SSL 伺服器數位憑證 IIS 10.0

操作手冊

機密等級：公開
版本：V5.4
文件編號：MNT-03-132
生效日期：114 年 6 月 3 日

臺灣網路認證股份有限公司
TAIWAN-CA. Inc.
台北市 100 延平南路 85 號 10 樓
電話:02-2370-8886
傳真:02-2370-0728
www.twca.com.tw

目　　錄

1.目的

1.1. 介紹 IIS 10.0 網頁伺服器之憑證請求檔產製步驟及 SSL 伺服器數位憑證安裝說明。

1.2. 符合本公司資訊安全政策之規範。

2.範圍

2.1. 本操作手冊適用於 IIS10.0 (Windows Server 2016 Web Server)。

3.參考資料

無。

4.定義

無。

5.作業程序

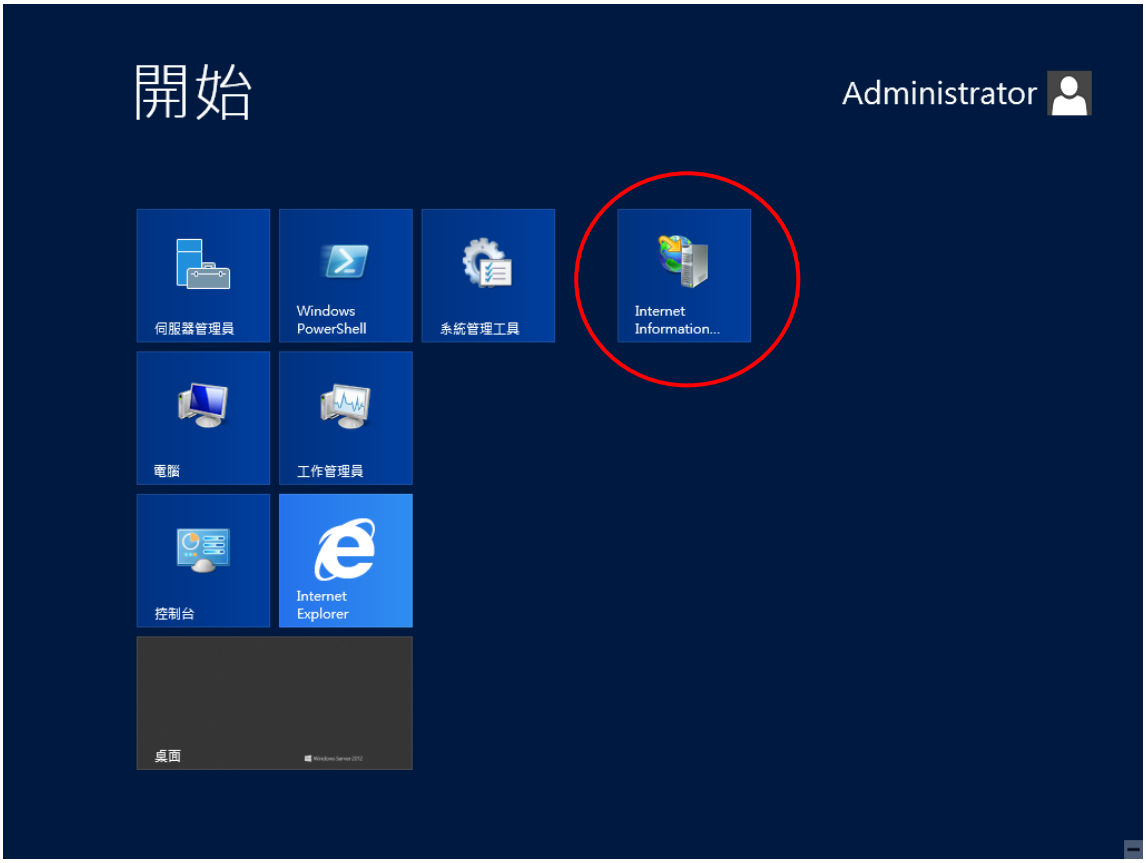
『請以 Administrator 系統管理者權限執行所有動作』

5.1 產生「憑證請求檔(CSR)」

※在產生的過程中，所有需要填入的資料，請務必以英文方式填寫！

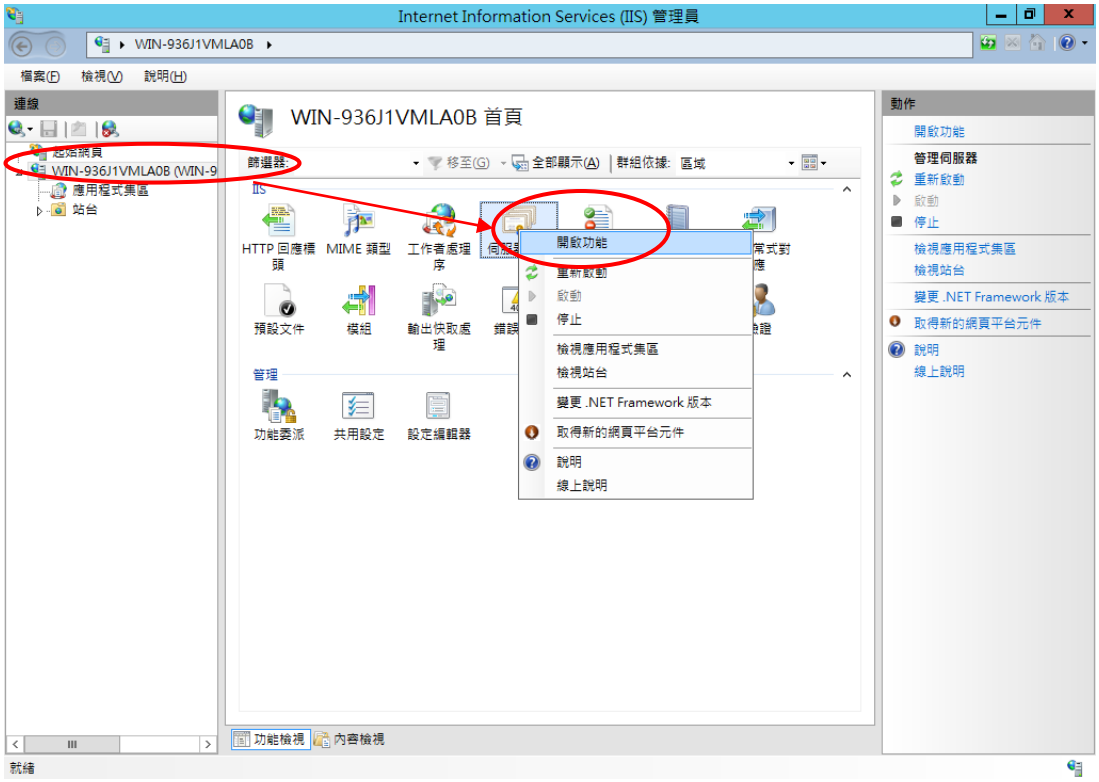
5.1.1 執行網際網路資訊服務(IIS)管理員

開啟開始頁面→點選 Internet Information Services(IIS)管理員。



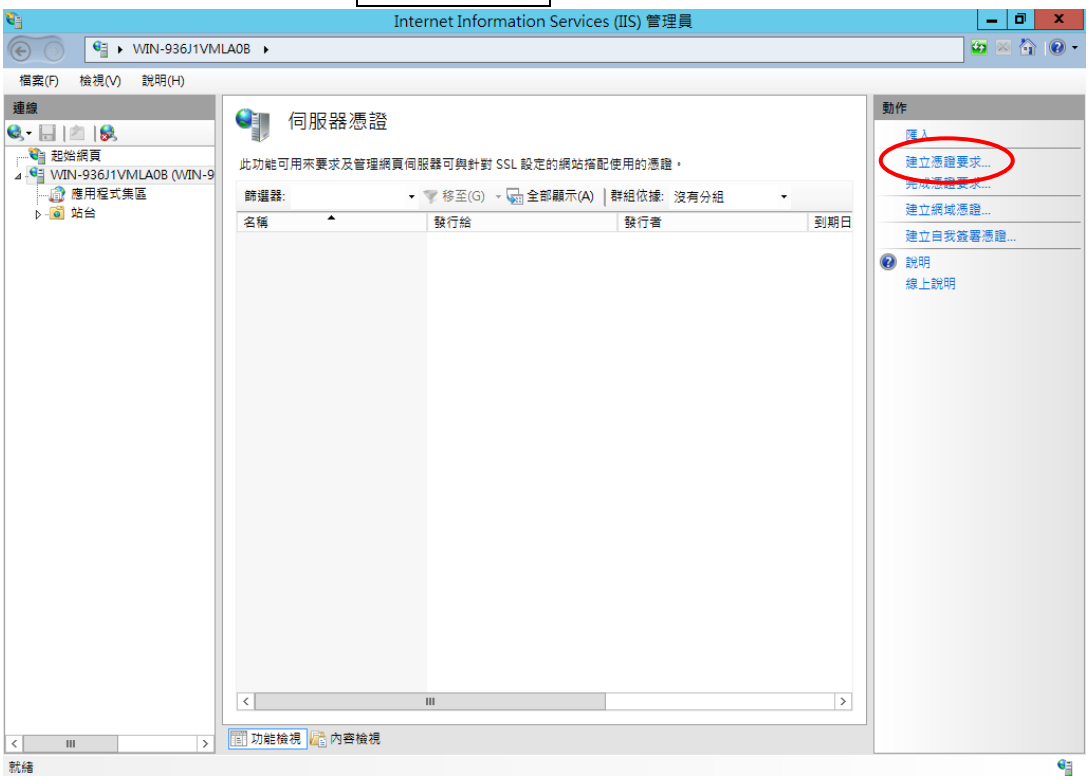
5.1.2 準備產生憑證請求檔(1)

先選擇左側欄位中電腦名稱(電腦名稱\Administrator)→再於伺服器憑證選項按滑鼠右鍵，點選開啟功能。



5.1.3 準備產生憑證請求檔(2)

點選右側欄位中建立憑證要求。



5.1.4 輸入憑證資訊(1)

5.1.4.1 **一般名稱(M)**：網站名稱，請填貴公司欲加密的網址名稱，不必加 http://或 https://。

5.1.4.2 **組織(O)**：公司名稱，可使用縮寫，必須以英文方式填寫！

（如：臺灣網路認證股份有限公司為 **TWCA**）

5.1.4.3 **組織單位(U)**：使用該憑證之單位名稱，必須以英文方式填寫！

（如：系統部為 **SYSTEM**）

5.1.4.4 **縣市／位置**：城市全名，必須以英文方式填寫！

（如：**TAIPEI**）

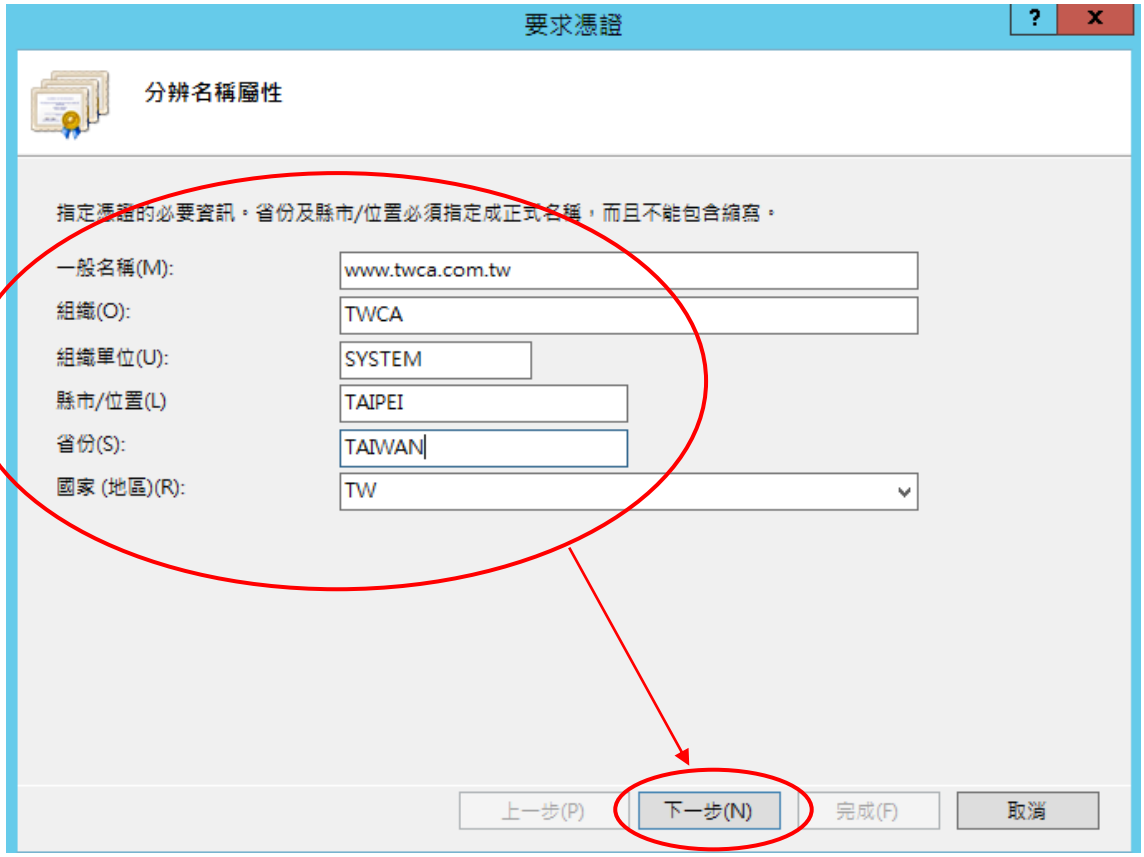
5.1.4.5 **省份**：國家全名，必須以英文方式填寫！

（如：**TAIWAN**）

5.1.4.6 **國家(地區)(R)**：選擇國家簡稱。

（如：**TW**）

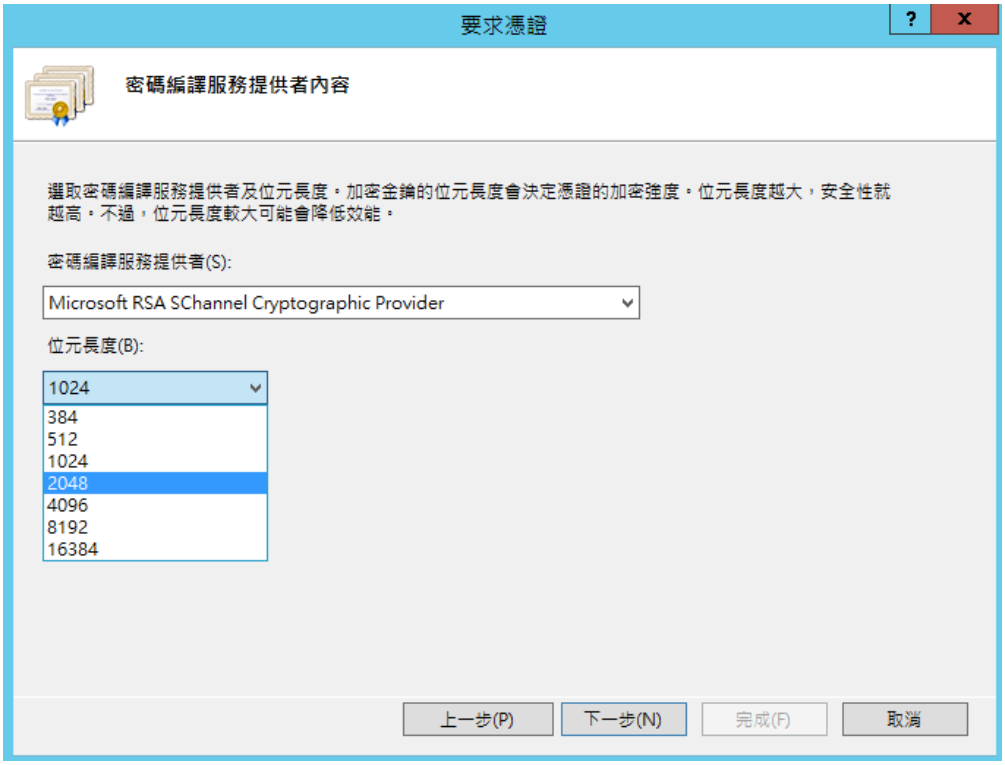
輸入憑證資訊完成後→點選下一步。

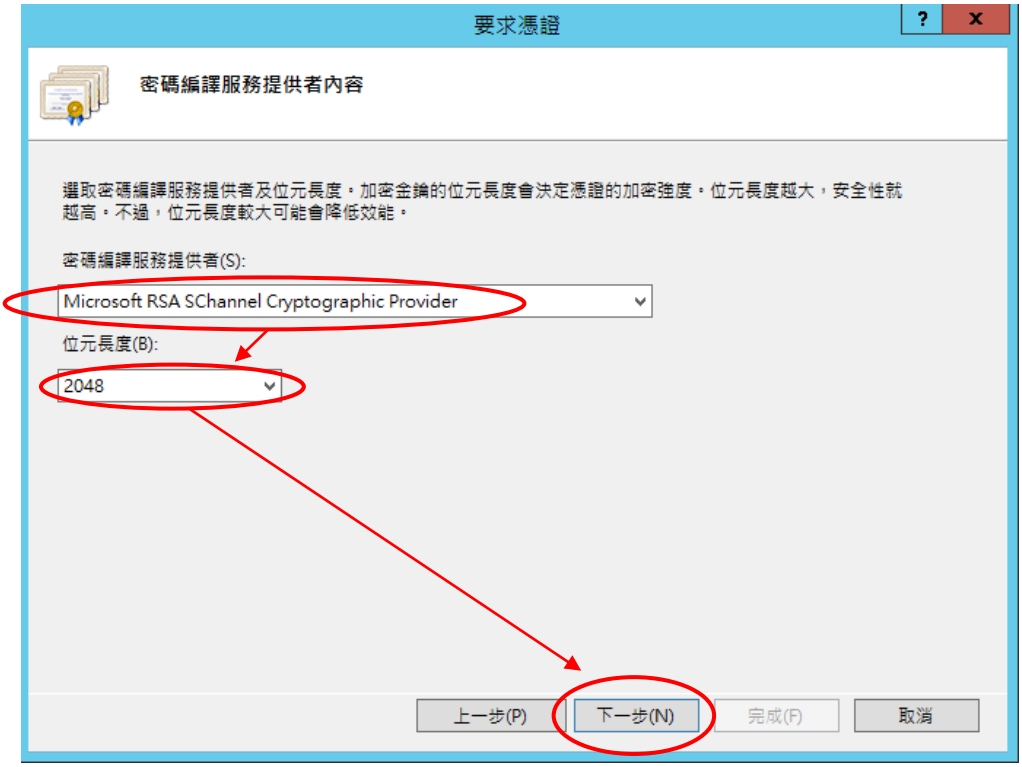


5.1.5 輸入憑證資訊(2)

5.1.5.1 **密碼編譯服務提供者**：請選擇 Microsoft RSA SChannel Cryptographic Provider。

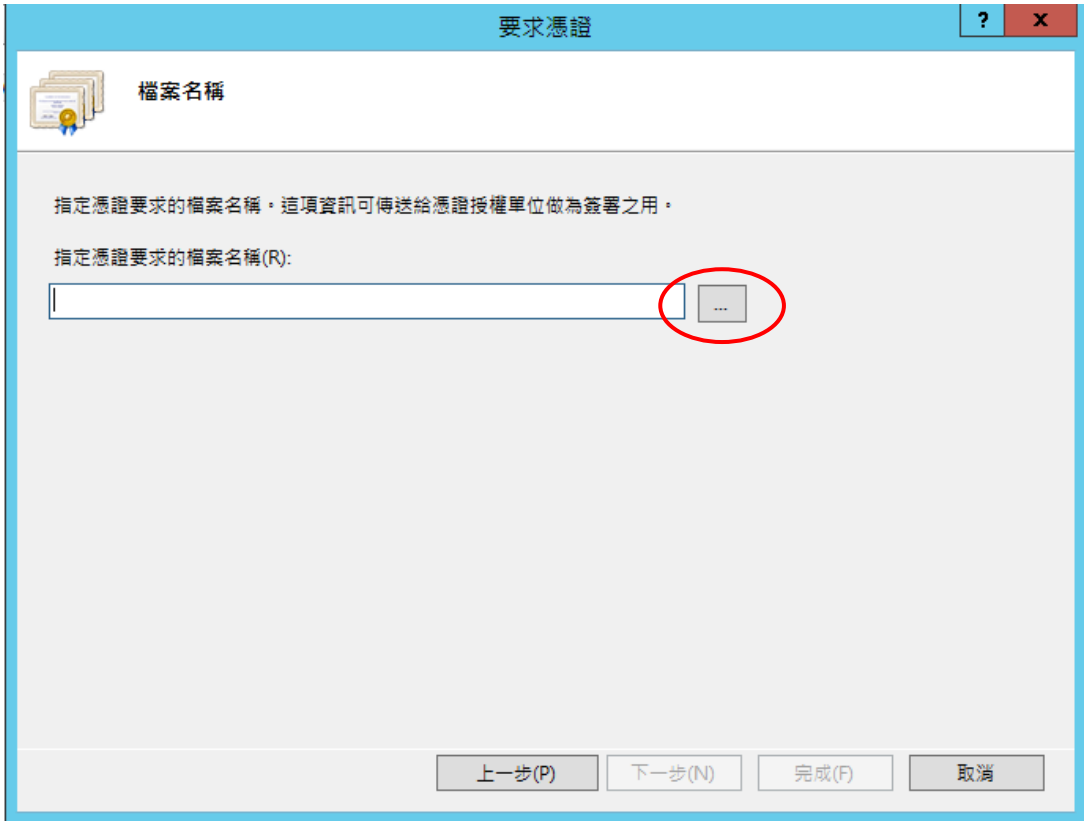
5.1.5.2 **位元長度**：請選擇 **2048** 位元長度。點選下一步。

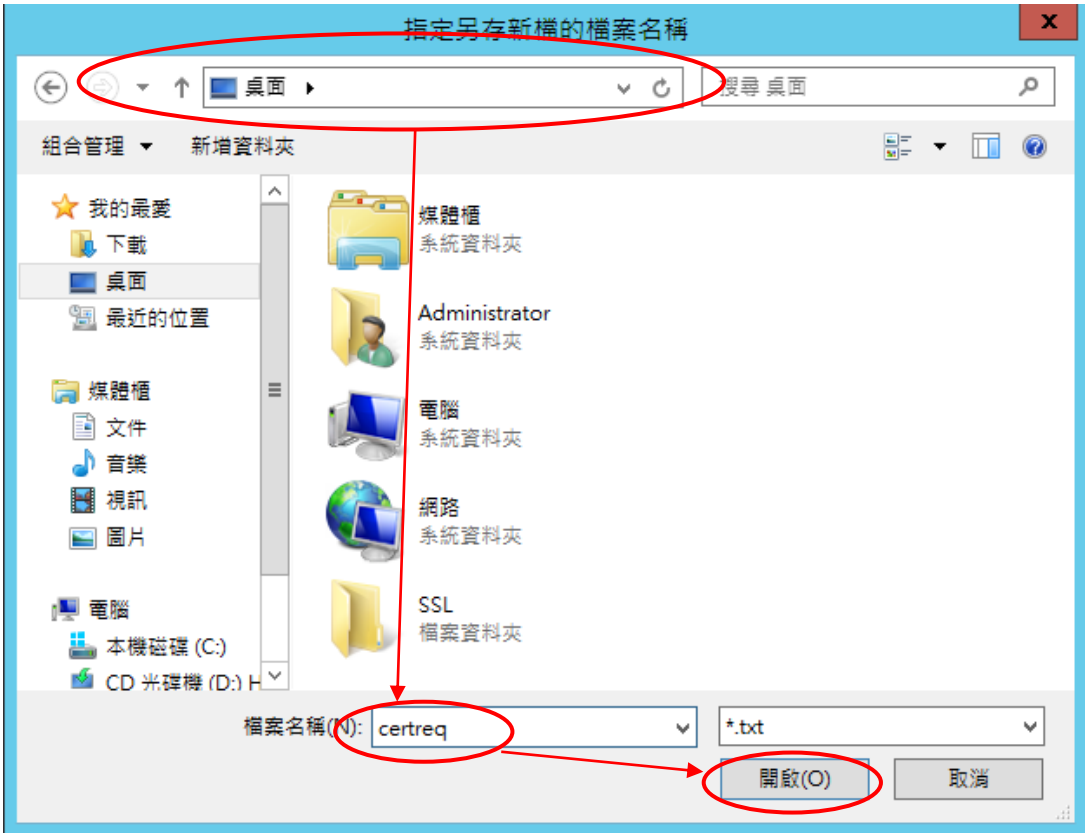




5.1.6 指定憑證請求檔名稱及存放路徑

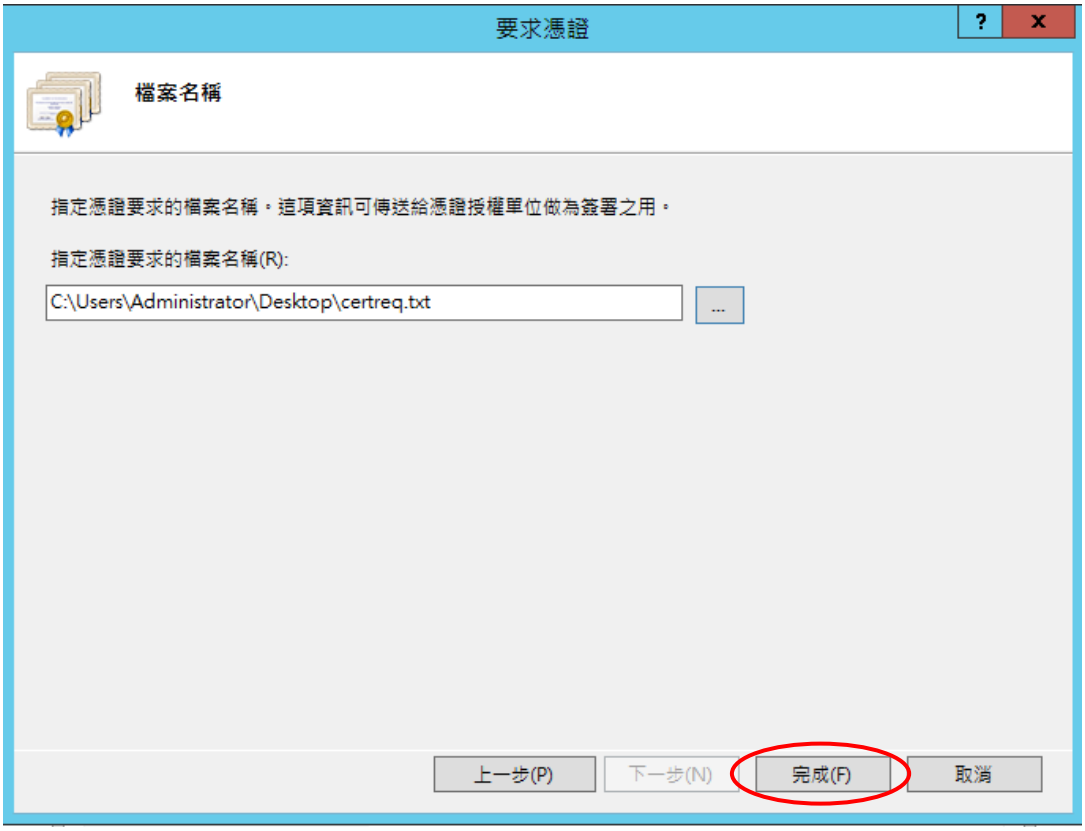
請點選…自行指定憑證請求檔的存放路徑及檔名。





5.1.7 儲存憑證請求檔

確認存放路徑及指定檔名後，點選完成。



5.1.8 憑證請求檔內容

利用記事本開啟憑證請求檔，內容範例如下圖所示。

5.2 將製作好的憑證請求檔(CSR)上傳

5.2.1 連接 TWCA 網站(1)

連接至本公司首頁 http://www.twca.com.tw

點選憑證服務。

5.2.2 連接 TWCA 網站(1)

點選 SSL 憑證。

※如申請 EV SSL 伺服器憑證，請點選 TWCA EV SSL 類。

5.2.3 連接 TWCA 網站(2)

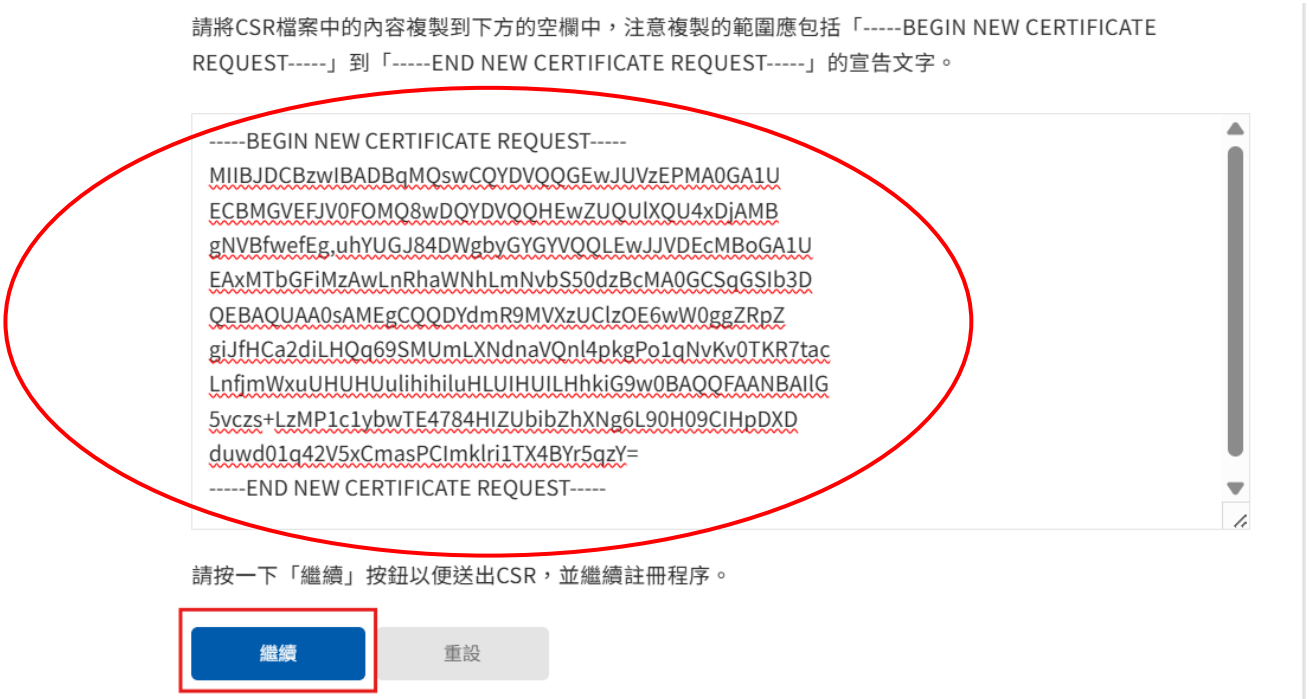
點選申請憑證。

5.2.4 連接 TWCA 網站(3)

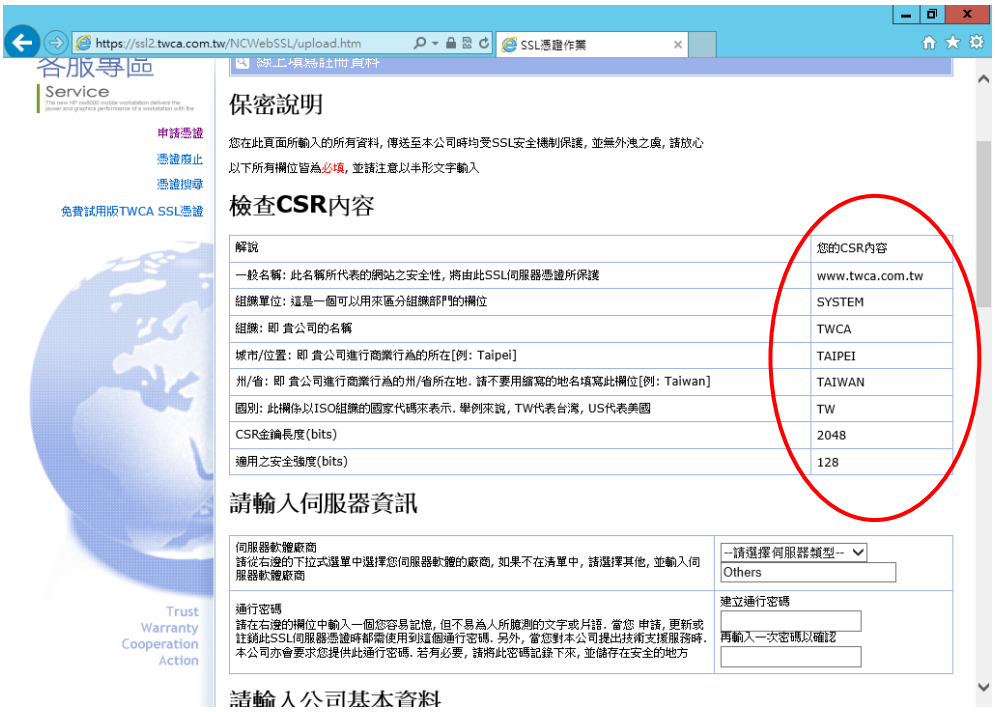
下拉至上傳 CSR (WEB)

5.2.5 貼上憑證請求檔

將瀏覽器視窗畫面往下拉，開啟在 5.1 章節產生的憑證請求檔，利用全選後複製貼上的方式(CSR 檔案內容包含-----BEGIN CERTIFICATE REQUEST-----、-----END CERTIFICATE REQUEST-----)，將製作好之憑證請求檔（CSR）內容貼到申請欄位中→選擇繼續。



5.2.6 再次檢視上傳之憑證請求檔案內容



5.2.7 設定通行密碼及選擇身分審驗方式

5.2.7.1 請自行設定通行密碼,該密碼請牢記，如您需要廢止憑證時,必須輸入此通行密碼。

請輸入通行密碼

通行密碼 此密碼是廢止憑證所需, 請務必記得, 並儲存在安全的地方	建立通行密碼

5.2.7.2 為符合 SSL 憑證國際審放標準，將審驗網域所有權者請您選擇以下一種審驗方式:

一、EMAIL 驗證：將會自動帶出網域註冊之 EAMIL 或者請選擇 admin@網域、administrator@網域、webmaster@網域、hostmaster@網域、postmaster@網域此六個 EMAIL 任一個 EMAIL 皆可進行身分驗證作業，選擇送出後系統將會寄出驗證信，請務必至該信箱完成驗證作業

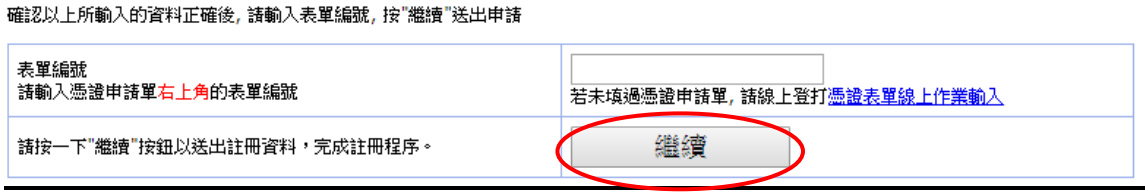
二、檔案驗證：請您填入收取該檔案收件人 EMAIL,您將在此 EMAIL 收到一附件檔案,請您依照信件說明將檔案放入,完成後請通知我們進行檔案驗證作業。

三、電話驗證：網域所有權人的資料可公開查詢到才能使用電話驗證,請您選擇進行電話驗證的時段,我們將依照您所選擇的去電驗證。

網域所有權

網域管理者	為符合SSL憑證國際審放標準，將審驗網域所有權請您選擇以下一種審驗方式。 網域所有權EMAIL驗證：點選確認後,系統將會自動寄出驗證信,請用戶務必至該信箱收信並點擊確認即可。 maintain@twca.com.tw (網域註冊資料來源由WHOIS取得) 或請選擇 admin@twca.com.tw administrator@twca.com.tw webmaster@twca.com.tw hostmaster@twca.com.tw postmaster@twca.com.tw 網站檔案驗證：(Whois資料設定為不揭露) 請您填入接收電子信箱: maintain@twca.com.tw ,將郵寄檔案及說明給您。 電話驗證:我們將以電話驗證方式確認網域所有權 請您留下方便聯絡的時間: 皆可 上午時段 下午時段

5.2.7.3 填寫表單編號，並確認以上表單內容輸入正確後，按繼續送出申請。



5.2.8 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，近日會完成驗證(以下畫面為選擇電話驗證的顯示結果)，憑證簽發後會以 Email 通知業務及技術聯絡人(TWCA SSL 伺服器數位憑證下載通知)，憑證亦可以在 TWCA 網站搜尋及下載。

5.3 下載已核發憑證

1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經審驗通過，將會寄送「SSL 伺服器數位憑證下載通知」電子郵件給相關聯絡人，郵件內容包含附件憑證鏈壓縮檔（cert.zip）及 TWCA SSL 動態認證標章之安裝說明與標章圖檔連結。

將附件憑證鏈壓縮檔 cert.zip 解壓縮後，可得到三個憑證鏈檔。

※內容及憑證用途如下圖所示：

將附件憑證鏈壓縮檔 cert.zip 解壓縮後，可得到四個憑證鏈檔。

※內容及憑證用途如下圖所示：

2 檔案下載說明

如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站憑證搜尋功能，下載憑證鏈壓縮檔。

5.3.1 連接 TWCA 網站(1)

連接至本公司首頁 https://www.twca.com.tw

點選客服專區，點選 SSL 伺服器憑證。

5.3.2 連接 TWCA 網站(3)

點選 TWCA SSL 類。

※如申請 EV SSL 伺服器憑證，請點選 TWCA EV SSL 類。

5.3.3 連接 TWCA 網站(4)

點選憑證搜尋。

5.3.4 輸入申請之網站名稱

在網站名稱中輸入憑證申請單上填寫之網站名稱(Common Name)，如 www.twca.com.tw (**注意，大小寫需一致，不必加 http://或 https://**)，輸入完成後，按下搜尋鍵。

5.3.5 下載憑證鏈壓縮檔

確認憑證相關資訊與申請相符後點選下載→憑證鏈，另開檔案下載視窗，按下另存新檔，儲存憑證鏈壓縮檔 cert.zip。

5.4 安裝根憑證

5.4.1 儲存根憑證

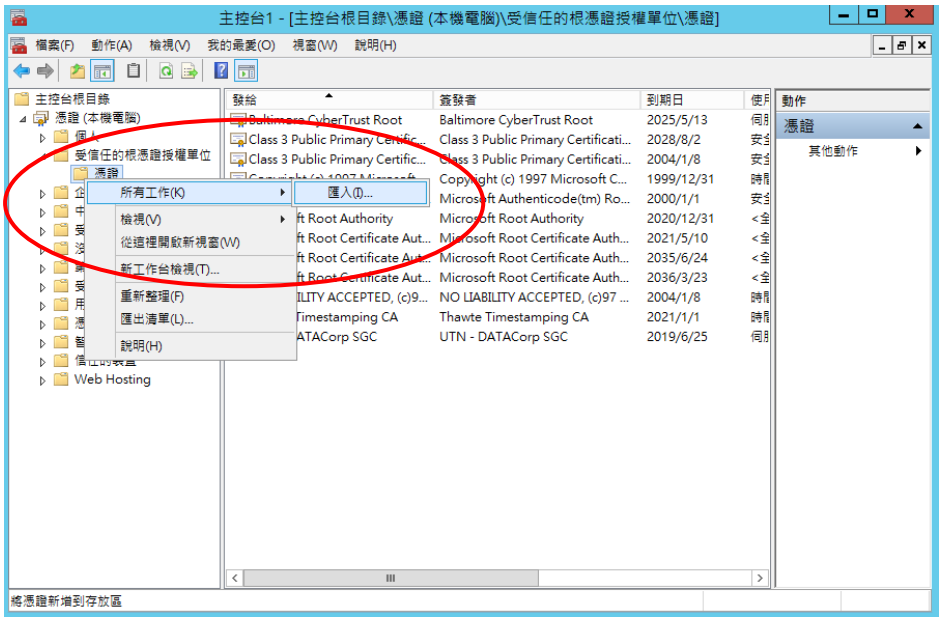
請參照 5.3 章節步驟，將根憑證檔（root.cer）儲存於電腦中可存取位置。

5.4.2 新增憑證管理單元

請參照 5.12 章節步驟，新增憑證管理單元。

5.4.3 安裝根憑證(1)

點選展開主控台根目錄內的憑證（本機電腦）→展開信任的根憑證授權→於憑證上按滑鼠右鍵選所有工作→點選匯入。



5.4.4 安裝根憑證(2)

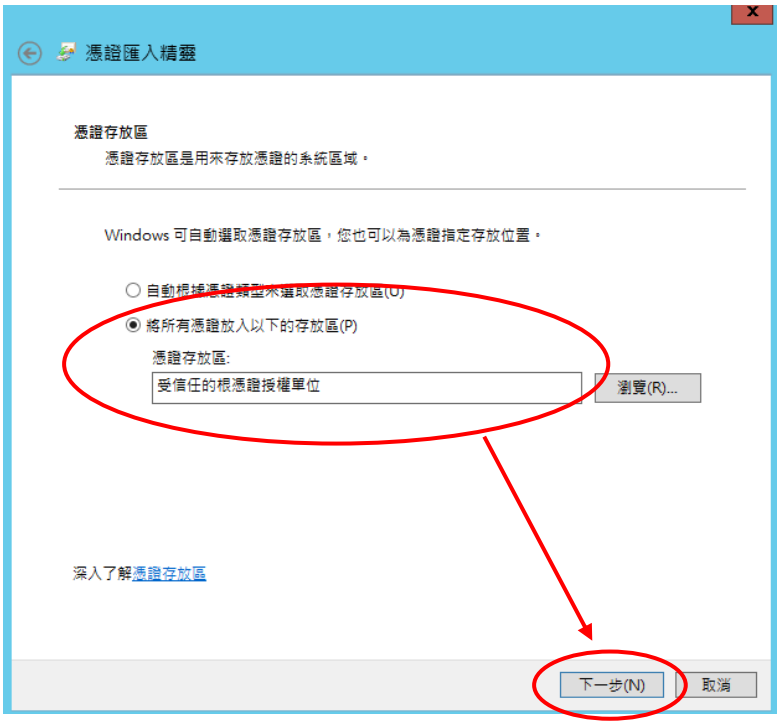
啟動歡迎使用憑證匯入精靈→點選下一步。

5.4.5 安裝根憑證(3)

點選瀏覽，指定根憑證檔（root.cer）所在位置→點選下一步。

5.4.6 安裝根憑證(4)

按預設點選將所有憑證放入以下的存放區→憑證存放區→信任的根憑證授權→點選下一步。

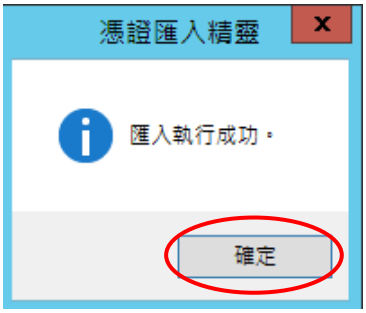


5.4.7 安裝根憑證(5)

點選完成

5.4.8 完成根憑證安裝

點選確定。



5.5 安裝中繼憑證

5.5.1 儲存中繼憑證

請參照 5.3 章節步驟，將中繼憑證檔（uca.cer）儲存於電腦中可存取位置。**如 5.3 章節解壓縮後得到四個憑證鏈檔，請儲存兩張中繼憑證（uca_1.cer 與 uca_2.cer）於電腦中可存取位置，並重複以下步驟安裝。**

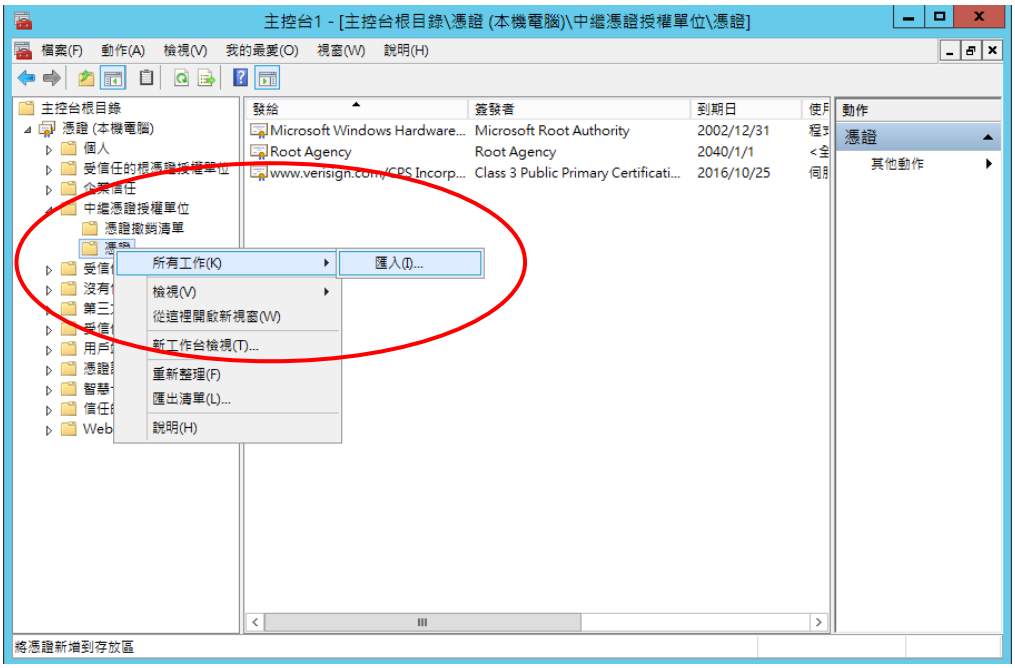
- **三層憑證鏈請參照步驟 5.5.3**
- **四層憑證鏈請參照步驟 5.5.9**

5.5.2 新增憑證管理單元

請參照 5.12 章節步驟，新增憑證管理單元。

5.5.3 安裝中繼憑證(1)

點選展開主控台根目錄內的憑證（本機電腦）→展開中繼憑證授權→於憑證上按滑鼠右鍵選所有工作→點選匯入。



5.5.4 安裝中繼憑證(2)

啟動歡迎使用憑證匯入精靈→點選下一步。

5.5.5 安裝中繼憑證(3)

點選瀏覽，指定中繼憑證檔（uca.cer）存放位置→點選下一步。

5.5.6 安裝中繼憑證(4)

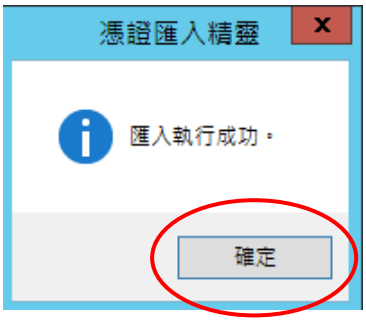
按預設點選將所有憑證放入以下的存放區→憑證存放區→中繼憑證授權→ 點選下一步。

5.5.7 安裝中繼憑證(5)

點選完成。

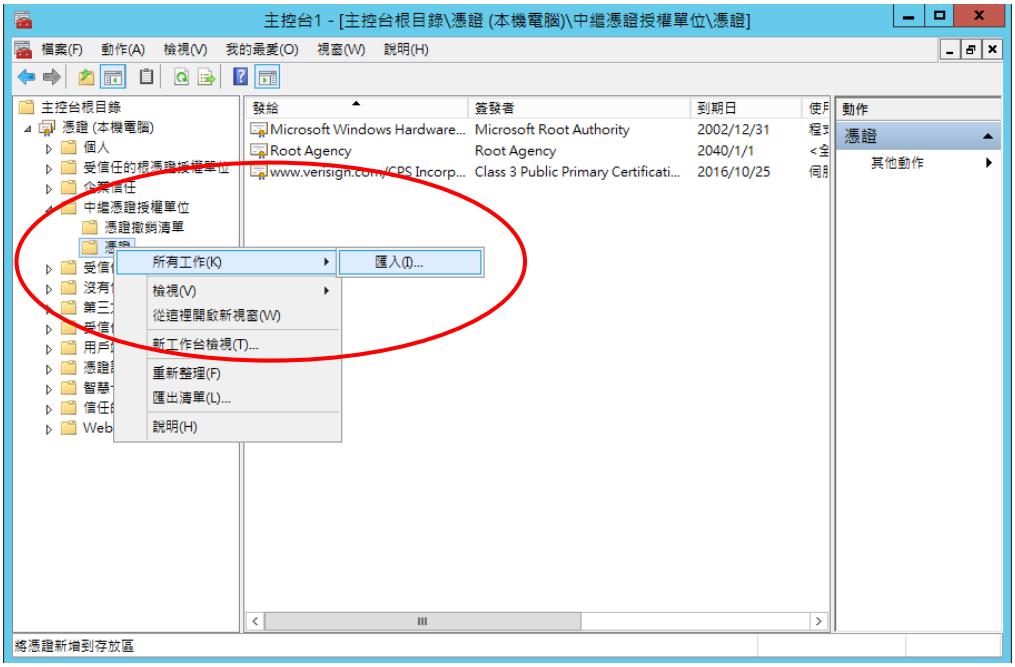
5.5.8 完成中繼憑證安裝

點選確定。



5.5.9 安裝中繼憑證 1(1)

點選展開主控台根目錄內的憑證（本機電腦）→展開中繼憑證授權→於憑證上按滑鼠右鍵選所有工作→點選匯入。



5.5.10 安裝中繼憑證 1(2)

啟動歡迎使用憑證匯入精靈→點選下一步。

5.5.11 安裝中繼憑證 1(3)

點選瀏覽，指定中繼憑證檔（uca1.cer）存放位置→點選下一步。

5.5.12 安裝中繼憑證 1(4)

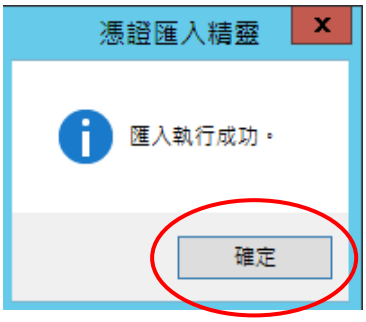
按預設點選將所有憑證放入以下的存放區→憑證存放區→中繼憑證授權→ 點選下一步。

5.5.13 安裝中繼憑證 1(5)

點選完成。

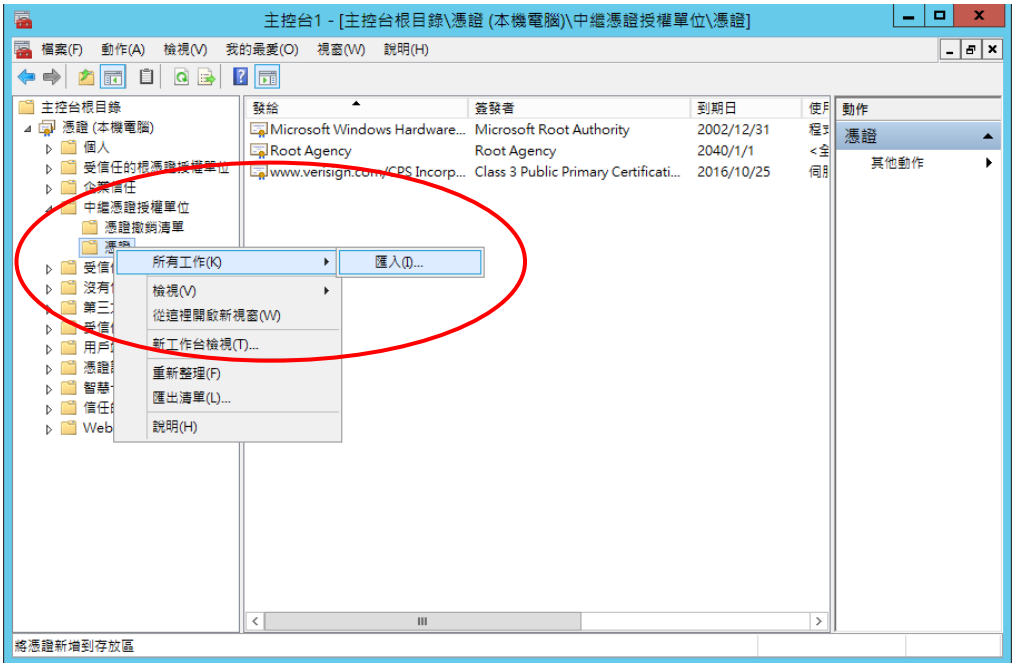
5.5.14 完成中繼憑證 1 安裝

點選確定。



5.5.15 安裝中繼憑證 2(1)

點選展開主控台根目錄內的憑證（本機電腦）→展開中繼憑證授權→於憑證上按滑鼠右鍵選所有工作→點選匯入。



5.5.16 安裝中繼憑證 2(2)

啟動歡迎使用憑證匯入精靈→點選下一步。

5.5.17 安裝中繼憑證 2(3)

點選瀏覽，指定中繼憑證檔（uca2.cer）存放位置→點選下一步。

5.5.18 安裝中繼憑證 2(4)

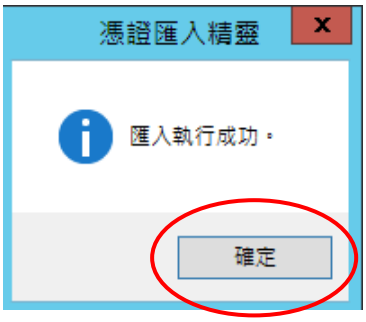
按預設點選將所有憑證放入以下的存放區→憑證存放區→中繼憑證授權→ 點選下一步。

5.5.19 安裝中繼憑證 2(5)

點選完成。

5.5.20 完成中繼憑證 2 安裝

點選確定。



5.6 安裝伺服器憑證

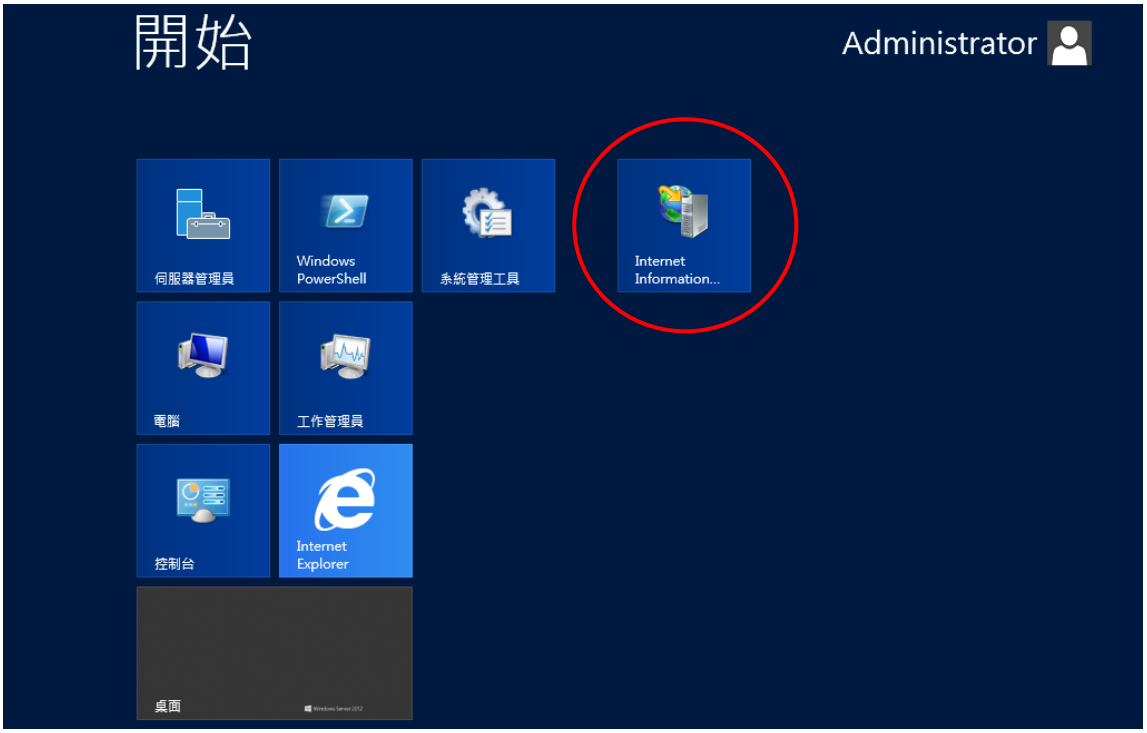
※在安裝伺服器憑證之前，請先完成根憑證及中繼憑證安裝作業！

5.6.1 儲存伺服器憑證檔

請參照 5.3 章節步驟，將伺服器憑證檔（server.cer）儲存於電腦中可存取位置。

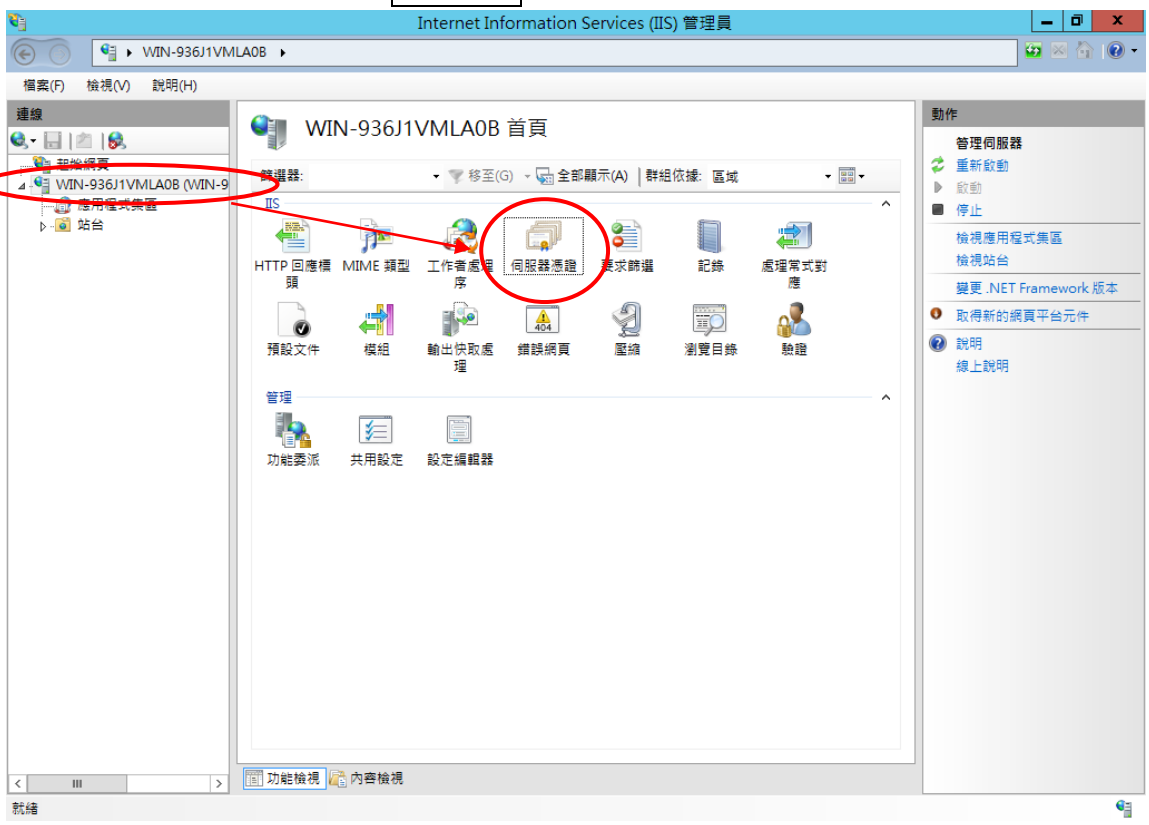
5.6.2 執行網際網路資訊服務(IIS)管理員

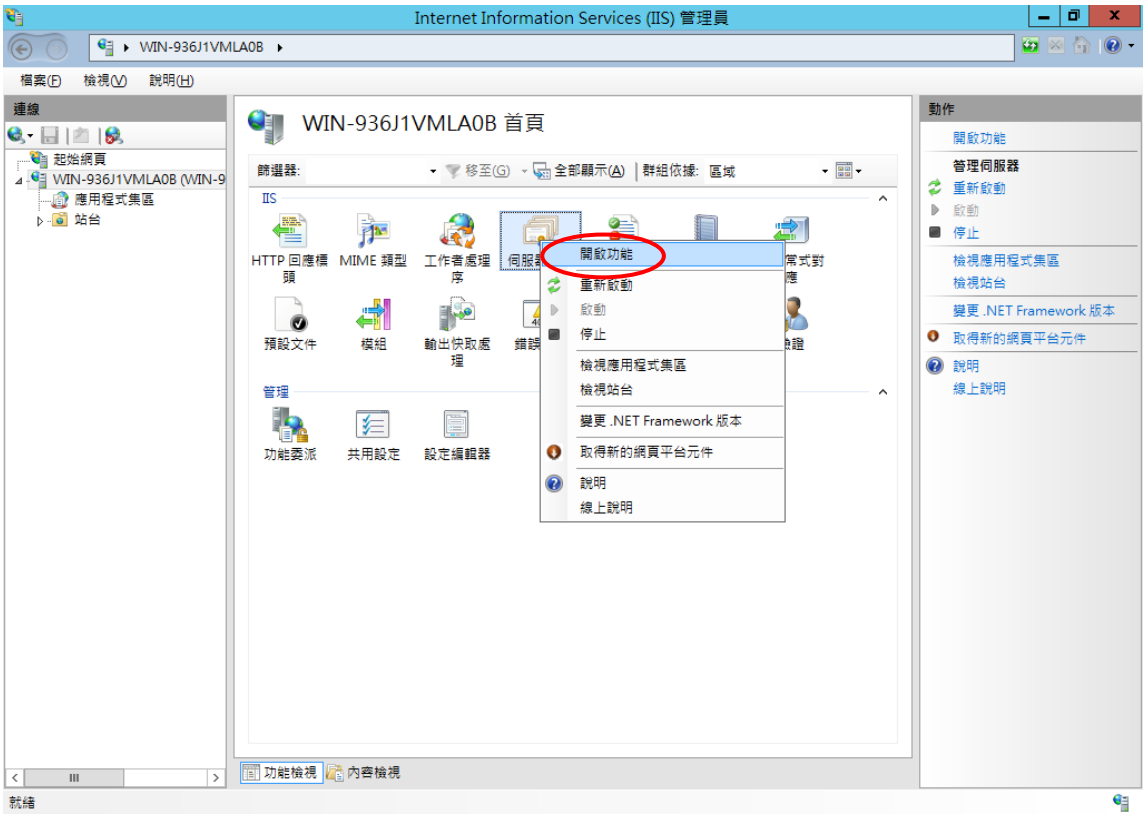
開啟開始頁面→點選 Internet Information Services(IIS)管理員。



5.6.3 安裝伺服器憑證(1)

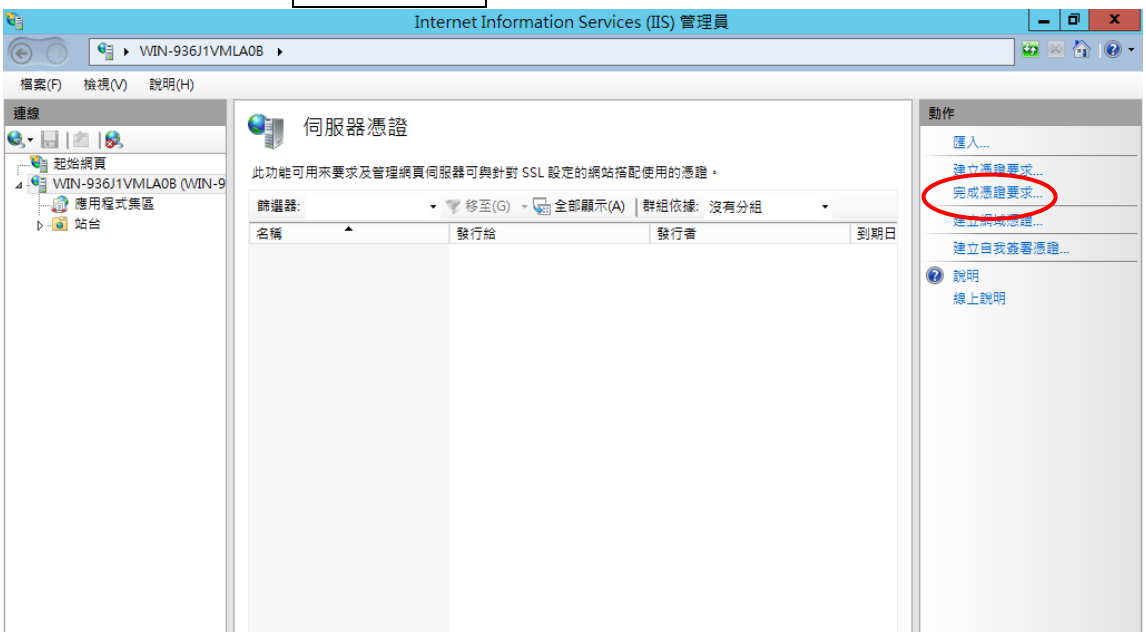
先選擇左側欄位中電腦名稱(電腦名稱\Administrator)→再於伺服器憑證選項按滑鼠右鍵，點選開啟功能。





5.6.4 安裝伺服器憑證(2)

點選右側欄位中完成憑證要求。

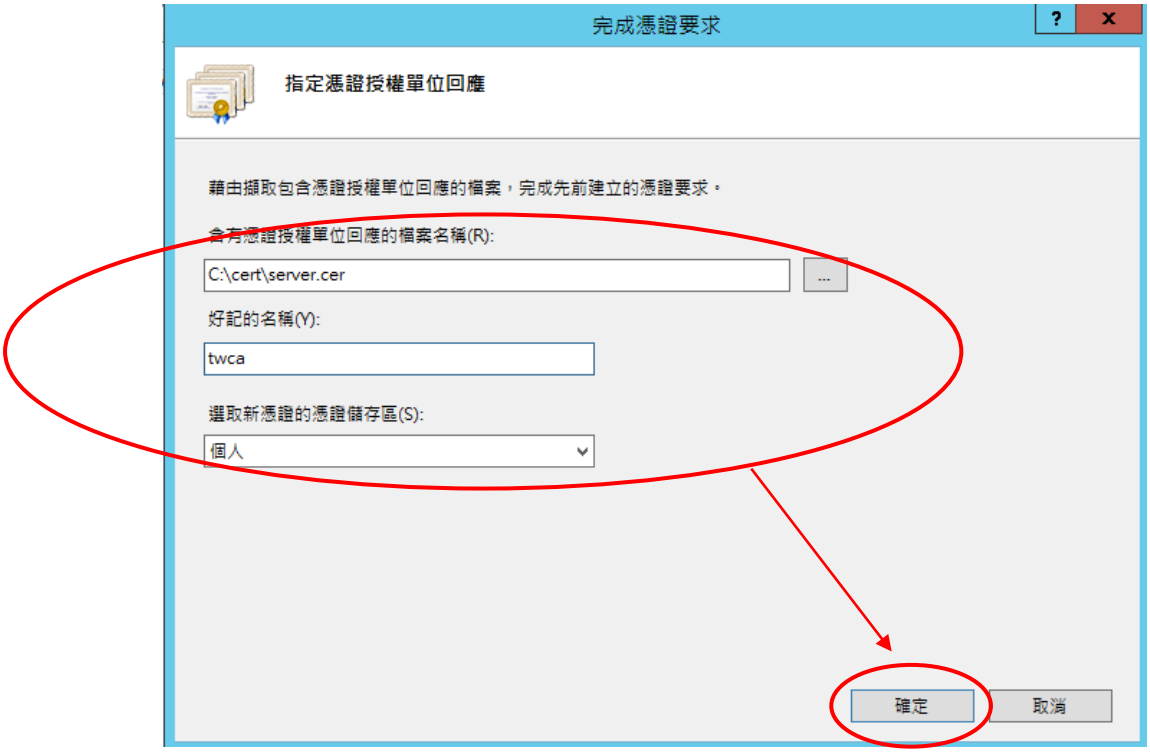


5.6.5 安裝伺服器憑證(3)

5.6.5.1 **含有憑證授權單位回應的檔案名稱(R)：**瀏覽選擇伺服器憑證檔路徑及檔名（如：**server.cer**）。

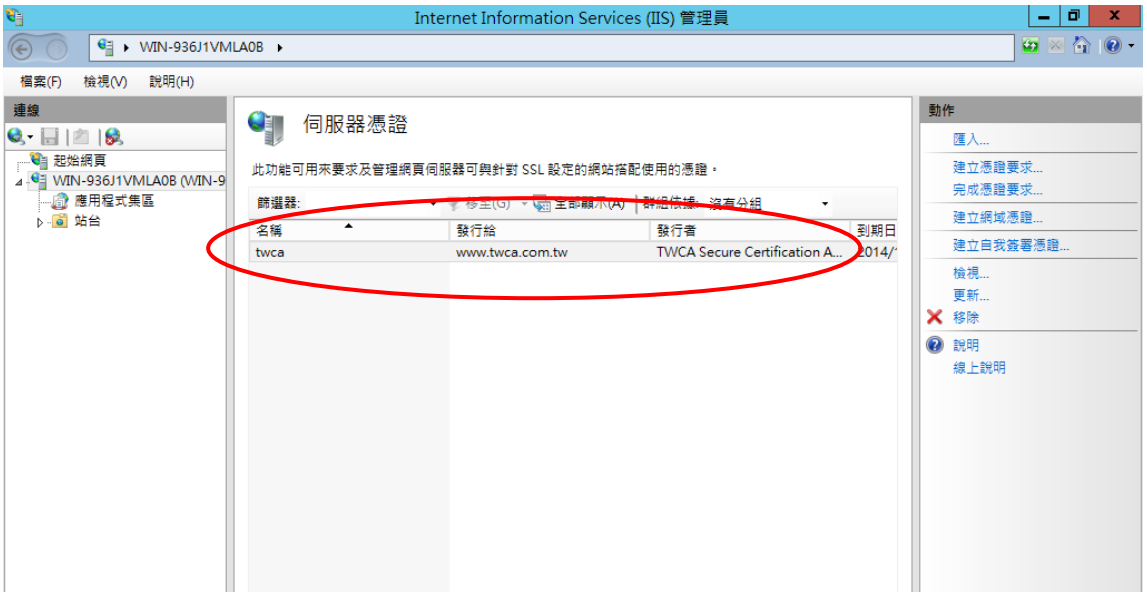
5.6.5.2 **好記的名稱(Y)：**此用途為顯示此憑證的名稱，請自行指定（如：**twca**）

設定完成後，點選確定。



5.6.6 安裝伺服器憑證(4)

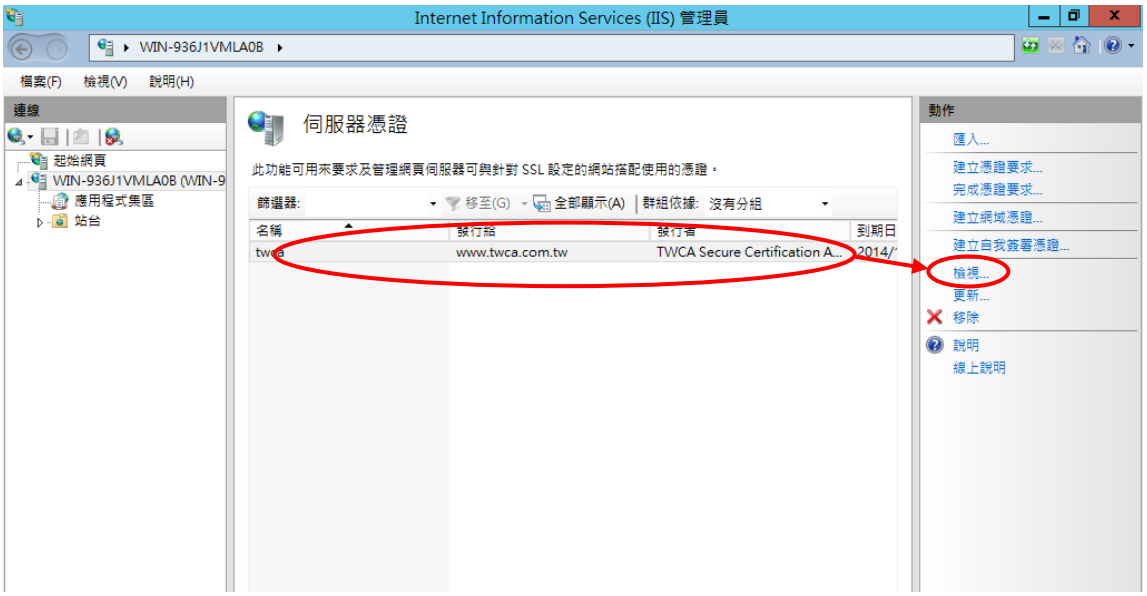
伺服器憑證欄位顯示已安裝之憑證，完成伺服器憑證安裝。



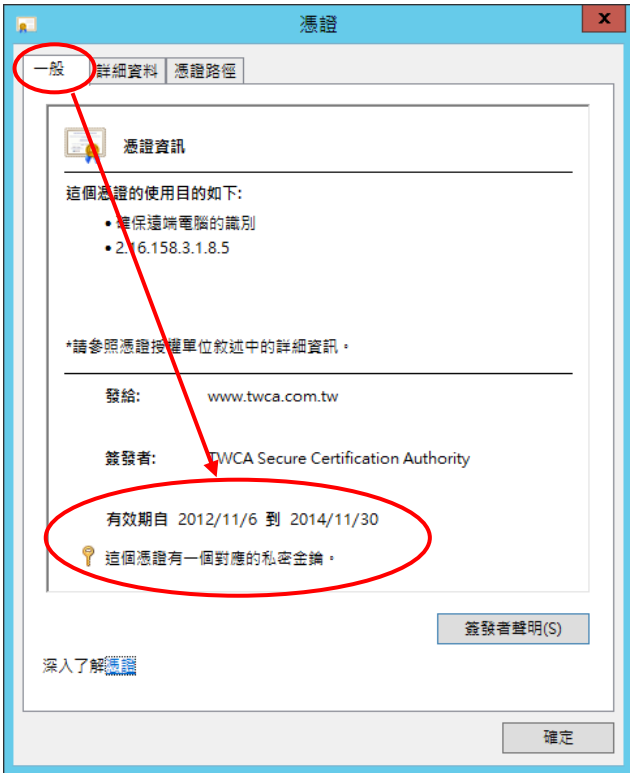
5.7 檢視憑證是否安裝成功

5.7.1 利用 IIS 伺服器憑證功能檢視

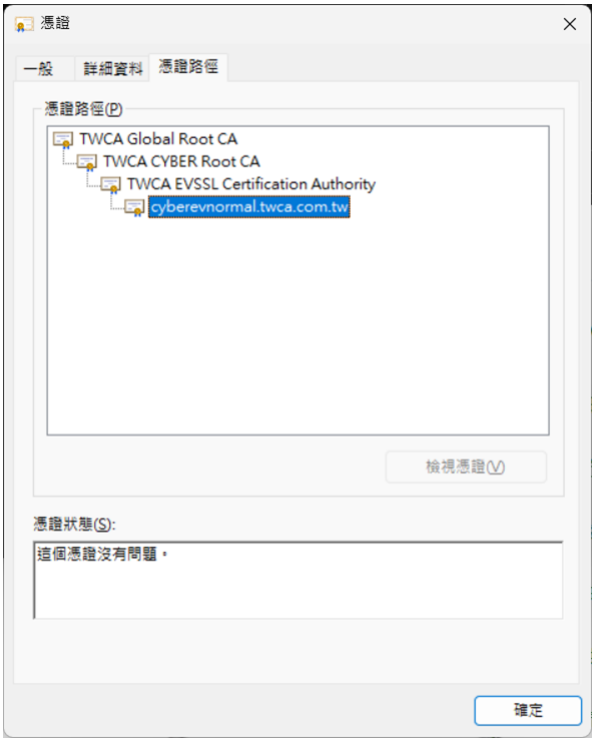
請參照 5.6.3 章節步驟，開啟伺服器憑證功能，並點選開啟欲檢視之憑證。



5.7.1.1 一般欄位：請確認有效期起迄時間是否正確，
並於下方顯示這個憑證有一個對應的私密金鑰。



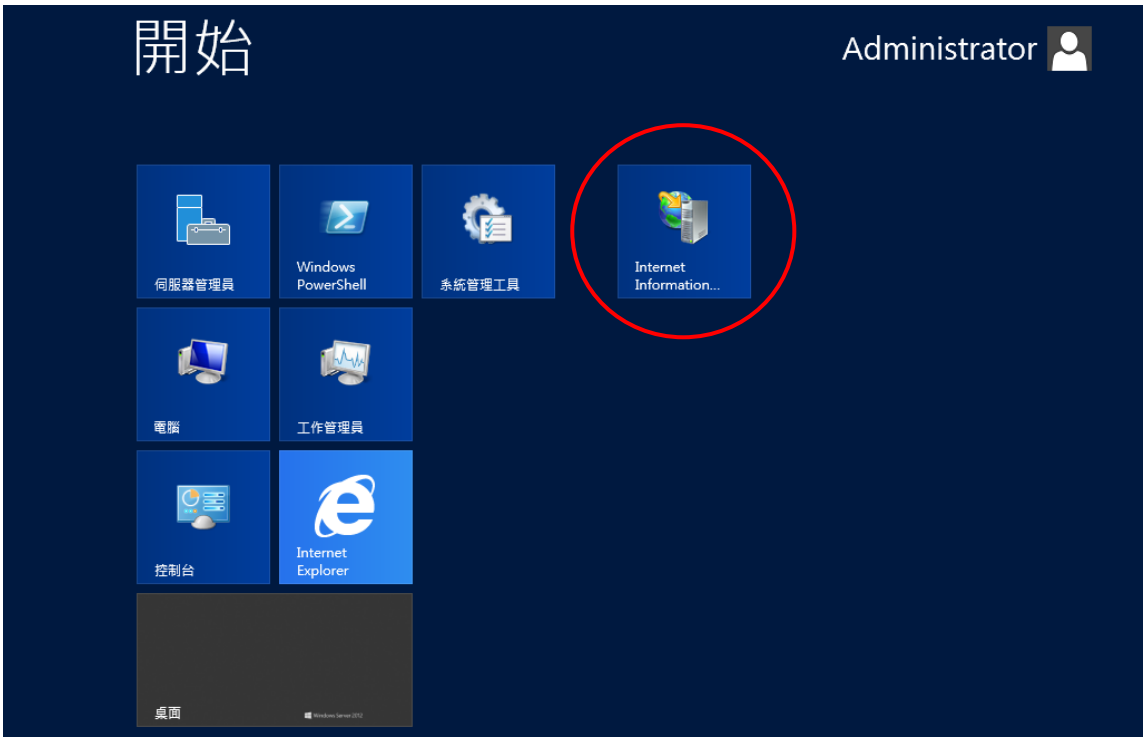
5.7.1.2 憑證路徑欄位：請確認憑證鏈是否正確，且憑證狀態顯示這個憑證沒有問題，可確認憑證已安裝成功。(憑證路徑會因瀏覽器不同而存在三階層或四階層兩種不同的架構，兩種架構皆表示憑證安裝沒有問題。)



5.8 繫結 SSL 憑證

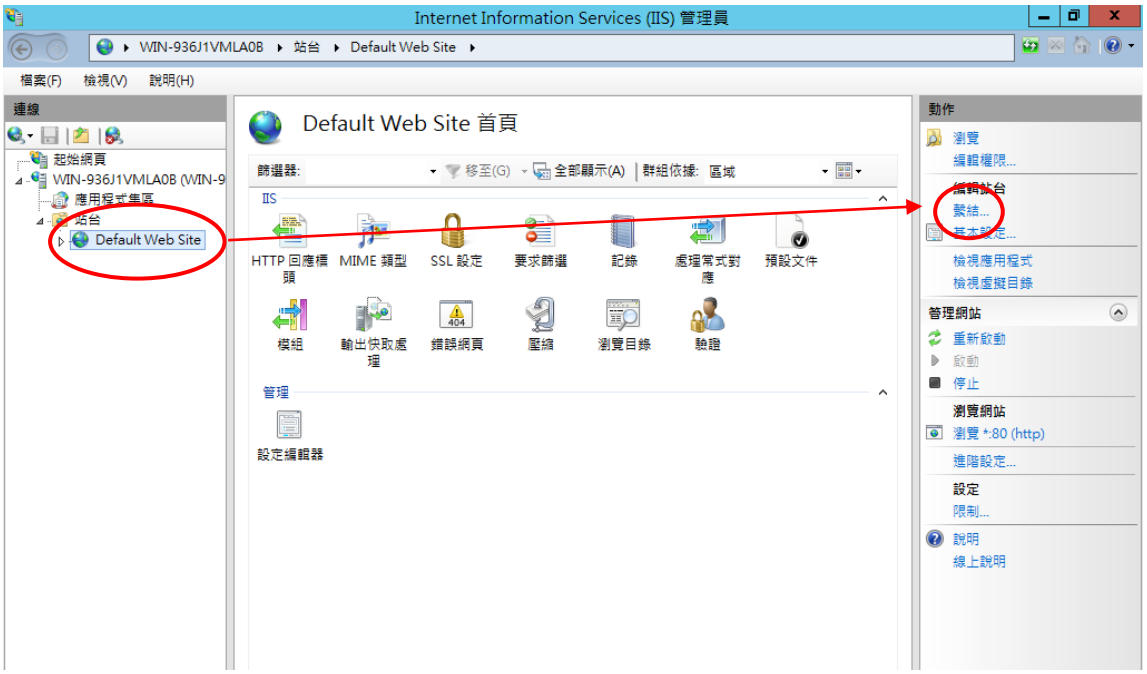
5.8.1 執行網際網路資訊服務(IIS)管理員

開啟開始頁面→點選 Internet Information Services(IIS)管理員。



5.8.2 繫結 SSL 憑證(1)

選擇左側欄位中電腦名稱(電腦名稱\Administrator)→展開點選欲設定 SSL 憑證加密的站台→於右側欄位點選繫結。

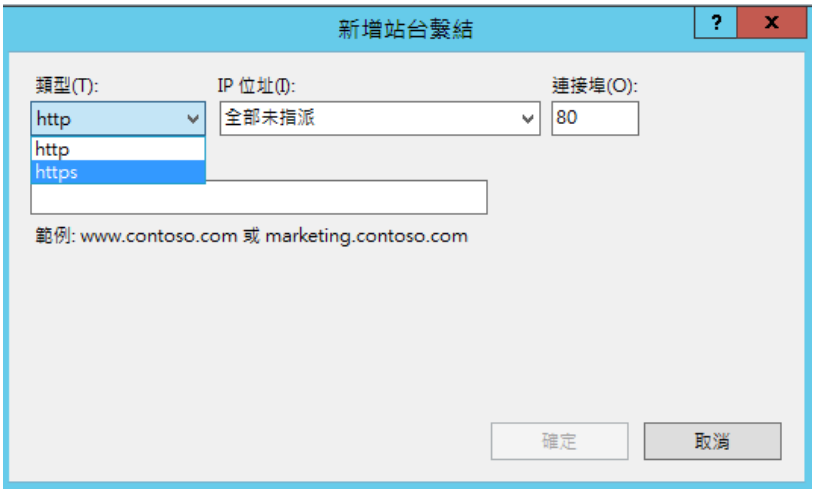


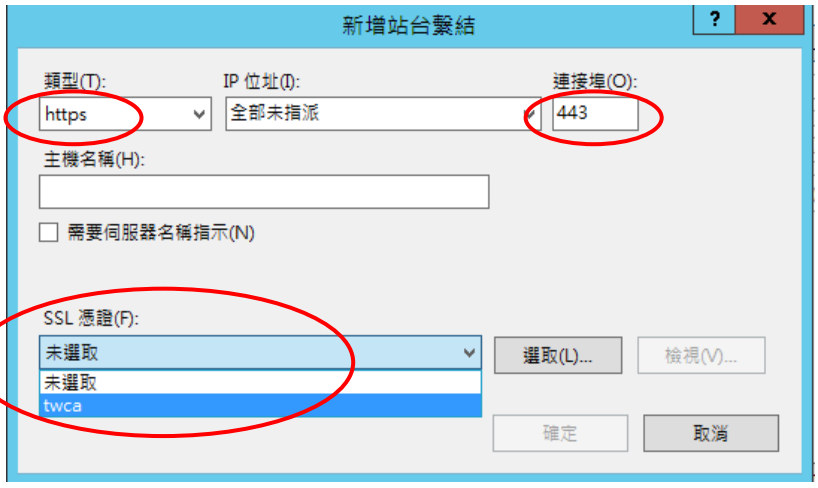
5.8.3 繫結 SSL 憑證(2)

點選新增，新增 SSL 連接埠設定。

5.8.4 繫結 SSL 憑證(3)

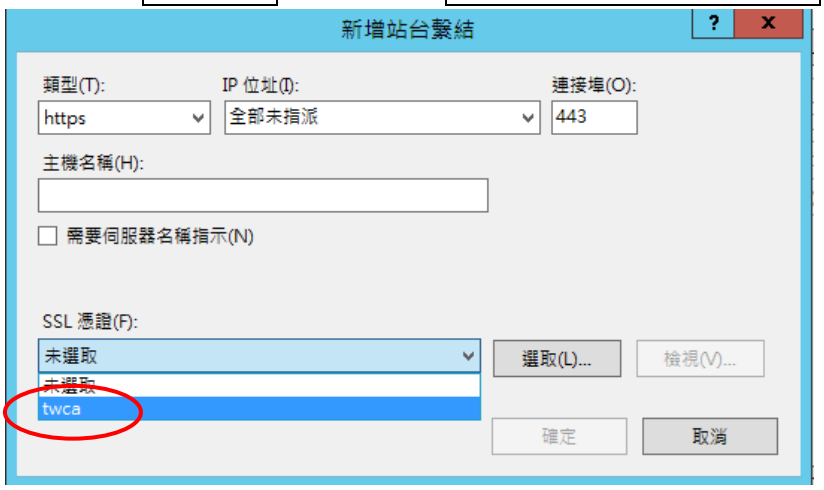
下拉類型選項，選擇 https，使連接埠選項顯示 SSL 預設 443 埠，並出現 SSL 憑證選項可供選擇。

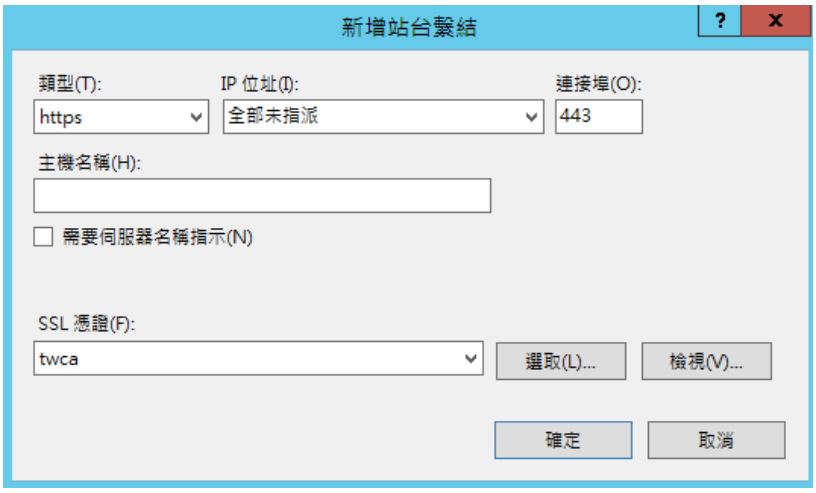




5.8.5 繫結 SSL 憑證(4)

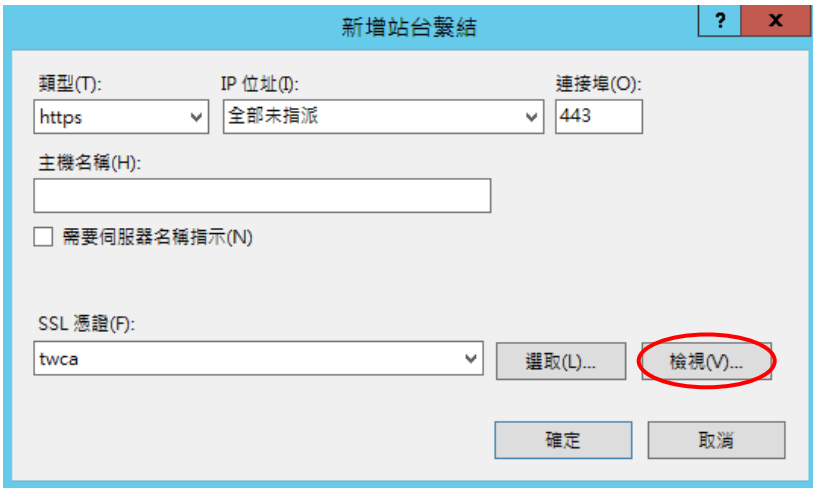
下拉 SSL 憑證選項，選擇 5.6 章節安裝之伺服器憑證。

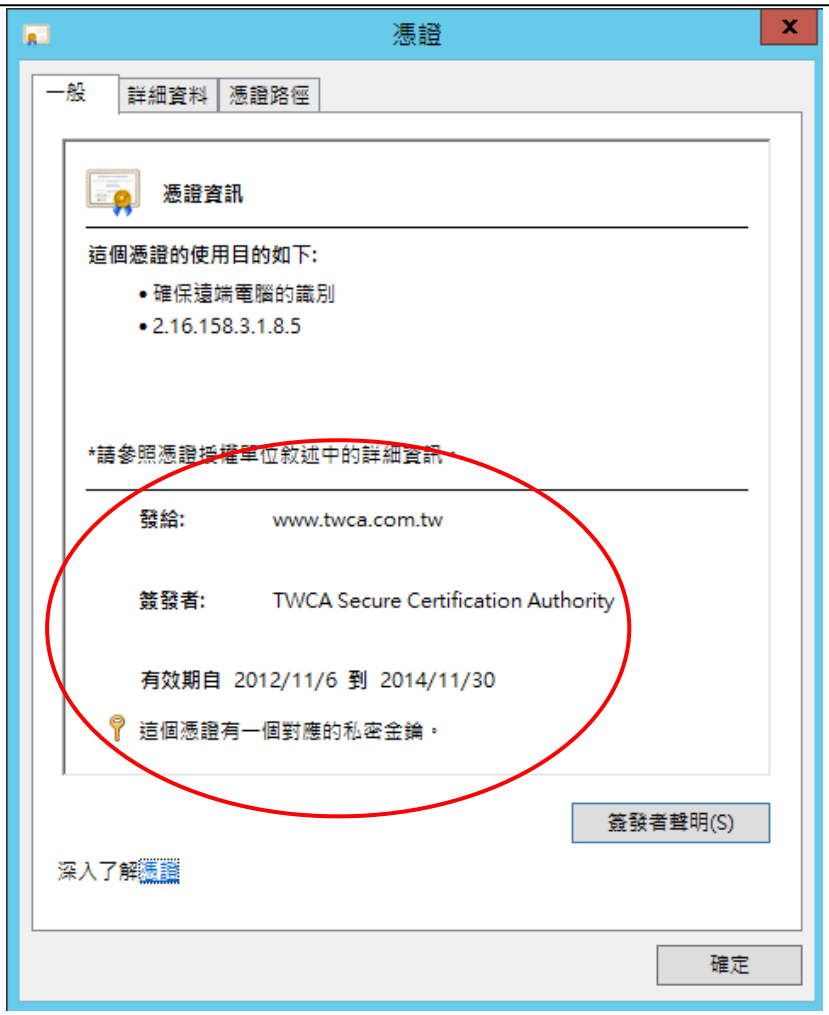




5.8.6 確認選擇的憑證是否正確

點選檢視，確認選擇的憑證是否正確。





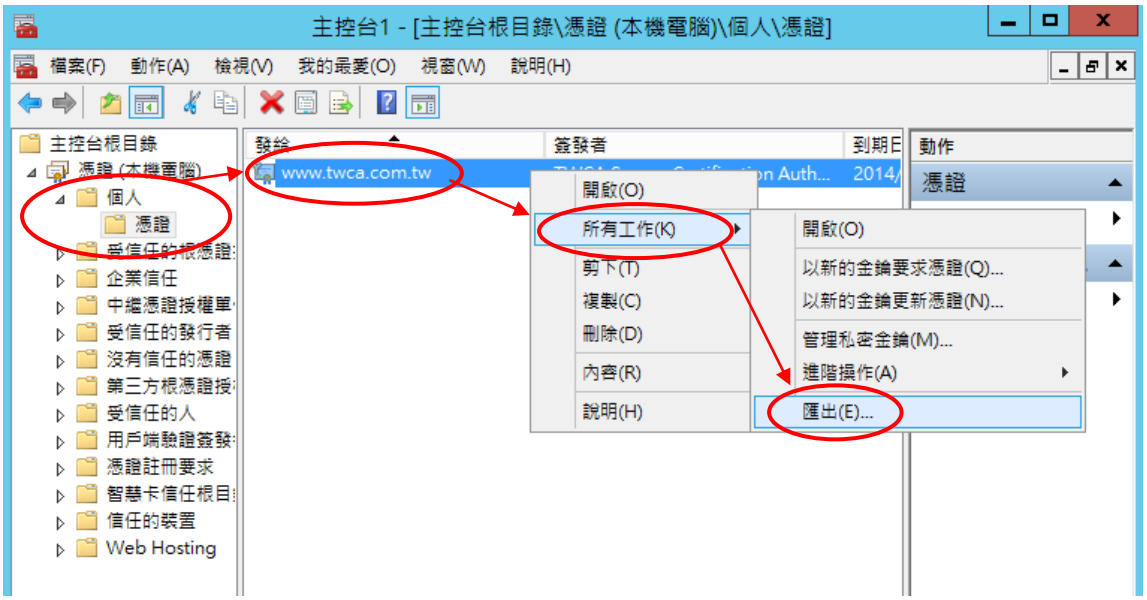
5.9 匯出憑證(備份)

5.9.1 新增憑證管理單元

請參照 5.12 章節步驟，新增憑證管理單元。

5.9.2 匯出憑證(1)

點選展開主控台根目錄內的憑證（本機電腦）→個人→憑證，在欲匯出的伺服器憑證上按右鍵所有工作→點選匯出。



5.9.3 匯出憑證(2)

啟動歡迎使用憑證匯出精靈→點選下一步。

5.9.4 匯出憑證(3)

點選是，匯出私密金鑰(Y)→點選下一步。

5.9.5 匯出憑證(4)

點選個人資訊交換-PKCS#12(.PFX)→勾選如果可能的話，包含憑證中所有的憑證、啟用憑證隱私權→點選下一步。

5.9.6 匯出憑證(5)

設定匯出資料的保護密碼→點選下一步。(請務必記住此密碼，匯入憑證時需使用)

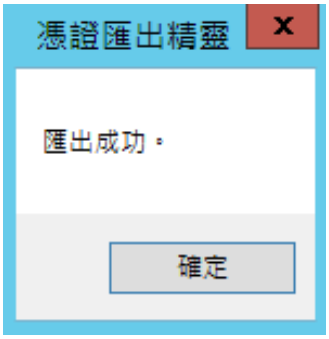
備註:系統版本過舊在加密選項必需選擇 TripleDES-SHA1，避免系統不支援

5.9.7 匯出憑證(6)

點選瀏覽→指定一個匯出檔案存放的路徑與檔名(副檔名固定為.PFX)→點選下一步。

5.9.8 完成匯出憑證(備份)

點選完成，完成匯出憑證(備份)。



5.10 匯入憑證(還原)

5.10.1 安裝根憑證

請參照 5.4 章節步驟，進行根憑證安裝作業

5.10.2 安裝中繼憑證

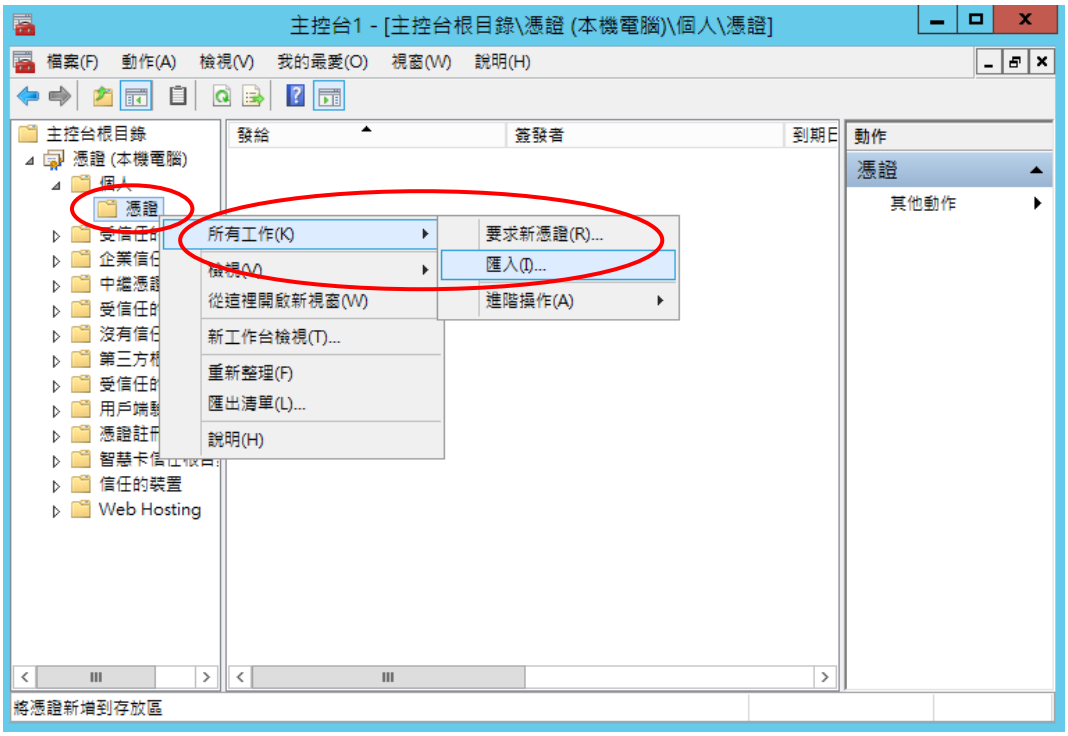
請參照 5.5 章節步驟，進行中繼憑證安裝作業

5.10.3 新增憑證管理單元

請參照 5.12 章節步驟，新增憑證管理單元。

5.10.4 匯入憑證(1)

點選展開主控台根目錄內的憑證（本機電腦）→個人→憑證，按滑鼠右鍵→所有工作 →點選匯入。

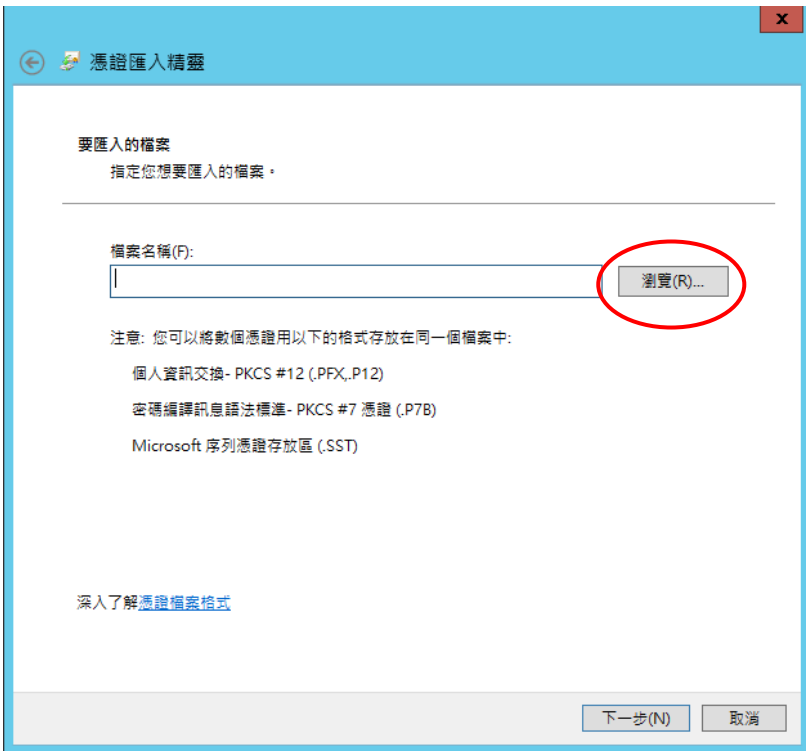


5.10.5 匯入憑證(2)

啟動歡迎使用憑證匯入精靈→點選下一步。

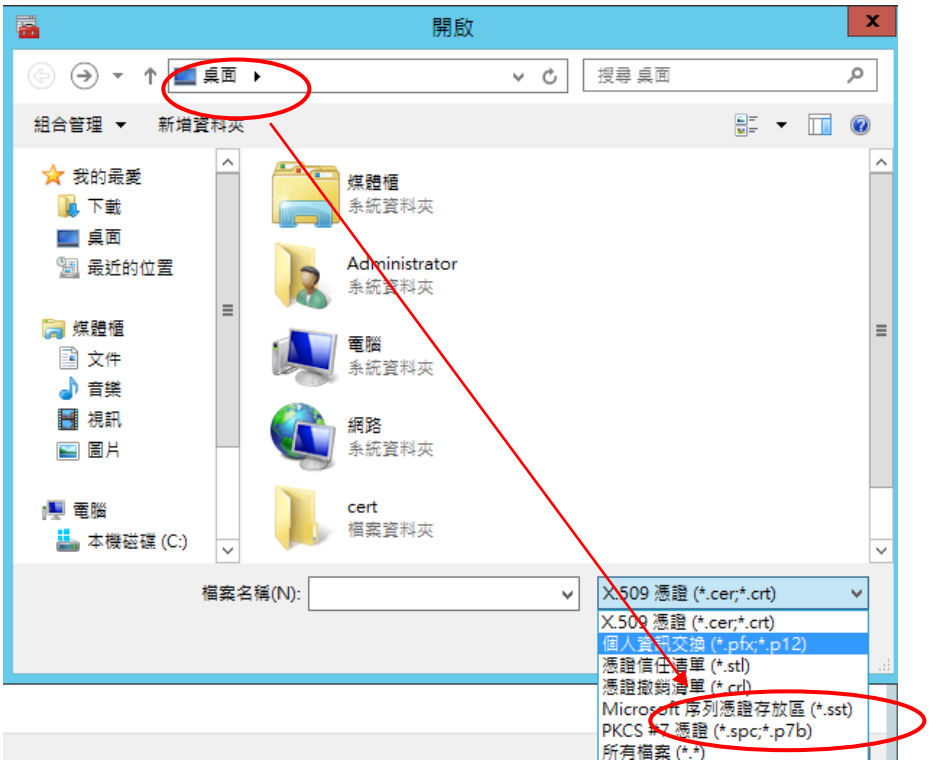
5.10.6 匯入憑證(3)

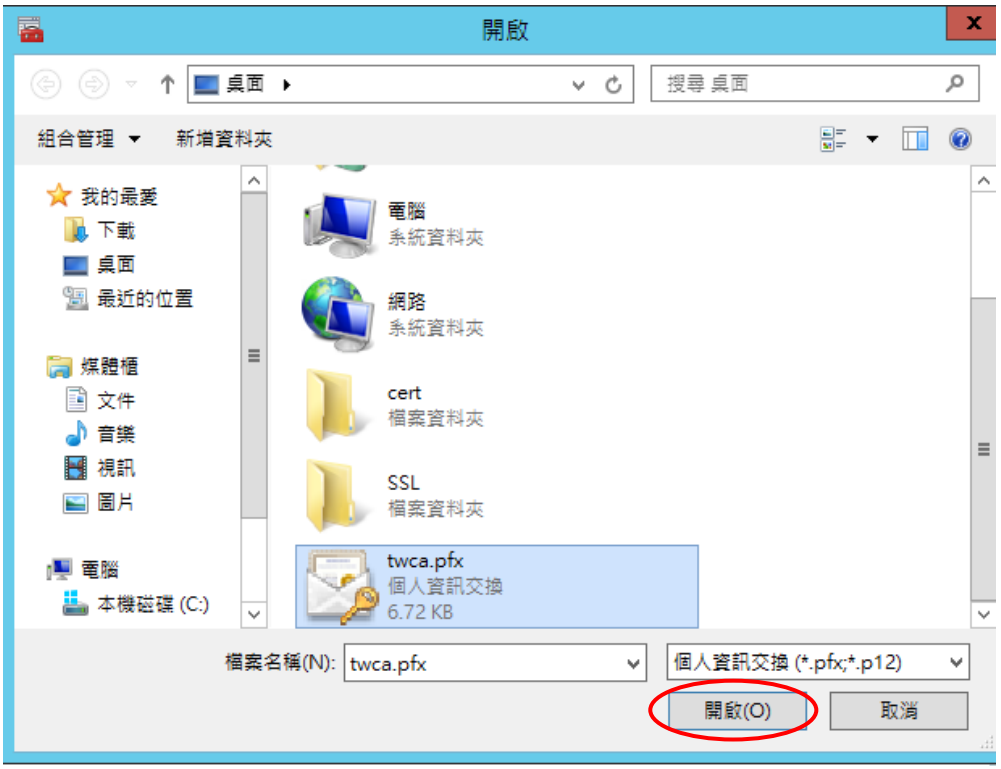
點選瀏覽。



5.10.7 匯入憑證(4)

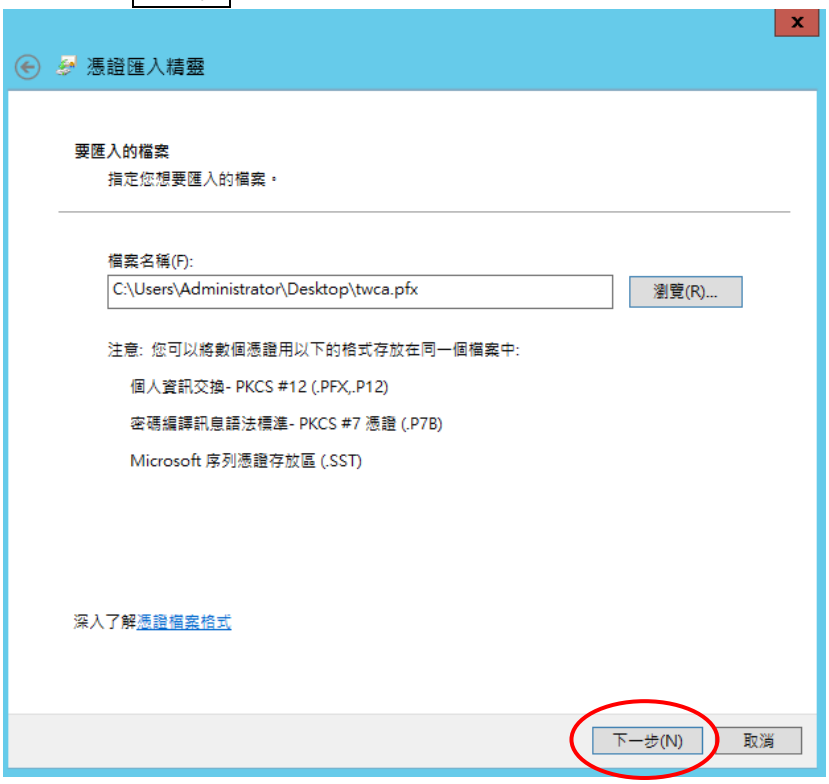
指定到當初匯出備份的檔案(*.PFX) →點選開啟舊檔。





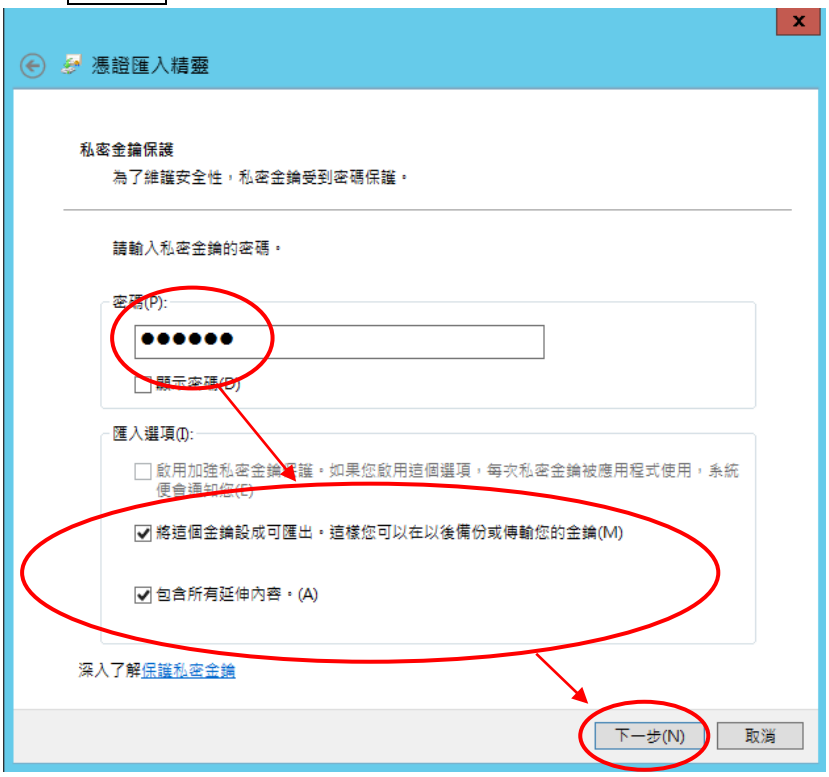
5.10.8 匯入憑證(5)

點選下一步。



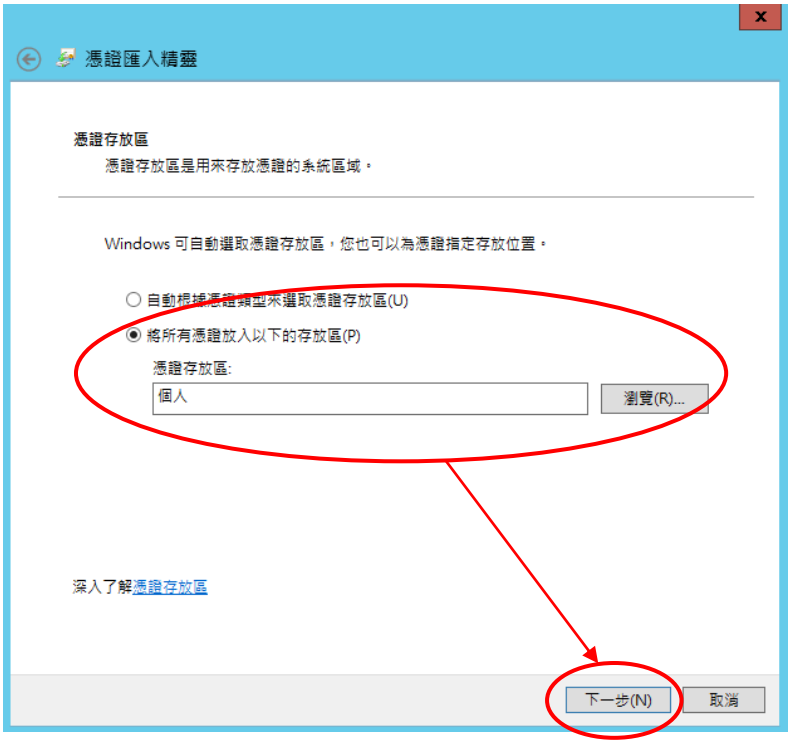
5.10.9 匯入憑證(6)

輸入當初匯出(備份)憑證時所設定的密碼 →勾選將私密金鑰標示成可匯出。這樣您可以在以後備份或傳輸您的金鑰及包含所有延伸內容→點選下一步。



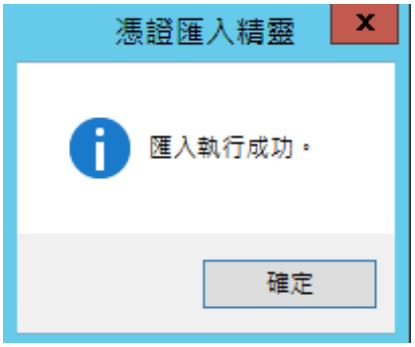
5.10.10 匯入憑證(7)

按預設點選將所有憑證放入以下的存放區→憑證存放區→個人→點選下一步。



5.10.11 匯入憑證(8)

點選完成。



5.10.12 繫結 SSL 憑證

請參照 5.8 章節步驟進行繫結 SSL 憑證作業，完成匯入憑證(還原)。

5.11 更新 SSL 憑證

5.11.1 申請說明

臺灣網路認證公司會在 SSL 伺服器憑證到期前二個月發出憑證更新通知信給　貴公司。這二個月內您隨時可以至本公司網站 http://www.twca.com.tw 下載申請表單，填寫完畢後寄回臺灣網路認證公司，即可進行 SSL 憑證更新申請。

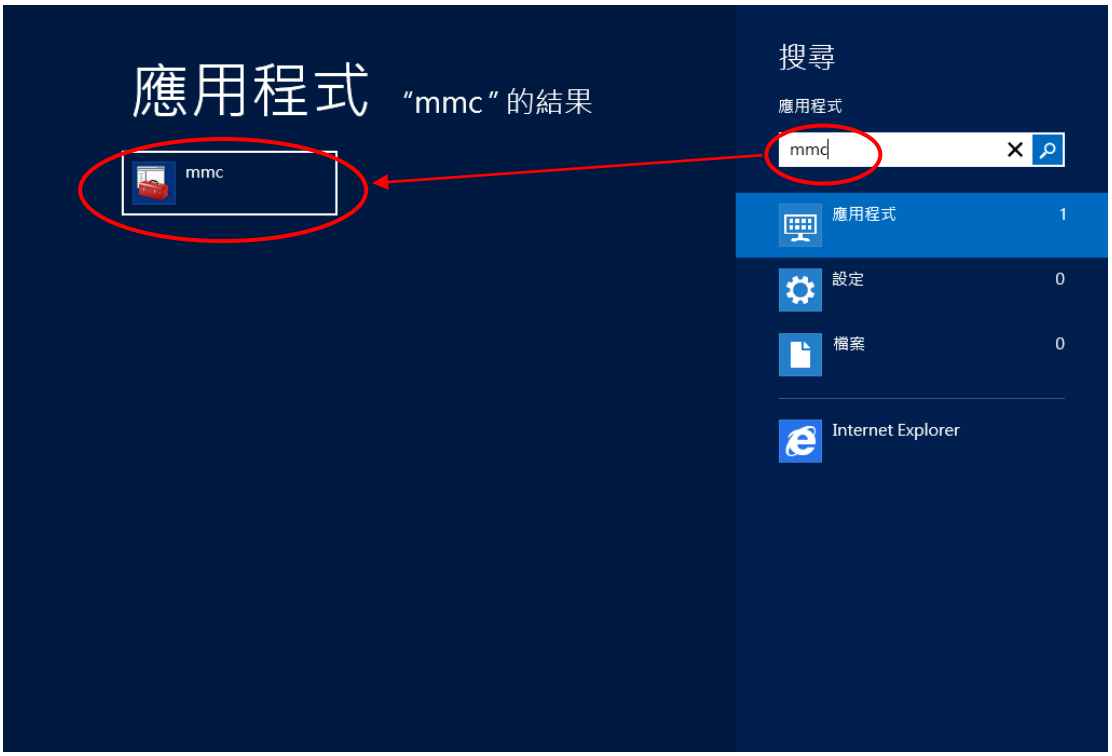
5.11.2 更新步驟

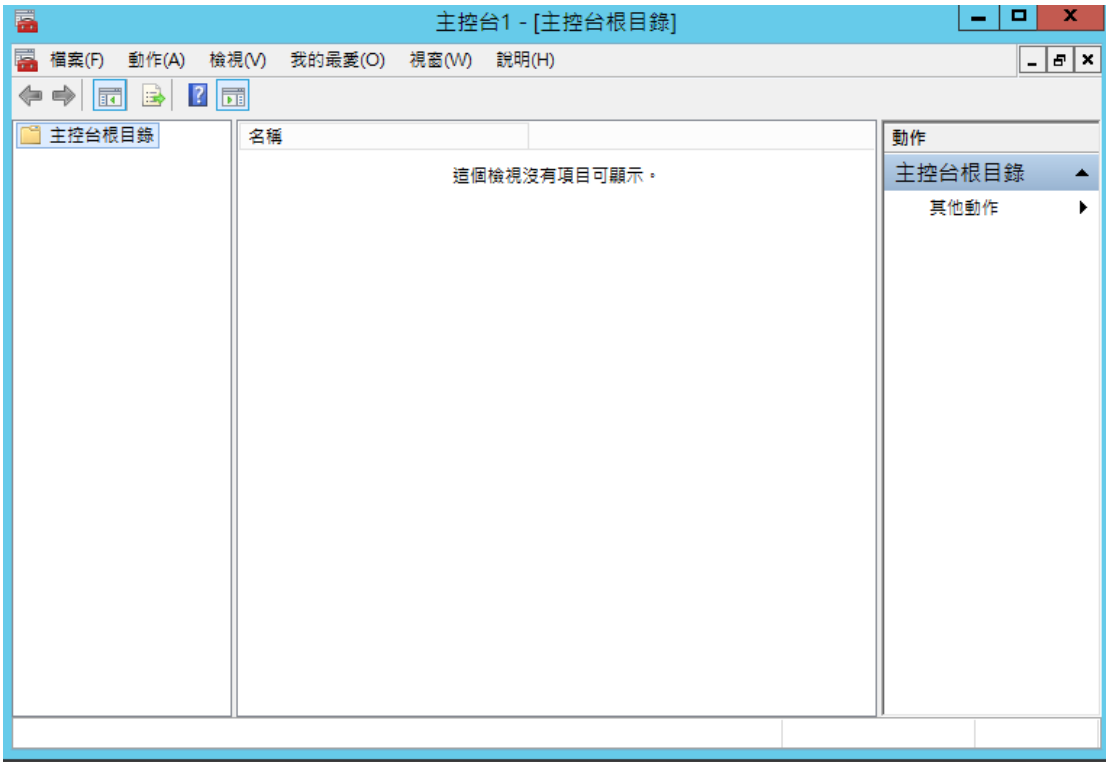
請參照 5.1 至 5.8 章節步驟申請安裝憑證，即可完成 SSL 憑證更新。

5.12 新增憑證管理單元

5.12.1 開啟 MMC 主控台

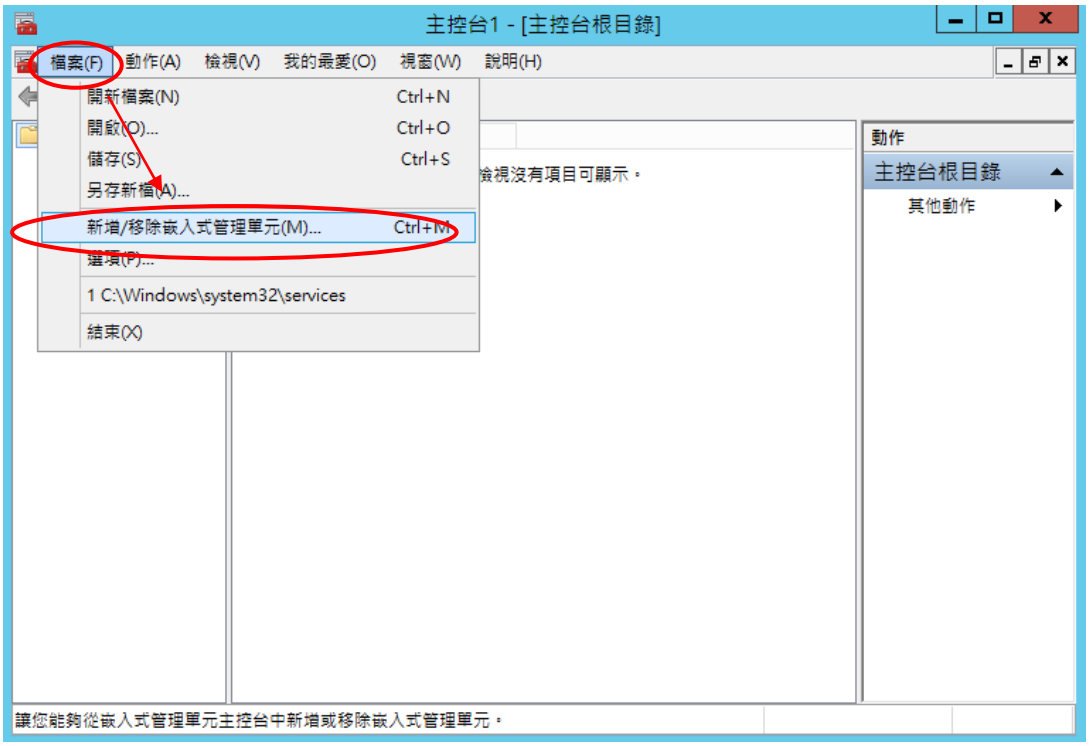
開啟開始頁面→搜尋列中輸入 mmc→點擊開啟 mmc。





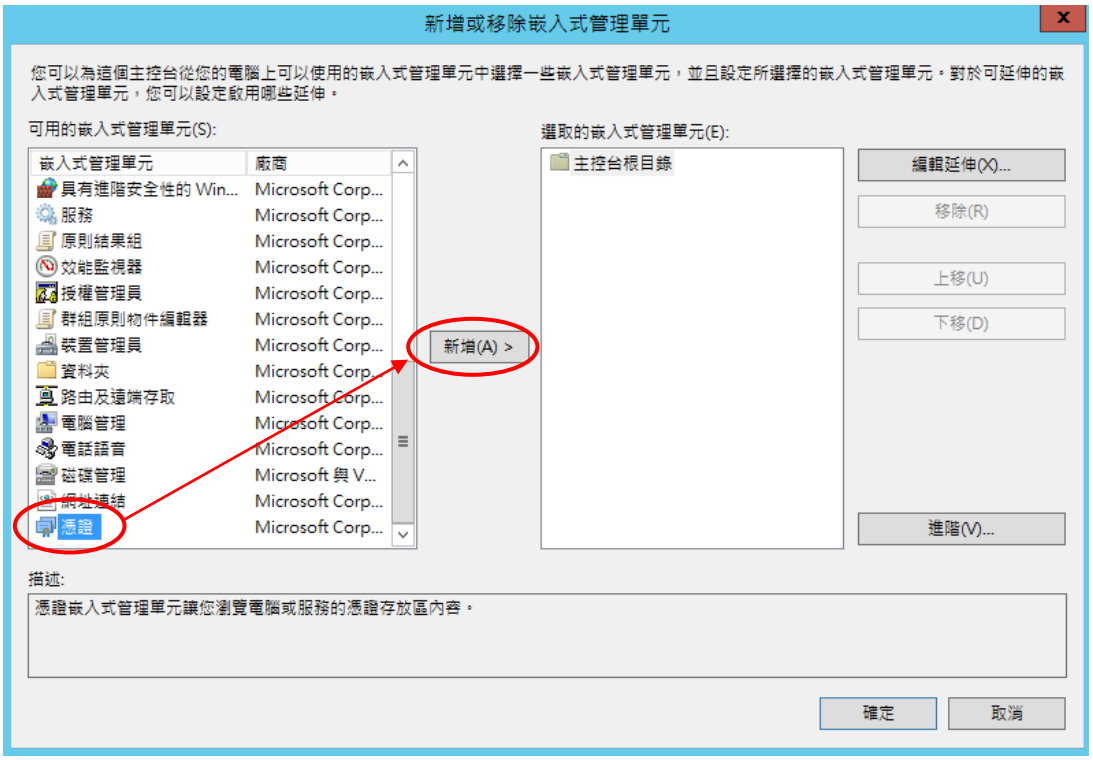
5.12.2 新增/移除嵌入式管理單元

點選檔案→點選新增/移除嵌入式管理單元。



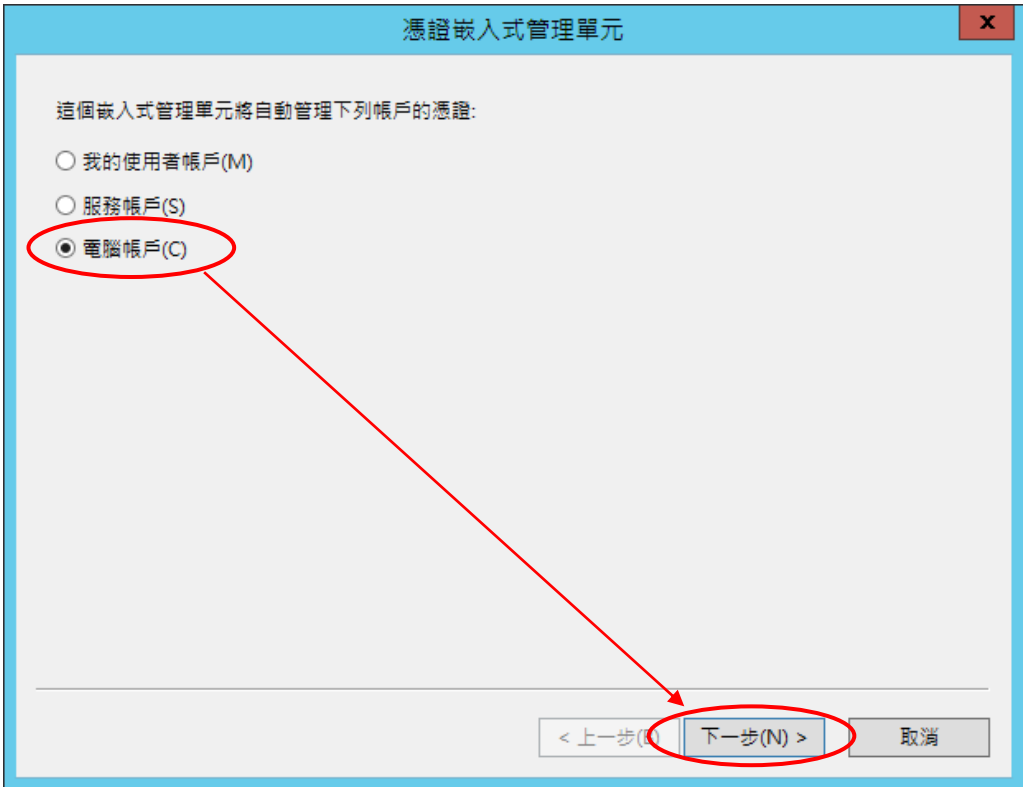
5.12.3 新增憑證管理單元(1)

點選憑證→點選新增。



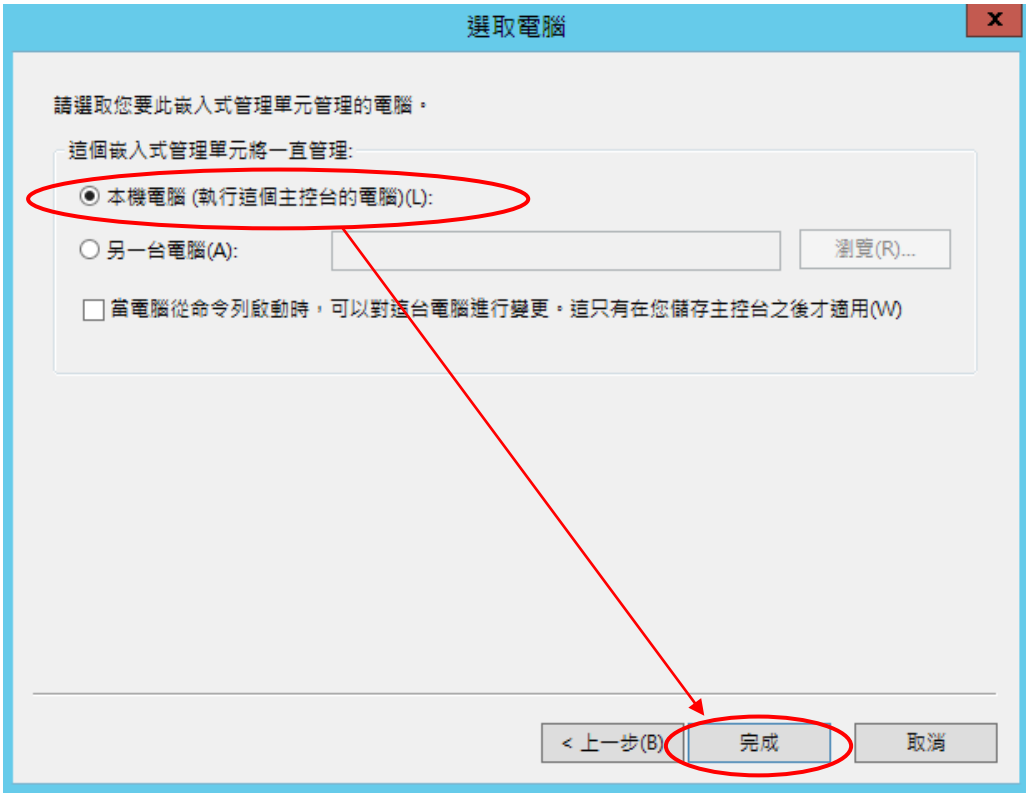
5.12.4 新增憑證管理單元(2)

選擇電腦帳戶→點選下一步。



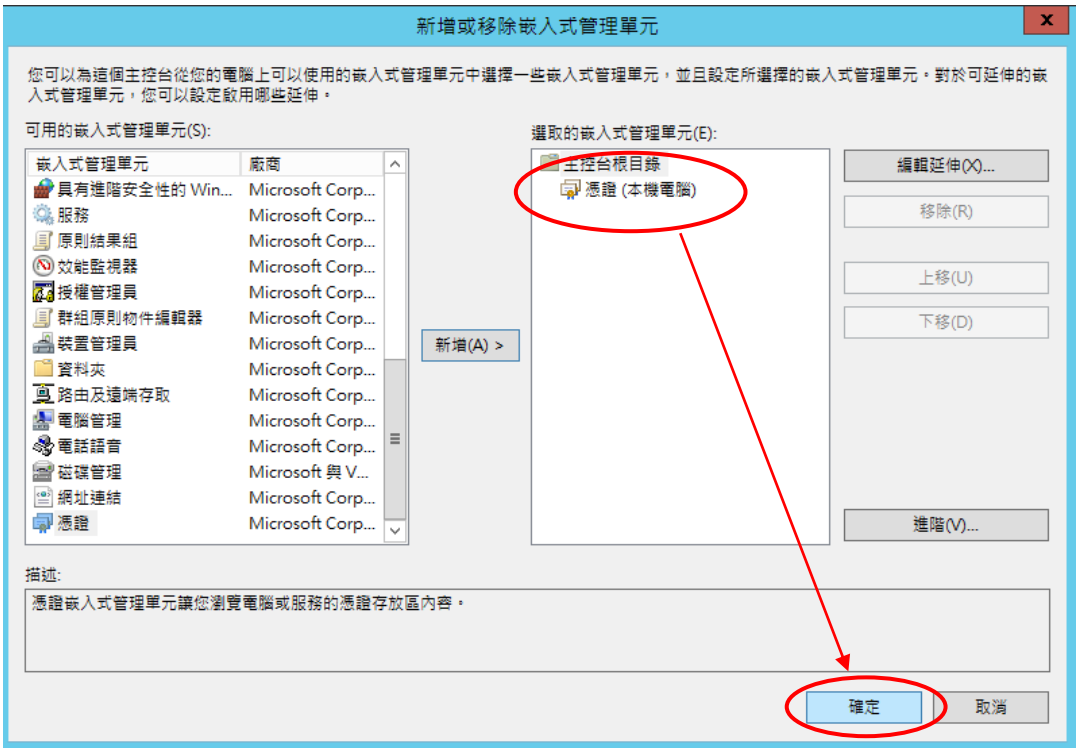
5.12.5 新增憑證管理單元(3)

點選本機電腦(執行這個主控台的電腦)→點選完成。



5.12.6 新增憑證管理單元完成

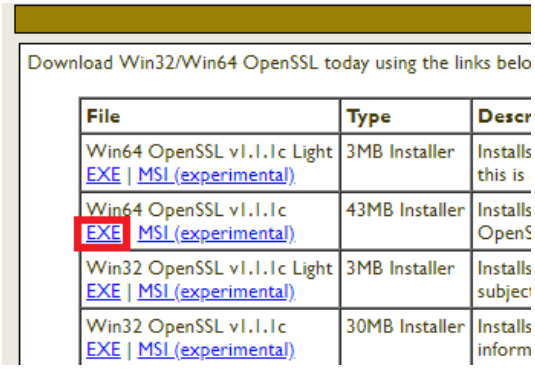
當憑證(本機電腦)新增完成後→點選確定。



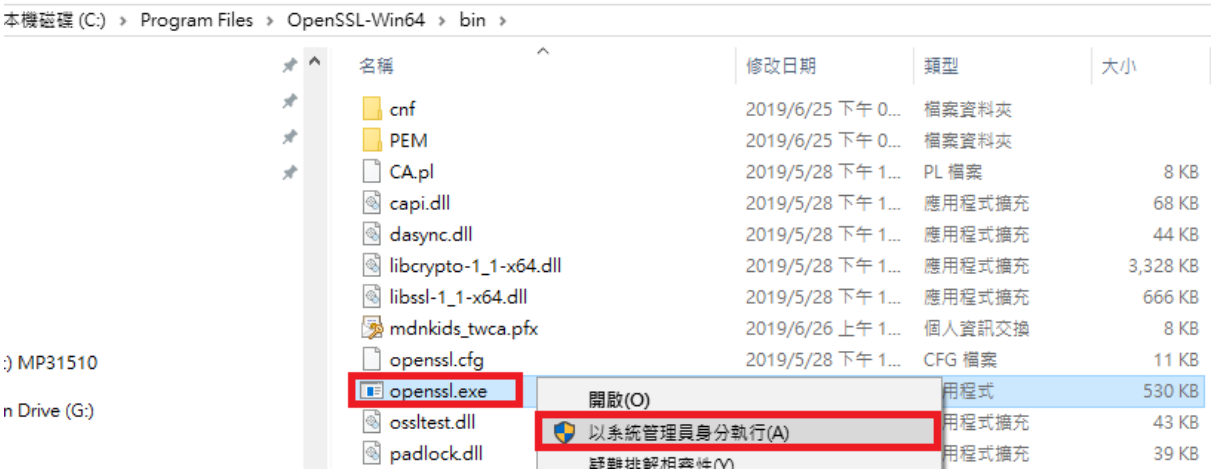
6.常見問題

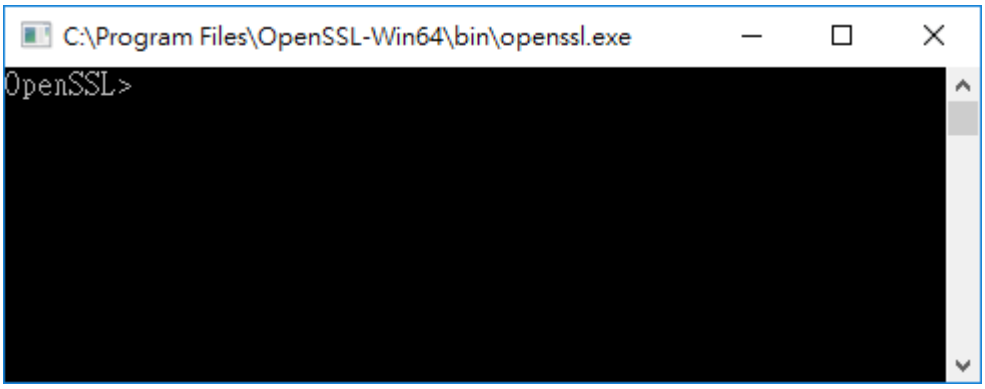
6.1如何以工具檢測憑證鏈是否有安裝(使用 openssl 工具)

請至 https://slproweb.com/products/Win32OpenSSL.html，依照您的作業系統版本，下載 exe 執行檔並安裝(請不要安裝 light 版本)，安裝步驟一直點選下一步，直到安裝完畢。

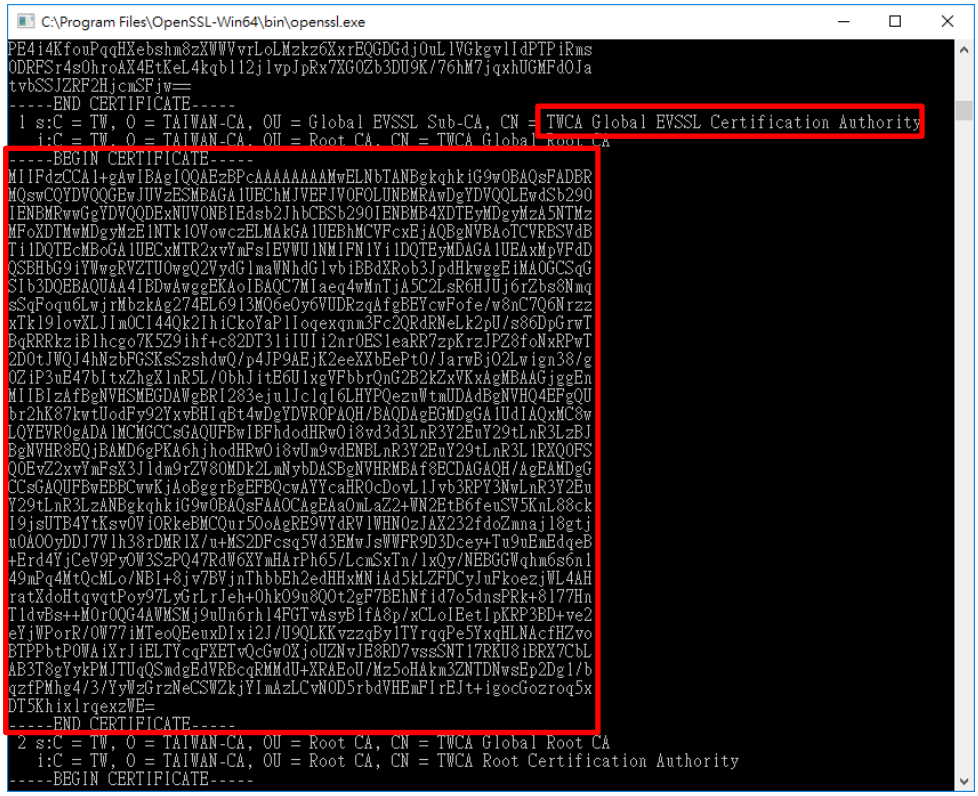


接著到 openssl 目錄的 bin 底下，以系統管理員身分執行 openssl.exe。





執行指令: s_client -connect www.twca.com.tw:443 -showcerts，其中 www.twca.com.tw 請改成您的網站 CN，執行後可以此網站安裝了那些憑證，每一個-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----所包夾的區塊即為一張憑證，而該區塊上面就是該憑證的資訊，CN 可識別這是哪一張憑證。注意:需要看到至少回應兩個區塊(兩張憑證)以上。



6.2若新憑證安裝後，由 internet 連線網站顯示仍為舊憑證，分為以下幾種可能。

6.2.1 更新完憑證後服務未重啟。

6.2.2 憑證是安裝在多台伺服器上，每一台皆需更換。

6.2.3 裝錯台伺服器。

6.2.4 前端可能有其他網路設備有安裝憑證，需一併更換。

6.2.5 您的網站有可能是委外管理。

請先在伺服器本機確認網站所顯示的憑證為新憑證，在依以上幾種情況確認。

情況 6.2.1:

請重啟服務，重新由 internet 連線網站再次確認。

情況 6.2.2:

原因說明:您的網站可能是架設在多台伺服器上，因為您現在連線到的剛好是沒有更新到憑證的伺服器，才會看到舊的憑證。

解決方式:請確認每一台伺服器都匯入憑證後，再重新連線網站確認是否看到新憑證。

情況 6.2.3:

原因說明:您安裝憑證的這台伺服器，並不是對外提供服務的伺服器。

解決方式:若懷疑憑證裝錯台，可藉由關閉目前這台伺服器的服務，重新由 internet 連線網站，確認是否已看不到憑證資訊，若依舊看的到，則代表此台伺服器並非提供服務的伺服器。等找到正確的伺服器後再將憑證匯

入。

情況 6.2.4:

原因說明:使用者從 internet 連線至貴公司網站，可能會先經過網路設備，再到網站伺服器。所以若網站伺服器已更換憑證，網路設備卻沒一併更換，當連線經過網路設備時，就會看到舊的憑證。

解決方式:若要確認從 internet 上看到的憑證是不是目前這台伺服器所裝的，可藉由關閉目前這台伺服器的服務，重新由 internet 連線網站，確認是否已看不到憑證資訊，若看不到，可確認憑證確實是裝在這台伺服器。

情況 6.2.5:

原因說明:您的網站伺服器並非建在公司內部，而是建在外部廠商那一端。

解決方式:若您的 CSR 是由廠商提供的，請直接將憑證轉交給廠商，請他們協助安裝;若 CSR 是由貴公司產製，請將憑證及金鑰一併提供給廠商，再請他們協助安裝。

6.3 使用 HTTPS 連線網頁，Chrome 瀏覽器會出現警告訊息(不安全網頁)

您的網頁，可能有嵌入一些非經 https 加密連線取得的內容。

原因說明:為了用戶隱私和安全，一旦使用 Google 的 Chrome 瀏覽器連線到某個網頁，原始內容包含非經 https 加密連線取得的圖片、影片、音訊等，瀏覽器就會將該網站視為不安全。

解決方式:使用 Chrome 瀏覽器連到網站後按 F12，點選 Console 可看到錯誤訊息，藉此確認您的網頁有哪些非經 https 加密連線取得的內容。請移除這些內容，或改由 https 方式取得，再使用 chrome 以 https://連線您的網站，確認是否不再出現不安全網頁訊息。

6.4 IIS 匯入憑證後，憑證消失

原因說明:在執行**「完成憑證要求」**時的伺服器，必須與**「建立憑證要求」**時的伺服器**同一台**，因建立憑證要求時，私密金鑰會一併產生在該伺服器，如果憑證發下來是裝在另一台伺服器就會找不到當初那一把私密金鑰，以致於無法順利完成憑證要求，**現象是安裝完成後會看到憑證，但是按下 F5 重新整理後，該憑證就會立即消失**。

解決方式:請確認現在安裝的這台伺服器，是否為當初建立憑證要求的伺服器，若安裝的伺服器是當初建立憑證要求的伺服器，則表示金鑰已遺失，**請參考以下作法，重新產製 CSR 並交付給 TWCA 客服，等待再一次核發憑證。**

因金鑰遺失, 無法安裝憑證者，步驟如下：
＊憑證重發需 3-5 工作日，重發新憑證之同時，也會同步廢止前一張憑證＊（重要提醒） 1. 請重製新 CSR（含:新金鑰）並上傳至 www.twca.com.tw/Portal/service/ssl_1_3.html，完成後，請 copy 畫面，貼在信件內文。 2. 告知要重發的 CN 名稱及公司統編，並留下您的聯絡資料。 3. 信件主旨，填：需重發憑證（已上傳 CSR 檔)。 4. Email 至：sslcc@twca.com.tw。 5. TWCA 重發後，會寄到原本申請單所填之技術人員信箱。(請向原技術同仁取得憑證檔)。 6. 新憑證安裝好後，建議依手冊 5.9 章節進行**備份**作業（金鑰與憑證)。

注意:**建立憑證要求之後，安裝前盡量避免對伺服器異動，減少金鑰再次遺失的可能**。

6.5 安裝憑證需要.crt 檔(或 PEM 格式檔)，可是 TWCA 核發的 SSL 憑證都是.cer 檔，該如何進行格式轉換？

TWCA 提供的.cer 檔預設編碼和.crt 的編碼格式一樣，都是 PEM(Base64)格式，.cer 可直接安裝或將副檔名改成.crt 或.pem 使用即可。

6.6 IIS 備份(匯出)的是.pfx 檔案，可是設備安裝 SSL 需要的是 PKCS#12 或.p12 檔案，格式該如何轉換？

.pfx 和.p12 是相同的。兩者都是 PKCS#12 文件，IIS 匯出的.pfx 檔案可直接使用在您的設備，不須轉換。

6.7 憑證格式轉換手冊:

IIS 及 Apache SSL 憑證轉換說明手冊

Apache 與 JKS 移轉手冊

7.附件

無。