

中華電信 HiPKI 憑證管理中心 (OVTLSCA)

Windows Server IIS 7、8、10 憑證備份與還原

聲明：本說明文件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。本說明文件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，若因參考本說明文件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。

請依照您的Server(2008、2012、2016)版本，參考對應的憑證備份與還原步驟。

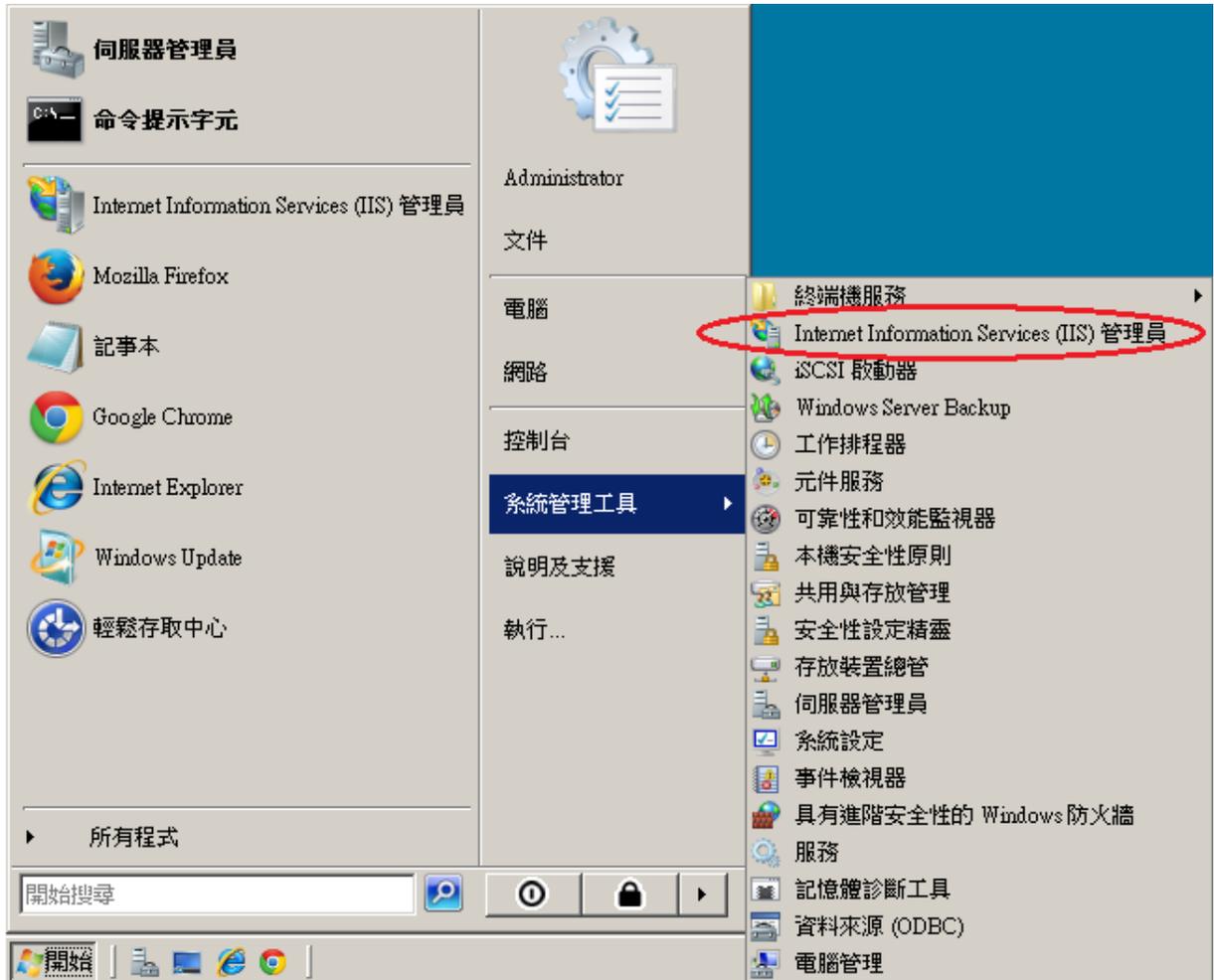
目錄

憑證備份步驟.....	2
Windows Server 2008	2
Windows Server 2012	4
Windows Server 2016	6
憑證還原步驟.....	8
Windows Server 2008	8
Windows Server 2012	19
Windows Server 2016	31

憑證備份步驟

Windows Server 2008

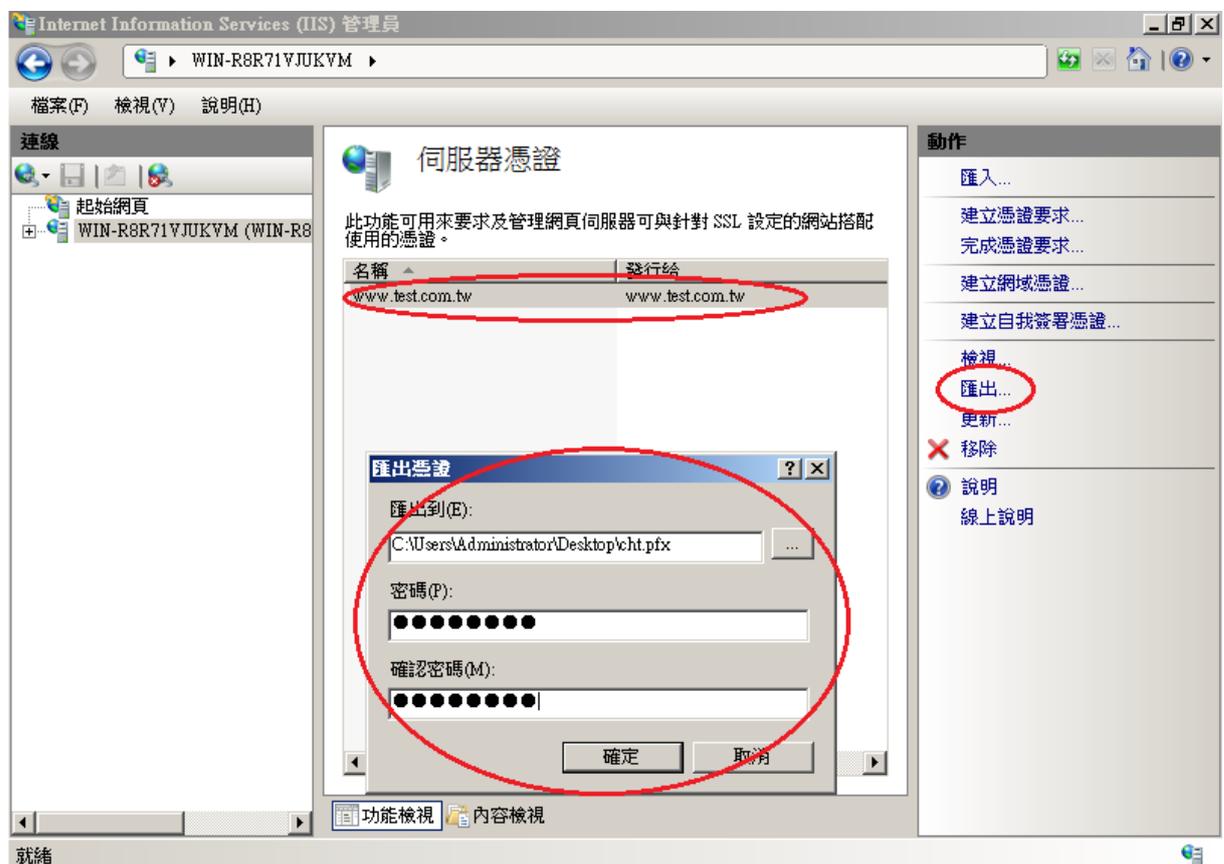
1. 點選「開始」→「系統管理工具」→「Internet Information Services (IIS)管理員」。



2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。

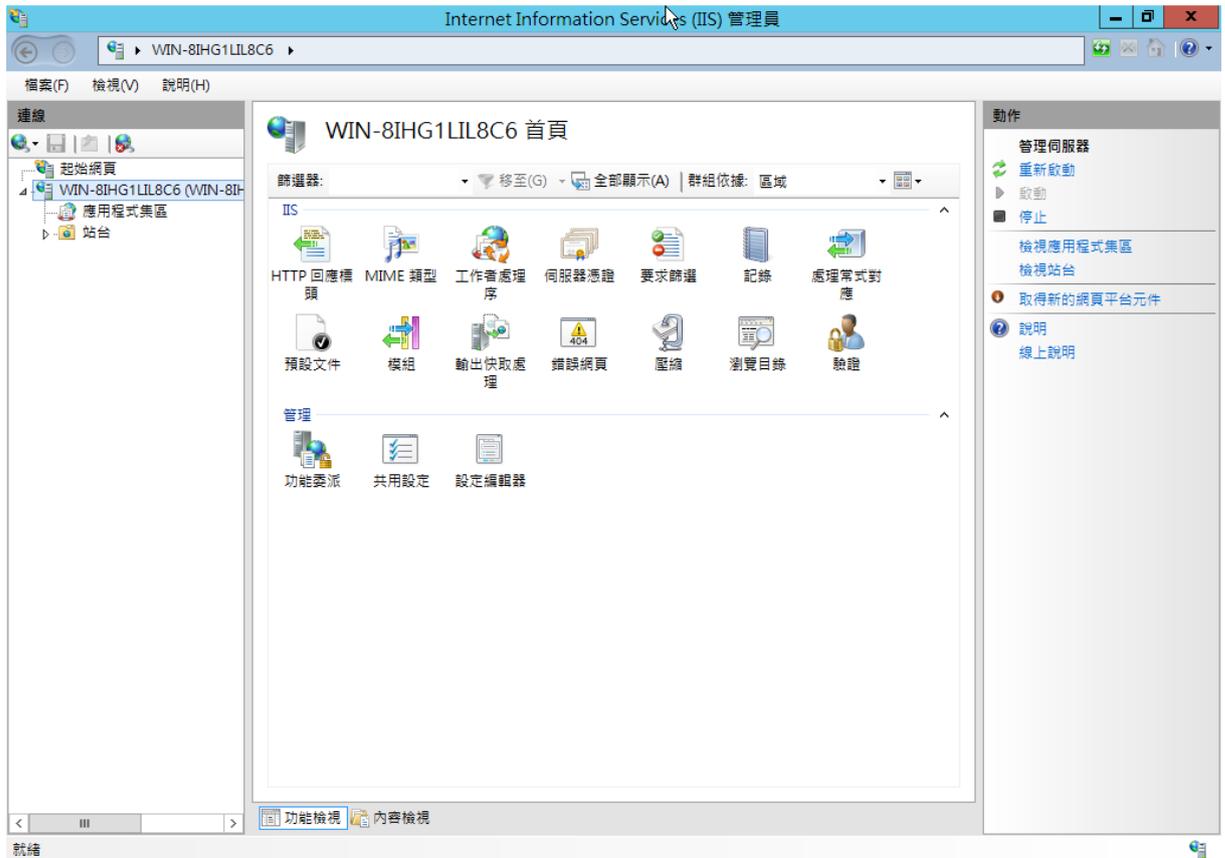


3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。

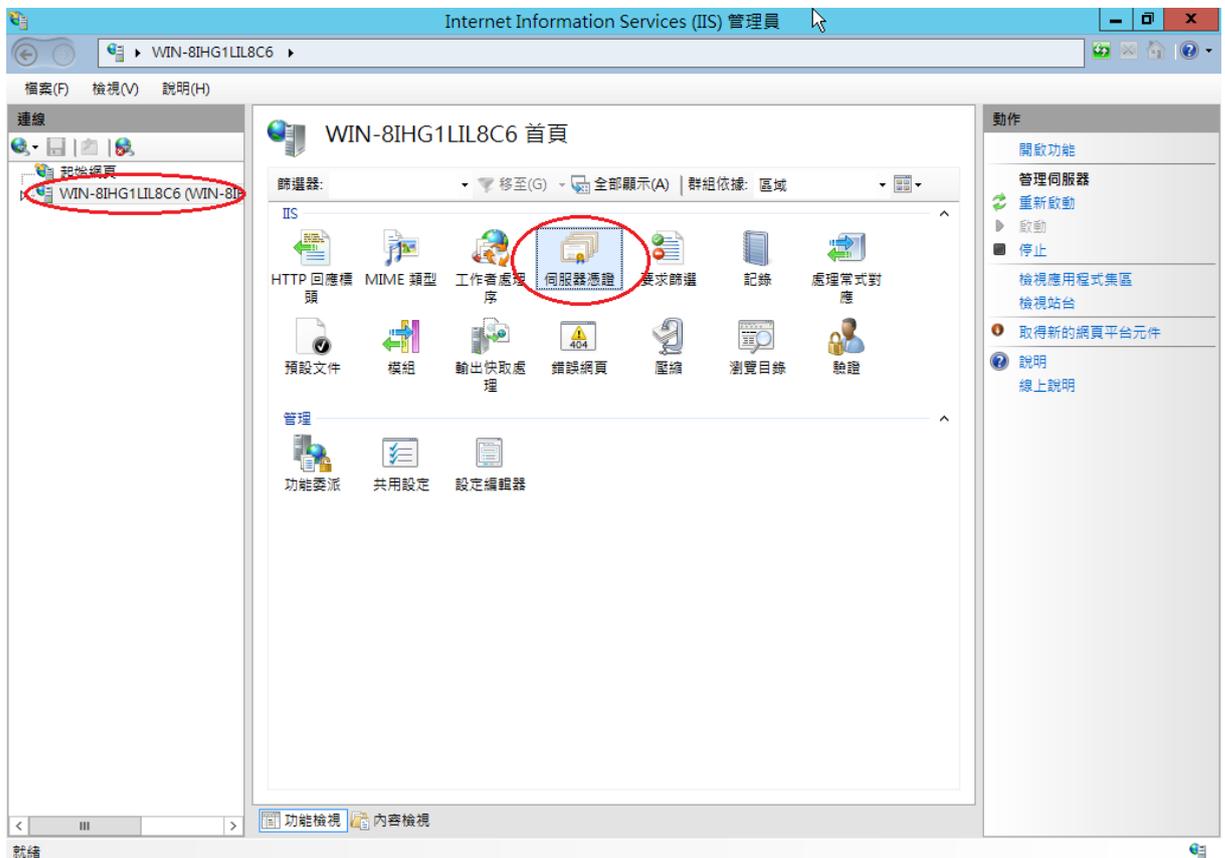


Windows Server 2012

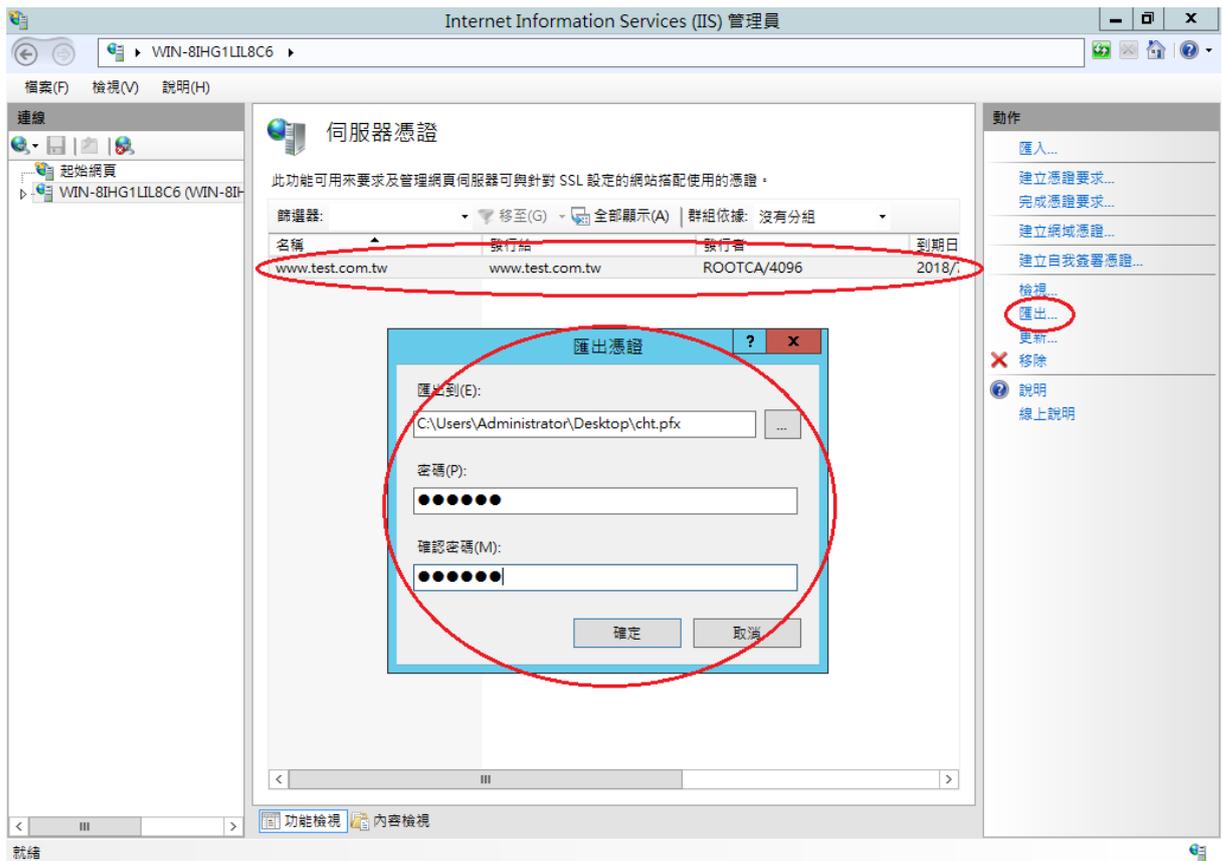
1. 開啟「Internet Information Services (IIS)管理員」。



2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。

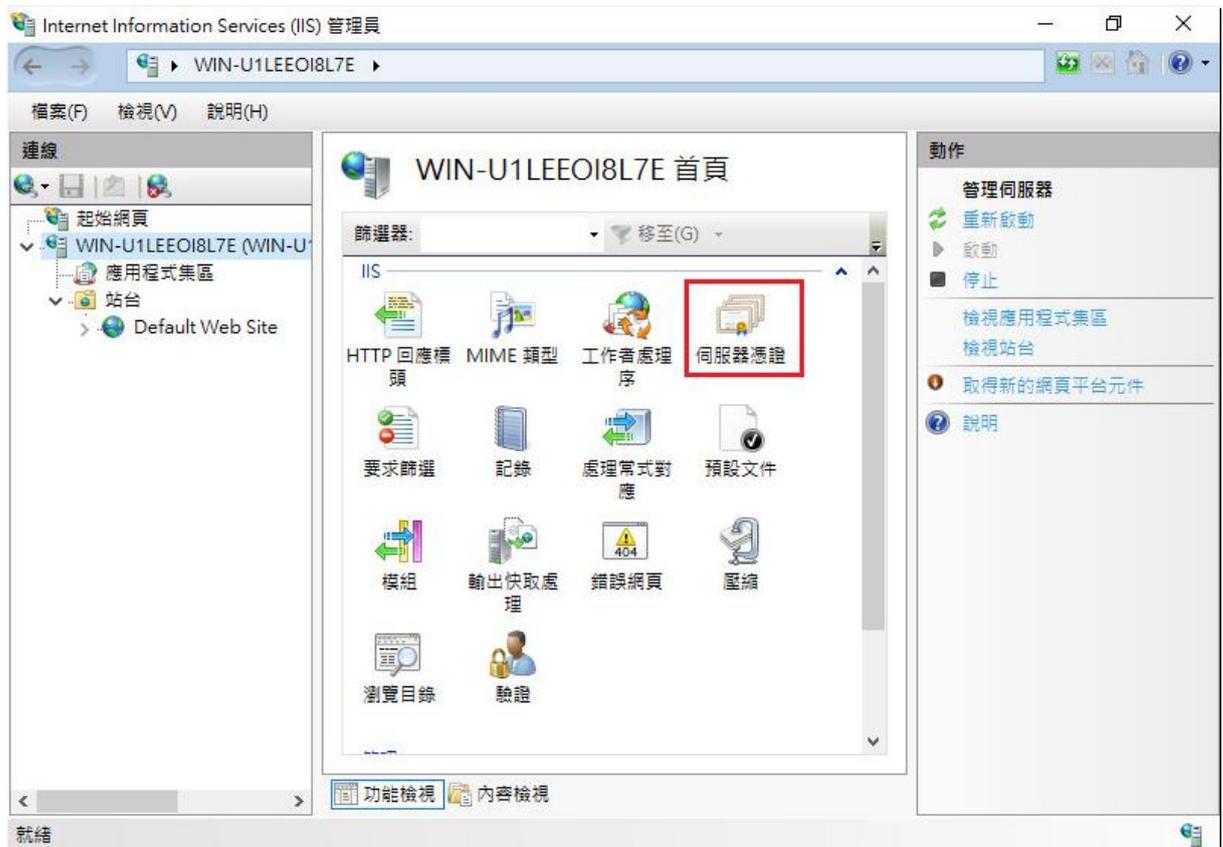


3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。

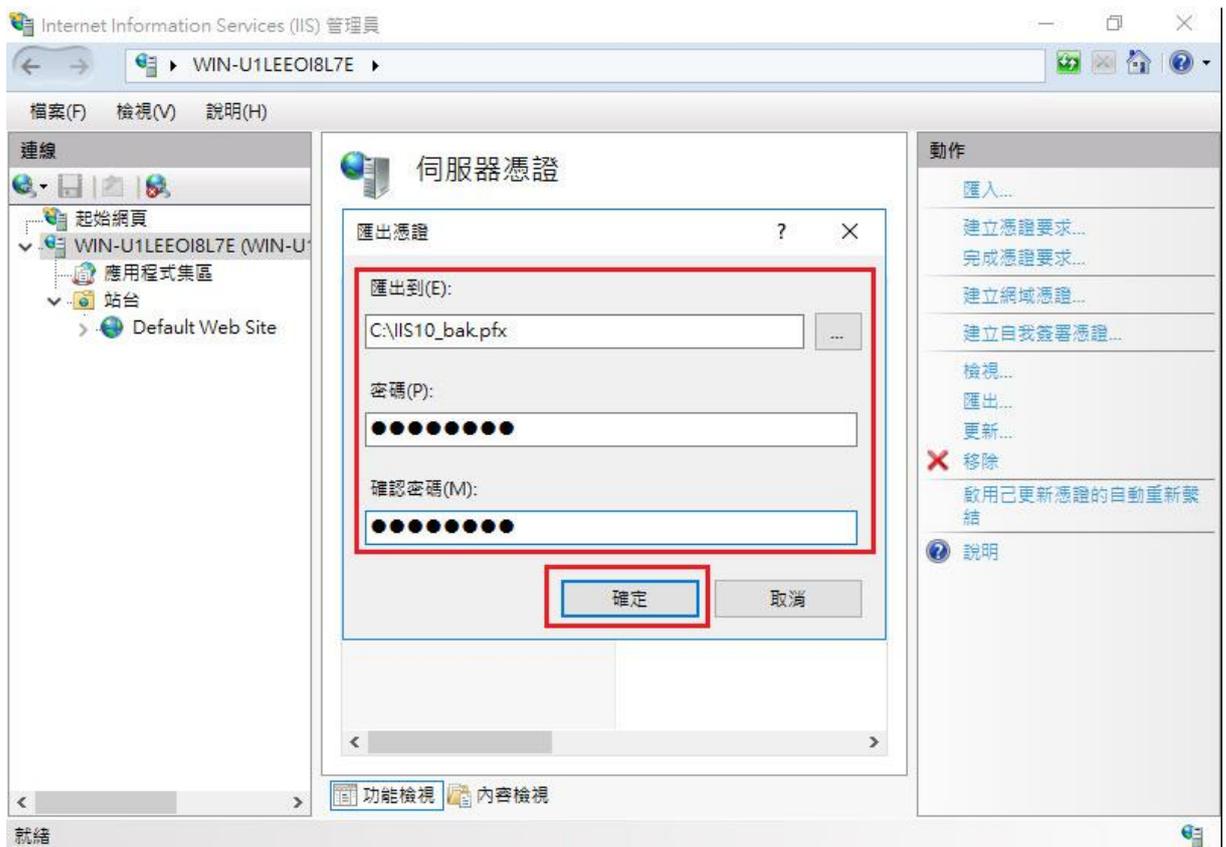
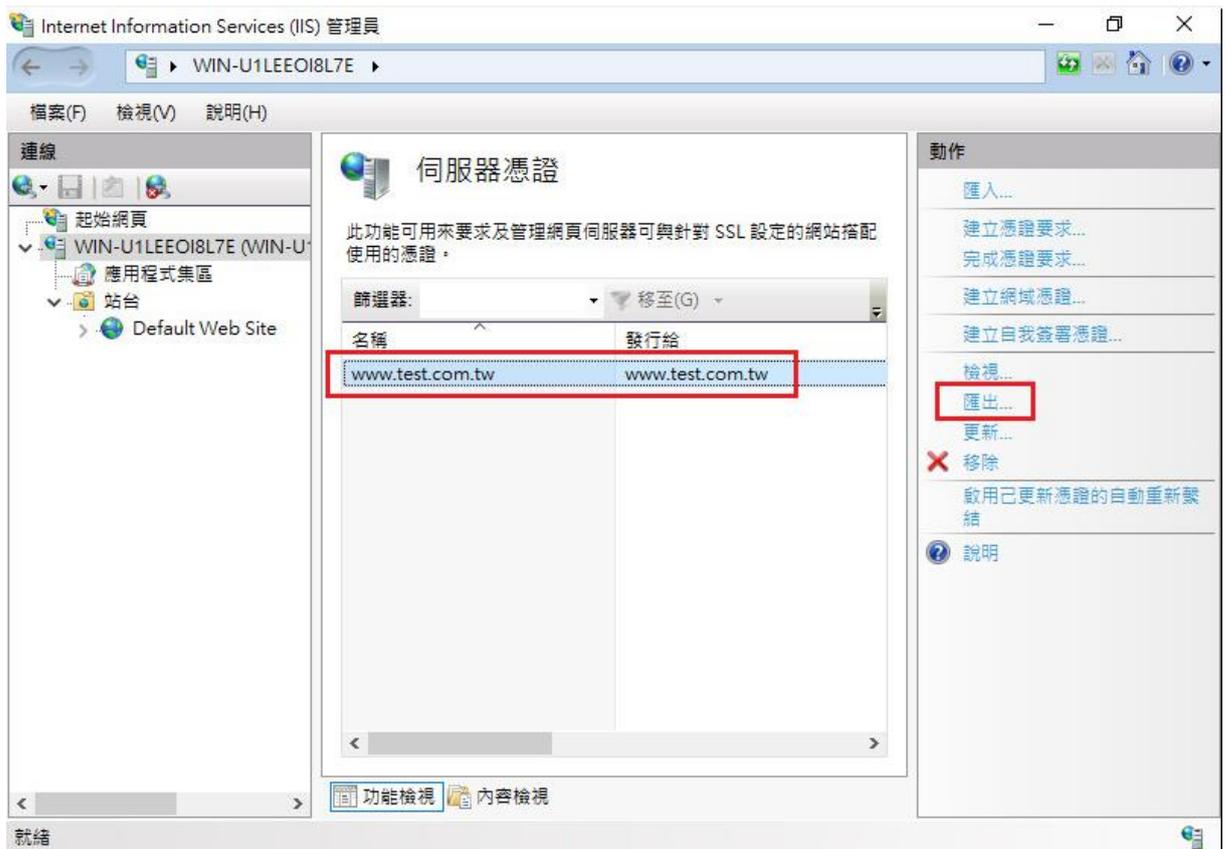


Windows Server 2016

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



3. 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。



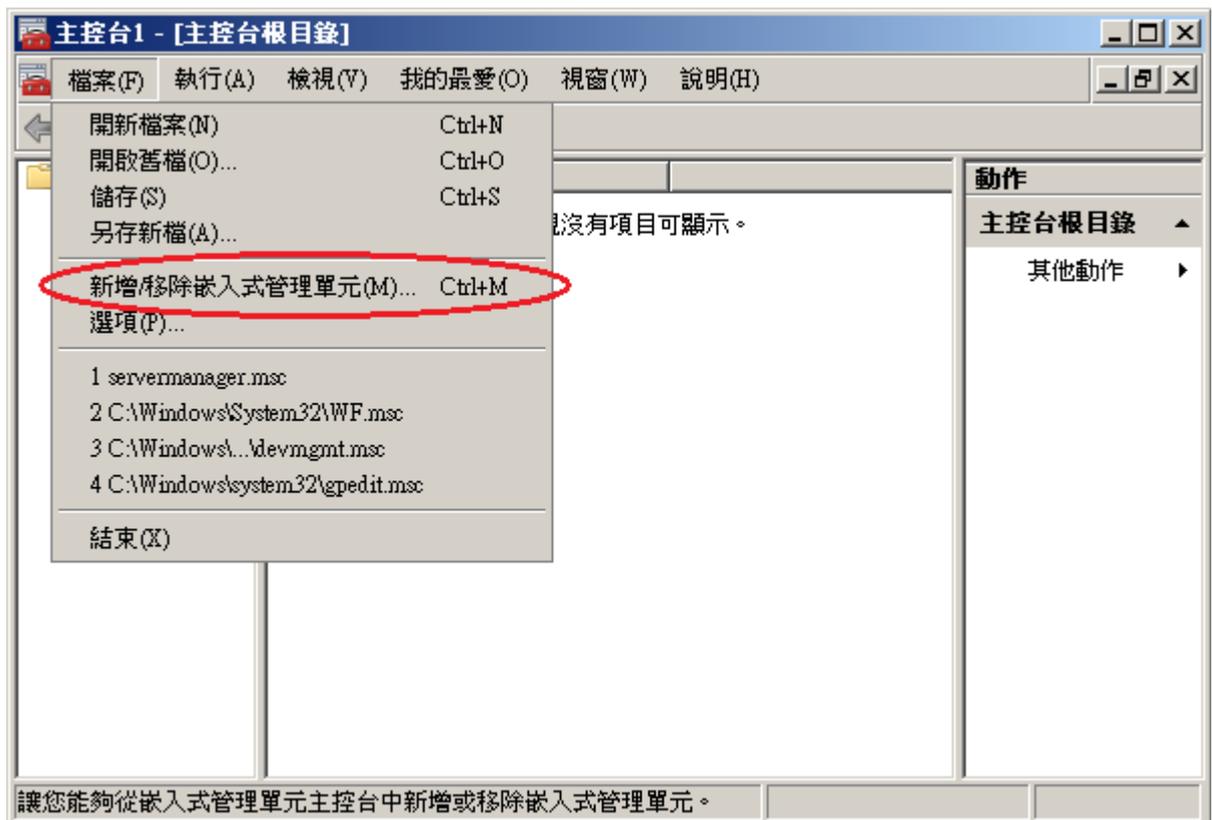
憑證還原步驟

Windows Server 2008

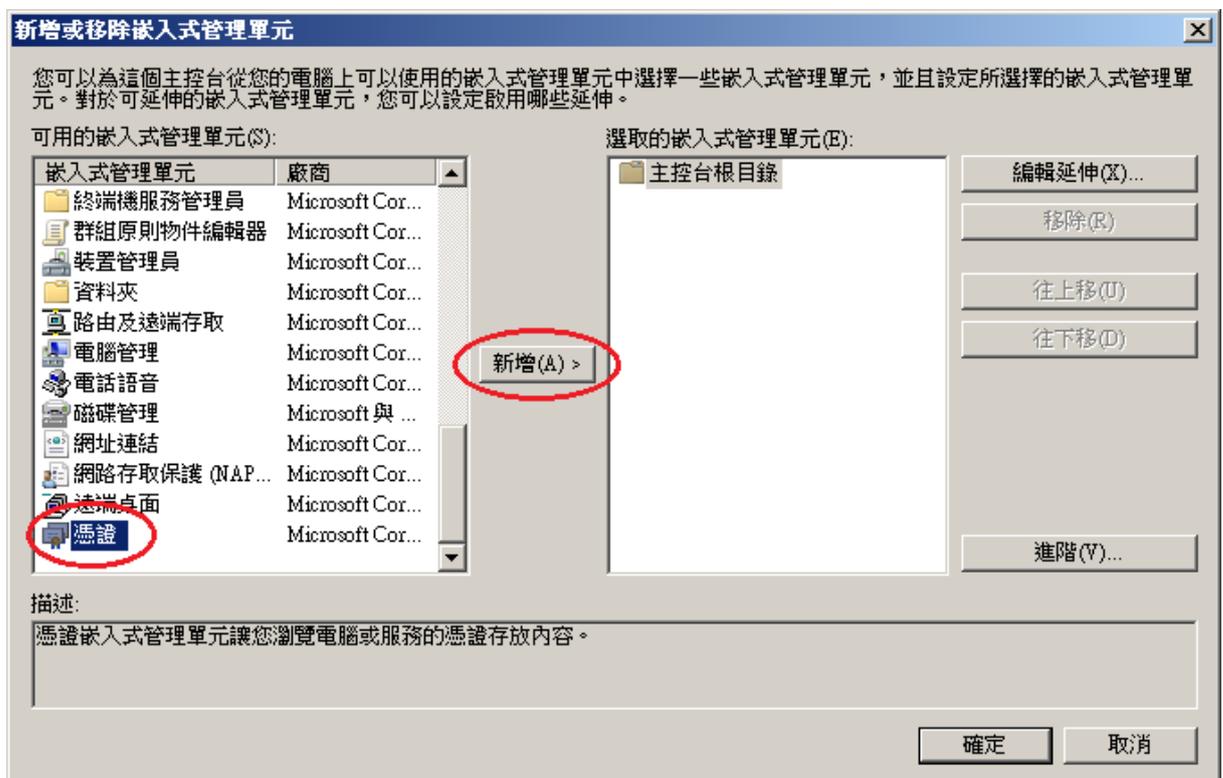
1. 「開始」→「輸入 mmc」，按下「Enter」。



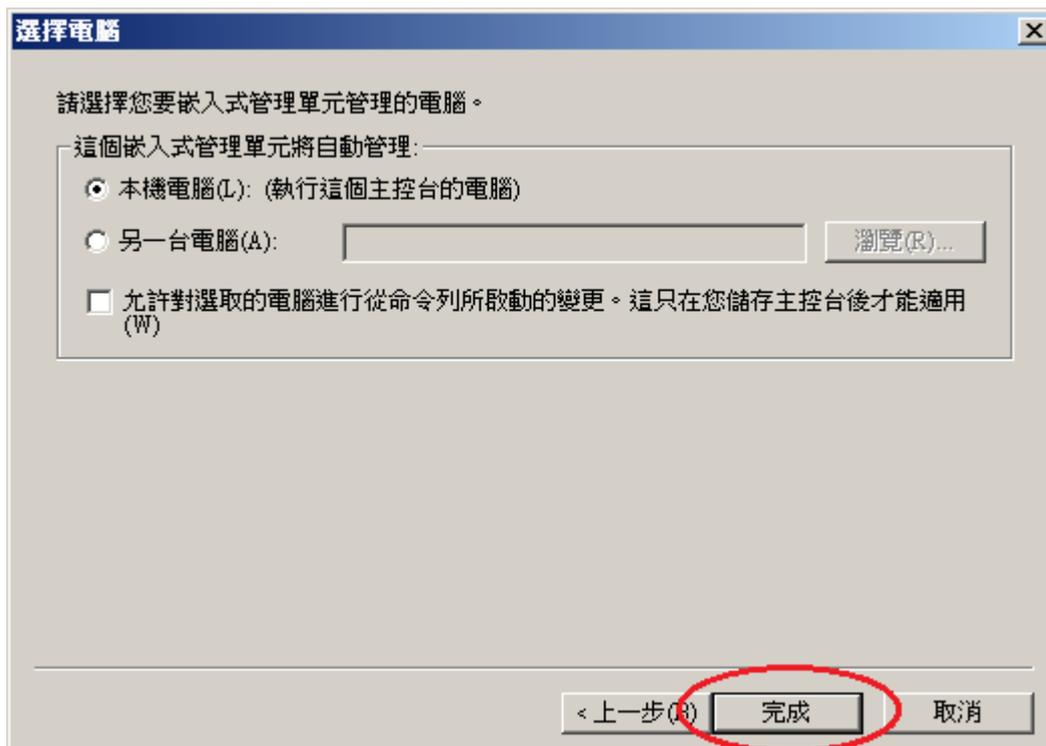
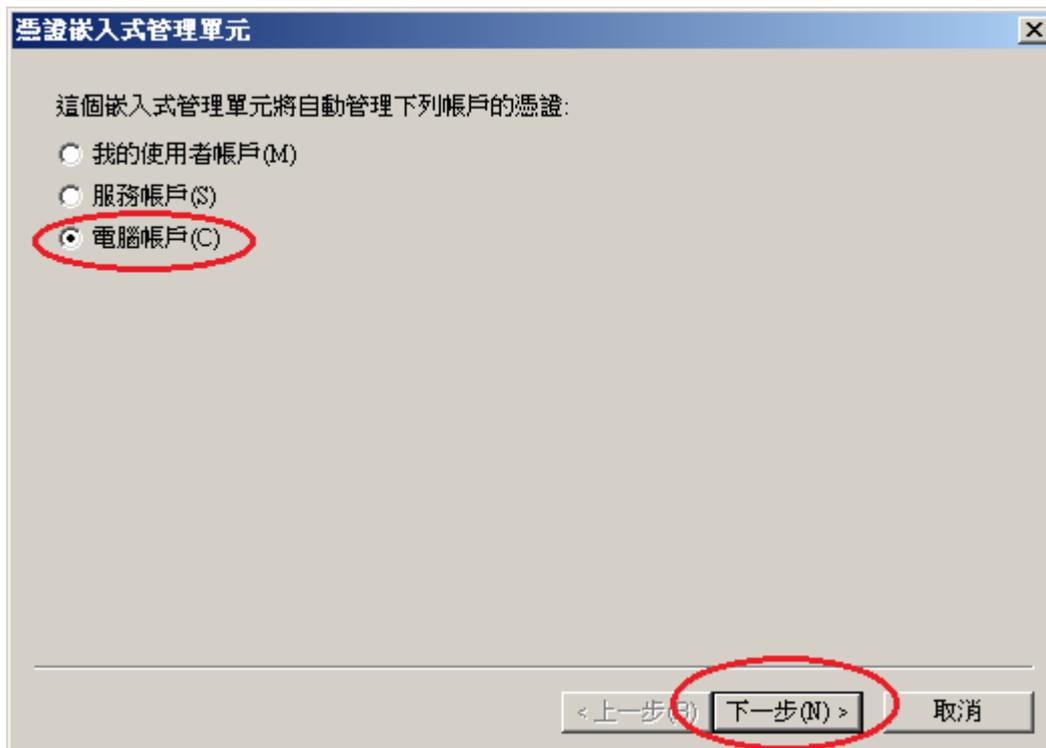
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。



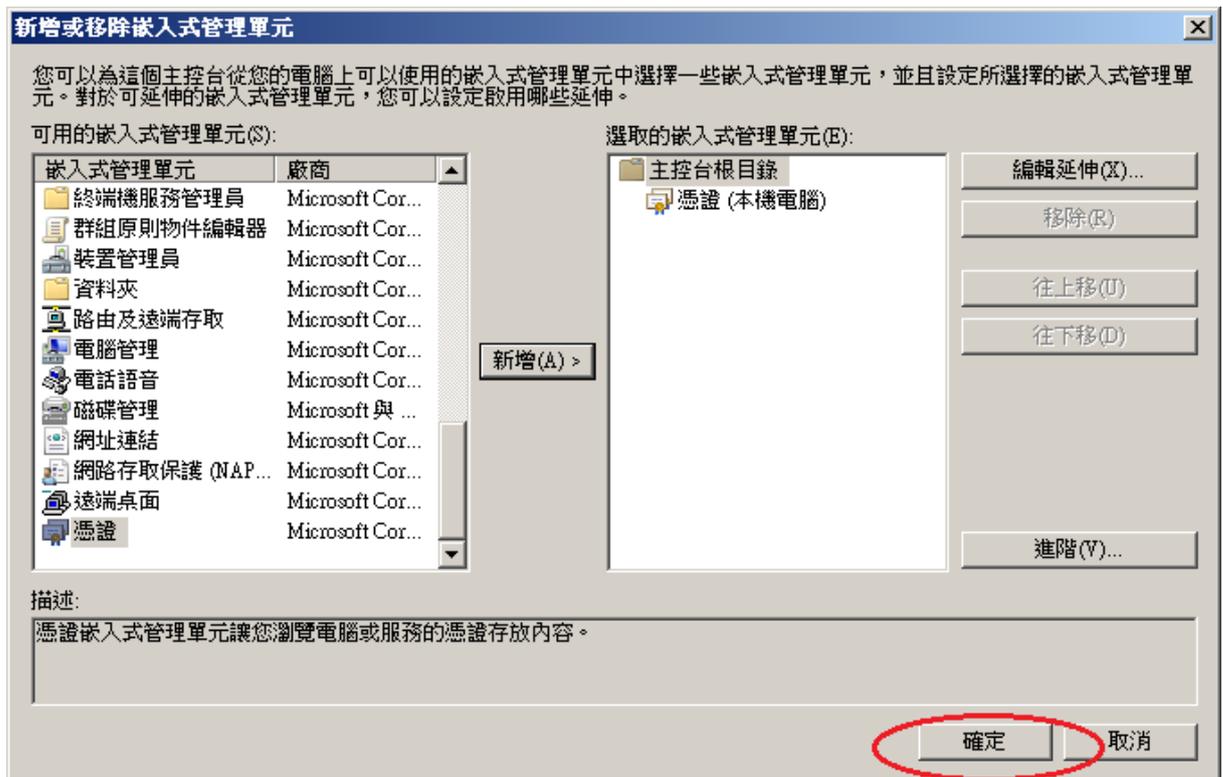
3. 點選「憑證」→「新增」



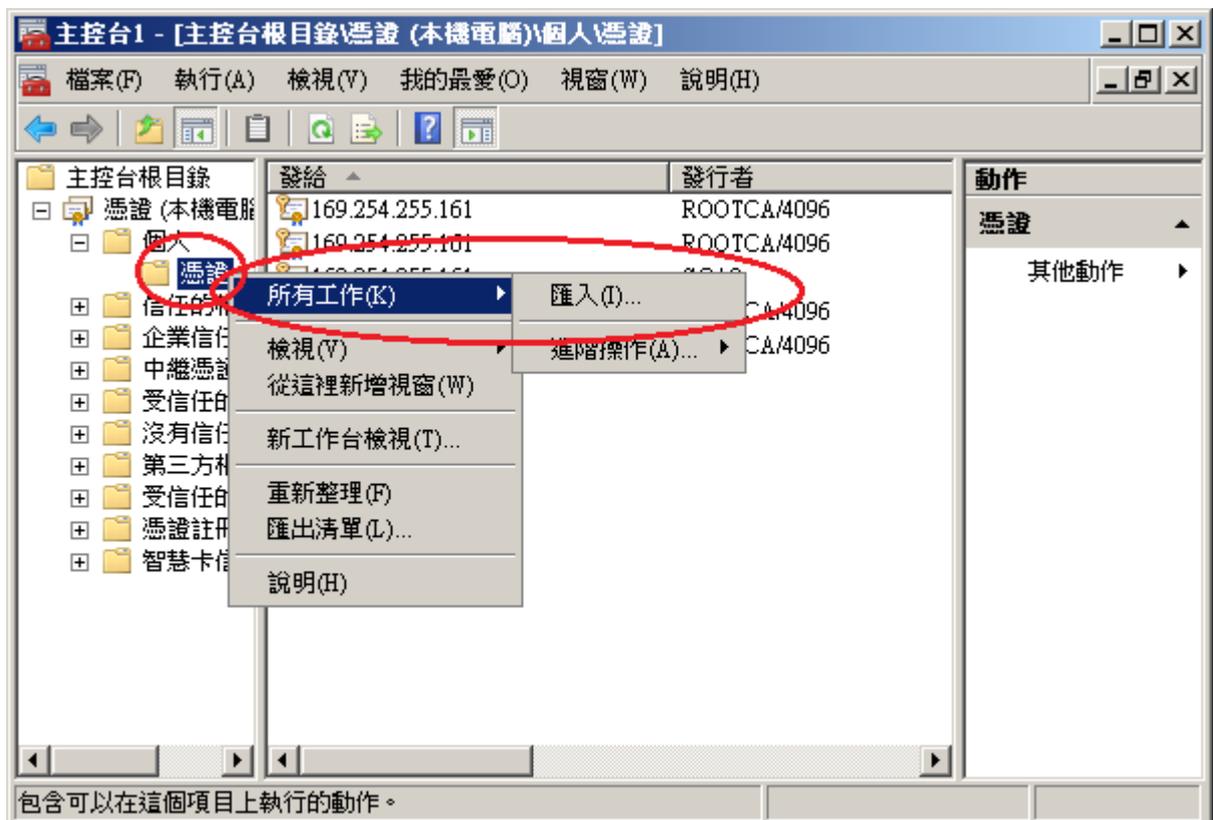
「電腦帳戶」→「下一步」→「完成」。



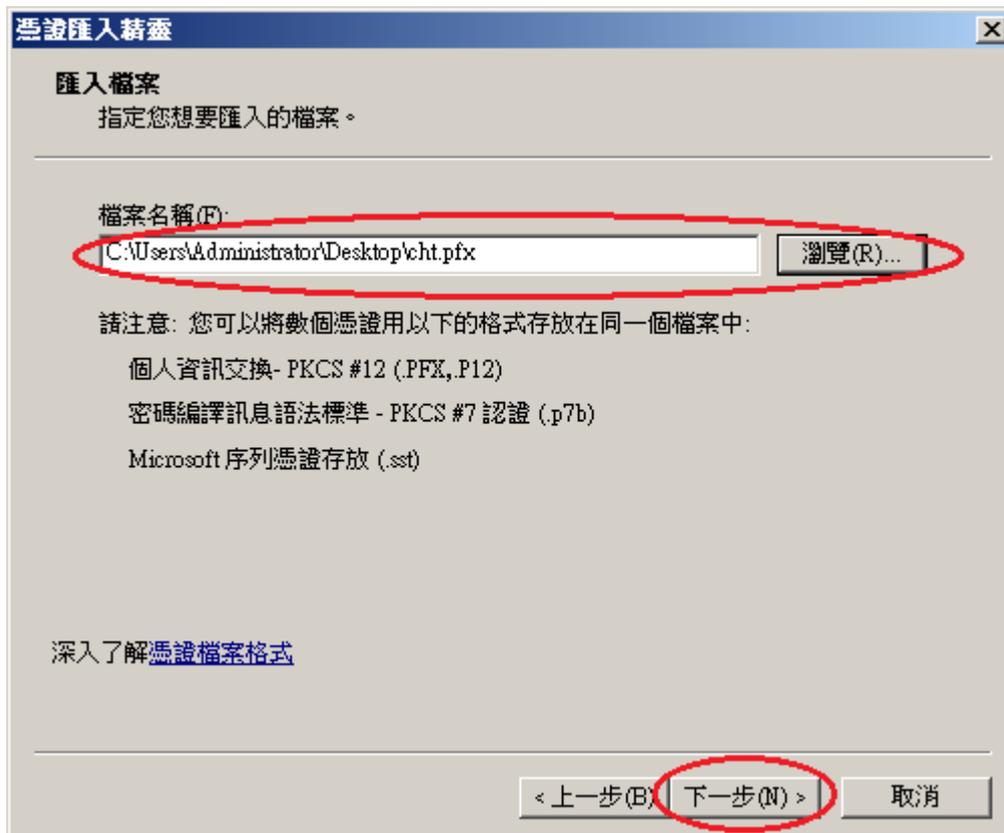
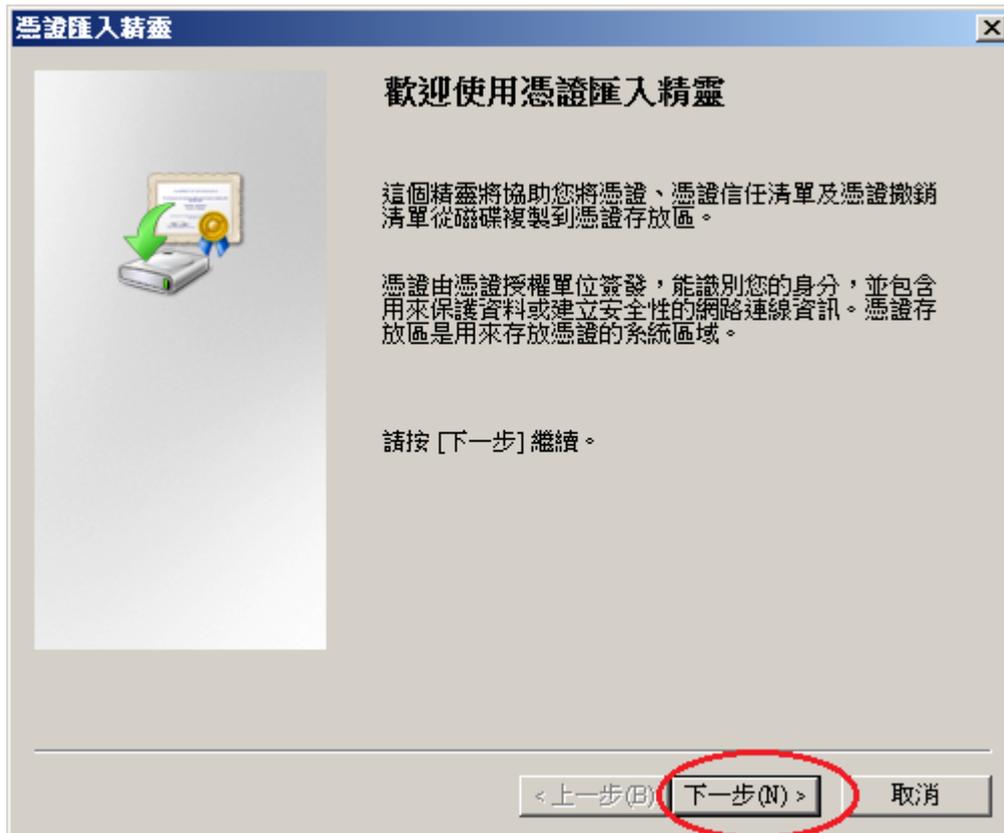
「確定」。



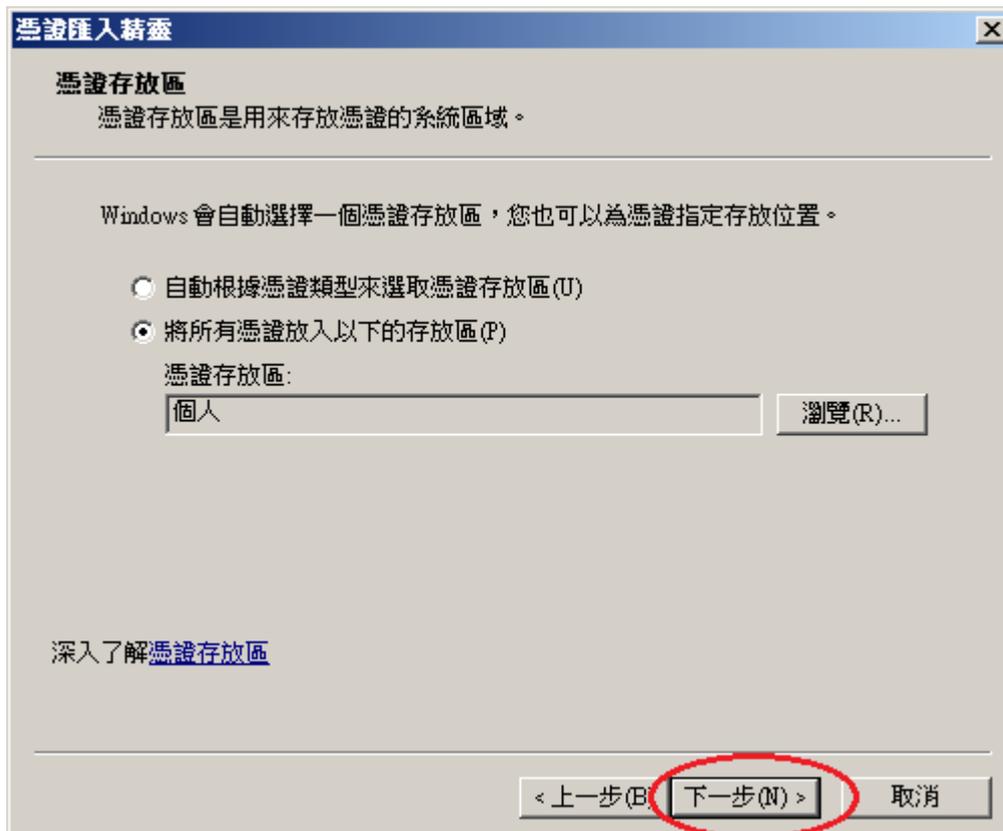
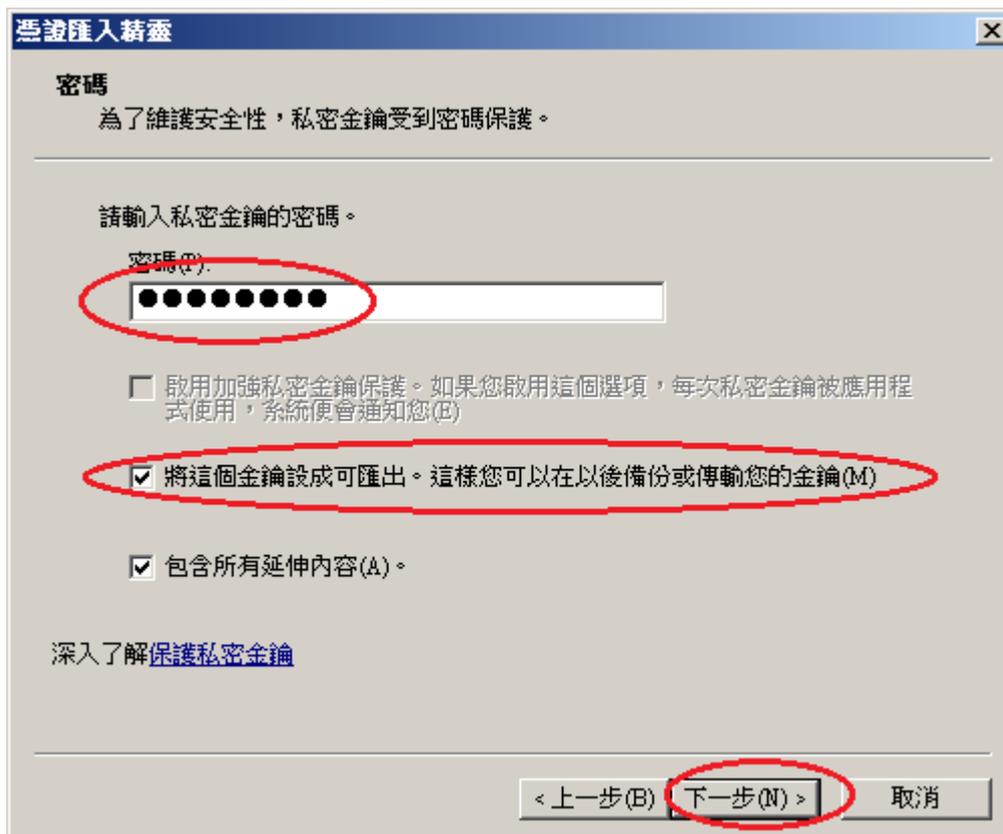
4. 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

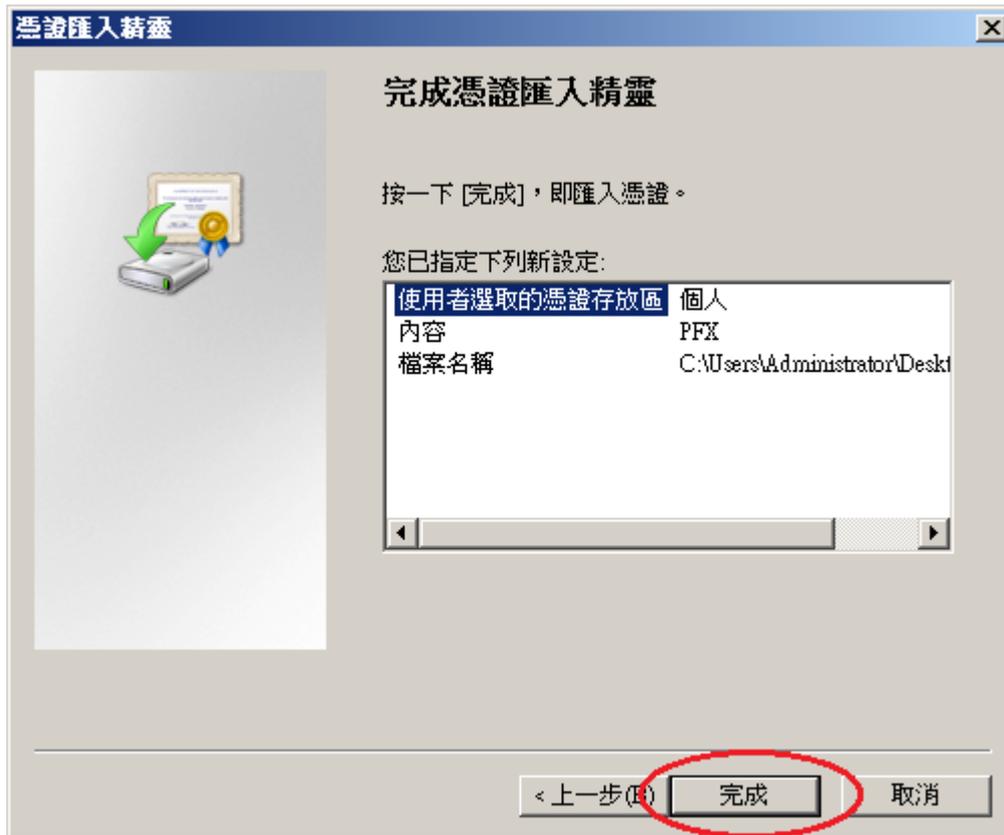


5. 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

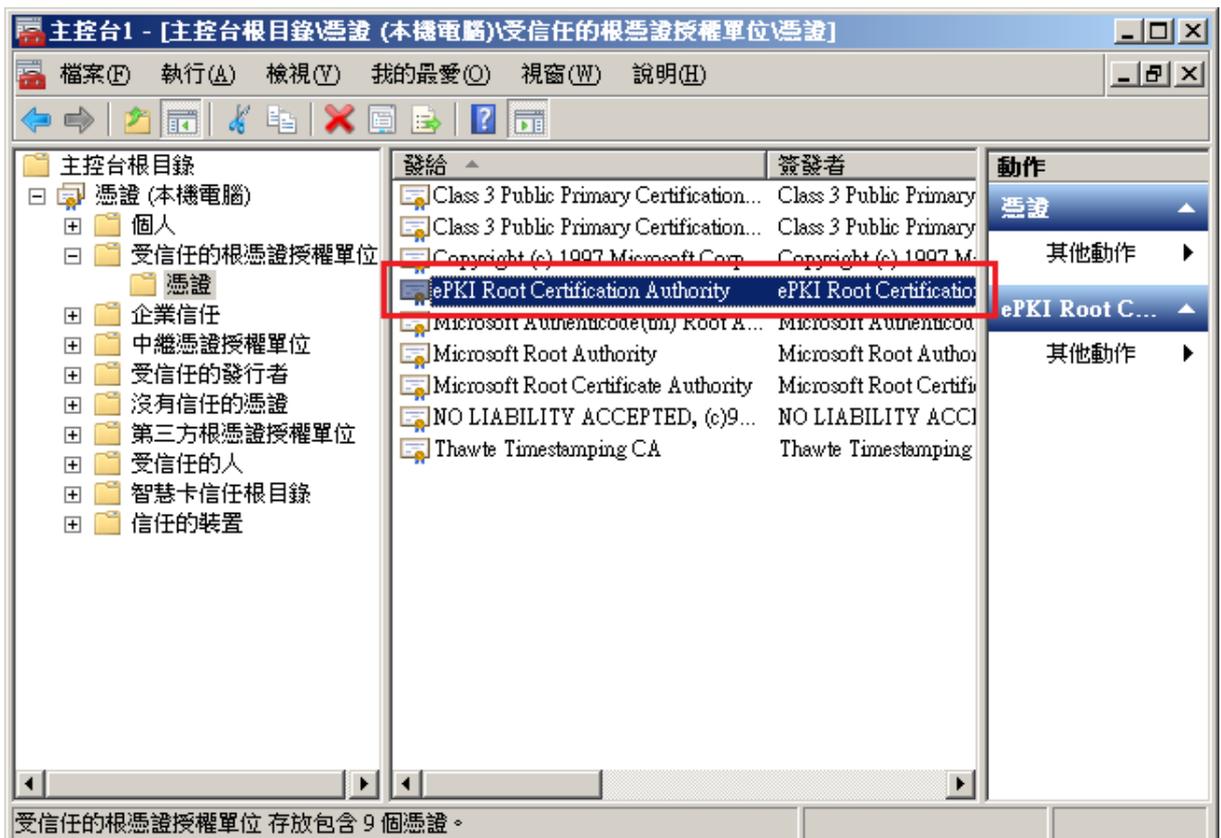
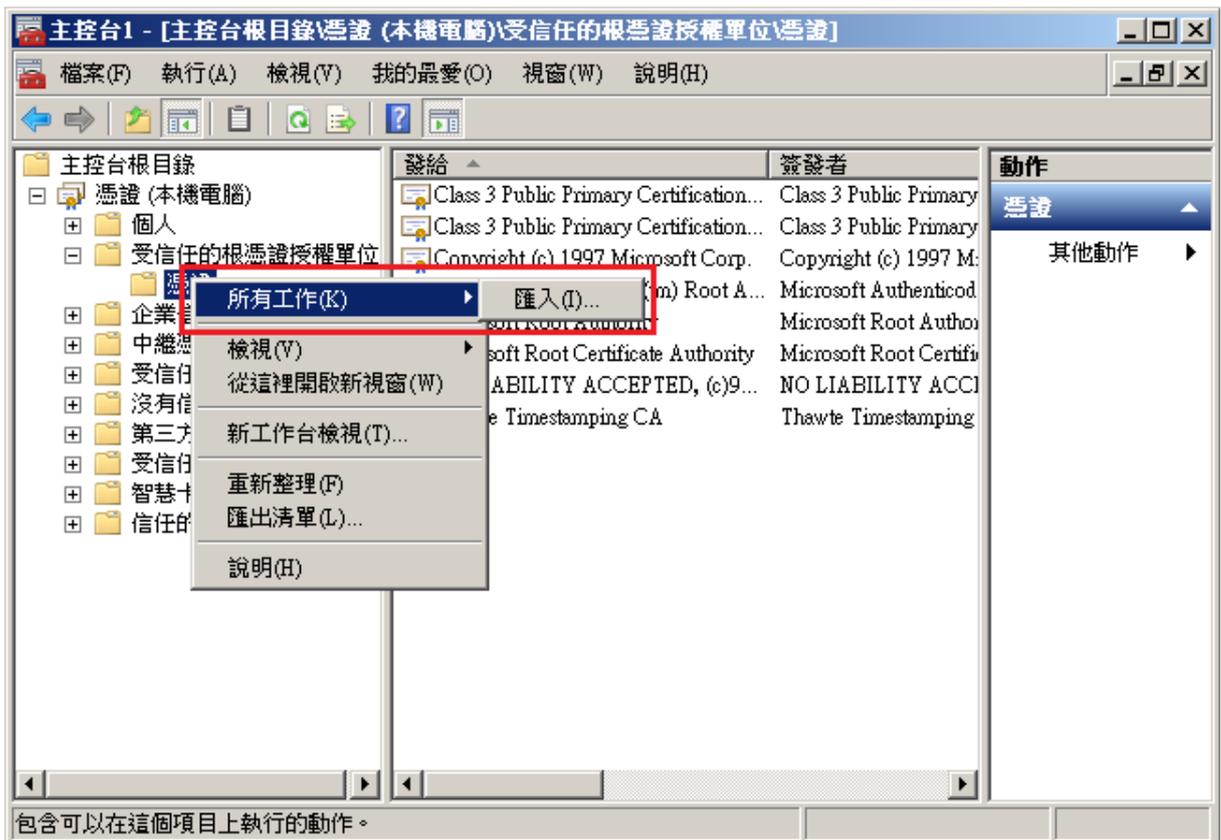


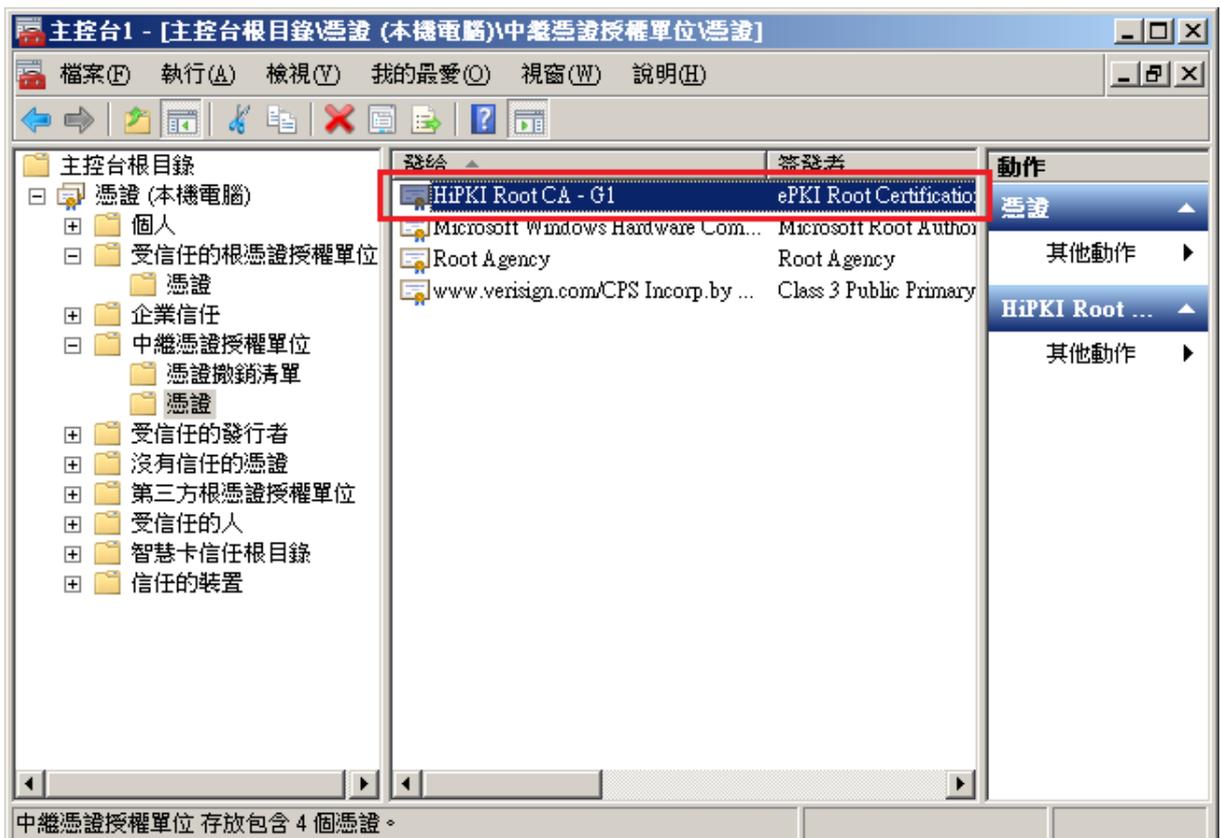
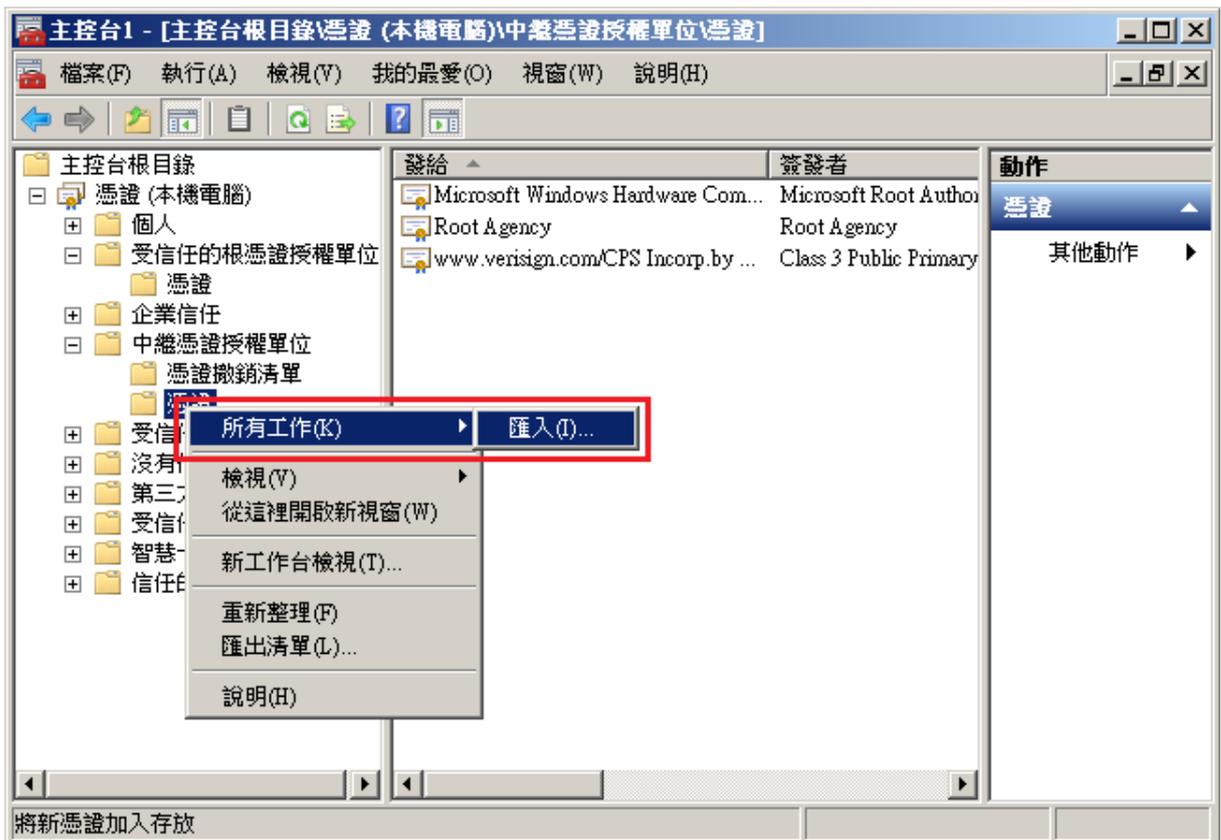
輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。

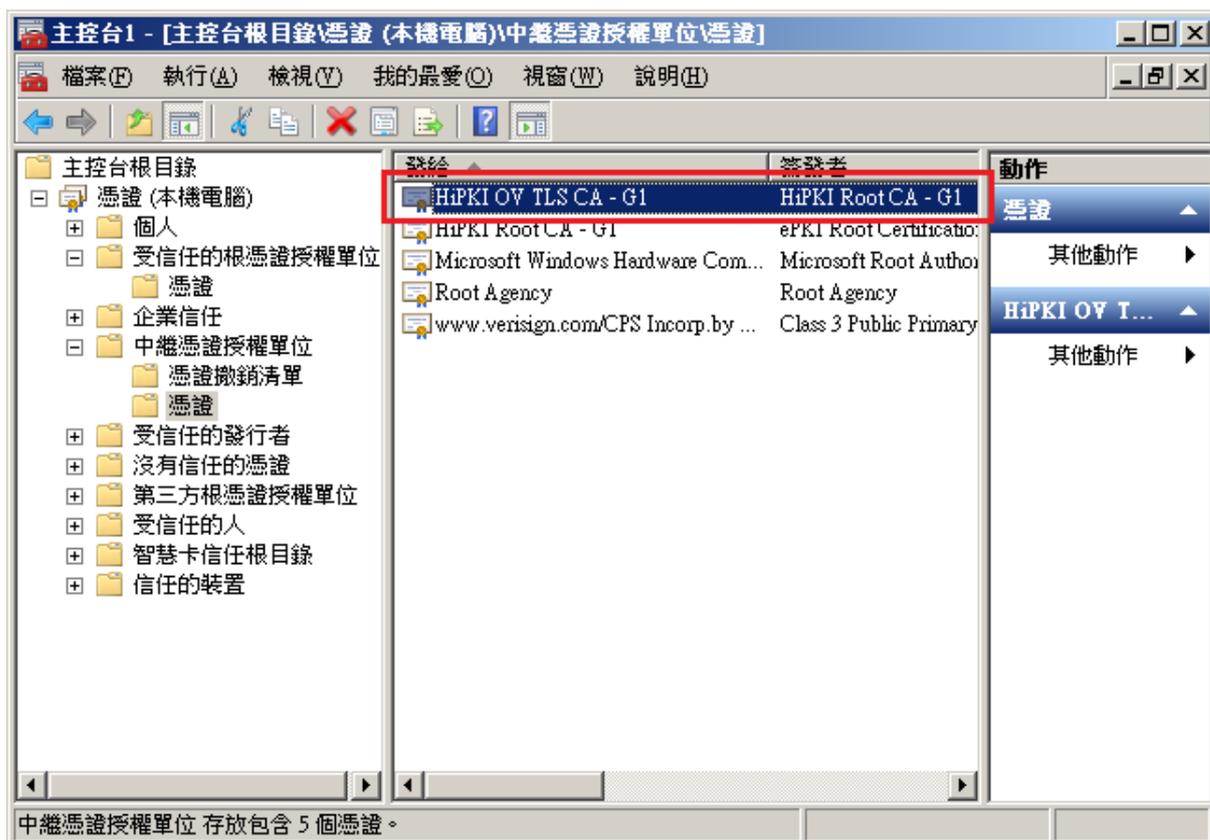




6. 於「信任的根憑證授權單位」匯入 eCA 憑證
於「中繼憑證授權單位」匯入 eCA to HRCA 與 HiPKI OV TLS CA 憑證。
eCA 憑證：
https://eca.hinet.net/download/ROOTeCA_64.crt
eCA to HRCA 憑證：
<https://eca.hinet.net/download/eCA1-to-HRCA1.crt>
HiPKI OV TLS CA 憑證：
https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

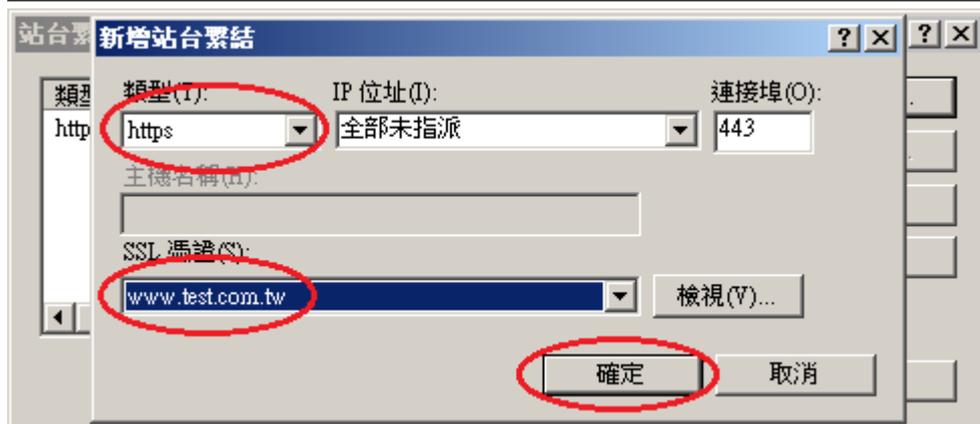






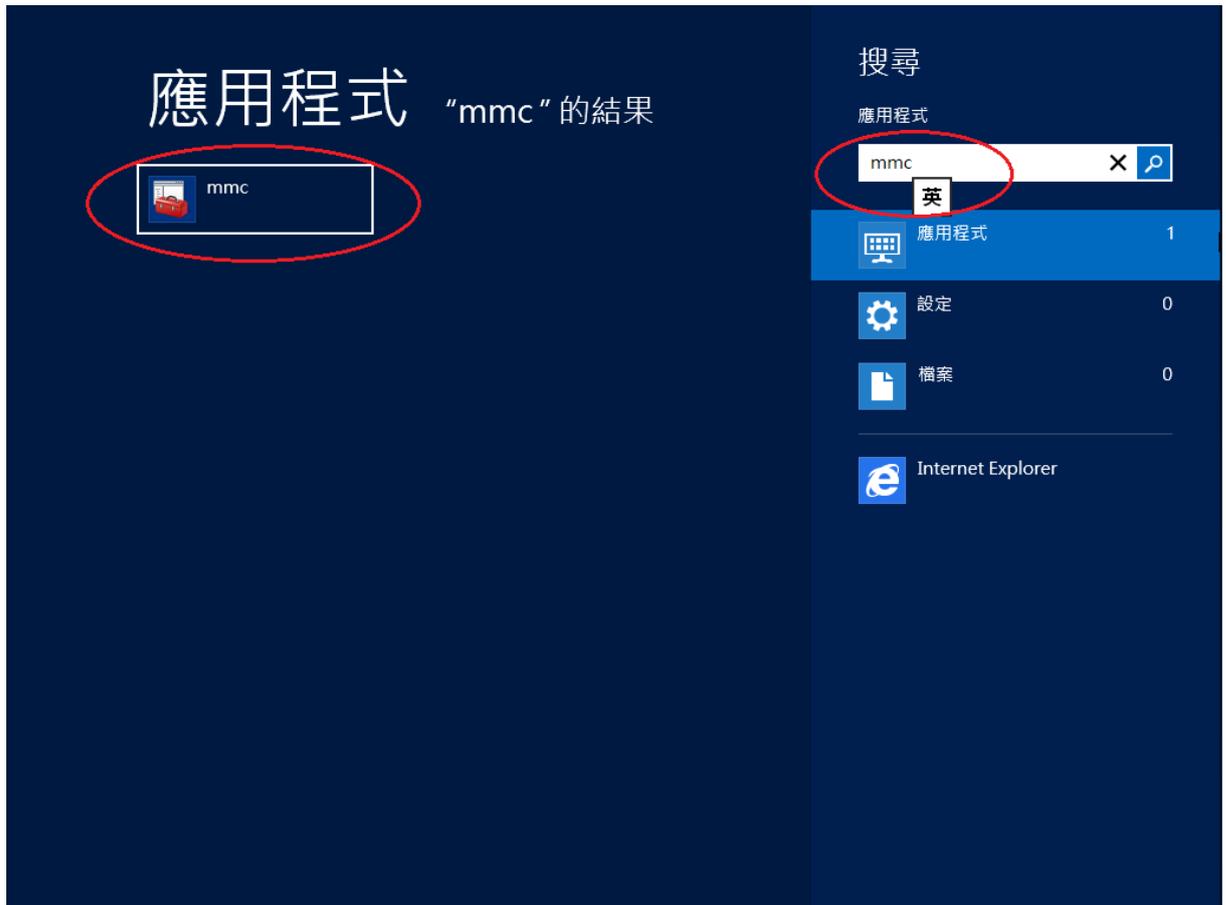
- 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。



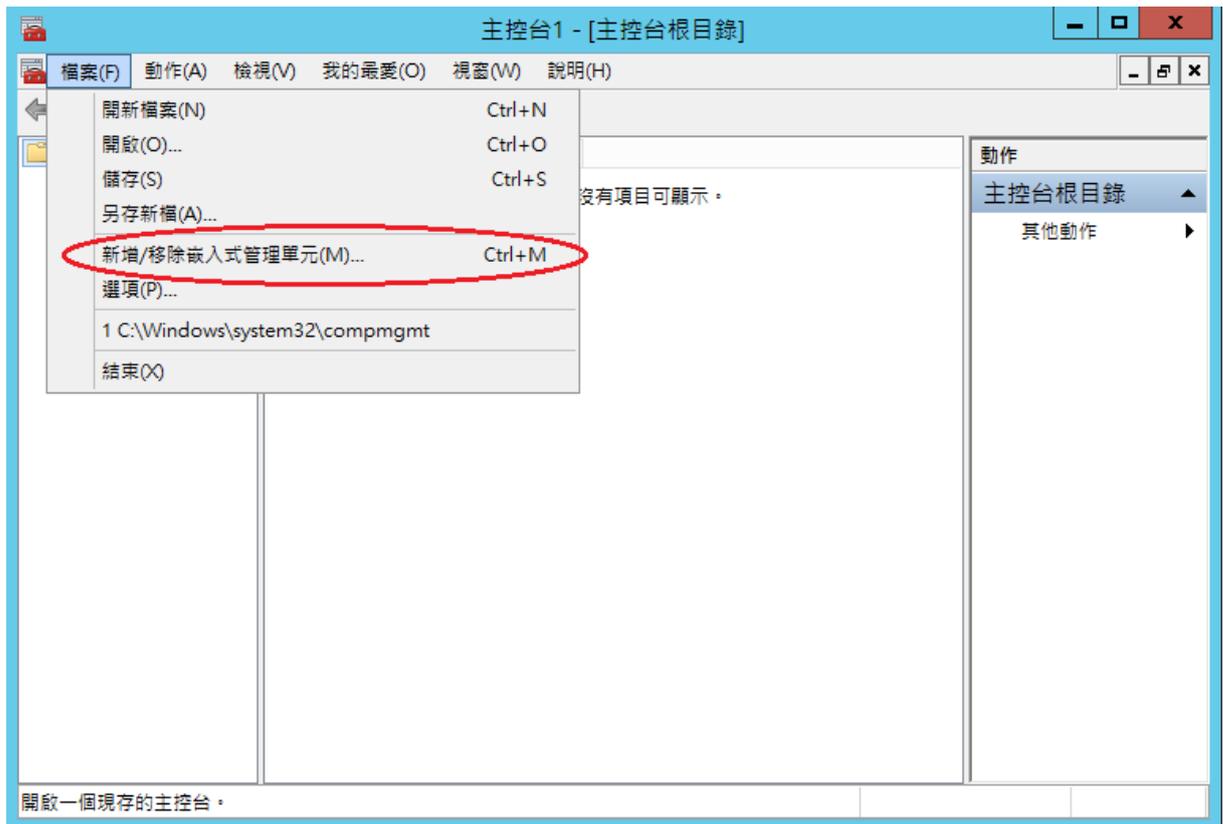


8. 以 https 連線，測試 https 網頁是否正常。

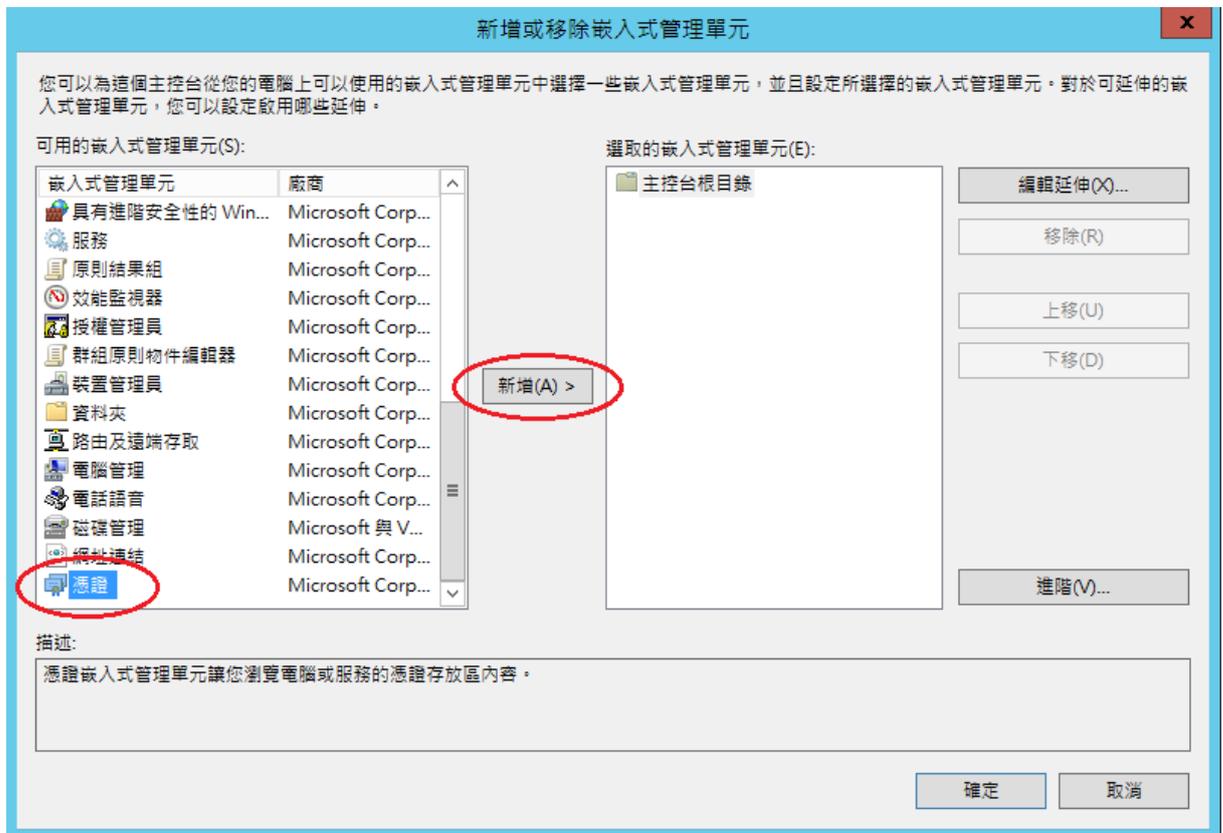
1. 「開始」→「輸入 mmc」，按下「Enter」。



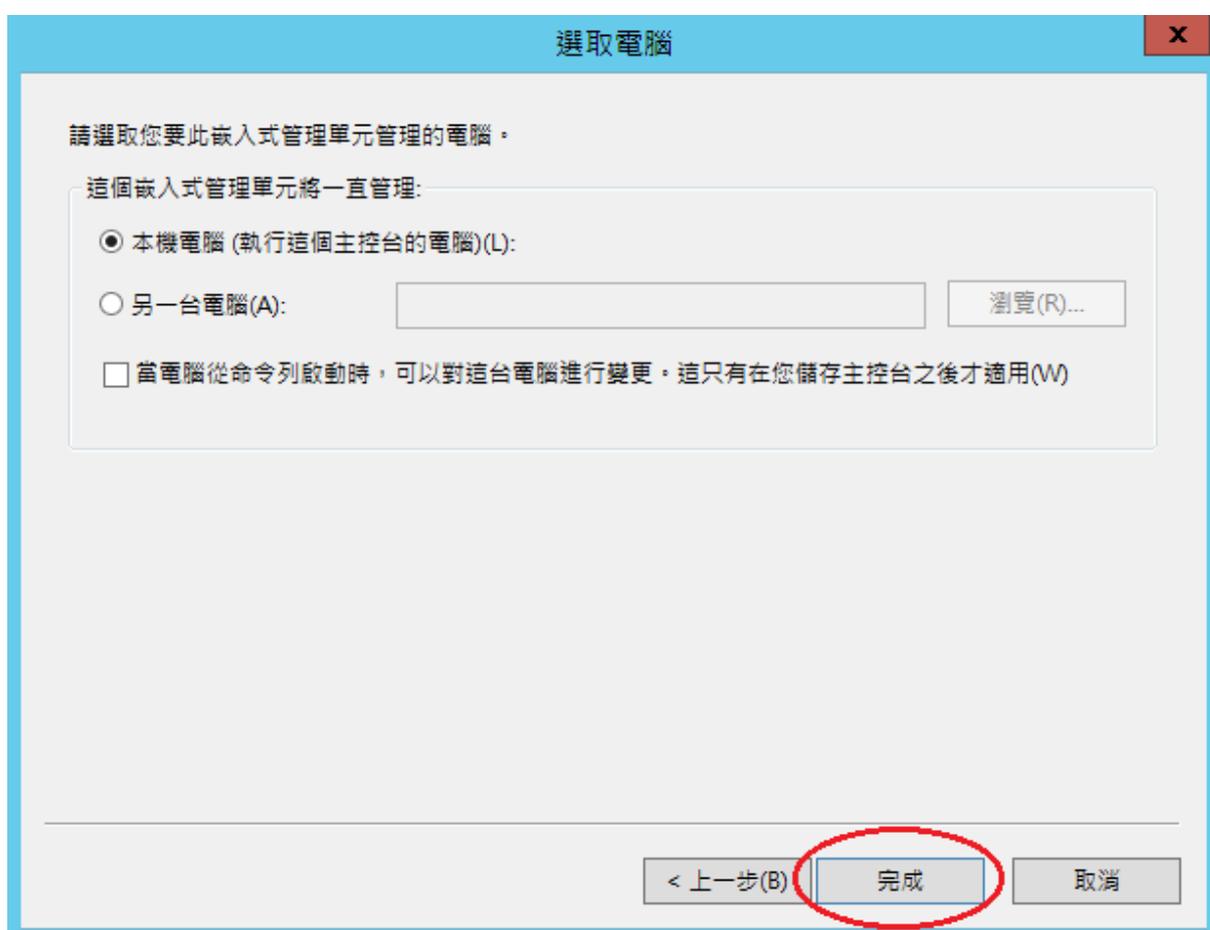
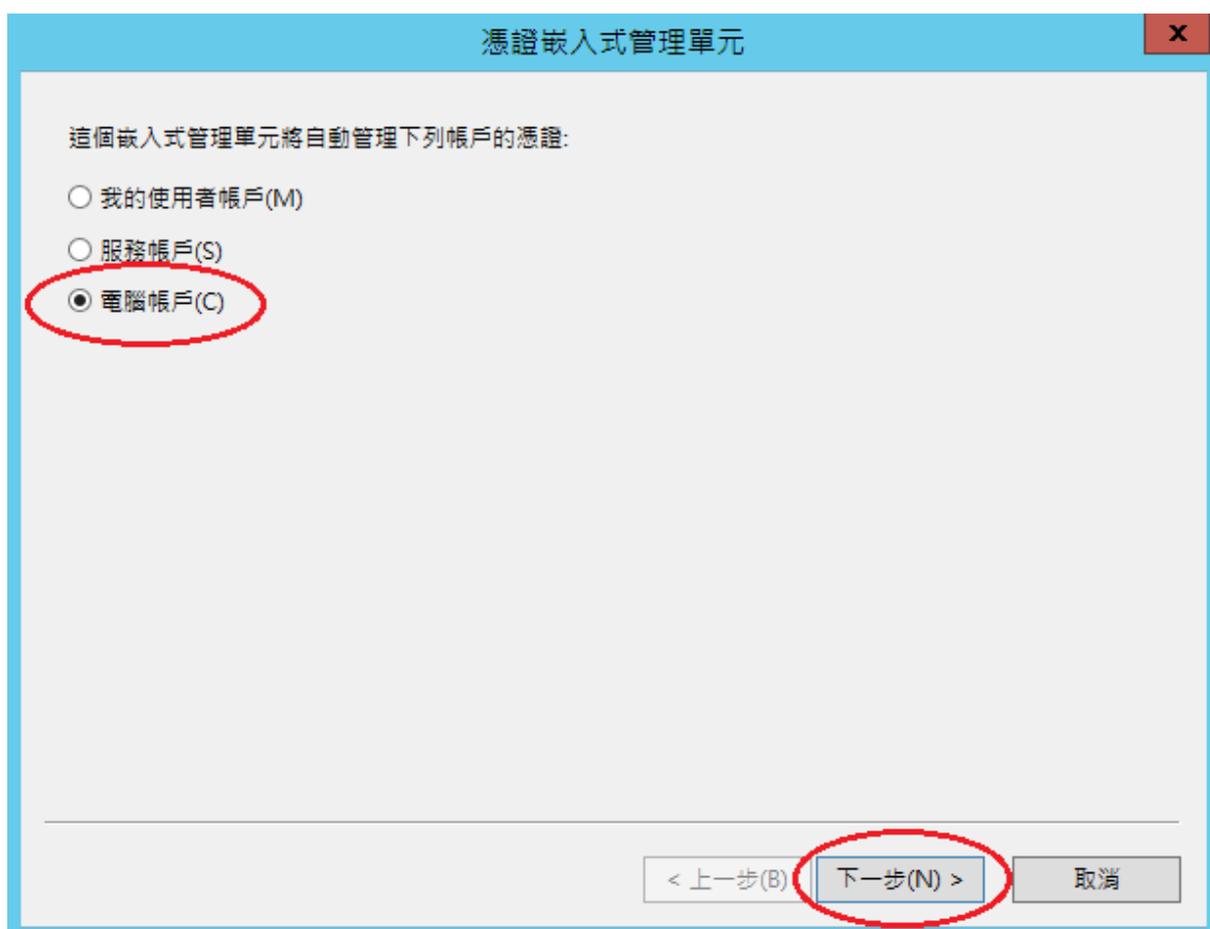
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。



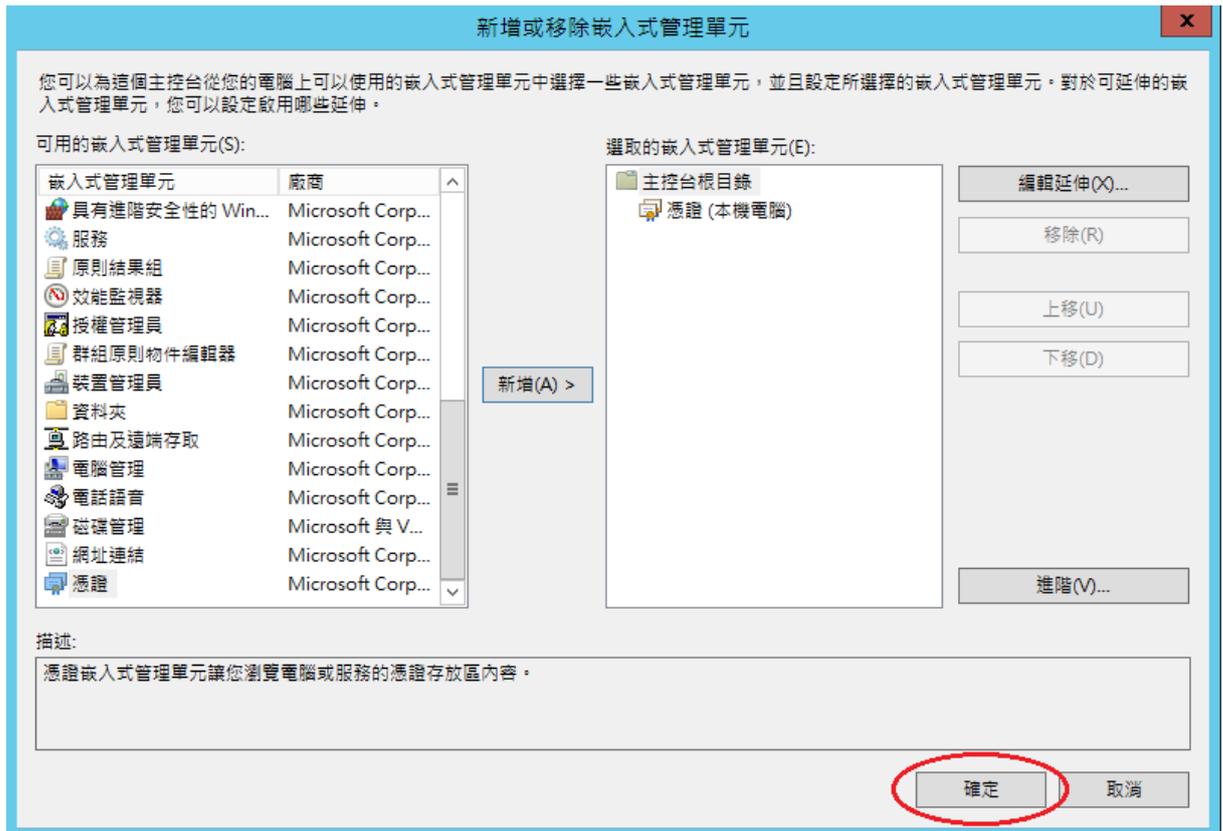
3. 點選「憑證」→「新增」



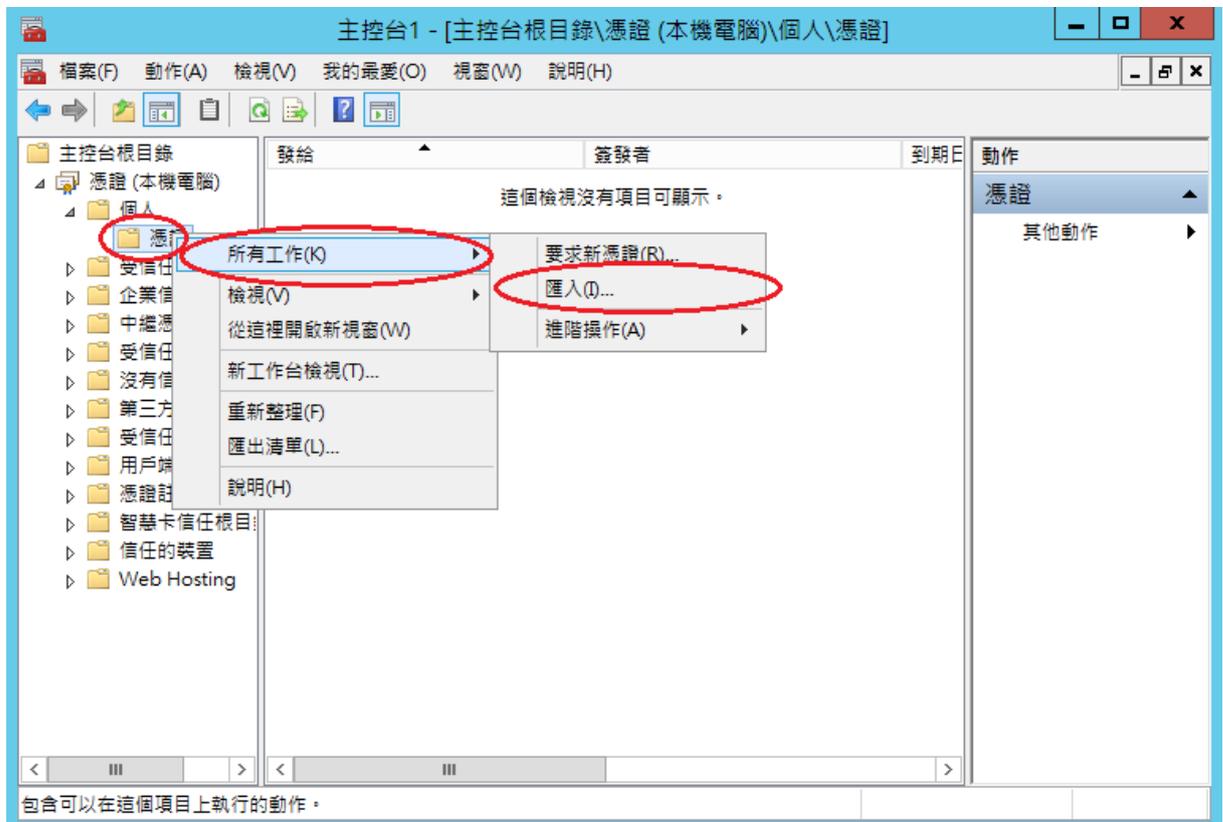
「電腦帳戶」→「下一步」→「完成」。



「確定」。



- 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」



- 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

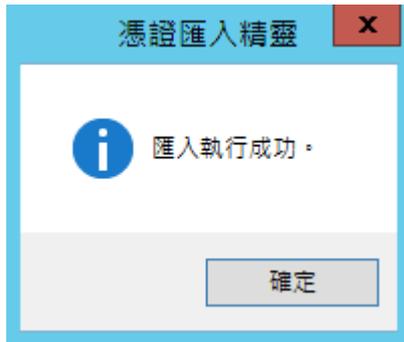




輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。







6. 於「信任的根憑證授權單位」匯入 eCA 憑證
 於「中繼憑證授權單位」匯入 eCA to HRCA 與 HiPKI OV TLS CA 憑證。
 eCA 憑證：

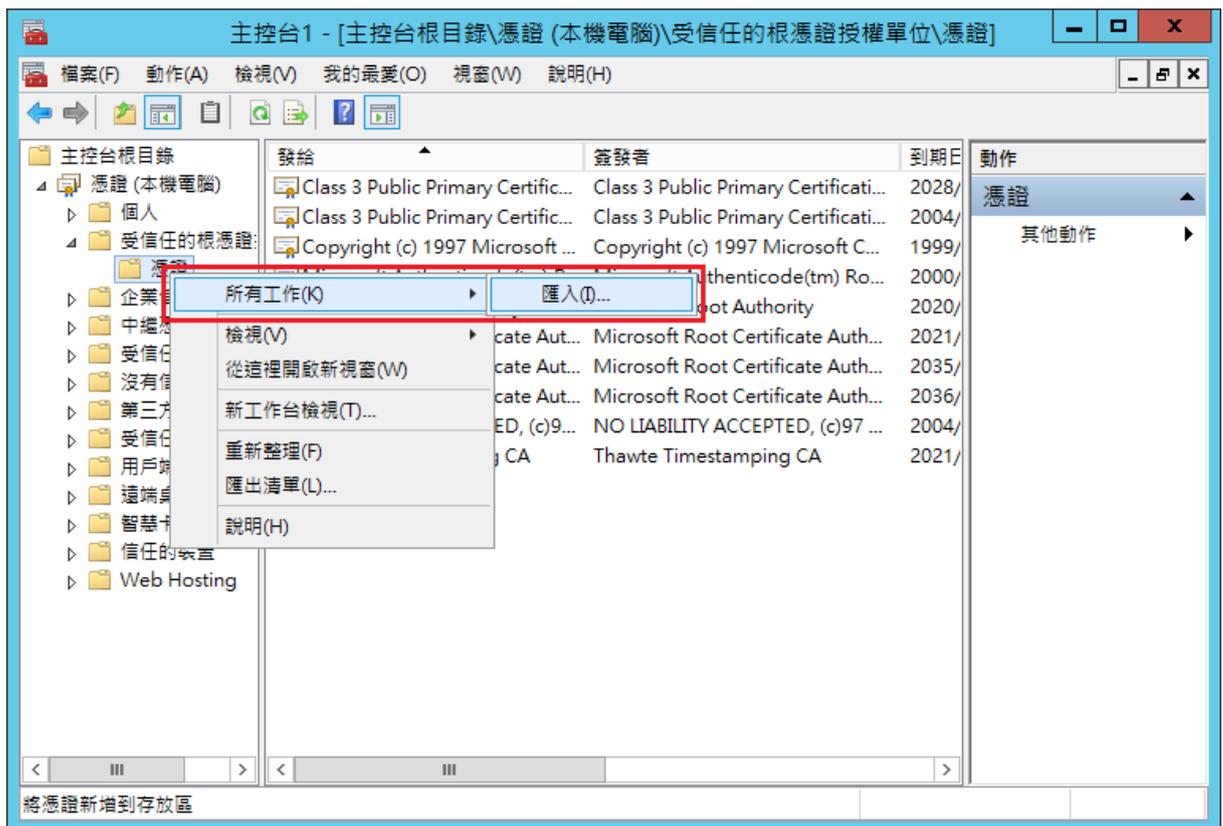
https://eca.hinet.net/download/ROOTeCA_64.crt

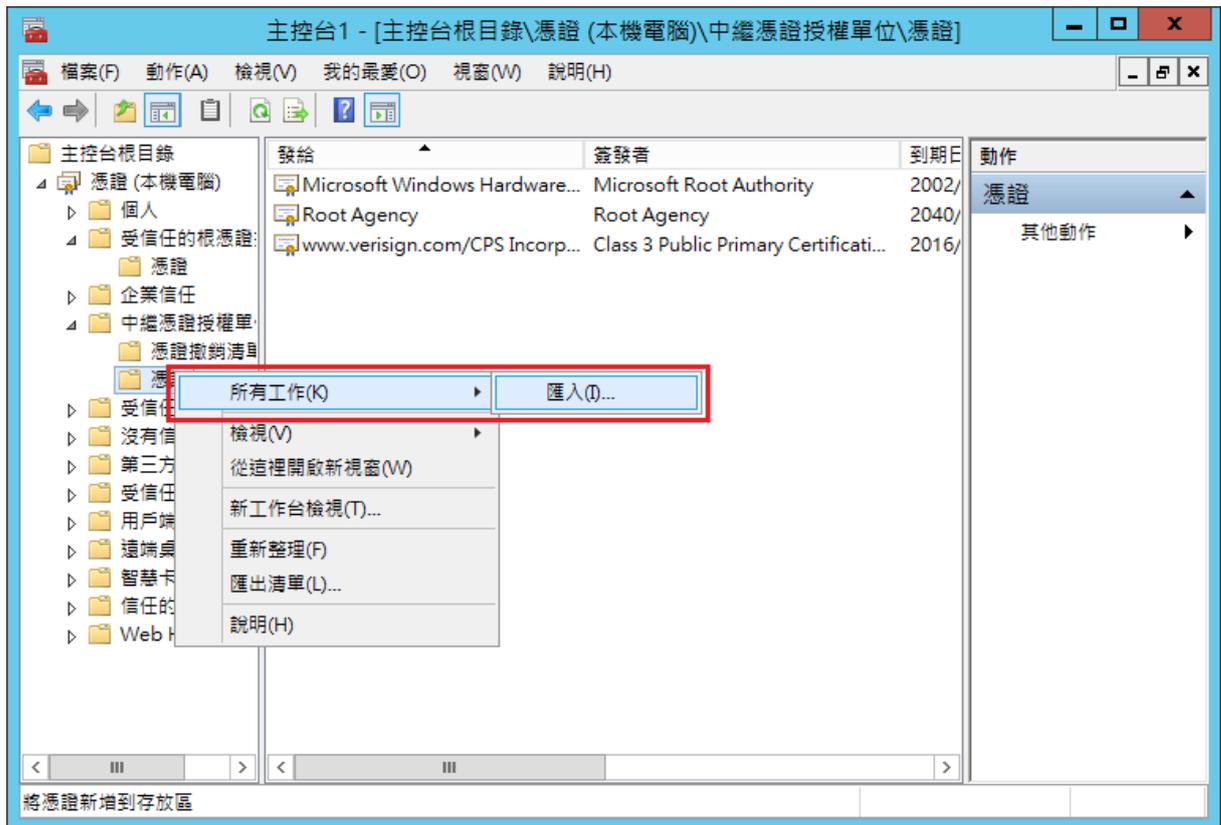
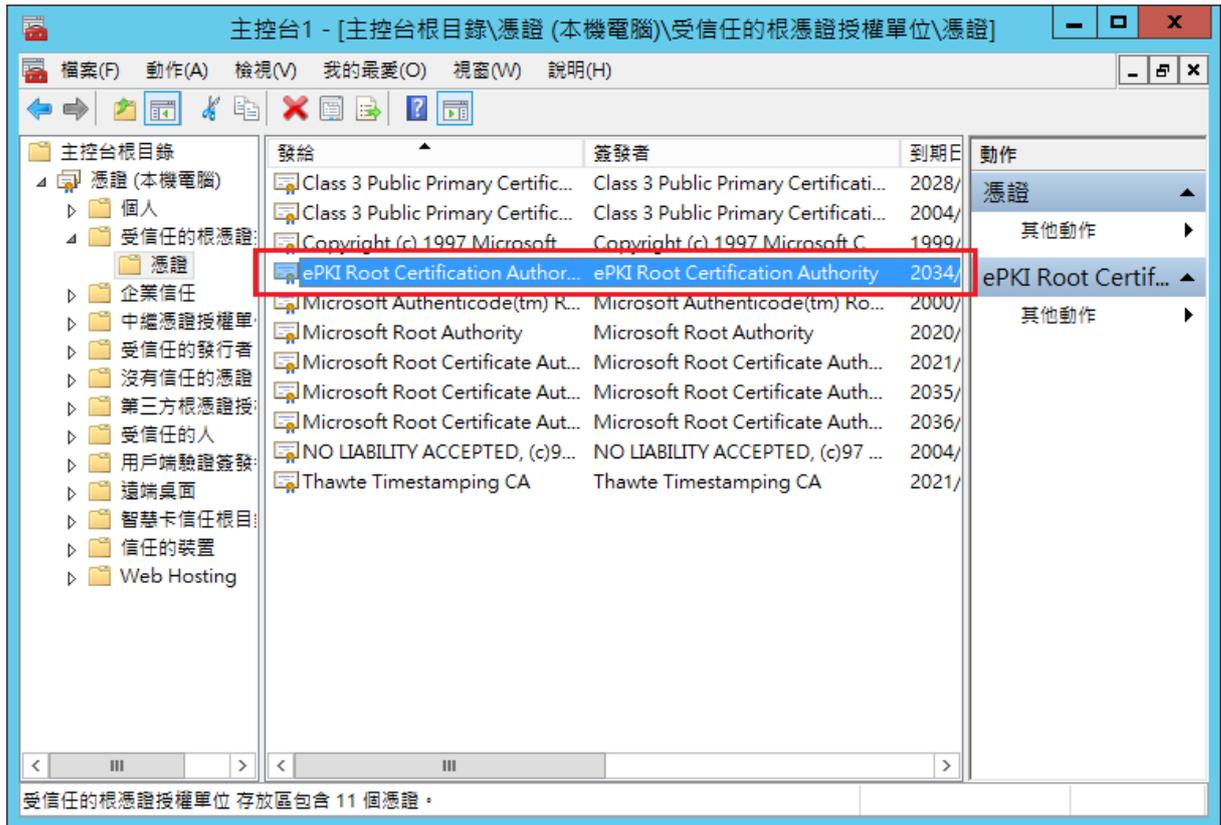
eCA to HRCA 憑證：

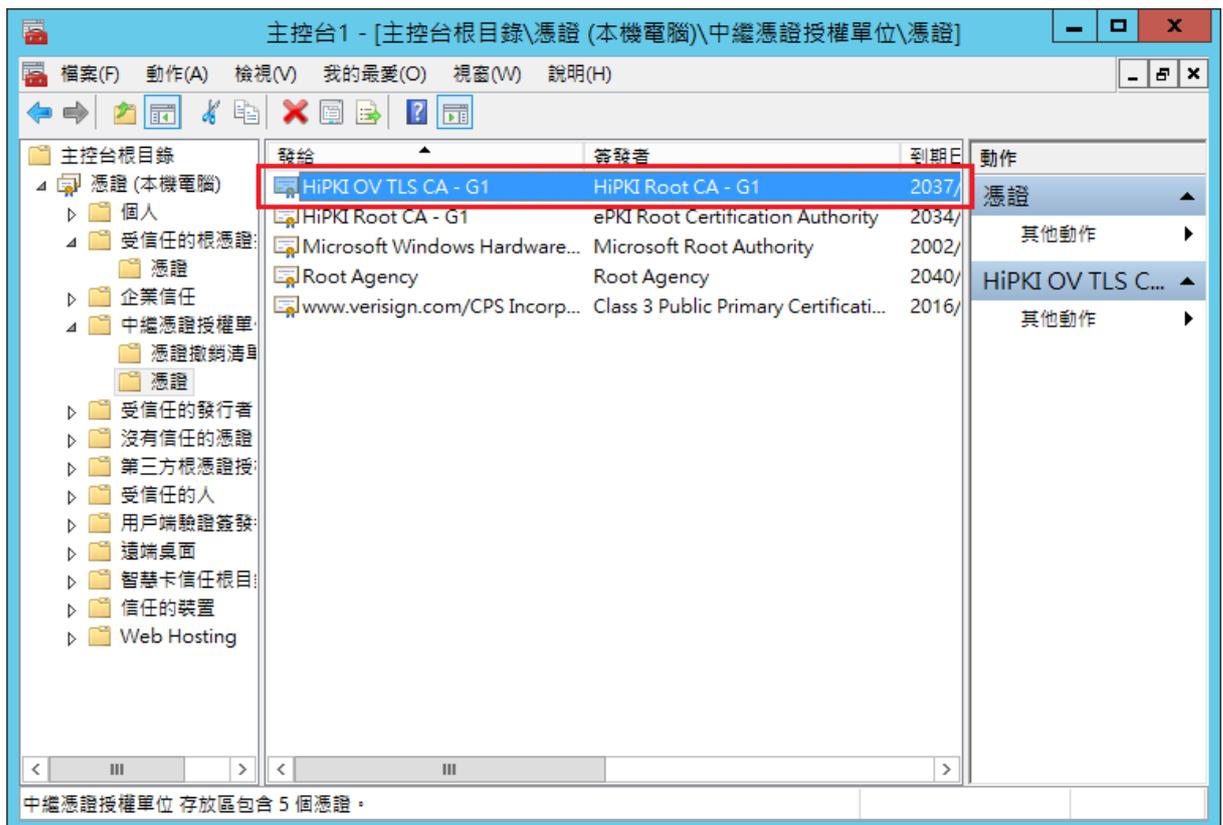
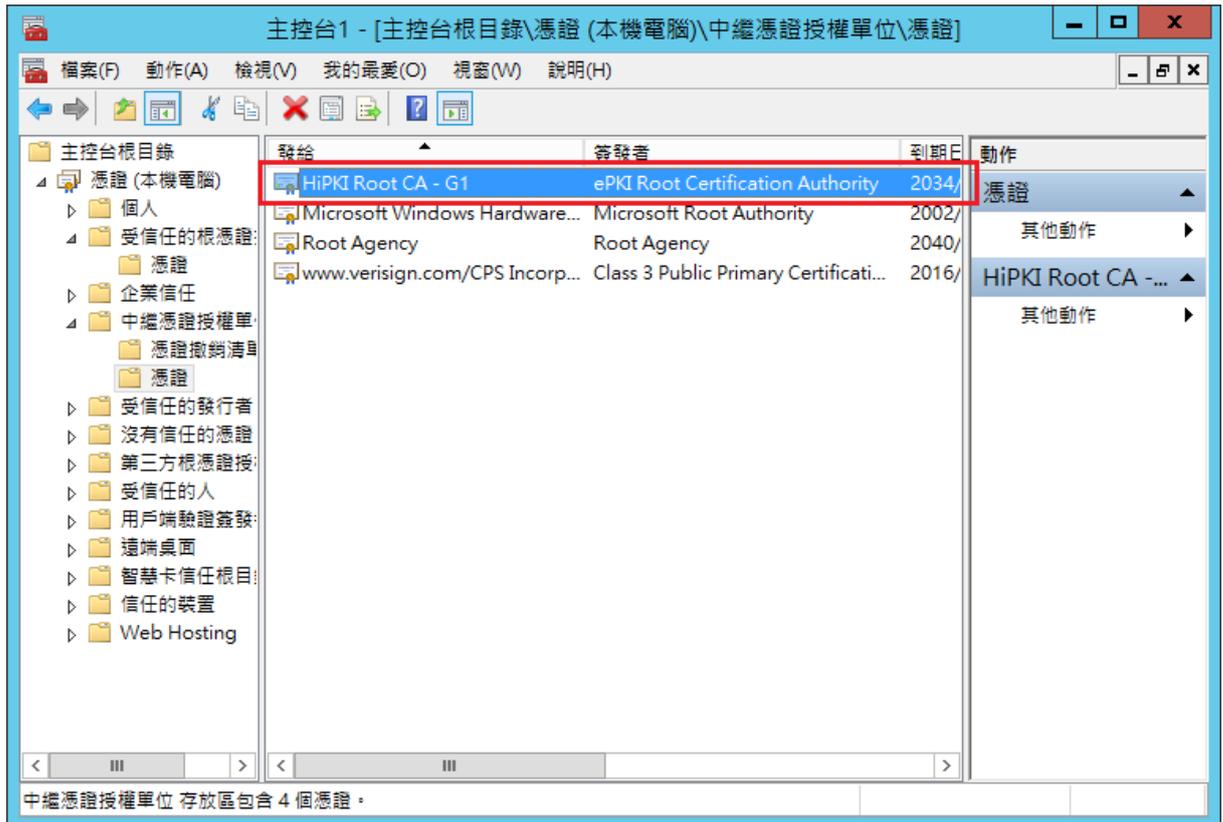
<https://eca.hinet.net/download/eCA1-to-HRCA1.crt>

HiPKI OV TLS CA 憑證：

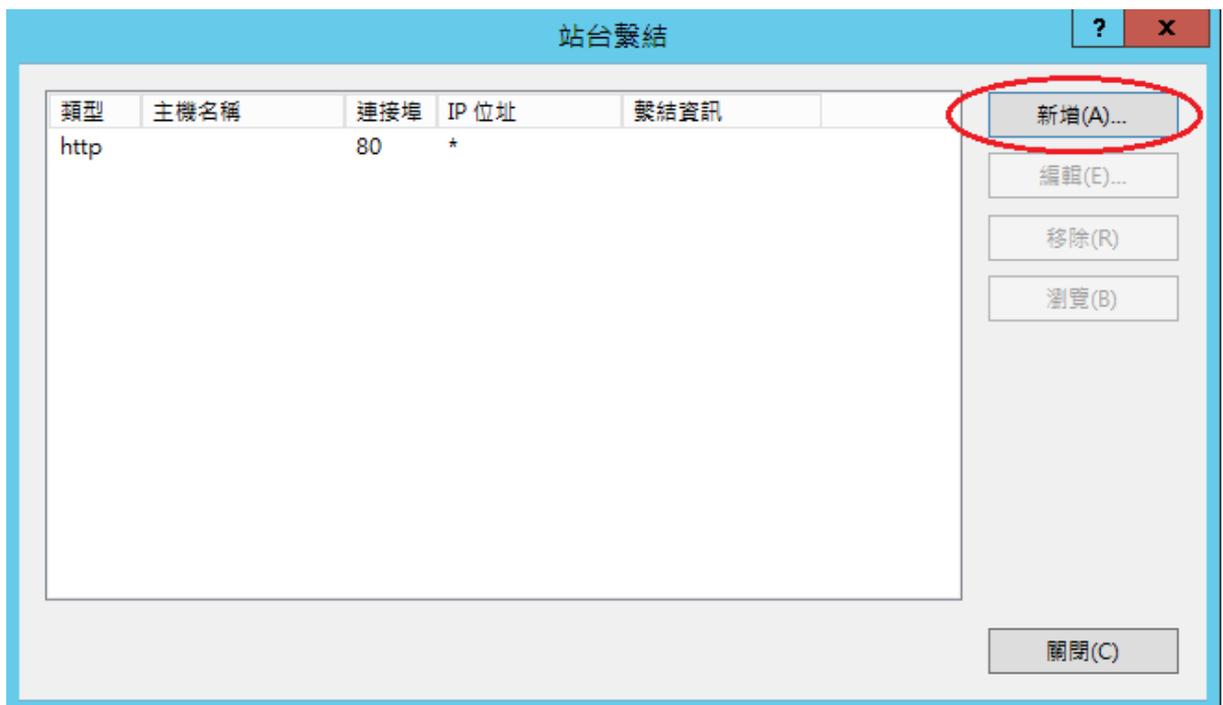
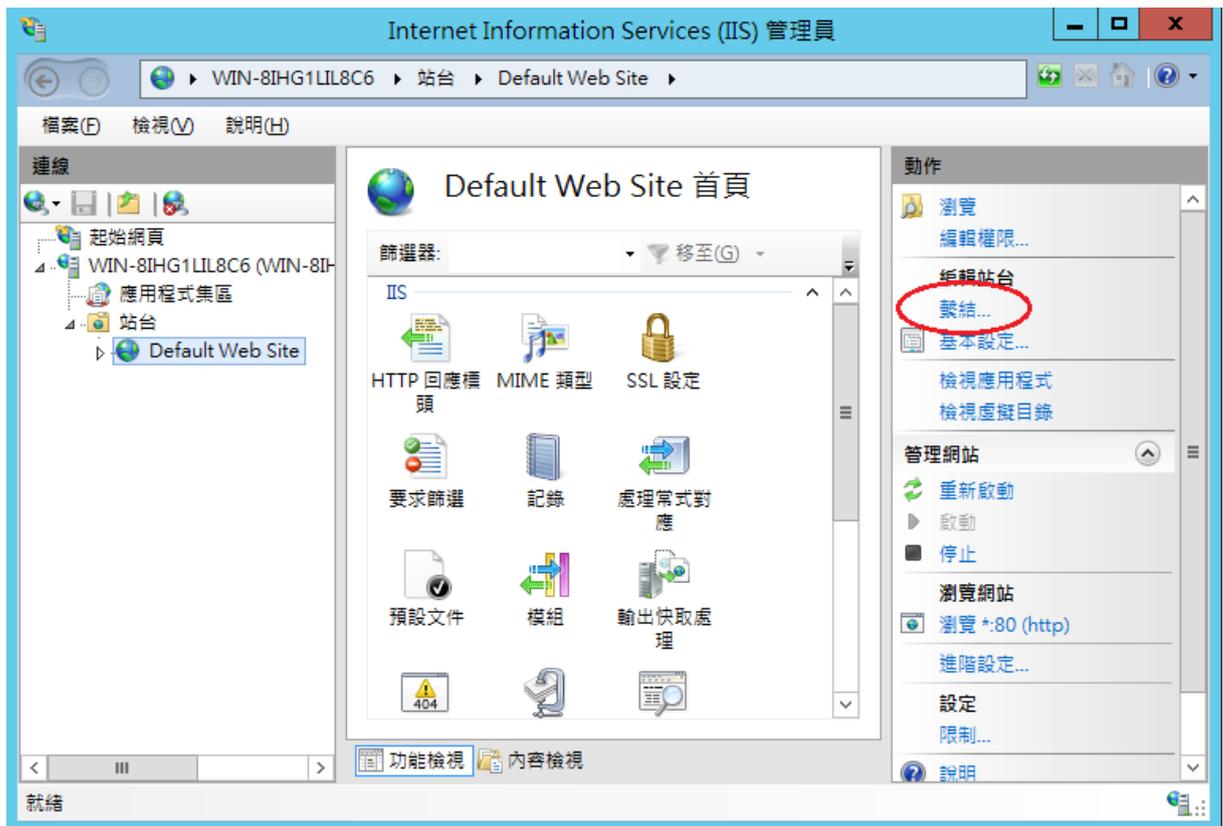
https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt







- 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。



新增站台繫結

類型(T): **https** IP 位址(I): 全部未指派 連接埠(O): 443

主機名稱(H):

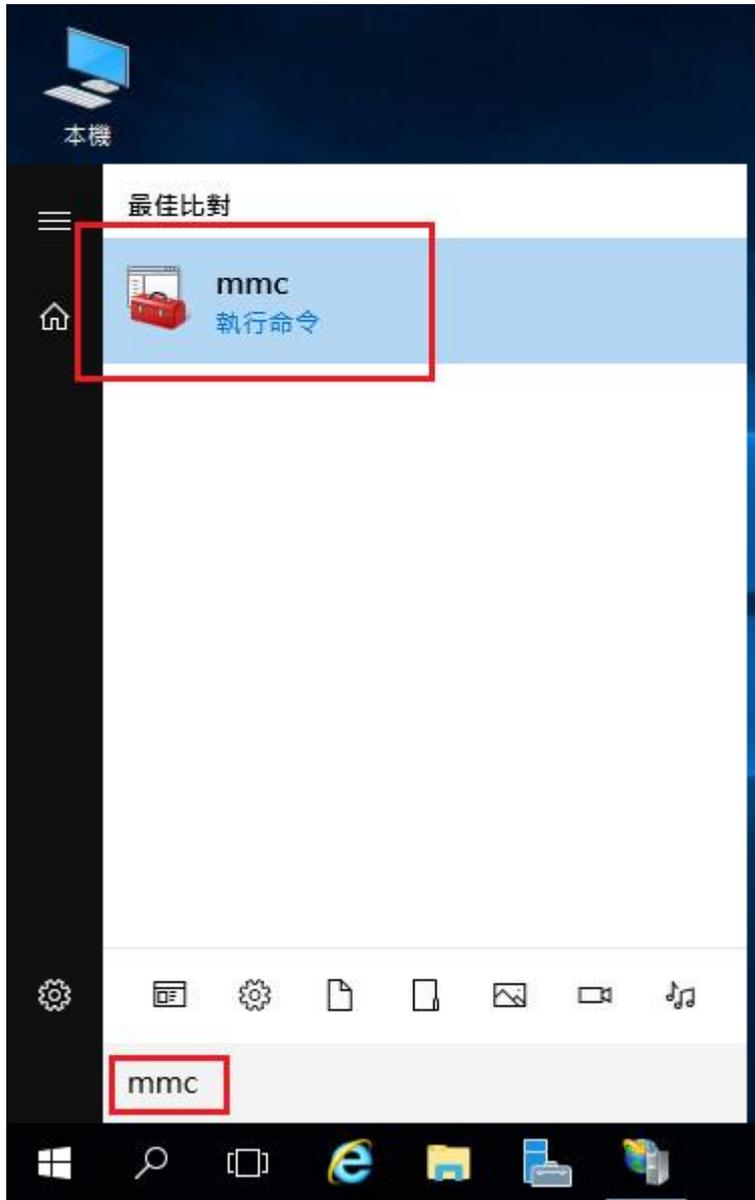
需要伺服器名稱指示(N)

SSL 憑證(S): **www.test.com.tw** 選取(L)... 檢視(V)...

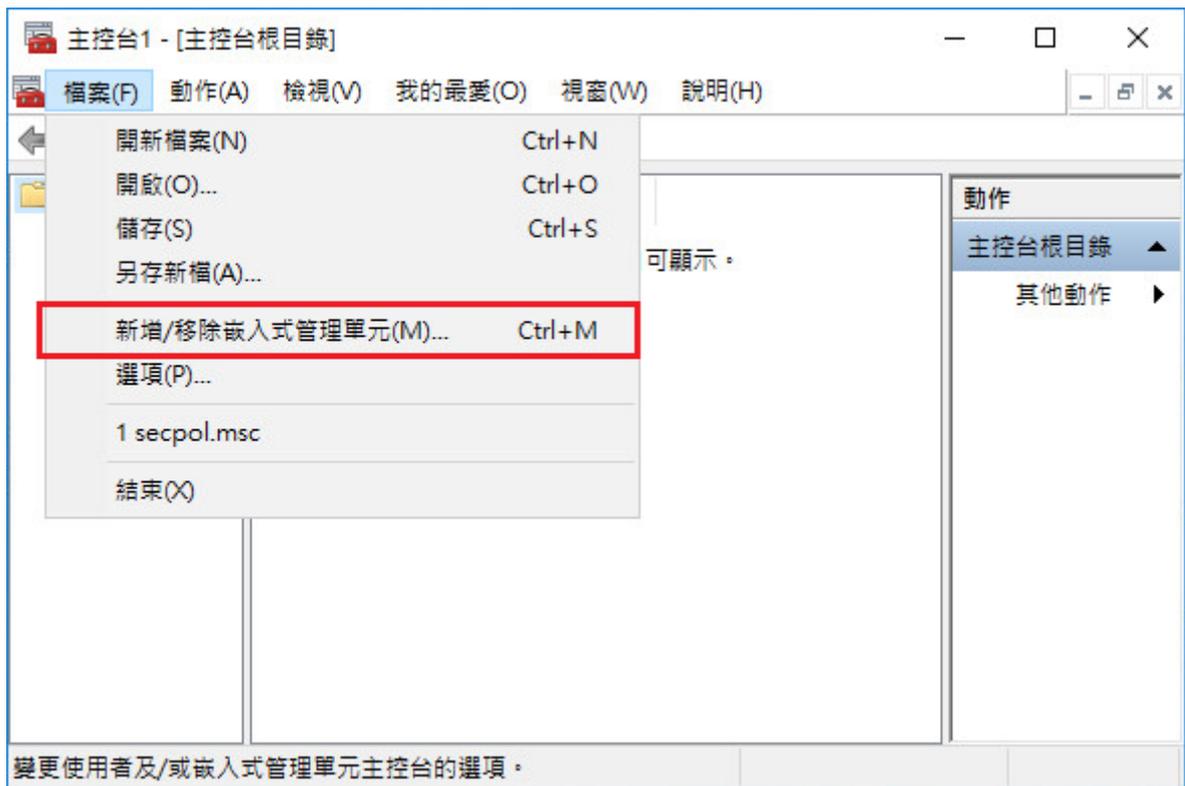
確定 取消

- 以 https 連線，測試 https 網頁是否正常。

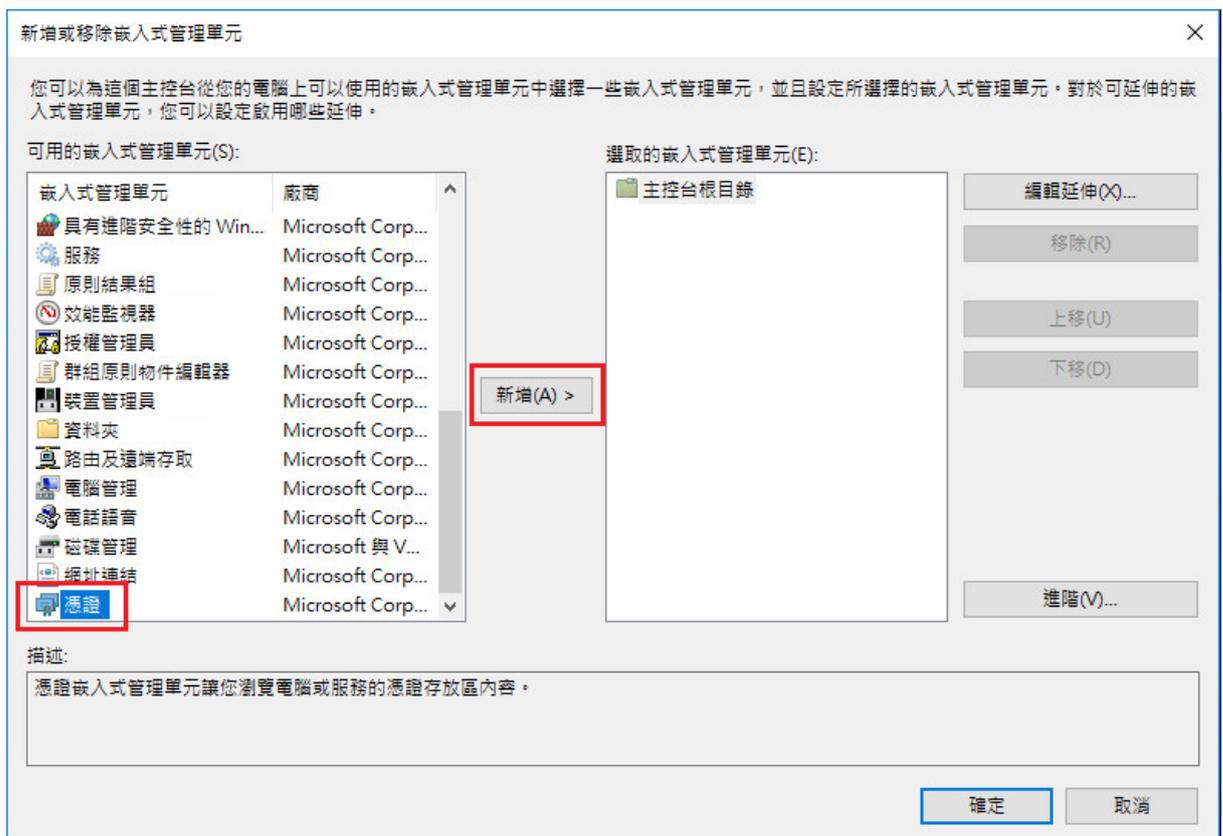
1. 「開始」→「輸入 mmc」，按下「Enter」。



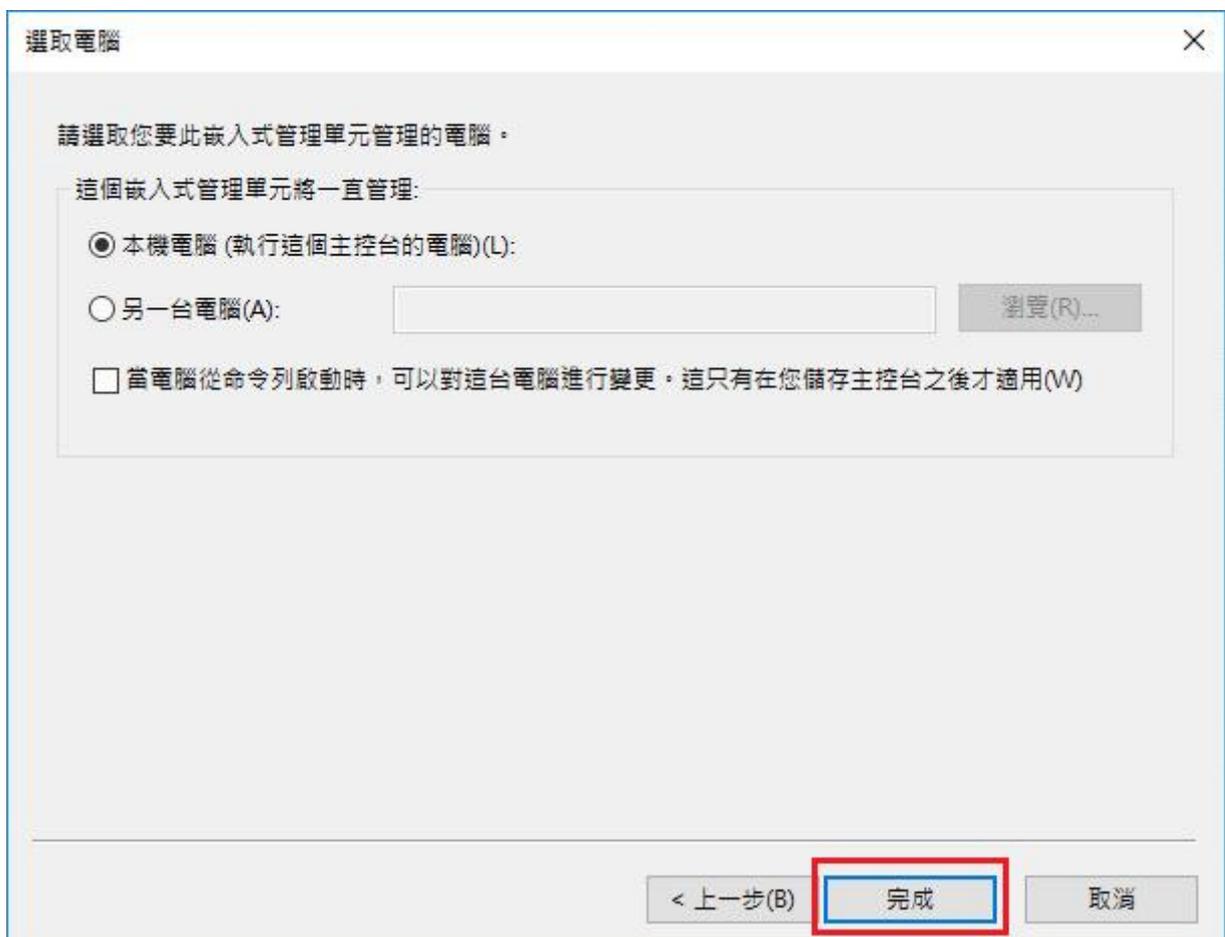
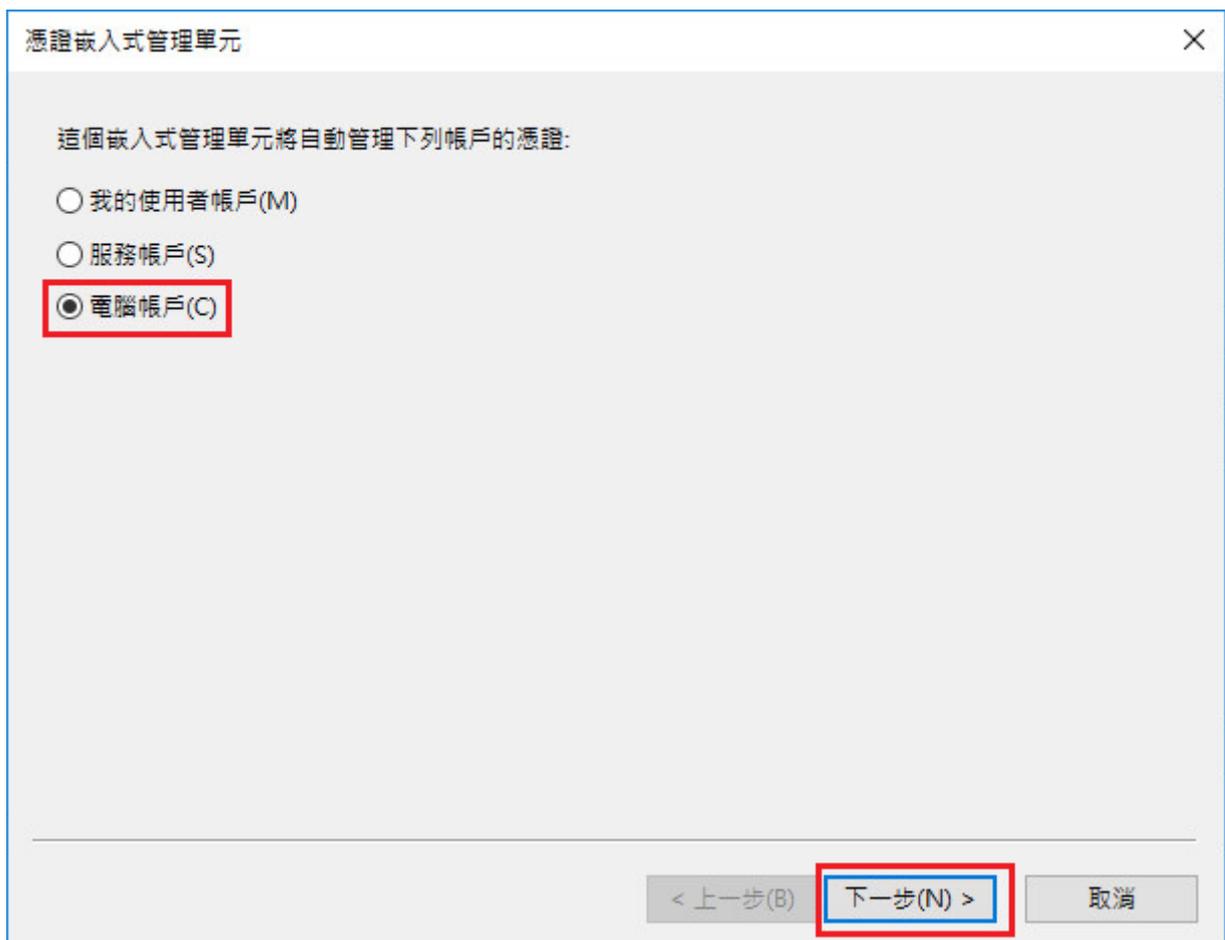
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。



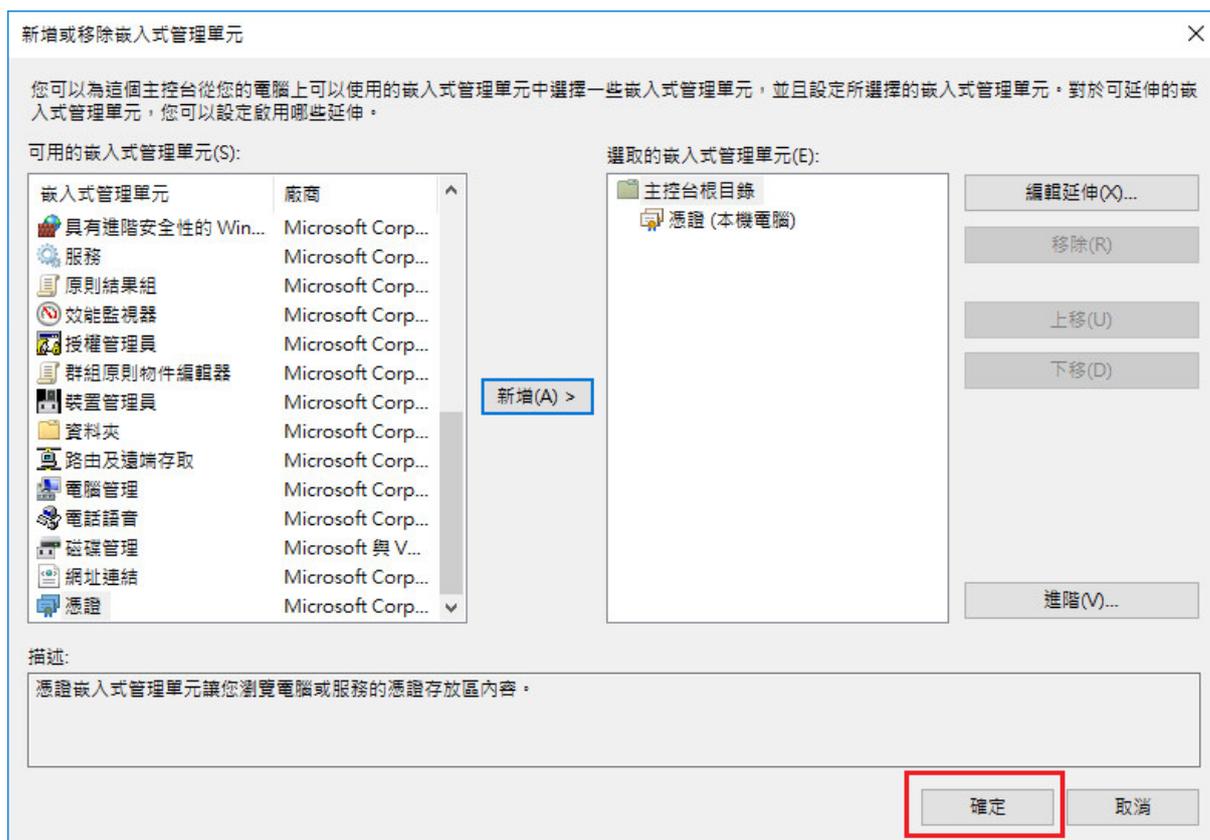
3. 點選「憑證」→「新增」



「電腦帳戶」→「下一步」→「完成」。



「確定」。



4. 於「信任的根憑證授權單位」匯入 eCA 憑證
於「中繼憑證授權單位」匯入 eCA to HRCA 與 HiPKI OV TLS CA 憑證。
eCA 憑證：

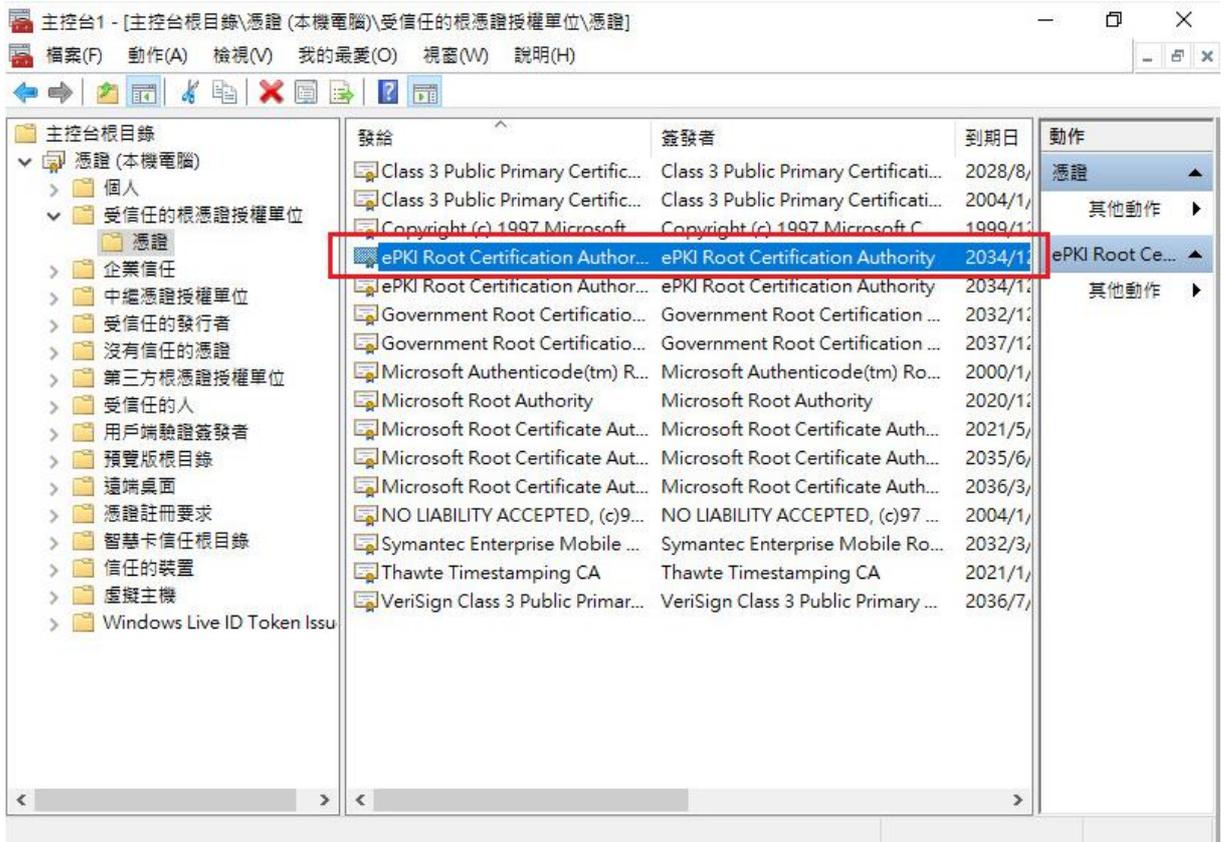
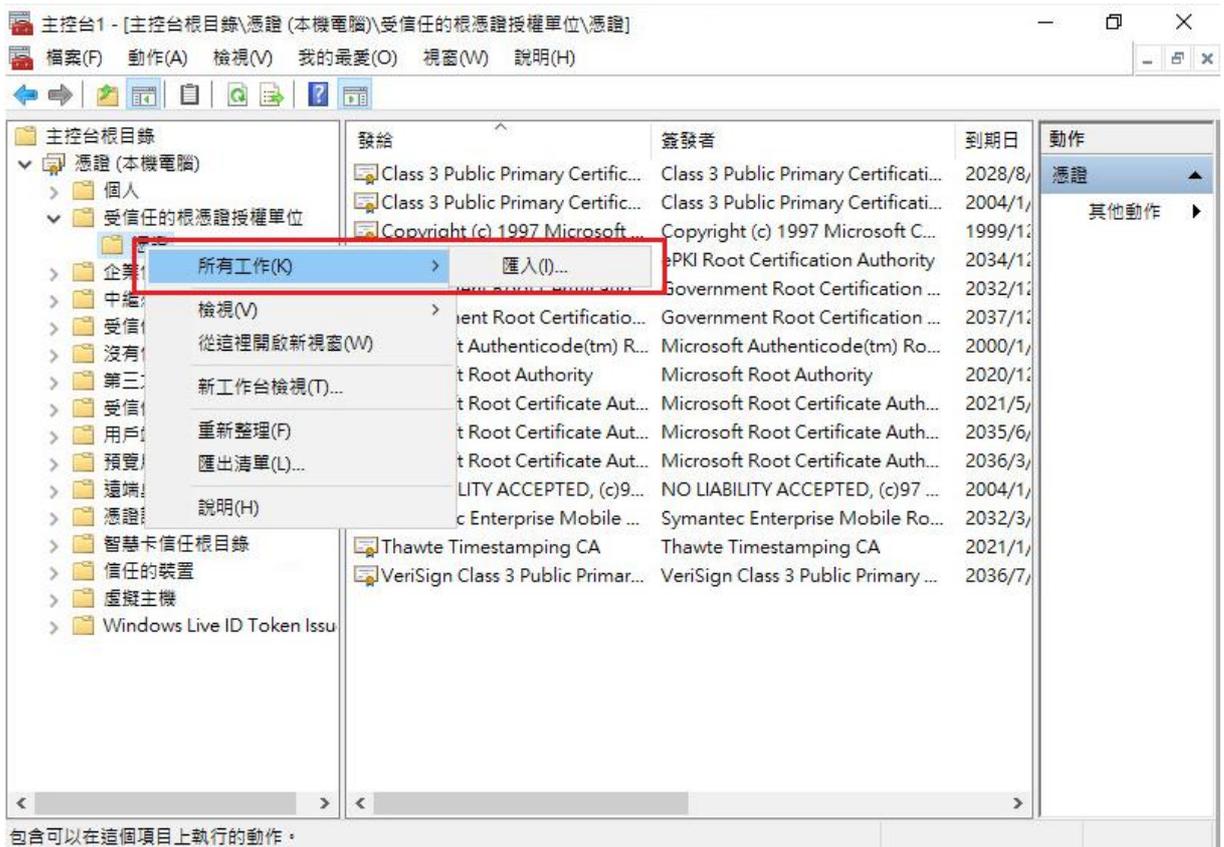
https://eca.hinet.net/download/ROOTeCA_64.crt

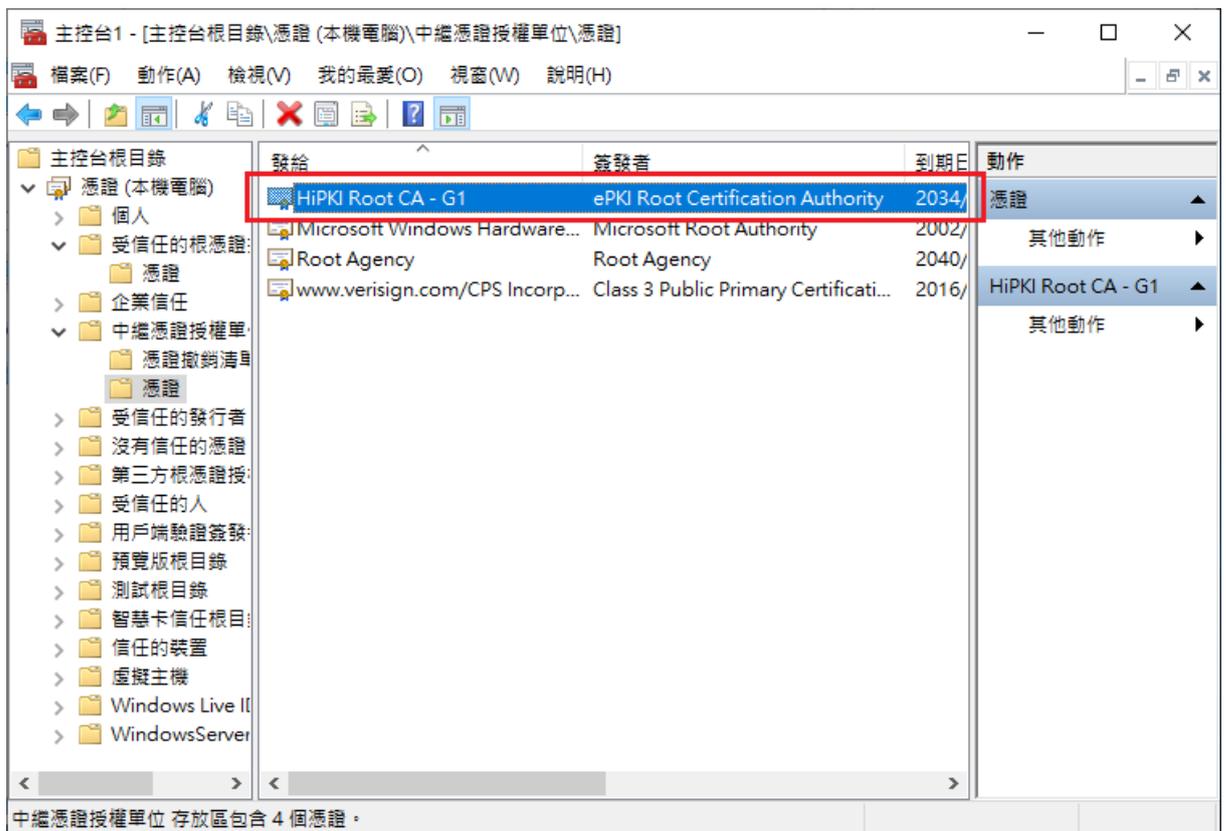
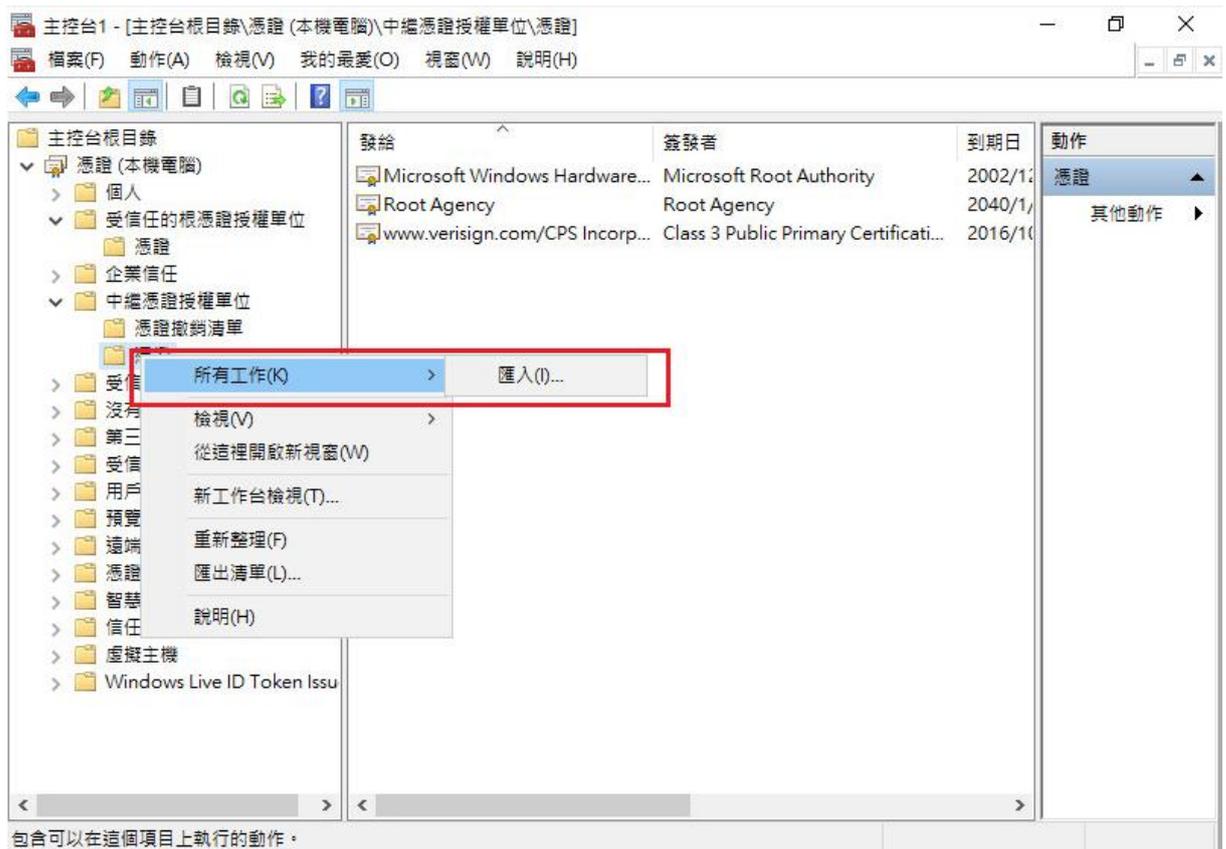
eCA to HRCA 憑證：

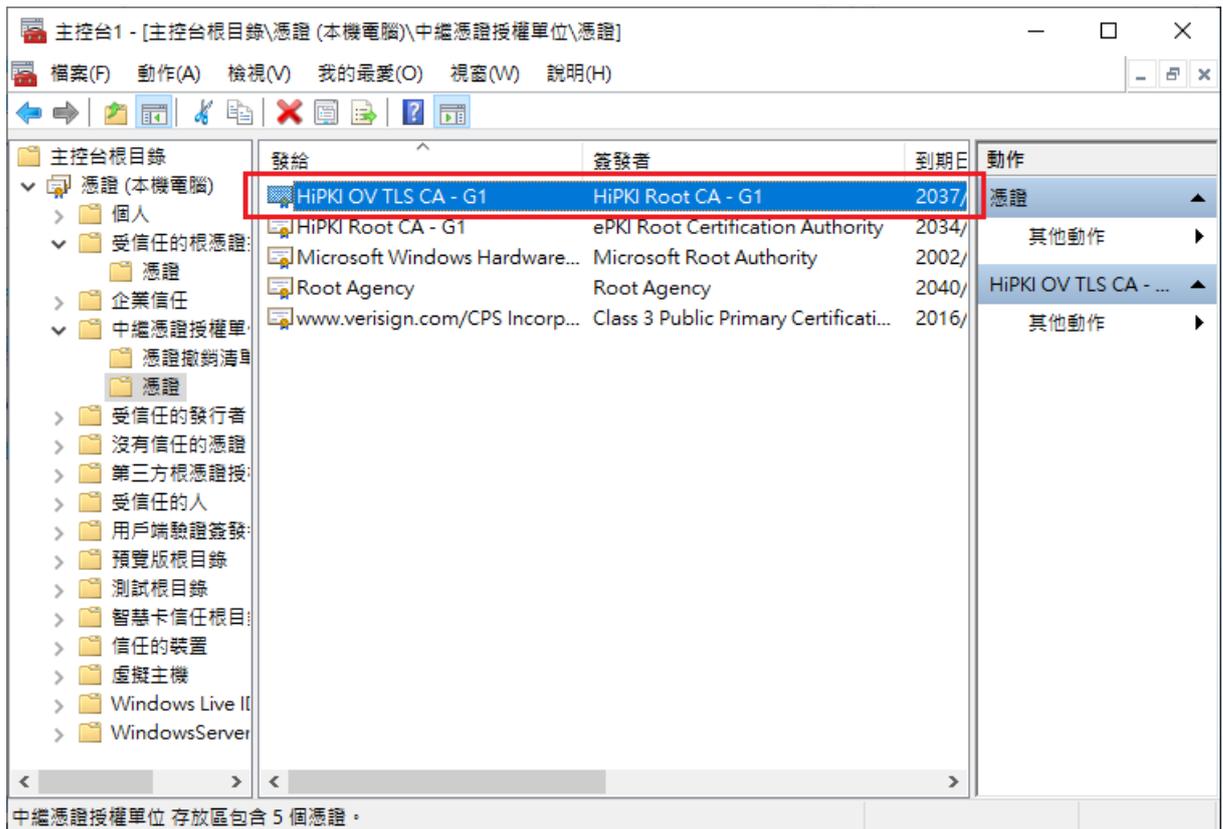
<https://eca.hinet.net/download/eCA1-to-HRCA1.crt>

HiPKI OV TLS CA 憑證：

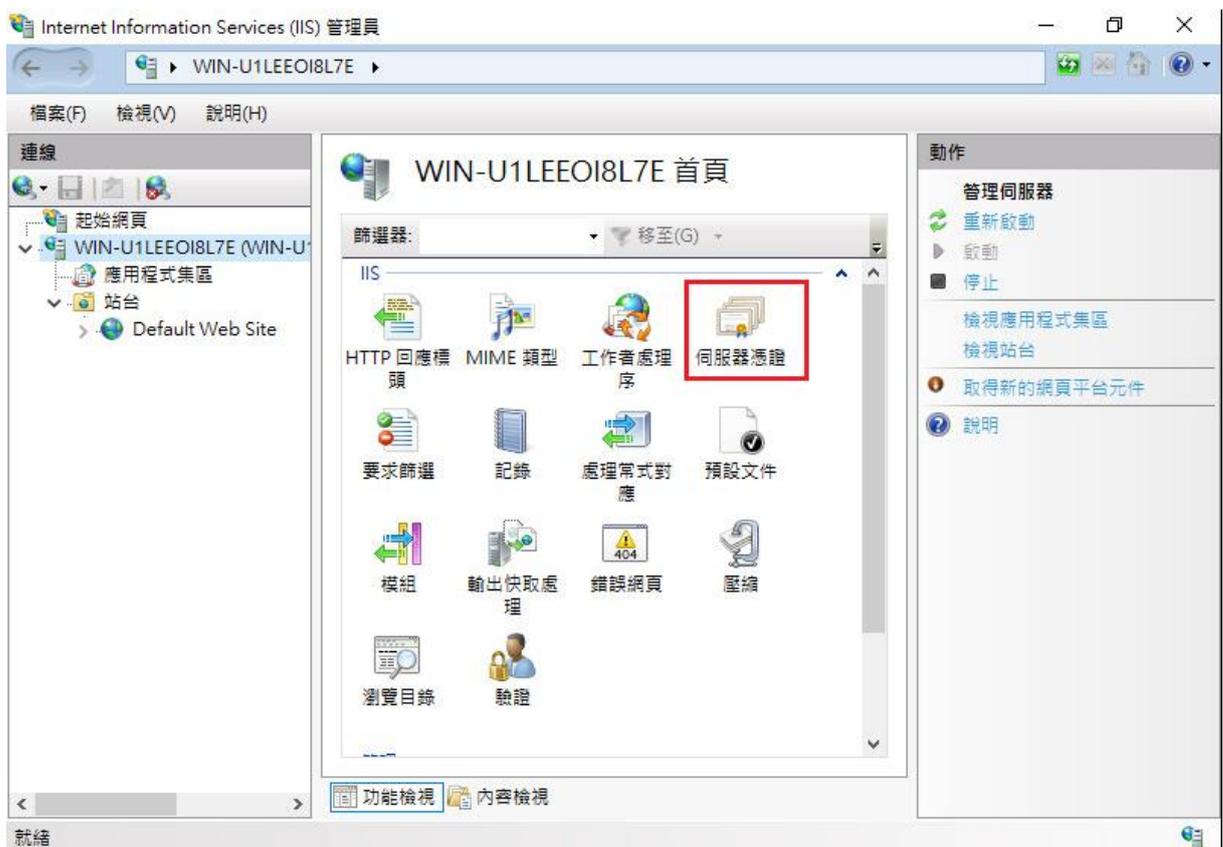
https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt



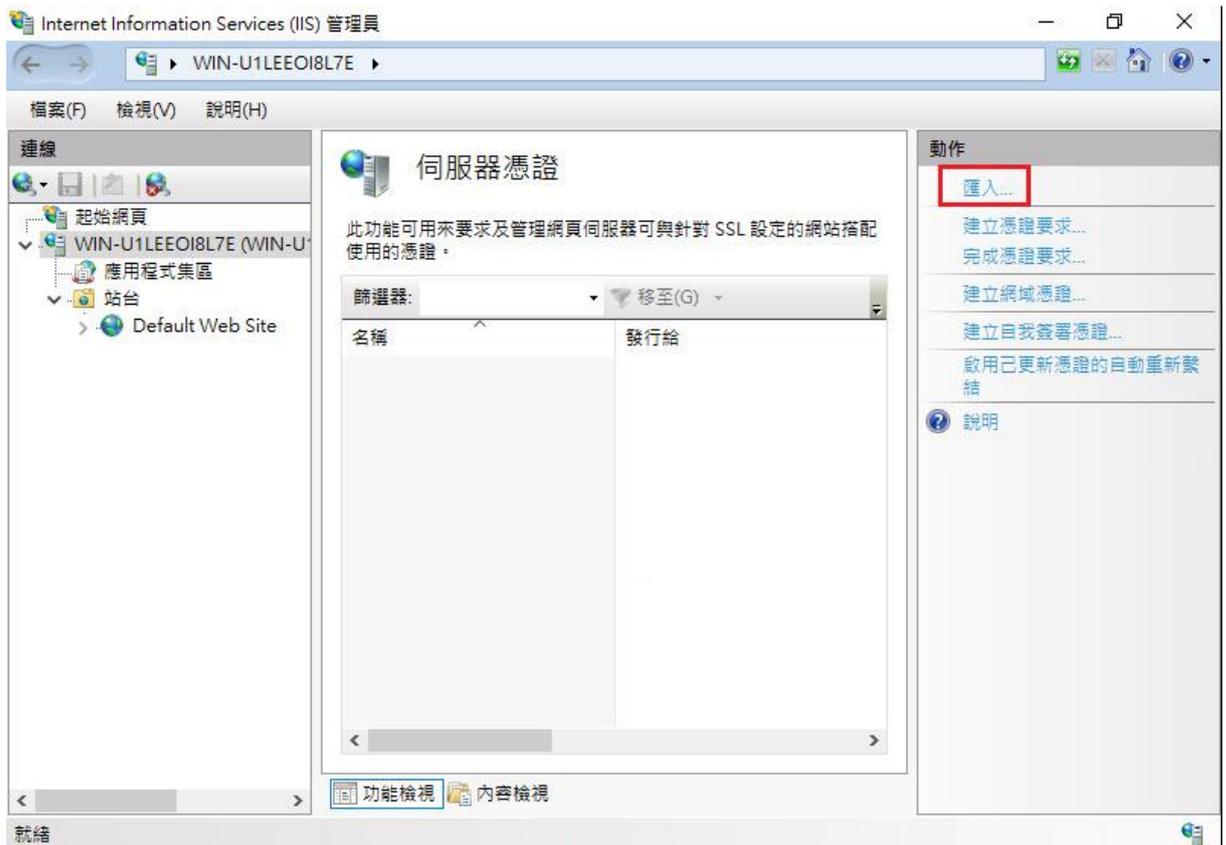




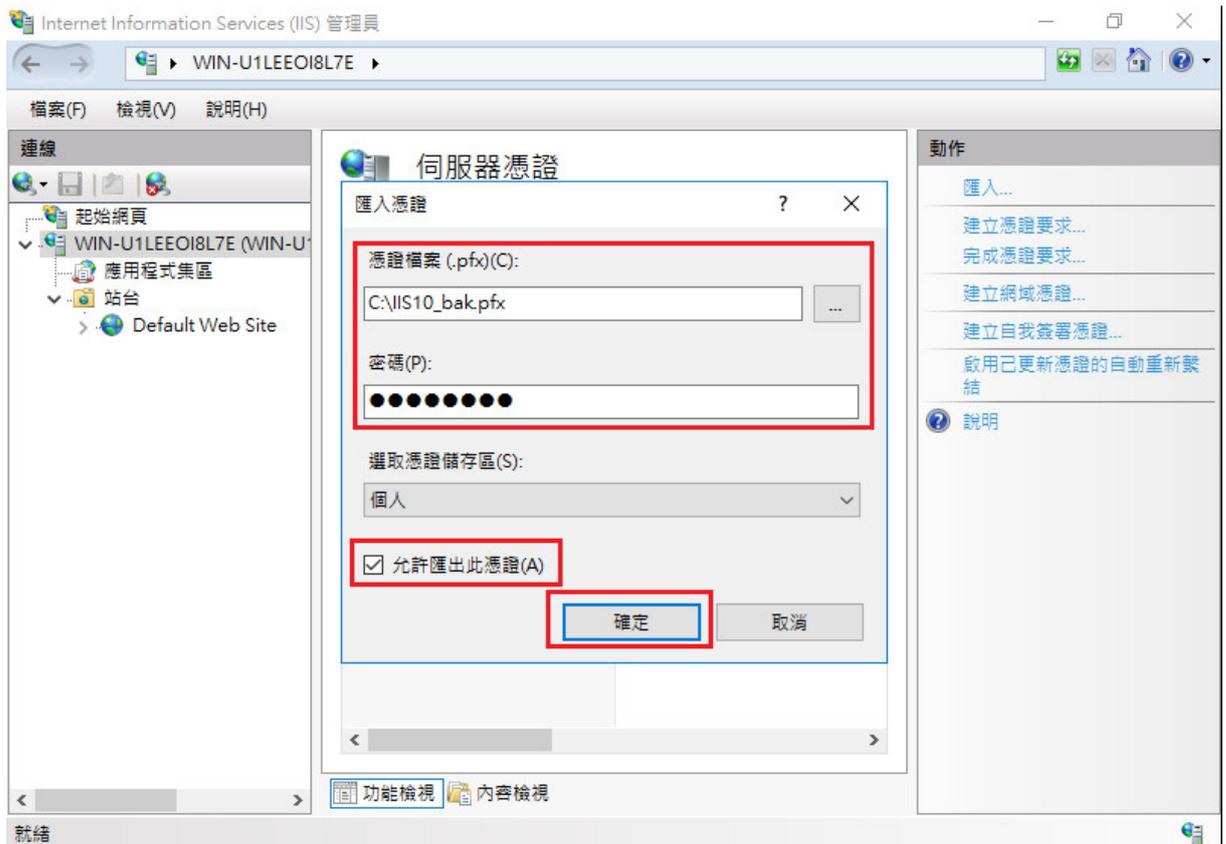
5. 開啟「Internet Information Services (IIS)管理員」。
6. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。

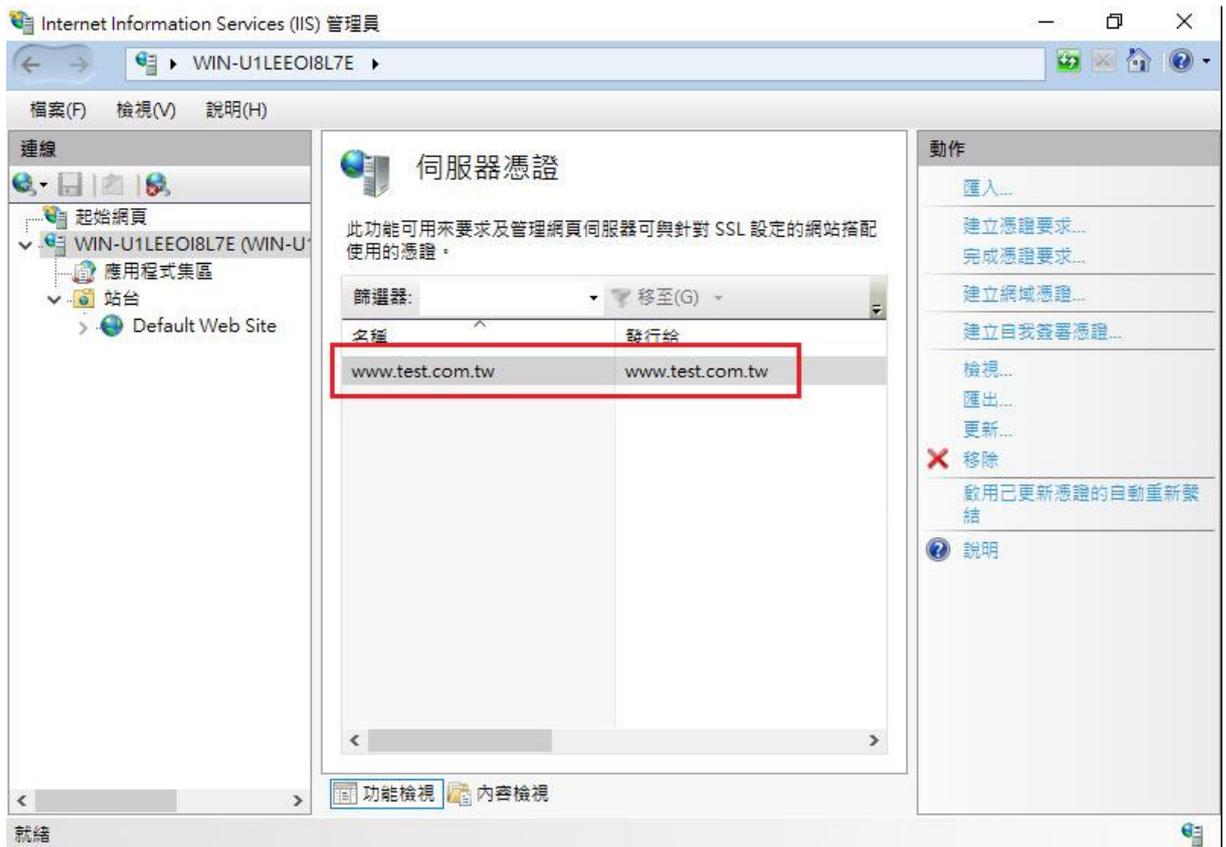


7. 點選右邊的「匯入」。

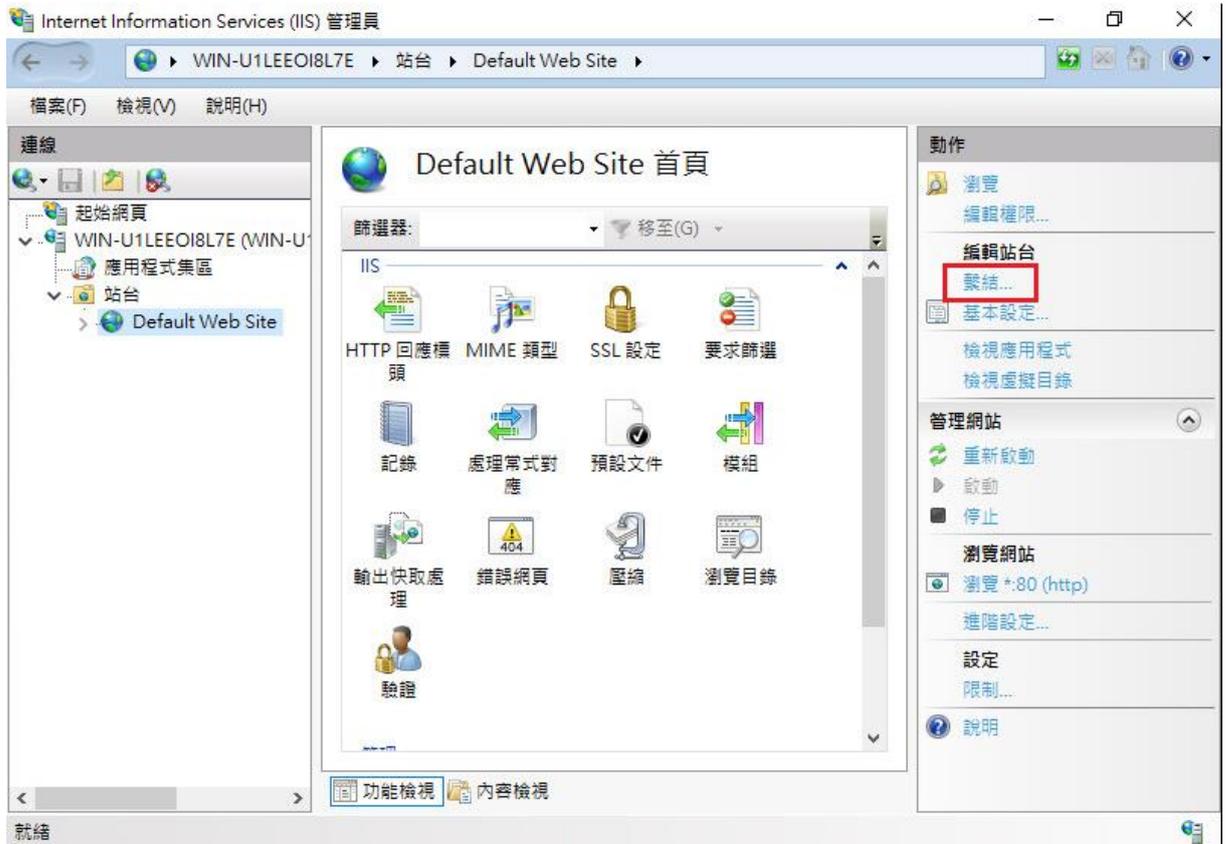


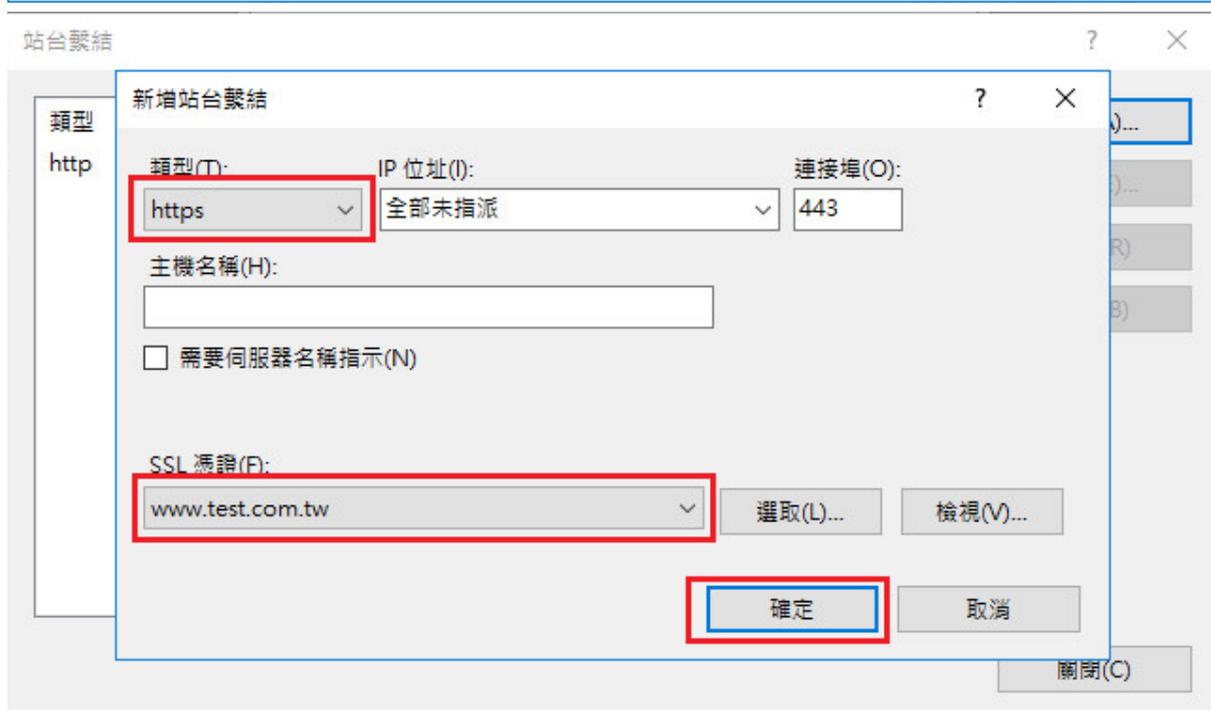
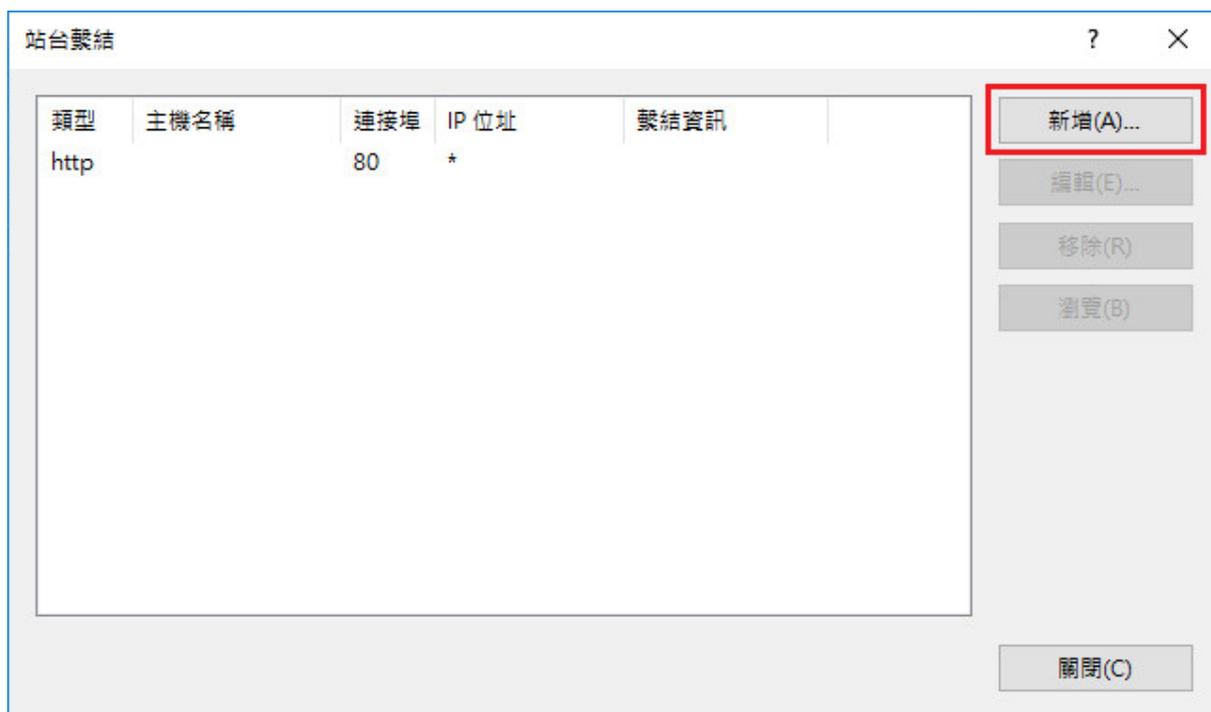
8. 輸入憑證檔案路徑與密碼，並勾選「允許匯出此憑證」後，按下確定。

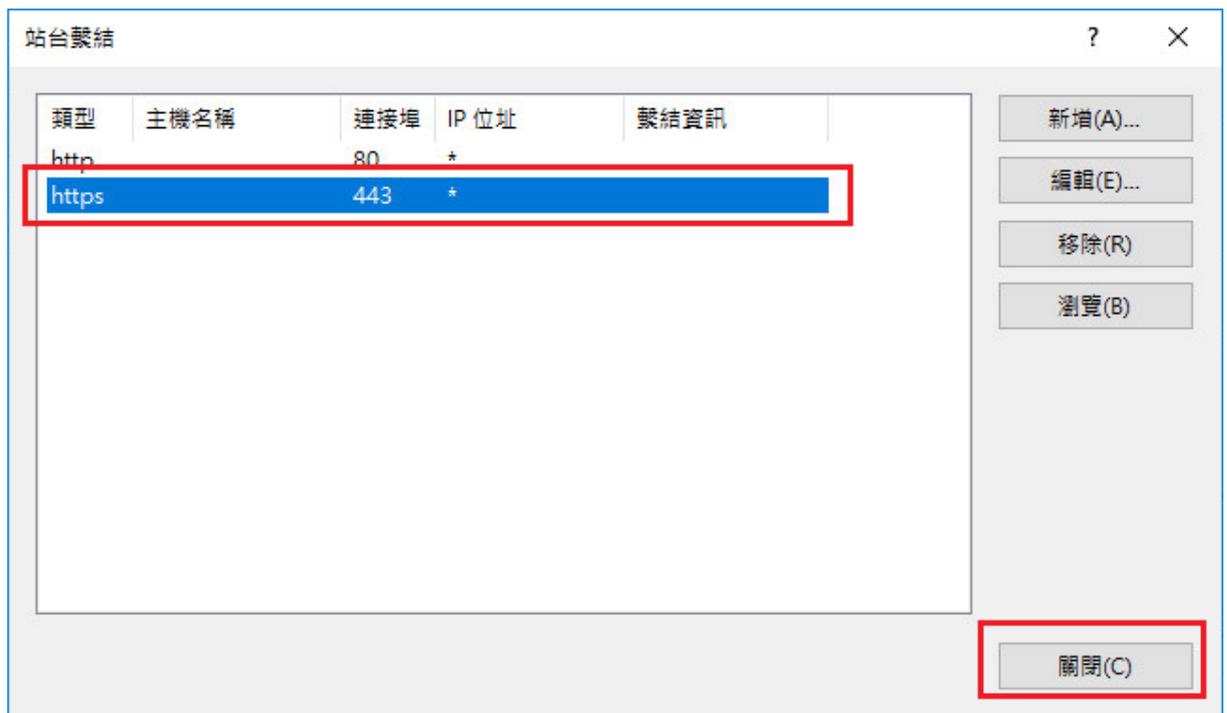




9. 點選左邊的站台。之後重新透過「繫結」來啟用憑證與 https。







10. 以 https 連線，測試 https 網頁是否正常。