

# SSL 伺服器數位憑證 Apache2.2 伺服器操作手冊

---

機密等級：公開

版本：V5.1

文件編號：MNT-03-083

生效日期：110 年 8 月 10 日



臺灣網路認證股份有限公司

**TAIWAN-CA. Inc.**

台北市 100 延平南路 85 號 10 樓

電話:02-2370-8886

傳真:02-2370-0728

[www.twca.com.tw](http://www.twca.com.tw)

## 目 錄

<b>1.目的</b> .....	<b>1</b>
<b>2.範圍</b> .....	<b>2</b>
<b>3.參考資料</b> .....	<b>3</b>
<b>4.定義</b> .....	<b>4</b>
<b>5.作業程序</b> .....	<b>5</b>
5.1 前置作業.....	5
5.2 產製「金鑰」.....	6
5.3 產生「憑證請求檔(CSR)」.....	7
5.4 將製作好的憑證請求檔(CSR)上傳.....	9
5.5 下載已核發憑證.....	15
5.6 安裝憑證.....	18
5.7 設定 SSL 模式.....	21
5.8 驗證 SSL 功能.....	24
5.9 異常排除.....	28
5.10 備份／復原憑證.....	29
5.11 更新 SSL 憑證.....	30
<b>6.常見問題</b> .....	<b>31</b>
<b>7.附件</b> .....	<b>32</b>

## 1.目的

- 1.1. 介紹 Apache2.2 網頁伺服器之金鑰、憑證請求檔產製步驟及 SSL 伺服器數位憑證安裝說明。
- 1.2. 符合本公司資訊安全政策之規範。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 2. 範圍

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

### 3. 參考資料

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 4. 定義

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5. 作業程序

### 5.1 前置作業

#### 5.1.1 安裝 Apache 2.2 Web 伺服器軟體

Apache 2.2 Web 伺服器軟體是由 Apache 組織所提供的 Web 伺服器軟體，可至 <http://httpd.apache.org/> 下載，本操作手冊安裝環境為 Apache 2.2 (Windows 版)，在此不另外說明安裝方法，如對安裝過程有任何問題，請聯絡本公司協助處理。

#### 5.1.2 安裝 OpenSSL 軟體

Apache 需搭配 OpenSSL 軟體來產製金鑰，Apache 2.2 已內建 OpenSSL 軟體，軟體存在 %Apache2.2%\bin\ 目錄裡，如果要另外安裝 OpenSSL 可至 <http://www.openssl.org/> 下載，在此不另外說明安裝方法，如對安裝過程有任何問題，請聯絡本公司協助處理。

## 5.2 產製「金鑰」

5.2.1 在%Apache2.2%\bin\目錄下，輸入

```
openssl genrsa -out c:\server.key 2048
```

(指令反白部份請依實際路徑決定，-out 即為產生的金鑰檔存放位置)

```
openssl genrsa -out c:\server.key 2048
```

完成上列指令後會在 C:\下產生檔案名稱為 server.key 的 2048 位元長度

RSA 金鑰檔，使用文字編輯器打開金鑰檔後可看到如下內容



```
server.key - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC6IjbjIC512WY0FyxQ2MDSYd1y+7UcIP13P2J39U+wIn3TmCRb
k01RvMWxpqR1n+/j71108UHj0+W3F4J+w6yGfEmnFS+pg80hGKGR0tU6519MWXLS
4XnJ9ekI2j7CWn4YeP02szyp4u+WjM9UKx/iimLG6U8t1785+r07ThPcPwIDAQAB
AoGAGjVvHRQ09rEh3vvUUZ3vqK/3CpW+t7Y9emkGaHW2PsrchMrLc8mN/ZBjFdyt
E5Ltqf6tLY7XM+2TNw7d7X9uMSWHwMaQrE648d/08i146II/qY+4VQcgrkihTM2
GiB5pvLdJAHxQjHv0tY7zPGBtsAHw9wxCDDEj1H5yubX40ECQDaw8MY4tSa/UyF
LSH6+kFYmKsKEoAJw1FXt9uUhzeXQiUciWuoBDeUvc6o0FK1gS6Ffv692FGNxQaU
U28WXPWpAkEA2jhcPUQQA2ZSUzuH7Kvxid/pWTW5Z14QFFASXtCb2AvqxjqQz9F3
Neptvr/IDg0s+tU/kkAzxyAmH+jdJ/2jpwJAVIkJ8ux+GrLTySS6SIvyGHaiYPfg
keakzyzi2ZGtM6/R/vNEtntLeU4yX7CnFJW6iPwtaxqhJ22NeocCjsnWYQJAJsU0
vf8Nb00yu08Ma2RxWcnKr+r3sgHoc+3WFbqCtFQIFog5SnMw9wdb0FRKuxK0HSze
SqHUKT+JBopYgjZyaQJBAI213VJYGES1j41z4XpAmKF0hUdDqbUHu1k+85U+ebK0
rM816xnxUDW0ES1si0Rn3/uUctb0hitPpSpqc4sq2==
-----END RSA PRIVATE KEY-----
```



### 5.3 產生「憑證請求檔(CSR)」

#### 5.3.1 在% Apache2.2%\bin\目錄下，輸入

```
openssl req -new -key c:\server.key -out c:\server.csr
```

(指令反白部份請依實際路徑決定，-key 所指定的路徑即為 5.2 節所產生的金鑰檔位置，-out 即為產生的 CSR 存放位置)

```
openssl req -new -key c:\server.key -out c:\server.csr
```

此時會要求輸入憑證內容，說明如下：

請輸入 2 碼國碼(如 TW)，**必填**

```
Country Name (2 letter code) [AU]:TW
```

請輸入州/省別(如 TAIWAN)，**必填**

```
State or Province Name (full name) [Some-State]:TAIWAN
```

請輸入所在城市(如 TAIPEI)，**必填**

```
Locality Name (eg, city) []:TAIPEI
```

請輸入組織名稱(如 TWCA)，**必填**

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TWCA
```

請輸入單位名稱(如 IT、SYSTEM)，**必填**

```
Organizational Unit Name (eg, section) []:SYSTEM
```

請填貴公司欲加密的網站名稱(如 www.twca.com.tw)，**必填**

```
Common Name (eg, YOUR name) []:www.twca.com.tw
```

請輸入申請人員 Email，可不填

```
Email Address []:SSL@twca.com.tw
```

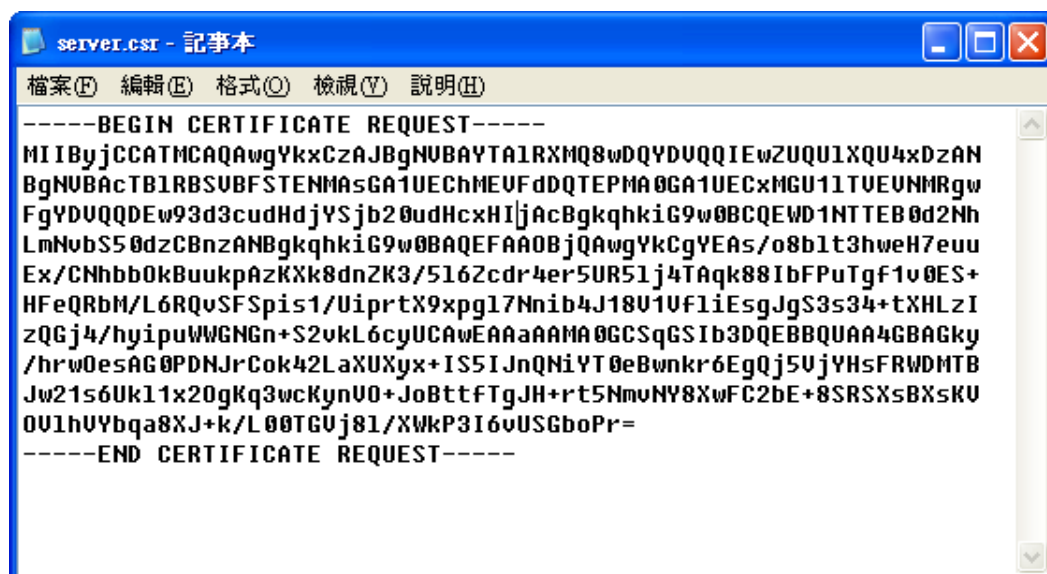
最後會要求輸入額外資訊，**請勿填寫任何資料，直接按 Enter 即可**

```
A challenge password []:
```

```
An optional company name []:
```

完成上列指令後會在 C:\下產生 server.csr 的檔案，此檔即為憑證請求檔，

使用文字編輯器打開金鑰檔後可看到如下內容



```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYjCCATMCAQAwYkxCZAJBGNuBAYTA1RXMQ8wDQYDUQIEwZUQU1XQU4xDzAN
BgNVBACTB1RBSVBFSTENMA5GA1UEChMEVFdDQTEPMA0GA1UECzMGU11TVEUNMRgw
FgYDUQQDEw93d3cudHdjYSjb20udHcxHIjAcBgkqhkiG9w0BCQEW1NTTEB0d2Nh
LmNvbS50dzCBnzANBkgqhkiG9w0BAQEFAA0BjQAwYkCgYEA5/o8b1t3hweH7euu
Ex/CNhbb0kBuukpAzKXk8dnZK3/5162cdr4er5UR51j4TAqk88IbFPuTgf1v0ES+
HFeQRbM/L6RQvSFSpis1/UiprtX9xpg17Nnib4J18U1UFliEsgJgS3s34+tXHLzI
zQGj4/hyipuWwGNGn+S2vkL6cyUCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4GBAGky
/hrw0esAG0PDNjrCok42LaXUXyx+IS5IJnQNiYT0eBwnkr6EgQj5UjYHsFRWDMTB
Jw21s6Uk11x20gKq3wcKynU0+JoBttFTgJH+rt5NmVNY8XwFC2bE+8SRSXsBXsKV
0V1hUyYbqa8XJ+k/L00TGvj81/XWkP3I6vUSGboPr=
-----END CERTIFICATE REQUEST-----
```

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.4 將製作好的憑證請求檔(CSR)上傳

### 5.4.1 連接 TWCA 網站(1)

連接至本公司首頁 <https://www.twca.com.tw>

點選 **憑證服務**，點選 **SSL 憑證**。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.4.2 連接 TWCA 網站(2)

點選 **申請憑證**。

※如申請 EV SSL 伺服器憑證，請點選 **EV SSL 憑證**。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.4.3 連接 TWCA 網站(3)

將瀏覽器視窗畫面往下拉，上傳 CSR。

**3 上傳 CSR (WEB)**

上傳憑證請求檔(CSR)

請依據適用之『憑證操作手冊』產生憑證請求檔(CSR)，手冊取得請來電02-2370-8886#9 洽詢。

**產生憑證請求檔(CSR)後**

請將CSR以純文字的方式儲存成為檔案（建議檔案名稱為Certreq.txt）後，請以純ASCII的文字編輯器（如記事本）來開啟此檔。注意不要使用文書處理軟體（如WORD）開啟，因為它們會額外插入文字的格式指令及控制字元。

- 傳送憑證申請檔 (CSR)

以下為CSR檔案的內容範例： ——BEGIN NEW CERTIFICATE REQUEST——  
MIIBJDCBzwIBADBqMQswCQYDVQQGEwJUVzEPMA0GA1U  
ECBGMGVEFJV0FOMQ8wDQYDVQQHEwZUQU4xXjAMB  
gNVBfweFg,uhYUGJ84DWgbyGYGVVQLEwJJVDEcMBoGA1U  
EAXMTbGFIMzAwLnRhaWNhLmNvbS50dzBcMA0GCsqGSib3D  
QEBAQUAA0AMEgCQQDYdmR9MVXzUCIzOE6wW0ggZRpZ  
giJfHCa2diLHQq69SMUmLXNdnVQnl4pkgPo1qNvKv0TKR7tac  
LnfmWxuUHUHUulihihiluHLUIHULHhkiG9w0BAQQFAANBAIIG  
5vczs+LzMP1c1ybwTE4784HIZUbibZhXNg6L90H09CIHpDXD  
duwd01q42V5xCmasPCImkIri1TX4BYr5qzY= ——END NEW CERTIFICATE REQUEST——

請將CSR檔案中的內容複製到下方的空欄中，注意複製的範圍應包括「-----BEGIN NEW CERTIFICATE REQUEST-----」到「-----END NEW CERTIFICATE REQUEST-----」的宣告文字。

## 5.4.4 貼上憑證請求檔

開啟在 5.3 章節產生的憑證請求檔，利用 **全選後複製貼上**的方式(CSR 檔案內容包含-----BEGIN CERTIFICATE REQUEST-----、-----END CERTIFICATE REQUEST-----)，將製作好之憑證請求檔（CSR）內容貼到申請欄位中→選擇**繼續**。

- 傳送憑證申請檔 (CSR)

以下為CSR檔案的內容範例： ——BEGIN NEW CERTIFICATE REQUEST——  
MIIBJDCBzwIBADBqMQswCQYDVQQGEwJUVzEPMA0GA1U  
ECBGMGVEFJV0FOMQ8wDQYDVQQHEwZUQU4xXjAMB  
gNVBfweFg,uhYUGJ84DWgbyGYGVVQLEwJJVDEcMBoGA1U  
EAXMTbGFIMzAwLnRhaWNhLmNvbS50dzBcMA0GCsqGSib3D  
QEBAQUAA0AMEgCQQDYdmR9MVXzUCIzOE6wW0ggZRpZ  
giJfHCa2diLHQq69SMUmLXNdnVQnl4pkgPo1qNvKv0TKR7tac  
LnfmWxuUHUHUulihihiluHLUIHULHhkiG9w0BAQQFAANBAIIG  
5vczs+LzMP1c1ybwTE4784HIZUbibZhXNg6L90H09CIHpDXD  
duwd01q42V5xCmasPCImkIri1TX4BYr5qzY= ——END NEW CERTIFICATE REQUEST——

請將CSR檔案中的內容複製到下方的空欄中，注意複製的範圍應包括「-----BEGIN NEW CERTIFICATE REQUEST-----」到「-----END NEW CERTIFICATE REQUEST-----」的宣告文字。

-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIBJDCBzwIBADBqMQswCQYDVQQGEwJUVzEPMA0GA1U  
ECBGMGVEFJV0FOMQ8wDQYDVQQHEwZUQU4xXjAMB  
gNVBfweFg,uhYUGJ84DWgbyGYGVVQLEwJJVDEcMBoGA1U  
EAXMTbGFIMzAwLnRhaWNhLmNvbS50dzBcMA0GCsqGSib3D  
QEBAQUAA0AMEgCQQDYdmR9MVXzUCIzOE6wW0ggZRpZ  
giJfHCa2diLHQq69SMUmLXNdnVQnl4pkgPo1qNvKv0TKR7tac  
LnfmWxuUHUHUulihihiluHLUIHULHhkiG9w0BAQQFAANBAIIG  
5vczs+LzMP1c1ybwTE4784HIZUbibZhXNg6L90H09CIHpDXD  
duwd01q42V5xCmasPCImkIri1TX4BYr5qzY= ——END NEW CERTIFICATE REQUEST-----

請按一下「繼續」按鈕以便送出CSR，並繼續註冊程序。

**繼續** 重設

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.4.5 再次檢視上傳之憑證請求檔案內容



## 5.4.6 設定通行密碼及選擇身分審驗方式

5.4.6.1 請自行設定通行密碼,該密碼請牢記,如您需要廢止憑證時,必須輸入此通行密碼。

請輸入通行密碼

通行密碼 此密碼是廢止憑證所需, 請務必記得, 並儲存在安全的地方	建立通行密碼 <input type="password"/>
--------------------------------------	------------------------------------

5.4.6.2 為符合 SSL 憑證國際審放標準, 將審驗網域所有權者請您選擇以下一種審驗方式:

**一、EMAIL 驗證**: 將會自動帶出網域註冊之 EMAIL 或者請選擇

admin@網域、administrator@網域、webmaster@網域、hostmaster@網域、postmaster@網域此六個 EMAIL 任一個 EMAIL 皆可進行身分驗證作業, 選擇送出後系統將會寄出驗證信, 請務必至該信箱完成驗證作業

**二、檔案驗證**: 請您填入收取該檔案收件人 EMAIL, 您將在此 EMAIL 收到一附件檔案, 請您依照信件說明將檔案放入, 完成後請通知我們進行檔案驗證作業。

**三、電話驗證**: 網域所有權人的資料可公開查詢到才能使用電話驗證, 請您選擇進行電話驗證的時段, 我們將依照您所選擇的去電驗證。

本資料為臺灣網路認證股份有限公司專有之財產, 非經書面許可, 不准透露或使用本資料, 亦不准複印, 複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 網域所有權

為符合SSL憑證國際審放標準，將審驗網域所有權請您選擇以下一種審驗方式。

網域所有權EMAIL驗證：點選確認後，系統將會自動寄出驗證信，請用戶務必至該信箱收信並點擊確認即可。

maintain@twca.com.tw (網域註冊資料來源由WHOIS取得)

或請選擇

admin@twca.com.tw

administrator@twca.com.tw

webmaster@twca.com.tw

hostmaster@twca.com.tw

postmaster@twca.com.tw

---

網站檔案驗證：(Whois資料設定為不揭露)

請您填入接收電子信箱：，將郵寄檔案及說明給您。

---

電話驗證：我們將以電話驗證方式確認網域所有權

請您留下方便聯絡的時間： 皆可  上午時段  下午時段

5.4.6.3 填寫表單編號，並確認以上表單內容輸入正確後，按繼續送出申請。

確認以上所輸入的資料正確後，請輸入表單編號，按“繼續”送出申請

表單編號 請輸入憑證申請單 <b>右上角</b> 的表單編號	<input type="text"/> 若未填過憑證申請單，請線上登打 <a href="#">憑證表單線上作業輸入</a>
請按一下“繼續”按鈕以送出註冊資料，完成註冊程序。	<input type="button" value="繼續"/>

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

### 5.4.7 送出後等待 CA 系統簽發憑證

CSR 上傳完成後，近日會完成驗證(以下畫面為選擇電話驗證的顯示結果)，憑證簽發後會以 Email 通知業務及技術聯絡人(TWCA SSL 伺服器數位憑證下載通知)，憑證亦可以在 TWCA 網站搜尋及下載。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.



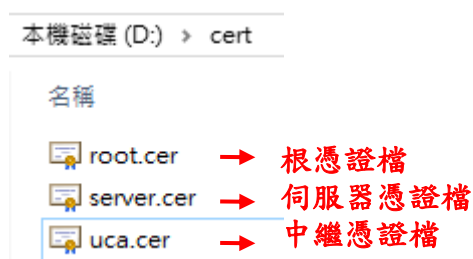
## 5.5 下載已核發憑證

### 1 相關檔案說明

若上傳之 CSR 及相關聯絡資料經審驗通過，將會寄送「SSL 伺服器數位憑證下載通知」電子郵件給相關聯絡人，郵件內容包含附件憑證鏈壓縮檔 (cert.zip) 及 TWCA SSL 動態認證標章之安裝說明與標章圖檔連結。

將附件憑證鏈壓縮檔 cert.zip 解壓縮後，可得到三個憑證鏈檔。

※內容及憑證用途如下圖所式：



### 2 檔案下載說明

如果因為貴公司之 mail server 設定，導致無法順利取得附件憑證鏈壓縮檔案，請依照下列步驟，利用本公司網站 [憑證搜尋](#) 功能，下載憑證鏈壓縮檔。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

### 5.5.1 連接 TWCA 網站(1)

連接至本公司首頁 <https://www.twca.com.tw>

點選 **憑證服務**，點選 **SSL 憑證**。



### 5.5.2 連接 TWCA 網站(2)

點選 **憑證搜尋**。

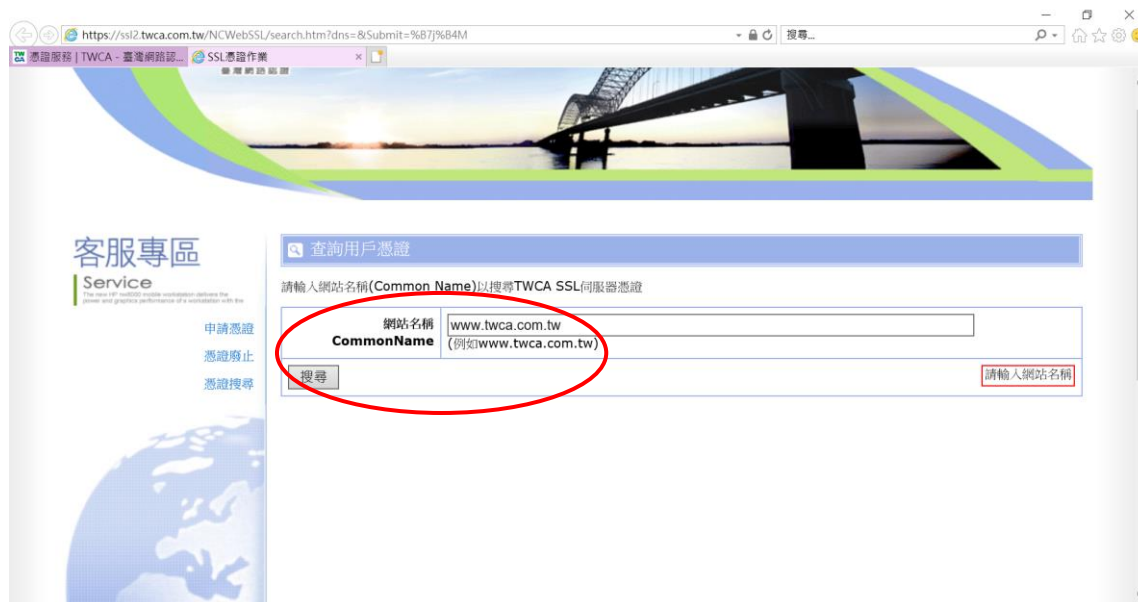


本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

### 5.5.3 輸入申請之網站名稱

在**網站名稱**中輸入憑證申請單上填寫之**網站名稱(Common Name)**，如  
**www.twca.com.tw** (注意，大小寫需一致，不必加 **http://**或 **https://**)，輸  
入完成後，按下**搜尋**鍵。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

### 5.5.4 下載憑證鏈壓縮檔

確認憑證相關資訊與申請相符後點選「下載」→「憑證鏈」，另開檔案下載視窗，按下「另存新檔」，儲存憑證鏈壓縮檔 cert.zip。



## 5.6 安裝憑證

### 5.6.1 Apache 在安裝 SSL 憑證時會使用到三種檔案：

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

- 於 5.2 章節產製的 SSL 伺服器金鑰「server.key」
- 於 5.5 章節取得的伺服器憑證檔「server.cer」
- 於 5.5 章節取得的中繼憑證檔「uca.cer」

先備妥並將其存放至%Apache2.2%\conf 目錄下(實際目錄可自行決定)。

## 5.6.2 編輯%Apache2.2%\conf\extra 目錄下的 httpd-ssl.conf 檔案

### 5.6.2.1 安裝伺服器憑證

搜尋「SSLCertificateFile」字串，可找到其中的 SSLCertificateFile 設定，此設定是 SSL 伺服器憑證存放完整路徑，請依 5.6.1 章節檔案存放路徑設定，路徑前後請用「”」包起來。

```
httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.cer"
```

### 5.6.2.2 安裝 SSL 伺服器金鑰

搜尋「SSLCertificateKeyFile」字串，可找到其中的 SSLCertificateKeyFile 設定，此設定是 SSL 伺服器金鑰存放完整路徑，請依 5.6.1 章節檔案存放路徑設定，路徑前後請用「”」包起來。

```
httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server.key"
```

### 5.6.2.3 安裝中繼憑證

搜尋「SSLCertificateChainFile」字串，可找到其中的 SSLCertificateChainFile 設定，此設定是中繼憑證存放完整路徑，請依 5.6.1 章節檔案存放路徑設定，路徑前後請用「”」包起來。

```
httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
SSLCertificateChainFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/uca.cer"
```

完成「httpd-ssl.conf」內上述設定後儲存檔案，即完成憑證安裝。

### 5.6.3 重新啟動 Apache 服務

重新啟動完成即可進入 5.8 節，驗證 SSL 功能。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.7 設定 SSL 模式

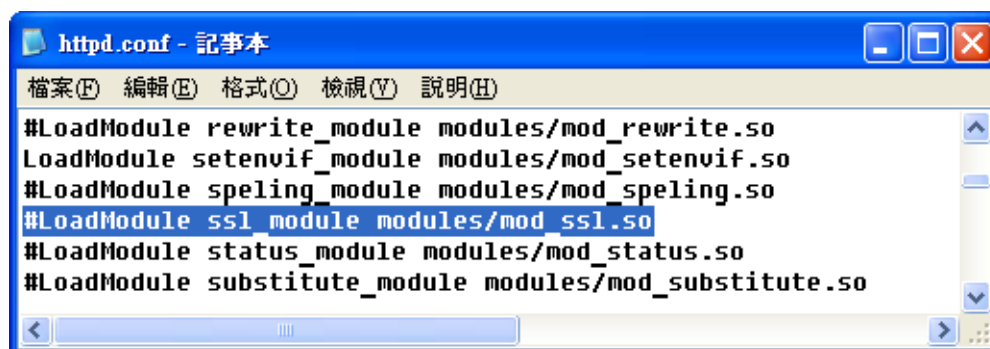
※若安裝主機非首次申請 SSL 憑證，SSL 功能正常，此章節可跳過不必設定！

### 5.7.1 編輯%Apache2.2%\conf 目錄下的 httpd.conf 檔案

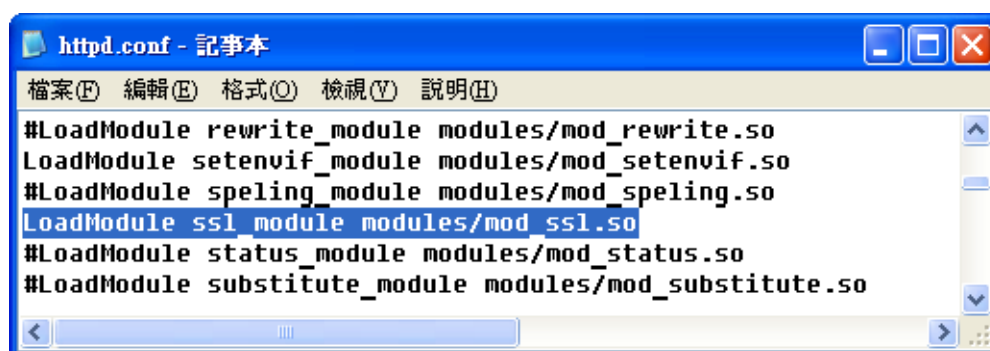
#### 5.7.1.1 載入 SSL 模組

搜尋「mod\_ssl.so」字串，可找到其中的

LoadModule ssl\_module modules/mod\_ssl.so 指令，如果指令前有#字號，請將該指令前的#字號移除。



```
httpd.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
```



```
httpd.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
#LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
#LoadModule speling_module modules/mod_speling.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule status_module modules/mod_status.so
#LoadModule substitute_module modules/mod_substitute.so
```

## 5.7.1.2 載入額外的設定檔 httpd-ssl.conf

搜尋 httpd-ssl.conf (httpd-ssl.conf 設定檔是負責 SSL 的相關設定)，可找到其中的 Include conf/extra/httpd-ssl.conf 指令，如果指令前有 # 字號，請將該指令前的 # 字號移除。



```
httpd.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
#Include conf/extra/httpd-default.conf
# Secure (SSL/TLS) connections
#Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
```



```
httpd.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
#Include conf/extra/httpd-default.conf
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
```

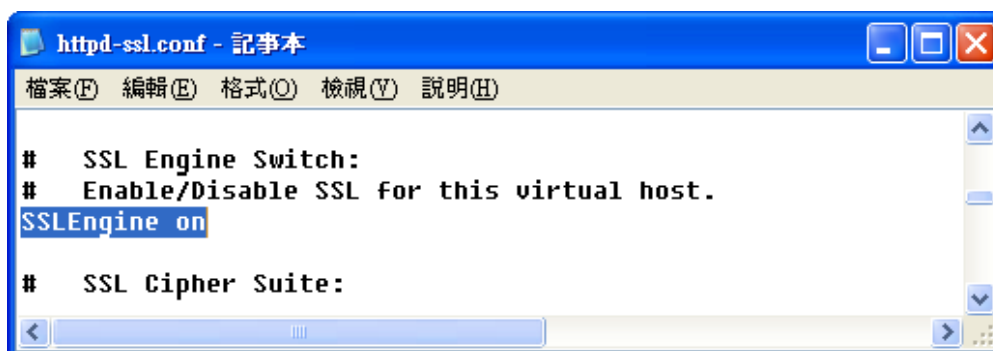
確認完 httpd.conf 內上述兩項設定後儲存檔案。



## 5.7.2 編輯%Apache2.2%\conf\extra 目錄下的 httpd-ssl.conf 檔案

### 5.7.2.1 啟用 SSL 功能

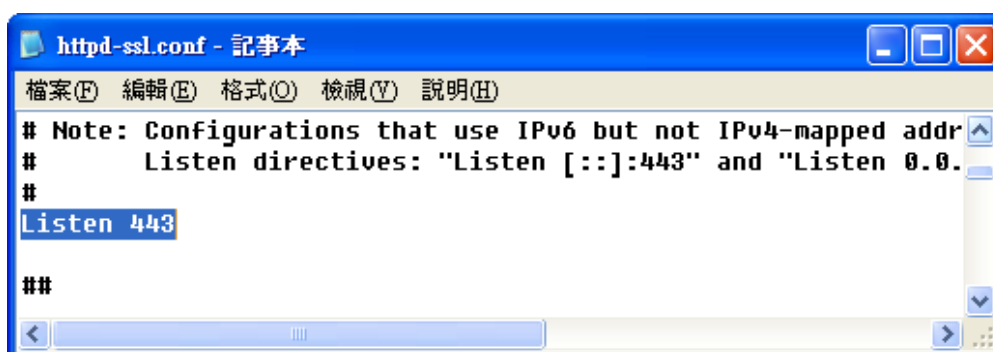
搜尋「SSLEngine」字串，可找到其中的指令 SSLEngine on / off，SSLEngine on 表示啟用 SSL 功能，如果不啟用 SSL 就將 on 改為 off 即可，這裡請設定為 on。



```
httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
# SSL Cipher Suite:
```

### 5.7.2.2 設定 SSL 連接埠

搜尋「Listen」字串，可找到其中的指令 Listen 443，443 Port 是 SSL(https)功能的預設 Port，如果要設定為其他 Port 再修改設定，否則一律設定為 443 即可。

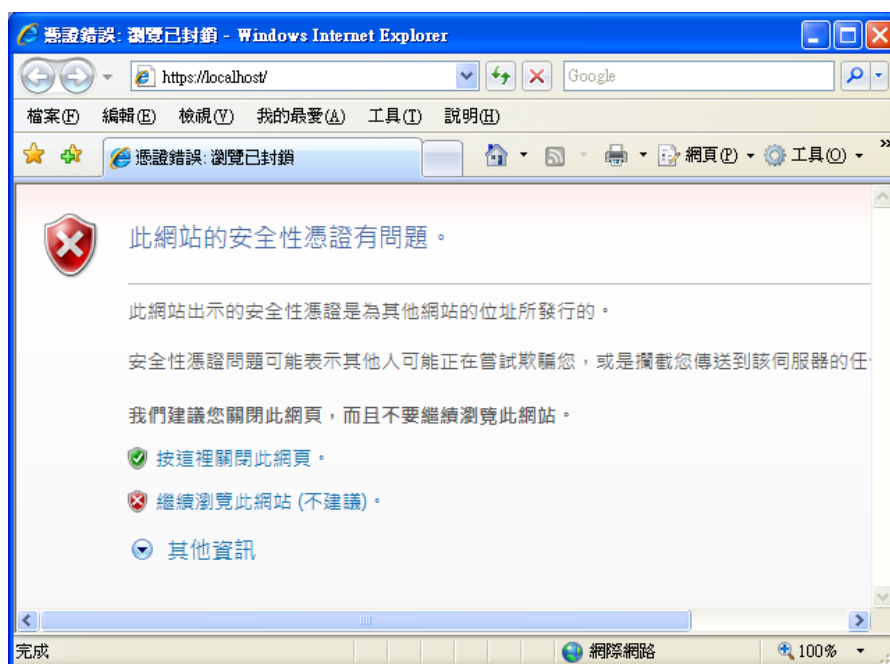


```
httpd-ssl.conf - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
# Note: Configurations that use IPv6 but not IPv4-mapped addr
# Listen directives: "Listen [::]:443" and "Listen 0.0.
#
Listen 443
###
```

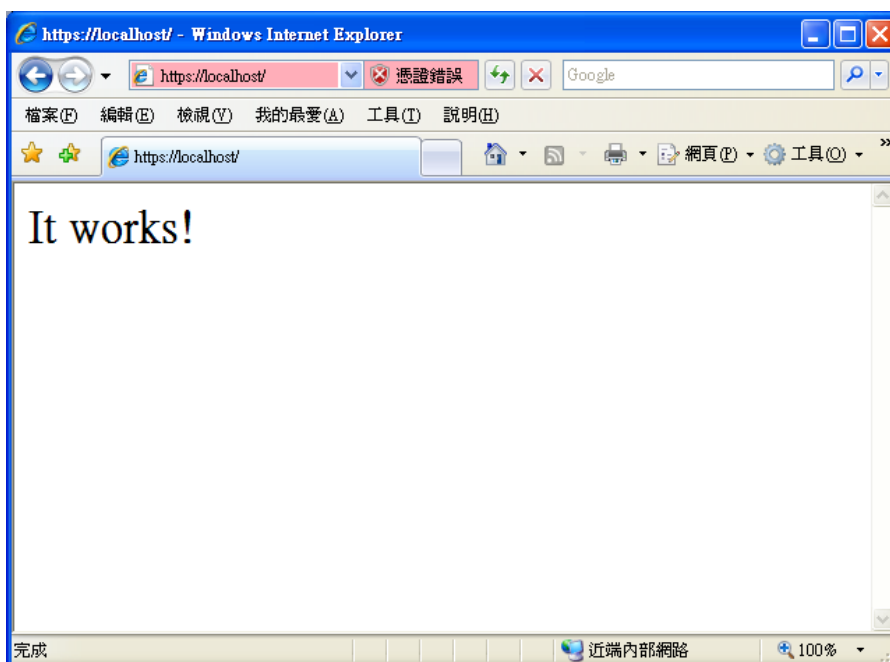
## 5.8 驗證 SSL 功能

### 5.8.1 本機驗證

Apache 重新啟動完成後開啟瀏覽器直接連接至本機 <https://localhost>，此時出現警告訊息是正常的，因為憑證記載內容與網址不符 (非 localhost)，請點選「繼續瀏覽此網站(不建議)」即可。



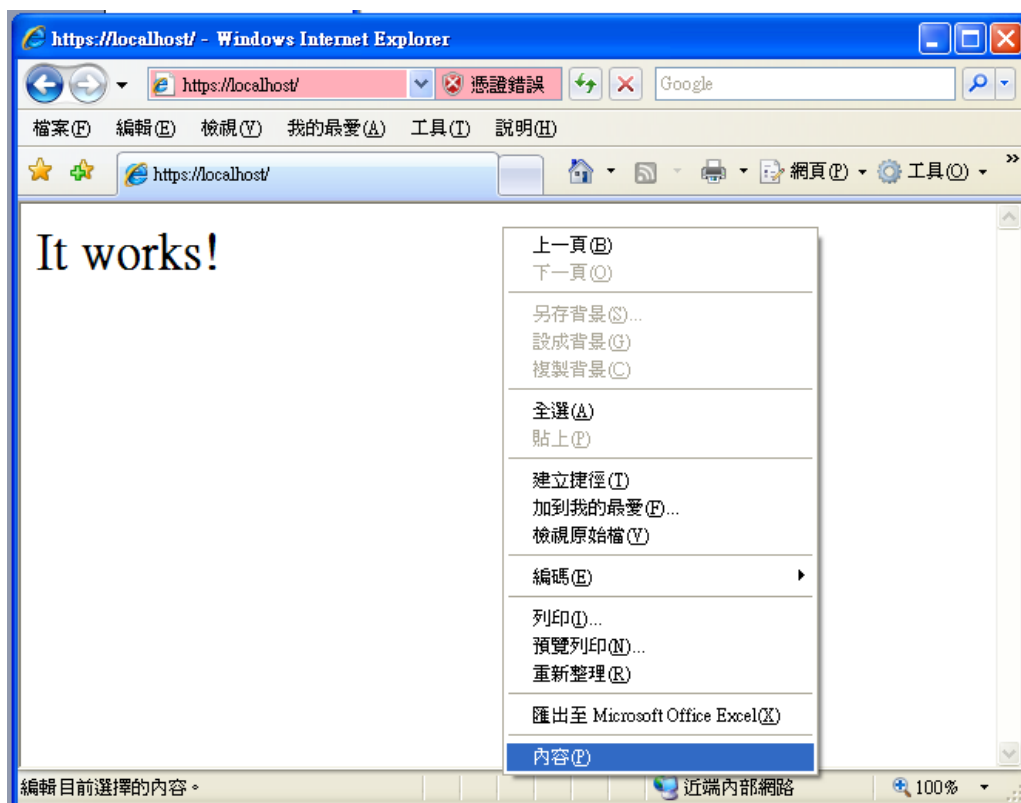
如果瀏覽器出現 It Works! 字樣代表 Apache 已正常服務，且 SSL 功能已啟用。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

在瀏覽器按滑鼠右鍵出現功能清單，點選「內容」，



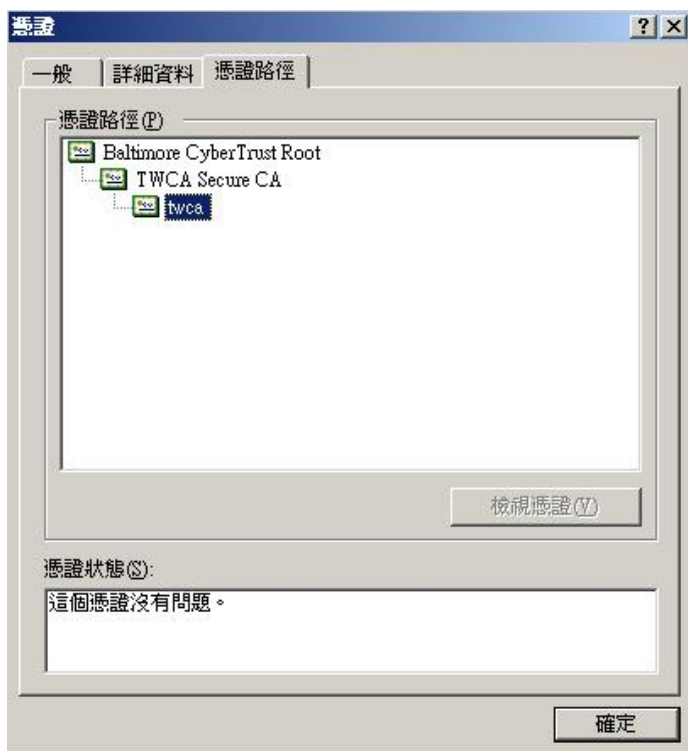
此時會出現網頁資訊，確認網頁是否已加密，點選「憑證」可檢視憑證資訊



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

**憑證路徑**欄位：請確認憑證鏈是否正確，且**憑證狀態**顯示**這個憑證沒有問題**，可確認憑證已安裝成功。



本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.8.2 外部驗證

驗證程序和 5.8.1 節相同，只是連線位址改為實際網址，

如 <https://www.twca.com.tw>



## 5.8.3 為何連線位址正確卻無法顯示網頁？

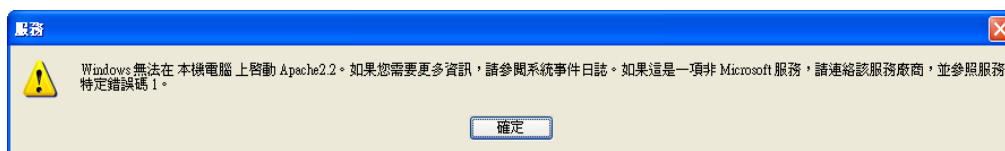
https 連線埠預設使用 443 Port，如果 5.7.7.2 節設定 Listen Port 非 443，則連線時須指定連線 Port，如 <https://www.twca.com.tw:8443>

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.9 異常排除

如果完成 5.6 及 5.7 章節設定後，重新啟動 Apache 時出現下面的錯誤訊息，表示 SSL 設定有誤，請檢視%Apache2.2%\logs\error.log 檔，該檔案內會記錄啟動失敗原因，待問題排除後再重新啟動。  
如果持續發生問題，請聯絡本公司協助處理。



### 5.10 備份／復原憑證

請將 5.6.1 章節指定的三個檔案備份起來(金鑰、伺服器憑證、中繼憑證)，再依照 5.6 章節的步驟設定，即可復原憑證。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 5.11 更新 SSL 憑證

### 5.11.1 申請說明

臺灣網路認證公司會在 SSL 伺服器憑證到期前二個月發出憑證更新通知信給 貴公司。這二個月內您隨時可以至本公司網站 <https://www.twca.com.tw> 下載申請表單，填寫完畢後寄回臺灣網路認證公司，即可進行 SSL 憑證更新申請。

### 5.11.2 更新步驟

#### 5.11.2.1 備份憑證檔

在進行更新前請記得備份原有的 SSL 伺服器憑證及伺服器金鑰。

#### 5.11.2.2 更新憑證

若安裝主機(站台)非首次申請 SSL 憑證，SSL 功能正常，請參照 5.2 至 5.6 章節申請安裝憑證，即可完成 SSL 憑證更新。



## 6. 常見問題

6.1 請參閱 [https://www.twca.com.tw/picture/file/SSL 常見技術問題手冊.pdf](https://www.twca.com.tw/picture/file/SSL常見技術問題手冊.pdf)。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.

## 7. 附件

無。

本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

The information contained herein is the exclusive property of TWCA and shall not be distributed, reproduced, or disclosed in whole or in part without prior written permission of TWCA.