

---

## 目錄

◆ <a href="#">一、cPanel</a> . . . . .	p. 1
◆ <a href="#">二、Plesk</a> . . . . .	p. 3
◆ <a href="#">附錄：LiteSpeed WebAdmin Console</a> . . . . .	p. 5
◆ <a href="#">附件：操作範例圖</a> . . . . .	p. 7

---

## 一、cPanel 篇 ( 以主流版本為準 )

cPanel 是 Linux 虛擬主機最常見的管理系統。安裝時需將憑證、私鑰與中繼憑證鏈分別貼入對應欄位。

### 安裝步驟

1. **登入 cPanel**：找到「**安全性 (Security)**」區塊，點選 **SSL/TLS**。
2. **管理 SSL 網站**：點選「**安裝並管理網站的 SSL ( Install and Manage SSL for your site (HTTPS) )**」下方的「**管理 SSL 網站 (Manage SSL Sites)**」。
3. **選擇網域**：在「**網域 ( Domain )**」下拉選單中選擇您準備安裝憑證的網址。
4. **填入憑證內容**：依下列說明分別填入三個欄位。
  - **憑證 (CRT)**：用記事本開啟 [憑證序號].cer，將全文內容完整複製 ( 包含 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE----- 標籤 ) 並貼入此欄位。
  - **私鑰 (KEY)**：用記事本開啟當初產製 CSR 時的 private.key，將全文內容完整複製 ( 包含 -----BEGIN PRIVATE KEY----- 與 -----END PRIVATE KEY----- 標籤 ) 並貼入此欄位。
  - **憑證授權單位組合 (CABUNDLE)**：此欄位需放入完整的中繼憑證鏈，用記事本開啟 CHTOVCA.crt，將全文內容完整複製 ( 包含 -----BEGIN CERTIFICATE----- 與 -----END CERTIFICATE----- 標籤 ) 並貼入此欄位。

**⚠ 注意：** 每個檔案內容的 BEGIN / END 標籤都必須完整保留，否則瀏覽器在驗證憑證鏈時可能會失敗。

5. 完成安裝：點擊底部的「**安裝憑證 (Install Certificate)**」按鈕。

### 技術提醒

- cPanel 有「自動填充 (Autofill)」功能，若已先在「憑證」分頁上傳過檔案，系統可能在選擇網域後會自動帶出憑證內容，請務必核對是否為最新的中華電信憑證。
  - CABUNDLE 缺漏或格式錯誤是最常見的安裝問題，會導致部分裝置顯示憑證鏈警告，請務必確認。
-

## 二、Plesk 篇 ( 以主流版本為準 )

Plesk 常用於 Windows 或專業 Linux 主機，其介面邏輯以「憑證庫」為中心，安裝分為「新增憑證」與「套用憑證」兩個階段。

### 階段一：新增憑證

1. **進入 SSL 設定**：在左側選單點選「**網站與域名** ( Websites & Domains )」，進入您的網域頁面，在 Dashboard 點選 **SSL/TLS 證書** ( SSL/TLS Certificates )。
2. **進入進階設定**：點選「**進階設定** ( Advanced Settings )」；或者先點選「**下載或移除現有的證書** ( Download or remove existing certificates )」的「**管理** ( Manage )」按鈕，再點選「**進階設定** ( Advanced Settings )」按鈕。
3. **新增憑證**：點選「**添加 SSL/TLS 證書** ( Add SSL/TLS Certificate )」，向下捲動至「**上傳證書檔** ( Upload the certificate files )」區塊，依序填入：
  - **私鑰 (\*.key)**： 上傳 private.key。
  - **證書 (\*.crt)**： 上傳 [憑證序號].cer。
  - **CA 證書 (\*.ca.crt)**： 上傳 CHTOVCA.crt。

若偏好以文字格式操作，亦可在「**以文本形式上傳證書** ( Upload the certificate as text )」區塊，使用記事本開啟憑證、私鑰檔案和中繼憑證 ( 檔案名稱同上述 3. )，將各檔案全文內容複製貼上至對應的欄位。

▶ **上傳檔案**和記事本開啟檔案內容**複製貼上**擇一操作即可，請勿同時使用。

## 階段二：套用憑證至網域

4. **套用憑證**：返回「網站與域名」主頁面，進入「**主機設定 (Hosting Settings)**」( 部分較新版本 Plesk 稱為「Hosting & DNS」標籤)。在「**安全**」區塊確認已勾選「**SSL / TLS 支援 (Enable SSL / TLS support)**」選項，並在「**證書**」下拉選單中選取您剛才新增的憑證名稱，最後按「**確定 ( Save )**」儲存 ( 較舊版本要先點擊「**套用 (Apply)**」按鈕，再按「**Ok**」按鈕完成設定 )。

**⚠ 注意：** 若未完成此步驟，憑證雖已上傳至憑證庫，但網域實際上尚未啟用 HTTPS，瀏覽器仍無法使用 SSL 連線。

## 附錄：LiteSpeed WebAdmin Console 篇

本教學適用直接透過 LiteSpeed 官方管理介面 ( Port 7080 ) 進行設定的網站管理者 ( 如 OpenLiteSpeed 或自建伺服器環境 )。

- ▶ 若您的 LiteSpeed 是透過 cPanel 或 Plesk 管理，請直接參考前述章節，無需手動修改 WebAdmin 設定。

### 安裝步驟

1. 登入 WebAdmin：進入 LiteSpeed 管理後台 ( 通常為 `https://您的伺服器 IP:7080` )。
  2. 進入網站接聽設定：在左側選單點選「Listeners」( 早期版本為上方選單 Configuration > Listeners )，在清單中找到負責 HTTPS 的 Listener 名稱 ( 通常為 SSL，Port 連接埠為 443 )，點擊 Listener 名稱連結或者右側 Action 欄位的「ViewEdit ( 查看/編輯 )」。
- ▶ 若找不到 Port：443 的 Listener，可能需要手動新增一支接聽 443 Port 的 Listener。( 或者您的主機使用其他非 443 Port 連接埠 Listener 接聽 HTTPS 連線 )
3. 切換至 SSL 分頁：進入 Listener 後，點選上方的「SSL」分頁進行憑證設定。
  4. 設定憑證檔案路徑：點選「SSL Private Key & Certificate」標題欄右側的 Edit 編輯按鈕，進入設定編輯模式。

- ▶ **重要提醒：** 私鑰及憑證檔案需先上傳到伺服器空間，才能取得以下設定所需的絕對路徑。

### 做法一：使用憑證串鏈 Bundle 檔案

SSL Private Key & Certificate	
Private Key File ( 私鑰檔案 )	伺服器中的 private.key 檔案絕對路徑
Certificate File ( 憑證檔案 )	手動合併後的 certBundle.pem 檔案在伺服器中的絕對路徑 ( 檔案內容包含 [憑證序號].cer、CHTOVCA.crt 全文，必須為 .pem 格式 )
Chained Certificate ( 串鏈憑證 )	Yes
CA Certificate Path	留空
CA Certificate File	留空

## 做法二：分開設定憑證與中繼憑證

SSL Private Key & Certificate	
Private Key File ( 私鑰檔案 )	伺服器中的 private.key 檔案絕對路徑
Certificate File ( 憑證檔案 )	伺服器中的 [憑證序號].cer 檔案絕對路徑
Chained Certificate ( 串鏈憑證 )	No 或 Not Set
CA Certificate Path	留空
CA Certificate File	伺服器中的 CHTOVCA.crt 絕對路徑

### CA Certificate Path 與 CA Certificate File 的差異

- **CA Certificate File**：指定單一的中繼憑證「檔案」路徑。
- **CA Certificate Path**：指定存放多個中繼憑證檔案的「資料夾」目錄路徑。

▶ 兩者擇一輸入即可，請勿同時設定。

5. **儲存並重啟**：設定完成後，點選「SSL Private Key & Certificate」標題欄右側的「**Save** ( 儲存 )」按鈕，並點選頁面頂端藍色提示框的「**Graceful Restart** ( 平滑重啟 )」字串 ( 舊版本 )，或**綠色重整圖示** ( 新版本 ) 使設定生效。

▶ 以上操作情境假設管理者在已設定好的 SSL 主機進行憑證更新。若您正在建立新主機，您可能還需要進行後續的 SSL Protocol 和 Virtual Host Mappings 設定。

# 附件 操作範例圖

圖 1 記事本開啟憑證檔案



[憑證序號].cer

拖曳進記事本



CHTOVCA.crt

拖曳進記事本



圖 2 certBundle.pem 複製貼上的順序

# 把憑證內容複製貼到 certBundle.pem

certBundle.pem (編輯中)

用記事本開啟憑證檔案



另存新檔

certBundle.pem