

SSL 憑證 Apache 憑證安裝說明


 網址申請

 虛擬主機

 SSL 憑證

 郵件主機

 IDC 服務

 資安服務

 搜尋行銷



SSL 憑證

感謝您使用 WIS 匯智數位憑證服務，並在申請期間配合憑證中心規定完成審核程序。

當您收到 WIS 匯智寄發的數位憑證完成通知，代表已經完成所有驗證程序，接著依循本說明文件逐步將憑證安裝至伺服器後，即可開始使用數位憑證為伺服器與使用者之間的資料傳輸加密。

以下 Apache 伺服器的安裝步驟僅供參考，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。有任何問題可與我們聯繫，將有專員引導您排除障礙。

版權聲明

本文件內容僅授權 WIS 匯智數位憑證用戶使用，WIS 匯智資訊股份有限公司保留所有權利。

商標聲明

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

WIS 匯智盡力製作本說明文件，確保其正確性，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。

若對本文件有任何指正或建議，請利用下列資訊與我們聯繫：

服務電話 (02)2718-7200

服務傳真 (02)2718-1922

電子信箱 service@wis.com.tw

營業地址 10544 台灣台北市松山區復興北路 337 號 6 樓

內容

一、安裝前注意事項.....	2
二、準備憑證.....	3
(一)公開金鑰	3
(二)中繼憑證	4
三、安裝憑證與中繼憑證.....	5
四、檢查憑證安裝是否正確.....	7
(一)瀏覽器使用 https 開啟認證網址.....	7
(二)WIS 匯智 SSL 伺服器憑證安裝檢查器	8
(三)GeoTrust Certificate Installation Checker	9
五、數位憑證備份與更新.....	10
(一)備份	10
(二)更新	10

一、安裝前注意事項

數位憑證是由私密金鑰 (private key) 與公開金鑰 (public key) 兩個部分組成, 在進行安裝及使用數位憑證前, 須將私密金鑰與公開金鑰檔案放置於伺服器可讀取之儲存區中。

依伺服器網路環境不同而實際需求各異, 以下列出安裝時常見忽略的狀況:

- ✓ 系統是否已安裝 OpenSSL¹ 與 mod_SSL² ?
- ✓ Apache 是否已載入 mod_SSL 模組³ ?
- ✓ 伺服器是否正常連上 Internet ?
- ✓ HTTPS 協定之通訊埠是否開啟⁴ ?
- ✓ 部分狀況下, 伺服器需要額外的固定 IP⁵ 支援; 此時需調整網址之 A 紀錄⁶。
- ✓ 與伺服器串連的網路設備通訊埠的狀態是否設定完成⁷ ?

若無法確認網路環境, 或您非相關設備或服務的權限擁有者, 應與設備、系統所屬管理員或該服務、設備提供商諮詢及確認。

安裝過程中, 因操作錯誤或其他不可預期因素, 可能導致系統資料異常、毀損, 請在系統更動前, 將重要系統及資料進行備份。

¹ <http://www.openssl.org/>

² <http://www.modssl.org/>

³ 可查詢 httpd Config File 中的 Include 描述進行確認。

⁴ HTTPS 協定預設使用 Port 443, 但使用者可依實際狀況進行調整。

⁵ 多個網站共用同一台伺服器的情況下(如虛擬主機), 需要利用額外的固定 IP 以解決通訊埠不足的問題。

⁶ 須注意您是否擁有修改 DNS(Domain Name Service) Server 權限, 且 DNS 紀錄修改需要生效時間。

⁷ 例如防火牆、負載平衡裝置、代理伺服器, 可能須調整規則、開啟通訊埠, 甚至部分設備也需要安裝、支援數位憑證。

二、準備憑證

每種伺服器接受之憑證檔案格式不同⁸，安裝前轉換為適合的格式才能順利完成。下列安裝說明中，將提示伺服器安裝步驟中接受的檔案格式。

安裝中您必須準備公開金鑰、中繼憑證，以及對應的私密金鑰⁹。以下說明公開金鑰和中繼憑證取得方式。

(一) 公開金鑰

憑證核發成功後，指定之 Email 信箱將可收到國外認證中心發的英文通知信與 WIS 匯智的中文通知信，信中公開金鑰以純文字方式顯示。



信件內容中從『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』為止，看似亂碼的文字即為公開金鑰的內容。

開啟文件編輯軟體，並將從『-----BEGIN CERTIFICATE-----』至『-----END CERTIFICATE-----』完整複製至編輯器中，以『.cert』作為副檔名儲存於伺服器可存取之位置中。

⁸ 依據 X.509 標準(RFC 4158)，憑證檔案格式有 DER、PKCS#7、PKCS#12 等，衍生副檔名常見有 .pem、.cer、.crt、.der、.p7b、.p7c、.pfx、.p12 等。

⁹ 私密金鑰應於 CSR 產生時自行妥善保管，若遺失或損毀必須重新申請憑證。

(二)中繼憑證

電腦運算能力於近十年內大幅提升，為確保使用GeoTrust憑證用戶網路資料傳輸安全，GeoTrust於 2010-07-22 起將根憑證由 1024 位元全面升級為 2048 位元¹⁰。早於此時間點發行之瀏覽器中，未包含此 2048 位元根憑證資料，所以需要利用中繼憑證(Intermediate Certificate)進行交互驗證¹¹，確保舊版瀏覽器中使用HTTPS連線時不會出現錯誤或警告訊息。

請依您選購的憑證類別下載中繼憑證:

憑證名稱	中繼憑證連結
QuickSSL 專業憑證 (QuickSSLPremium)	http://ssl.wis.com.tw/download/chain-qp.cer
企業識別數位憑證 (TrueBusinessID)	http://ssl.wis.com.tw/download/chain-tid.cer
企業識別延伸憑證 (TrueBusinessID with EV)	http://ssl.wis.com.tw/download/chain-ev.cer
企業識別多域名憑證 (TruBusinessID Wildcard)	http://ssl.wis.com.tw/download/chain-tid.cer
企業識別多子網域憑證 (TrueBusinessID Multidomain)	http://ssl.wis.com.tw/download/chain-tid.cer

下載後，請使用編輯器將之另存為『.crt』檔案。

¹⁰ 根憑證位元數代表使用數位憑證加密資料時，可使用之最高加密強度。數值越大表示加密強度越強，伺服器與使用者端加解密所需運算時間也越長。

¹¹ 透過瀏覽器信任清單中之憑證私密金鑰為中繼憑證進行簽章；利用憑證樹系可「向上信任」的關係，使未納於信任清單中的中繼憑證得到瀏覽器的信賴。

三、安裝憑證與中繼憑證

在 Apache 中安裝數位憑證需要編輯系統設定檔 (Config File)，因為 Apache 設定檔的儲存位置與名稱經常依發行版本不同而各異，以下列出常見的系統設定檔存放位置，實際狀況應依伺服器情況為準：

常見存放路徑	常見檔案名稱
/etc/httpd	httpd.conf
/etc/httpd/vhosts.d/	ssl.conf
/etc/httpd/sites/	

1. 打開系統設定檔，找到<VirtualHost>區塊。
2. 在 <VirtualHost 192.168.0.1:443> 與< /VirtualHost>區塊中加入下列幾行設定：

SSLEngine On

SSLCertificateFile /公開金鑰儲存路徑/公開金鑰檔案名稱.crt

SSLCertificateKeyFile /私密金鑰儲存路徑/私密金鑰檔案名稱.key

SSLCertificateChainFile /中繼憑證儲存路徑/中繼憑證檔案名稱.crt¹²

例如：

```
[root@www ~]# vi /etc/httpd/httpd.conf

<VirtualHost 219.84.160160:443>
DocumentRoot /var/www/ssl_html
ServerName ssl.wis.com.tw
SSLEngine on
SSLCertificateFile /user/local/ssl/crt/ssl_wis_com_public.crt
SSLCertificateKeyFile /user/local/ssl/private/ssl.wis_com_private.key
SSLCertificateChainFile /user/local/ssl/crt/chain-tid.crt
</VirtualHost>
```

¹² 在部分狀況下，系統不是使用 SSLCertificateChainFile，若您採用此設定無效，請替換成 SSLCACertificateFile 進行設定。

3. 修改完畢後，儲存並關閉文字編輯器。
4. 重啟 Apache 前，以下列指定測試修改過後的設定檔是否設置正確。
`apachectl configtest13`
5. 利用下列指令重啟 Apache¹⁴
`apachectl restart`

或下指令先停止然後再開啟 `apachectl`

```
apachectl stop
apachectl start
```

重啟完畢請查看系統訊息，以確認 Apache 是否重啟成功。也可以透過 `httpd` 的 `Error Log15` 與 `Access Log16`，確認 Apache 執行狀況。

¹³ 也可以使用 `apachectl -t`

¹⁴ 在部分狀況下，重啟 Apache 支援 SSL 的指令為 `apachectl startssl`，或您也可以直接使用 `httpd restart` 指令重啟整個 `httpd` 服務。

¹⁵ `Error Log` 紀錄 Apache HTTP Server 執行時產生的錯誤訊息，一般常見預設位置為 `/var/log/httpd/error_log`、`/var/log/http-error.log` 等，正確檔案路徑與設置請查詢 `Config File` 檔案中 `ErrorLog` 描述。

¹⁶ `Access Log` 紀錄 Apache HTTP Server 所有的執行訊息，一般預設路徑與檔案位置為 `/var/log/httpd/access_log`、`/var/log/http-access.log` 等，正確檔案路徑與設置請查詢 `Config File` 檔案中 `AccessLog` 描述。

四、檢查憑證安裝是否正確

下列 3 種檢查方式您只需要選擇一種進行檢測¹⁷即可。

(一) 瀏覽器使用 https 開啟認證網址

在瀏覽器中輸入『https://+認證之完整網址』，若可正常顯示表示憑證已安裝成功(各瀏覽器的顯示方式略有不同)。



¹⁷ 由於伺服器本身系統錯誤、伺服器網路環境、安裝過程不當操作等問題，皆可能造成錯誤，族繁不及詳載於此。本文件僅供安裝使用，若在安裝中出現錯誤，請記下詳細的錯誤訊息或操作步驟、畫面後，與我們聯繫以取得對應的障礙排除說明及協助。

(二)WIS 匯智 SSL 伺服器憑證安裝檢查器

開啟連結 <http://ssl.wis.com.tw/openssl/checkservercert.asp>

依網頁中指示，分別輸入『域名』、『伺服器埠』、『驗證碼』後，點選『讀取憑證』。

SSL伺服器憑證安裝檢查器

域名: (例如: www.myssl.com.tw)
伺服器埠:
驗證碼: 

有效憑證

伺服器IP: 219.84.160.160
域名: *.wis.com.tw
備用域名: *.wis.com.tw、wis.com.tw
頒發機構: Equifax Secure Certificate Authority
金鑰長度: 1024 位
簽名演算法: sha1RSA
有效期: 2010-5-5 15:08:50 ~ 2012-5-7 23:31:53 (還有 311 天到期)

憑證1:
使用者: *.wis.com.tw
頒發者: Equifax Secure Certificate Authority
有效期: 2010-5-5 15:08:50 ~ 2012-5-7 23:31:53

憑證2:
使用者: Equifax Secure Certificate Authority
頒發者: Equifax Secure Certificate Authority
有效期: 1998-8-23 0:41:51 ~ 2018-8-23 0:41:51

若無錯誤訊息表示憑證已安裝成功。

(三) GeoTrust Certificate Installation Checker

開啟下列連結：

<https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=SO9557&actp=LIST>

依網頁中指示，分別輸入『Enter your Web Server's domain name (認證網域)』、『Enter your port(443 is default for SSL)(伺服器埠)』，點選『Test this Web Server(測試這個網站)』。

Resolution

Enter your Web Server's domain name:	<input type="text" value="ssl.wis.com.tw"/>
Enter your port (443 is default for SSL):	<input type="text" value="443"/>
Test this Web Server	
Status: Successful	
<p>ssl.wis.com.tw is successfully secured by an SSL certificate. The following certificates are correctly installed:</p> <p>-----Certificate 1----- --Issued To-- Organization: 匯智資訊股份有限公司 Organizational Unit: IT Dept Common Name: *.wis.com.tw Locale: Taipei, Taiwan Country: TW</p> <p>--Issued By-- Organization: Equifax Organizational Unit: Equifax Secure Certificate Authority Country: US</p> <p>Valid from Wed May 05 15:08:50 CST 2010 to Mon May 07 23:31:53 CST 2012 Serial Number (hex): 12b706 -----</p>	

狀態(Status)顯示為成功(Successful)，即表示伺服器憑證已安裝完成。

五、數位憑證備份與更新

(一) 備份

WIS 匯智數位憑證在憑證有效期間內，提供憑證重置(Reissue)與更新的服務。不過重置過程需與新申請憑證時相同，必須再次產生私密金鑰與 CSR、驗證、簽發公開金鑰等程序後，才可再取得憑證。將可能耽誤寶貴的系統復原時間。基於資安考量，建議系統管理者將數位憑證進行備份。

Apache 備份的方式很簡單，請將您的私密金鑰、公開金鑰¹⁸複製至您的備份儲存設備即可。

(二) 更新

憑證更新時，需要重新產生 CSR¹⁹、私密金鑰、公開金鑰與中繼憑證等檔案。

一般狀況下，中繼憑證為憑證中心的公開檔案，在憑證更新時不會進行異動；而公、私金鑰為獨一無二的金鑰對，故每次進行更新需產生新的 CSR 檔，而且有新的金鑰對。

故於憑證更新時，需更動 Apache 設定檔中 SSLCertificateFile、SSLCertificateKeyFile 這兩行描述。請參考「安裝憑證與中繼憑證」一節進行設定。

更新檔案路徑與名稱²⁰後，請重啟Apache已讓更動的設定載入。

¹⁸ 中繼憑證您可隨時透過網際網路下載，不需特別備份。基於資安考量，建議您備份公、私密金鑰時，再加上密碼保護等措施，並妥善保存備份資料，以避免私密金鑰外洩。

¹⁹ CSR 為 Certificate Signing Request(憑證請求檔)的縮寫，與 private key 為對應的檔案。利用 CSR 提交至憑證中心，便可避免私密金鑰外洩，又可讓憑證中心簽核對應的 public key。

²⁰ 若更替新憑證時直接覆寫舊檔案名稱與位置，及不須再調動 Config File 設定，但仍需重啟 Apache，讓設定值得以更新。



www.wis.com.tw

Contact

若對本文件有任何指正或建議，請利用下列資訊與我們聯繫

服務電話 (02)2718-7200

服務傳真 (02)2718-1922

電子信箱 service@wis.com.tw

營業地址 10544 台灣台北市松山區復興北路337號6樓