SSL 數位憑證

Windows Server 2008 R2 憑證安裝說明





106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

【版權及商標聲明】

本文件由 Cloudmax 匯智製作,並保留所有權利。

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。

本文件所引用之各商標及商品名稱分屬其合法註冊公司所有,絕無侵權之意,特此聲明。

【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



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

目錄

— `	CSR 產生	.1
_`	 憑證安裝	.4
	1.安裝	4
	2.匯入	6
\equiv 、	憑證轉檔 PFX	.8
四、	憑證匯出	.9
	1.使用主控台(MMC)	9
	2.使用 Internet Information Services (IIS) 管理員	16



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

一、CSR 產生

1. 「開始」→「系統管理工具」→「Internet Information Service (IIS) 管理員」。



2. 左方「連線」工作視窗中選取認證網域之伺服器後,於「功能檢視」視窗點選「IIS > 伺服器憑證」。





106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

3. 點擊右方「建立憑證要求...」。

Internet Information Services (IIS) 管理員	
▲ Wikt-7035K0H121 檔案(F) 檢視(V) 說明(H)		
建設保 ● ● ● ● ● ● ● ● ● ● ● ● ●	● 印服器憑證 此就能可用來要求及管理網頁伺服器可與針對 SSL 設定的網 站搭配使用的憑證。 ● 予 ● WMSvc-WIN-70S9RUIH21	動作 匯入 建立憑證要求 完成憑證要求 建立網域憑證 建立目我簽署憑證 ② 說明 線上說明
就緒		କ ୍ଲା::

4. 輸入相關資訊。

一般名稱(M):	poc.cloudmax.com.tv	
組織(O):	Cloudmax Internet Inc.	
組織單位(U):	Tech	
縣市/位置(L)	Taipei	
省份(S):	Taiwan	
國家 (地區)(R):	TW	T



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

5. 選擇「Microsoft RSA SChannel Cryptographic Provider」· 位元長度「2048」。

要求整體	? ×
密碼編譯服務提供者內容	
選取密碼編譯服務提供者及位元長度。加密金鑰的位元長度會決定憑證的加密強度。位元長度 越大,安全性就越高。不過,位元長度較大可能會降低效能。 密碼編譯服務提供者(S):	
Microsoft RSA SChannel Cryptographic Provider	
位元長度(B):	
2048	
<u>上一步(P)</u> 下一步(N) 完成(F) 取消	<u>i</u>

6. 輸入要儲存的檔名,「完成」。

登 底水	<u>? ×</u>
檔案名稱	
指定憑證要求的檔案名稱。這項資訊可傳送給憑證	授權單位做為簽署之用。
指定憑證要求的檔案名稱(R):	
C: certred.txt	



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

二、憑證安裝

1. 安裝



1.2 左方「連線」工作視窗中選取認證網域之伺服器後,於「功能檢視」視窗點選「IIS > 伺服器憑證」。





106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

1.3 點擊右方「完成憑證要求...」。

完成豐證要求	<u>?</u> ×
指定憑證授權單位回應	
藉由擷取包含憑證授權單位回應的檔案,完成先前建立的憑證要求。 含有憑證授權單位回應的檔案名稱(R):	
CApoc.cloudmax.com.tw_CER.cer	
好記的名稱(Y):	
poc.cloudmax.com.tw	
	確定 取消

「確定」後即可看到憑證已安裝完成。 1.4

Partices (IIS) 管理員	
🔇 💽 📲 🕨 WIN-70S9RUI	H21K >) 🖸 🖂 🟠 I 🛛 🔹
檔案(F) 檢視(V) 說明(H)		
連続 ● ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	 ● 同服器憑證 此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站 ▲ 整行結 ● 整行結 ● WMSvc-WIN-70S9RUIH21K 	動作 理之憑證要求 建立還證要求 建立回我簽署憑證 建立自我簽署憑證 酸視 運道 酸混 酸視 運当 頭折 × 移除 2 說明<
就緒		u <u>a</u> .:



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

2. 匯入

使用 OpenSSL 產生 CSR,請使用匯入

點擊右方「匯入...」。 2.1



- 「憑證檔案(.pfx)(C):」輸入要匯入的憑證檔(.pfx)路徑。 2.2
 - 「密碼(P):」輸入建立.pfx 檔案時加密的密碼。

Enternet Information Services	[II] 登理員	
📀 💽 📲 🕨 WIN-7089RUI	H21K >) 🔯 🖂 🏠 1 🔞 👻
檔案(F) 檢視(V) 說明(H)		
建設結網頁 ● ● ● WIN-70SPRUIH21K (WIN-7 ● ● ● 登台 ● ● ● 登台 ● ● ● Default Web Site	 ● 同服器憑證 ▶ 助能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站 ▲ 餐▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	動作 匯入 建立憑證要求 完成憑證要求 建立網域憑證 建立目我簽署憑證 建立自我簽署憑證 ② 說明 錄上說明
就緒		• <u>.</u>



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

2.3 「確定」後即可看到憑證已安裝完成。

Thernet Information Services (IIS) 管理員	
🔇 🕥 📲 🕨 WIN-70S9RUI	H21K >	🖸 🖄 🔯 •
檔案(F) 檢視(V) 說明(H)		
連線 ● ・ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	● 伺服器憑證 此功能可用來要求及管理網頁伺服器可與針對 SSL 設定的網站 信紹使用的憑證。 名稱 ◆ 發行給 發行者 WMSvc·WIN-7OS9RUIH21K WMSvc- poc cloudmax.com tw AlphaSSI ● poc cloudmax.com tw ● 回 の記述 ● 回 の記述	西九 建立憑證要求 東立聽城愚證 建立自我簽署憑證 検視 運出 更新 ※ 移除 ② 說明 線上說明
駅離		



 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
 ^{t.} +886-2-2718-7200
 f. +886-2-2718-7200
 f. +886-2-2718-1922

 106073, Taiwan (R.O.C.)

三、憑證轉檔 PFX

若您是使用 Linux 產生的 SSL 的 key 與 csr 檔案‧在簽發完成後會取得一個合法的 SSL crt 檔案‧就必需將 SSL key 與取得的 crt 檔案轉為 Windows IIS 所使用的憑證 pfx 檔案。

需要的清單如下:

- 憑證私鑰檔 (如 domain.key)
- 憑證檔 (如 domain.cer、domain.crt)
- 簽發者憑證檔 (如 domain_CA.cer、domain_CA.crt) 等等

接著使用 Openssl 指令轉換為 pkcs12 格式,如下

Demo >openssl pkcs12 -export \
> -out poc.cloudmax.com.tw.pfx \
> -inkey poc.cloudmax.com.tw_KEY.key \
> -in poc.cloudmax.com.tw_CER.cer \
> -certfile poc.cloudmax.com.tw_CA.cer

openssl pkcs12 -export -out 要儲存的名稱.pfx -inkey 憑證私鑰檔.key -in 憑證檔.cer -certfile 簽發者憑證檔 CA.cer



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

四、憑證匯出

- 使用主控台 (MMC) 1.
 - 1.1 「開始」點擊執行後輸入 mmc。

		_		-
	輸入程式、 會自動開創	資料夾、文件) X。	或網際網路資源的	的名稱,Windows
開啟(O):	mmd			•
	🥵 必須存	月系統管理權限:	才能建立此工作。	i
		確定	取消	瀏覽(B)

1.2 點擊左上角「檔案」 → 「新增/移除嵌入式管理員元(M)...」。

屬主控台1 - [主控台根目錄]		
🚠 檔案(F) 執行(A) 檢視(V) 我的最愛(O)	視窗(W) 說明(H)	_8×
◆ 開新檔案(N) Ctrl+N		
■ 開設舊檔(0) Ctrl+0		動作
日本15 50 50 50 50 50 50 50 50 50 50 50 50 50	這個檢視沒有項目可顯示。	主控台根目錄 🔺
新增移除嵌入式管理單元(M) Ctrl+M 選項(P)		其他動作 ▶
1 ServerManager.msc 2 C.\Windows\system32\WF.msc		
開 散一個現存的主控台。		



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

1.3 尋找到「憑證」後點中間的「新增(A)>」。

人式管理單元	▶ 廠商 ▲	1 主控台根目錄	編輯延伸(X)
装置管理員	Microsoft Cor		採[]余(R)
資料夾	Microsoft Cor		15/147/449
路田皮逐病仔取	Microsoft Cor		L40 m
电脑管理	Microsoft Cor		
电前行自	Microsoft 61		下移(D)
2830年1日3王 2月11月3百8年	Microsoft Cor 新增	曾(A) >	
啊~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Microsoft Col		
读端点面	Minsoft Cor		
运动 (A)	Microsoft Cor		
法端点面服務管理員	Microsoft Cor		
應證	Microsoft Cor		1
	•		進階(\)
		- E	

1.4 選擇「電腦帳戶(C)」。

豊ਡ祓入式管理軍 元	X
這個嵌入式管理單元將自動管理下列帳戶的憑證:	
○ 我的使用者帳戶(M)	
○ 服務帳戶(\$)	
● 電腦帳戶(C)	
< 上一步(B) 下一步(N)> 取消



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

1.5 選擇「本機電腦(執行個這主控台的電腦)(L):」 → 「完成」。

選取您要此嵌入式管理 這個嵌入式管理單元將	理單元管理的電腦。 等一直管理:		
 ● 本機電腦 (執行這) 	個主控台的電腦)(L)):	
C 另一台電腦(A):			瀏覽(R)
Ⅰ 留电脑征前令列指 才適用(W)	X重加時, 可 XX 新经早日	电脑進行變更。這只有	住心随仔土控育之後

完成後可看到「憑證(本機電腦)」會出現在右邊方框內,點選「確定」。 1.6

入式管理單元	廠商		「主控台根目銘」	
裝置管理員	Microsoft Cor			
資料夾	Microsoft Cor			移除(R)
路由及遠端存取	Microsoft Cor			
電腦管理	Microsoft Cor			上移(U)
電話語音	Microsoft Cor			
磁碟管理	Microsoft 與		*F##(4) > 1	下移(U)
網址連結	Microsoft Cor			
網路存取保護 (NAP	Microsoft Cor			
遠端点面	Microsoft Cor			
遠端桌面工作階段…	Microsoft Cor			
遠端点面服務管理員	Microsoft Cor			
憑證	Microsoft Cor	_		SH-Dit on
		-		建陷(Y)



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F, No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

1.7 選擇「個人」 → 「憑證」後可看到有安裝哪些憑證,點擊滑鼠右鍵 → 「所有工作」 → 「匯出」。

● 邊 (本橋電腦) ● Doc.6 Lowd max com. tv 10.1 abs 2 Lowd max com. ts 55 - G2 20174 意記 ● 図 ● Max com. tv ● III 121K 20261 ● III 121K ● III 121K ● III 121K ● III 121K ● IIII 121K ● III 121K ● IIII 121K ● IIIII 121K ● IIIII 121K ● IIIII 121K ● IIIII 121K ● IIIIII 121K ● IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	mpce.eloudmax.com.tw ☆ WMSvc-WIN-7OS9RUIH21K	開設舊檔(0) 所有工作(K) → 剪下(T) 複製(C) 刪除(D) 內容(R)	256 - G2 UIH21K 開散舊檔(0) 以新的金編星 以新的金編星 管理私密金針	2017/1 2026/1 更求憑證(Q) 更新憑證(N) 角(M)	查 道	其他動作 cloud max.com.t 其他動作
通過 所有工作(公) → 開散舊檔(0) 其他動作 2 企業信任 剪下(I) 以新的金鑰要求憑證(Q) 其他動作 2 中離愚證按權單位 複製(C) 以新的金鑰更新憑證(Q) 其他動作 2 中離愚證按權單位 複製(C) 以新的金鑰更新憑證(Q) 其他動作 2 空信任的憑證 一 內容(R) 證階操作(A) → 其他動作 2 空信任的人 該明(H) 匯出(E) 其他動作 2 透識註冊要求 該明(H) 匯出(E)		所有工作(K) ▶ 剪下(T) 複製(C) 刪除(D) 內容(R)	開散舊檔(0) 以新的金鑰 以新的金鑰 管理私密金針	要求憑證(Q) 更新憑證(N) 角(M)		其他動作 :loudmax.com.t 其他動作
○ 企業信任 第下(T) 以新的金鑰要求憑證(Q) 2loud moxe.com. ○ 企業信任 第下(T) 以新的金鑰要求憑證(Q) 2loud moxe.com. ○ 中継憑證授權單位 以新的金鑰更新憑證(N) 其他動作 ○ 沒信任的發行者 問除(D) 管理私密金鑰(M) 其他動作 ○ 第三方根憑證授者 內容(R) 進階操作(A) → ○ 客mob Desktop 證書 ○ 希認註冊要求		剪下(T) 複製(C) 刪除(D) 內容(R)	以新的金鑰里 以新的金鑰里 管理私密金針	要求憑證(Q) 更新憑證(N) 龠(M)		cloud max com t 其他動作
1 中継憑證接權單位 複製(C) 以新的金鑰更新憑證(M) 其他動作 2 受信任的發行者 一 管理私密金鑰(M) 3 第三方根憑證授者 内容(R) 進階操作(A) → 3 至信任的人 3 該明(H) 匯出(E) 3 配書物生常任相目針 回 回答生作信的联票者		複製(C) 刪除(D) 內容(R)	以新的金鑰員 管理私密金銷	更新憑證(№) 龠(M)		其他動作
○ 沒有信任的憑證 ● 一 沒有信任的憑證 ● 管理私密金鑰(M) ○ 沒有信任的憑證 內容(R) 進階操作(A) ○ 愛信任的人 ○ 簡整卡信任根目針 ○ 勿替於卡信任根目針		····································	管理私密金飾	龠(M)		
□ 第二方根急渡後和 Pi合(K) 理論就下(K) / □ 登信任的人 説明(H) 匯出(E) □ 透路(於日常書 100 (100 (100 (100 (100 (100 (100 (100		NA(K)				
□ ② Remote Desktop 説明(t) 建正(t) □ ③ 憑證注冊要求 □ ② 控括卡信任根目針		Non an				
3 2			匯出(E)			

1.8 「下一步」。

憑證匯出精靈		×
	歡迎使用憑證匯出精靈	
	這個精靈將協助您從憑證存放區將憑證、憑證信任 清單及憑證撤銷清單複製到您的磁碟中。	
8	憑證由憑證授權單位簽發,能識別您的身分,並包含 用來保護資料或建立安全網路連線的資訊。憑證存放 區是用來存放憑證的系統區域。	
	請按 [下一步] 繼續。	
	<上一步(B) 下一步(N) > 取消	



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

1.9 選擇「是·匯出私密金鑰(Y)」。

遺匯出精靈		×
匯出私密金論 您可以選擇將私密金論與憑證一起國	匯出。	
私密金鑰受到密碼的保護。如果您到 一頁輸入密碼。	要將私密金鑰與憑證一起匯出,您必須在下	
您想將私密金鑰與憑證一起匯出?		
● 是,匯出私密金鑰(Y)		
○ 否,不要匯出私密金鑰(0)		
深入了解匯出私密金鑰		
	<上一步(B) 下一步(N) > 取消	i

1.10 選擇「個人資訊交換·PKCS #12 (.PFX)(P)」·下方選擇依個人需求勾選。

諸選	取您想要使用的格式:
C	,DER 編碼二位元 X.509 (CER)(D)
C)Base-64 編碼 X.509 (.CER)(%)
C	・加密編譯訊息語法標準 - PKCS #7 憑證 (P7B)(C) 「 如果可能的話,包含憑證路徑中的所有憑證(D)
6	/個人資訊交換 - PKCS #12 (PFX)(P)
	✓ 如果可能的話,包含憑證路徑中的所有憑證(U)
	「如果匯出成功即刪除私密金鑰(K)
	□ 匯出所有延伸內容(A)
C)Microsoft序列憑證存放 (.sst)(T)
了解	馬鋒檔案格式



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

1.11 輸入要保護的密碼 → 「下一步」。

遺匯出精靈		×
密碼 為了安全性,您必須使用密碼保護	私密金鑰。	
輸入並確認密碼。		
密碼(P):		
輸入並確認密碼 (必要)(C):		
•••••		
		Ter 234

1.12 輸入要儲存憑證的路徑後「下一步(N)」。

檔案名稱(F):	
C:\exportcert.pfx	瀏覽(R)



106073 台北市大安區仁愛路四段 25 號 3 樓 t.+886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

1.13 點選「完成」後,「確認」以關閉匯出成功之訊息。

	完成憑證匯出精靈	
	您已經成功地完成憑證匯出精靈。 您已指定下列新設定:	
4	檔案名稱 C:\exporter 匯出金論 是 包含憑證路徑中的所有憑證 是 檔案格式 個人資訊公	rt.pfx ī换 (*.pfx)
	▲ 匯出成功。 確定	
	<u> </u>]



106073 台北市大安區仁愛路四段 25 號 3 樓 t. +886-2-2718-7200 3F., No. 25, Sec. 4, Ren'ai Rd., Da' an Dist., Taipei City 106073, Taiwan (R.O.C.)

f. +886-2-2718-1922

使用 Internet Information Services (IIS) 管理員 2.

點選右邊的「匯出...」。 2.1



輸入要儲存憑證的路徑、輸入要保護的密碼 → 「確定」。 2.2

匪出憑證		? ×
匯出到(E):		
C:\exportcert.pfx		
密碼(P):		

確認密碼(M):		
••••••		
	確定] 取消
	Contraction of the second	