

SSL 伺服器數位憑證 Apache2.4 伺服器操作手冊(適用於 UNIX)

機密等級：公開

版本：V5.1

文件編號：MNT-03-110

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

目 錄

1.目的	1
2.範圍	2
3.參考資料	3
4.定義	4
5.作業程序	5
5.1 前置作業.....	5
5.2 產製「金鑰」.....	9
5.3 產生「憑證請求檔(CSR)」	10
5.4 將製作好的憑證請求檔(CSR)上傳	12
5.5 下載已核發憑證.....	18
5.6 設定 SSL 模式.....	22
5.7 安裝憑證.....	25
5.8 驗證 SSL 功能.....	27
5.9 異常排除.....	31
5.10 備份／還原憑證.....	32
5.11 更新 SSL 憑證.....	33
6.常見問題	34
7.附件	35

1.目的

- 1.1. 介紹 Apache2.4(適用於 UNIX 環境)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

本操作手冊以 CentOS(Version 5.8-i386)的 Linux 作業系統為範例。

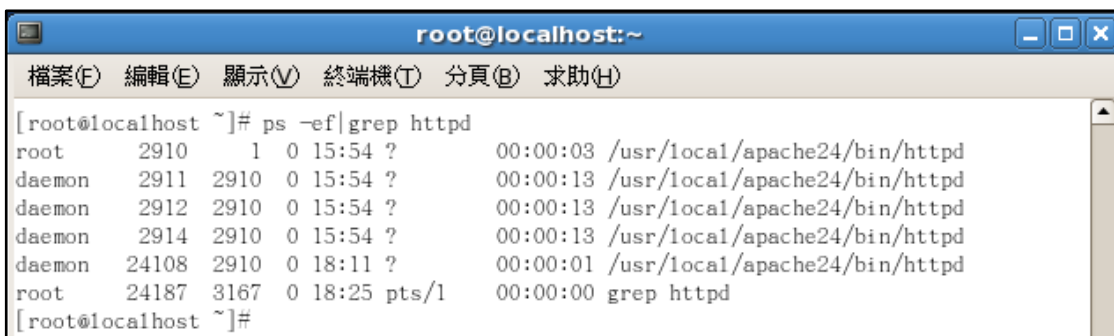
5.1.1 確認 Apache 是否安裝，並查詢 Apache 設定檔路徑

Apache 2.4 Web 伺服器軟體是由 Apache 組織所提供的 Web 伺服器軟體，可執行下列指令確認伺服器主機的 Apache 環境現況：

1. 確認 Apache 是否於作業系統執行緒中，可執行下列指令：

```
ps -ef |grep httpd
```

同時亦可確定 Apache 之安裝路徑。(備註：以下 Apache 路徑以 `/usr/local/apache24/` 為例)。



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# ps -ef|grep httpd  
root      2910      1  0 15:54 ?        00:00:03 /usr/local/apache24/bin/httpd  
daemon    2911    2910  0 15:54 ?        00:00:13 /usr/local/apache24/bin/httpd  
daemon    2912    2910  0 15:54 ?        00:00:13 /usr/local/apache24/bin/httpd  
daemon    2914    2910  0 15:54 ?        00:00:13 /usr/local/apache24/bin/httpd  
daemon   24108    2910  0 18:11 ?        00:00:01 /usr/local/apache24/bin/httpd  
root     24187    3167  0 18:25 pts/1    00:00:00 grep httpd  
[root@localhost ~]#
```

2. 查詢 Apache 套件版本，可執行下列指令：

```
/usr/local/apache24/bin/apachectl -v
```

以下圖為例，版本為 Apache 2.5.6(UNIX)。(備註：Apache 2 或更早之版本，SSL 之設定檔為 `ssl.conf`；Apache 2.2、Apache 2.4 版本，SSL 之設定檔為 `httpd-ssl.conf`)



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# /usr/local/apache24/bin/apachectl -v  
Server version: Apache/2.4.6 (Unix)  
Server built:   Sep 20 2013 17:34:31  
[root@localhost ~]#
```

3. 確認 Apache 設定檔路徑，可執行下列指令：

find / -name httpd.conf



```
root@localhost:~  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# find / -name httpd.conf  
/root/httpd-2.4.6/docs/conf/httpd.conf  
/usr/local/apache24/conf/original/httpd.conf  
/usr/local/apache24/conf/httpd.conf  
[root@localhost ~]#
```

4. 建立存放憑證鏈之目錄(SSL_Certs)，可執行下列指令：

mkdir SSL_Certs

新增一存放憑證鏈相關檔案之目錄，供日後憑證管理使用。(備註：
以下憑證鏈存放路徑以/usr/local/apache24/SSL_Certs 為例)



```
root@localhost:/usr/local/apache24  
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)  
[root@localhost ~]# cd /usr/local/apache24/  
[root@localhost apache24]# ls  
bin build cgi-bin conf error htdocs icons include logs man manual modules  
[root@localhost apache24]# mkdir SSL_Certs  
[root@localhost apache24]# ls  
bin cgi-bin error icons logs manual SSL_Certs  
build conf htdocs include man modules  
[root@localhost apache24]#
```

5.1.2 安裝 OpenSSL 軟體

Apache 需搭配 OpenSSL 軟體來產製金鑰，可執行下列指令確認伺服器主機是否支援 OpenSSL，可執行下列指令：

yum install mod_ssl openssl

1. 若伺服器主機不支援 OpenSSL，Linux 將下載最新版本的 OpenSSL，更新完成後會顯示更新項目清單與 **Complete!**。


```

root@localhost:~
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
[root@localhost ~]# yum install mod_ssl openssl
Loaded plugins: fastestmirror, security
Loading mirror speeds from cached hostfile
 * base: ftp.cs.pu.edu.tw
 * extras: ftp.cs.pu.edu.tw
 * updates: ftp.cs.pu.edu.tw
Setting up Install Process
Package openssl-0.9.8e-26.el5_9.1.i686 already installed and latest version
Resolving Dependencies
--> Running transaction check
--> Package mod_ssl.i386 1:2.2.3-82.el5.centos set to be updated
--> Processing Dependency: libdistcache.so.1 for package: mod_ssl
--> Processing Dependency: libnsl.so.1 for package: mod_ssl
--> Running transaction check
--> Package distcache.i386 0:1.4.5-14.1 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch          Version                Repository            Size
=====
Installing:
mod_ssl                 i386          1:2.2.3-82.el5.centos updates               97 k
Installing for dependencies:
distcache               i386          1.4.5-14.1             base                  119 k
=====

Transaction Summary
=====

```

```

root@localhost:~
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
distcache             i386          1.4.5-14.1             base                  119 k
=====
Transaction Summary
=====
Install      2 Package(s)
Upgrade     0 Package(s)

Total download size: 215 k
Is this ok [y/N]: y
Downloading Packages:
(1/2): mod_ssl-2.2.3-82.el5.centos.i386.rpm | 97 kB 00:00
(2/2): distcache-1.4.5-14.1.i386.rpm       | 119 kB 00:00
-----
Total                                           417 kB/s | 215 kB 00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing      : distcache                               1/2
  Installing      : mod_ssl                               2/2

Installed:
  mod_ssl.i386 1:2.2.3-82.el5.centos

Dependency Installed:
  distcache.i386 0:1.4.5-14.1

Complete!

```

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. 若伺服器主機已有最新版本的 OpenSSL，檢測之 package 為最新版本，且會顯示 **Nothing to do**。

```
[root@localhost ~]# yum install mod_ssl openssl
Loaded plugins: fastestmirror, security
Loading mirror speeds from cached hostfile
* base: ftp.cs.pu.edu.tw
* extras: ftp.cs.pu.edu.tw
* updates: ftp.cs.pu.edu.tw
Setting up Install Process
Package 1:mod_ssl-2.2.3-82.el5.centos.i386 already installed and latest version
Package openssl-0.9.8e-26.el5_9.1.i686 already installed and latest version
Nothing to do
```

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.

5.2 產製「金鑰」

5.2.1 執行下列指令

```
openssl genrsa -out /usr/local/apache24/SSL_Certs/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)

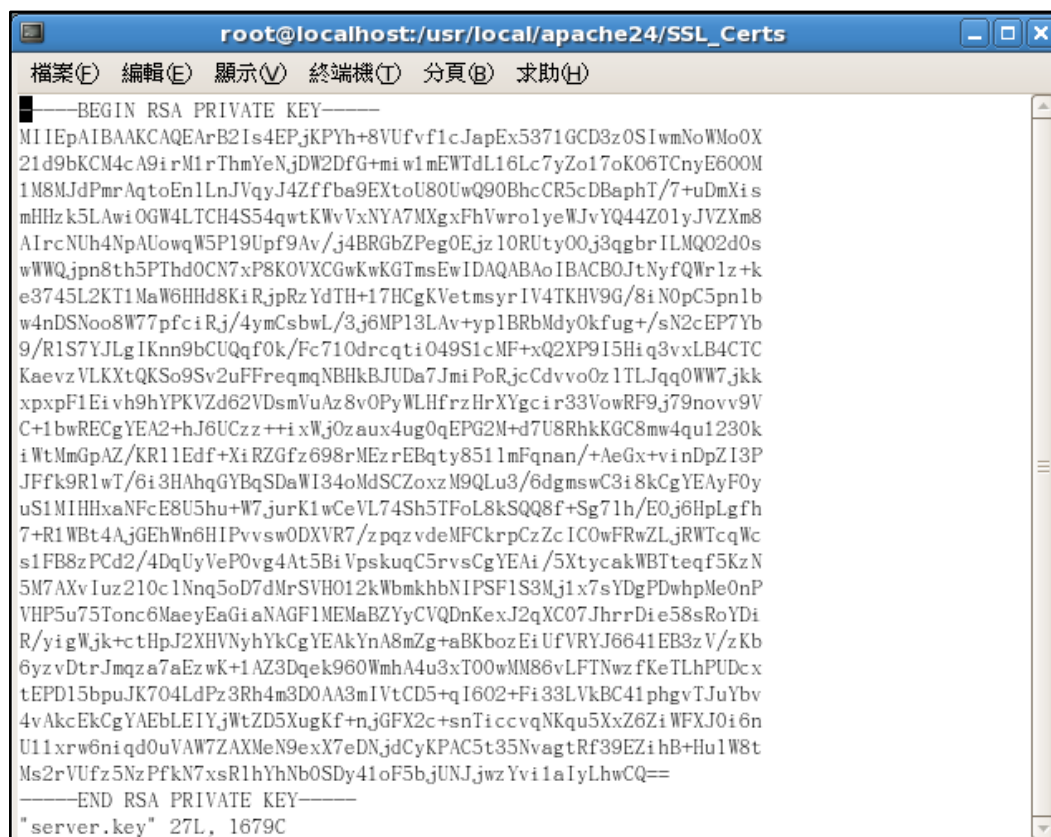


```

root@localhost:~
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
[root@localhost ~]# openssl genrsa -out /usr/local/apache24/SSL_Certs/server.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
[root@localhost ~]#

```

完成上列指令後會在 `/usr/local/apache24/SSL_Certs` 目錄下產生檔案名稱為 `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



```

root@localhost:/usr/local/apache24/SSL_Certs
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEArB2Is4EPjKPYh+8VUfvf1cJapEx5371GCD8z0SIwmNoWm0X
21d9bKCM4cA9i rM1rThmYeNjDW2DFG+mi w1mEWTdL16Lc7yZo17oK06TCnyE600M
1M8MJdPmrAqtoEnlLnJVqyJ4Zffba9EXtoU80UwQ90BhcCR5cDBaphT/7+uDmXi s
mHHzk5LAWiOGW4LTCH4S54qwtKWvVxNYA7MXgxFhVwrolyeWJvYQ44Z01yJVZXm8
A1rcNUh4NpAUowqW5P19Upf9Av/j4BRGbzPeg0Ejz10RUty00j3qgbrILMQ02d0s
wWWQjpn8th5PThdOCN7xP8KOVXC6wKwKGtmsEwIDAQABoIBACB0JtNyfQWr1z+k
e3745L2KT1MaW6HHd8KiRjprZyDTH+17HCgKVetmsyrIV4TKHV9G/8iN0pC5pn1b
w4nDSNoo8W77pfc1Rj/4ymCsbwL/3j6MP13LAv+yplBRbMdyOkfug+/sN2cEP7Yb
9/R1S7YJLgIKnn9bCUQqf0k/Fc710drcqt1049S1cMF+xQ2XP9I5Hiq3vxLB4CTC
KaevzVLKXtQKSo9Sv2uFFreqmqNBHkBJUDa7JmiPoRjCdvvo0z1TLJqq0WW7jkk
xpxpF1Ei v h9hYPKVZd62VDsmVuAz8v0PyWLHfrzHrXYgci r33VowRF9j79novv9V
C+1bwRECgYEA2+hJ6UCzz++i xWjOzaux4ug0qEPG2M+d7U8RhkKGC8mw4qu1230k
iWtMmGpAZ/KR11Edf+XiRZGfz698rMEzrEBqty8511mFqnan/+AeGx+vinDpZ13P
JFfk9R1wT/6i3HAhqGYBqSDaWI34oMdSCZoxz M9QLu3/6dgmSwC3i8kCgYEAyF0y
uS1MIHhxaNfC8U5hu+W7jurK1wCeVL74Sh5TFoL8kSQQ8f+Sg71h/E0j6HplGfh
7+R1WBt4AjGEhWn6HIPvvsWDXVR7/zpqzvdMFCkrcpZcZcICowFRwZLjRWTcqWc
s1FB8zPCd2/4DqUyVeP0vg4At5BiVpskuqC5rvsCgYEAi/5XtycakWBTteqf5KzN
5M7AXvIuz210c1Nnq5oD7dMrSVH012kWbmkhbnIPSF1S3Mj1x7sYDgPDwhpMe0nP
VHP5u75Tonc6MaeyEaGi aNAGF1MEMaBZYyCVQDnKexJ2qXC07JhrrDie58sRoYDi
R/yigWjk+ctHpJ2XHVnyhYkCgYEAkYnA8mZg+aBKbozEiUfVRYJ6641EB3zV/zKb
6yzvDtrJmqa7aEzWk+1AZ3Dqek960WmhA4u3xT00wMM86vLFTNwzfKeTLhPUDcx
tEPD15bpuJK704LdPz3Rh4m3D0AA3mIVtCD5+q1602+Fi33LvkBC41phgvTJuYbv
4vAkcEkCgYAEbLE1YjWtZD5XugKf+njGFx2c+snTi ccvqNKqu5XxZ6zi WFXJOi6n
U11xrw6niqd0uVAW7ZAXMeN9exX7eDNjdCyKPAC5t35Nvagtrf39Ezi hB+HulW8t
Ms2rVufz5NzPfkN7xsR1hYhNb0SDy41oF5bjUNJjwzYvi1aIyLhwCQ==
-----END RSA PRIVATE KEY-----
"server.key" 27L, 1679C

```

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.

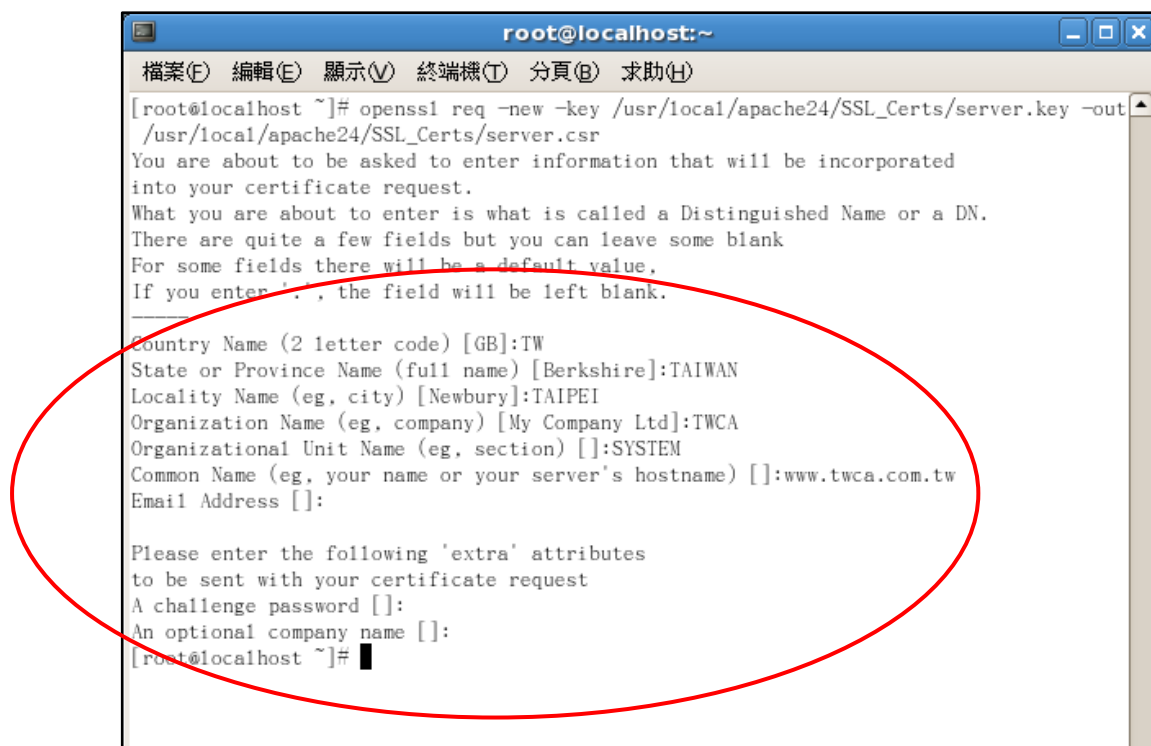
5.3 產生「憑證請求檔(CSR)」

5.3.1 執行下列指令

```
openssl req -new -key /usr/local/apache24/SSL_Certs/server.key -out
```

```
/usr/local/apache24/SSL_Certs/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)



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 ) [ GB ] : TW
```

請輸入州/省別(如 TAIWAN)，**必填**

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

請輸入所在城市(如 TAIPEI)，**必填**

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

請輸入組織名稱(如 TWCA)，**必填**

```
Organization Name ( eg, company ) [ My Company Ltd ] : TWCA
```

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.

請輸入單位名稱(如 IT、SYSTEM)，**必填**

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

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

Common Name (eg, your name or your server's hostname) []:

www.twca.com.tw

請輸入申請人員 Email，可不填

Email Address []:

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**

**Please enter the following 'extra'
to be sent with your certificaterequest
A challenge password []:
An optional company name []:**

完成上列指令後會在 **/usr/local/apache24/SSL_Certs** 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



```
root@localhost:/usr/local/apache24/SSL_Certs
-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQAwTELMAkGA1UEBhMCVFcxDzANBgNVBAgTB1RBSVdBTjEPMAG
A1UEBxMGVEFJUEVJMQ0wCwYDVQQKEwRUVONBMQ8wDQYDVQLEwZWVWVWVWVWVW
BgNVBAMTD3d3dy50d2NhLmNvbS50dzCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAKwidiLOBD4y_j21fvFVH735XCWqRMed+5Rgg989EiMJjaFjKNF9pXfWyg
jOHAPYqzJa04ZmHjYw1tg3xvposJZhFk3S5ei308maJe6Cjukwp8h0jJJJTPDCXT
5qwKraBJ9S5yVasieGX322vRF7aFPNFMEpdAYXakeXAwWqYU/+/rg514rJhx850S
wMI_jhIuCoWh+EueKsLS1r1cTWAozF4MRYVcK6NcnIib2E00GdNciVWV5vACK3DVI
eDaQFKMK1uT9fVKX/QL/4+AURm2T3oNBI89dEVLcjjo96oG6yCzEDtndLMF1k16Z
/LYeT04XdAje8T/Cj1VwhsCsChk5rBMCawEAaAAMA0GCSqGS1b3DQEBBQUAA4IB
AQAC9MzSL83v2Gjm/RWiNUAWKGOEzcfYeis3tr1PBdaJzrCBxz1008Kvni0j53og
o4GS0yILBFVkwkbPowi1EqCG7qdSDAmpmhaFQugOe6e9Ijk2YvAWjDjv8HF/RB
gu/kf/zhBSxVqJTSpgF00g/C1v1RNpXwINTy40hN0kN+Z00QG3AbFiu2kTurDi7B
3d2Vyl2AvWqVF3eDjbC6Nvn1rYv8xXPV2K29ZWSNXwuE9VQdJgvZ/meF1yJfpVW+
1SumNNdPtKby0AQJzS8+1yfmsH21LHtrEnE2ZXHjiBnSJW8U1v7SprgVdAP6Qi3
yPu4aRbOhfjFkoNwJrBBJPV3
-----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**。



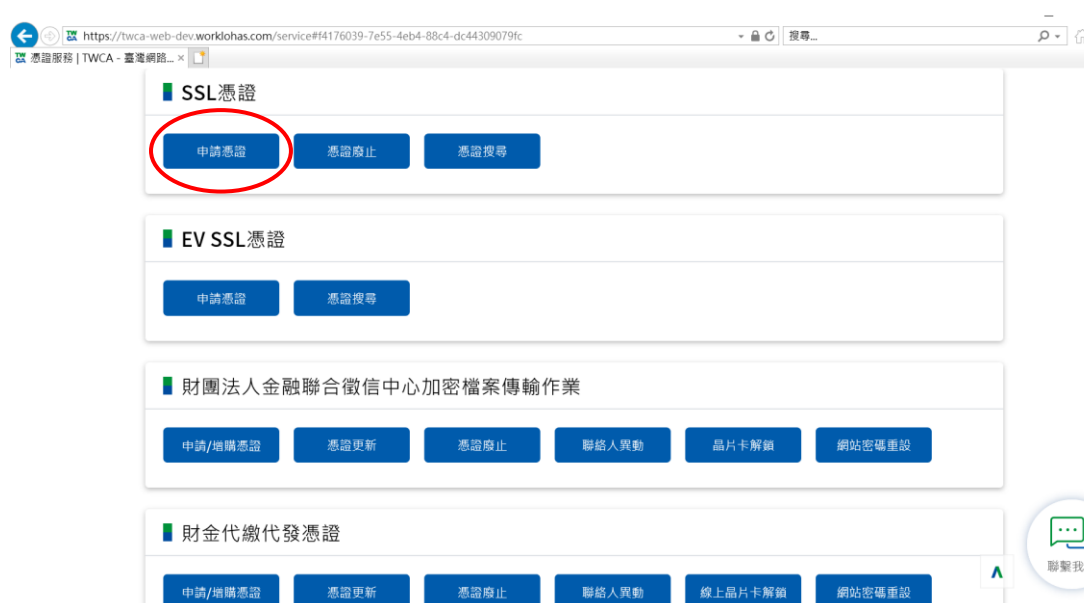
本資料為臺灣網路認證股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

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。



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**。



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

線上填寫註冊資料

保密說明
您在此頁面所輸入的所有資料，傳送呈本公司時均受SSL安全機制保護，並無外洩之虞，請放心
以下所有欄位皆為**必填**，並請注意以半形文字輸入

檢查CSR內容

解說	您的CSR內容
一般名稱：此名稱所代表的網站之安全性，將由此SSL伺服器憑證所保護	www.twca.com.tw
組織單位：這是一個可以用來區分組織部門的欄位	TWCA
組織：即 貴公司的名稱	SYSTEM
城市/位置：即 貴公司進行商業行為的所在[例：Taipei]	TAIPEI
州/省：即 貴公司進行商業行為的州/省所在地。請不要用縮寫的地名填寫此欄位[例：Taiwan]	TAIWAN
國別：此欄係以ISO組織的國家代碼來表示。舉例來說，TW代表台灣，US代表美國	TW
CSR金鑰長度(bits)	2048

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，

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.

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。

網域所有權

網域管理者	<p>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。</p> <p><input checked="" type="radio"/> 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。</p> <p><input type="radio"/> maintain@twca.com.tw (網域註冊資料來源由WHOIS取得)</p> <p>或請選擇</p> <p><input type="radio"/> admin@twca.com.tw</p> <p><input type="radio"/> administrator@twca.com.tw</p> <p><input type="radio"/> webmaster@twca.com.tw</p> <p><input type="radio"/> hostmaster@twca.com.tw</p> <p><input type="radio"/> postmaster@twca.com.tw</p>
	<p><input type="radio"/> 網站檔案驗證：(Whois資料設定為不揭露)</p> <p>請您填入接收電子信箱：<input type="text" value="maintain@twca.com.tw"/>，將郵寄檔案及說明給您。</p>
	<p><input type="radio"/> 電話驗證：我們將以電話驗證方式確認網域所有權</p> <p>請您留下方便聯絡的時間：<input checked="" type="radio"/> 皆可 <input type="radio"/> 上午時段 <input type="radio"/> 下午時段</p>

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 右上角 的表單編號	<input type="text"/> 若未填過憑證申請單，請線上登打 憑證表單線上作業輸入
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.

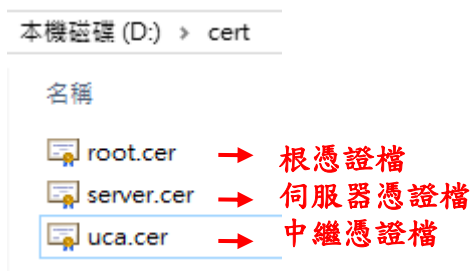
5.5 下載已核發憑證

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。



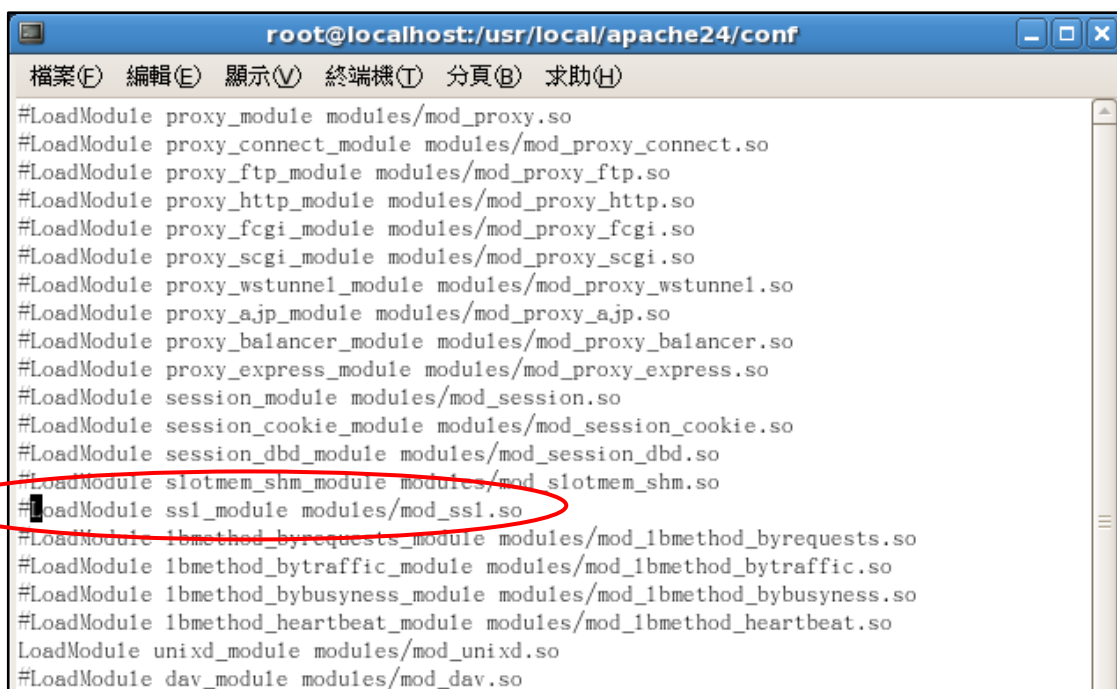
5.6 設定 SSL 模式

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

5.6.1 編輯 /usr/local/apache24/conf 目錄下的 httpd.conf 檔案

5.6.1.1 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。



```
root@localhost:/usr/local/apache24/conf
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/mod_session_cookie.so
#LoadModule session_dbd_module modules/mod_session_dbd.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule dav_module modules/mod_dav.so
```



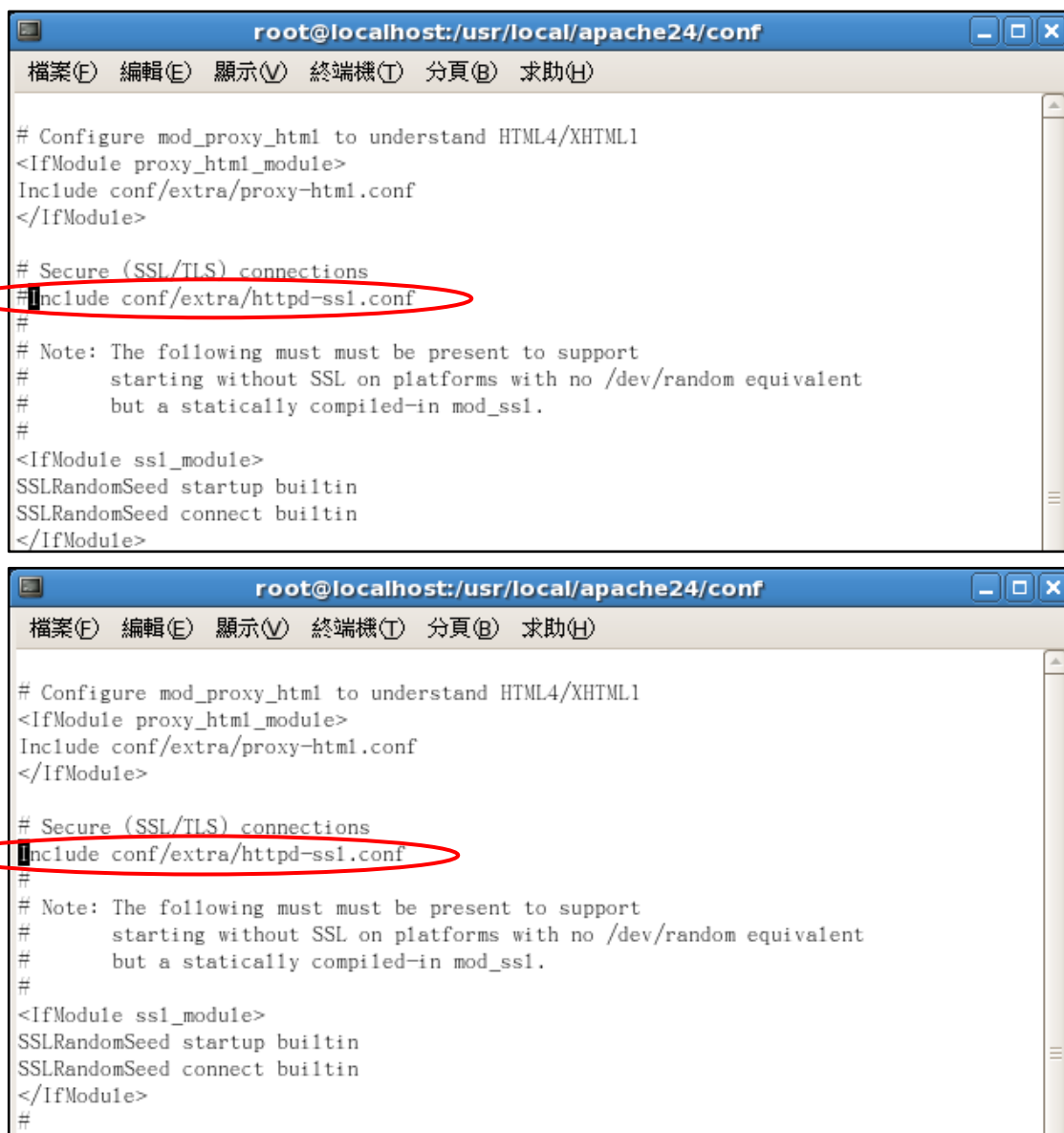
```
root@localhost:/usr/local/apache24/conf
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_connect_module modules/mod_proxy_connect.so
#LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
#LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
#LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
#LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
#LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
#LoadModule proxy_express_module modules/mod_proxy_express.so
#LoadModule session_module modules/mod_session.so
#LoadModule session_cookie_module modules/mod_session_cookie.so
#LoadModule session_dbd_module modules/mod_session_dbd.so
#LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule ssl_module modules/mod_ssl.so
#LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
#LoadModule lbmethod_bytraffic_module modules/mod_lbmethod_bytraffic.so
#LoadModule lbmethod_bybusyness_module modules/mod_lbmethod_bybusyness.so
#LoadModule lbmethod_heartbeat_module modules/mod_lbmethod_heartbeat.so
LoadModule unixd_module modules/mod_unixd.so
#LoadModule dav_module modules/mod_dav.so
LoadModule status_module modules/mod_status.so
```

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.

5.6.1.2 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。



```
root@localhost:/usr/local/apache24/conf
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>

# Secure (SSL/TLS) connections
# Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

root@localhost:/usr/local/apache24/conf
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

# Configure mod_proxy_html to understand HTML4/XHTML1
<IfModule proxy_html_module>
Include conf/extra/proxy-html.conf
</IfModule>

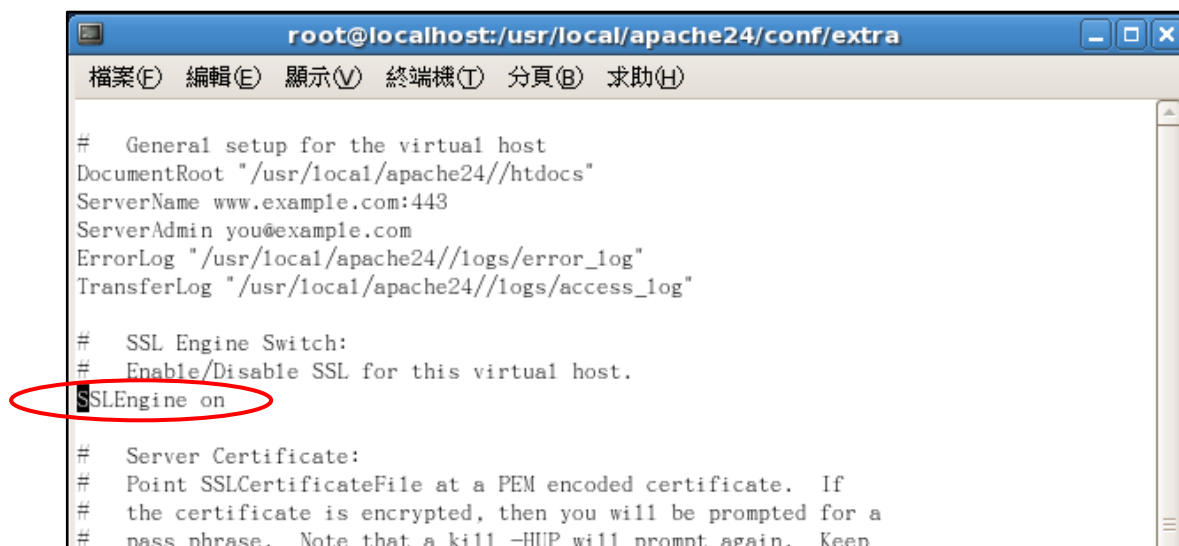
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
#
# Note: The following must must be present to support
#       starting without SSL on platforms with no /dev/random equivalent
#       but a statically compiled-in mod_ssl.
#
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>
#
```

確認完 httpd.conf 內上述兩項設定後儲存檔案。

5.6.2 編輯 `/usr/local/apache24/conf/extra` 目錄下的 `httpd-ssl.conf` 檔案

5.6.2.1 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`。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

# General setup for the virtual host
DocumentRoot "/usr/local/apache24/htdocs"
ServerName www.example.com:443
ServerAdmin you@example.com
ErrorLog "/usr/local/apache24/logs/error_log"
TransferLog "/usr/local/apache24/logs/access_log"

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# 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
```

5.6.2.2 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。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)

#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
# Note: Configurations that use IPv6 but not IPv4-mapped addresses need two
# Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
#
Listen 443

##
## SSL Global Context
##
## All SSL configuration in this context applies both to
```

5.7 安裝憑證

5.7.1 Apache 在安裝 SSL 憑證時會使用到三種檔案：

- 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 `/usr/local/apache24/SSL_Certs` 目錄下(實際目錄可自行決定)。

5.7.2 編輯 `/usr/local/apache24/conf/extra` 目錄下的 `httpd-ssl.conf` 檔案

5.7.2.1 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 5.7.1 章節檔案存放路徑設定，路徑前後請用「`"`」包起來。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(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.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "/usr/local/apache24/SSL_Certs/server.cer"
#SSLCertificateFile "/usr/local/apache24/conf/server-dsa.crt"
#SSLCertificateFile "/usr/local/apache24/conf/server-ecc.crt"
```

5.7.2.2 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 5.7.1 章節檔案存放路徑設定，路徑前後請用「`"`」包起來。



```
root@localhost:/usr/local/apache24/conf/extra
檔案(F) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(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.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "/usr/local/apache24/SSL_Certs/server.key"
#SSLCertificateKeyFile "/usr/local/apache24/conf/server-dsa.key"
#SSLCertificateKeyFile "/usr/local/apache24/conf/server-ecc.key"

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
```

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.

5.7.2.3 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 5.7.1 章節檔案存放路徑設定，路徑前後請用「"」包起來。



```
root@localhost:~/usr/local/apache24/conf/extra
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(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 "/usr/local/apache24/SSL_Certs/uca.cer"
```

完成「httpd-ssl.conf」內上述設定後儲存檔案，即完成憑證安裝。

5.7.3 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。

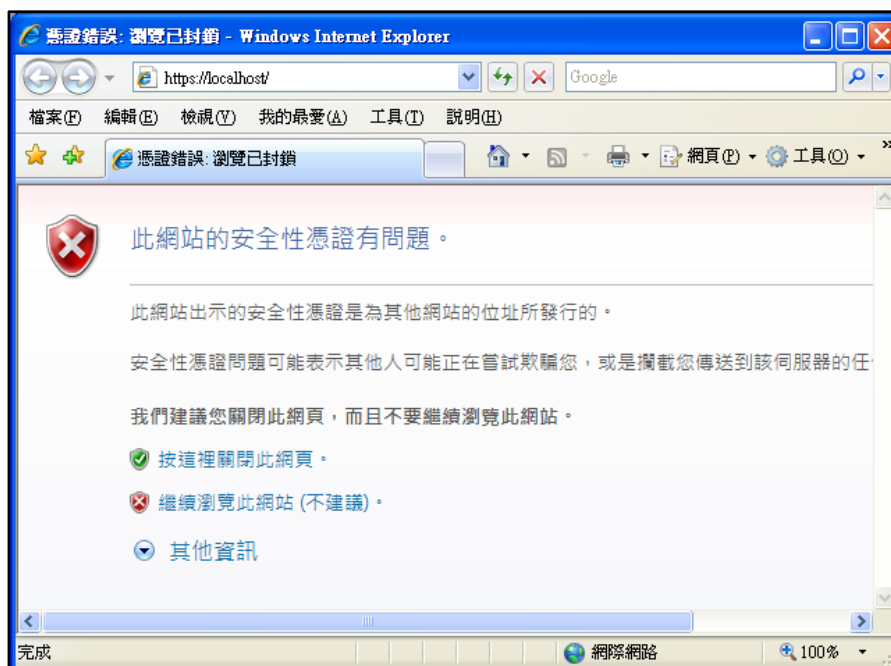


```
root@localhost:~
檔案(E) 編輯(E) 顯示(V) 終端機(T) 分頁(B) 求助(H)
[root@localhost ~]# /usr/local/apache24/bin/apachectl restart
[root@localhost ~]#
```

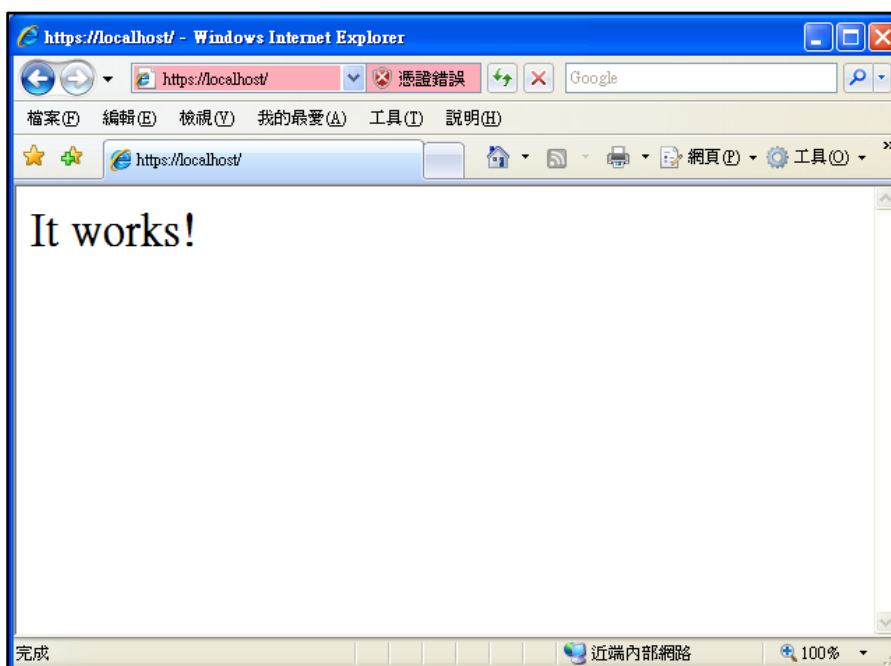
5.8 驗證 SSL 功能

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。



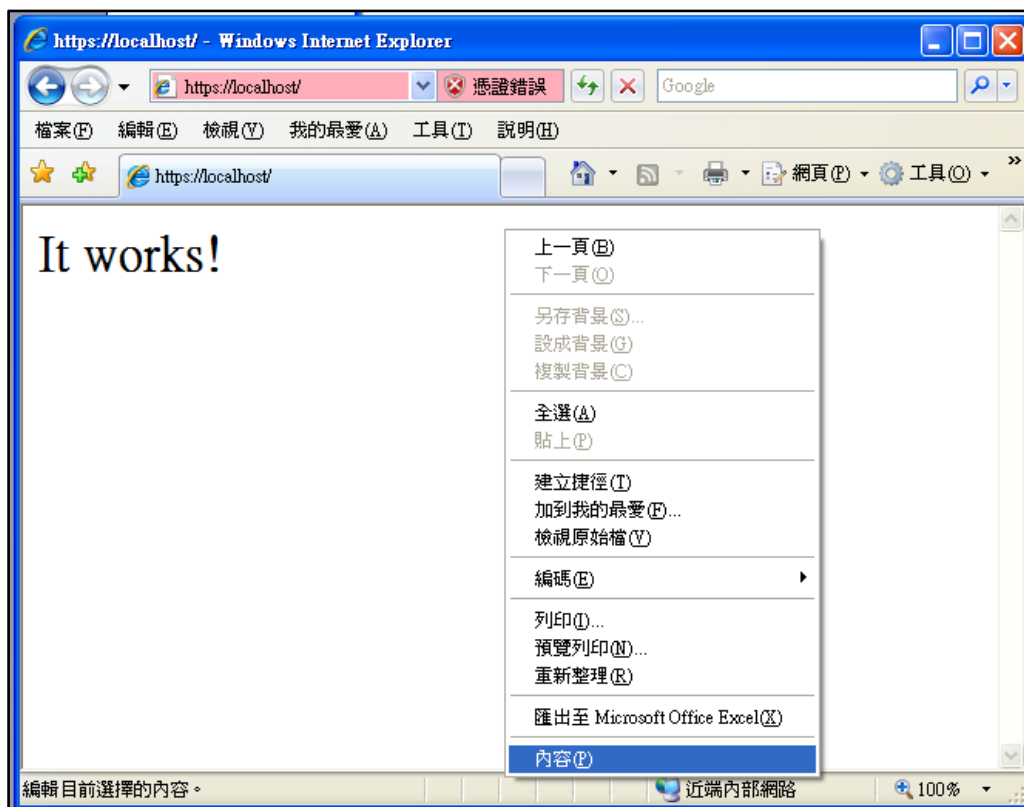
如果瀏覽器出現 It Works! 字樣代表 Apache 已正常服務，且 SSL 功能已啟用。



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

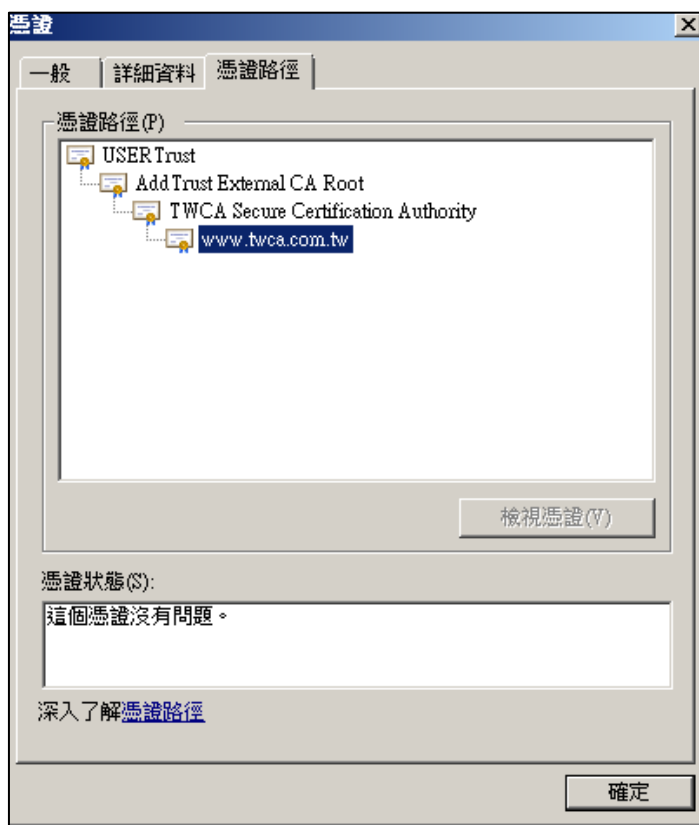
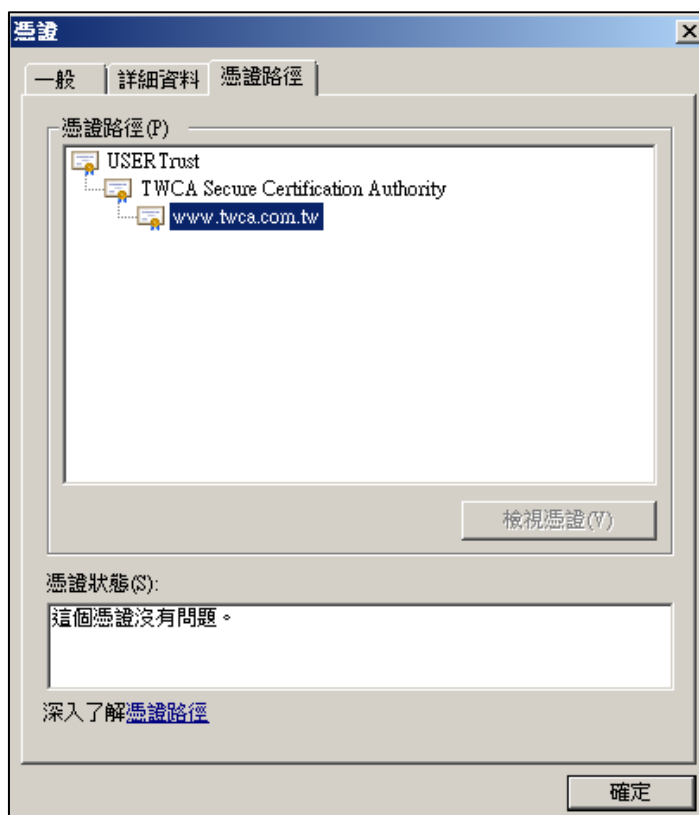
訊



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。(憑證路徑會因瀏覽器不同而存在三階層或四階層兩種不同的架構，兩種架構皆表示憑證安裝沒有問題。)



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 5.6.2.2 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，若無法正常重新啟動 Apache 時，表示 SSL 設定有誤，請檢視 `/usr/local/apache24/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／還原憑證

請將 5.7.1 章節指定的憑證鏈與金鑰檔案備份起來(金鑰、伺服器憑證、中繼憑證)，再依照 5.7.2 至 5.7.3 章節的步驟設定，即可還原憑證。

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參考 5.7.1 章節步驟，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

請參照 5.2 至 5.7 章節申請安裝憑證，並利用 5.8 章節驗證 SSL 憑證是否更新成功，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%20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.