

中華電信通用憑證管理中心(PublicCA)

Windows Exchange 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。

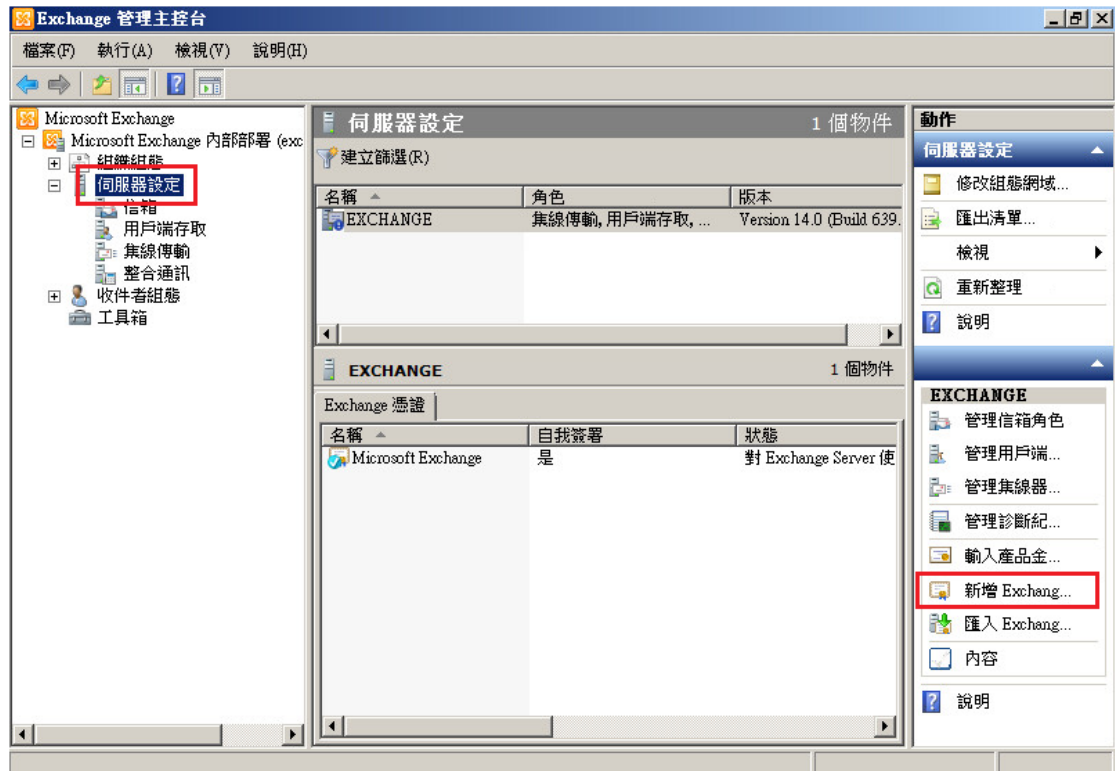
本說明書的申請程序，已經在 Windows Server 2008 R2 + Exchange Server 2010 測試過，您所使用的版本或環境可能與本版本有所差異，若是如此，則請參考您的 Exchange 相關使用手冊，適度調整申請步驟。

目錄


Windows Exchange SSL 憑證請求檔製作手冊.....	2
Windows Exchange SSL 憑證安裝操作手冊.....	9
附件一：萬用網域憑證安裝操作手冊.....	28

Windows Exchange SSL 憑證請求檔製作手冊

- 一、 開啟「Exchange 管理主控台」→點選「伺服器設定」→「新增 Exchange 憑證」。



- 二、 輸入一個好記的名稱後，點選「下一步」。


 **新增 Exchange 憑證**

- 簡介
- 網域範圍
- 憑證設定
- 完成

簡介
此嚮導將協助您判斷應用程式正常運作所需的憑證類型。
繼續之前，建議您先閱讀[這些文件](#)，瞭解有關 Exchange Server 服務和憑證需求。

輸入憑證的易記名稱(E):

三、 可點選啟用萬用字元

 **新增 Exchange 憑證**

- 簡介
- 網域範圍
- 憑證設定
- 完成

網域範圍
若要使用萬用字元自動將此憑證套用至所有子網域，請在下面輸入父網域名稱。
若稍後要新增子網域但不想更新現有憑證，此功能非常實用。

啟用萬用字元憑證(E)
根網域萬用字元 (例如 contoso.com 或 *.contoso.com)(D):

或是不啟用萬用字元

新增 Exchange 憑證

- 簡介
- 網域範圍**
- 憑證設定
- 完成

網域範圍
若要使用萬用字元自動將此憑證套用至所有子網域，請在下面輸入父系網域名稱。若稍後要新增子網域但不想更新現有憑證，此功能非常實用。

啟用萬用字元憑證 (E)
根網域萬用字元 (例如 contoso.com 或 *.contoso.com)(D):

說明(H) < 上一步(B) **下一步(N) >** 取消

新增 Exchange 憑證

- 簡介
- 網域範圍
- Exchange 組態**
- 憑證網域
- 憑證設定
- 完成

Exchange 組態
使用此頁面來描述您的 Microsoft Exchange 組態和網域資訊。如果嚮導未自動提供這項資訊，請自行輸入。

同盟共用

用戶端存取伺服器 (Outlook Web App)

- Outlook Web App 位於內部網路上
用於內部存取 Outlook Web App 的網域名稱:
- Outlook Web App 位於網際網路上
用於存取 Outlook Web App 的網域名稱 (範例: mail.contoso.com):

用戶端存取伺服器 (Exchange ActiveSync)

- 已啟用 Exchange Active Sync
用於存取 Exchange ActiveSync 的網域名稱 (範例: mail.contoso.com):

用戶端存取伺服器 (Web 服務、Outlook Anywhere 和自動探索)

- Exchange Web 服務已啟用
- Outlook Anywhere 已啟用

組織的外部主機名稱 (範例: mail.contoso.com):

說明(H) 重試(T) < 上一步(B) **下一步(N) >** 取消

新增 Exchange 憑證

簡介
 網域範圍
 Exchange 組態
 憑證網域
 憑證設定
 完成

Exchange 組態
 使用此頁面來描述您的 Microsoft Exchange 組態和網域資訊。如果嚮導未自動提供這項資訊，請自行輸入。

mail.test.tw

用戶端存取伺服器 (Web 服務、Outlook Anywhere 和自動探索)

Exchange Web 服務已啟用
 Outlook Anywhere 已啟用

組織的外部主機名稱 (範例: mail.contoso.com):
 mail.test.tw,test.tw

自動探索服務可使用長格式 (例如: autodiscover.contoso.com) 或短格式 (例如: contoso.com) 的 URL。請指定使用長格式或短格式的 URL。

內部網路上使用的自動探索
 網際網路上使用的自動探索

長 URL (範例: autodiscover.contoso.com)
 簡短的 URL (範例: contoso.com)
 另一個格式的 URL (範例: 使用 DNS SRV 方法時)

輸入您要使用的自動探索 URL:
 autodiscover.test.tw

用戶端存取伺服器 (POP/IMAP)

內部網路使用 POP/IMAP
 網際網路使用 POP/IMAP

說明(H) 重試(T) < 上一步(B) 下一步(N) > 取消

新增 Exchange 憑證

簡介
 網域範圍
 Exchange 組態
 憑證網域
 憑證設定
 完成

Exchange 組態
 使用此頁面來描述您的 Microsoft Exchange 組態和網域資訊。如果嚮導未自動提供這項資訊，請自行輸入。

網際網路上使用的自動探索

長 URL (範例: autodiscover.contoso.com)
 簡短的 URL (範例: contoso.com)
 另一個格式的 URL (範例: 使用 DNS SRV 方法時)

輸入您要使用的自動探索 URL:
 autodiscover.test.tw

用戶端存取伺服器 (POP/IMAP)

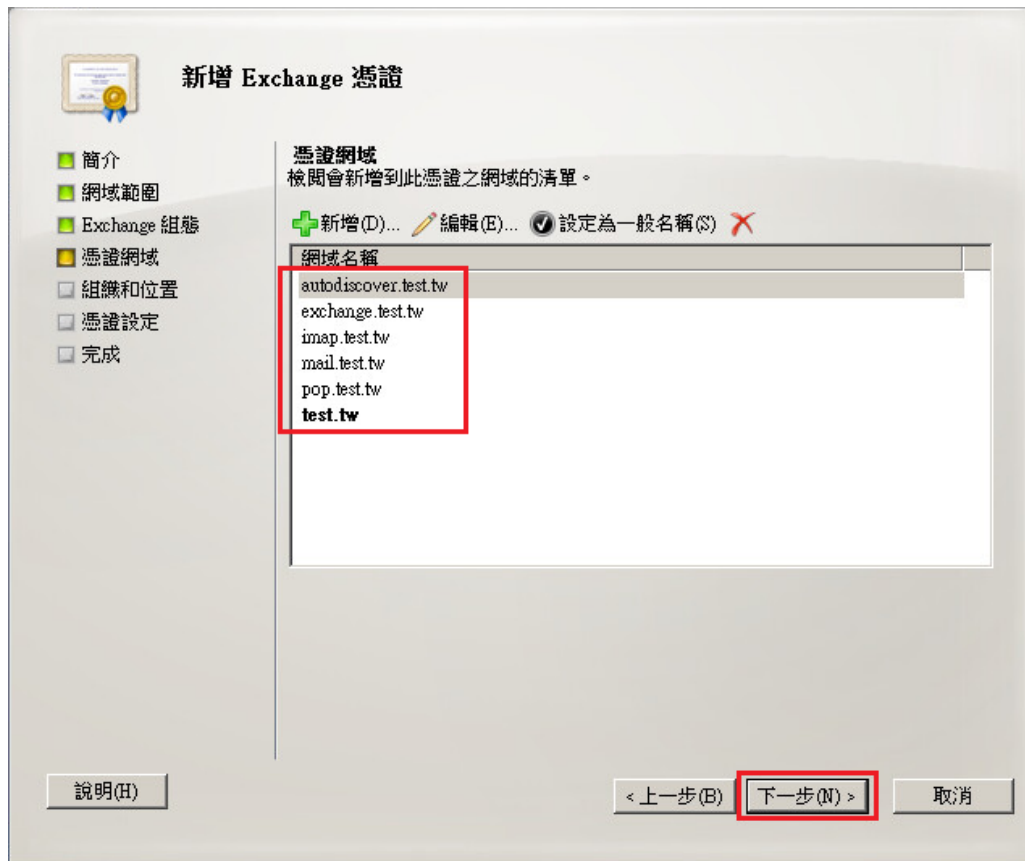
內部網路使用 POP/IMAP
 網際網路使用 POP/IMAP

用於 POP 的網域名稱 (範例: pop.contoso.com):
 pop.test.tw

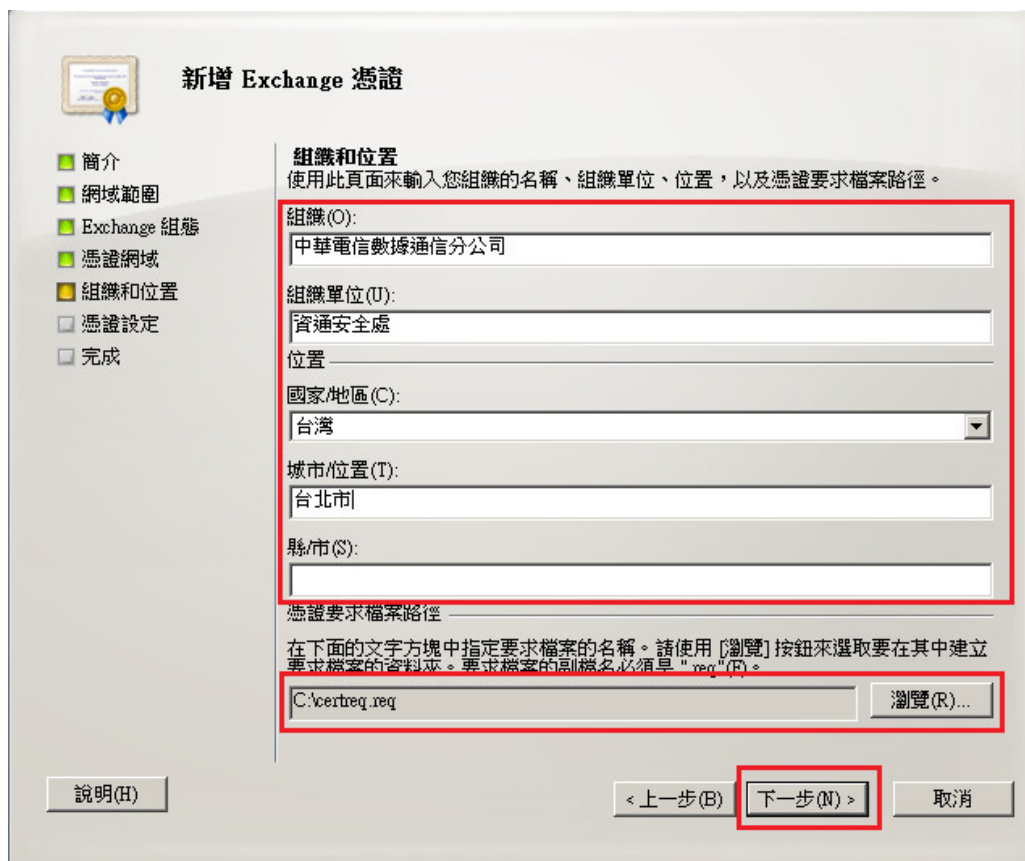
用於 IMAP 的網域名稱 (範例: imap.contoso.com):
 imap.test.tw

整合通訊伺服器
 集線傳輸伺服器
 傳統 Exchange Server

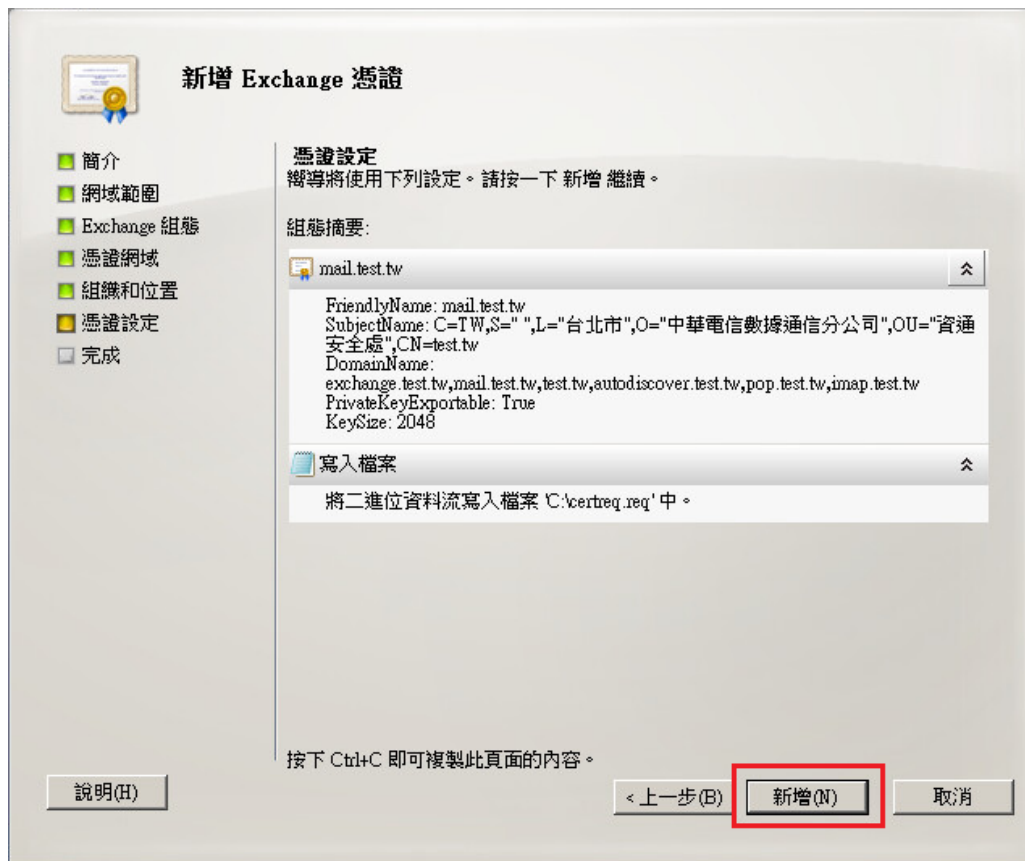
說明(H) 重試(T) < 上一步(B) 下一步(N) > 取消



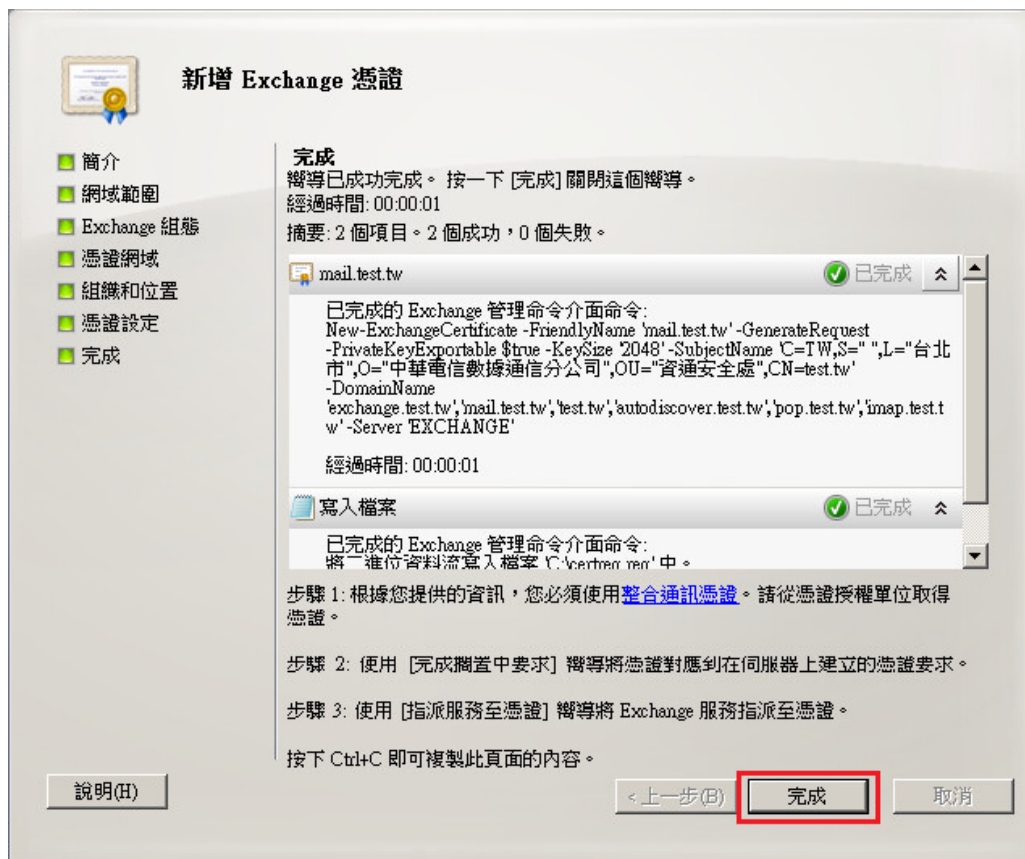
- 四、 輸入組織相關資訊。縣/市(S)若無請輸入空白。
選擇憑證請求檔儲存位置後，點選「下一步」。



五、 確認資訊無誤後，點選「新增」。



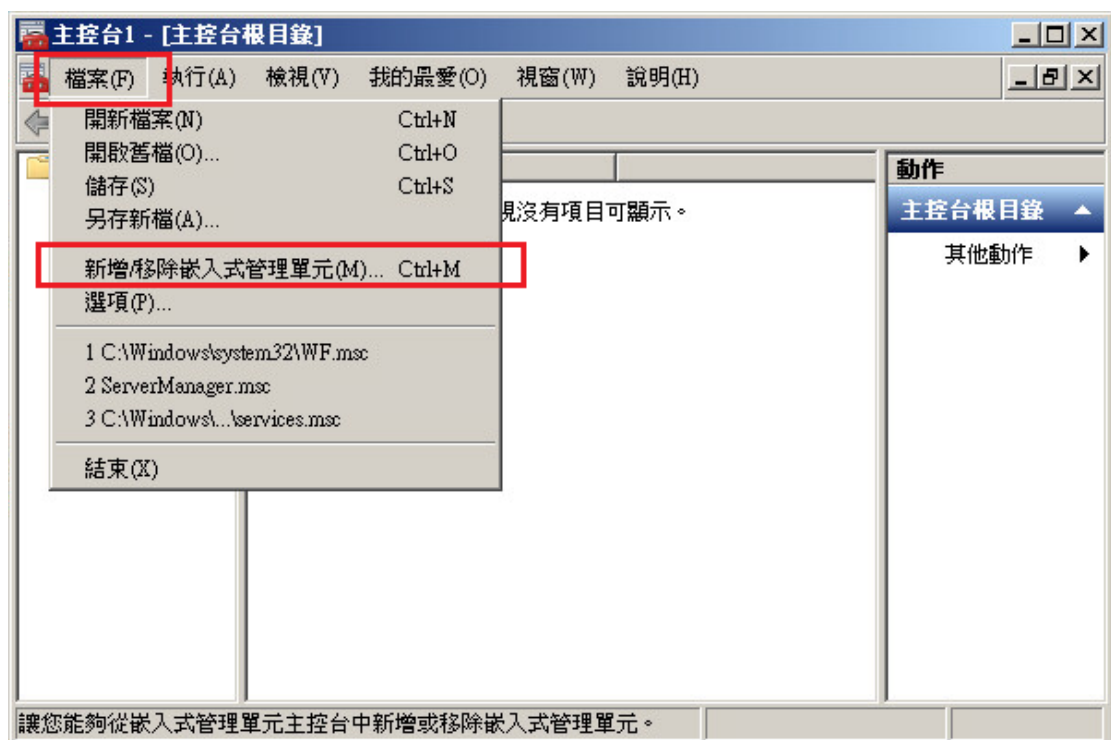
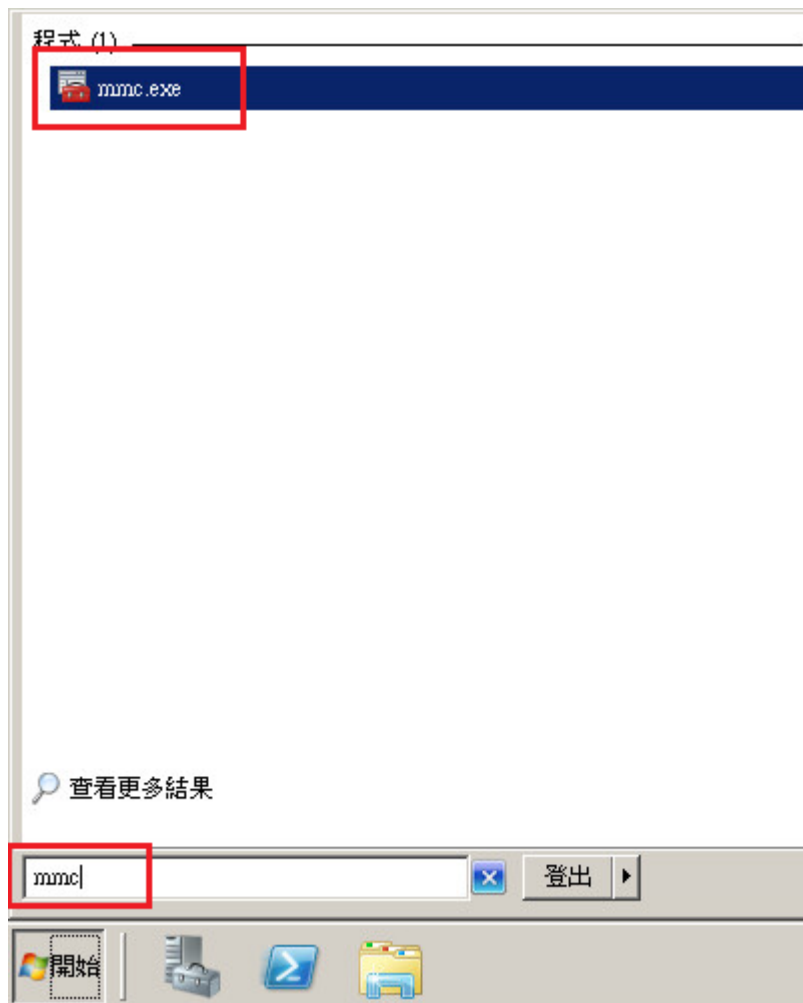
六、 點選「完成」。

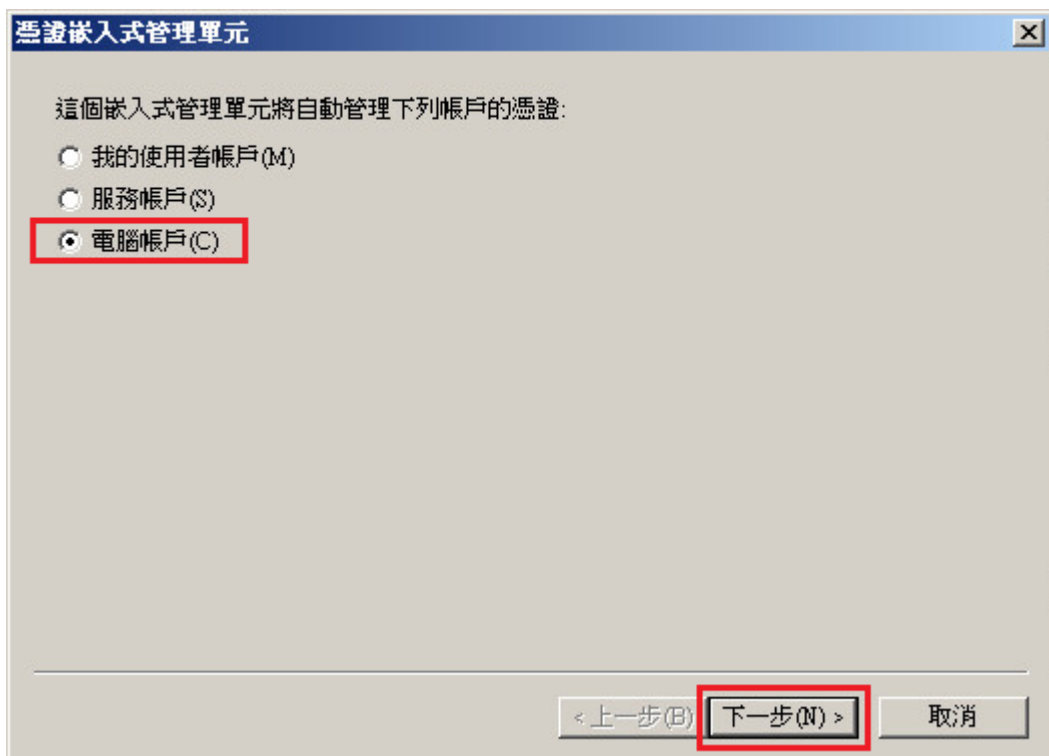
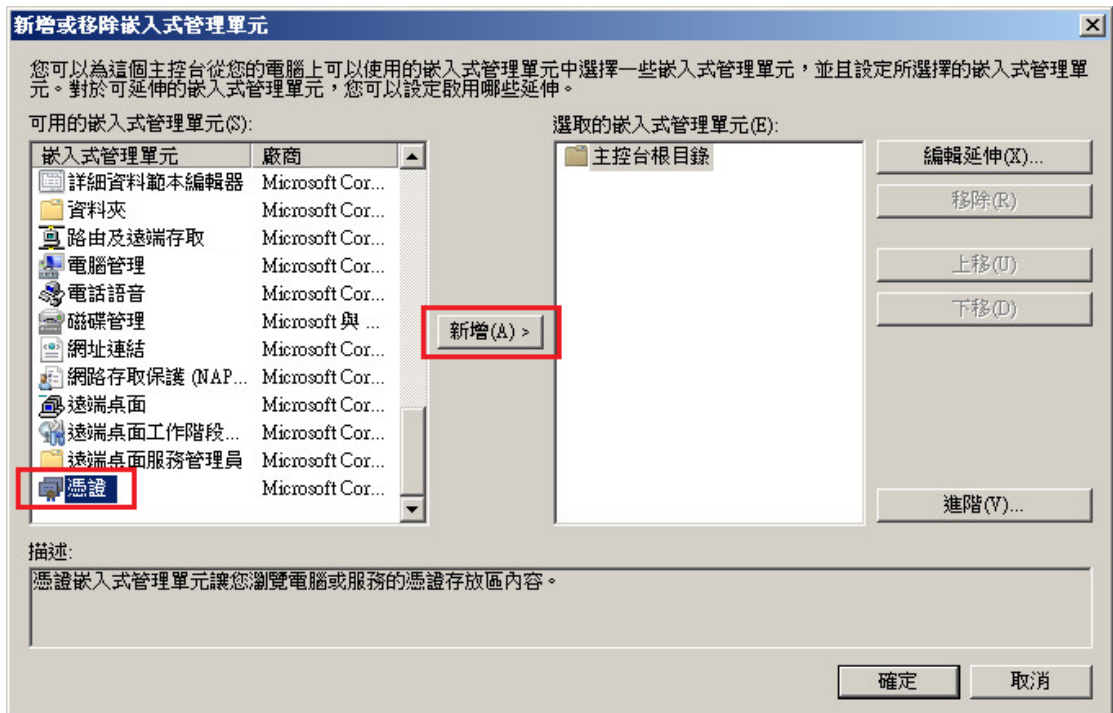


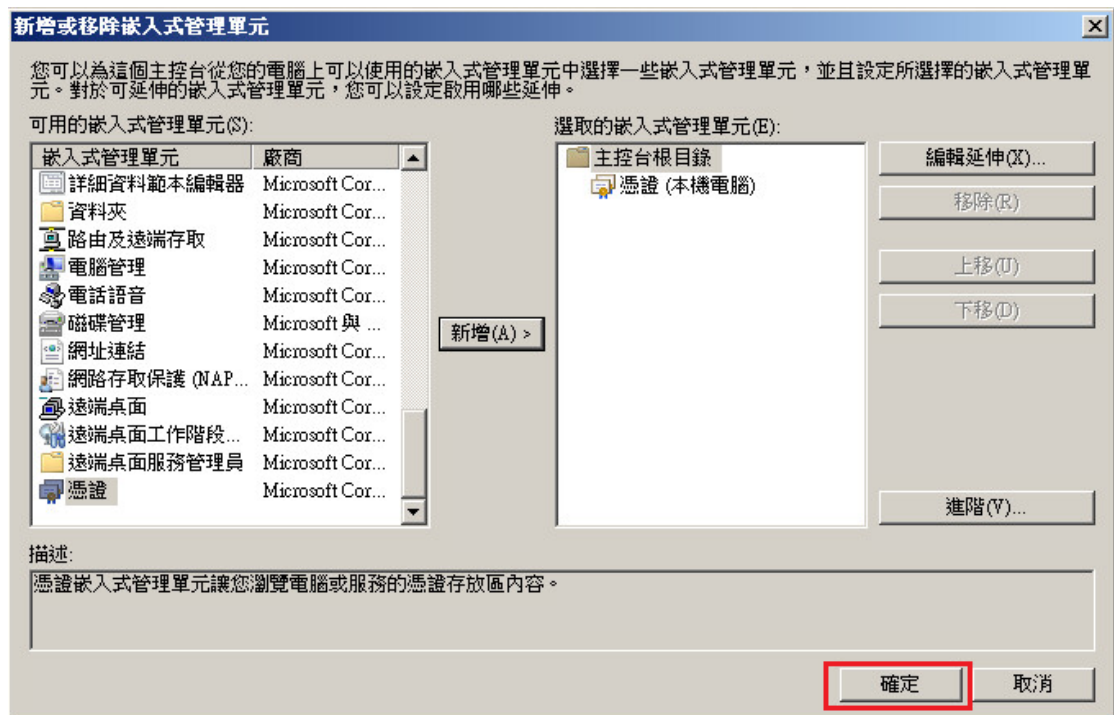
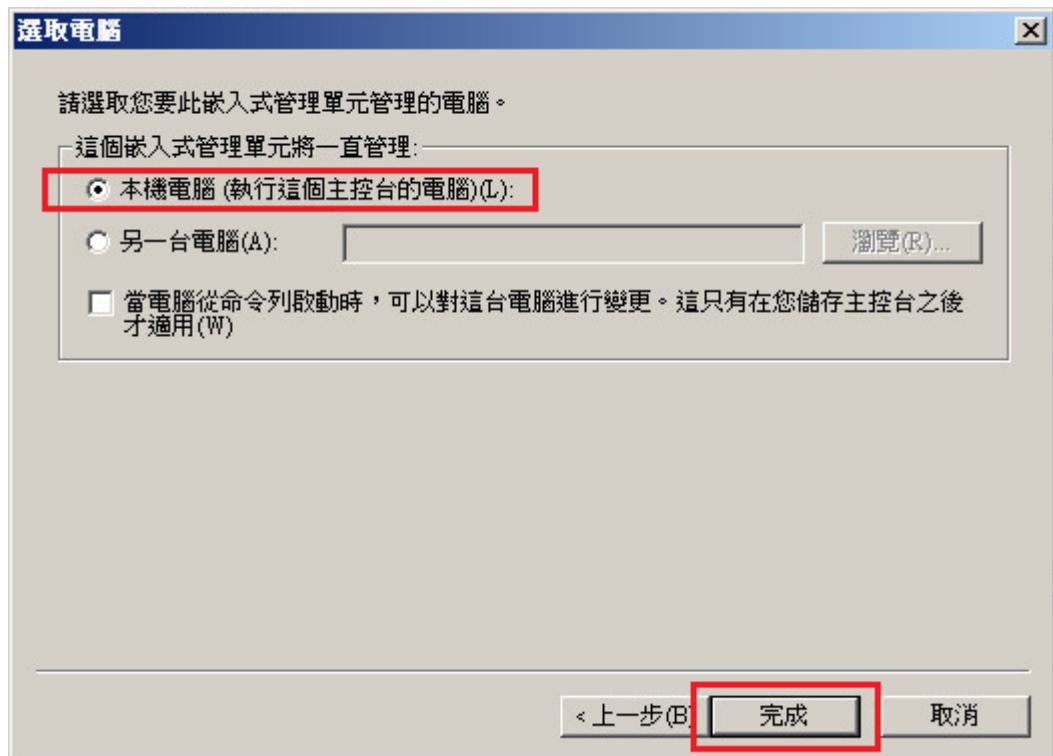
- 七、 此時憑證請求檔(certreq.txt)製作完成，使用憑證請求檔至中華電信通用憑證管理中心網站 (<http://publicca.hinet.net/>) 依照網頁說明申請 SSL 憑證 (以文字編輯器如記事本開啟憑證請求檔，全選及複製檔案內容，將憑證請求檔貼上 SSL 憑證申請網頁之表單。)。若屬於中華電信公司各單位申請 SSL 憑證者，請從企業入口網站電子表單之資訊表單 IS14-伺服器應用軟體憑證申請/異動單提出申請。
- 八、 補充說明 1: 中華電信通用憑證管理中心之程式會擷取憑證請求檔中的公開金鑰，但不會使用憑證請求檔中於步驟四所輸入之資訊，而是以於申請網頁上所填入的組織資訊為準而記載於所簽發的 SSL 憑證裡面的欄位[如憑證主體名稱(Subject Name)欄位]。
- 九、 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，憑證管理中心審驗客戶之身分與網域名稱擁有權或控制權後，所簽發的憑證會包含客戶之組織身分、完全吻合網域名稱與公開金鑰在憑證內。後續先安裝 SSL 憑證串鏈在產生憑證請求檔之站台，再將私密金鑰與憑證備份匯入其他站台，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)

Windows Exchange SSL 憑證安裝操作手冊

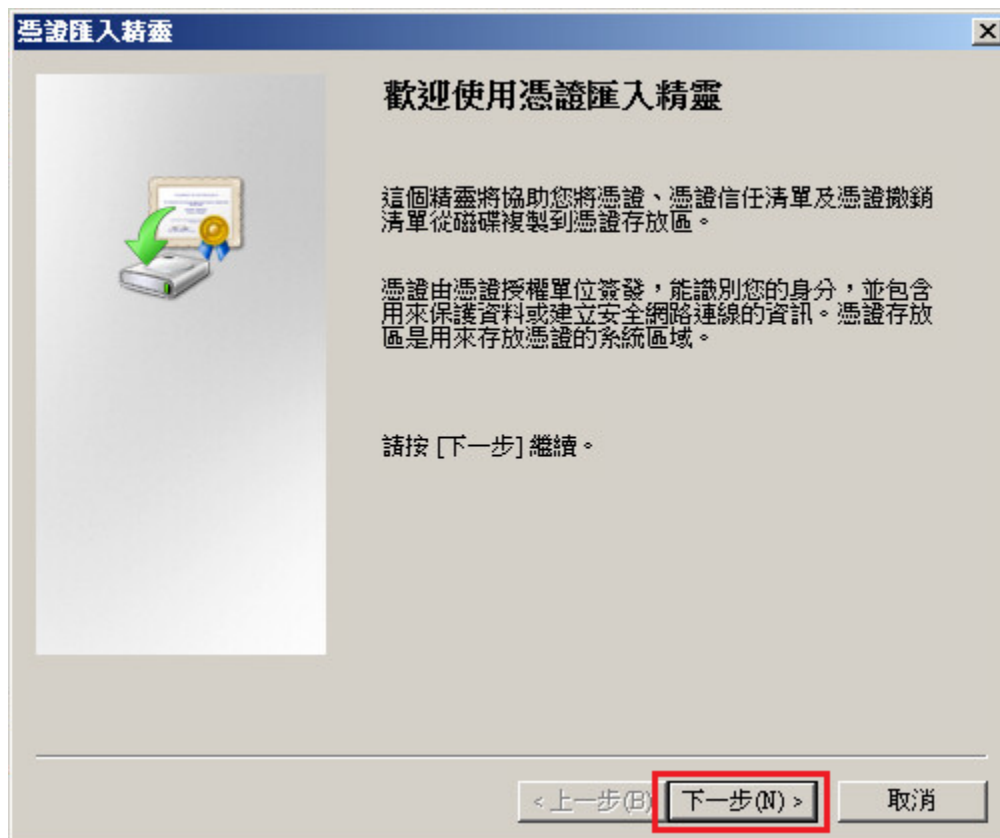
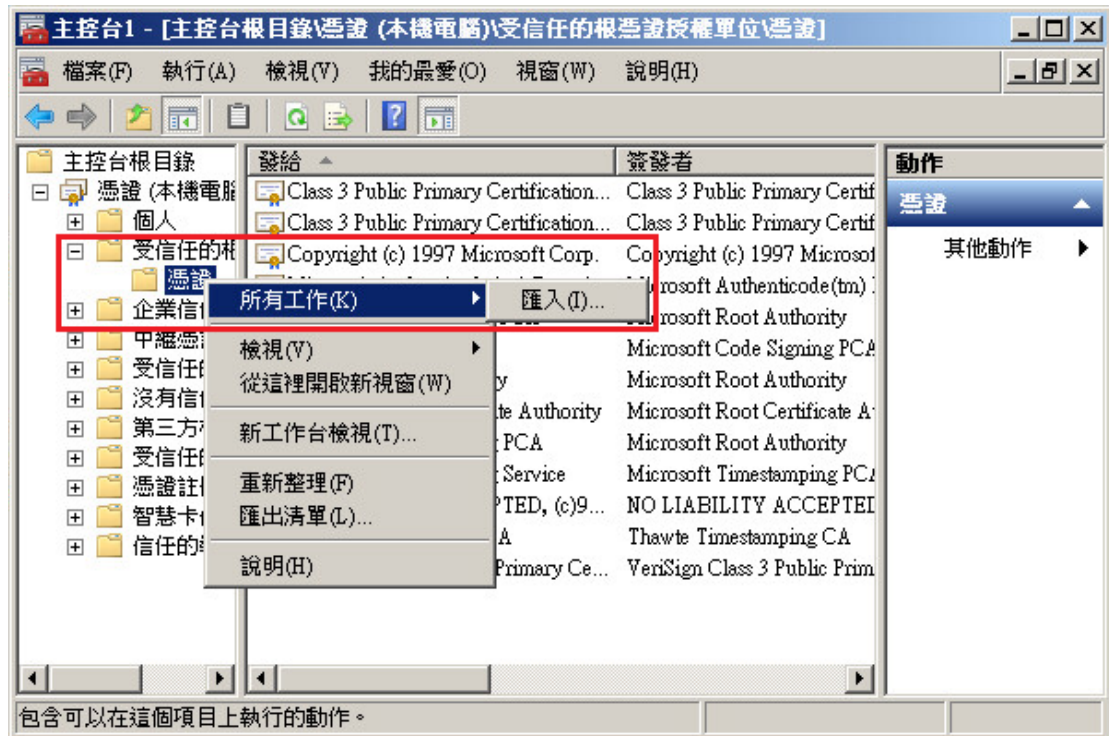
- 一、 下載憑證串鏈，包含 3 張憑證，分別是(1)eCA 根憑證(ePKI Root CA 憑證，也就是中華電信憑證總管理中心自簽憑證)、(2)PublicCA 中繼憑證(中華電信通用憑證管理中心自身憑證)與(3)PublicCA 簽發給用戶的 SSL 伺服器憑證，可採以下兩種方式之一取得：
 1. 您若是本公司之客戶，技術聯絡人的電子郵件信箱會收到憑證串鏈壓縮檔，解壓縮後包括 3 個檔案，分別是 eCA 根憑證(檔名為 ROOTeCA_64.crt)、PublicCA 中繼憑證(檔名為 PublicCA2_64.crt)與用戶端 SSL 伺服器軟體憑證(檔名為 32 個英數字所組成，此為憑證序號)。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。

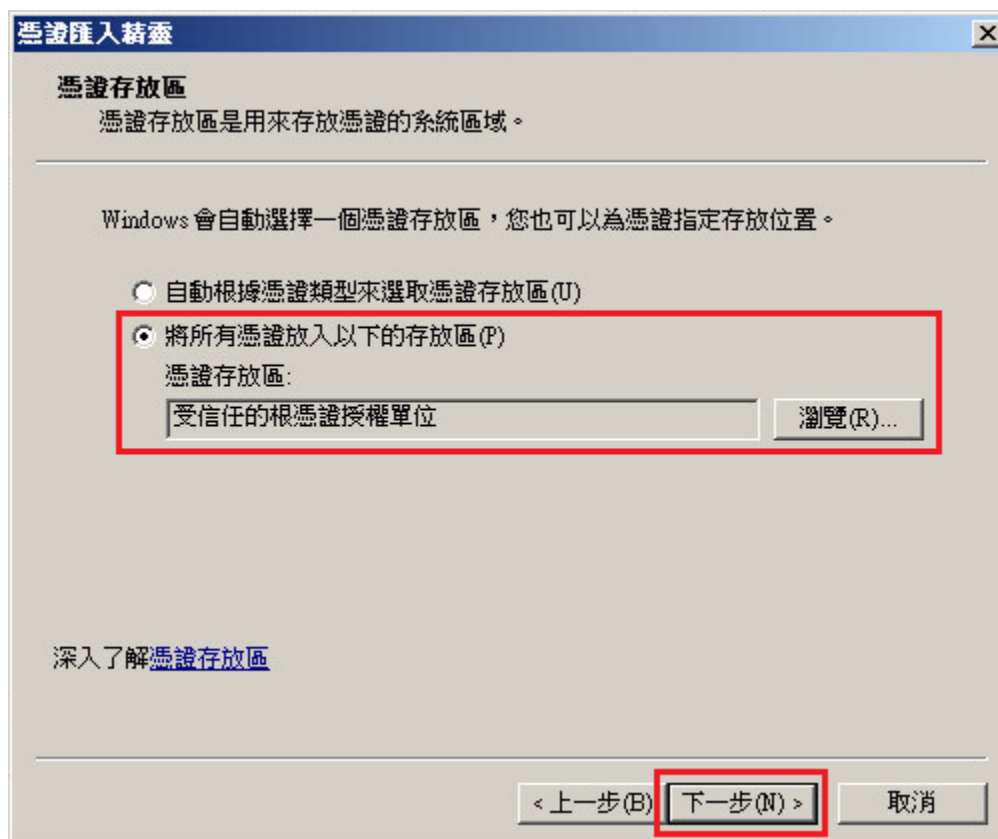
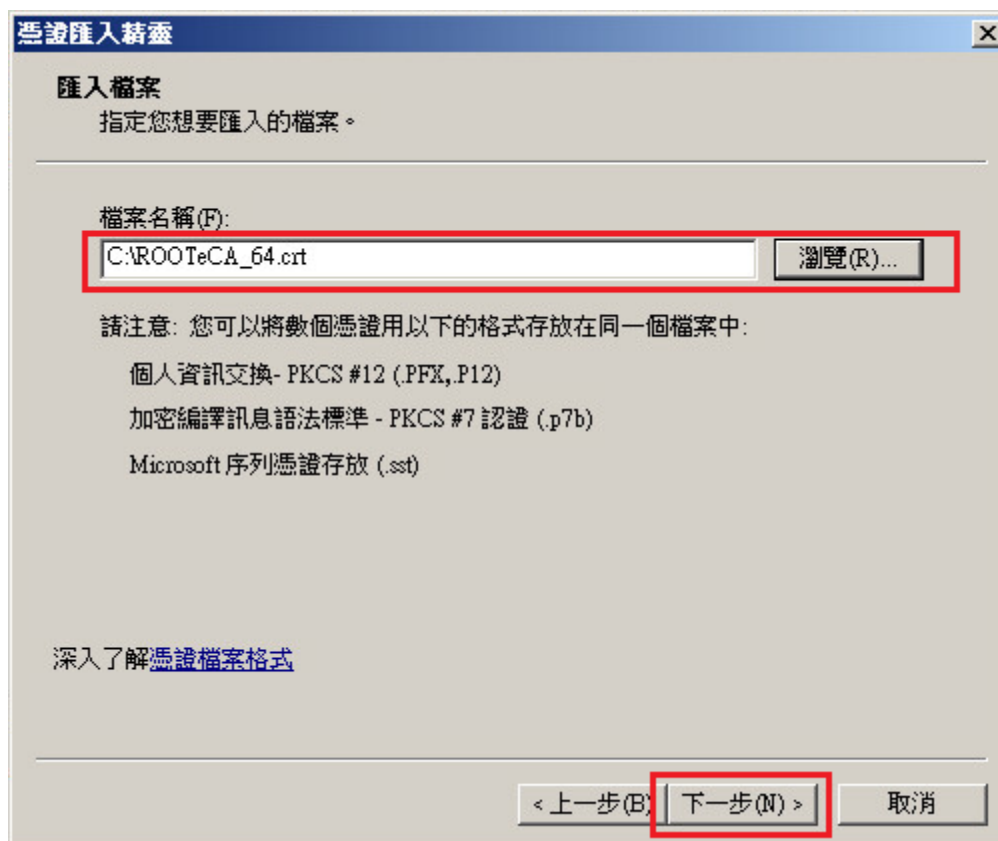


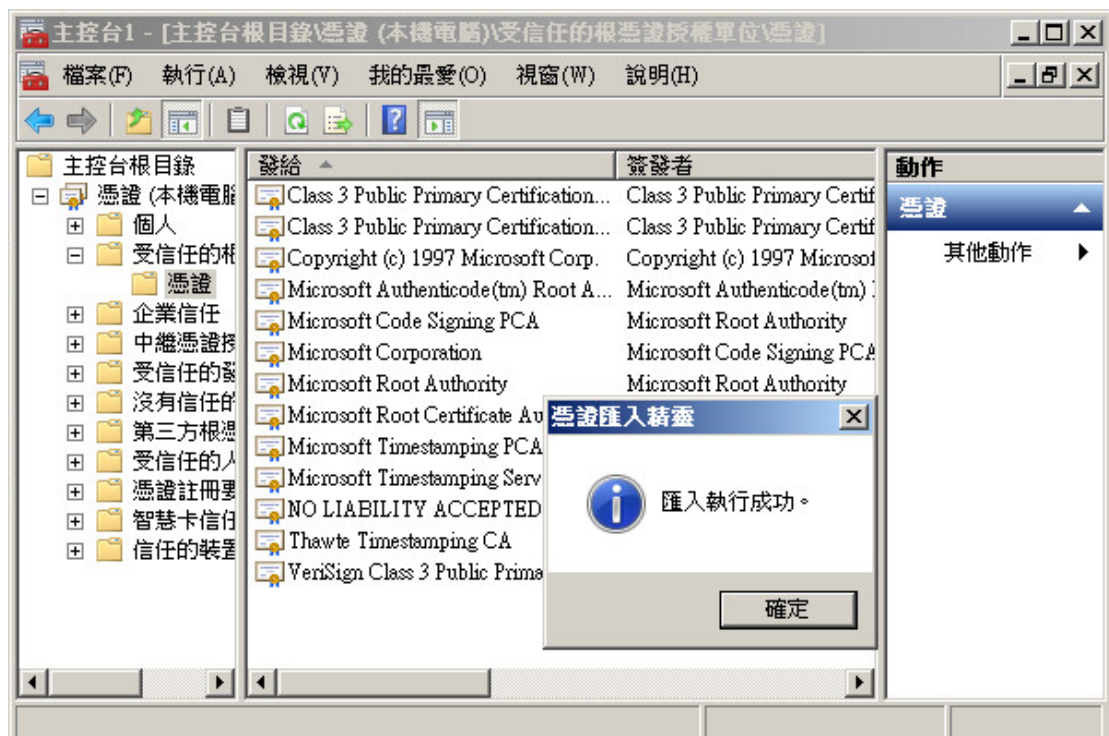


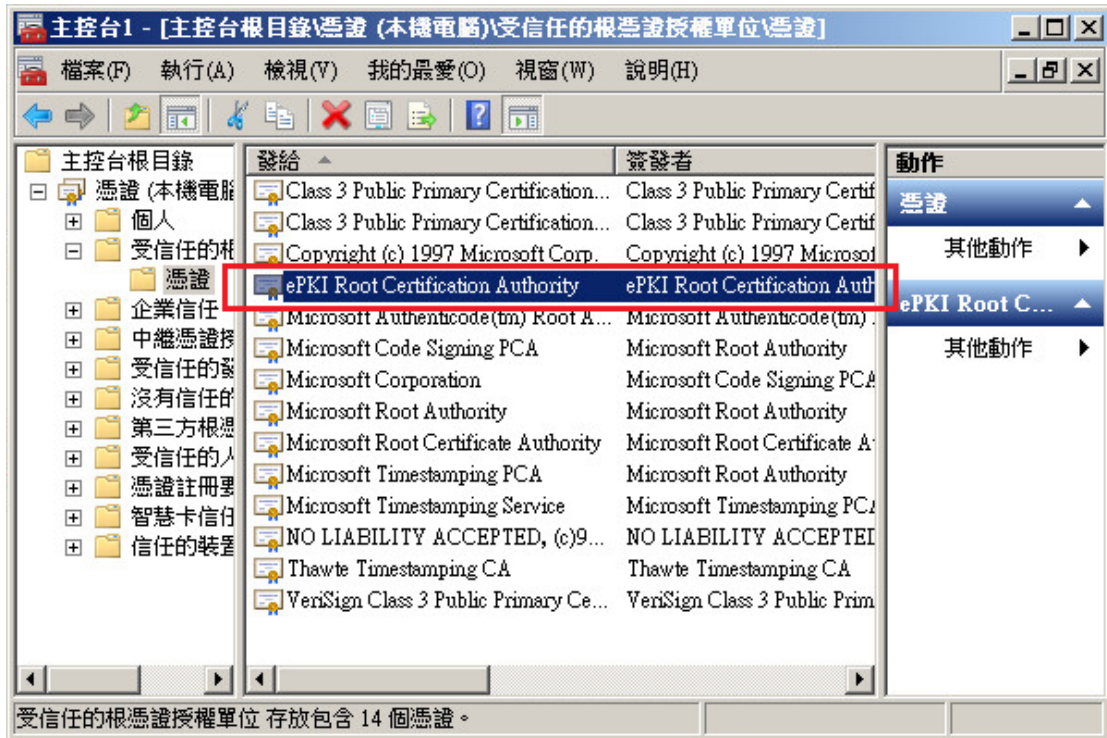


四、於「受信任的根憑證授權單位」匯入 eCA 根憑證。

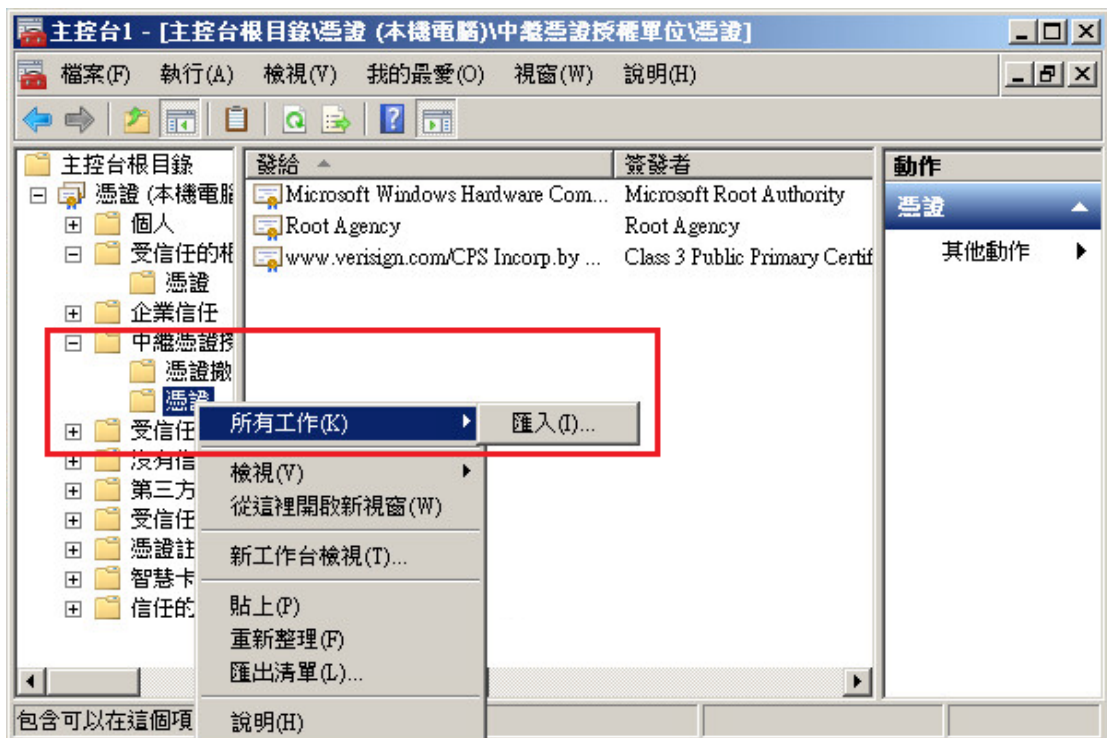


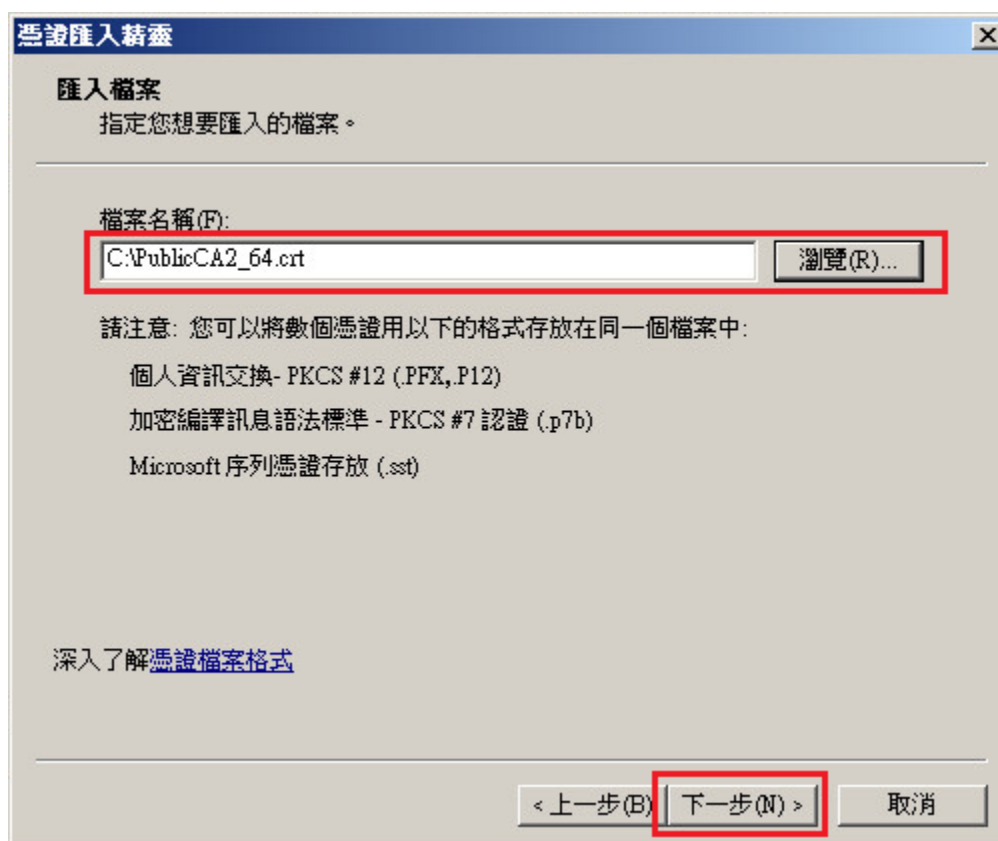
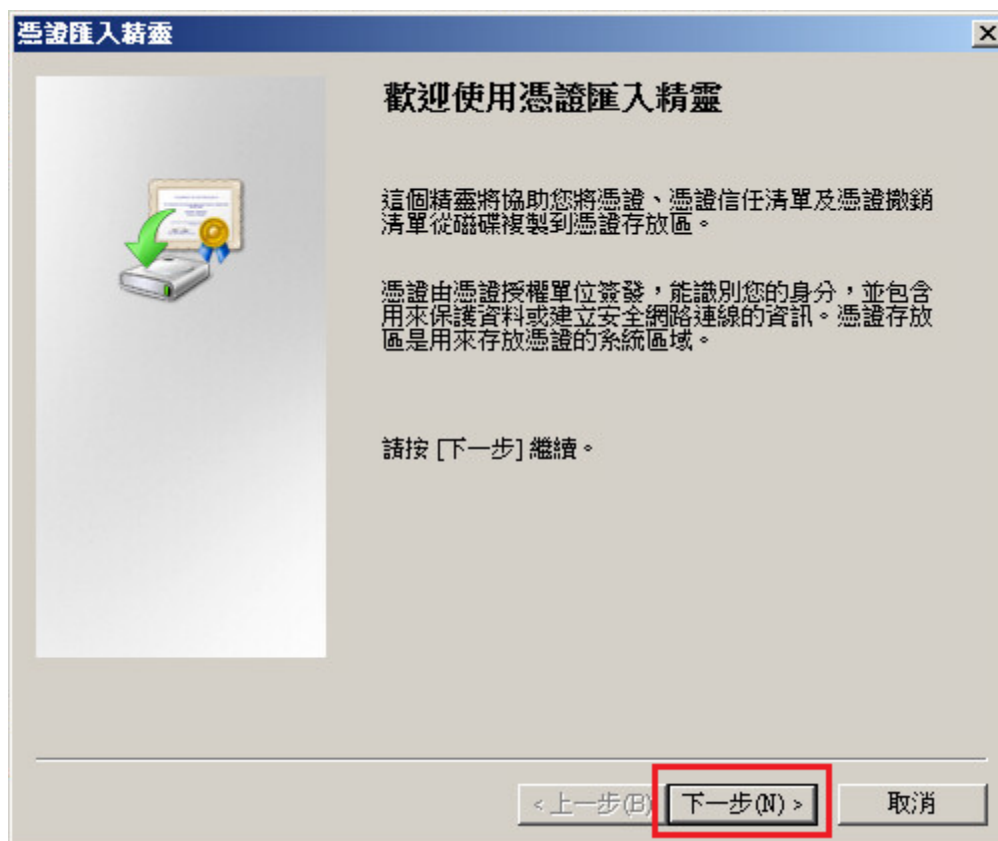


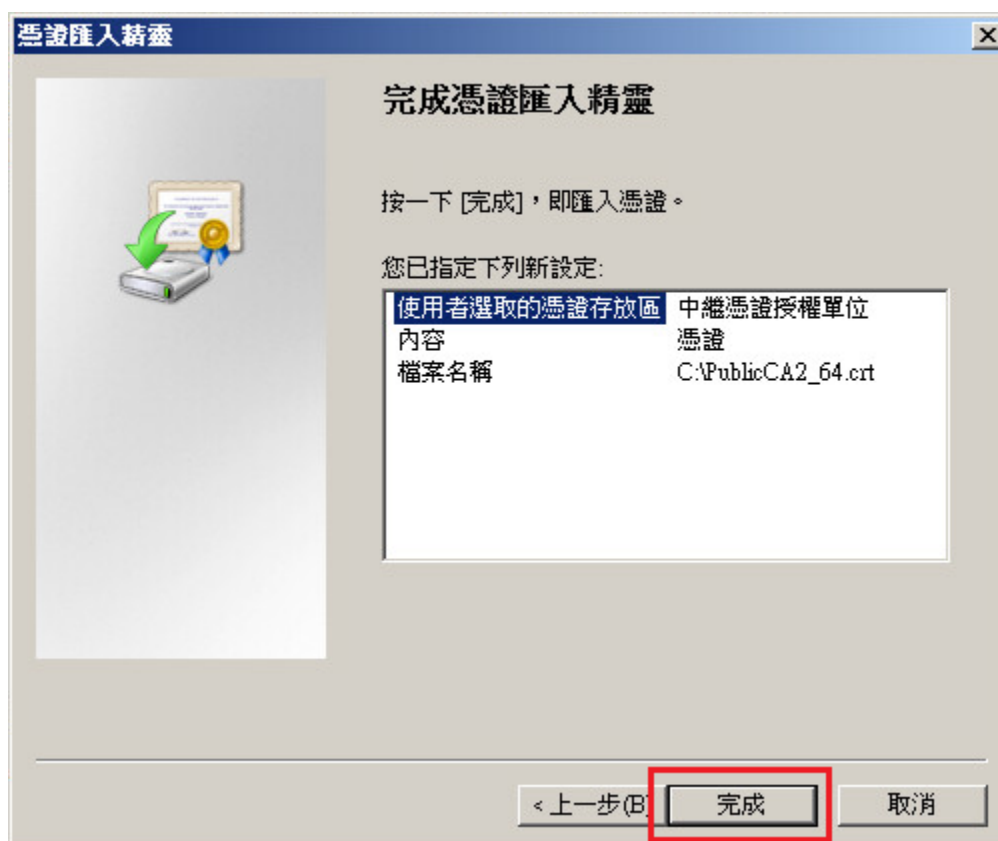
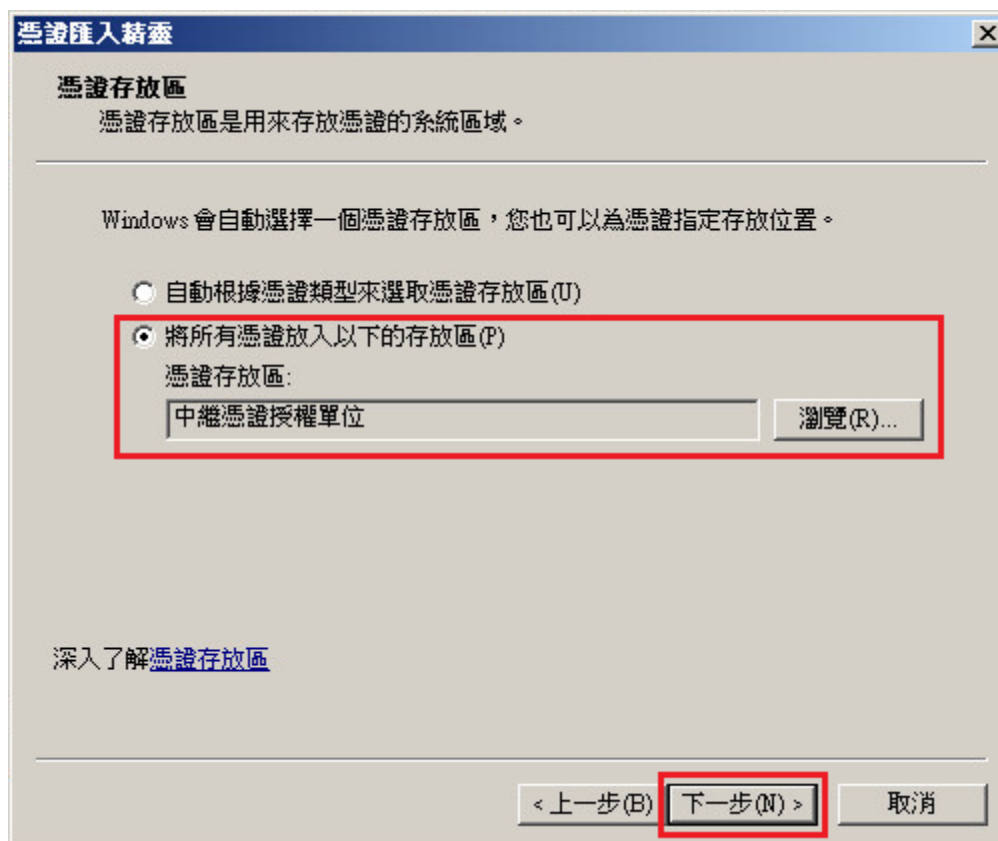


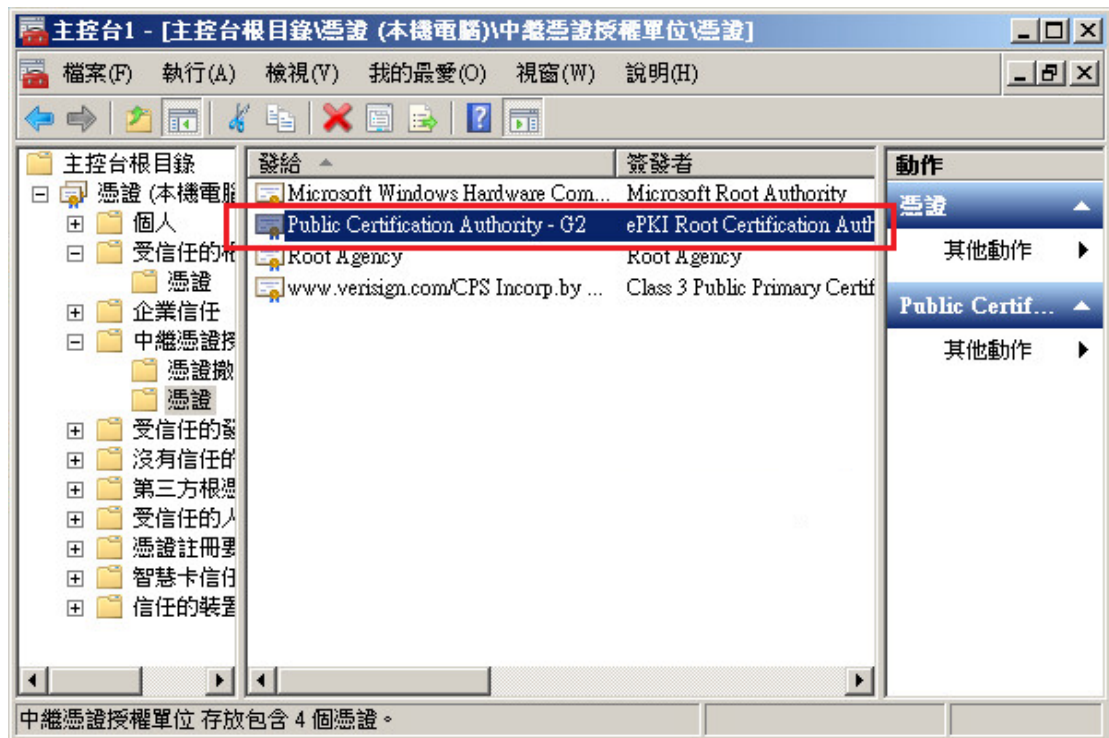
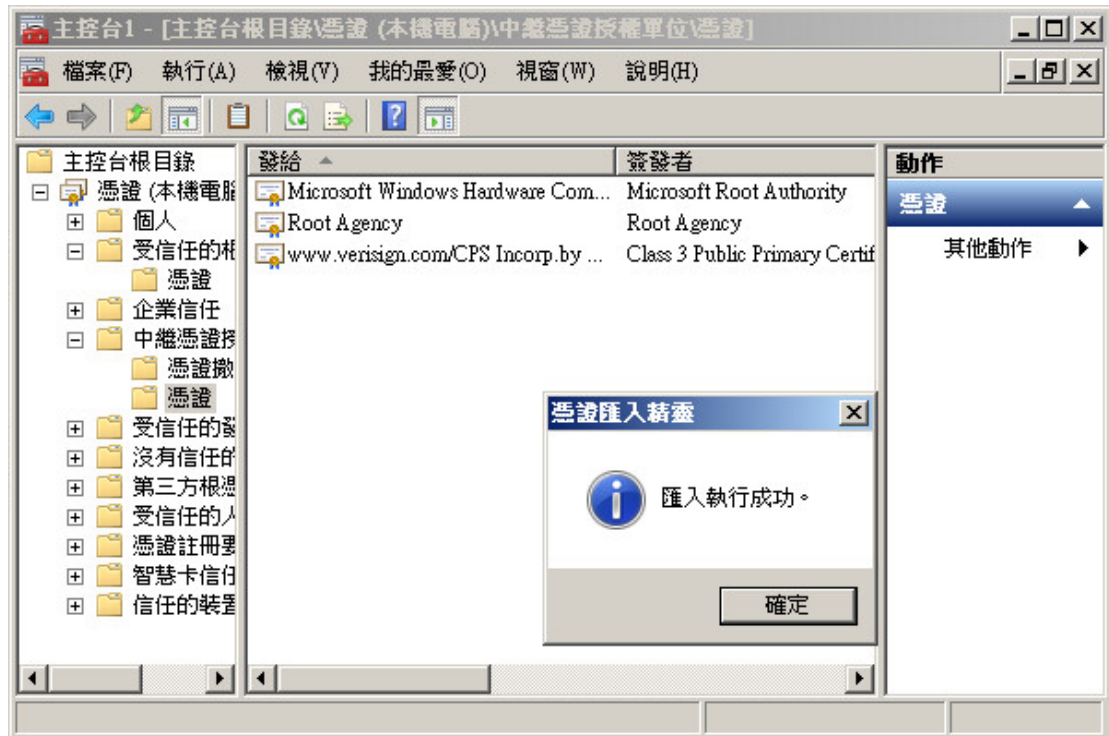


五、 於「中繼憑證授權單位」匯入 PublicCAG2 中繼憑證。

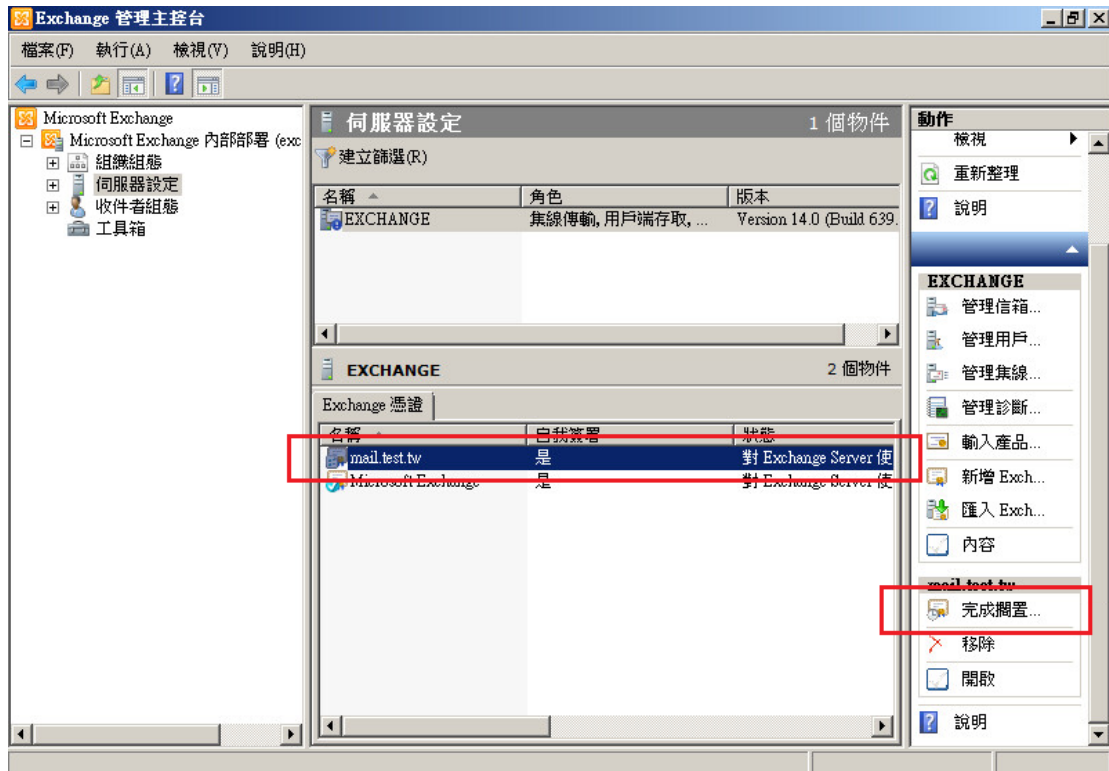




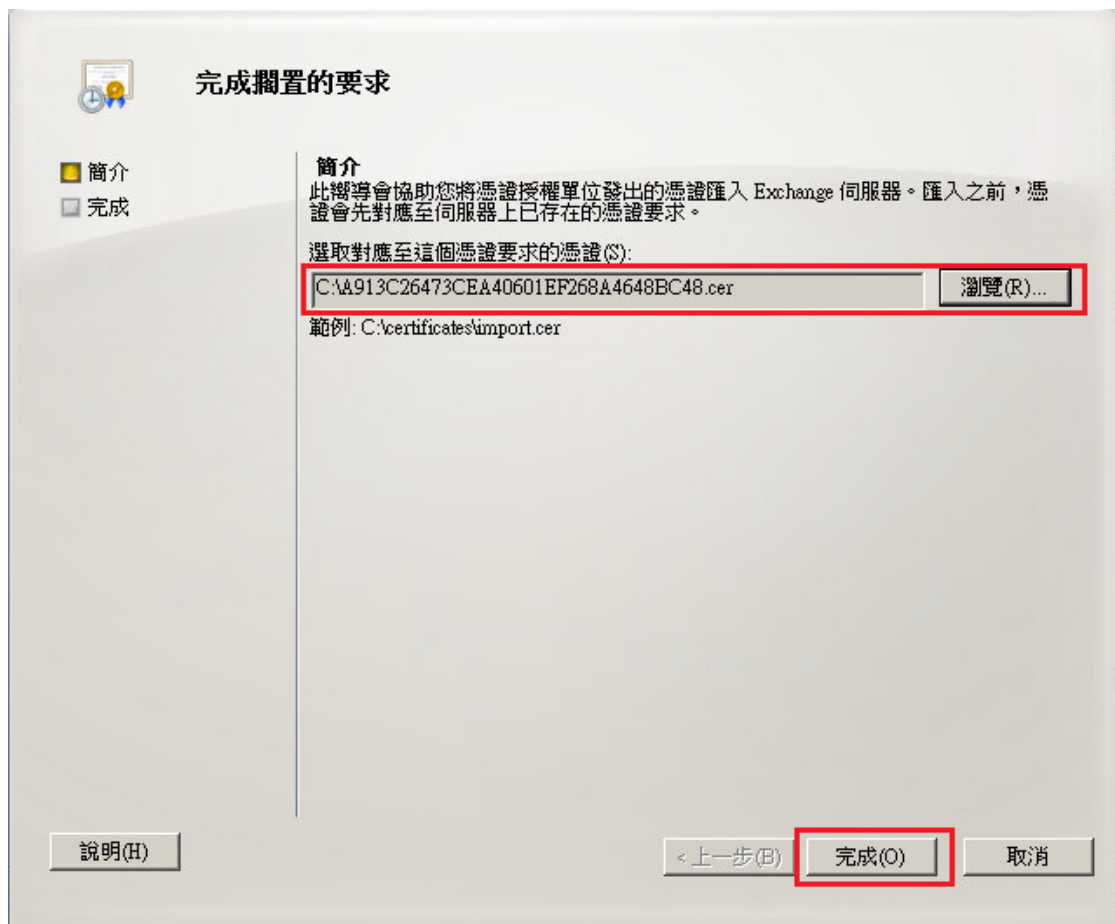


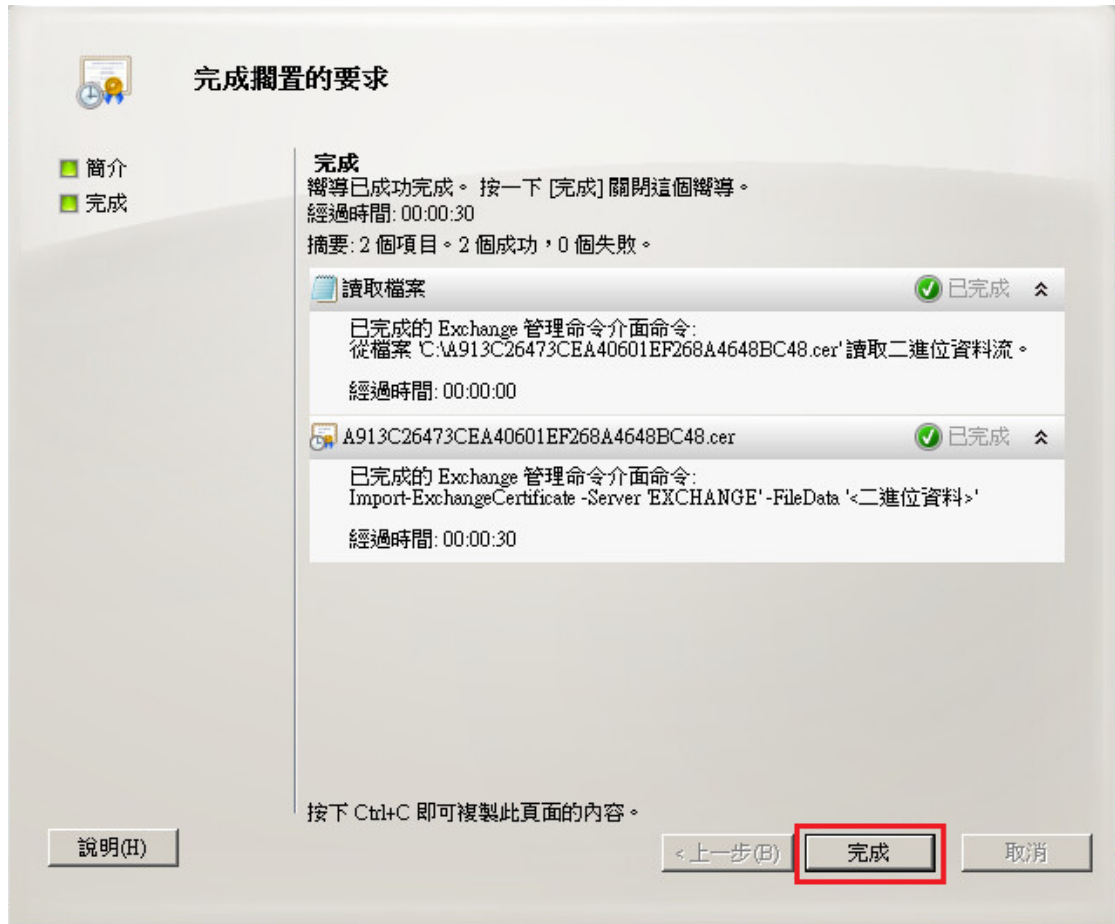


六、 開啟「Exchange 管理主控台」，先點選憑證，接著點選右邊「完成擱置的要求」。

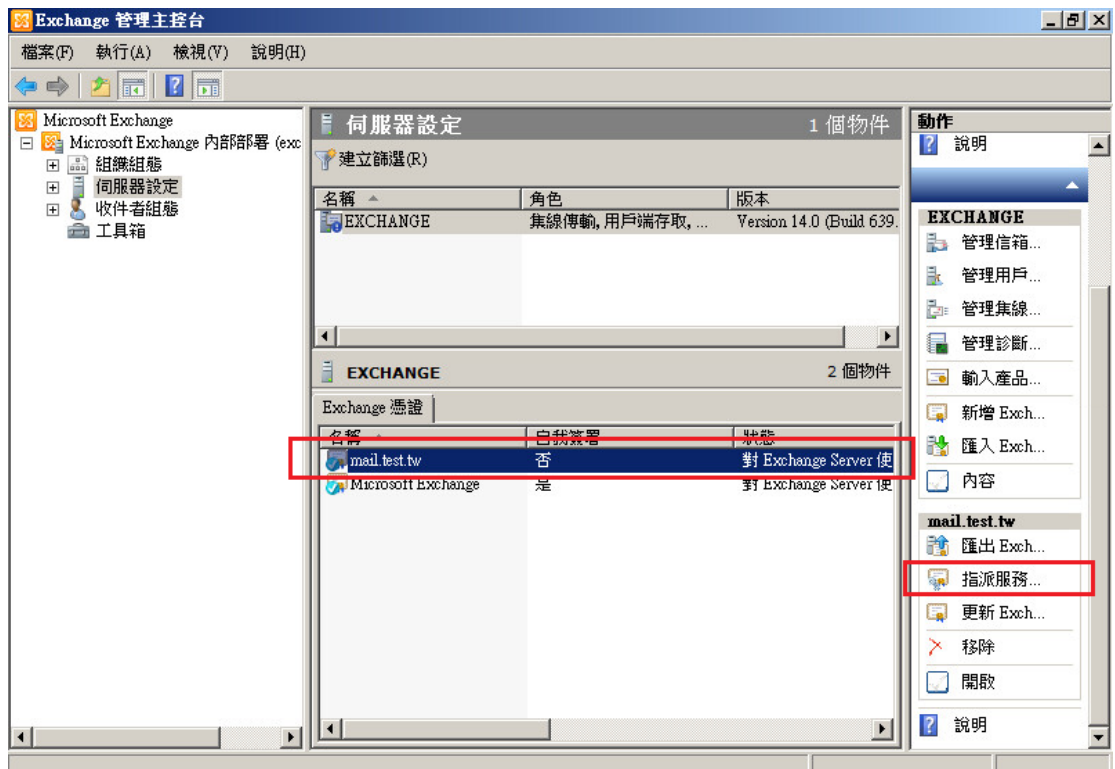


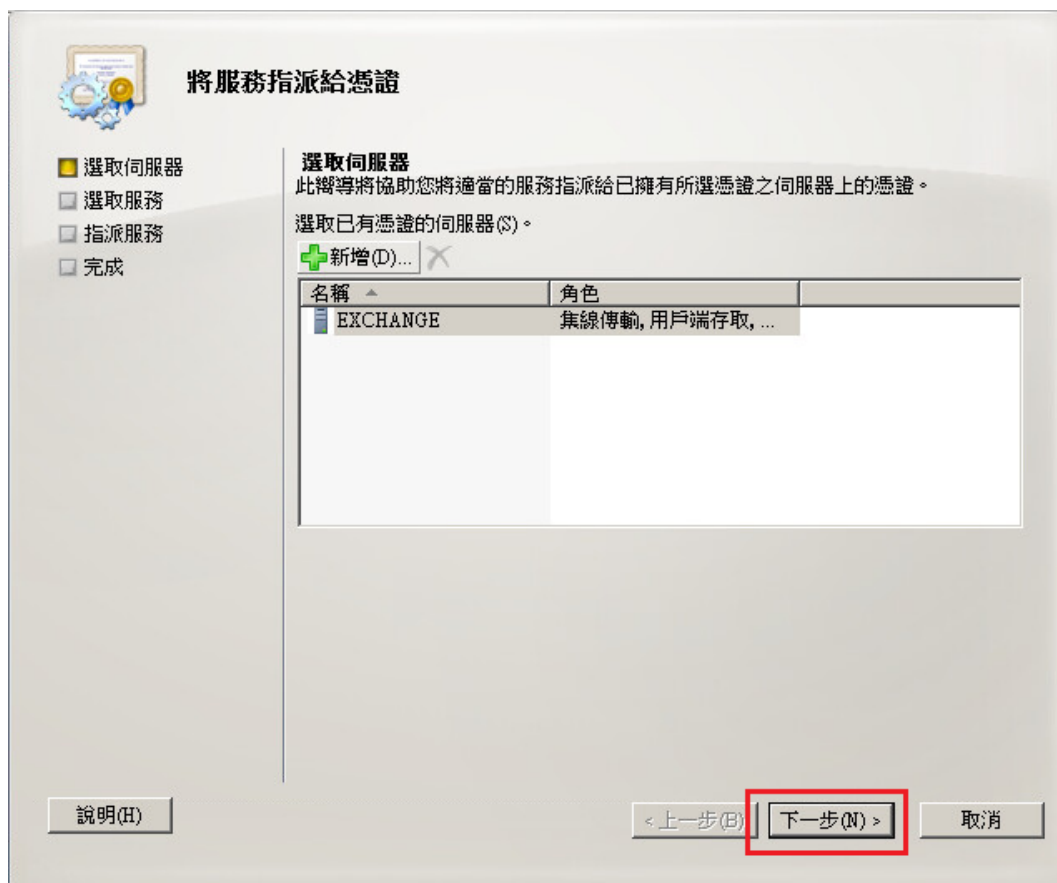
七、 匯入用戶端 SSL 憑證。(檔名為 32 個英數字所組成)



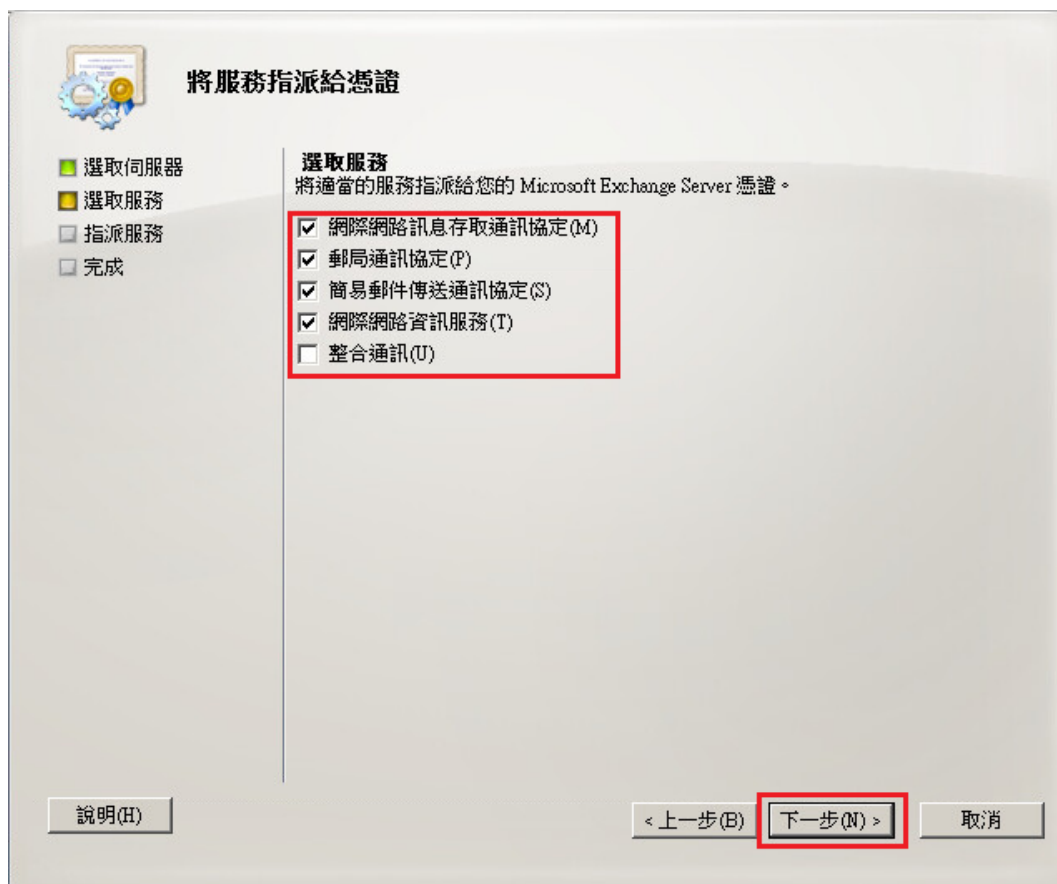


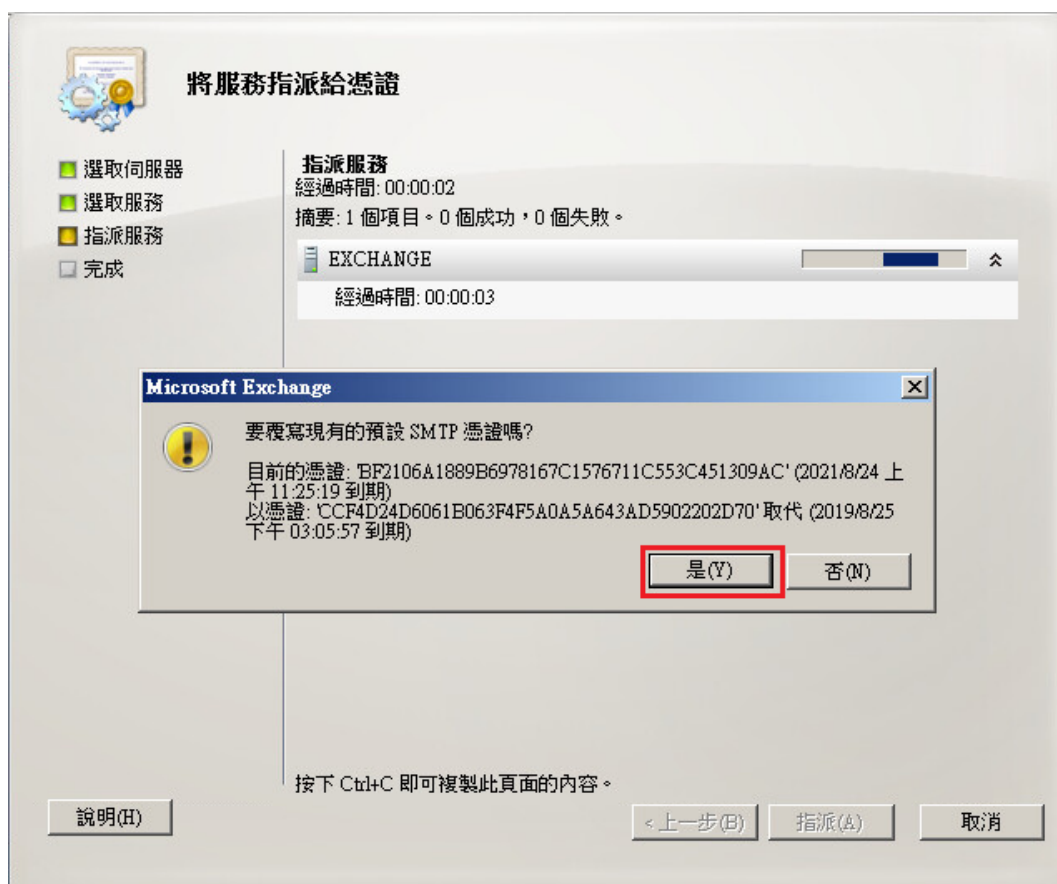
- 八、 指派服務給憑證。
若您是安裝萬用網域憑證，請至 Page. [28](#)

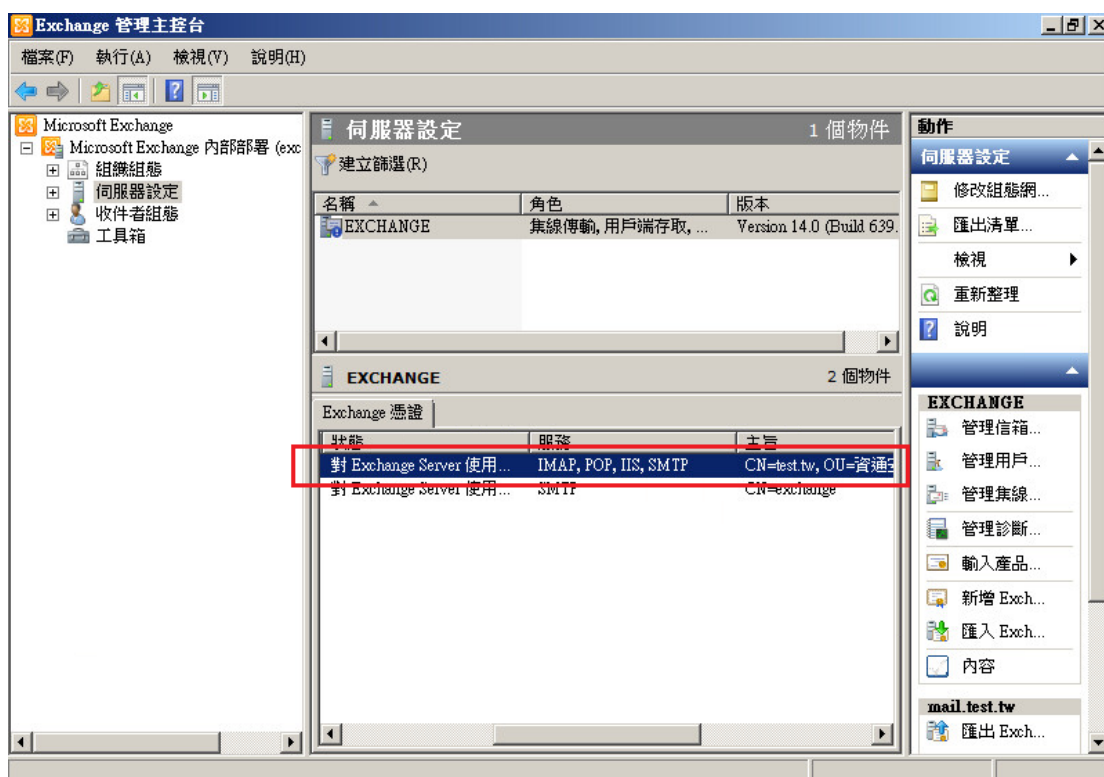
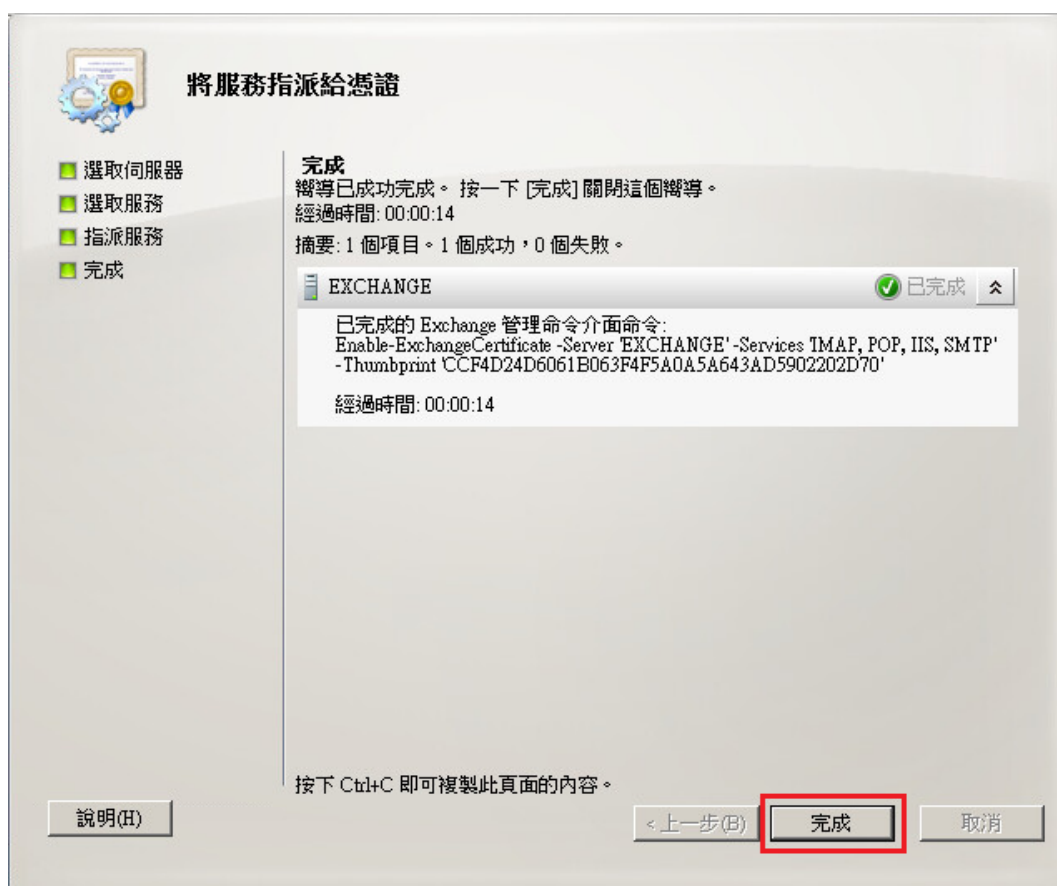




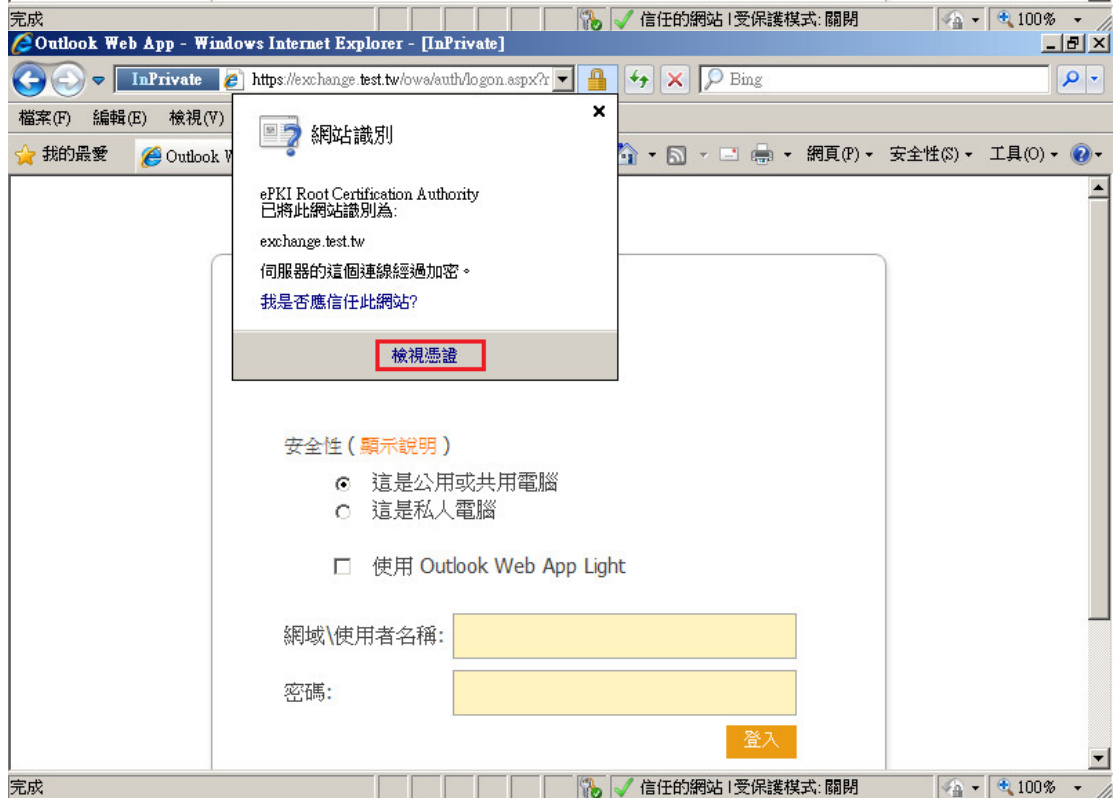
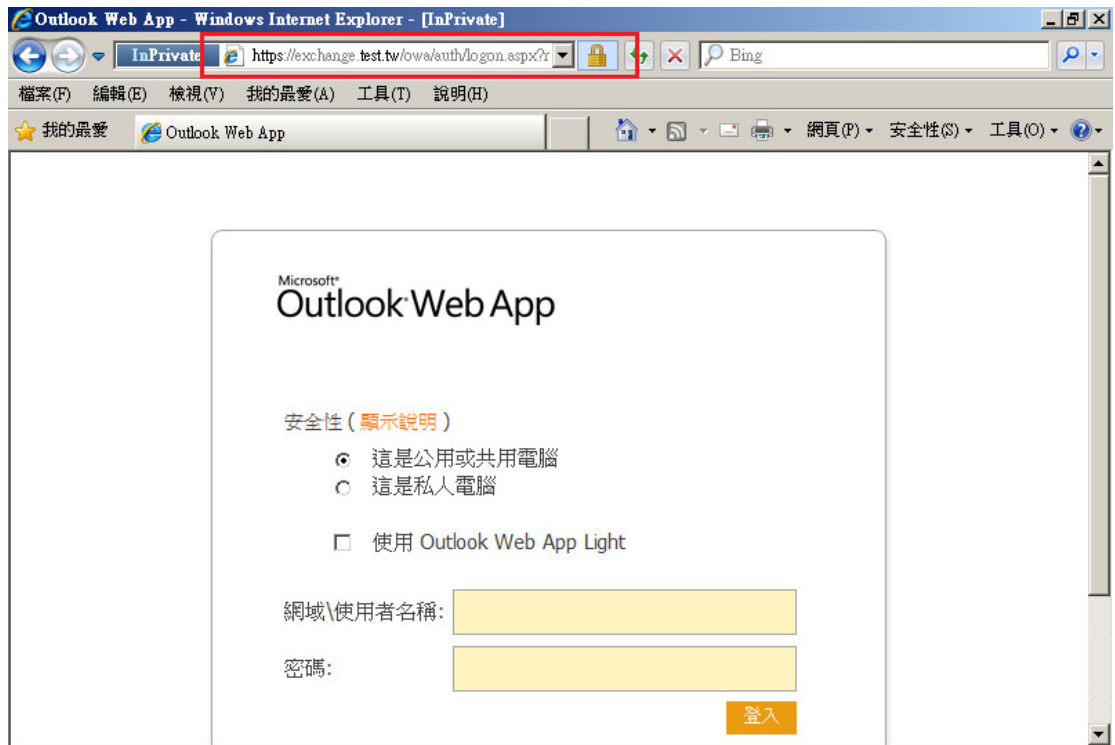
視需求選取服務

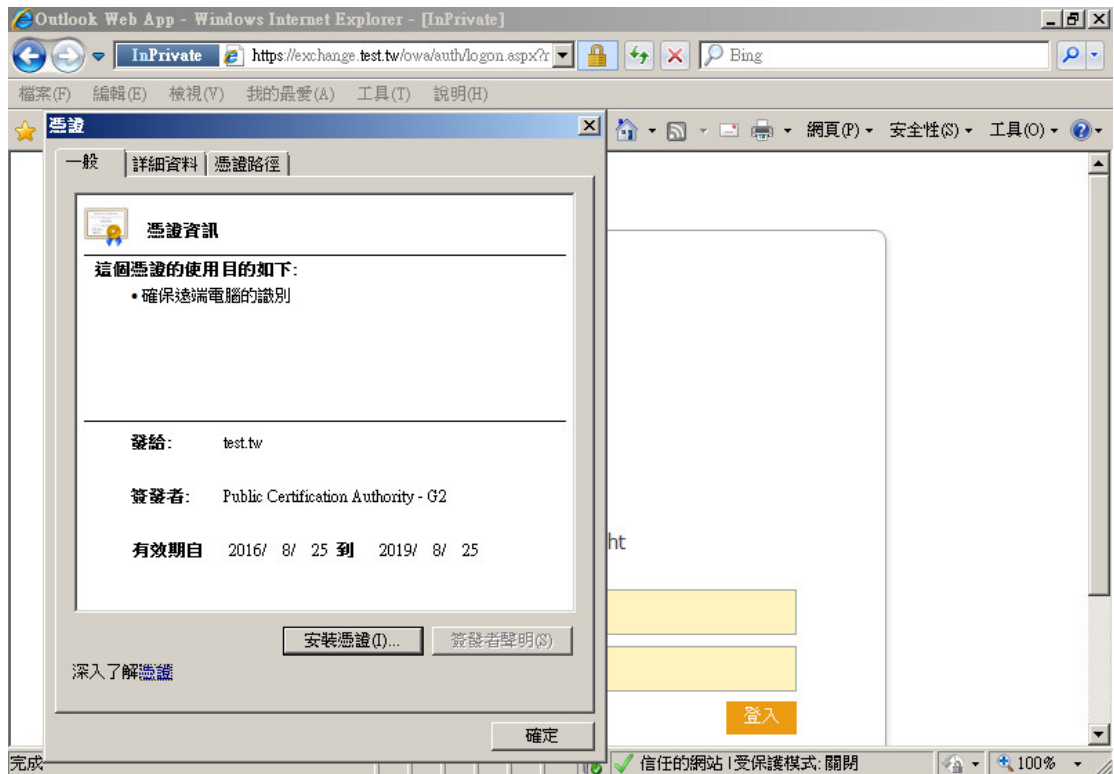






九、 完成後，若您有指派 IIS(owa)服務，可以透過瀏覽器驗證 HTTPS 是否正常。



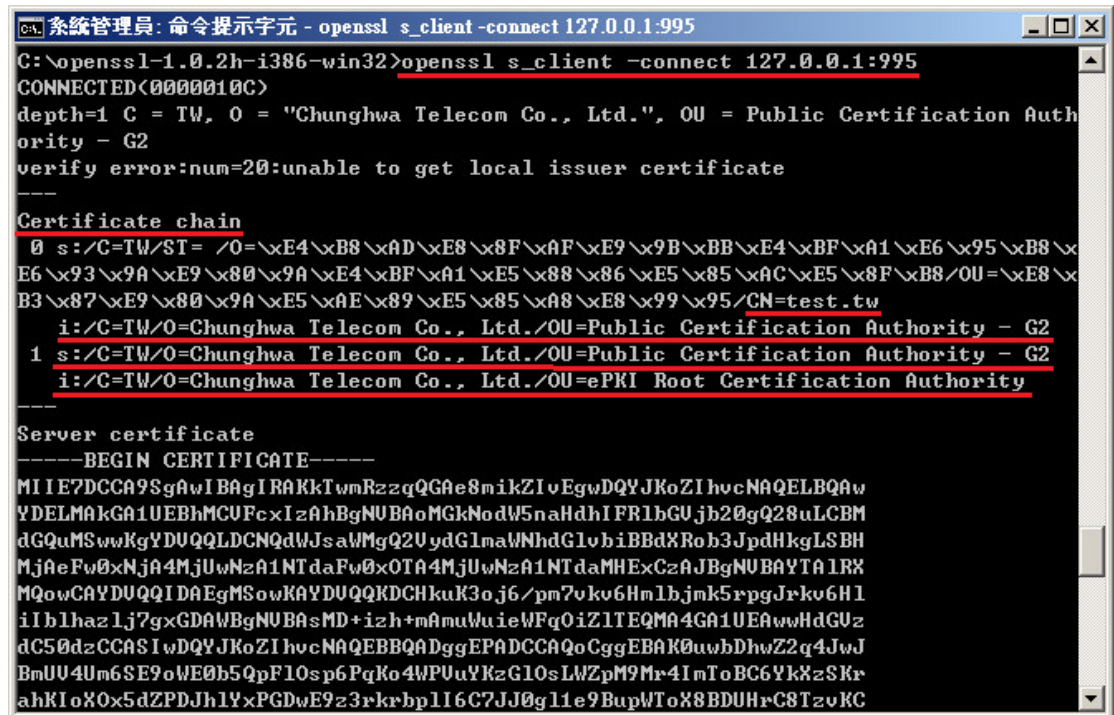


POP3、IMAP4 可用其他郵件軟體進行測試

也可使用 OpenSSL 測試憑證鏈是否正確，指令如下：

openssl s_client -connect <ip:port 或是 domain:port>

POP3 預設為 995 port、IMAP4 預設為 993 port




```

CA 系統管理員: 命令提示字元
C:\openssl-1.0.2h-i386-win32>openssl s_client -connect 127.0.0.1:993
CONNECTED(0000010C)
depth=1 C = TW, O = "Chunghwa Telecom Co., Ltd.", OU = Public Certification Authority - G2
verify error:num=20:unable to get local issuer certificate
-----
Certificate chain
 0 s:/C=TW/ST=/O=\xE4\xB8\xAD\xE8\x8F\xAF\xE9\x9B\xBB\xE4\xBF\xA1\xE6\x95\xB8\x
E6\x93\x9A\xE9\x80\x9A\xE4\xBF\xA1\xE5\x88\x86\xE5\x85\xAC\xE5\x8F\xB8/OU=\xE8\x
B3\x87\xE9\x80\x9A\xE5\xAE\x89\xE5\x85\xA8\xE8\x99\x95/CN=test.tw
   i:/C=TW/O=Chunghwa Telecom Co., Ltd./OU=Public Certification Authority - G2
 1 s:/C=TW/O=Chunghwa Telecom Co., Ltd./OU=Public Certification Authority - G2
   i:/C=TW/O=Chunghwa Telecom Co., Ltd./OU=ePKI Root Certification Authority
-----
Server certificate
-----BEGIN CERTIFICATE-----
MIIE7DCCA9SgAwIBAgIRAKkTwmRzzqQGAe8mikZiVegwDQYJKoZIhvcNAQELBQAw
YDELMAkGA1UEBhMCUFcxIzAhBgNVBAoMGkNodW5naHdhIFRlbnCUjB20gQ28uLCBM
dGQUMSwwKgYDUQQQLDCNqdWJsaWUgQ2UydG1maWNhdGlvbiBBdXRob3JpdHkgLSBH
MjAeFw0xNjA4MjUwNzA1NTdaFw0xOTA4MjUwNzA1NTdaMHExCzAJBgNVBAYTA1RX
MQowCAQYDUQQIDAEgMSowKAYDUQQKDCHkuK3oJ6/pm7vkv6Hmlbjmk5rpgJrkv6Hl
iIb1haz1j7gxGDAWBgNVBAsMD+izh+mAmuWuieWFq0iZ1TEQMA4GA1UEAwwHdGUz
dC50dzCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAK0uwbDhwZ2q4JwJ
BmUU4Um6SE9oWE0b5QpF10sp6PqKo4WPUuYKzG10sLWZpM9Mr4ImToBC6YkXzSKr
ahKI0x0x5dZPDJh1YxPGDwE9z3rkrbp116C7JJ0g11e9BupWToX8BDUHrC8TzvKC

```

十、 安裝 SSL 安全認證標章：

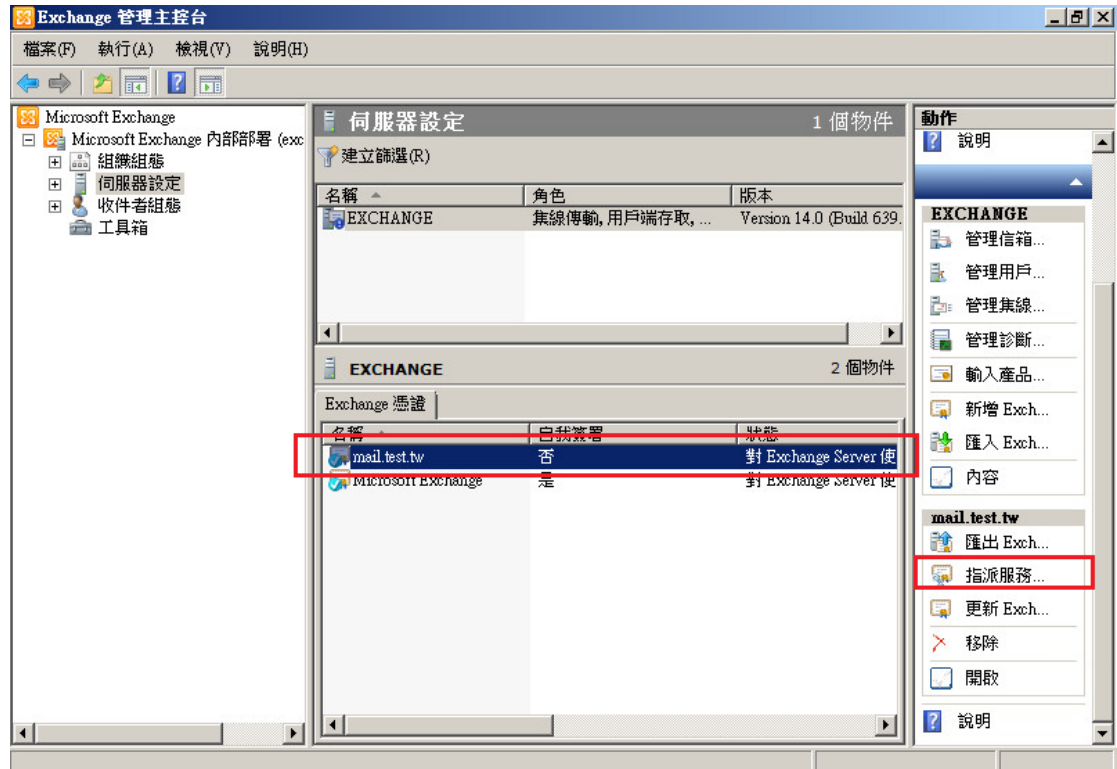
請用戶參考技術聯絡人的電子郵件信箱所收到 SSL 憑證串鏈電子郵件內文的 SSL 安全認證標章安裝說明，將網站 SSL 安全認證標章安裝成功，網友點選 SSL 安全認證標章後可瀏覽您所維護網站所安裝 SSL 憑證的狀態與資訊。您也可參考 <http://publicca.hinet.net/SSL-01.htm> 下方有 SSL 安全認證標章之安裝說明。

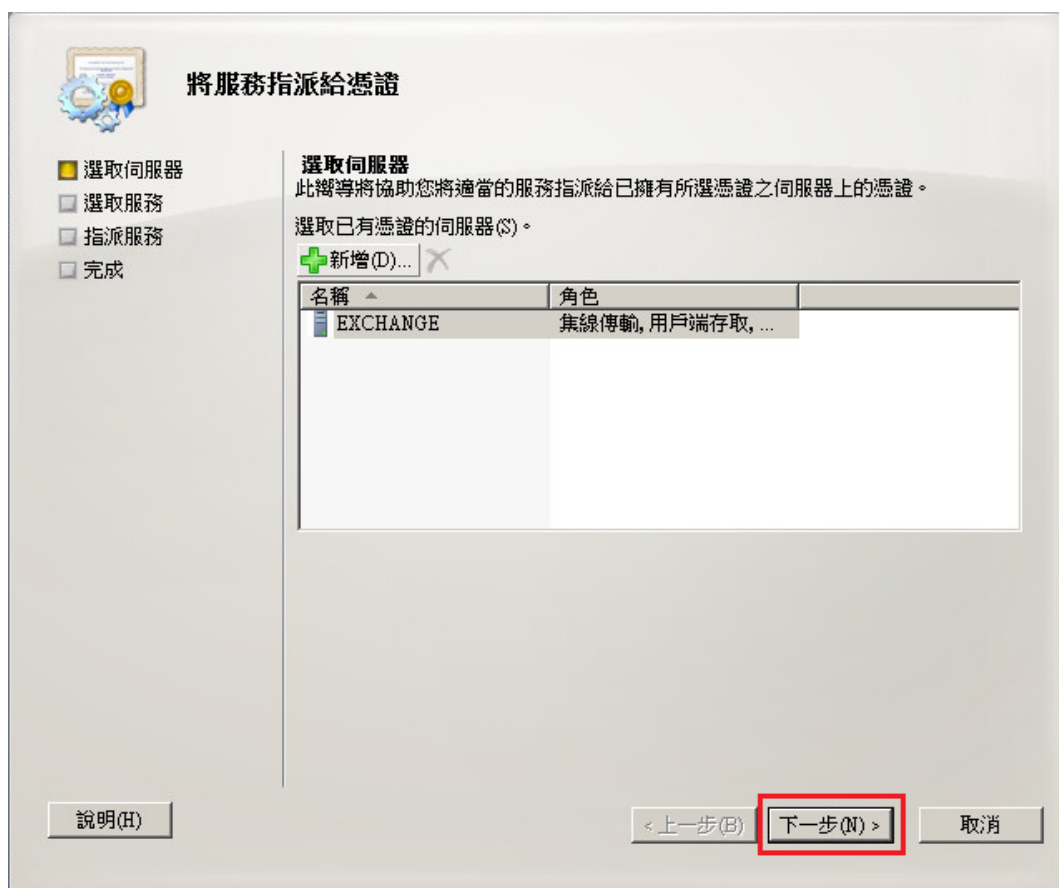
請中華電信公司負責維護網站的同仁，參考從電子表單之資訊表單「IS14-伺服器應用軟體憑證申請/異動單」所下載 SSL 憑證串鏈檔案中的 SSLSealispec.txt，將網站 SSL 安全認證標章安裝成功。

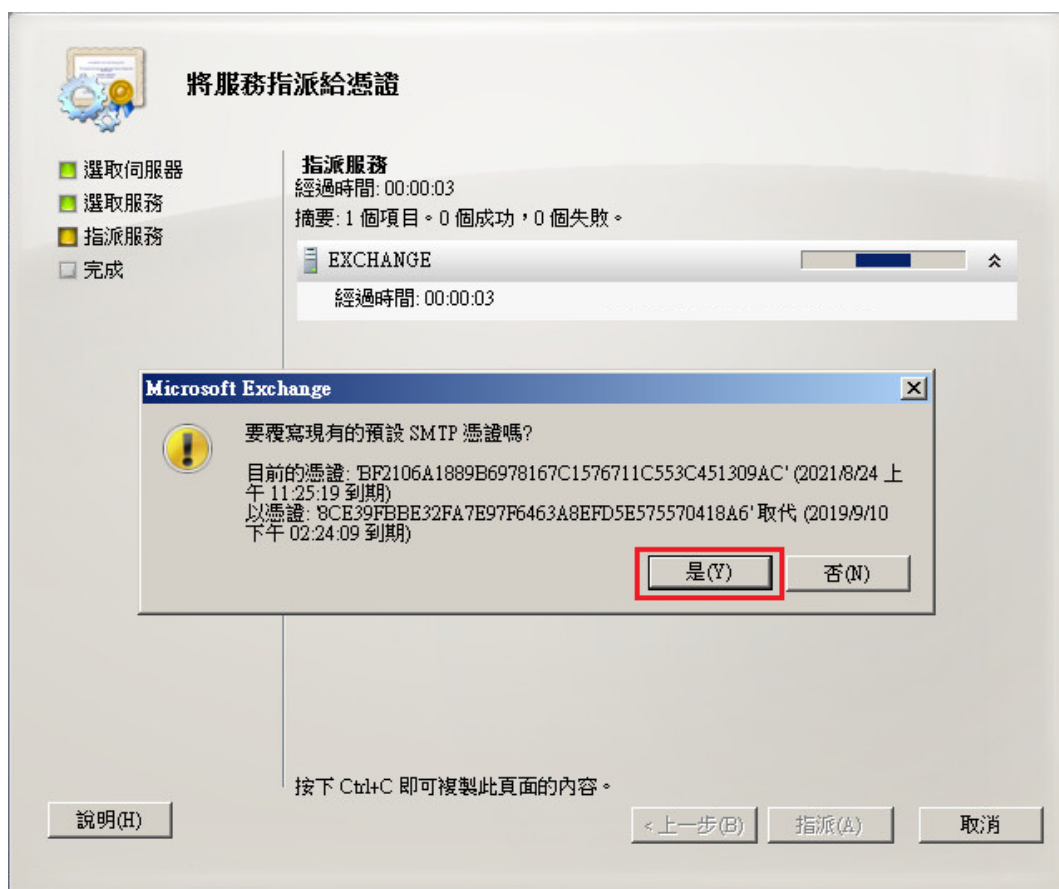
附件一：萬用網域憑證安裝操作手冊

若您尚未完成憑證安裝，請先至憑證安裝操作手冊(Page. 9)進行憑證匯入。

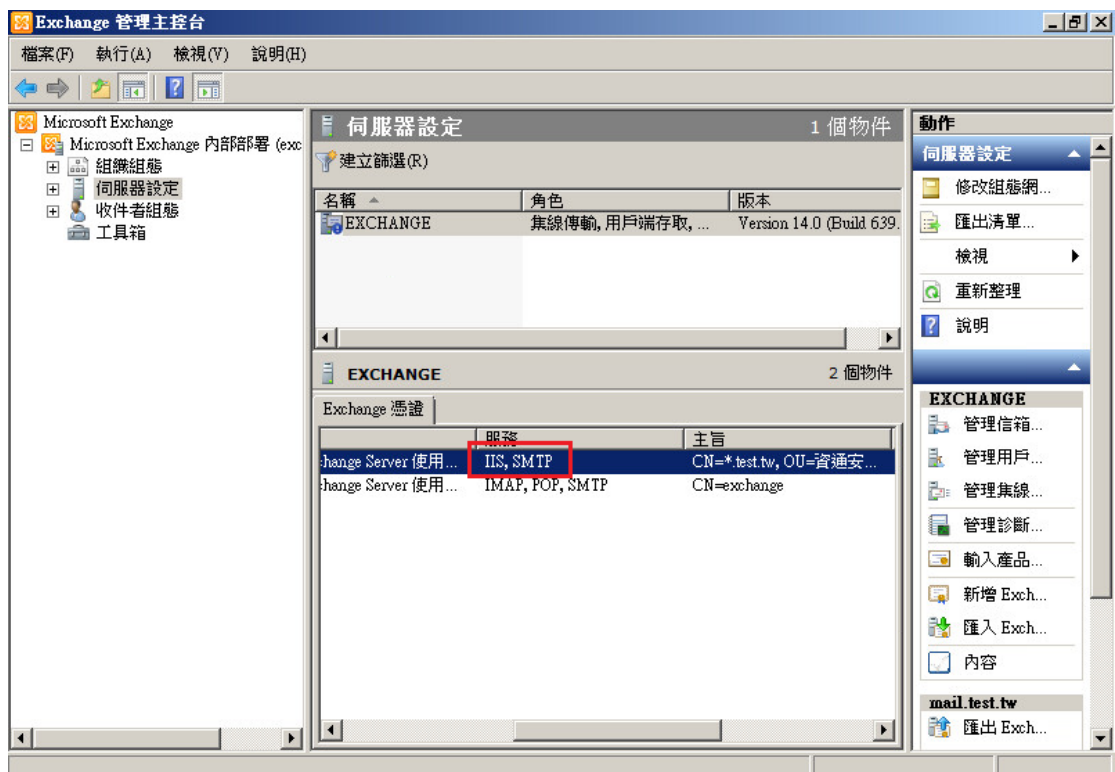
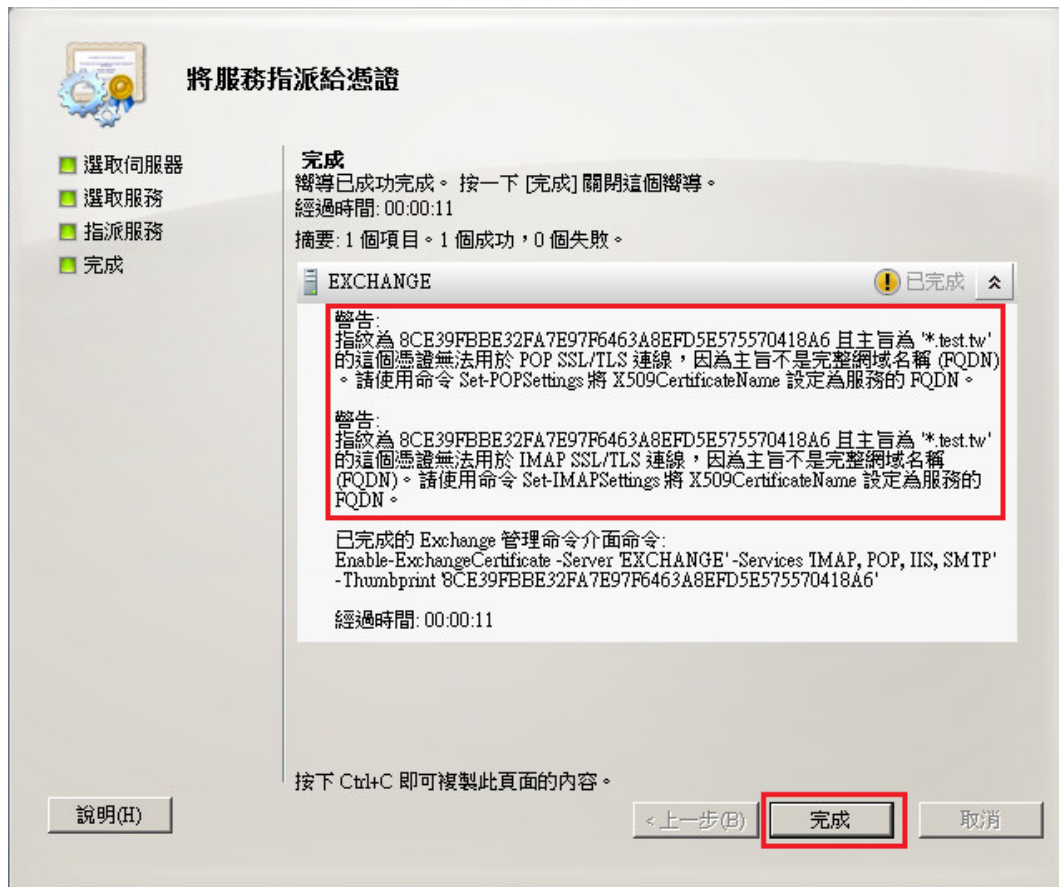
一、 指派服務給萬用網域憑證。



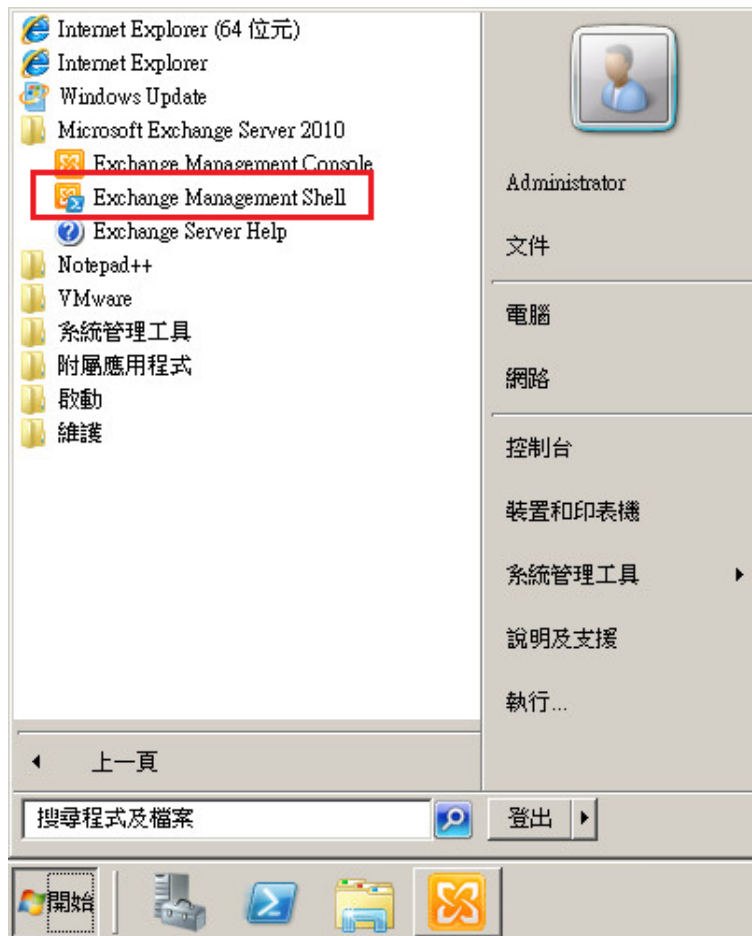




這裡會遇到無法將萬用網域憑證指派給 POP、IMAP 服務，需要以指令方式設定。



二、 開啟 Exchange Management Shell



三、 執行以下指令進行操作

分別輸入 *Get-PopSettings*、*Get-ImapSettings* 查看目前設定

```
Machine: exchange.test.tw

要擷取有類似識別碼的物件群組嗎？您可以在 Identity 參數中使用萬用字元來比對多個物件。類型：

Get-Mailbox *John*
Get-ReceiveConnector *toso.com
Get-JournalRule *discovery*

詳細資訊: Connecting to exchange.test.tw
詳細資訊: Connected to exchange.test.tw.
[PS] C:\Windows\system32>Get-PopSettings

UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::110, 0.0.0.0:110>  <:::995, 0... SecureLogin  exchange

[PS] C:\Windows\system32>Get-ImapSettings

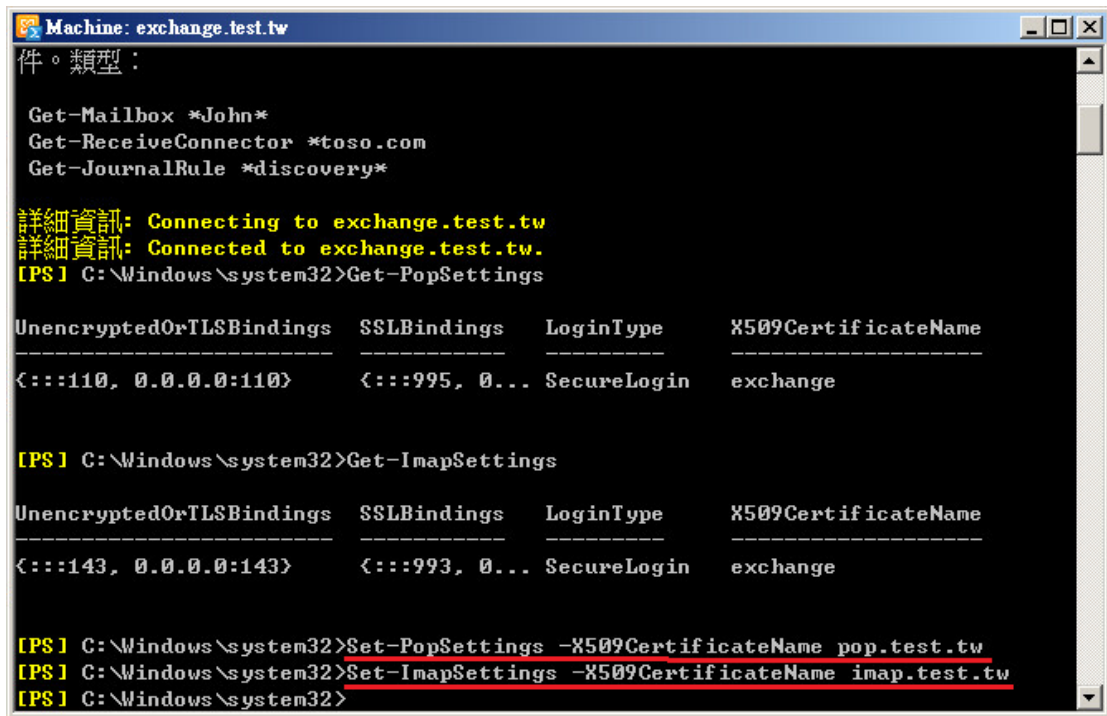
UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::143, 0.0.0.0:143>  <:::993, 0... SecureLogin  exchange

[PS] C:\Windows\system32>
```


輸入以下指令，設定 pop3、imap4 憑證

Set-PopSettings -X509CertificateName <pop 網址>

Set-ImapSettings -X509CertificateName <imap 網址>



```
Machine: exchange.test.tw
件。類型：

Get-Mailbox *John*
Get-ReceiveConnector *toso.com
Get-JournalRule *discovery*

詳細資訊: Connecting to exchange.test.tw
詳細資訊: Connected to exchange.test.tw.
[PS] C:\Windows\system32>Get-PopSettings

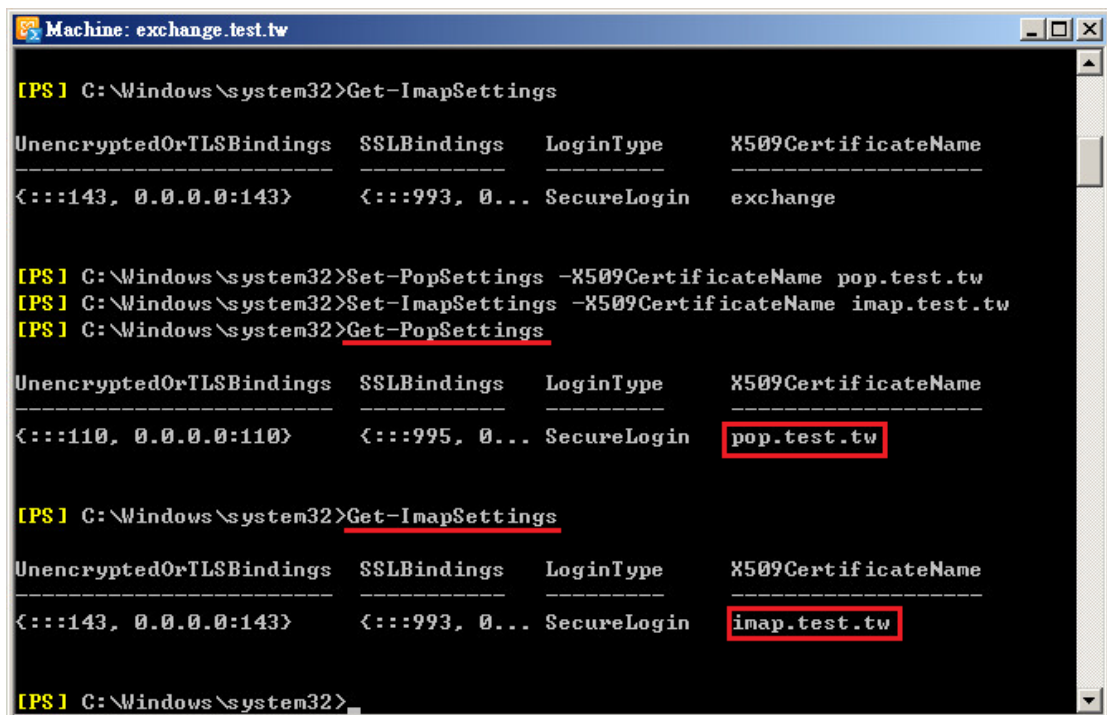
UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::110, 0.0.0.0:110>    <:::995, 0... SecureLogin  exchange

[PS] C:\Windows\system32>Get-ImapSettings

UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::143, 0.0.0.0:143>    <:::993, 0... SecureLogin  exchange

[PS] C:\Windows\system32>Set-PopSettings -X509CertificateName pop.test.tw
[PS] C:\Windows\system32>Set-ImapSettings -X509CertificateName imap.test.tw
[PS] C:\Windows\system32>
```

可再次輸入 *Get-PopSettings*、*Get-ImapSettings* 查看是否設定成功



```
Machine: exchange.test.tw

[PS] C:\Windows\system32>Get-ImapSettings

UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::143, 0.0.0.0:143>    <:::993, 0... SecureLogin  exchange

[PS] C:\Windows\system32>Set-PopSettings -X509CertificateName pop.test.tw
[PS] C:\Windows\system32>Set-ImapSettings -X509CertificateName imap.test.tw
[PS] C:\Windows\system32>Get-PopSettings

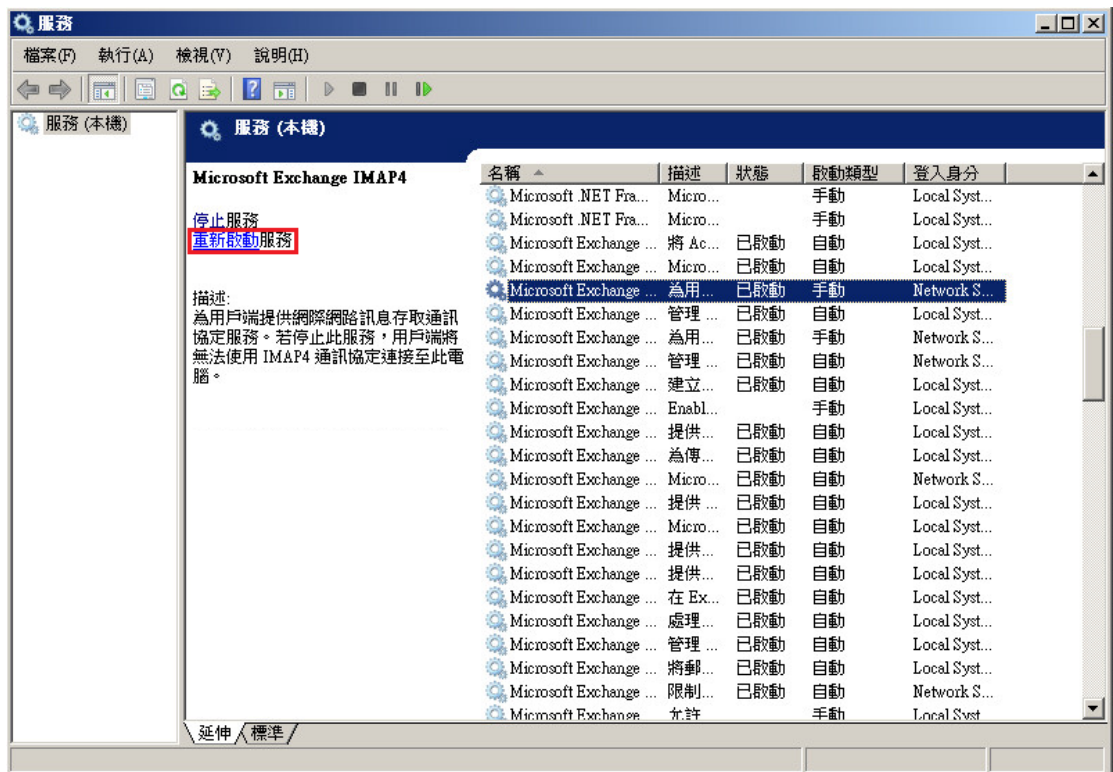
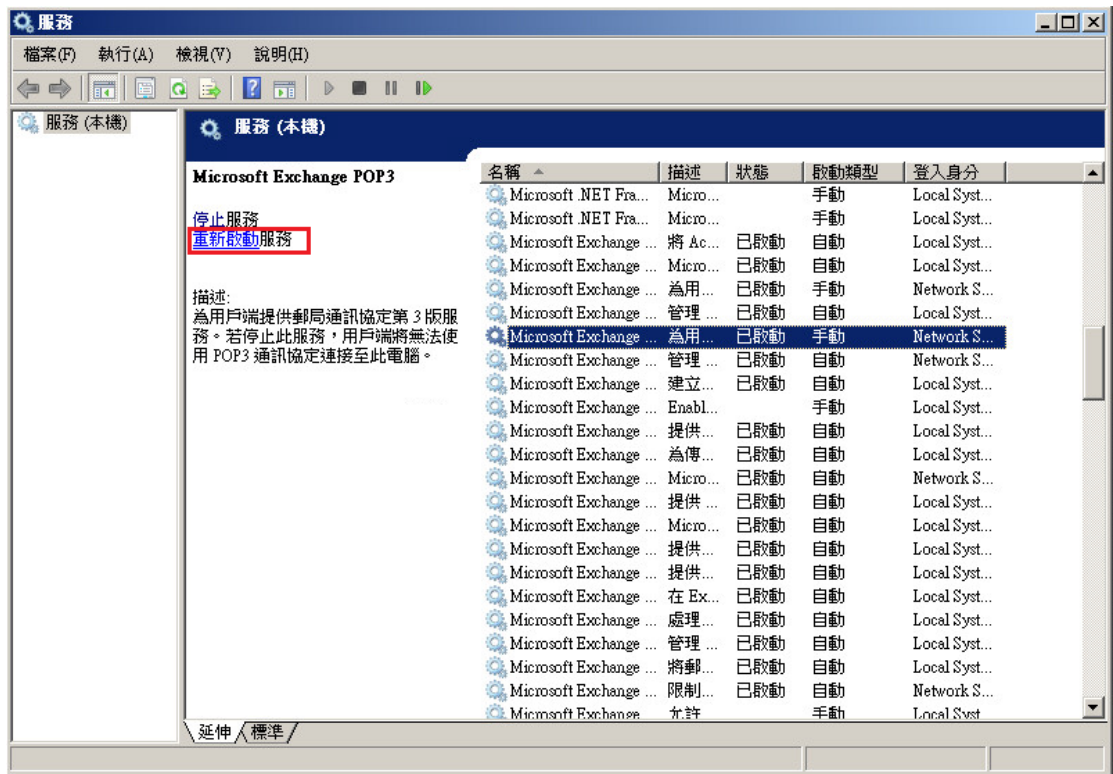
UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::110, 0.0.0.0:110>    <:::995, 0... SecureLogin  pop.test.tw

[PS] C:\Windows\system32>Get-ImapSettings

UnencryptedOrTLSBindings  SSLBindings  LoginType  X509CertificateName
-----
<:::143, 0.0.0.0:143>    <:::993, 0... SecureLogin  imap.test.tw

[PS] C:\Windows\system32>
```

四、 需要重啟 POP3、IMAP4 服務，憑證指派才能生效



五、 完成後，可依照憑證安裝操作手冊(Page. 24)進行相關測試。