

政府伺服器數位憑證管理中心(GTLSCA)

Windows IIS 8.0 SSL 憑證請求檔製作與憑證安裝手冊

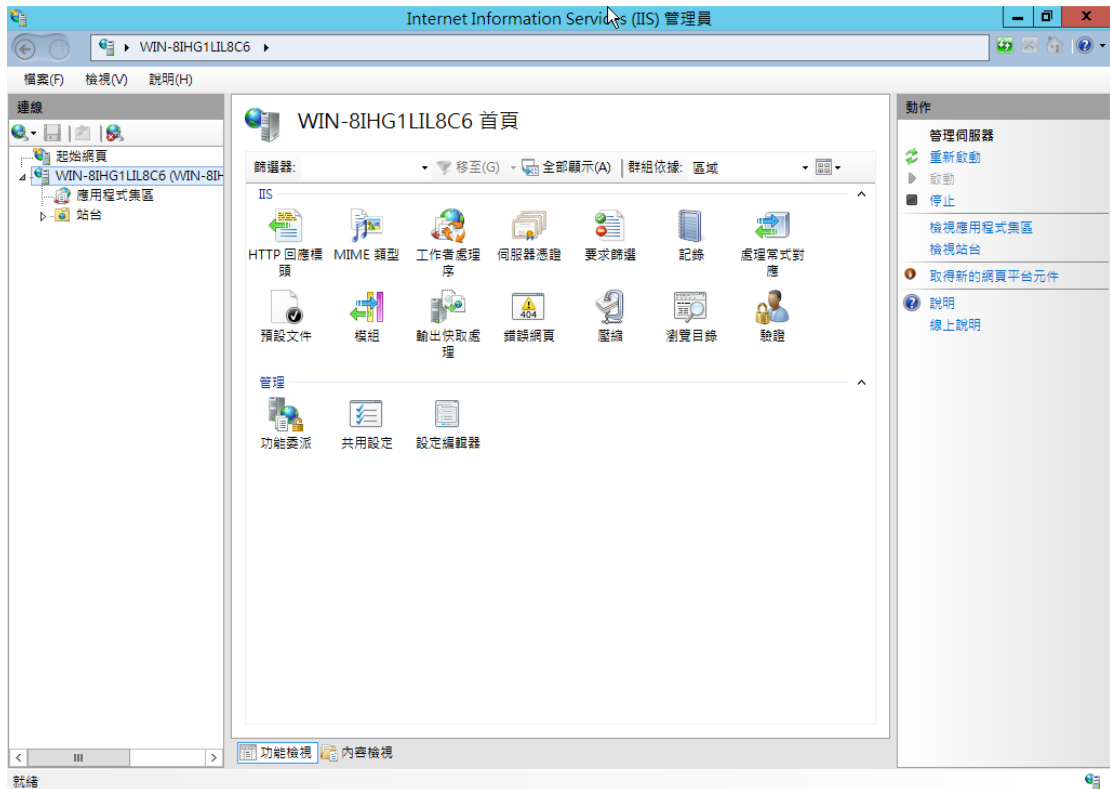
聲明：本手冊之智慧財產權為中華電信股份有限公司（以下簡稱本公司）所有，本公司保留所有權利。本手冊所敘述的程序係將本公司安裝相關軟體的經驗分享供申請 SSL 伺服器軟體憑證用戶參考，若因參考本手冊所敘述的程序而引起的任何損害，本公司不負任何損害賠償責任。

目錄

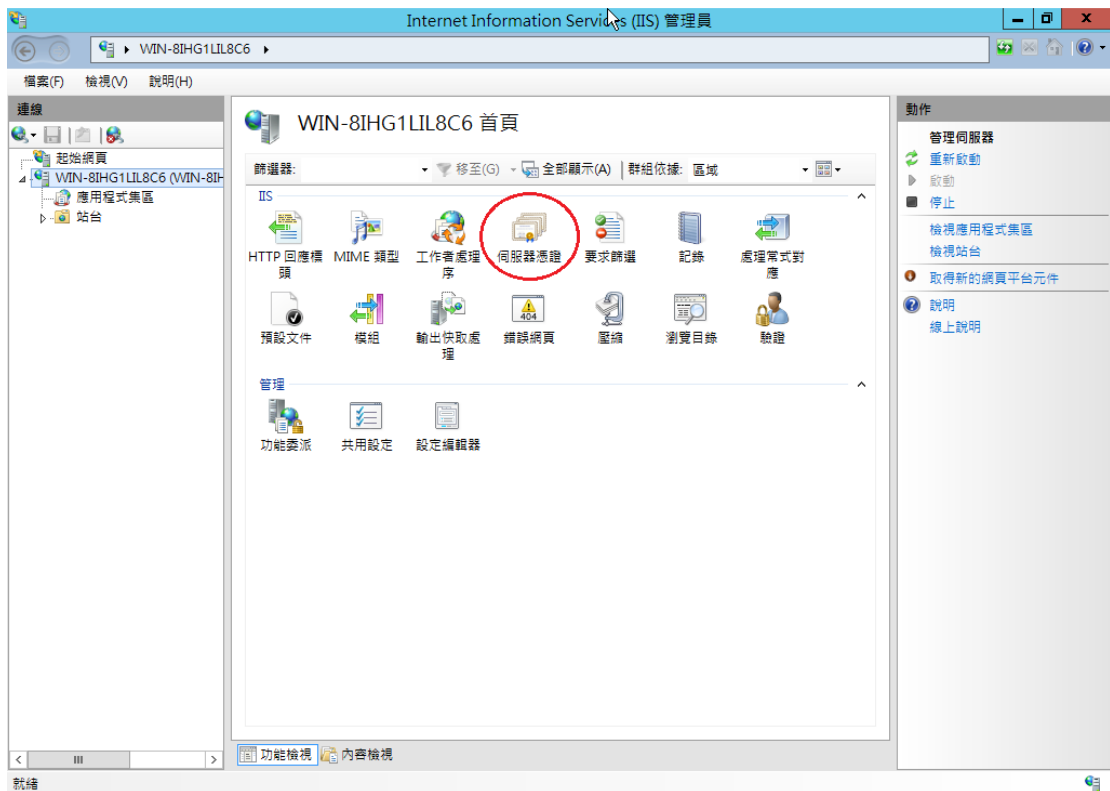
Windows IIS 8.0 SSL 憑證請求檔製作手冊.....	2
Windows IIS 8.0 SSL 憑證安裝操作手冊.....	6
附件一：停用 SSLv2、SSLv3.....	19

Windows IIS 8.0 SSL 憑證請求檔製作手冊

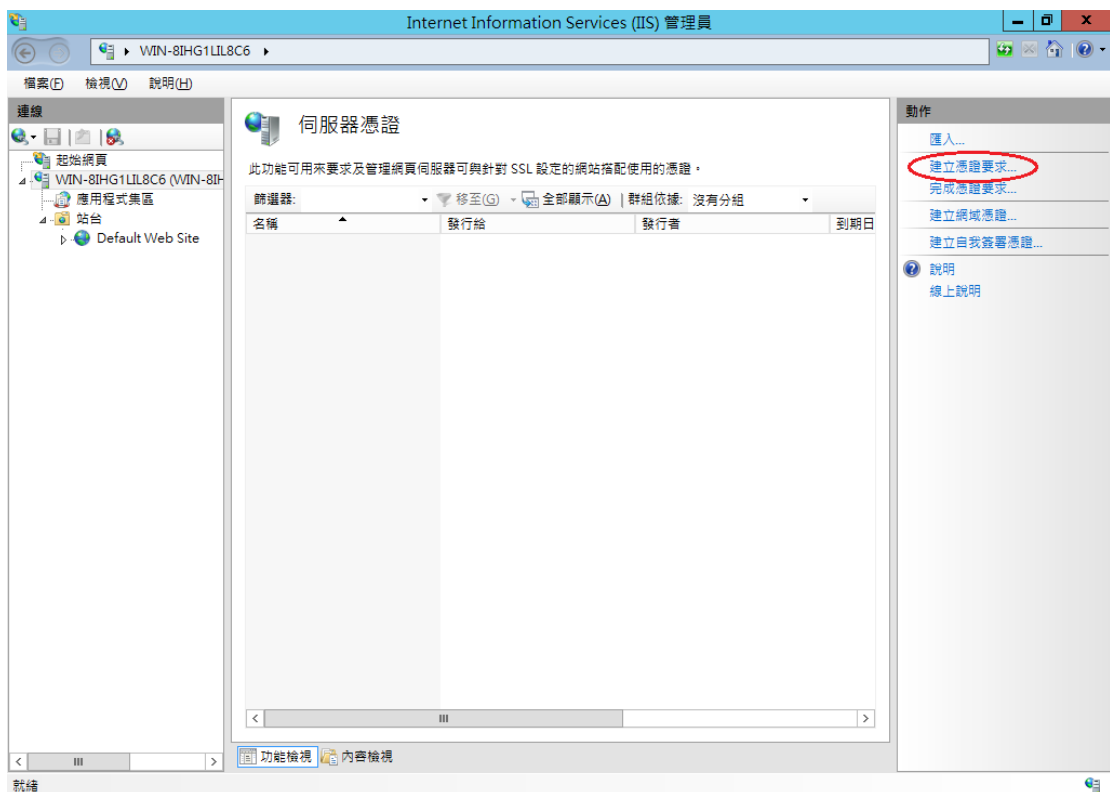
一、 開啟「Internet Information Services (IIS) 管理員」



二、 點選主機連線預設名稱(預備申請與安裝 SSL 憑證的網站)，再點選畫面右邊「伺服器憑證」兩下。



三、 點選「建立憑證要求」



四、 輸入以下所有欄位資料，輸入完成後請點選「下一步」，多網域憑證申請填一個代表網站名稱即可，實際憑證核發資料是以申請書填寫為主。

要求憑證

分辨名稱屬性

指定憑證的必要資訊。省份及縣市/位置必須指定成正式名稱，而且不能包含縮寫。

一般名稱(M):	www.test.com.tw
組織(O):	中華電信股份有限公司數據分公司
組織單位(U):	政府網路處
縣市/位置(L):	台北
省份(S):	none
國家(地區)(R):	TW

上一步(P) 下一步(N) 完成(F) 取消

五、 選擇密碼編譯服務提供者『Microsoft RSA SChannel Cryptographic Provider』，金鑰長度選擇『2048』位元。

要求憑證

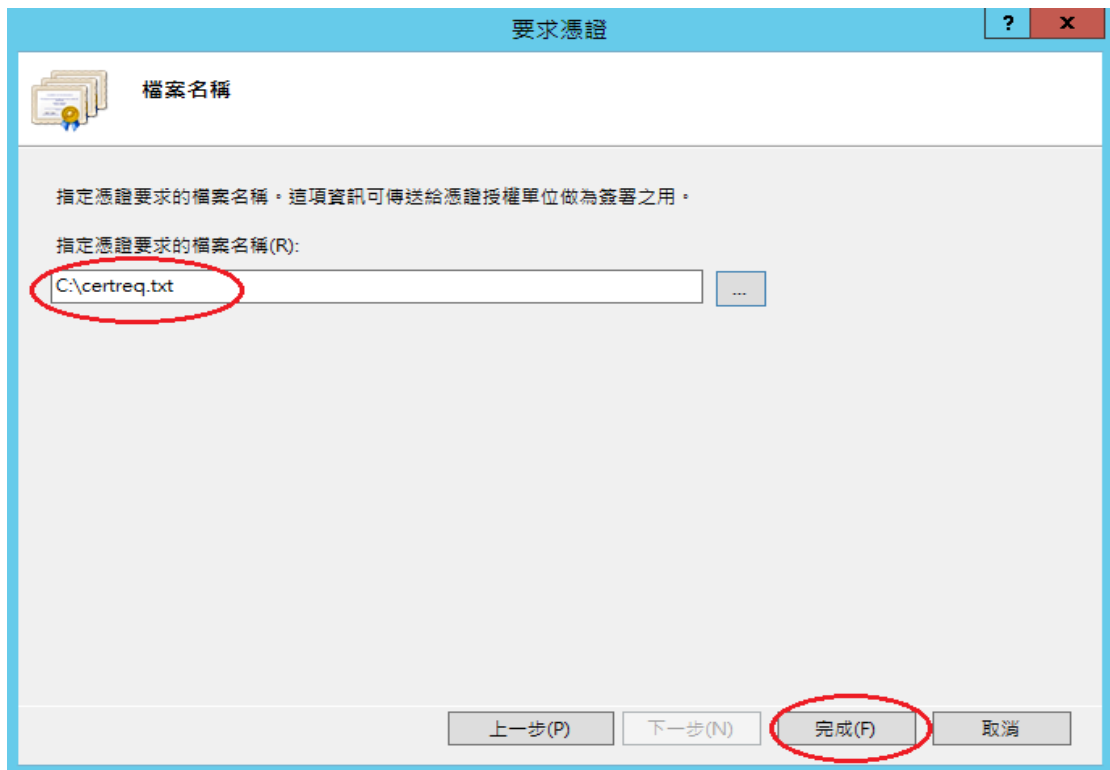
密碼編譯服務提供者內容

選取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。位元長度越大，安全性就越高。不過，位元長度較大可能會降低效能。

密碼編譯服務提供者(S):	Microsoft RSA SChannel Cryptographic Provider
位元長度(B):	2048

上一步(P) 下一步(N) 完成(F) 取消

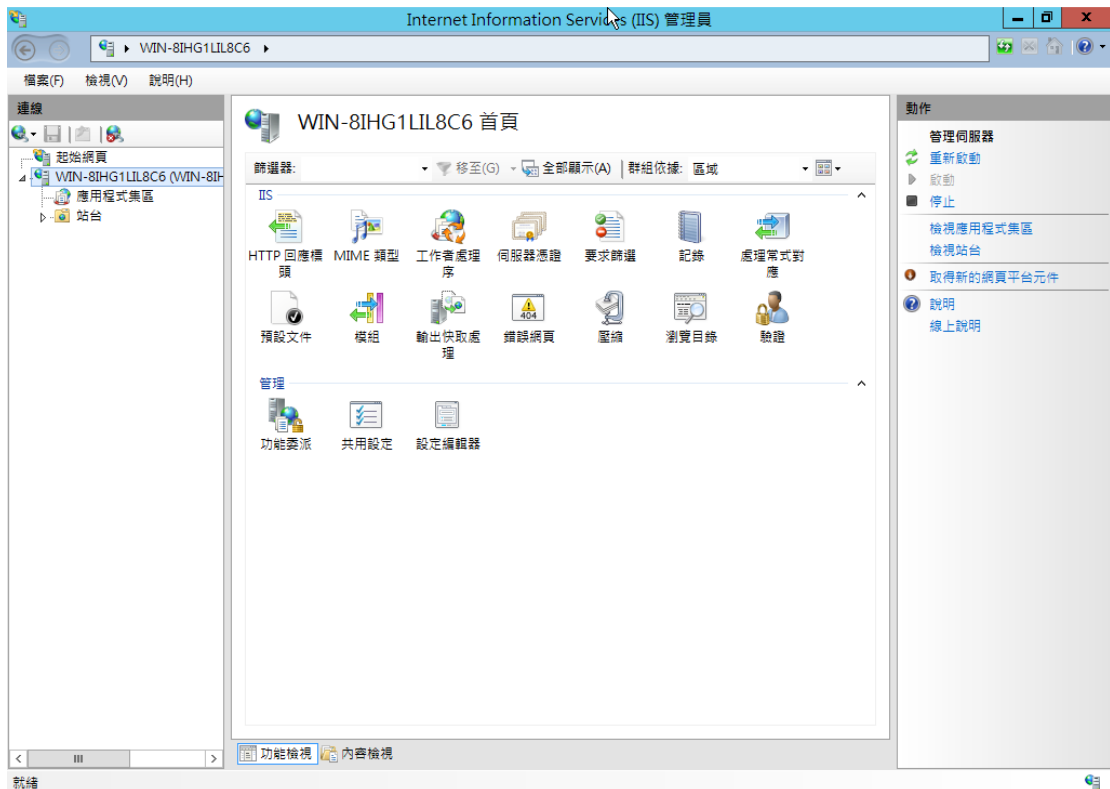
六、 指定儲存憑證請求檔的檔案名稱與存放位置，確認後請點選「完成」。



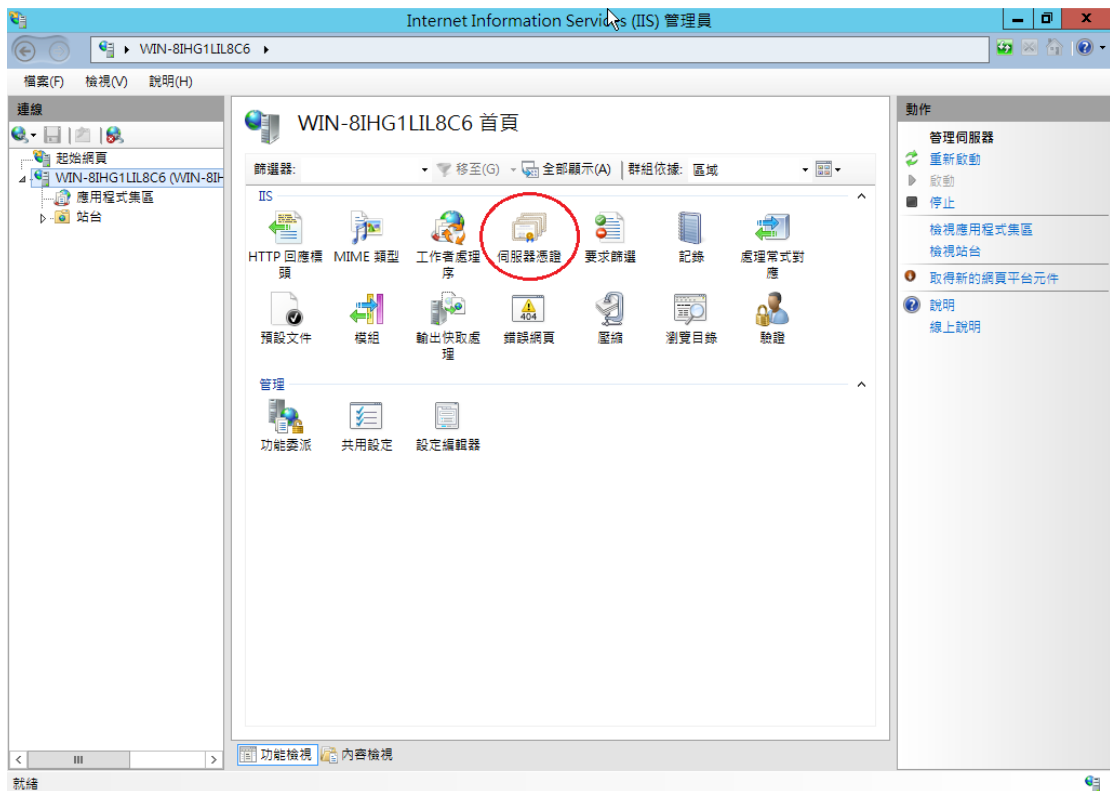
- 七、 此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至憑證管理中心 (<https://gca.nat.gov.tw>) 申請 SSL 憑證。

Windows IIS 8.0 SSL 憑證安裝操作手冊

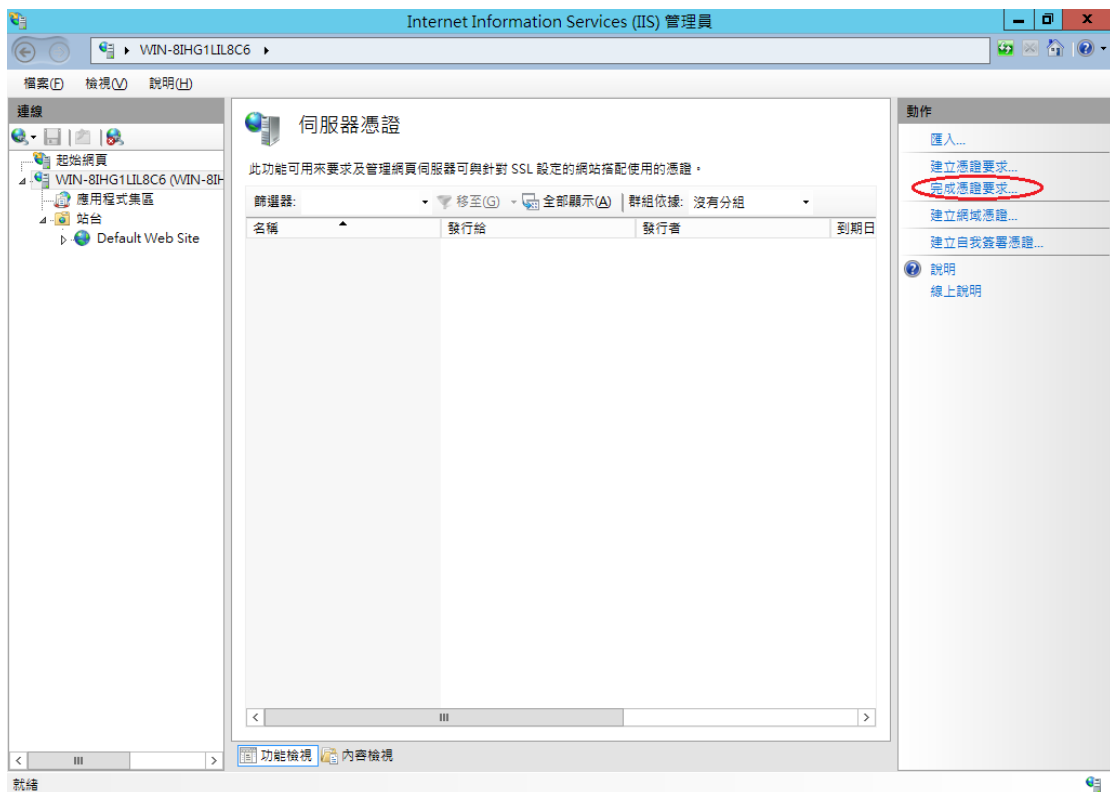
一、開啟「Internet Information Services (IIS) 管理員」。



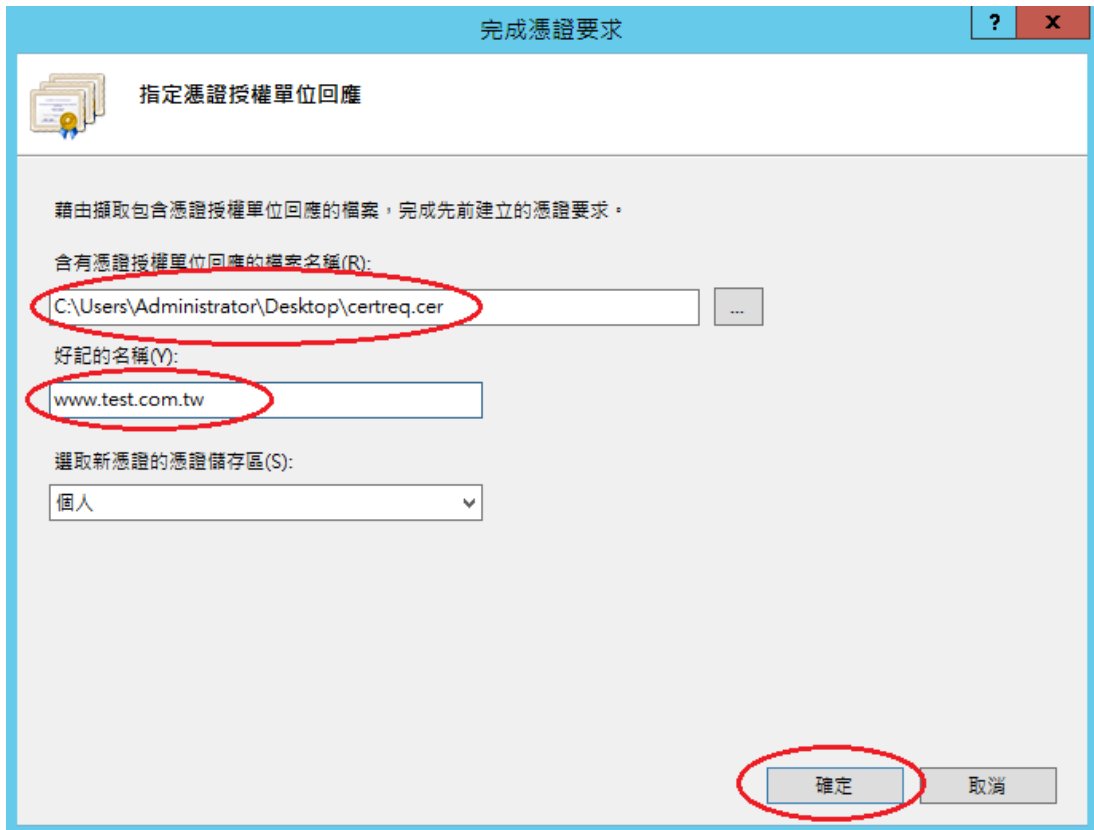
二、點選主機連線預設名稱，再點選畫面右邊「伺服器憑證」。



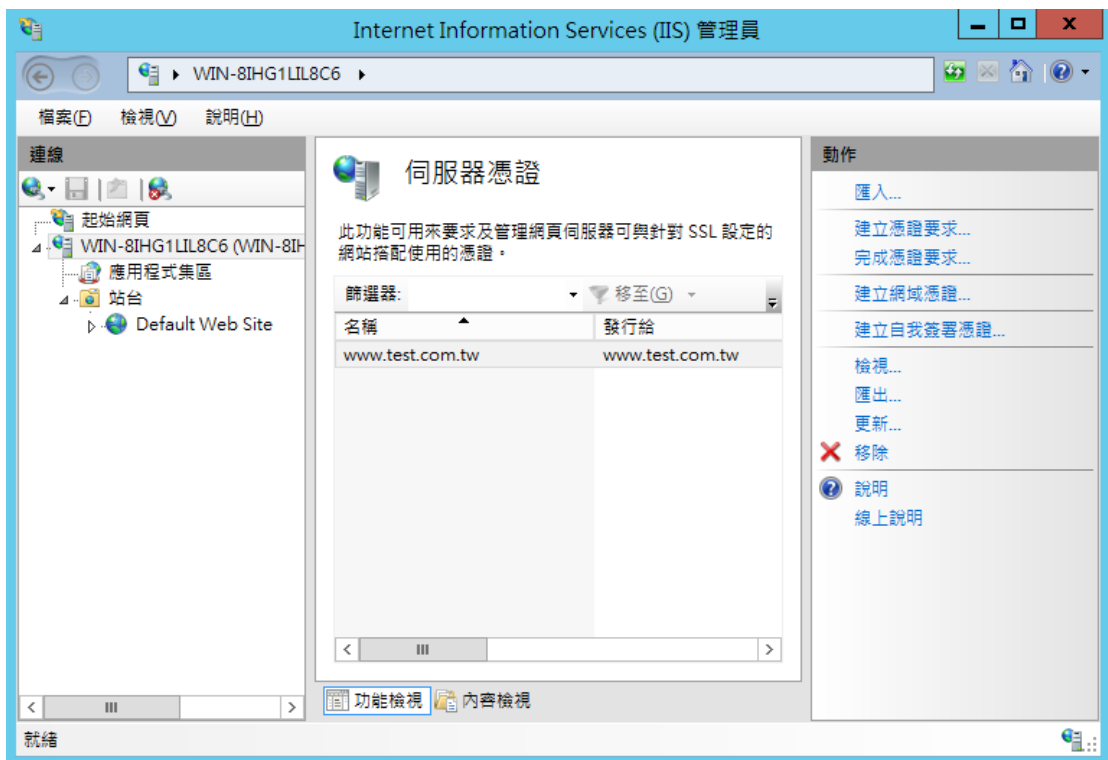
三、點選「完成憑證要求」。



四、如下圖，選擇至憑證管理中心申請之 SSL 憑證，並輸入好記的名稱(一般填寫 Domain Name)。



五、步驟 4 按「確定」，出現完成憑證要求的畫面。



六、至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案，下載網址為

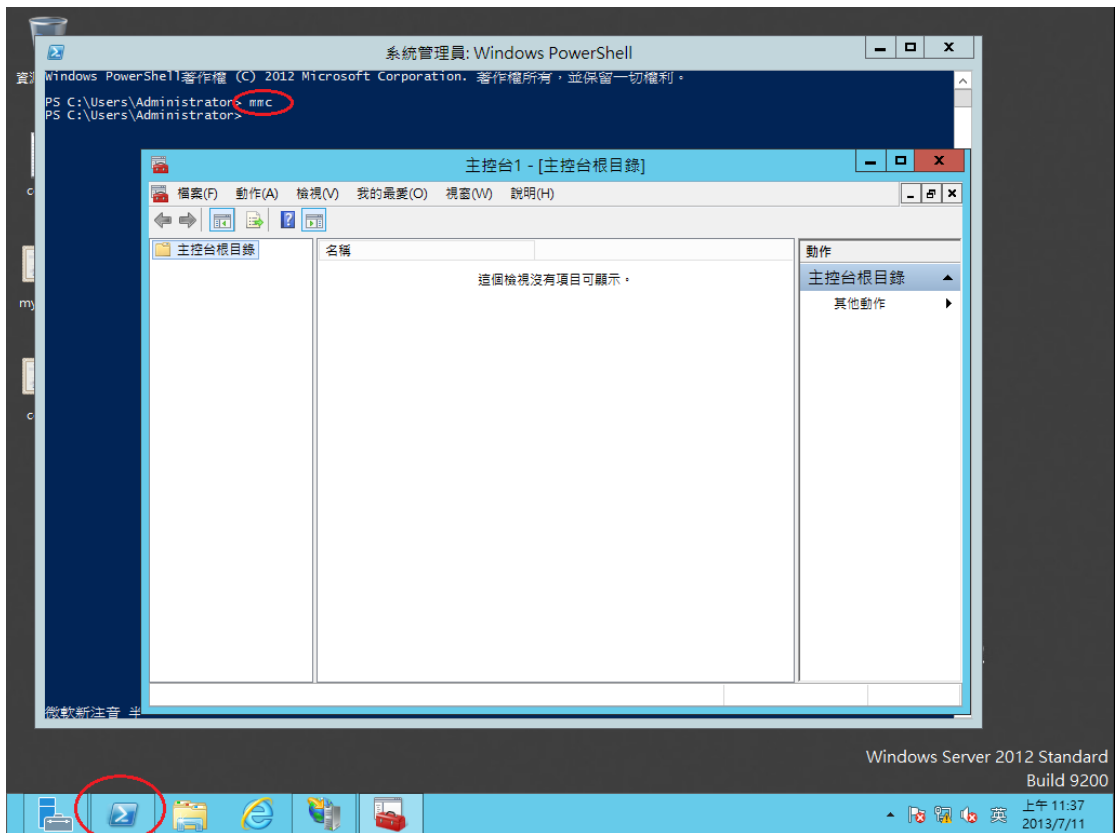
https://gtlscn.nat.gov.tw/download/GTLSCA_All.zip

七、將 GTLSCA_All.zip 解壓縮，可以得到 ROOTeCA_64.crt、

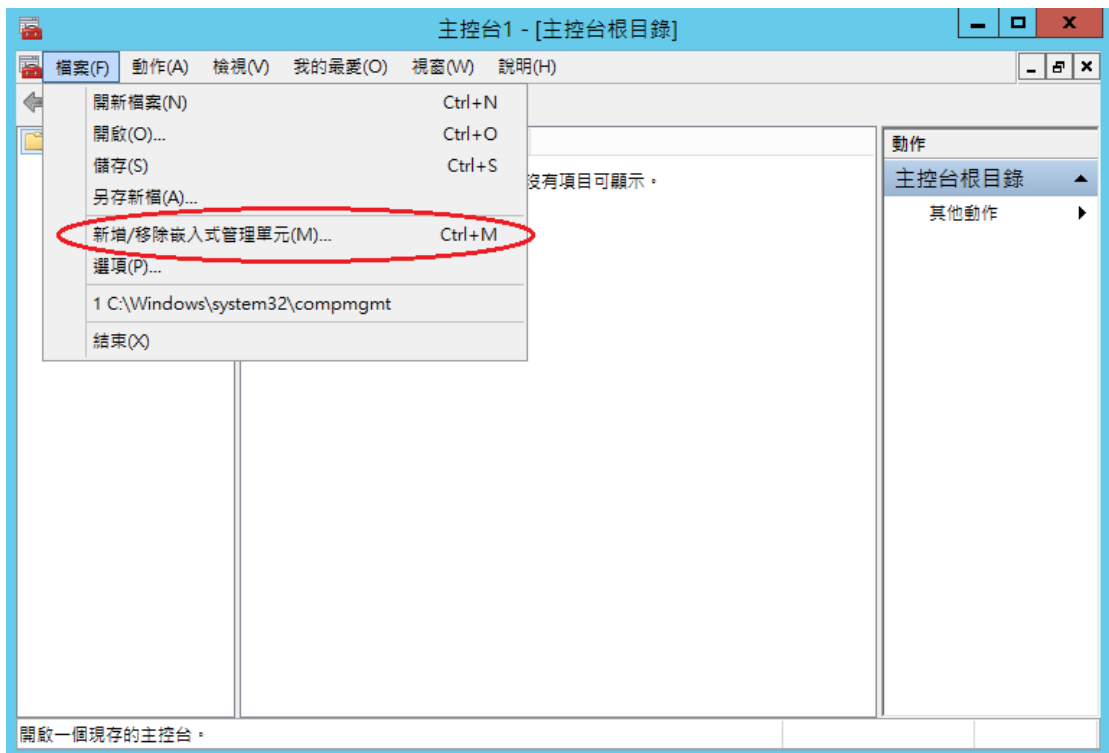
eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案。

八、接著要安裝 eCA 自發憑證及 GTLSCA 憑證。

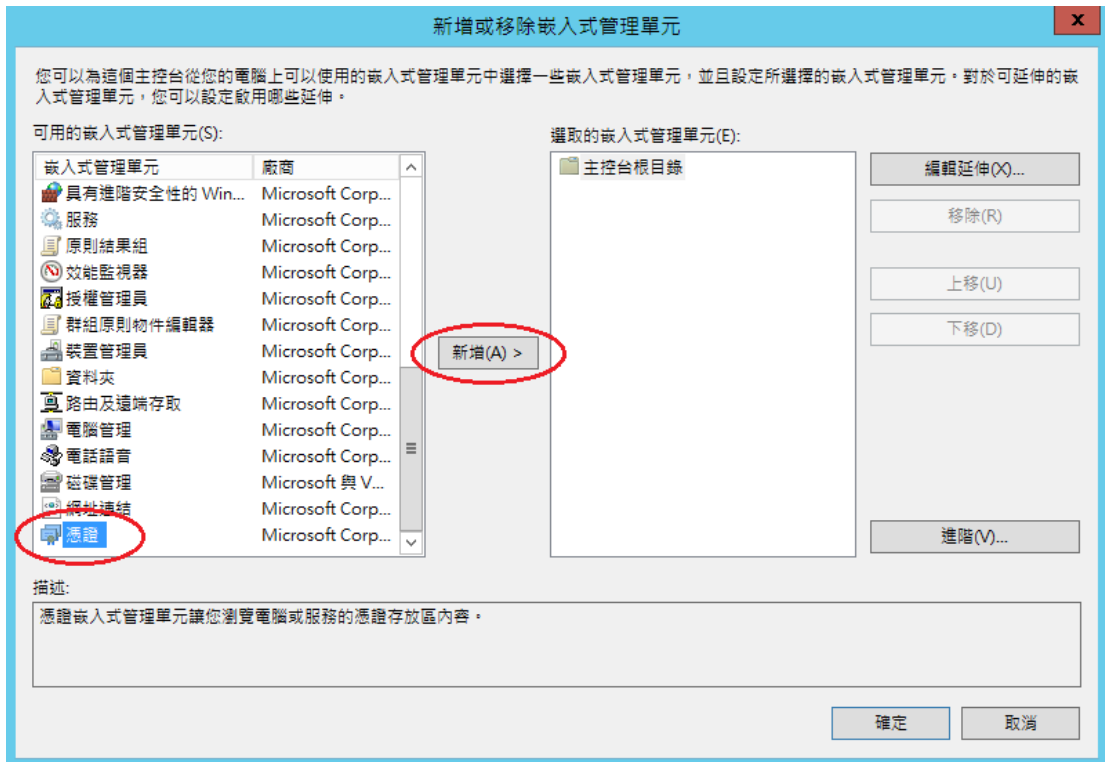
請先點選左下角的「Windows PowerShell」→輸入「mmc」→按下「Enter」。



九、選擇「新增/移除嵌入式管理單元」。



十、接著點選「憑證」→「新增」。

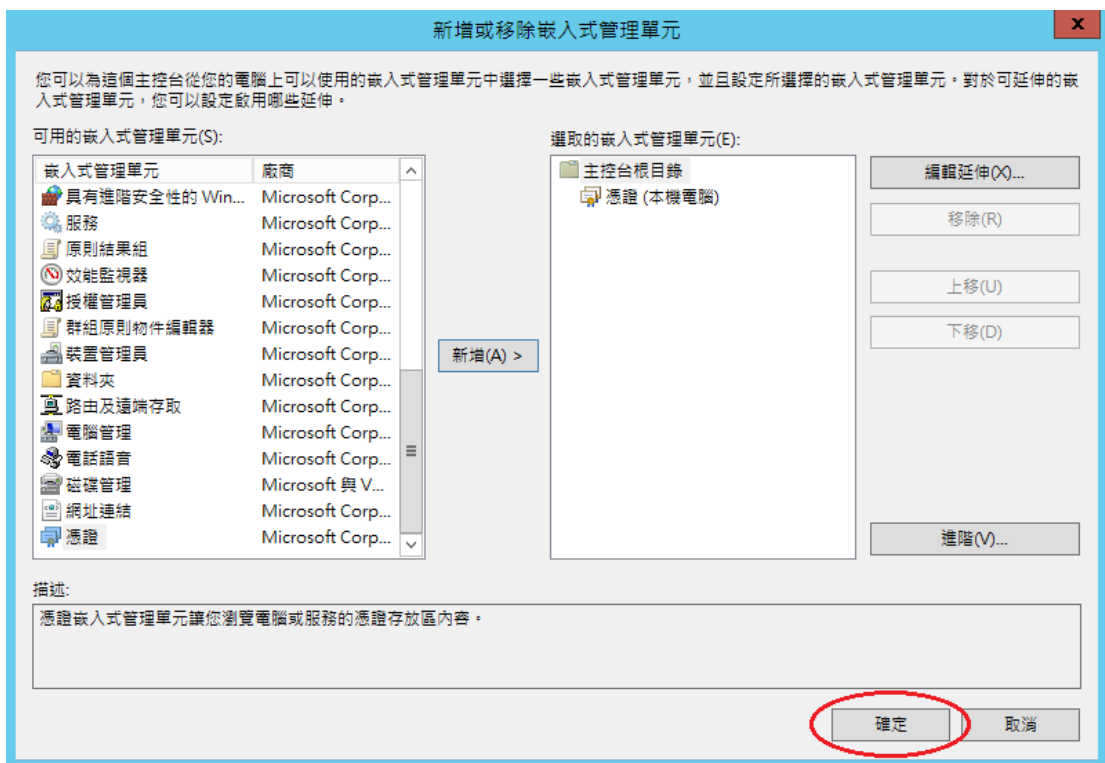


選擇「電腦帳戶」→「下一步」→「完成」。

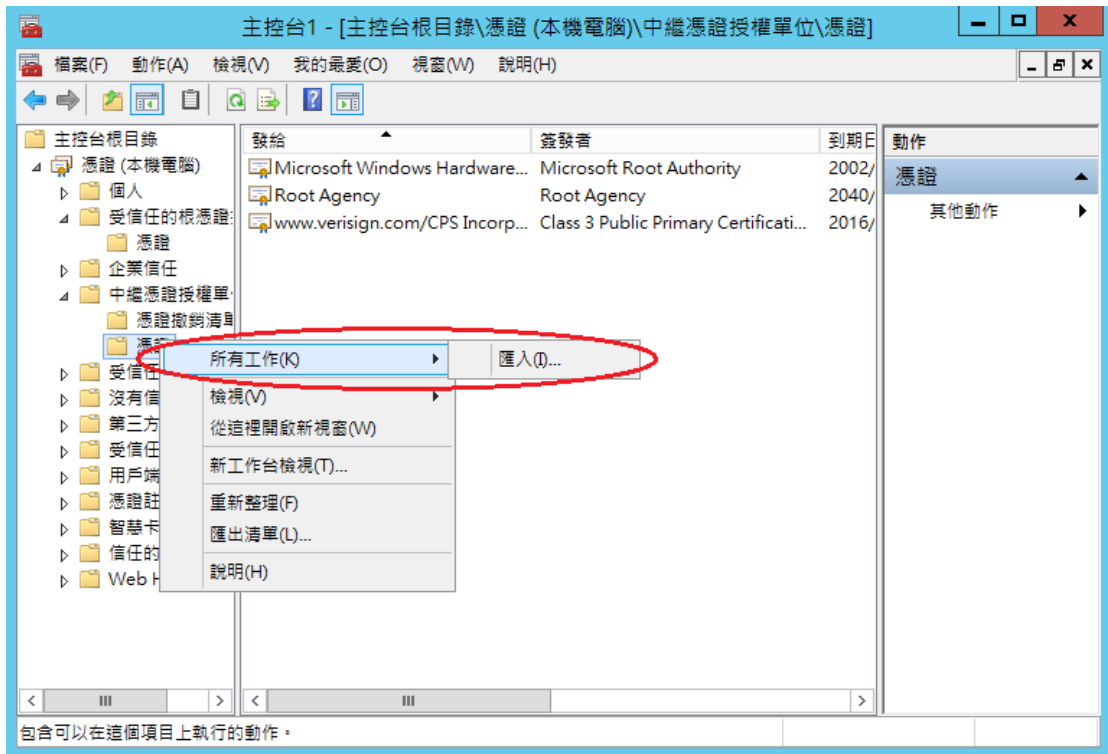




最後按下「確定」。

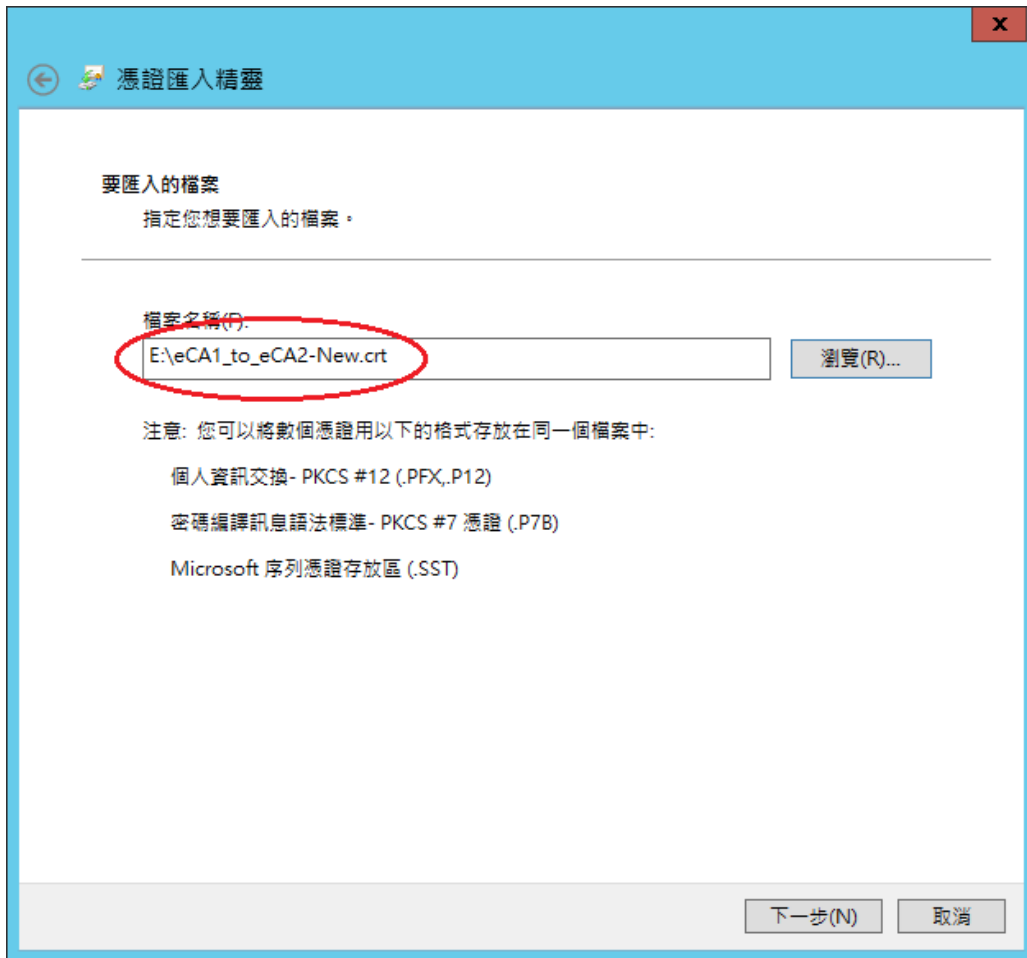


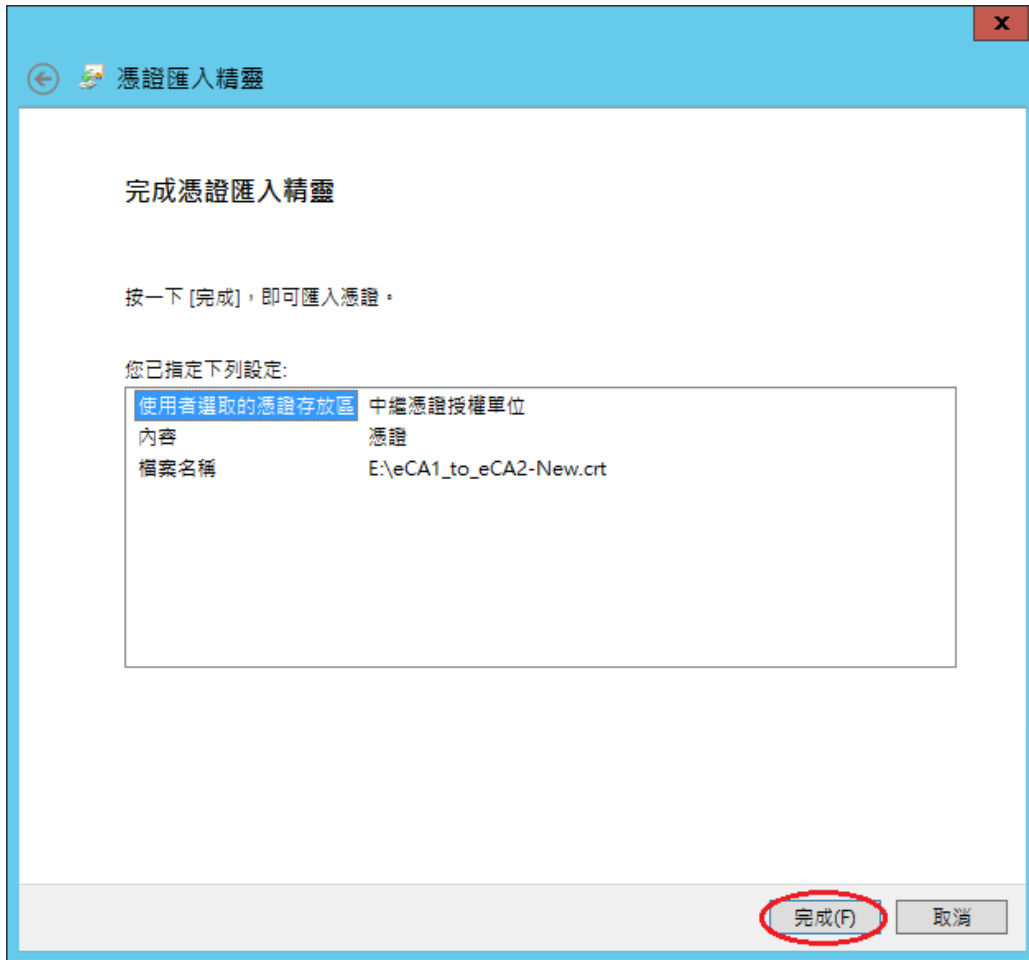
十一、匯入 eCA 自發憑證。在「中繼憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



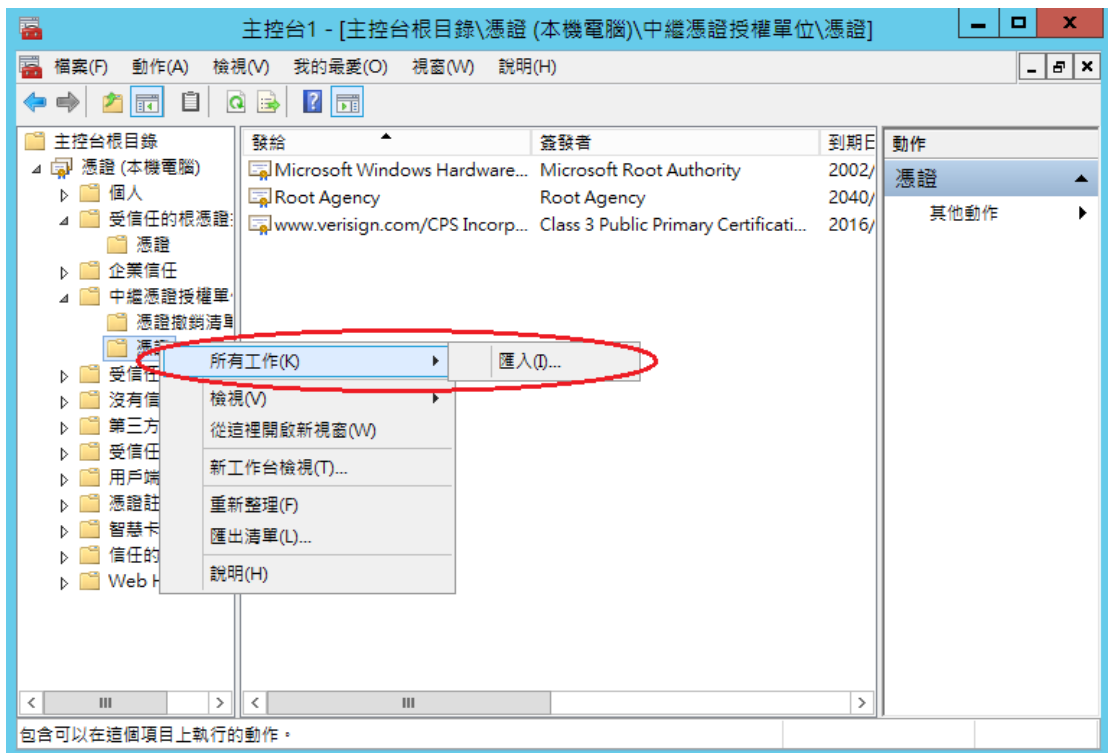
依照下列步驟匯入自發憑證。



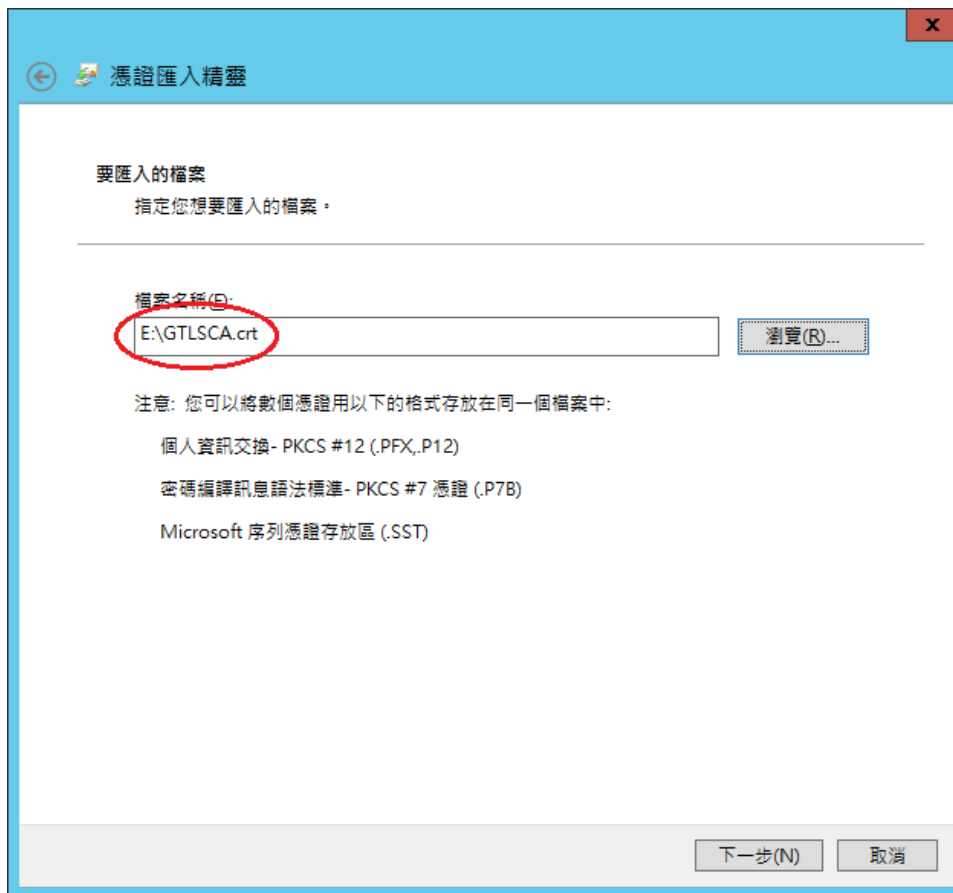




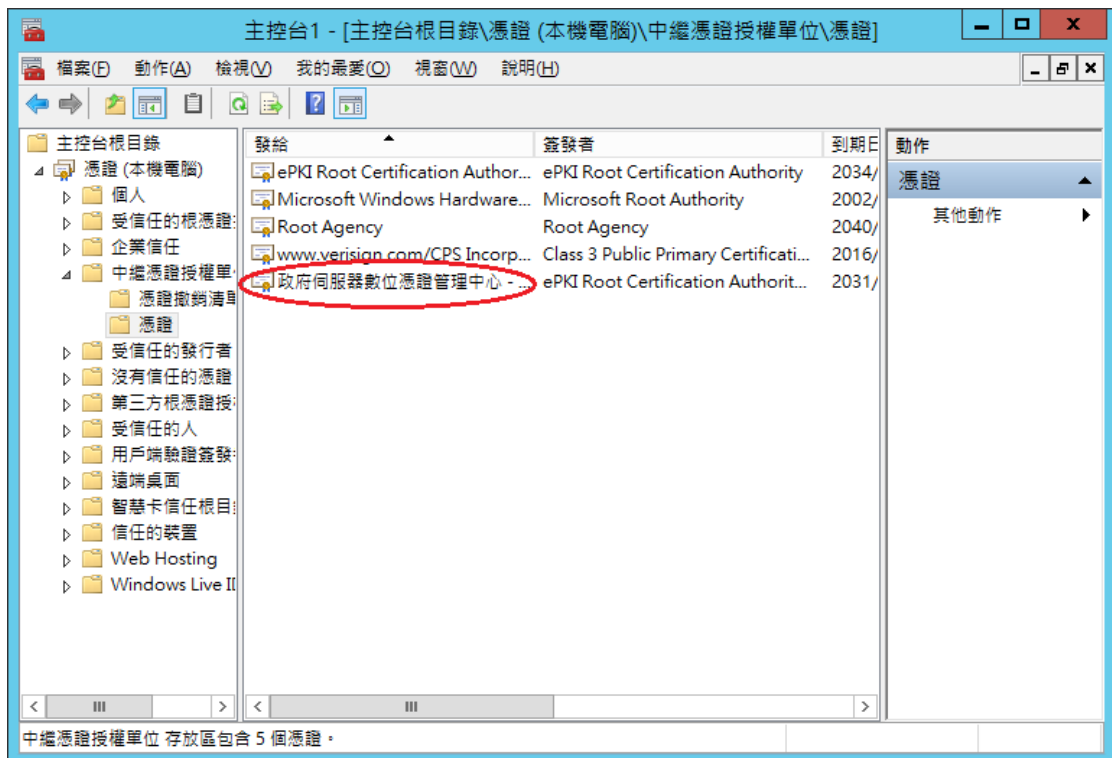
十二、匯入 GTLSCA 憑證。在「中繼憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



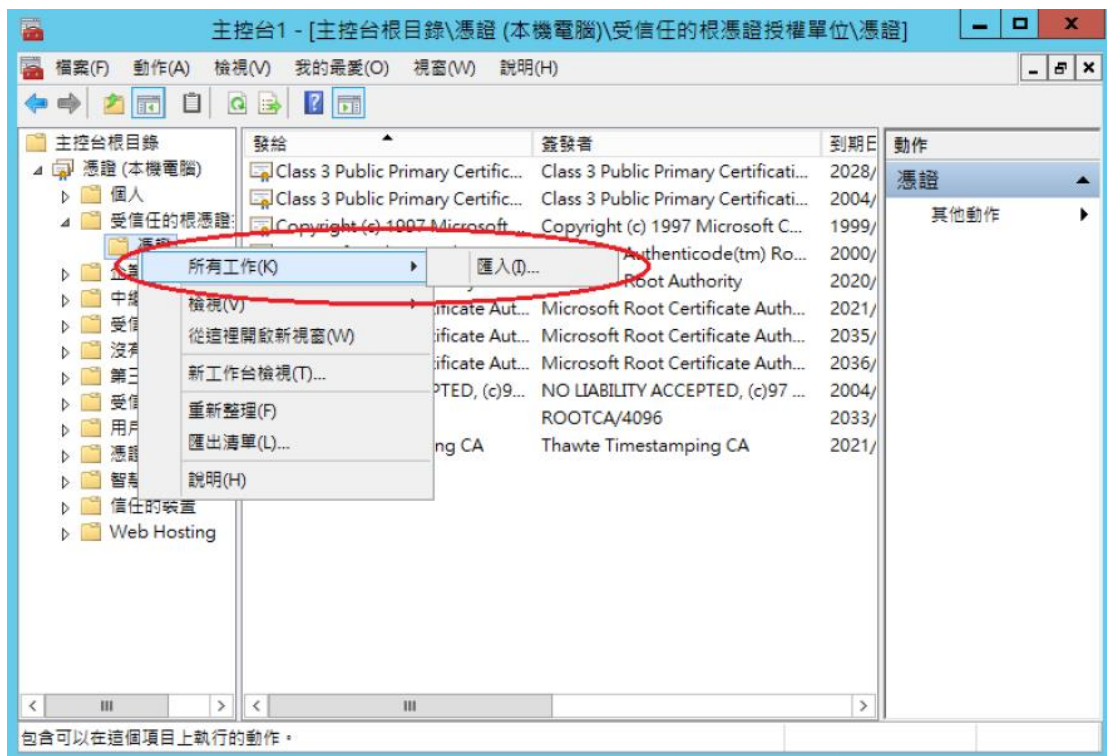
依照上述匯入 eCA 自發憑證的步驟，匯入 GTLSCA 憑證。



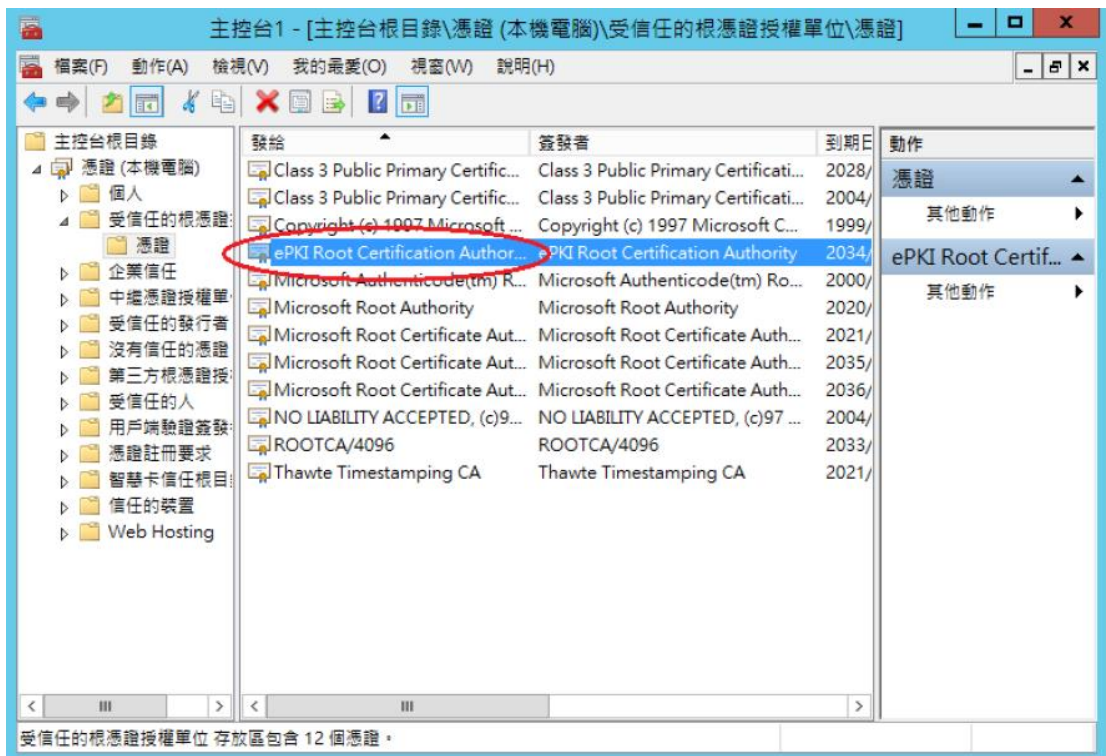
成功匯入後，可以看到 GTLSCA 的憑證。



十三、匯入 eCA 根憑證。在「受信任的根憑證授權單位」下的「憑證」按下右鍵，選擇「所有工作」→「匯入」。



成功匯入後，可以看到 eCA 的根憑證。

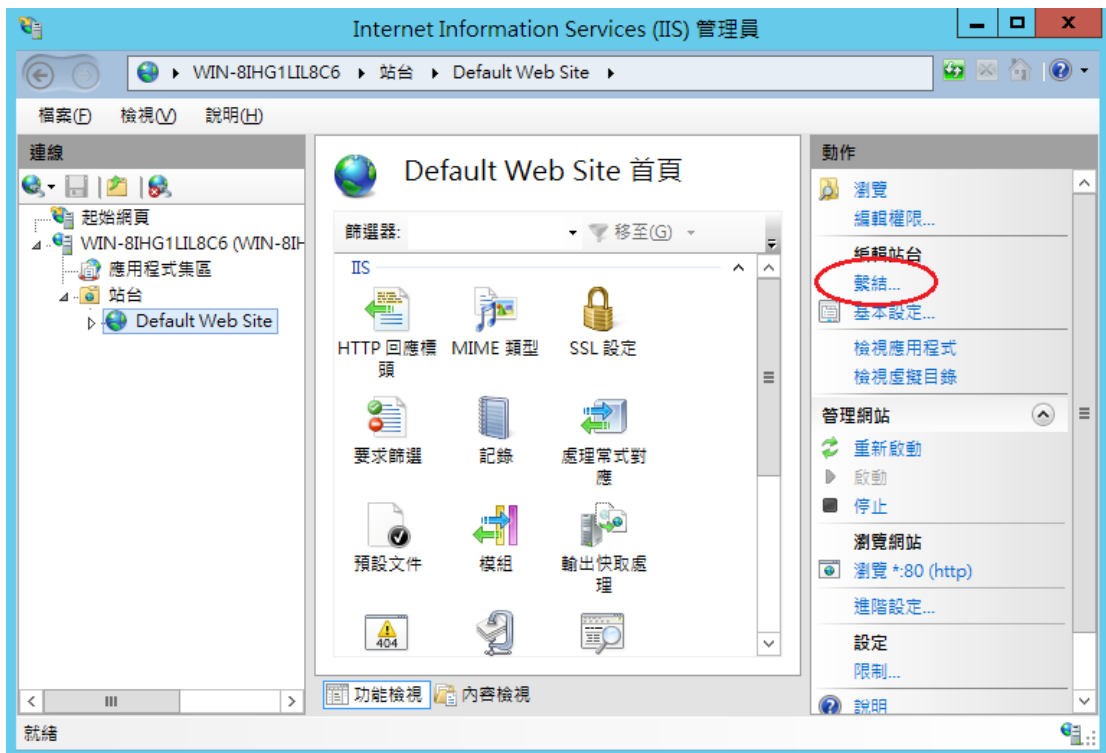


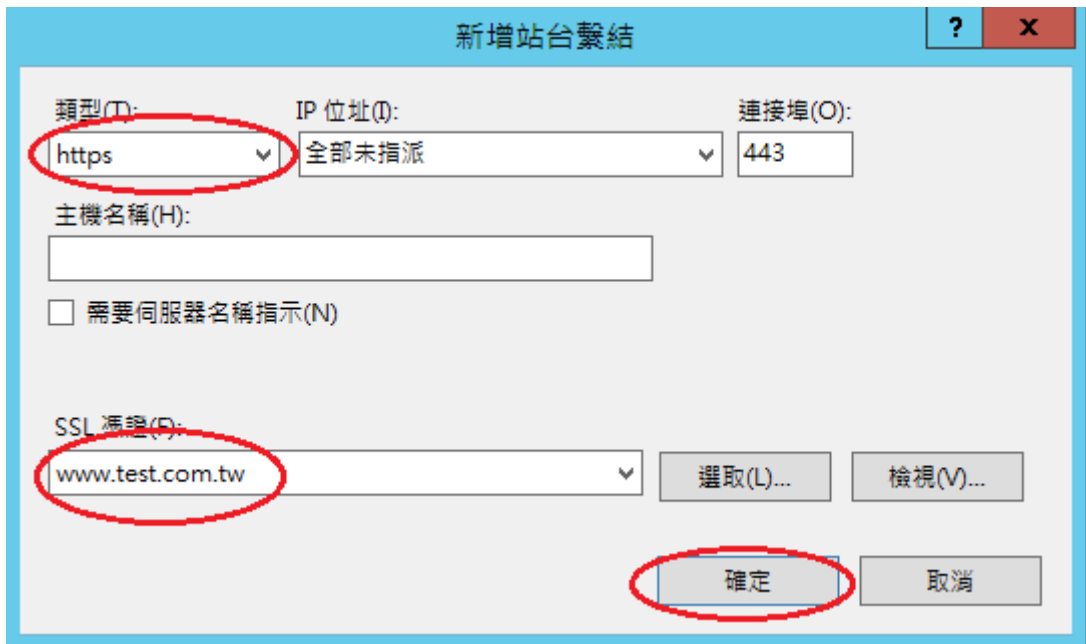
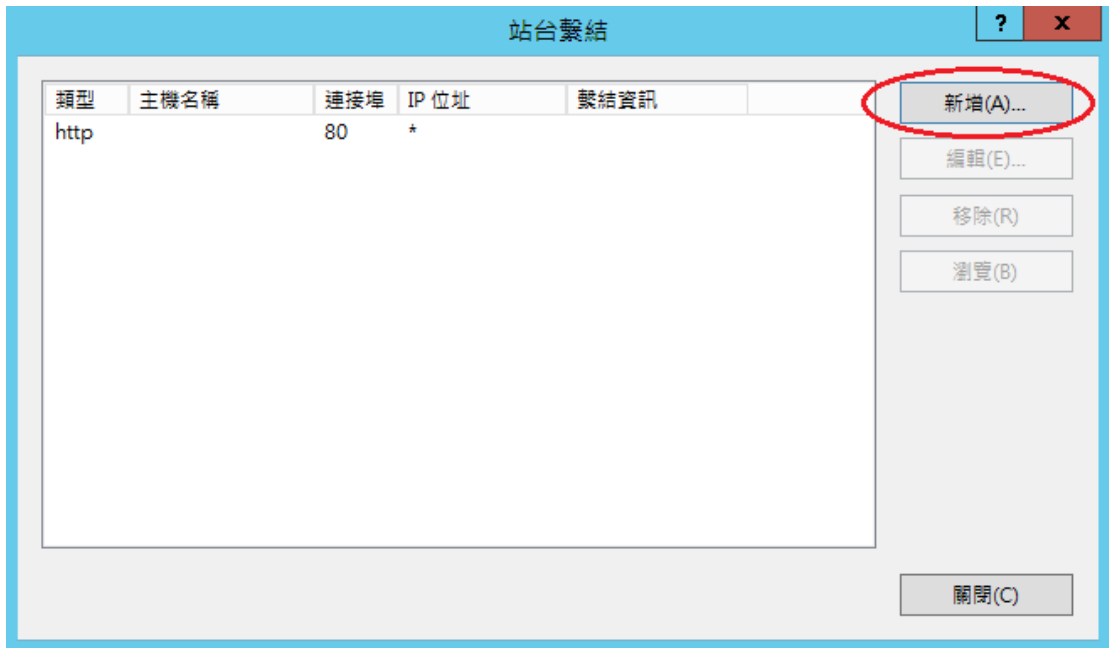
十四、檢查「受信任的根憑證授權單位」中是否有 ePKI Root Certification

Authority - G2 的憑證(到期日為 2037/12/31)，若有請刪除。

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

→ 新增→類型『https』、連接埠 『443』，選擇要安裝在此站台之 SSL 憑證 (www.test.com.tw)。





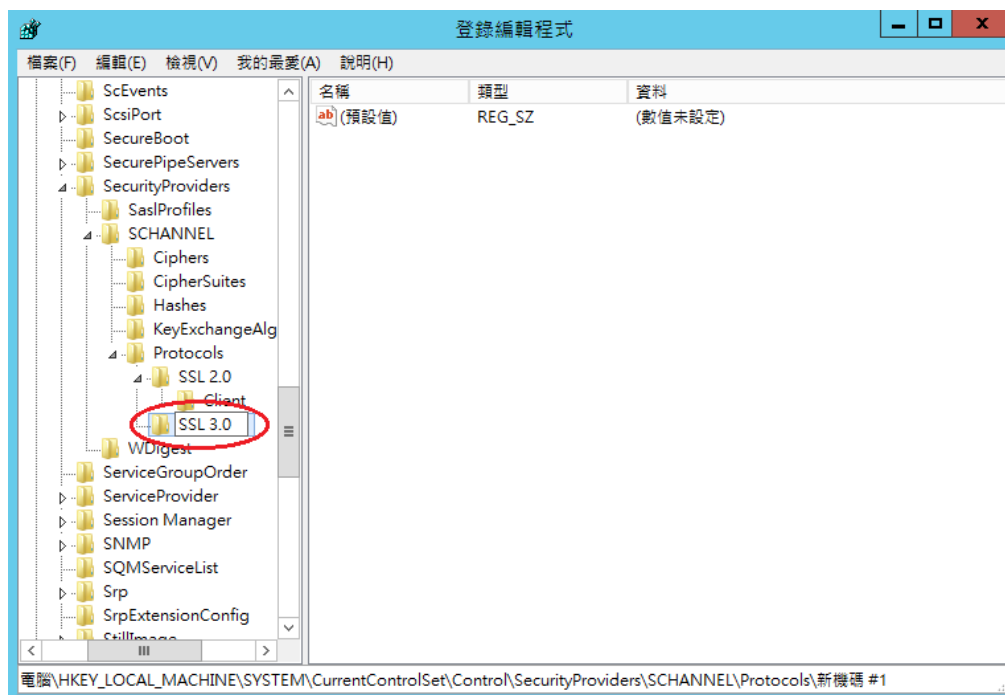
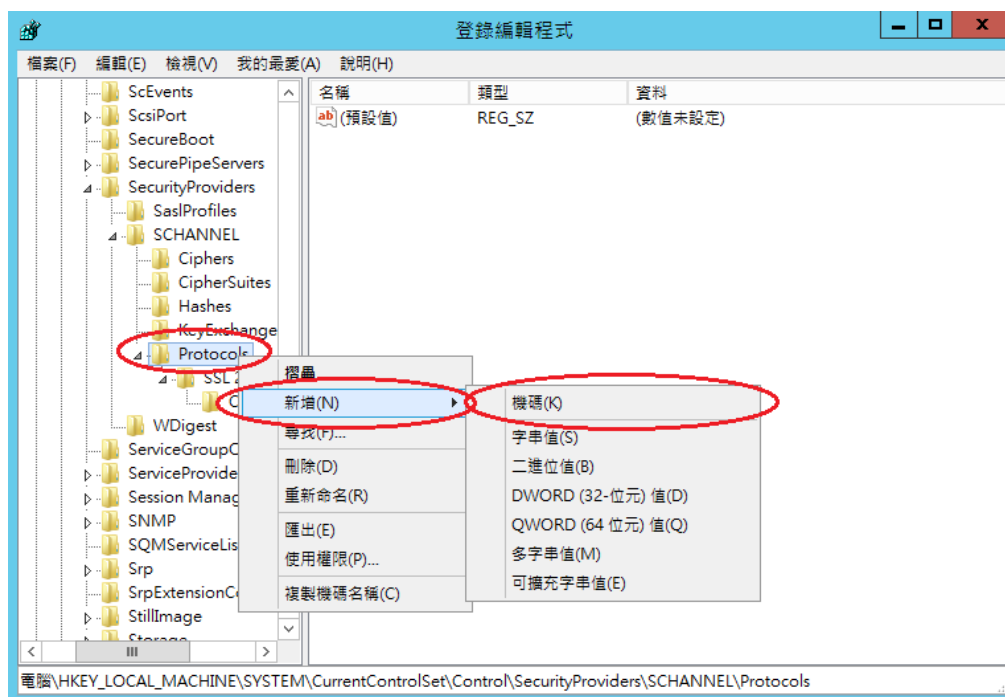
十六、依照您的網路架構，您可能需要於防火牆開啟對應 https 的 port。

附件一：停用 SSLv2、SSLv3

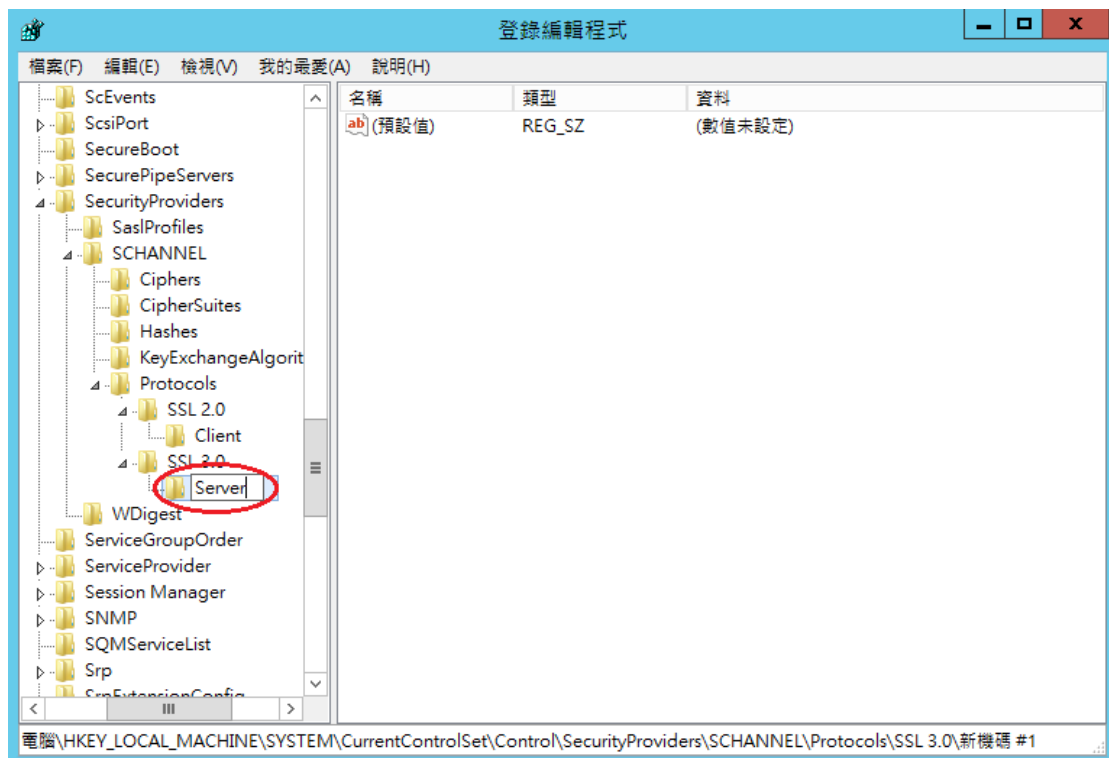
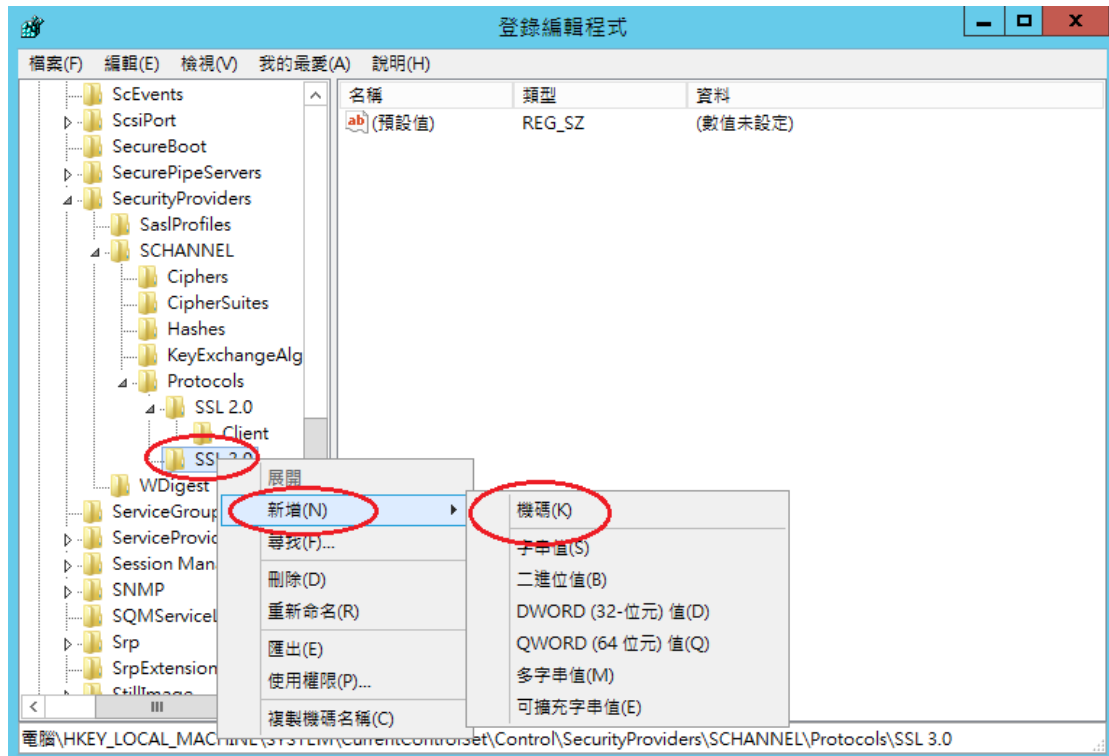
- 一、 經測試，IIS8 SSL2.0 預設是關閉的，若您的 SSL2.0 是開啟的，您可以依照以下關閉 SSL 3.0 的作法來關閉 SSL2.0。
- 二、 開啟登錄檔編輯程式，依照以下路徑找到 Protocols。

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProvider
s\SCHANNEL\Protocols

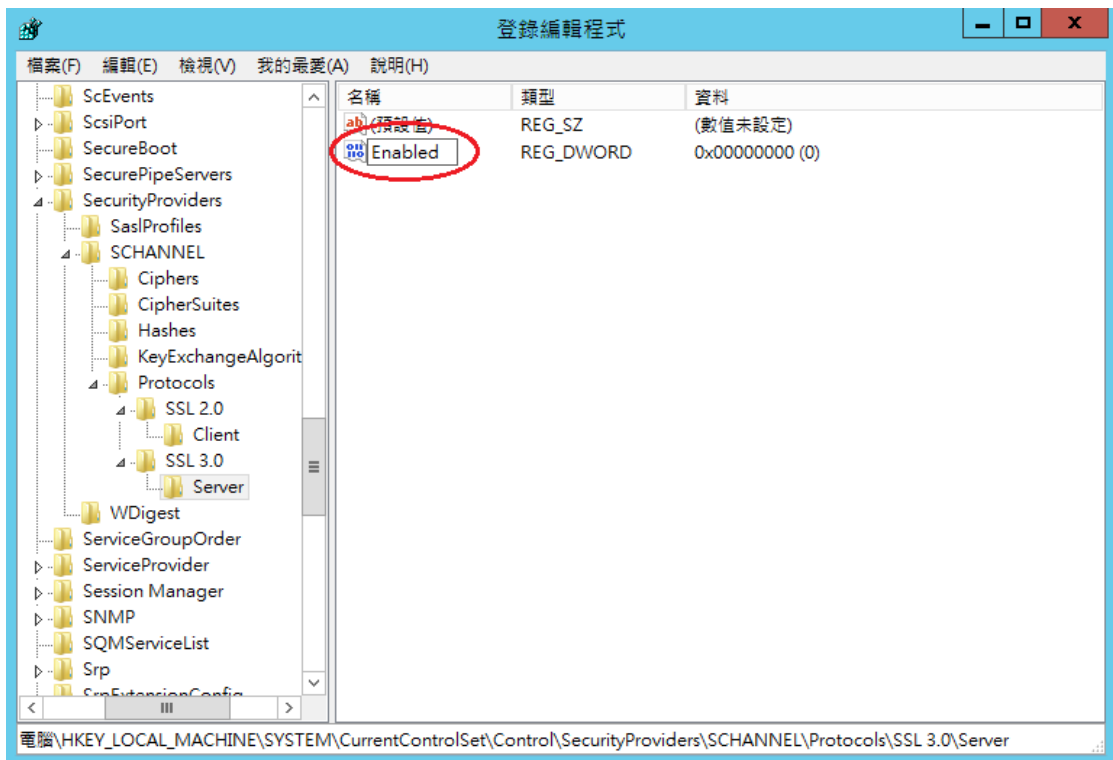
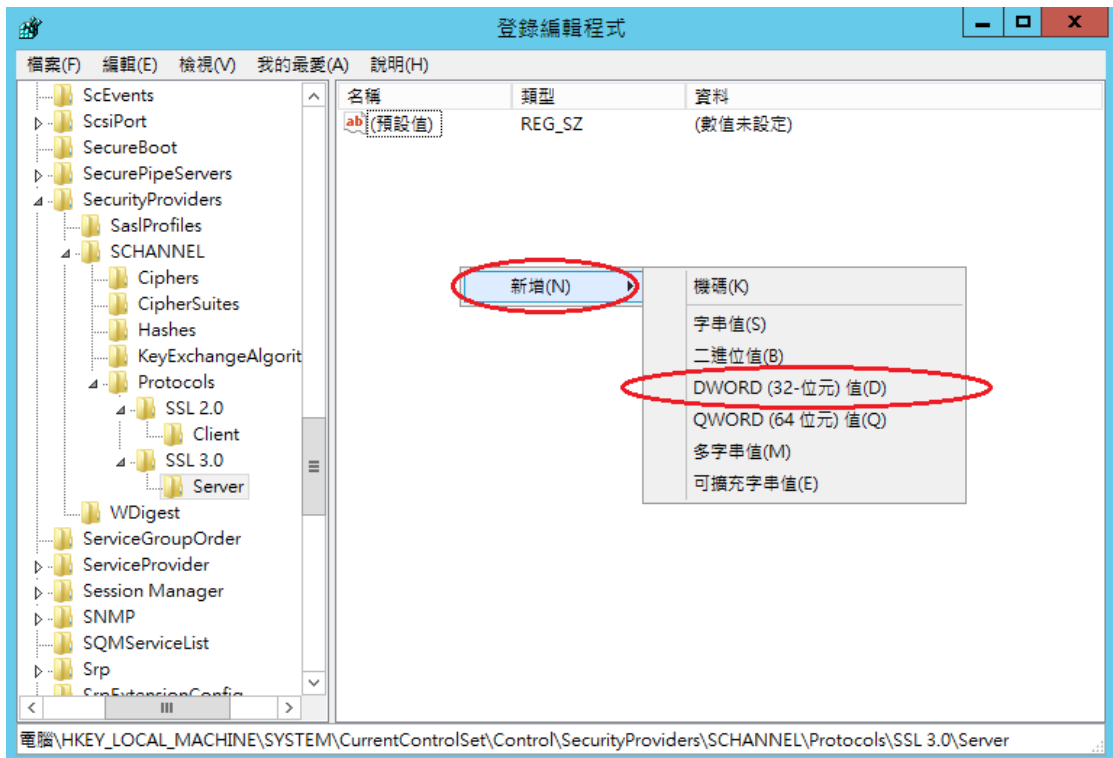
在 Protocols 的機碼上，按下右鍵→新增→機碼，然後輸入「SSL 3.0」。



三、 在 SSL3.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」。



四、 接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值，然後輸入「Enabled」，並確認資料欄位值為「0x00000000 (0)」，若不是，請手動將值改為 0。



五、 重新啟動電腦。