政府伺服器數位憑證管理中心(GTLSCA)

Windows Server IIS 6、7、8、10 憑證備份與還原

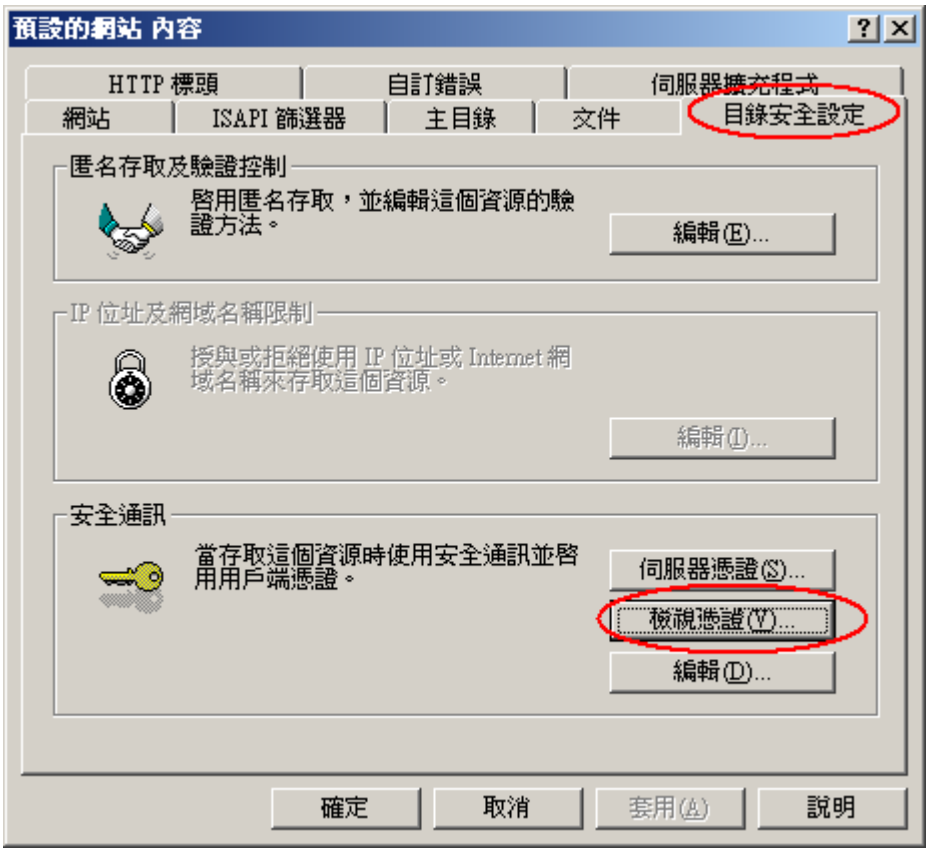
請依照您的Server(2003、2008、2012、2016)版本，參考對應的憑證備份與還原步驟。

目錄

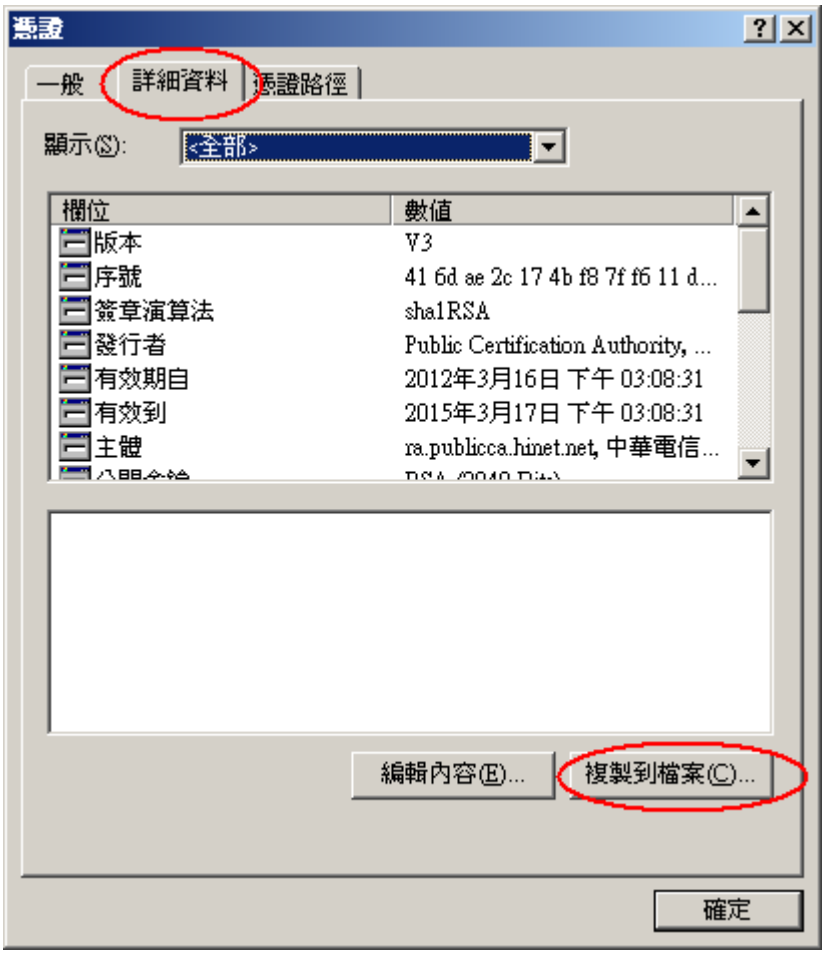
憑證備份步驟

Windows Server 2003

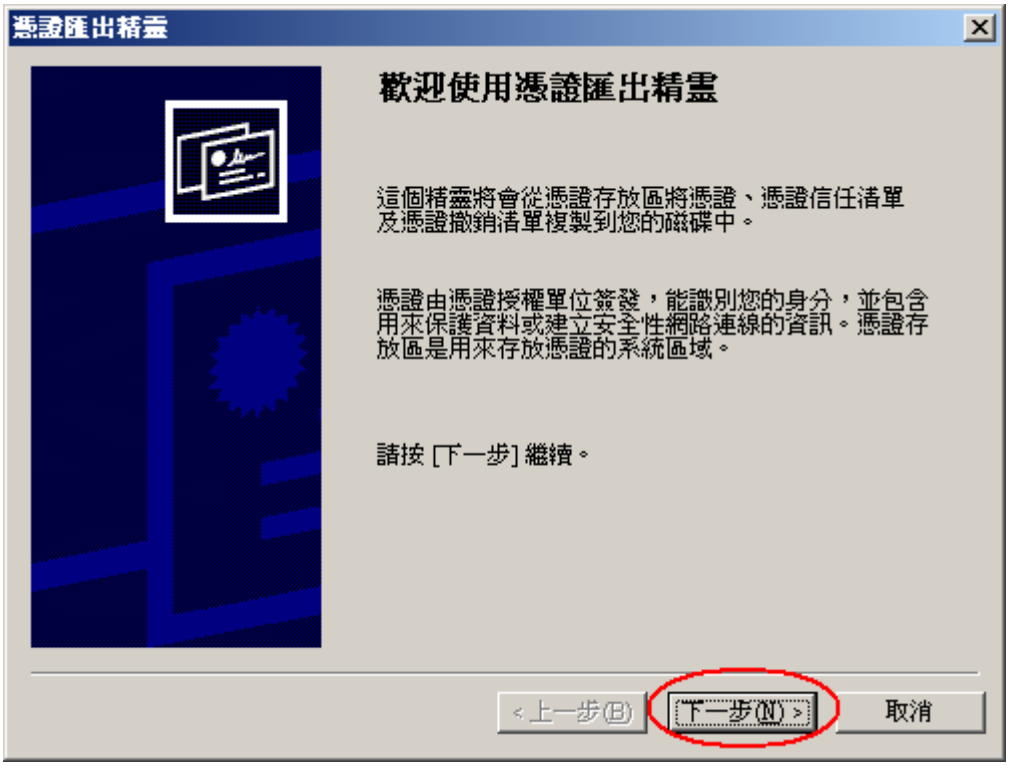
1. 「開始」→「設定」→「控制台」→「系統管理工具」→「Internet 服務管理員」→點選服務站台(滑鼠右鍵、選內容)→「目錄安全設定」→「檢視憑證」。



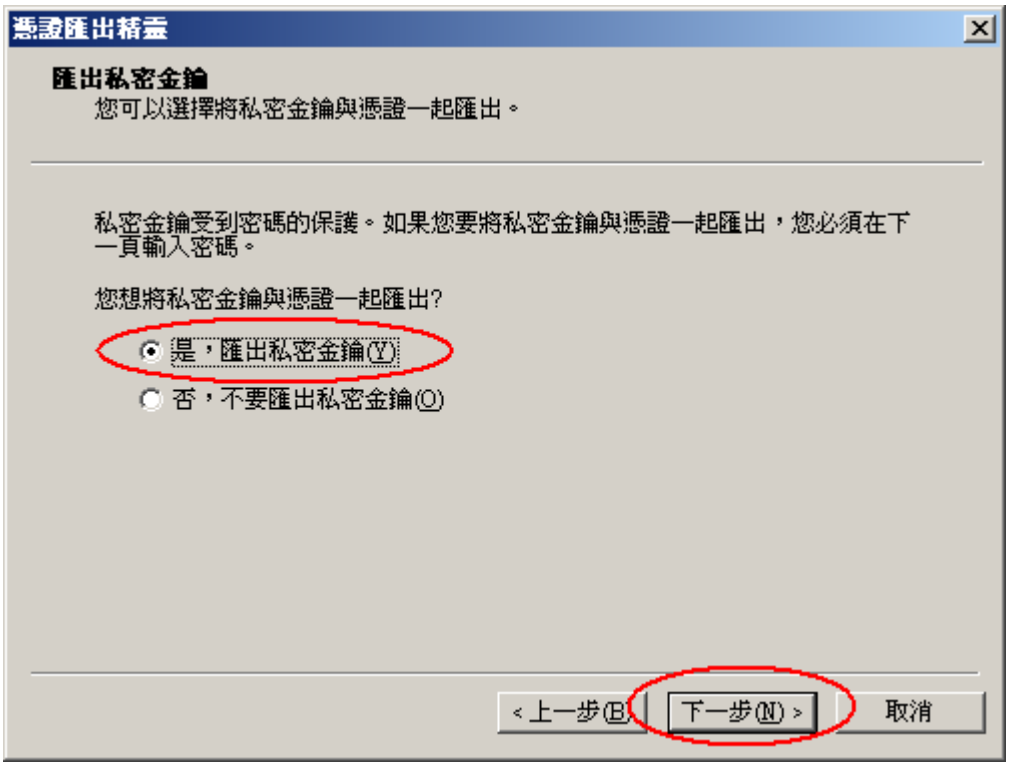
2. 點選「詳細資料」→「複製到檔案」。



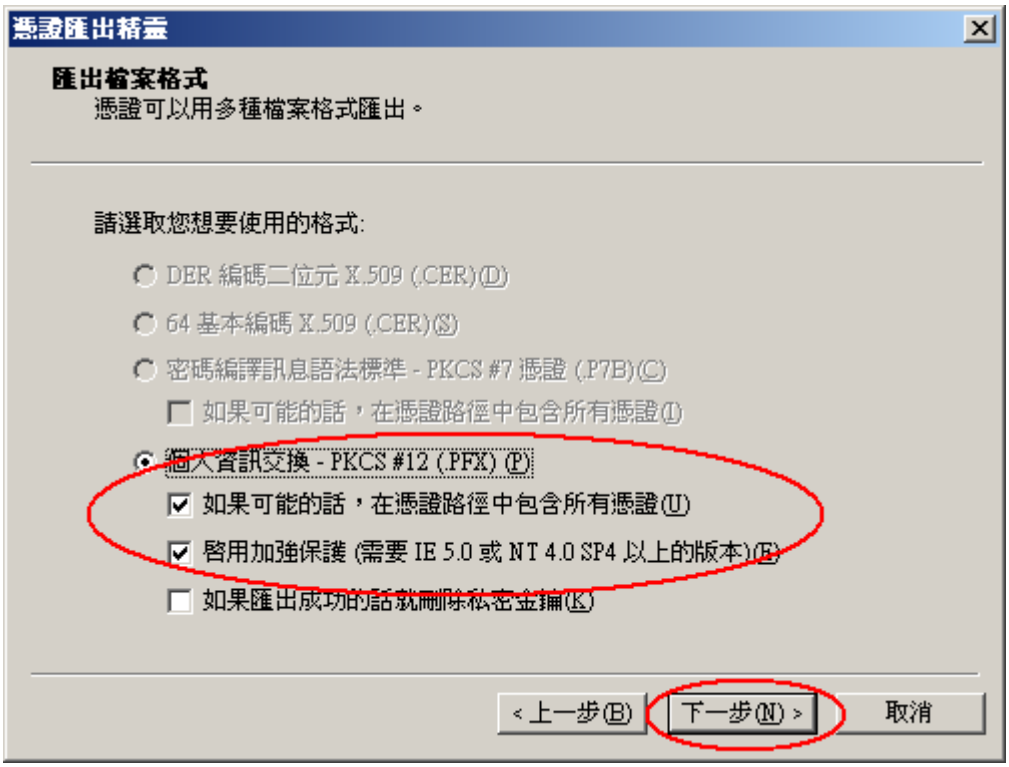
3. 點選「下一步」



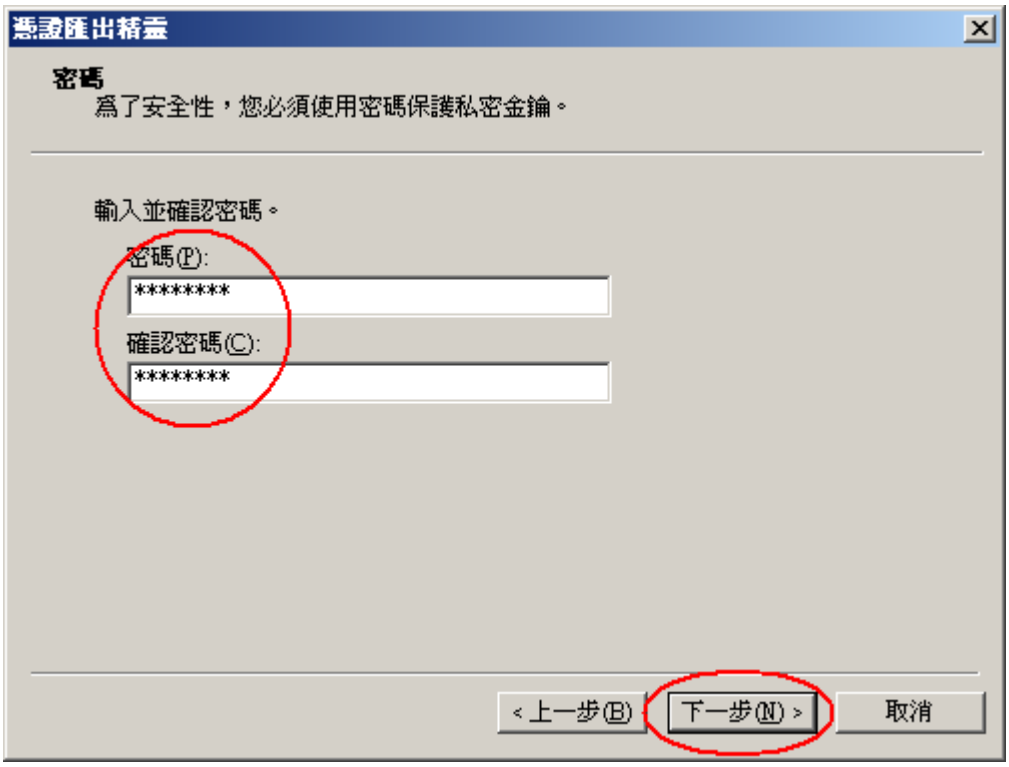
4. 選擇 「匯出私密金鑰」→「下一步」



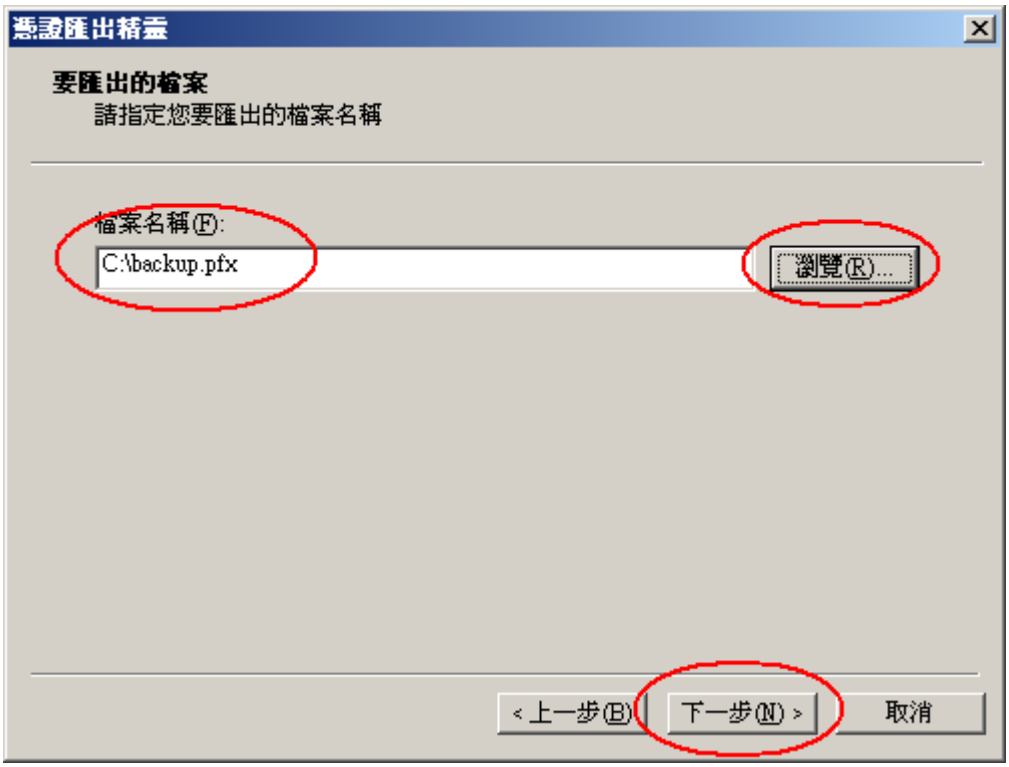
5. 選擇「啟用加強保護」



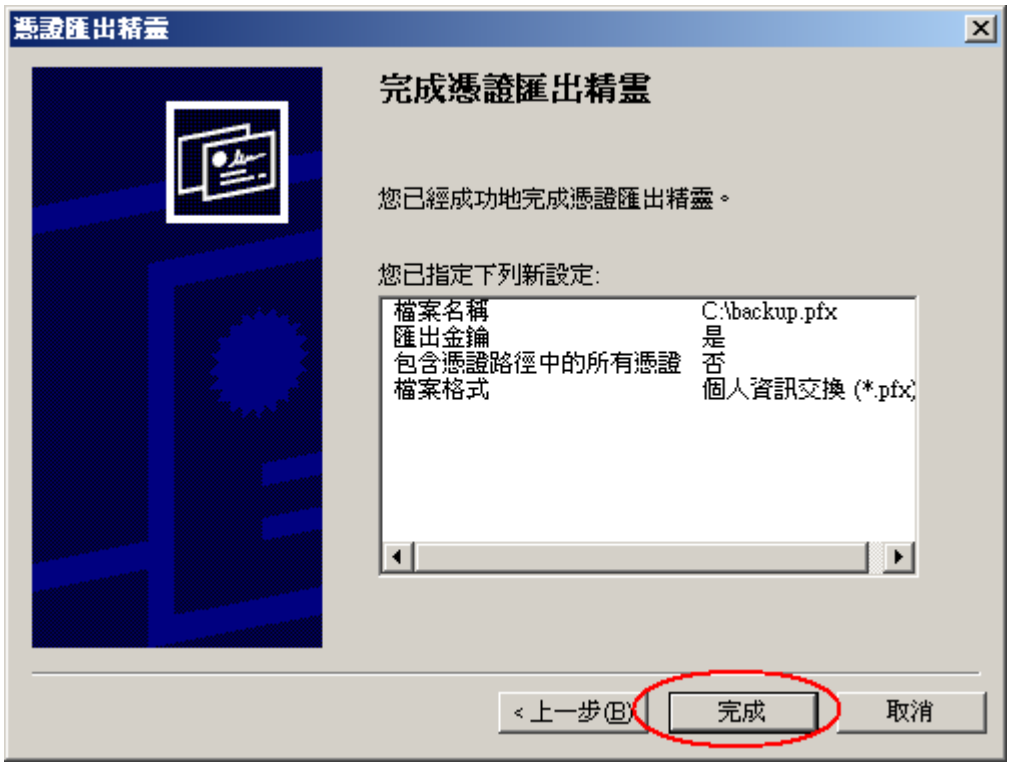
6. 輸入密碼保護



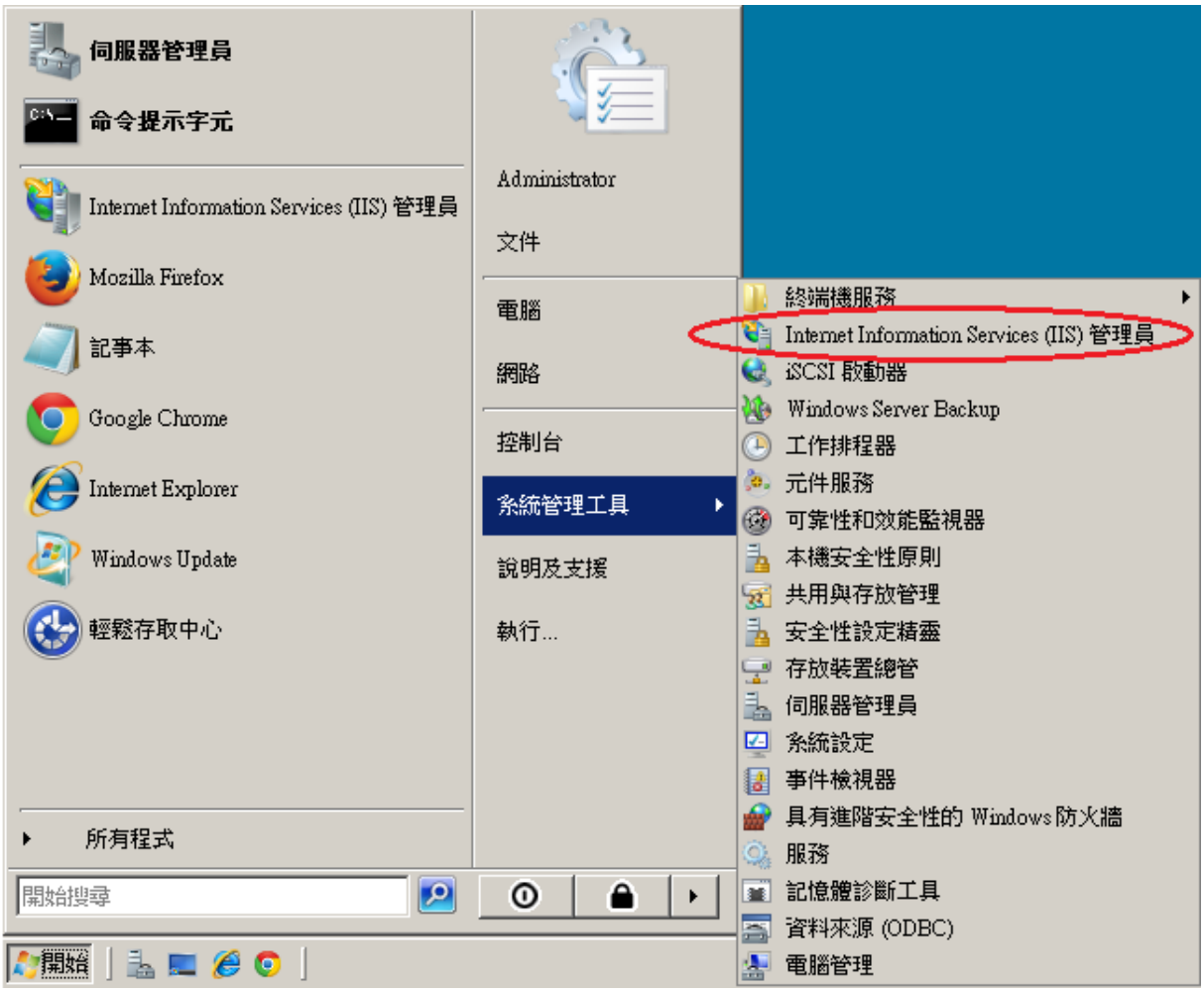
7. 輸入自定檔案名稱*.PFX



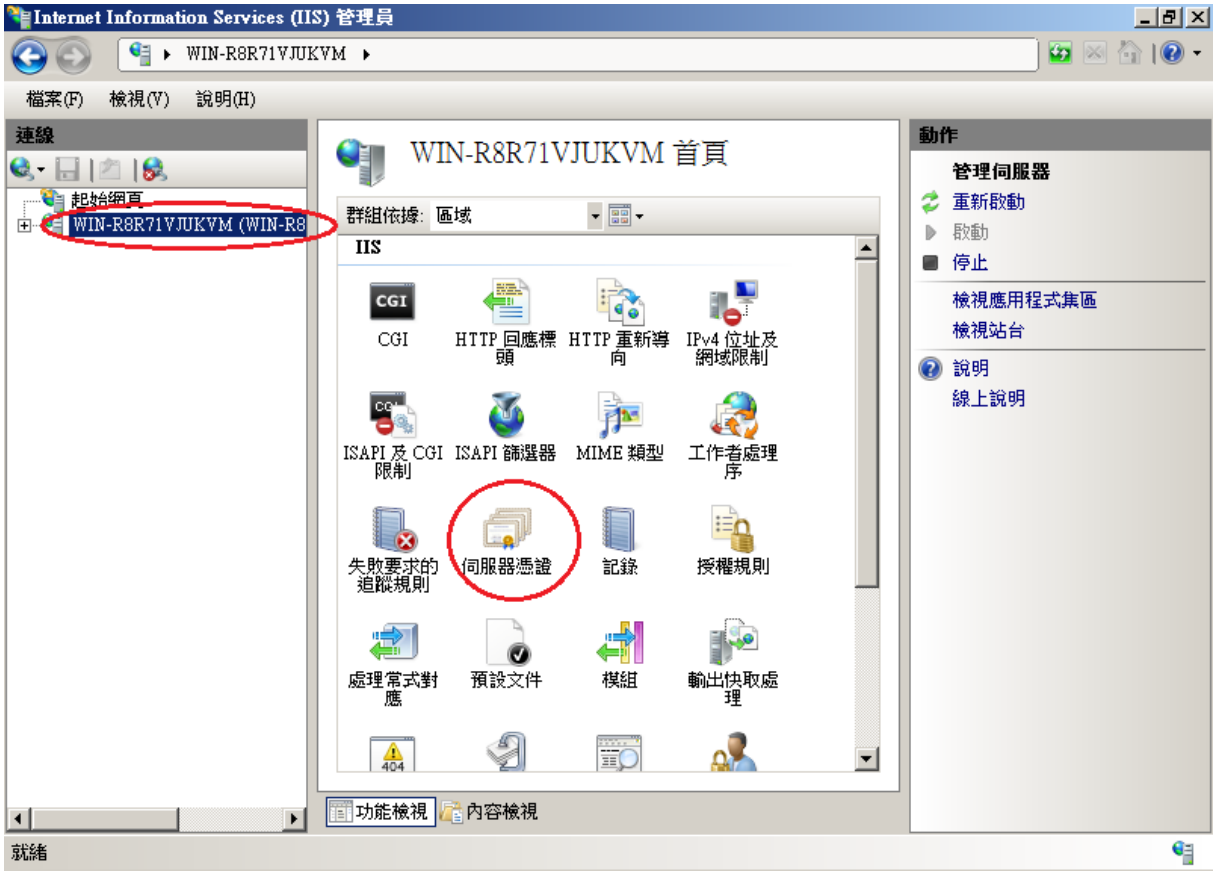
8. 完成匯出憑證


憑證匯出精靈
完成憑證匯出精靈
您已經成功地完成憑證匯出精靈。
您已指定下列新設定:
檔案名稱 C:\backup.pfx
匯出金鑰 是
包含憑證路徑中的所有憑證 否
檔案格式 個人資訊交換 (*.pfx)
< 上一步(B)
完成
取消

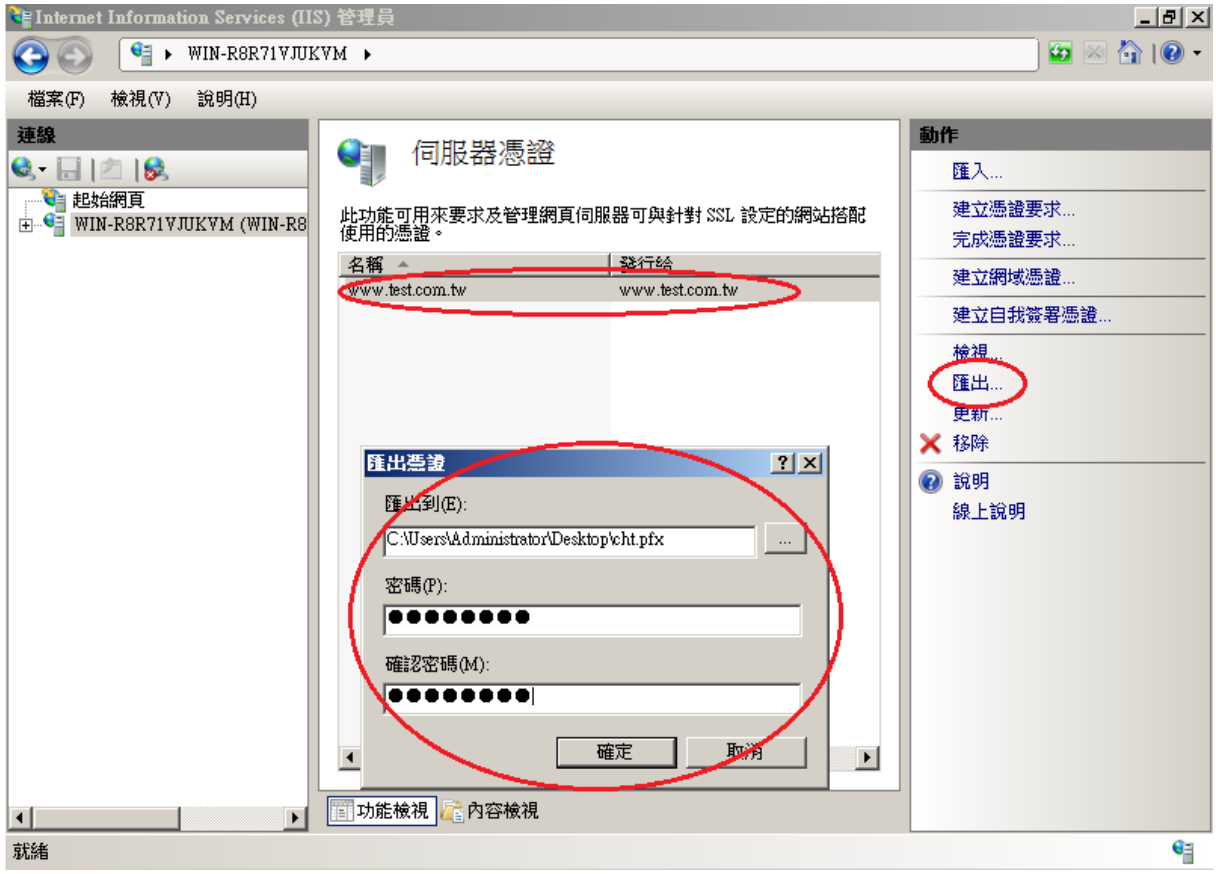
1. 點選 「開始」→ 「系統管理工具」→「Internet Information Services (IIS)管理員」。



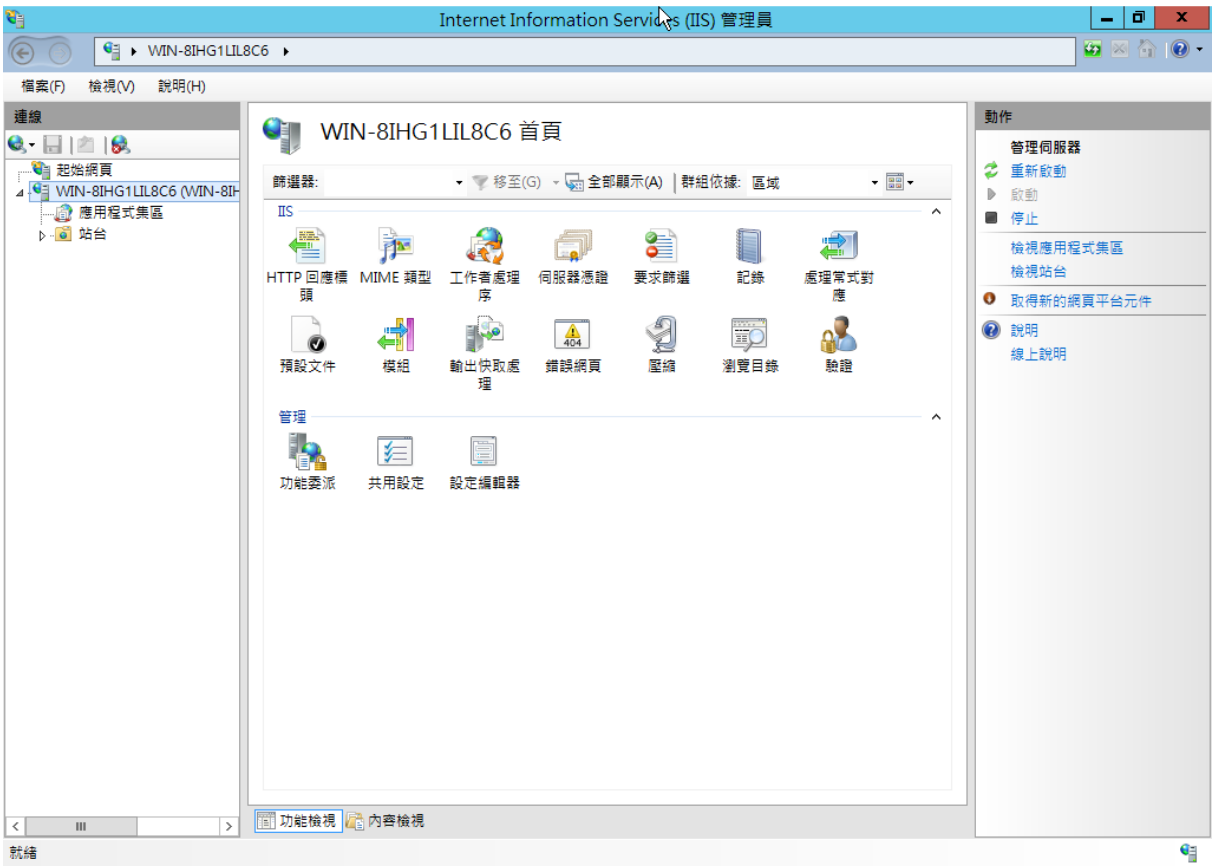
2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



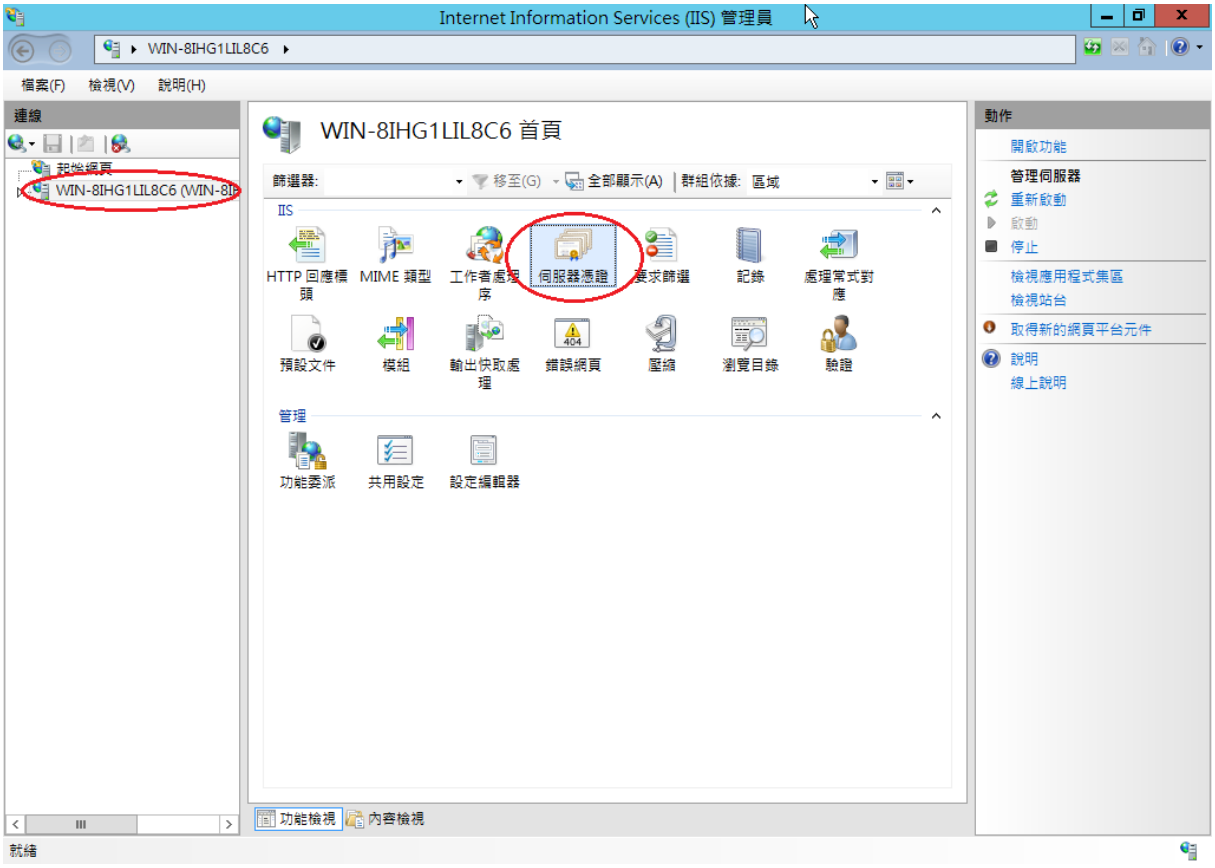
3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。



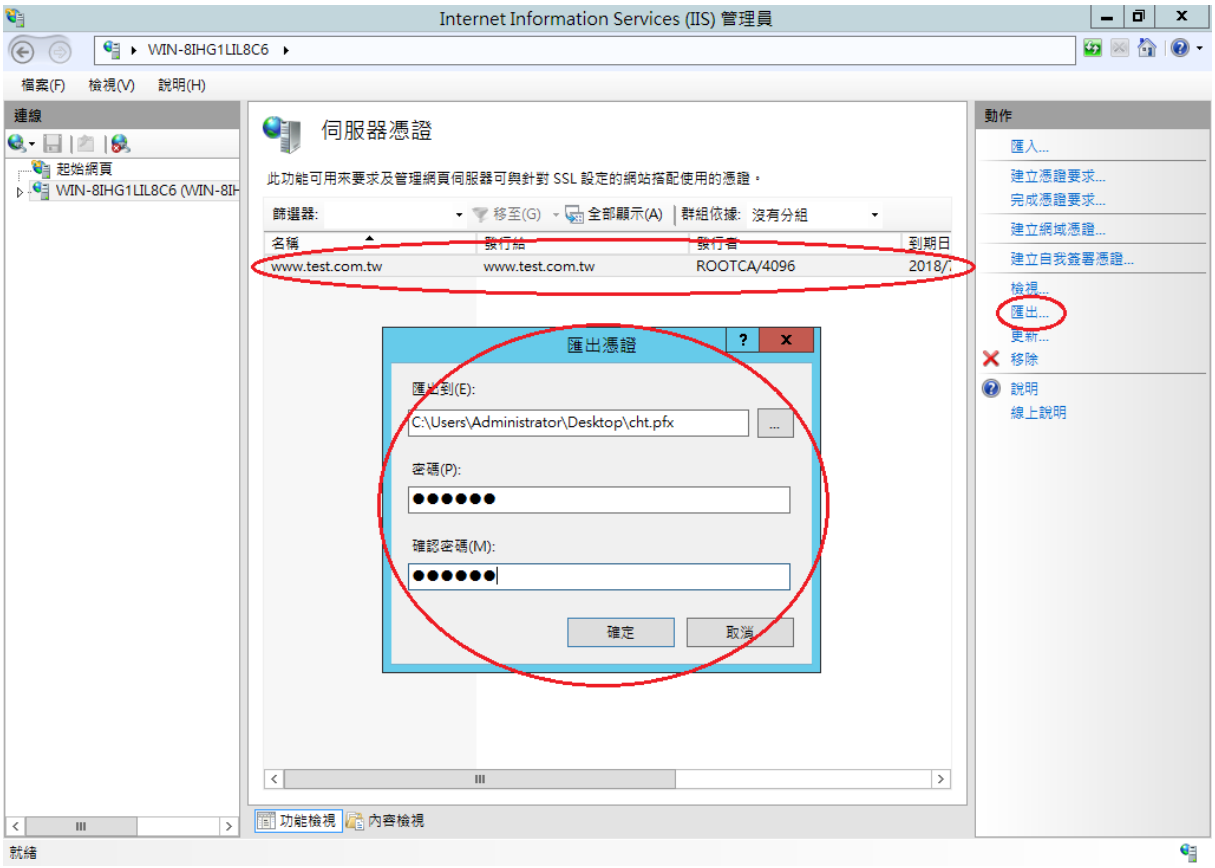
1. 開啟「Internet Information Services (IIS)管理員」。



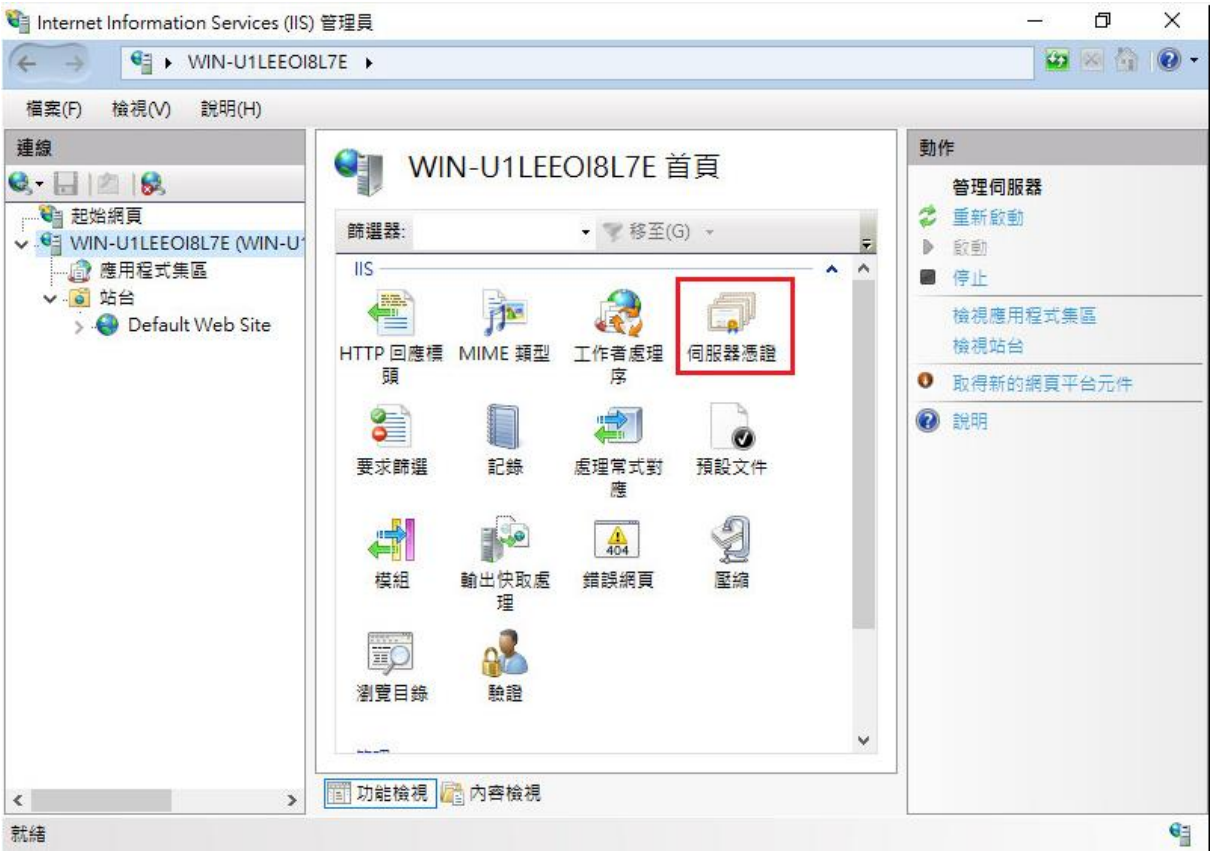
2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



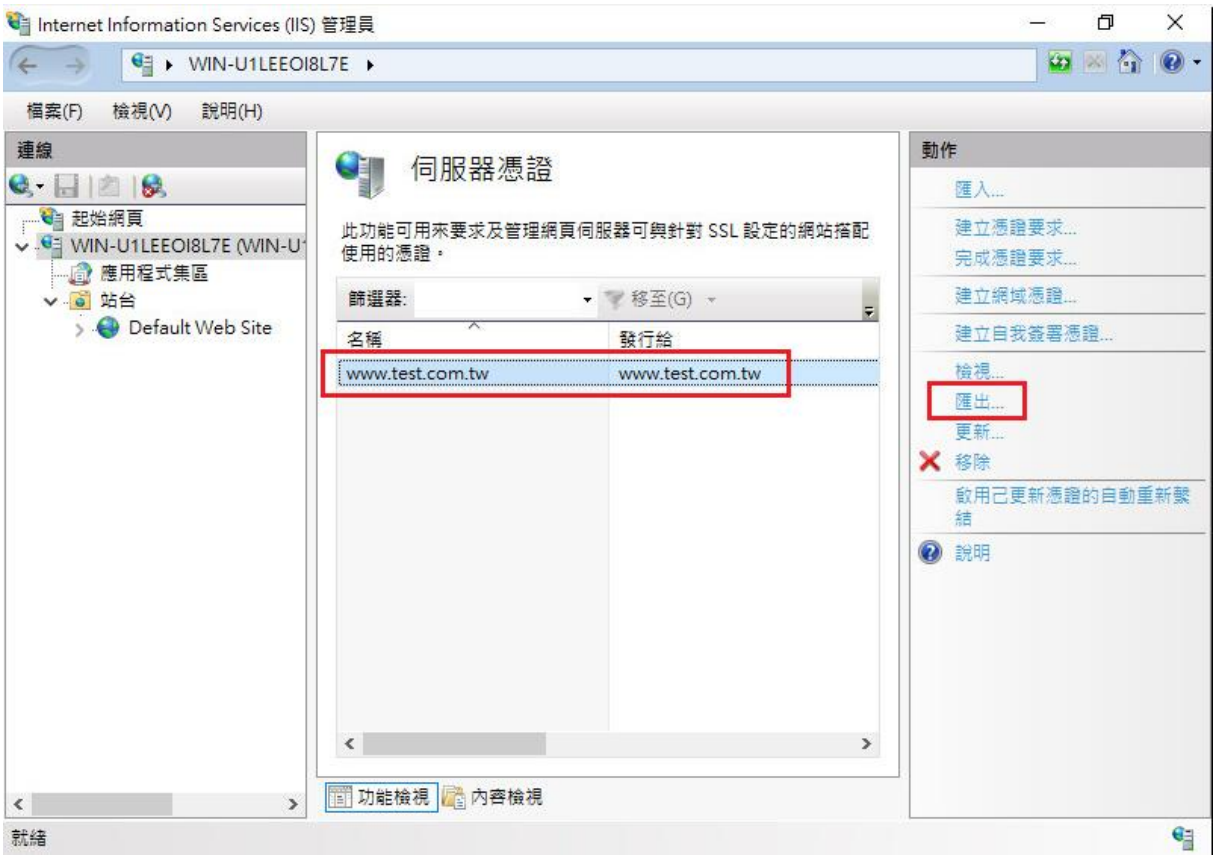
3. 先點選要匯出的憑證，然後按下右邊畫面的「匯出」，依據匯出憑證的視窗填上路徑與密碼(此組密碼若忘記了，將會無法使用匯出的憑證檔)。到此，憑證備份完成。

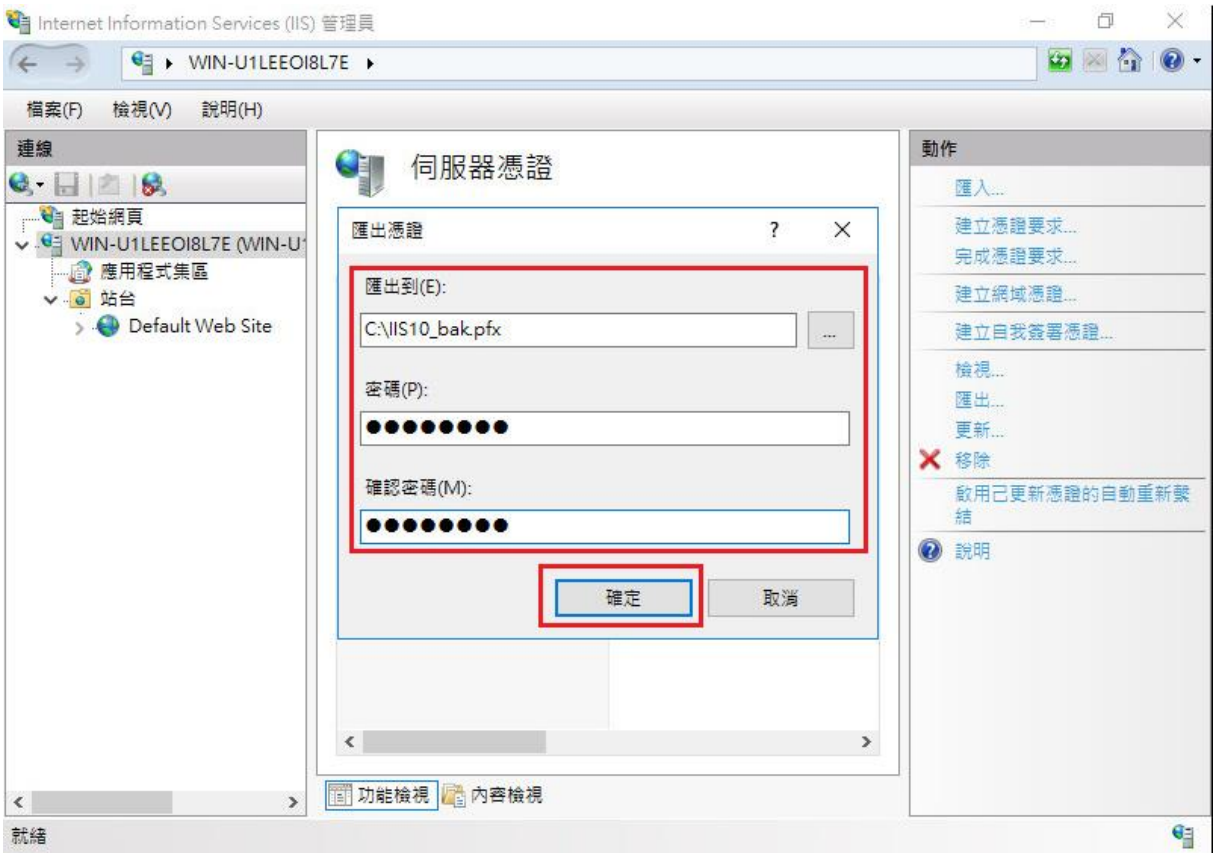


1. 開啟「Internet Information Services (IIS)管理員」。
2. 在左邊點選主機名稱，再點選畫面右邊的「伺服器憑證」。



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。

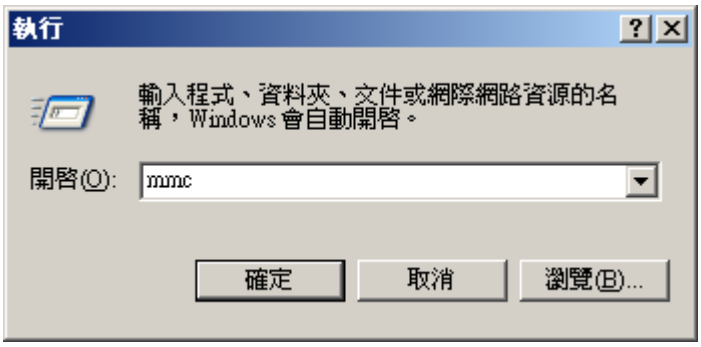

Internet Information Services (IIS) 管理員
WIN-U1LEEOI8L7E
檔案(F) 檢視(V) 說明(H)
連線
起始網頁
WIN-U1LEEOI8L7E (WIN-U1
應用程式集區
站台
Default Web Site
伺服器憑證
此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站搭配使用的憑證。
篩選器:
移至(G)
名稱
發行給
www.test.com.tw
www.test.com.tw
功能檢視
內容檢視
就緒
動作
匯入...
建立憑證要求...
完成憑證要求...
建立網域憑證...
建立自我簽署憑證...
檢視...
匯出...
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-U1
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

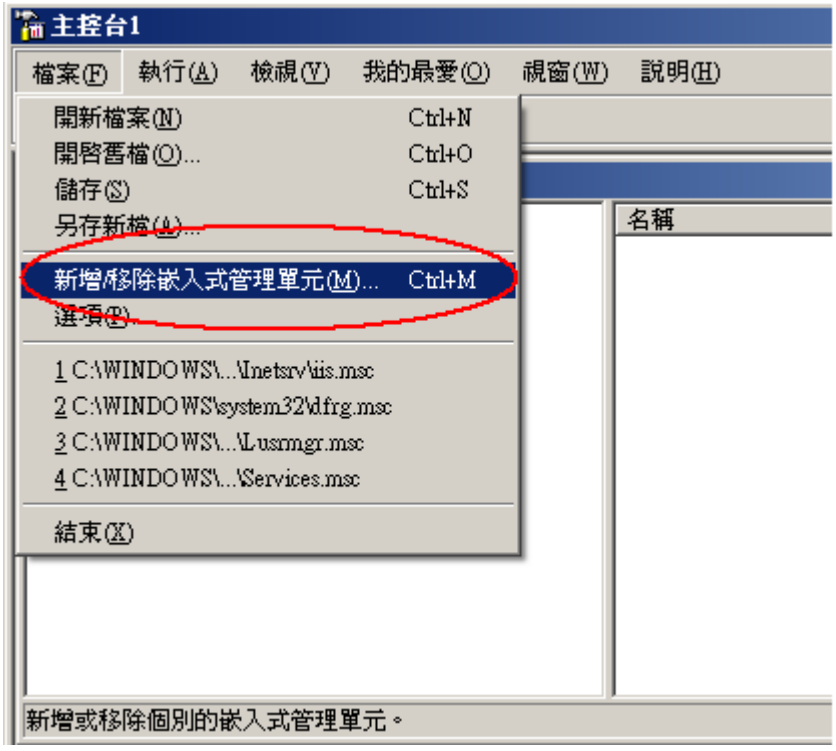
憑證還原步驟-匯入 SSL 憑證

Windows Server 2003

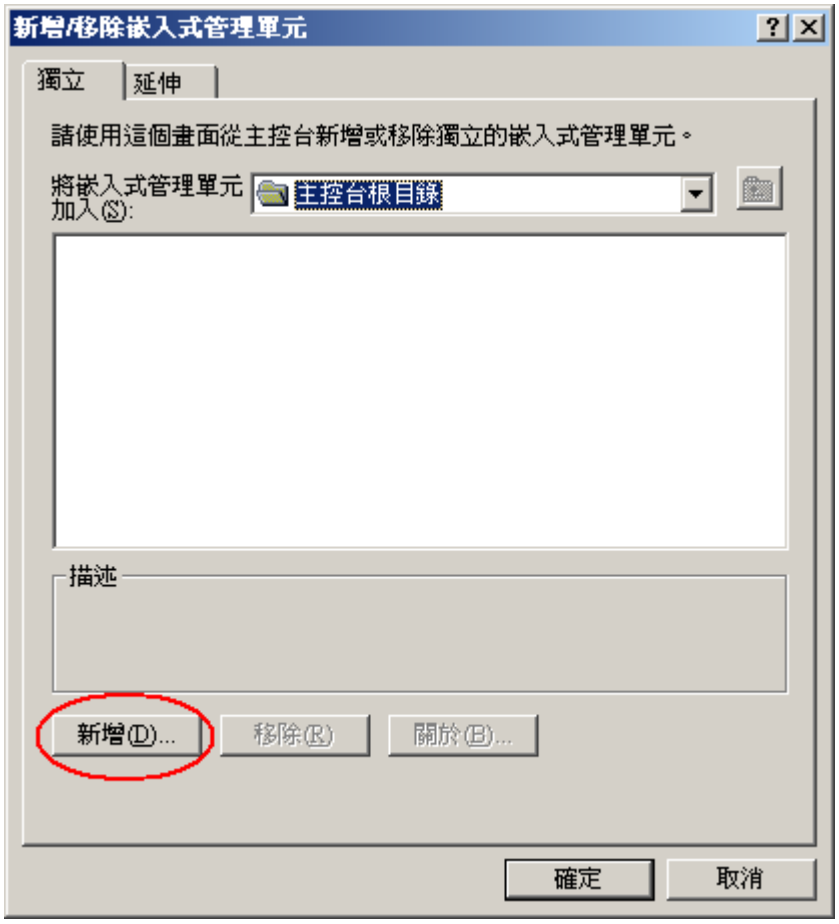
1. 由「開始」→執行→輸入 mmc，執行主控台



2. 進入主控台後，選擇「新增/移除嵌入式入式管理單元」

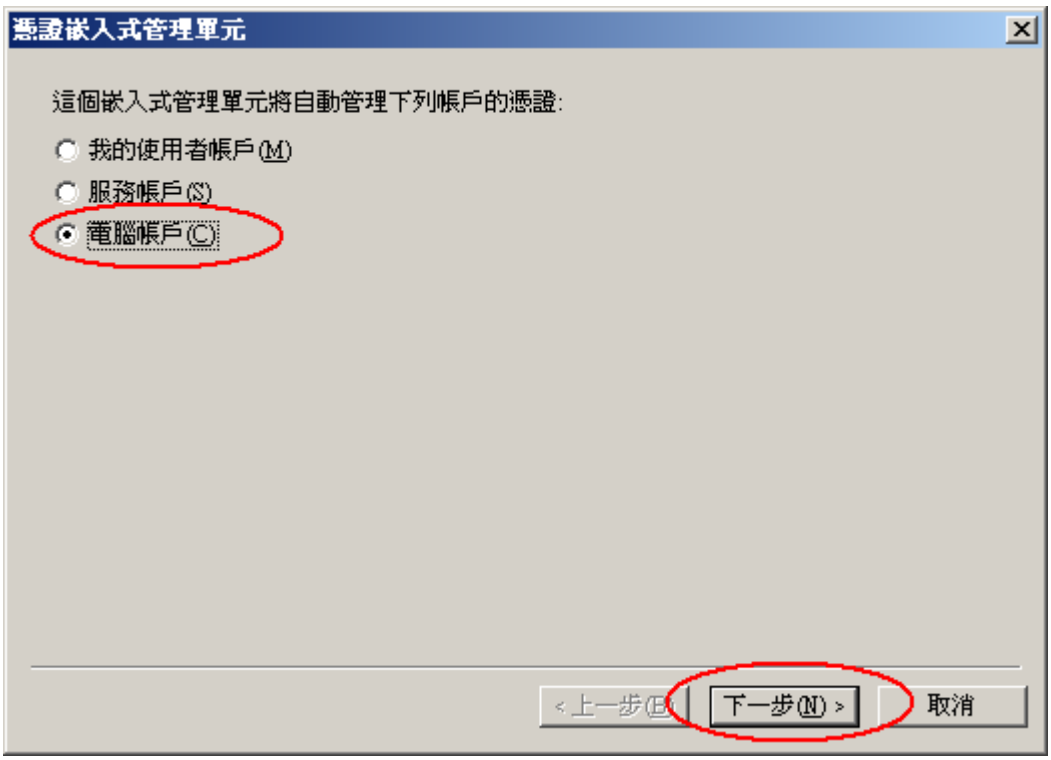


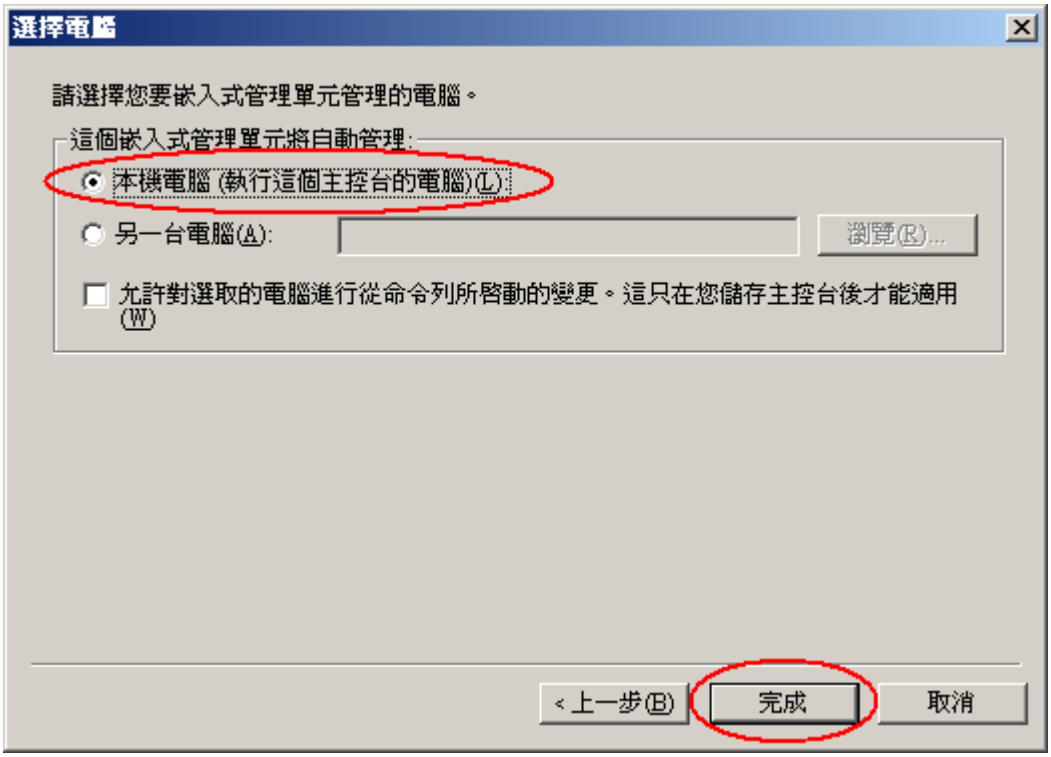
新增憑證管理單元。點選「新增」

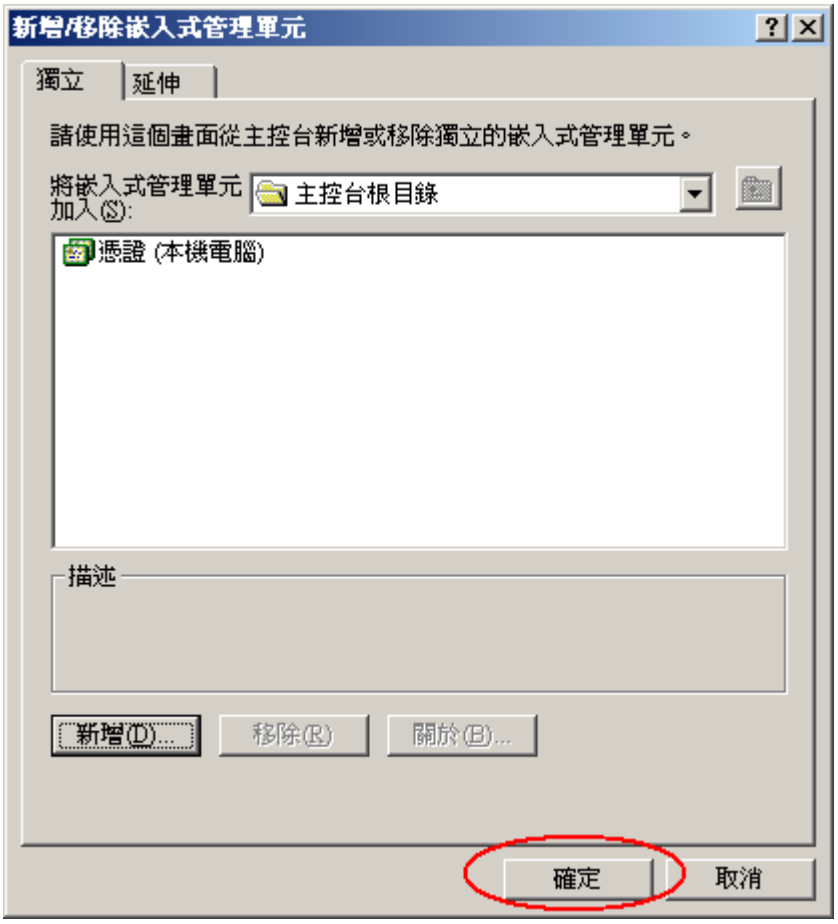


選擇「憑證」

點選電腦帳戶及本機電腦


憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


選擇電腦
請選擇您要嵌入式管理單元管理的電腦。
這個嵌入式管理單元將自動管理:
本機電腦 (執行這個主控台的電腦)(L)
另一台電腦(A):
瀏覽(R)...
允許對選取的電腦進行從命令列所啓動的變更。這只在您儲存主控台後才能適用(W)
< 上一步(B)
完成
取消

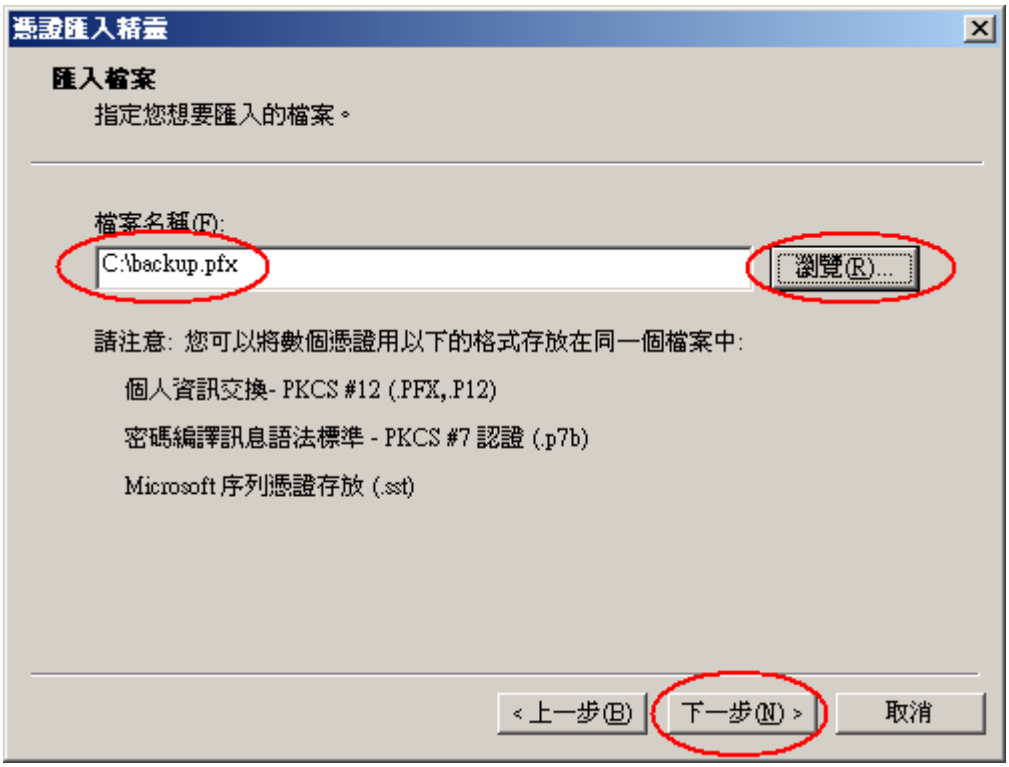


3. 匯入憑證。

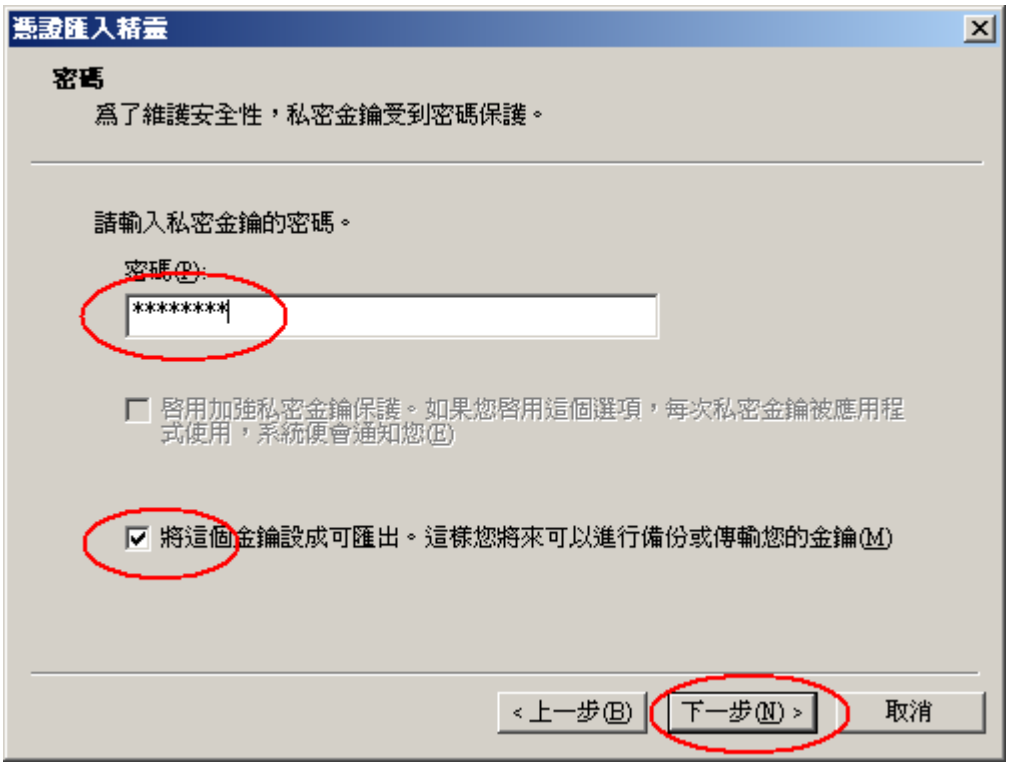
點選「個人」→憑證→所有工作→匯入

使用憑證匯入精靈→下一步

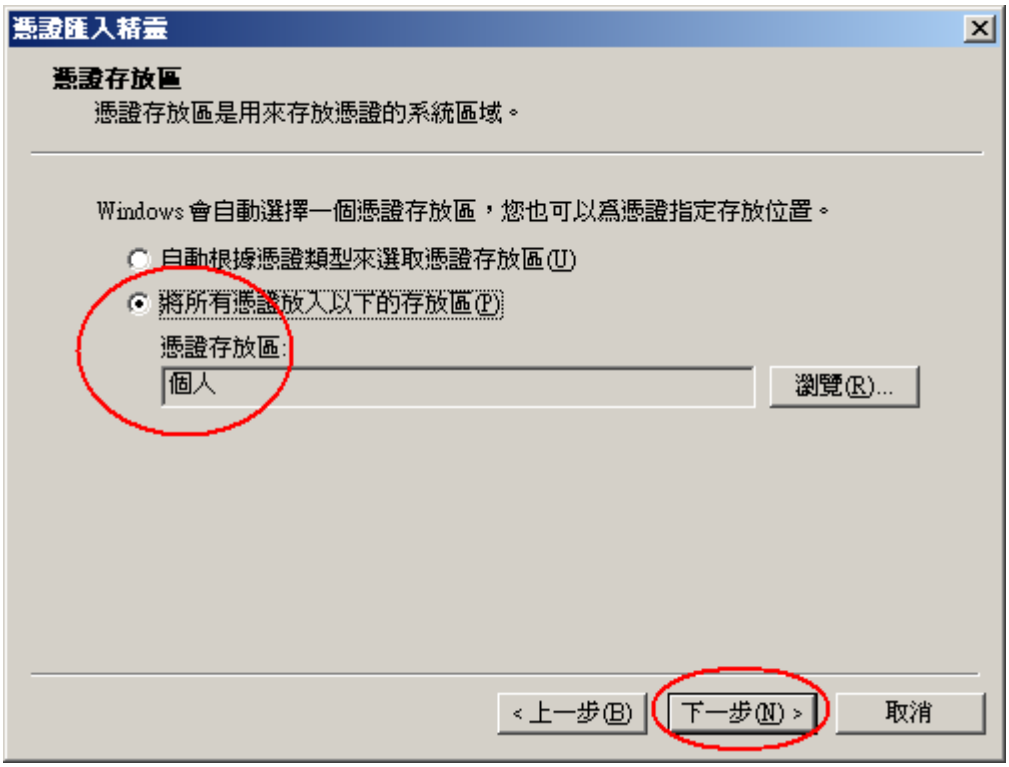
瀏覽→選擇備份之*.pfx



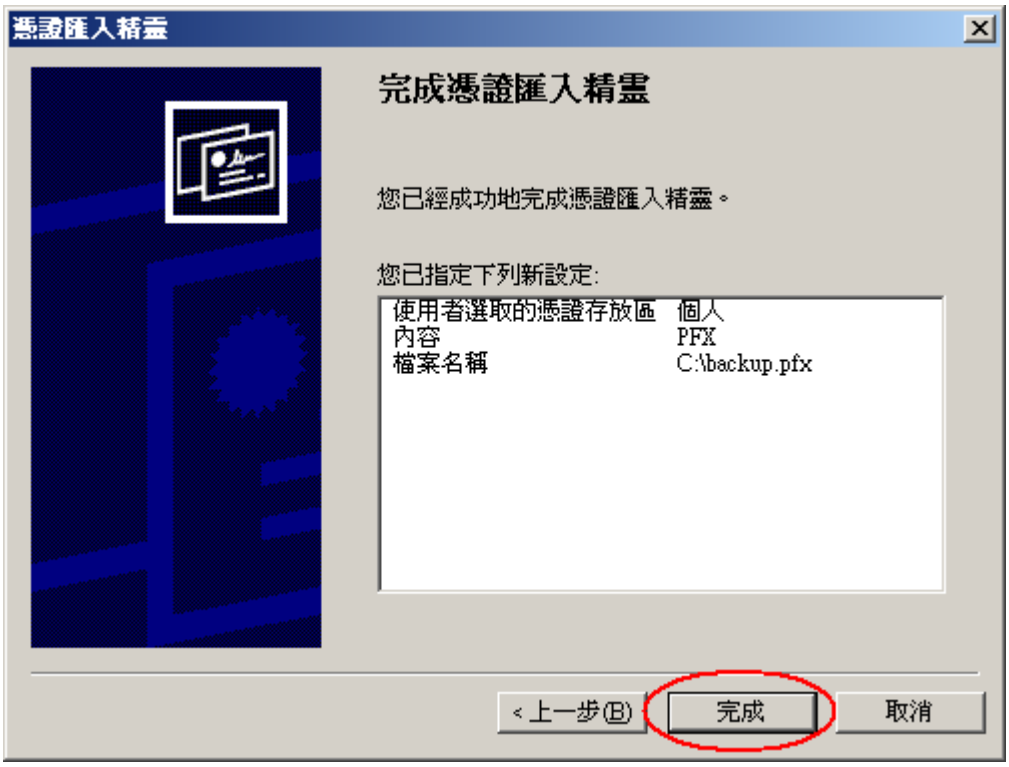
輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。



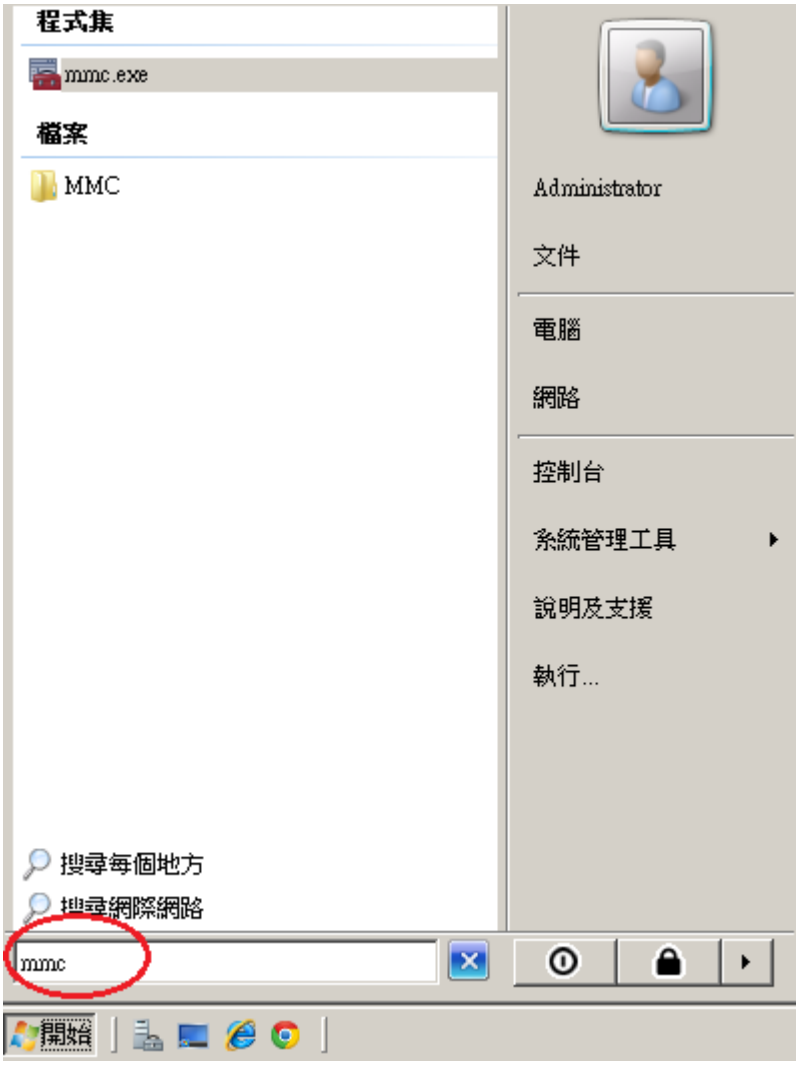
憑證匯入到個人→下一步



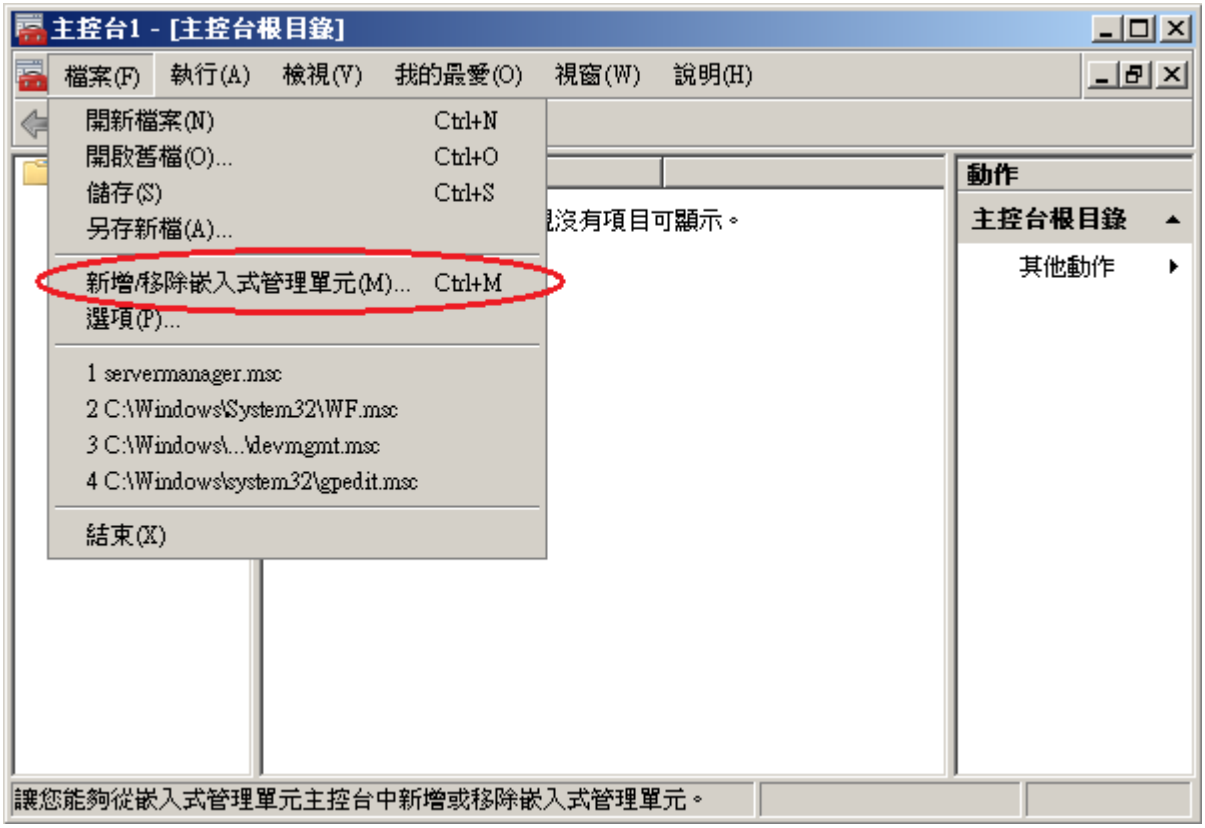
完成匯入憑證


憑證匯入精靈
完成憑證匯入精靈
您已經成功地完成憑證匯入精靈。
您已指定下列新設定:
使用者選取的憑證存放區 個人
內容 PFX
檔案名稱 C:\backup.pfx
< 上一步(B)
完成
取消

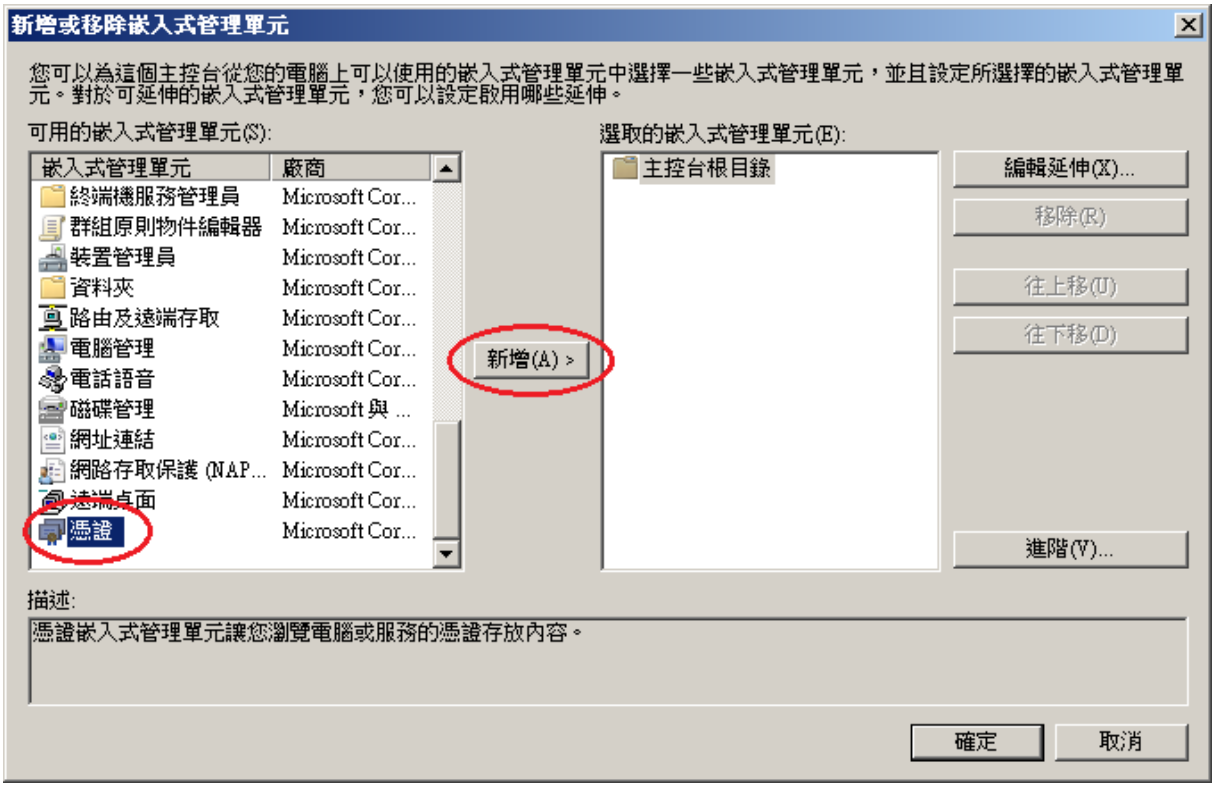
1. 「開始」→「輸入 mmc」，按下「Enter」。



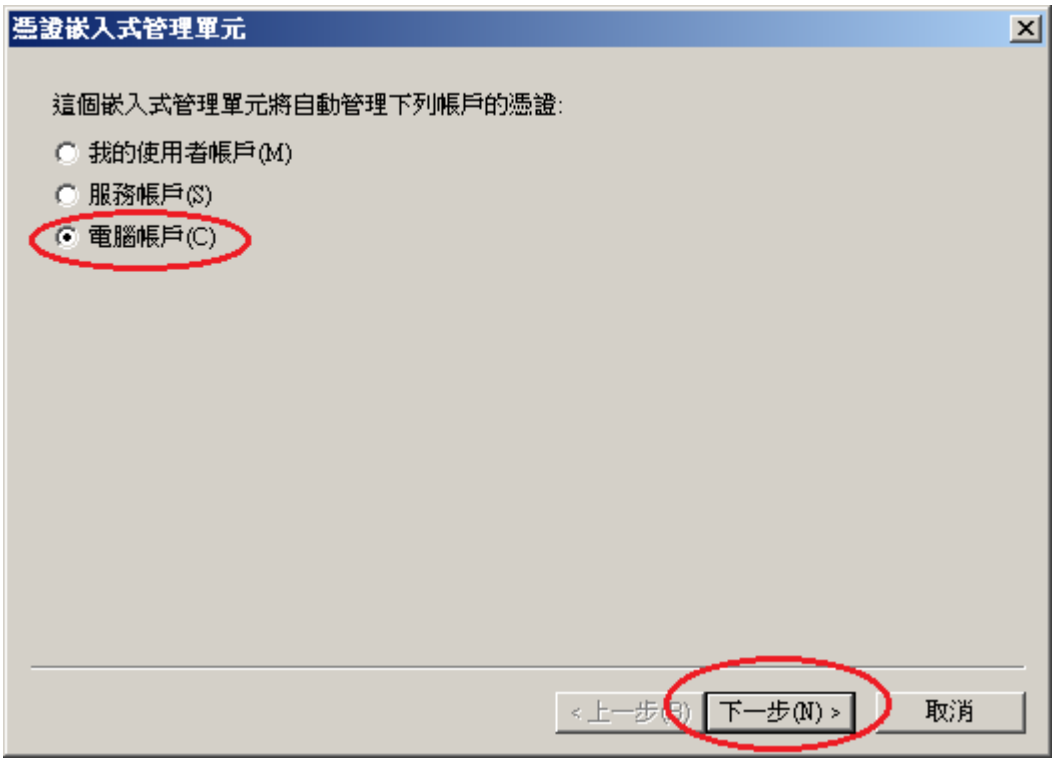
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。

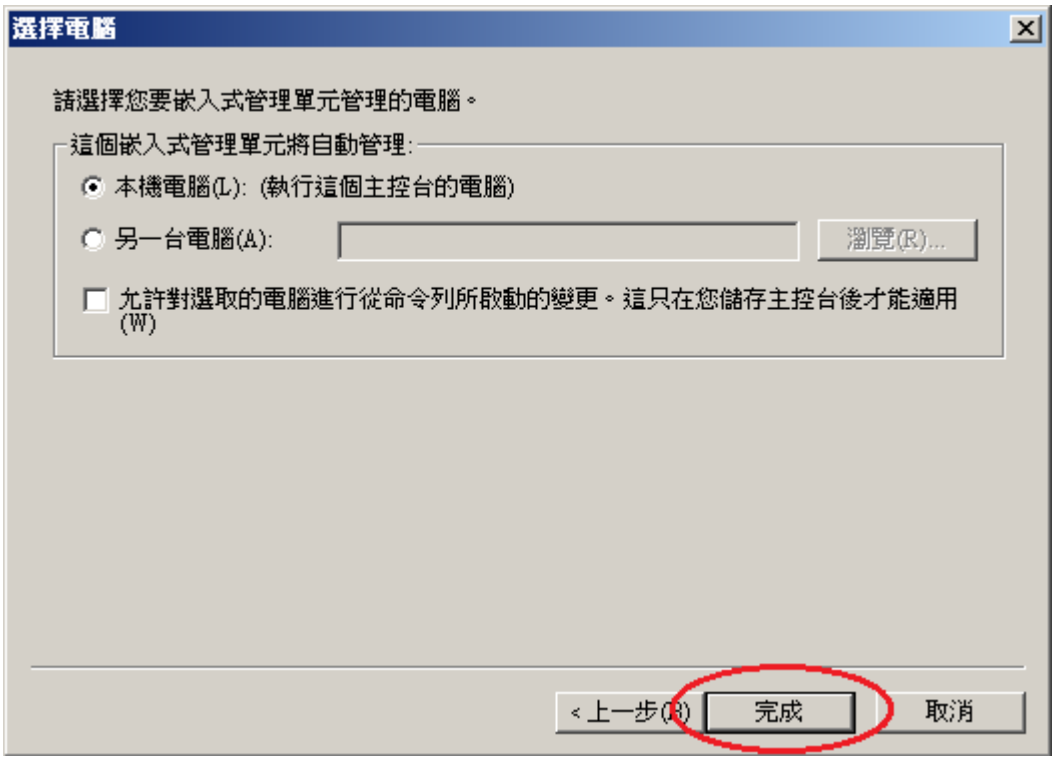


3. 點選「憑證」→「新增」

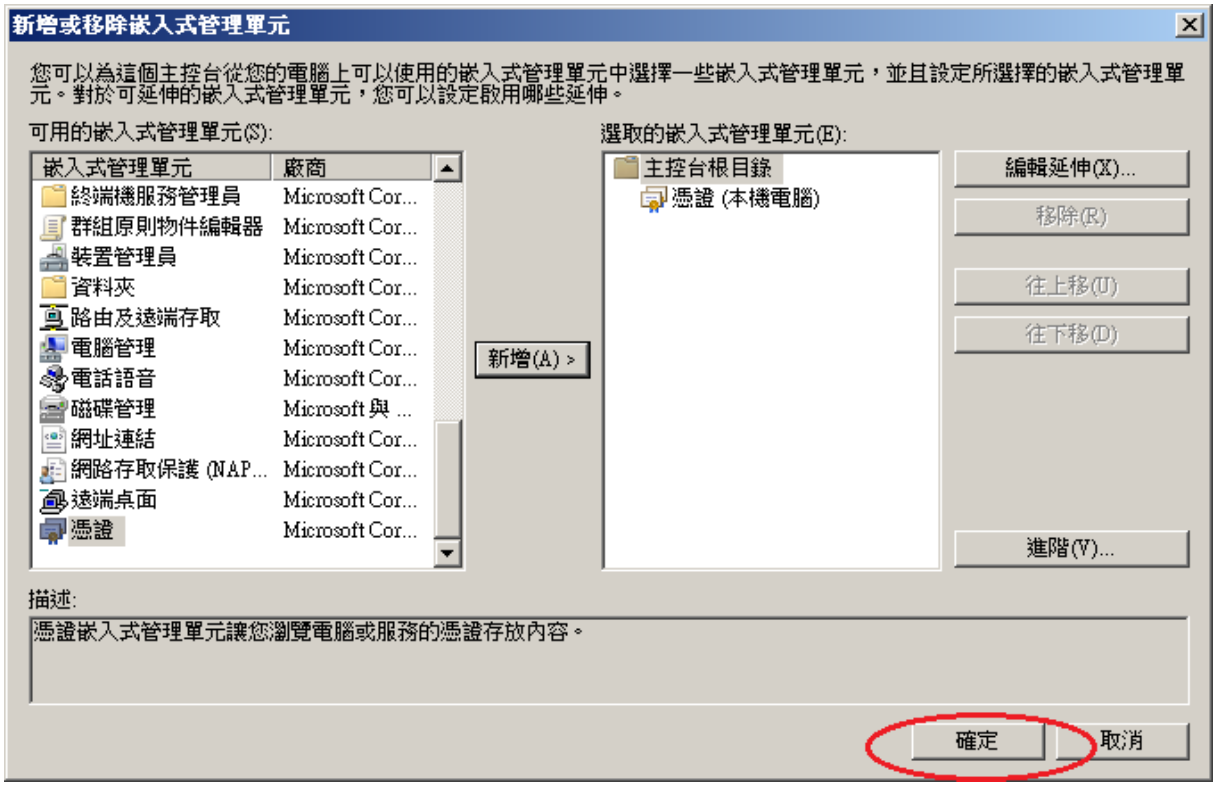


「電腦帳戶」→「下一步」→「完成」。

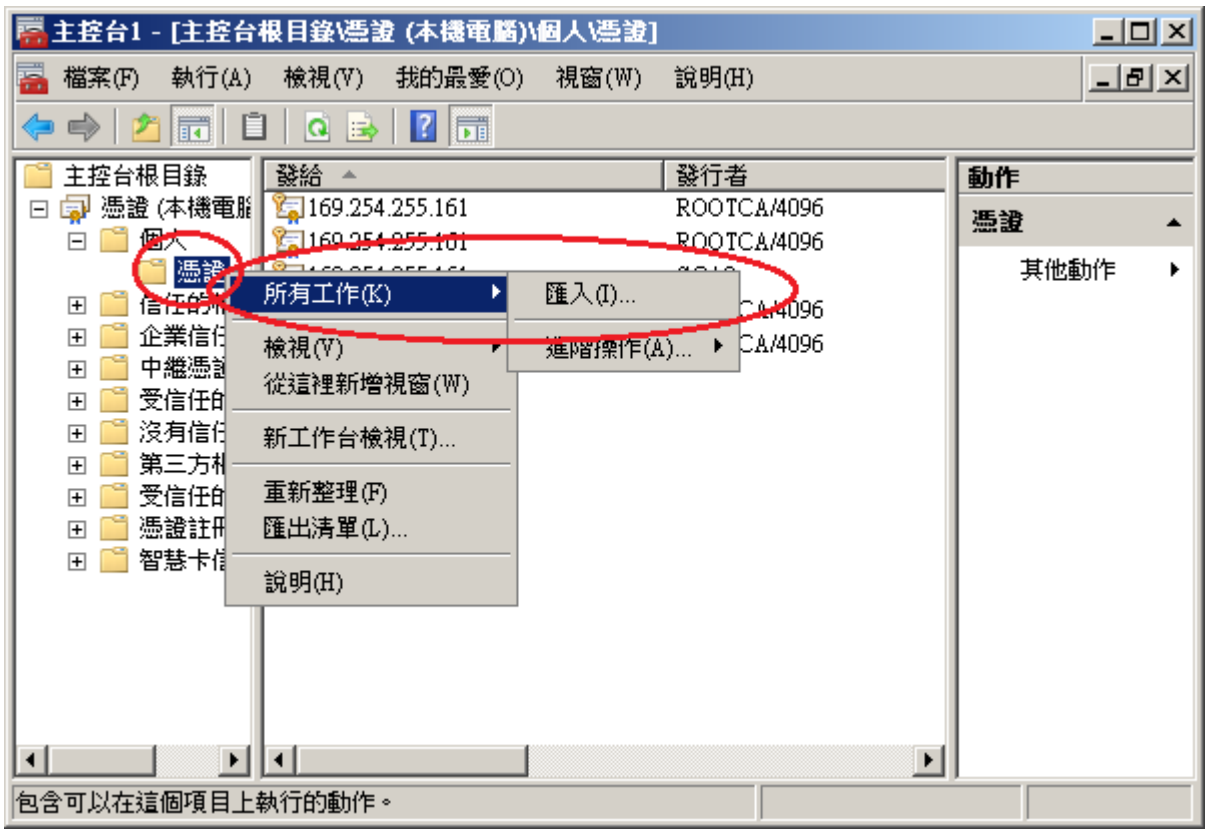

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


選擇電腦
請選擇您要嵌入式管理單元管理的電腦。
這個嵌入式管理單元將自動管理:
本機電腦(L): (執行這個主控台的電腦)
另一台電腦(A):
瀏覽(R)...
允許對選取的電腦進行從命令列所啟動的變更。這只在您儲存主控台後才能適用(W)
< 上一步(B)
完成
取消

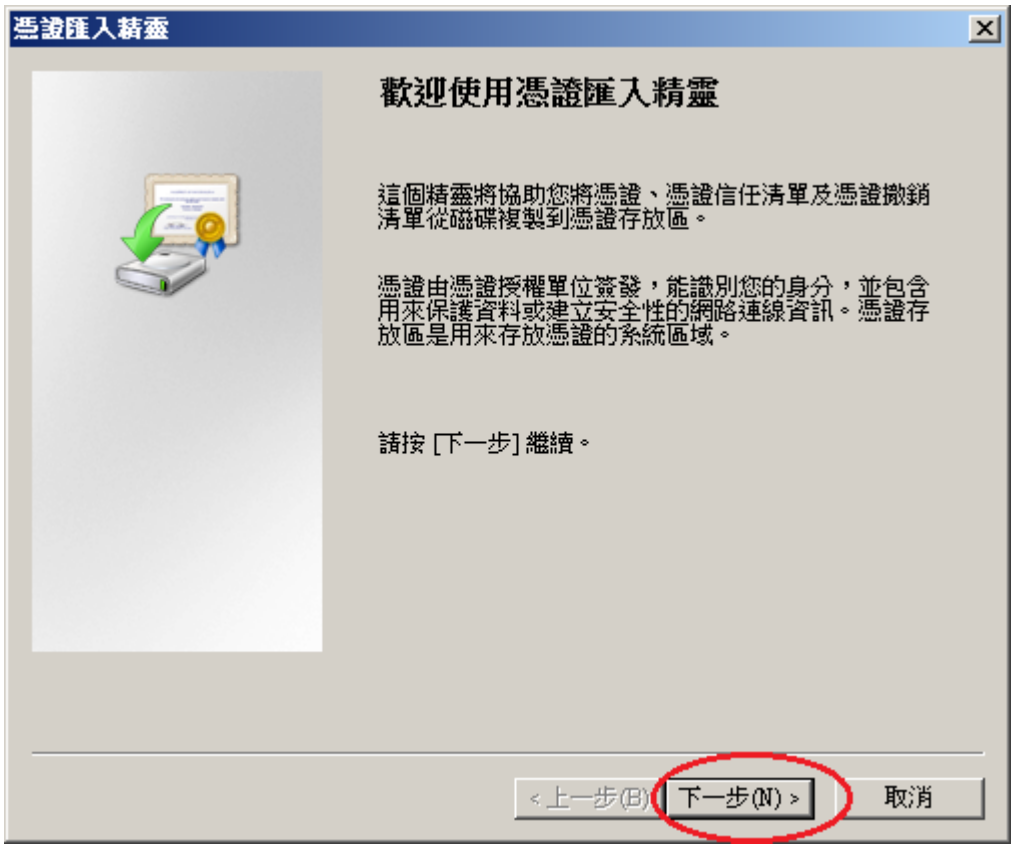
「確定」。

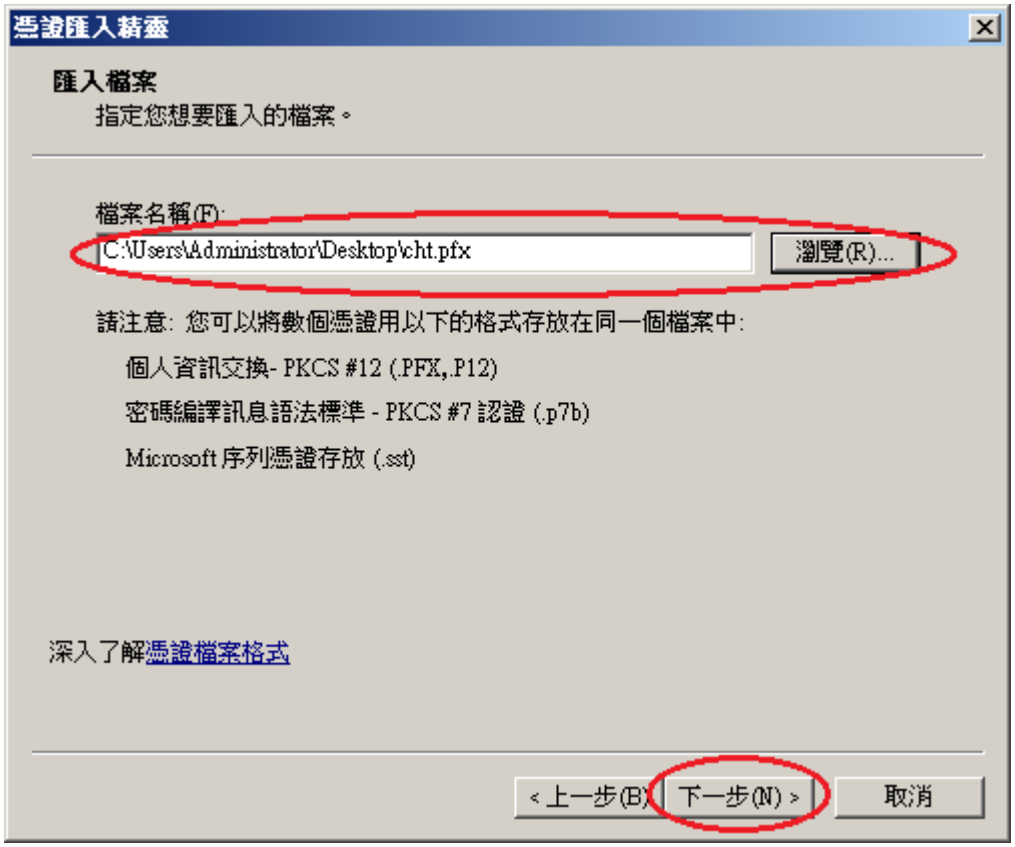


4. 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

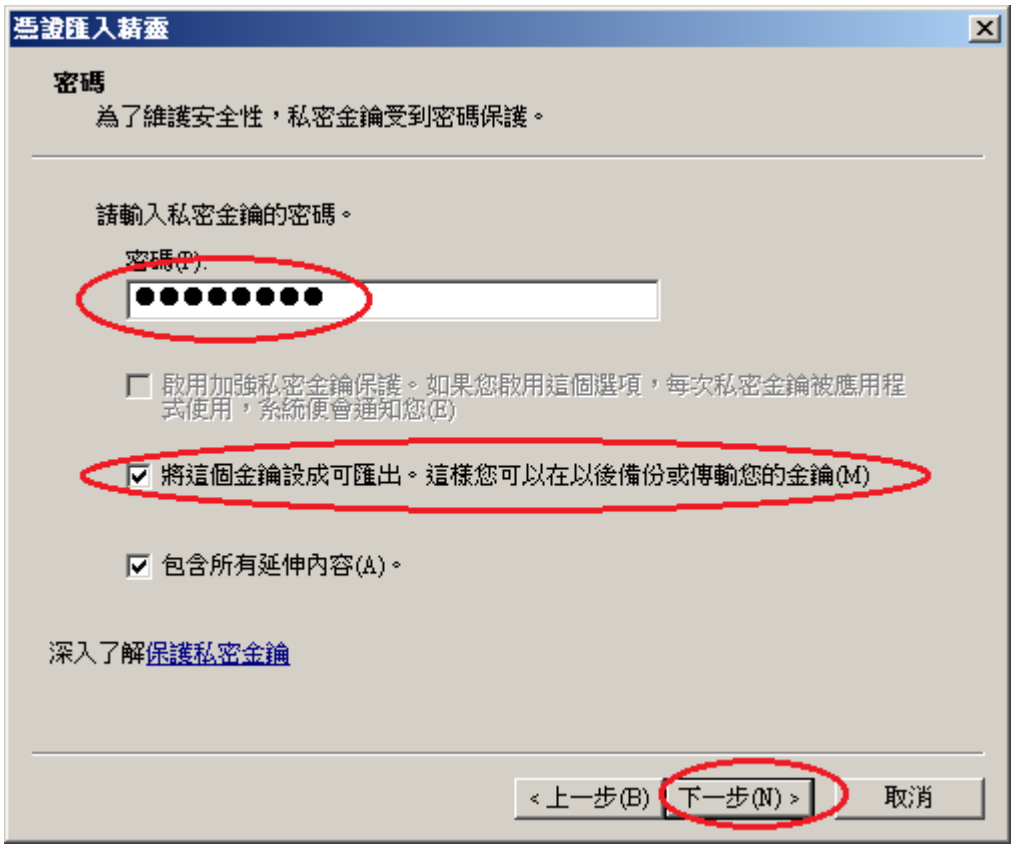


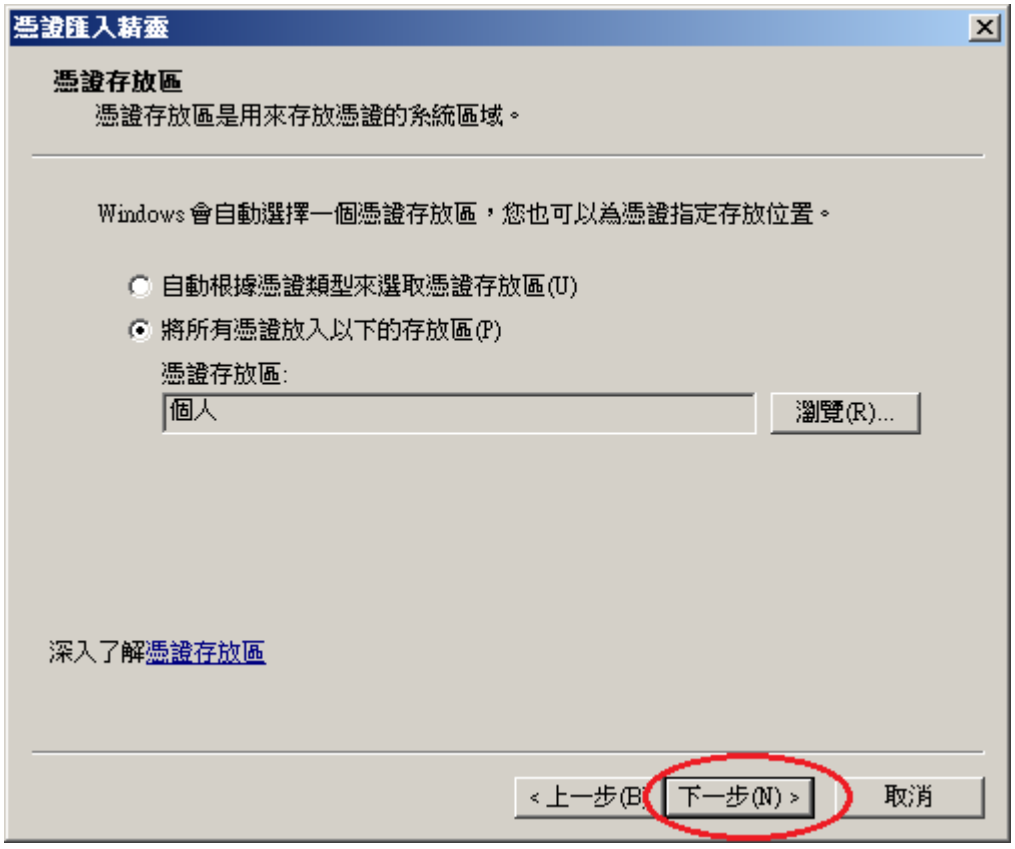
5. 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

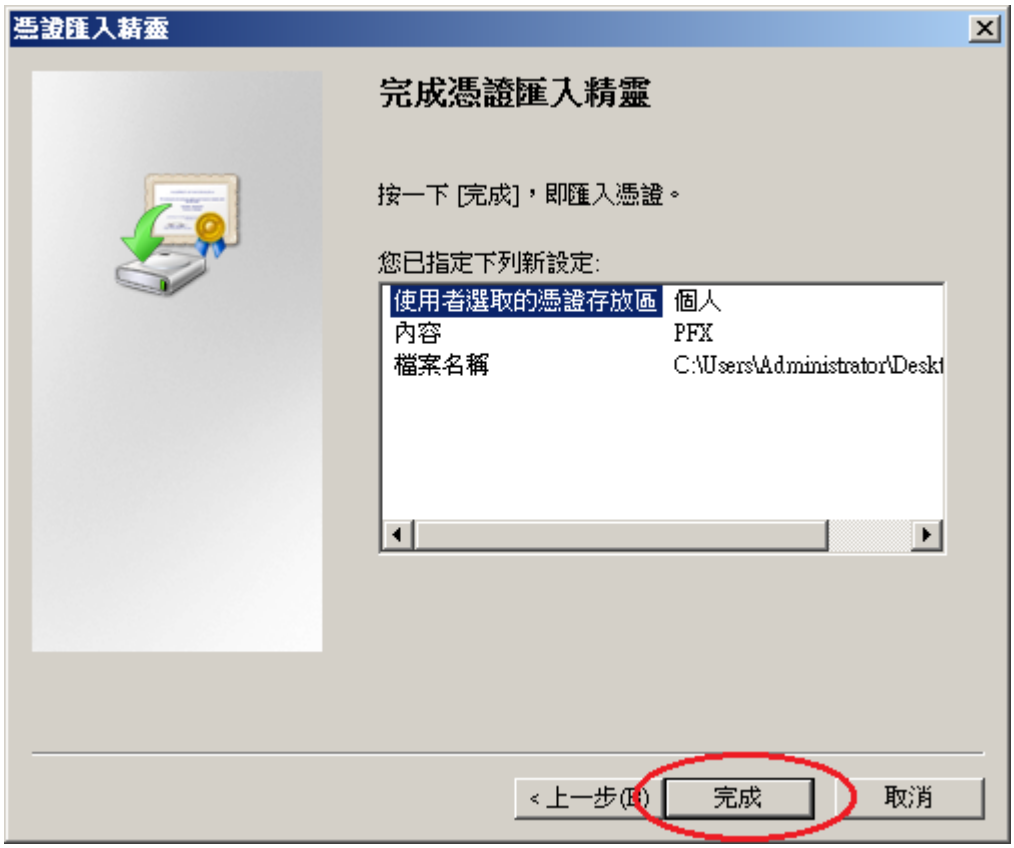




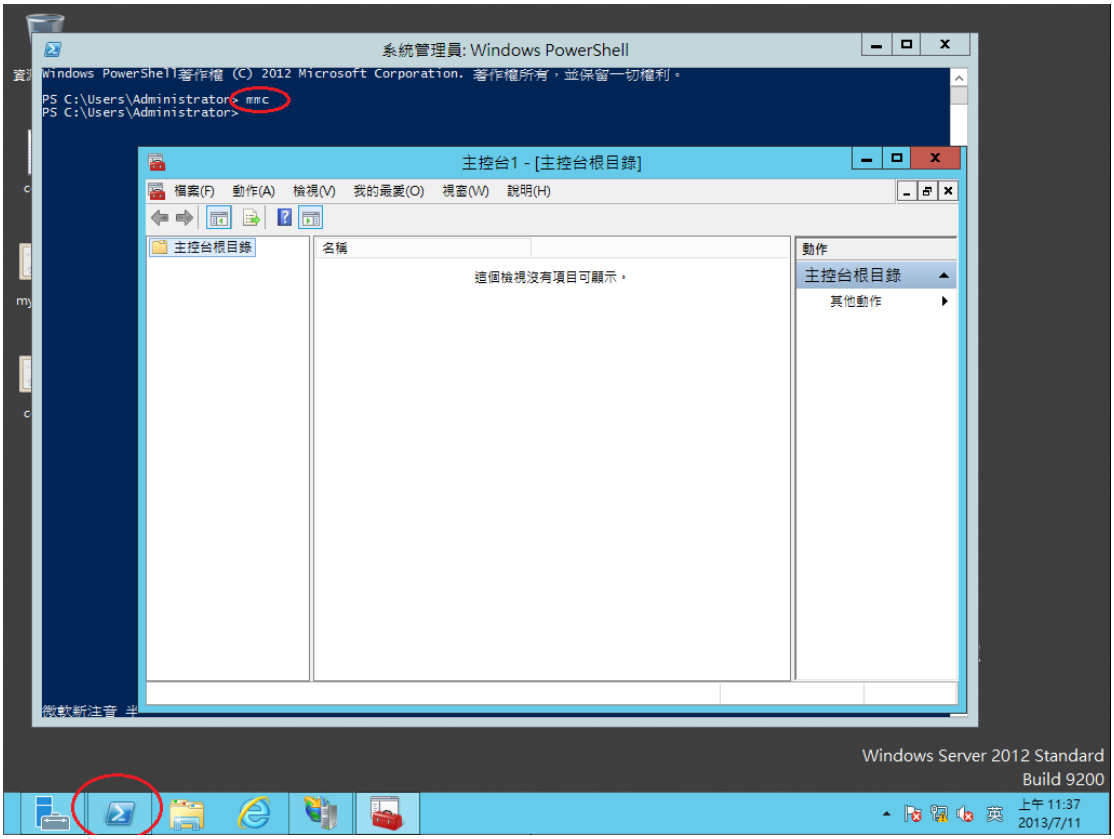
輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。


憑證匯入精靈
密碼
為了維護安全性，私密金鑰受到密碼保護。
請輸入私密金鑰的密碼。
密碼(P):
●●●●●●●●
啟用加強私密金鑰保護。如果您啟用這個選項，每次私密金鑰被應用程式使用，系統便會通知您(E)
將這個金鑰設成可匯出。這樣您可以在以後備份或傳輸您的金鑰(M)
包含所有延伸內容(A)。
深入了解保護私密金鑰
< 上一步(B)
下一步(N) >
取消

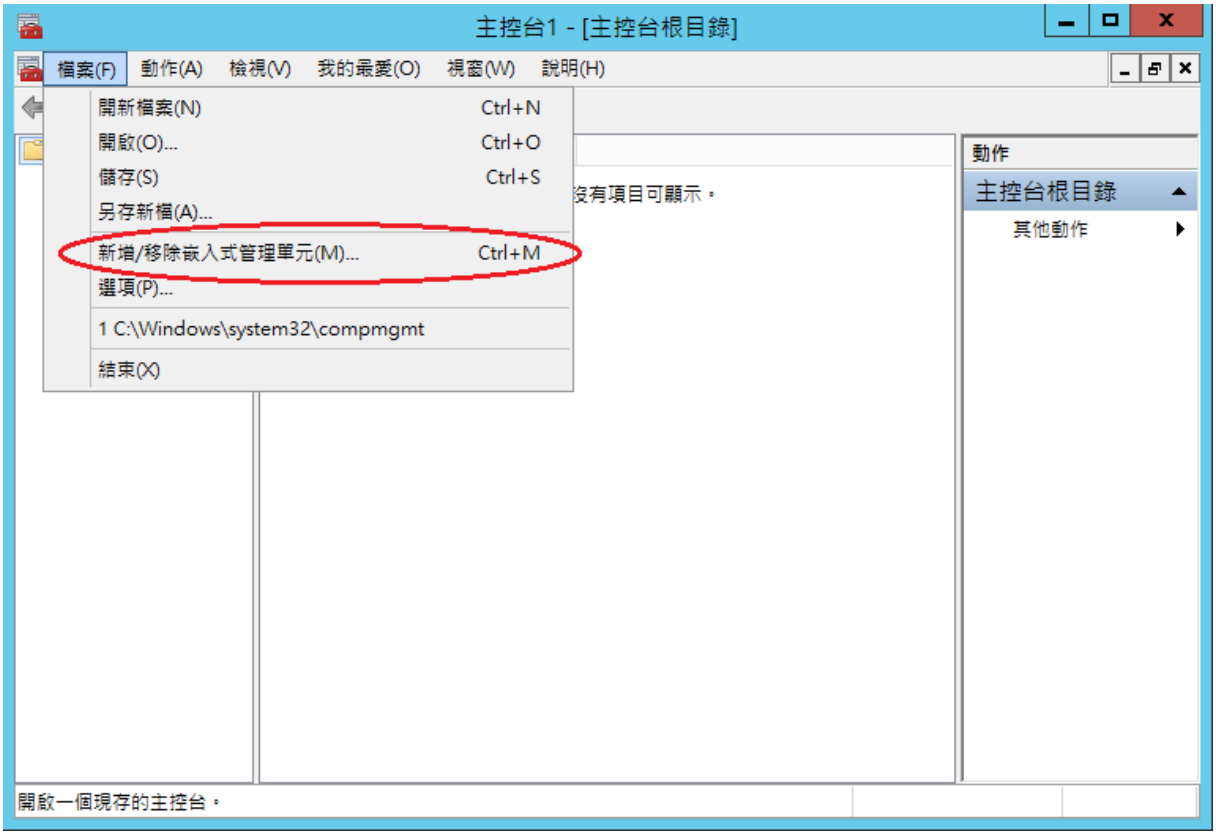

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 會自動選擇一個憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
個人
瀏覽(R)...
深入了解憑證存放區
< 上一步(B)
下一步(N) >
取消


憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即匯入憑證。
您已指定下列新設定:
使用者選取的憑證存放區
個人
內容
PFX
檔案名稱
C:\Users\Administrator\Deskt
< 上一步(B)
完成
取消

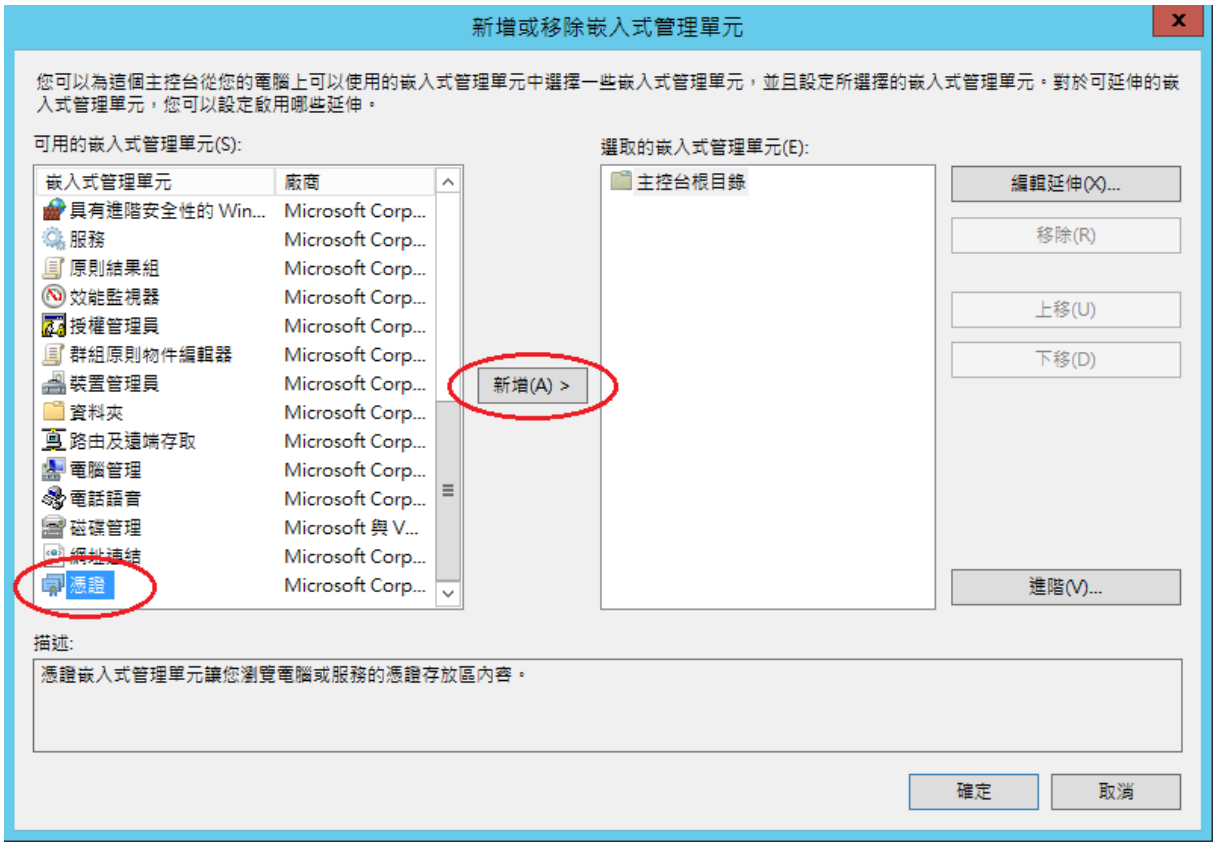
1. 請先點選左下角的「Windows PowerShell」→輸入「mmc」→按下「Enter」。



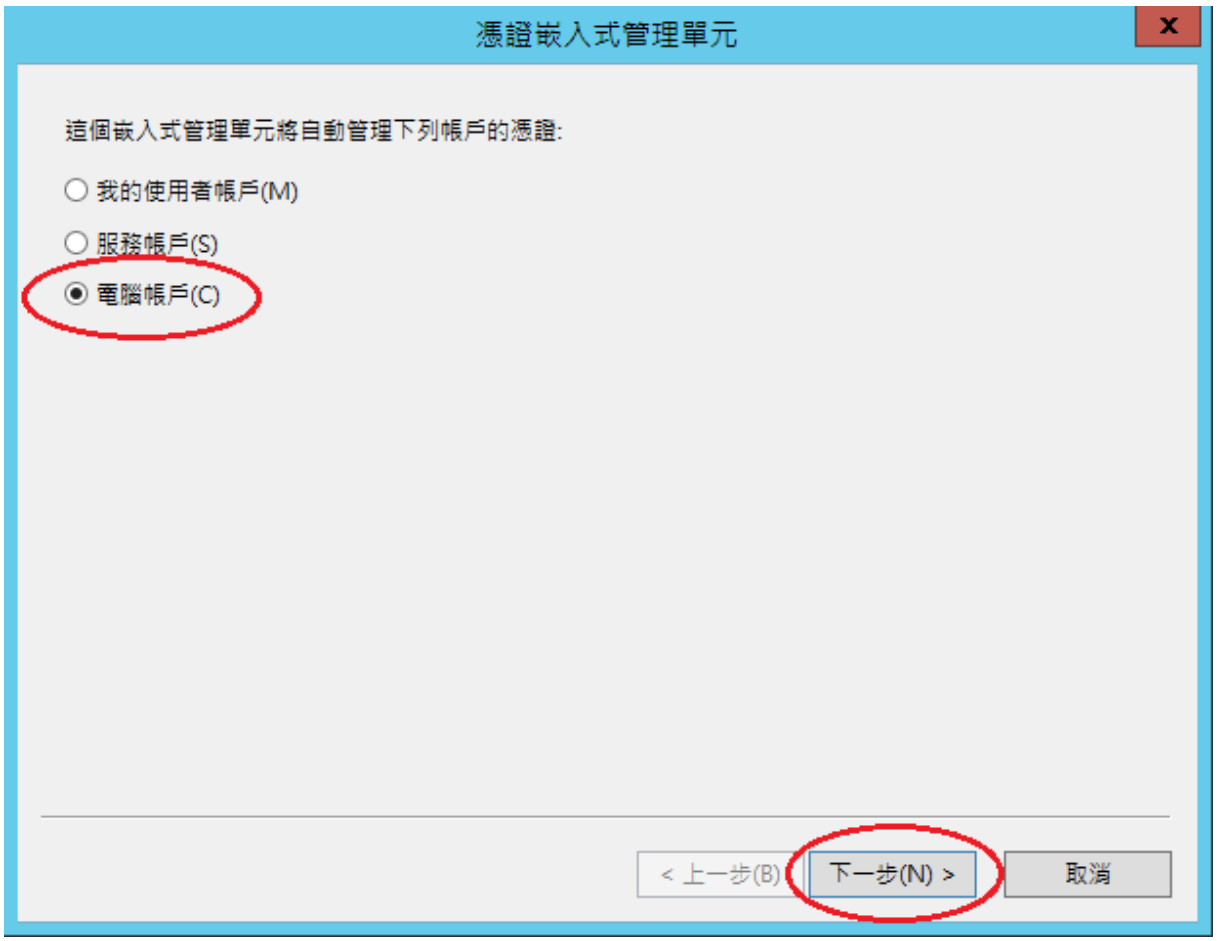
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。

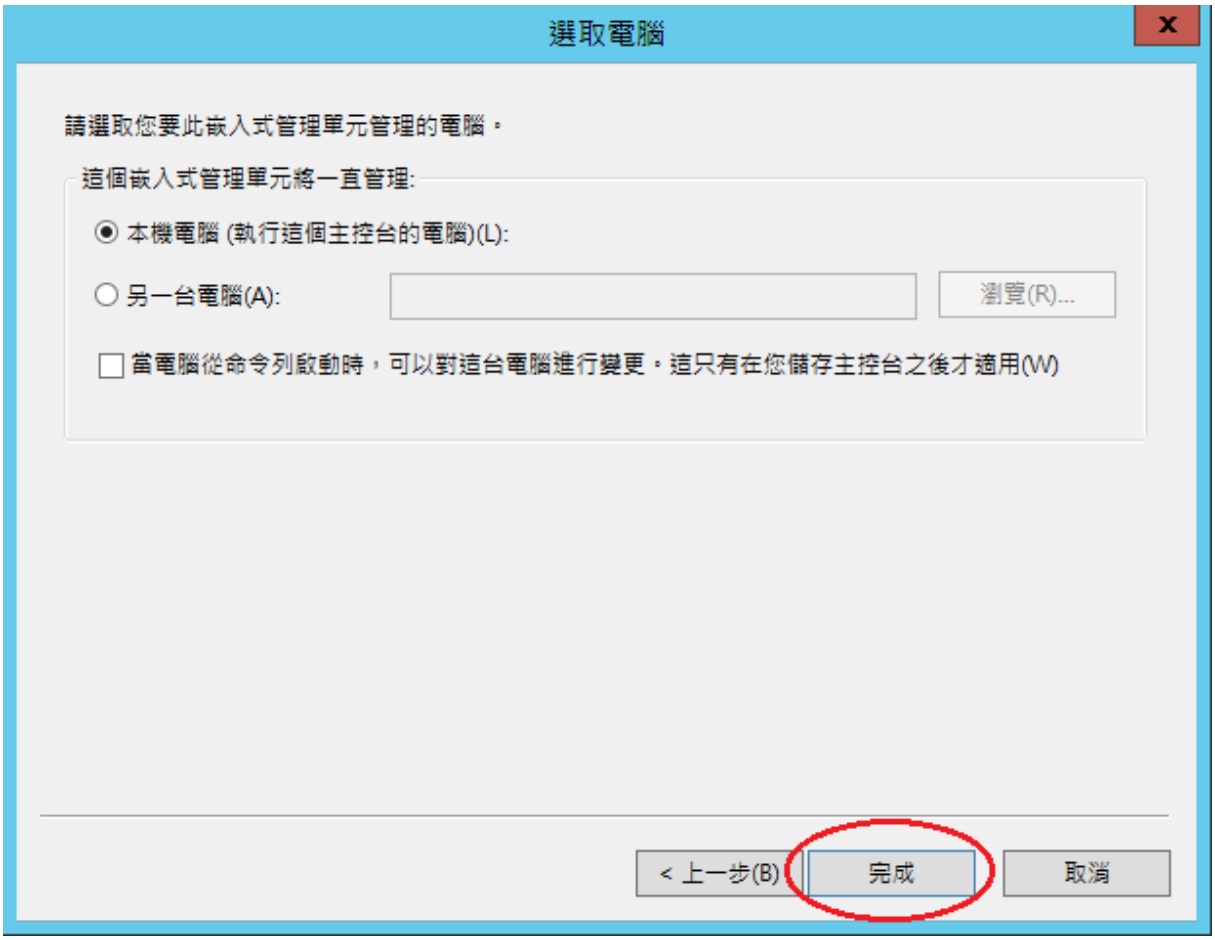


3. 點選「憑證」→「新增」

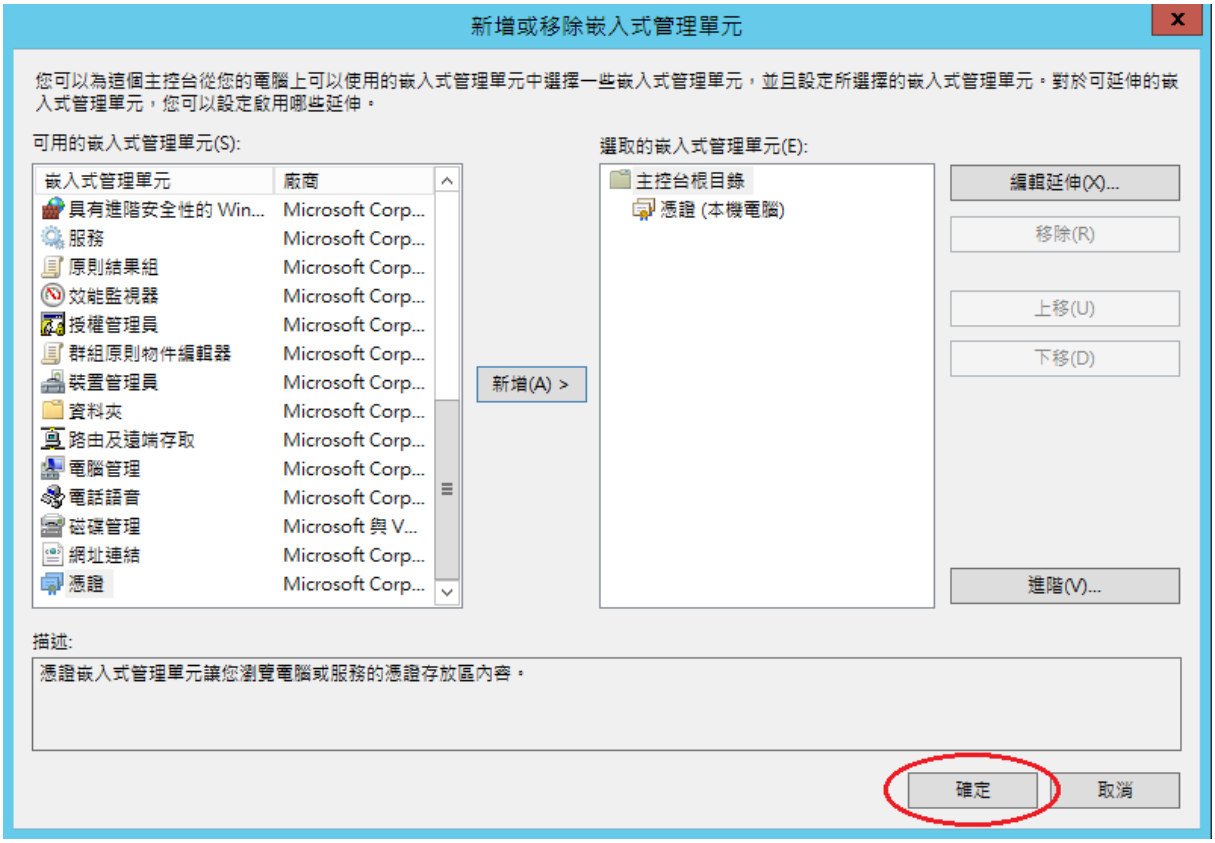


「電腦帳戶」→「下一步」→「完成」。

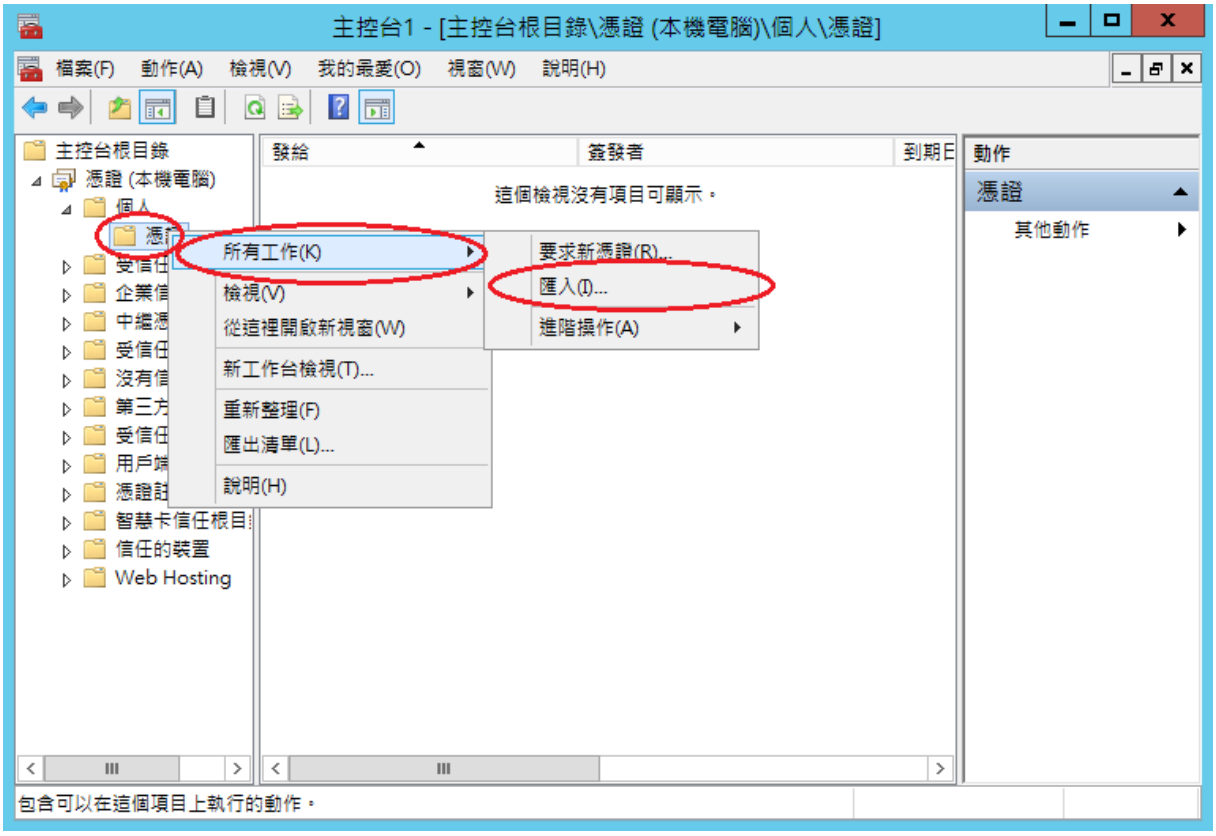




「確定」。

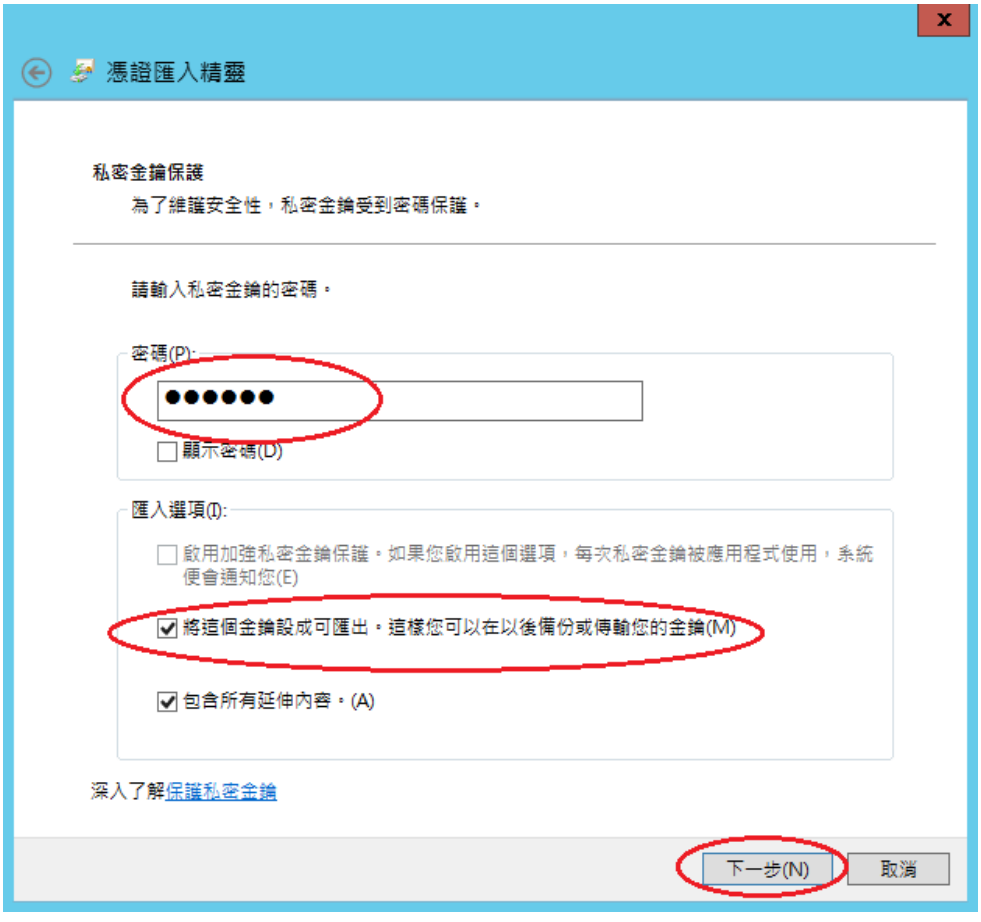


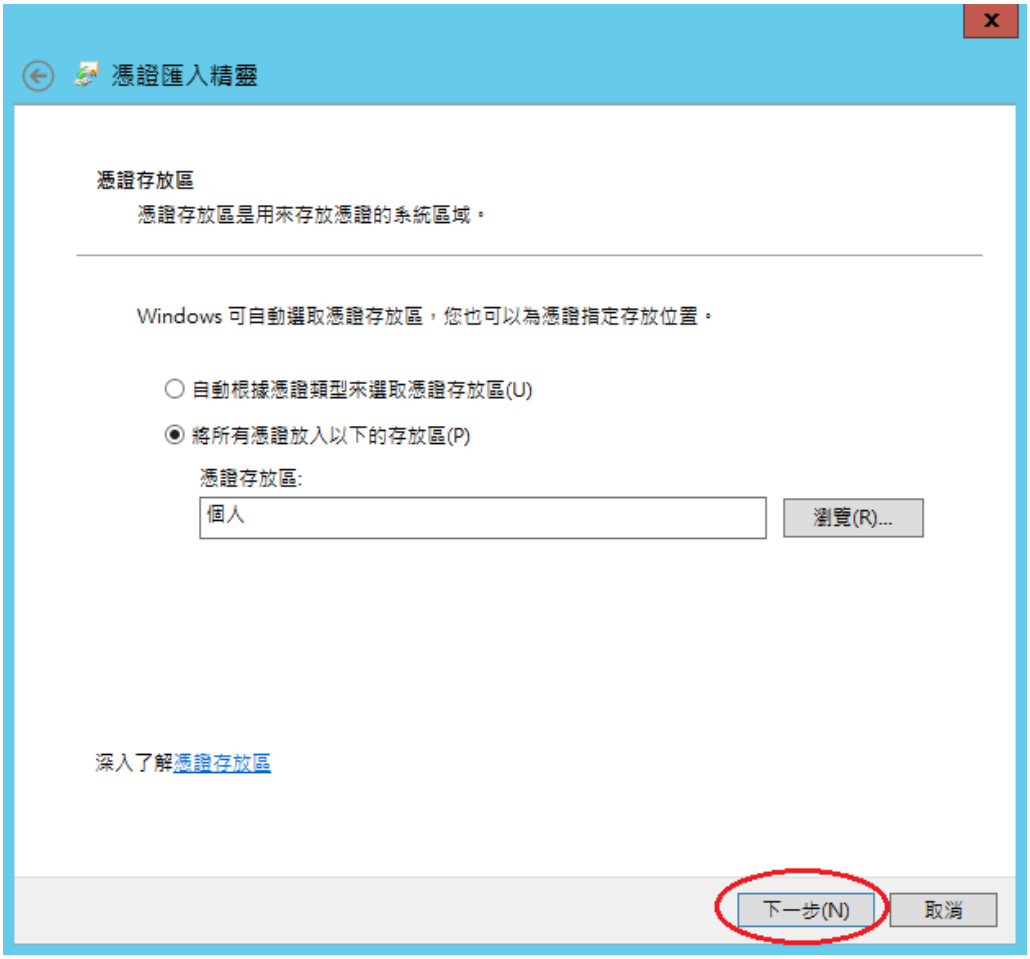
4. 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

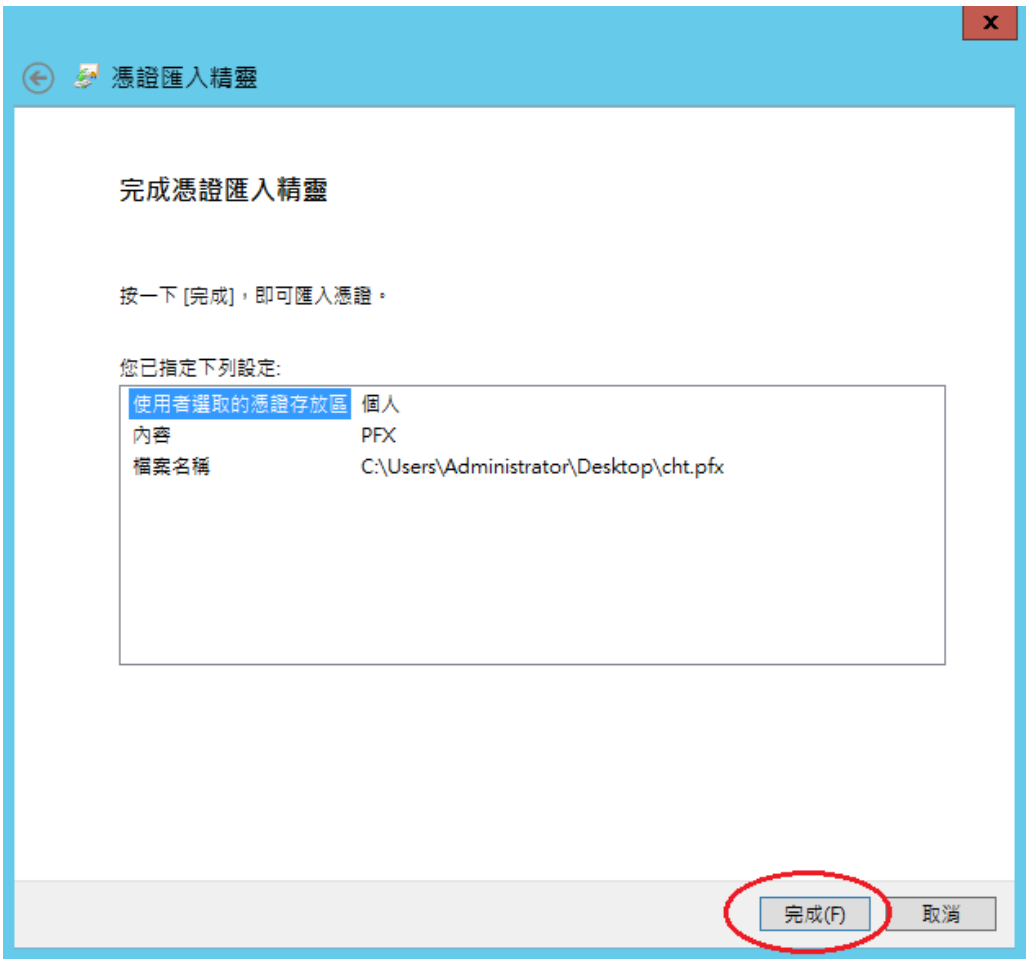


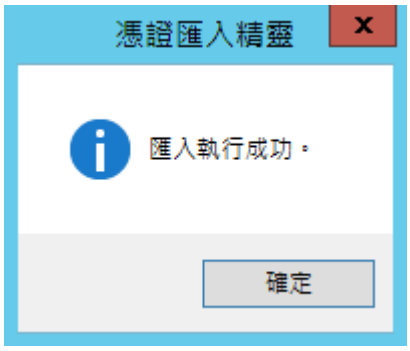
5. 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。

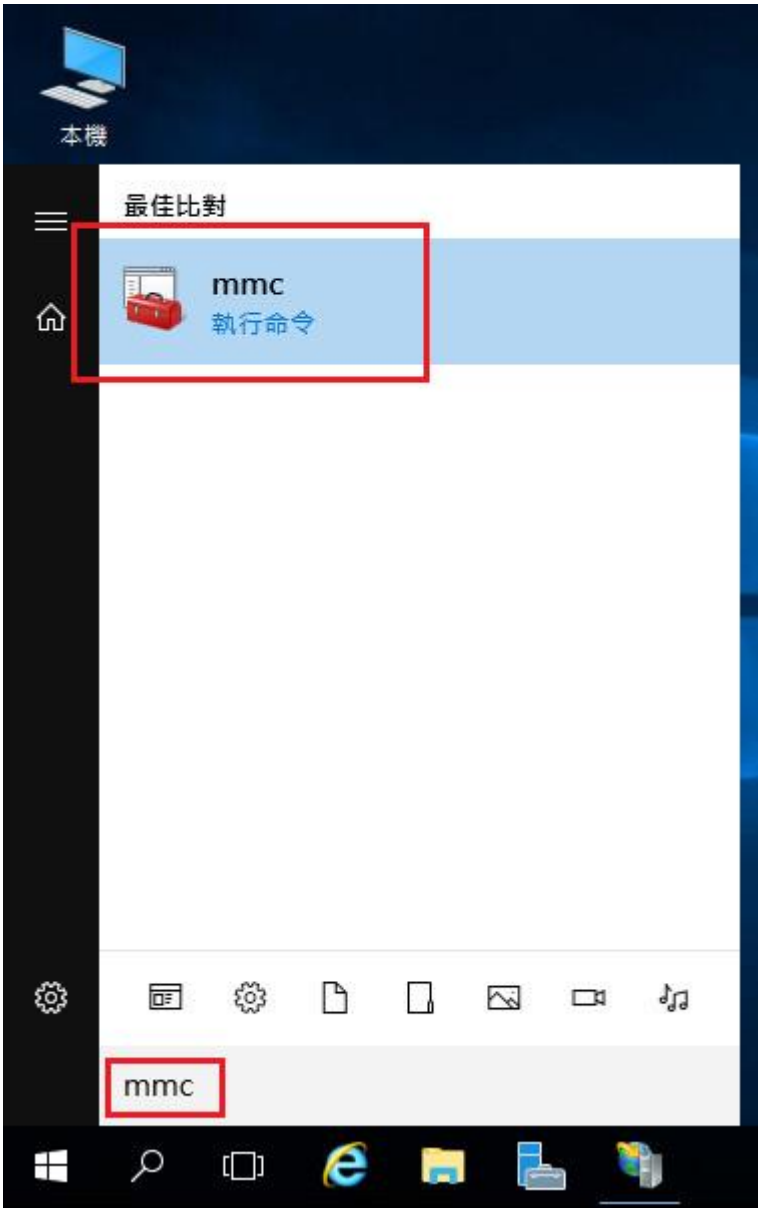



憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
個人
瀏覽(R)...
深入了解憑證存放區
下一步(N)
取消

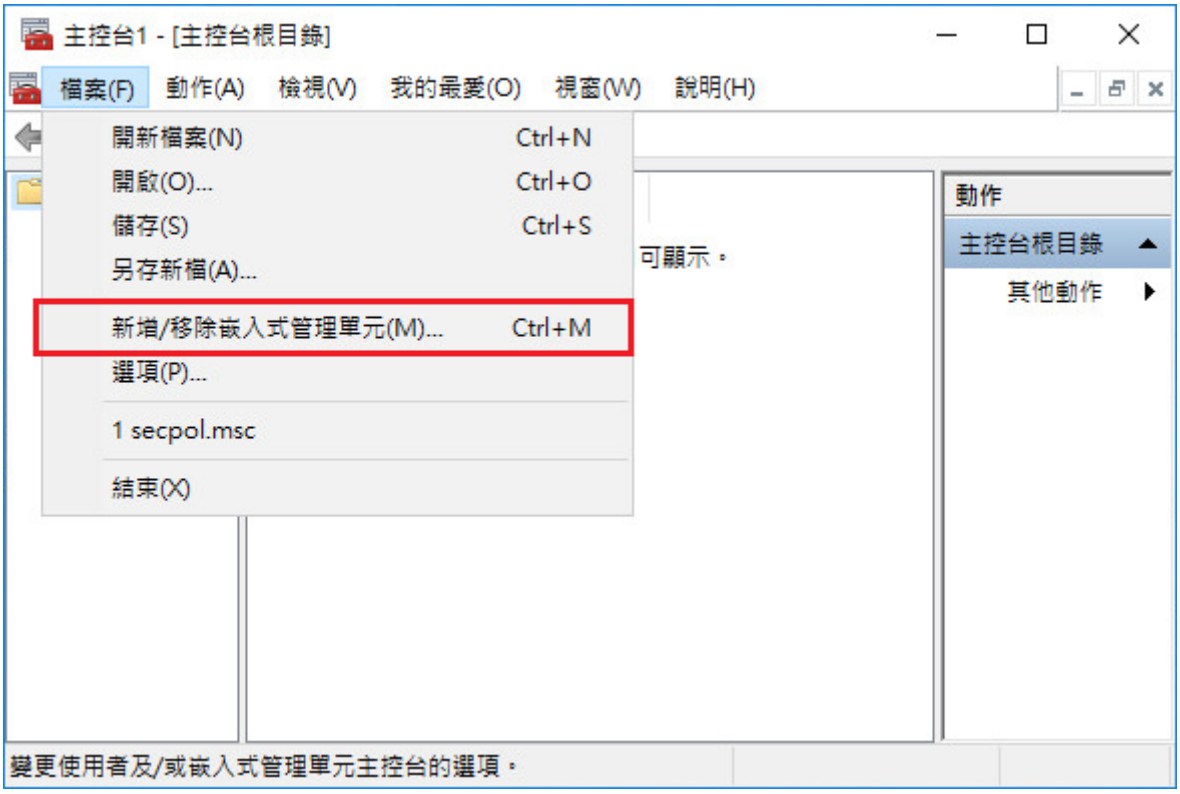

憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即可匯入憑證。
您已指定下列設定:
使用者選取的憑證存放區 個人
內容 PFX
檔案名稱 C:\Users\Administrator\Desktop\cht.pfx
完成(F)
取消


憑證匯入精靈
匯入執行成功。
確定

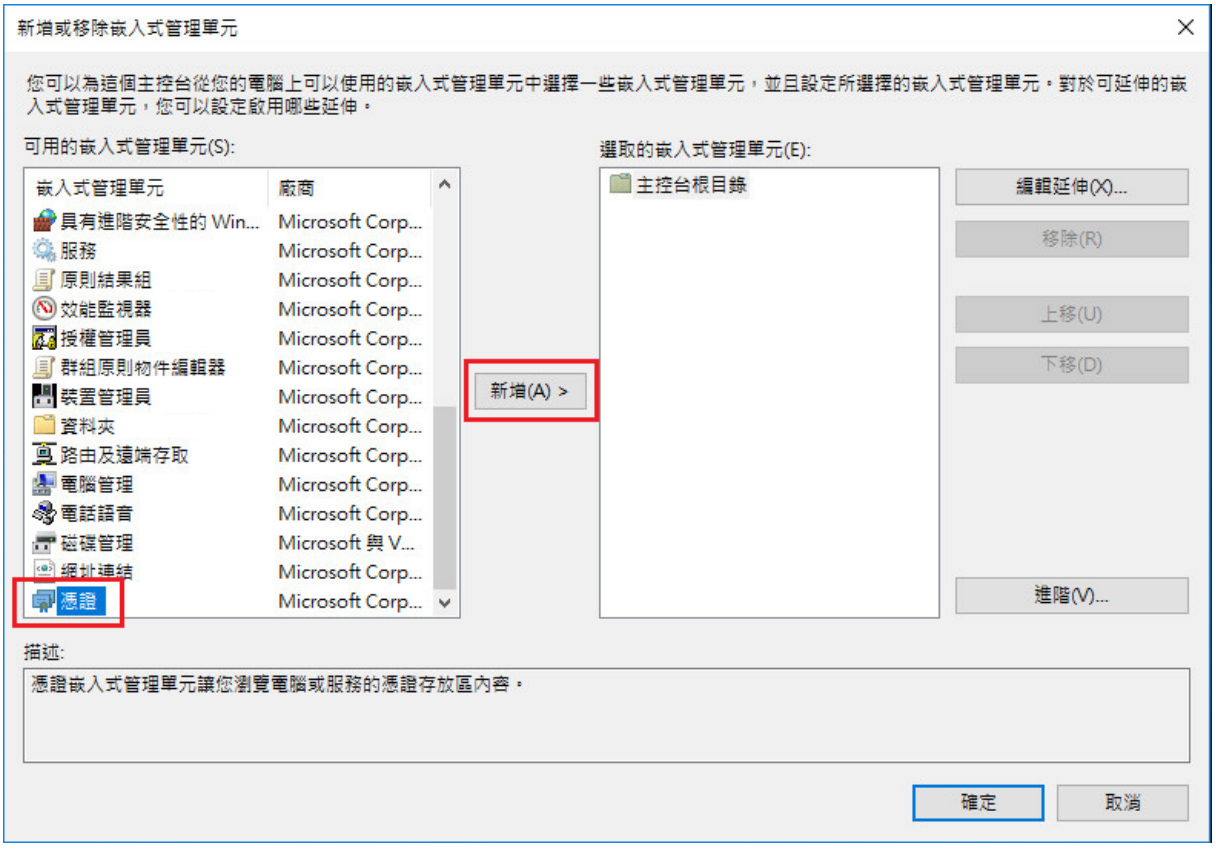
1. 「開始」→「輸入 mmc」，按下「Enter」。



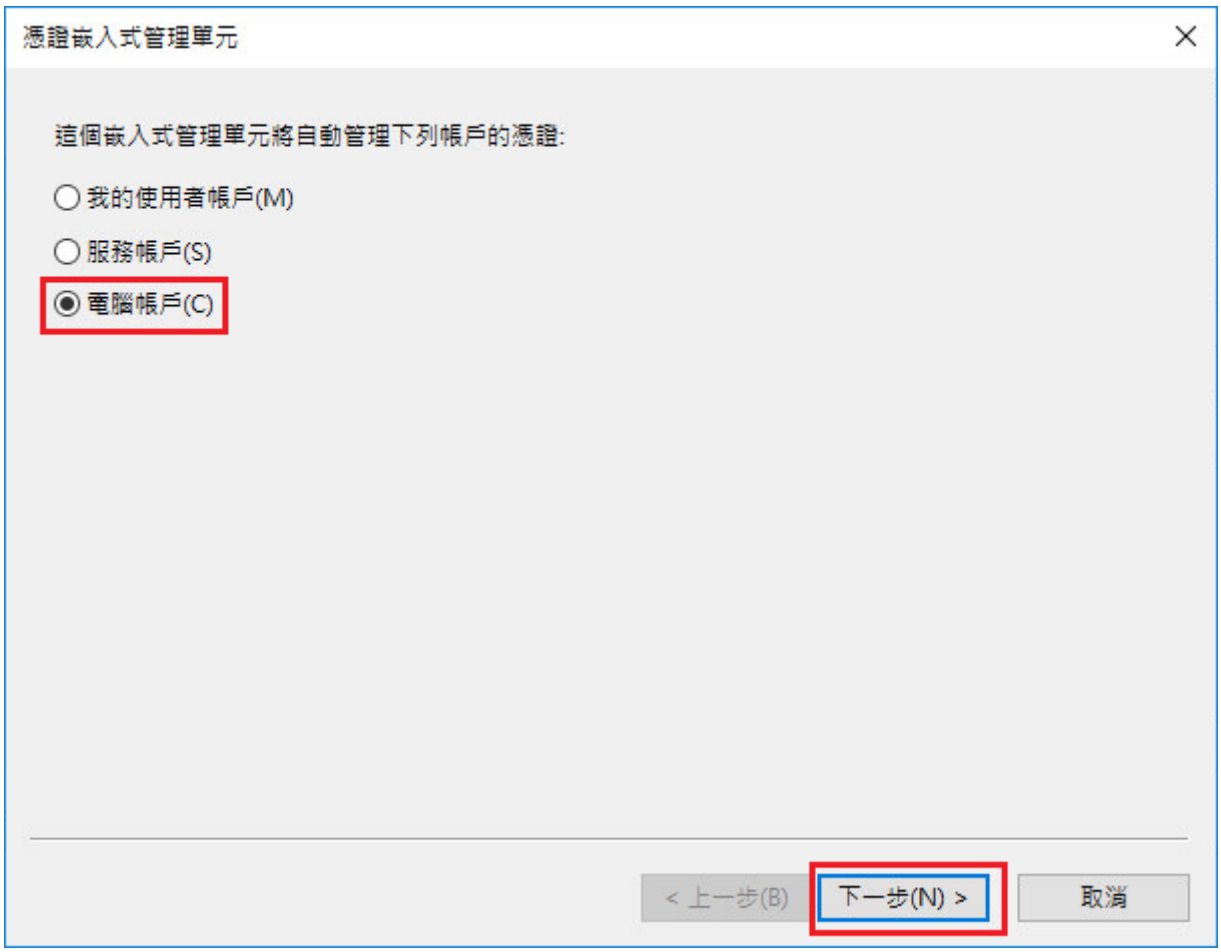
2. 選擇「檔案」→「新增/移除嵌入式管理單元」。

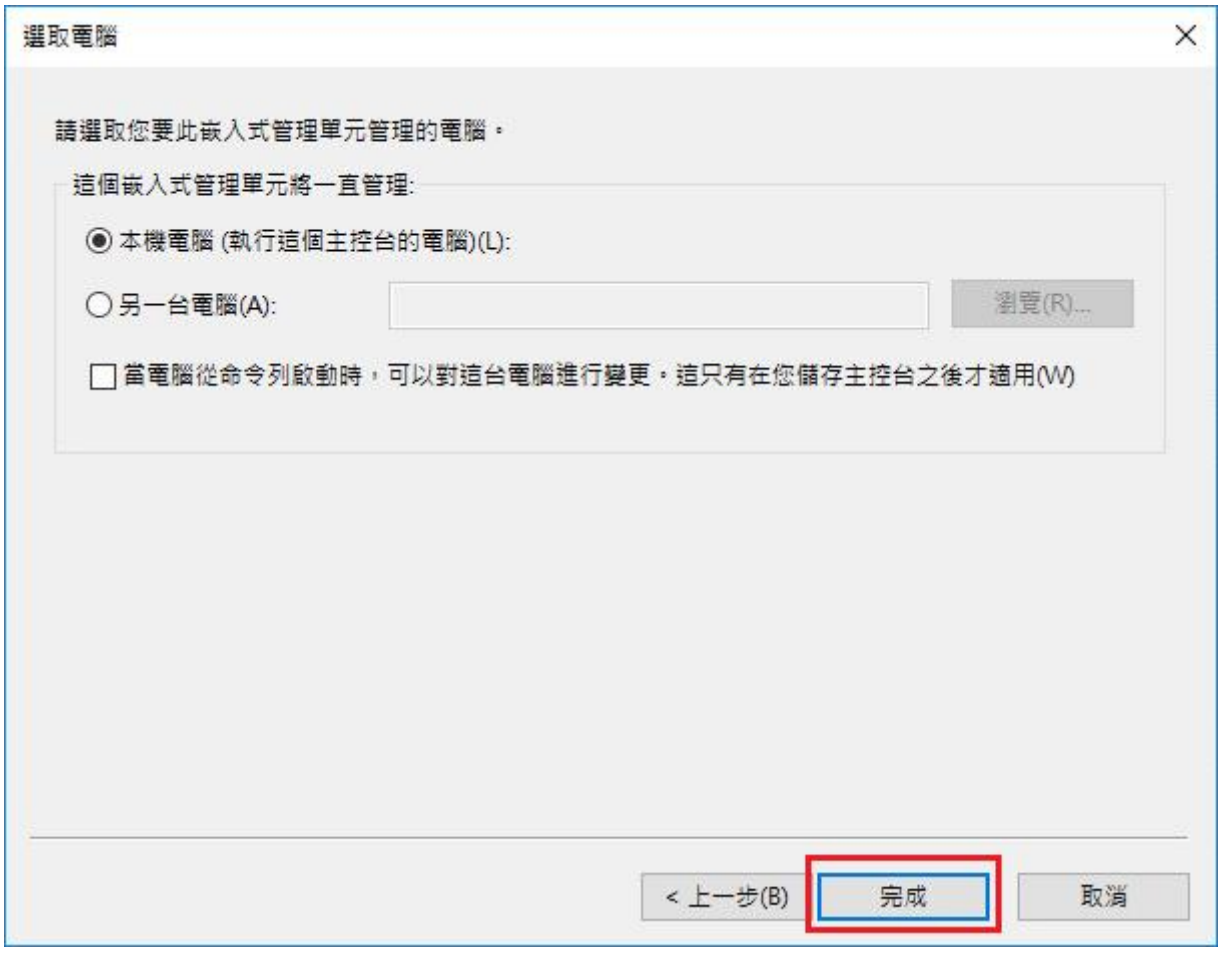


3. 點選「憑證」→「新增」

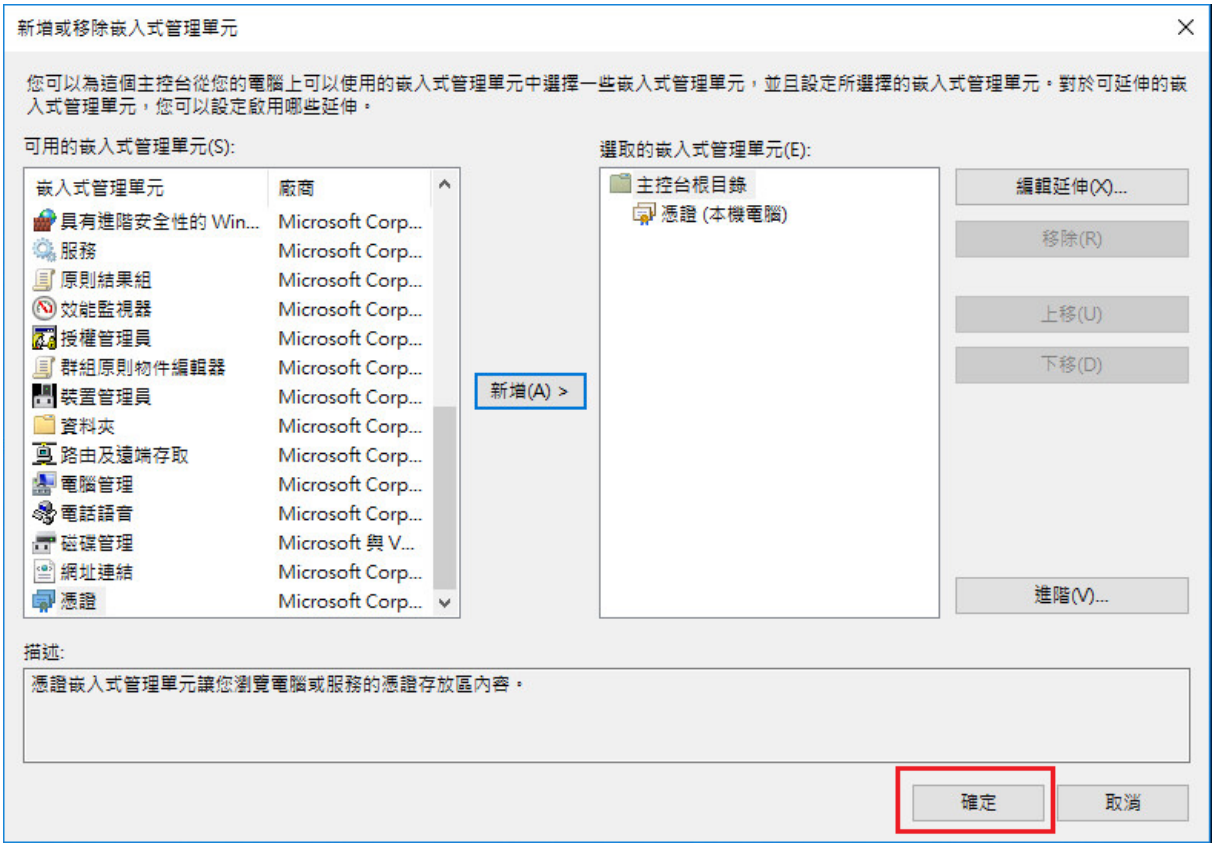


「電腦帳戶」→「下一步」→「完成」。

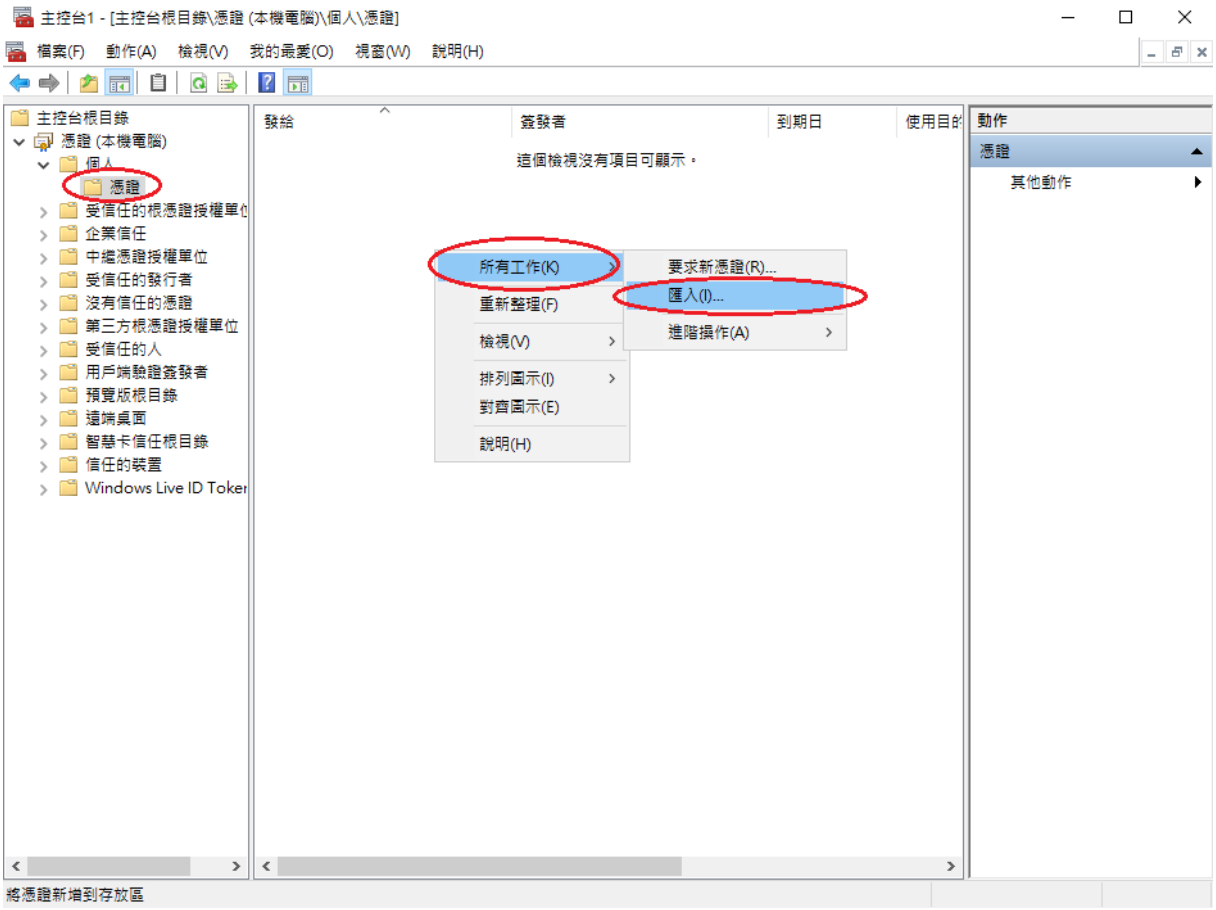

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消


選取電腦
請選取您要此嵌入式管理單元管理的電腦。
這個嵌入式管理單元將一直管理:
本機電腦 (執行這個主控台的電腦)(L):
另一台電腦(A):
瀏覽(R)...
當電腦從命令列啟動時，可以對這台電腦進行變更。這只有在您儲存主控台之後才適用(W)
< 上一步(B)
完成
取消

「確定」。

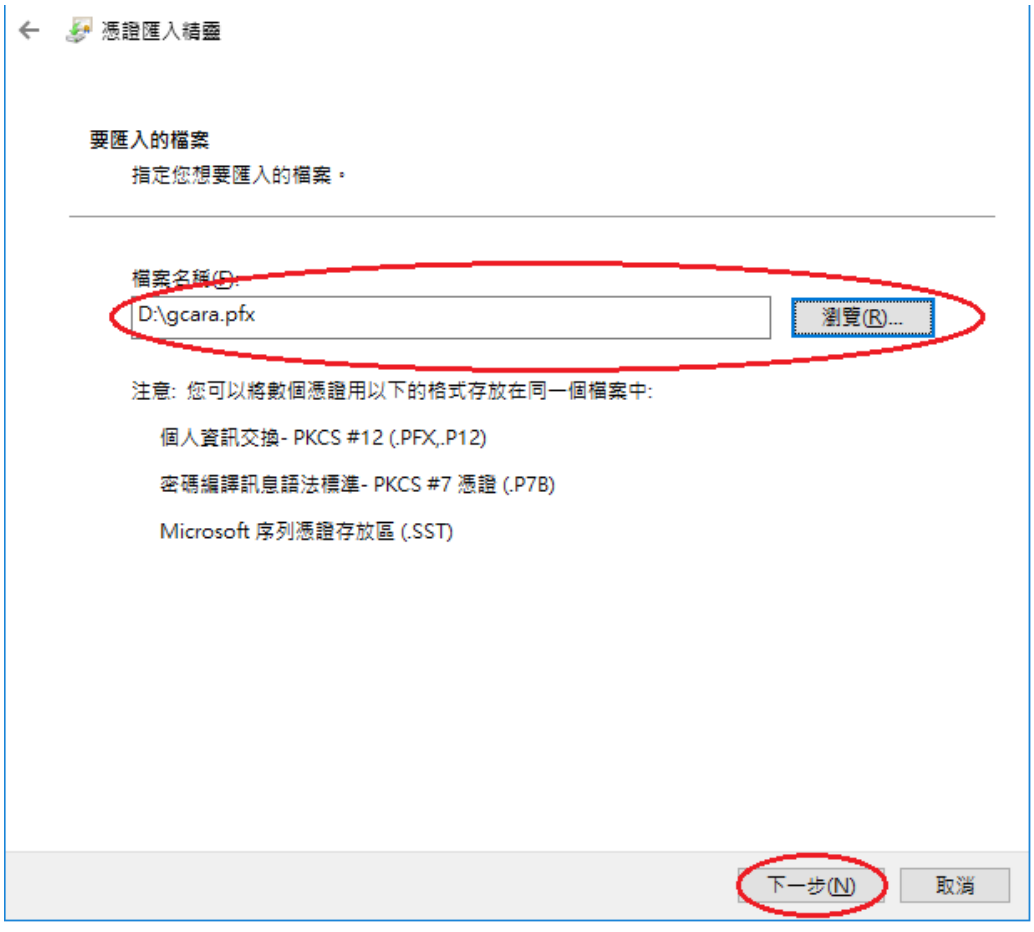


4. 點選到個人下的憑證，按下右鍵「所有工作」→「匯入」

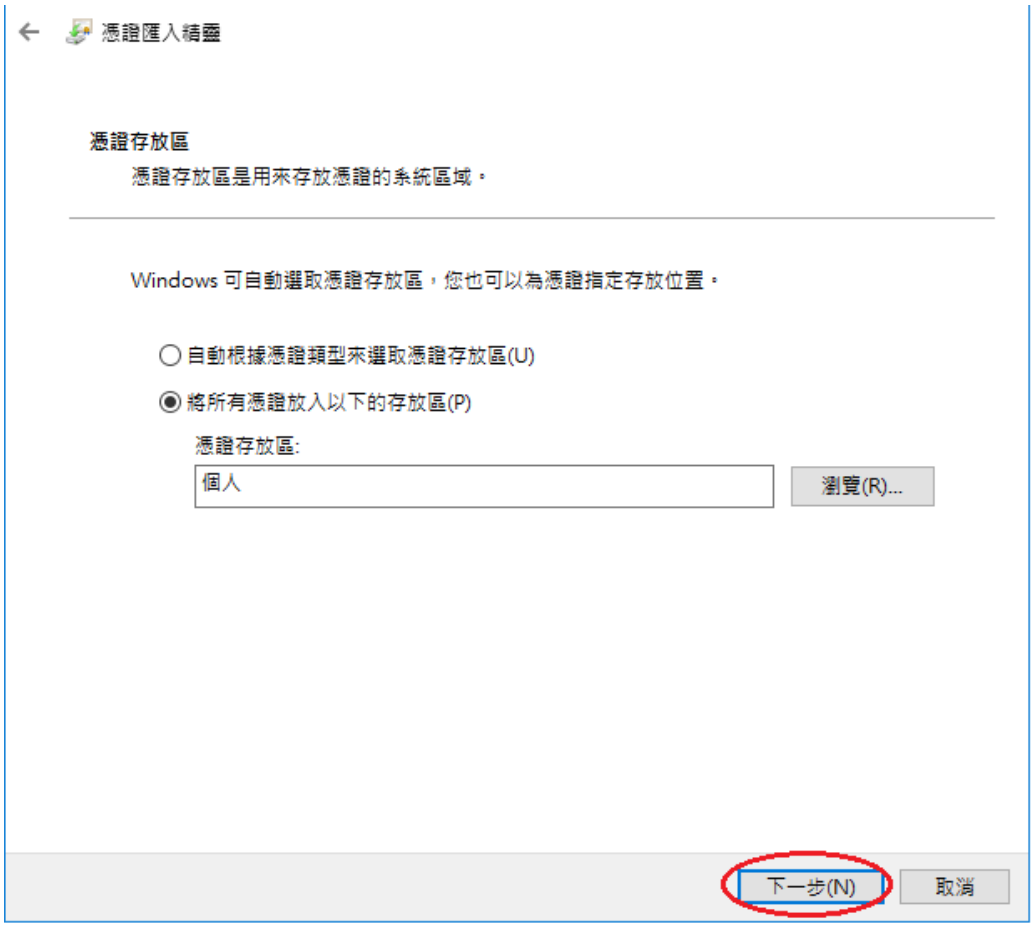


5. 選擇之前備份的憑證檔，輸入密碼來執行匯入動作。

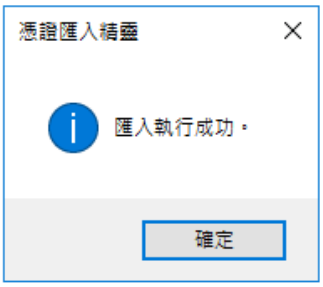

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消


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

輸入匯出時設定之密碼，以及勾選「將這個金鑰設成可匯出」。


憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
個人
瀏覽(R)...
下一步(N)
取消

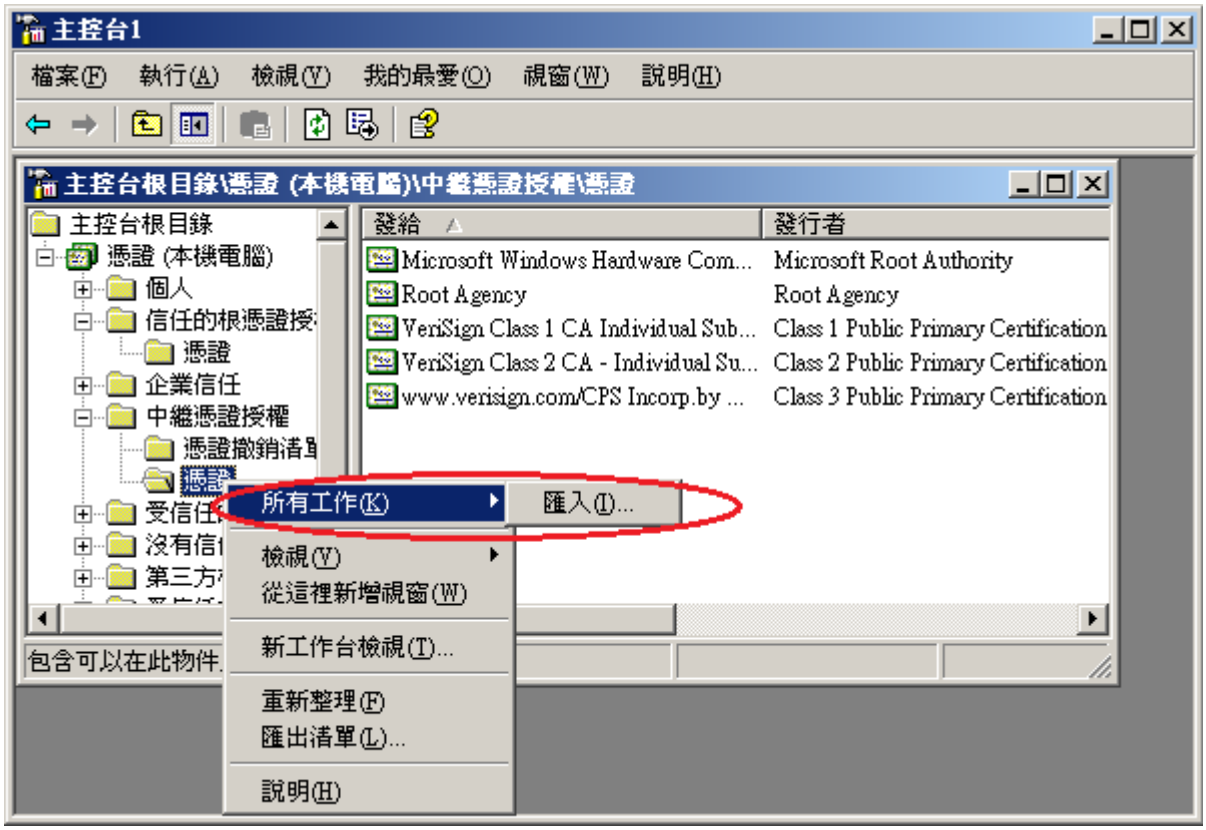

憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即可匯入憑證。
您已指定下列設定:
使用者選取的憑證存放區 個人
內容 PFX
檔案名稱 D:\gcara.pfx
完成(F)
取消

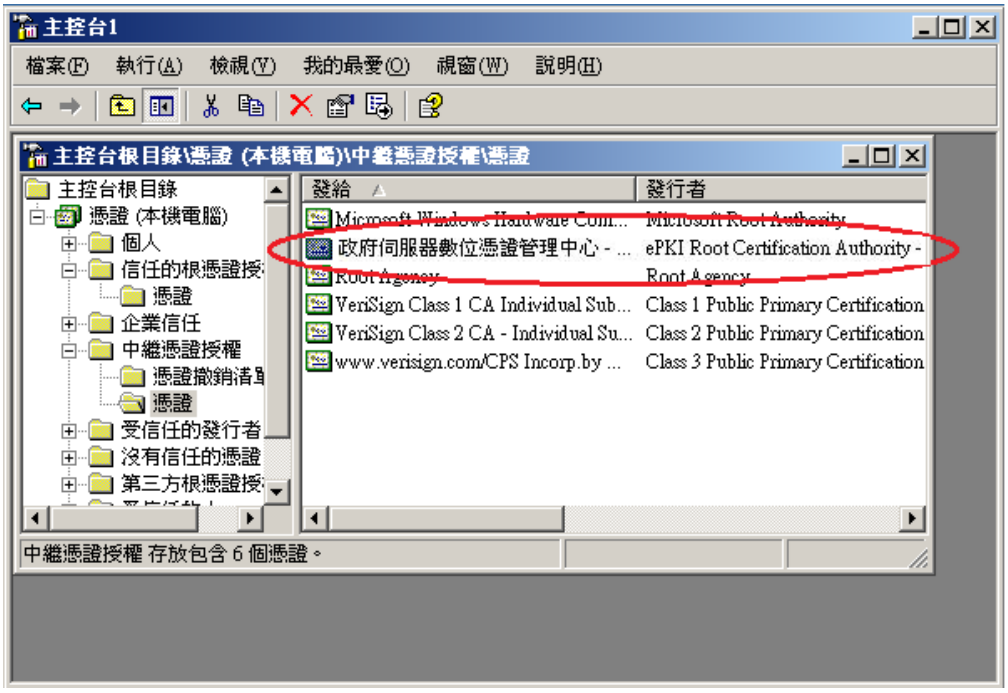

憑證匯入精靈
匯入執行成功。
確定

憑證還原步驟-匯入憑證串鍊

Windows Server 2003

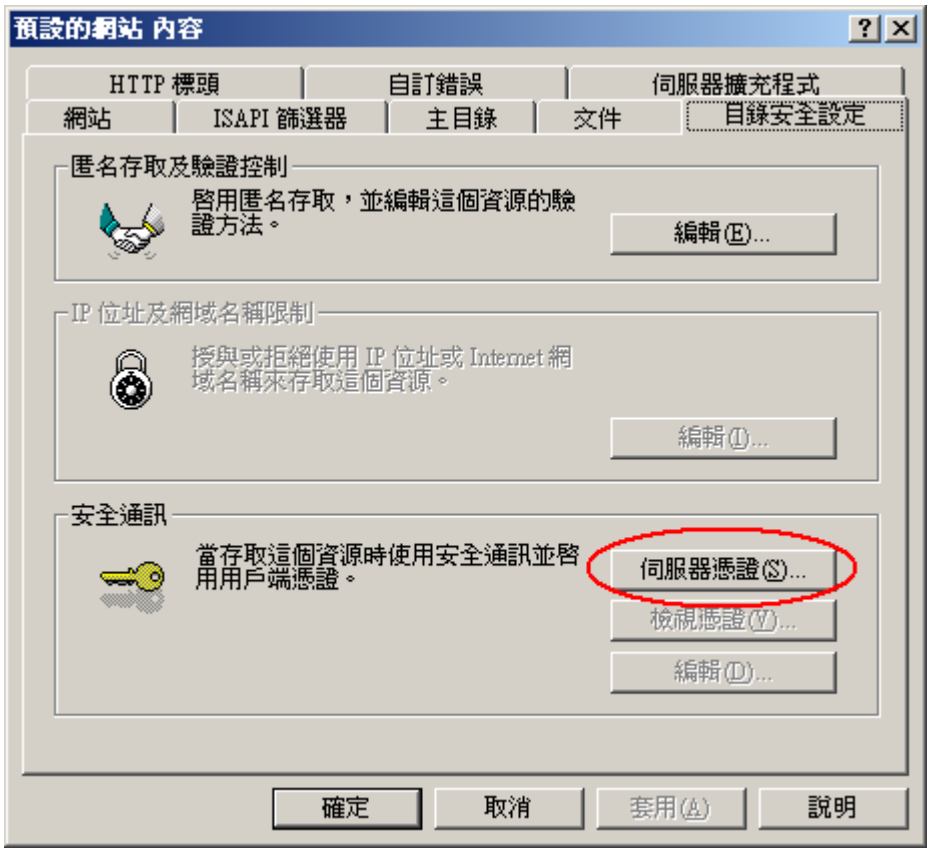
1. 請至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案，下載網址為 https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip
2. 將 GTLSCA_All.zip 解壓縮，可以得到 ROOTeCA_64.crt、eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案
3. 於「信任的根憑證授權」匯入 ROOTeCA_64.crt，操作流程請參考步驟 4。
4. 於「中繼憑證授權」匯入 eCA1_to_eCA2-New.crt 與 GTLSCA.crt。
   下方截圖為匯入範例





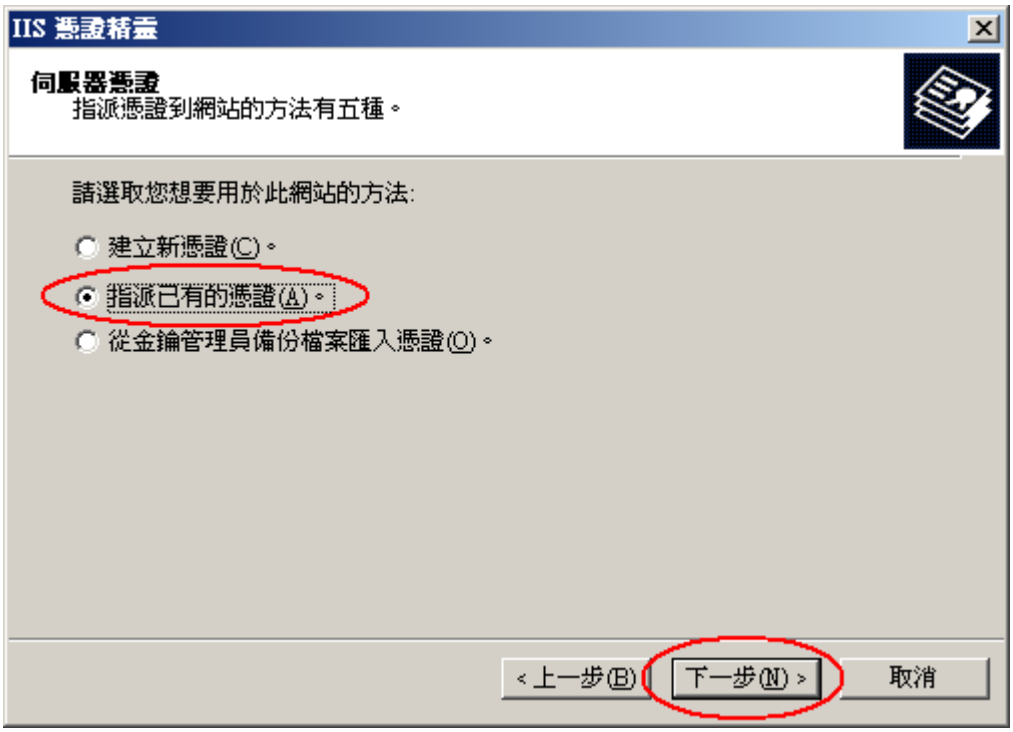
5. ROOTeCA_64.crt 因 Windows 本身大多已內建，不需另外匯入。
6. 檢查「信任的根憑證授權」中是否有 ePKI Root Certification Authority - G2 的憑證(到期日為 2037/12/31)，若有請刪除。
7. 設定 IIS。

   開始」→「設定」→「控制台」→「系統管理工具」→「Internet 服務管理員」→點選服務站台(滑鼠右鍵、選內容)→「目錄安全設定」→「伺服器憑證」

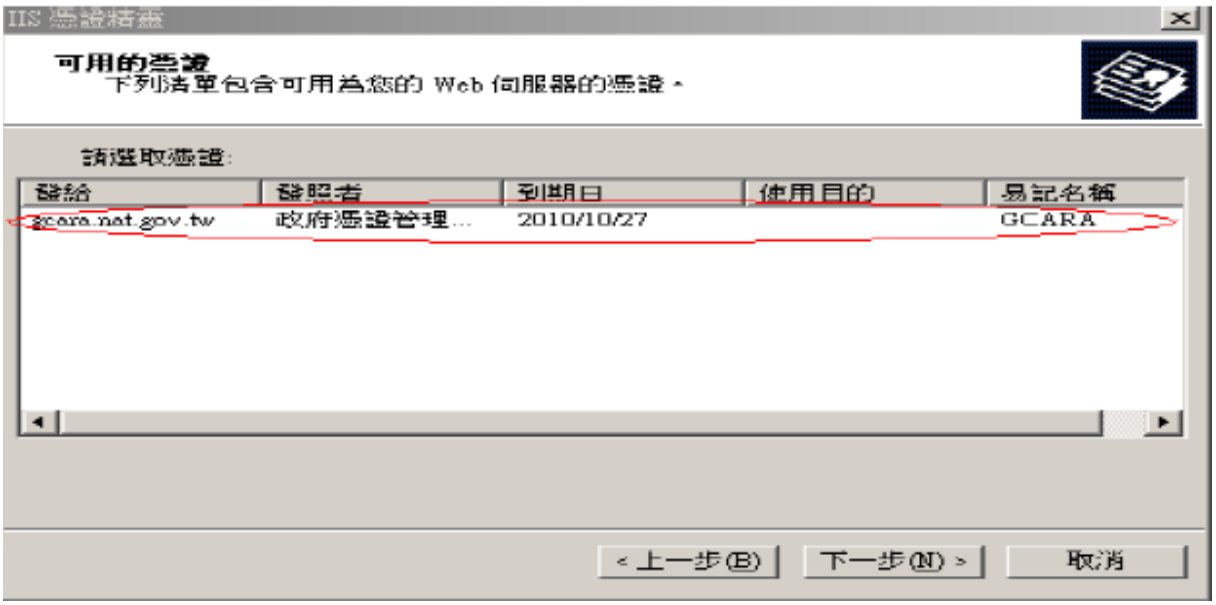


點選「下一步」

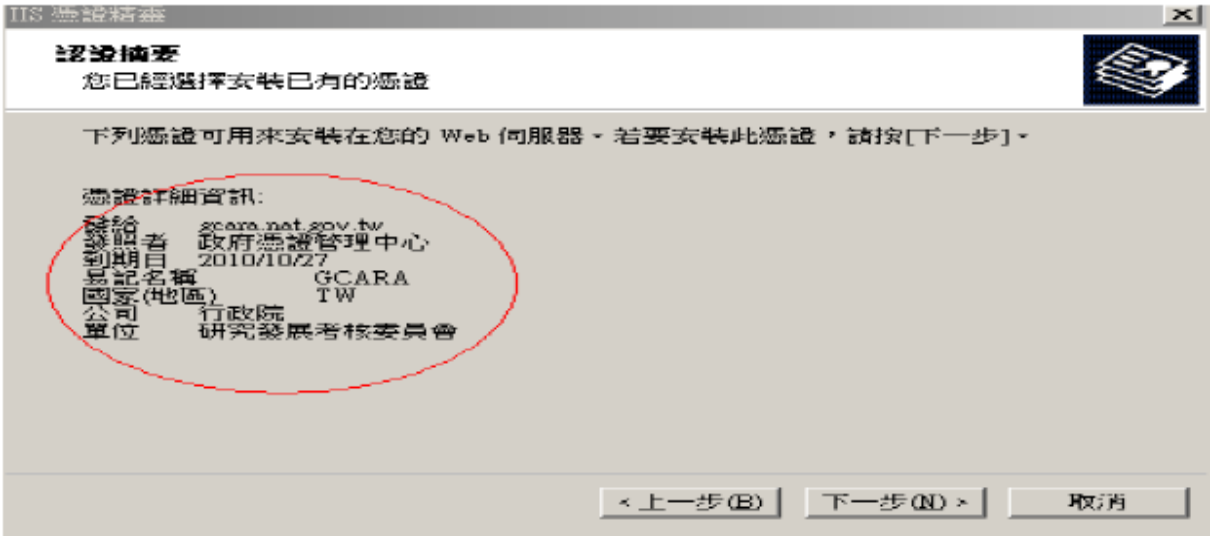
點選「指派已有的憑證」



選擇匯入之憑證→下一步


IIS 憑證精靈
可用的憑證
下列清單包含可用為您的 Web 伺服器的憑證。
請選取憑證:
發給
發照者
到期日
使用目的
易記名稱
gcara.nat.gov.tw
政府憑證管理...
2010/10/27
GCARA
< 上一步(B)
下一步(N) >
取消

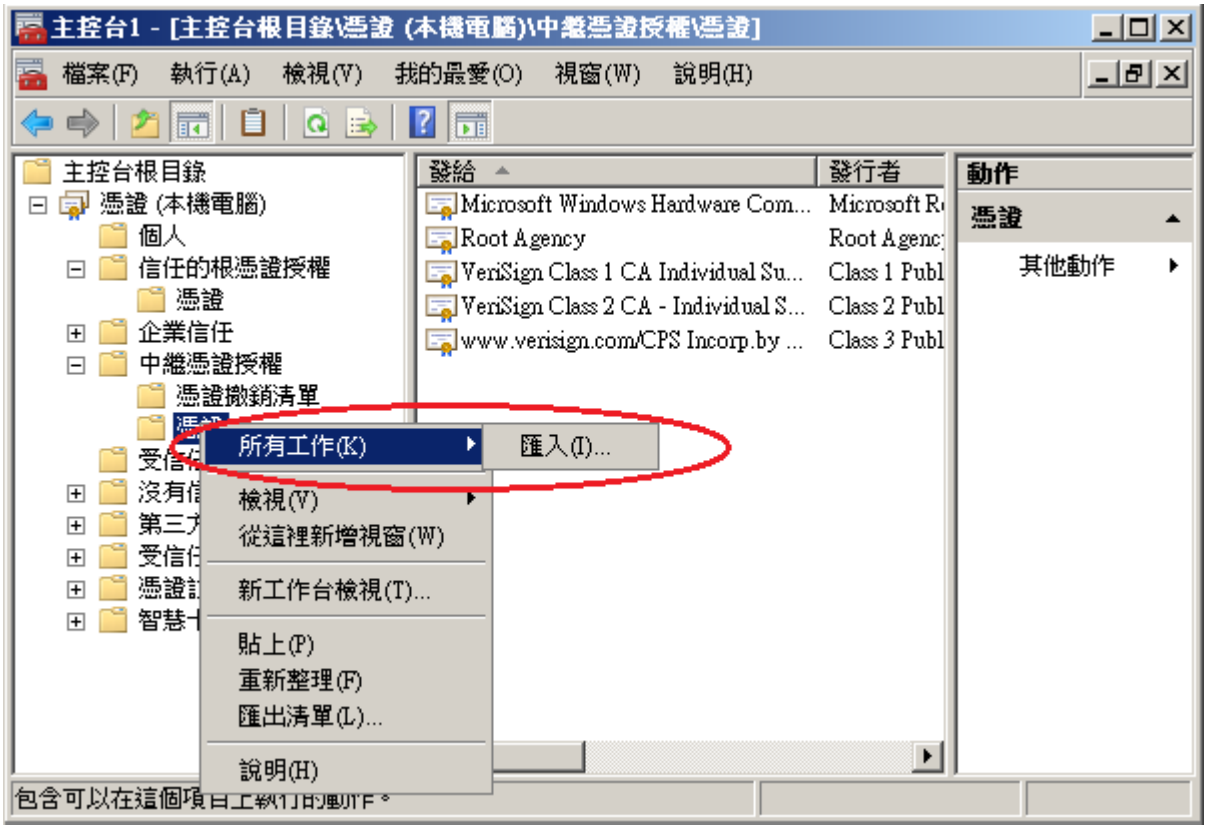
檢視憑證詳細資料

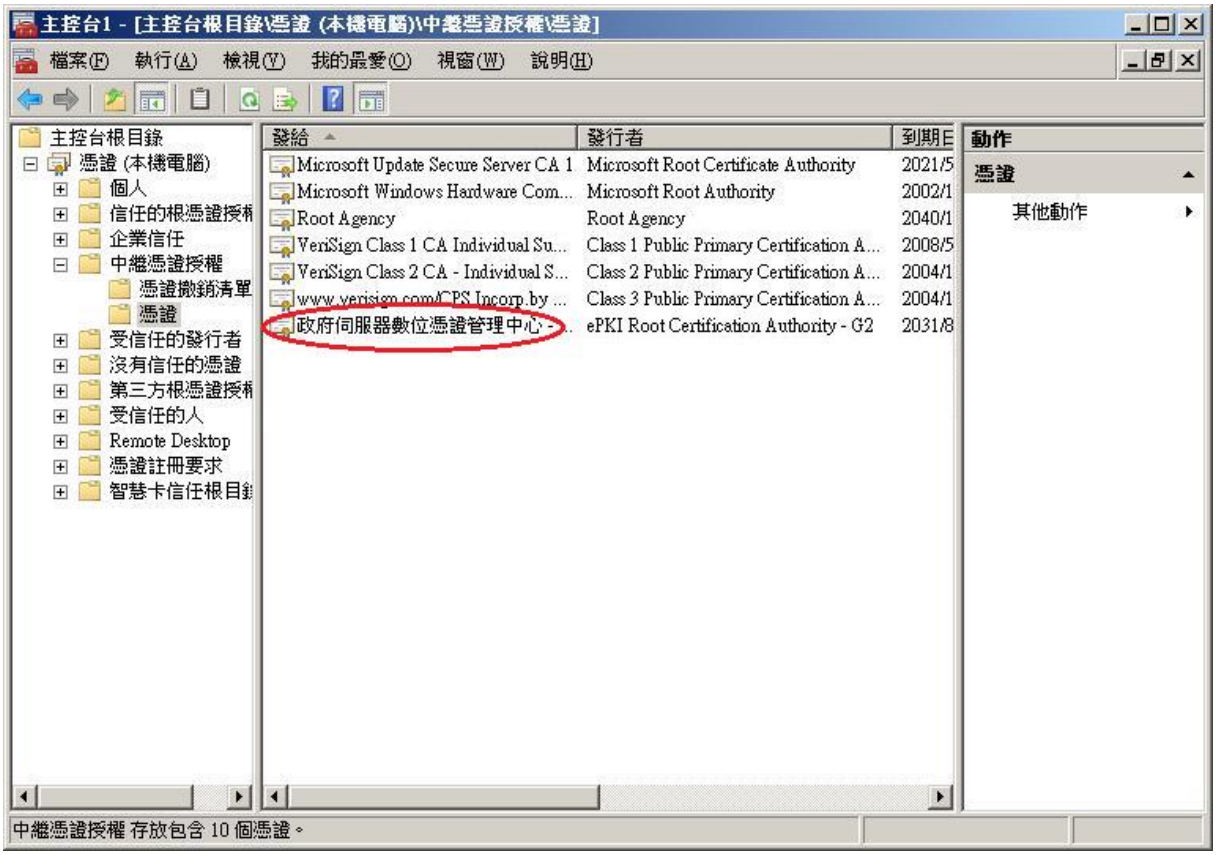

IIS 憑證精靈
認證摘要
您已經選擇安裝已有的憑證
下列憑證可用來安裝在您的 Web 伺服器。若要安裝此憑證，請按[下一步]。
憑證詳細資訊:
發給 gcara.nat.gov.tw
發照者 政府憑證管理中心
到期日 2010/10/27
易記名稱 GCARA
國家(地區) TW
公司 行政院
單位 研究發展考核委員會
< 上一步(B)
下一步(N) >
取消

完成

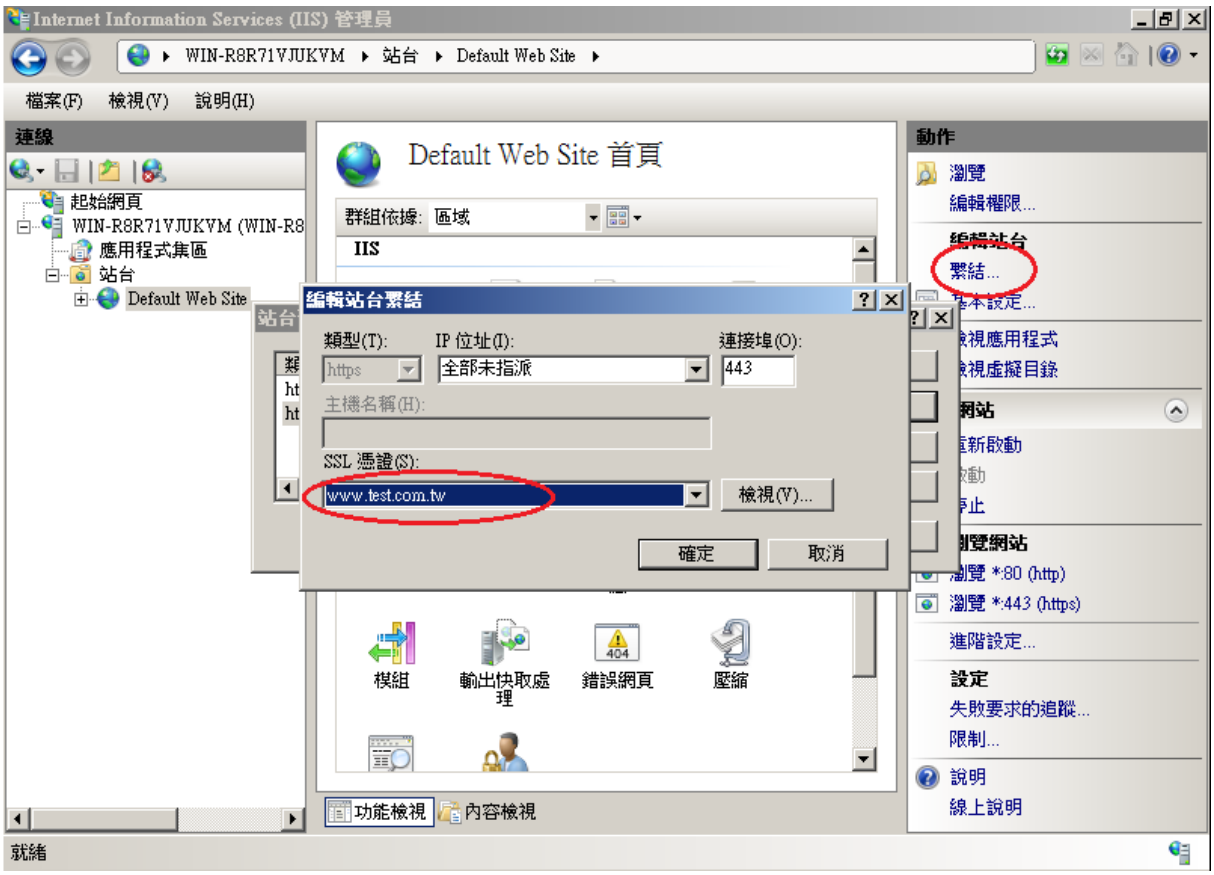

IIS 憑證精靈
正在完成 Web 伺服器憑證精靈
您已經成功完成 Web 伺服器憑證精靈。
目前已安裝憑證在此電腦。
如果您將來需要更新，取代，或刪除此新憑證，請再次使用精靈。
請按 [完成] 來關閉此精靈。
< 上一步(B)
完成
取消

1. 請至 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://gtlsca.nat.gov.tw/download/GTLSCA_All.zip
2. 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
3. 於「信任的根憑證授權」匯入 ROOTeCA_64.crt，操作流程請參考步驟 4。
4. 於「中繼憑證授權」匯入 eCA1_to_eCA2-New.crt 與 GTLSCA.crt。
   下方截圖為匯入範例



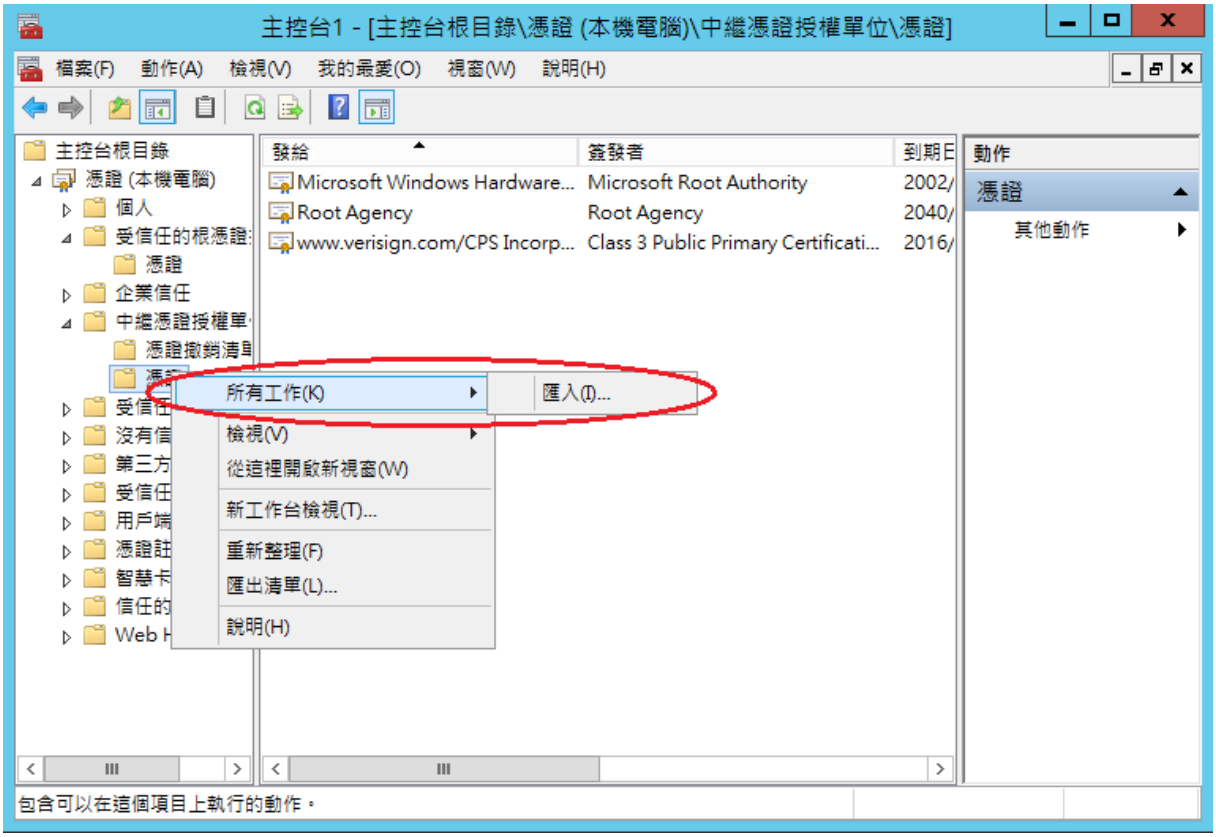


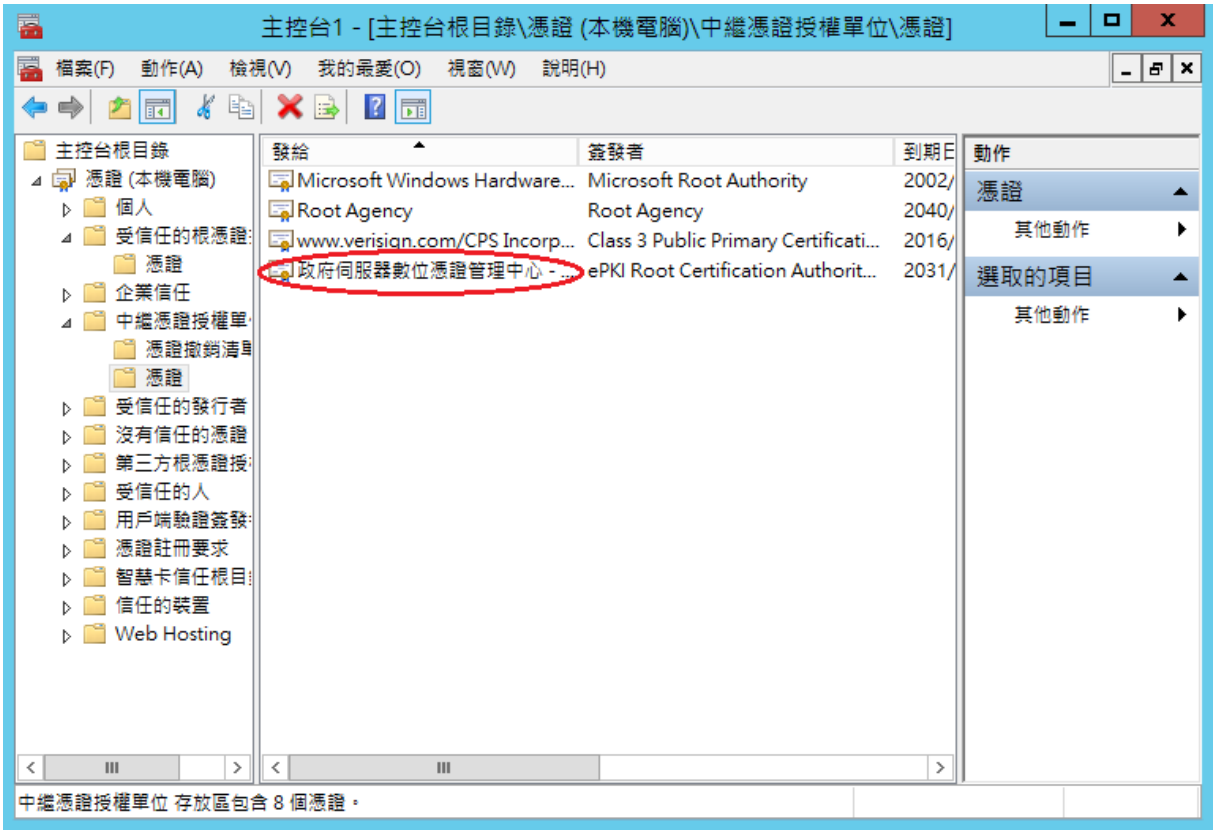
5. ROOTeCA_64.crt 因 Windows 本身大多已內建，不需另外匯入。
6. 檢查「信任的根憑證授權」中是否有 ePKI Root Certification Authority - G2 的憑證(到期日為 2037/12/31)，若有請刪除。
7. 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。



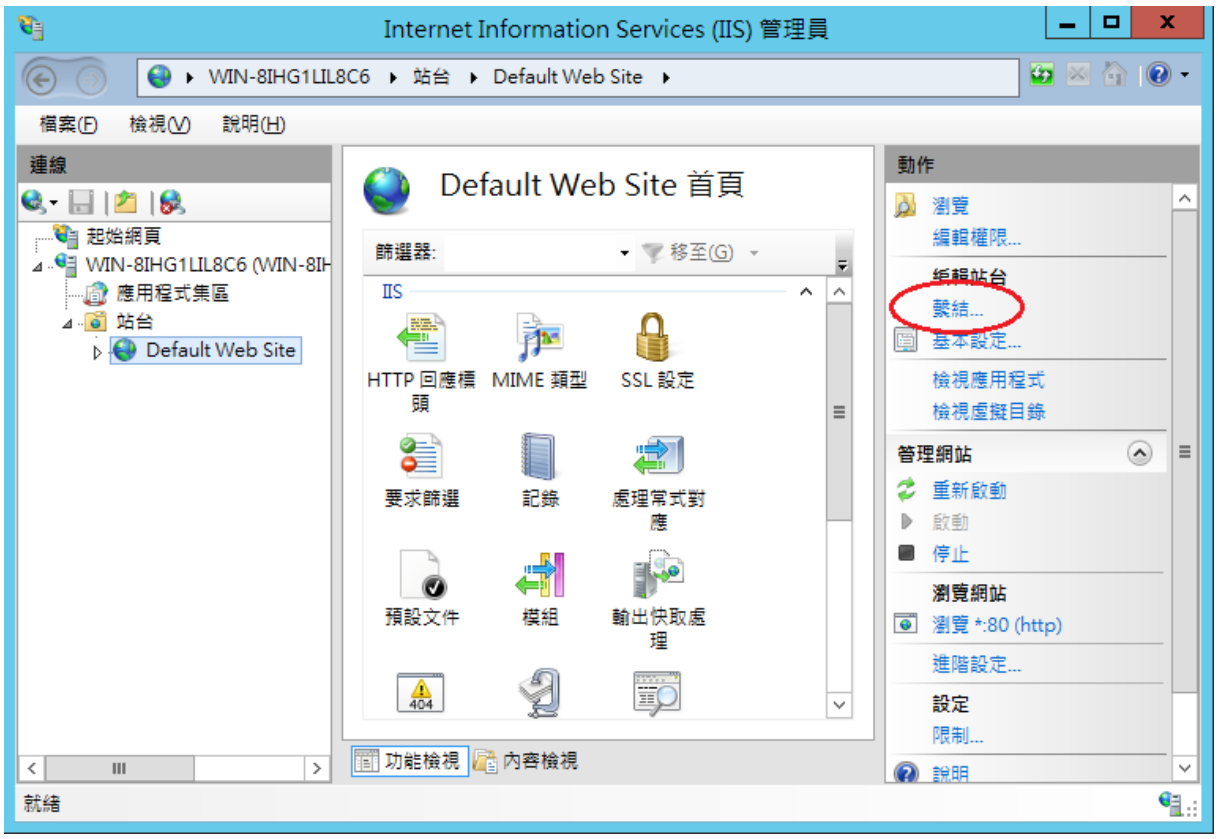
8. 以 https 連線，測試 https 網頁是否正常。

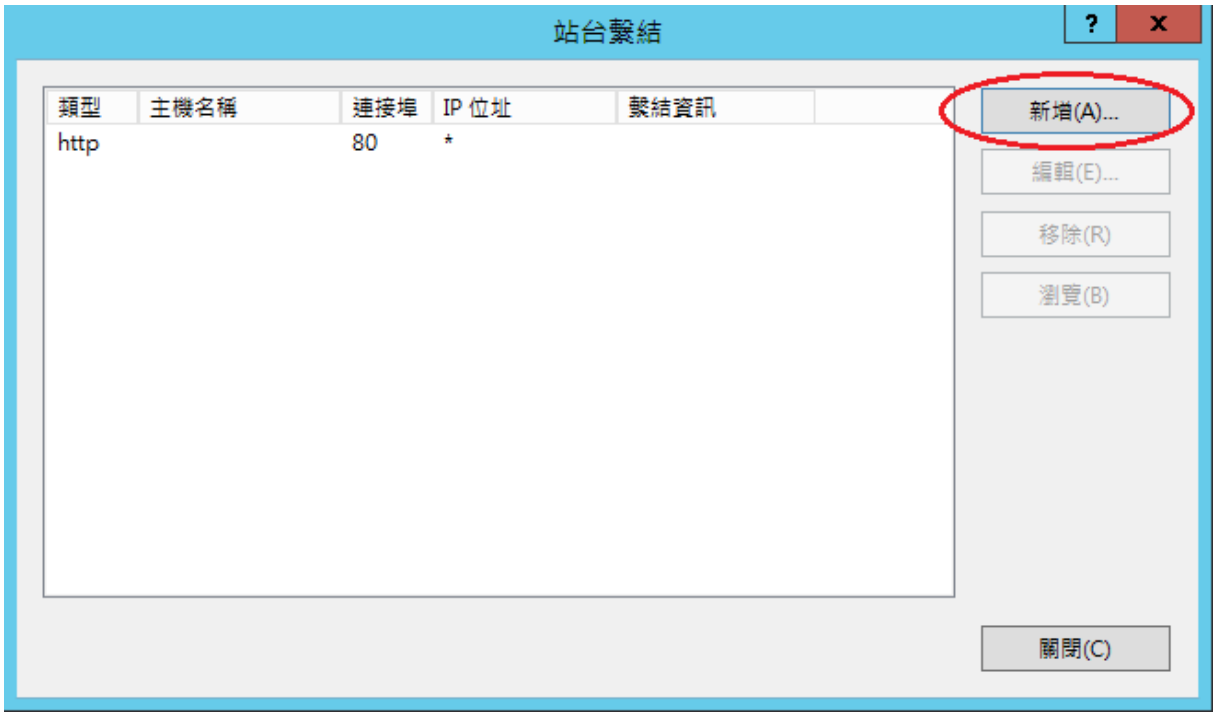
1. 請至 GTLSCA 網站下載已經壓縮打包好的憑證串鏈檔案，下載網址為 https://gtlsca.nat.gov.tw/download/GTLSCA_All.zip
2. 將 GTLSCA_All.zip 解壓縮，可以得到 ROOTeCA_64.crt、eCA1_to_eCA2-New.crt 和 GTLSCA.crt 共 3 個檔案
3. 於「信任的根憑證授權」匯入 ROOTeCA_64.crt，操作流程請參考步驟 4。
4. 於「中繼憑證授權」匯入 eCA1_to_eCA2-New.crt 與 GTLSCA.crt。
   下方截圖為匯入範例





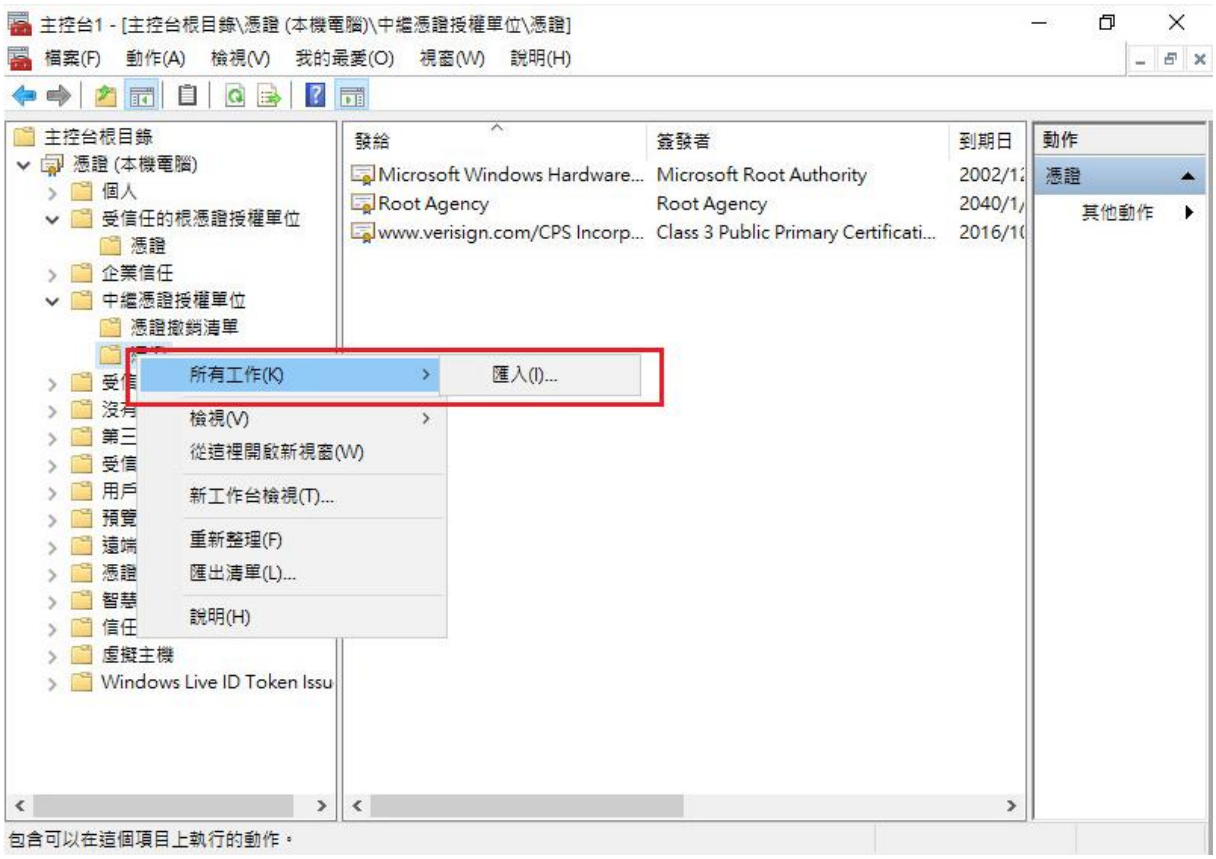
5. ROOTeCA_64.crt 因 Windows 本身大多已內建，不需另外匯入。
6. 檢查「受信任的根憑證授權單位」中是否有 ePKI Root Certification Authority - G2 的憑證(到期日為 2037/12/31)，若有請刪除。
7. 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。

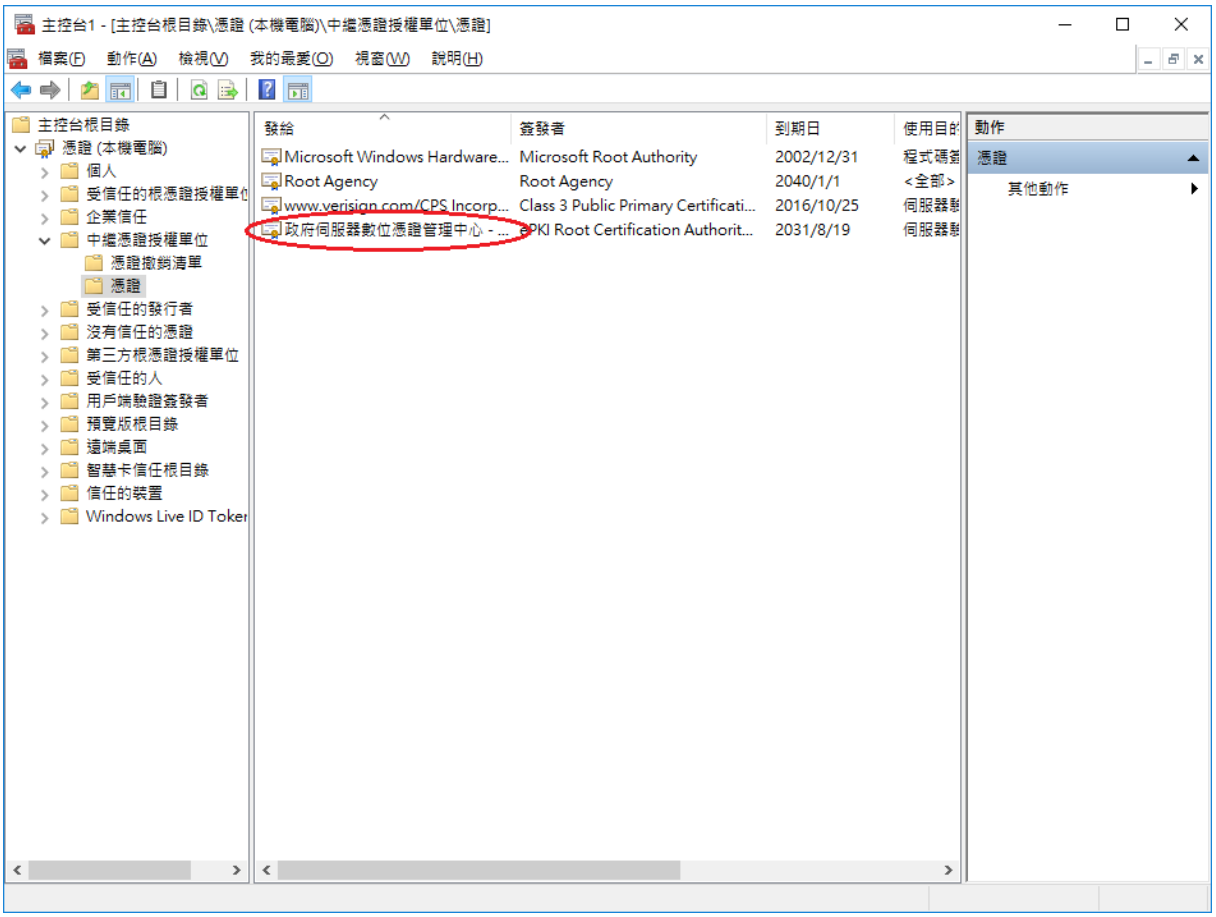

Internet Information Services (IIS) 管理員
WIN-8IHG1LIL8C6 ▸ 站台 ▸ Default Web Site ▸
檔案(F) 檢視(V) 說明(H)
連線
起始網頁
WIN-8IHG1LIL8C6 (WIN-8IH
應用程式集區
站台
Default Web Site
Default Web Site 首頁
篩選器:
移至(G)
IIS
HTTP 回應標頭
MIME 類型
SSL 設定
要求篩選
記錄
處理常式對應
預設文件
模組
輸出快取處理
功能檢視
內容檢視
動作
瀏覽
編輯權限...
繫結...
基本設定...
檢視應用程式
檢視虛擬目錄
管理網站
重新啟動
啟動
停止
瀏覽網站
瀏覽 *:80 (http)
進階設定...
設定
限制...
說明
就緒


站台繫結
類型
主機名稱
連接埠
IP 位址
繫結資訊
http
80
*
新增(A)...
編輯(E)...
移除(R)
瀏覽(B)
關閉(C)

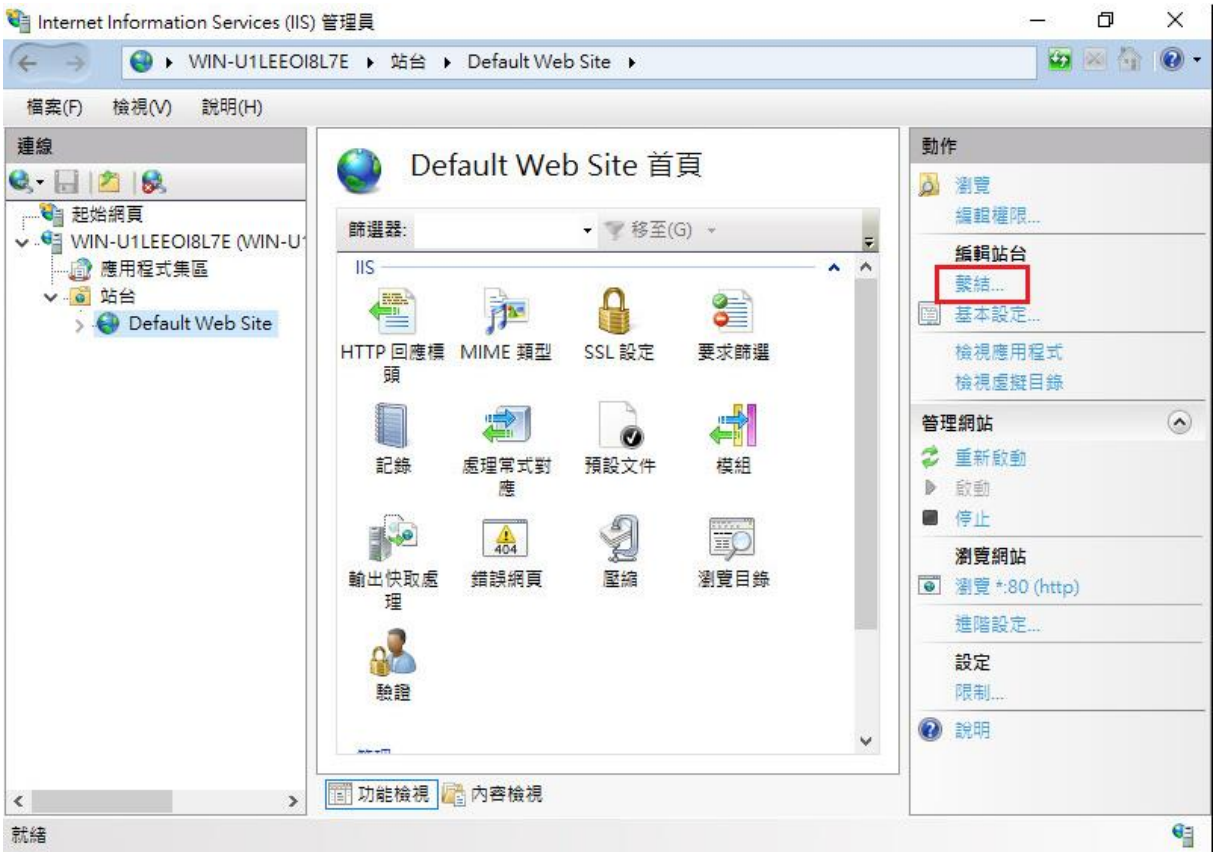
8. 以 https 連線，測試 https 網頁是否正常。

1. 請至 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://gtlsca.nat.gov.tw/download/GTLSCA_All.zip
2. 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
3. 於「信任的根憑證授權」匯入 ROOTeCA_64.crt，操作流程請參考步驟 4。
4. 於「中繼憑證授權」匯入 eCA1_to_eCA2-New.crt 與 GTLSCA.crt。
   下方截圖為匯入範例

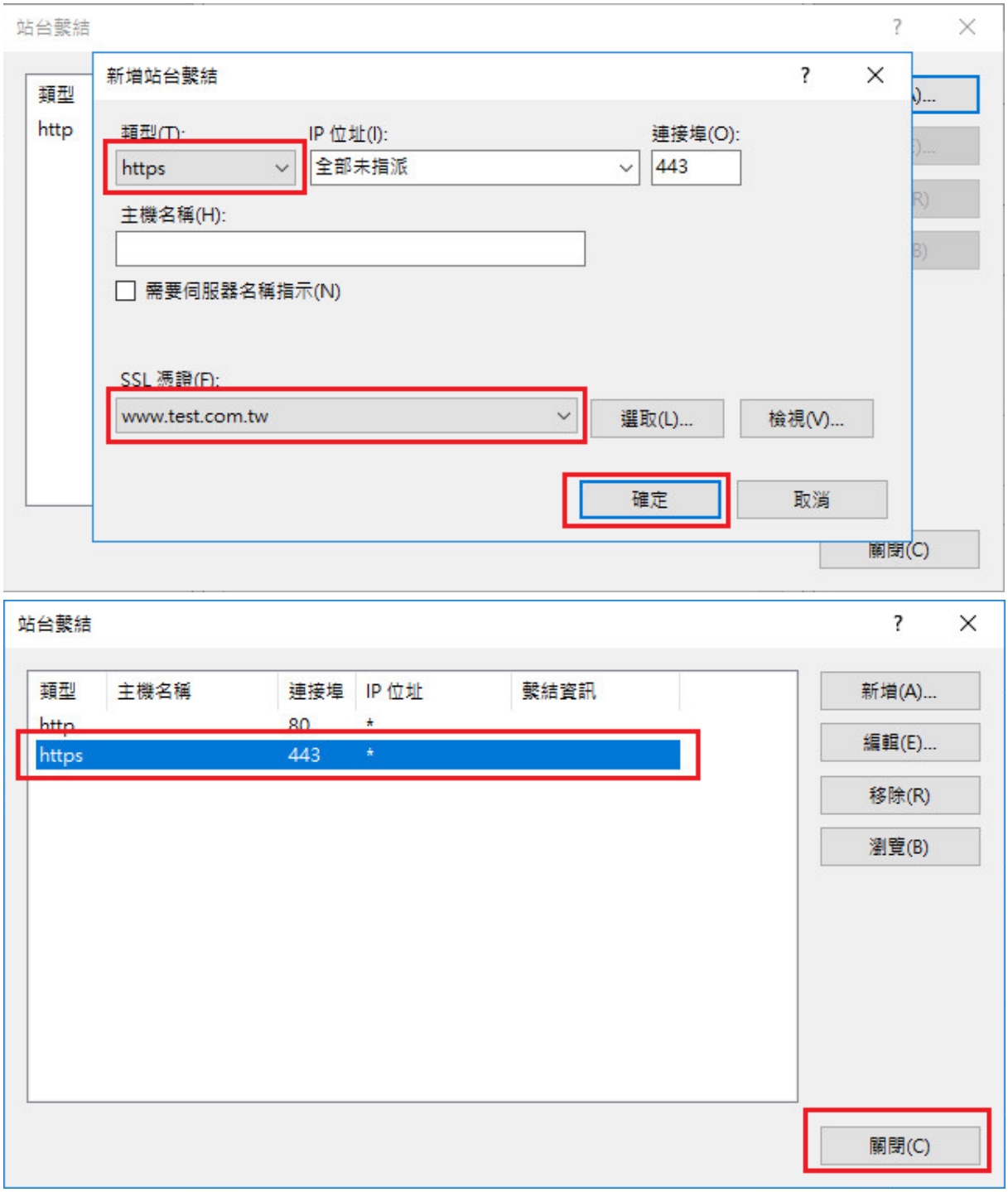




5. ROOTeCA_64.crt 因 Windows 本身大多已內建，不需另外匯入。
6. 檢查「受信任的根憑證授權單位」中是否有 ePKI Root Certification Authority - G2 的憑證(到期日為 2037/12/31)，若有請刪除。
7. 開啟「Internet Information Services (IIS)管理員」，點選「伺服器憑證」即可看到憑證檔案。之後重新透過「繫結」來啟用憑證與 https。


Internet Information Services (IIS) 管理員
WIN-U1LEEOI8L7E ▸ 站台 ▸ Default Web Site ▸
檔案(F) 檢視(V) 說明(H)
連線
起始網頁
WIN-U1LEEOI8L7E (WIN-U1
應用程式集區
站台
Default Web Site
Default Web Site 首頁
篩選器:
移至(G)
IIS
HTTP 回應標頭
MIME 類型
SSL 設定
要求篩選
記錄
處理常式對應
預設文件
模組
輸出快取處理
錯誤網頁
壓縮
瀏覽目錄
驗證
功能檢視
內容檢視
動作
瀏覽
編輯權限...
編輯站台
繫結...
基本設定...
檢視應用程式
檢視虛擬目錄
管理網站
重新啟動
啟動
停止
瀏覽網站
瀏覽 *:80 (http)
進階設定...
設定
限制...
說明
就緒


站台繫結
類型
主機名稱
連接埠
IP 位址
繫結資訊
http
80
*
新增(A)...
編輯(E)...
移除(R)
瀏覽(B)
關閉(C)



8. 以 https 連線，測試 https 網頁是否正常。