

中華電信 HiPKI 憑證管理中心 (OVTLSCA)

Windows Lync Server SSL 憑證請求檔製作與憑證安裝手冊

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。

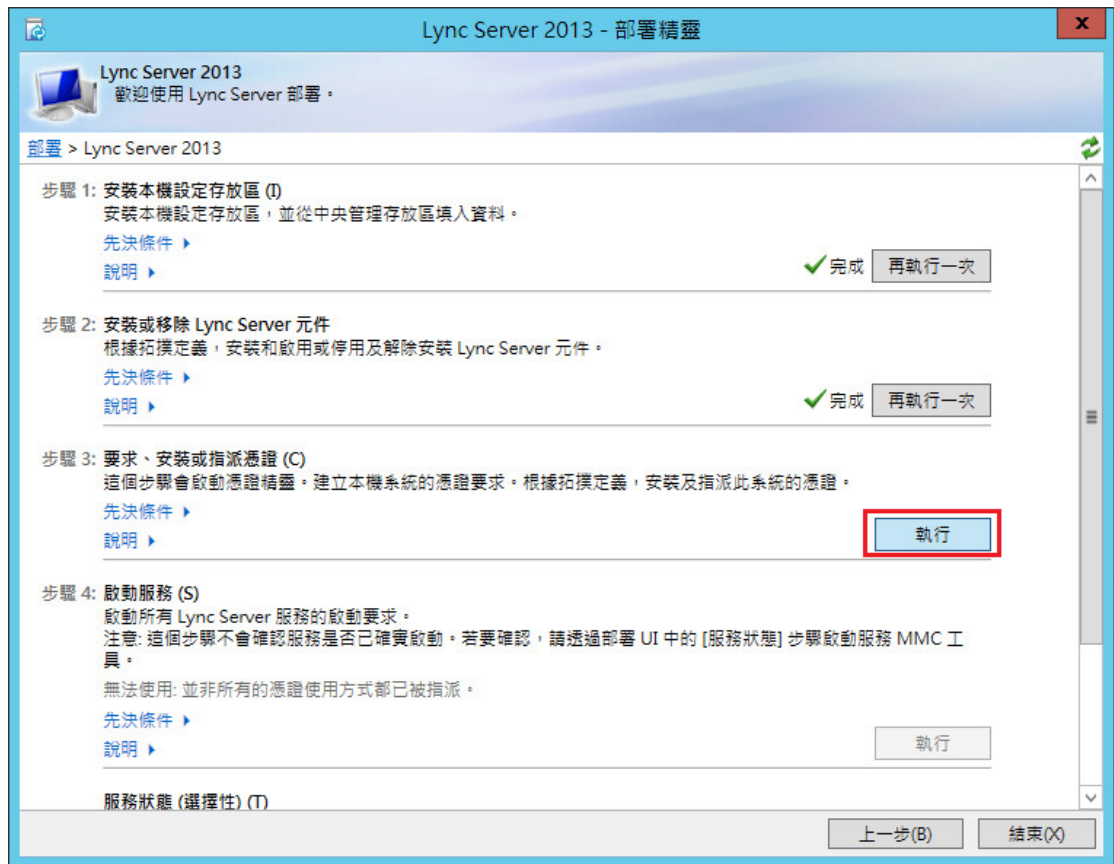
本說明書的申請程序，已經在 Windows Server 2012 + Lync Server 2013 測試過，您所使用的版本或環境可能與本版本有所差異，若是如此則請參考您的 Lync 相關使用手冊，適度調整申請步驟。

目錄

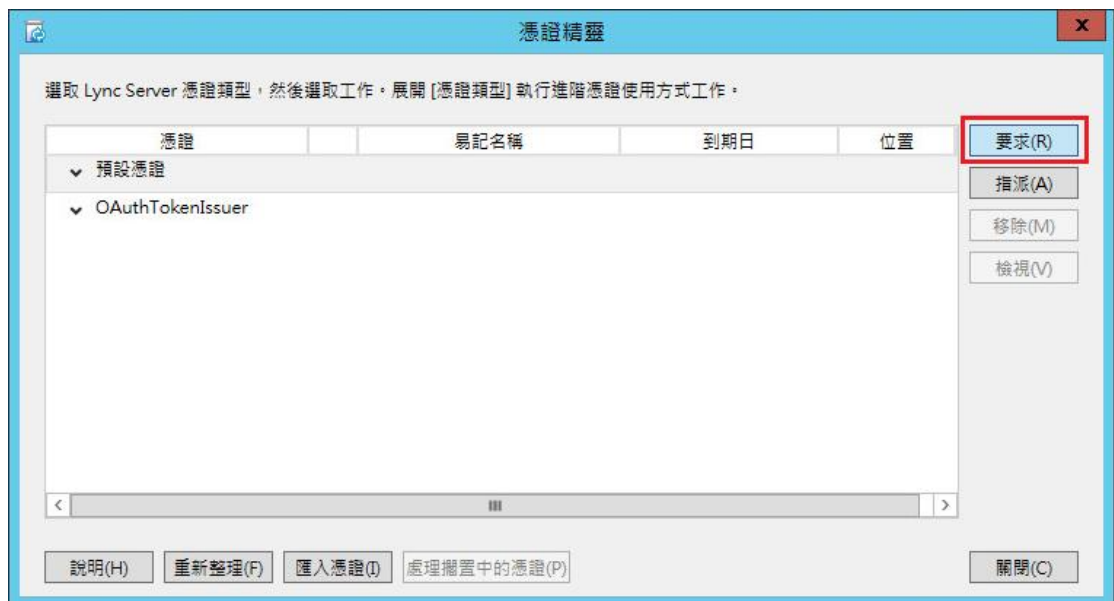
Windows Lync Server SSL 憑證請求檔製作手冊	2
Windows Lync Server SSL 憑證安裝操作手冊	11

Windows Lync Server SSL 憑證請求檔製作手冊

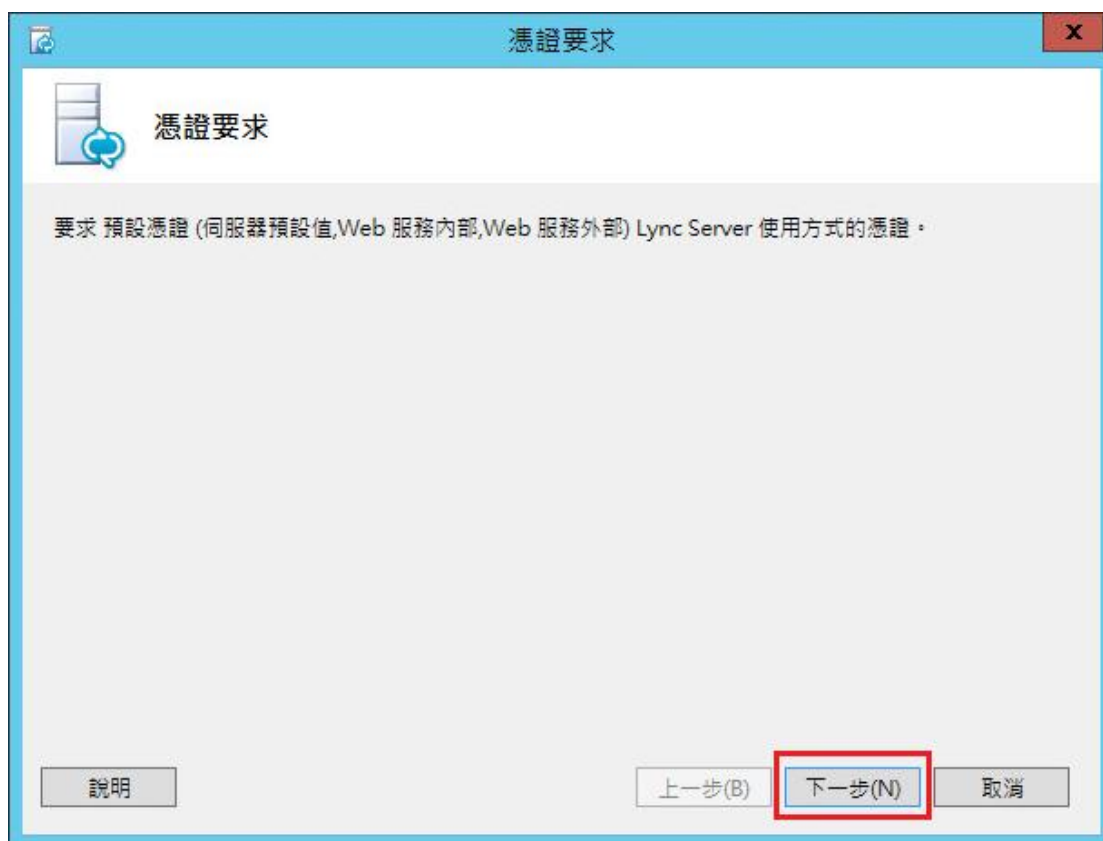
- 一、 開啟「Lync Server 部署精靈」至下圖位置，並點選「執行」。



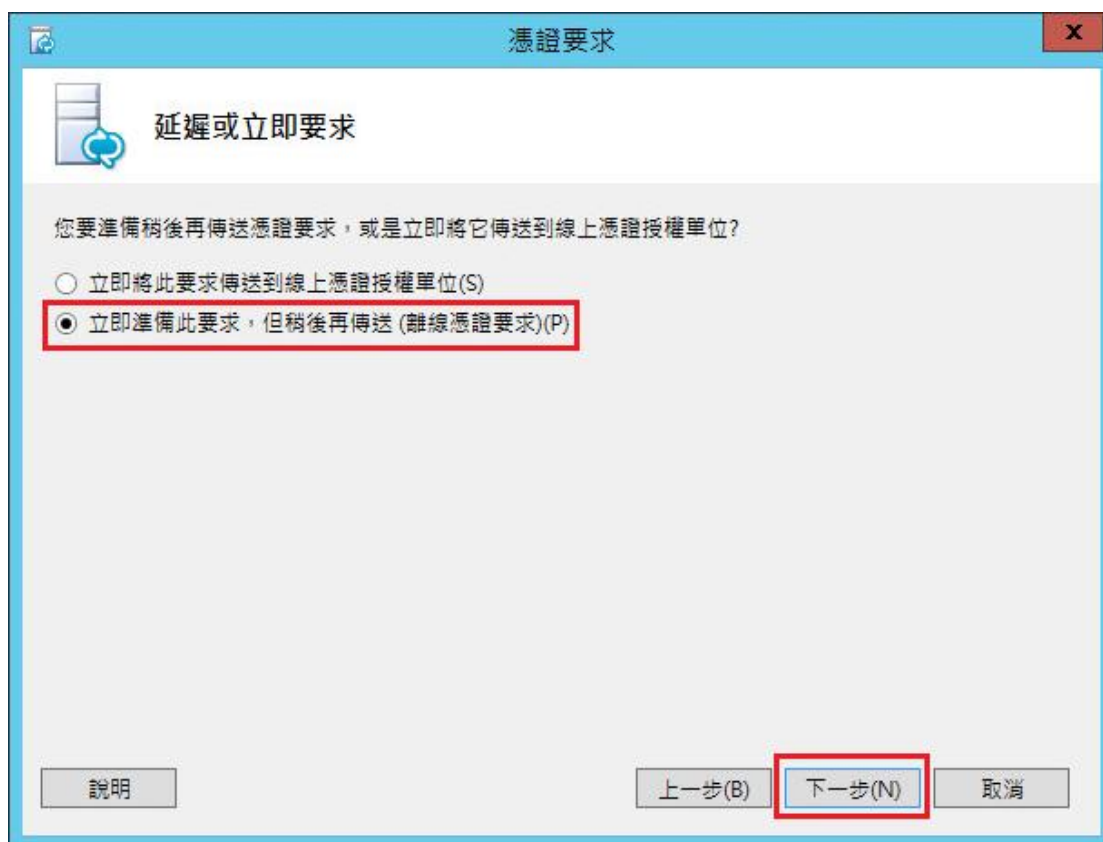
- 二、 點選「要求」。



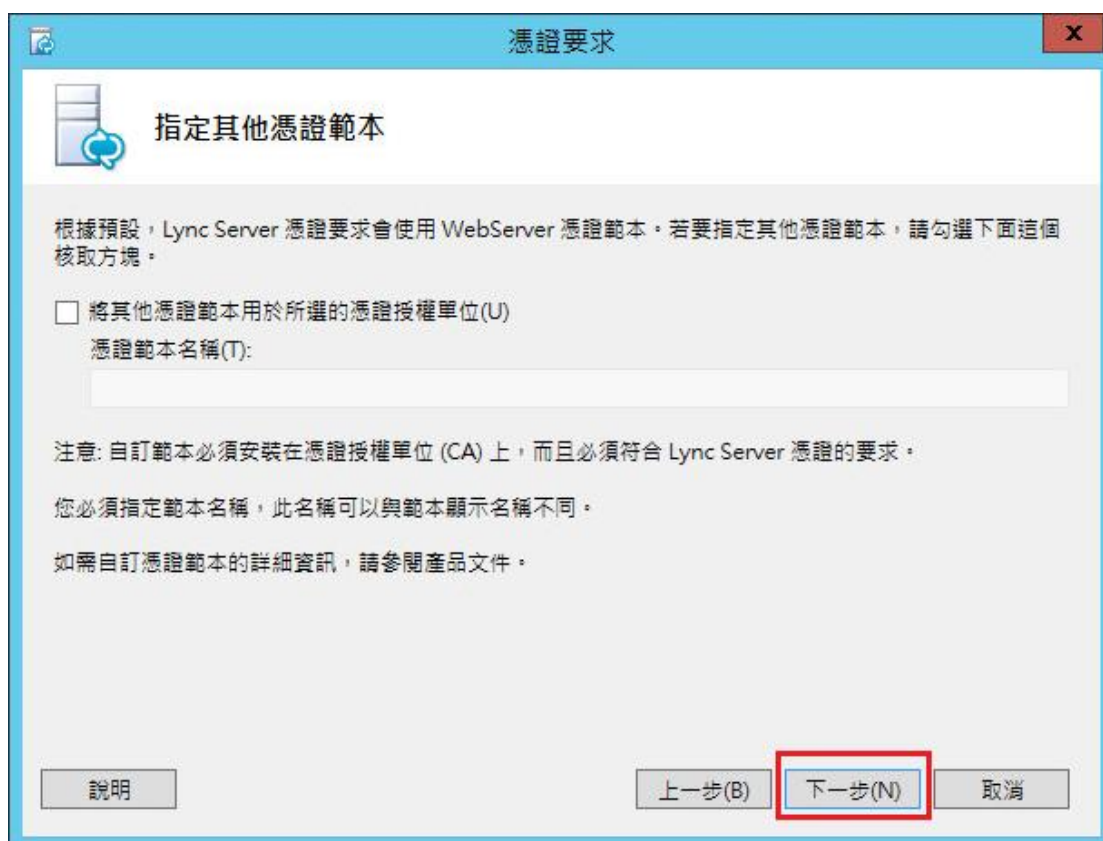
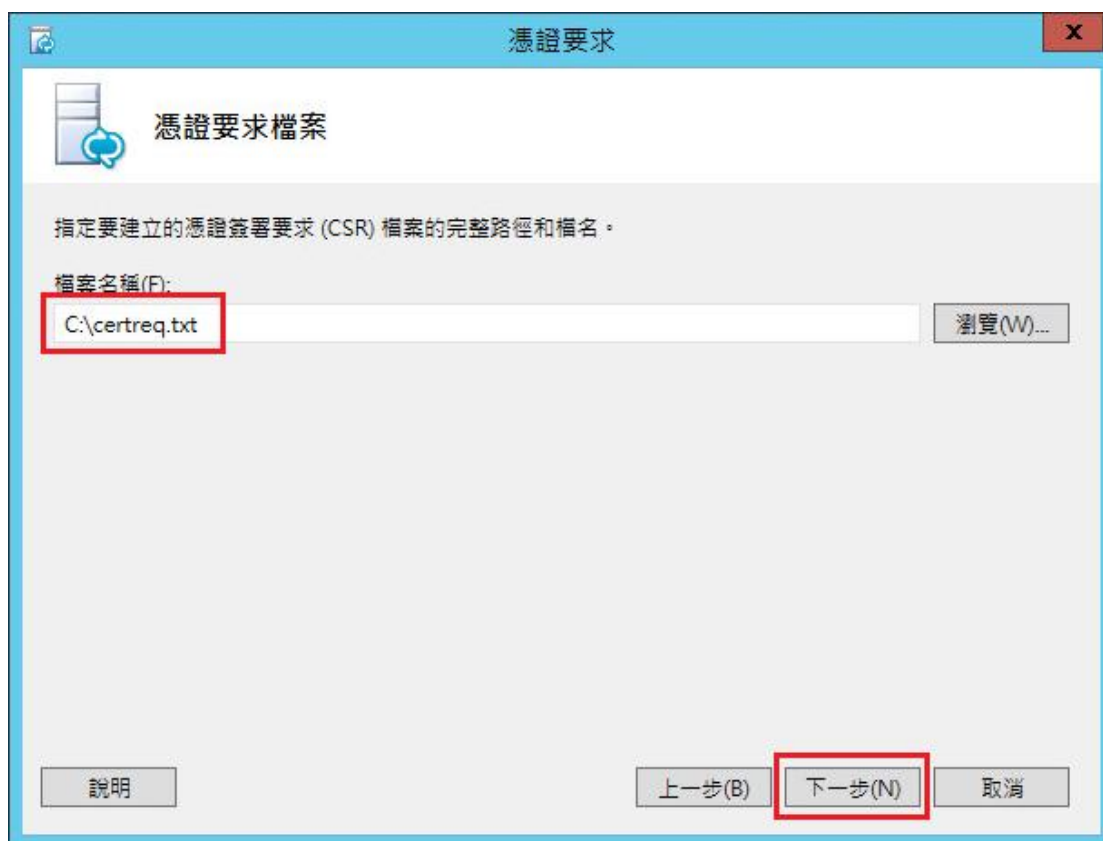
- 三、 依照以下步驟進行操作



四、 選擇「立即準備此要求，但稍後再傳送」



選擇存檔位置



五、 金鑰長度選擇「2048」，並勾選「將憑證的私密金鑰標記為可匯出」，以便未來備份或是金鑰轉移。請注意依照國際密碼學趨勢，請使用 RSA 2048

位元(含)以上金鑰長度。

憑證要求

名稱和安全性設定

請輸入新憑證的名稱。這個名稱應以容易參考和記憶為原則。

注意: 易記名稱不應與主體名稱混淆, 後者是自動根據此電腦上的憑證使用方式決定的。

易記名稱(F):
LYNC.test.tw

位元長度(L):
2048

將憑證的私密金鑰標記為可匯出(M)

說明 上一步(B) 下一步(N) 取消

六、 填入「組織資訊」與「地理資訊」。

憑證要求

組織資訊

請輸入貴組織的名稱和您的組織單位。這通常是組織的法定名稱和您的所屬部門名稱。

如需詳細資訊, 請參閱憑證授權單位的網站。

組織(O):
中華電信股份有限公司數據分公司

組織單位(U):
資通安全處

說明 上一步(B) 下一步(N) 取消

憑證要求

地理資訊

國家/地區(C):
台灣

州/省(S):
none

城市/位置(L):
台北市

[州/省] 和 [城市/位置] 必須是完整的，而且正式名稱不可包含縮寫。

說明 上一步(B) 下一步(N) 取消

憑證要求

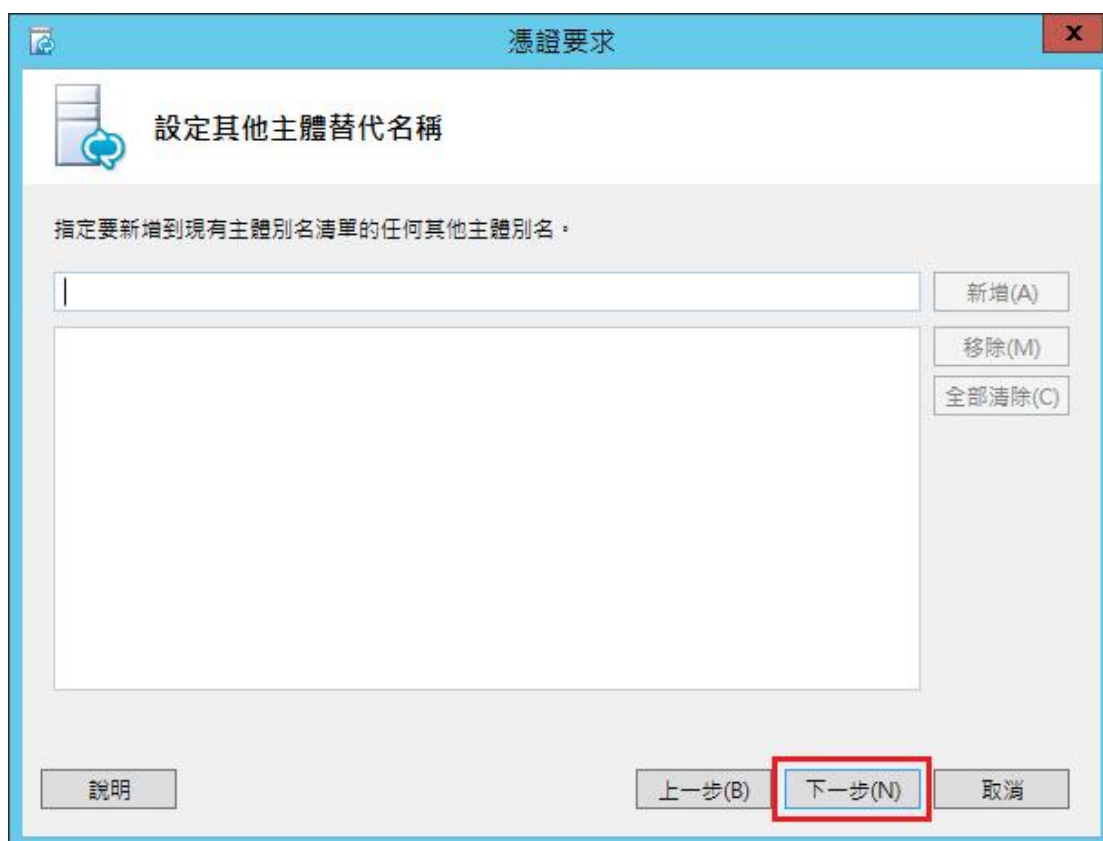
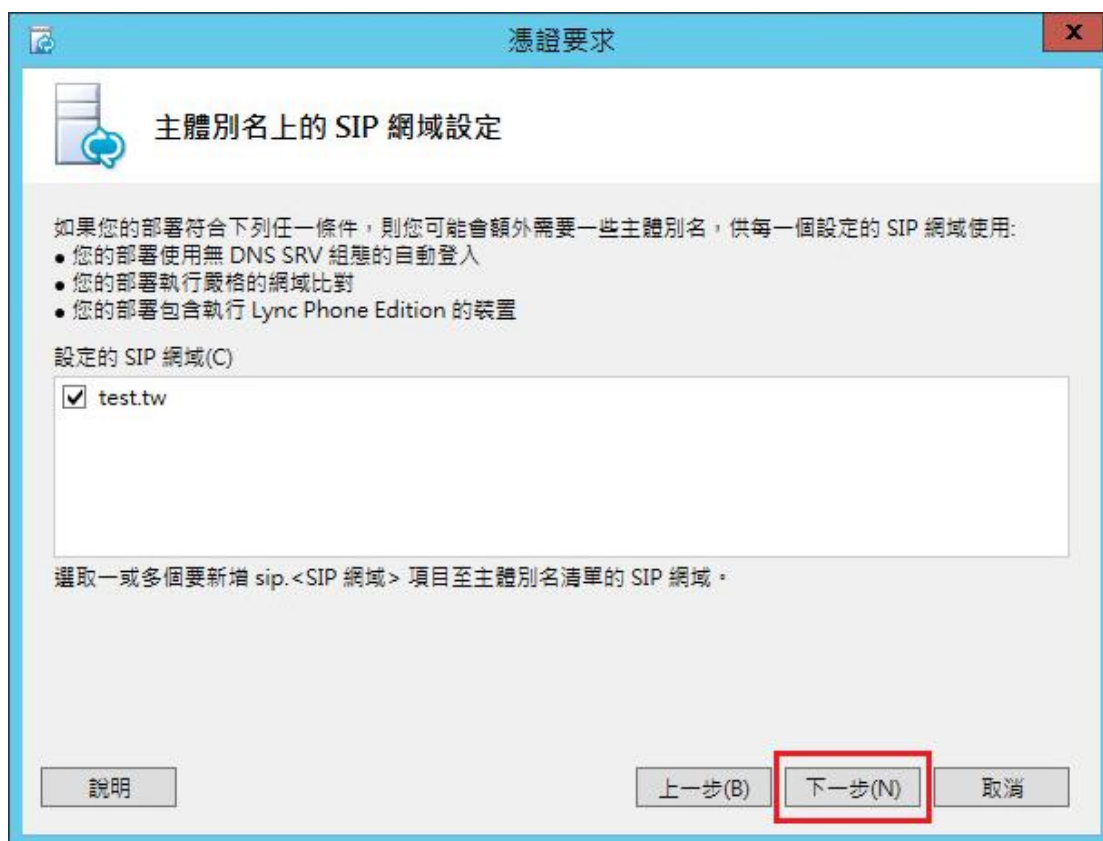
主體名稱 / 主體替代名稱

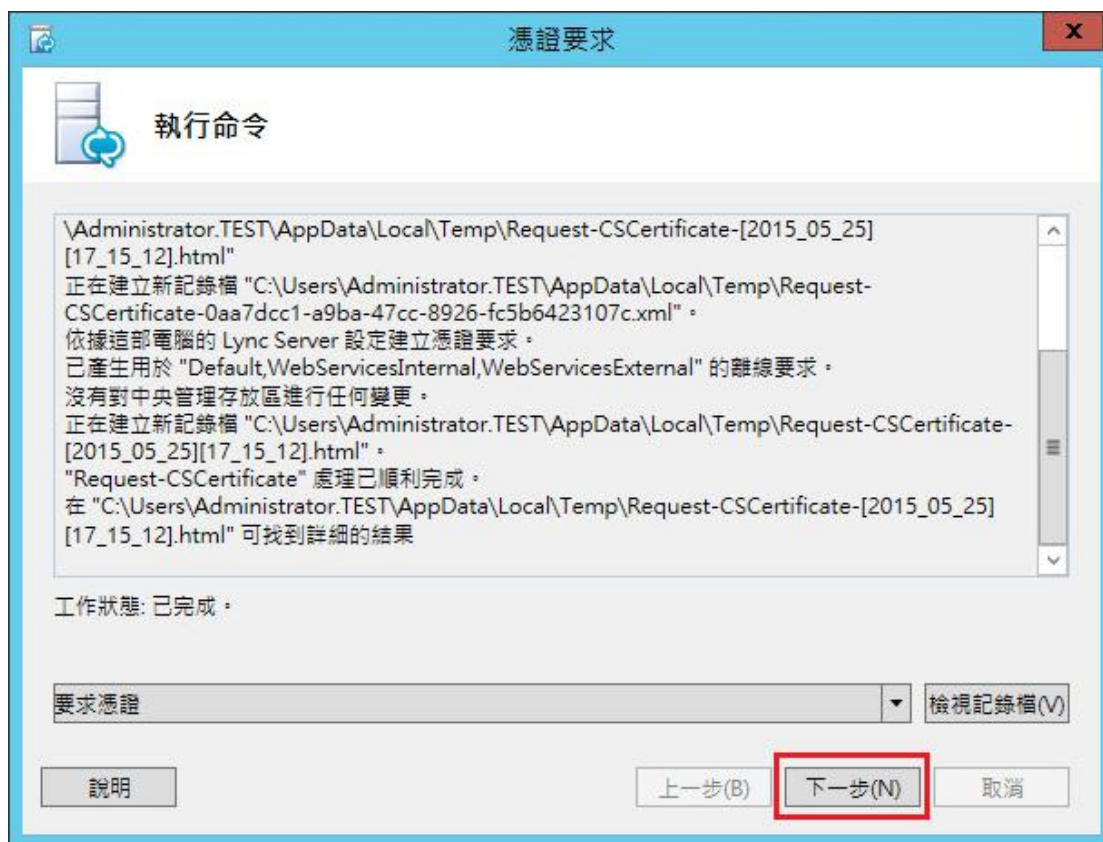
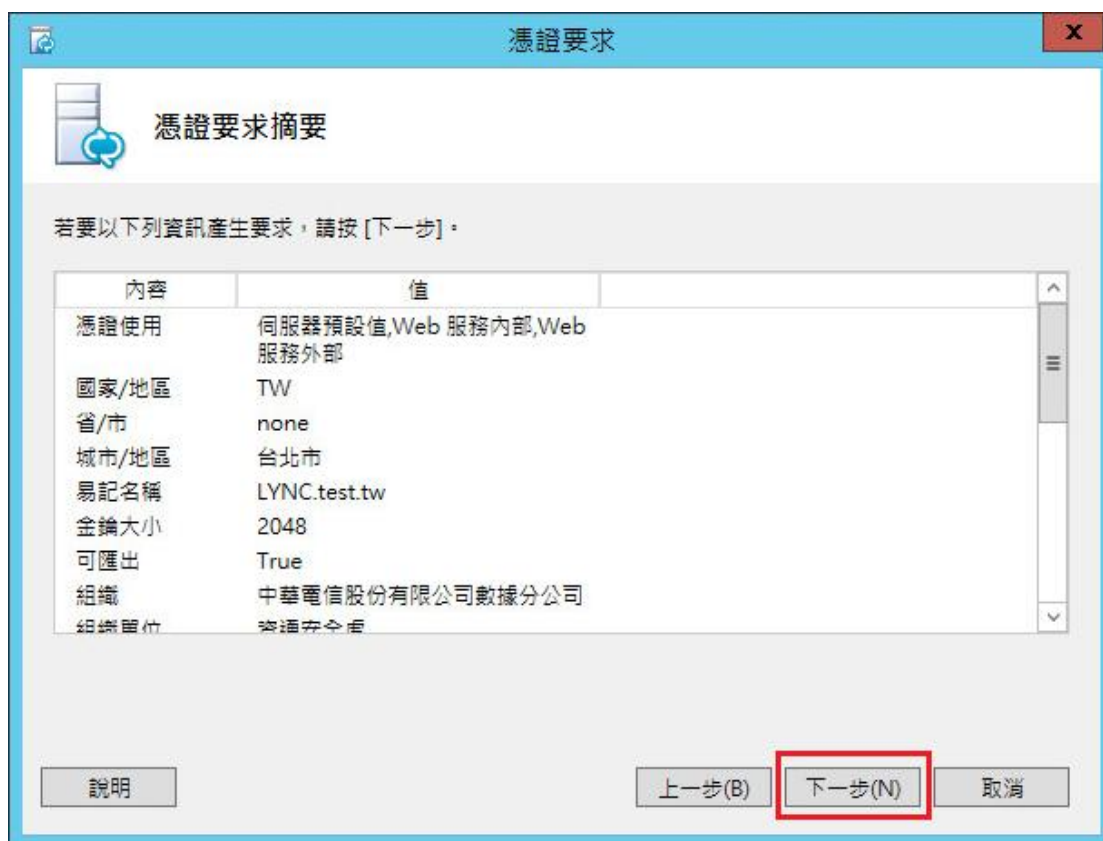
主體名稱和主體別名會自動填入以下內容。

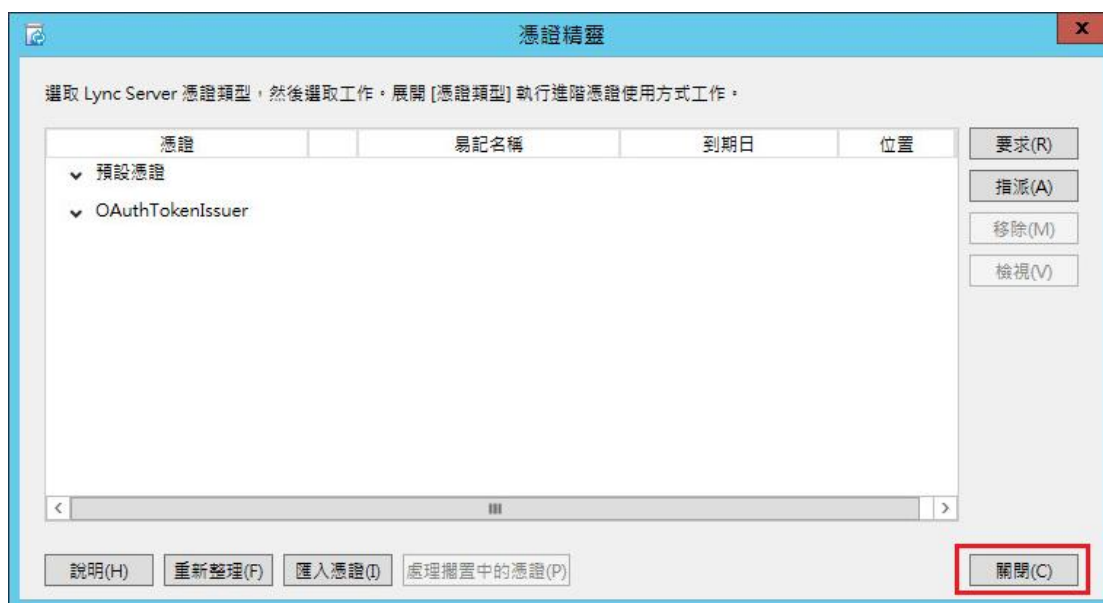
主體名稱:
LYNC.test.tw

主體別名:
LYNC.test.tw
dialin.test.tw
meet.test.tw
admin.test.tw
LyncdiscoverInternal.test.tw

說明 上一步(B) 下一步(N) 取消







七、 此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信公開金鑰基礎建設服務網站 (<https://chtca.hinet.net/>) 依照網頁說明申請 SSL 憑證。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。

補充說明 1: 中華電信公開金鑰基礎建設服務之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於上圖所輸入之資訊，而是以於申請

網頁上所填入的組織資訊與完全吻合網域名稱(Fully Qualified Domain Name, FQDN)為準，並記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)之一般名稱(Common Name)或憑證主體別名(Subject Alternative Name)等欄位]。

補充說明 2:若您是申請多網域 SSL 憑證或萬用網域 SSL 憑證，僅需要產生 1 個憑證請求檔(產生憑證請求檔之過程就是幫您的伺服器產製 1 對金鑰對，私密金鑰與密碼由伺服器管理者保管，公開金鑰會包含在憑證請求檔內，憑證管理中心審驗您的身分與網域名稱擁有權或控制權後，所簽發的憑證會記載申請者的組織資訊、完全吻合網域名稱與公開金鑰在 SSL 憑證內。後續先安裝 SSL 憑證串鏈於產生憑證請求檔之站台，再將私密金鑰與憑證備份後匯入其他站台，不同廠牌伺服器之匯出與匯入可參考手冊或寫電子郵件給本管理中心技術客服信箱 caservice@cht.com.tw 詢問，不需要每個網站站台都分別產生憑證請求檔。

Windows Lync Server SSL 憑證安裝操作手冊

一、 下載憑證串鏈，包含 4 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)eCA to HRCA 交互憑證(eCA 簽發給 HRCA 之交互憑證)、(3)HiPKI OV TLS CA 中繼憑證(中華電信 HiPKI OV TLS 憑證管理中心自身憑證)與(4)OV TLS CA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 4 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、eCA to HRCA 交互憑證(檔名為 eCA1-to-HRCA1.crt)、OV TL SCA 中繼憑證(檔名為 OVTLSCA1_b64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。

若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 4 個檔案。

2. 從網站查詢與下載：

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：

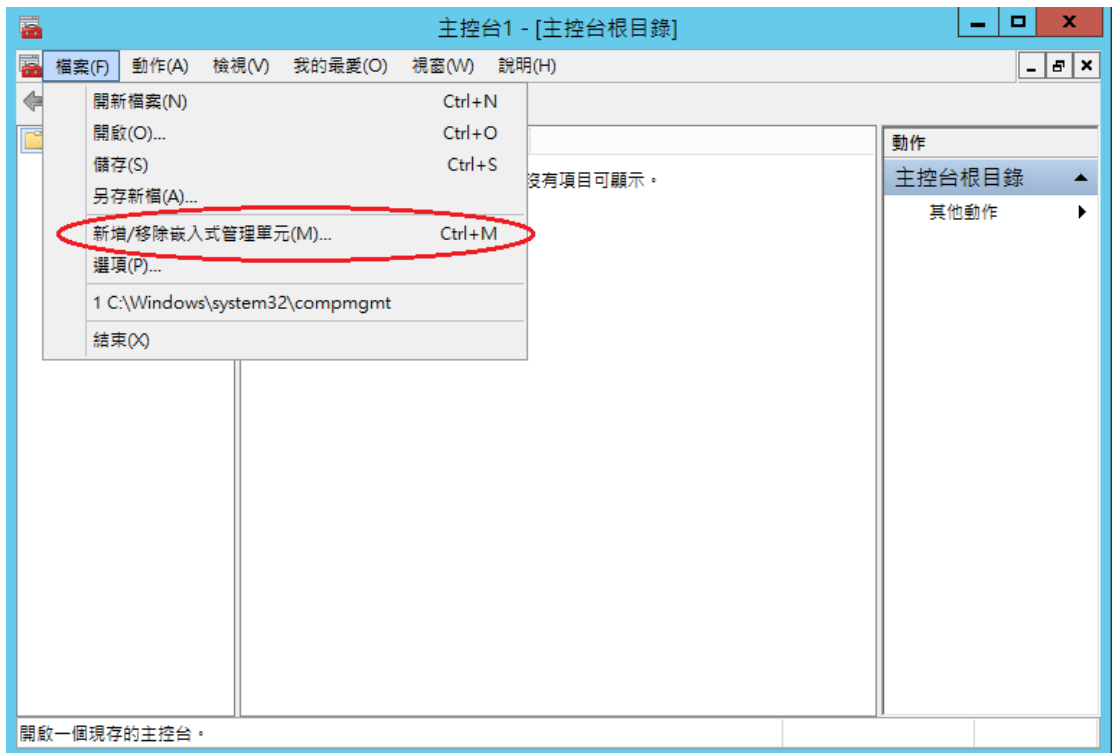
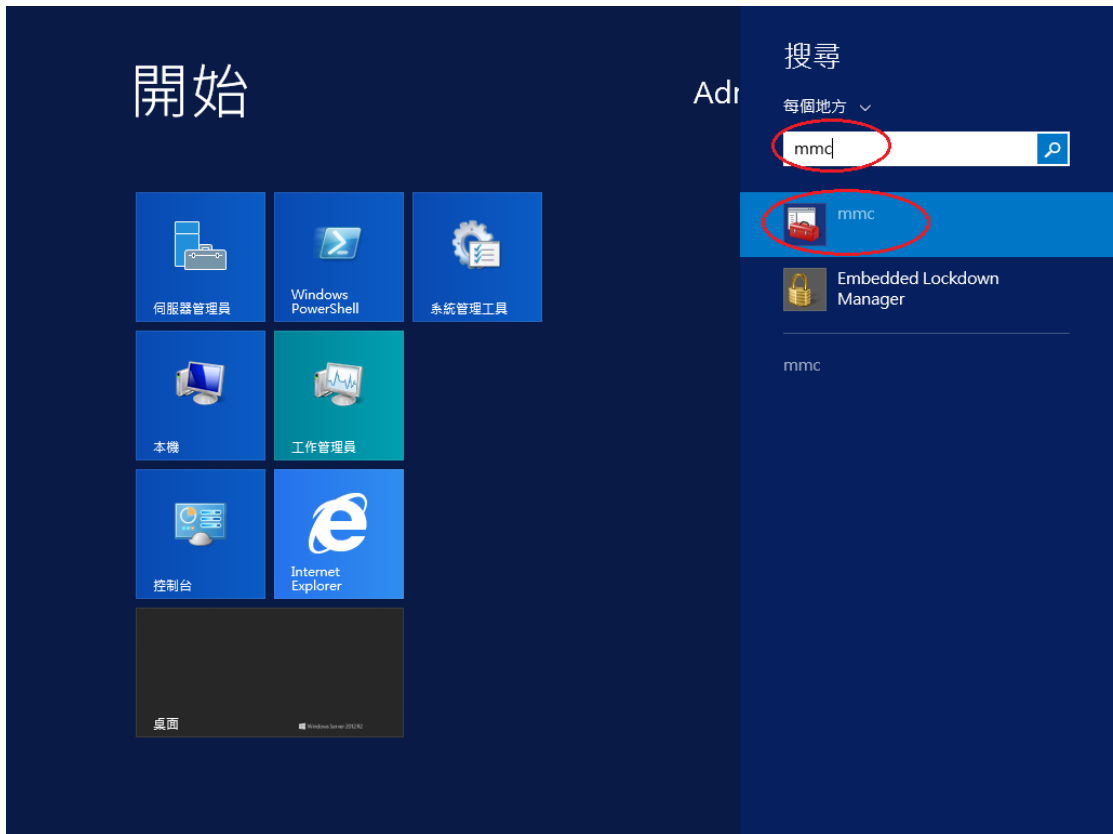
https://eca.hinet.net/repository-h/download/OVTLSCA1_b64.crt

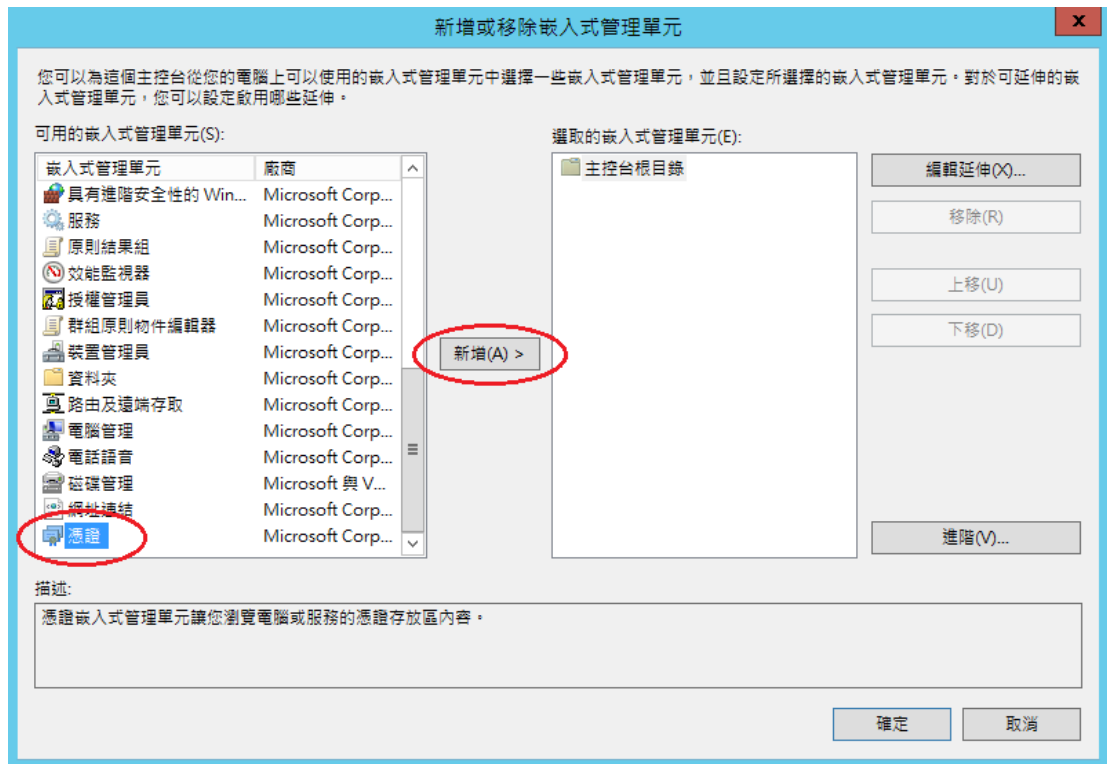
SSL 憑證下載：您若是本公司之客戶，請至 CHTCA 網站點選「TLS 憑證效期查詢及下載」，進行 SSL 憑證下載。

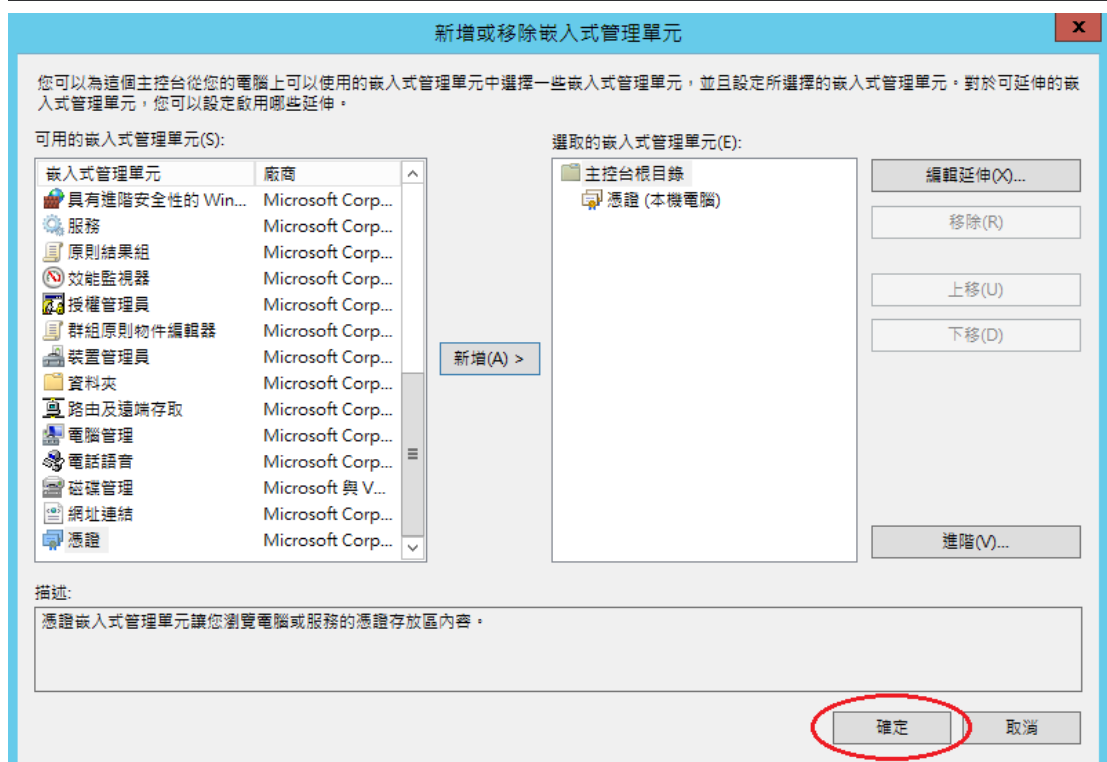
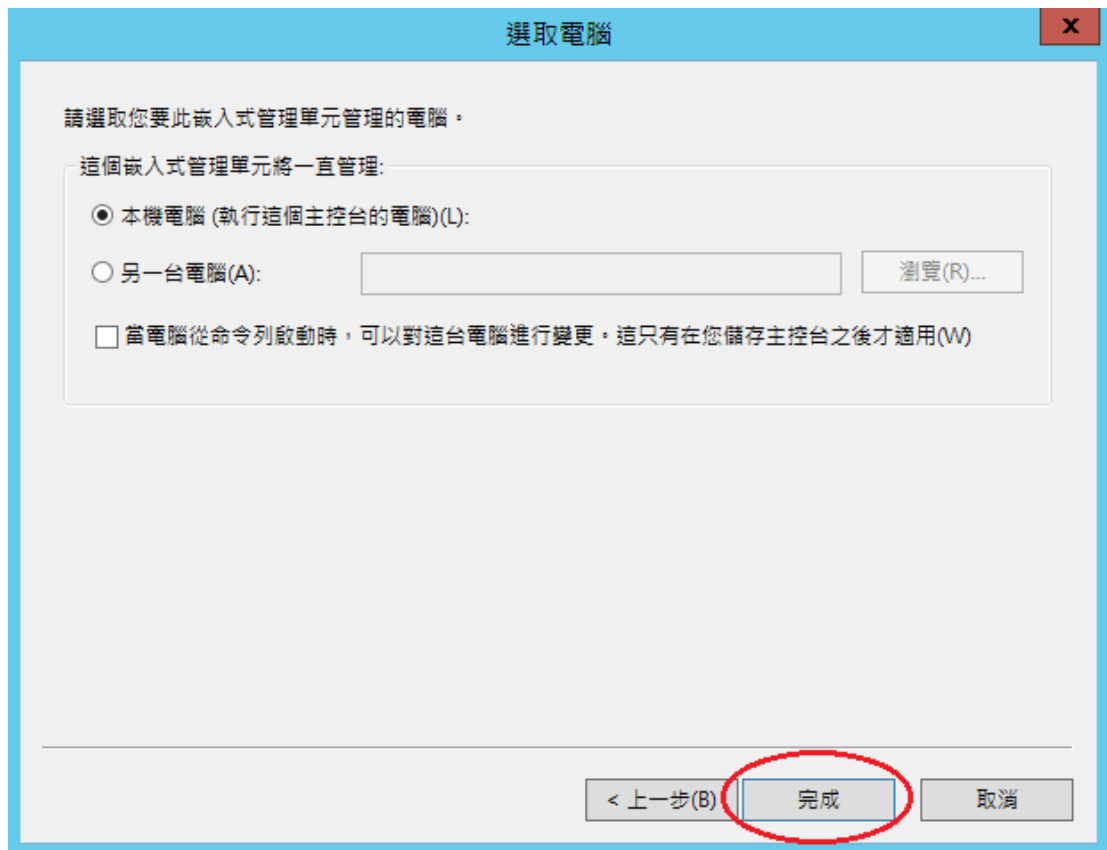
若您是中華電信之員工，負責管理單位之伺服器，請至 <https://chtra.cht.com.tw/> 點選「憑證與卡片作業」，再點選「憑證查詢」，下載 SSL 憑證。

二、 開啟 mmc 安裝根憑證及中繼憑證。

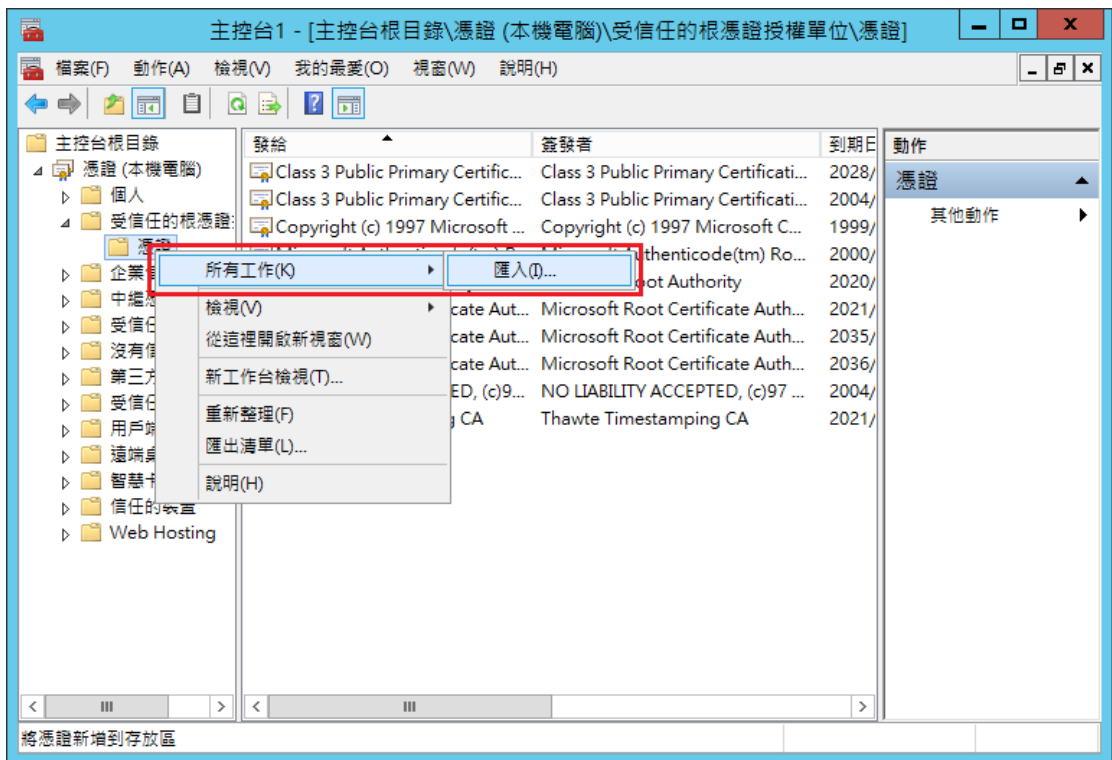
點選「開始」→輸入「mmc」→點選「mmc」，並依下圖操作。

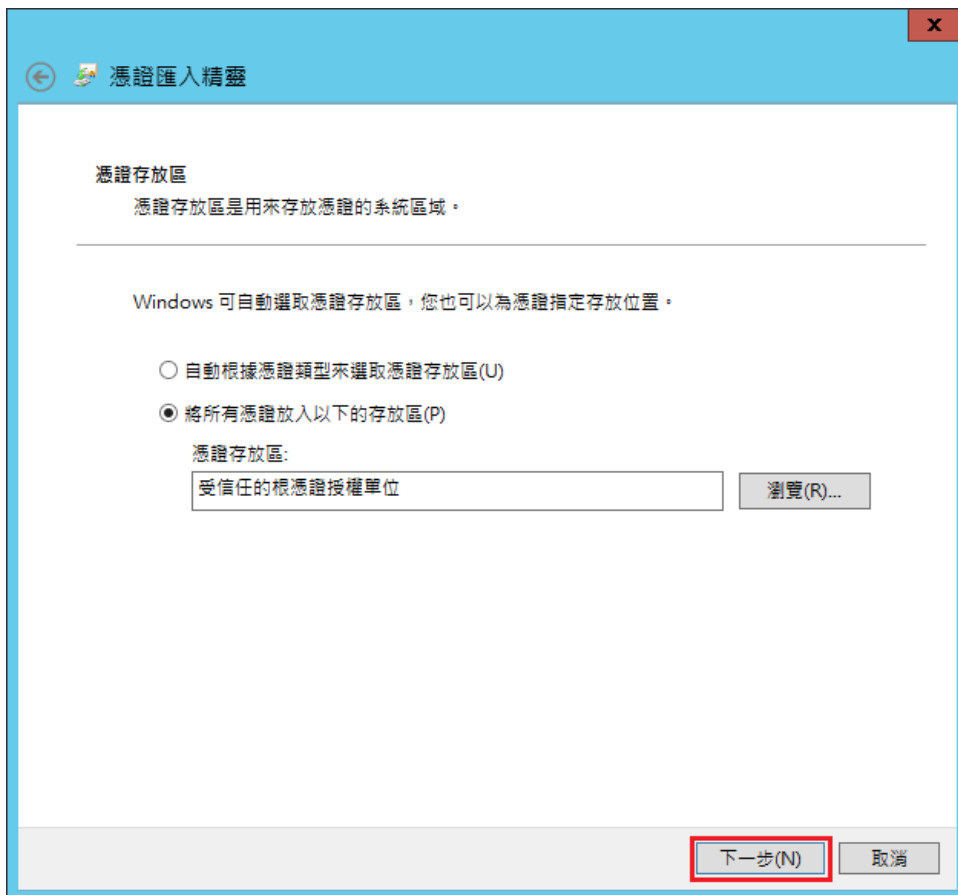


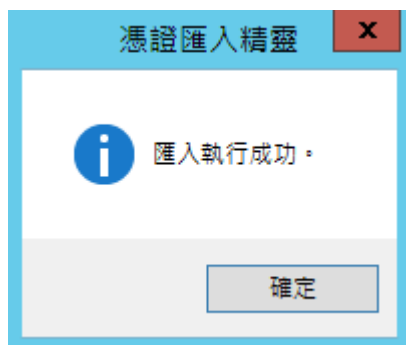


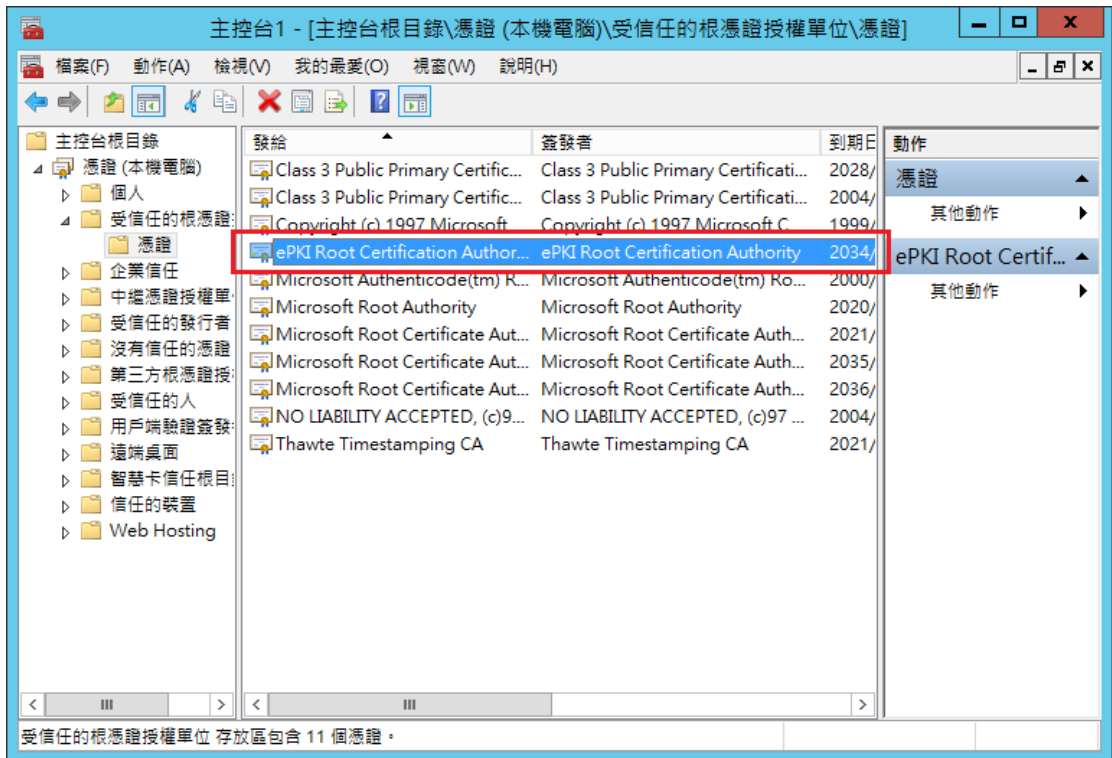


三、於「受信任的根憑證授權單位」匯入根憑證。

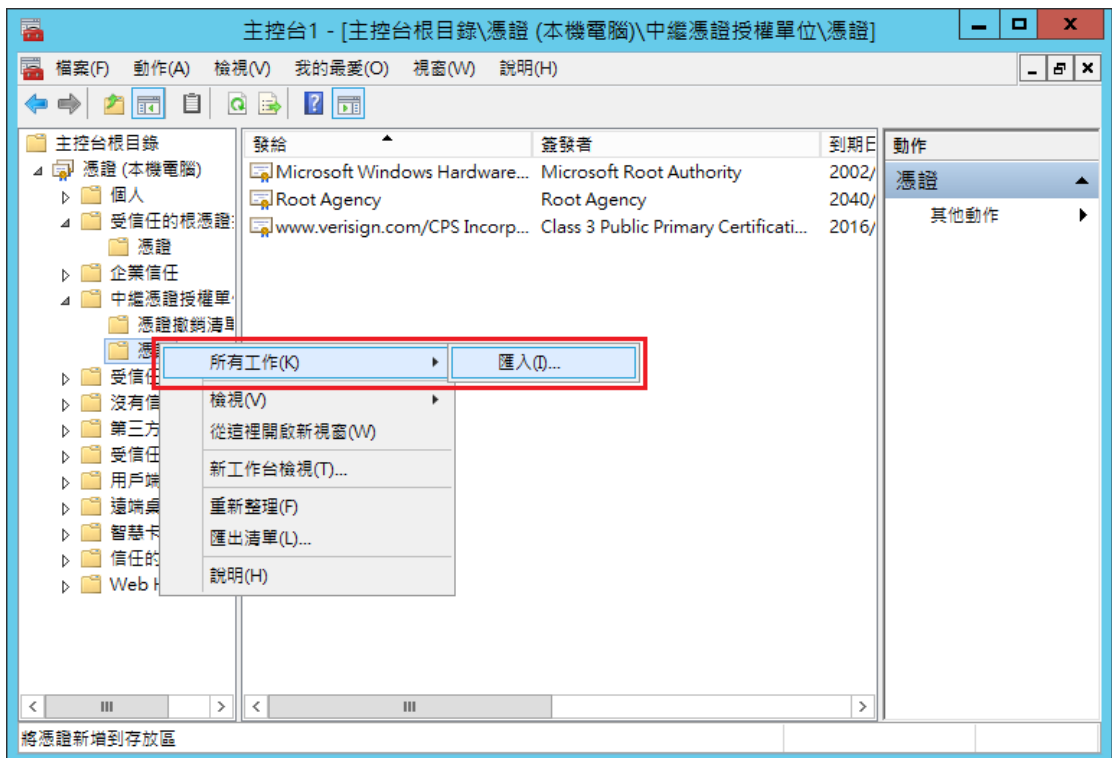


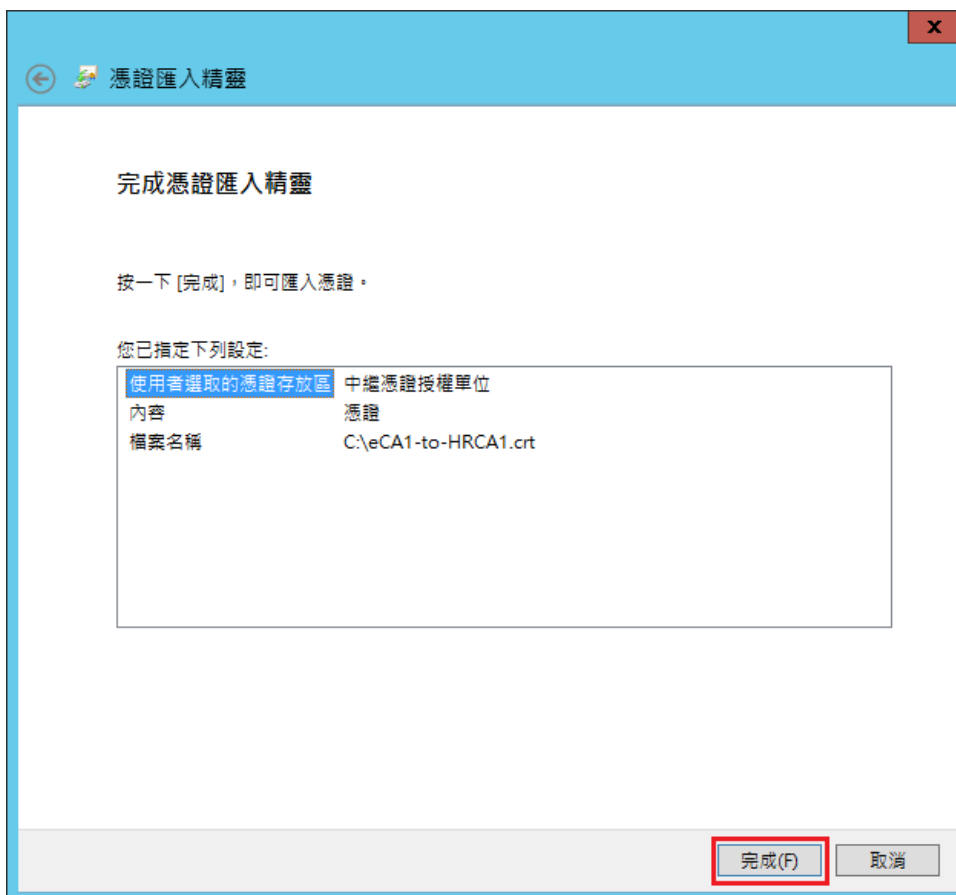
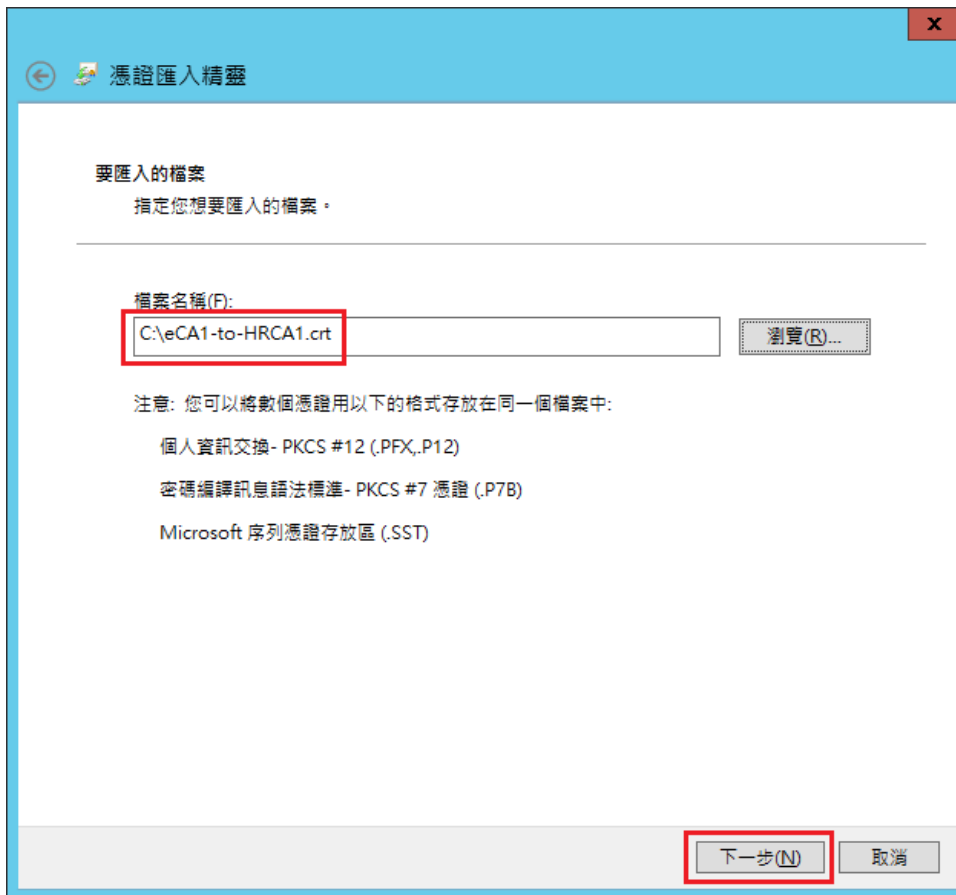


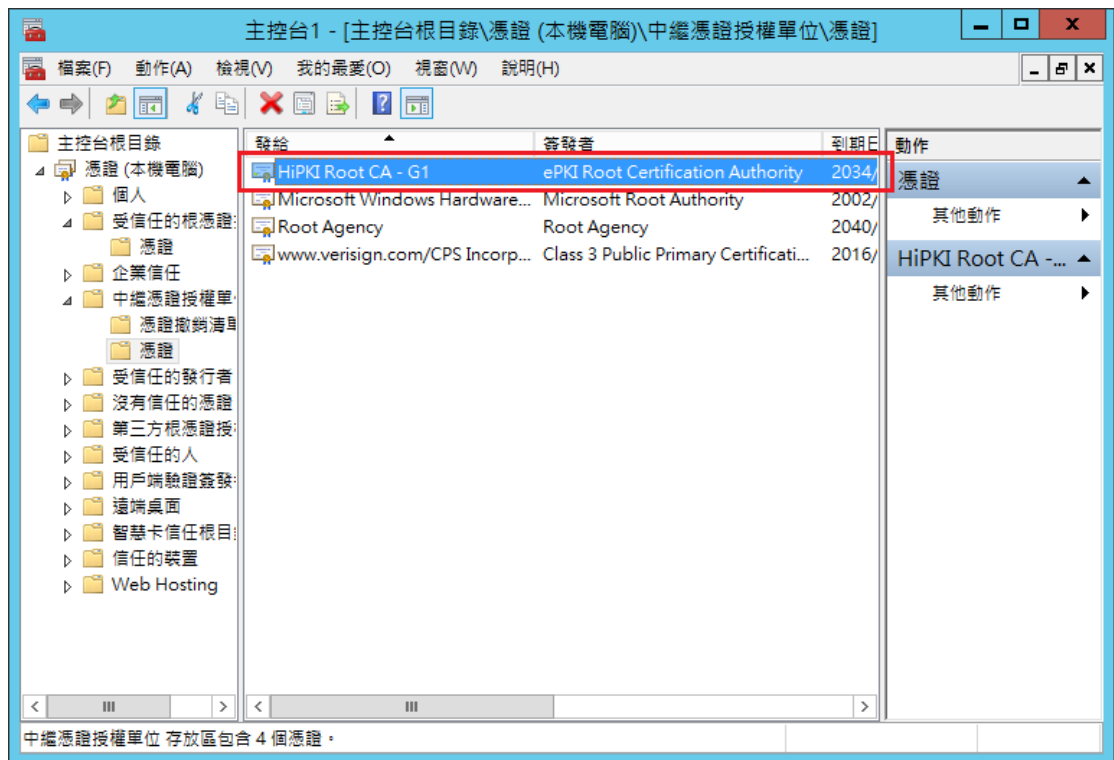




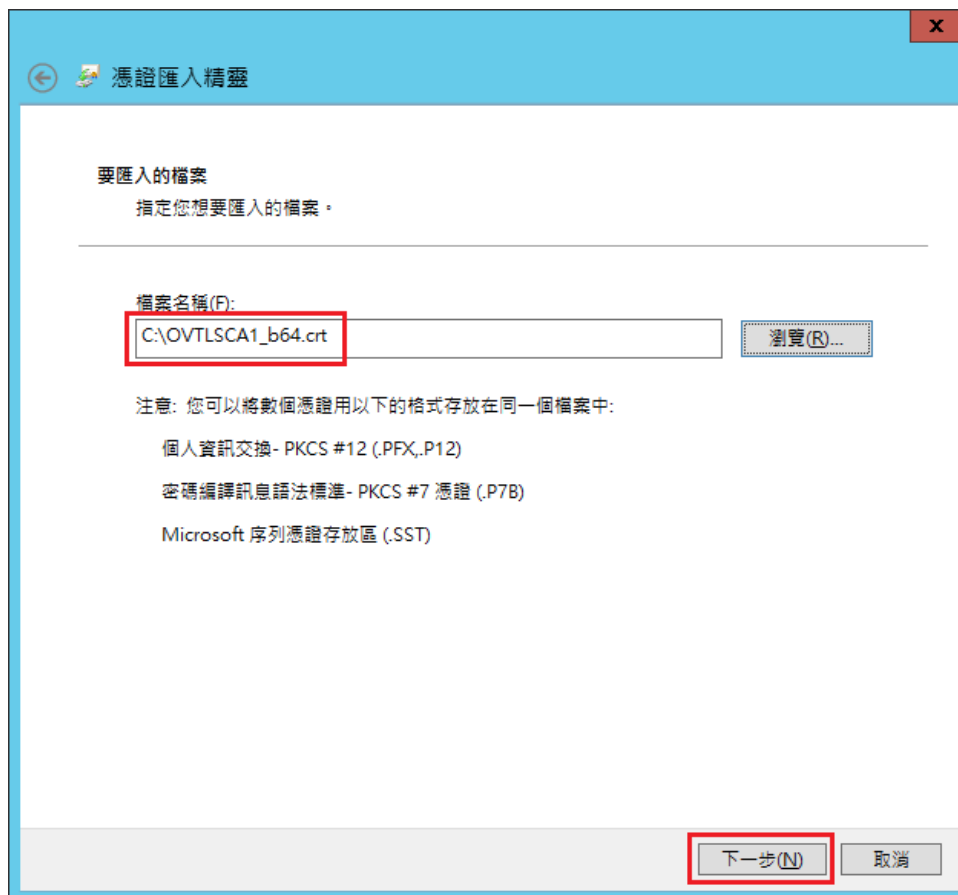
四、於「中繼憑證授權單位」匯入交互憑證。依照上述匯入根憑證的步驟，匯入交互憑證。

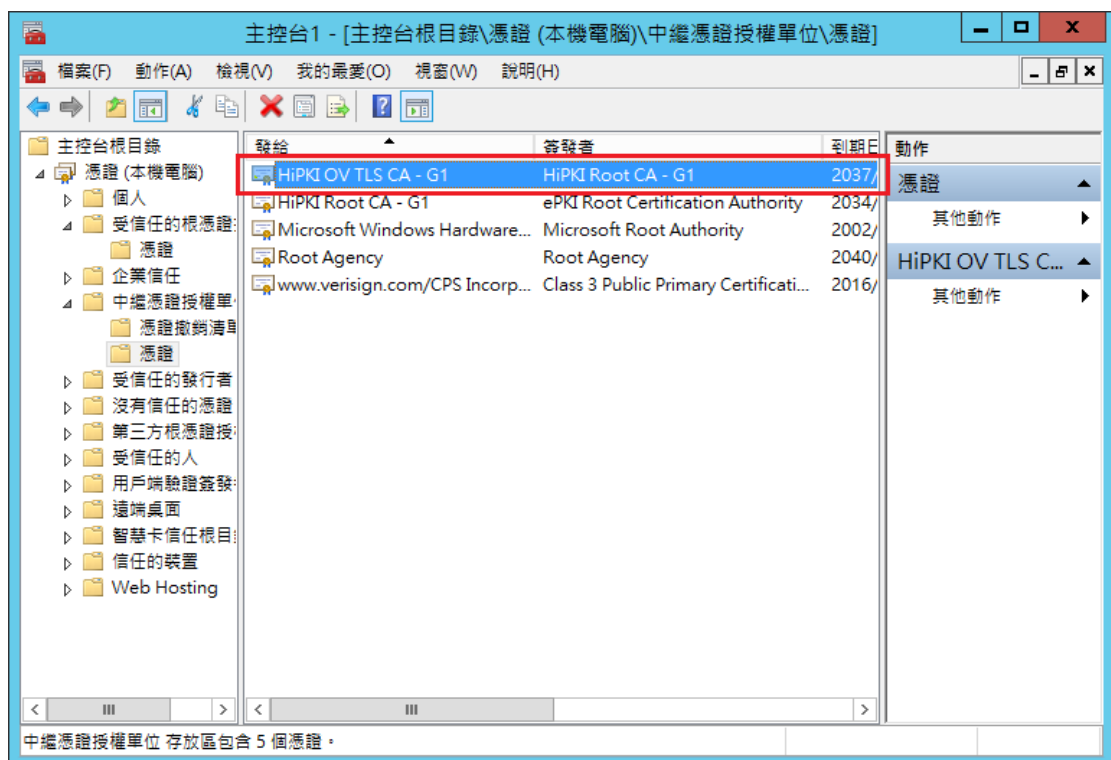
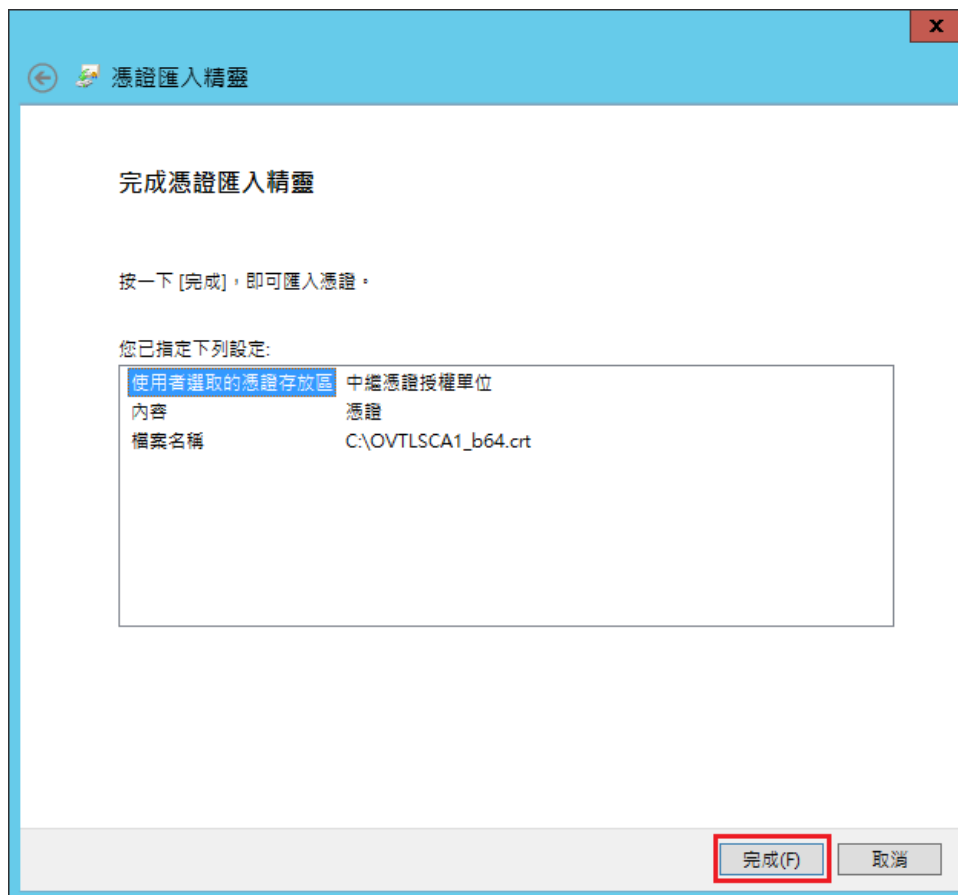




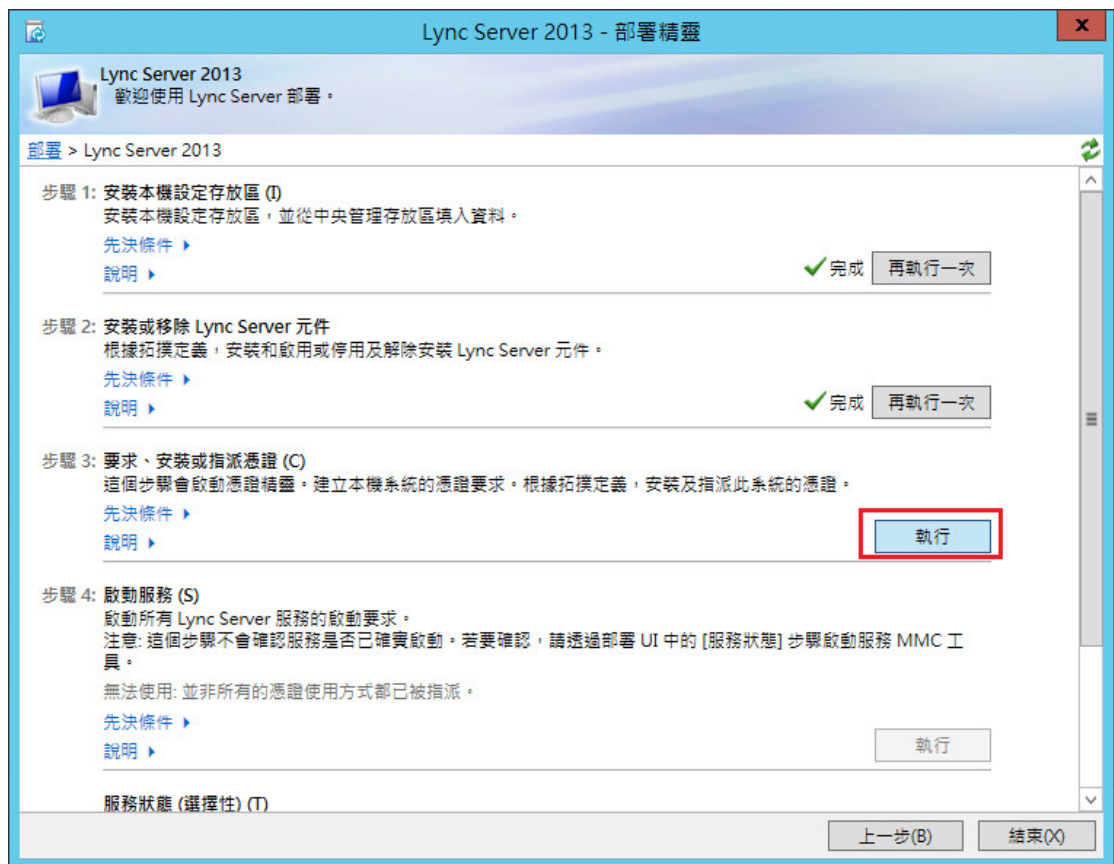


- 五、 於「中繼憑證授權單位」匯入中繼憑證。依照上述匯入根憑證的步驟，匯入中繼憑證。

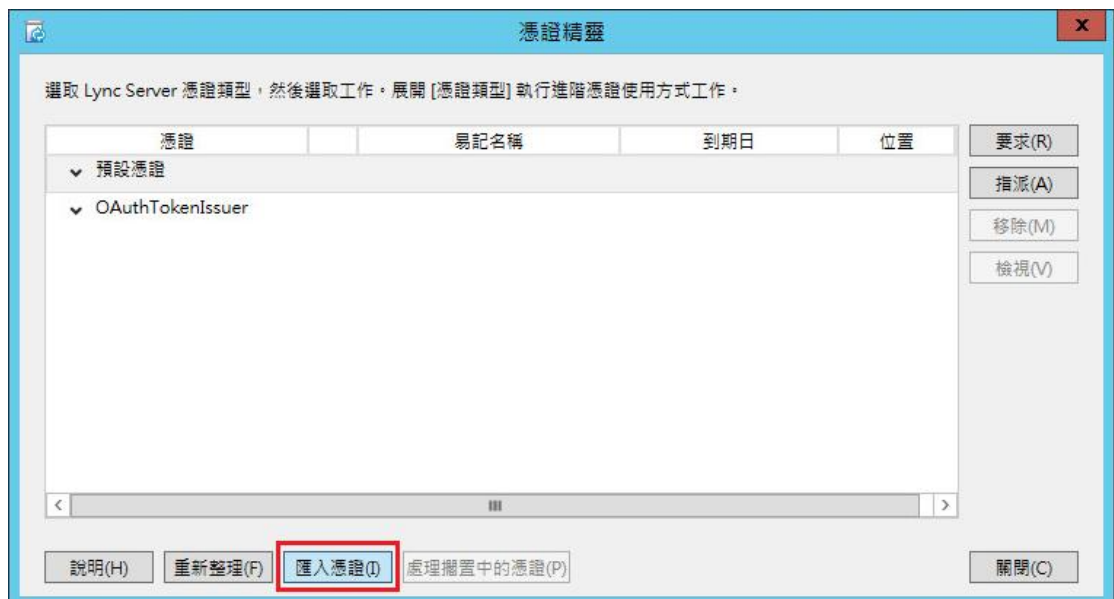


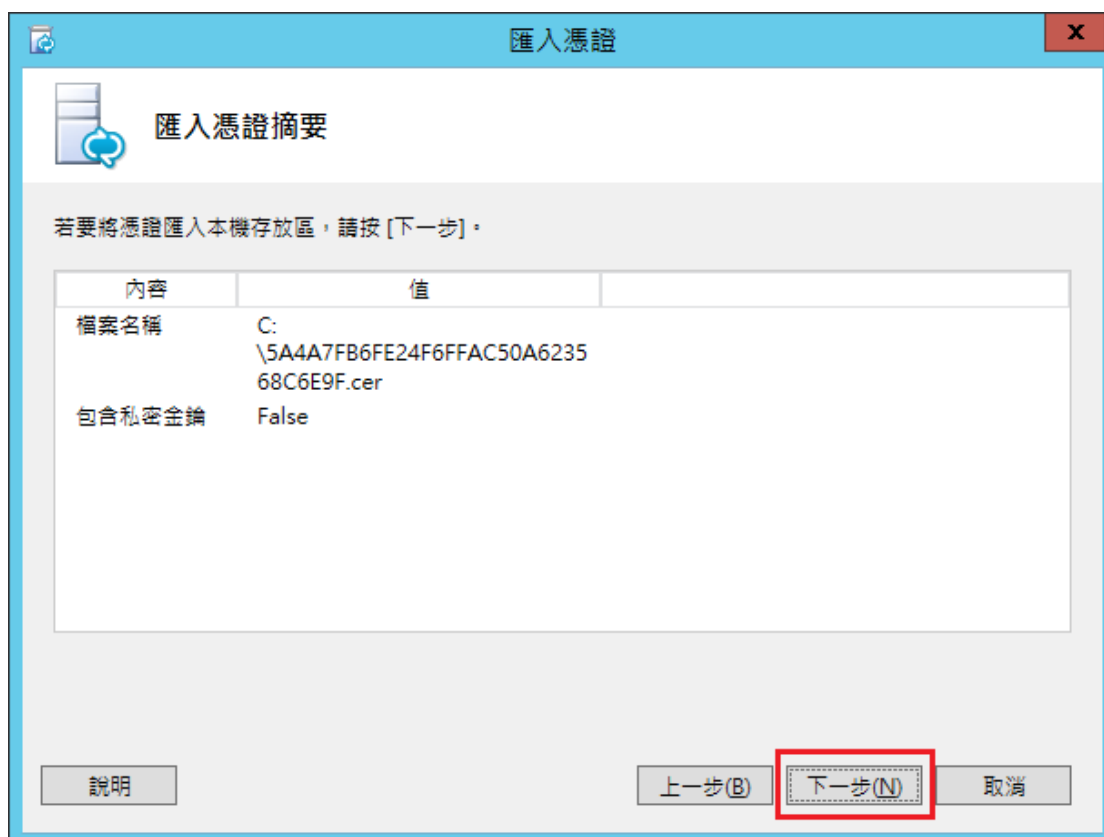
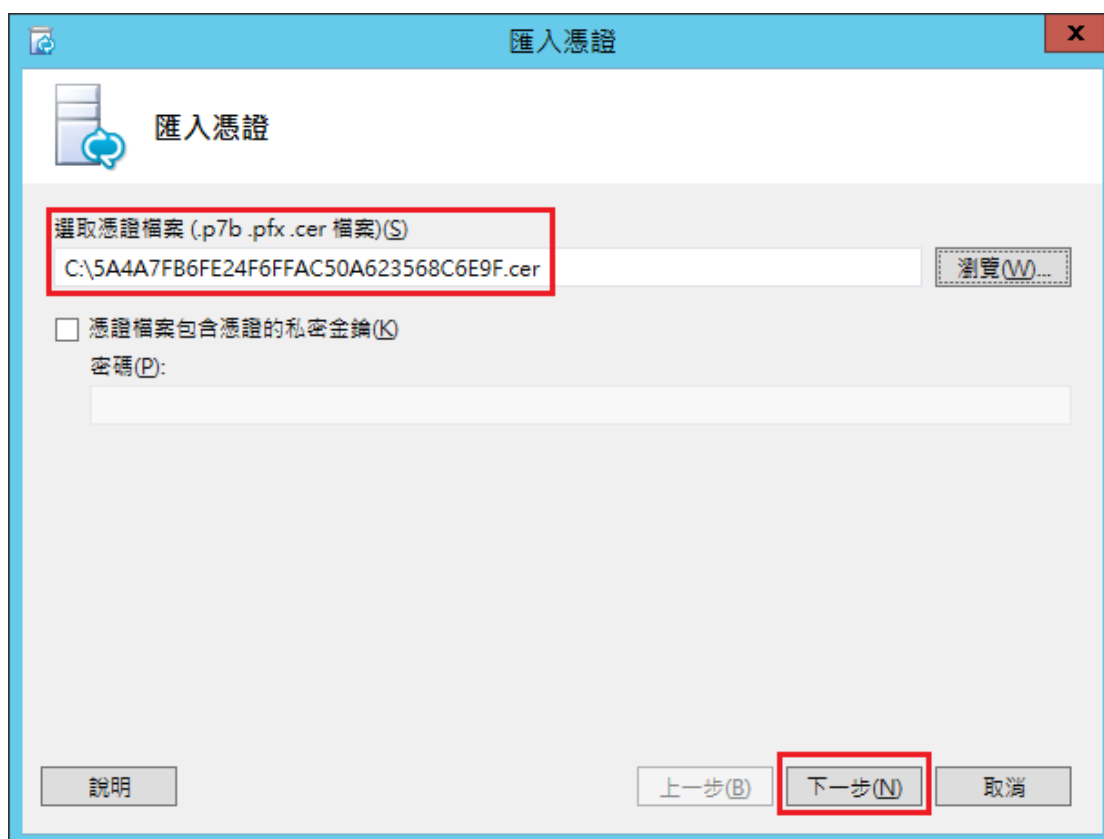


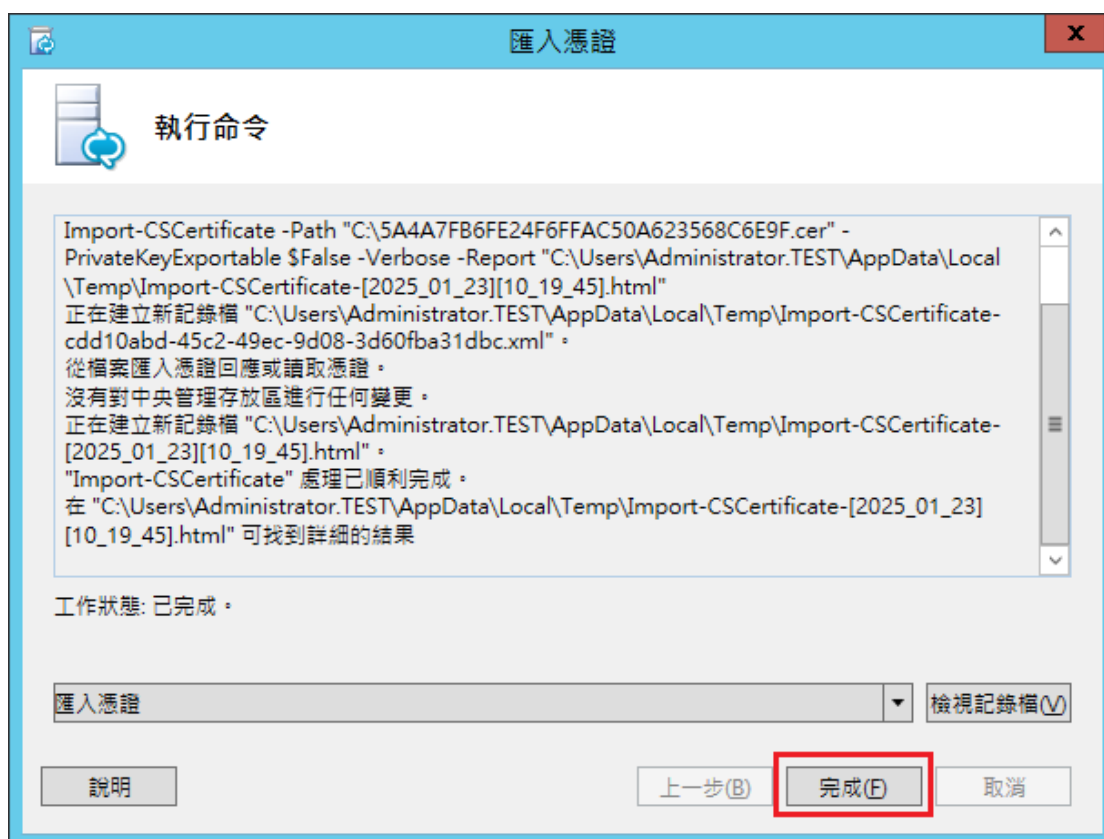
六、 開啟「Lync Server 部屬精靈」至下圖位置，並點選「執行」。



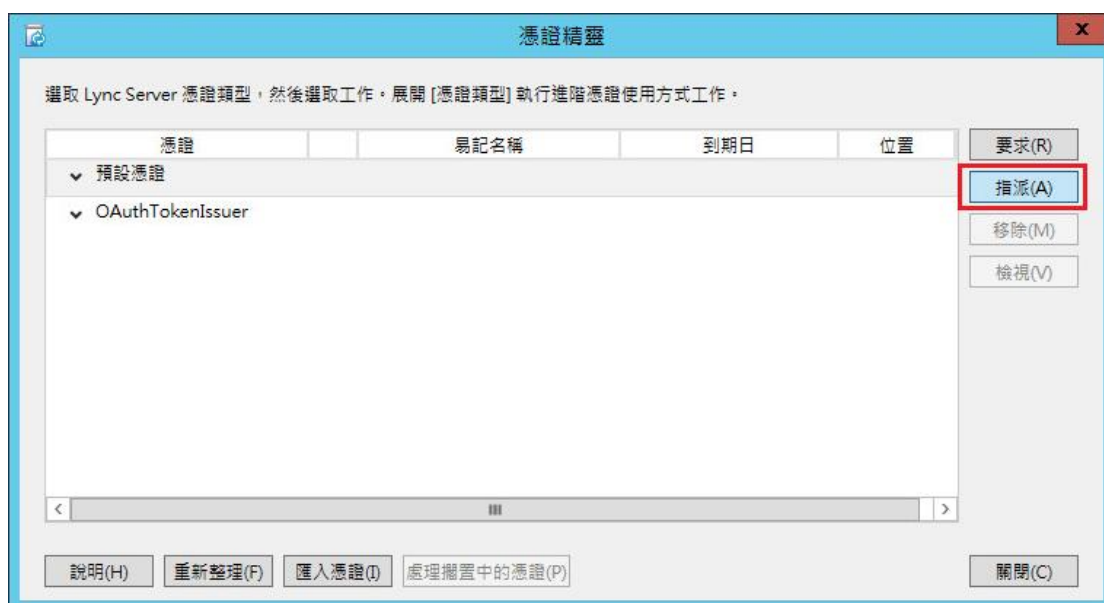
七、 匯入用戶端 SSL 憑證。(檔名為 32 個英數字所組成)

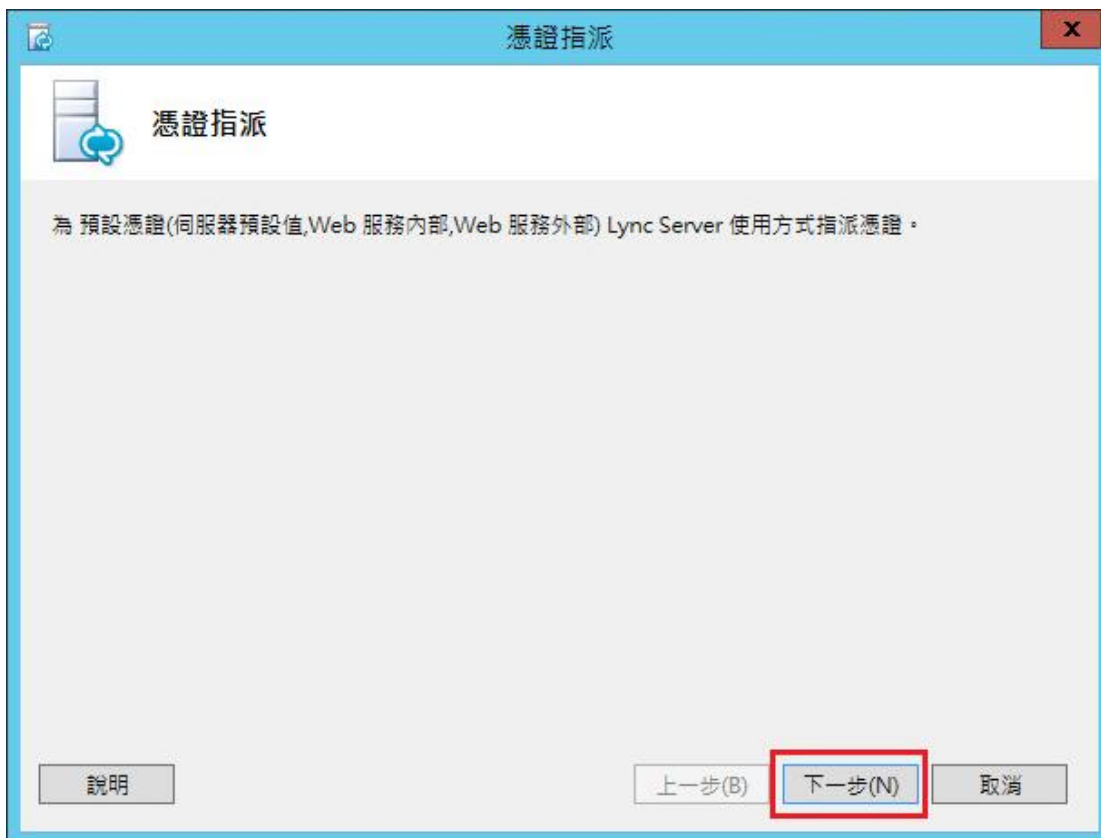


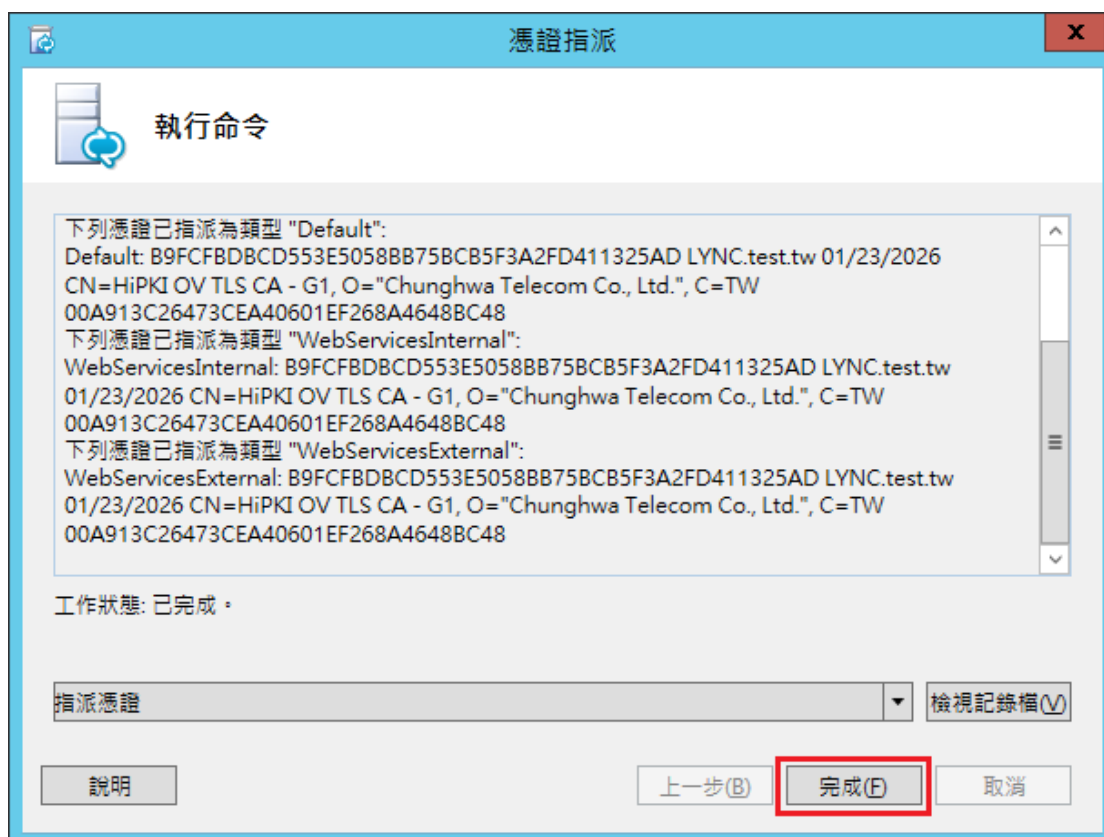
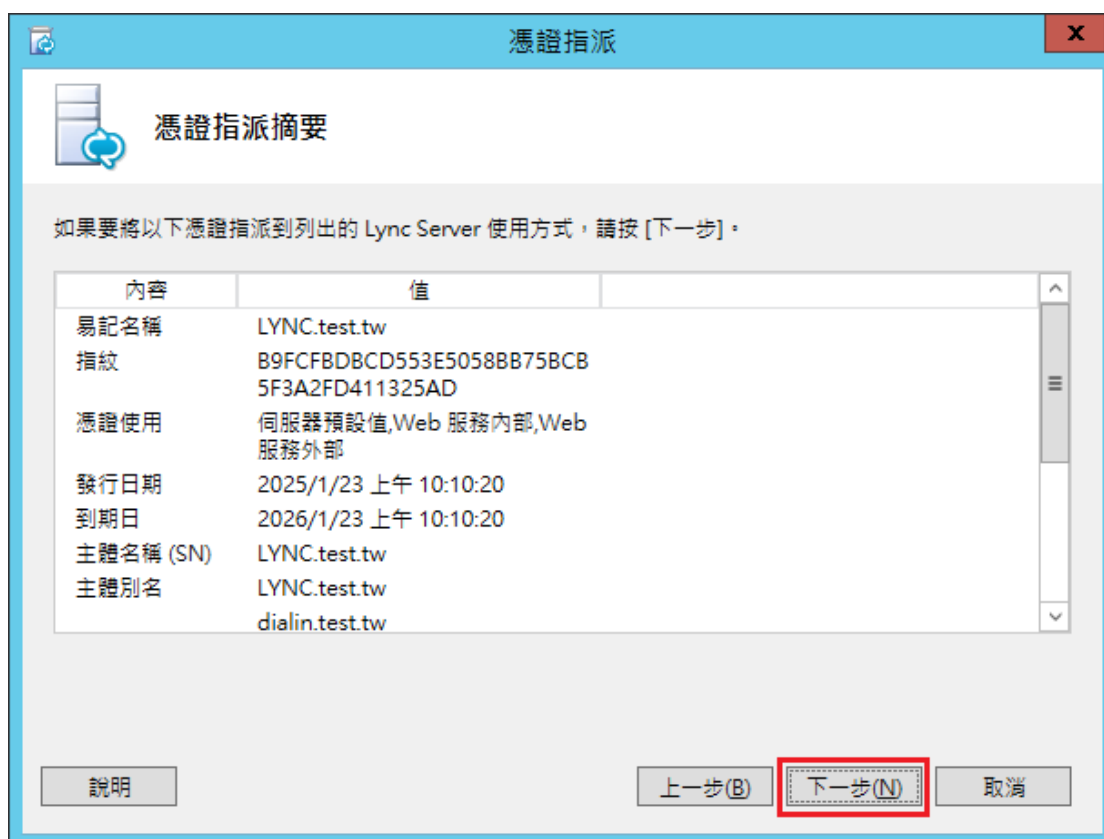


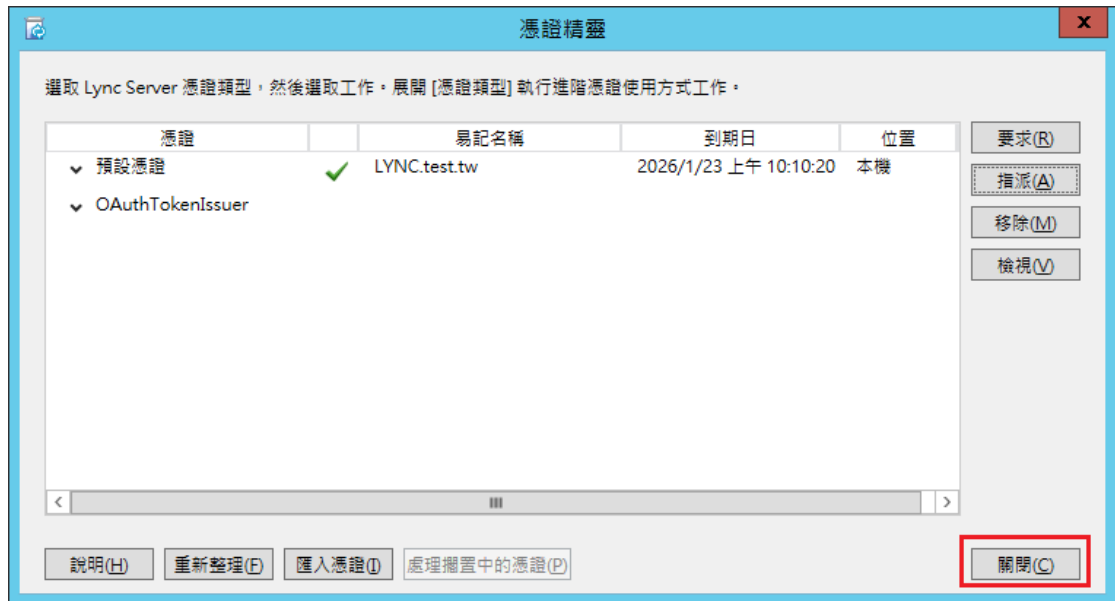


八、 指派 SSL 憑證。



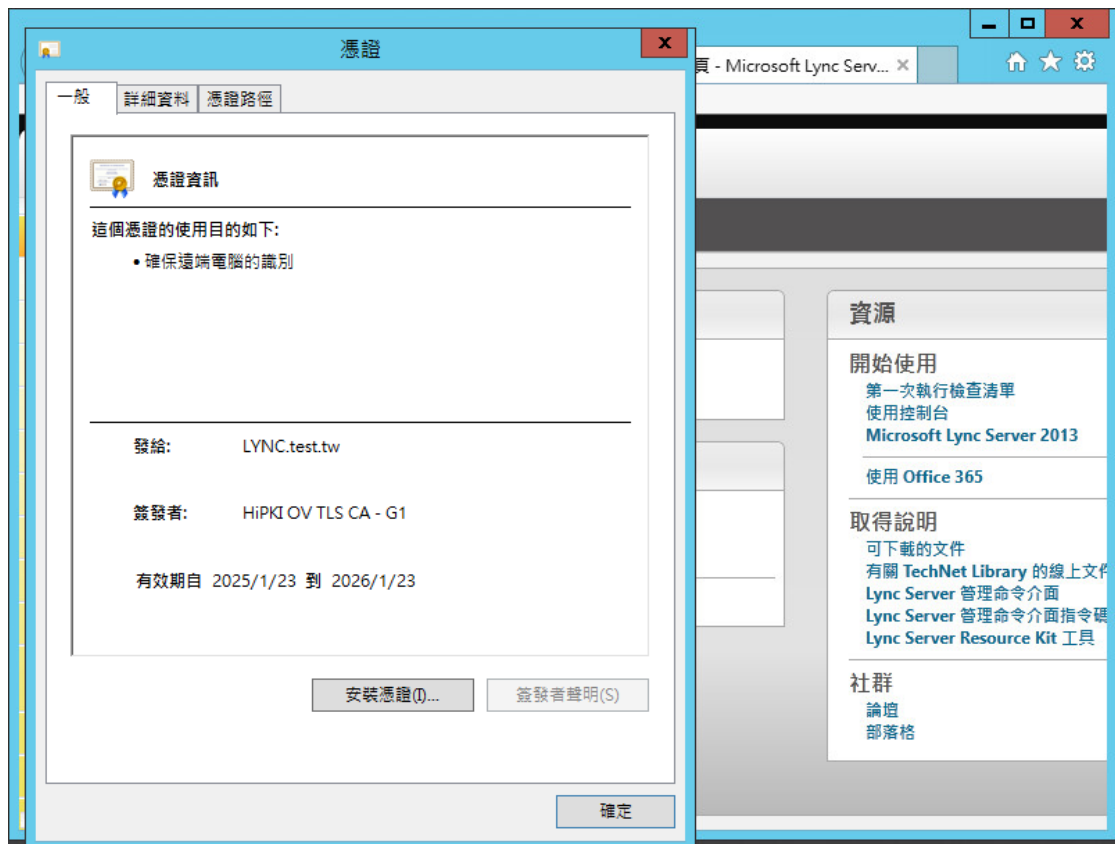
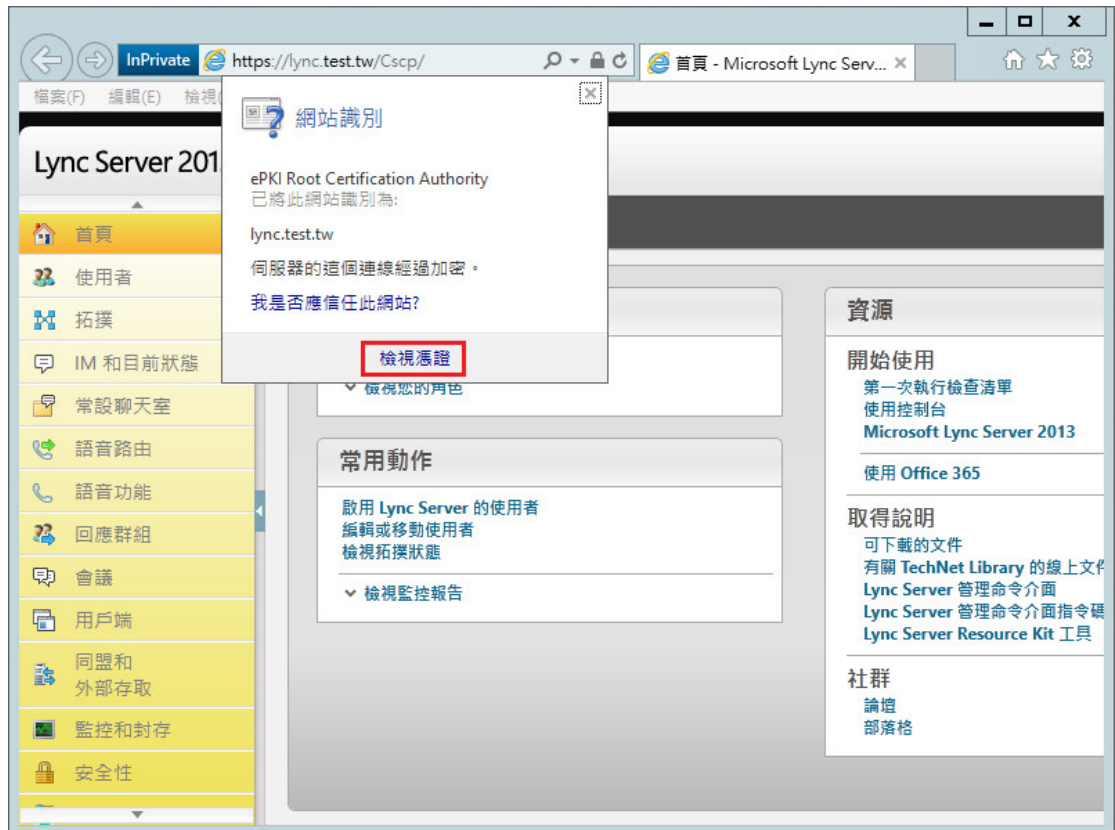






九、憑證全部指派完成，且啟動服務後，可以透過瀏覽器驗證 HTTPS 是否正常。(範例以系統管理存取 URL 測試 HTTPS 服務)





- 十、 安裝 SSL 安全認證標章：
請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文

的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。

請中華電信公司負責維護網站的同仁，參考從企業入口網站電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。