匯智資訊股份有限公司

SSL 數位憑證

Windows Server 2012 R2 憑證安裝說明

匯智資訊
cloudmax
www.cloudmax.com.tw

匯智 資訊股份有限公司
106073 台北市大安區仁愛路四段 25 號 3 樓
3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City
106073, Taiwan (R.O.C.)
t. +886-2-2718-7200
f. +886-2-2718-1922

【版權及商標聲明】

文件提供之安裝步驟僅供參考，詳細狀況依伺服器版本或所在網路環境、架構而有些微差別，請依實際狀況或系統提供商資訊為準，若於安裝上有任何問題可與我們聯繫，將有專員引導您排除障礙。

【有限擔保責任聲明】

Cloudmax 匯智盡力製作本說明文件其正確性，但不擔保本文件無任何瑕疵，亦不為使用本說明文件而引起之衍生利益損失或意外損毀之損失擔保責任。若對本文件有任何疑問與建議，可利用下方資訊與我們聯繫：

電話：+886-2-2718-7200

傳真：+886-2-2718-1922

信箱：service@cloudmax.com.tw

匯智資訊 cloudmax

匯智 資訊股份有限公司

106073 台北市大安區仁愛路四段 25 號 3 樓
3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City
106073, Taiwan (R.O.C.)

t. +886-2-2718-7200
f. +886-2-2718-1922

目錄

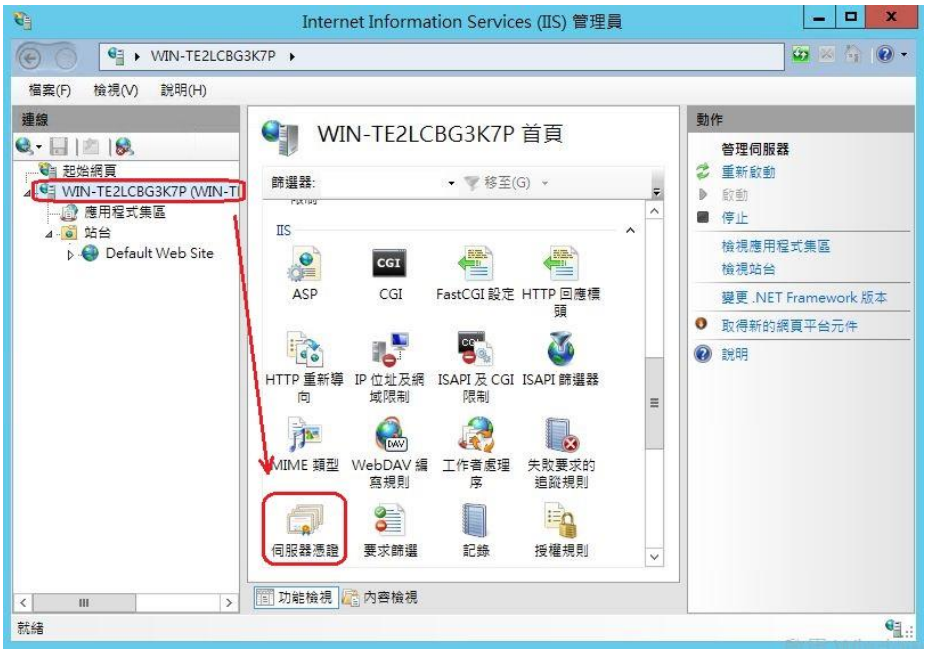
匯智資訊 cloudmax

匯智 資訊股份有限公司
106073 台北市大安區仁愛路四段 25 號 3 樓
3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City
106073, Taiwan (R.O.C.)
t. +886-2-2718-7200
f. +886-2-2718-1922

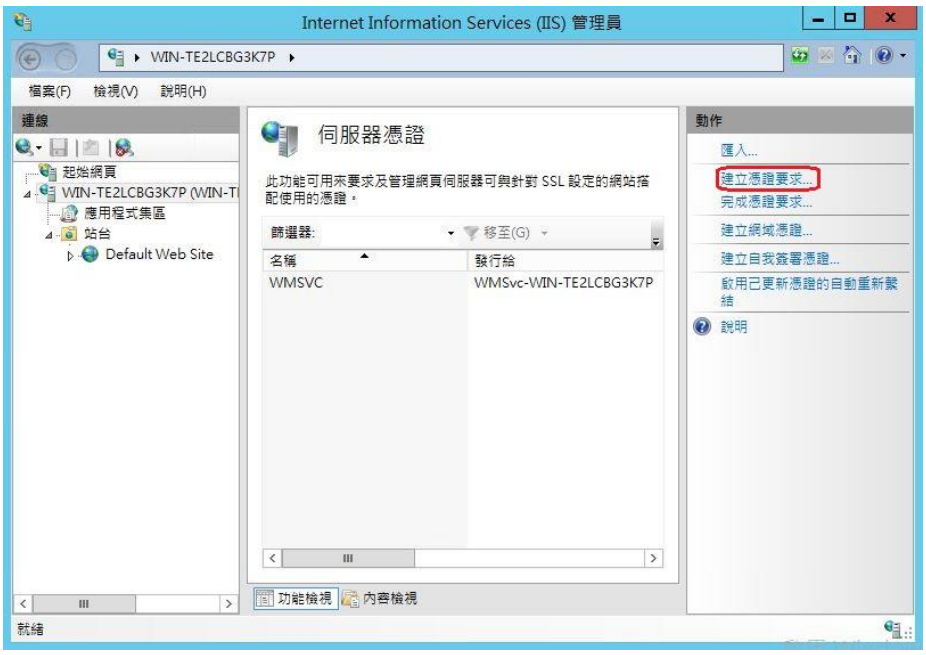
一、CSR 產生

1. 「開始」 → 「Internet Information Service (IIS) 管理員」。

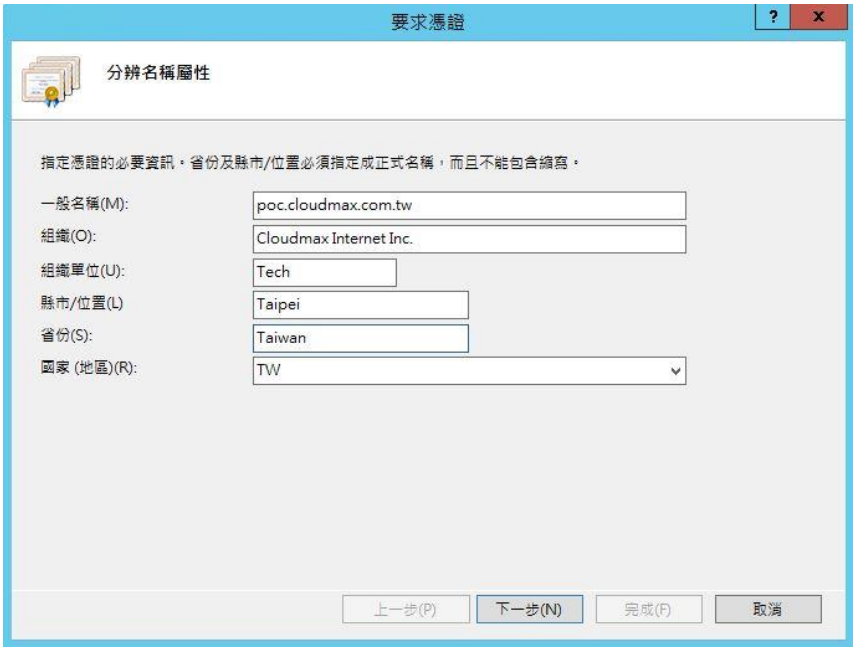
2. 左方「連線」工作視窗中選取認證網域之伺服器後，於「功能檢視」視窗點選「IIS > 伺服器憑證」。



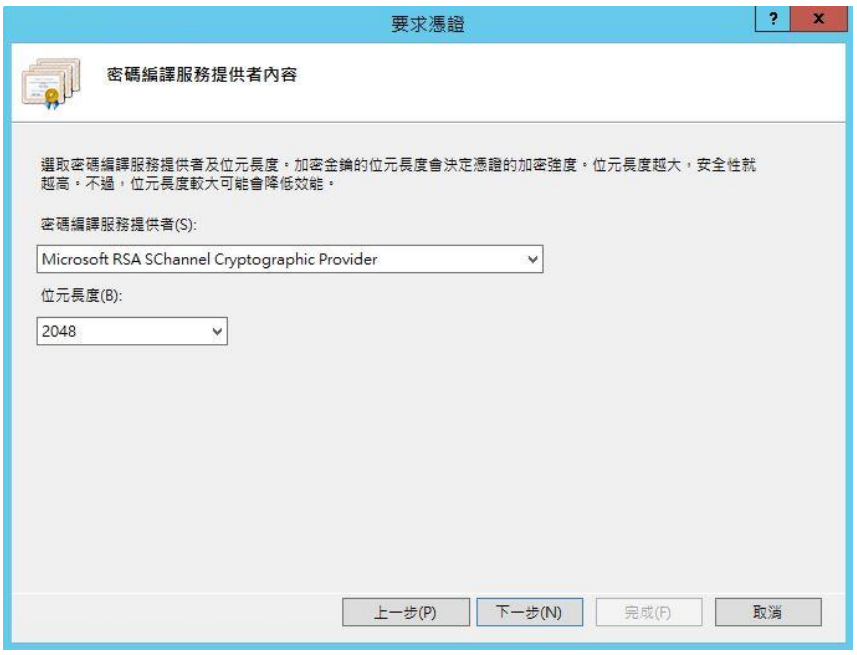
3. 點擊右方「建立憑證要求...」。



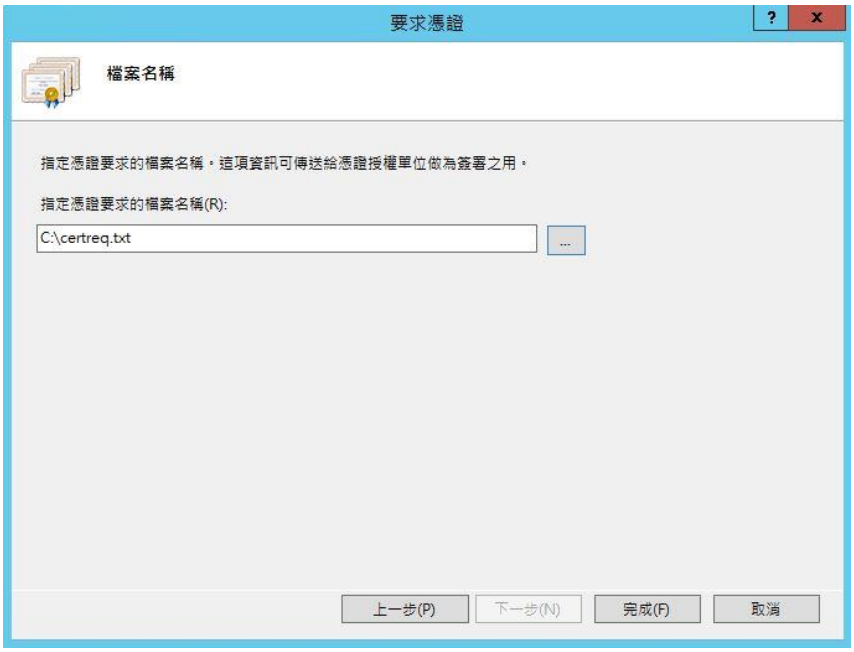
4. 輸入相關資訊。



5. 選擇「Microsoft RSA SChannel Cryptographic Provider」，位元長度「2048」。



6. 輸入要儲存的檔名，「完成」。



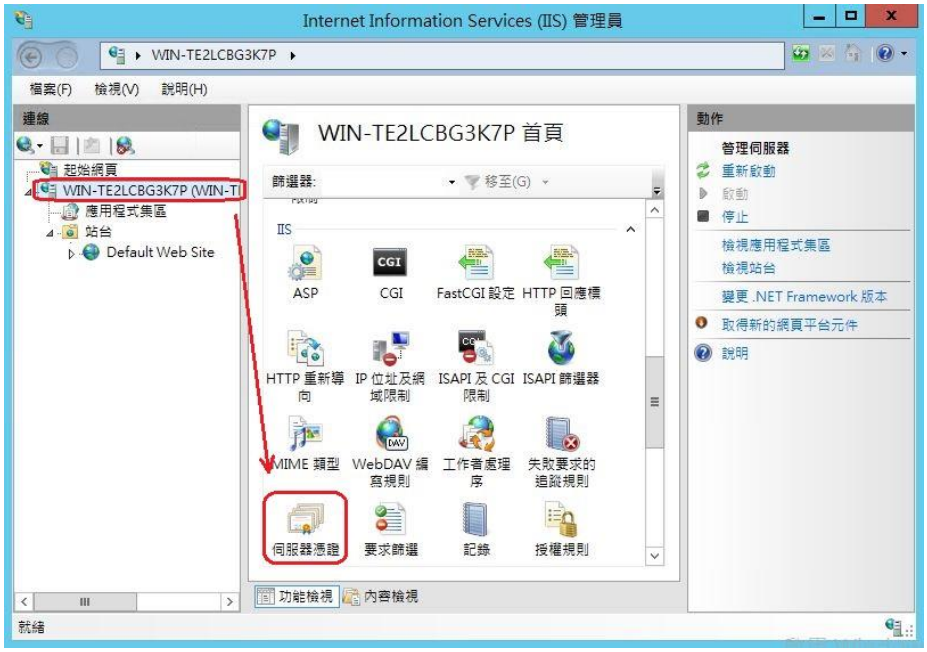
二、憑證安裝

1. 安裝

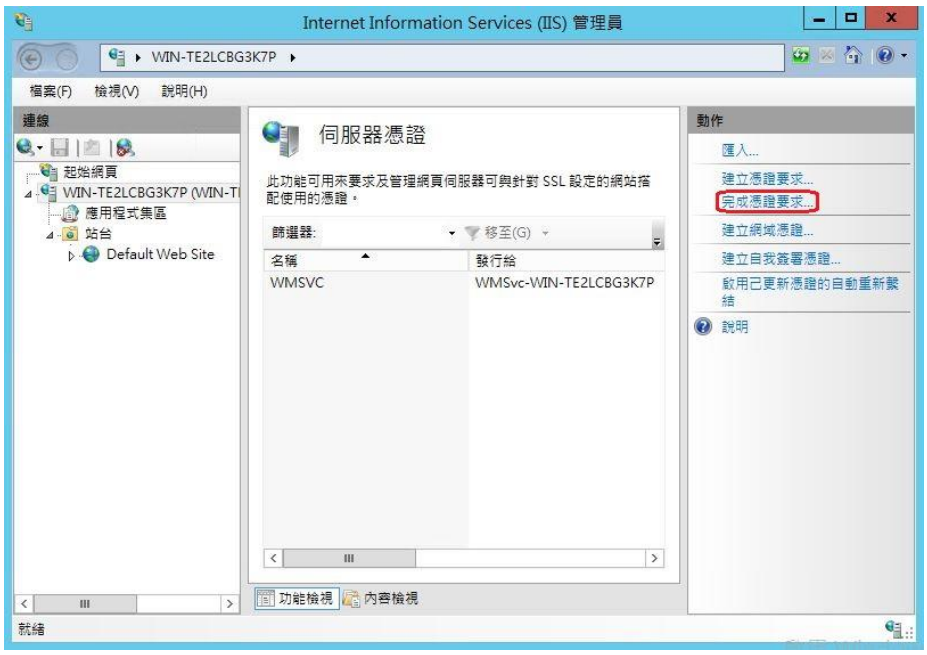
採用 IIS 精靈產生 CSR，請直接使用附檔名為『.cer』的格式完成安裝。

1.1 「開始」 → 「Internet Information Service (IIS) 管理員」

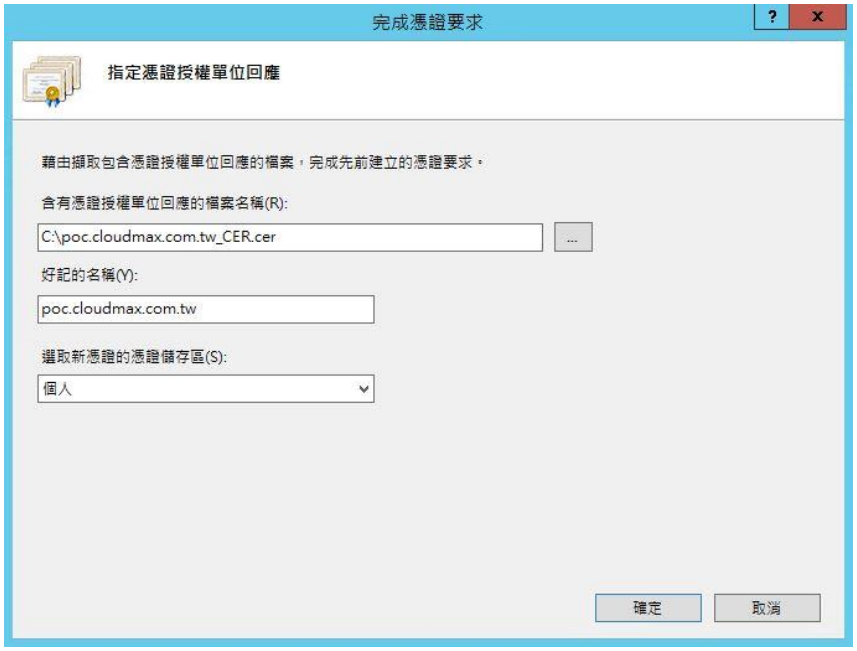
1.2 左方「連線」工作視窗中選取認證網域之伺服器後，於「功能檢視」視窗點選「IIS > 伺服器憑證」。



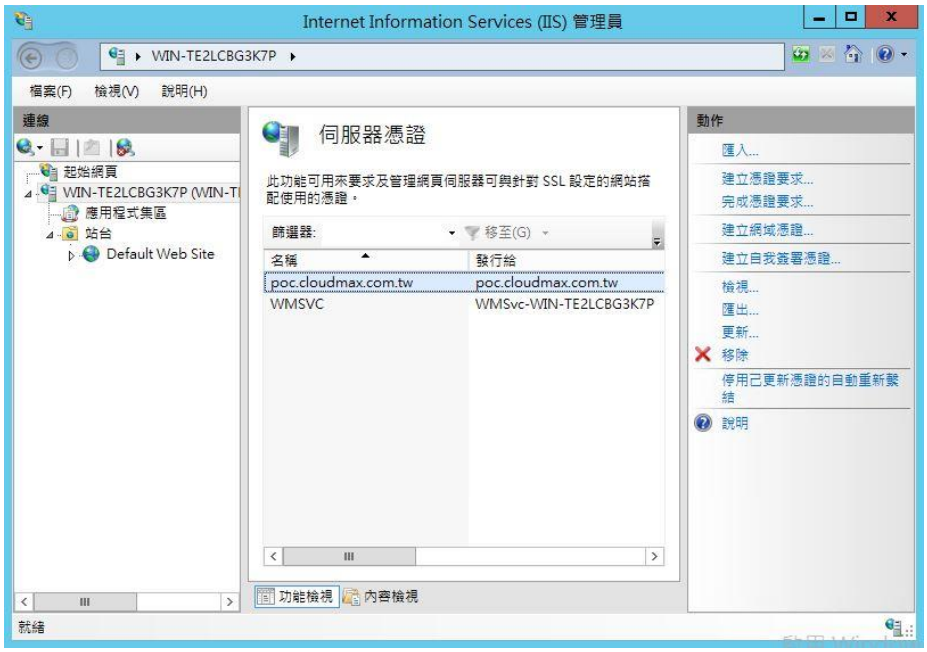
1.3 點擊右方「完成憑證要求...」。



1.4 「含有憑證授權單位回應的檔案名稱(R):」輸入要安裝的憑證。
「好記的名稱(Y): 」輸入憑證名稱或自己好記的名字。
「選取新憑證的儲存區」依個人喜好選擇。



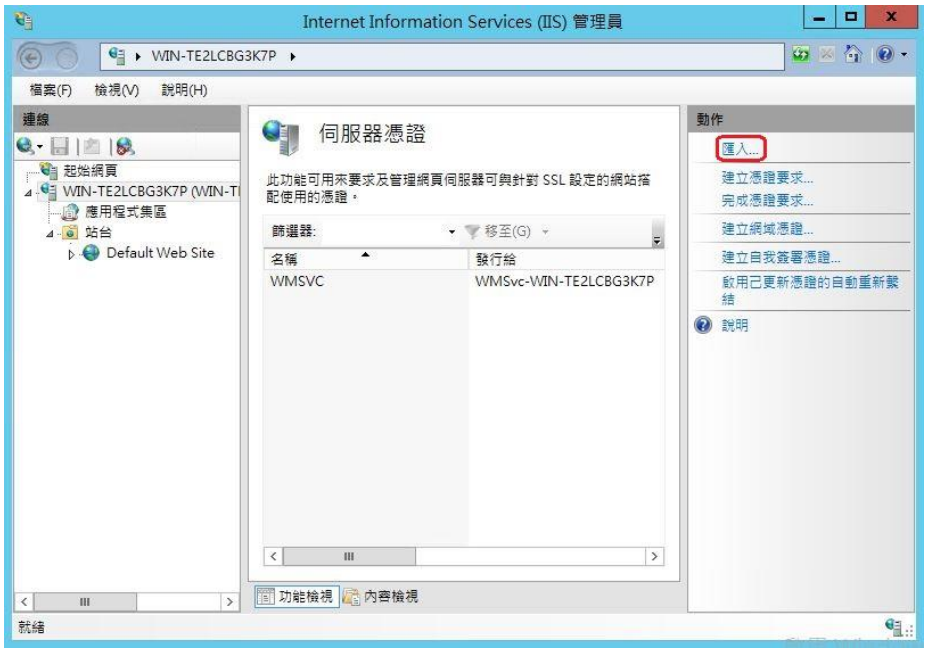
1.5 「確定」後即可看到憑證已安裝完成。



2. 匯入

使用 OpenSSL 產生 CSR，請使用匯入

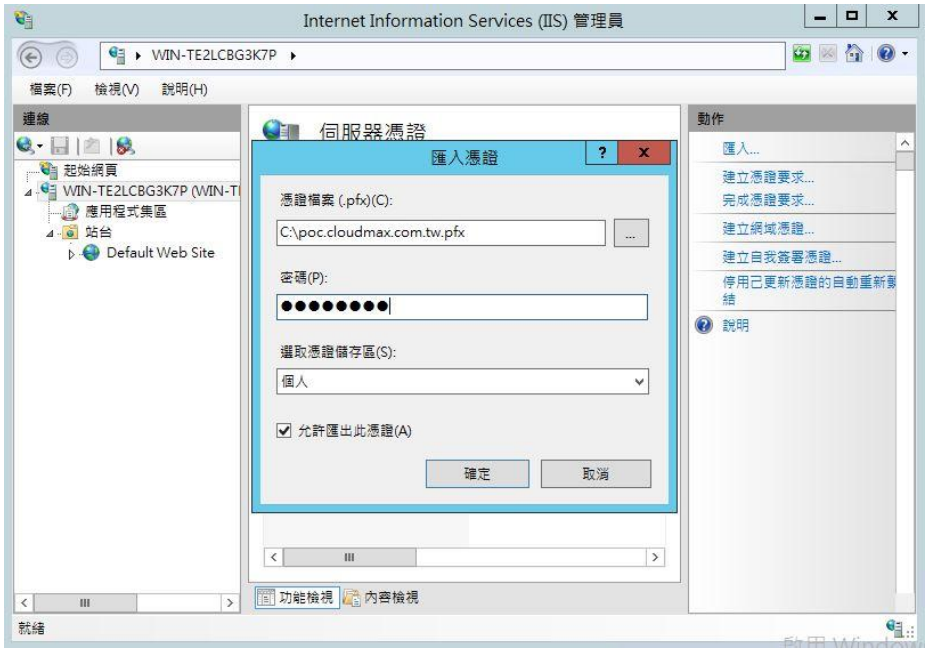
2.1 點擊右方「匯入...」。



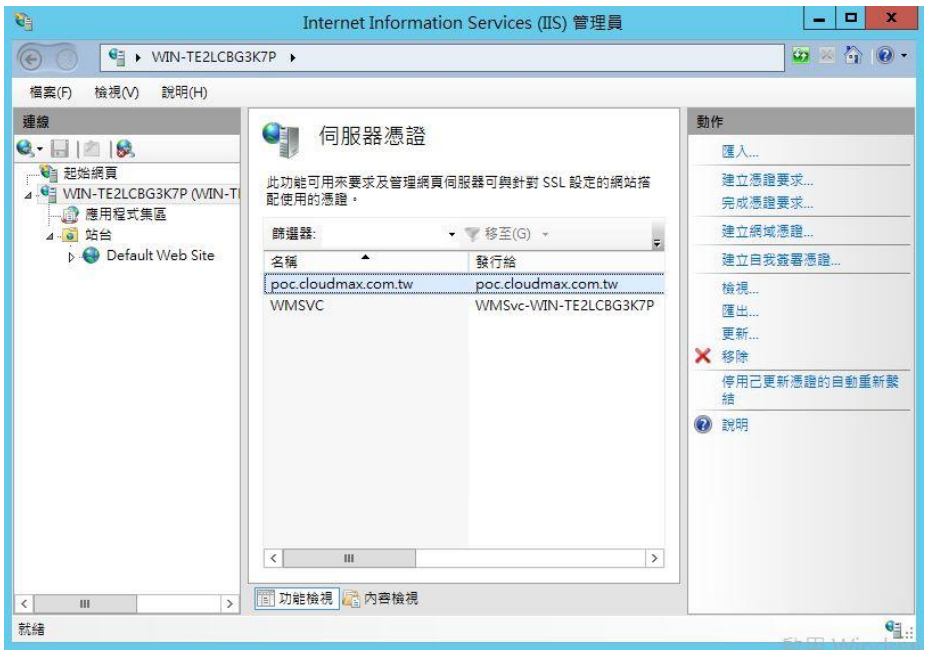
2.2 「憑證檔案(.pfx)(C):」輸入要匯入的憑證檔(.pfx)路徑。

「密碼(P):」輸入建立.pfx 檔案時加密的密碼。

「選取憑證儲存區」依個人喜好選擇。



2.3 「確定」後即可看到憑證已安裝完成。



三、憑證轉檔 PFX

若您是使用 Linux 產生的 SSL 的 key 與 csr 檔案，在簽發完成後會取得一個合法的 SSL crt 檔案，就必需將 SSL key 與取得的 crt 檔案轉為 Windows IIS 所使用的憑證 pfx 檔案。

需要的清單如下：

- 憑證私鑰檔 (如 domain.key)
- 憑證檔 (如 domain.cer、domain.crt)
- 簽發者憑證檔 (如 domain_CA.cer、domain_CA.crt) 等等

接著使用 Openssl 指令轉換為 pkcs12 格式，如下

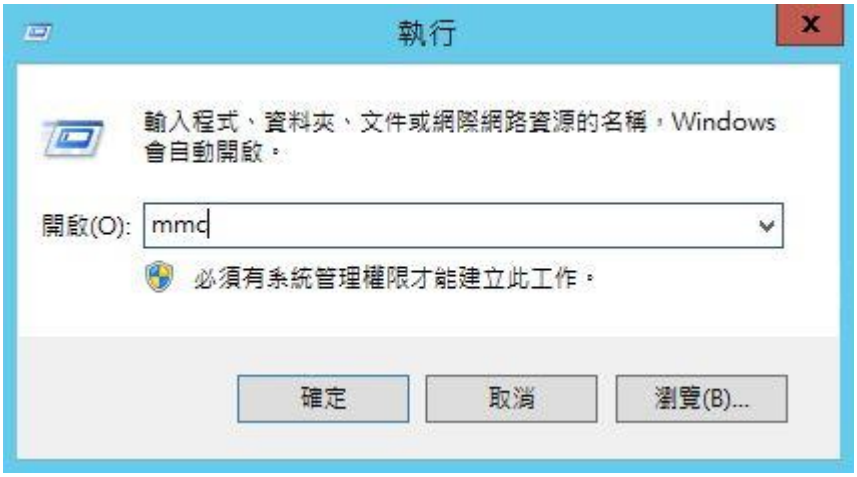
```
Demo >openssl pkcs12 -export \
> -out poc.cloudmax.com.tw.pfx \
> -inkey poc.cloudmax.com.tw_KEY.key \
> -in poc.cloudmax.com.tw_CER.cer \
> -certfile poc.cloudmax.com.tw_CA.cer
```

openssl pkcs12 -export -out 要儲存的名稱.pfx -inkey 憑證私鑰檔.key -in 憑證檔.cer -certfile 簽發者憑證檔_CA.cer

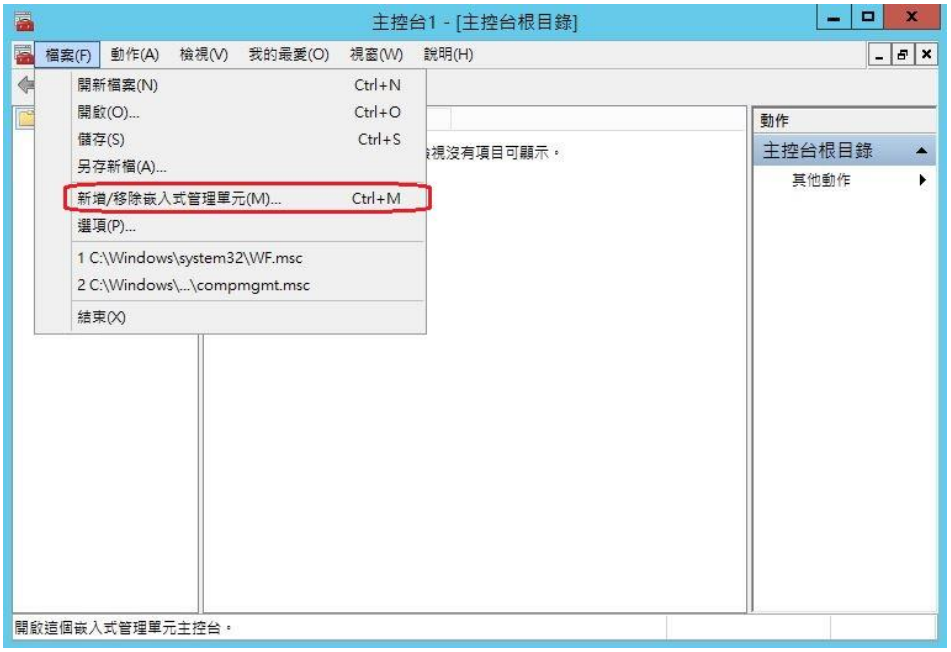
四、憑證匯出

1. 使用主控台（MMC）

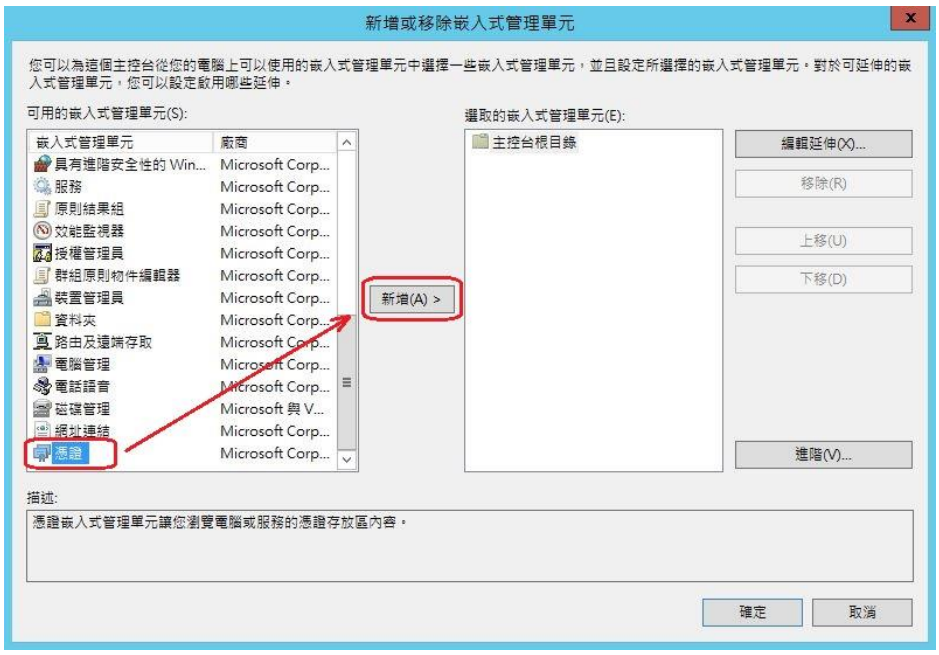
1.1 「開始」點擊執行後輸入 mmc。



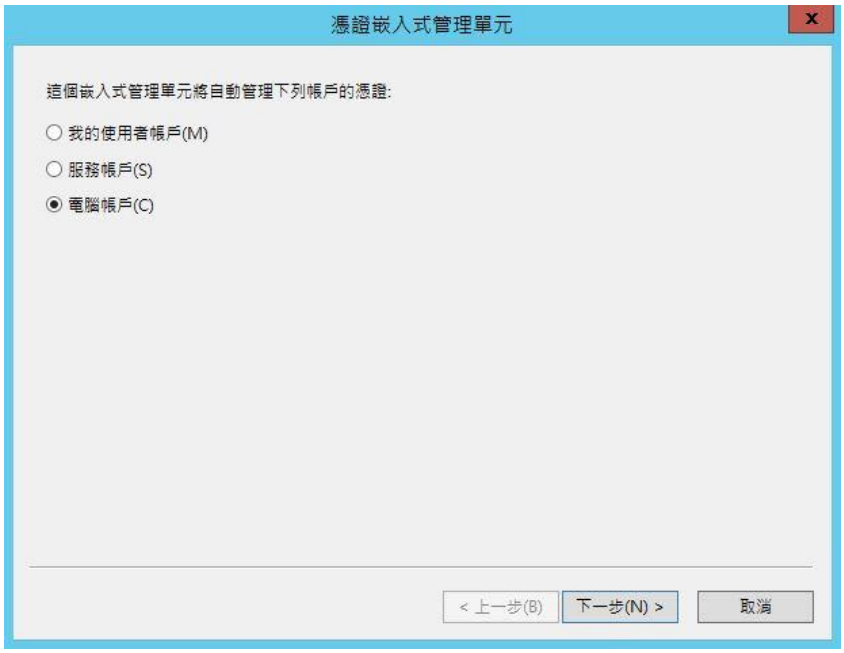
1.2 點擊左上角「檔案」 → 「新增/移除嵌入式管理員元(M)...」。



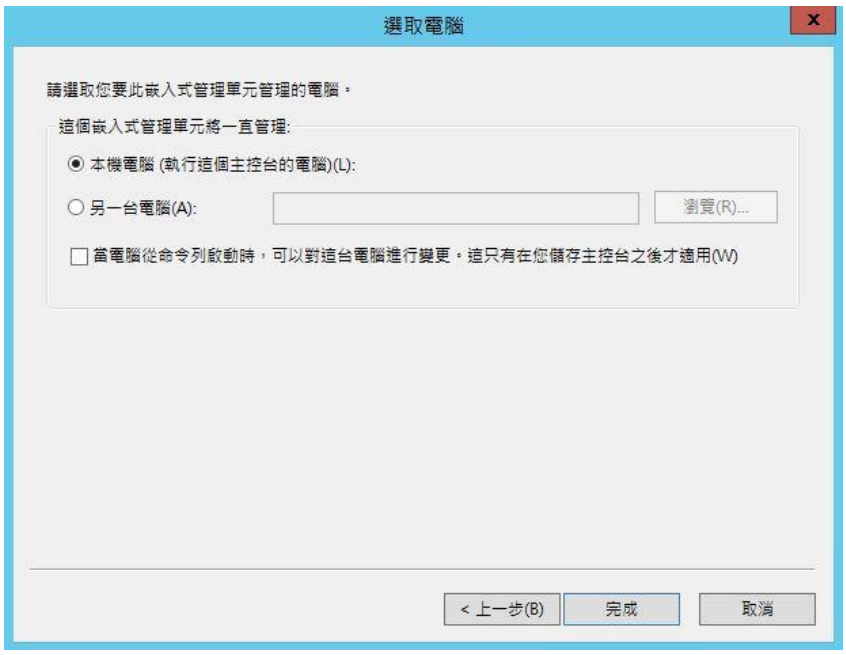
1.3 尋找到「憑證」後點中間的「新增(A) >」。



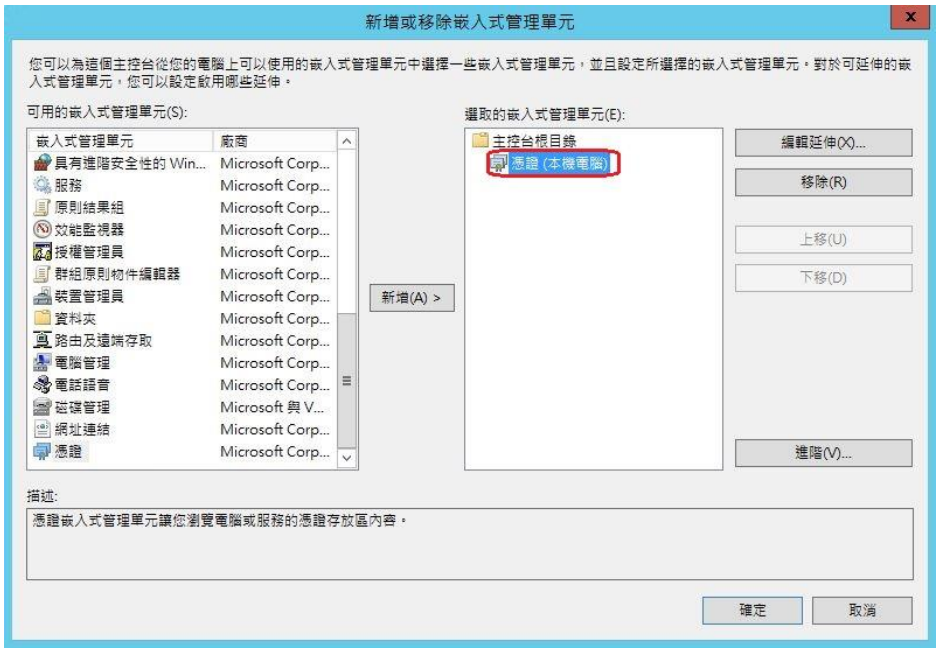
1.4 選擇「電腦帳戶(C)」。



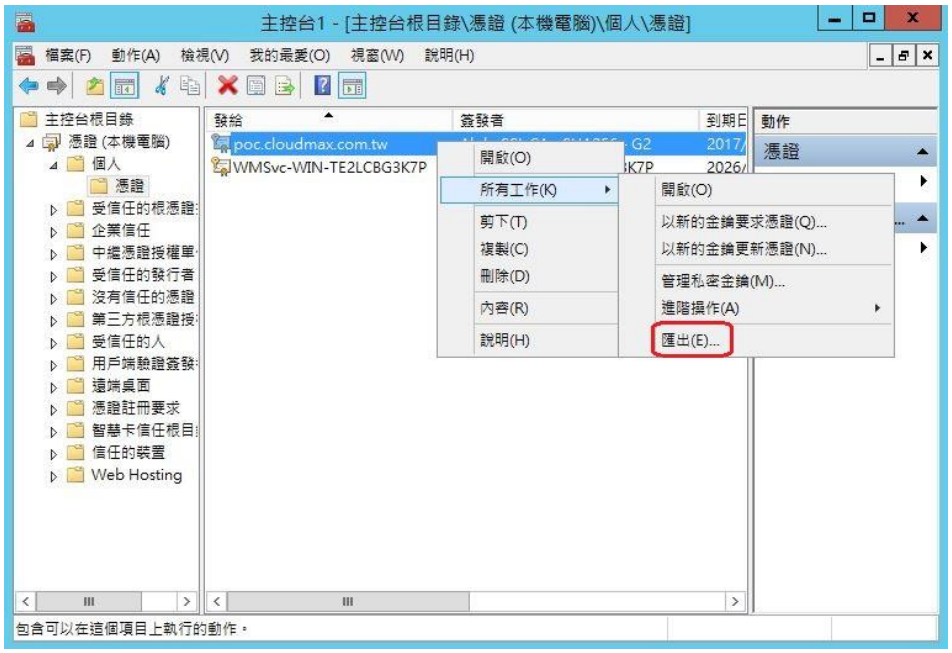
1.5 選擇「本機電腦(執行個這主控台的電腦)(L):」 → 「完成」。



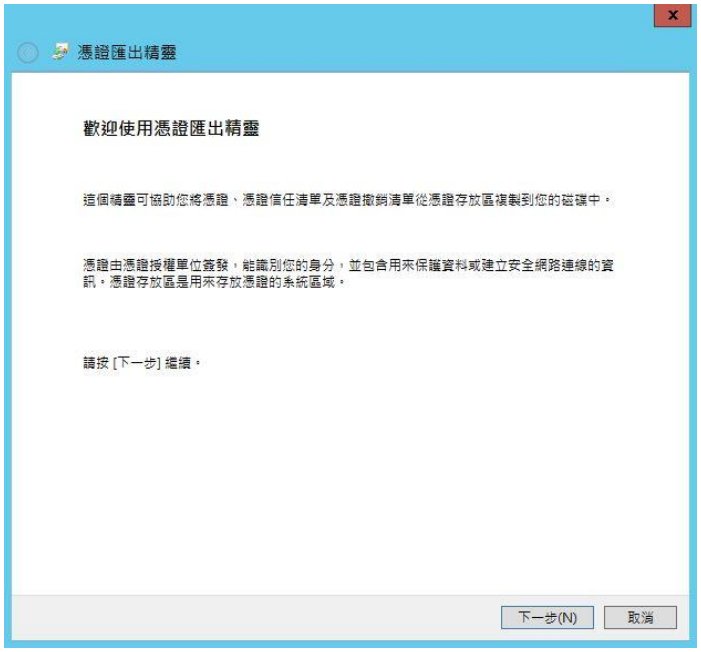
1.6 完成後可看到「憑證(本機電腦)」會出現在右邊方框內，點選「確定」。



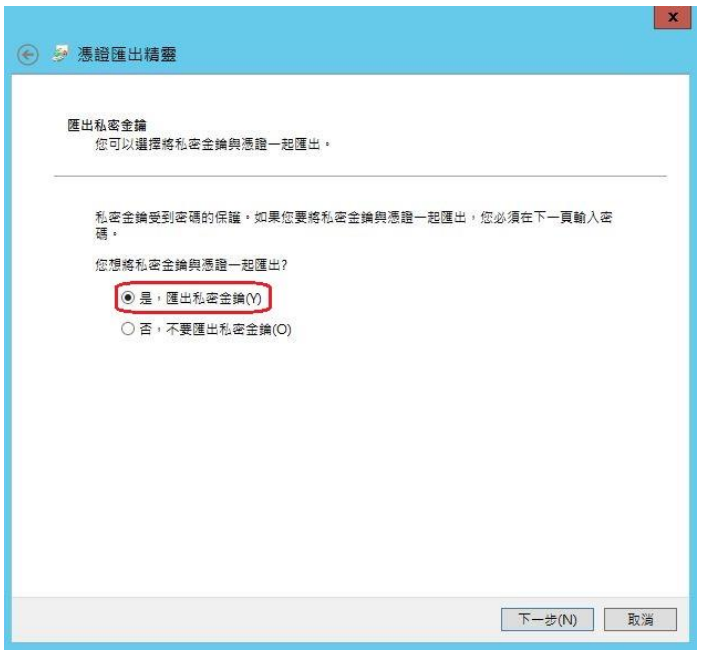
1.7 選擇「個人」 → 「憑證」後可看到有安裝哪些憑證，點擊滑鼠右鍵 → 「所有工作」 → 「匯出」。



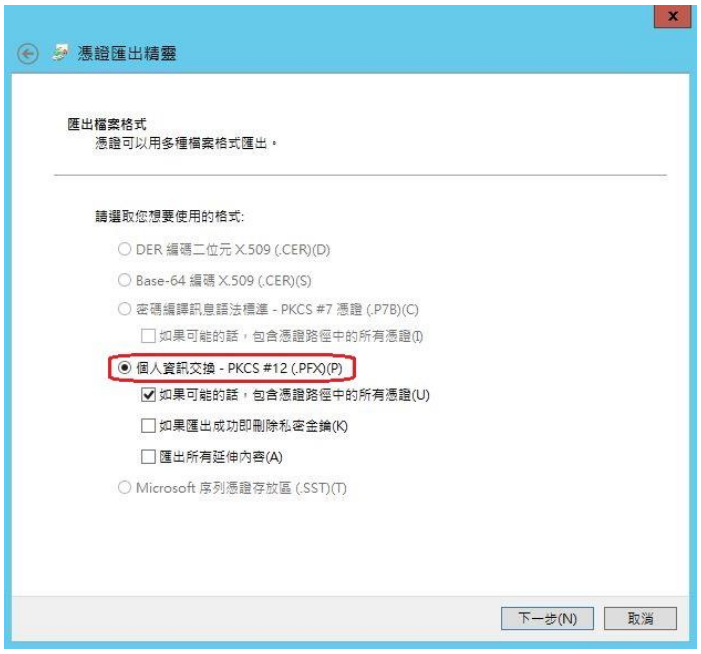
1.8 「下一步」。



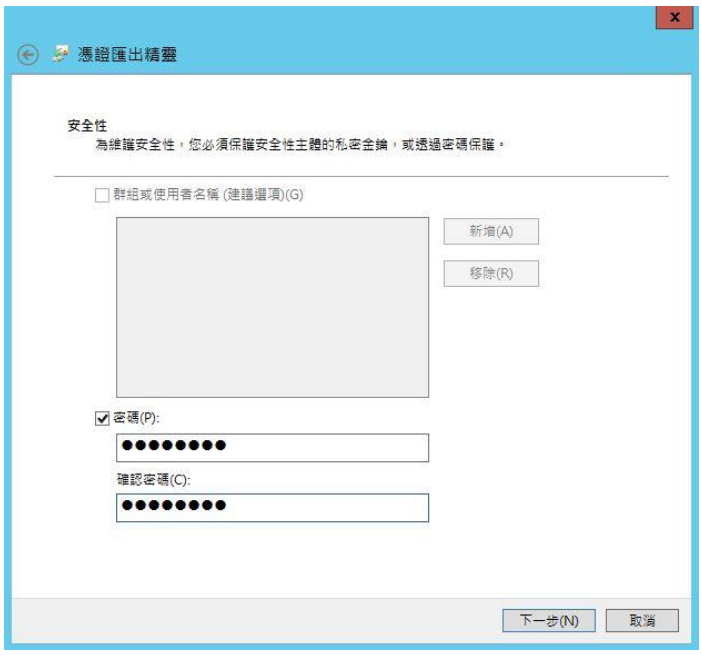
1.9 選擇「是，匯出私密金鑰(Y)」。



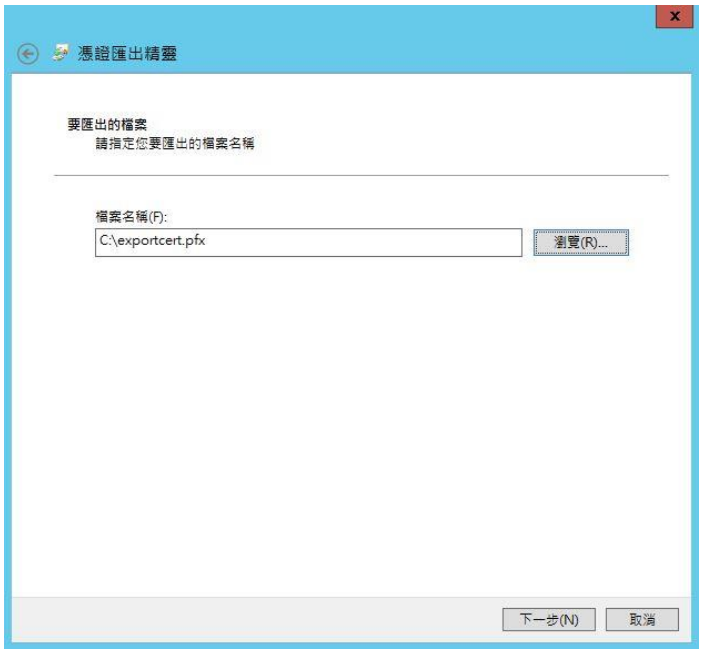
1.10 選擇「個人資訊交換，PKCS #12 (.PFX)(P)」，下方選擇依個人需求勾選。



1.11 輸入要保護的密碼 → 「下一步」。



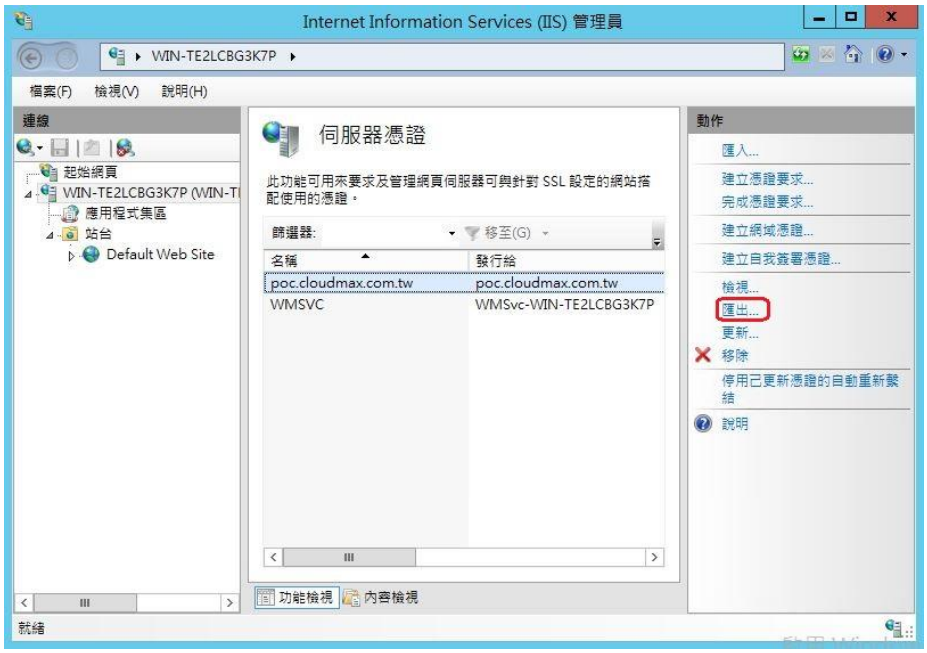
1.12 輸入要儲存憑證的路徑後「下一步(N)」。



1.13 點選「完成」後，「確認」以關閉匯出成功之訊息。

2. 使用 Internet Information Services (IIS) 管理員

2.1 點選右邊的「匯出...」。



2.2 輸入要儲存憑證的路徑、輸入要保護的密碼 → 「確定」