

## [ 六、GeoTrust 憑證安裝教學 ]

請根據您的伺服器軟體，查看服務憑證安裝的詳細方法，如果有任何問題，請聯繫亞太客服或您的伺服器環境提供商。

### ■ Apache 2.2

#### 一、安裝憑證文件

##### 1. 將憑證內容存為一個檔：

您會收到一封 APTG 憑證完成的通知信件，憑證內容將附在郵件中。您需要將郵件中的憑證部分的內容用 Vi 或 Notepad 存成一個純文字檔案。不要將其存成 Microsoft Word 或其他文字處理軟體格式，並確定憑證內容中不含有空行和空格，檔案名可以為 server.cer。如下所示：



將保存好的 server.cer 檔和製作 CSR 時候生成的 server.key 一起複製到伺服器上。

##### 2. 中繼憑證：

您將會於開通信件中，查找到 中繼憑證 檔案的文本資訊，如同步驟 1，您需要將郵件中的憑證部分的內容用 Vi 或 Notepad 存成一個純文字檔案。不要將其存成 Microsoft Word 或其他文字處理軟體格式，並確定憑證內容中不含有空行和空格，檔案名可以為 ca.cer。

##### 3. 修改 httpd.conf 文件：

Apache 一般有 2 個版本下載，一個是帶 SSL 模組的，一個是不帶 SSL 的，請首先檢查自己的 SSL 是包含了 SSL 模組的，否則就沒法做了。Apache 的參數配置都在 httpd.conf 檔中，SSL 配置也是如此，此外還可以通過 include httpd-ssl.conf 來包含一個專門配置 SSL 的配置檔，如果啟動了 httpd-include ssl.conf，則可以打開 httpd-ssl.conf 來配置相應參數。

一般，我們直接在 httpd.conf 檔中直接配置 SSL 參數：

```
#載入模組 mod_ssl.so，此模組是啟用 SSL 功能必須的。
LoadModule ssl_module modules/mod_ssl.so

#監聽 443 埠
Listen 443

#建立一個 SSL 的虛擬站點，避免 SSL 配置影響原來 HTTP 的站點配置。
<VirtualHost _default_:443>
    DocumentRoot "C:/Program Files/Apache2/htdocs"
    ServerName www.myssl.cn:443
    SSLEngine on
```

```
#憑證本體，把相對應的檔案路徑放入即可
SSLCertificateFile "C:/SSL/server.cer"
#憑證金鑰，把相對應的檔案路徑放入即可
SSLCertificateKeyFile "C:/SSL/server.key"
#中
繼憑證，把相對應的檔案路徑放入即可
SSLCertificateChainFile "C:/SSL/ca.cer"
ErrorLog "C:/Program Files/Apache2/logs/error.log"
TransferLog "C:/Program Files/Apache2/logs/access.log"
</VirtualHost>

#說明主站是使用 HTTP 通信的，只有上面虛擬站點有 SSL
SSLEngine off
```

配置參數說明如下 (完整的 SSL 配置參數見[這裏](#)):

- Listen 443

SSL 協定監聽的埠，同下面 Virtualhost 中的埠需要匹配，SSL 協定缺省使用 443 埠，也有使用 8443 的情況。

- SSLEngine on

SSL 功能打開，如果在 Virtualhost 出現這句，則僅作用於虛擬主機點配置範圍，這個虛擬主機點全部使用 SSL 通信，如果出現在 Virtualhost 外，則作用於全局，整個伺服器都使用 SSL ( HTTPS ) 通信，不能採用 HTTP 通信，所以通常都在 Virtualhost 中加這句。

- SSLCertificateFile :

憑證文件，server.cer

- SSLCertificateKeyFile

私鑰文件，server.key

- SSLCertificateChainFile

4. 重新啟動 Apache，如果是在 Linux 下，輸入：

```
apachectl stop
```

```
apachectl startssl
```

## ■ Windows 2000 - IIS 5.0

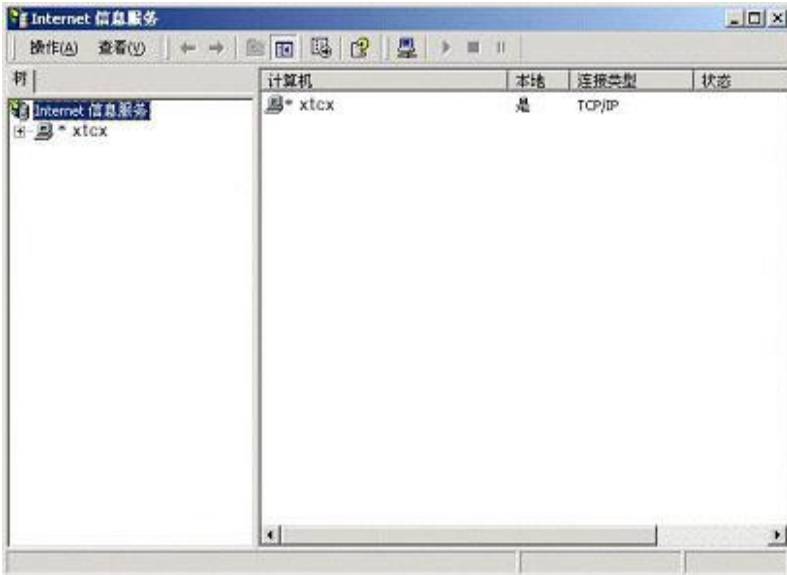
### 一、憑證安裝

1. 當您收到 APTG 郵件後，您就可以安裝並使用您的伺服器憑證了。將郵件中的憑證內容拷貝貼到一個純文字檔案中（包含-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----），存成一個“server.cer”文件，如下圖所示：



-> 在 Windows 系統將呈現此圖示，點擊二下可看到憑證詳細資訊

2. 如下圖所示，選擇“開始選單”->“程式”->“管理工具”->“Internet 伺服器管理”，將會出現如下視窗



3. 於上圖“Internet 伺服器管理”頁面中，展開站點列表，於您要應用伺服器憑證的站點按右鍵，選擇“屬性”->開啟“屬性視窗”，將開啟下圖頁面



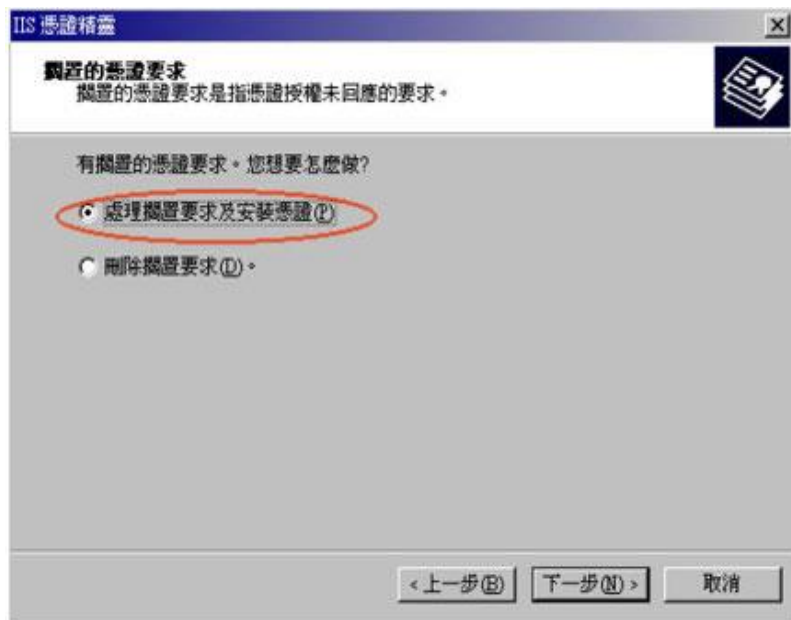
4. 點選"目錄安全性"選單，點選"伺服器憑證"按鈕，如下圖



5. 將會開啟下圖示窗，即可開始設定憑證安裝流程，直接點選下一步



6. 下圖視窗中選擇“處理擱置要求及安裝憑證”，點選“下一步”



7. 於下圖瀏覽部份選擇於步驟一儲存成“server.cer”的檔案，點選“下一步”



8. 將出現您所安裝憑證的詳細資訊，如下圖所示，點選“下一步”



9. 出現下圖，表示已完成憑證安裝，點選完成即可！



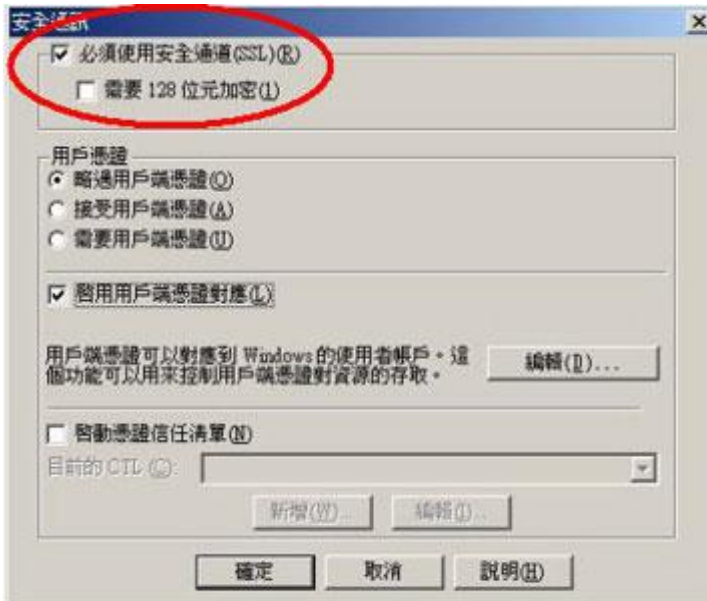
## 二、配置服务器的 SSL：

1. 回到站點屬性視窗，點選"目錄安全性"標籤，如下圖所示，點選"編輯"按鈕。

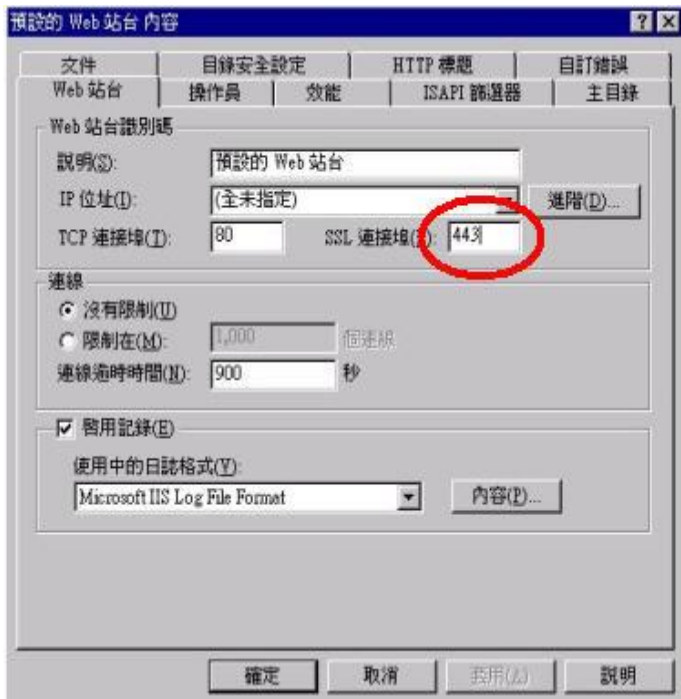




2. 將開啟下圖頁面，勾選"申請安全通道"選項，其他選項可依據需要進行設置，勾選完成後點選"完成"即可。



3. 接著回到視窗後，選擇"Web 站點"選項，將"SSL 連接埠"設定為 443，按"確定"按鈕，完成設置。



4. 這樣，您的伺服器憑證已經配置完畢了！接下來安裝中繼憑證。

### 三、中繼憑證安裝方式：

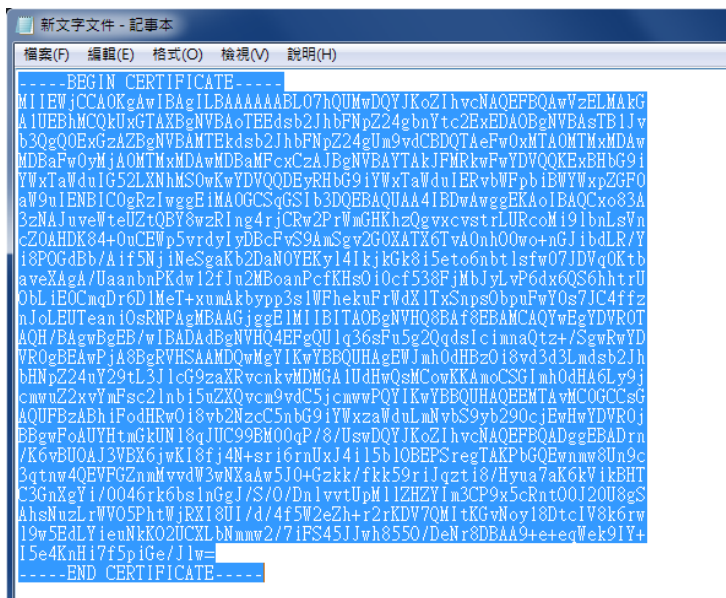
#### 1. 請查看開通信件中之「中繼憑證」資料

中繼憑證：

```
-----BEGIN CERTIFICATE-----
MIIEWjCCAOKgAwIBAgILBAAAAAABL07hQUmWdQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBHMCMQkUxGTAXBgNVBAoTEEdsb2JhbFNPZ24gbnYtc2EwEDA0BgNVBAsTB1Jv
b3QgOGEwGzAZBgNVBAMTEkdsb2JhbFNPZ24gUm9vdCBDQTAeFw0xMTA0MTMxMDAw
MDBaFw0yMjA0MTMxMDAwMDBaMFcxZjA1BzBAYTAkIjFMRkwFwYDVQoExBHBg9i
YWxTaWduIG52LXNhMS0wKwYDVQQDEyRHBG9iYXVudWJlIERvbWVpbiB1eWwYDzGFO
aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCo83A
3zNAJuveWteUzTQBY8wzRIng4rjCRw2PrWmGHKhZQgvxcvstrLURcoMl9lbnLsVn
cZOAHDk84+0uCEWp5vrdYlYDbcFvS9AmSgv2G0XATX6TVA0nh00wo+nG1jbdLR/Y
i8POGdAb/Aif5NjiNeSgAkB2DaNOYEKyl4IkjkGk8i5eto6nbtlsfw07JDVq0Ktb
aveXAgA/UaanbnPKdw12fJn2MBoanPcFKHs010cf538FjMbJyLvp6dx6QS6hhtRU
ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdXITxSnpsObpuFwY0s7JC4ffz
nJoLEUTean10sRNPAGMBAAGjggEiMIIBIATAOBgNVHQ8BAf8EBAMCAQYwEgYDVRO0
AQH/BAGwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcImnaQtz+/SgwRwYD
VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAQEwJmh0dHBz0i8vd3d3Lmdsb2Jh
bHNpZ24uY29tL3JlcG9zaXRvcnkVMDMGA1UdHwQSMCOWKKAmoCSGImh0dHA6Ly9j
cmwuZ2xvYmFsc2lnbi5uZXQvcn9vdC5jcmwwPQYIKwYBBQUHAQEEMTAwMCGCCSG
AQUBzABhIFodHRwOi8vb2Nzc5bnG9iYXVudWJlIERvbWVpbiB1eWwYDVR0jBBgwFo
AUyHtmGUKN18qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEBADrn
/K6vBU0AJ3VBX6jwK18fj4N+sr16rnUxJ4i15b10BEPsregTAKPbGQEWnmw8Un9c
3qtnw4QEVFGZnmMvvdW3wNXaAw5J0+Gzkk/fkk59r1JqztI8/Hyua7aK6kVikBHT
C3GnXgYi/0046rk6bs1nGgJ/S/O/DnlvvtUpMlZHZYIm3CP9x5cRnt00J2008gS
AhsNuzLrWV05PhtWjRX18UI/d/4f5W2eZh+r2rKDV7QM1tKGVNoy18Dtc1V8k6rw
19w5EdLYieuNkK02UCXLBnmw2/7iPS45Jjwh8550/DeNr8DBAA9+e+eqWek91Y+
I5e4KnH17f5pIGe/Jlw=
-----END CERTIFICATE-----
```

#### 2. 請複製憑證資訊，需包含『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』完整資訊

#### 3. 開啟記事本，將複製的資訊貼上，並將此憑證檔案存檔成為附檔名為 ca.cer 之檔案格式，呈現如下：



→ 資訊貼上記事本



ca.cer

→ 存檔後圖示呈現樣式

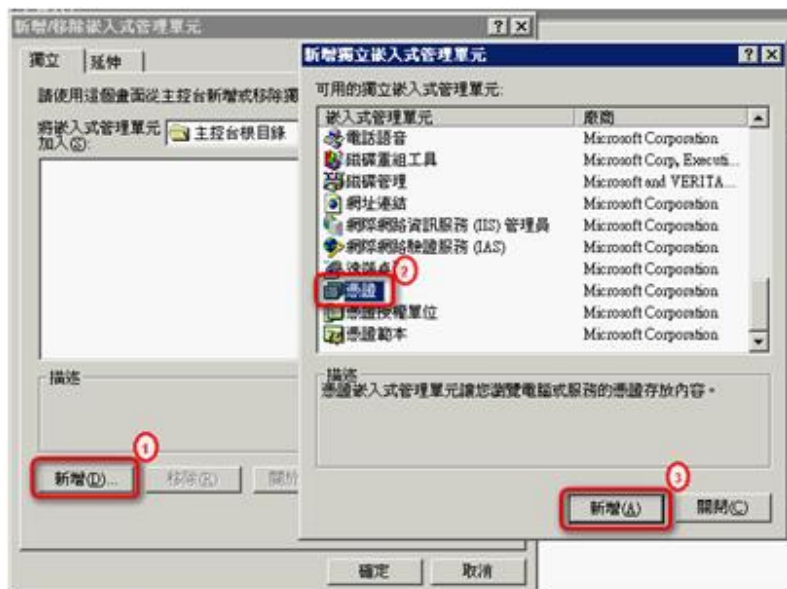
#### 4. 接下來執行：開始 -> 執行(R)，輸入“mmc”

#### 5. 於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元

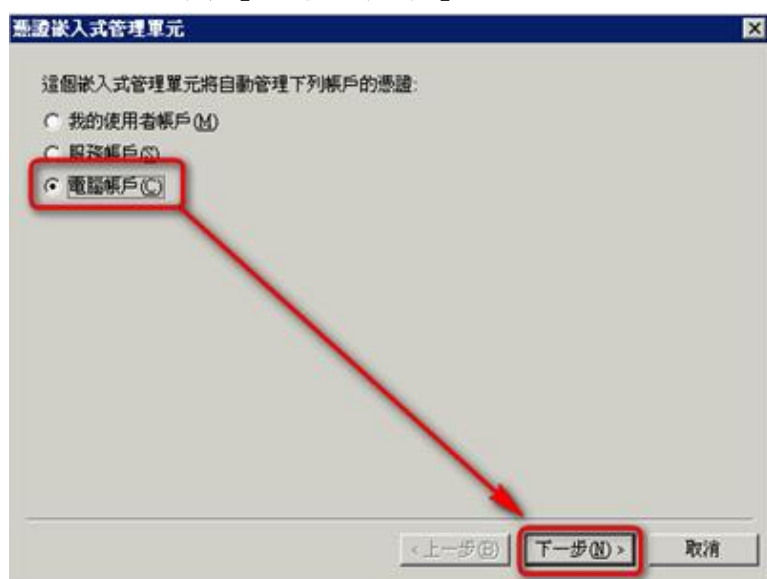




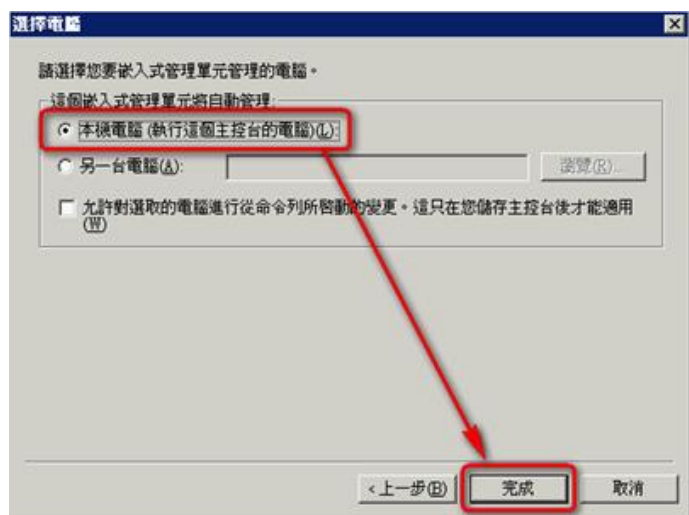
6. 點選『新增』，然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增



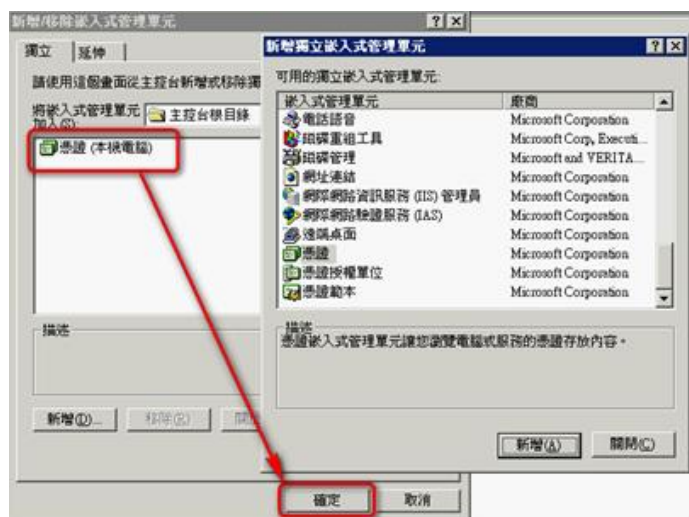
8. 選擇『電腦帳戶』，然後『下一步』



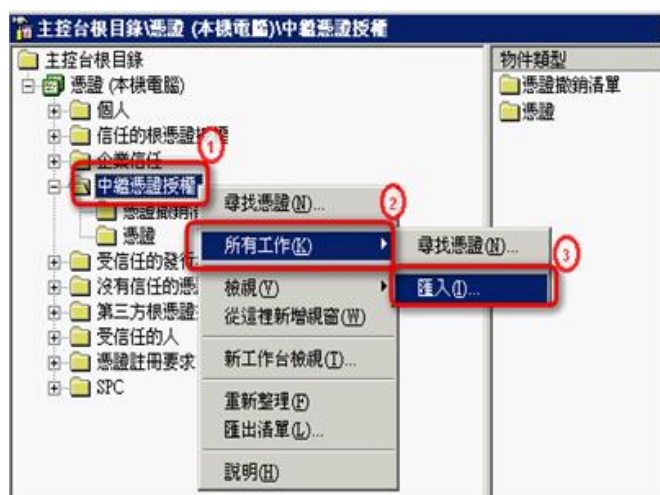
9. 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



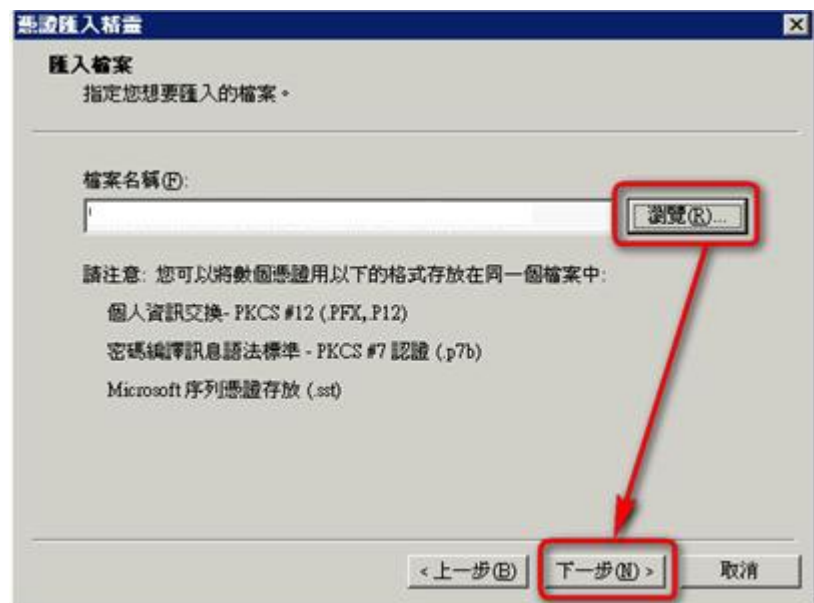
10. 完成後，在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示，點選『確定』完成憑證管理單元新增程序



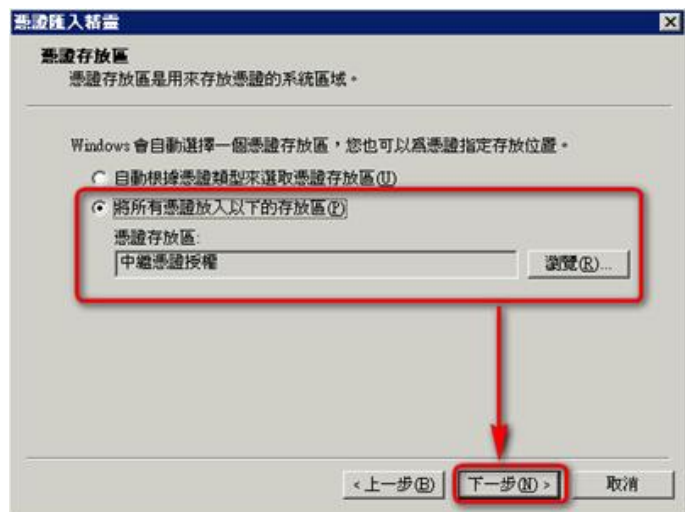
11. 開啟憑證主控台，在『中繼憑證授權』點選右鍵，『所有工作 > 匯入』。系統執行憑證匯入精靈歡迎畫面後，『下一步』



12. 用『瀏覽』選擇於步驟 3 所存下來的憑證檔案後，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』



\*以上步驟完成後，表示已完成憑證安裝流程，您可使用電腦及行動裝置於於 **URL** 中輸入 **https://**您的網站網址，即可查看憑證是否正常使用了。

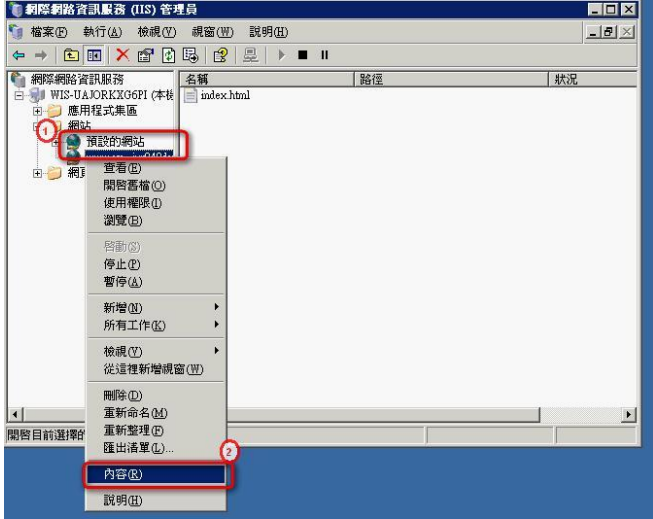
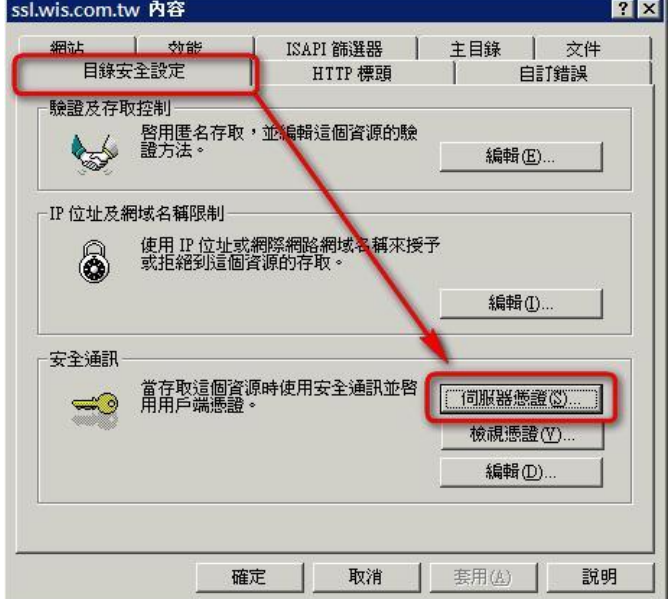
## ■ Windows 2003 - IIS 6.0

當您收到 APTG 的郵件後，您就可以安裝並使用您的伺服器憑證了。將郵件中的憑證內容拷貝粘貼到一個純文字檔案中 ( 包含 -----BEGIN CERTIFICATE-----和-----END CERTIFICATE----- )，存成一個"server.cer"文件，如下圖所示：



-> 在 Windows 系統將呈現此圖示，點擊二下可看到憑證詳細資訊

### 一、憑證安裝方式：

1	點選當時執行的站台/內容
	
2	目錄安全設定 / 伺服器憑證
	
3	選擇"處理擱置的憑證要求"，下一步



4 出現如下視窗，點選“瀏覽”選擇步驟一所儲存的檔案，下一步



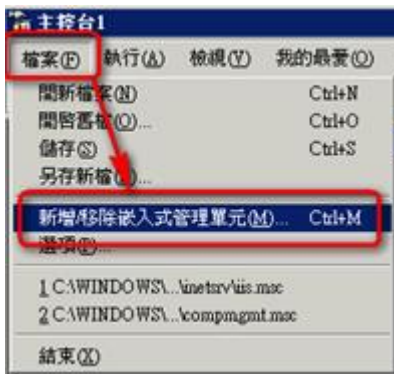
5 下圖視窗中設定 SSL 連接埠，HTTPS 預設使用 443 port，請依照實際狀況來進行設定，下一步->完成



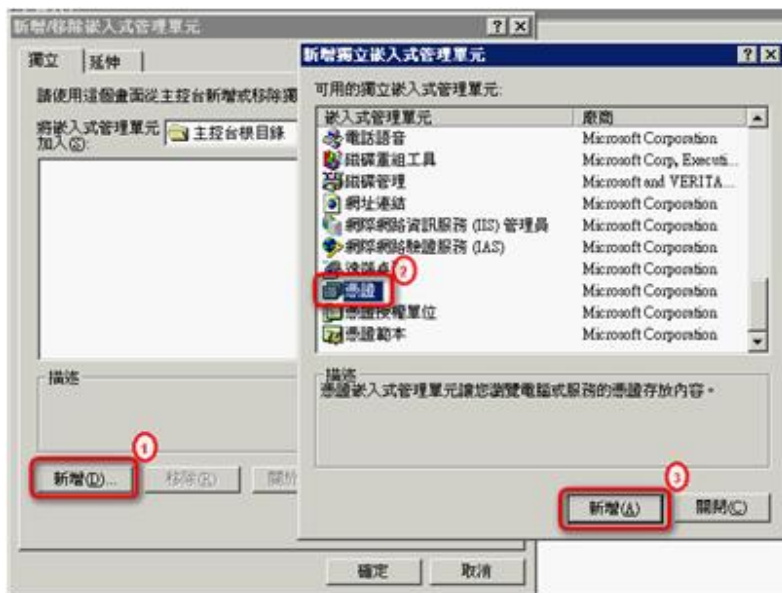
二、中繼憑證安裝方式：

1	<p>請協助查看憑證資訊檔案文本資料中「中繼憑證」</p> <p><b>中繼憑證：</b></p> <pre>-----BEGIN CERTIFICATE----- MIIEWjCCAOKgAwIBAgILBAAAAAAABL07hQUMwDQYJKoZIhvcNAQEFBQAwwVzELMAkG A1UEBHMCCQkUxGTAXBgNVBAoTEEdsb2JhbFNPZ224gbnYtc2ExEDA0BgNVBAsTB1Jv b3QgQ0EwGzAZBgNVBAMTEkdsb2JhbFNPZ224gUm9vdCBDQTAeFw0xMTA0MTMxMDAw MDBaFw0yMjA0MTMxMDAwMDBaMFcxZjBGNVBAITAkZFMkRkFwYDVoVQkEzBHhg9i YwxtaWduIG52LXNhMS0wKwYDVoVQkEYRhBg9iYwxtaWduIERvbWVpbiBwYXpZGF0 aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXo83A 3zNAJuveWteUztQB8wzRIng4rjCRw2PrWmGHKhZQgvcvstrLURcoM19IbnLsVn cZ0AHDk84+0uCEWp5vrdyIyDbcFvS9AmSgv2G0XATX6TvA0nh00wo+nGjIbdLR/Y i8POgdBb/Aif5NjiNeSgAkB2DaNOYEKy141kjkGk815eto6nbt1sfw07IDVq0Ktb aveXAgA/UaanbnPKdw12fJn2MBoanPcFKHs0icf538FjMbjLylVp6dx6Qs6hhtrU ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdXITxSnpsObpuFwY0s7JC4ffz nJOLEUTeani0sRNPAGMBAAGjggEIMIIBITA0BgNVHQ8BAf8EBAMCAQYwEgYDVR0T AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimnaQtz+/SgwRwYD VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAQEWEJmh0dHBz018vd3d3Lmdsb2Jh bHNpZ224y29tL3JlcG9zaXRvcnkvdMDMGA1UdHwQSMCOWKKAmoCSGImh0dHA6Ly9j cmwwZ2xvYmFsc2lnbi5uZXQvcn9vdC5jcmwwPQYIKwYBBQUHAQEEMTAwMCGCCSgS AQUFBzABhIFodHRwOi8vb2Nzc2N5bG9iYwxtaWduLnVbS9yb290cjEwHwYDVR0j BBgwFoAUYHtmGkUN18qJUC99BM00qP/8/UsWdQYJKoZIhvcNAQEFBQADggEBAERn /K6vBUOAj3WEX6jwKI8fj4N+sr16rnUxJ4i15b10BEPSregTAKPbGQEWnmw8Un9c 3qtnw4QEVFGZnmMvvdW3wNXaAw5J0+Gzkk/fkk59r1jqtz18/Hyua7aK6kVikBHT C3GnxgY1/0046rk6bs1nGgJ/S/O/DnlvvtUpMl1ZHZY1m3CP9x5cRnt00J20U8gS AhsNuzLrWW05PhTvjRxi8UI/d/4f5W2eZh+r2rKDV7QM1tKgvNoy18Dtc1V8k6rw l9w5EdLYieuNkK02UCXLBnmw2/7IFs45Jjwh8550/DeNr8DBAA9+e+eqWek91Y+ I5e4KnH17f5piGe/Jlw= -----END CERTIFICATE-----</pre>
2	<p>請複製憑證資訊，需包含『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』完整資訊</p>
3	<p>開啟記事本，將複製的資訊貼上，並將此憑證檔案存檔成為附檔名為 <b>ca.cer</b> 之檔案格式，呈現如下：</p>
	 <p>新文字文件 - 記事本</p> <p>檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)</p> <pre>-----BEGIN CERTIFICATE----- MIIEWjCCAOKgAwIBAgILBAAAAAAABL07hQUMwDQYJKoZIhvcNAQEFBQAwwVzELMAkG A1UEBHMCCQkUxGTAXBgNVBAoTEEdsb2JhbFNPZ224gbnYtc2ExEDA0BgNVBAsTB1Jv b3QgQ0EwGzAZBgNVBAMTEkdsb2JhbFNPZ224gUm9vdCBDQTAeFw0xMTA0MTMxMDAw MDBaFw0yMjA0MTMxMDAwMDBaMFcxZjBGNVBAITAkZFMkRkFwYDVoVQkEzBHhg9i YwxtaWduIG52LXNhMS0wKwYDVoVQkEYRhBg9iYwxtaWduIERvbWVpbiBwYXpZGF0 aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCXo83A 3zNAJuveWteUztQB8wzRIng4rjCRw2PrWmGHKhZQgvcvstrLURcoM19IbnLsVn cZ0AHDk84+0uCEWp5vrdyIyDbcFvS9AmSgv2G0XATX6TvA0nh00wo+nGjIbdLR/Y i8POgdBb/Aif5NjiNeSgAkB2DaNOYEKy141kjkGk815eto6nbt1sfw07IDVq0Ktb aveXAgA/UaanbnPKdw12fJn2MBoanPcFKHs0icf538FjMbjLylVp6dx6Qs6hhtrU ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdXITxSnpsObpuFwY0s7JC4ffz nJOLEUTeani0sRNPAGMBAAGjggEIMIIBITA0BgNVHQ8BAf8EBAMCAQYwEgYDVR0T AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimnaQtz+/SgwRwYD VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAQEWEJmh0dHBz018vd3d3Lmdsb2Jh bHNpZ224y29tL3JlcG9zaXRvcnkvdMDMGA1UdHwQSMCOWKKAmoCSGImh0dHA6Ly9j cmwwZ2xvYmFsc2lnbi5uZXQvcn9vdC5jcmwwPQYIKwYBBQUHAQEEMTAwMCGCCSgS AQUFBzABhIFodHRwOi8vb2Nzc2N5bG9iYwxtaWduLnVbS9yb290cjEwHwYDVR0j BBgwFoAUYHtmGkUN18qJUC99BM00qP/8/UsWdQYJKoZIhvcNAQEFBQADggEBAERn /K6vBUOAj3WEX6jwKI8fj4N+sr16rnUxJ4i15b10BEPSregTAKPbGQEWnmw8Un9c 3qtnw4QEVFGZnmMvvdW3wNXaAw5J0+Gzkk/fkk59r1jqtz18/Hyua7aK6kVikBHT C3GnxgY1/0046rk6bs1nGgJ/S/O/DnlvvtUpMl1ZHZY1m3CP9x5cRnt00J20U8gS AhsNuzLrWW05PhTvjRxi8UI/d/4f5W2eZh+r2rKDV7QM1tKgvNoy18Dtc1V8k6rw l9w5EdLYieuNkK02UCXLBnmw2/7IFs45Jjwh8550/DeNr8DBAA9+e+eqWek91Y+ I5e4KnH17f5piGe/Jlw= -----END CERTIFICATE-----</pre>  <p>→ 存檔後圖示呈現樣式</p>
4	<p>開始 &gt; 執行(R)，輸入“mmc”</p>
5	<p>於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元</p>

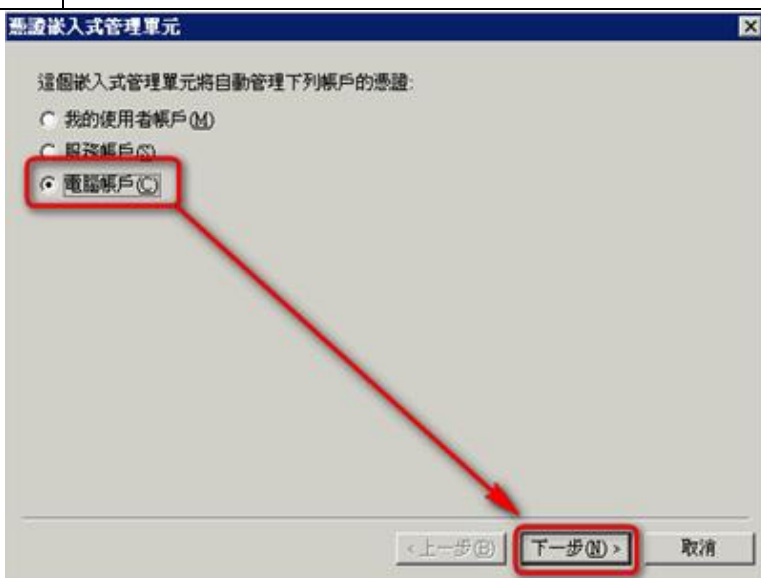




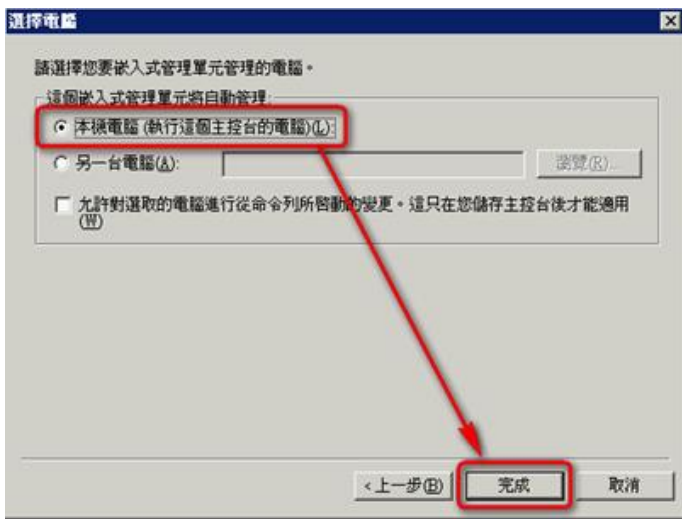
6 點選『新增』，然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增



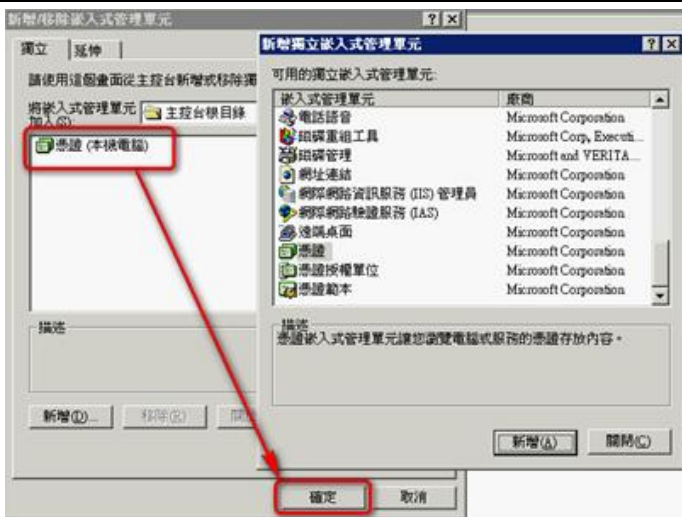
7 選擇『電腦帳戶』，然後『下一步』



8 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



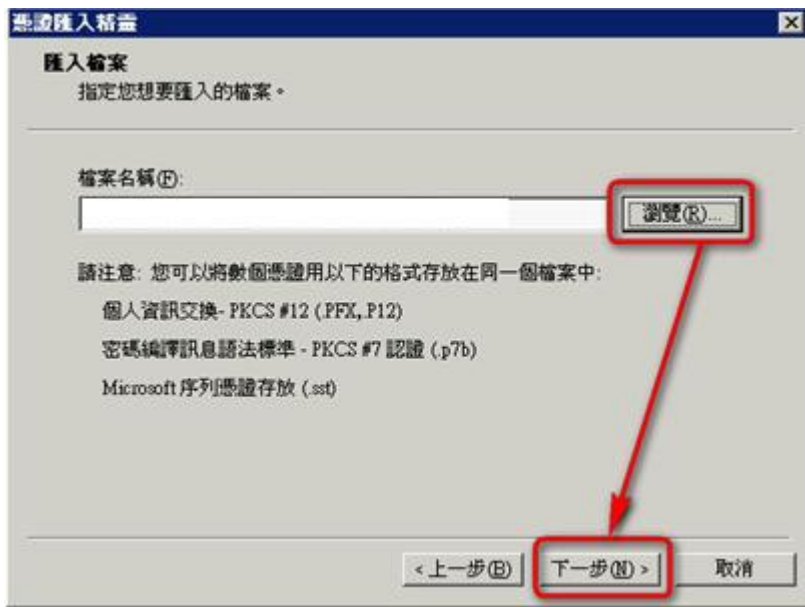
9 完成後，在「新增/移除嵌入式管理單元」視窗中將出現「憑證(本機電腦)」圖示，點選『確定』完成憑證管理單元新增程序



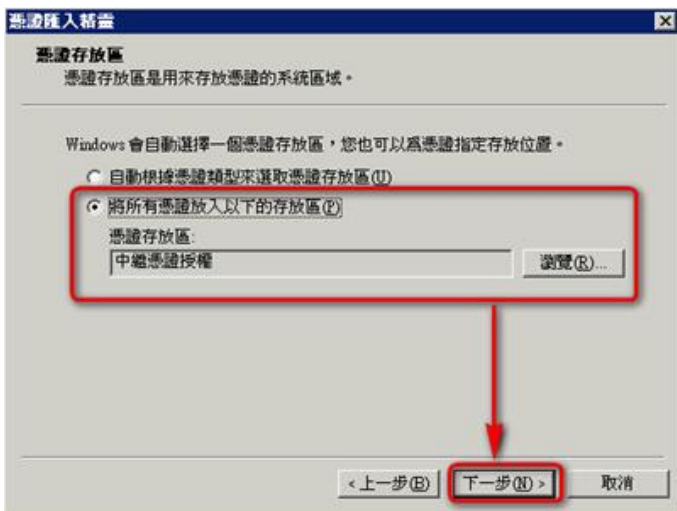
10 開啟憑證主控台，在『中繼憑證授權』點選右鍵，『所有工作 > 匯入』。系統執行憑證匯入精靈歡迎畫面後，『下一步』



11 用『瀏覽』選擇於步驟 3 所存下來的憑證檔案後，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』



\*以上步驟完成後，表示已完成憑證安裝流程，您可使用電腦及行動裝置於 **URL** 中輸入 **https://** 您的網站網址，即可查看憑證是否正常使用了。

## ■ IIS 7.0

### 一、憑證安裝

1. 當您收到 APTG 的郵件後，您就可以安裝並使用您的伺服器憑證了。將郵件中的憑證內容拷貝粘貼到一個純文字檔案中（包含-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----），存成一個“server.cer”文件，如下圖所示：



-> 在 Windows 系統將呈現此圖示，點擊二下可看到憑證詳細資訊

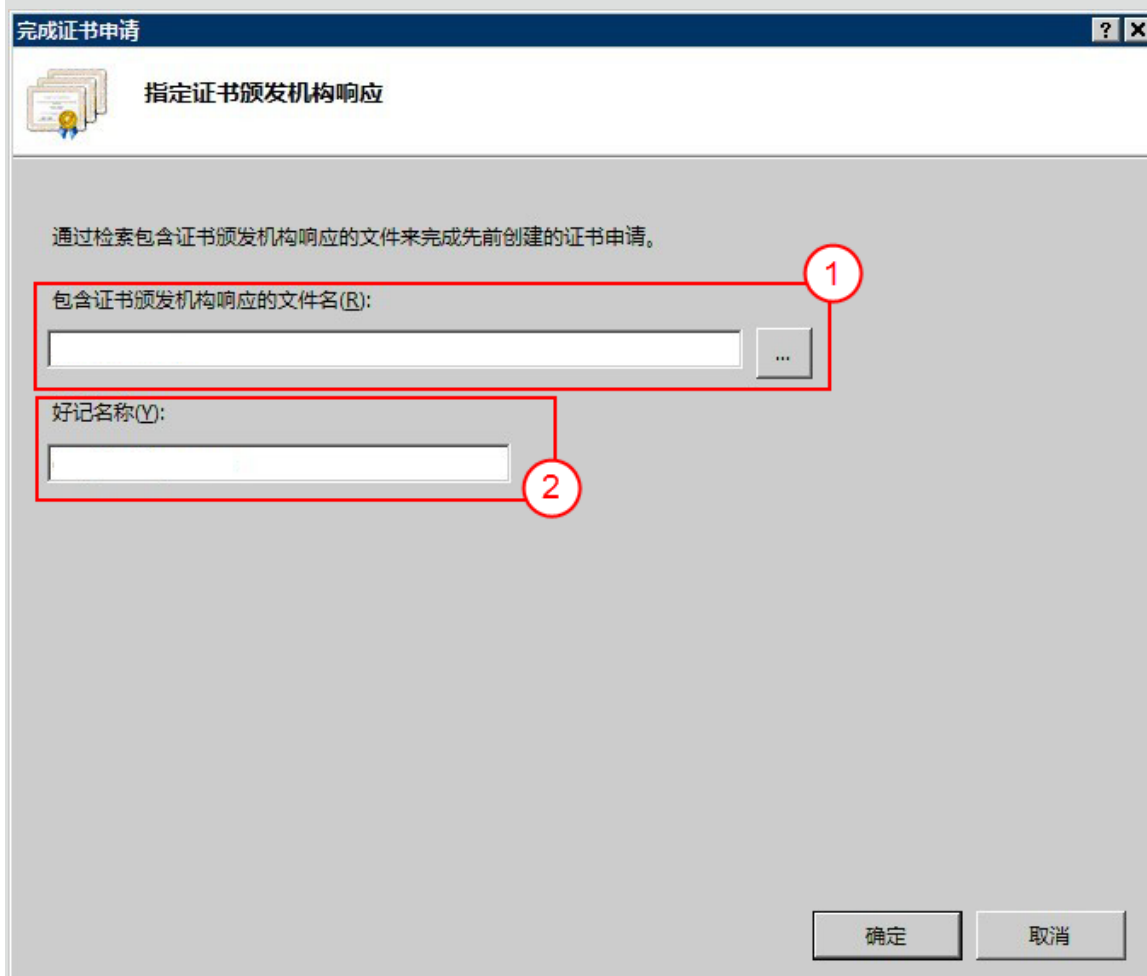
2. 打開 IIS 服務管理器，點擊計算機名稱，雙擊打開右側的伺服器憑證圖標



3. 雙擊打開伺服器憑證後，點擊右側的完成數位憑證申請

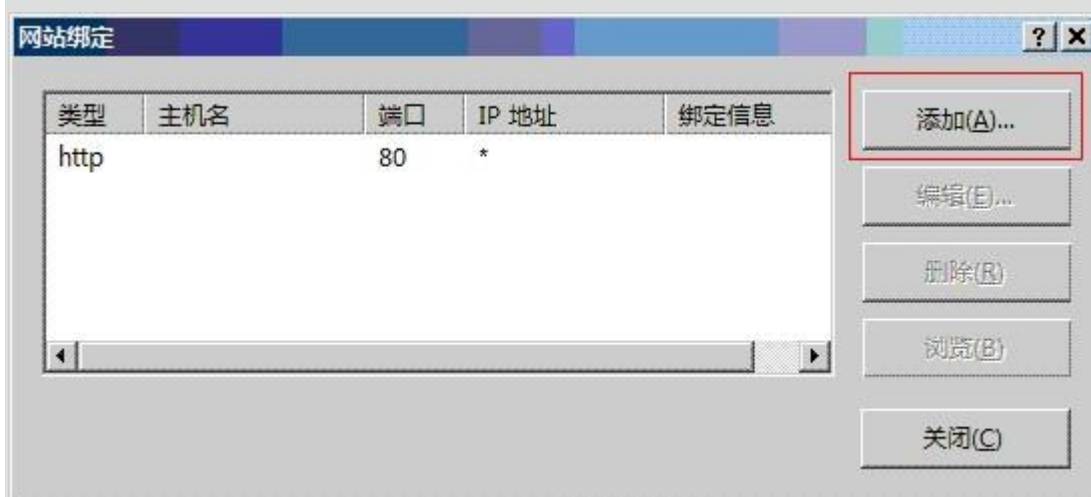
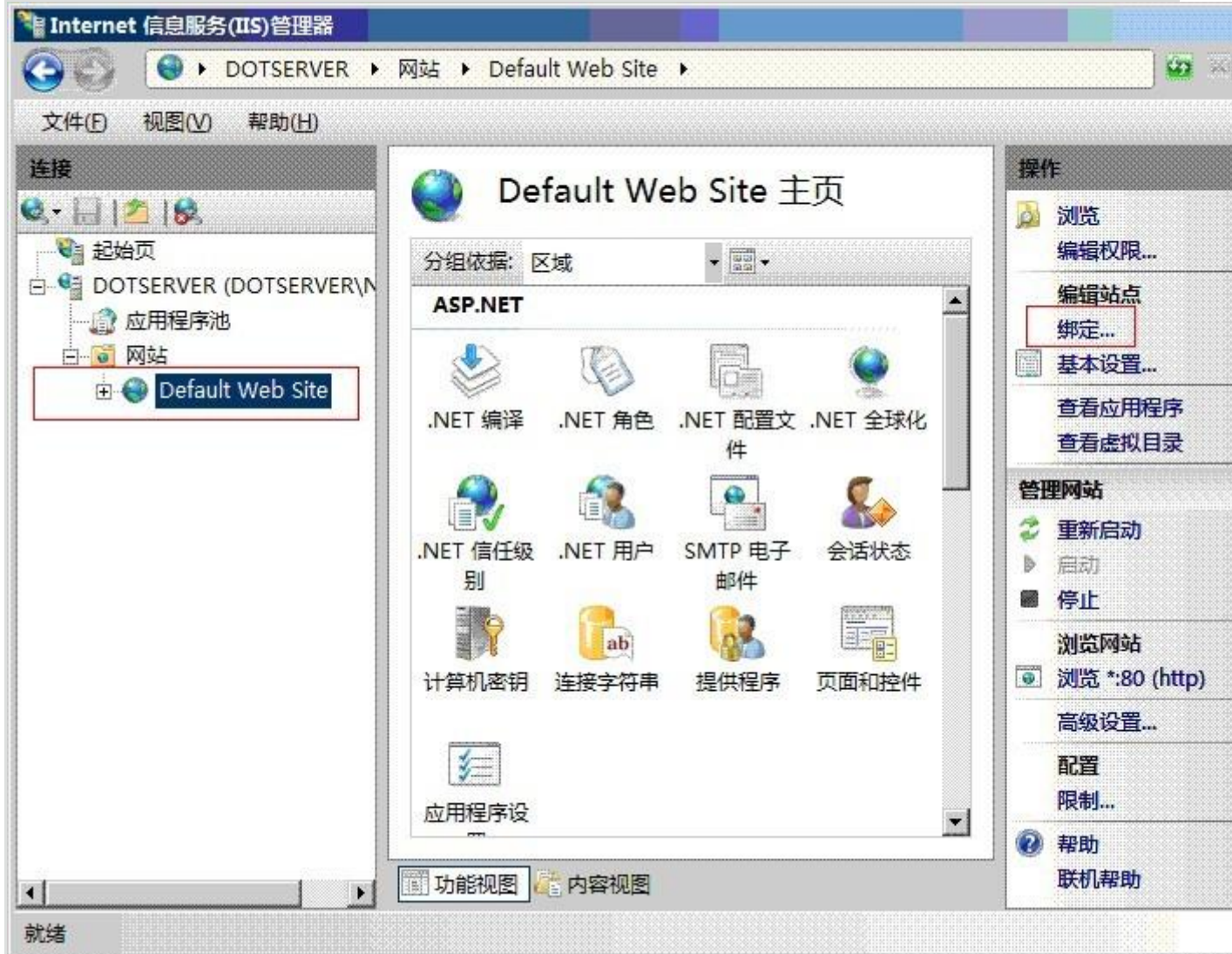


4. 請於下圖中區塊 1 中點選“瀏覽”，選擇步驟一儲存的檔案，區塊 2 的部份請輸入一個好記的名稱，點擊確定即可



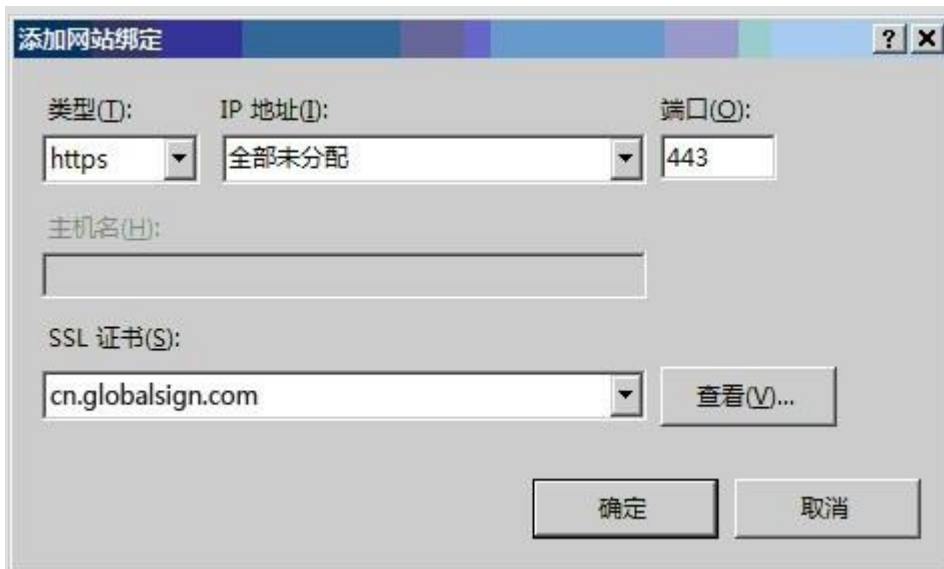


5. 點擊網站下的站點名稱，點擊右側的綁定

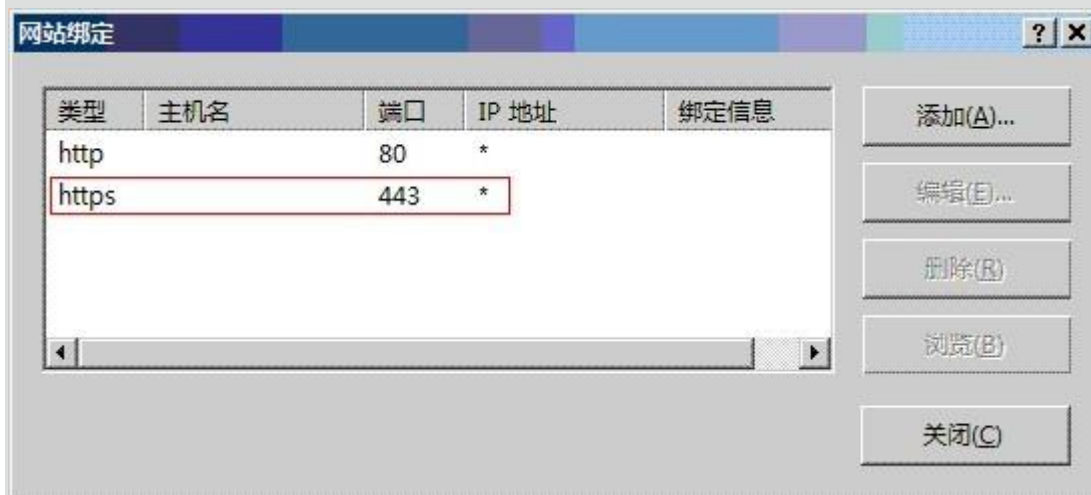


6. 添加網站綁定內容：選擇類型為 https，端口 443 和指定對應的 SSL 數位憑證，點擊確定，於 SSL 憑證下拉選單中找到剛才設定的憑證資訊(即為上面設定的好記名稱)





7. 打開網站綁定界面後，點擊添加

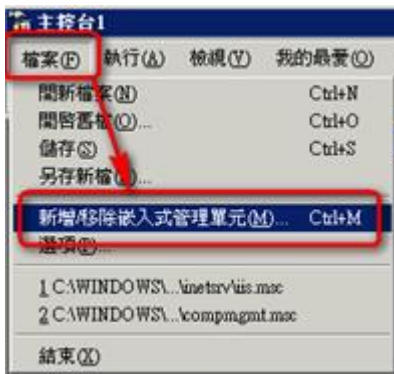


8. 添加完成後，網站綁定界面將會看到剛剛添加的內容

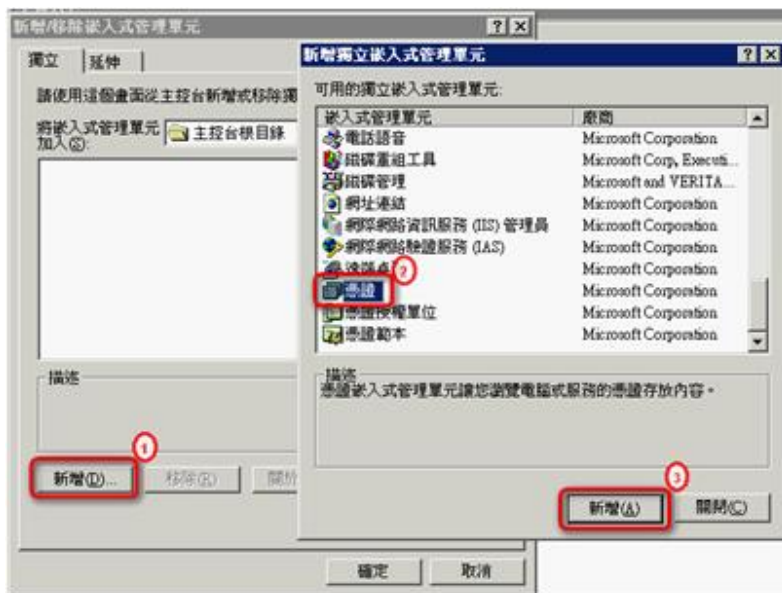
9. 這樣，您的伺服器憑證已經配置完畢了! 接下來安裝中繼憑證。

二、中繼憑證安裝方式：

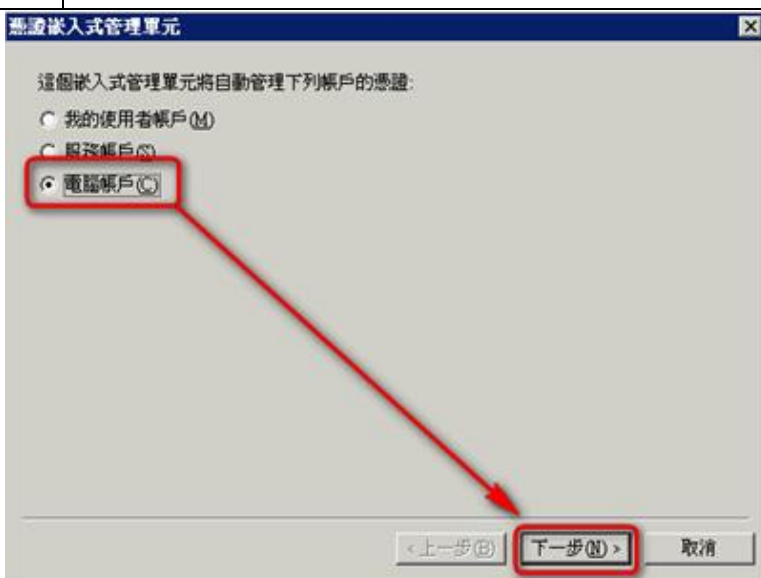
1	<p>請查看開通信件中之「中繼憑證」資料</p> <p><b>中繼憑證：</b></p> <pre> -----BEGIN CERTIFICATE----- MIIEWjCCA0KgAwIBAgILBAAAAAABL07hQUmWdQYJKoZIhvcNAQEFBQAwVzELMAkG A1UEBHMCCkUxGTAXBgNVBAAoTEEdsb2JhbFNPZ224gbnYtc2ExEDA0BgNVBAsTB1Jv b3QgQ0ExGzAZBgNVBAMTEkdsb2JhbFNPZ224gUm9vdCBDQTAeFw0xMTA0MTMxMDAw MDBaFw0yMjA0MTMxMDAwMDBaMFcxZjBGNVBAITAkJFMRkwFwYDVQKExBHBG9i YWxTaWduIG52LXNhMS0wKwYDVQQEYRhbG9iYXN0eS9yYXN0eS9yYXN0eS9yYXN0eS9y aW9uIENBIC0gRzIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCo83A 3zNAJuveWteUzTQBY8wzRIng4rjCRw2PrWmGHKhZQgvcvstrLURcoM19bnLsVn cZOAHDK84+0uCEWp5vrdy1yDbcFvS9AmSgv2G0XATX6TVA0nh00wo+nGj1bdLR/Y i8POGdBb/Aif5NjiNeSgAkB2DaNOYEKyl41kjkGk815eto6nbt1sfw07IDVq0Ktb aveXAgA/UaanbnPKdw12fJw2MBoanPcFKHs0icf538FjMbjLvlvP6dx6QS6hhtrU ObLiE0CmqDr6D1MeT+xumAkbypp3s1WFhekuFrWdXITxSnpsObpuFwY0s7JC4ffz nJoleUTEani0sRNPAGMBAAAgggEiMIIBITAOBgNVHQ8BAf8EBAMCAQYwEgYDVRO0 AQH/BAgwBgEB/wIBADAdBgNVHQ4EFgQUlq36sFu5g2QqdsIcimmnaQtz+/SgwRwYD VR0gBEAwPjA8BgRVHSAAMDQwMgYIKwYBBQUHAQEwJmhdHBz018vd343LmSb2Jh bHNpZ224uY29tL3JlcG9zaXRvcnkvdMDGA1UdHwQSMCovKKAmoCSGImh0dHA6Ly9j cmwwZ2xvYmFsc2lnbi5uZXQvcn9vdC5jcmwwPQYIKwYBBQUHAQEEMTAwMC0GCCsG AQUFBzABhFodHRwOi8vb2NzcC5nbG9iYXN0eS9yYXN0eS9yYXN0eS9yYXN0eS9yYXN0eS9y BBgwFoAUYHtmGkUN18qJUC99BM00qP/8/UswDQYJKoZIhvcNAQEFBQADggEBADErn /K6vBUOAJ3WBX6jwKI8fj4N+sr16rnUxJ4i15b10BEPSregTAKPBGQEWnmw8Un9c 3qtnw4QEVFGZnm1vvdW3wNXaAw5J0+Gzkk/fkk59r1jqtz18/Hyua7aK6kVikBHT C3GnXgY1/0046rk6bs1nGgJS/O/DnlvvtUpM1ZHZY1m3CP9x5cRnt00J20U8gS AhsNuzLrWw05PhtWjRXI8UI/d/4f5W2eZhr2rKDV7QM1tKGvNoy18Dtc1V8k6rw l9w5EdLYieunKk02UCXLBnmw2/7IFS45Jjwh8550/DeNr8DBAA9+e+eqWek91Y+ I5e4KnH17f5piGe/Jlw= -----END CERTIFICATE----- </pre>
2	<p>請複製憑證資訊，需包含『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』完整資訊</p>
3	<p>開啟記事本，將複製的資訊貼上，並將此憑證檔案存檔成為附檔名為 <b>ca.cer</b> 之檔案格式，呈現如下</p>
 <p>→ 存檔後圖示呈現樣式</p>	
4	<p>開始 &gt; 執行(R)，輸入“mmc”</p>
5	<p>於主控台視窗中點選 檔案 / 新增/移除嵌入式管理單元</p>



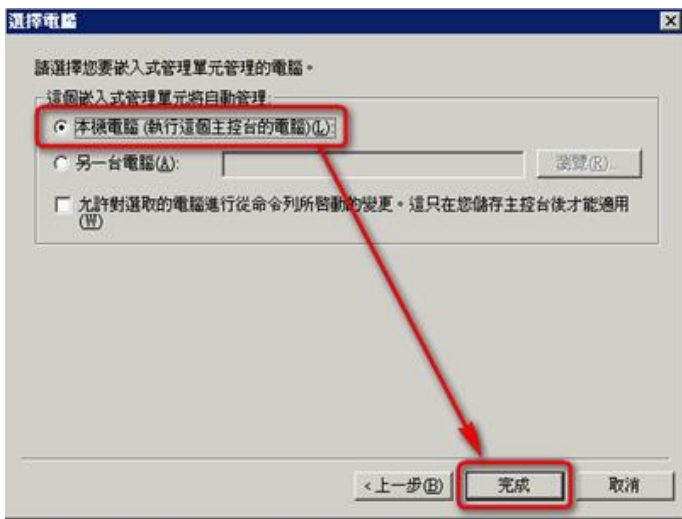
6 點選『新增』，然後在彈跳出來的「新增獨立嵌入式管理單元」視窗中點選 憑證/ 新增



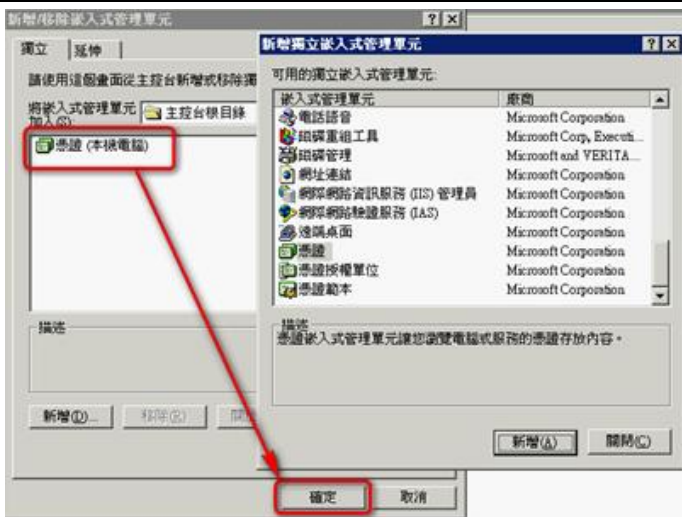
7 選擇『電腦帳戶』，然後『下一步』



8 選擇『本機電腦(執行這個主控台的電腦)』，然後完成



- 9 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



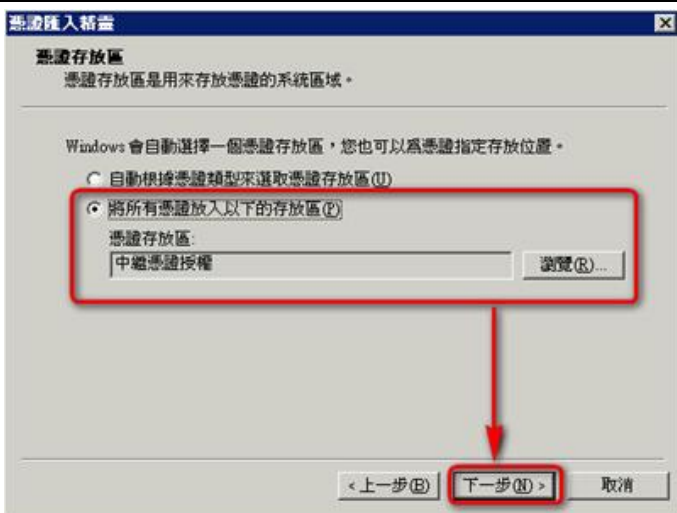
- 10 開啟憑證主控台，在『中繼憑證授權』點選右鍵，『所有工作 > 匯入』。系統執行憑證匯入精靈歡迎畫面後，『下一步』



- 11 用『瀏覽』選擇下載的中繼憑證檔案位置，然後點選『下一步』



- 12 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』



\*以上步驟完成後，表示已完成憑證安裝流程，您可使用電腦及行動裝置於 **URL** 中輸入 **https://** 您的網站網址，即可查看憑證是否正常使用了。

■ Tomcat

一、獲取並安裝伺服器憑證

1. 開啟記事本，依據購買方案將以下根憑證資訊複製存檔為 root.cer

購買 EV 等級使用的 CA Root

```
-----BEGIN CERTIFICATE-----
MIID/jCCAuagAwIBAgIQFaxulBmyeUtB9iepwXgPHzANBgkqhkiG9w0BAQsFADCB
mDELMaKGA1UEBhMCVVMx FjAUBgNVBAoT DUdlb1RydXN0IEluYy4xOTA3BgNVBASt
MChjKSAyMDA4IEdlb1RydXN0IEluYy4gLSBGb3IyYXV0aG9yaXplZCB1c2Ugb25s
eTE2MDQGA1UEAxMtR2VvVHJ1c3QgUHJpbWVyeSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cm10eSAtIEczMB4XDTA4MDQwMjAwMDAwMFoXDTM3MTIwMTIzNTk1OVowgZgx CzAJ
BgNVBAYTAIVTMRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMTkwNwYDVQQL EzAoYykg
MjAwOCBHZW9UcnVzdCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNIIG9ubHkxNjA0
BgNVBAMTLUdlb1RydXN0IFByaW1hcncgQ2VydGlmaWNhdGlvb1BBdXR0b3JpdHkg
LSBHMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANziXmJYHTNXOTIz
+uvLh4yn1ErdBojqZi4xmKU4kB6Yzy5jK/BGvESyiaHAKAxJcCGVn2TAppMSAmUm
hsalifD614SgcK9PGpc/BkTVyetyEH3kMSj7HGHmKAdEc5IiaacDiGydY8hS2pgn
5whMcD60yRLBxWeDXTPzAxHsatBT4tG6NmCUgLthY2xbF37fQJQeqw3CIShwiP/W
JmxsYAQITIV+fe+/IEjetx3dcI0FX4ilm/LC7urRQEFTYjgdVgbFA0dRIBn8exAL
DmKudIW/X3e+PkkBUz2YJQN2JFodtNuJ6nnlM7P7pMKEF/BqxqjsHQ9gUdfeZC
huOI1UcCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYw
HQYDVR0OBBYEFMR5yo6hTgMdHNxr2zFbID4/MH8tMA0GCSqGSIb3DQEBCwUAA4IB
AQAtxRPPVoB7eni9n64smefv2t+UXglpp+duaIy9cr5HqQ6XErhK8WTTod8INNTB
zU6B8A8ExCSzNjbGppow32hnc9f5joWJ7w5elShKKiePEI4ufIbEAp7aDHdIdkQN
kv39sxY2+hENHYwOB4lqKVb3cvTdfZx3NWZXqxNT2I7BQMXXExZacse3aQHEerGD
AWH9jUGhIbJBJVz88P6DAod8DQ3PLghcSkANPuyBYeYk28rgDi0Hsj5W3I31QYUH
SJsMC8tJP33st/3LjWeJGqvtux6jAAgIFyqCXDFdRootD4abdNIF+9RAsXqqaC2G
spki4cErx5z481+oghLrGRET
-----END CERTIFICATE-----
```

非 EV 等級使用的 CA Root

```
-----BEGIN CERTIFICATE-----
MIIDVDCCAjygAwIBAgIDAjRWMA0GCSqGSIb3DQEBBQUAMEIx CzAJBgNVBAYTAIVT
MRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMRswGQYDVQQDExJHZW9UcnVzdCBHbG9i
YWwgQ0EwHhcNMDIwNTIxMDQwMDAwWhcNMjIwNTIxMDQwMDAwWjBCMqSwCQYDVQQG
EwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjEybWVyeSBDZXJ0aWZpY2F0aW9u
R2xvYmFsIENBMiIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2swYYzD9
9BcjGlZ+W988bDjkcdb4kdS8odhM+KhDtgPpTSEHCiJaWC9mOSm9BXiLnTjoBbdq
fnGk5sRgprDvgOSJKA+eJdbtg/OtpPHmMICGDUUna2YRpIuT8rxh0PBFpVXLVDv
iS2Aelet8u5fa9IAjBkU+BQVNdnARqN7csiRv8IVK83QIz6cJmTM386DGXHKtubU
1XupGc1V3sjs0l44U+VcT4wt/lAjNvxm5suOpDkZALeVAjmRCw7+OC7RHQWa9k0+
```



```
bw8HHa8sHo9gOeL6NIMTOdReJivbPagUvTLrGAMoUgRx5aszPeE4uwc2hGKceeoW
MPRfwCvocWvk+QIDAQABo1MwUTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbTA
ephoyYn7qwVkdBF9qn1luMrMTjAfBgNVHSMEGDAWgBTAephoyYn7qwVkdBF9qn1l
uMrMTjANBgkqhkiG9w0BAQUFAAOCAQEAQNeMpauUvXVSOKVCUn5kaFOSPcPilKIn
Z57QzxpER+nBsqTP3UEaBU6bS+5Kb1VSsyShNwrrZHYqLizz/Tt1kL/6cdjHPTfS
tQWVYrmm3ok9Nns4d0iXrKYGjy6myQzCspIFAMfOEVeiIuCl6rYVSAIk6I5PdPcF
PseKUgzbFbS9bZvlxrFUaKnjaZC2mqUPuLk/IH2uSrW4nOQdtqvmIKXBx4Ot2/Un
hw4EbNX/3aBd7YdStysVAq45pmp06drE57xNNB6pXE0zX5IJL4hmXXeXxx12E6nV
5fEWCRE11azbJHFWLJhWC9kXtNHjUStedevV0NxpNO3CBWaAocvmMw==
-----END CERTIFICATE-----
```

完畢後請執行以下程序：

#### 1.將根憑證匯入

```
keytool -import -trustcacerts -keystore c:\server.jks -alias root -file root.cer
```

2.將 APTG 發送之開通通知信件中，提供的中繼憑證資料複製，以記事本儲存為"ca.cer"檔案，並執行以下命令導入中繼憑證：

```
keytool -import -trustcacerts -keystore c:\server.jks -alias dvroot -file ca.cer
```

3.將 APTG 發送之開通通知信件中，提供的憑證本體資料複製，以記事本儲存為"server.cer"檔案，並執行以下命令導入憑證本體：

```
keytool -import -trustcacerts -keystore c:\server.jks -alias tomcat -file server.cer
```

第一步全部完成後，表示數位憑證已經完全安裝到 server.jks 這個文件中，請備份此文件並妥善保存，以後如有更換伺服器或重裝系統，就可以直接使用此文件。

## 二、更新 server.xml 配置文件

用文本編輯器打開 "\$JAKARTA\_HOME/conf/server.xml"

找到去除注釋並更新以下內容：

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.coyote.tomcat5.CoyoteConnector"
    port="8443" minProcessors="5" maxProcessors="75"
    enableLookups="true" disableUploadTimeout="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS" keystoreFile =server.jks
    keystorePass="*****" />
-->
```

如果你要使用默認的 SSL 端口，請將 8443 端口改為 443 端口，keystoreFile 和 keystorePass 是 JKS 文件對應的路徑和

密碼。

注意：不同 tomcat 版本，修改 server.xml 的方式不同，請參考 tomcat 說明

tomcat 6.0 <http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>

tomcat 5.5 <http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html>

tomcat 4.1 <http://tomcat.apache.org/tomcat-4.1-doc/ssl-howto.html>

按照以上的步驟配置完成後，重新啟動 TOMCAT 後就可以使用 https://www.domain.com 來訪問了如有任何問題或疑問請直接與我們聯繫，謝謝！

## ■ Lotus Domino

### 一、憑證安裝：

用戶依照官網所提供的安裝說明，無法安裝成功，會出現以下訊息。

### Install Certificate into Key Ring

The Certificate Authority will notify when your signed certificate is ready. The specifics depend on the Certificate Authority, but typically you will receive an e-mail specifying a URL where you can pick up the certificate. Once you have obtained the signed certificate, this form lets you install it into your key ring. **Note:** Before installing this certificate, it is recommended that you install the certificate of the signing Certificate Authority in your key ring as a Trusted Root. If you haven't already done so, choose "Accept This Authority In Your Server" from the main menu of the Certificate Authority Web site to obtain the CA certificate.

#### Key Ring Information

Key Ring File Name

#### Quick Help

Specify the key ring file.

#### Certificate Information

Certificate Source  File  
 Clipboard

File Name

Merge Certificate into h

#### Lotus Notes

### Unrecognized Certificate Authority signature.

The server certificate cannot be installed in your server key ring because the signature is from a CA that is not listed as a Trusted Root. This is due to one of the following:

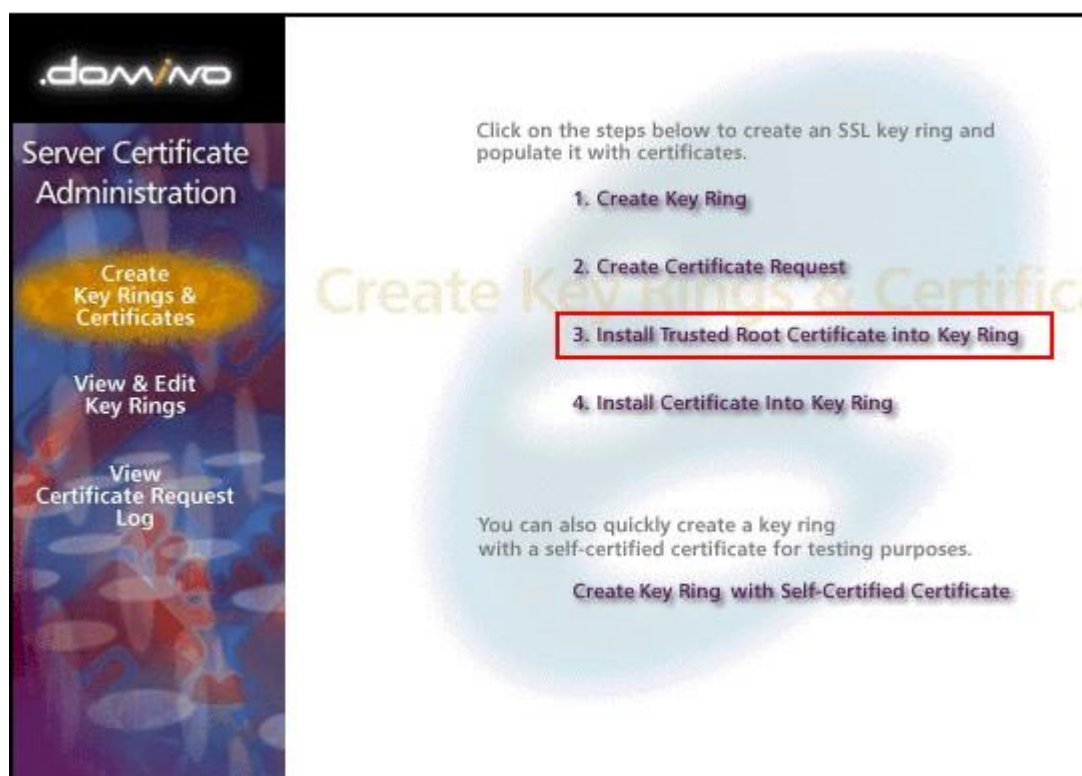
1. A certificate for the signing CA is not present in your server key ring.
2. A certificate for the signing CA is present in your server key ring, but it is not marked as a Trusted Root.

You can install the server certificate anyway, or you can exit for now to install the CA certificate in your server key ring and mark it as a Trusted Root.

**Click OK to install the server certificate anyway.**  
**Click Cancel to exit.**

發生此問題之用戶請於伺服器安裝 GT 的根憑證，操作方式如下

1. 進入『Install Trusted Root Certificate into Key Ring』



2. 於 certificate Source 選擇 Clipboard

Install Trusted Root Certificate	
<p>Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. <b>Note:</b> This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.</p>	
Key Ring Information	Quick Help
Key Ring File Name <input type="text" value="d:\lotus\dominold\data\filename.kyr"/>	Specify the key ring file.
Certificate Information	
Certificate Label <input type="text"/>	The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.
Certificate Source <input type="radio"/> File <input checked="" type="radio"/> Clipboard	The source of the certificate can be from a file or from the clipboard.
Certificate from Clipboard: <input type="text"/>	Paste clipboard contents into this field. <b>Note:</b> The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.

3. 於跳出之下方文字方框輸入： [GeoTrust root 根憑證]

開啟記事本，依據購買方案將以下根憑證資訊複製存檔為 root.cer

購買 EV 等級使用的 CA Root

```
-----BEGIN CERTIFICATE-----
MIID/jCCAuagAwIBAgIQFaxulBmyeUtB9iepwXgPHzANBgkqhkiG9w0BAQsFADCB
mDELMaKGA1UEBhMCVVMxMjYwMzYwMzYwMzYwMzYwMzYwMzYwMzYwMzYwMzYwMzYw
MChjKSAyMDA4IEdlb1RydXN0IEluYy4gLSBGb3IyYXV0aG9yaXplZCB1c2Ugb25s
eTE2MDQGA1UEAxMTR2VvVHJ1c3QgUHJpbWVyeSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cmI0eSAtIEczMB4XDTA4MDQwMjYwMzYwMzYwMzYwMzYwMzYwMzYwMzYwMzYwMzYw
BgNVBAYTAIVTMRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMTkwNwYDVQQLZSAAoYykg
MjAwOCBHZW9UcnVzdCBJbmMuIC0gRm9yIGF1dGhvcml6ZWQgdXNlIG9ubHkxNjA0
BgNVBAMTLUdlb1RydXN0IFByaW1hcncgQ2VydGlmaWNhdGlubiBBdXR0b3JpdHkg
LSBHMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANziXmJYHTNXOTIz
+uvLh4yn1ErdBojqZI4xmKU4kB6Yzy5jK/BGvESyiaHAKAxJcCGVn2TAppMSAmUm
hsalifD614SgcK9PGpc/BkTVyetyEH3kMSj7HGHmKAdEc5IaacDiGydY8hS2pgn
5whMcD60yRLBxWeDXTPzAxHsatBT4tG6NmCUgLthY2xbF37fQJQeqw3CIShwiP/W
JmxsYAQITIV+fe+/IEjetx3dcI0FX4ilm/LC7urRQEFTyJgdVgbFA0dRIBn8exAL
DmKudIW/X3e+PkkBUz2YJQN2JFodtNuJ6nnlitrM7P7pMKEF/BqxqjsHQ9gUdfeZC
huOI1UcCAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYw
HQYDVR0OBBYEFMR5yo6hTgMdHNxr2zFbID4/MH8tMA0GCSqGSIb3DQEBCwUAA4IB
AQAAtxRPPVoB7eni9n64smefv2t+UXglpp+duaIy9cr5HqQ6XErhK8WTTod8INNTB
zU6B8A8ExCSzNjBgpqow32hnc9f5joWJ7w5elShKKiePEI4ufIbEAp7aDHdIdkQN
kv39sxY2+hENHYwOB4lqKvb3cvTdfZx3NWZXqxNT2I7BQMXXExZacse3aQHEerGD
AWH9jUGhIbJBJVz88P6DAod8DQ3PLghcSkANPuyBYeYk28rgDi0Hsj5W3I31QYUH
SJSMC8tJP33st/3LjWeJGqvtux6jAAgIFyqCXDFdRootD4abdNIF+9RAsXqqaC2G
spki4cErX5z481+oghLrGRET
-----END CERTIFICATE-----
```

非 EV 等級使用的 CA Root

```
-----BEGIN CERTIFICATE-----
MIIDVDCCAjygAwIBAgIDAJRWMA0GCSqGSIb3DQEBBQUAMEIxCzAJBgNVBAYTAIVT
MRYwFAYDVQQKEw1HZW9UcnVzdCBJbmMuMRswGQYDVQQDEw1HZW9UcnVzdCBHbG9i
YWwgQ0EwHhcNMDIwNTIxMDQwMDAwWhcNMjYwMzYwMzYwMzYwMzYwMzYwMzYwMzYw
EwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjE5bWVkb3R1c2Ugb25sR2xvYmFs
IENBMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAA2swYYzD9
9BcjGIZ+W988bDjkcdb4kdS8odhM+KhDtgPpTSEHCiJaWC9mOSm9BXiLnTjoBbdq
fnGk5sRgprDvgOSJKA+eJdbtg/OtppHHmMICGDUUna2YRpIuT8rxh0PBFpVXLVDv
iS2Aelet8u5fa9IAjkbU+BQVNdnARqN7csiRv8IVK83QlZ6cJmTM386DGXHKtubU
-----END CERTIFICATE-----
```

```
1XupGc1V3sjs0l44U+VcT4wt/IAjNvxm5suOpDkZALeVAjmRCw7+OC7RHQWa9k0+
bw8HHa8sHo9gOeL6NIMTOdReJivbPagUvTLrGAMoUgRx5aszPeE4uwc2hGKceeoW
MPRfwCvocWvk+QIDAQABo1MwUTAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbTA
ephofjYn7qwVkdBF9qn1luMrMTjAfBgNVHSMEGDAWgBTAephofjYn7qwVkdBF9qn1l
uMrMTjANBgkqhkiG9w0BAQUFAAOCAQEANeMpauUvXVSOKVCUn5kaFOSPeCpilKIn
Z57QzxpER+nBsqTP3UEaBU6bS+5Kb1VSsyShNwrrZHYqLizz/Tt1kL/6cdjHPTfS
tQWVYrmm3ok9Nns4d0iXrKYgjy6myQzCsplFAMfOEVEiIuCl6rYVSAIk6l5PdPcF
PseKUgzbFbS9bZvlxrFUaKnjaZC2mqUPuLk/IH2uSrW4nOQdtqvmIKXBx4Ot2/Un
hw4EbNX/3aBd7YdStysVAq45pmp06drE57xNNB6pXE0zX5IJL4hmXXeXxx12E6nV
5fEWCRE11azbJHFWLJhWC9kXtNHjUStedejV0NxPNO3CBWaAocvmMw==
-----END CERTIFICATE-----
```

4. 再次進入『[Install Trusted Root Certificate into Key Ring](#)』

5. 於 certificate Source 選擇 Clipboard

6. 於跳出之下方文字方框輸入：[頒發下來您的憑證資訊]

\*資料請都使用文本方式寫入，並將-----BEGIN CERTIFICATE-----、-----END CERTIFICATE-----兩行字串，不要複製寫入。

7. 再次進入『[Install Trusted Root Certificate into Key Ring](#)』

8. 於 certificate Source 選擇 Clipboard

9. 於跳出之下方文字方框輸入：[對應的中繼憑證檔案]

\*資料請都使用文本方式寫入，並將-----BEGIN CERTIFICATE-----、-----END CERTIFICATE-----兩行字串，不要複製寫入。

10. 進入『[Install Certificate into Key Ring](#)』



domino

## Server Certificate Administration

- Create Key Rings & Certificates
- View & Edit Key Rings
- View Certificate Request Log

### Create Key Rings & Certificates

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate Into Key Ring

You can also quickly create a key ring with a self-certified certificate for testing purposes.

[Create Key Ring with Self-Certified Certificate](#)

#### 11. 於 certificate Source 選擇 Clipboard

Install Certificate into Key Ring	
<p>The Certificate Authority will notify when your signed certificate is ready. The specifics depend on the Certificate Authority, but typically you will receive an e-mail specifying a URL where you can pick up the certificate. Once you have obtained the signed certificate, this form lets you install it into your key ring. <b>Note:</b> Before installing this certificate, it is recommended that you install the certificate of the signing Certificate Authority in your key ring as a Trusted Root. If you haven't already done so, choose "Accept This Authority In Your Server" from the main menu of the Certificate Authority Web site to obtain the CA certificate.</p>	
<p><b>Key Ring Information</b></p> <p>Key Ring File Name <input type="text" value="d:\notus\domino\data\filename.kyr"/></p>	<p><b>Quick Help</b></p> <p>Specify the key ring file.</p>
<p><b>Certificate Information</b></p> <p>Certificate Source <input type="radio"/> File <input checked="" type="radio"/> Clipboard</p> <p>Certificate from Clipboard: <input type="text" value=""/></p>	<p>The source of the certificate can be from a file or from the clipboard.</p> <p>Paste the clipboard contents into this field.</p> <p><b>Note:</b> The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.</p>
<p>Merge Certificate into Key Ring</p>	



12. 於跳出之下方文字方框輸入最後憑證所核發的資訊。

13. 憑證即可正常安裝於伺服器。