中華電信通用憑證管理中心(PublicCA)

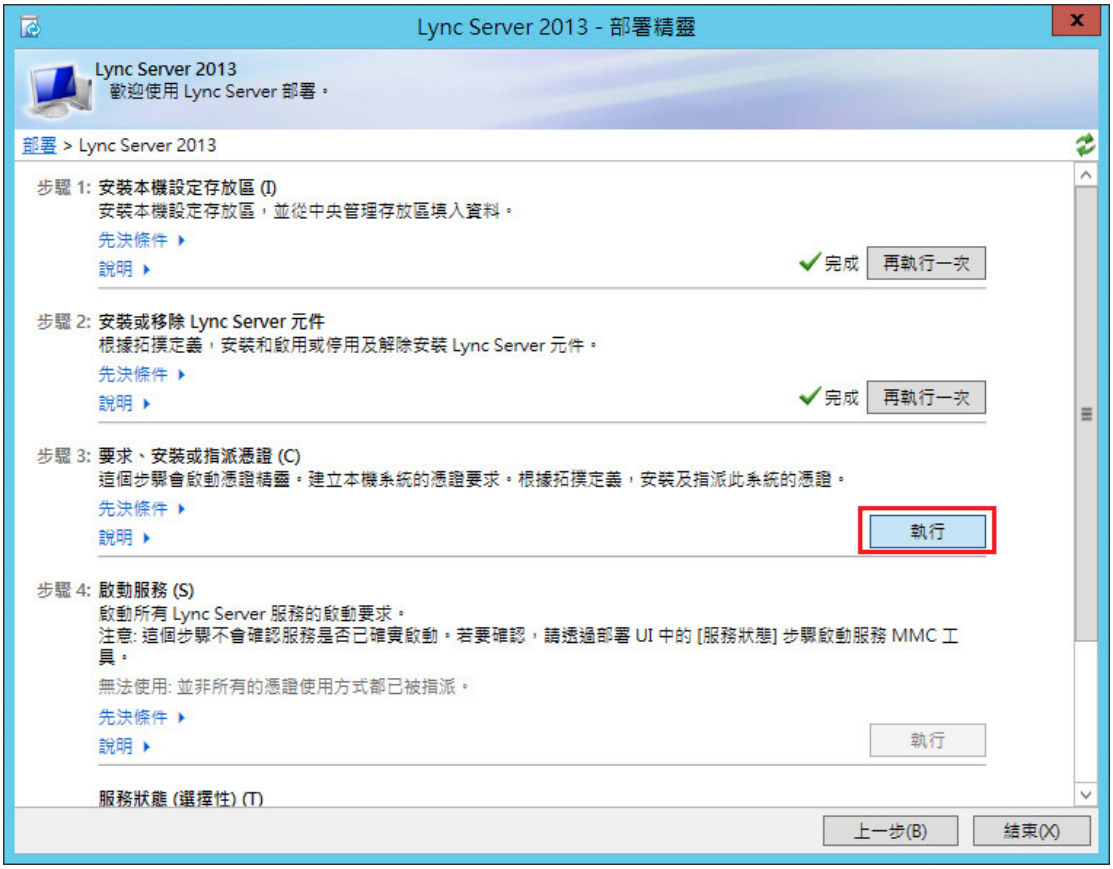
Windows Lync Server SSL 憑證請求檔製作與憑證安裝手冊

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。

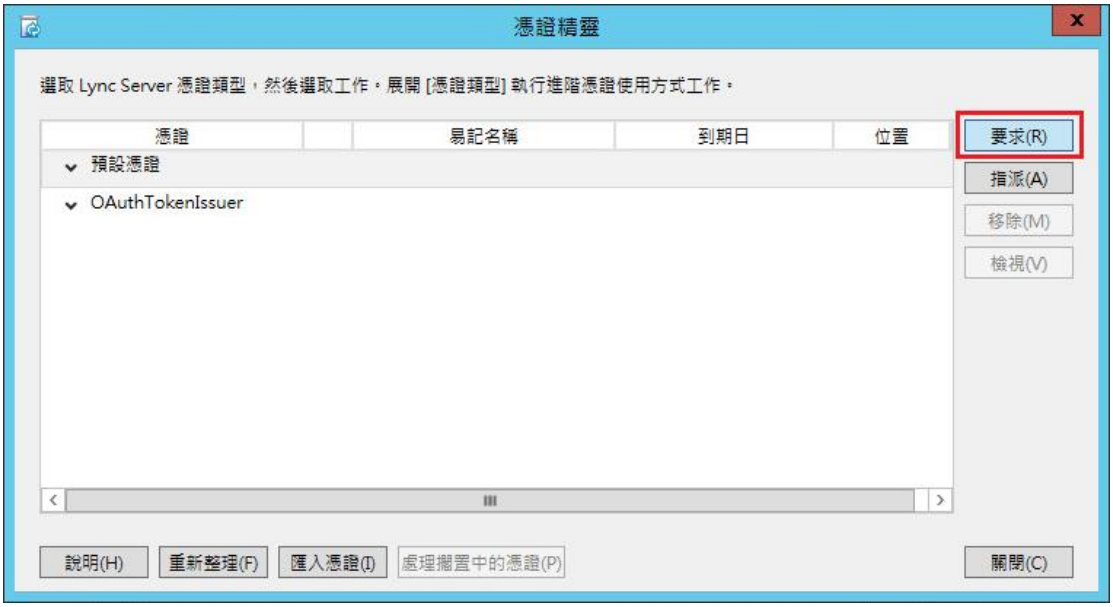
目錄

Windows Lync Server SSL 憑證請求檔製作手冊

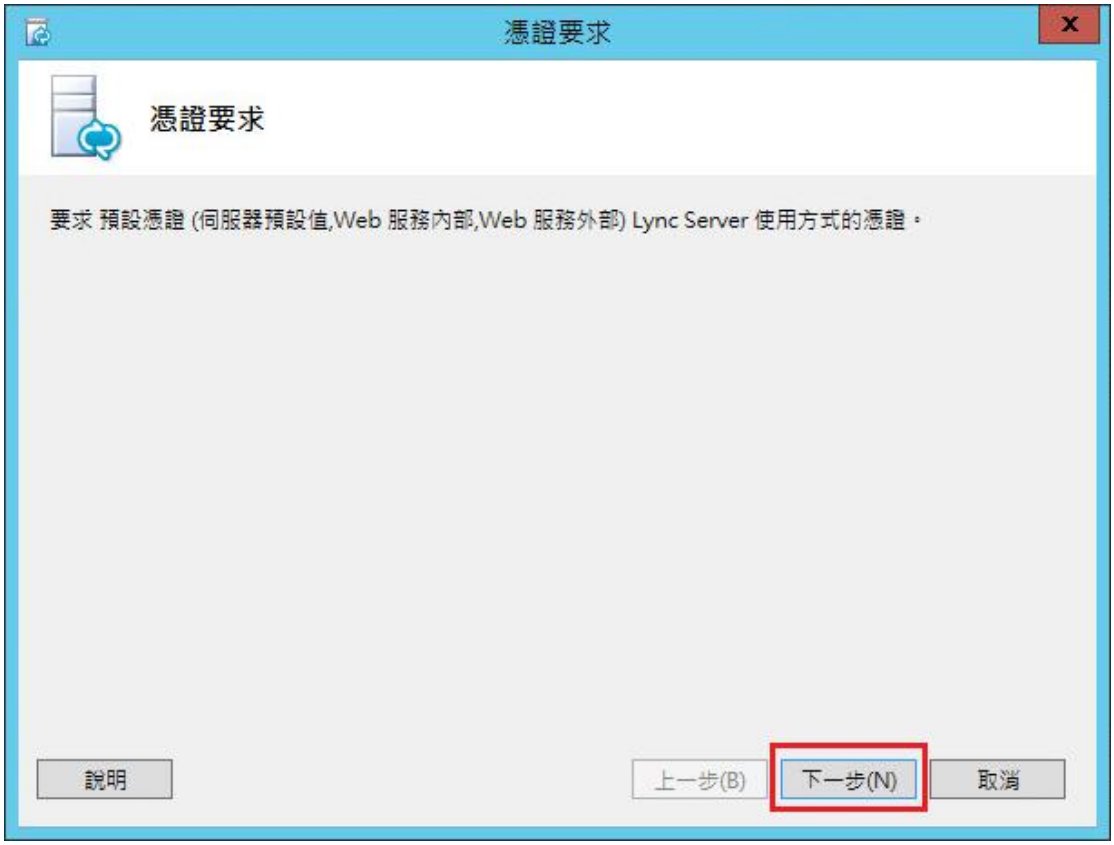
一、　開啟「Lync Server 部署精靈」至下圖位置，並點選「執行」。



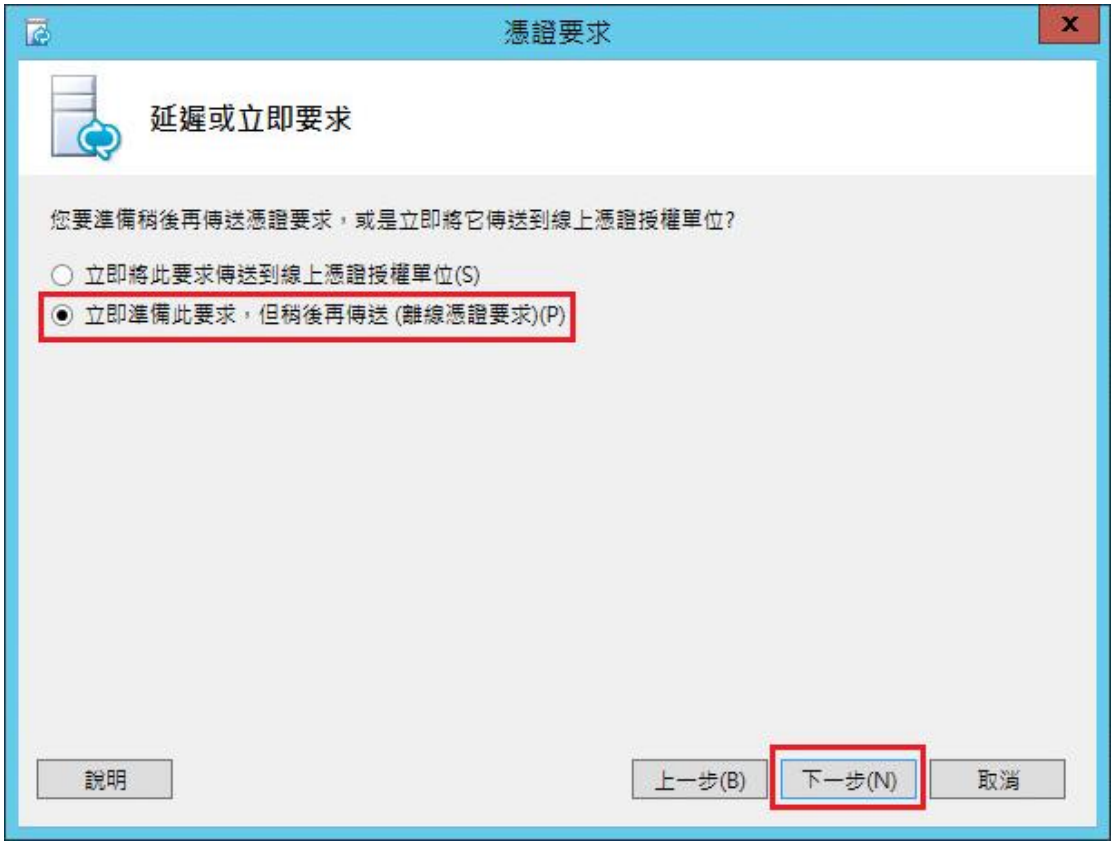
二、　點選「要求」。



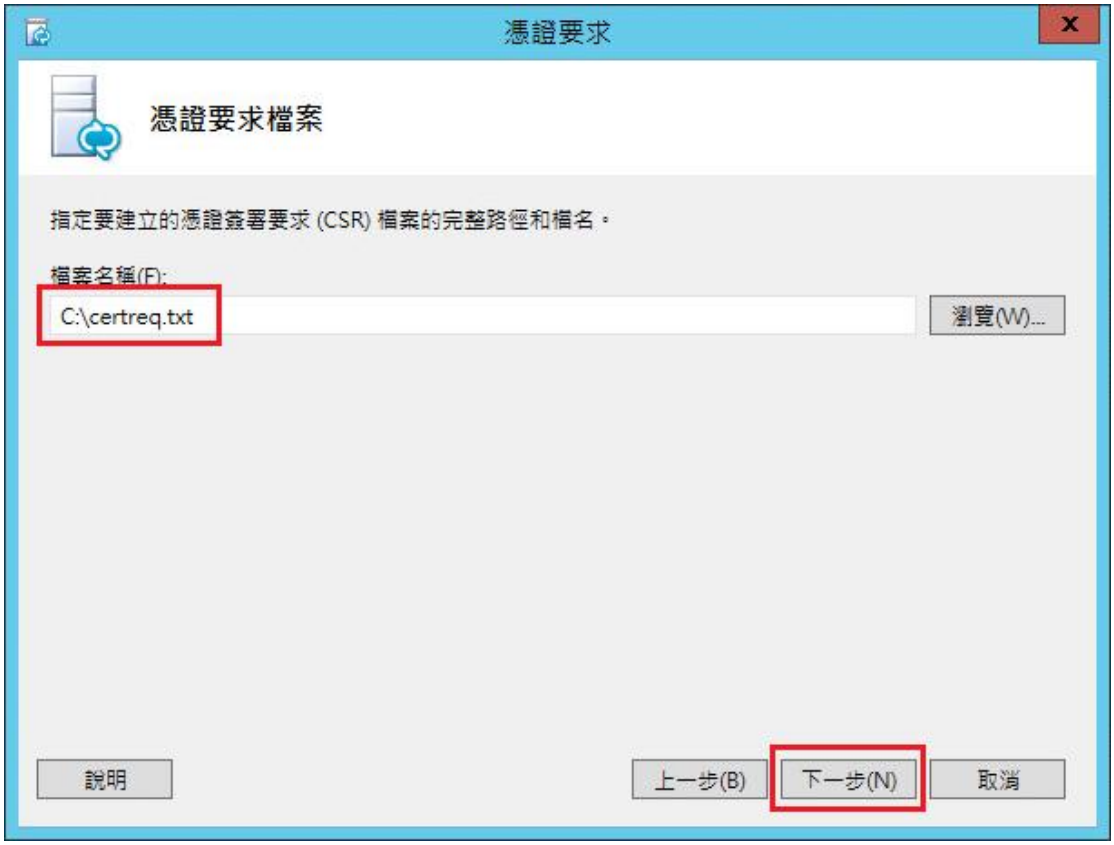
三、　依照以下步驟進行操作

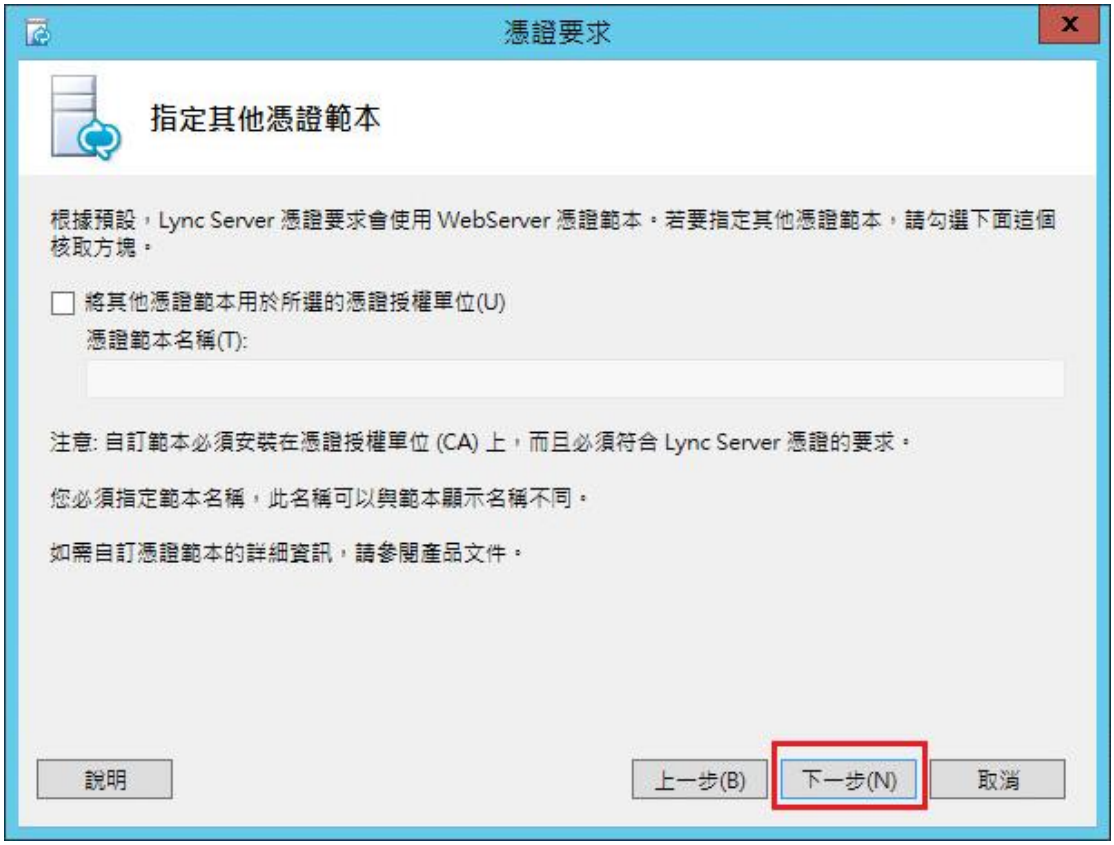


四、　選擇「立即準備此要求，但稍後再傳送」



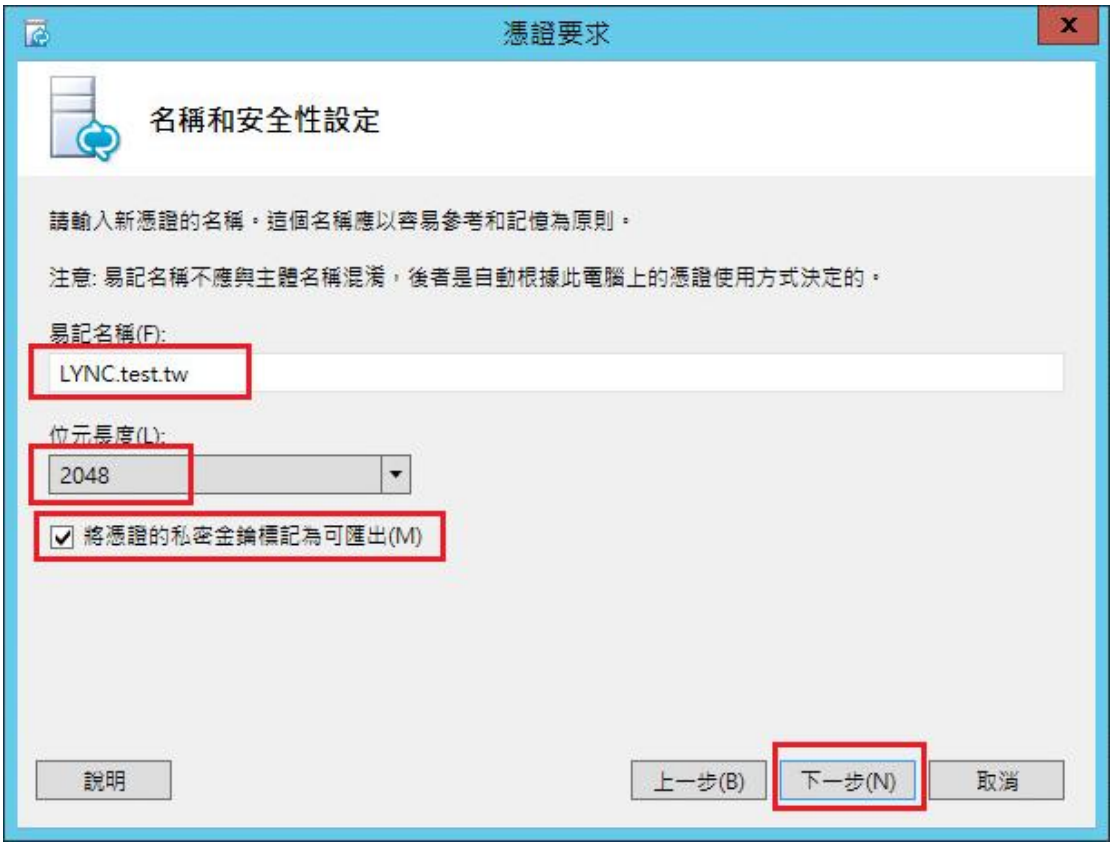
選擇存檔位置



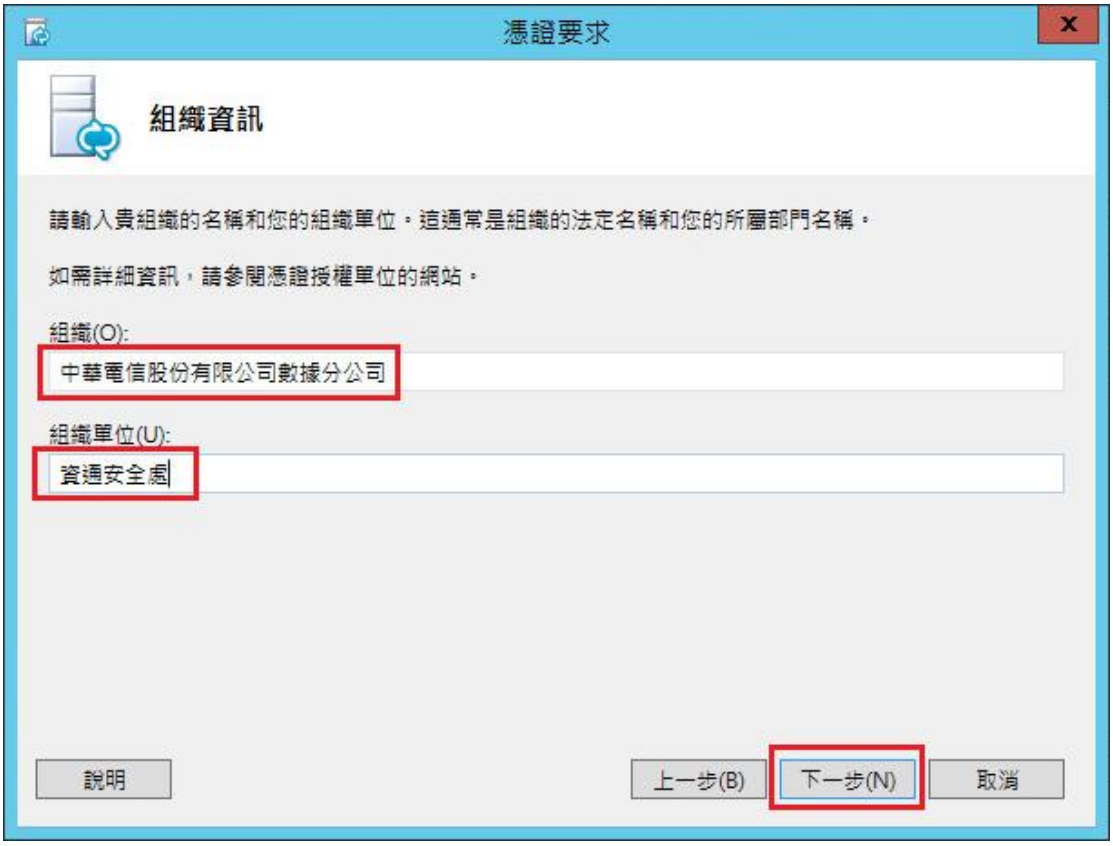


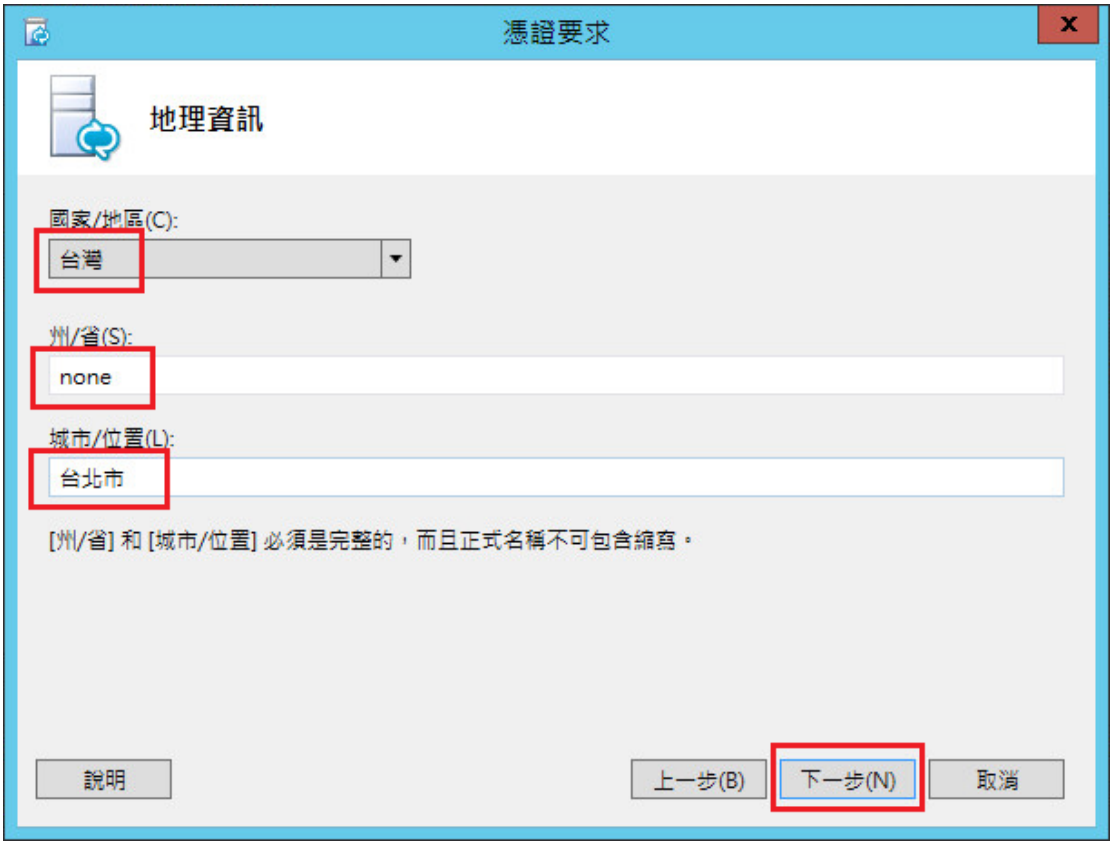
五、　　金鑰長度選擇「2048」，並勾選「將憑證的私密金鑰標記為可匯出」，以便未來備份或是金鑰轉移。請注意依照國際密碼學趨勢，請使用 RSA 2048

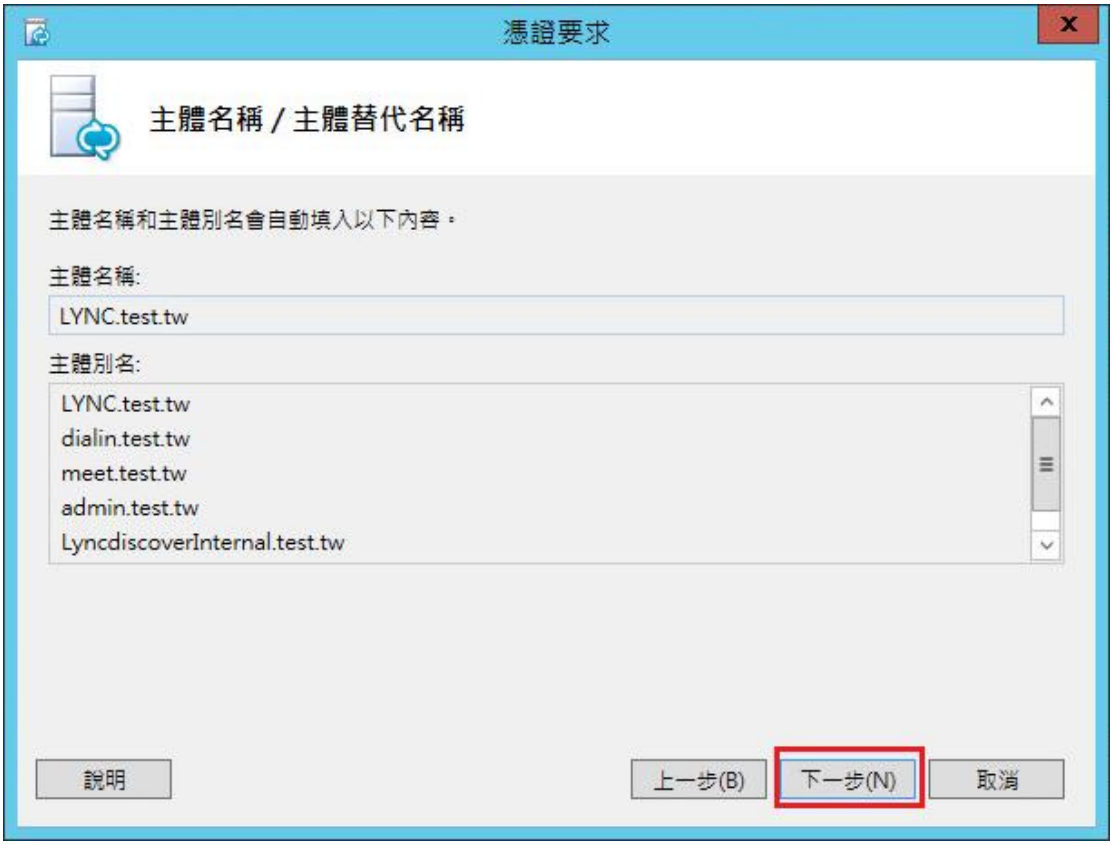
位元(含)以上金鑰長度。

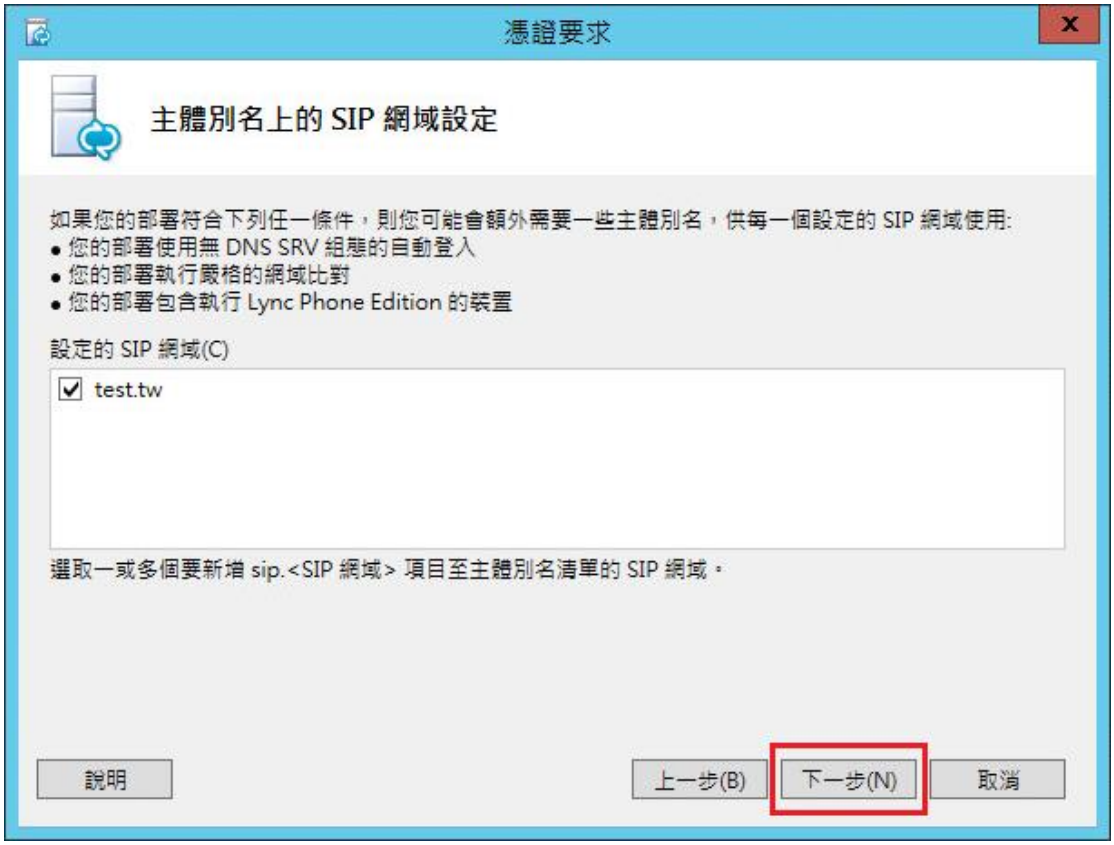


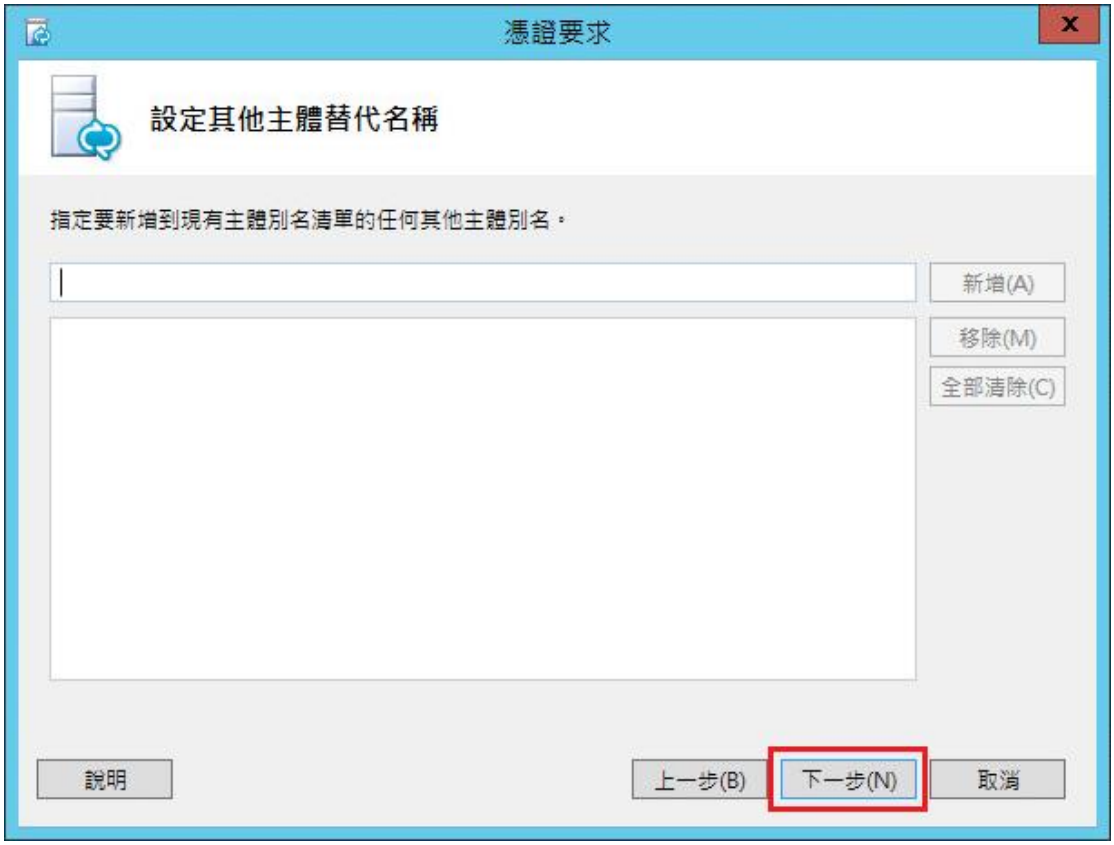
六、 填入「組織資訊」與「地理資訊」。

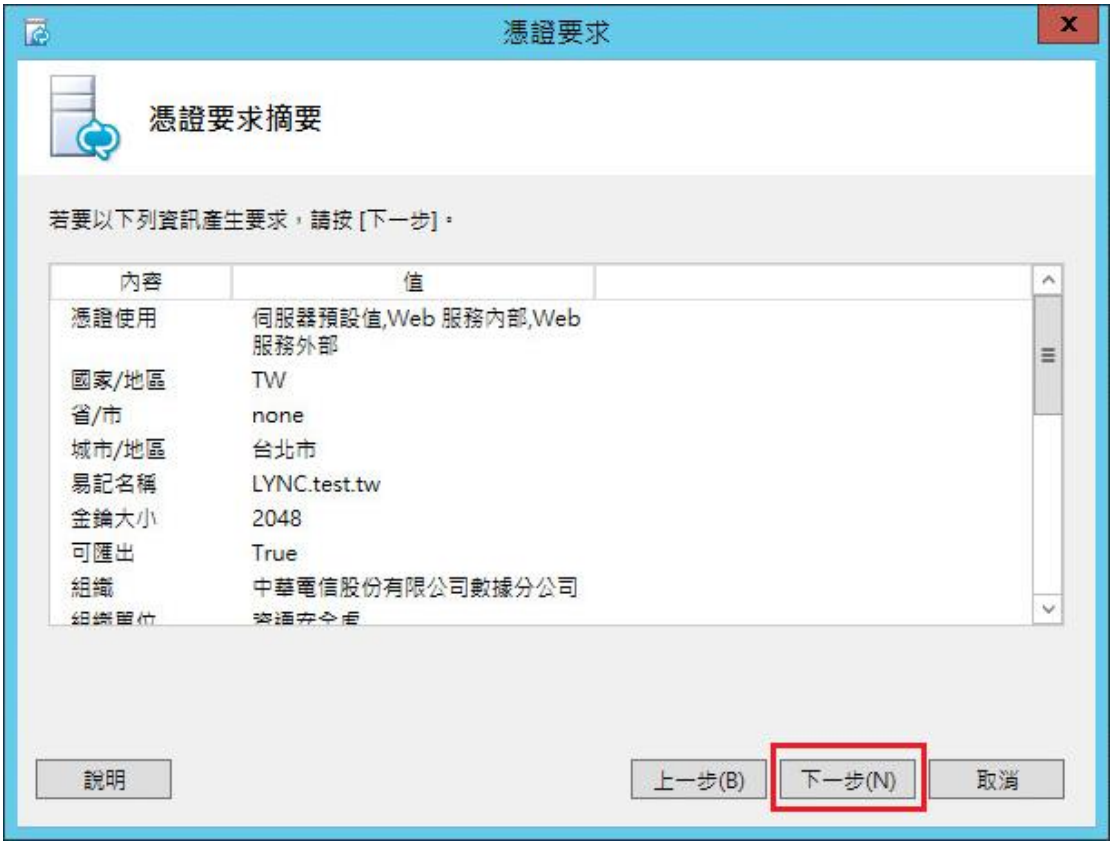


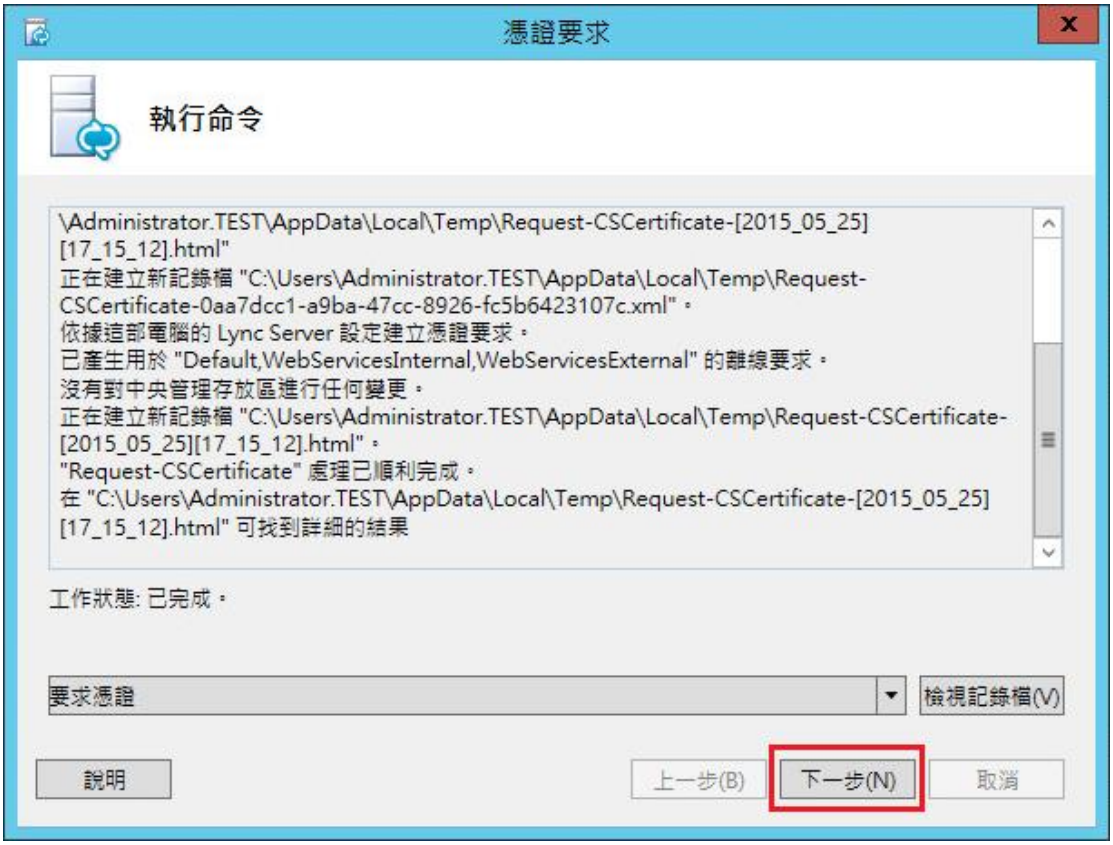

憑證要求
地理資訊
國家/地區(C):
台灣
州/省(S):
none
城市/位置(L):
台北市
[州/省] 和 [城市/位置] 必須是完整的，而且正式名稱不可包含縮寫。
說明
上一步(B)
下一步(N)
取消

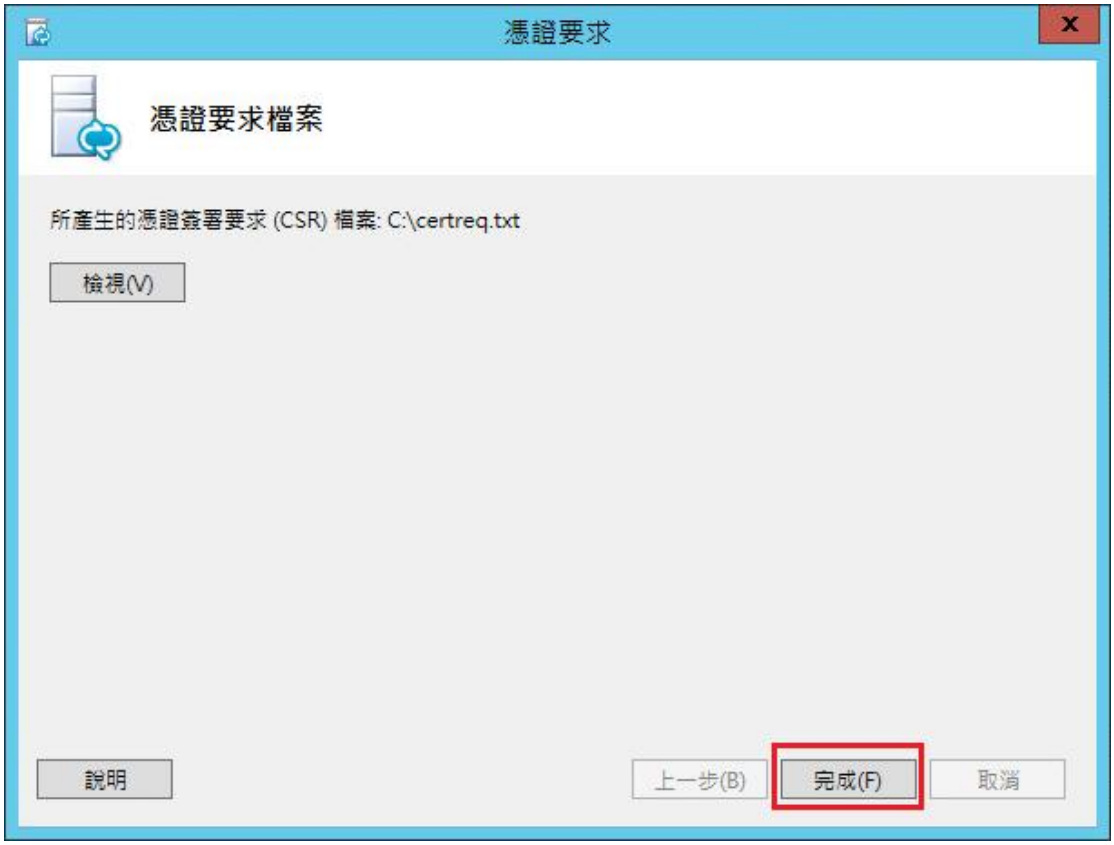

憑證要求
主體名稱 / 主體替代名稱
主體名稱和主體別名會自動填入以下內容。
主體名稱:
LYNC.test.tw
主體別名:
LYNC.test.tw
dialin.test.tw
meet.test.tw
admin.test.tw
LyncdiscoverInternal.test.tw
說明
上一步(B)
下一步(N)
取消

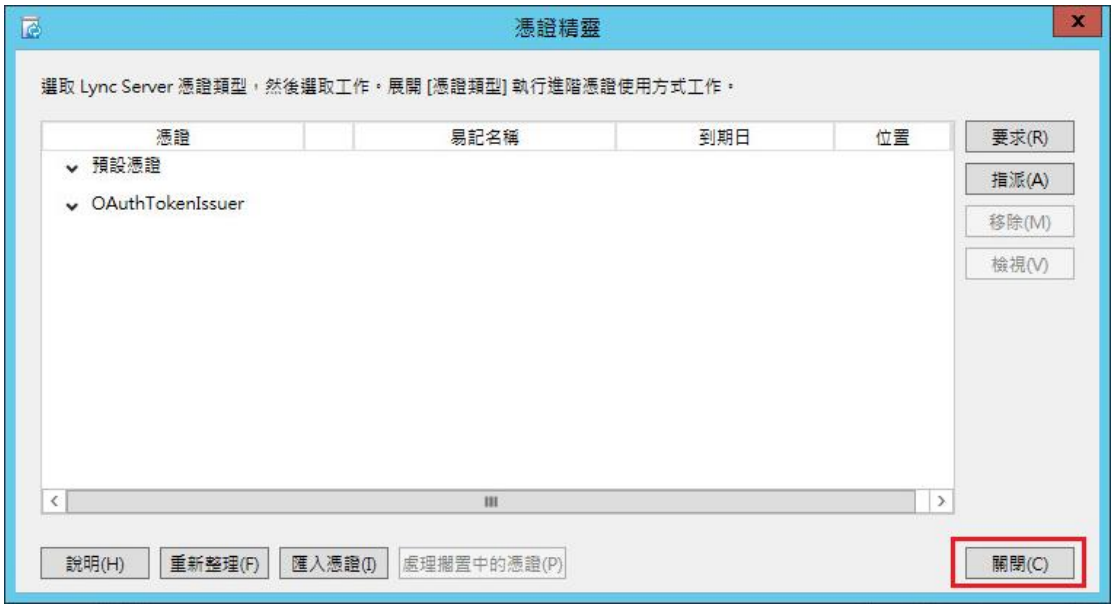

憑證要求
主體別名上的 SIP 網域設定
如果您的部署符合下列任一條件，則您可能會額外需要一些主體別名，供每一個設定的 SIP 網域使用:
• 您的部署使用無 DNS SRV 組態的自動登入
• 您的部署執行嚴格的網域比對
• 您的部署包含執行 Lync Phone Edition 的裝置
設定的 SIP 網域(C)
test.tw
選取一或多個要新增 sip.<SIP 網域> 項目至主體別名清單的 SIP 網域。
說明
上一步(B)
下一步(N)
取消


憑證要求
設定其他主體替代名稱
指定要新增到現有主體別名清單的任何其他主體別名。
新增(A)
移除(M)
全部清除(C)
說明
上一步(B)
下一步(N)
取消


憑證要求
憑證要求摘要
若要以下列資訊產生要求，請按 [下一步]。
內容
值
憑證使用
伺服器預設值,Web 服務內部,Web 服務外部
國家/地區
TW
省/市
none
城市/地區
台北市
易記名稱
LYNC.test.tw
金鑰大小
2048
可匯出
True
組織
中華電信股份有限公司數據分公司
說明
上一步(B)
下一步(N)
取消


憑證要求
執行命令
\Administrator.TEST\AppData\Local\Temp\Request-CSCertificate-[2015_05_25][17_15_12].html"
正在建立新記錄檔 "C:\Users\Administrator.TEST\AppData\Local\Temp\Request-CSCertificate-0aa7dcc1-a9ba-47cc-8926-fc5b6423107c.xml"。
依據這部電腦的 Lync Server 設定建立憑證要求。
已產生用於 "Default,WebServicesInternal,WebServicesExternal" 的離線要求。
沒有對中央管理存放區進行任何變更。
正在建立新記錄檔 "C:\Users\Administrator.TEST\AppData\Local\Temp\Request-CSCertificate-[2015_05_25][17_15_12].html"。
"Request-CSCertificate" 處理已順利完成。
在 "C:\Users\Administrator.TEST\AppData\Local\Temp\Request-CSCertificate-[2015_05_25][17_15_12].html" 可找到詳細的結果
工作狀態: 已完成。
要求憑證
檢視記錄檔(V)
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通用憑證管理中心網站(http://publicca.hinet.net/)依照網頁說明申請SSL憑證（以文字編輯器如記事本開啟憑證請求檔，全選及複製檔案內容，將憑證請求檔貼上SSL憑證申請網頁之表單。)。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。

八、 若此張憑證還有牽涉不同廠牌伺服器之匯出與匯入，可參考本管理中心

之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

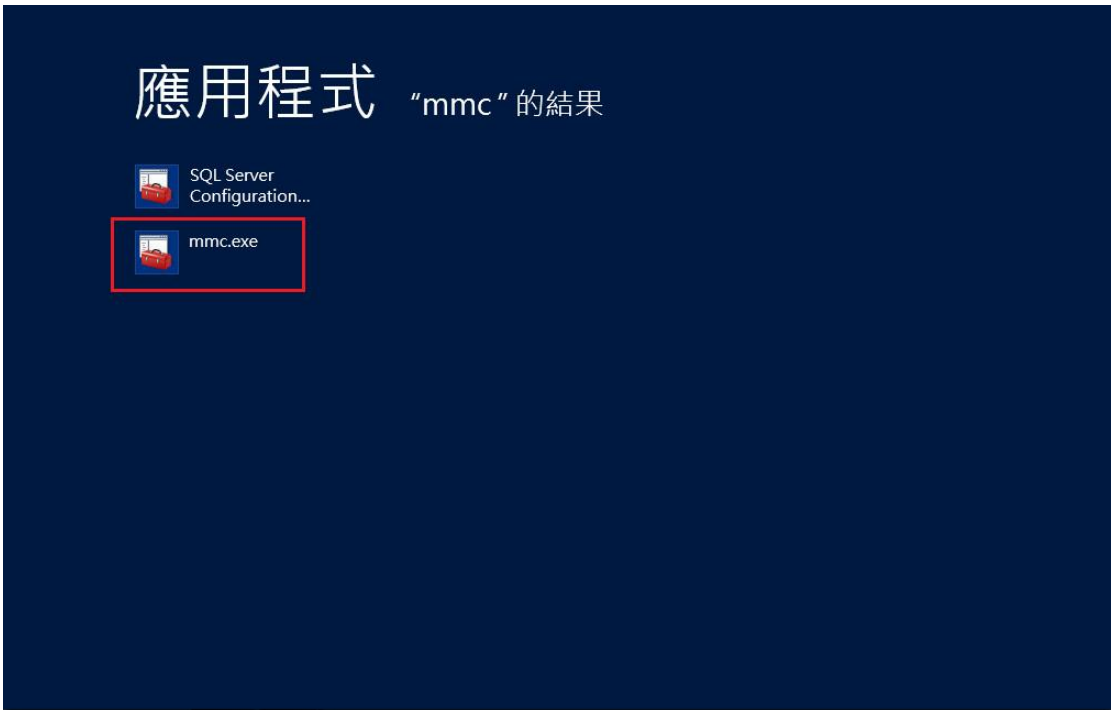
Windows Lync Server SSL 憑證安裝操作手冊

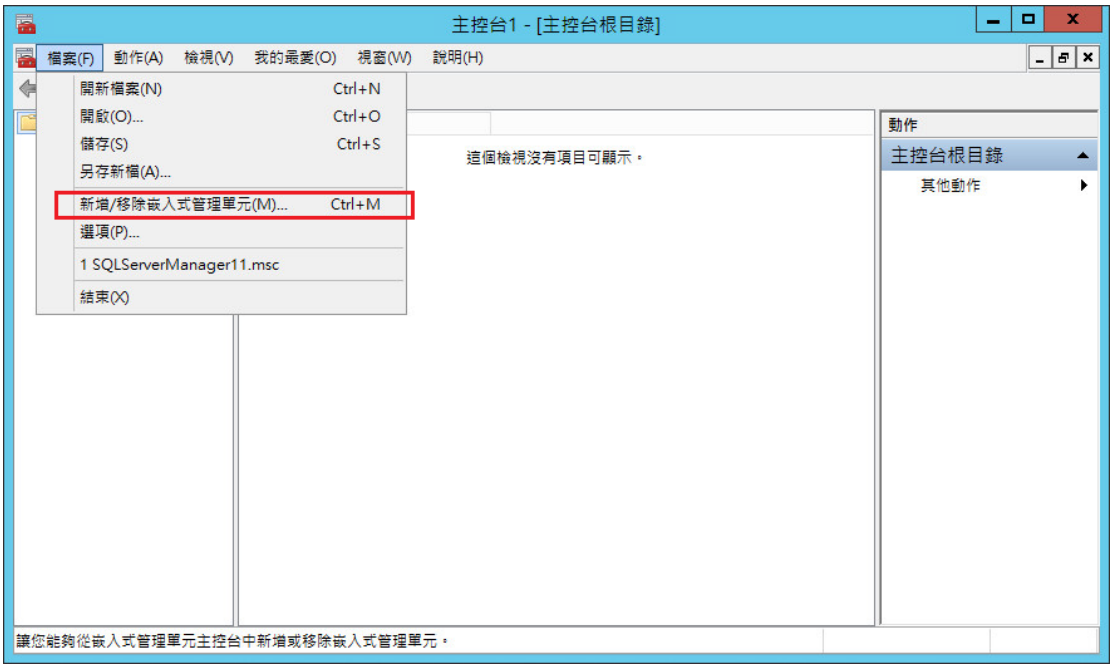
一、 下載憑證串鏈，包含 3 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：

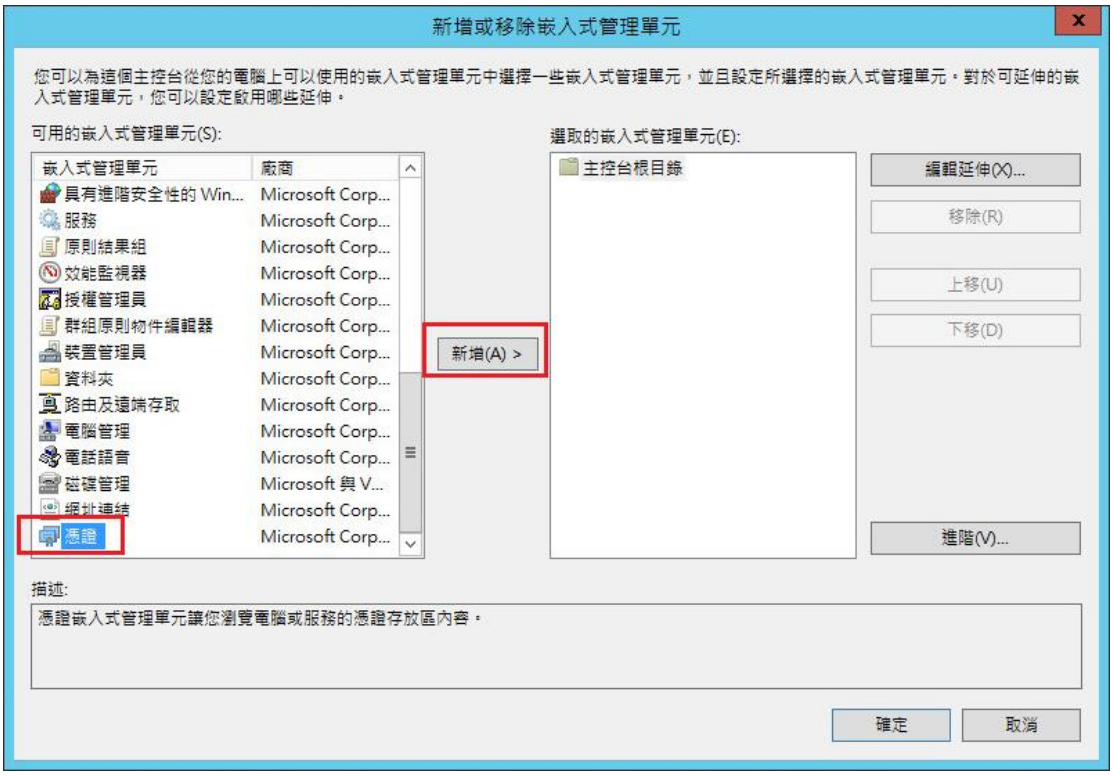
1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。若是中華電信之所屬單位，於經審驗核准申請之電子表單的資訊表單「IS 14-伺服器應用軟體憑證申請/異動單」頁面下方，可以下載憑證串鏈壓縮檔，解壓縮後可以取得憑證串鏈 3 個檔案。
2. 從網站查詢與下載：
   eCA 憑證：
   http://epki.com.tw/download/ROOTeCA_64.crt
   PublicCA G2 憑證：
   http://epki.com.tw/download/PublicCA2_64.crt
   SSL 憑證下載：您若是本公司之客戶，請至 PublicCA 網站點選「SSL 憑證服務」再點選「SSL 憑證查詢及下載」，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 http://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。

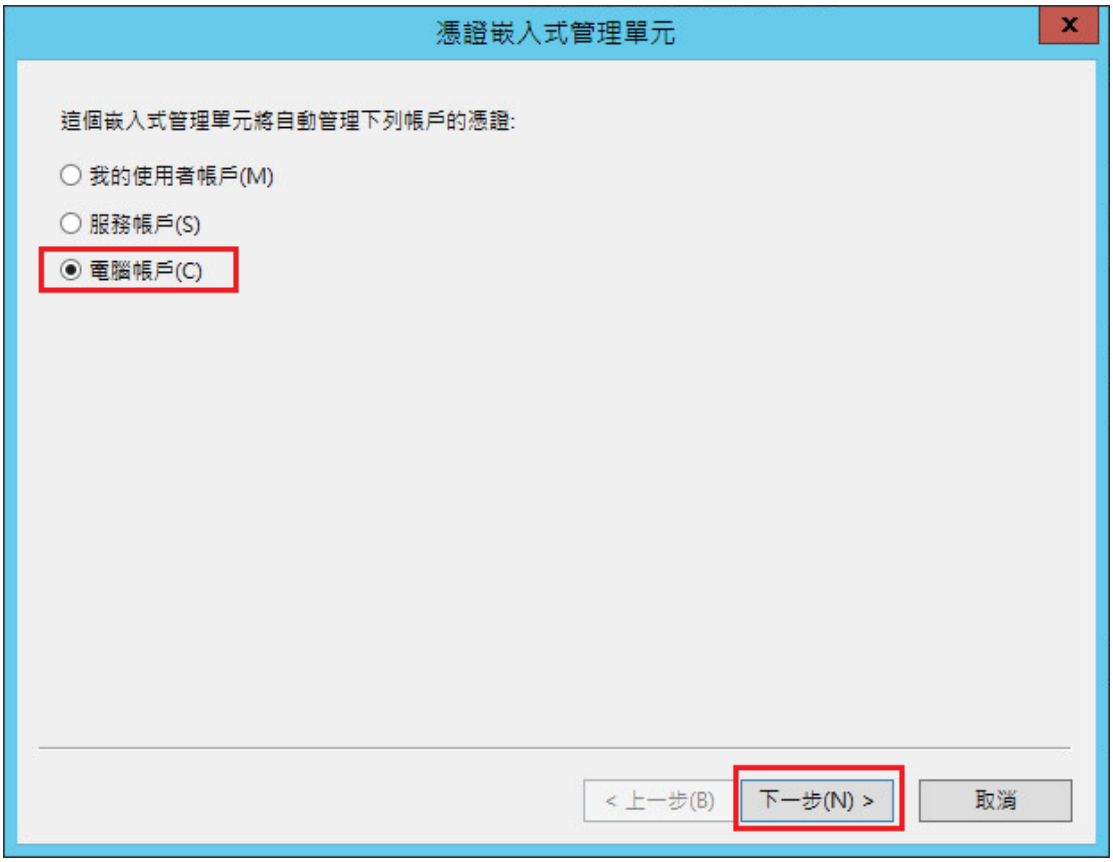
二、 有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節，請參閱問與答之金鑰長度與演算法(https://publicca.hinet.net/SSL-08-06.htm)

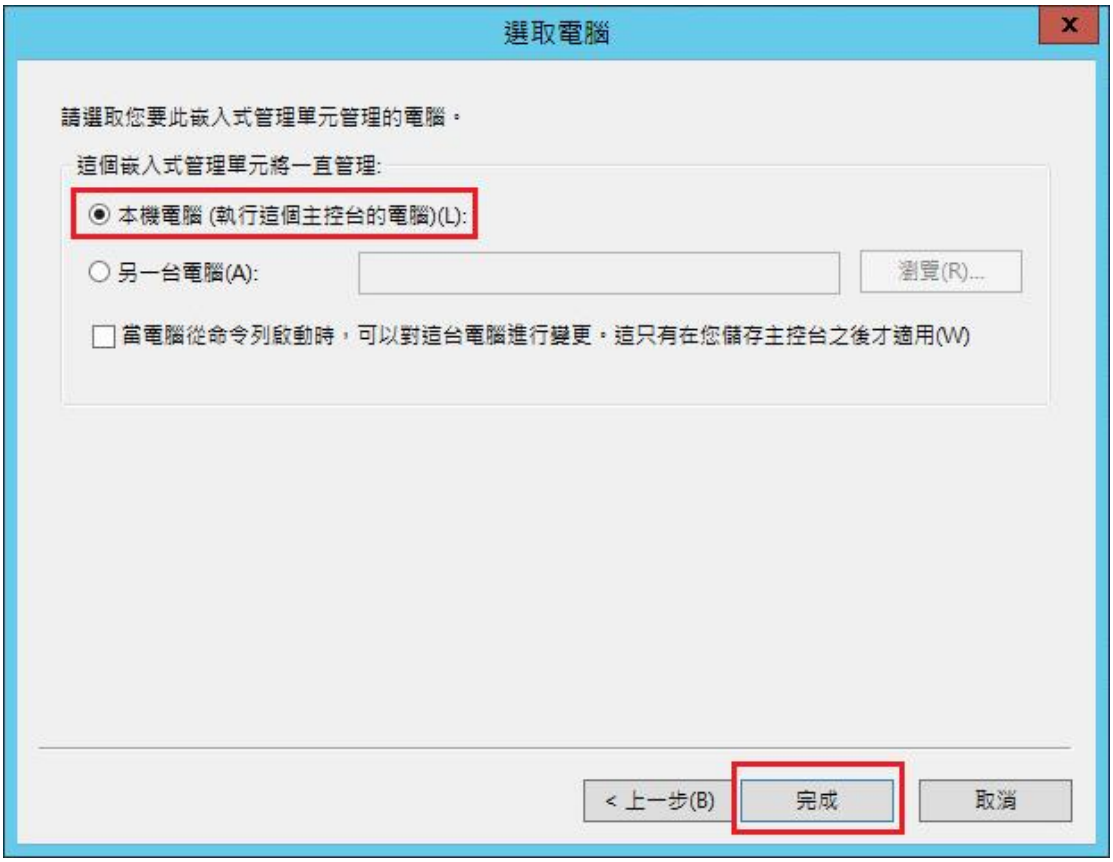
三、 開啟 mmc 安裝根憑證及中繼憑證。
開始→輸入「mmc」→點選「mmc.exe」，並依下圖操作。

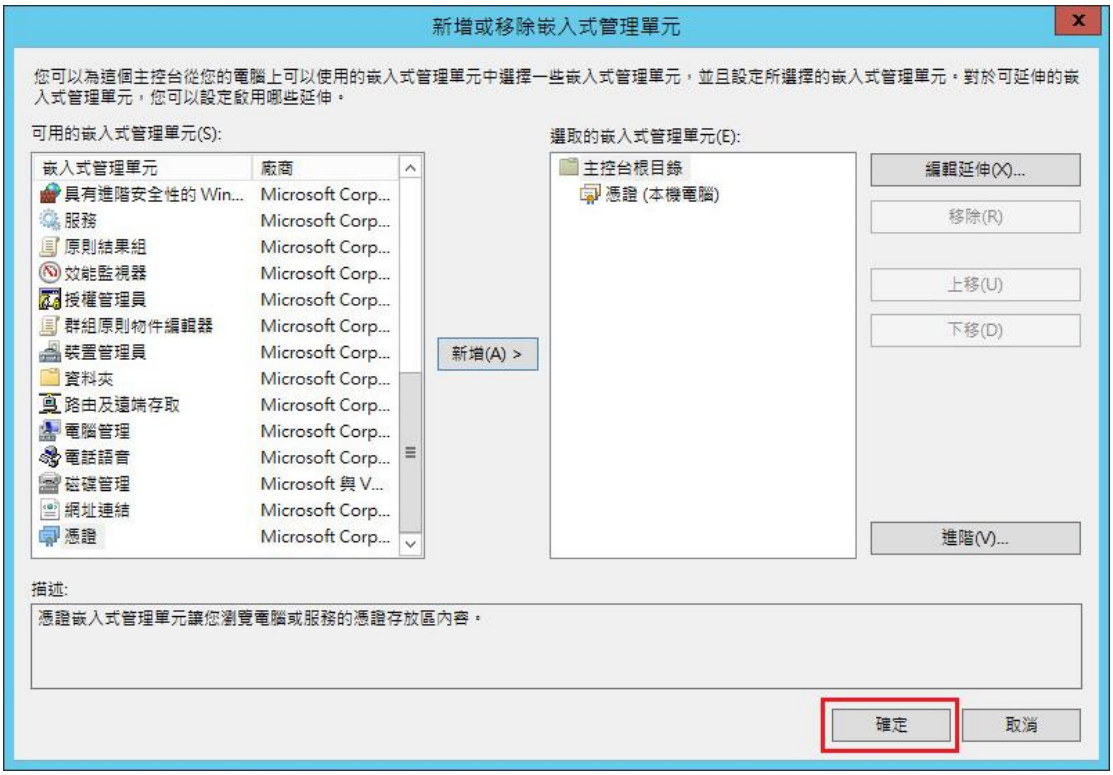

應用程式 "mmc" 的結果
SQL Server Configuration...
mmc.exe


主控台1 - [主控台根目錄]
檔案(F)
動作(A)
檢視(V)
我的最愛(O)
視窗(W)
說明(H)
開新檔案(N) Ctrl+N
開啟(O)... Ctrl+O
儲存(S) Ctrl+S
另存新檔(A)...
新增/移除嵌入式管理單元(M)... Ctrl+M
選項(P)...
1 SQLServerManager11.msc
結束(X)
這個檢視沒有項目可顯示。
動作
主控台根目錄
其他動作
讓您能夠從嵌入式管理單元主控台中新增或移除嵌入式管理單元。

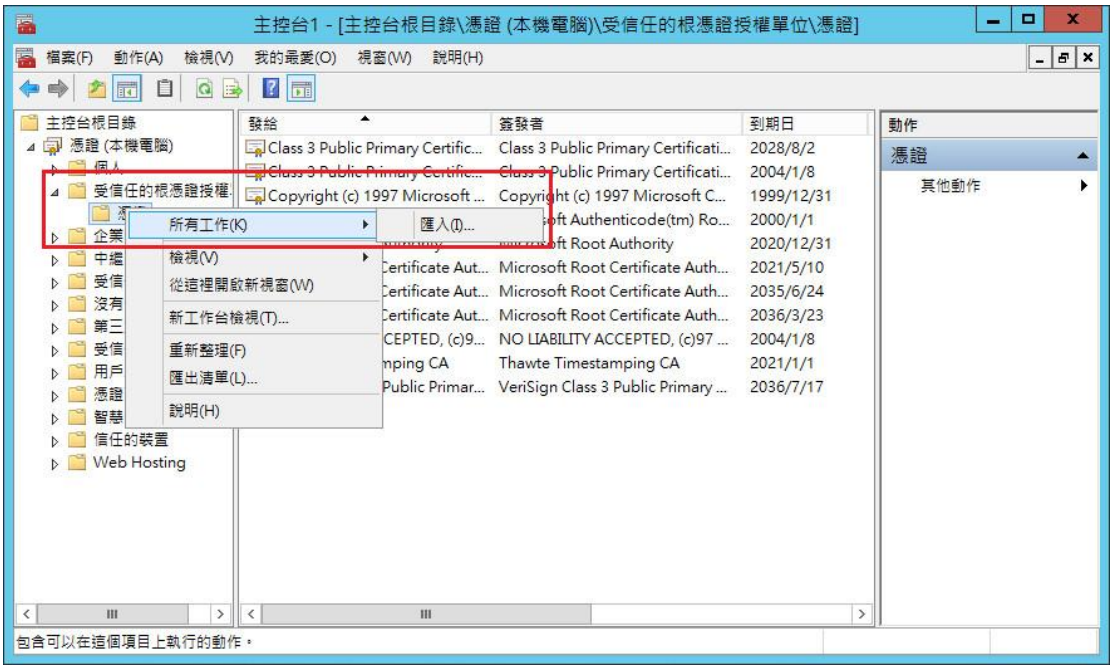

新增或移除嵌入式管理單元
您可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式管理單元，並且設定所選擇的嵌入式管理單元。對於可延伸的嵌入式管理單元，您可以設定啟用哪些延伸。
可用的嵌入式管理單元(S):
嵌入式管理單元
廠商
具有進階安全性的 Win...
Microsoft Corp...
服務
原則結果組
效能監視器
授權管理員
群組原則物件編輯器
裝置管理員
資料夾
路由及遠端存取
電腦管理
電話語音
磁碟管理
Microsoft 與 V...
網址連結
憑證
新增(A) >
選取的嵌入式管理單元(E):
主控台根目錄
編輯延伸(X)...
移除(R)
上移(U)
下移(D)
進階(V)...
描述:
憑證嵌入式管理單元讓您瀏覽電腦或服務的憑證存放區內容。
確定
取消

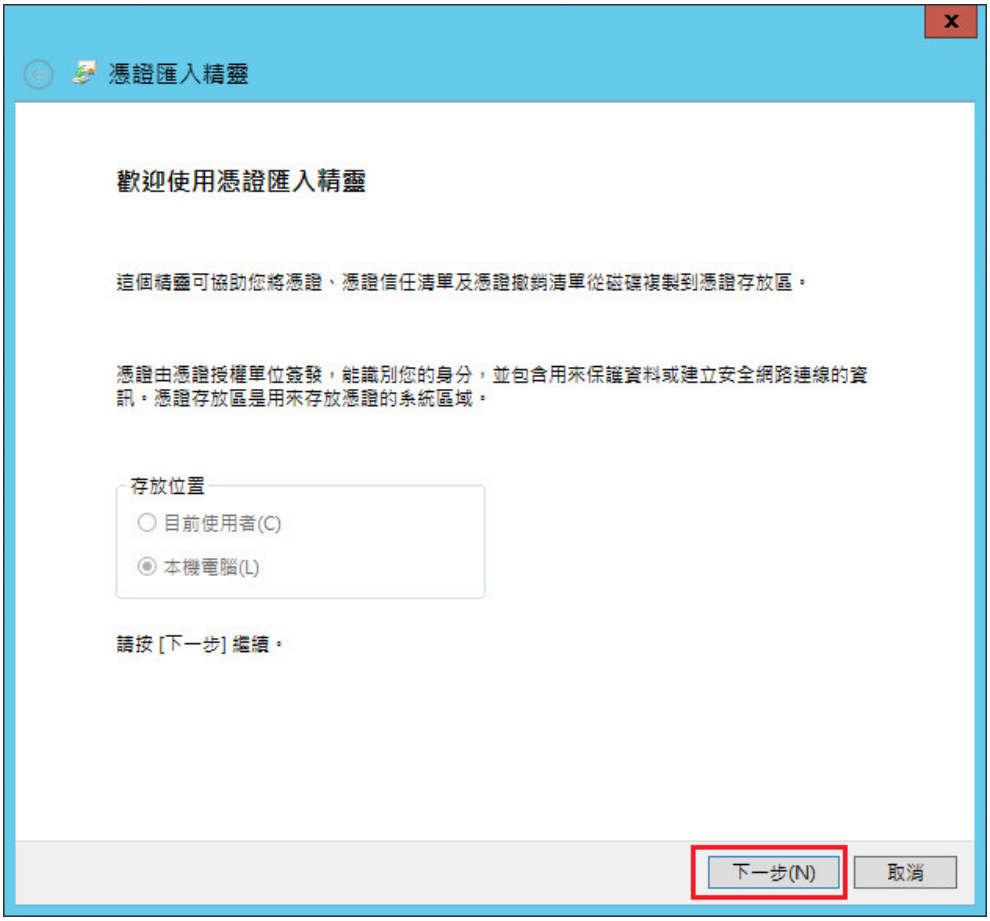

憑證嵌入式管理單元
這個嵌入式管理單元將自動管理下列帳戶的憑證:
我的使用者帳戶(M)
服務帳戶(S)
電腦帳戶(C)
< 上一步(B)
下一步(N) >
取消

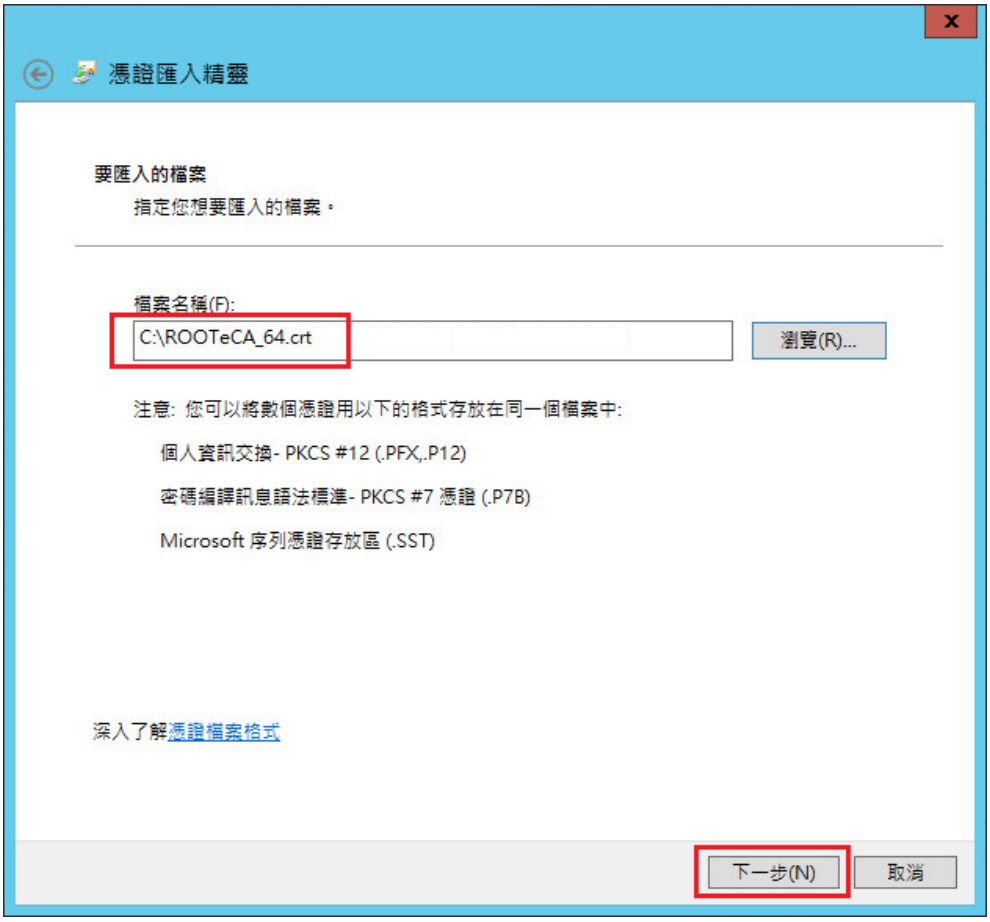

選取電腦
請選取您要此嵌入式管理單元管理的電腦。
這個嵌入式管理單元將一直管理:
本機電腦 (執行這個主控台的電腦)(L):
另一台電腦(A):
瀏覽(R)...
當電腦從命令列啟動時，可以對這台電腦進行變更。這只有在您儲存主控台之後才適用(W)
< 上一步(B)
完成
取消

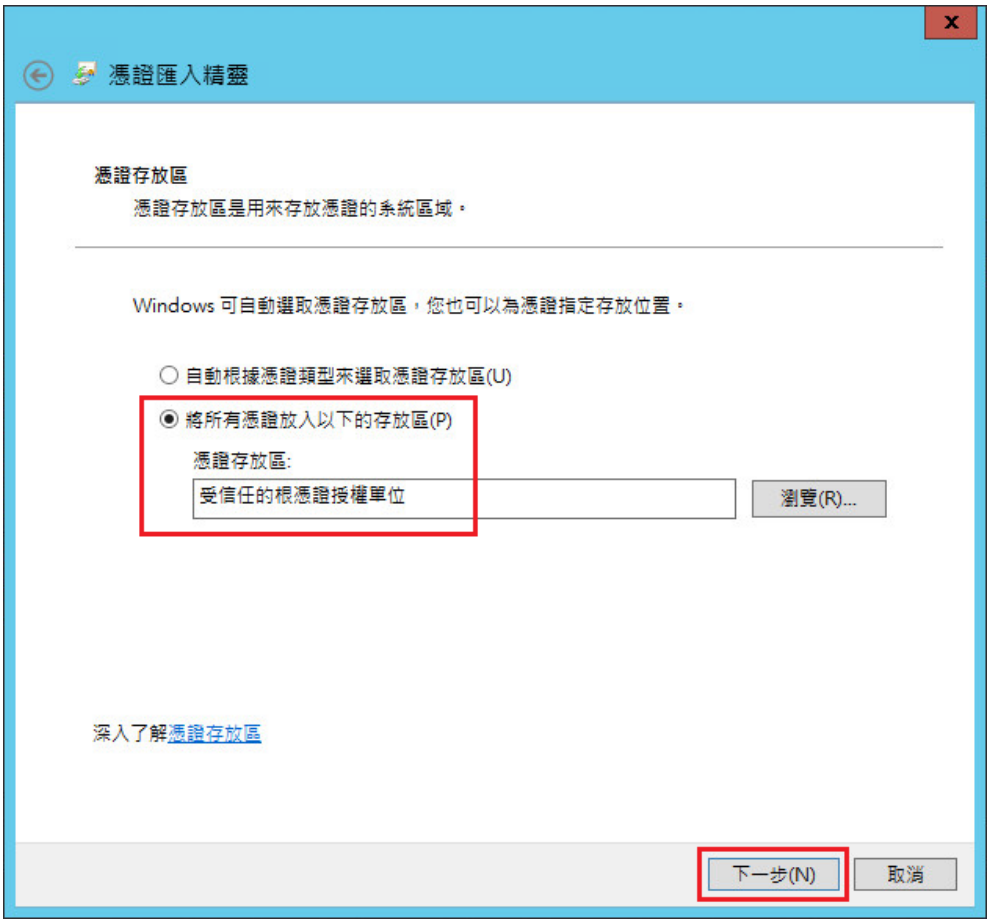

新增或移除嵌入式管理單元
您可以為這個主控台從您的電腦上可以使用的嵌入式管理單元中選擇一些嵌入式管理單元，並且設定所選擇的嵌入式管理單元。對於可延伸的嵌入式管理單元，您可以設定啟用哪些延伸。
可用的嵌入式管理單元(S):
嵌入式管理單元
廠商
具有進階安全性的 Win... Microsoft Corp...
服務 Microsoft Corp...
原則結果組 Microsoft Corp...
效能監視器 Microsoft Corp...
授權管理員 Microsoft Corp...
群組原則物件編輯器 Microsoft Corp...
裝置管理員 Microsoft Corp...
資料夾 Microsoft Corp...
路由及遠端存取 Microsoft Corp...
電腦管理 Microsoft Corp...
電話語音 Microsoft Corp...
磁碟管理 Microsoft 與 V...
網址連結 Microsoft Corp...
憑證 Microsoft Corp...
新增(A) >
選取的嵌入式管理單元(E):
主控台根目錄
憑證 (本機電腦)
編輯延伸(X)...
移除(R)
上移(U)
下移(D)
進階(V)...
描述:
憑證嵌入式管理單元讓您瀏覽電腦或服務的憑證存放區內容。
確定
取消

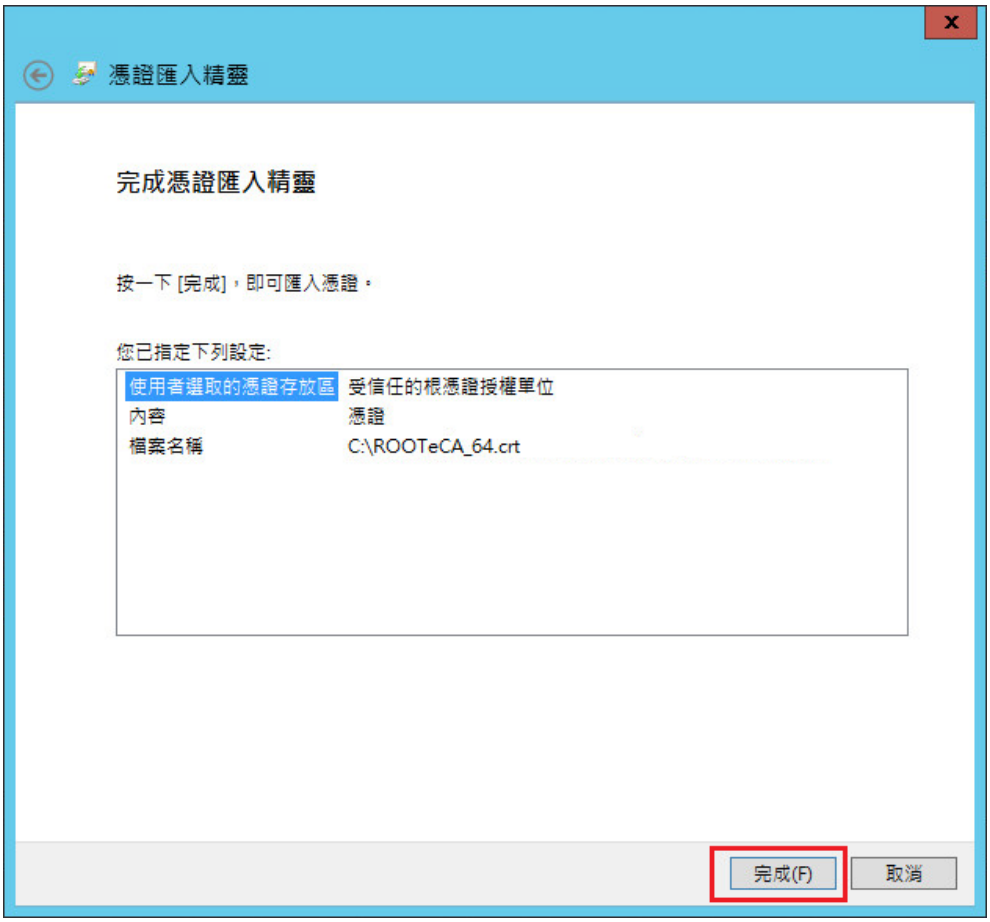
四、 匯入 eCA 根憑證。

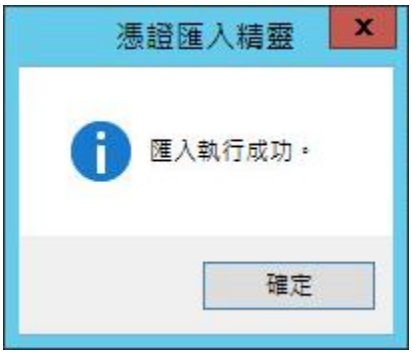

主控台1 - [主控台根目錄\憑證 (本機電腦)\受信任的根憑證授權單位\憑證]
檔案(F) 動作(A) 檢視(V) 我的最愛(O) 視窗(W) 說明(H)
主控台根目錄
憑證 (本機電腦)
個人
受信任的根憑證授權
企業
中繼
受信
沒有
第三
受信
用戶
憑證
智慧
信任的裝置
Web Hosting
發給
簽發者
到期日
Class 3 Public Primary Certific...
Class 3 Public Primary Certificati...
2028/8/2
Class 3 Public Primary Certificati...
2004/1/8
Copyright (c) 1997 Microsoft ...
Copyright (c) 1997 Microsoft C...
1999/12/31
oft Authenticode(tm) Ro...
2000/1/1
oft Root Authority
2020/12/31
Certificate Aut...
Microsoft Root Certificate Auth...
2021/5/10
Certificate Aut...
Microsoft Root Certificate Auth...
2035/6/24
Certificate Aut...
Microsoft Root Certificate Auth...
2036/3/23
CEPTED, (c)9...
NO LIABILITY ACCEPTED, (c)97 ...
2004/1/8
mping CA
Thawte Timestamping CA
2021/1/1
Public Primar...
VeriSign Class 3 Public Primary ...
2036/7/17
所有工作(K)
檢視(V)
從這裡開啟新視窗(W)
新工作台檢視(T)...
重新整理(F)
匯出清單(L)...
說明(H)
匯入(I)...
動作
憑證
其他動作
包含可以在這個項目上執行的動作。

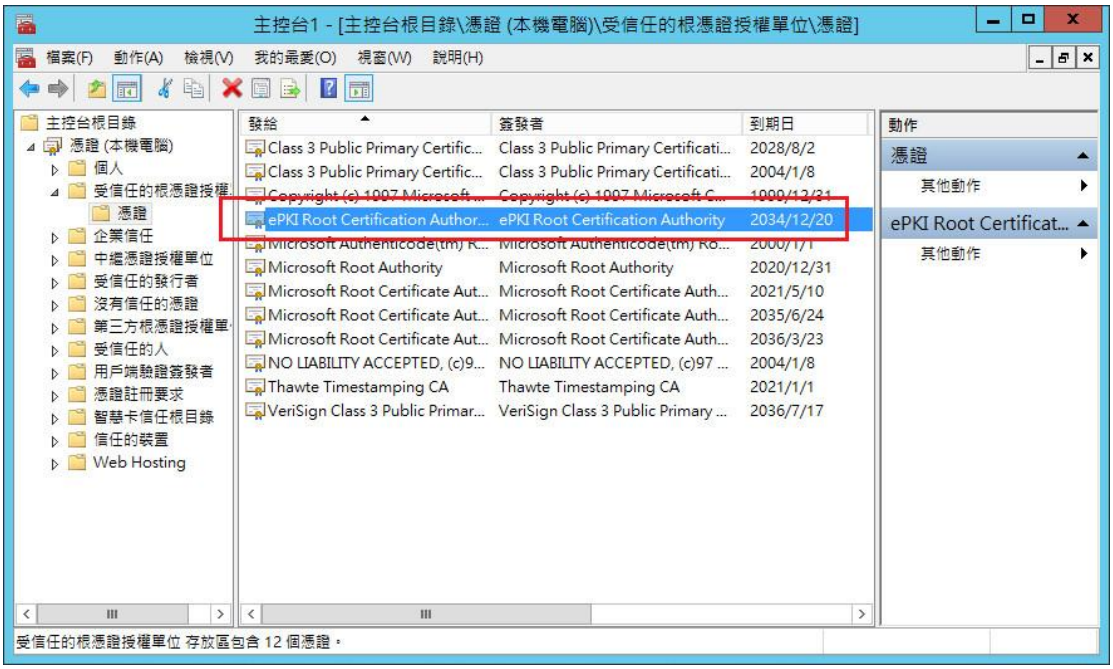

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消


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):
C:\ROOTeCA_64.crt
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)
深入了解憑證檔案格式
下一步(N)
取消

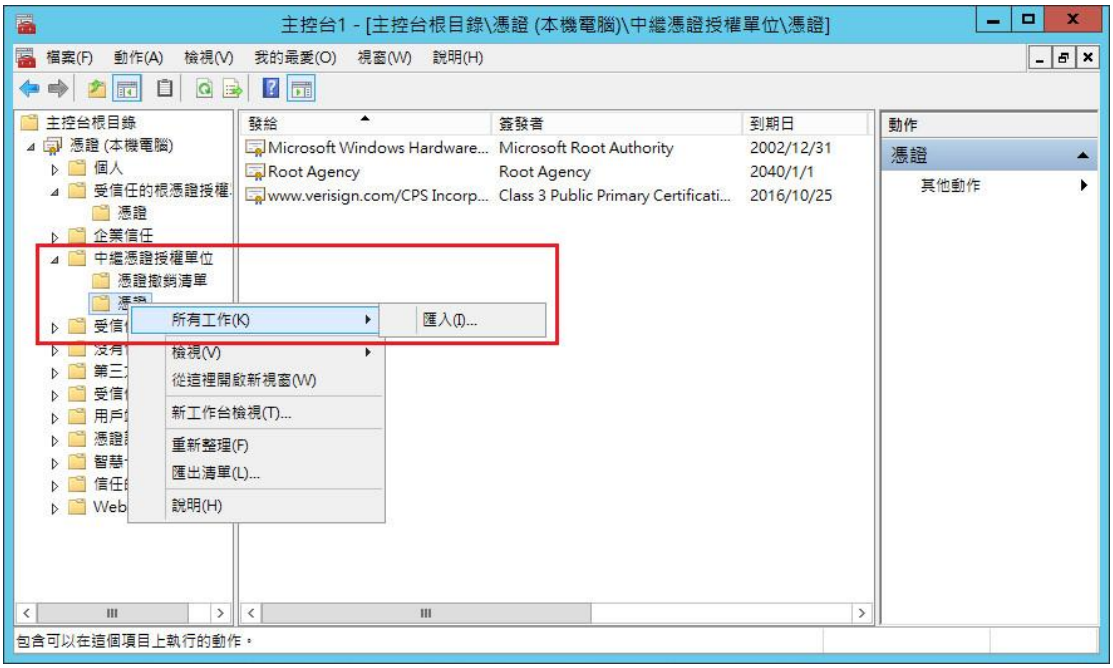

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
受信任的根憑證授權單位
瀏覽(R)...
深入了解憑證存放區
下一步(N)
取消

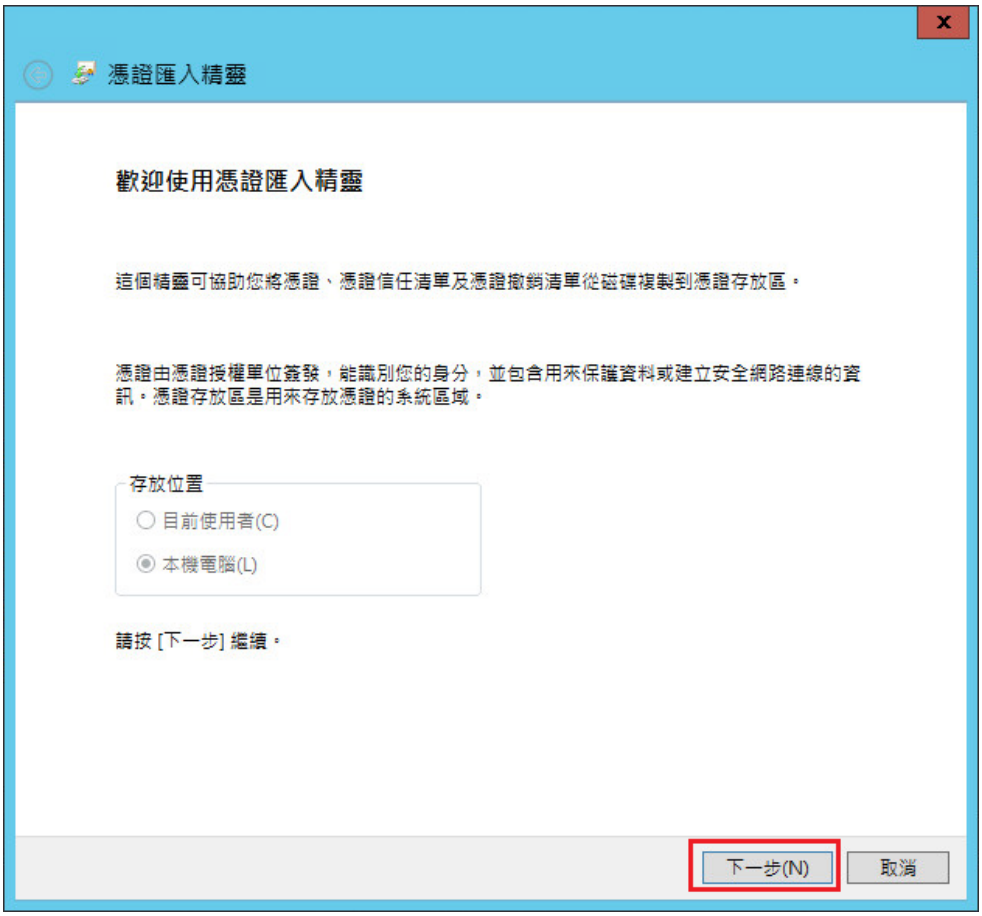

憑證匯入精靈
完成憑證匯入精靈
按一下 [完成]，即可匯入憑證。
你已指定下列設定:
使用者選取的憑證存放區
受信任的根憑證授權單位
內容
憑證
檔案名稱
C:\ROOTeCA_64.crt
完成(F)
取消

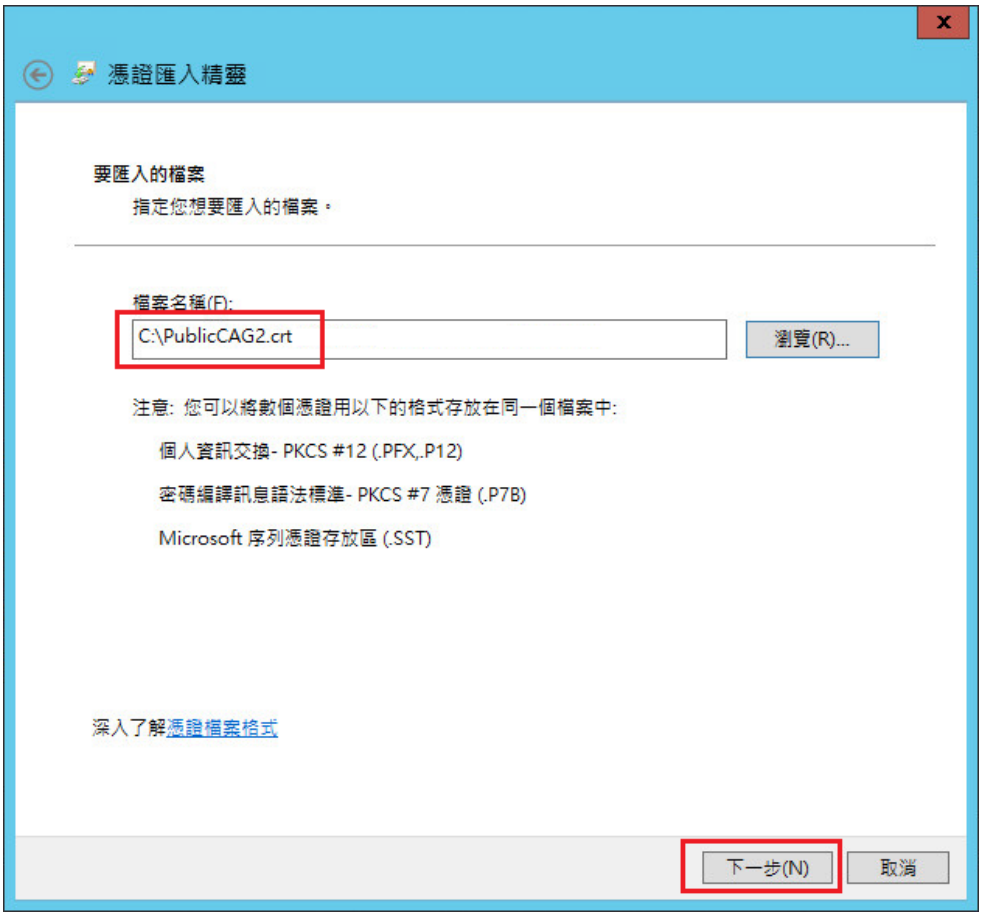

憑證匯入精靈
匯入執行成功。
確定

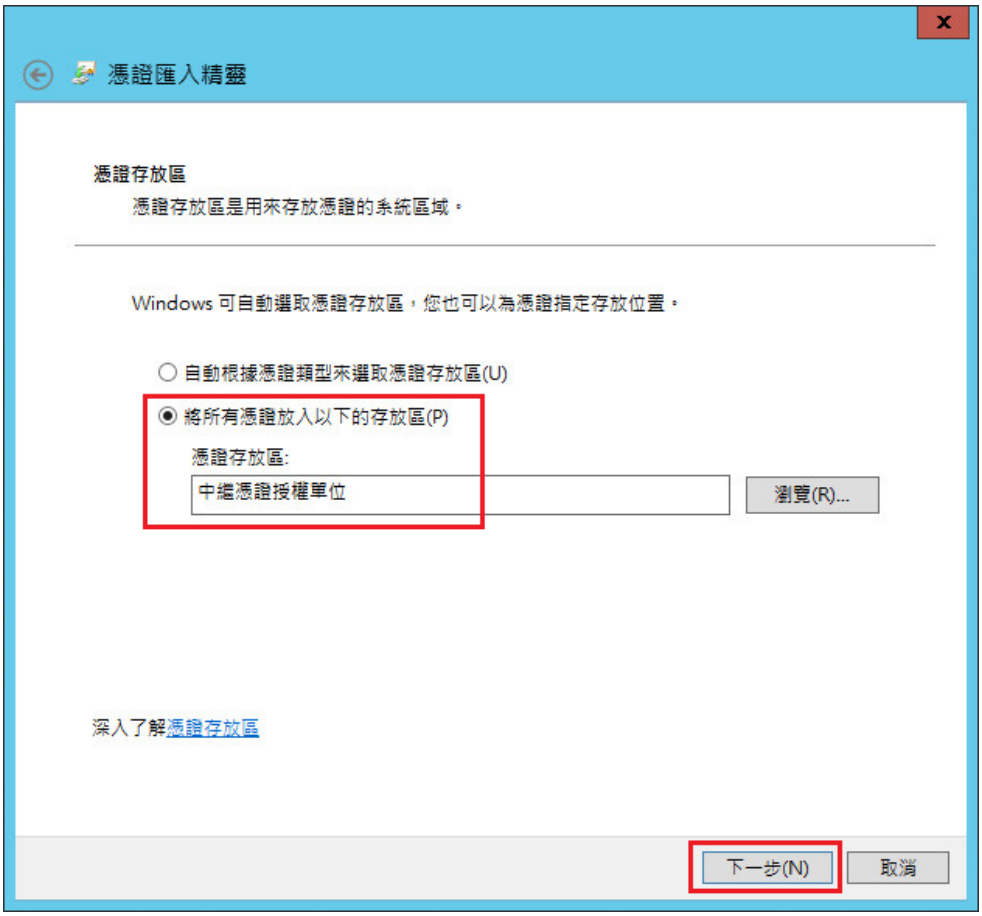


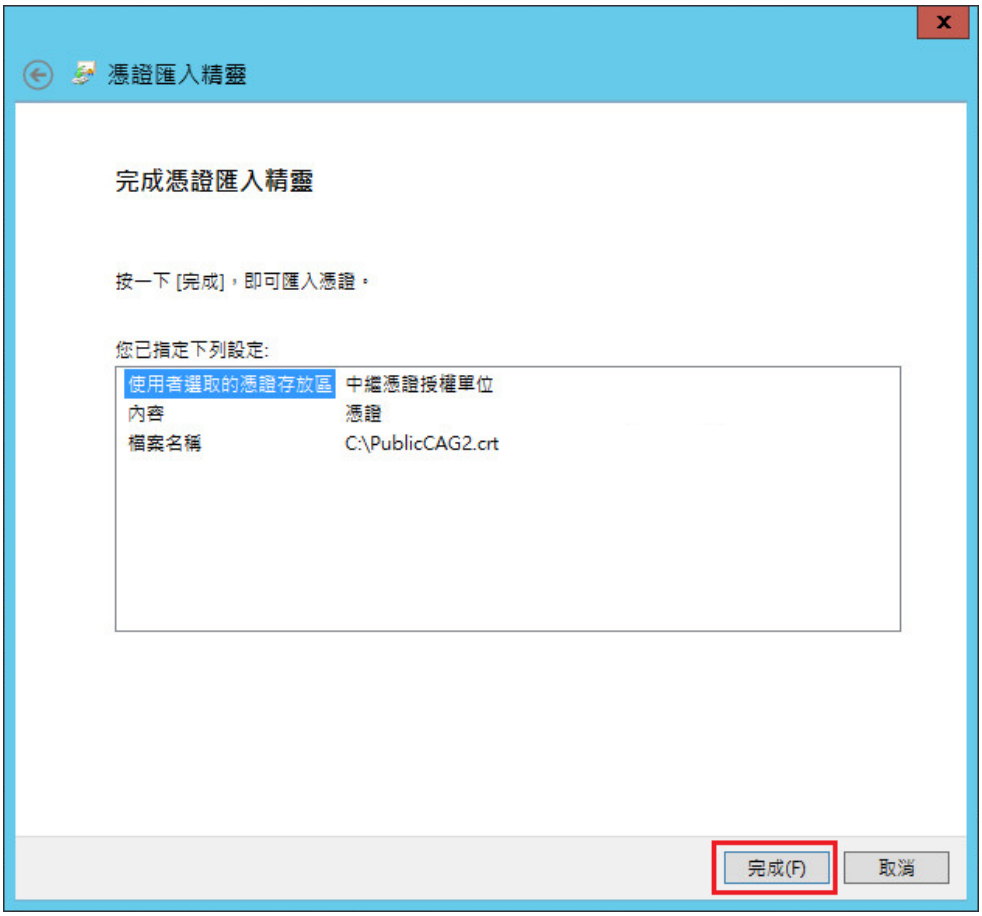
五、 匯入 PublicCAG2 中繼憑證。

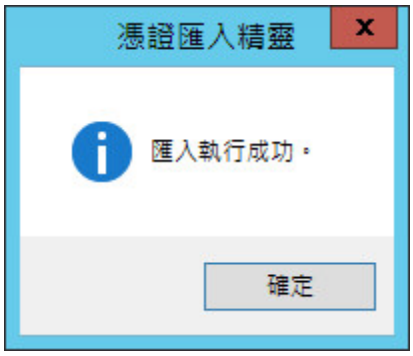


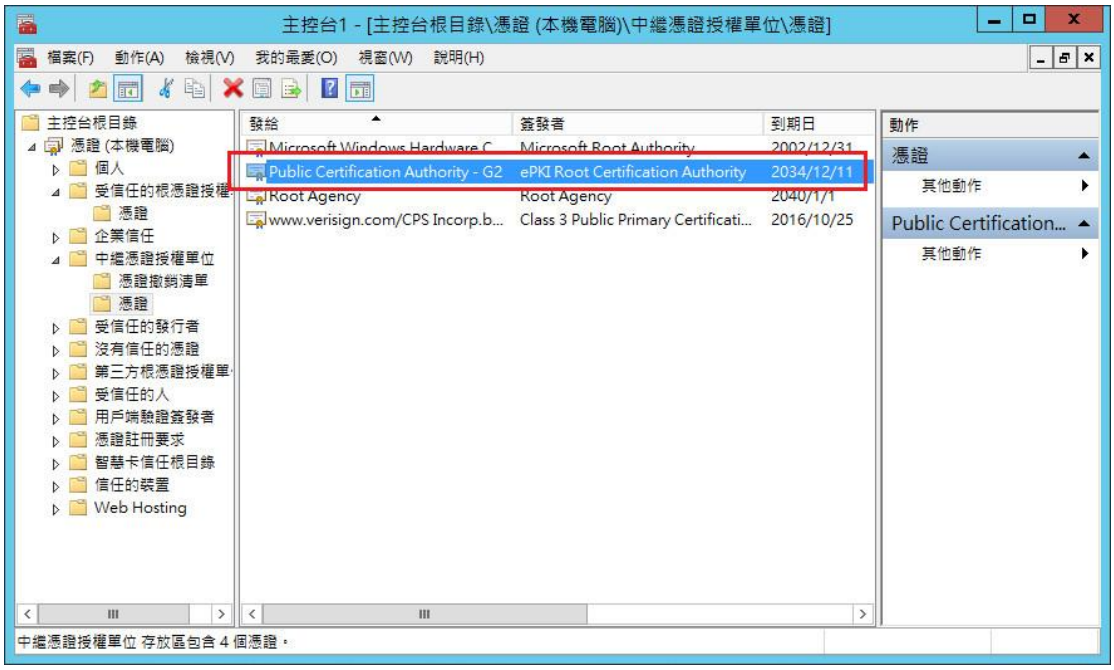

憑證匯入精靈
歡迎使用憑證匯入精靈
這個精靈可協助您將憑證、憑證信任清單及憑證撤銷清單從磁碟複製到憑證存放區。
憑證由憑證授權單位簽發，能識別您的身分，並包含用來保護資料或建立安全網路連線的資訊。憑證存放區是用來存放憑證的系統區域。
存放位置
目前使用者(C)
本機電腦(L)
請按 [下一步] 繼續。
下一步(N)
取消


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):
C:\PublicCAG2.crt
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)
深入了解憑證檔案格式
下一步(N)
取消

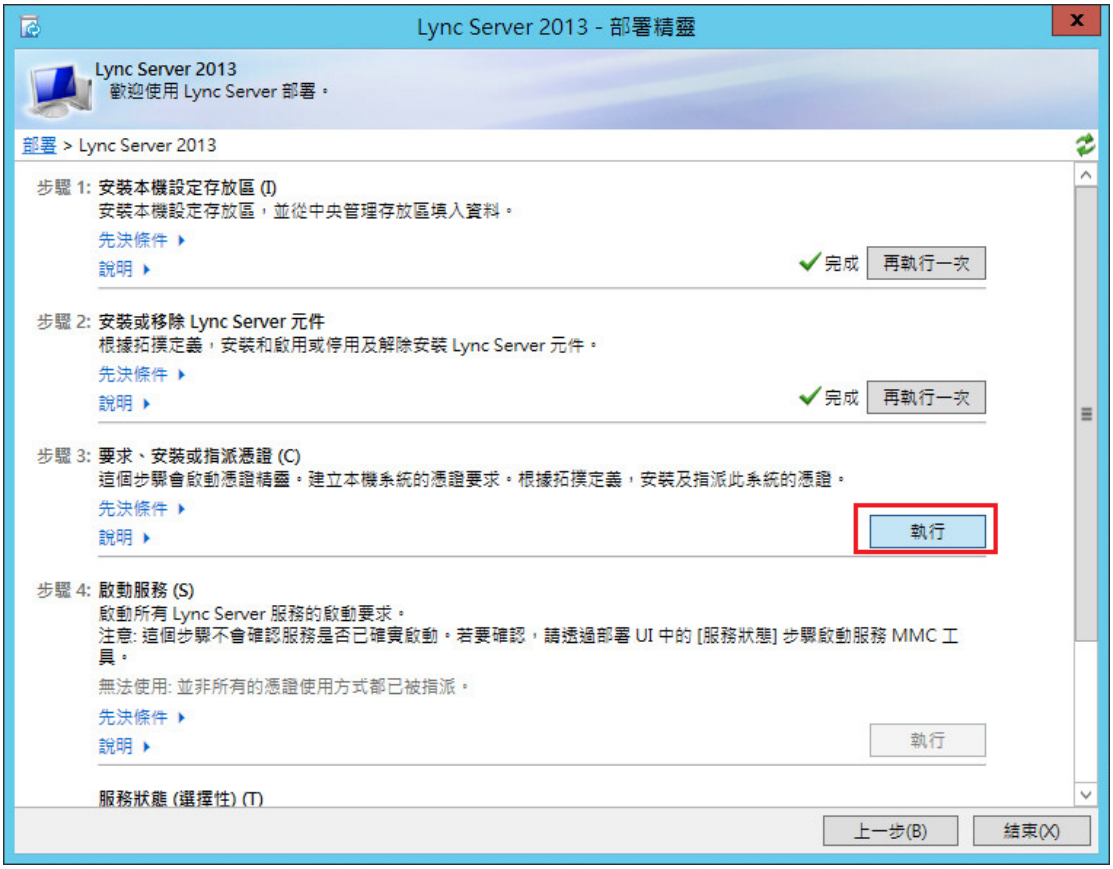

憑證匯入精靈
憑證存放區
憑證存放區是用來存放憑證的系統區域。
Windows 可自動選取憑證存放區，您也可以為憑證指定存放位置。
自動根據憑證類型來選取憑證存放區(U)
將所有憑證放入以下的存放區(P)
憑證存放區:
中繼憑證授權單位
瀏覽(R)...
深入了解憑證存放區
下一步(N)
取消


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 中繼憑證授權單位
內容 憑證
檔案名稱 C:\PublicCAG2.crt
完成(F)
取消

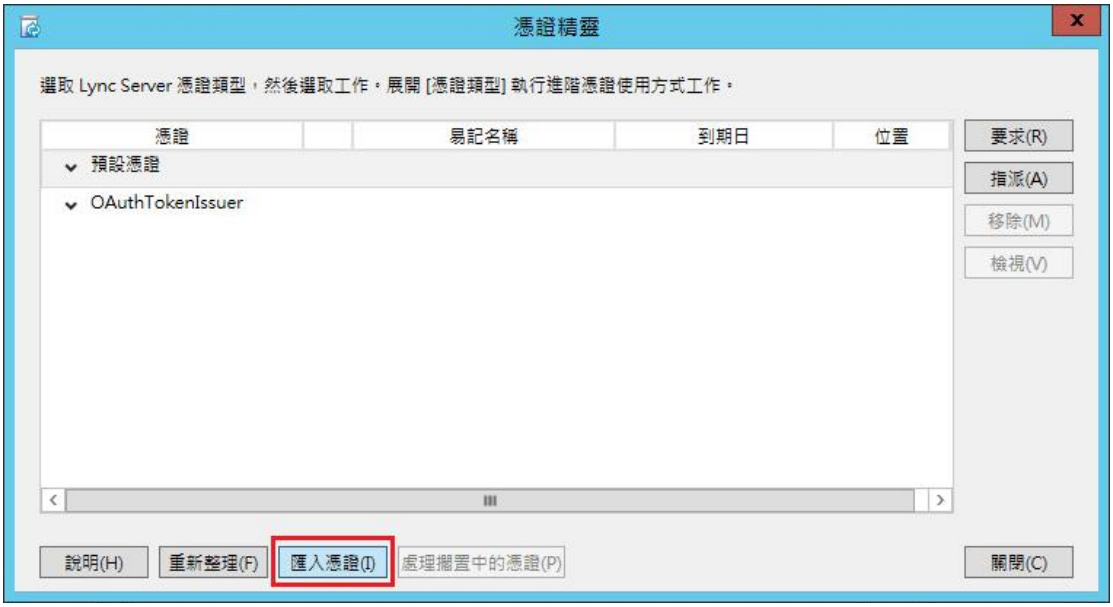


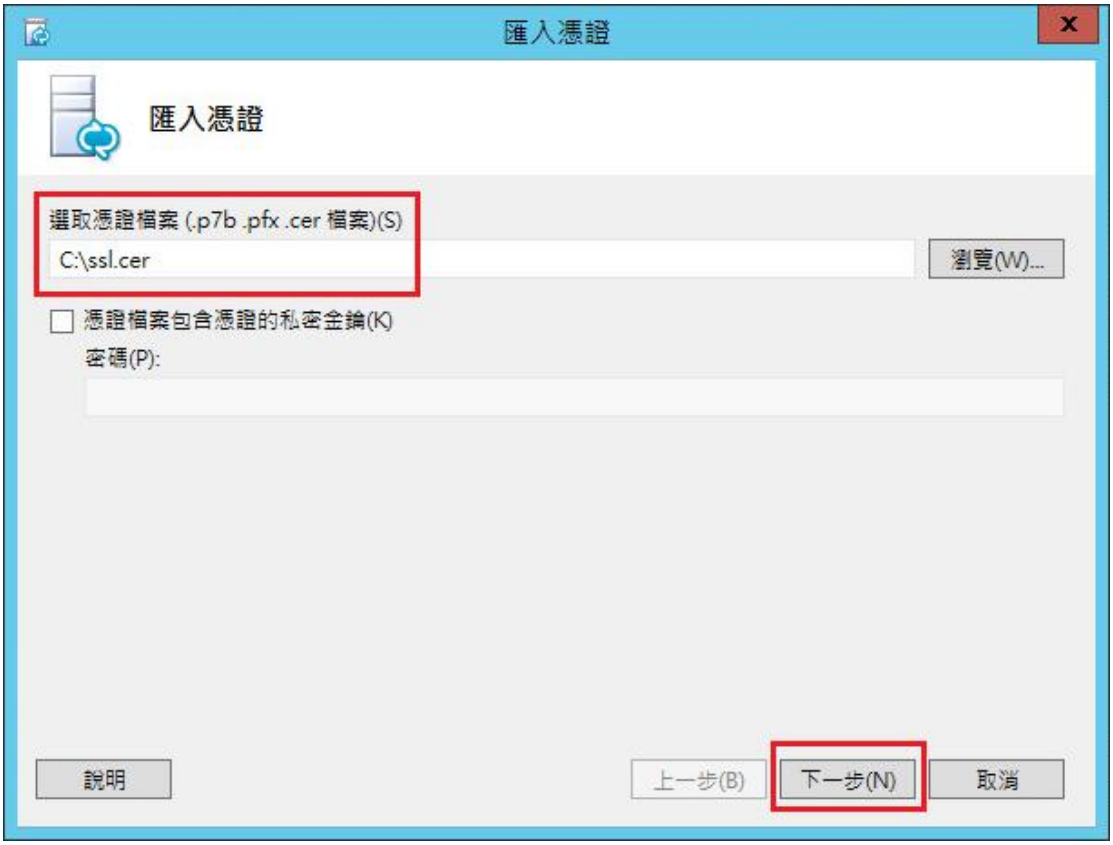


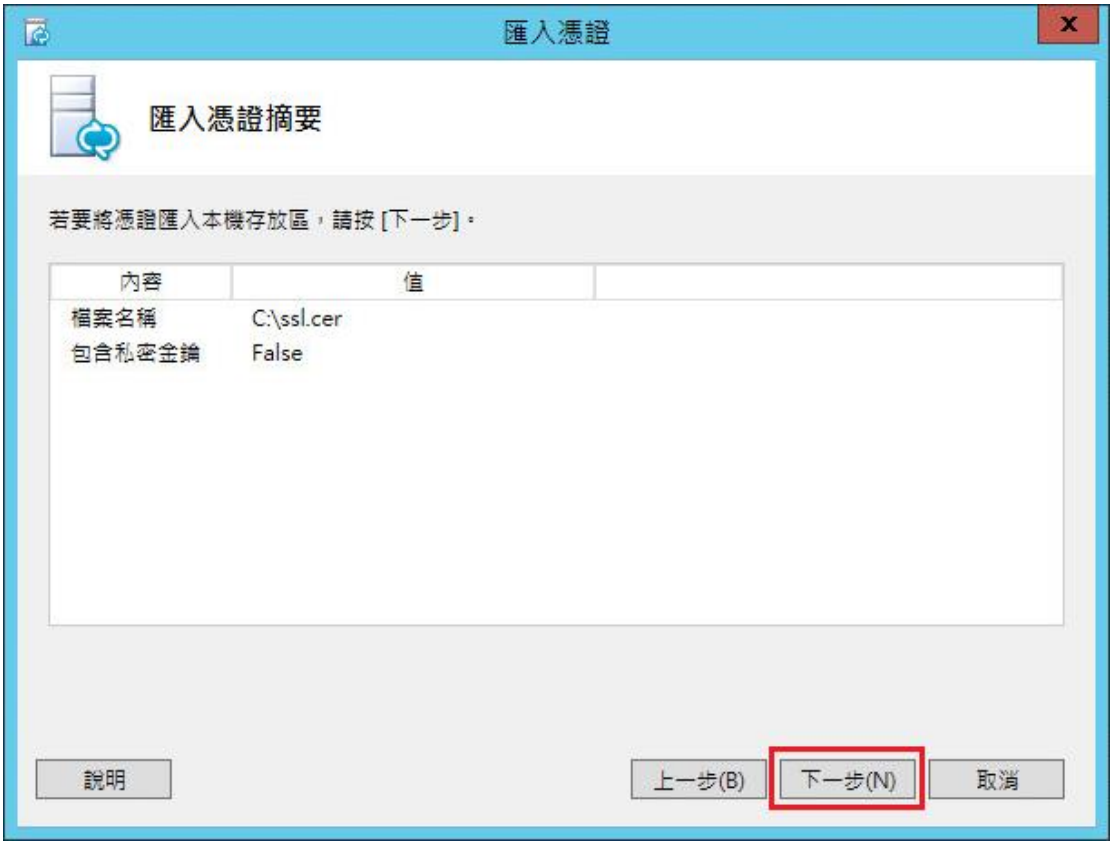
六、 開啟「Lync Server 部屬精靈」至下圖位置，並點選「執行」。

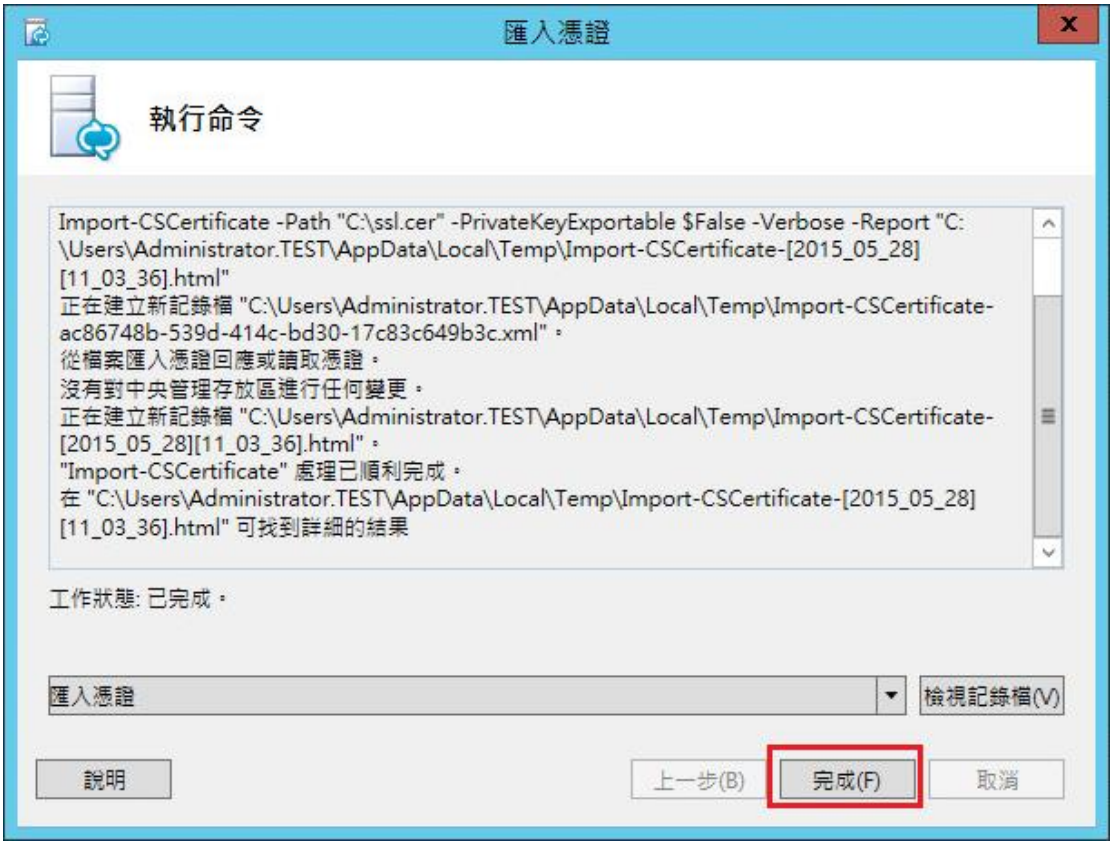


七、 匯入用戶端 SSL 憑證。(檔名為 32 個英數字所組成，範例檔名為 ssl.cer)

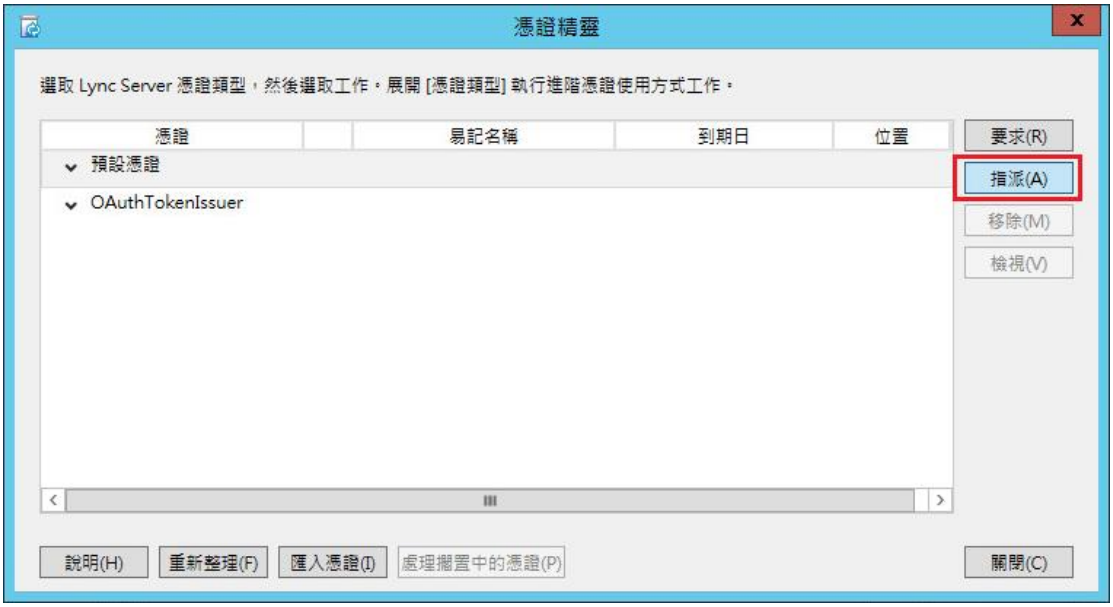


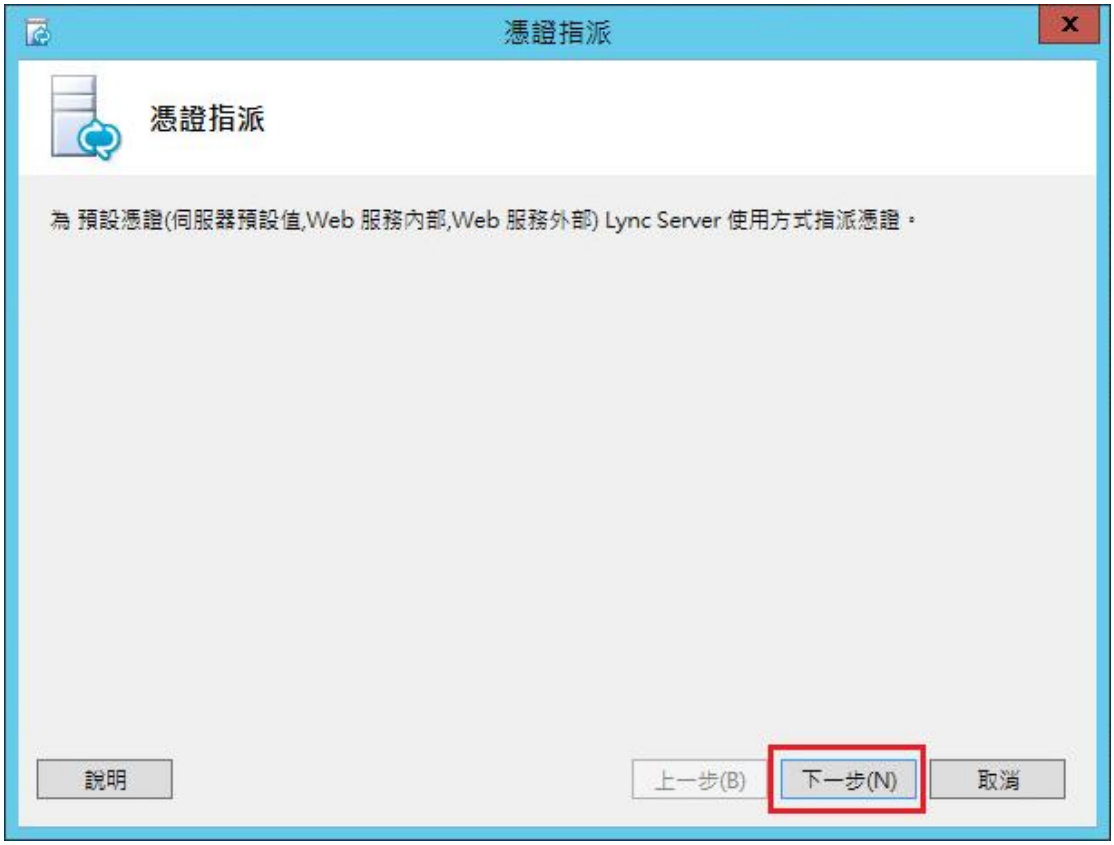

匯入憑證
匯入憑證
選取憑證檔案 (.p7b .pfx .cer 檔案)(S)
C:\ssl.cer
瀏覽(W)...
憑證檔案包含憑證的私密金鑰(K)
密碼(P):
說明
上一步(B)
下一步(N)
取消

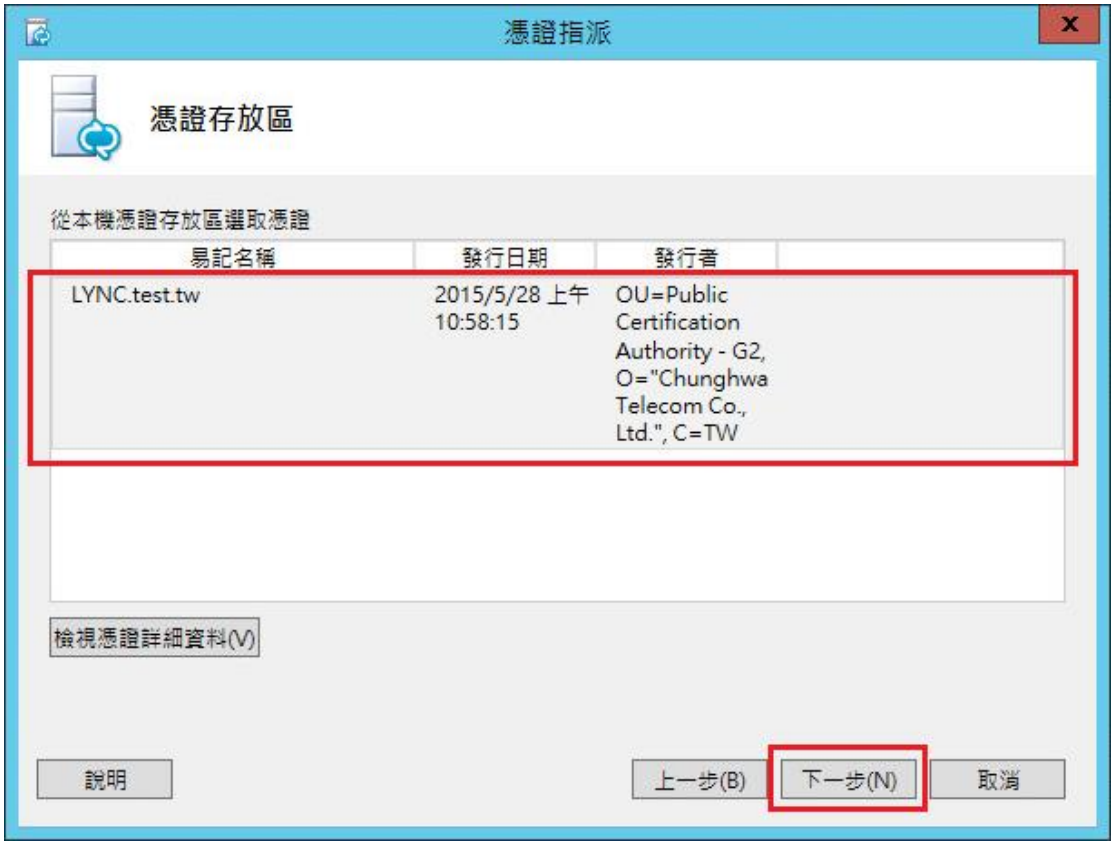

匯入憑證
匯入憑證摘要
若要將憑證匯入本機存放區，請按 [下一步]。
內容
值
檔案名稱
C:\ssl.cer
包含私密金鑰
False
說明
上一步(B)
下一步(N)
取消

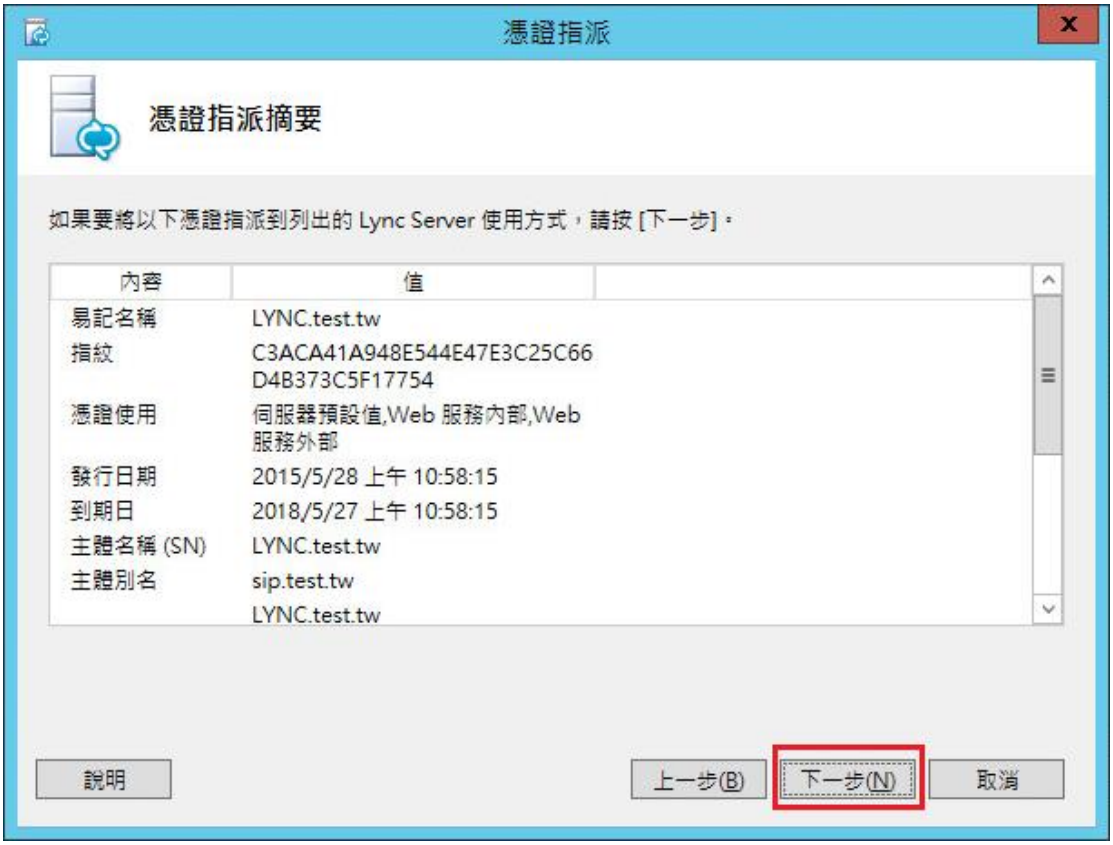

匯入憑證
執行命令
Import-CSCertificate -Path "C:\ssl.cer" -PrivateKeyExportable $False -Verbose -Report "C:\Users\Administrator.TEST\AppData\Local\Temp\Import-CSCertificate-[2015_05_28][11_03_36].html"
正在建立新記錄檔 "C:\Users\Administrator.TEST\AppData\Local\Temp\Import-CSCertificate-ac86748b-539d-414c-bd30-17c83c649b3c.xml"。
從檔案匯入憑證回應或讀取憑證。
沒有對中央管理存放區進行任何變更。
正在建立新記錄檔 "C:\Users\Administrator.TEST\AppData\Local\Temp\Import-CSCertificate-[2015_05_28][11_03_36].html"。
"Import-CSCertificate" 處理已順利完成。
在 "C:\Users\Administrator.TEST\AppData\Local\Temp\Import-CSCertificate-[2015_05_28][11_03_36].html" 可找到詳細的結果
工作狀態: 已完成。
匯入憑證
檢視記錄檔(V)
說明
上一步(B)
完成(F)
取消

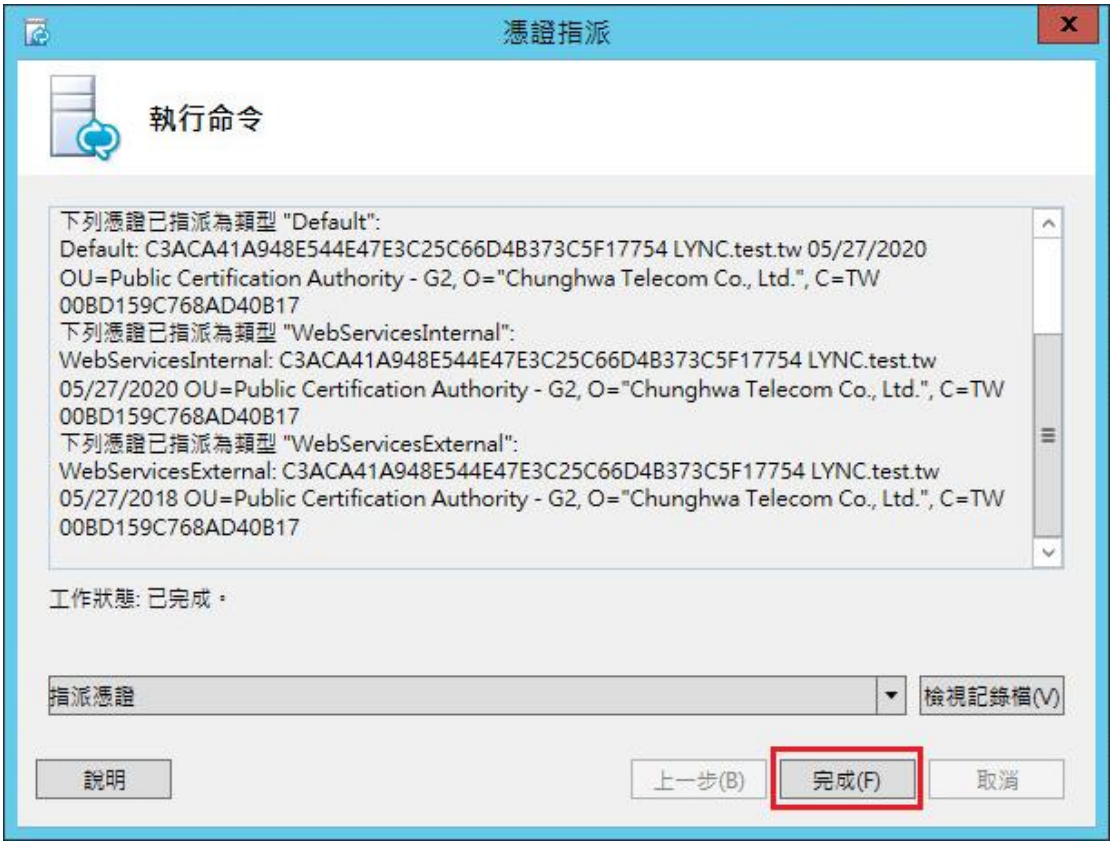
八、 指派 SSL 憑證。

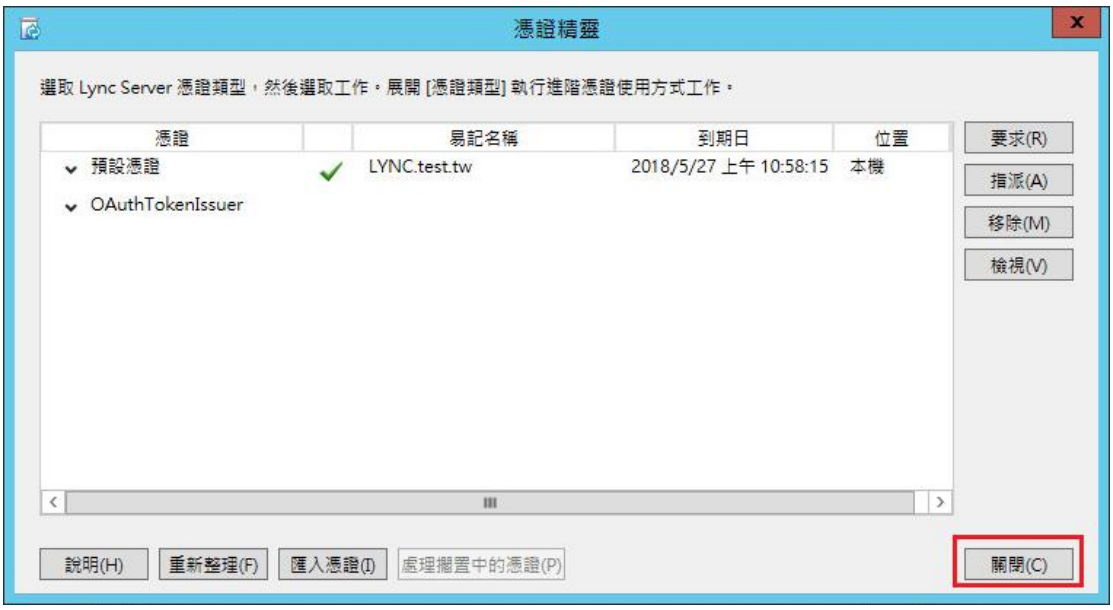

憑證精靈
選取 Lync Server 憑證類型，然後選取工作。展開 [憑證類型] 執行進階憑證使用方式工作。
憑證
易記名稱
到期日
位置
預設憑證
OAuthTokenIssuer
要求(R)
指派(A)
移除(M)
檢視(V)
說明(H)
重新整理(F)
匯入憑證(I)
處理擱置中的憑證(P)
關閉(C)


憑證指派
憑證指派
為 預設憑證(伺服器預設值,Web 服務內部,Web 服務外部) Lync Server 使用方式指派憑證。
說明
上一步(B)
下一步(N)
取消

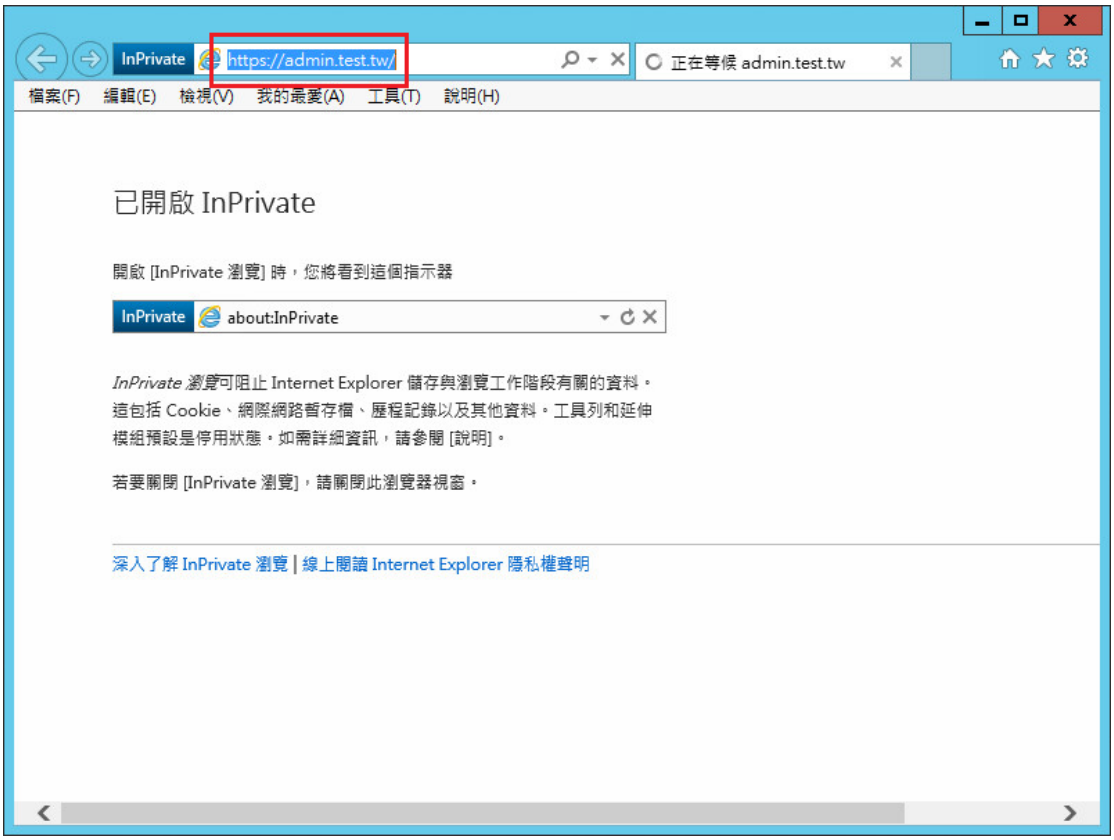

憑證指派
憑證存放區
從本機憑證存放區選取憑證
易記名稱
發行日期
發行者
LYNC.test.tw
2015/5/28 上午 10:58:15
OU=Public Certification Authority - G2, O="Chunghwa Telecom Co., Ltd.", C=TW
檢視憑證詳細資料(V)
說明
上一步(B)
下一步(N)
取消


憑證指派
憑證指派摘要
如果要將以下憑證指派到列出的 Lync Server 使用方式，請按 [下一步]。
內容
值
易記名稱
LYNC.test.tw
指紋
C3ACA41A948E544E47E3C25C66 D4B373C5F17754
憑證使用
伺服器預設值,Web 服務內部,Web 服務外部
發行日期
2015/5/28 上午 10:58:15
到期日
2018/5/27 上午 10:58:15
主體名稱 (SN)
LYNC.test.tw
主體別名
sip.test.tw
LYNC.test.tw
說明
上一步(B)
下一步(N)
取消

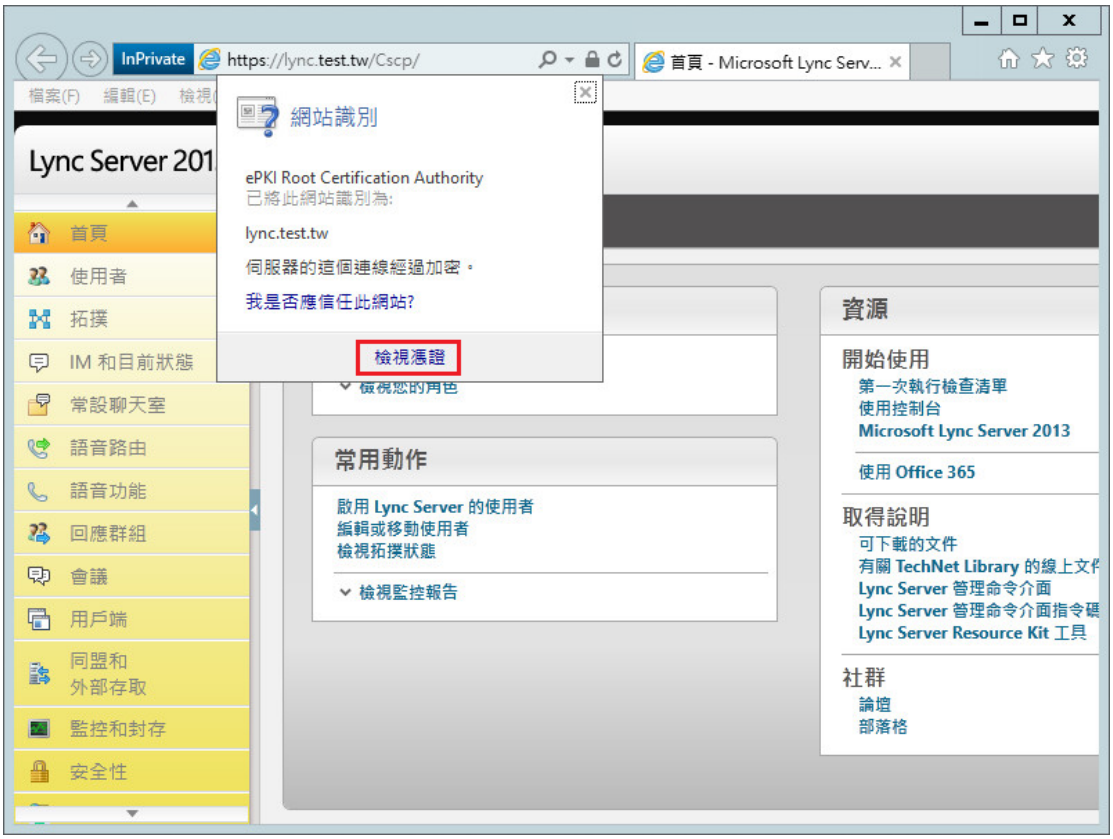

憑證指派
執行命令
下列憑證已指派為類型 "Default":
Default: C3ACA41A948E544E47E3C25C66D4B373C5F17754 LYNC.test.tw 05/27/2020 OU=Public Certification Authority - G2, O="Chunghwa Telecom Co., Ltd.", C=TW 00BD159C768AD40B17
下列憑證已指派為類型 "WebServicesInternal":
WebServicesInternal: C3ACA41A948E544E47E3C25C66D4B373C5F17754 LYNC.test.tw 05/27/2020 OU=Public Certification Authority - G2, O="Chunghwa Telecom Co., Ltd.", C=TW 00BD159C768AD40B17
下列憑證已指派為類型 "WebServicesExternal":
WebServicesExternal: C3ACA41A948E544E47E3C25C66D4B373C5F17754 LYNC.test.tw 05/27/2018 OU=Public Certification Authority - G2, O="Chunghwa Telecom Co., Ltd.", C=TW 00BD159C768AD40B17
工作狀態: 已完成。
指派憑證
檢視記錄檔(V)
說明
上一步(B)
完成(F)
取消

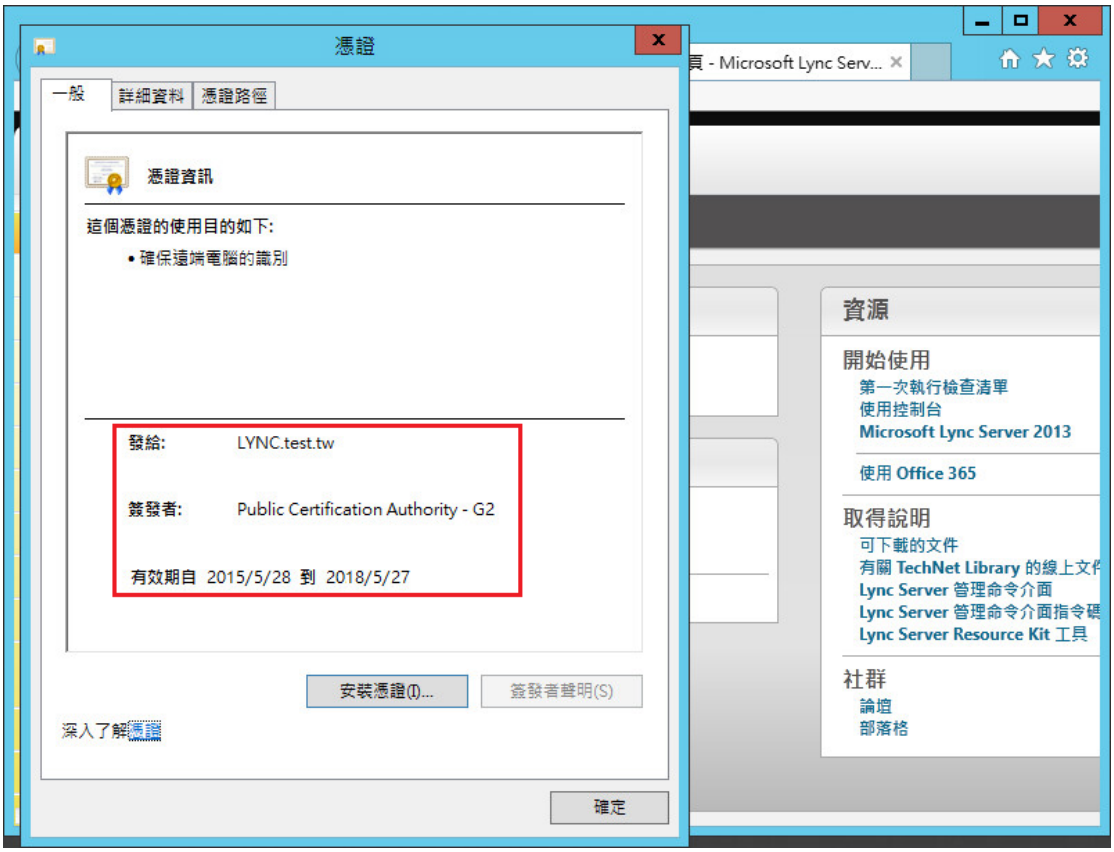


九、 憑證全部指派完成，且啟動服務後，可以透過瀏覽器驗證 HTTPS 是否正常。(範例以系統管理存取 URL 測試 HTTPS 服務)


InPrivate
https://admin.test.tw/
正在等候 admin.test.tw
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
已開啟 InPrivate
開啟 [InPrivate 瀏覽] 時，您將看到這個指示器
InPrivate about:InPrivate
InPrivate 瀏覽可阻止 Internet Explorer 儲存與瀏覽工作階段有關的資料。這包括 Cookie、網際網路暫存檔、歷程記錄以及其他資料。工具列和延伸模組預設是停用狀態。如需詳細資訊，請參閱 [說明]。
若要關閉 [InPrivate 瀏覽]，請關閉此瀏覽器視窗。
深入了解 InPrivate 瀏覽 | 線上閱讀 Internet Explorer 隱私權聲明


InPrivate
https://lync.test.tw/Cscp/
首頁 - Microsoft Lync Serv...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
Lync Server 2013
首頁
使用者
拓撲
IM 和目前狀態
常設聊天室
語音路由
語音功能
回應群組
會議
用戶端
同盟和外部存取
監控和封存
安全性
使用者資訊
歡迎使用，Administrator
檢視您的角色
常用動作
啟用 Lync Server 的使用者
編輯或移動使用者
檢視拓撲狀態
檢視監控報告
資源
開始使用
第一次執行檢查清單
使用控制台
Microsoft Lync Server 2013
使用 Office 365
取得說明
可下載的文件
有關 TechNet Library 的線上文件
Lync Server 管理命令介面
Lync Server 管理命令介面指令碼
Lync Server Resource Kit 工具
社群
論壇
部落格





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。您也可參考 http://publicca.hinet.net/SSL-01.htm 下方有 SSL 安全認證標章之安裝說明。

請中華電信公司負責維護網站的同仁，參考從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。