

2026/04/14 初版

本手冊說明如何在 Apache HTTP Server (2.4.8 以前版本) 上，完成中華電信 GlobalSign SSL/TLS 憑證及中繼憑證的安裝。安裝過程如以下所示：

修改設定檔 (安裝憑證) → 重啟伺服器

第一節 安裝前準備

開始前，請確認已取得以下四個檔案，建議將它們放在同一個資料夾以方便操作：

檔案名稱 (範例)	說明	來源
private.key	產製 CSR 時所生成的伺服器私鑰	自行保管
[憑證序號].cer	中華電信核發的伺服器憑證	中華電信
CHTOVCA.crt	中華電信新中繼憑證	中華電信
rootr46.crt	GlobalSign R46 根憑證	中華電信

第二節 修改 Apache SSL 設定檔

安裝新憑證，需修改 Apache 的 SSL 設定檔，讓伺服器知道新憑證、私鑰和中繼憑證的存放位置。

1. 開啟 Apache 的 SSL 設定檔 (檔名通常為 `ssl.conf` 或 `httpd-ssl.conf`，詳細路徑請參閱本教學附錄)。
2. 找到您網站對應的 `<VirtualHost *:443>` 設定區塊。
3. 確認 `ServerName` 後面的值是您要安裝憑證的網站網址 (FQDN)。
4. 依照下方範例，設定或更新憑證有關路徑：

ssl.conf 設定範例

```
<VirtualHost *:443>

    ServerName www.example.com

    SSLEngine on
```

```

# (1) 對應私鑰 (自行保管)
SSLCertificateKeyFile      ssl/private/private.key

# (2) 伺服器憑證 (中華電信核發)
SSLCertificateFile        ssl/certs/[憑證序號].cer

# (3) 中繼憑證 (中華電信核發)
SSLCertificateChainFile    ssl/certs/CHTOVCA.crt

... # 其餘設定不變

</VirtualHost>

```

Apache 指令	後面輸入的路徑內容
SSLCertificateKeyFile	產製 CSR 時的原始私鑰 private.key
SSLCertificateFile	[憑證序號].cer
SSLCertificateChainFile	CHTOVCA.crt

⚠ 版本差異

SSLCertificateChainFile 是 Apache 2.4.8 以前版本才有的指令；
2.4.8 (含) 以後版本已捨棄該指令，改以 SSLCertificateFile 直接讀取含有完整憑證鏈的 Bundle 檔案 (同 Nginx)。

第三節 重新啟動 Apache

修改設定檔後，必須重啟 Apache 才能讓新憑證生效。

■ Linux (systemd)

```
# CentOS / RHEL / Fedora 適用
sudo systemctl restart httpd

# Ubuntu / Debian 適用
sudo systemctl restart apache2
```

■ Linux (舊版本 service 指令)

```
# CentOS / RHEL / Fedora 適用
sudo service httpd restart

# Ubuntu / Debian 適用
sudo service apache2 restart
```

■ Windows (XAMPP / WampServer)

請透過控制面板點選「Stop」後再「Start」，或者在 Windows「服務」重啟 Apache 服務。

☑ 驗證

重啟後，以瀏覽器造訪 <https://您的網站網址>，點選網址列左端圖示查看網站資訊。

憑證階層應顯示：

```
GlobalSign R46 Root CA
  Chungwa Telecom GCC R46 OV TLS CA 2025
    伺服器憑證的 CN
```

也可使用 SSL Labs (<https://ssllabs.com/ssltest>) 進行線上完整驗證。

附錄 Apache SSL 設定檔常見路徑

若不確定設定檔位置，可執行下列指令讓 Apache 自行回報 ServerRoot，再到該目錄下尋找 ssl.conf 或 httpd-ssl.conf：

```
# Linux
apachectl -V | grep ServerRoot

# Windows (必須在 Apache bin 目錄下輸入以下指令)
httpd.exe -V | findstr ServerRoot
```

常見環境的 SSL 設定檔預設路徑如下表：

作業系統	SSL 設定檔路徑
Ubuntu / Debian	/etc/apache2/sites-available/default-ssl.conf
CentOS / RHEL / Fedora	/etc/httpd/conf.d/ssl.conf
Arch Linux	/etc/httpd/conf/extra/httpd-ssl.conf
SUSE / openSUSE	/etc/apache2/ssl-global.conf
XAMPP (Windows, 預設 C 槽)	C:\xampp\apache\conf\extra\httpd-ssl.conf
WampServer (Windows, 預設 C 槽)	C:\wamp64\bin\apache\apache[版本]\conf\extra\httpd-ssl.conf
MAMP (Windows, 預設 C 槽)	C:\MAMP\conf\apache\extra\httpd-ssl.conf
macOS 系統內建	/private/etc/apache2/extra/httpd-ssl.conf
macOS Homebrew (Intel)	/usr/local/etc/httpd/extra/httpd-ssl.conf
macOS Homebrew (Apple Silicon)	/opt/homebrew/etc/httpd/extra/httpd-ssl.conf
自行編譯安裝	/usr/local/apache2/conf/extra/httpd-ssl.conf