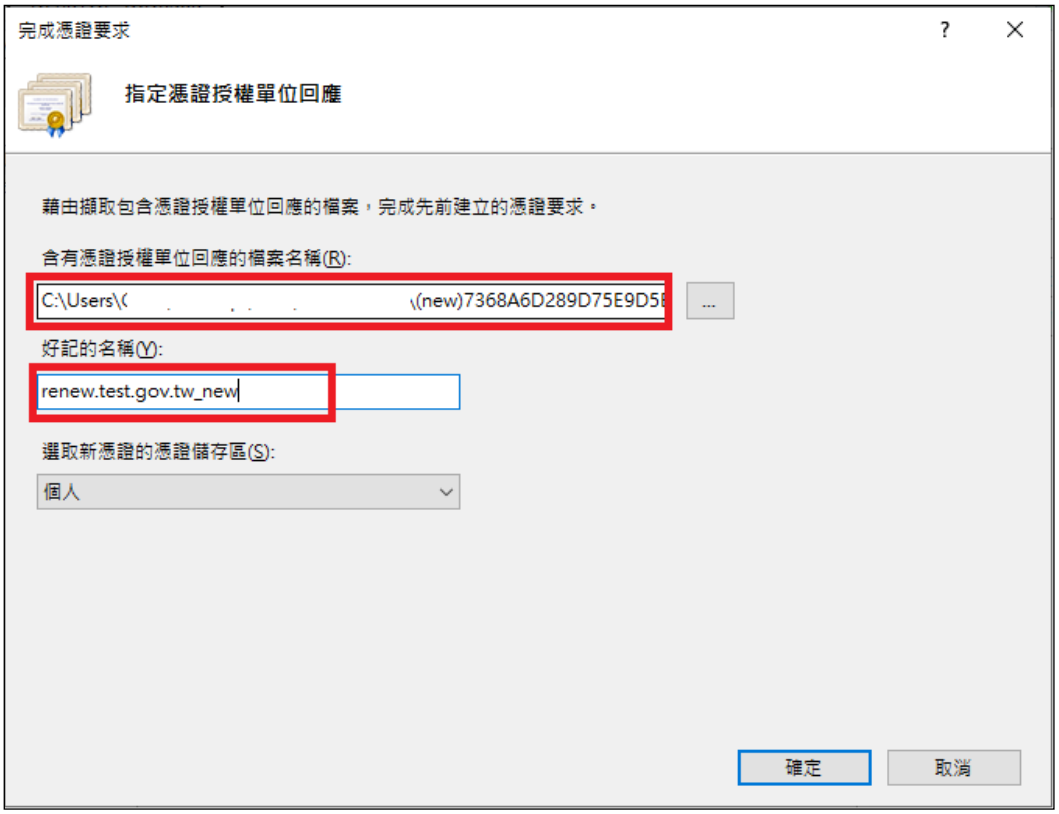
(1) 開啟「Internet Information Services (IIS)管理員」，點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



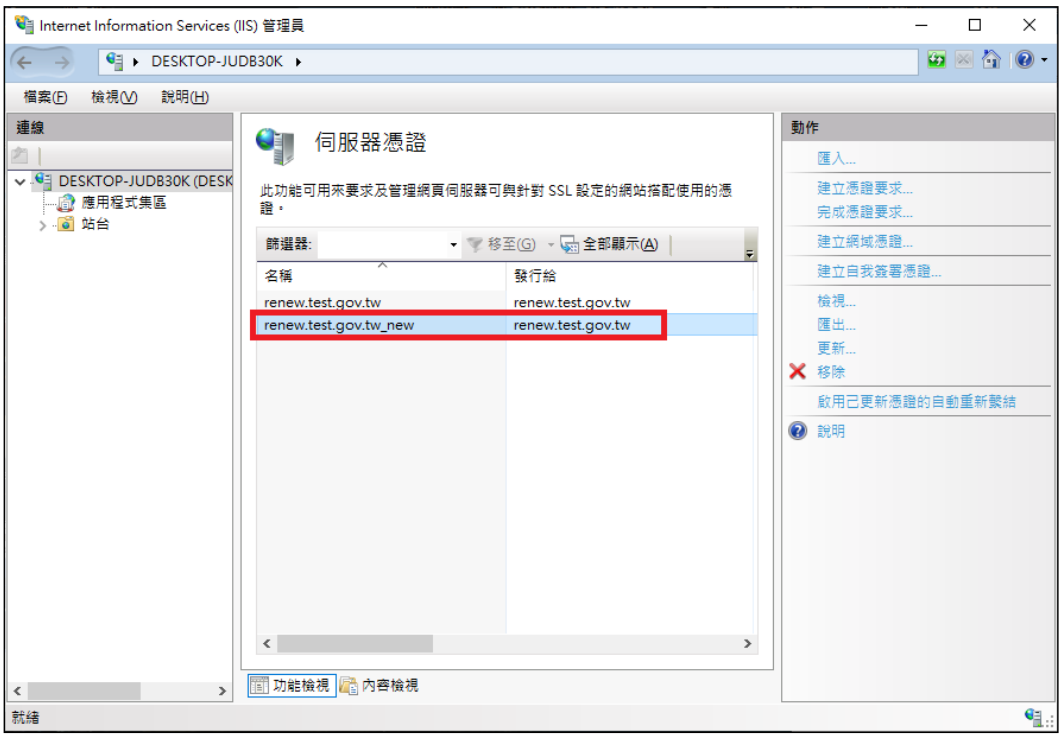
(2) 點選「完成憑證要求」。



(3) 選擇新的 TLS 憑證，並輸入好記的名稱。



(4) 按「確定」，出現完成憑證要求的畫面，多一條新憑證列表。(請重新整理確認憑證沒有消失，將憑證點 2 下開啟確認是否有其對應的私鑰。)

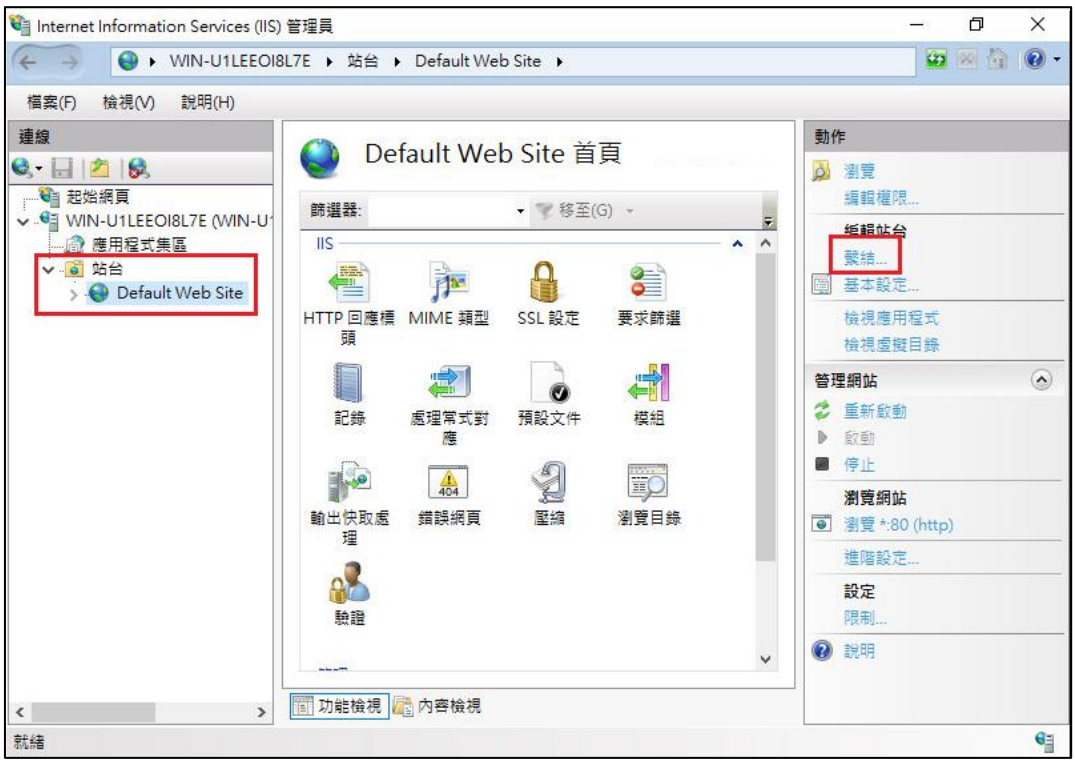


4. 將與私鑰結合的新憑證匯出並匯入至原主機，於 IIS 站台繫結選取新憑證即可。

(1) 匯出新憑證請參考第 1 點操作步驟(p.7 至 p.8)

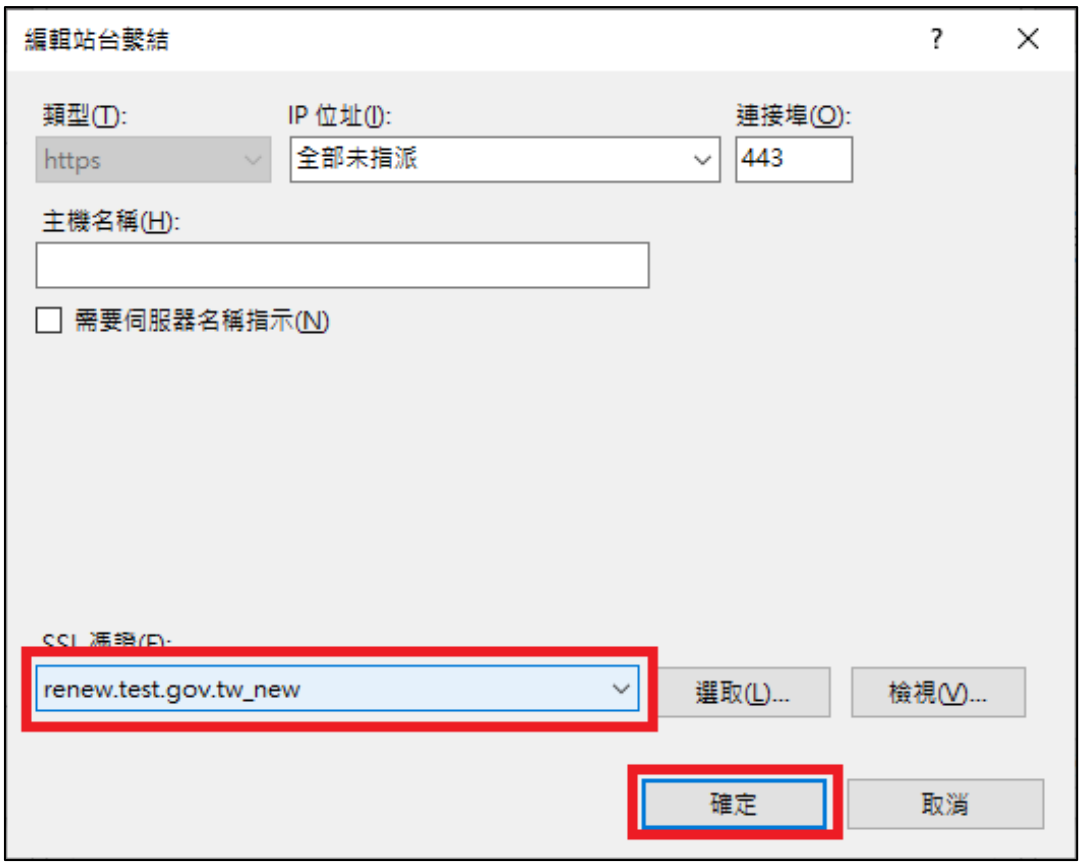
(2) 匯入新憑證請參考第 2 點操作步驟(p.9 至 p.14)

(3) 至原主機開啟「Internet Information Services (IIS)管理員」，點選要安裝的站台，本手冊以(Default Web Site)進行說明，選擇「繫結」。



(4) 選擇已存在的 https 443 連接埠，點選「編輯」。

(5) 重新選擇要安裝在此站台新的 TLS 憑證。

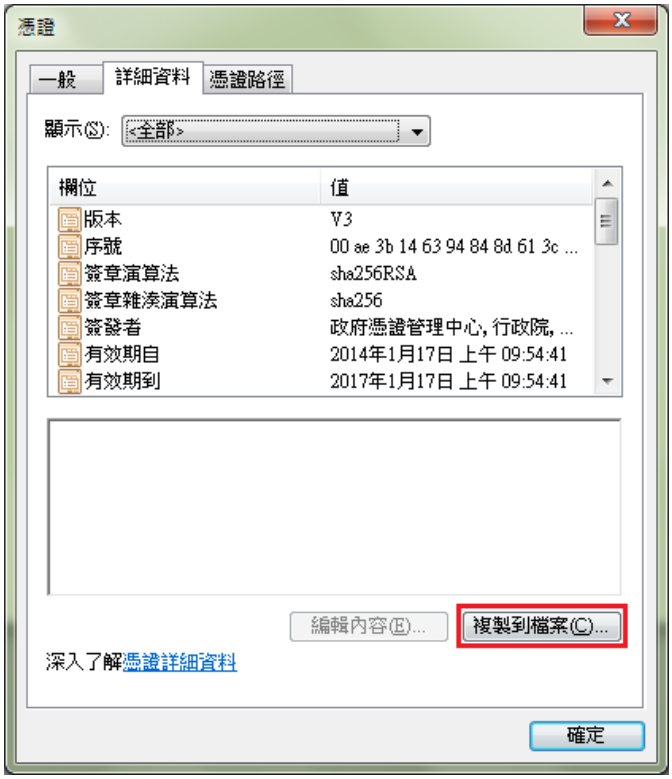

編輯站台繫結
類型(T):
https
IP 位址(I):
全部未指派
連接埠(O):
443
主機名稱(H):
需要伺服器名稱指示(N)
renew.test.gov.tw_new
選取(L)...
檢視(V)...
確定
取消

網站伺服器：Apache

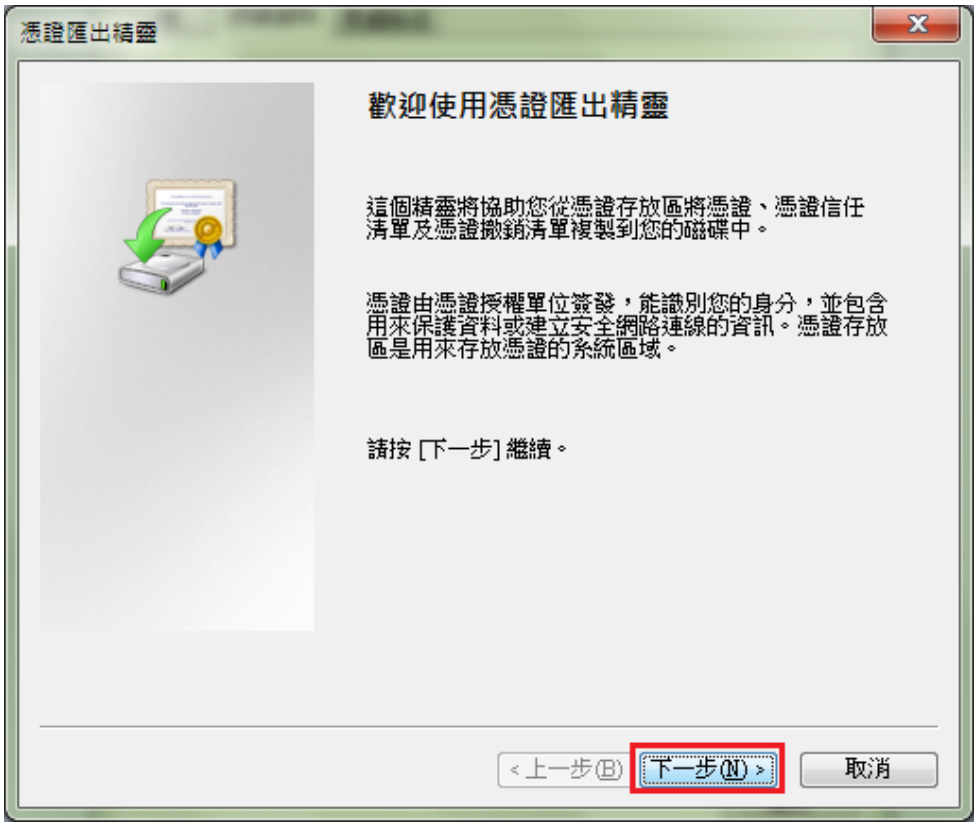
1. 將憑證由 DER 格式轉換為 Base64 格式。

(1) 點選憑證檔案後，選擇詳細資料。

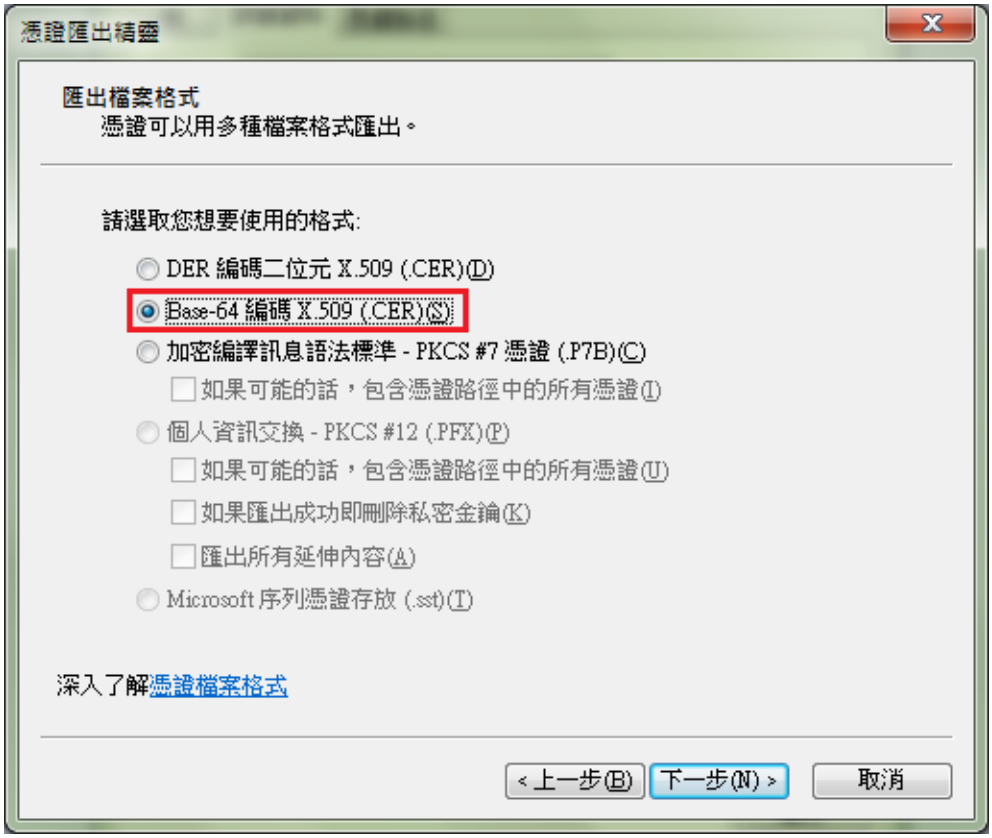
(2) 選擇複製到檔案。



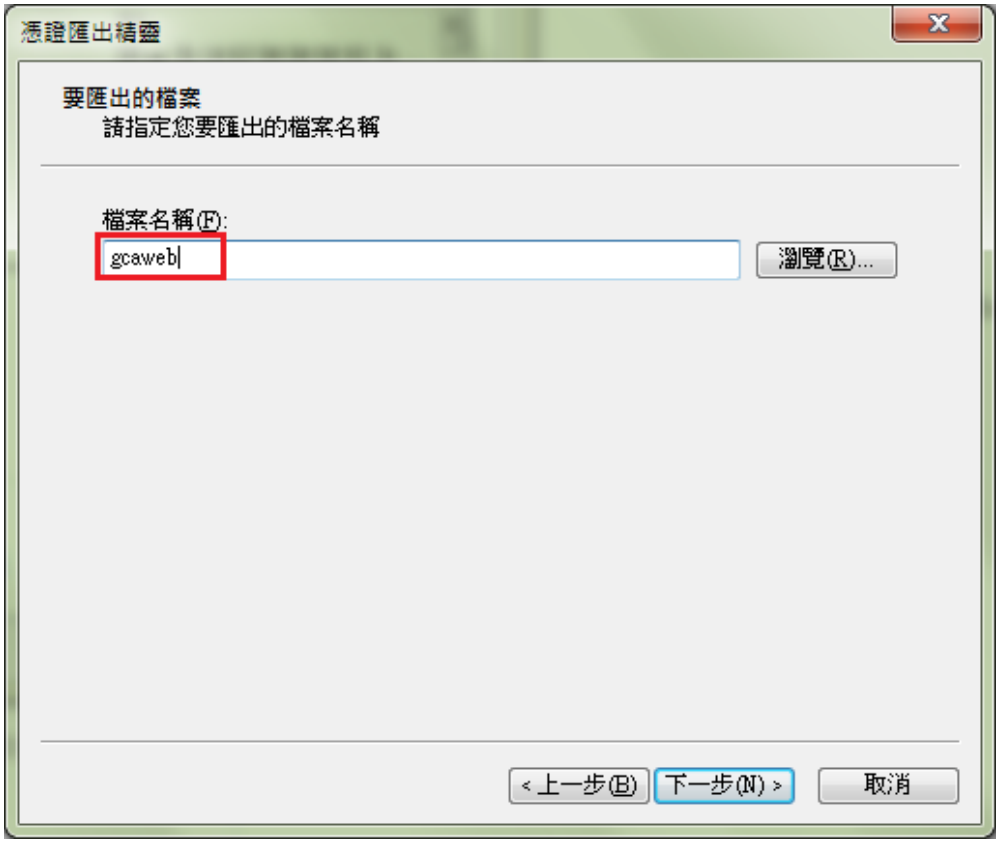
(3) 點選下一步。



(4) 選擇 Base64 編碼。



(5) 輸入檔案名稱。



(6) 完成轉換。

2. 以文字編輯器開啟 Base64 格式憑證，並與原憑證設定檔中的 TLS 憑證更換。

(1) 若 Apache 版本 < **2.4.8**，請參考以下步驟操作

i. 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為<apache 安裝路徑>\conf\extra\ 目錄下。
修改以下參數並存檔 SSLCertificateFile：伺服器憑證(*.crt)檔案路徑。

(2) 若 Apache 版本 >= **2.4.8**，請參考以下步驟操作

i. 利用文字編輯器開啟 httpd-ssl.conf，檔案可能位置為<apache 安裝路徑>\conf\extra\ 目錄下。

ii. 利用文字編輯器開啟原指定的憑證檔(範例為 sever.crt)，SSLCertificateFile 參數指定之位址。

```
SSLCertificateFile "/export/httpd-2.    /certs/gca server.crt"
SSLCertificateKeyFile "/export/httpd-2.    /certs/gca_server.key"
```

iii. 將憑證檔內容最上面的原 TLS 憑證，更換為步驟 1 轉換成 Base64 格式的新 TLS 憑證內容，可參考下圖。

iv. 將修改後的 TLS 憑證檔案存檔，檔案放置路徑跟原本 SSLCertificateFile 參數相同。

3. 重新啟動 Apache Server。

網站伺服器：Tomcat

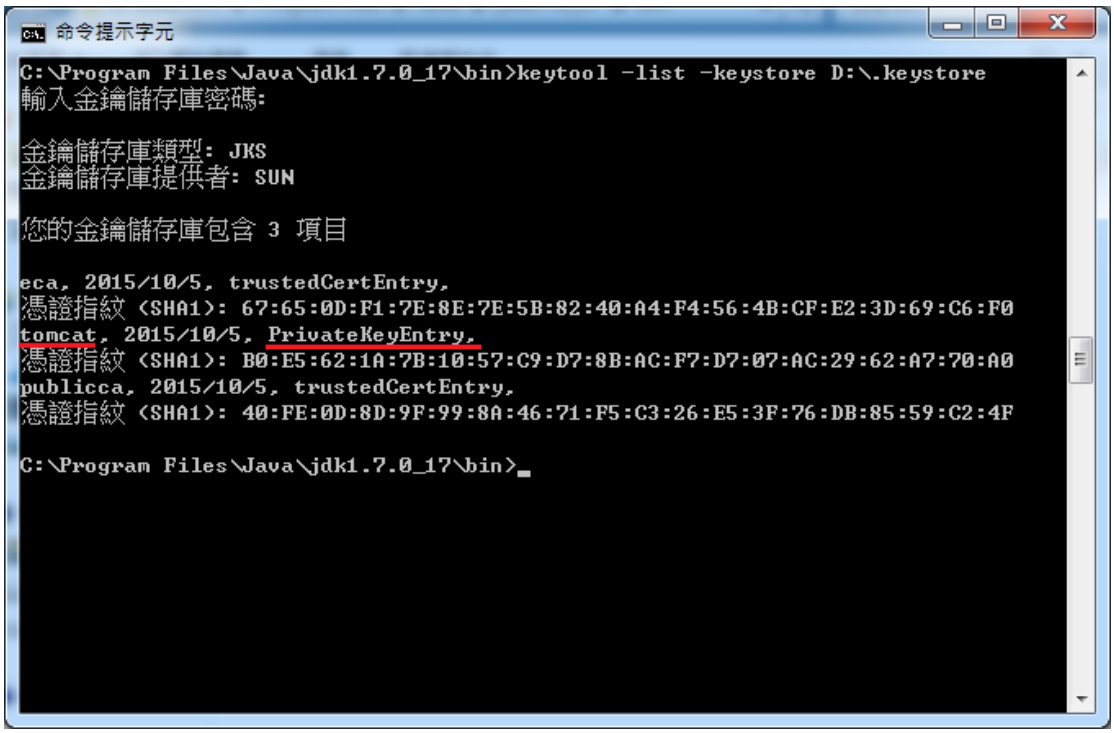
1. 請直接於原憑證安裝的 Keystore 重新匯入新憑證即可。

(1) 確認 PrivateKeyEntry 的 alias name

在 %JAVA_HOME%\bin 目錄下執行

keytool -list -keystore <keystore 檔案所在路徑>

- 待出現 Enter keystore password：請輸入密碼。
- 找到 PrivateKeyEntry 對應的 alias name，範例為 tomcat



(2) 匯入新的 TLS 伺服器應用軟體憑證。

在 %JAVA_HOME%\bin 目錄下執行

keytool -import -alias <PrivateKeyEntry 的 alias name> -file D:\(憑證名稱.cer) -keystore <keystore 檔案所在路徑>

- 待出現 Enter keystore password：請輸入密碼。

◆ 若直接於 Keystore 安裝新憑證有問題，也可參考以下方式安裝新憑證。

1. 先執行以下指令得到 keystore(jks 檔)裏含有私鑰(PrivateKeyEntry)的 alias name

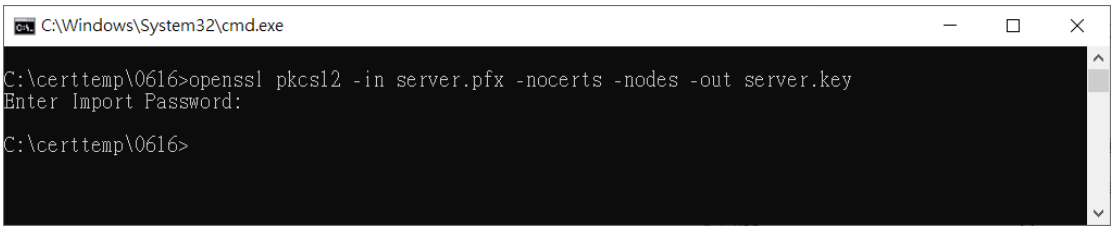
   keytool -list -keystore tomcat.jks

2. 執行以下 keytool 指令，將 JAVA Keystore (JKS) 轉檔為 PFX 檔

   keytool -importkeystore -srckeystore tomcat.jks -destkeystore server.pfx -srcstoretype jks -deststoretype pkcs12 -srcalias tomcat

3. 得到 PFX 檔案(範例為 server.pfx)後，再到有安裝 openssl 的電腦執行下面的指令，這樣就會得到私鑰 server.key

   openssl pkcs12 -in server.pfx -nocerts -nodes -out server.key



4. 重新至以下連結下載憑證串鏈檔，再依後續步驟執行

   https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip

5. 重新至 GCP 網站下載已簽發憑證，並命名為 install.crt，並依以下指令將 DER 格式憑證轉換為 B64 格式憑證，此處刻意將另存的 Base64 格式憑證命名為 install_B64.crt

   openssl x509 -inform der -in install.crt -out install_B64.crt

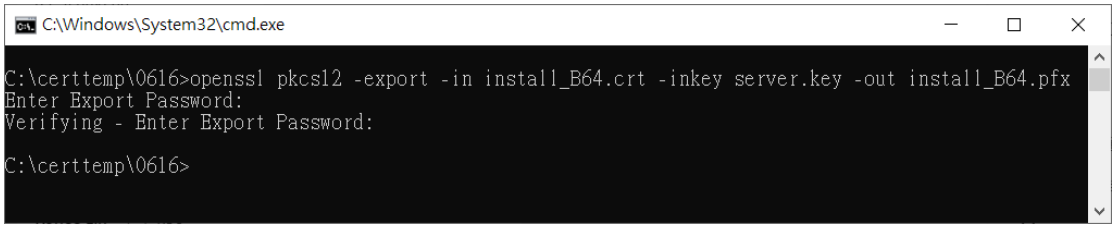
6. 以文字編輯器開啟 install_B64.crt，並將憑證串鏈檔 GTLSCA_All.zip 解開之所有憑證依下列順序以文字編輯器開啟，並全選貼至 install_B64.crt 後存檔，檔案大小約 11kb，此時 install_B64.crt 即具備所有中繼憑證。

憑證順序由上而下為 install_B64.crt -> GTLSCA.crt -> eCA1_to_eCA2-New.crt -> ROOTeCA_64.crt

*linux: cat install_B64.crt GTLSCA.crt eCA1_to_eCA2-New.crt ROOTeCA_64.crt > server.crt，再將 server.crt 改名為 install_B64.crt 以進行後續步驟

7. 將憑證及私鑰依以下步驟再次轉換為 pfx 格式

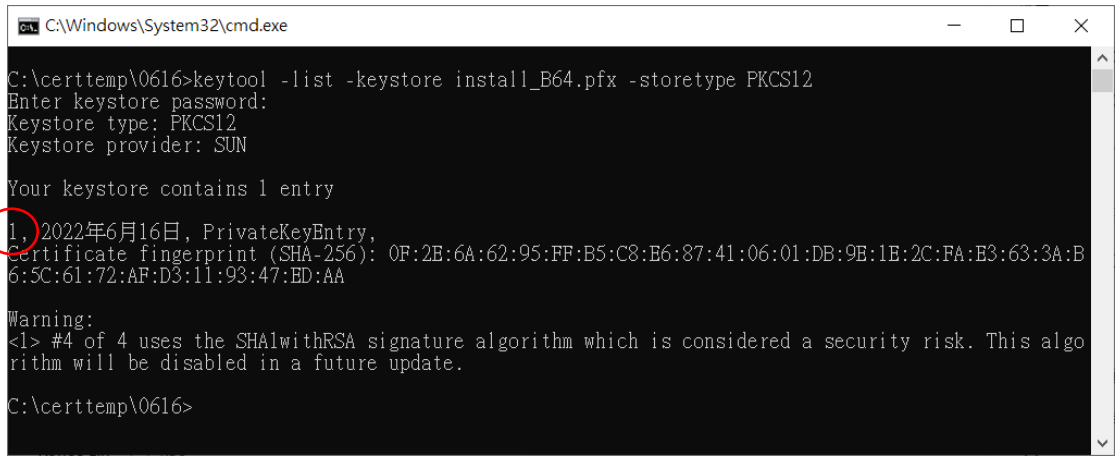
openssl pkcs12 -export -in install_B64.crt -inkey server.key -out install_B64.pfx



8. 將 pfx 轉換為 jks 格式

(1) 先以底下指令得到 pfx 檔私鑰(PrivateKeyEntry)的 alias name(下圖紅框處)

keytool -list -keystore install_B64.pfx -storetype PKCS12



(2) 依前述得到的 alias name 填入下列指令，以將 pfx 轉檔為 install.jks(alias name 為 tomcat，可自行替換)

keytool -importkeystore -srckeystore install_B64.pfx -destkeystore install.jks -srcstoretype pkcs12 -deststoretype jks -srcalias 1 -destalias tomcat