

中華電信通用憑證管理中心 (PublicCA)

Windows IIS 系列 SSL 憑證請求檔製作與安裝手冊附錄

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。

目錄

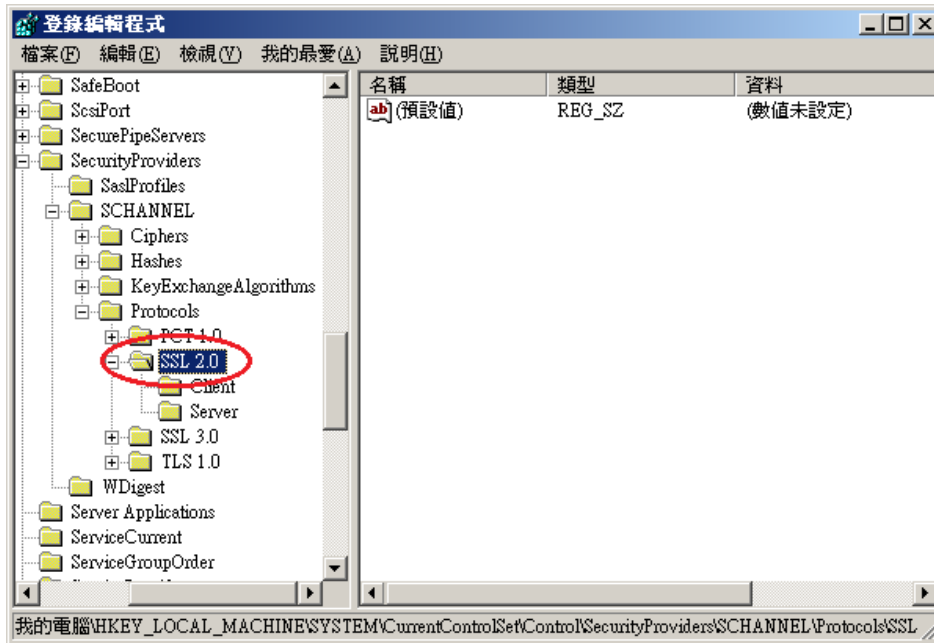
停用 SSLv2、SSLv3.....	2
Windows Server 2003 IIS 6.....	2
Windows Server 2008 IIS 7.....	7
Windows Server 2012 IIS 8.....	13
更換 SHA256 憑證.....	17
Windows Server 2003 IIS 6.....	17
Windows Server 2008 IIS 7.....	38
Windows Server 2012 IIS 8.....	51

停用 SSLv2、SSLv3

Windows Server 2003 IIS 6

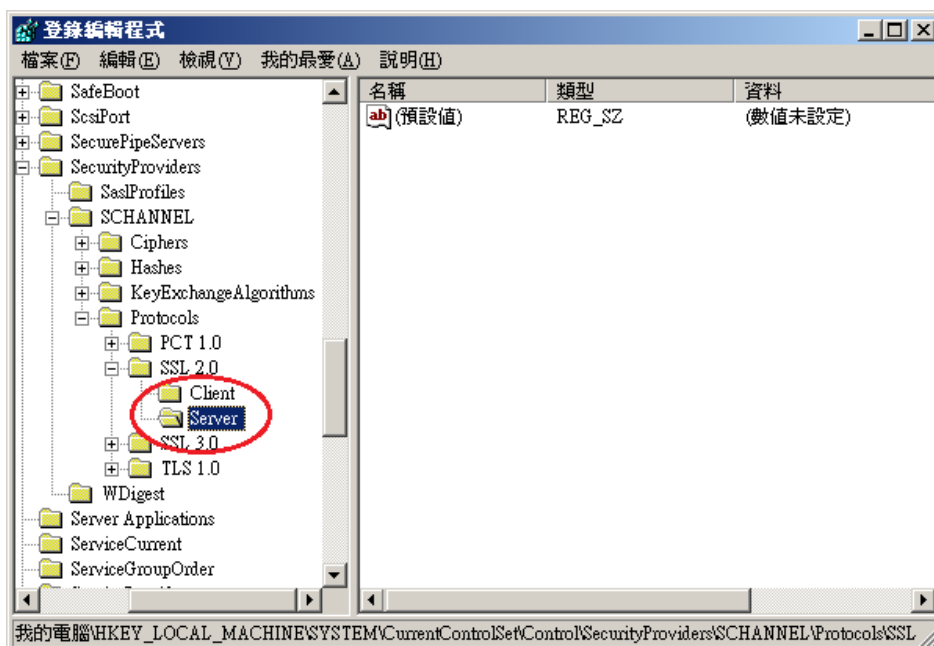
一、開啟登錄檔編輯程式，依照以下路徑找到 SSL2.0。

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0

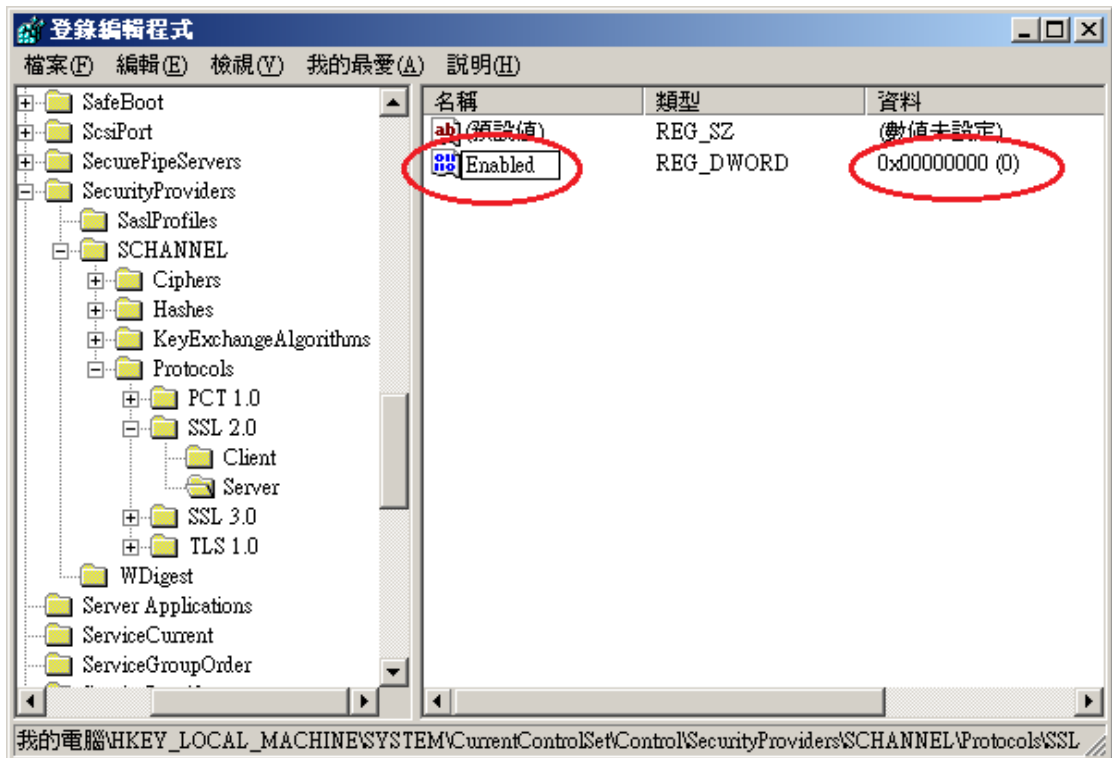
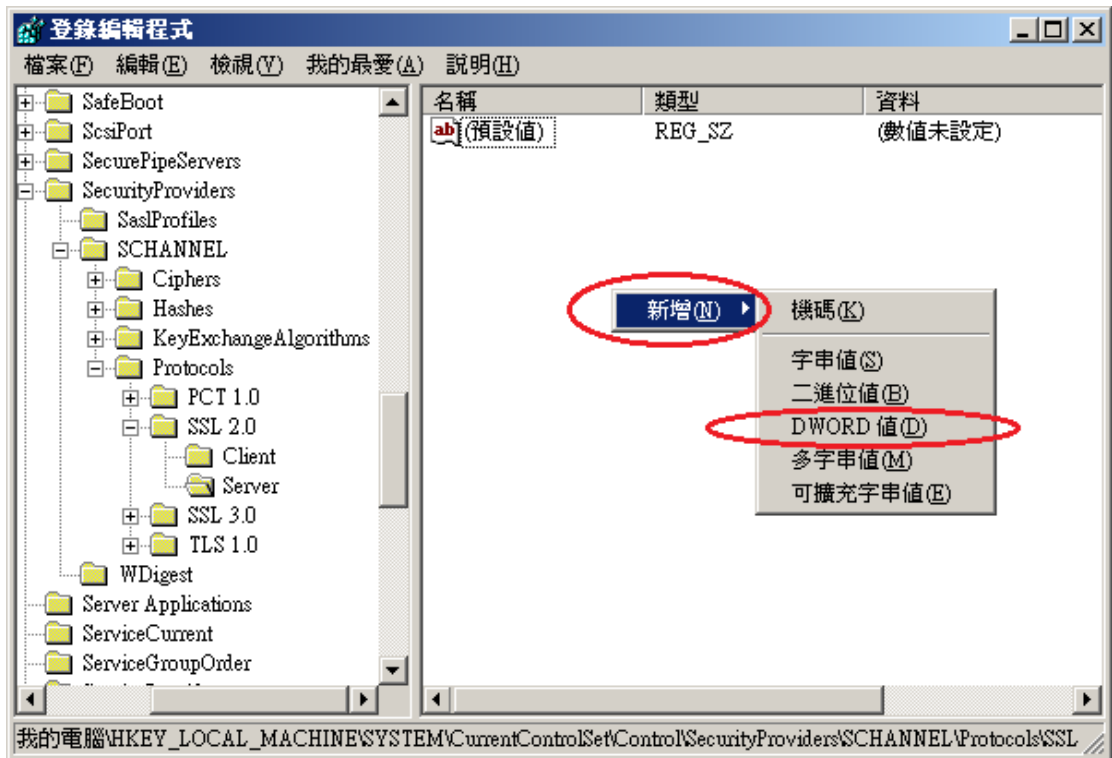


二、找到 SSL 2.0 下，「Server」的機碼，並點選之。

若無「Server」的機碼，請在 SSL2.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」。

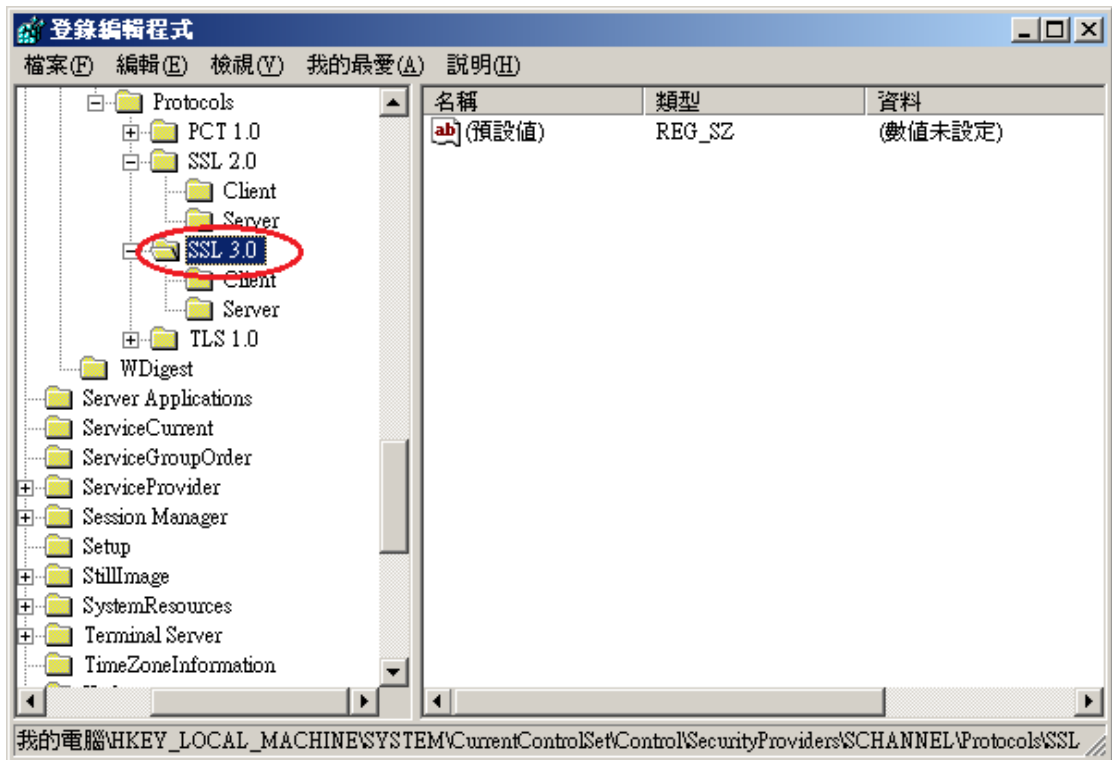


三、接著在右邊的畫面下按右鍵→新增→DWORD 值，然後輸入「Enabled」，並確認資料欄位值為「0x00000000 (0)」，若不是，請手動將值改為 0。



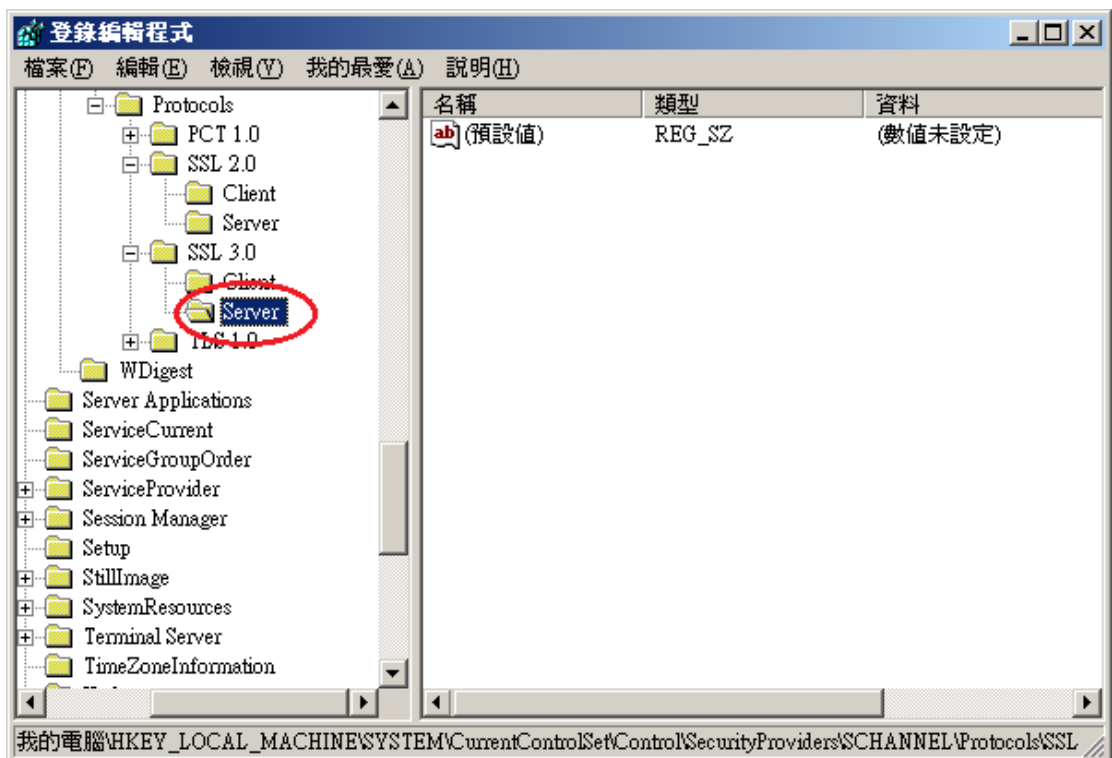
四、依照以下路徑找到 SSL3.0。

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0

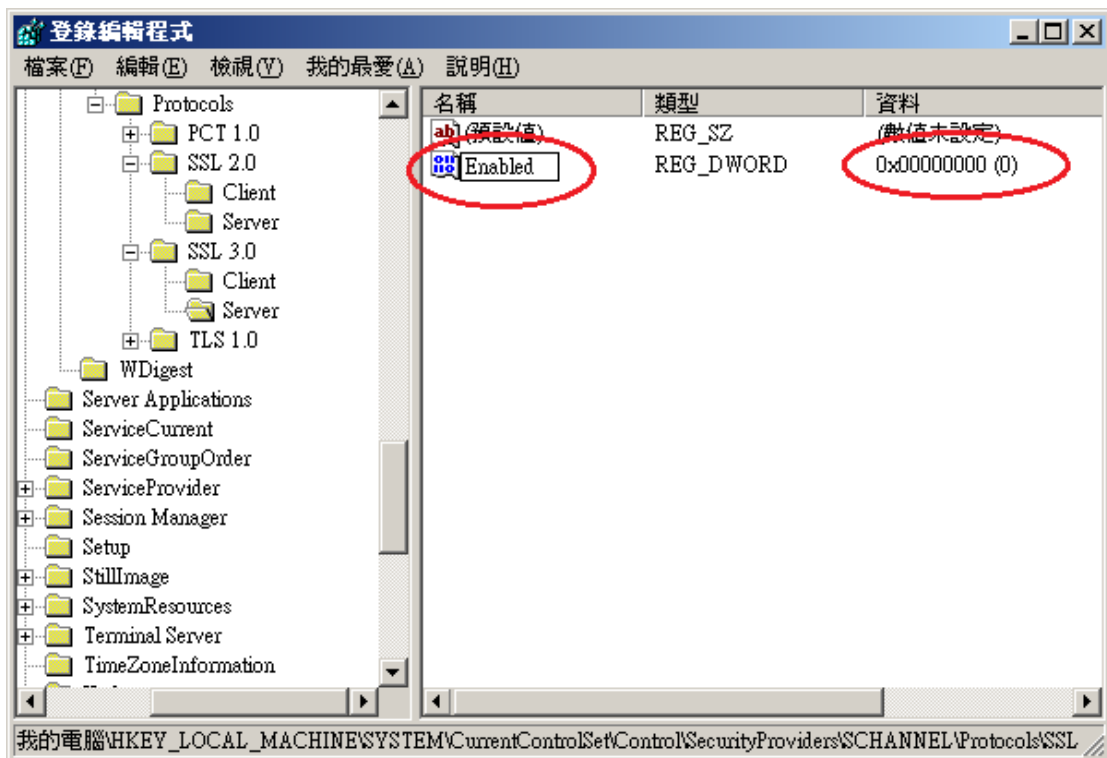
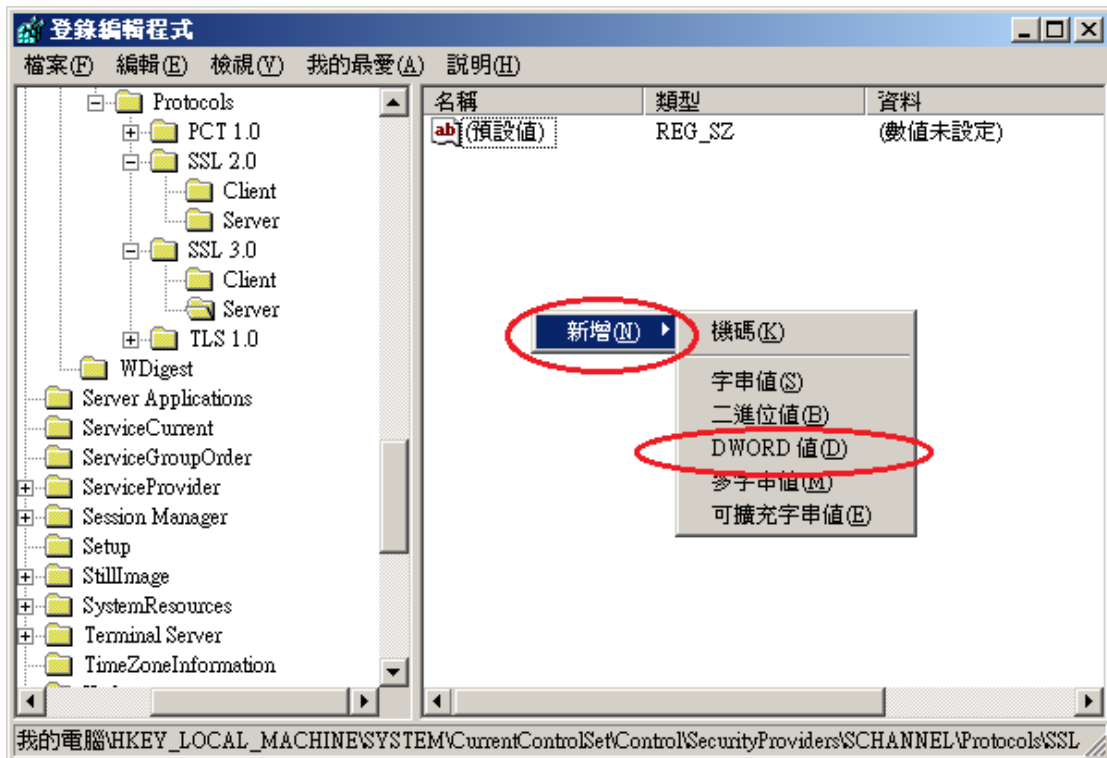


五、找到 SSL 3.0 下，「Server」的機碼，並點選之。

若無「Server」的機碼，請在 SSL3.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」。



六、接著在右邊的畫面下按右鍵→新增→DWORD 值，然後輸入「Enabled」，並確認資料欄位值為「0x00000000 (0)」，若不是，請手動將值改為 0。



七、重新啟動電腦。啟動完成後，可以使用測試工具（註 1、註 2）進行檢測，看 SSL 2.0、SSL3.0 是否已停用。

註 1: 例如行政院國家資通安全會報技服中心網頁

<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh> 有介紹兩種檢測伺服器端 SSL 協定的工具：(1) TestSSLServer

(<http://www.bolet.org/TestSSLServer/>) 與(2) QUALYS SSL LABS SSL Server Test 檢測工具(<https://www.ssllabs.com/sslltest/index.html>, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定, 因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點, 弱點編號 CVE-2014-3566 (POODLE), 故建議不要使用 SSL V3 協定, 請改用 TLS 最新協定。

註 2:

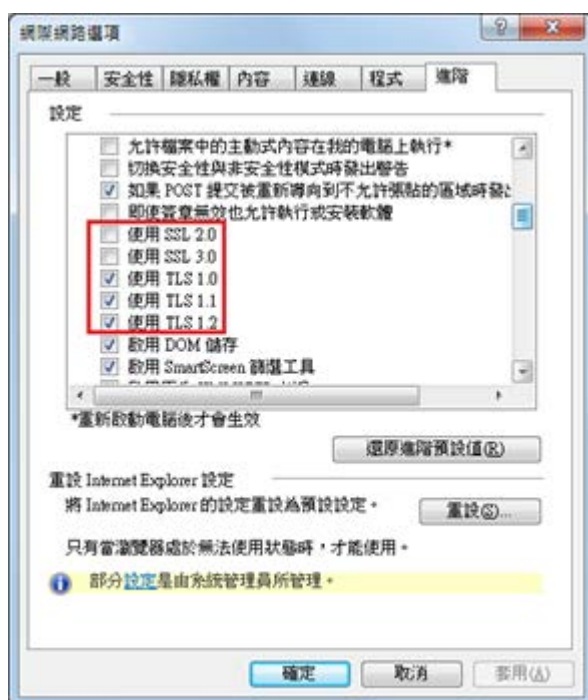
(1)若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考

<https://zmap.io/ssl3/browsers.html> 之英文說明

(2)請超連結至 <https://dev.ssllabs.com/sslltest/viewMyClient.html> 可檢測您用戶端之瀏覽器是否已經停用 SSL V3。

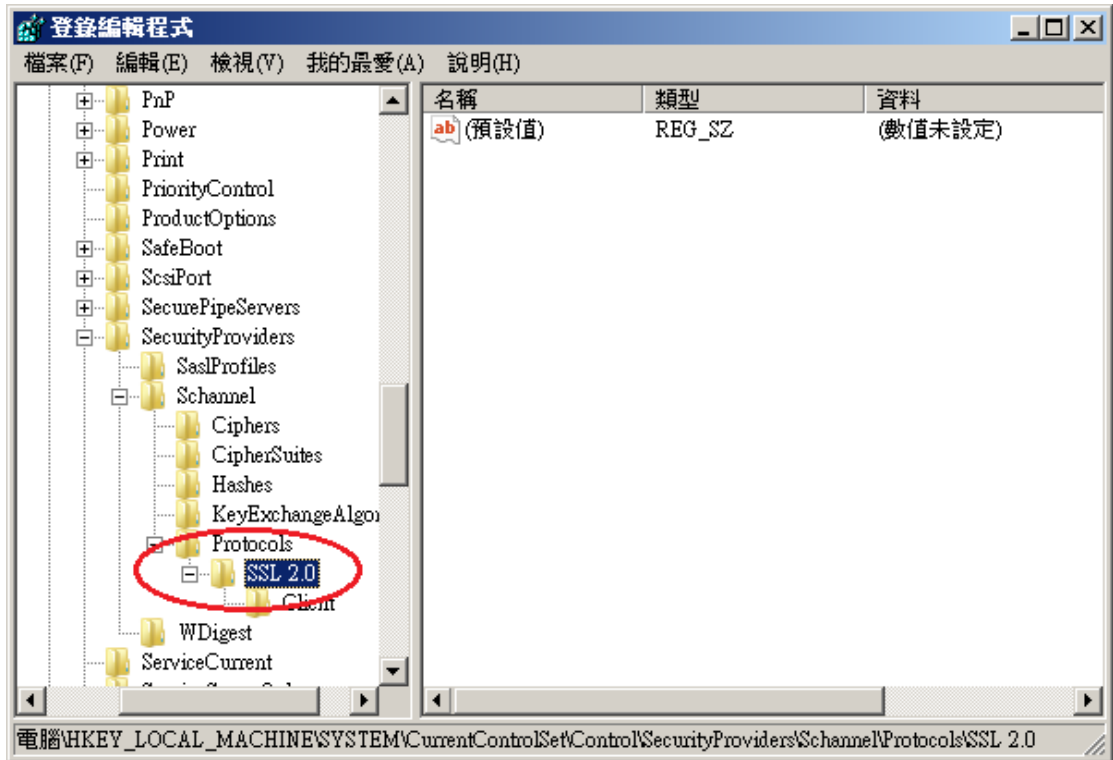
(3)若是 I.E. 瀏覽器可於工具列-> 網際網路選項->進階->安全性取消勾選使用 SSL V3 與使用 SSL V2, 或參考下圖設定 (取材自行政院國家資通安全會報技服中心網頁

<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh>)

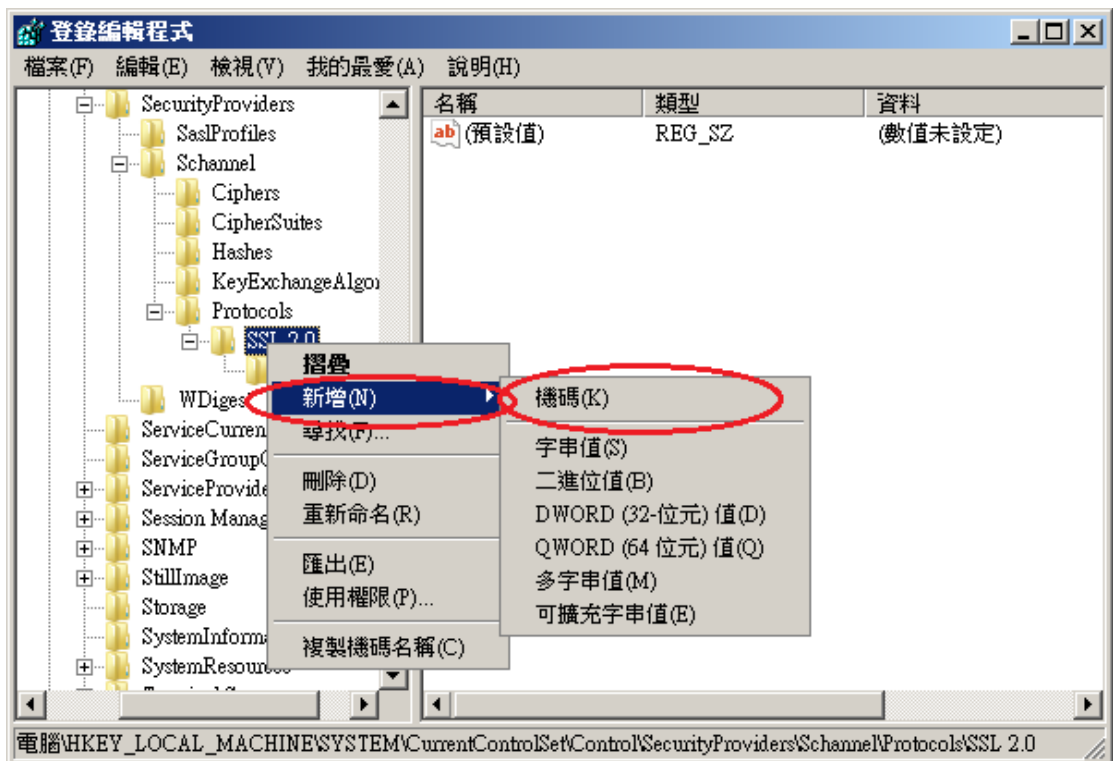


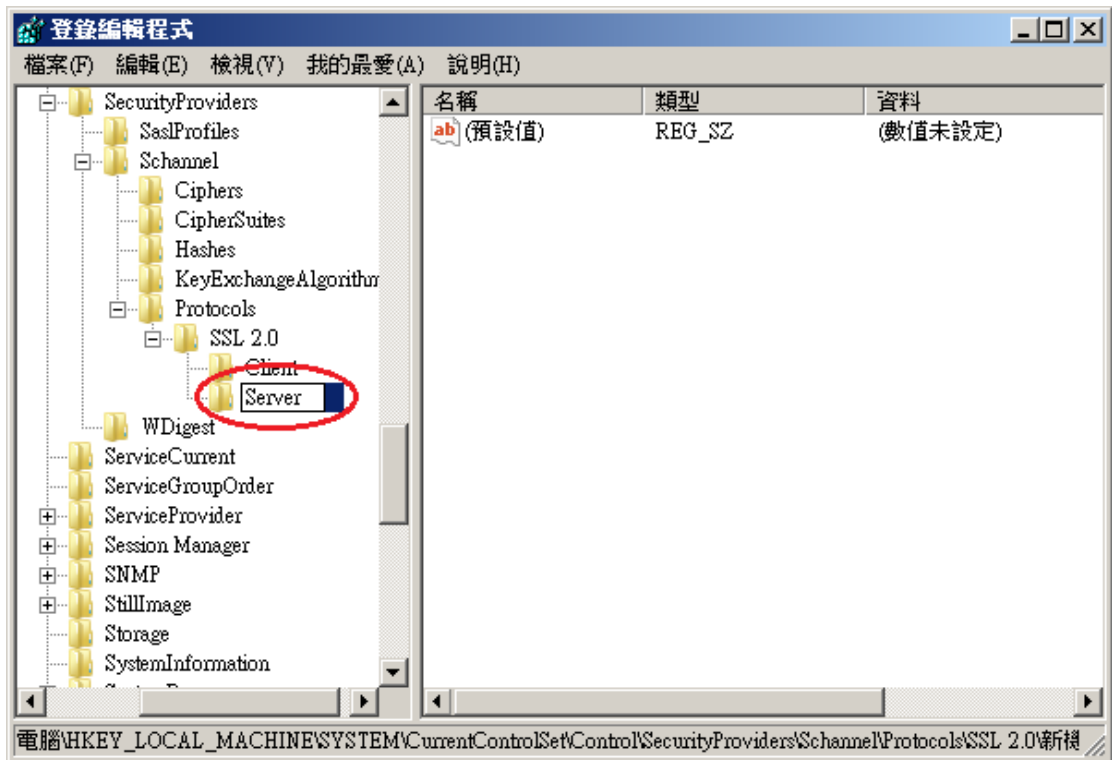
一、開啟登錄檔編輯程式，依照以下路徑找到 SSL2.0。

**HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProvider
ers\SCHANNEL\Protocols\SSL 2.0**

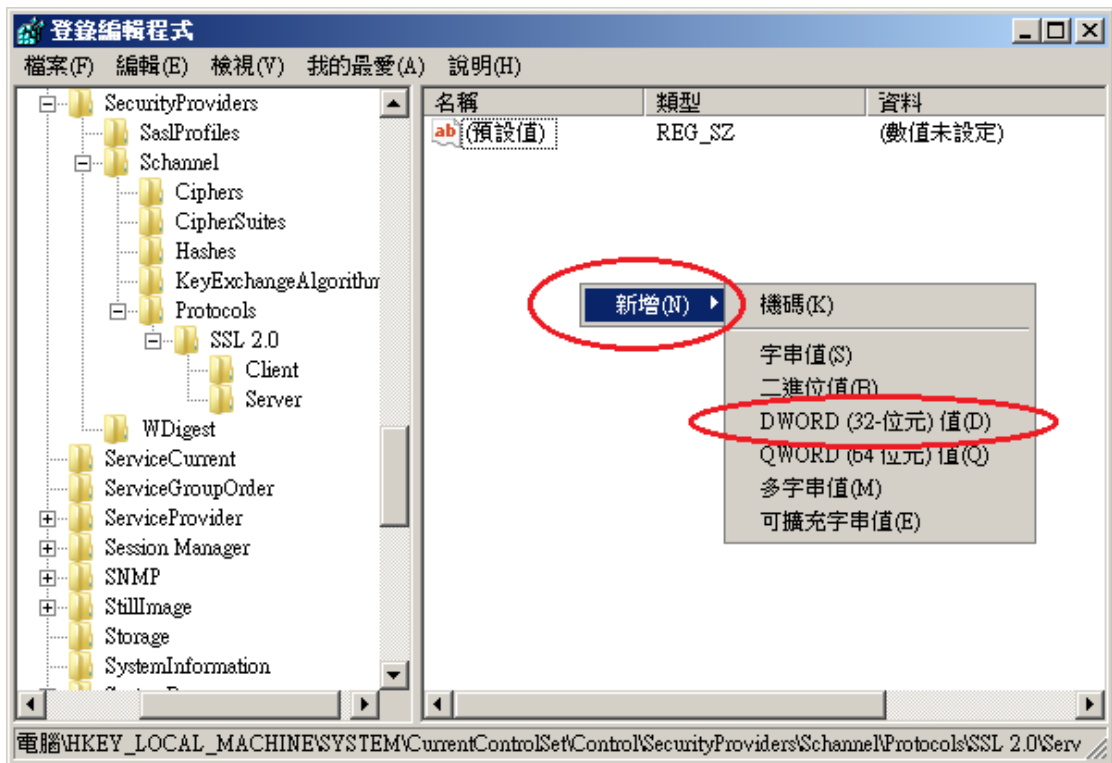


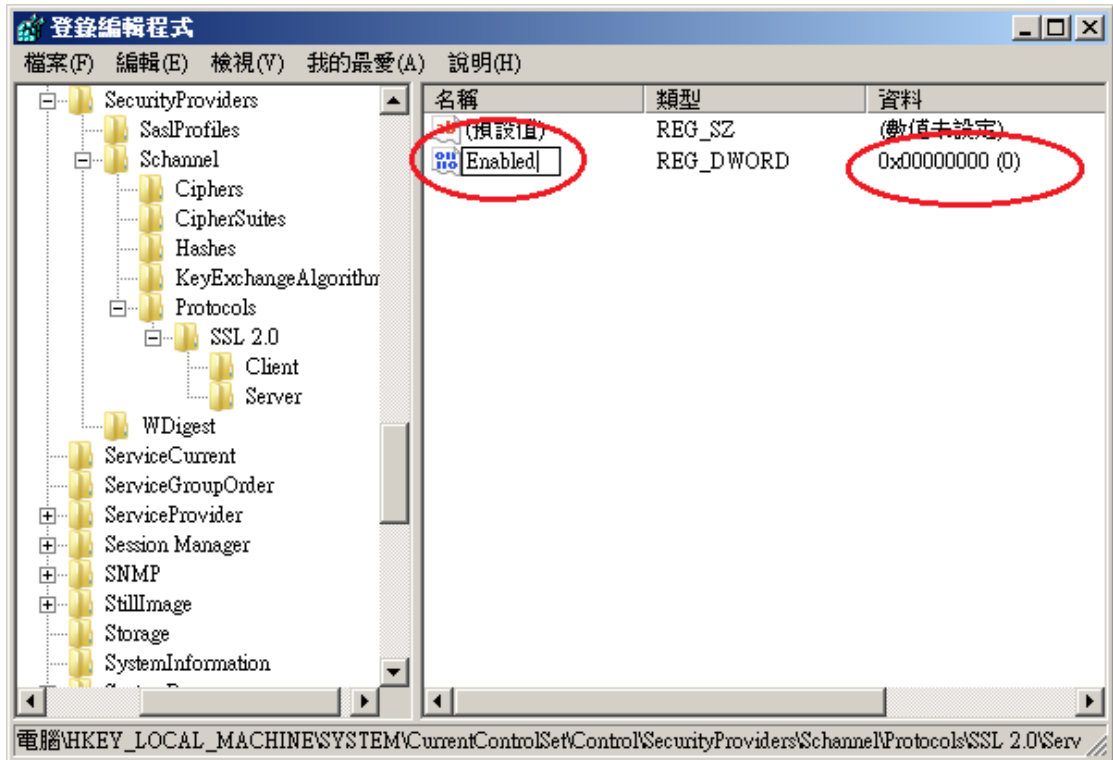
二、在 SSL2.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」。





三、接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值，然後輸入「Enabled」，並確認資料欄位值為「0x00000000 (0)」，若不是，請手動將值改為 0。



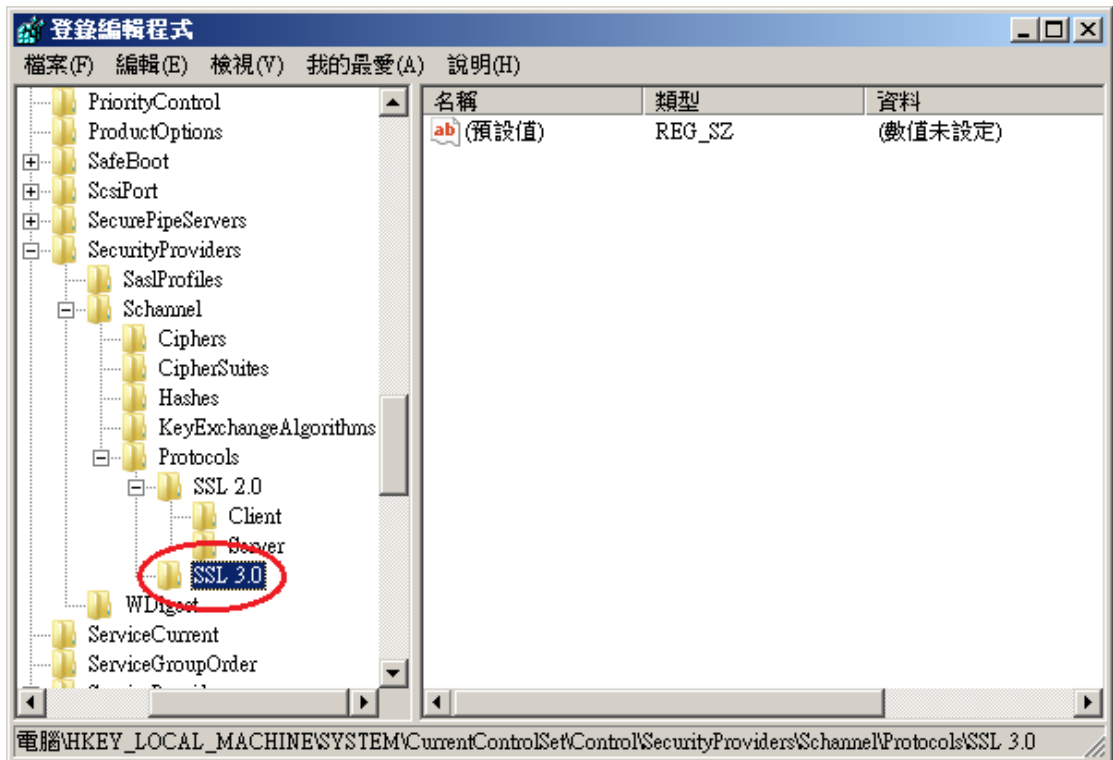


四、依照以下路徑找到 SSL3.0

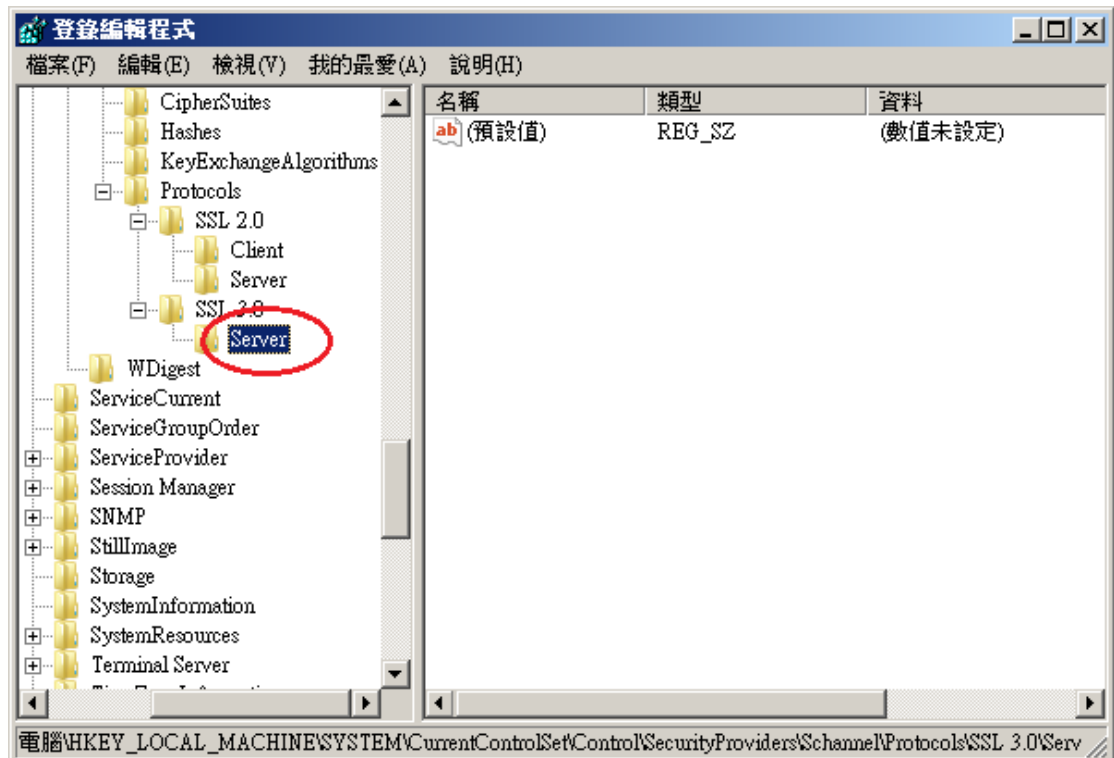
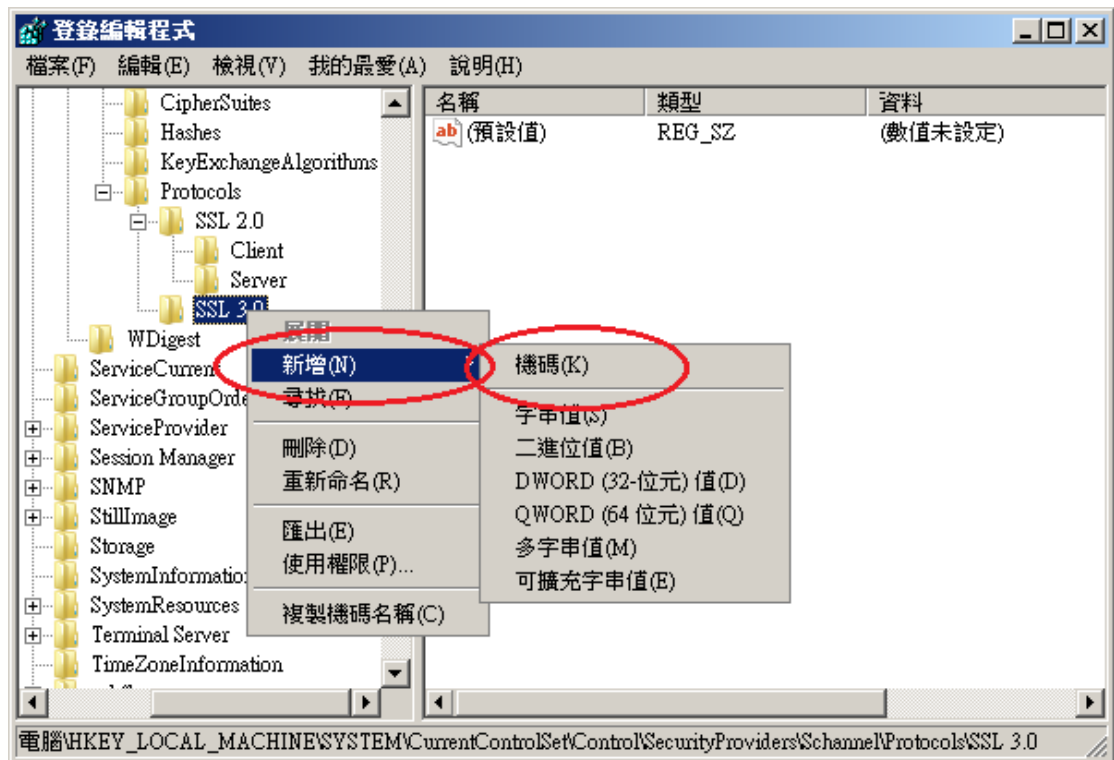
**HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProvider
s\SCHANNEL\Protocols\SSL 3.0**

若無 SSL3.0，請找到以下路徑，自行新增 SSL3.0 機碼。

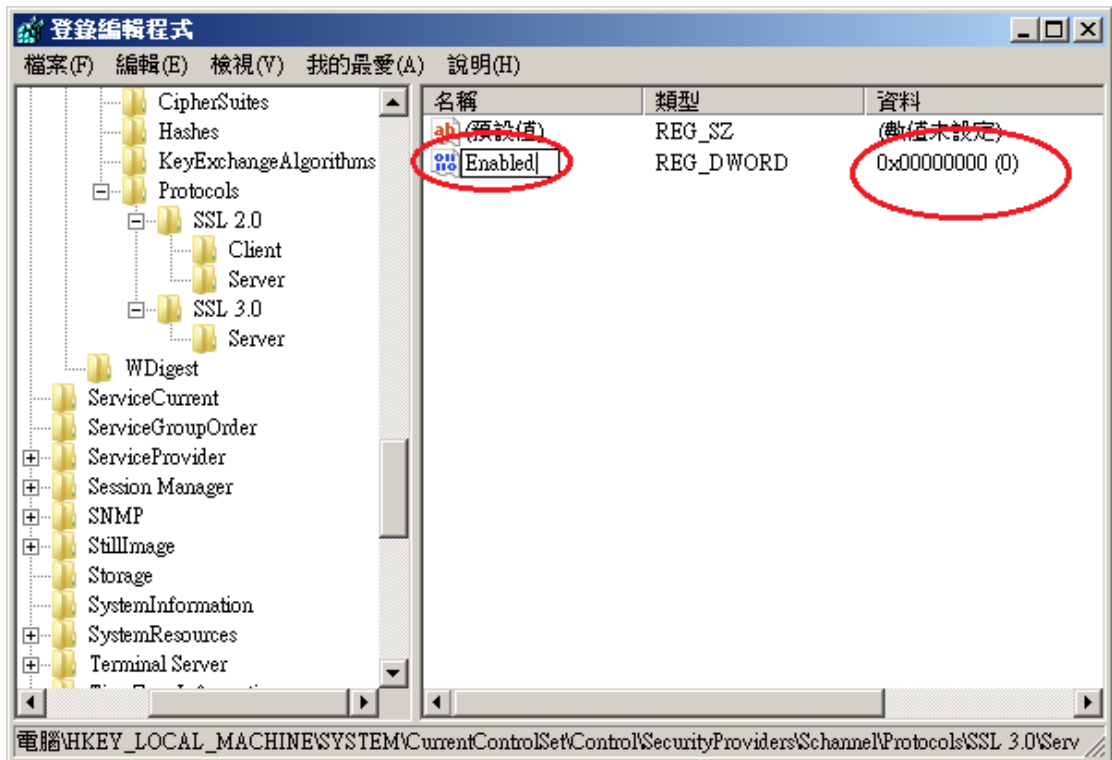
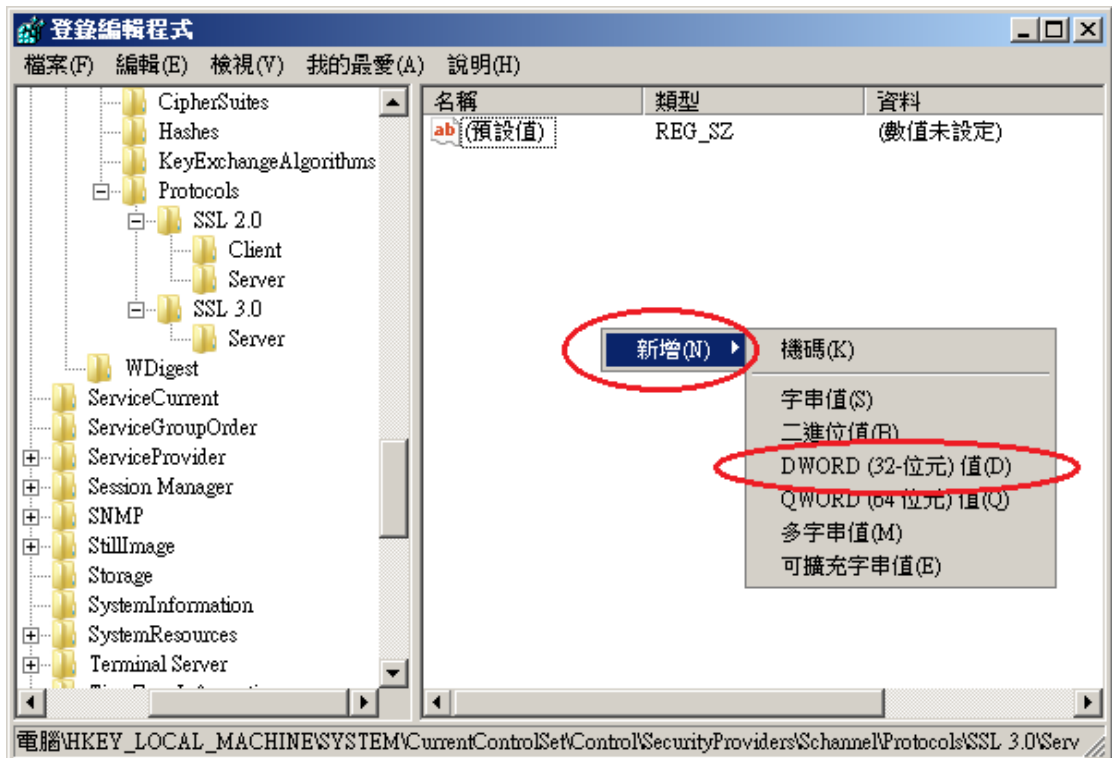
**HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProvider
s\SCHANNEL\Protocols**



五、在 SSL3.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」。



六、接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值，然後輸入「Enabled」，並確認資料欄位值為「0x00000000 (0)」，若不是，請手動將值改為 0。



七、重新啟動電腦。啟動完成後，使用可以測試工具（註 1、註 2）進行檢測，看 SSL 2.0、SSL3.0 是否已停用。

註 1: 例如行政院國家資通安全會報技服中心網頁

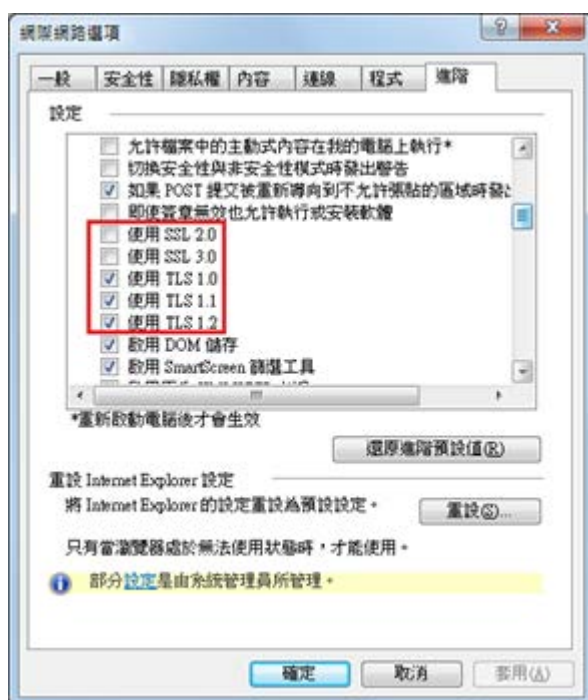
<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh> 有介紹兩種檢

測伺服器端 SSL 協定的工具：(1) TestSSLServer

(<http://www.bolet.org/TestSSLServer/>) (2) QUALYS SSL LABS SSL Server Test 檢測工具(<https://www.ssllabs.com/ssltest/index.html>, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定, 因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點, 弱點編號 CVE-2014-3566 (POODLE), 故建議不要使用 SSL V3 協定, 請改用 TLS 最新協定。

註 2:

- (1) 若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考 <https://zmap.io/sslv3/browsers.html> 之英文說明
- (2) 請超連結至 <https://dev.ssllabs.com/ssltest/viewMyClient.html> 可檢測您用戶端之瀏覽器是否已經停用 SSL V3。
- (3) 若是 I.E. 瀏覽器可於工具列-> 網際網路選項->進階->安全性取消勾選使用 SSL V3 與使用 SSL V2, 或參考下圖設定 (取材自行政院國家資通安全會報技服中心網頁 <http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh>)

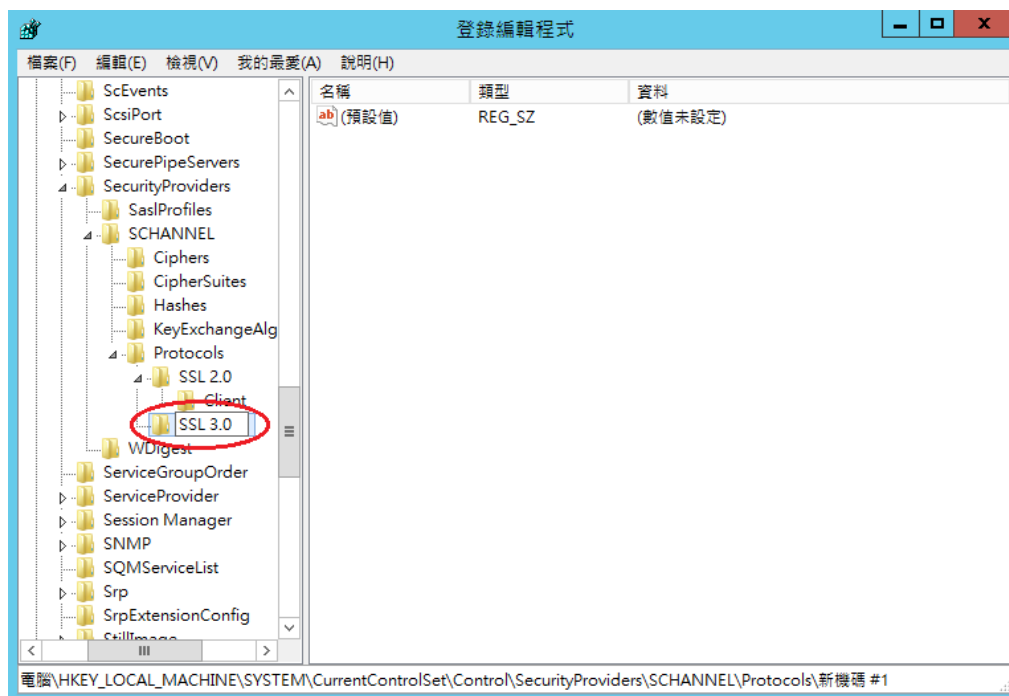
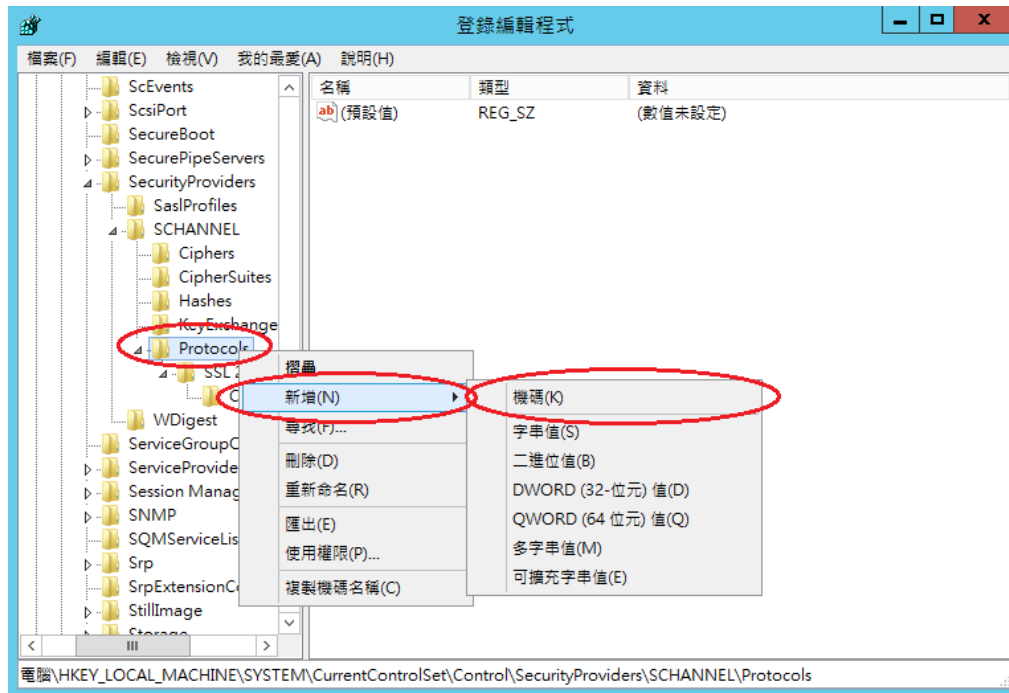


Windows Server 2012 IIS 8

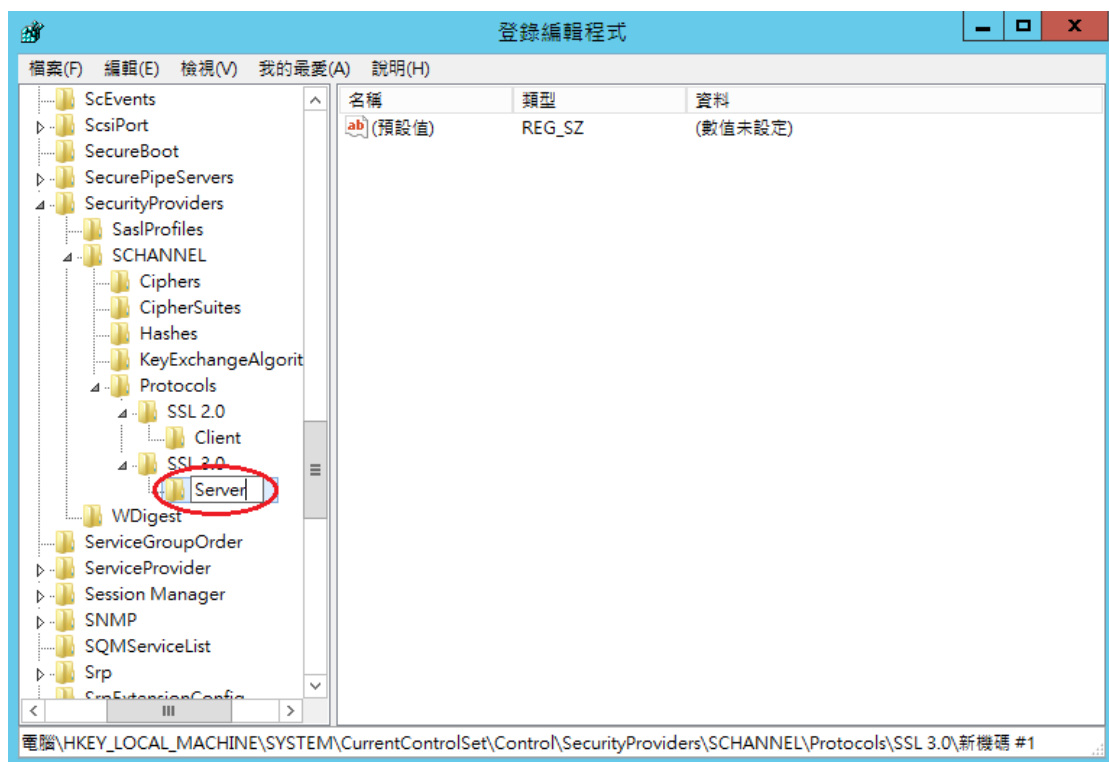
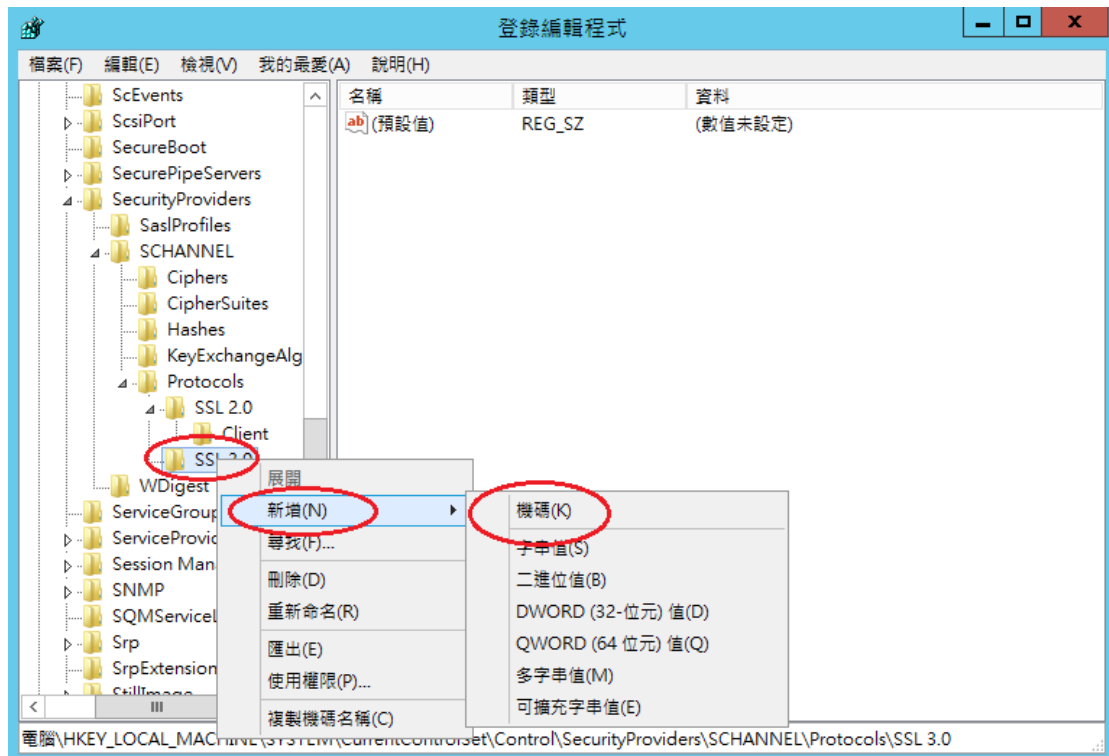
- 一、經測試，IIS8 SSL2.0 預設是關閉的，若您的 SSL2.0 是開啟的，您可以依照以下關閉 SSL 3.0 的作法來關閉 SSL2.0。
- 二、開啟登錄檔編輯程式，依照以下路徑找到 Protocols。

HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

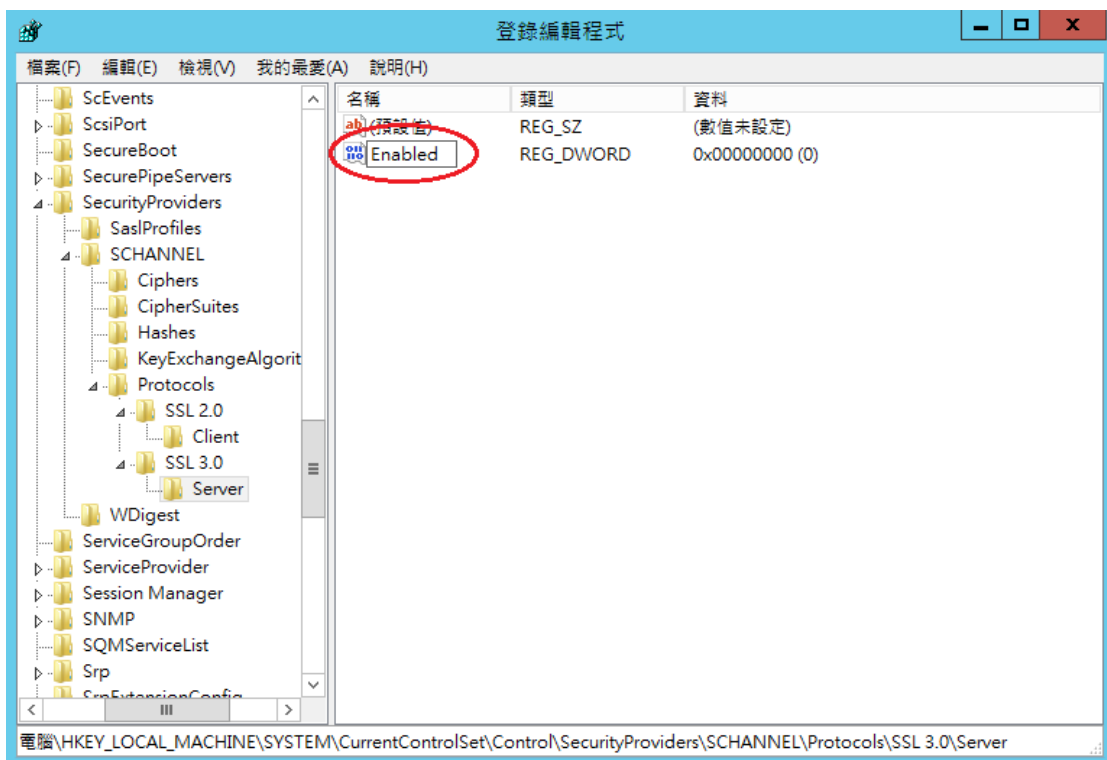
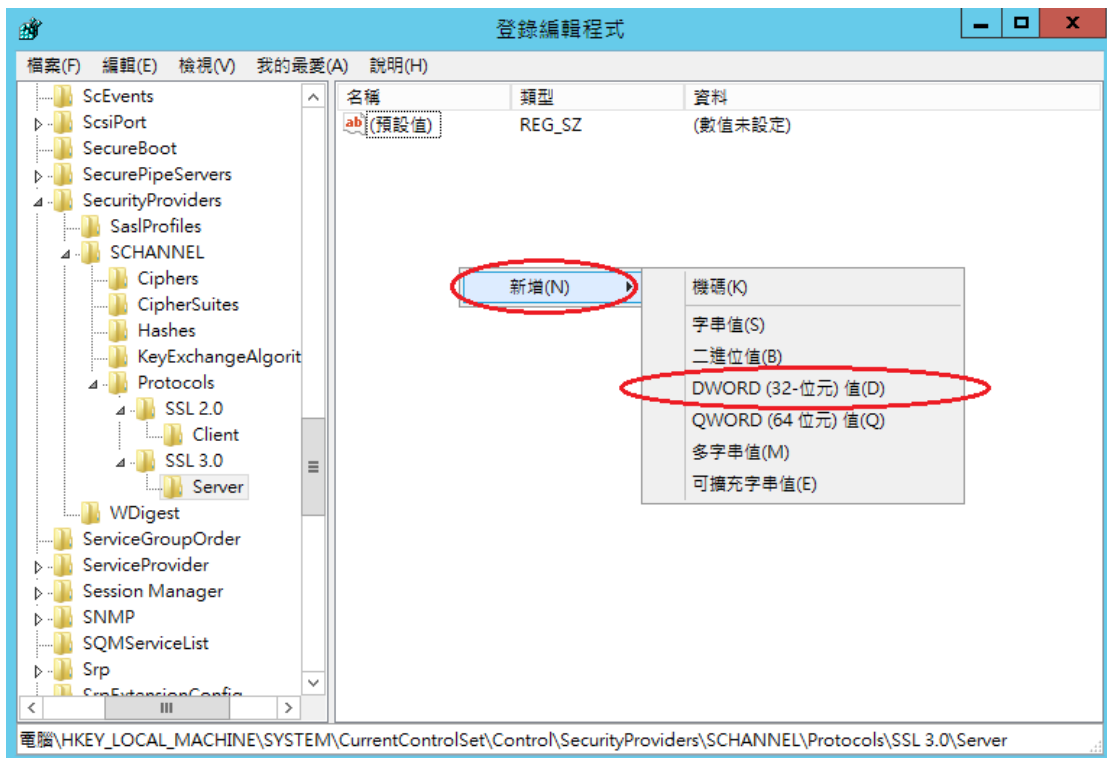
在 Protocols 的機碼上，按下右鍵→新增→機碼，然後輸入「SSL 3.0」。



三、在 SSL3.0 資料夾上按右鍵→新增→機碼，然後輸入「Server」。



四、接著在剛剛建立 Server 的資料夾下按右鍵→新增→DWORD(32-位元)值，然後輸入「Enabled」，並確認資料欄位值為「0x00000000 (0)」，若不是，請手動將值改為 0。



五、重新啟動電腦。啟動完成後，使用可以測試工具（註 1、註 2）進行檢測，看 SSL 2.0、SSL3.0 是否已停用。

註 1: 例如行政院國家資通安全會報技服中心網頁

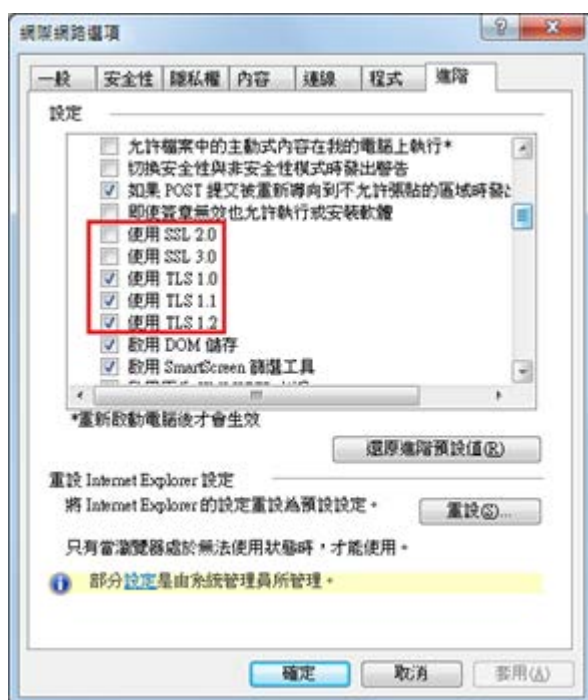
<http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh> 有介紹兩種檢

測伺服器端 SSL 協定的工具：(1) TestSSLServer

(<http://www.bolet.org/TestSSLServer/>) (2) QUALYS SSL LABS SSL Server Test 檢測工具(<https://www.ssllabs.com/ssltest/index.html>, 也是 CA/Browser Forum 網站建議的檢測工具)可偵測伺服器所使用之加密協定, 因 2014 年 10 月中國際公告了 SSLv3 加密協定存在中間人攻擊弱點, 弱點編號 CVE-2014-3566 (POODLE), 故建議不要使用 SSL V3 協定, 請改用 TLS 最新協定。

註 2:

- (1) 若是用戶端各平台之瀏覽器要停止使用 SSL V3 協定可參考 <https://zmap.io/ssl3/browsers.html> 之英文說明
- (2) 請超連結至 <https://dev.ssllabs.com/ssltest/viewMyClient.html> 可檢測您用戶端之瀏覽器是否已經停用 SSL V3。
- (3) 若是 I.E. 瀏覽器可於工具列-> 網際網路選項->進階->安全性取消勾選使用 SSL V3 與使用 SSL V2, 或參考下圖設定 (取材自行政院國家資通安全會報技服中心網頁 <http://www.icst.org.tw/NewInfoDetail.aspx?seq=1436&lang=zh>)



更換 SHA256 憑證

Windows Server 2003 IIS 6

- 一、適用於申請時，有同時取得 SHA1、SHA256 憑證。或是憑證再效期內，經由審驗人員再次核發 SHA256 憑證者。
- 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、需要先備妥 OpenSSL 軟體，或是找尋已安裝 OpenSSL 軟體的主機，後續將會使用到。

Windows 版 OpenSSL 軟體連結，可以只安裝「light」的版本即可：

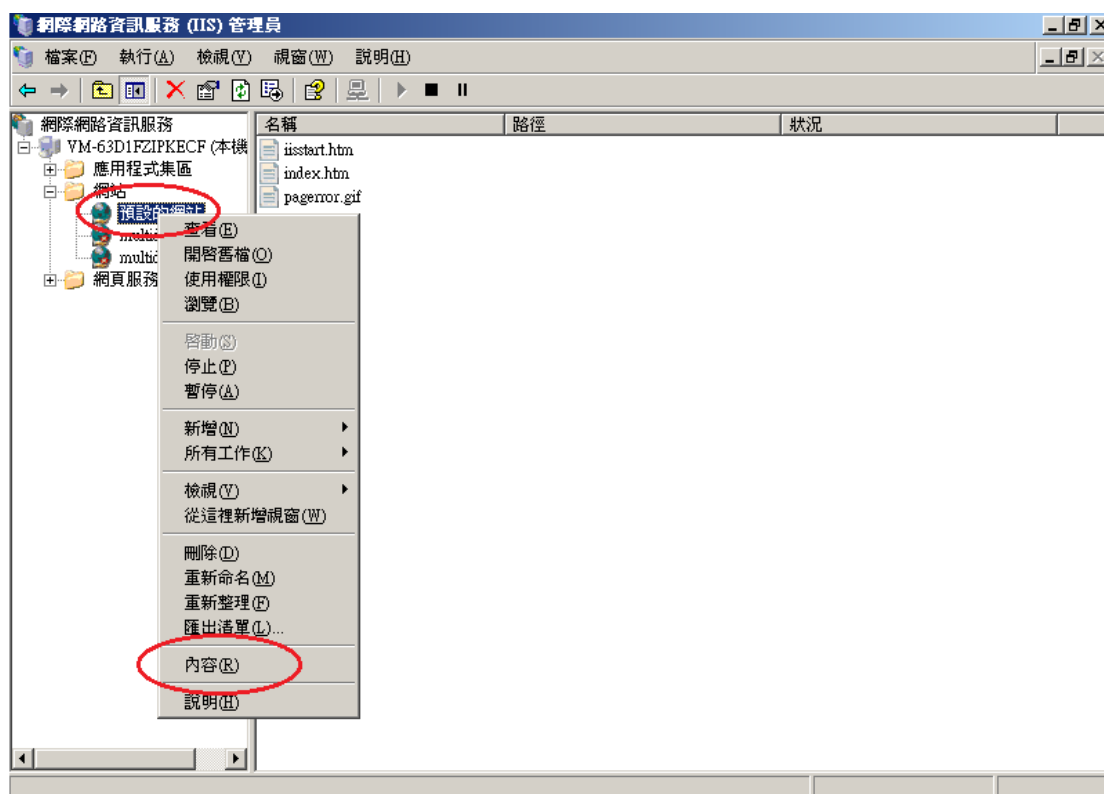
<https://www.openssl.org/related/binaries.html>

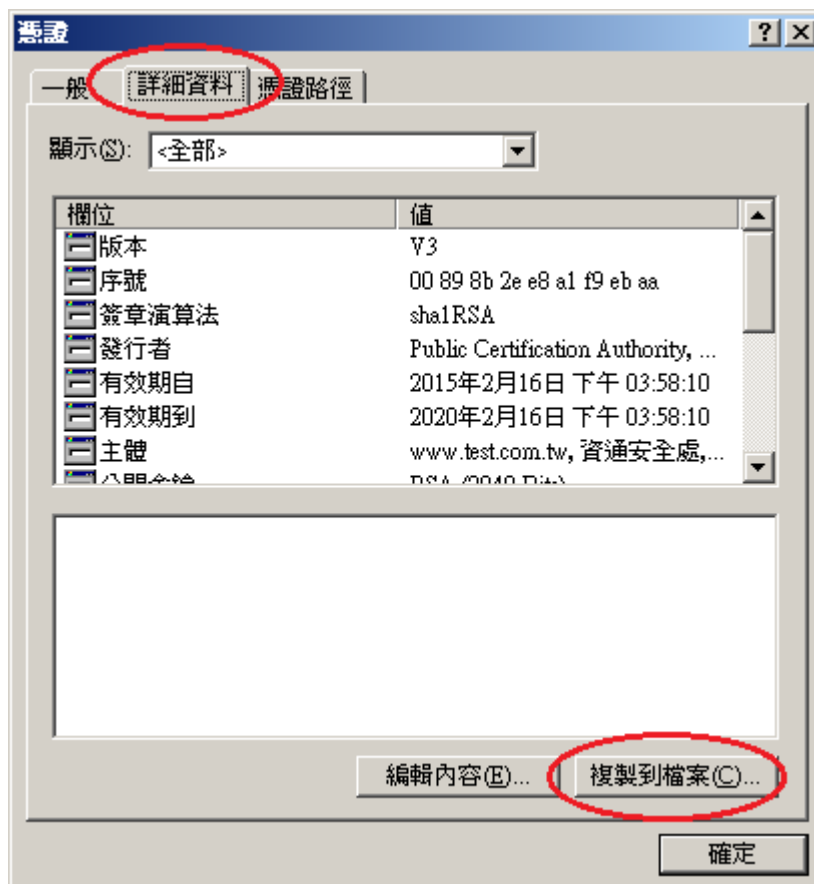
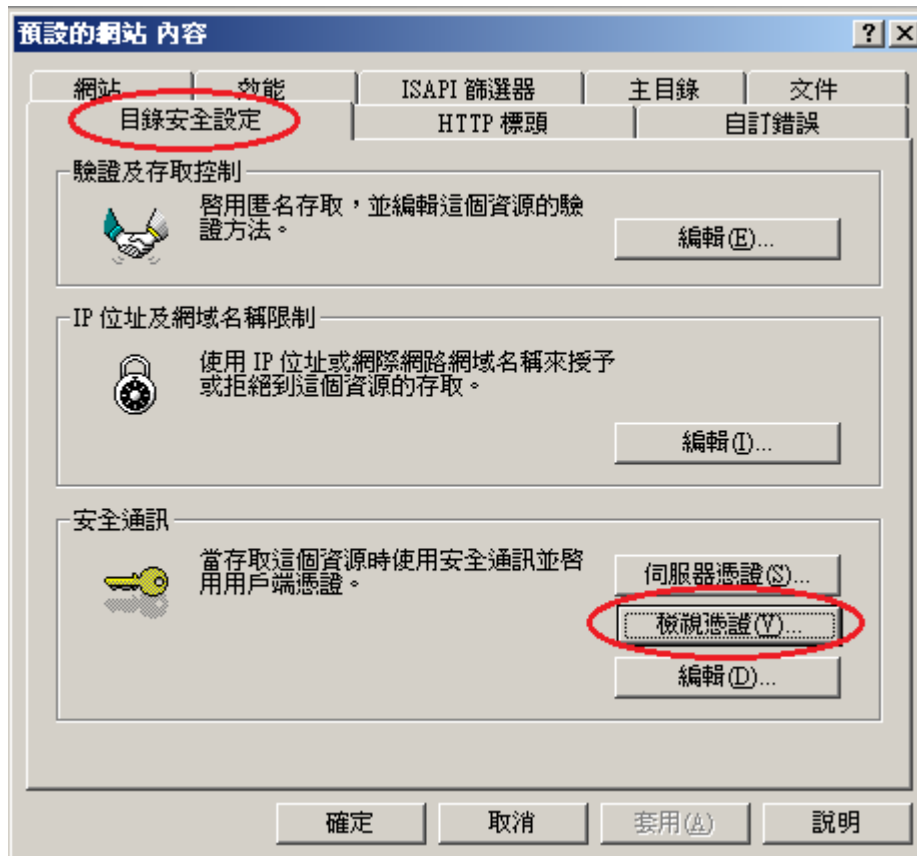
- 四、由於 Windows Server 2003 預設並不支援 SHA256 憑證，請依照您的需求參考以下連結，進行更新。

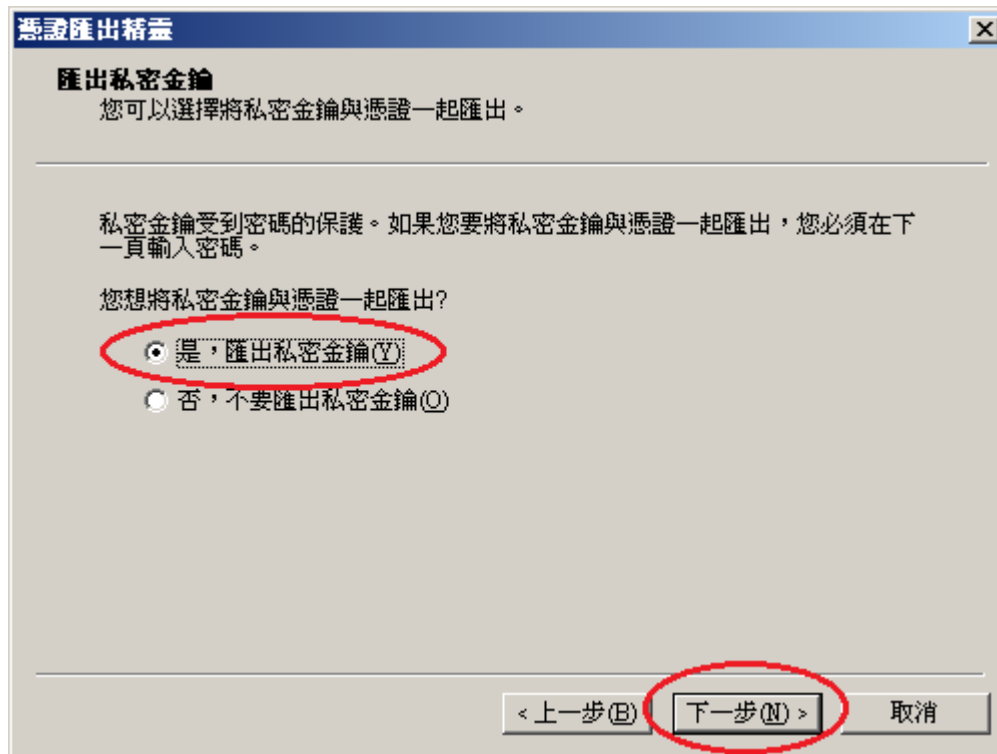
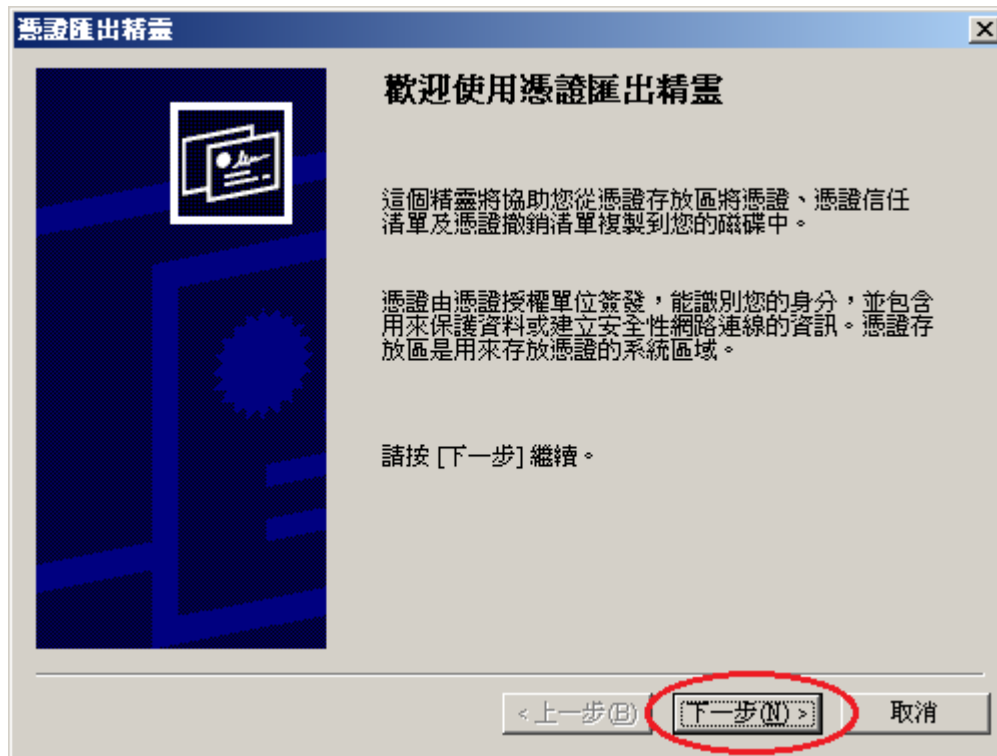
<http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx>

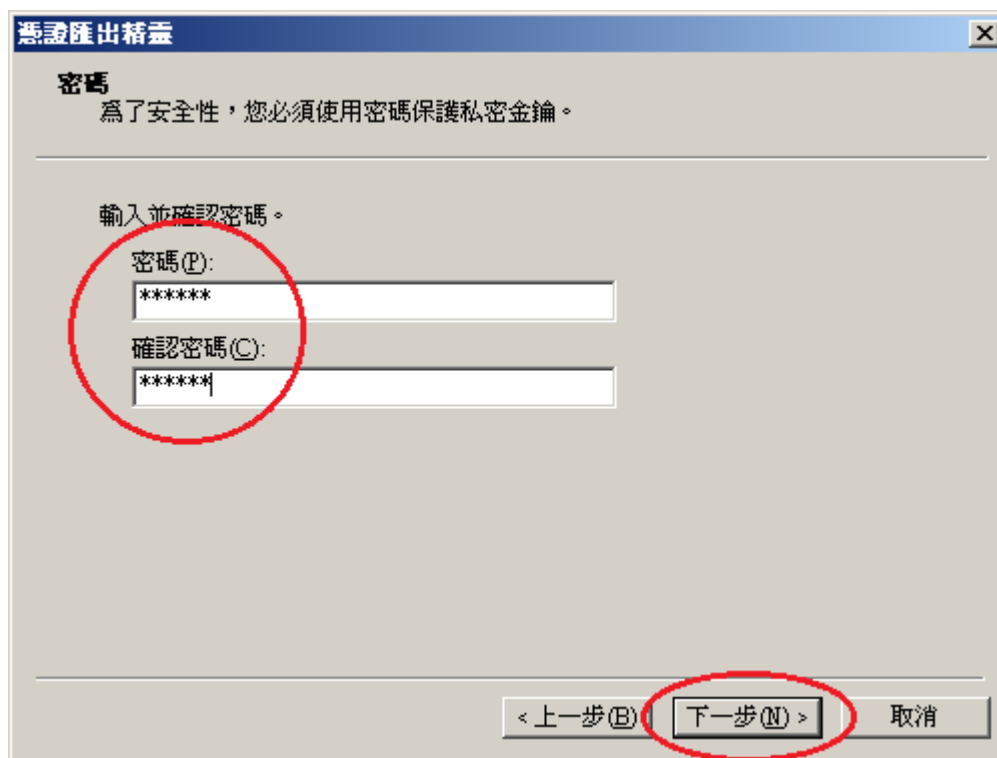
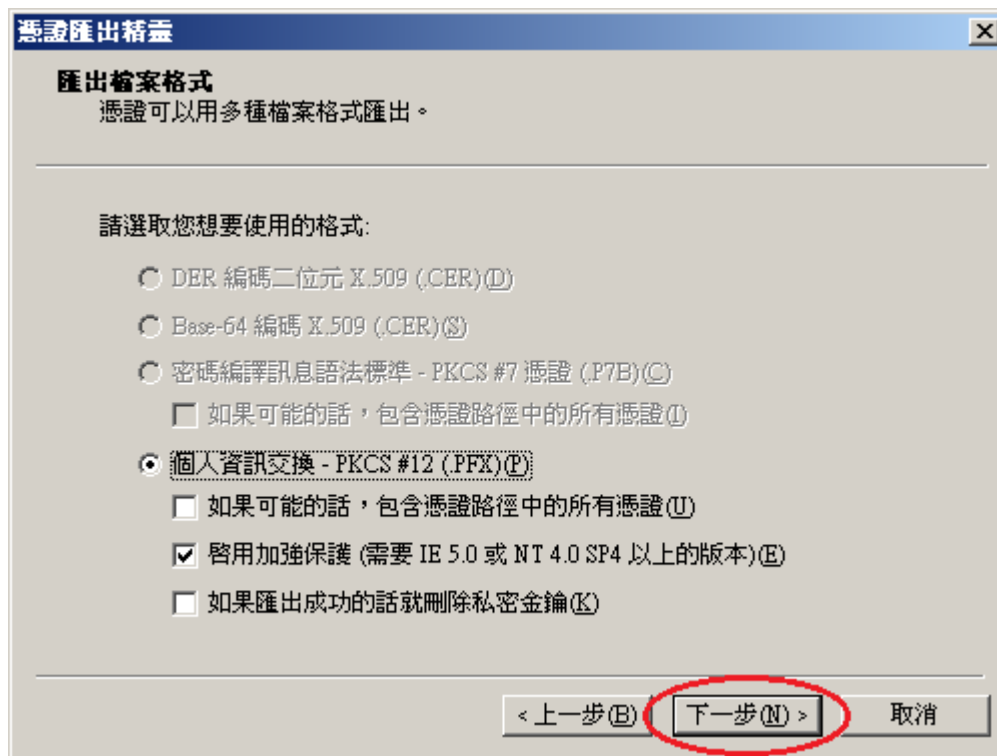
- 五、從 IIS 管理員匯出 SHA1 憑證與私密金鑰。

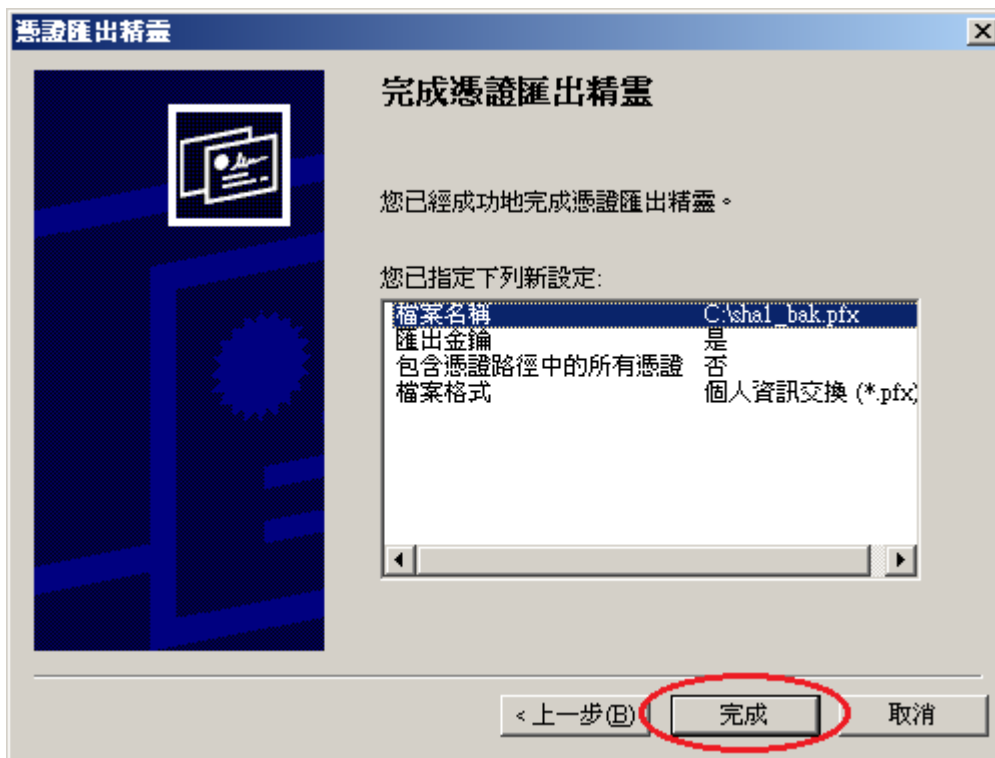
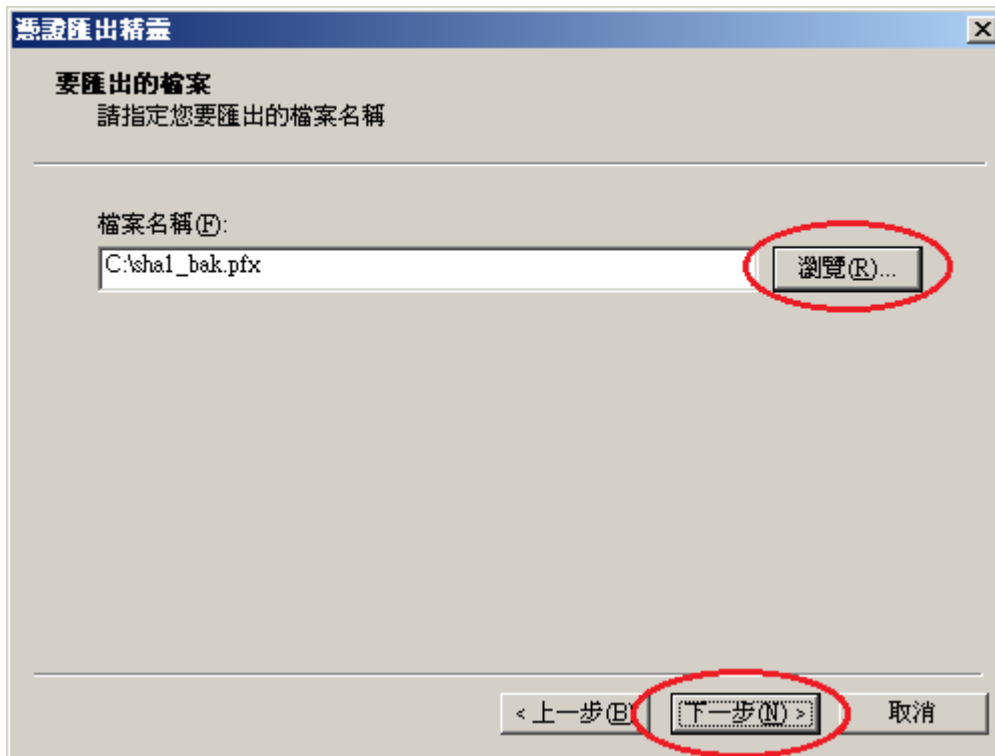
開啟 IIS 管理員，並對著安裝憑證的站台點選右鍵→內容





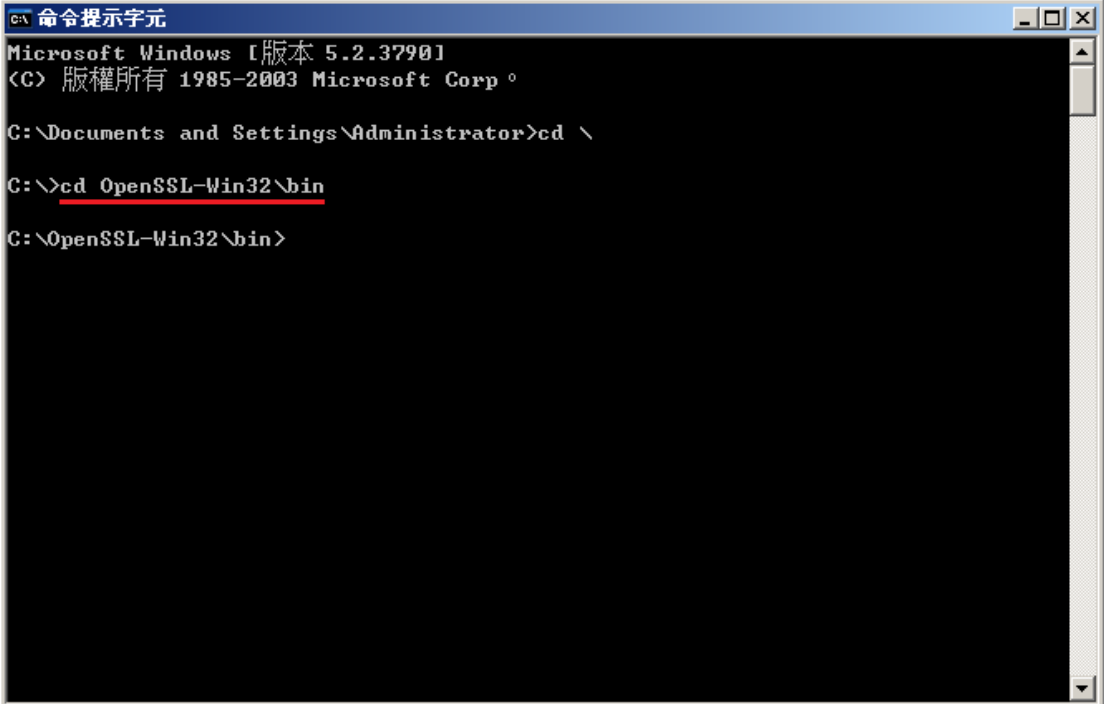






六、開啟「命令提示字元」，進入安裝 OpenSSL 目錄下的 bin 資料夾。

請依實際安裝路徑做調整



```
命令提示字元
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \

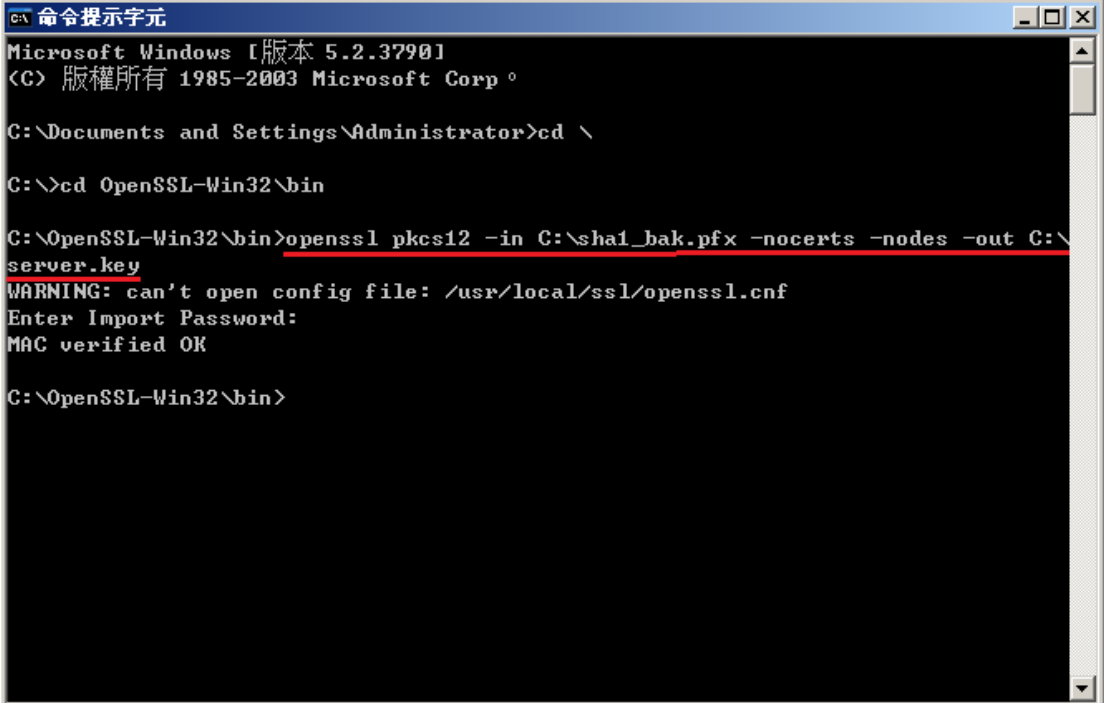
C:\>cd OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>
```

七、由 pfx 檔案分離出私密金鑰。

執行以下指令，並輸入從 IIS 匯出 pfx 時的密碼：

`openssl pkcs12 -in <pfx file path> -nocerts -nodes -out <save private key path>`



```
命令提示字元
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \

C:\>cd OpenSSL-Win32\bin

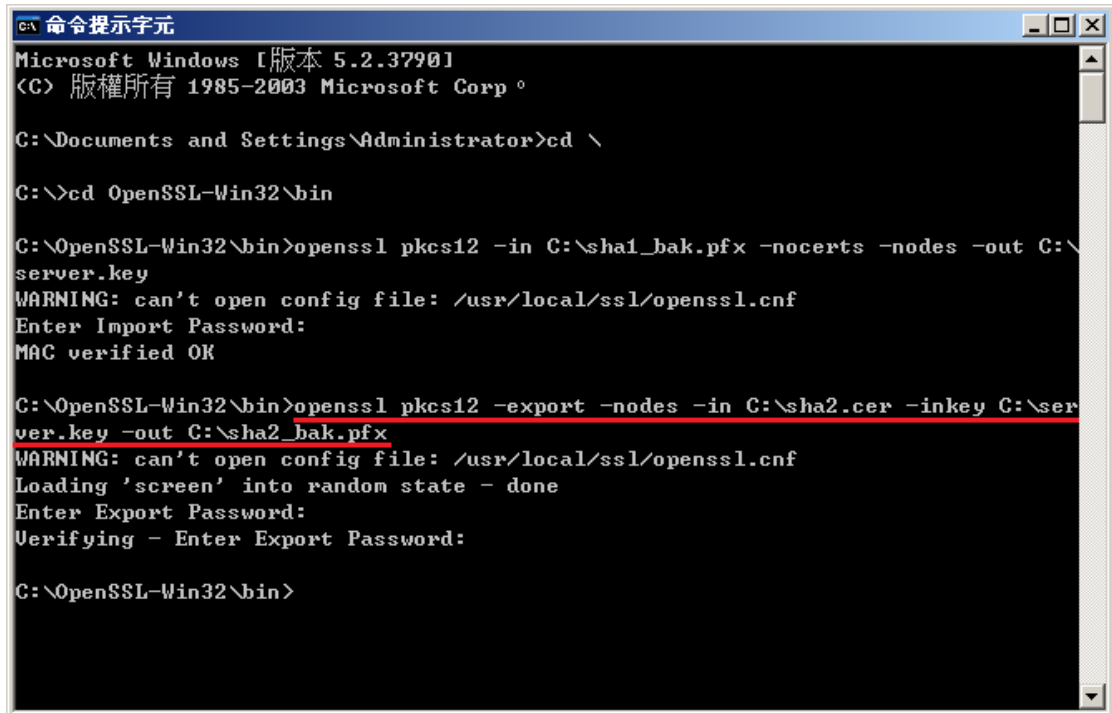
C:\OpenSSL-Win32\bin>openssl pkcs12 -in C:\sha1_bak.pfx -nocerts -nodes -out C:\server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Import Password:
MAC verified OK

C:\OpenSSL-Win32\bin>
```

八、將私密金鑰與 SHA256 憑證重新合併成 pfx 檔案

執行以下指令，並輸入兩次 pfx 檔案匯出密碼：

openssl pkcs12 -export -nodes -in <sha256 certificate path> -inkey <private key path> -out <save pfx path>



```
命令提示字元
Microsoft Windows [版本 5.2.3790]
(C) 版權所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \

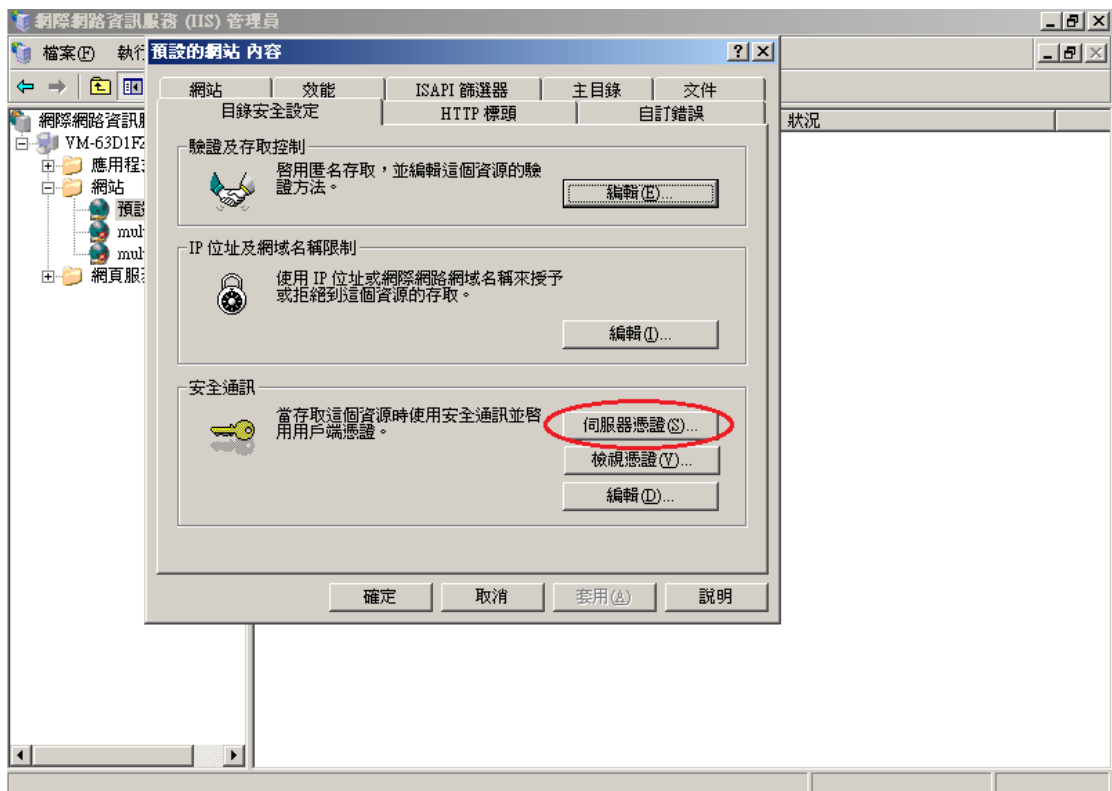
C:\>cd OpenSSL-Win32\bin

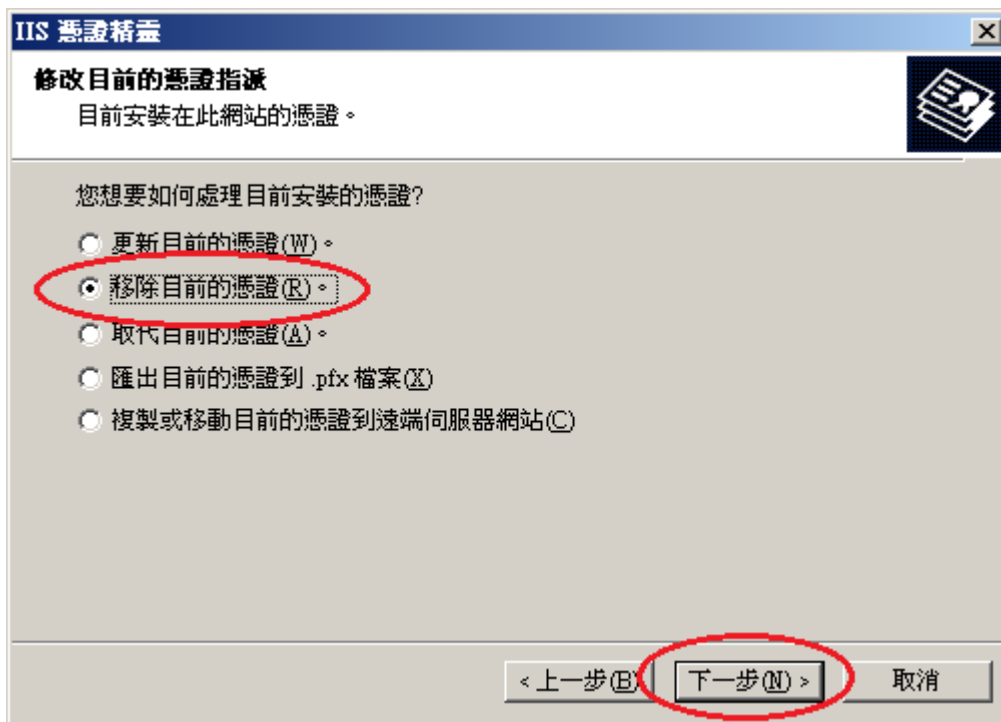
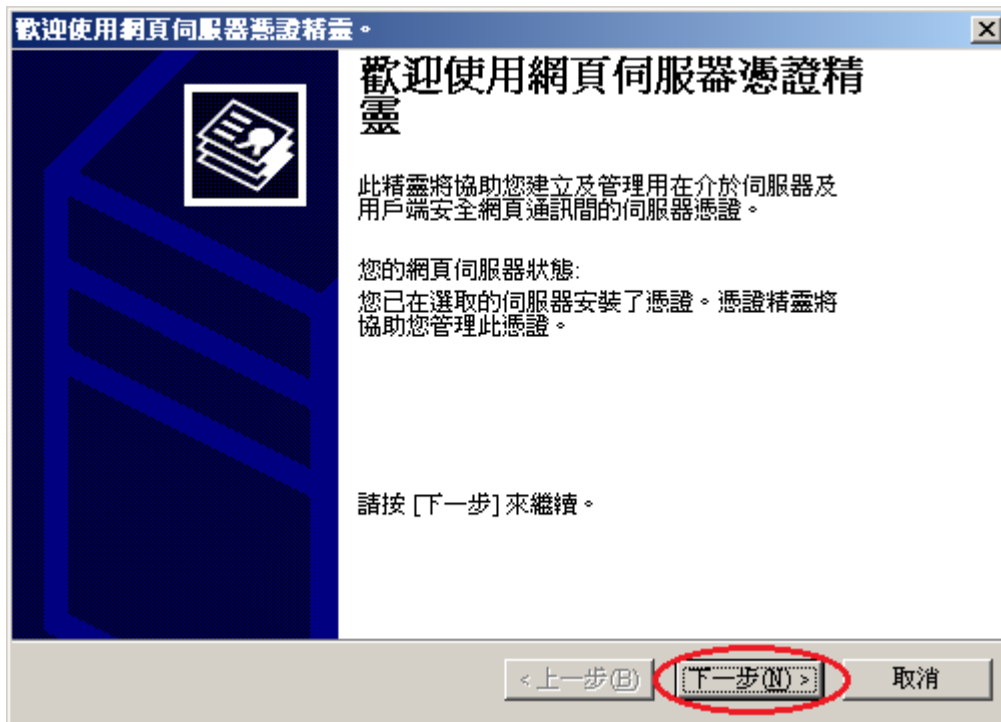
C:\OpenSSL-Win32\bin>openssl pkcs12 -in C:\sha1_bak.pfx -nocerts -nodes -out C:\server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Import Password:
MAC verified OK

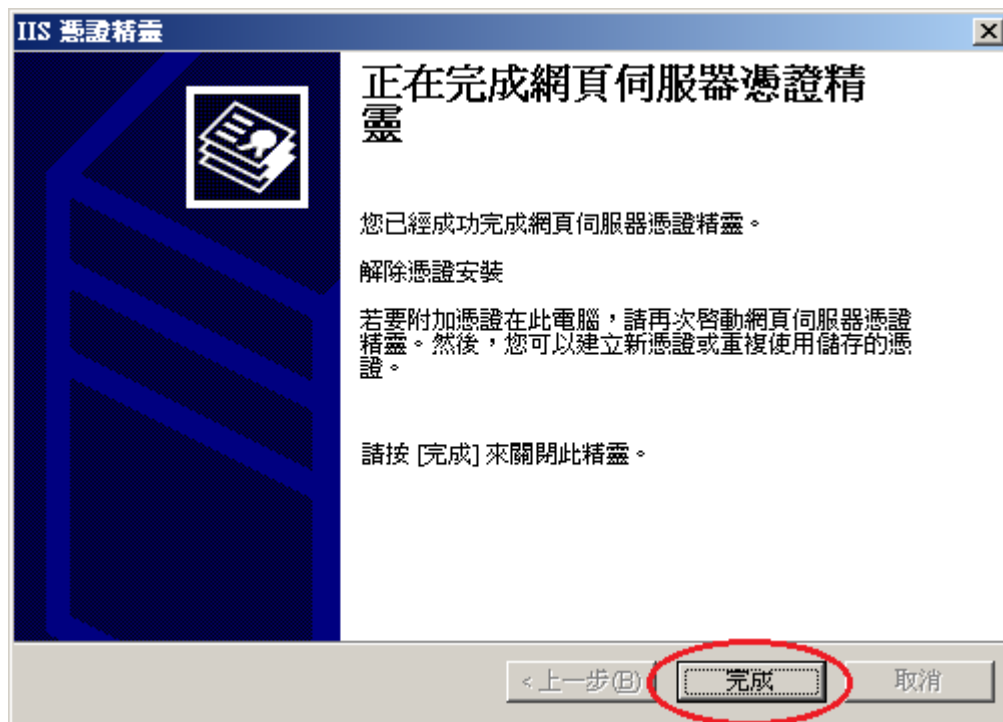
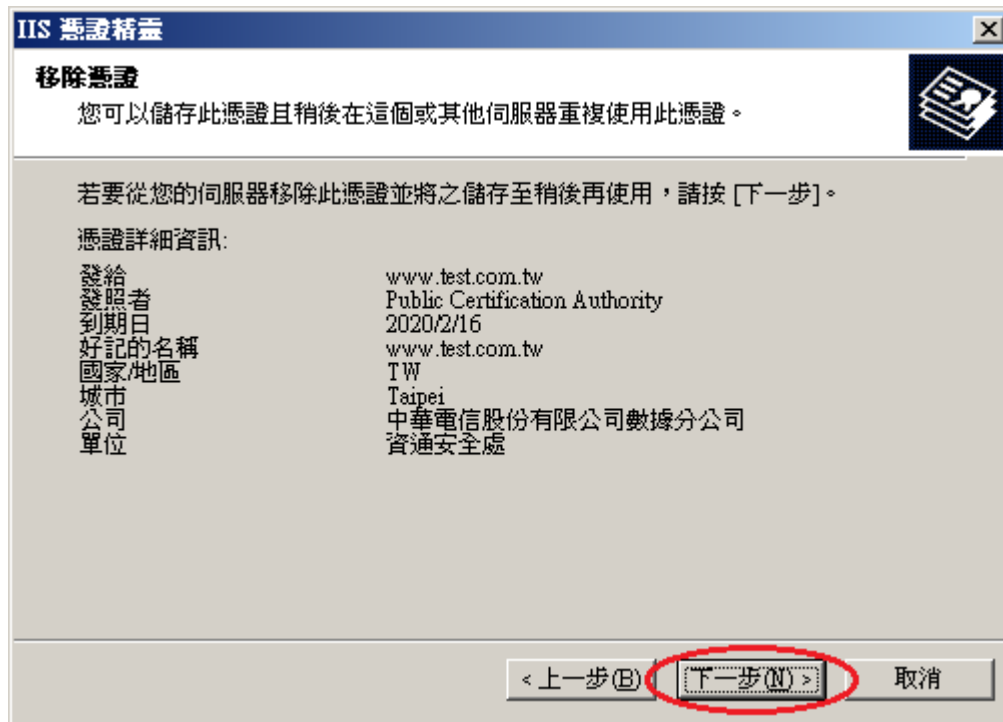
C:\OpenSSL-Win32\bin>openssl pkcs12 -export -nodes -in C:\sha2.cer -inkey C:\server.key -out C:\sha2_bak.pfx
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win32\bin>
```

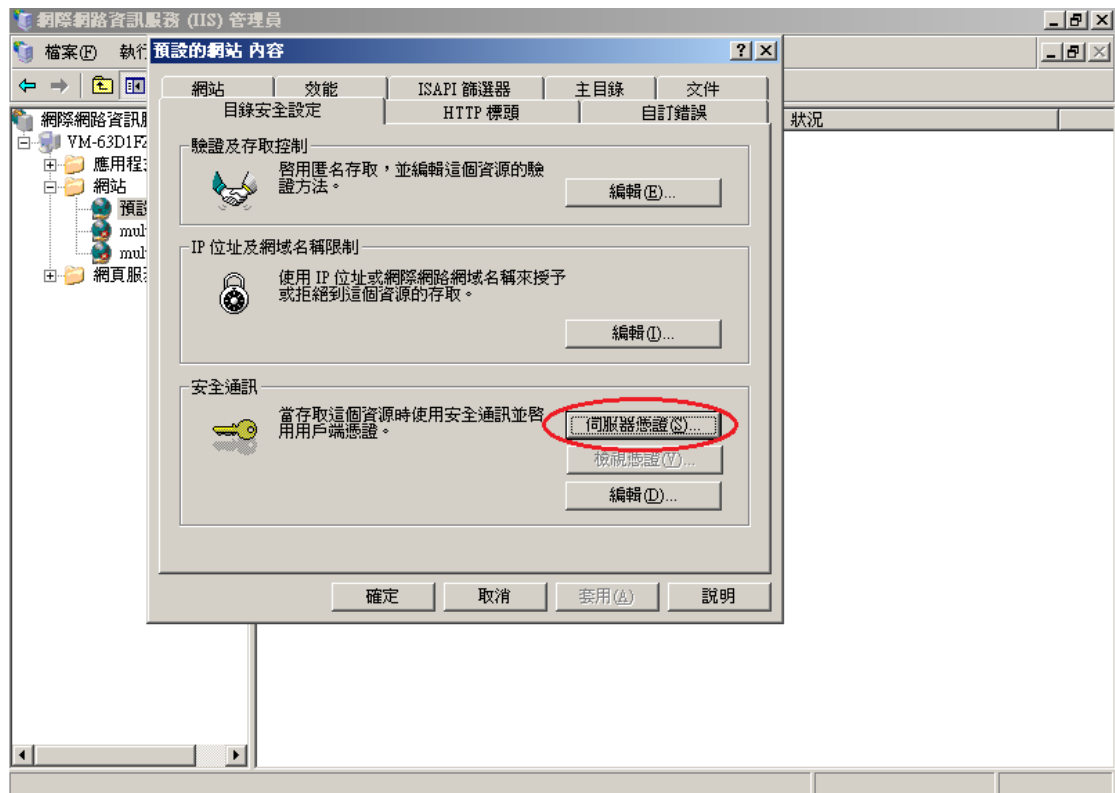
九、移除 SHA1 憑證，並匯入 SHA256 憑證。
回到 IIS 管理員，並點選「伺服器憑證」

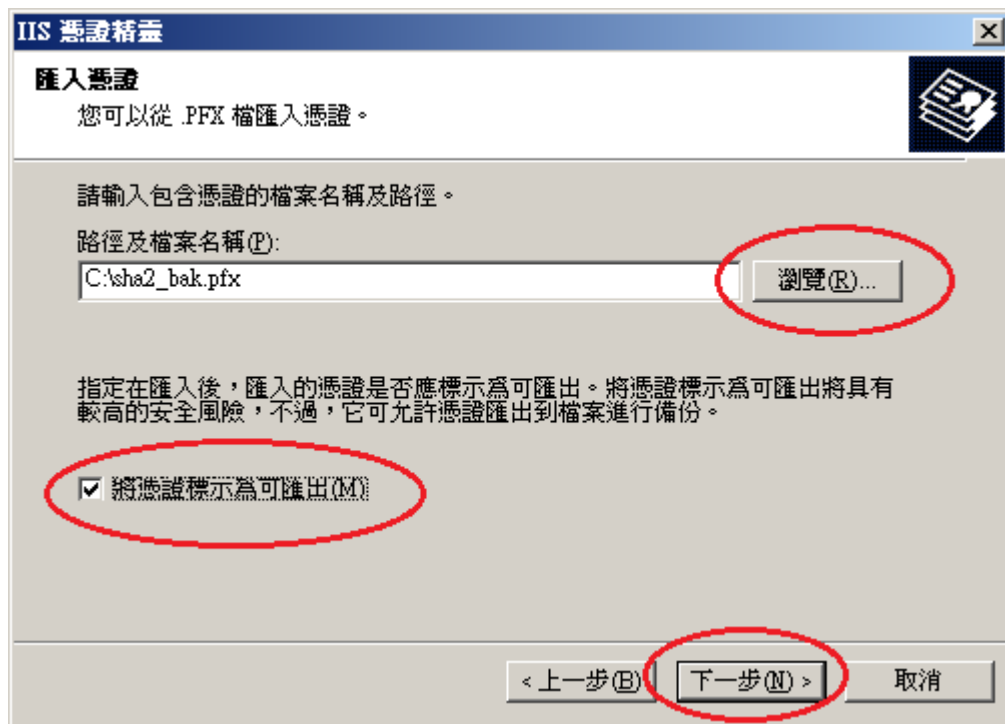
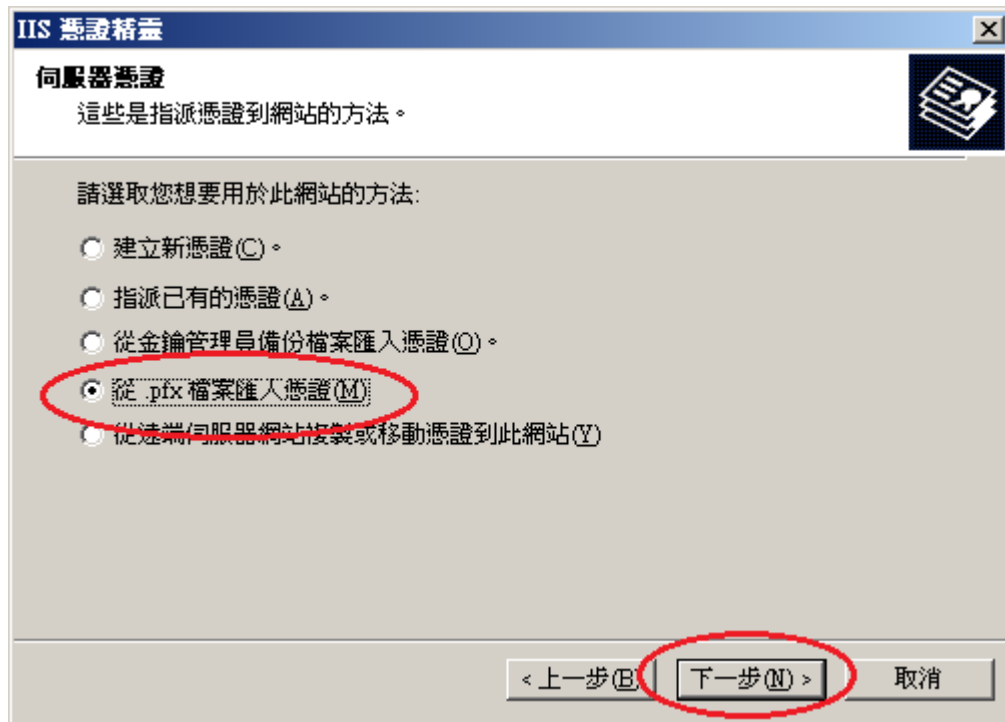






十、匯入 SHA256 憑證





IIS 憑證精靈 [X]

匯入憑證密碼
您必須提供密碼以匯入憑證。

請為您想要匯入的憑證輸入密碼。

密碼 (P):

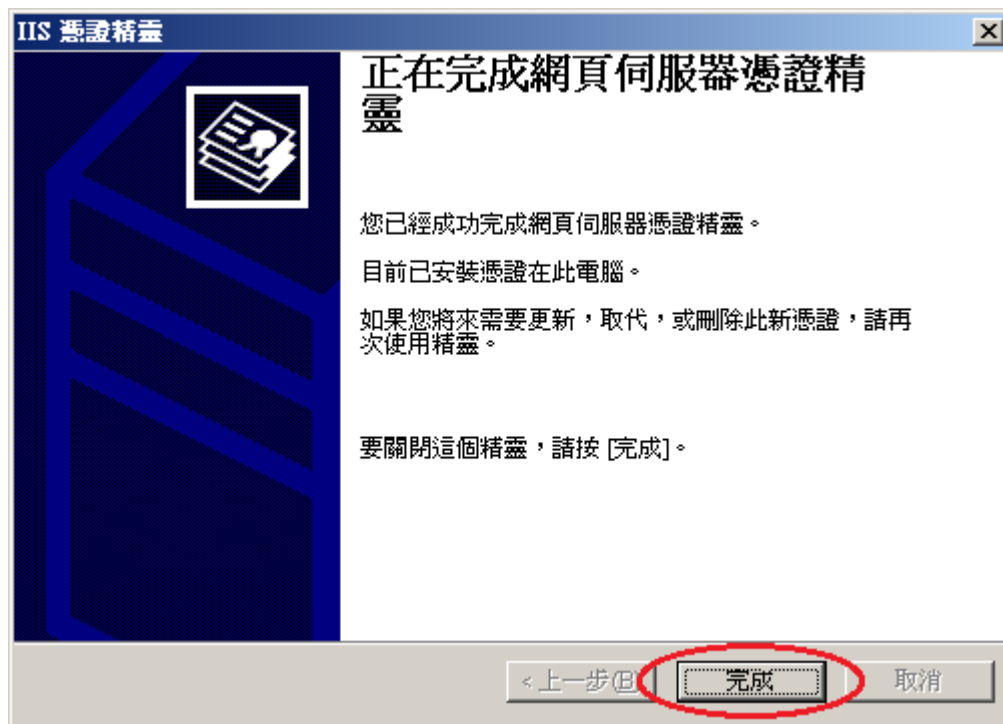
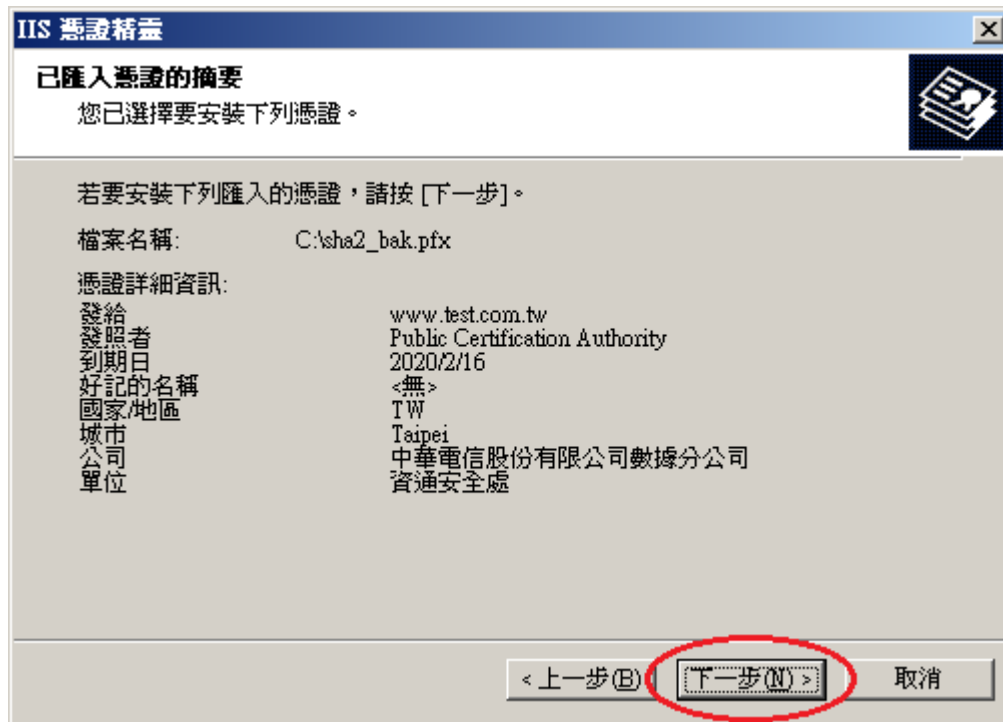
< 上一步 (B) **下一步 (N) >** 取消

IIS 憑證精靈 [X]

SSL 連接埠
為這個網站指定 SSL 連接埠。

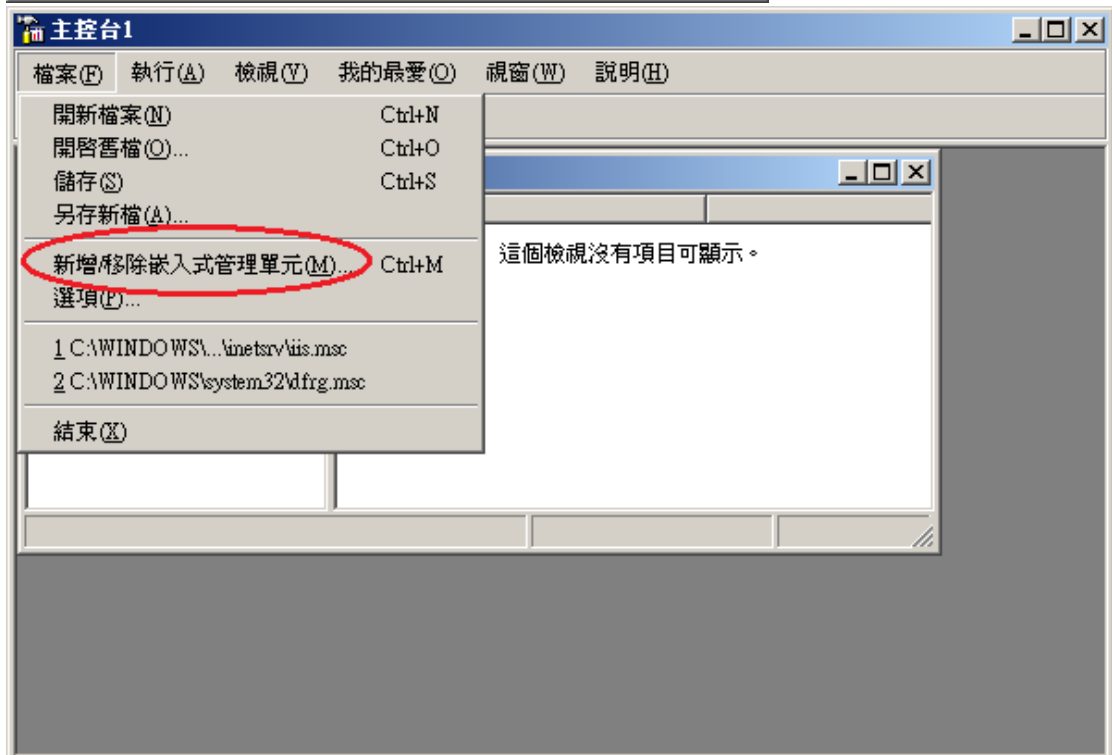
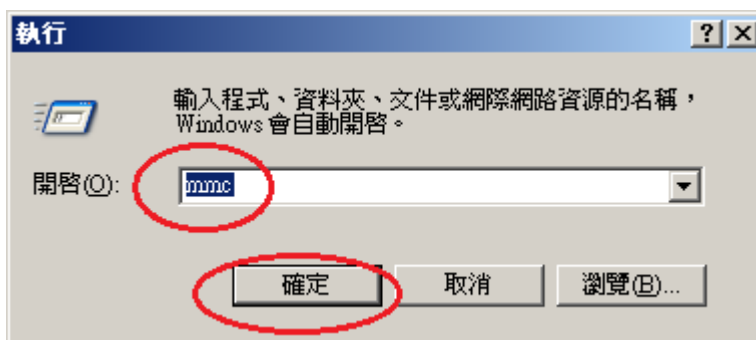
這個網站應該使用的 SSL 連接埠 (L):
443

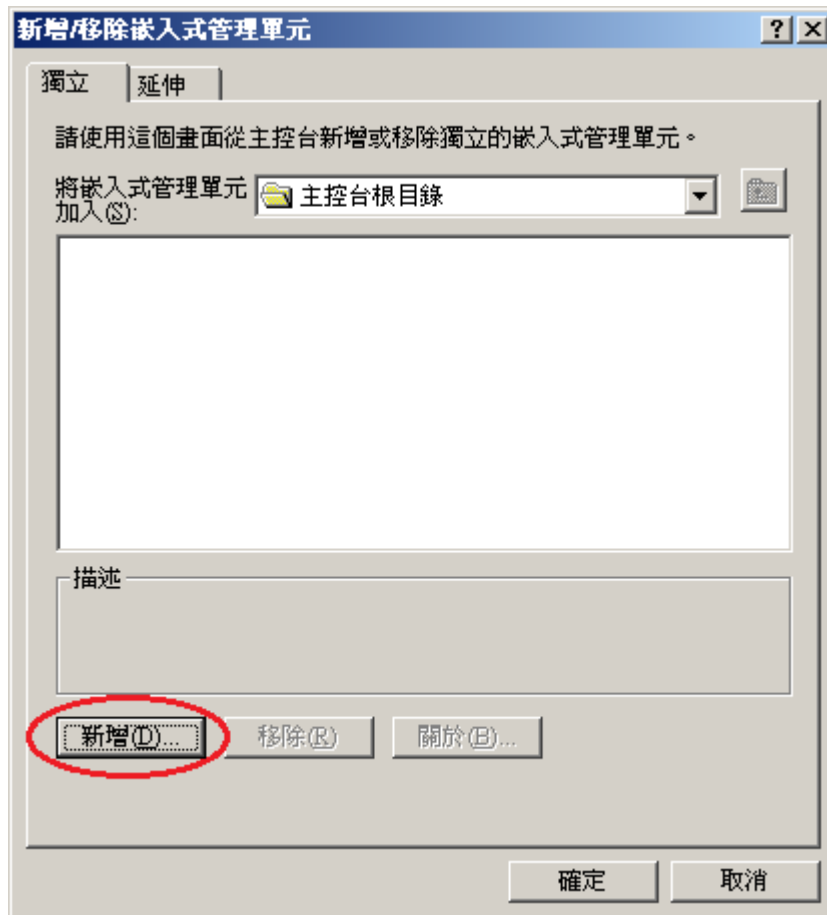
< 上一步 (B) **下一步 (N) >** 取消

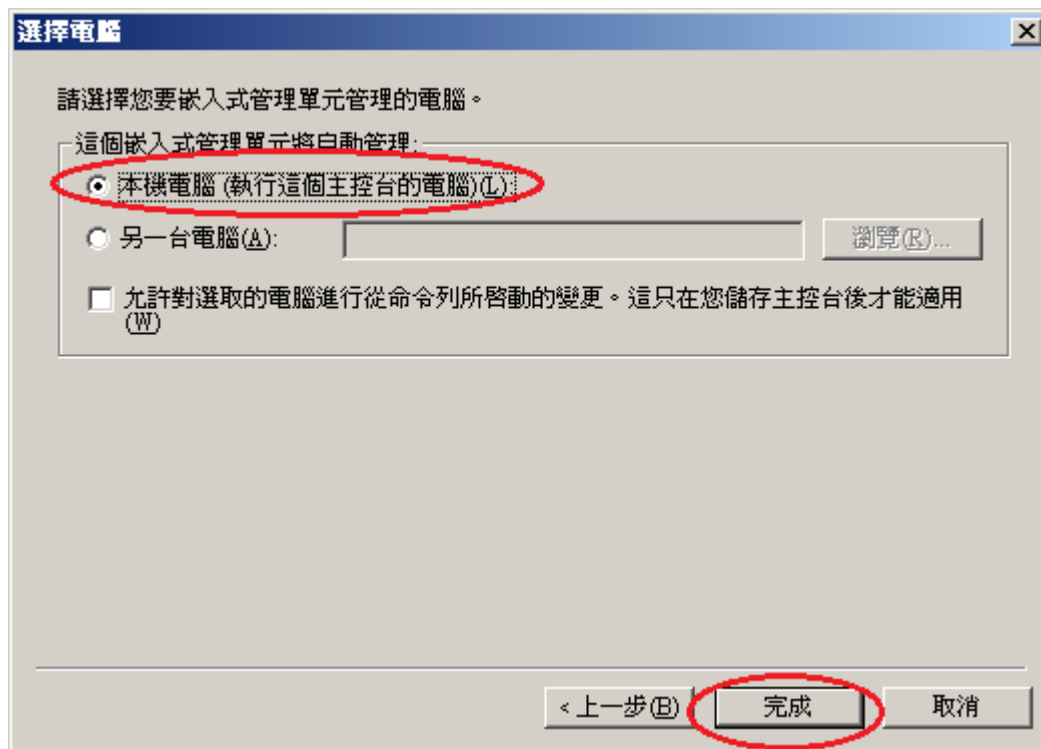
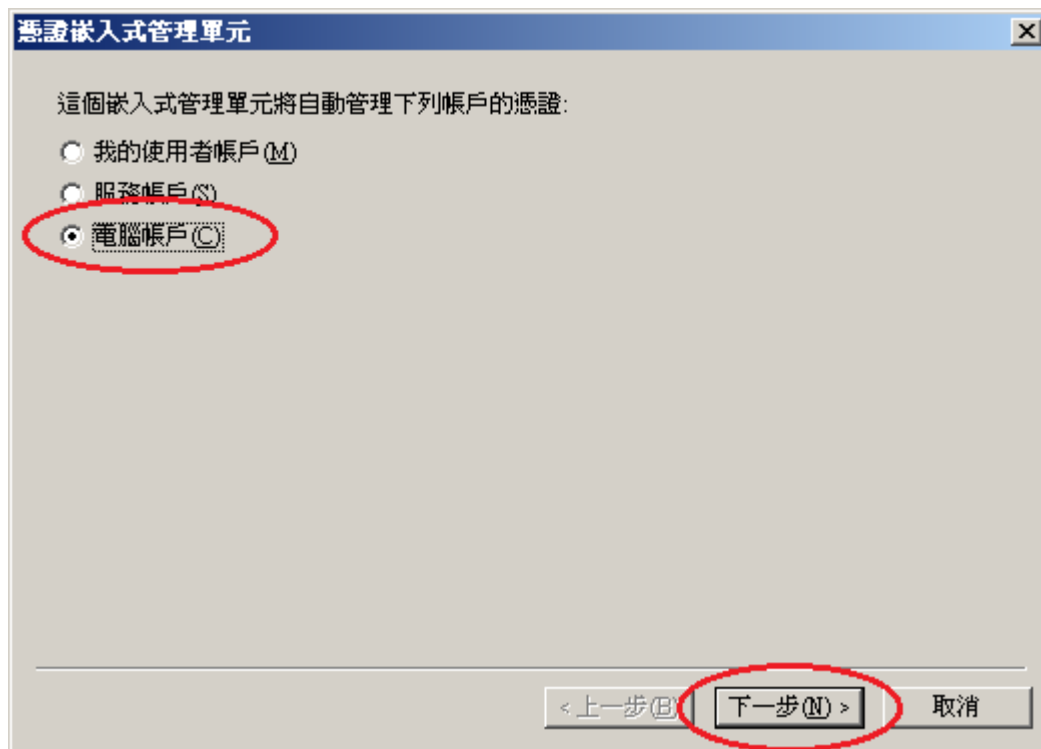


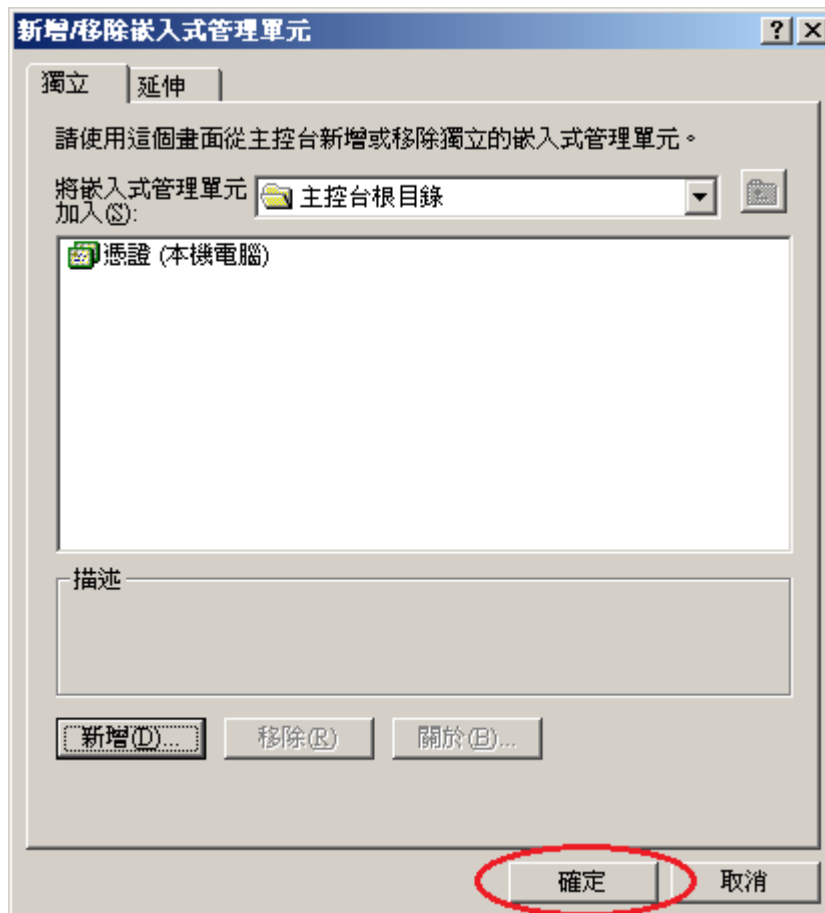
十一、 匯入 PublicCA G2 憑證(若曾經匯入過，可以略過此步驟)。

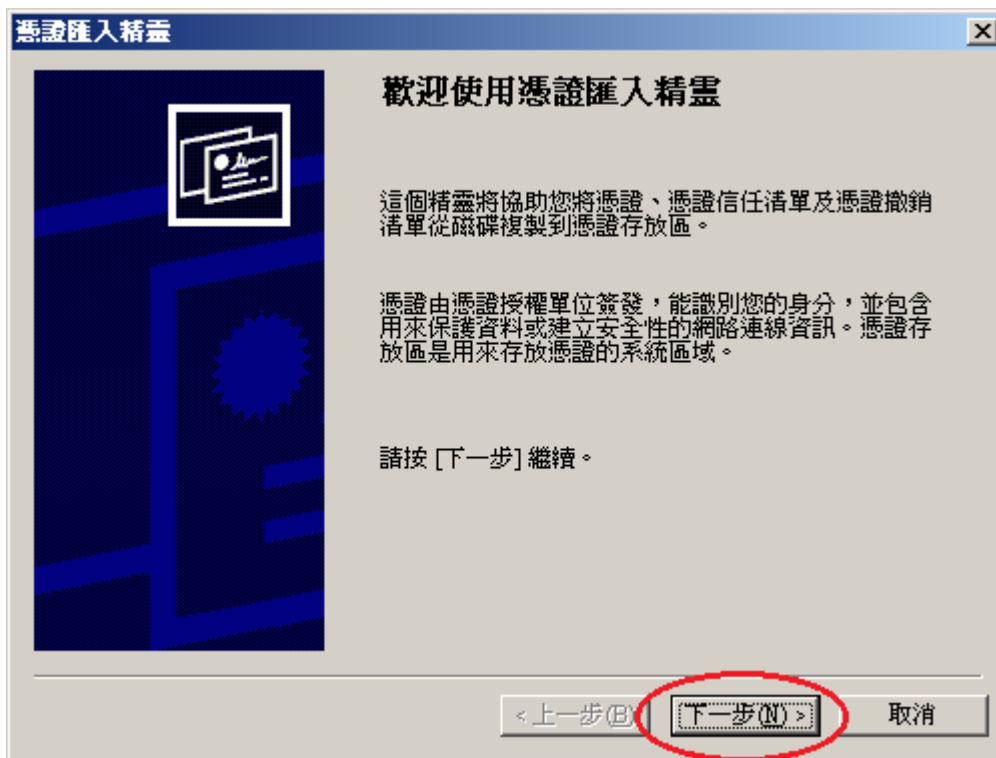
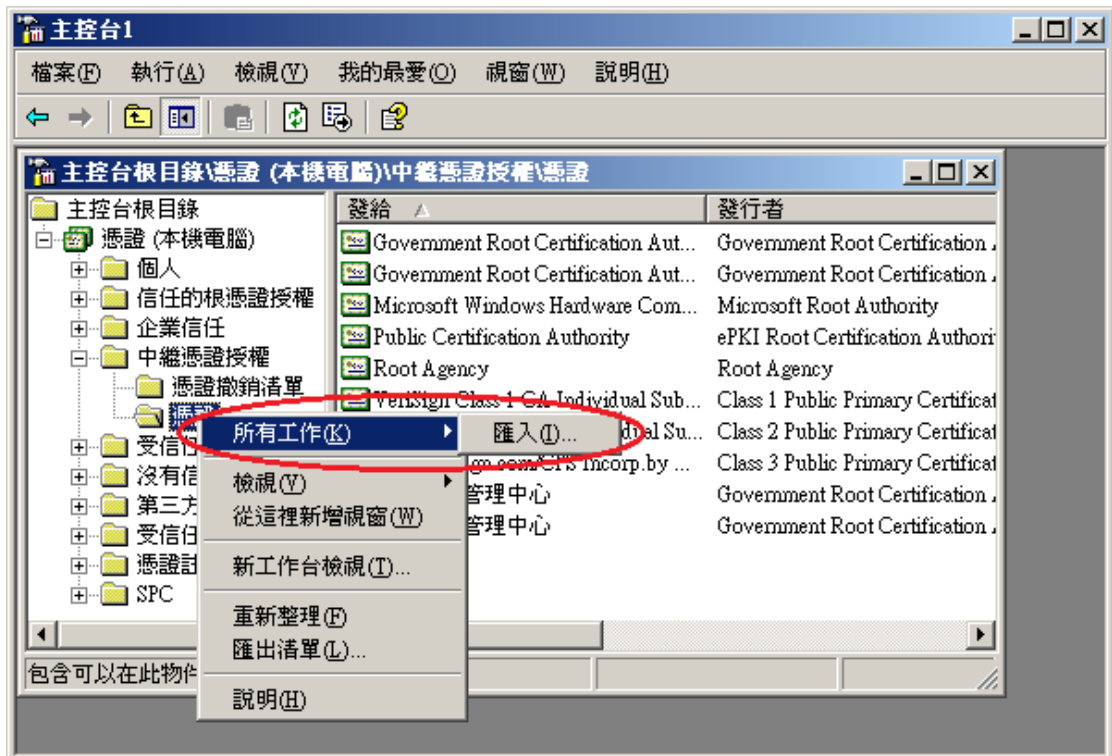
PublicCA G2 憑證：http://publicca.hinet.net/CHTM/download/PublicCA2_64.crt

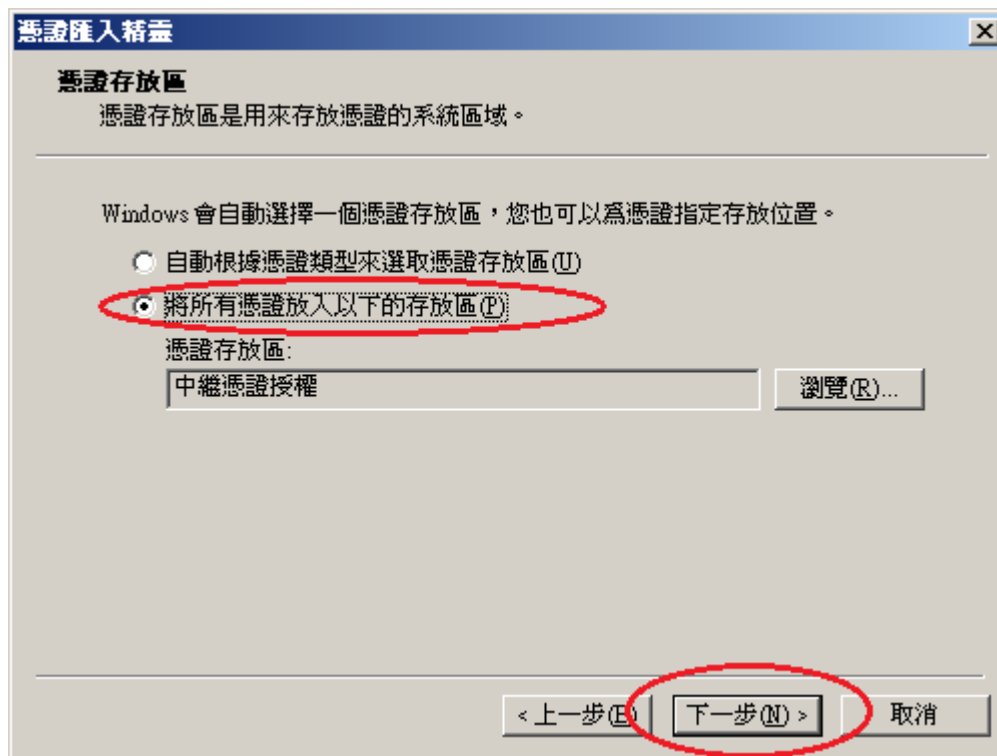
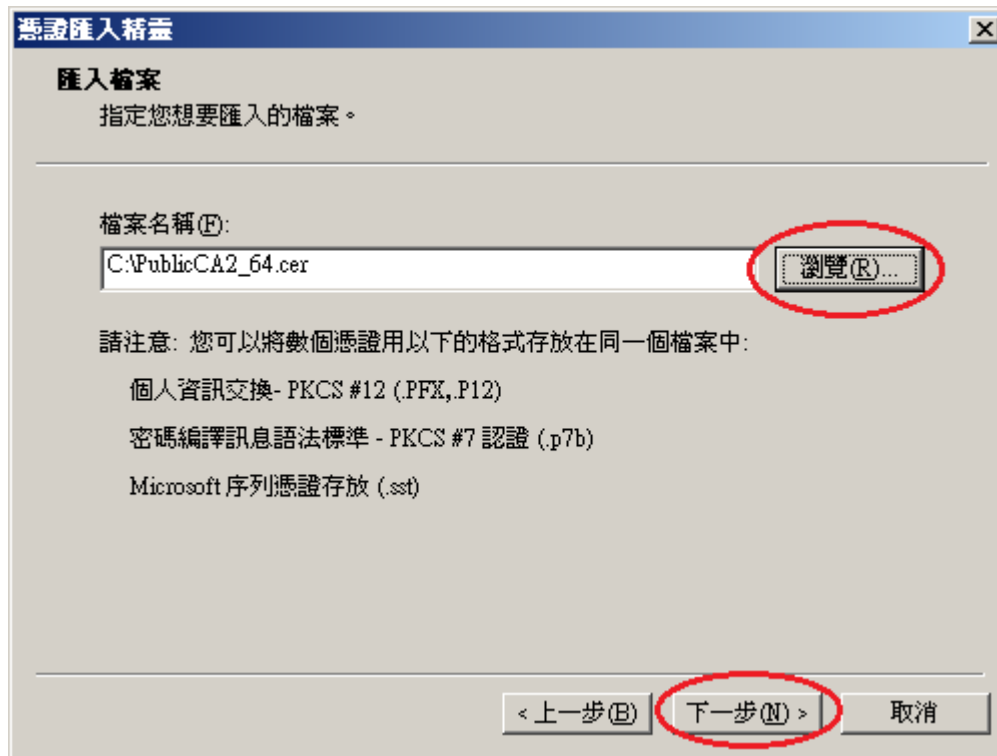


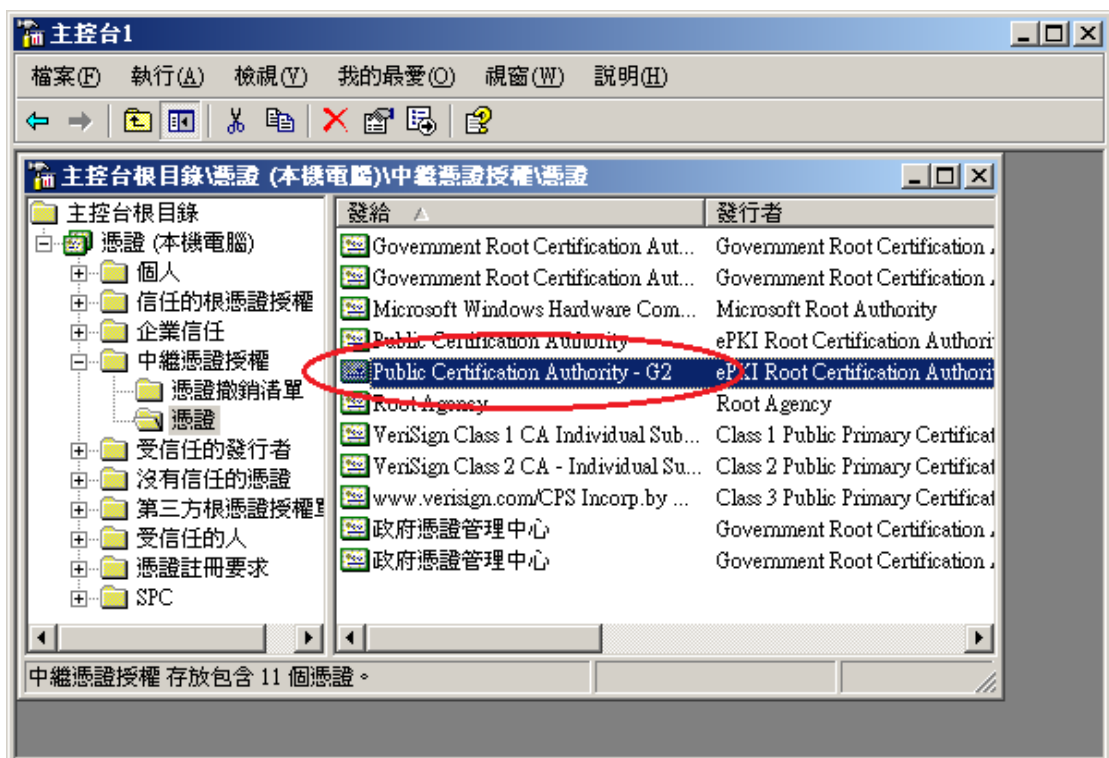
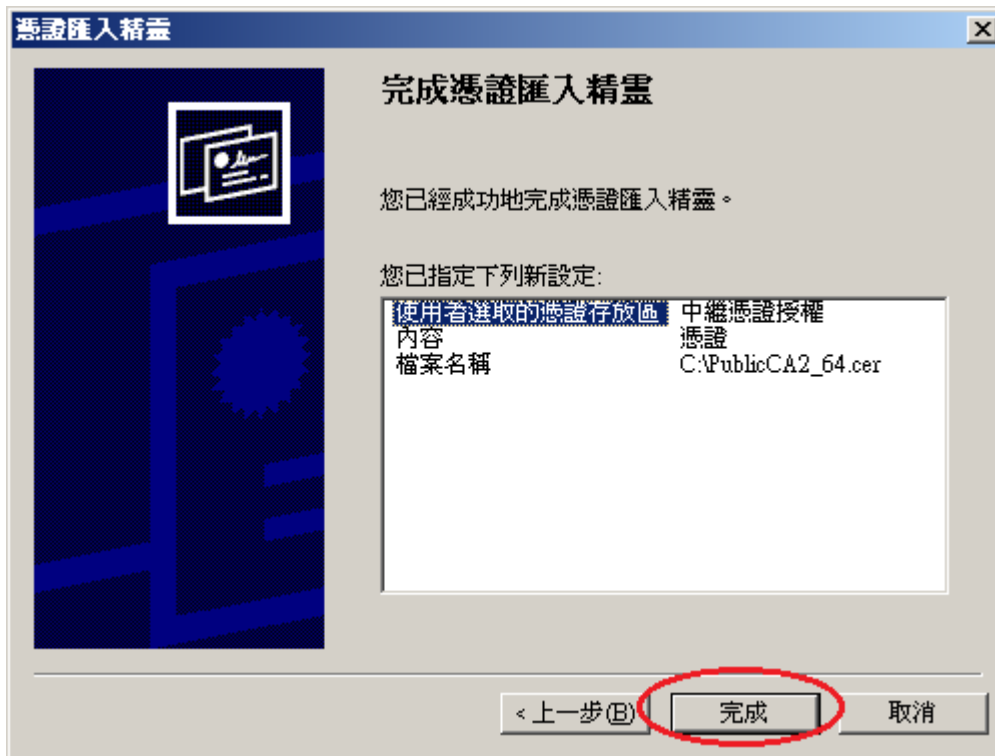




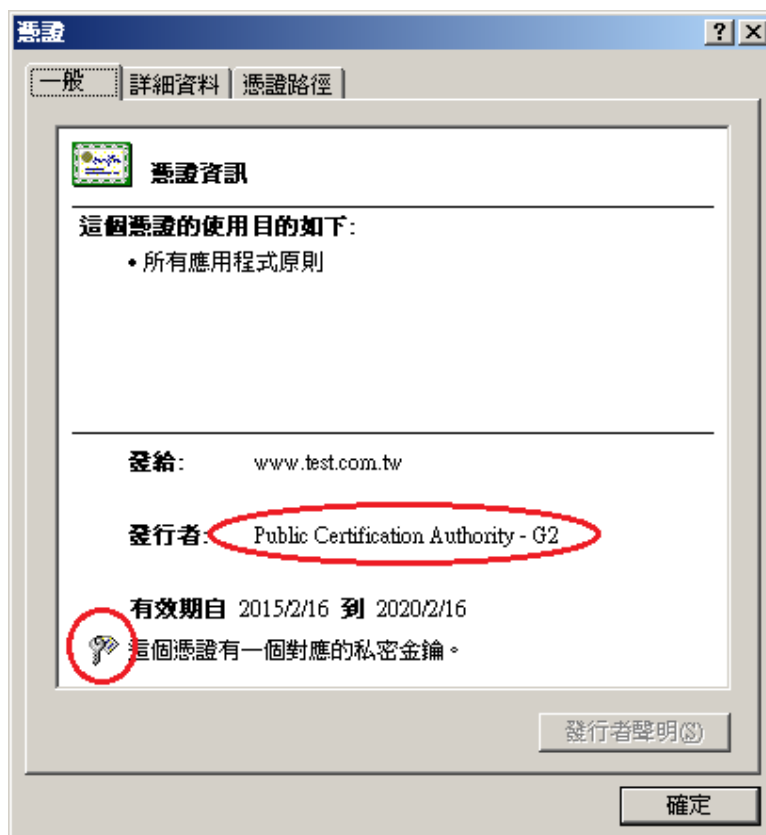
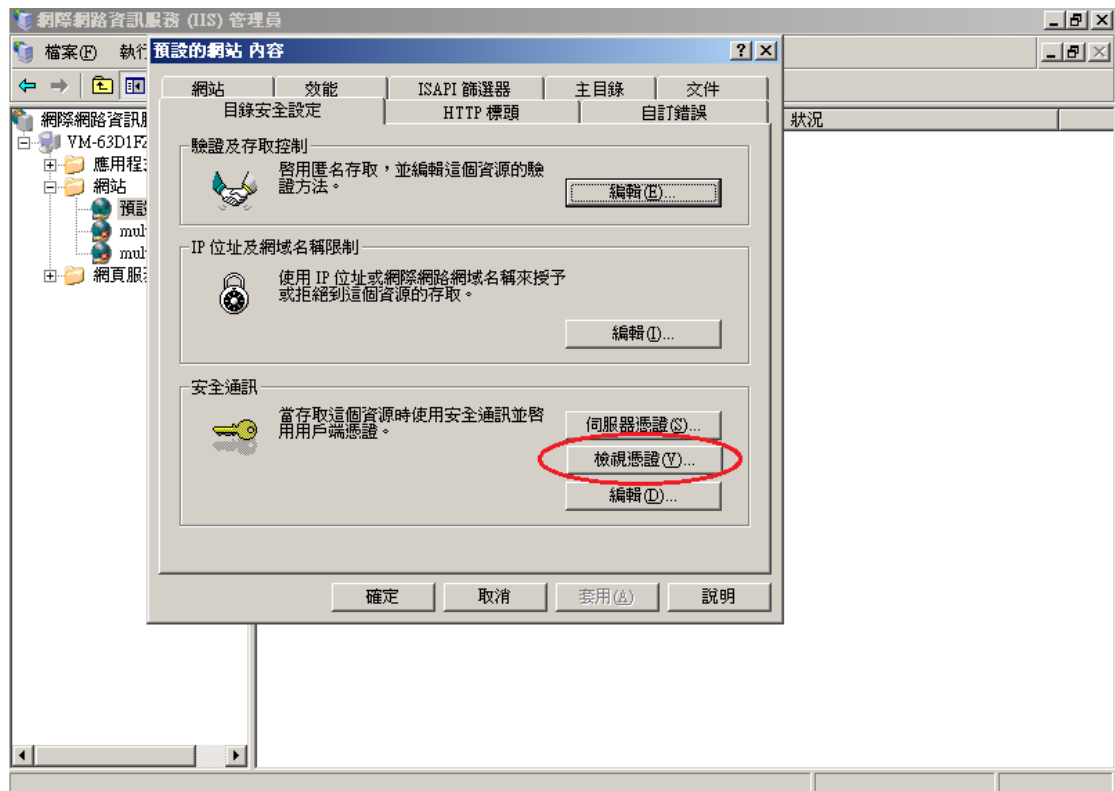








- 十二、 檢視 SHA256 憑證，並以瀏覽器檢視網頁是否正常運作。
回到 IIS 管理員，並點選「檢視憑證」



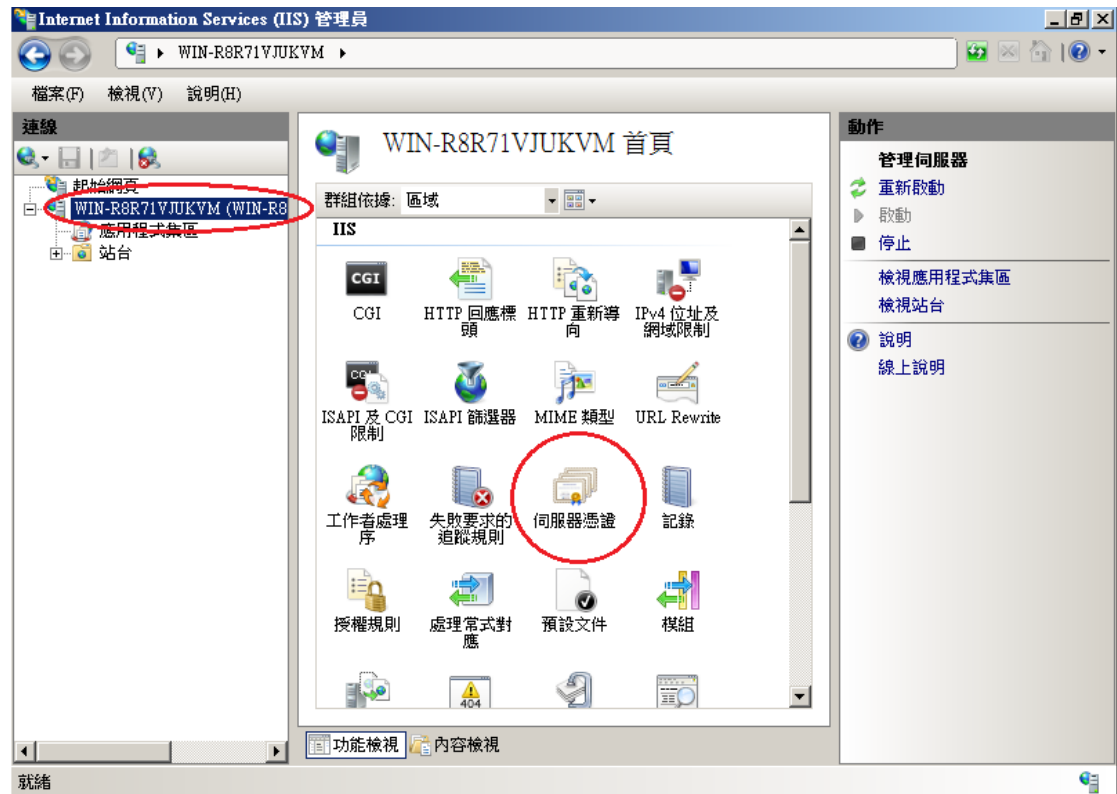
Windows Server 2008 IIS 7

- 一、適用於申請時，有同時取得 SHA1、SHA256 憑證。或是憑證在效期內，經由審驗人員再次核發 SHA256 憑證者。
- 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、需要先備妥 OpenSSL 軟體，或是找尋已安裝 OpenSSL 軟體的主機，後續將會使用到。

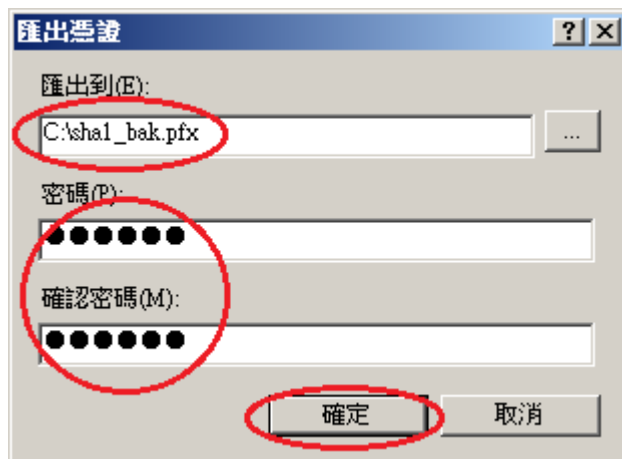
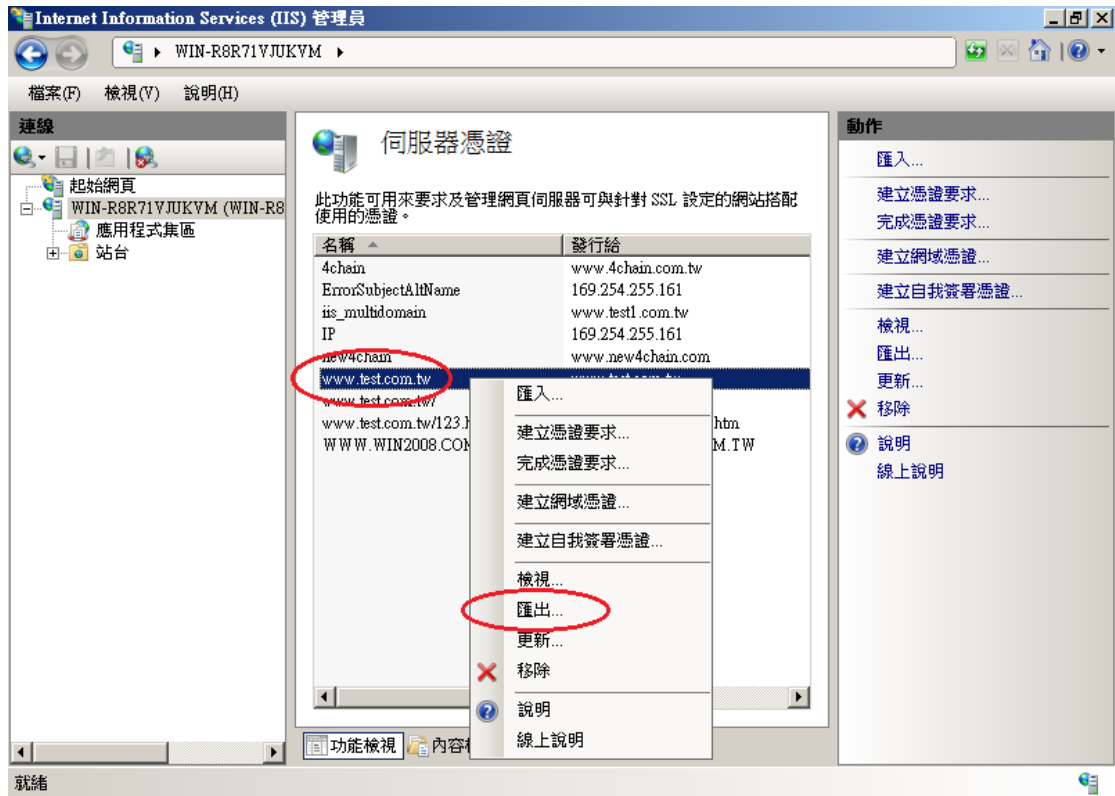
Windows 版 OpenSSL 軟體連結，可以只安裝「light」的版本即可：

<https://www.openssl.org/related/binaries.html>

- 四、從 IIS 管理員匯出 SHA1 憑證與私密金鑰。
開啟 IIS 管理員，點選「伺服器憑證」



於要匯出的憑證右鍵→匯出



五、開啟「命令提示字元」，進入安裝 OpenSSL 目錄下的 bin 資料夾。

請依實際安裝路徑做調整



```
CAV 系統管理員: 命令提示字元
Microsoft Windows [版本 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \

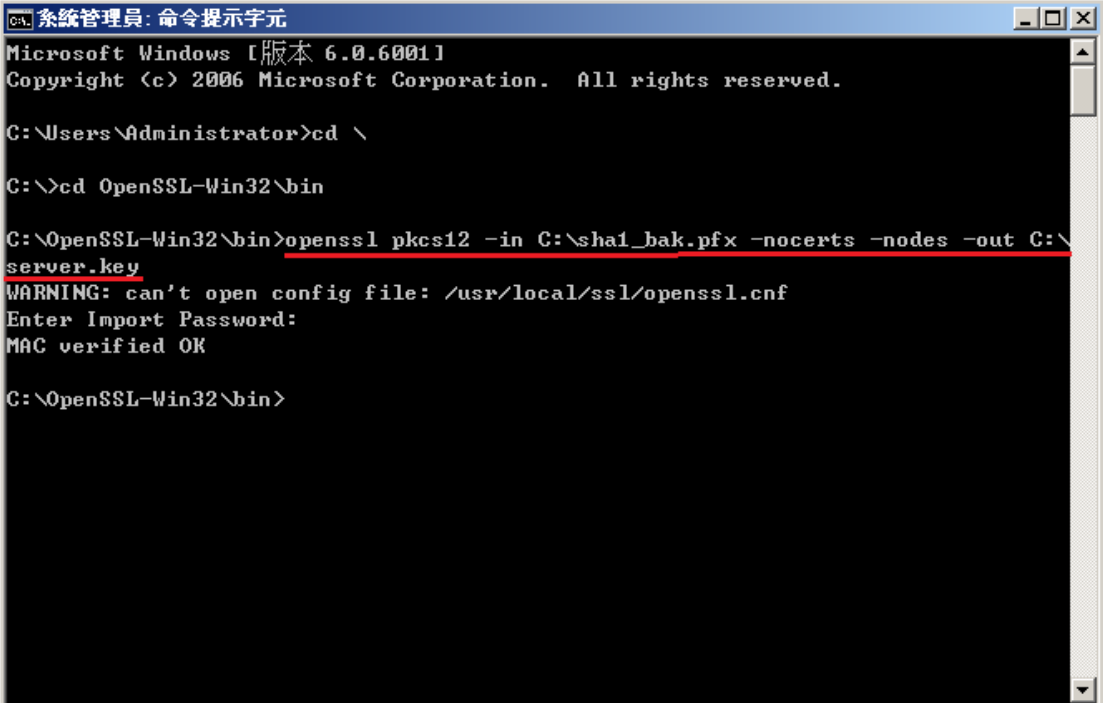
C:\>cd OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>
```

六、由 pfx 檔案分離出私密金鑰。

執行以下指令，並輸入從 IIS 匯出 pfx 時的密碼：

`openssl pkcs12 -in <pfx file path> -nocerts -nodes -out <save private key path>`



```
CAV 系統管理員: 命令提示字元
Microsoft Windows [版本 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \

C:\>cd OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>openssl pkcs12 -in C:\sha1_bak.pfx -nocerts -nodes -out C:\server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Import Password:
MAC verified OK

C:\OpenSSL-Win32\bin>
```

七、將私密金鑰與 SHA256 憑證重新合併成 pfx 檔案

執行以下指令，並輸入兩次 pfx 檔案匯出密碼：

openssl pkcs12 -export -nodes -in <sha256 certificate path> -inkey <private key path> -out <save pfx path> -name <alias name>



```
Microsoft Windows [版本 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \

C:\>cd OpenSSL-Win32\bin

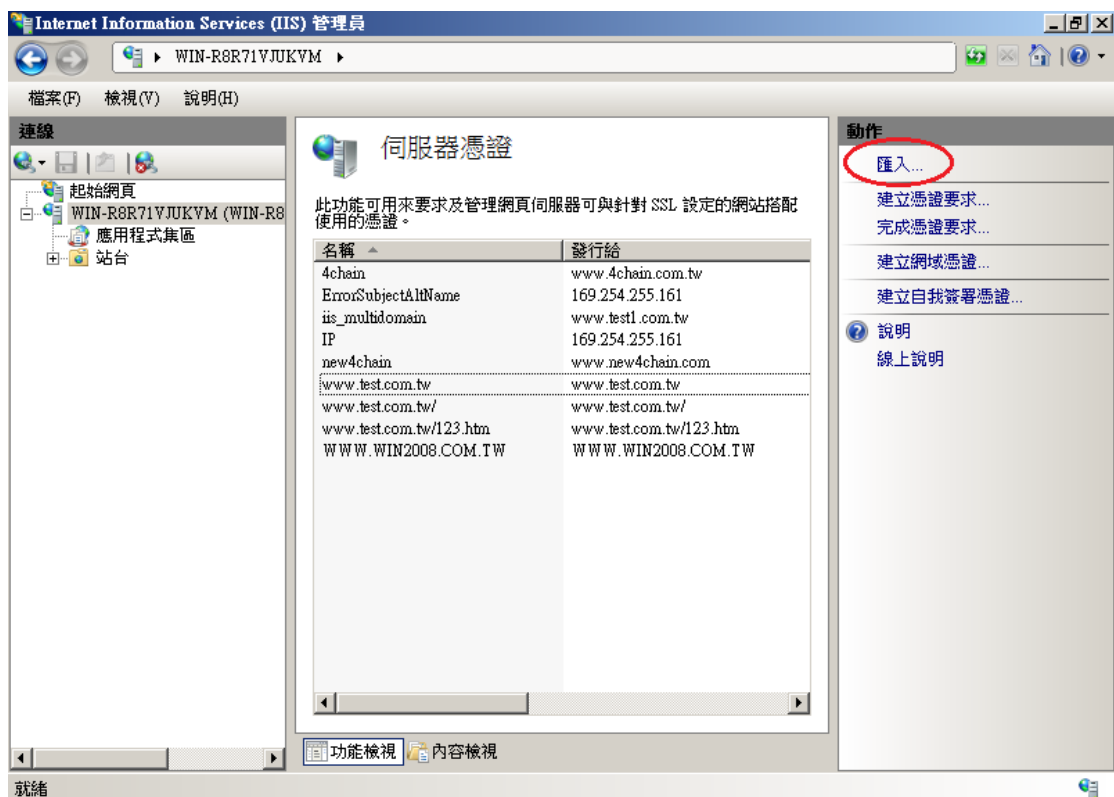
C:\OpenSSL-Win32\bin>openssl pkcs12 -in C:\sha1_bak.pfx -nocerts -nodes -out C:\server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Import Password:
MAC verified OK

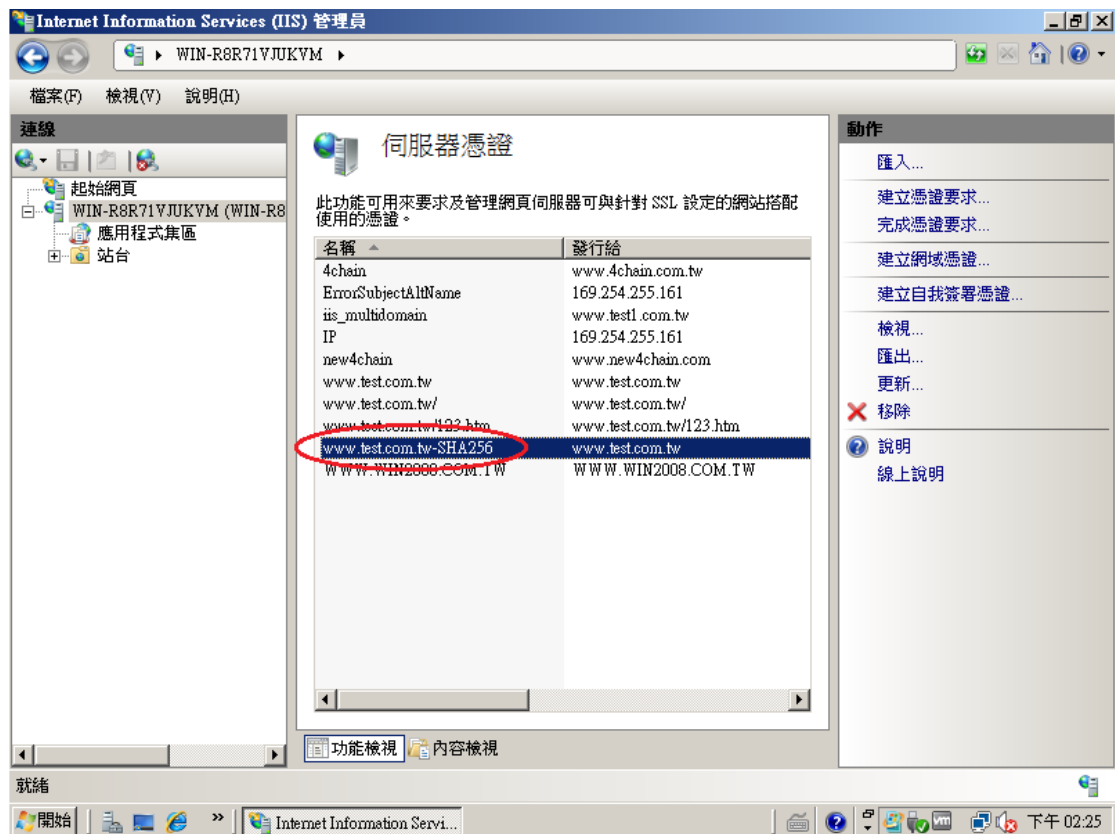
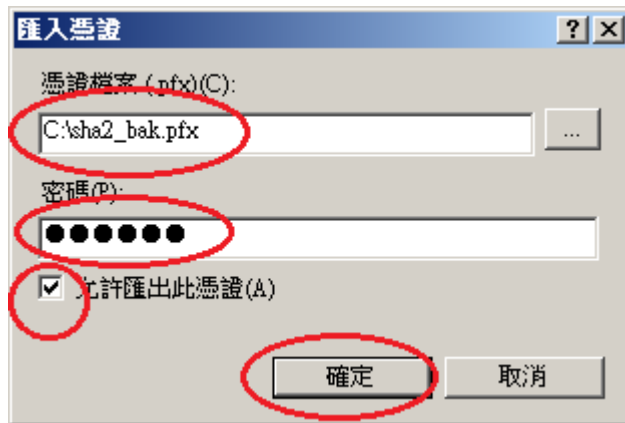
C:\OpenSSL-Win32\bin>openssl pkcs12 -export -nodes -in C:\sha2.cer -inkey C:\server.key -out C:\sha2_bak.pfx -name "www.test.com.tw-SHA256"
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win32\bin>
```

八、匯入 SHA256 憑證。

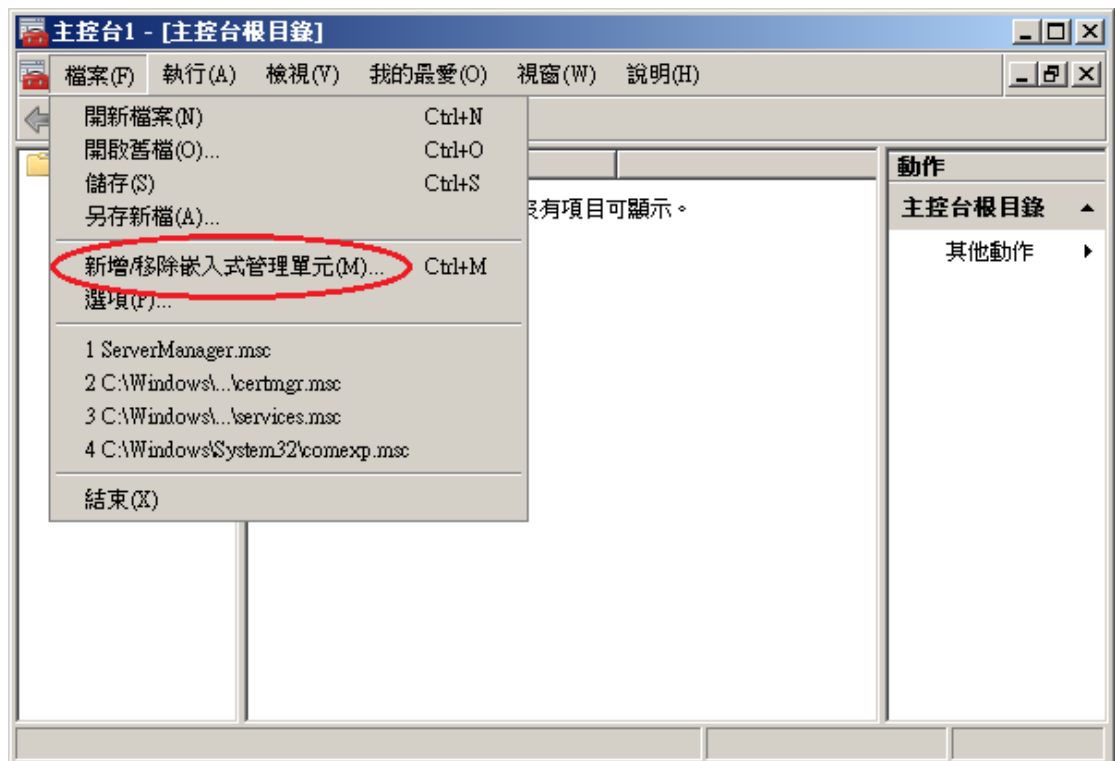
重新回到 IIS 管理員，並點選「匯入」

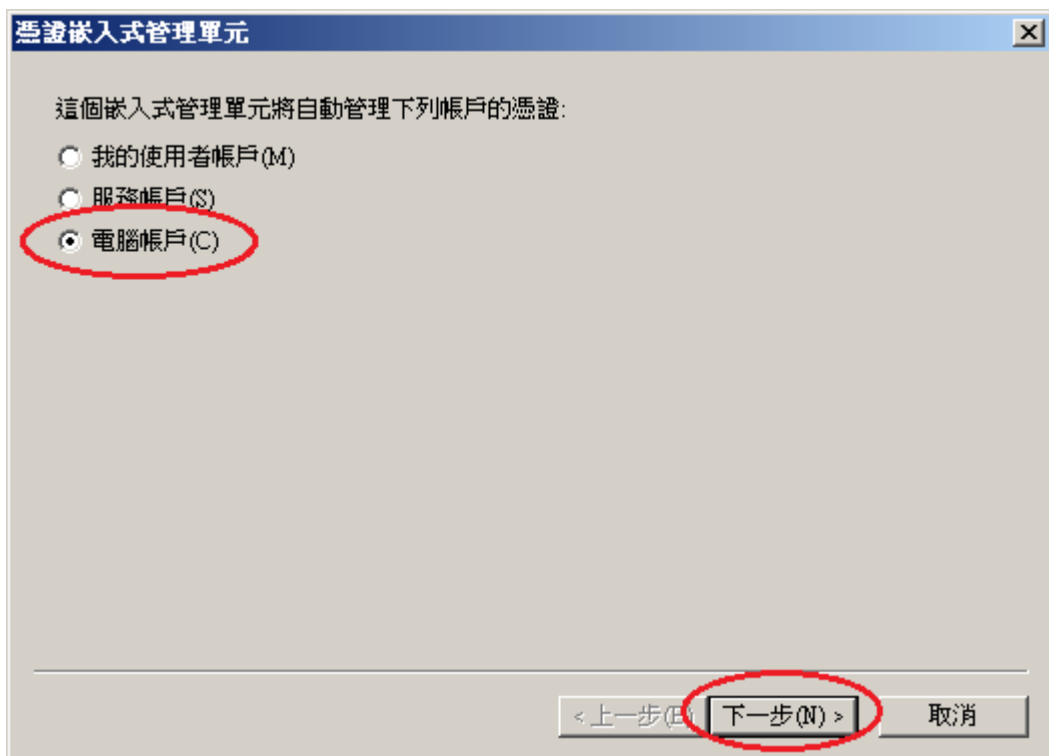
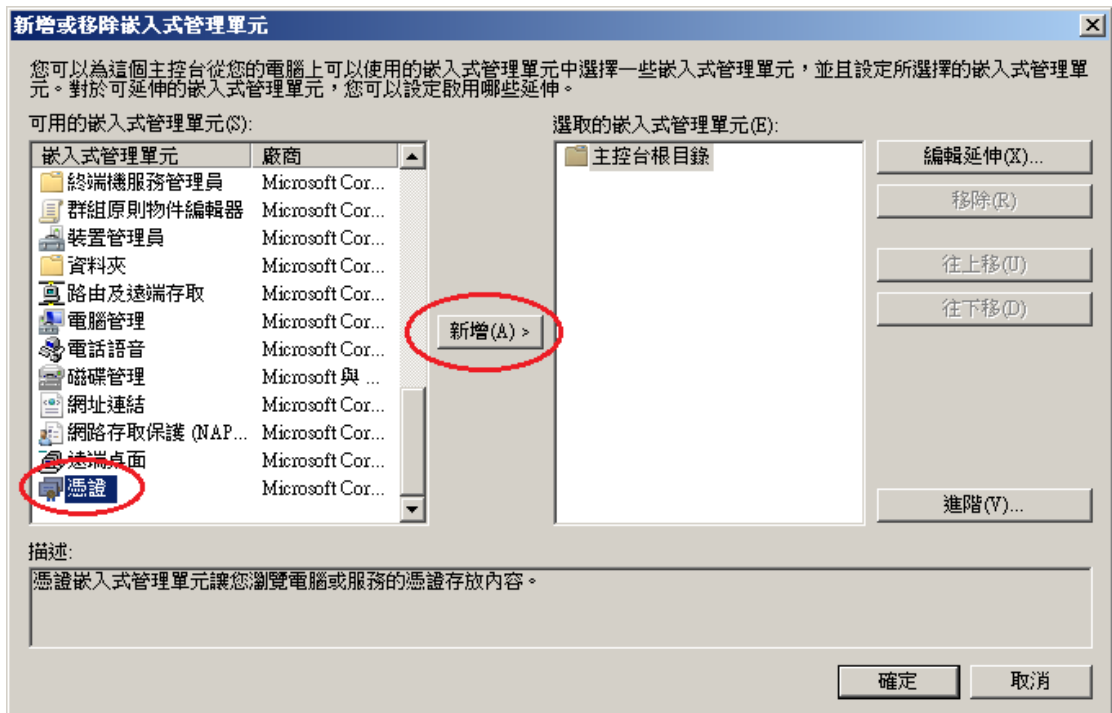


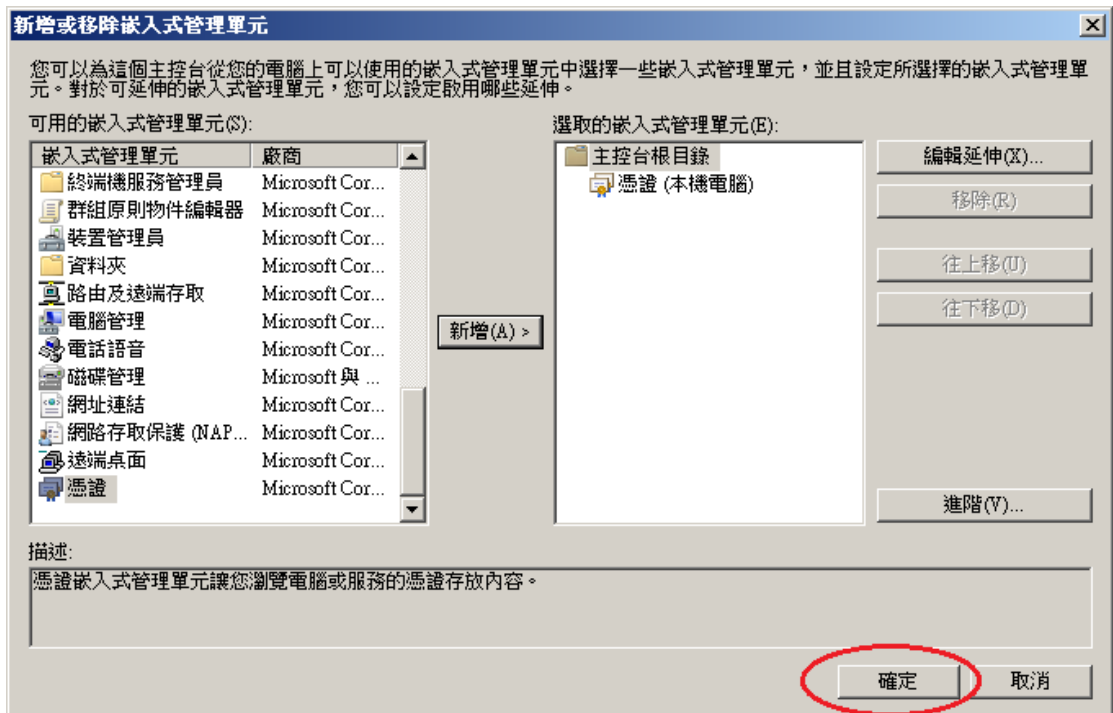
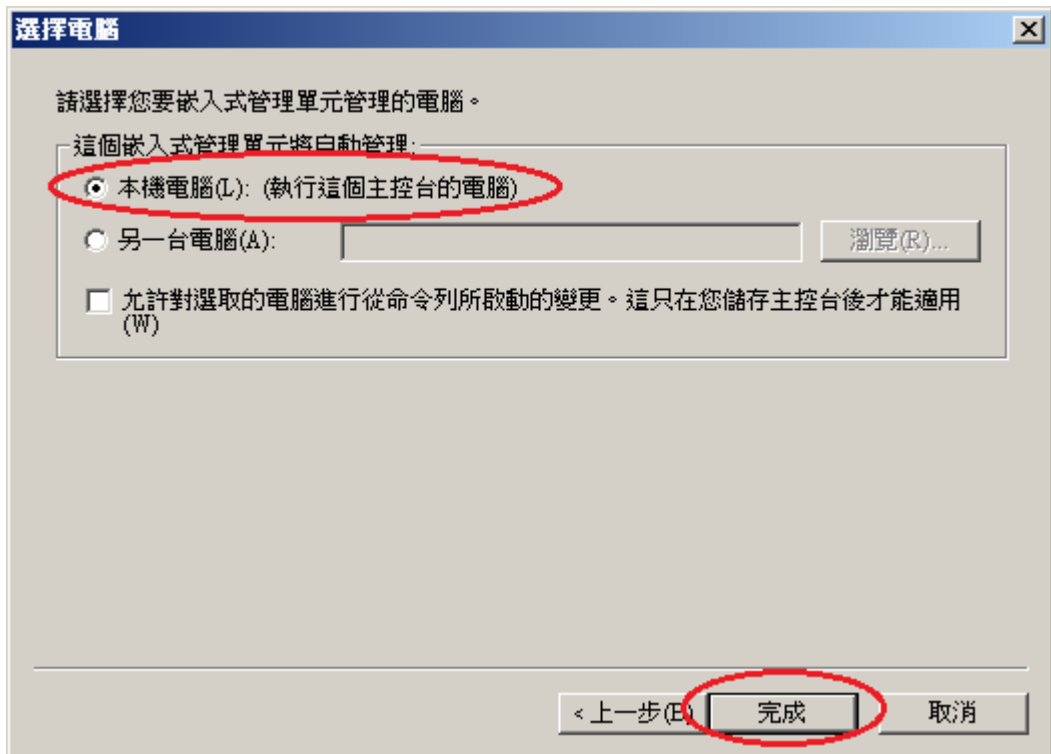


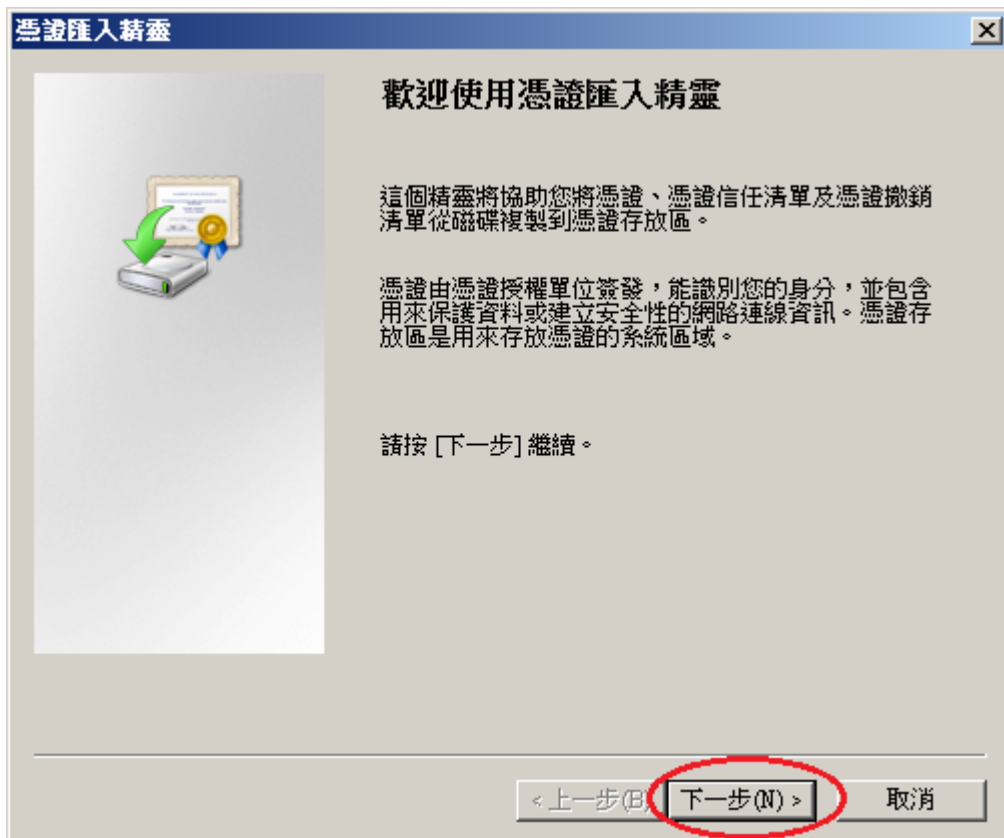
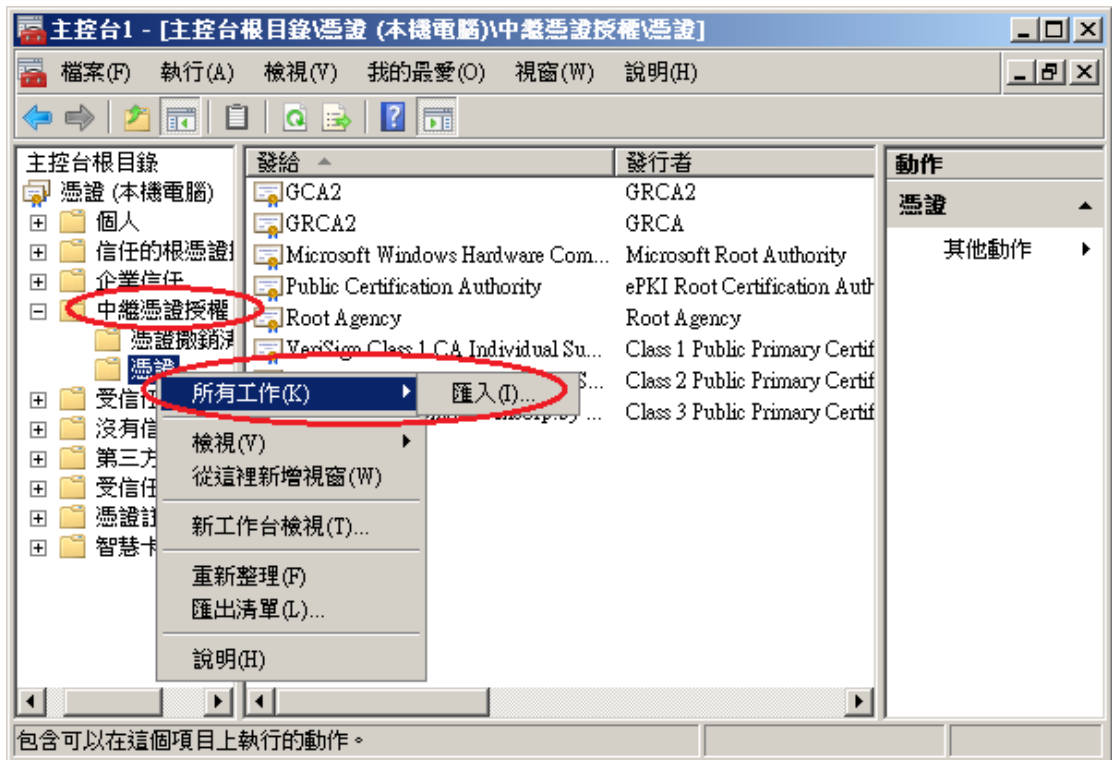
九、匯入 PublicCA G2 憑證(若曾經匯入過，可以略過此步驟)。

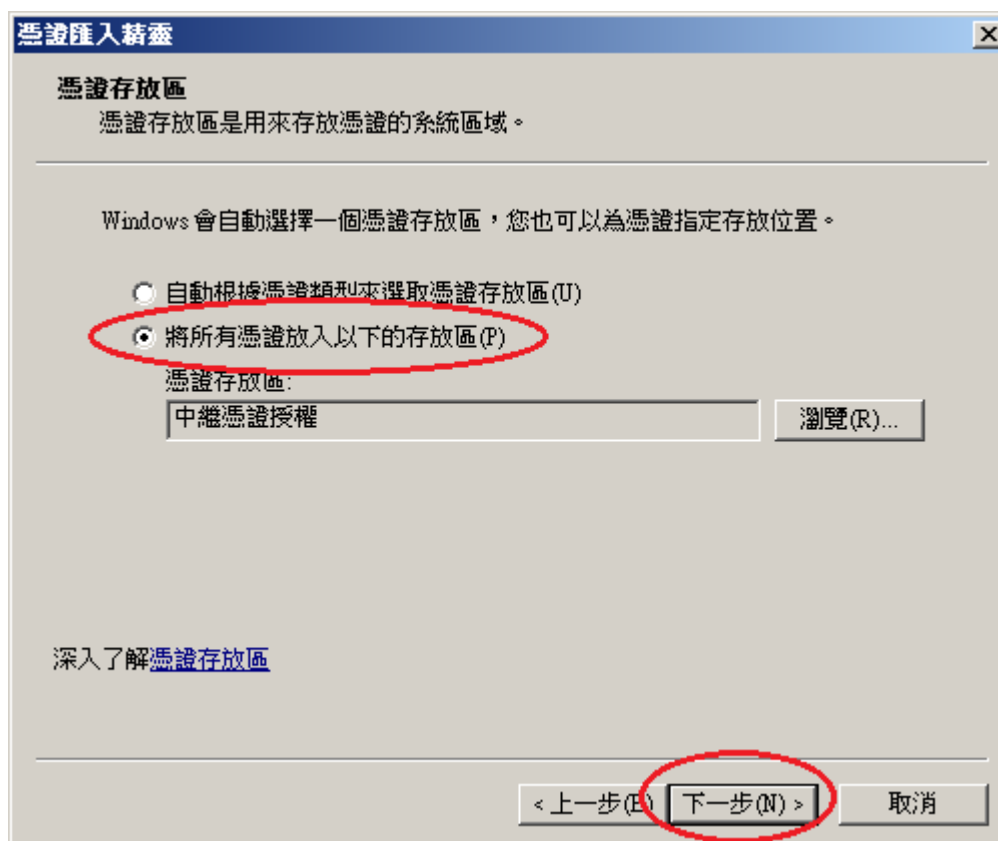
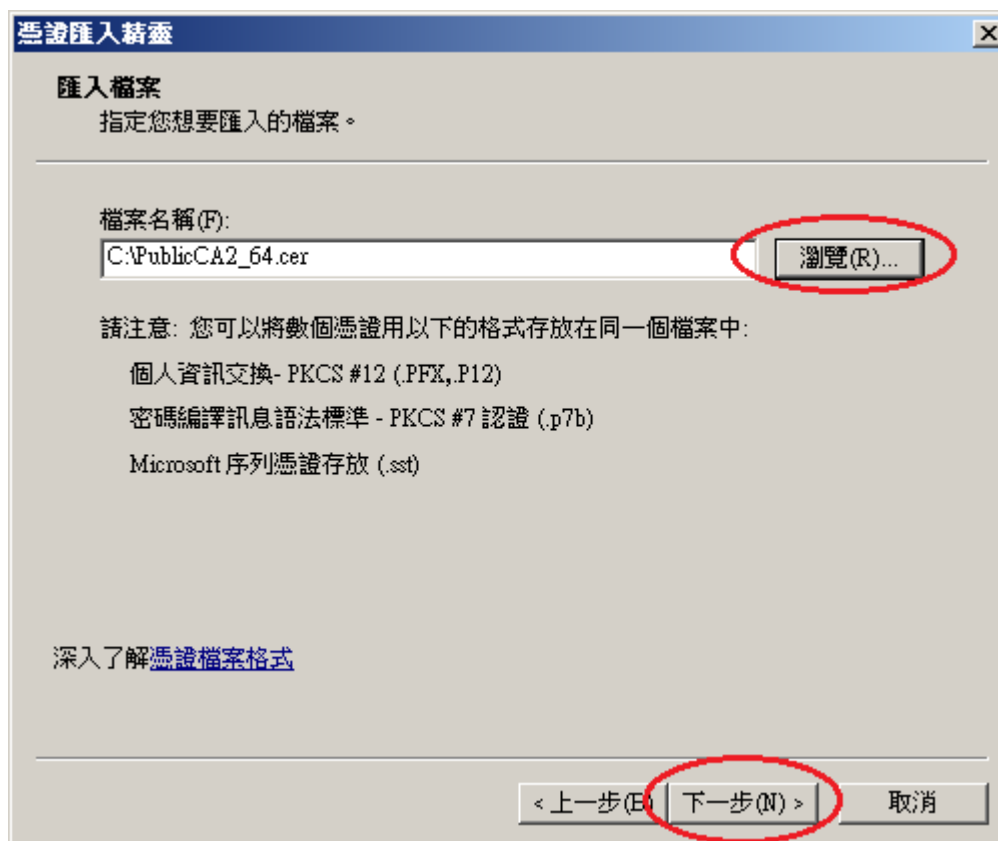
PublicCA G2 憑證：http://publicca.hinet.net/CHTM/download/PublicCA2_64.crt

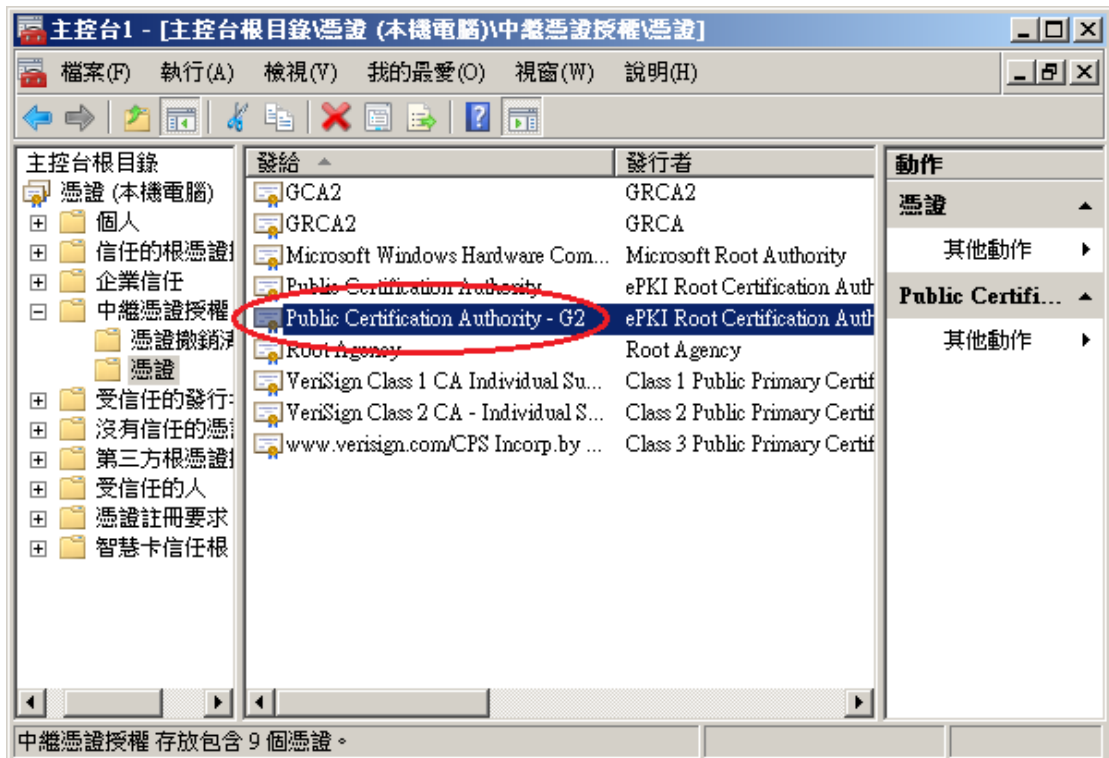
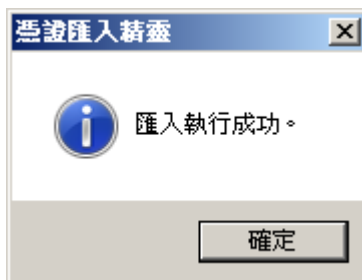
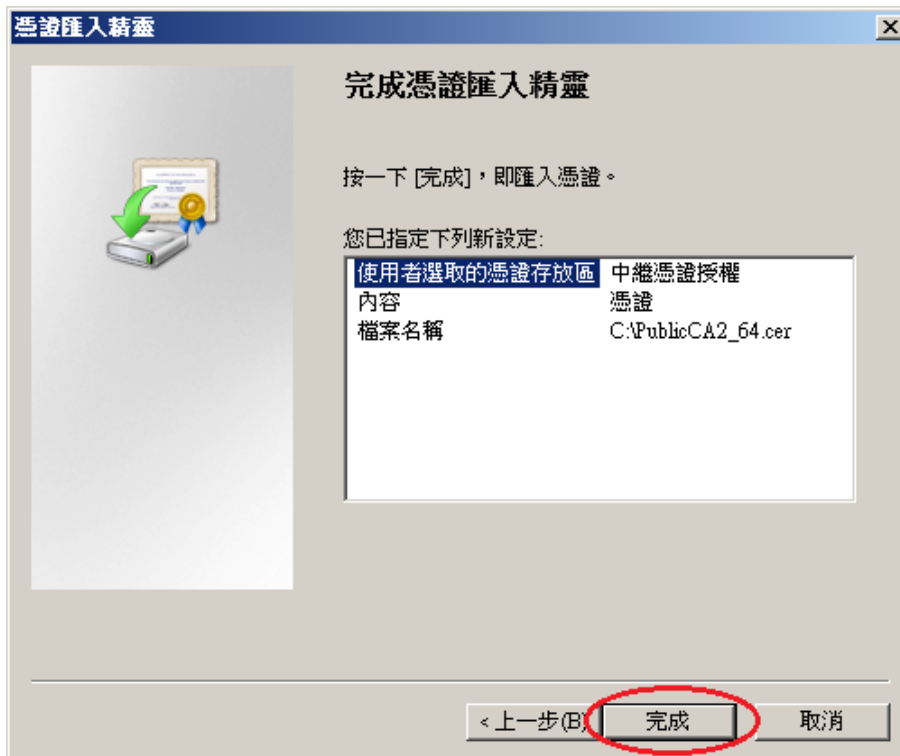






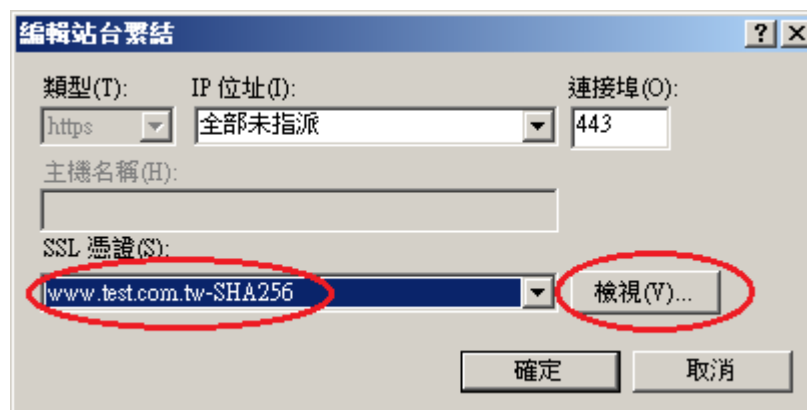
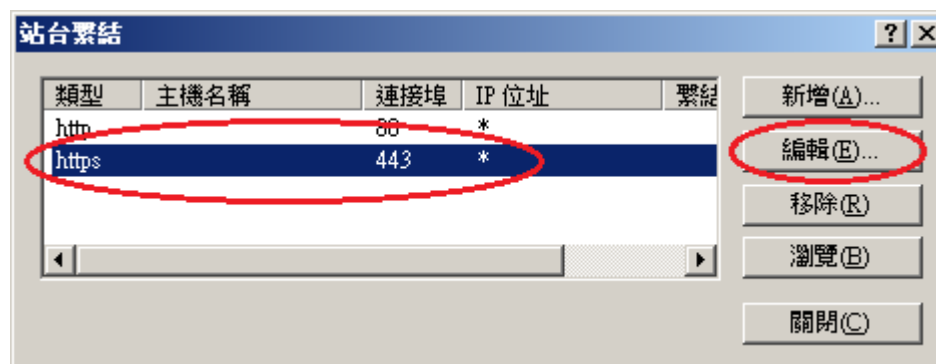
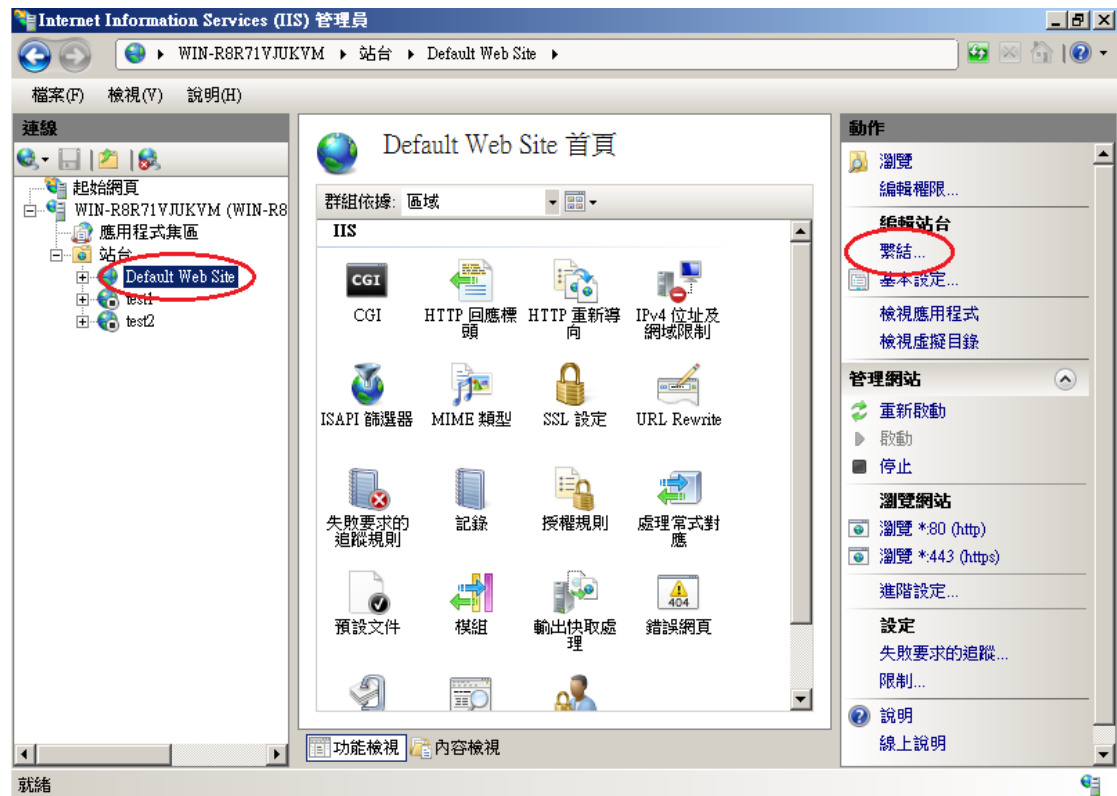


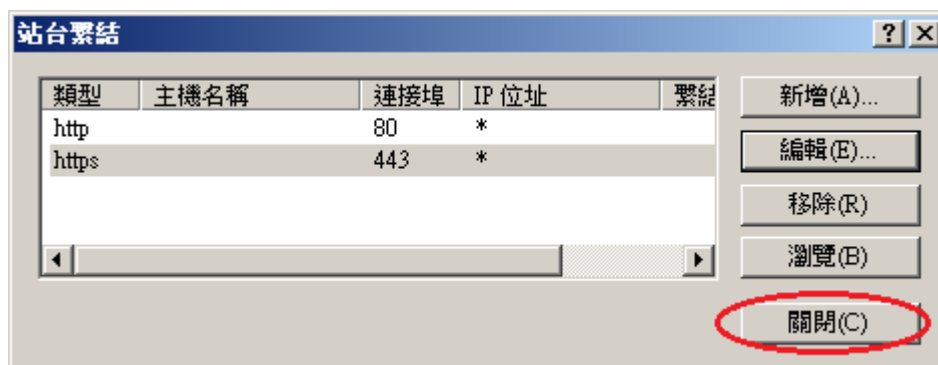
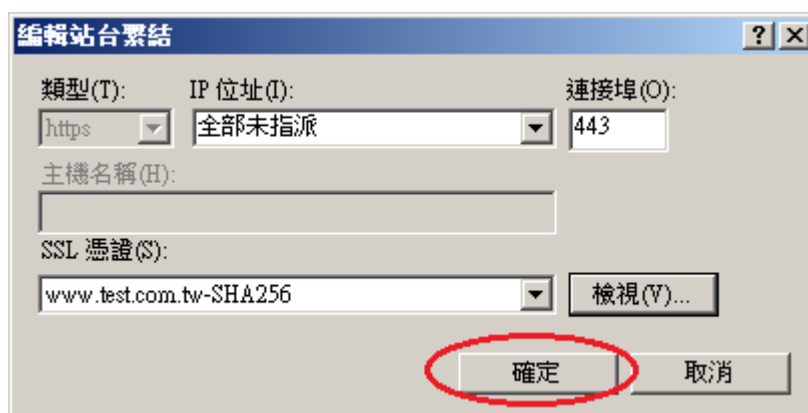
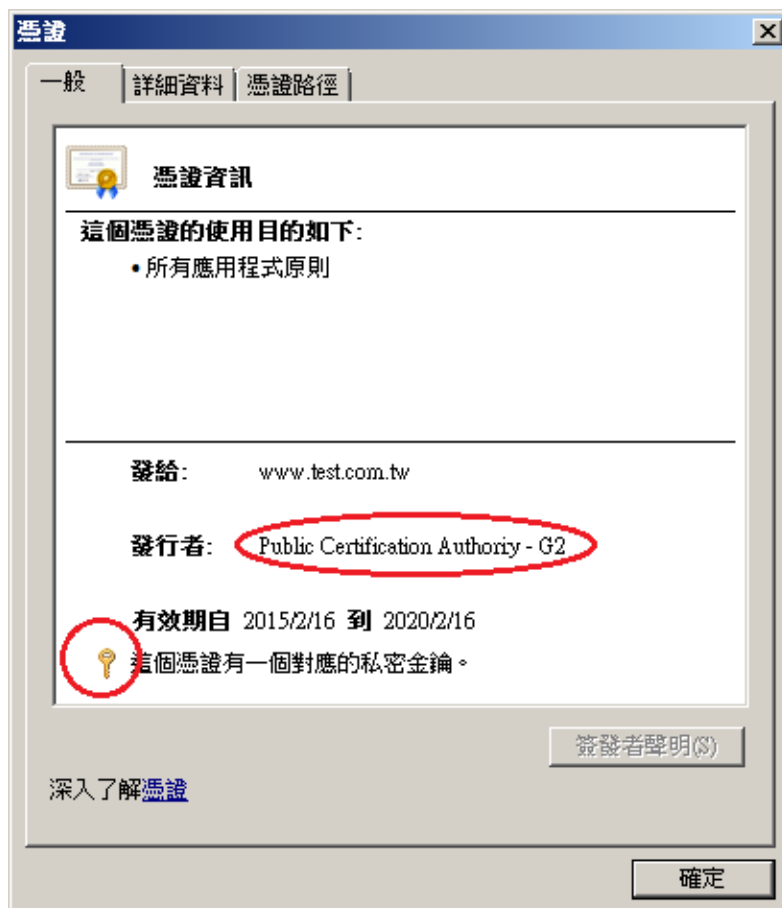




十、於站台上換上 SHA256 憑證。

點選需要更換 SHA256 憑證的站台→「繫結」





十一、以瀏覽器檢視網頁是否正常運作。

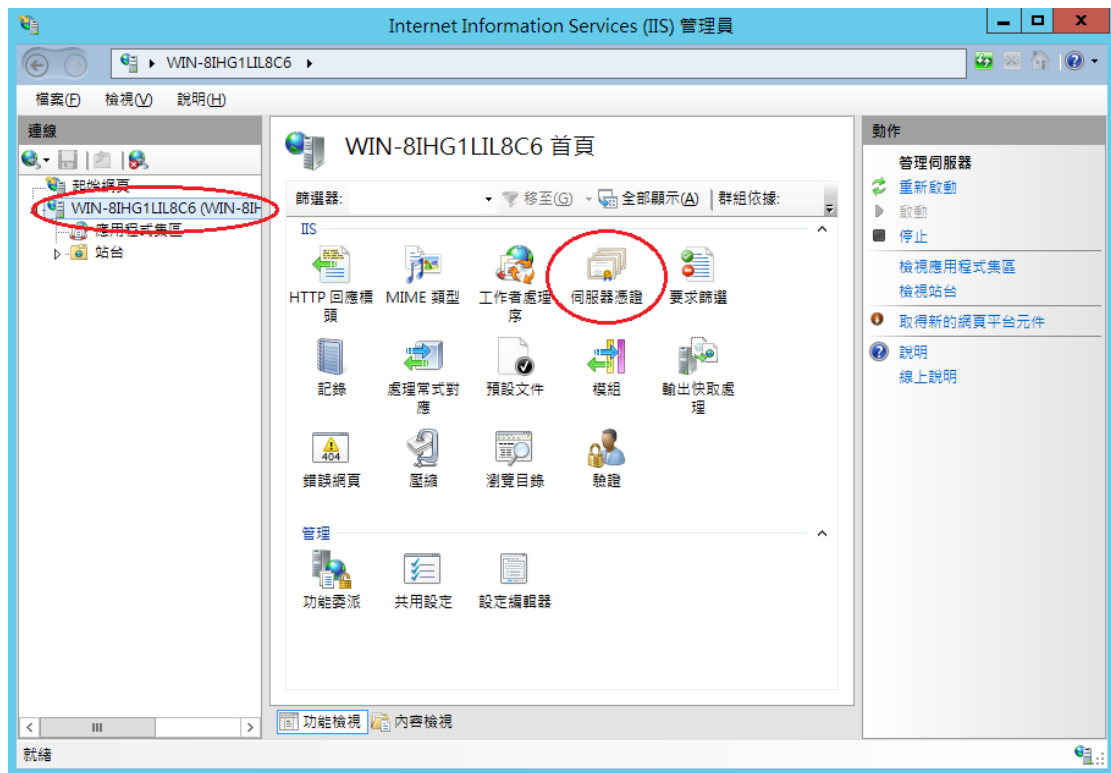
Windows Server 2012 IIS 8

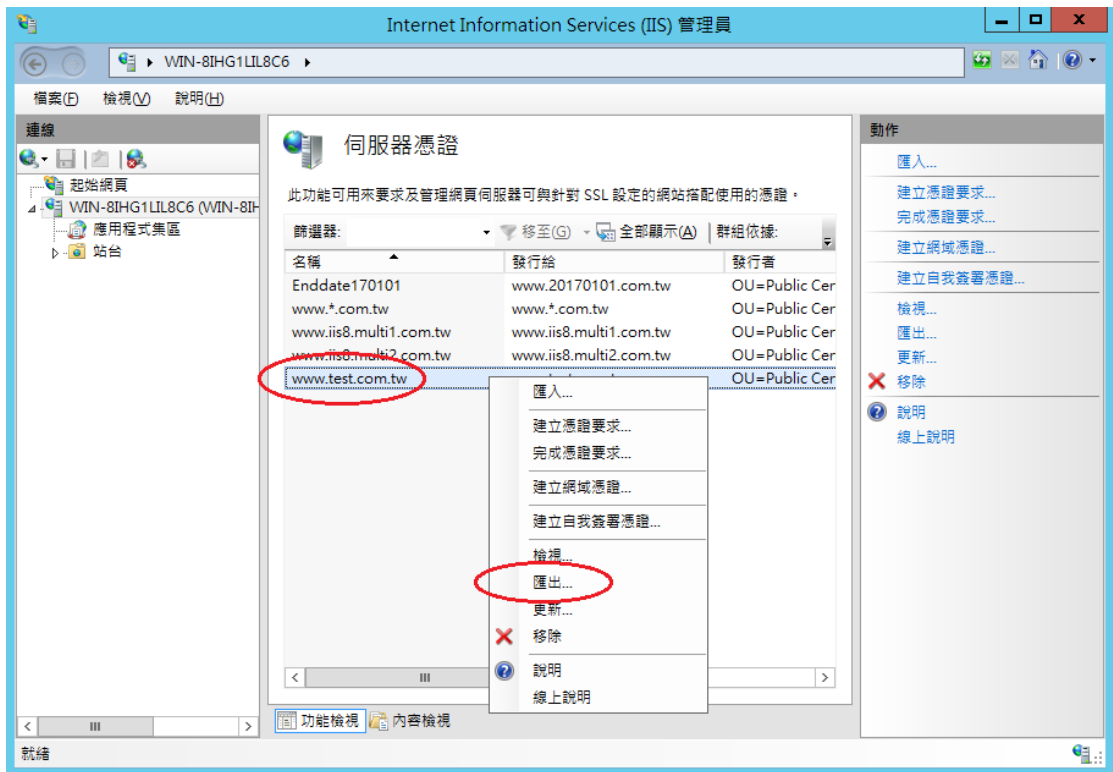
- 一、適用於申請時，有同時取得 SHA1、SHA256 憑證。或是憑證在效期內，經由審驗人員再次核發 SHA256 憑證者。
- 二、有關國際間漸進淘汰 SHA-1 憑證移轉至 SHA 256 憑證細節，請參閱問與答之金鑰長度與演算法(<https://publicca.hinet.net/SSL-08-06.htm>)。
- 三、需要先備妥 OpenSSL 軟體，或是找尋已安裝 OpenSSL 軟體的主機，後續將會使用到。

Windows 版 OpenSSL 軟體連結，可以只安裝「light」的版本即可：

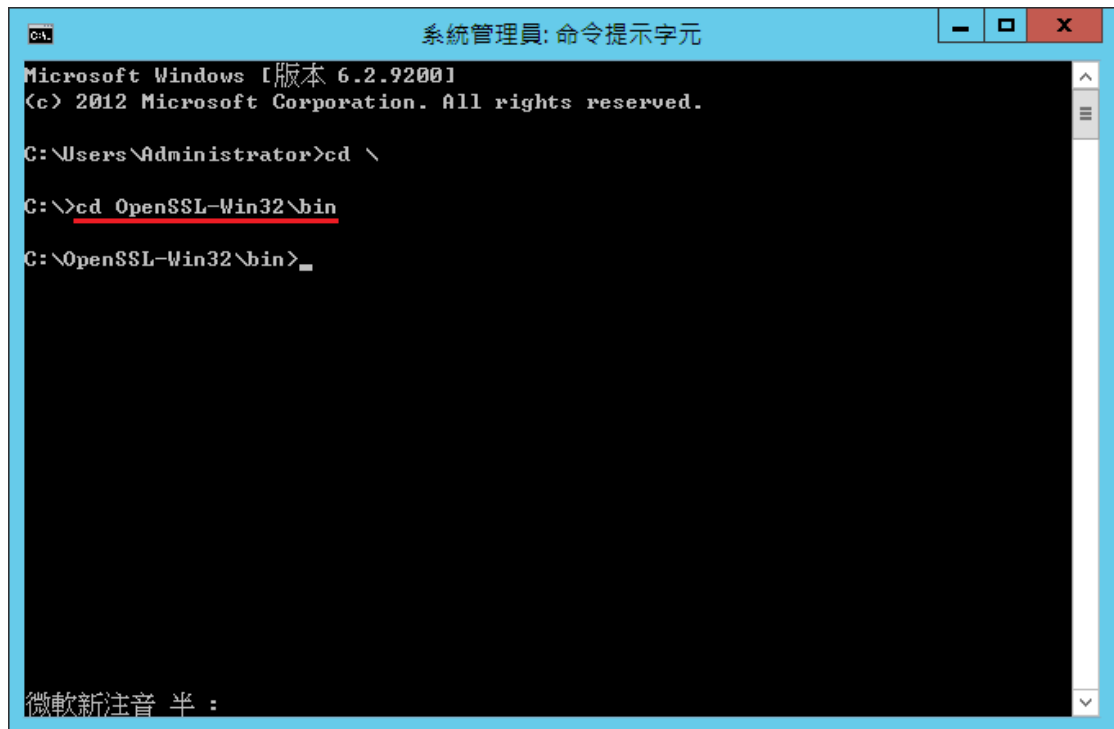
<https://www.openssl.org/related/binaries.html>

- 四、從 IIS 管理員匯出 SHA1 憑證與私密金鑰。
開啟 IIS 管理員，點選「伺服器憑證」





- 五、開啟「命令提示字元」，進入安裝 OpenSSL 目錄下的 bin 資料夾。
請依實際安裝路徑做調整



```
Microsoft Windows [版本 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

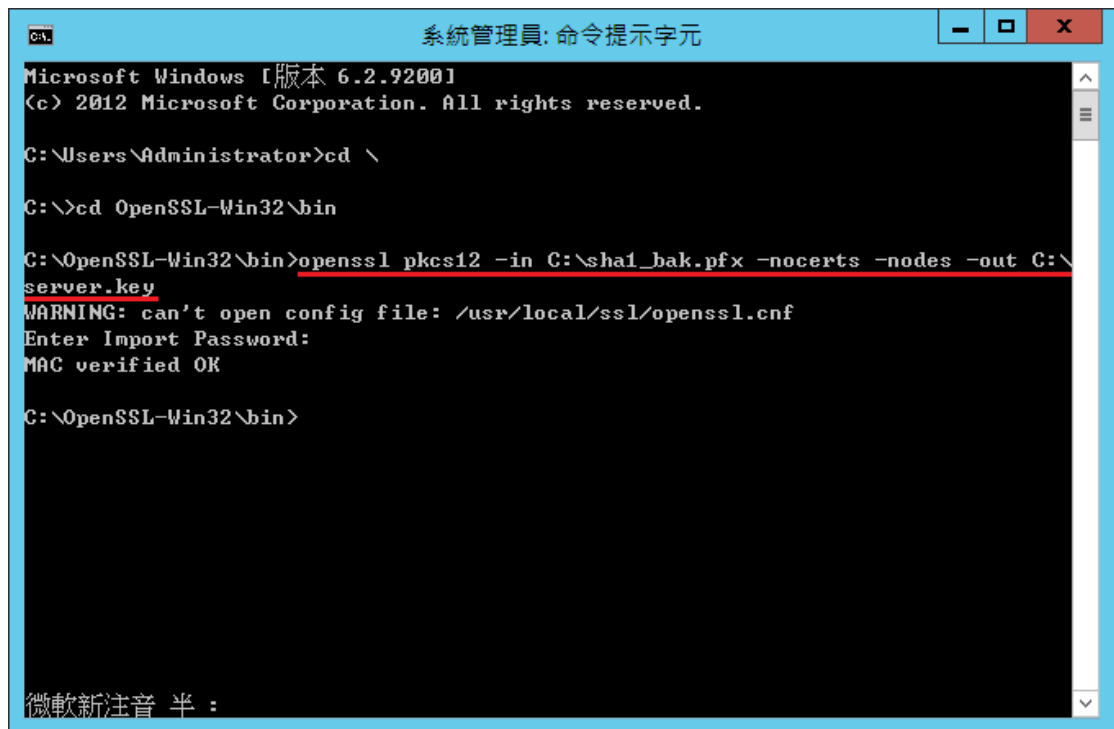
C:\Users\Administrator>cd \

C:\>cd OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>_
```

微軟新注音 半 :

- 六、由 pfx 檔案分離出私密金鑰。
執行以下指令，並輸入從 IIS 匯出 pfx 時的密碼：
openssl pkcs12 -in <pfx file path> -nocerts -nodes -out <save private key path>



```
Microsoft Windows [版本 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \

C:\>cd OpenSSL-Win32\bin

C:\OpenSSL-Win32\bin>openssl pkcs12 -in C:\sha1_bak.pfx -nocerts -nodes -out C:\server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Import Password:
MAC verified OK

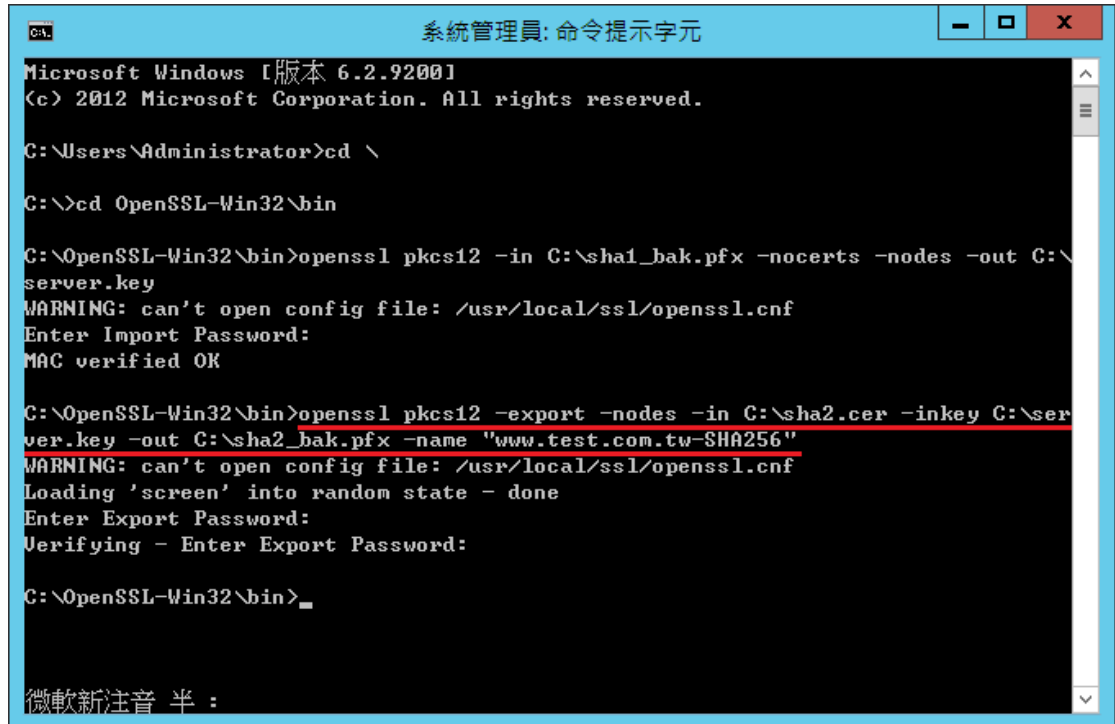
C:\OpenSSL-Win32\bin>
```

微軟新注音 半 :

七、將私密金鑰與 SHA256 憑證重新合併成 pfx 檔案

執行以下指令，並輸入兩次 pfx 檔案匯出密碼：

```
openssl pkcs12 -export -nodes -in <sha256 certificate path> -inkey <private key path> -out <save pfx path> -name <alias name>
```



```
Microsoft Windows [版本 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \

C:\>cd OpenSSL-Win32\bin

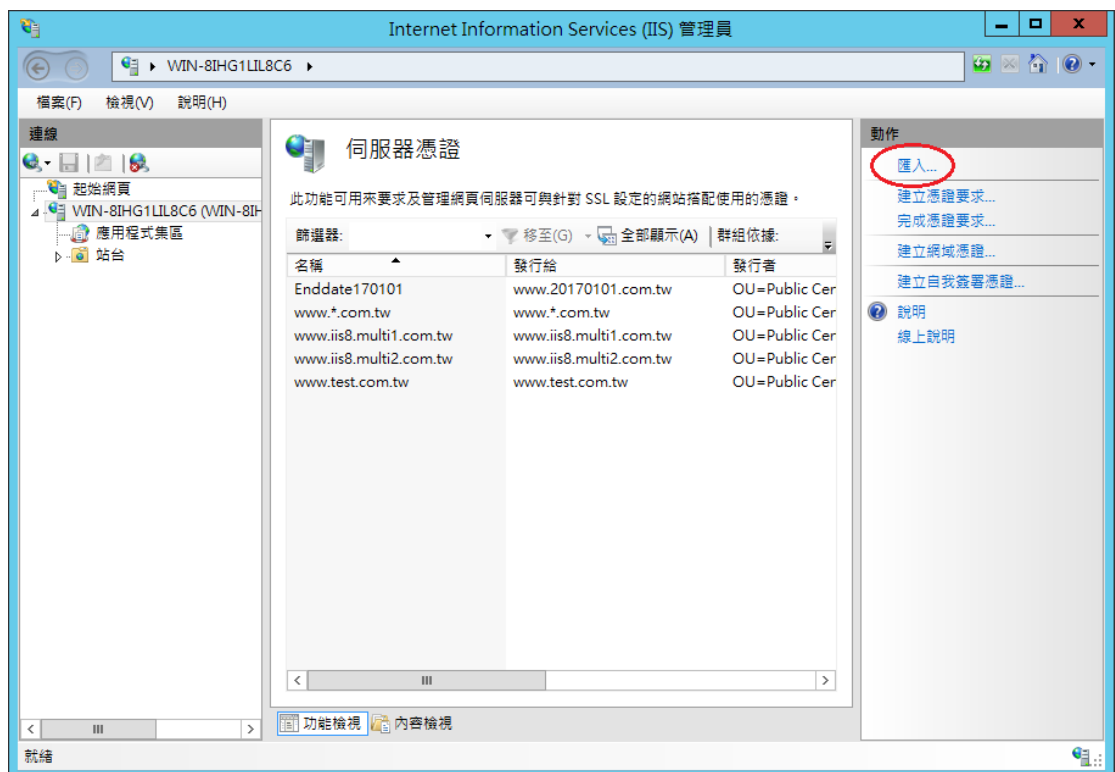
C:\OpenSSL-Win32\bin>openssl pkcs12 -in C:\sha1_bak.pfx -nocerts -nodes -out C:\server.key
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Enter Import Password:
MAC verified OK

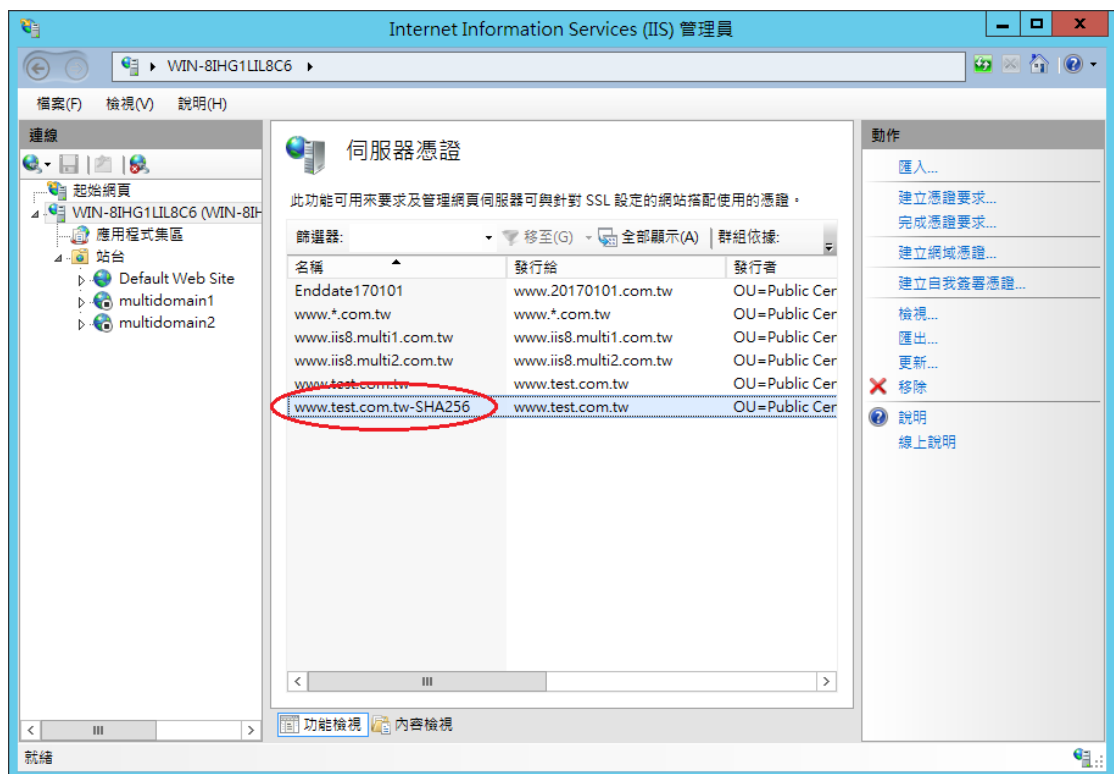
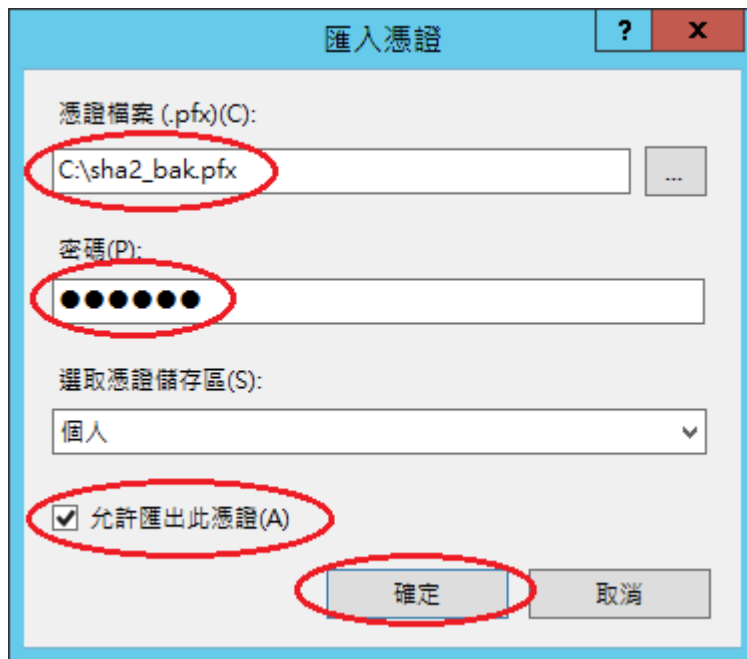
C:\OpenSSL-Win32\bin>openssl pkcs12 -export -nodes -in C:\sha2.cer -inkey C:\server.key -out C:\sha2_bak.pfx -name "www.test.com.tw-SHA256"
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Enter Export Password:
Verifying - Enter Export Password:

C:\OpenSSL-Win32\bin>
```

八、匯入 SHA256 憑證。

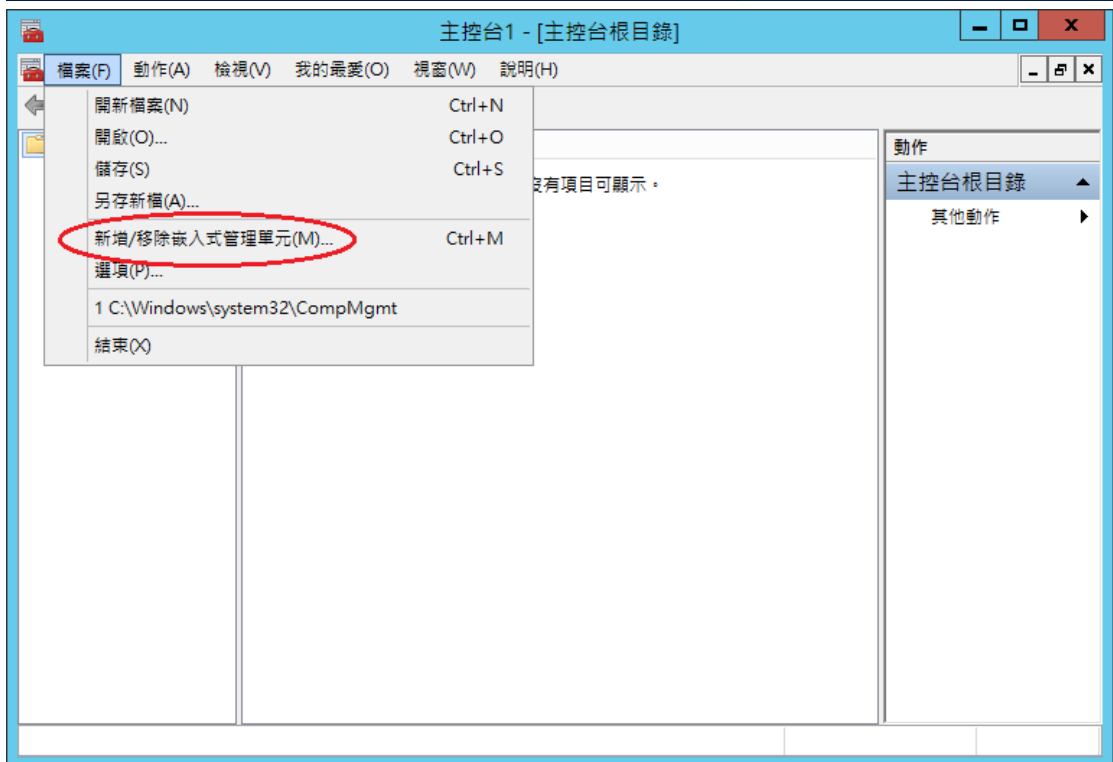
重新回到 IIS 管理員，並點選「匯入」

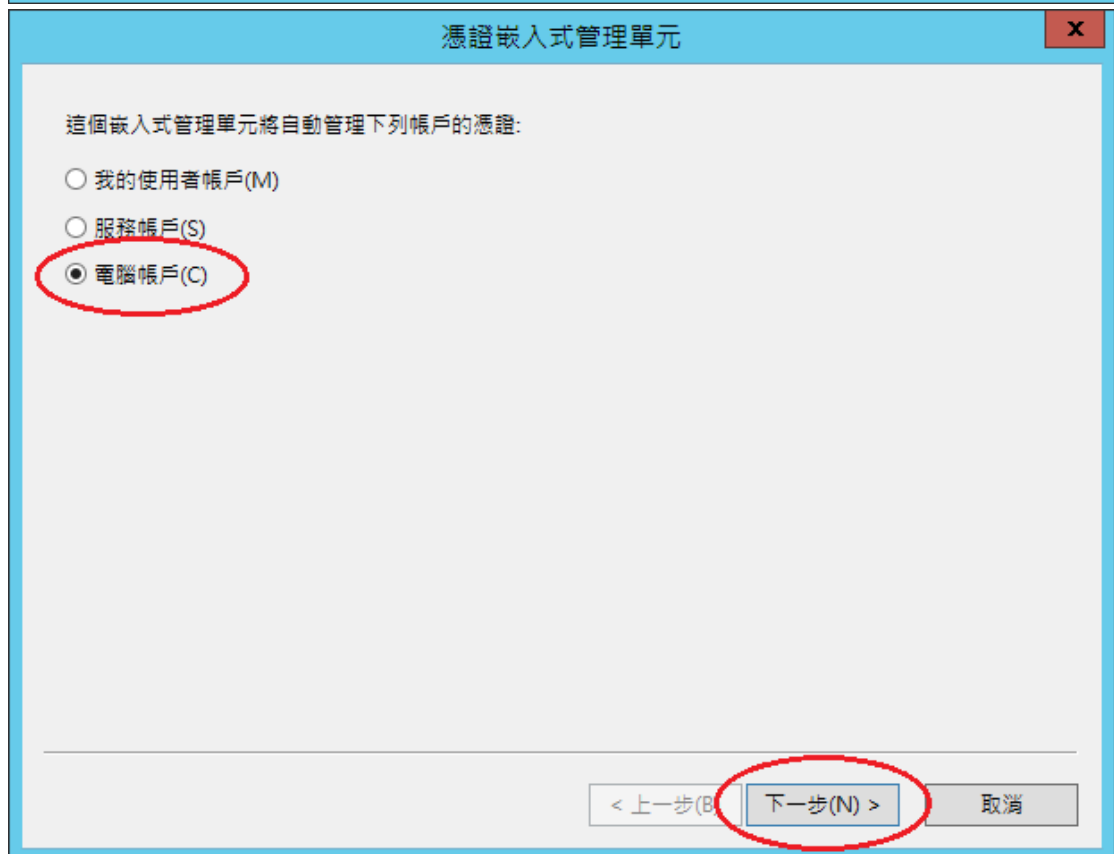
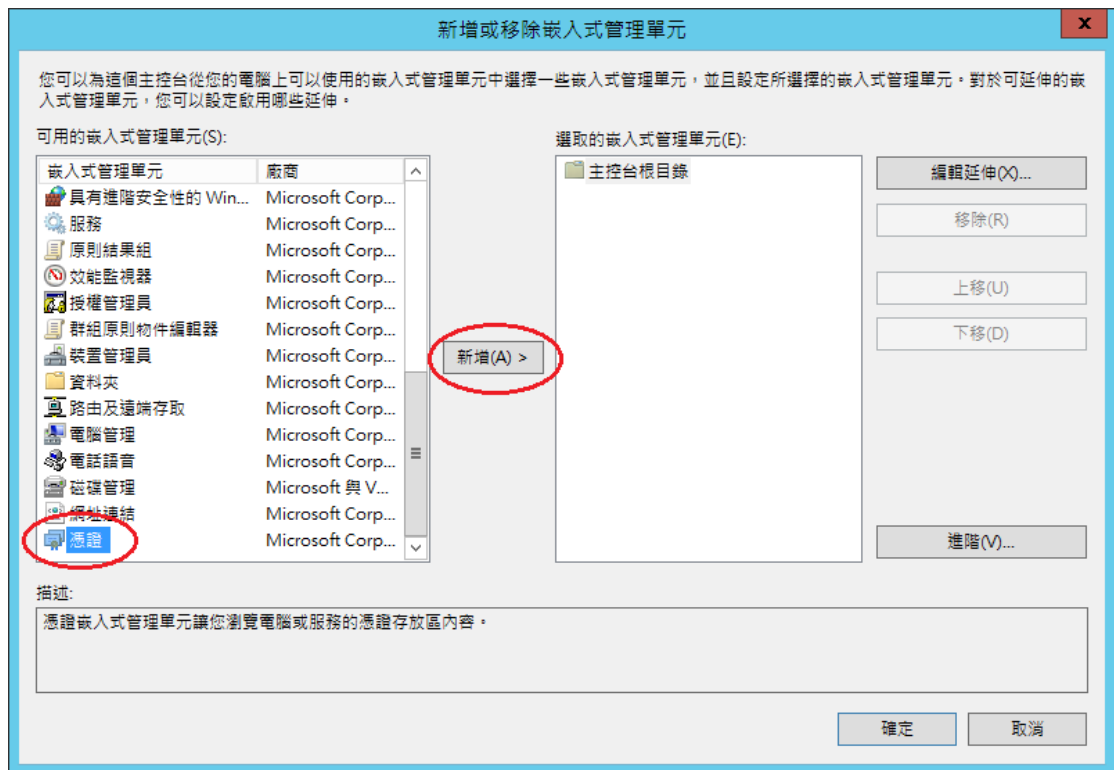


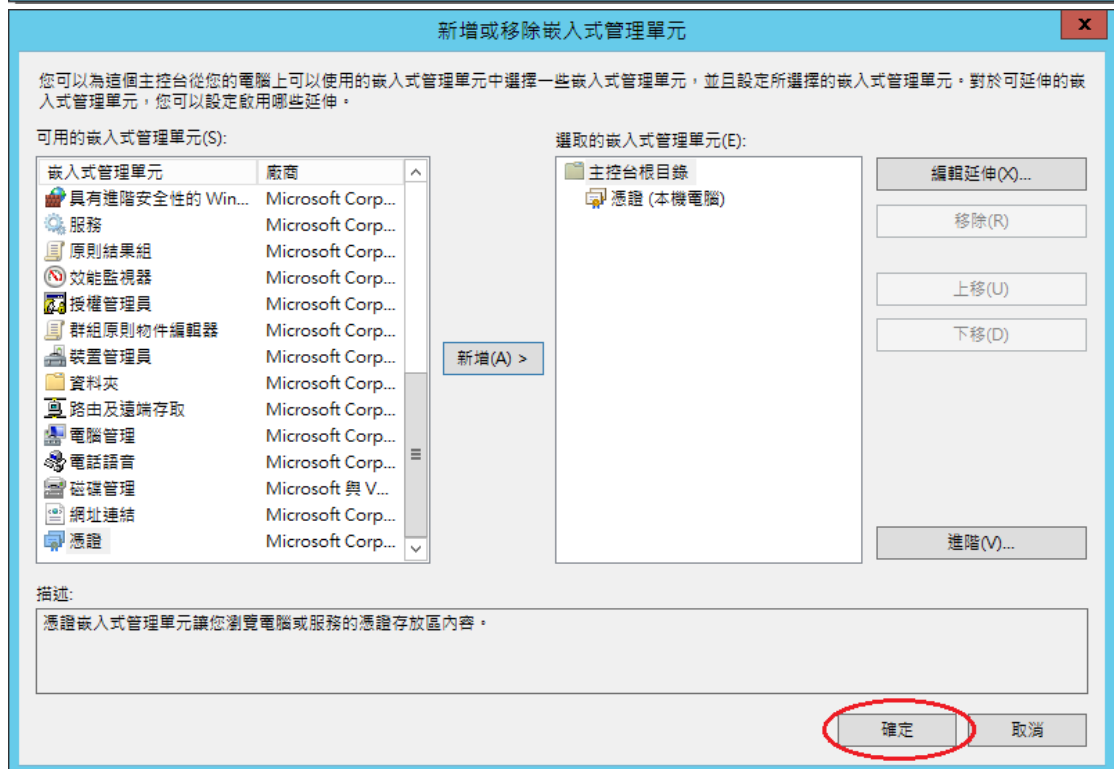


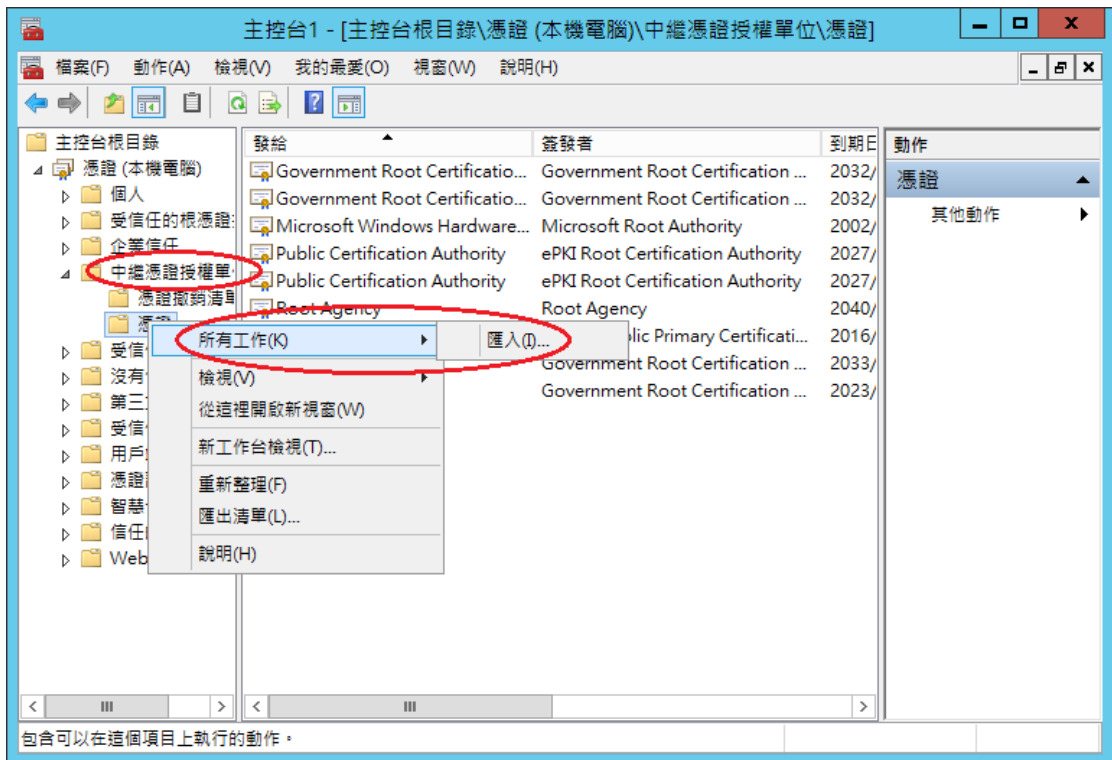
九、匯入 PublicCA G2 憑證(若曾經匯入過，可以略過此步驟)。

PublicCA G2 憑證：http://publicca.hinet.net/CHTM/download/PublicCA2_64.crt

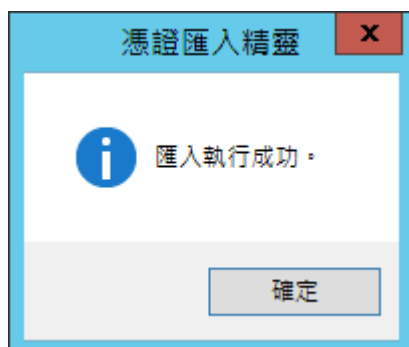


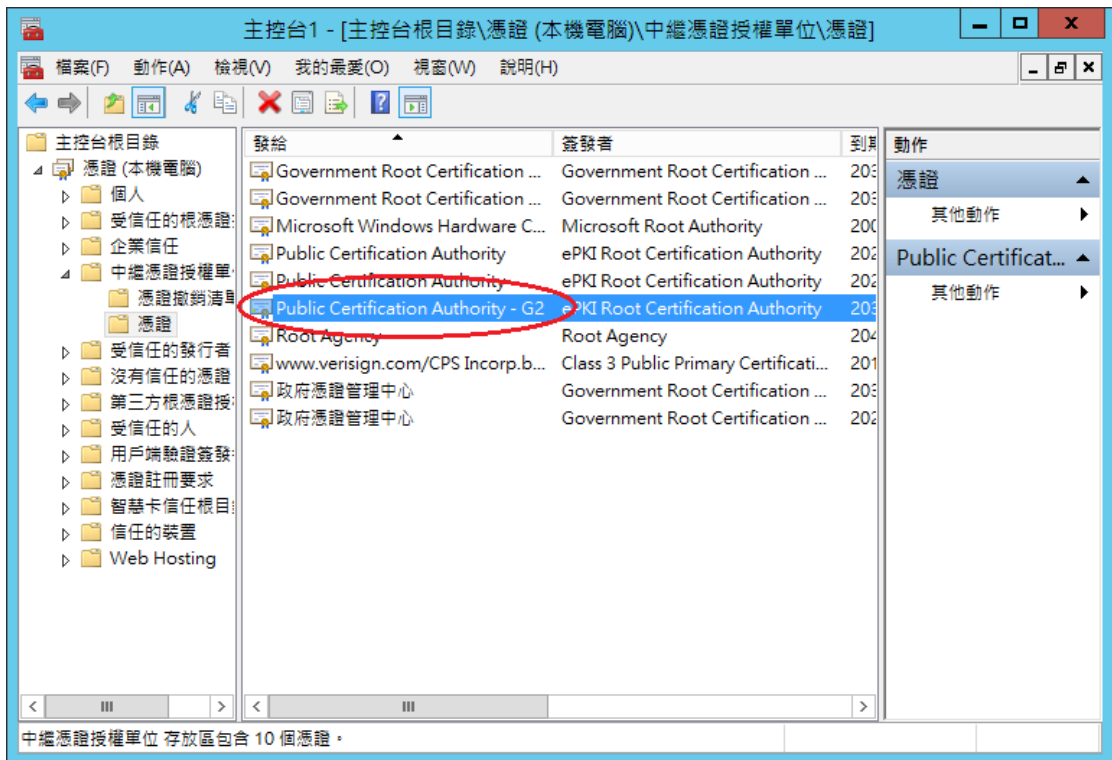




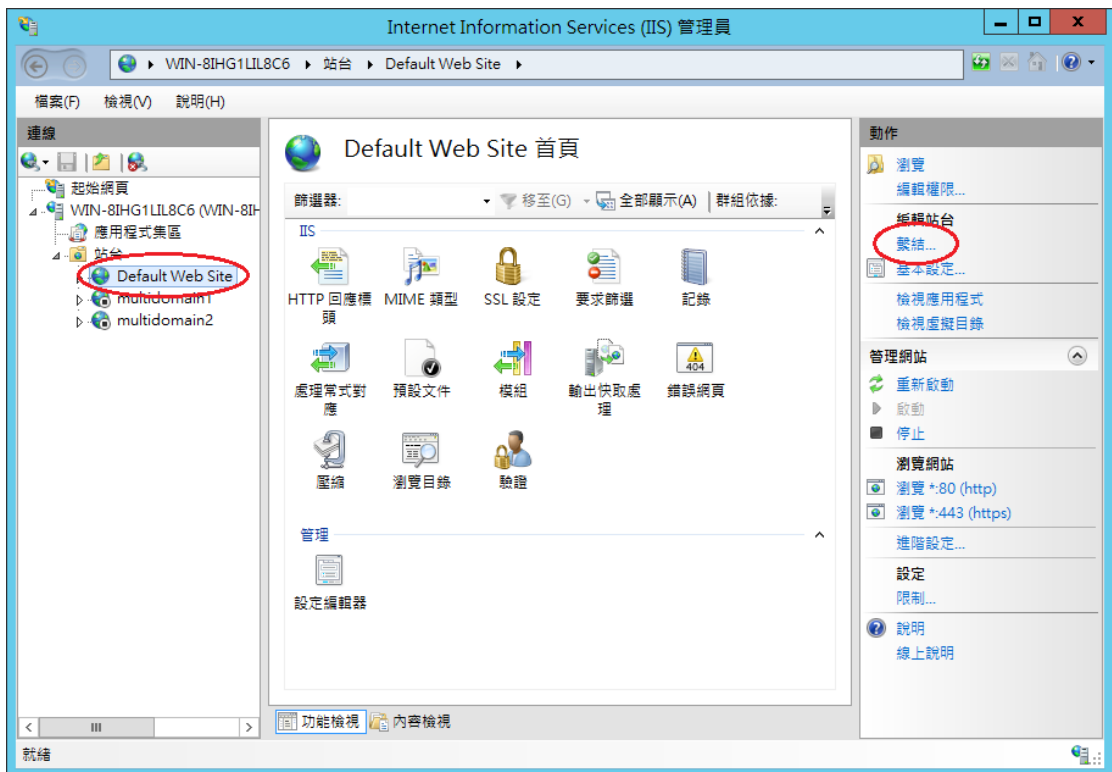


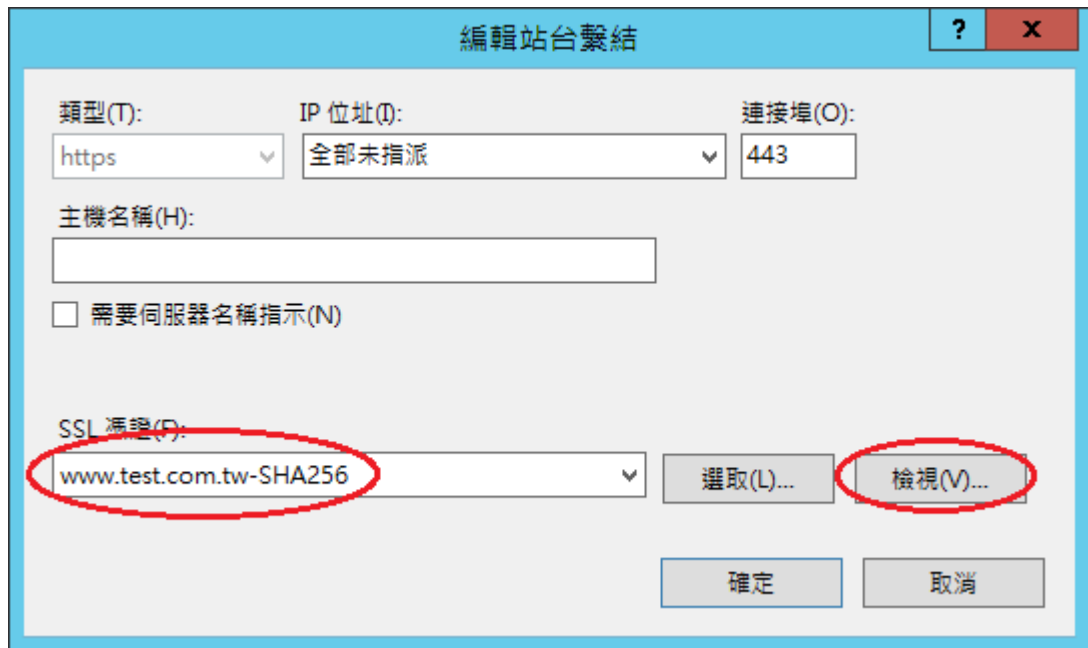
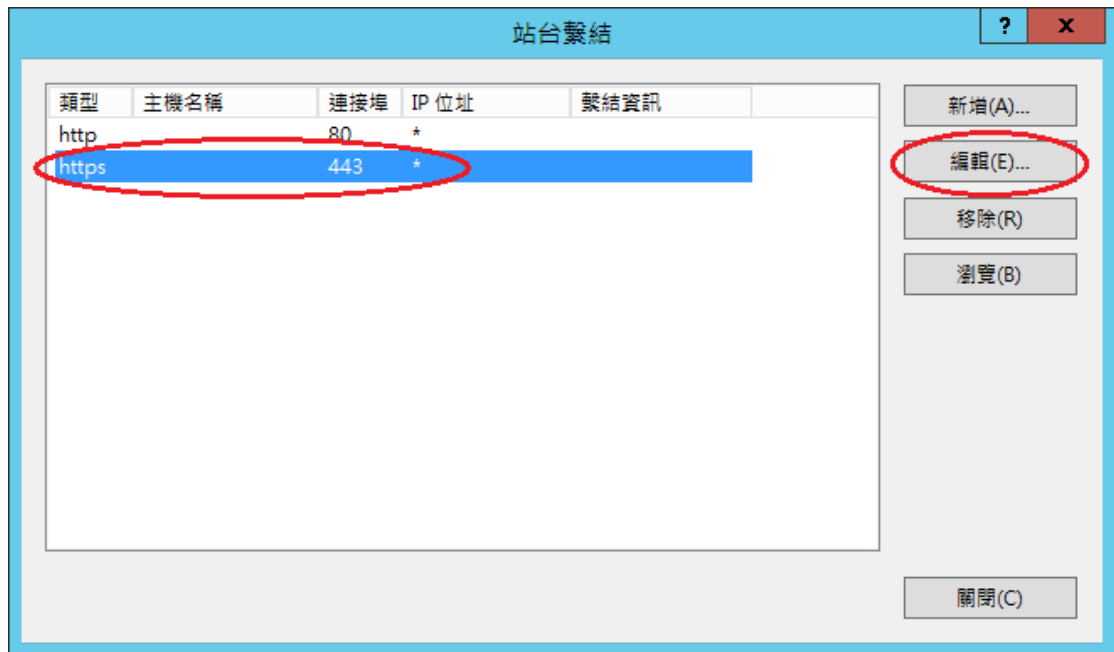


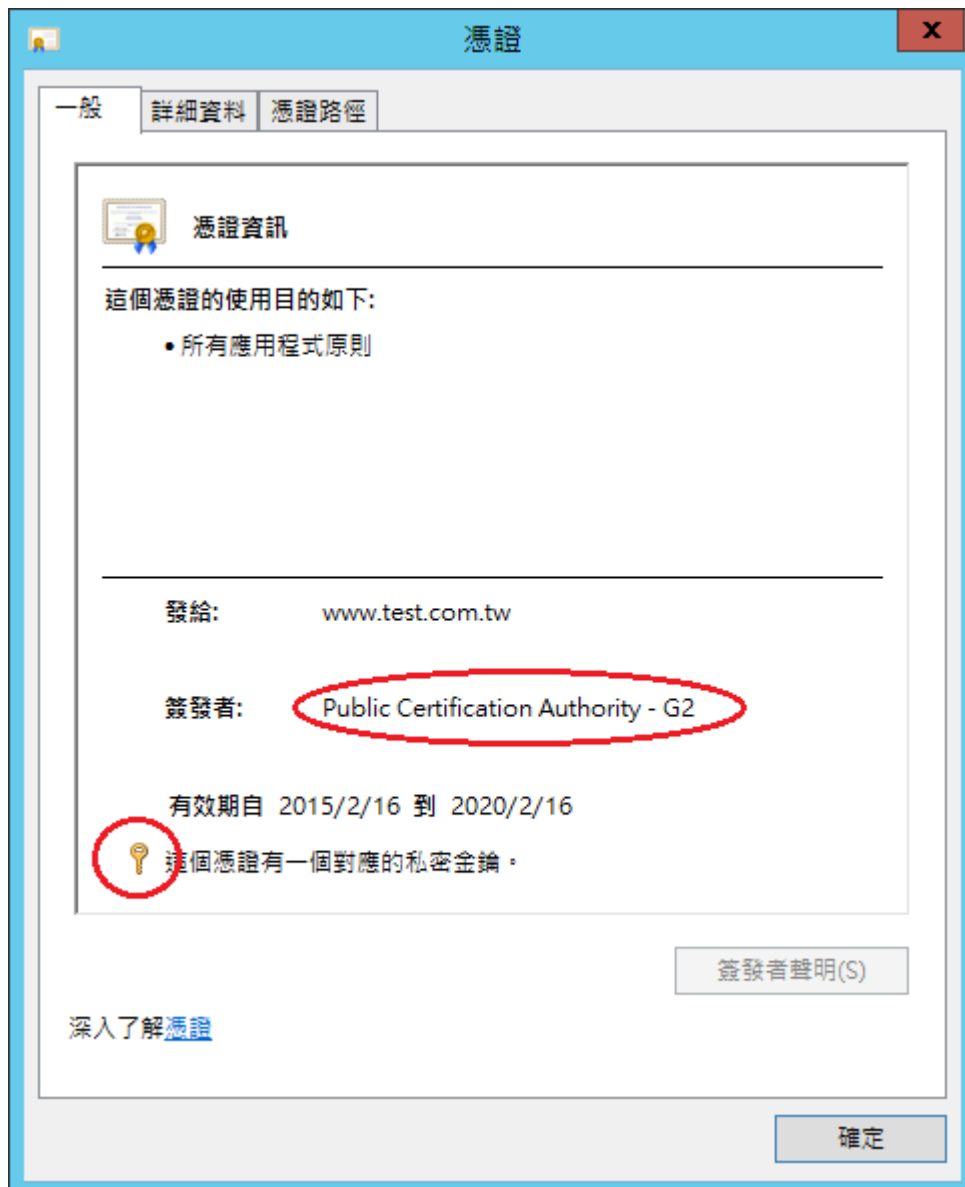


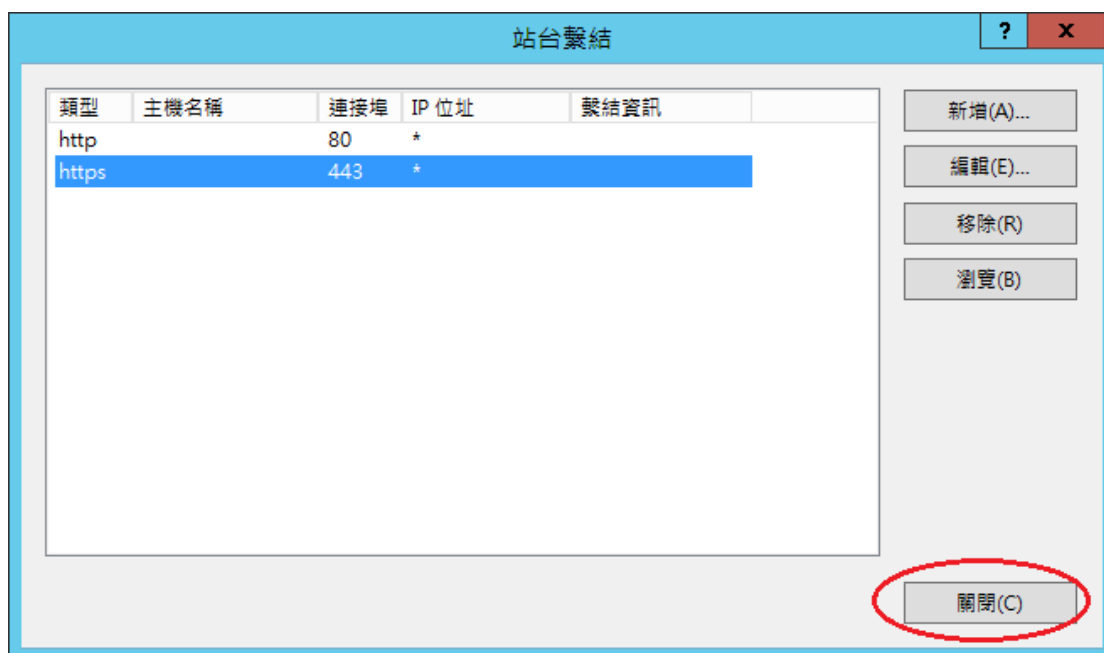


- 十、於站台上換上 SHA256 憑證。
 點選需要更換 SHA256 憑證的站台→「繫結」









十一、 以瀏覽器檢視網頁是否正常運作。