匯智資訊股份有限公司

SSL 數位憑證

IIS7 憑證安裝說明

匯智資訊
cloudmax
www.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

【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、選擇產生 CSR 檔案方式

CSR 檔案為提供給憑證中心驗證的檔案，透過此 CSR 檔案憑證中心將會簽發 CER 檔案；而產生 CSR 檔案的同時會一併會產出 KEY 檔案，而這三個檔案為互相匹配憑證才可正常運行。

1. 使用 OpenSSL 或透過線上生成工具產生 (申請 GeoTrust 使用)

若您為申請 GeoTrust 的憑證，我們建議您可以直接使用我們的 OpenSSL 線上產生工具，來快速產生 CSR 檔，並且將所產生出來的 CSR 檔案提交給匯智，一併產出的 KRY 檔案請您務必儲存，以利後續憑證安裝過程順利。

GeoTrust 線上生成 CSR 工具：

http://geotrust.cloudmax.com.tw/OpenSSL/CreateCSR.asp

SSL 線上應用工具：

https://www.cloudmax.com.tw/service/ssl-tools

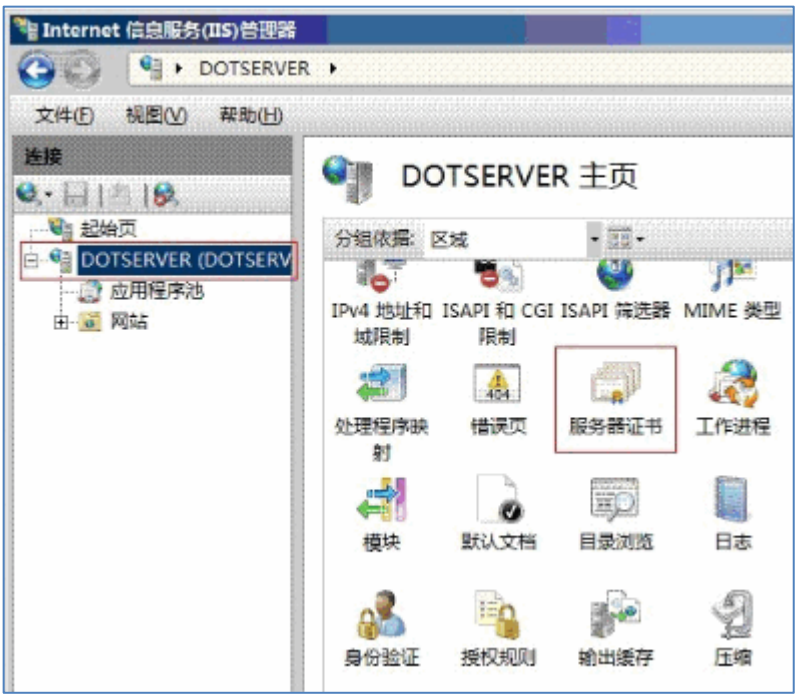
匯智資訊 cloudmax

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

2. 透過 IIS 伺服器產生 (申請 GlobalSign 使用)

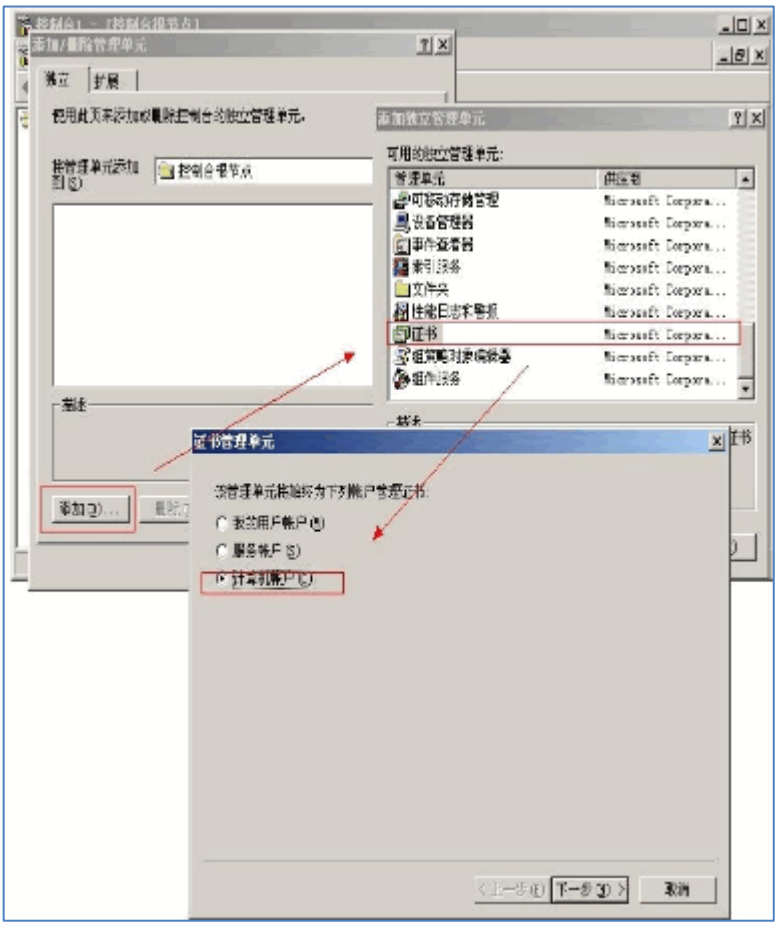
若您為申請 GlobalSign 的憑證，我們建議您直接於 IIS 伺服器上產生 CSR 的資訊，產生的步驟如下表：

1. 打開 IIS 服務管理器，點擊計算機名稱，雙擊打開右則的伺服器憑證圖標

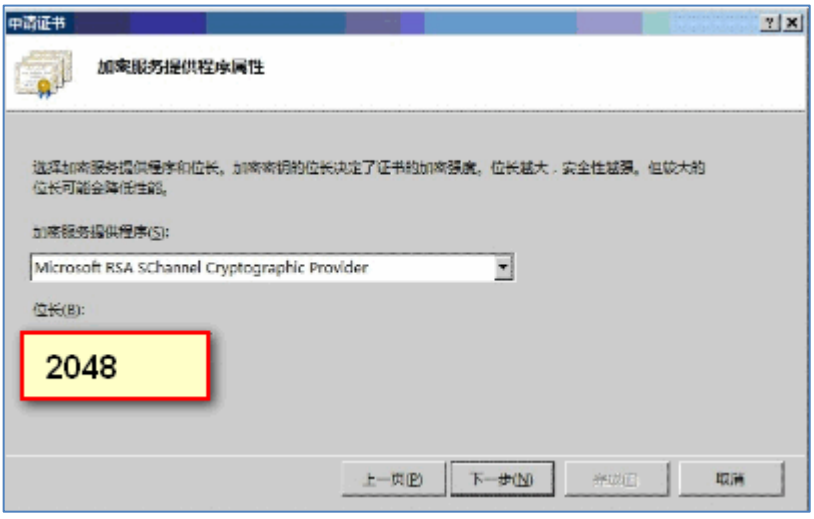


2 雙擊打開伺服器憑證後，點擊右則的創建憑證申請

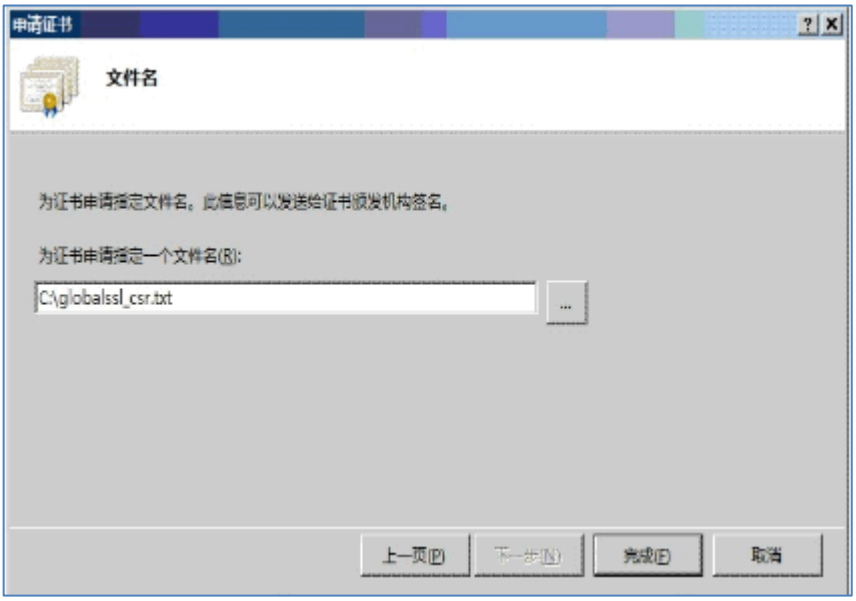
3 輸入申請數位憑證訊息（必須為英文字符），點擊下一步



4 選擇加密服務提供程序(默認)，密鑰長度目前憑證中心僅頒發 2048 的憑證資訊。



5 選擇憑證籤名請求（CSR）文件保存的路徑和文件名，點擊完成



*若透過 IIS 產生 CSR 檔案，KEY 檔案將會直接儲存於此 IIS 伺服器中。

二、安裝前注意事項

數位憑證是由私密金鑰（private key）與公開金鑰（public key)兩個部分組成，在進行安裝及使用數位憑證前，須將私密金鑰與公開金鑰檔案放置於伺服器可讀取之儲存區中。

依伺服器網路環境不同而實際需求各異，以下列出安裝時常見忽略的狀況：

·伺服器是否正常連上 Internet？

·HTTPS 協定之通訊埠是否開啟[1]？

·部分狀況下，伺服器需要額外的固定 IP[2]支援；此時需調整網址之 A 紀錄[3]。

·與伺服器串連的網路設備通訊埠的狀態是否設定完成[4]？

若無法確認網路環境，或您非相關設備或服務的權限擁有者，應與設備、系統所屬管理員或該服務、設備提供商諮詢及確認。

安裝過程中，因操作錯誤或其他不可預期因素，可能導致系統資料異常、毀損，請在系統更動前，將重要系統及資料進行備份。

[1] HTTPS 協定預設使用 Port 443，但使用者可依實際狀況進行調整。
[2] 多個網站共用同一台伺服器的情況下(如虛擬主機)，需要利用額外的固定 IP 以解決通訊埠不足的問題。
[3] 須注意您是否擁有修改 DNS(Domain Name Service) Server 權限，且 DNS 紀錄修改需要生效時間。
[4] 例如防火牆、負載平衡裝置、代理伺服器等，可能須調整規則、開啟通訊埠，甚至部分設備也需要安裝、支援數位憑證。

三、數位憑證安裝前準備確認事項

憑證核發成功後，指定的 Email 信箱將可收到國外認證中心發的英文通知信與匯智的中文通知信，而信中將會提供憑證中心所簽屬的 CER 檔案與憑證中繼憑證檔案，這些資訊將以純文字的方式來顯示，請您進行以下的動作確認所頒發的憑證資訊是否正確。

1 請協助查看憑證資訊檔案文本資料中


寄件者: WIS 匯智主機服務部 <service@wis.com.tw>
收件者: WIS 匯智主機服務部 <service@wis.com.tw>
副本:
主旨: [WIS 匯智回覆] 憑證完成通知

，您好：

貴公司的憑證已申請完成，下列資訊請您確認：

憑證有效期限: 2011-07-12 ~ 2014-07-14 (憑證到期時間以格林威治時間為準，請參考憑證訊息)

另外以下為憑證及標章安裝說明，供您參考設定。

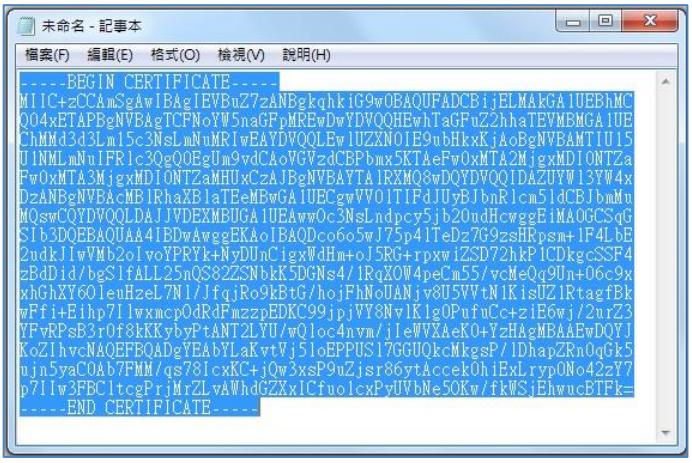
憑證資訊：

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

2 請複製憑證資訊(包含)『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』)

3 開啟純文字檔案，貼上您所複製的資訊



4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer)，所見的圖示將會變成 

5 請點擊憑證檔案，確認憑證網域、簽發者單位、有效期間是否為正常資訊

四、選擇安裝方式

上述的憑證資訊確認完畢後，我們即將開始要把憑證安裝於伺服器當中，於第一大項時，我們有介紹兩種因申請不同憑證廠商而建議的生成方式，請參考以下資訊來完成憑證安裝。

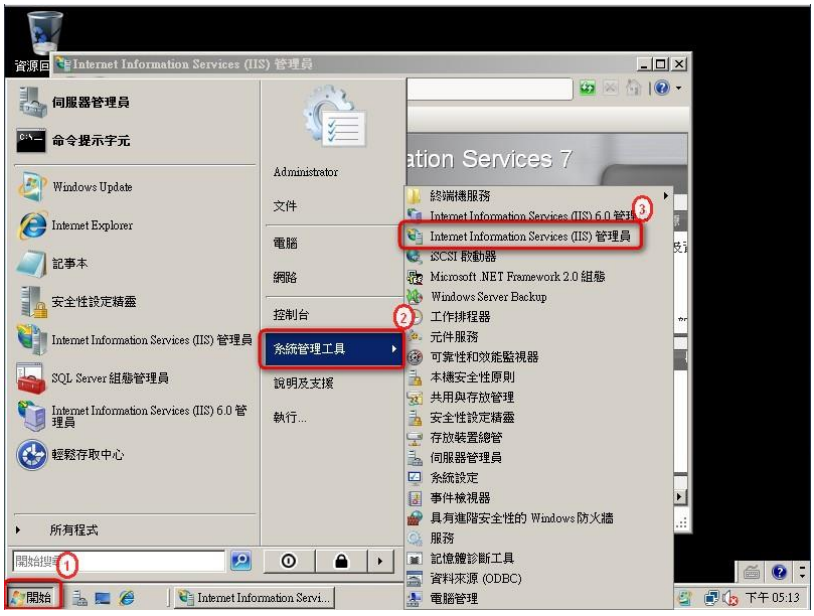
1. CSR 透過線上 OpenSSL 生成 (操作僅限申請 GeoTrust)

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件)以及 KEY 的文本資訊(當時透過 OpenSSL 或是線上生成工具時一併產生的 KEY 檔案)，請準備好兩項的資訊，連入 Geotrust PFX 線上合成工具，並且依照網頁指示完成 PFX 檔案的匯出。

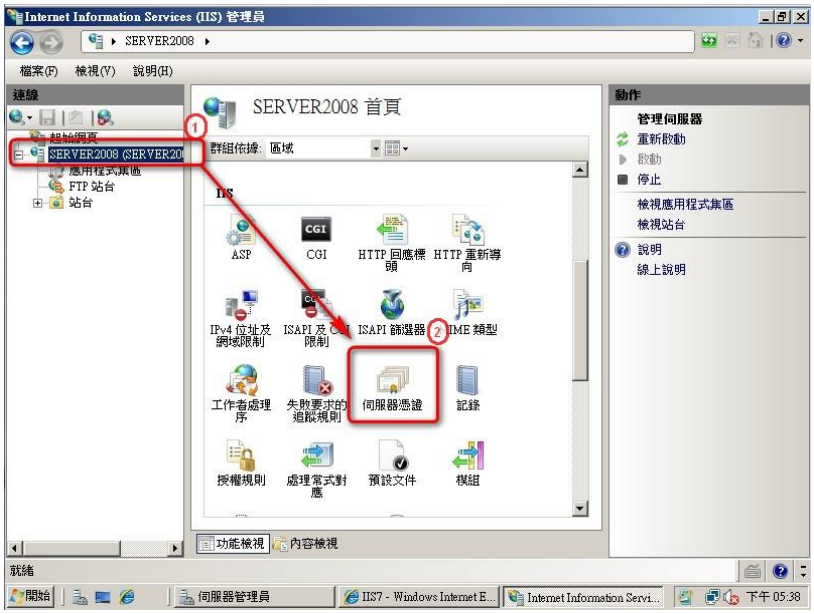
GeoTrust PFX 線上合成工具：http://geotrust.cloudmax.com.tw/OpenSSL/CreatePFX.asp

**** 僅限申請 GeoTrust 憑證適用，因線上合成工具會一併合成 GeoTrust 對應的中繼憑證。***

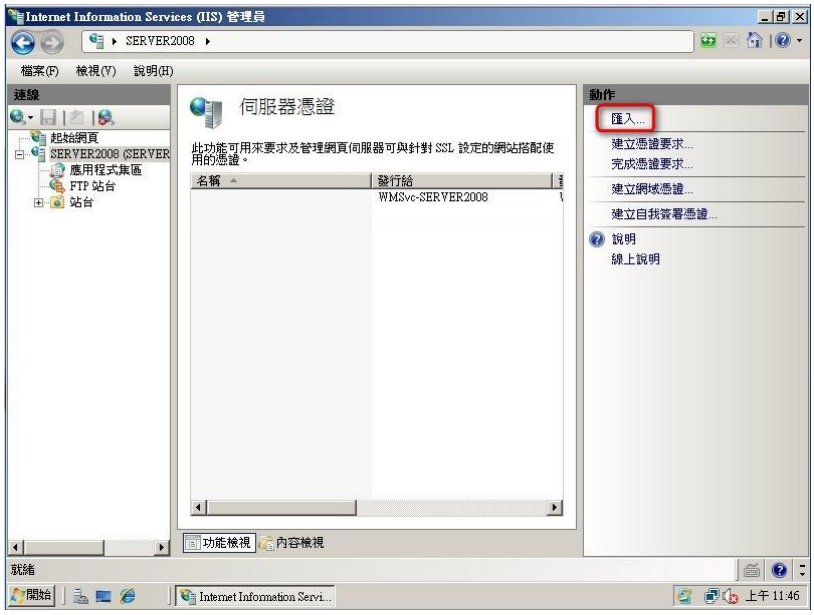
1. 點選『開始 > 系統管理工具 > Internet Information Services (IIS) 管理員』。



2 『連線』視窗中選擇伺服器後，點選『功能檢視 > IIS『伺服器憑證』。

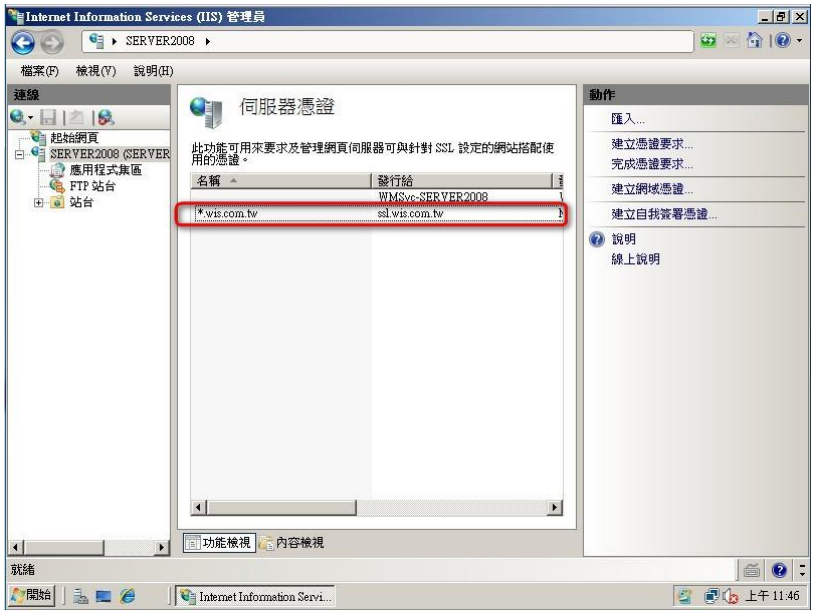


3 於右方『動作』工作視窗點選『匯入』。

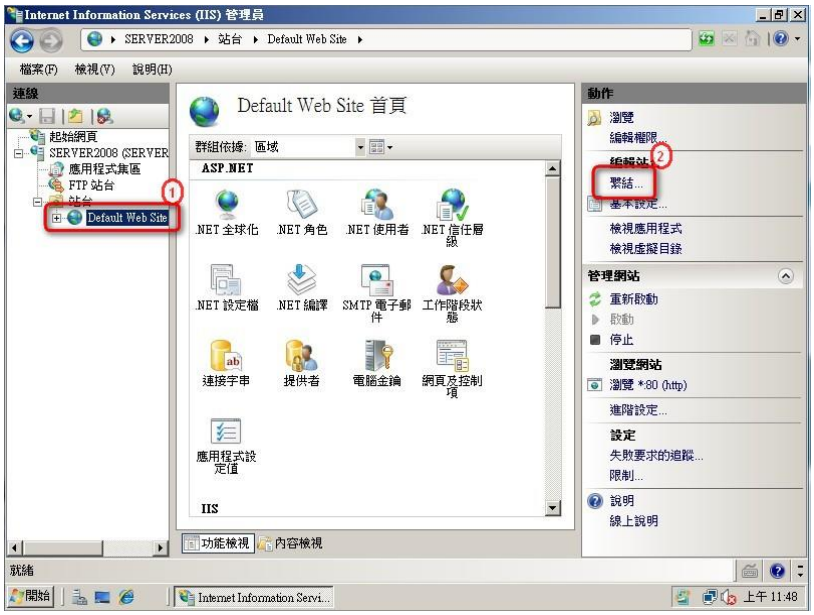


4 找到對應的 PFX 檔案路徑位置；『密碼(P)』中輸入線上工具合成時設定的密碼，最後按下『確定』

5 成功匯入之憑證將列於『伺服器憑證』工作視窗中。



6 『Internet Information Services (IIS) 管理員 > 站台』選取申請憑證之網站(若伺服器上只有一個站台則為『Default Web Site』)後，點選『動作 > 繫結』。



7 『新增(A)』。

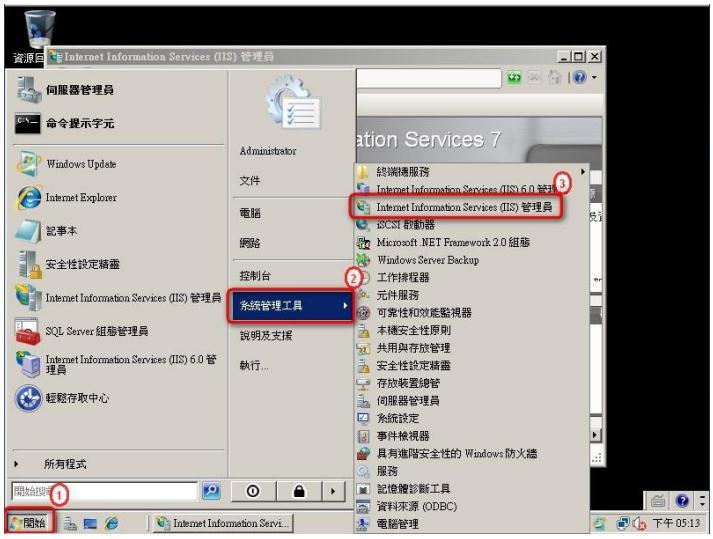
8 視實際部署狀況分別選擇及填入『新增站台繫結』工作視窗中要求之欄位，設定完畢後，按『確定』完成繫結。

憑證安裝完成，您可以直接跳到 五、檢查憑證安裝是否正確

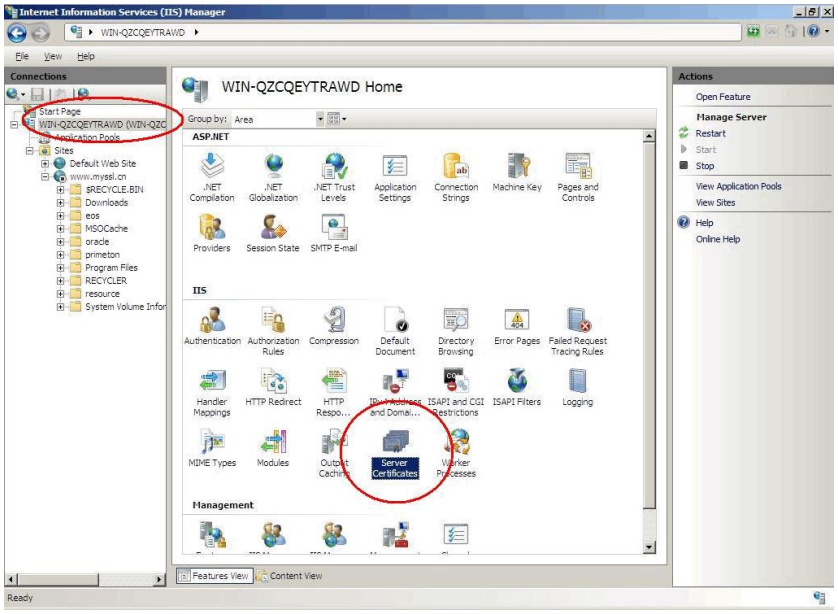
2. CSR 透過 IIS 伺服器產生

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件)，因您的 CSR 由 IIS 伺服器直接產生，所以 KEY 檔案將會直接保留再 IIS 中，請您依照以下的步驟將簽發下來的 CER 資訊匯入 IIS 伺服器：

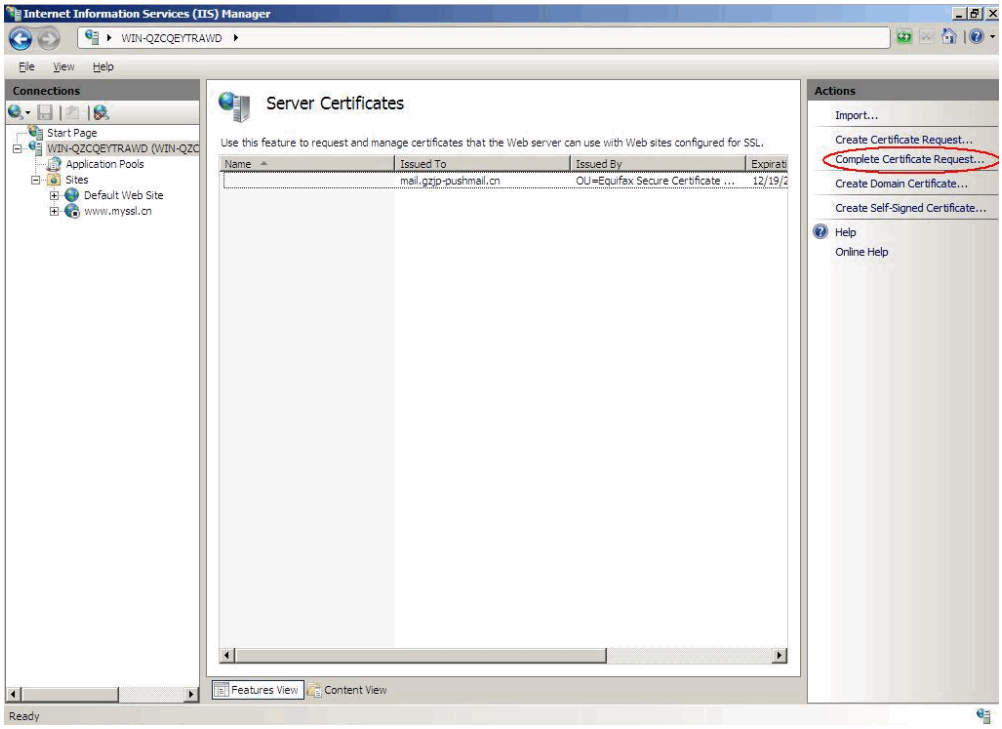
1 點選『開始 > 系統管理工具 > Internet Information Services (IIS) 管理員』。



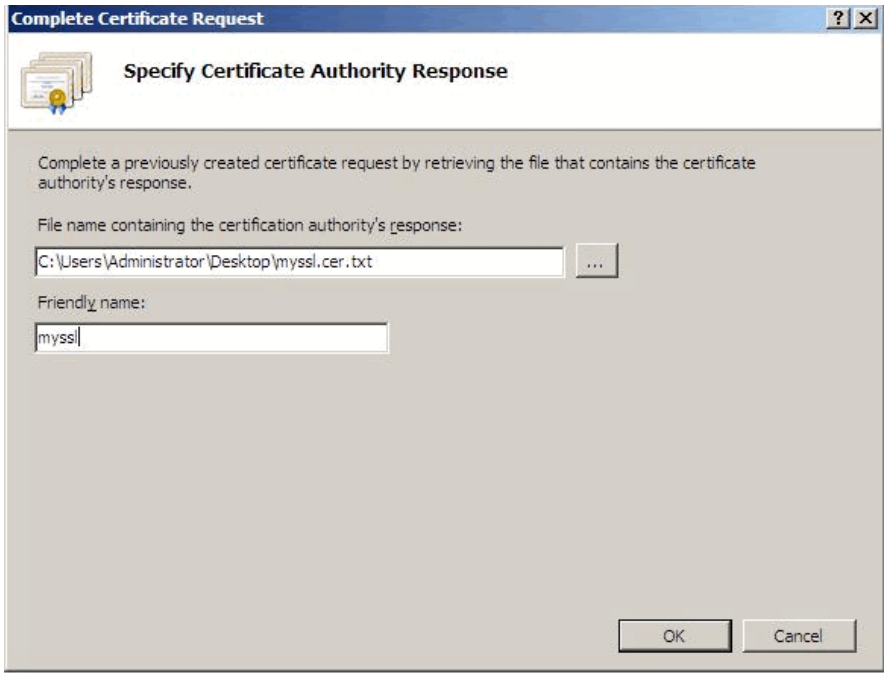
2 『連線』視窗中選擇伺服器後，點選『功能檢視 > IIS『伺服器憑證』。



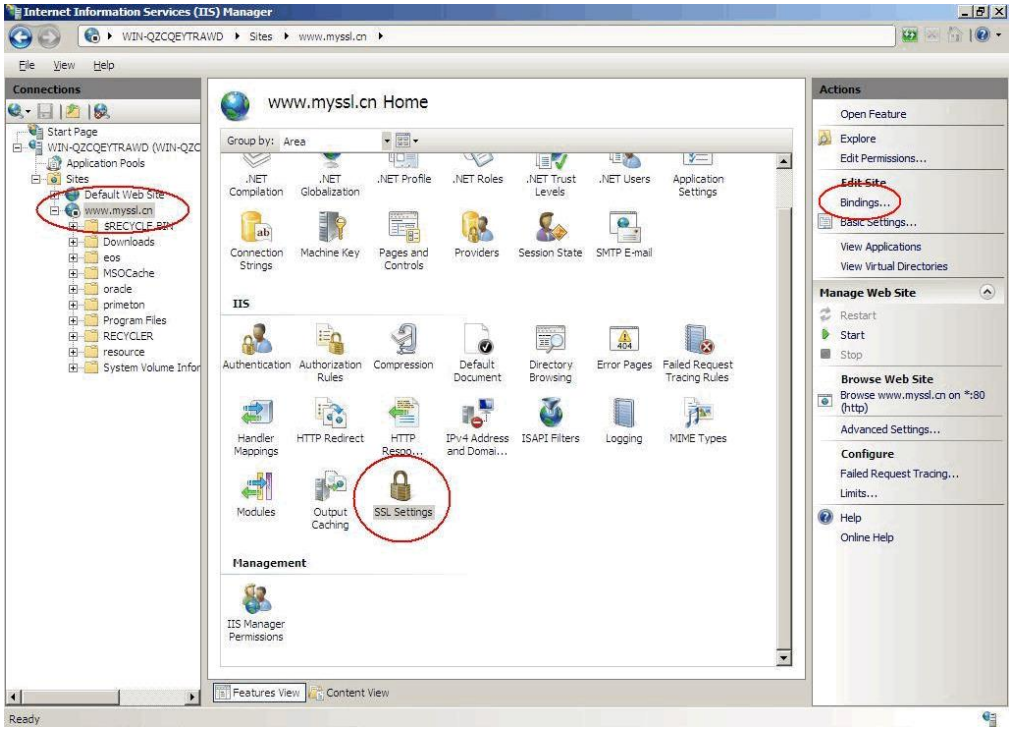
3 於右方『動作』工作視窗點選『完成憑證要求』。



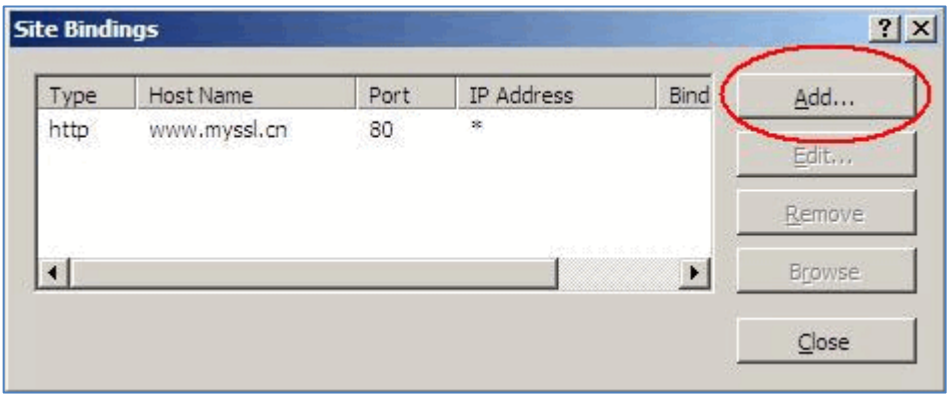
4 找尋核發下來的憑證檔案，並且取一個好記的名稱



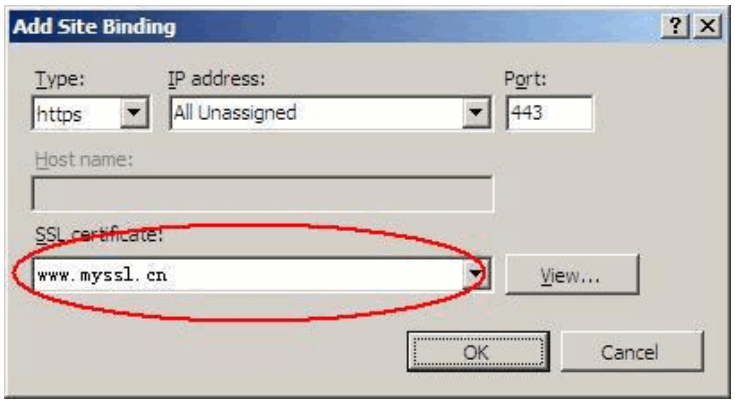
5 進入站台的 SSL 設定，並且點選繫結



6 點選加入



7 選擇剛剛所設定的 SSL 好記名稱的憑證



3. 匯入中繼憑證檔案

※ 若您的憑證有使用合成的方式匯入，可直接跳過此步驟。

電腦運算能力於近十年內大幅提升，為確保憑證用戶網路資料傳輸安全，各大憑證中心於 2010 年起開始做根憑證 1024 升級為 2048 位元的作業，而舊的瀏覽器因缺少 2048 位元的根憑證資料，所以需要利用中繼憑證來進行交互驗證，確保於舊版本瀏覽器使用 HTTPS 連線時，不會出現錯誤或警告訊息，請您依照以下的步驟來完成中繼憑證匯入動作：

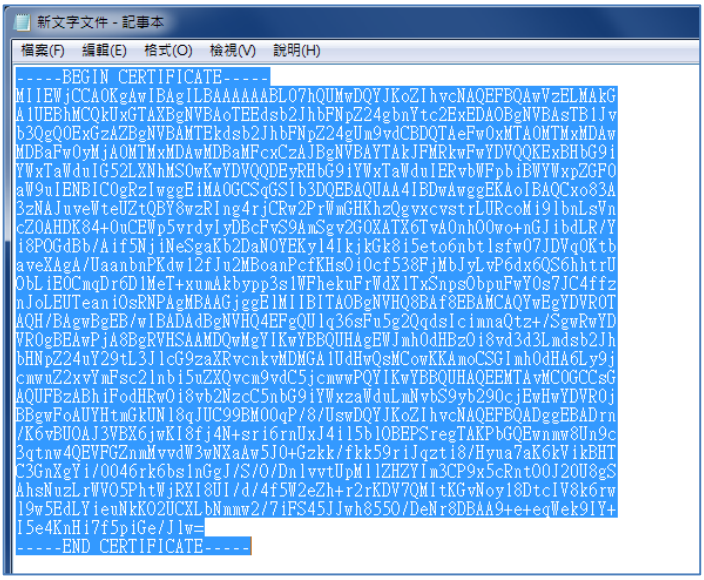
1 請協助查看憑證資訊檔案文本資料中「中繼憑證」

中繼憑證：

-----BEGIN CERTIFICATE-----
MIIEWjCCA0KgAwIBAgILBAAAAAABL07hQUMwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNpZ24gUm9vdCBDQTAeFw0xMTA0MTMxMDAw
MDBaFw0yMjA0MTMxMDAwMDBaMFcxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9i
YWxTaWduIG52LXNhMS0wKwYDVQQDEyRHbG9iYWxTaWduIERvbWFpbiBWYWxpZGF0
aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCxo83A
3zNAJuveWteUZtQBY8wzRIng4rjCRw2PrWmGHKhzQgvxcvstrLURcoMi9lbnLsVn
cZ0AHDK84+0uCEWp5vrdyIyDBcFvS9AmSgv2G0XATX6TvA0nhO0wo+nGJibdLR/Y
i8POGdBb/Aif5NjiNeSgaKb2DaN0YEKyl4IkjkGk8i5eto6nbtlsfw07JDVq0Ktb
aveXAgA/UaanbnPKdw12fJu2MBoanPcfKHsOi0cf538FjMbJyLvP6dx6QS6hhtrU
ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdXITxSnpsObpuFwY0s7JC4ffz
nJoLEUTeaniOsRNPAgMBAAGjggElMIIBITAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0T
AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimnaQtz+/SgwRwYD
VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAgEWJmh0dHBzOi8vd3d3Lmdsb2Jh
bHNpZ24uY29tL3JlcG9zaXRvcnkvMDMGA1UdHwQsMCowKKAmoCSGImh0dHA6Ly9j
cmwuZ2xvYmFsc2lnbi5uZXQvcm9vdC5jcmwwPQYIKwYBBQUHAQEEMTAvMC0GCCsG
AQUFBzABhiFodHRwOi8vb2NzcC5nbG9iYWxzaWduLmNvbS9yb290cjEwHwYDVR0j
BBgwFoAUYHtmGkUNl8qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEBADrn
/K6vBUOAJ3VBX6jwKI8fj4N+sri6rnUxJ4il5blOBEPSregTAKPbGQEwnmw8Un9c
3qtnw4QEVFGZnmMvvdW3wNXaAw5J0+Gzkk/fkk59riJqzti8/Hyua7aK6kVikBHT
C3GnXgYi/0046rk6bslnGgJ/S/O/DnlvvtUpMllZHZYIm3CP9x5cRntO0J20U8gS
AhsNuzLrWVO5PhtWjRXI8UI/d/4f5W2eZh+r2rKDV7QMItKGvNoy18DtcIV8k6rw
l9w5EdLYieuNkKO2UCXLbNmmw2/7iFS45JJwh855O/DeNr8DBAA9+e+eqWek9IY+
I5e4KnHi7f5piGe/Jlw=
-----END CERTIFICATE-----

2 請複製憑證資訊(包含)『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』)

3 開啟純文字檔案，貼上您所複製的資訊

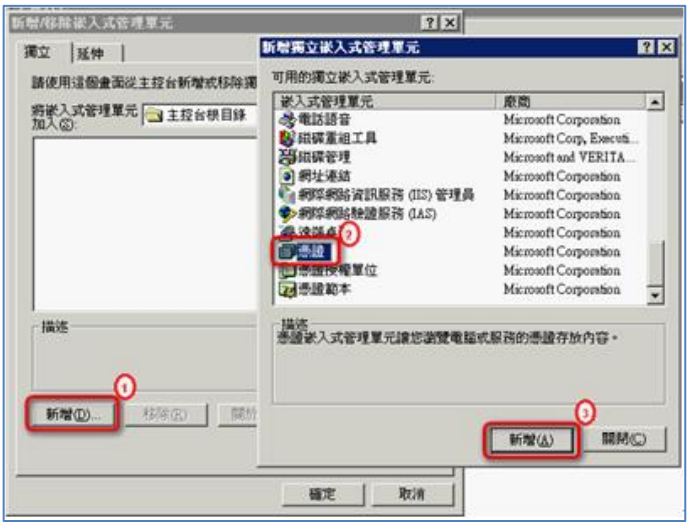


4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer)，所見的圖示將會變成 

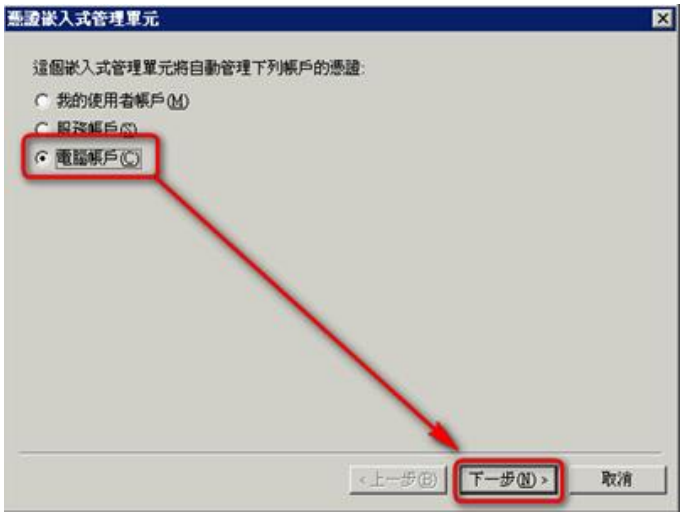
5 開始 > 執行(R)，輸入"mmc"

6 於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元

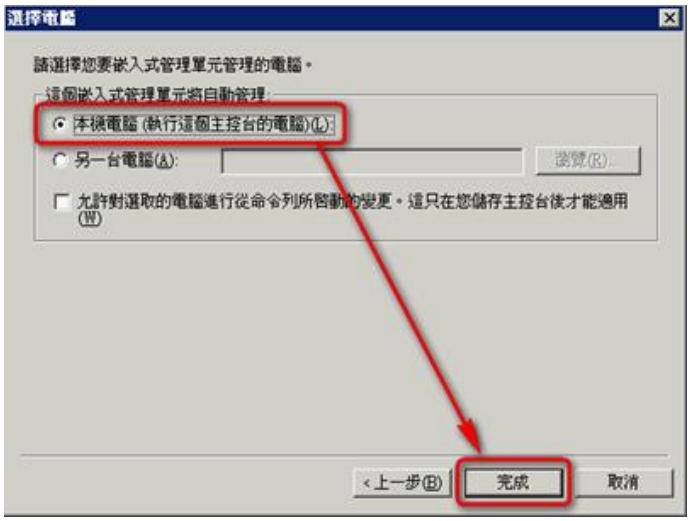
7 點選『新增』，然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增



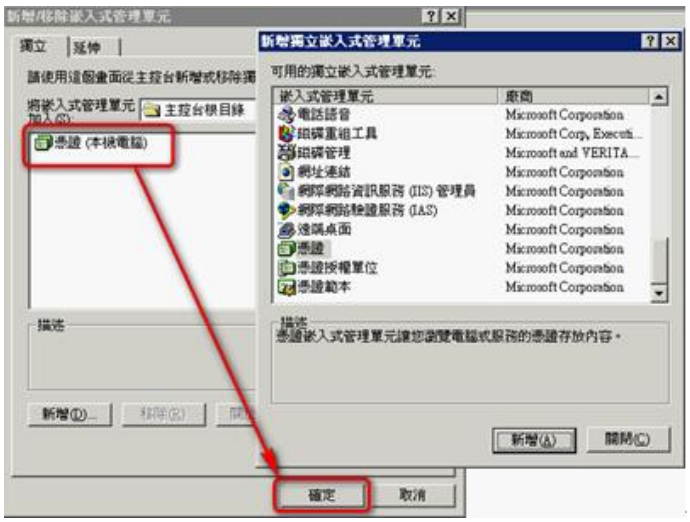
8 選擇『電腦帳戶』，然後『下一步』



9 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



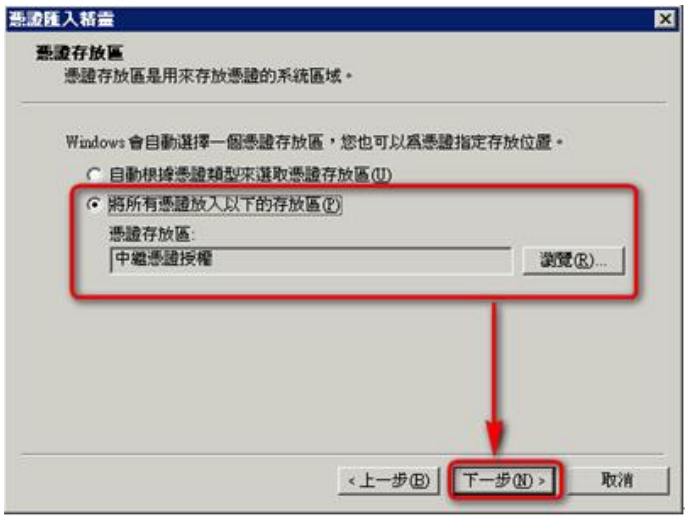
10 完成後，在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示，點選『確定』完成憑證管理單元新增程序



11 開啟憑證主控台，在『中繼憑證授權』點選右鍵，『所有工作 > 匯入 』。系統執行憑證匯入精靈歡迎畫面後，『下一步』

12 用『瀏覽』選擇下載的中繼憑證檔案位置，然後點選『下一步』

13 選擇『將所有憑證放入以下的存放區』，憑證存放區為預設的『中繼憑證授權』，然後『下一步』



憑證安裝完成，您可以直接跳到 五、檢查憑證安裝是否正確

五、檢查憑證安裝是否正確

您可以透過此驗證工具來確認憑證是否已經正確掛載：

GeoTrust：http://geotrust.cloudmax.com.tw/OpenSSL/checkservercert.asp

GlobalSign：https://globalsign.ssllabs.com/

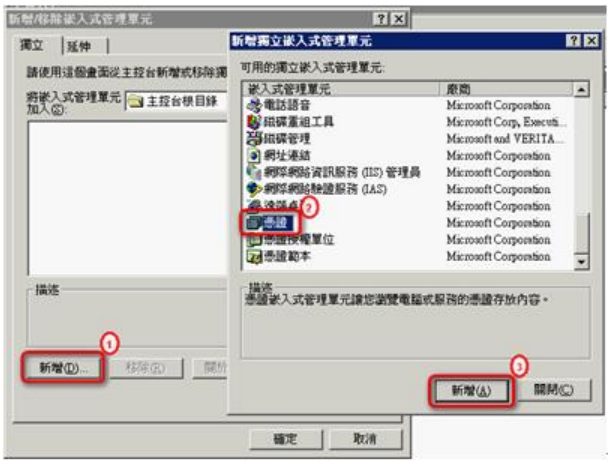
六、備份數位憑證

WIS 匯智數位憑證在憑證有效期間內，提供憑證重置(Reissue)與更新的服務。不過重置過程需與新申請憑證時相同，必須再次產生私密金鑰與 CSR、驗證、簽發公開金鑰等程序後，才可再取得憑證。將可能耽誤寶貴的系統復原時間。基於資安考量，建議系統管理者將數位憑證進行備份。備份的方式如下：

1 開始 > 執行(R)，輸入"mmc"
* 若已經有看到憑證項目請直接跳到本步驟 7

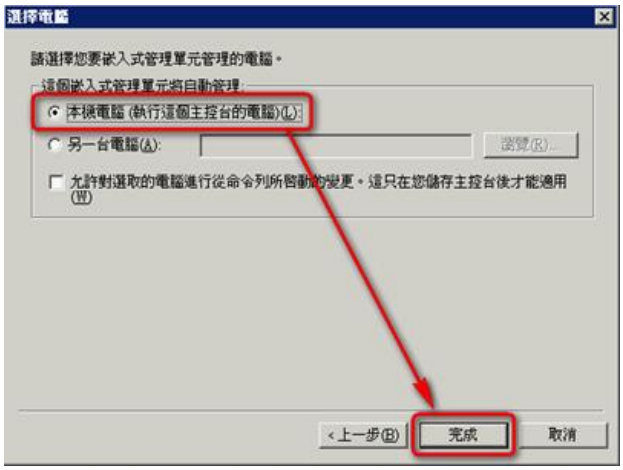
2 於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元

3 點選『新增』，然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增

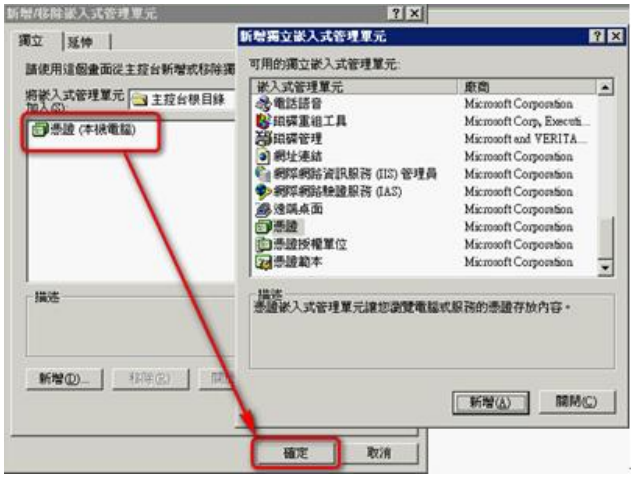


4 選擇『電腦帳戶』，然後『下一步』

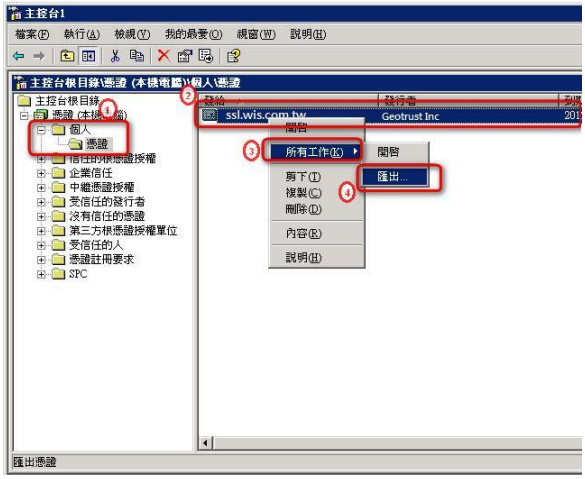
5 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



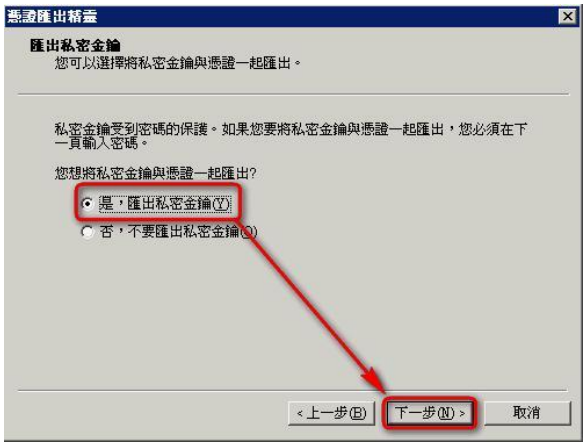
6 完成後，在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示，點選『確定』完成憑證管理單元新增程序



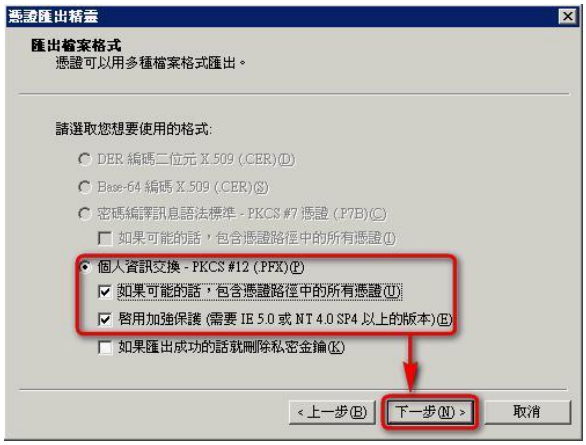
7 開啟憑證主控台，點選『個人 > 憑證』，於工作室窗選定欲備份的憑證後，右鍵，『所有工作 > 匯出』



8 於憑證精靈歡迎畫面點選『下一步>』後，選擇『是，匯出私密金鑰』，然後『下一步』



9 「匯出檔案格式」預設為「個人資訊交換-PKCS#12(.PFX)(P)」，請將『如果可能的話，包含憑證路徑中的所有憑證』



10 用『瀏覽』指定檔案匯出位置及名稱，然後『下一步(N)』

11 在憑證匯出精靈中自行設定設定 6 碼以上之保護密碼，『密碼(P)』及『確認密碼(C)』欄位需相同

12 憑證精靈最後將顯示匯出資訊，點選『完成』。在匯出成功訊息點選『確認』關閉工作視窗