# 匯智資訊股份有限公司

## SSL 數位憑證

## OpenVPN 憑證安裝說明

匯智資訊
cloudmax
www.cloudmax.com.tw

匯智資訊 cloudmax

**匯智** 資訊股份有限公司
106073 台北市大安區仁愛路四段 25 號 3 樓
3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City
106073, Taiwan (R.O.C.)
t. +886-2-2718-7200
f. +886-2-2718-1922

## 【版權及商標聲明】



文件提供之安裝步驟僅供參考，詳細狀況依伺服器版本或所在網路環境、架構而有些微差別，請依實際狀況或系統提供商資訊為準，若於安裝上有任何問題可與我們聯繫，將有專員引導您排除障礙。



## 【有限擔保責任聲明】

Cloudmax 匯智盡力製作本說明文件其正確性，但不擔保本文件無任何瑕疵，亦不為使用本說明文件而引起之衍生利益損失或意外損毀之損失擔保責任。若對本文件有任何疑問與建議，可利用下方資訊與我們聯繫：

電話：+886-2-2718-7200

傳真：+886-2-2718-1922

信箱：service@cloudmax.com.tw

匯智資訊 cloudmax

**匯智** 資訊股份有限公司

106073 台北市大安區仁愛路四段 25 號 3 樓
3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City
106073, Taiwan (R.O.C.)

t. +886-2-2718-7200
f. +886-2-2718-1922

# 目錄

匯智資訊 cloudmax

**匯智** 資訊股份有限公司
106073 台北市大安區仁愛路四段 25 號 3 樓
3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City
106073, Taiwan (R.O.C.)
t. +886-2-2718-7200
f. +886-2-2718-1922

## 一、產生憑證請求檔

執行下列命令產生金鑰配對 &憑證請求檔(CSR)

### 1. Cent OS or RedHat

openssl genrsa -out <key_filename>.key 2048 *(此 key 檔請務必保留)

openssl req -new -out <csr_filename>.csr -key <key_filename>.key

接著輸入憑證資訊 ， 依序為

- 國家名稱：使用無標點符號的兩個字母代碼表示國家，範例為 TW
- 州或省別：使用完整名稱，範例為 Taipei City
- 地區或城市：使用完整名稱，範例為 Taipei City
- 公司行號：即公司名稱，範例為 Cloudmax Inc.
- 組織單位：提出要求的部門或組織單位的名稱，範例為 IT Dept
- 一般名稱：「一般名稱」是指主機 + 網域名稱，範例為 poc.cloudmax.com.tw

注意：在產生 CSR 時，請勿輸入您的電子郵件地址 (email address)、通關詞組 (A challenge password) 或選用的公司名稱 (An option company name) ， 此三項直接 Enter 帶過即可。

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:TW
State or Province Name (full name) []:Taipei City
Locality Name (eg, city) [Default City]:Taipei City
Organization Name (eg, company) [Default Company Ltd]:Cloudmax Inc.
Organizational Unit Name (eg, section) []:IT Dept
Common Name (eg, your name or your server's hostname) []:poc.cloudmax.com.tw
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

### 2. Windows

下載 Openssl for Win32 http://slproweb.com/products/Win32OpenSSL.html

安裝後，於命令提示字元 (cmd)，移動至 openssl.exe 指令路徑

依預設應為 cd C:\OpenSSL-Win32\bin，接著執行

openssl.exe genrsa -out <key_filename>.key 2048 *(此 key 檔請務必保留)

openssl.exe req -new -key <key_filename>.key -out <csr_filename>.csr -config openssl.cfg

接著輸入憑證資訊 ， 依序為

- 國家名稱：使用無標點符號的兩個字母代碼表示國家，範例為 TW
- 州或省別：使用完整名稱，範例為 Taipei City
- 地區或城市：使用完整名稱，範例為 Taipei City
- 公司行號：即公司名稱，範例為 Cloudmax Inc.
- 組織單位：提出要求的部門或組織單位的名稱，範例為 IT Dept
- 一般名稱：「一般名稱」是指主機 + 網域名稱，範例為 poc.cloudmax.com.tw

注意：在產生 CSR 時，請勿輸入您的電子郵件地址 (email address)、通關詞組 (A challenge password) 或選用的公司名稱 (An option company name) ， 此三項直接 Enter 帶過即可。

## 二、憑證安裝

1. 安裝憑證 - Server 端

[ CentOS or RedHat ]

安裝完成 OpenVPN 套件後，OpenVPN 預設須將憑證放置於 /etc/openvpn 目錄下，拿到憑證後加上所保留的金鑰 key 檔，應有以下檔案：

- 金鑰 key 為 test.key
- 憑證商所簽署之憑證為 test.crt
- 憑證商中繼憑證為 ca.crt

須將金鑰 key、憑證商所簽屬之憑證、憑證商中繼憑證，放置於 /etc/openvpn 目錄下，並修改 /etc/openvpn/server.conf 中設定，範例如下：

```
ca ca.crt          #為憑證商中繼憑證 (憑證商交付伺服器憑證時，應會同時交付中繼憑證)
cert test.crt      #為伺服器憑證 (即提交CSR給憑證商後取得的)
key test.key       #為伺服器金鑰 (即先前產生CSR時保留的那把key)
```

完成後重啟 OpenVPN 服務，service openvpn restart

[ Windows ]

安裝完成 OpenVPN 套件後，OpenVPN 預設須將憑證放置於 C:\Program Files\OpenVPN\config 目錄下，拿到憑證後加上所保留的金鑰 key 檔，應有以下檔案：

- 金鑰 key 為 test.key
- 憑證商所簽署之憑證為 test.crt
- 憑證商中繼憑證為 ca.crt

須將金鑰 key、憑證商所簽屬之憑證、憑證商中繼憑證，放置於 /etc/openvpn 目錄下，並修改 /etc/openvpn/server.conf 中設定，範例如下：

```
ca ca.crt          #為憑證商中繼憑證 (憑證商交付伺服器憑證時，應會同時交付中繼憑證)
cert test.crt      #為伺服器憑證 (即提交CSR給憑證商後取得的)
key test.key       #為伺服器金鑰 (即先前產生CSR時保留的那把key)
```

完成後重啟 OpenVPN 服務，可由服務管理找到 OpenVPN Service ，點選右鍵重新啟動，或是命令提示字元(cmd)：

net stop "OpenVPN Service"

net start "OpenVPN Service"

2. 安裝憑證 - Client 端

[ CentOS or RedHat ]

OpenVPN 預設須將憑證放置於 /etc/openvpn 目錄下，故用戶端也需安裝 OpenVPN 套件。

用戶端需信任伺服器之憑證，因此須將 ROOT CA 憑證放置於 /etc/openvpn 目錄下，並修改 /etc/openvpn/client.conf 中設定。

完成後重啟 OpenVPN 服務：service openvpn restart。

[ Windows ]

OpenVPN 預設須將憑證放置於 C:\Program Files\OpenVPN\config 目錄下，故用戶端也需安裝 OpenVPN 套件。

用戶端需信任伺服器之憑證，因此須將 ROOT CA 憑證放置於 C:\Program Files\OpenVPN\config 目錄下，並修改 C:\Program Files\OpenVPN\config\client.ovpn 中設定。

完成後重啟 OpenVPN 服務，可由服務管理找到 OpenVPN Service，點選右鍵重新啟動，或是命令提示字元(cmd)：

net stop "OpenVPN Service"

net start "OpenVPN Service"

## 三、憑證匯出（伺服器憑證匯出）

[ CentOS or RedHat ]

以檔案形式使用憑證，若欲匯出，只需將 /etc/openvpn 目錄下的伺服器金鑰（.key 檔）、伺服器憑證檔（.crt 檔）、中繼憑證檔（.crt 檔）下載即可。

可使用如 WinSCP & FTP 之類方式下載。

[ Windows ]

以檔案形式使用憑證，若欲匯出，只需將 C:\Program Files\OpenVPN\config 目錄下的伺服器金鑰（.key 檔)、伺服器憑證檔(.crt 檔)、中繼憑證檔(.crt 檔) 複製即可存放。