

匯智資訊股份有限公司

SSL 數位憑證 Domino 憑證安裝說明

【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 Domino 8.5 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

目錄

一、透過 Domino 產生 CSR.....	1
二、安裝前注意事項.....	3
三、數位憑證安裝前準備確認事項.....	4
四、安裝方式.....	6
五、檢查憑證安裝是否正確.....	9

一、透過 Domino 產生 CSR

CSR 檔案為提供給憑證中心驗證的檔案，透過此 CSR 檔案憑證中心將會簽發 CER 檔案；

而產生 CSR 檔案的同時會一併會產出 KEY 檔案，而這三個檔案為互相匹配憑證才可正常運行。

1. 請先進入憑證管理服務，並且點擊 Create Key Ring



- 2 請輸入相關憑證資訊

Key Size Key Size: 2048	Key Size is the size of the public/private key pair in bits. The larger the key size, the greater the encryption strength. Note: This Edition of Domino provides the ability to generate RSA keys at both 1024 bits and 512 bits, in accordance with export regulations worldwide.
Distinguished Name Common Name: Organization: Organizational Unit: (optional) City or Locality: (optional) State or Province: (no abbreviations) Country: (two character country code)	The Distinguished Name is the information about your site that will appear in any certificates you create. Note: Make sure the Common Name matches the URL of your site. Some browsers check the Common Name and the site URL, and do not allow a connection if they don't match.

3 點擊繼續，將會請您確認相關資訊的視窗，再次點擊確認將會回到主選單

4 您可以在下方找到 Method 當中的 Paste into form on CA's site.，並且點擊下方的 Create Certificate Request

Name	Note: The key ring contains the Distinguished Name information that will be included in the certificate request.
Certificate Request Information Log Certificate Request: Yes	Log certificate requests for future reference. Note: Choose "View Certificate Request Log" in the main menu page to see a listing of all logged requests.
Method: <input checked="" type="radio"/> Paste into form on CA's site <input type="radio"/> Send to CA by e-mail	Choose how to submit the certificate request to the Certificate Authority. Note: The "Paste" method is recommended if it is supported by the Certificate Authority you are using.

5 將會開啟新的視窗，上方為您的 CSR 相關資訊，下方為 CSR 編碼，煩請您將下方編碼，以文字檔的方式保存好，並且寄送給匯智。

*若透過 Domino 產生 CSR 檔案，KEY 檔案將會直接儲存於此 Domino 伺服器中。

二、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：

- 伺服器是否正常連上 Internet ？
- HTTPS 協定之通訊埠是否開啟¹ ？
- 部分狀況下，伺服器需要額外的固定 IP² 支援；此時需調整網址之 A 紀錄³ 。
- 與伺服器串連的網路設備通訊埠的狀態是否設定完成⁴ ？

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

² 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。

³ 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。

⁴ 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。

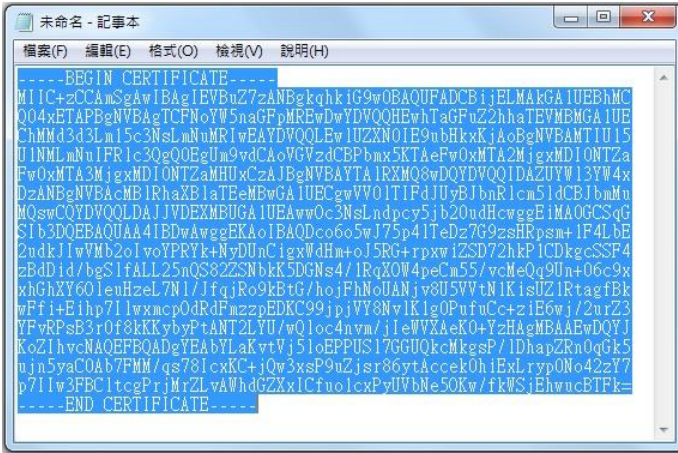
三、數位憑證安裝前準備確認事項


憑證核發成功後，指定的 Email 信箱將可收到國外認證中心發的英文通知信與匯智的中文通知信，而信中將會提供憑證中心所簽屬的 CER 檔案與憑證中繼憑證檔案，這些資訊將以純文字的方式來顯示，請您進行以下的動作確認所頒發的憑證資訊是否正確。

- 1 請協助查看憑證資訊檔案文本資料中



- 2 請複製憑證資訊(包含) 『-----BEGIN CERTIFICATE-----』 至 『-----END CERTIFICATE-----』)
- 3 開啟純文字檔案，貼上您所複製的資訊

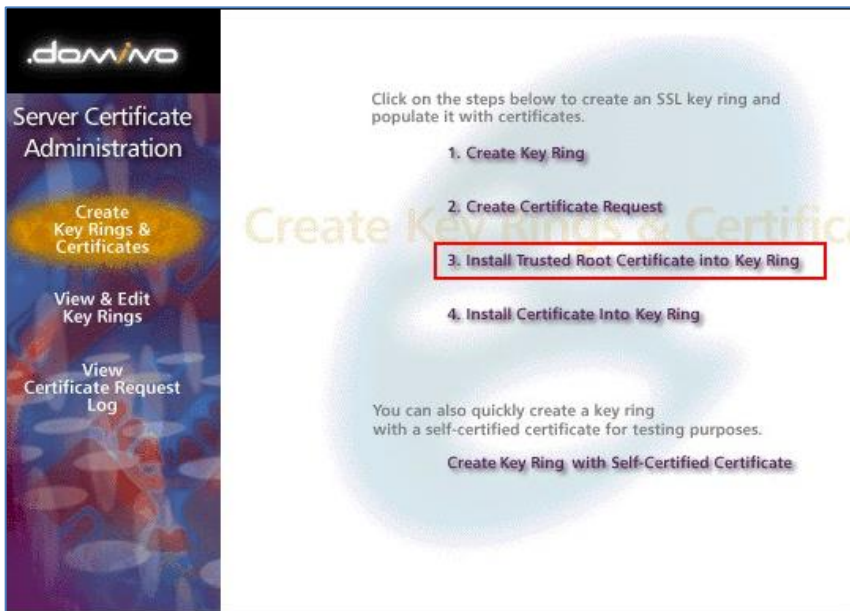


- 4 將此憑證資訊以另存新檔的方式儲存(儲存為附檔名為.cer)，所見的圖示將會變成 
- 5 請點擊憑證檔案，確認憑證網域、簽發者單位、有效期間是否為正常資訊

四、安裝方式

目前您的手上有 CER 的文本資訊(我們所提供給您的憑證核發完成信件)，因您的 CSR 由 Domino 伺服器直接產生，所以 KEY 檔案將會直接保留再 Domino 中，請您依照以下的步驟將簽發下來的 CER 資訊匯入 Domino 伺服器：

1 進入 Install Trusted Root Certificate into Key Ring



2 於 certificate Source 選擇 Clipboard

Install Trusted Root Certificate	
<p>Use this form to install the Certificate Authority Trusted Root certificate into the server key ring. If you haven't already done so, first obtain the Certificate Authority Trusted Root certificate by choosing "Accept This Authority In Your Server" from the main menu of Certificate Authority Web site. Note: This step of installing the Certificate Authority Trusted Root certificate into your server key ring is recommended before installing certificates signed by this Certificate Authority into the key ring.</p>	
Key Ring Information	Quick Help
<p>Key Ring File Name <input type="text" value="F:\otus\domain\data\filename.kyr"/></p>	<p>Specify the key ring file.</p>
Certificate Information	
<p>Certificate Label <input type="text"/></p> <p>Certificate Source <input type="radio"/> File <input checked="" type="radio"/> Clipboard</p> <p>Certificate from Clipboard: <input type="text"/></p>	<p>The identifier you'll see for this certificate when you choose "View & Edit Key Ring" from the main menu.</p> <p>The source of the certificate can be from a file or from the clipboard.</p> <p>Paste clipboard contents into this field.</p> <p>Note: The pasted certificate must include the "Begin Certificate" and "End Certificate" lines.</p>

3 於跳出之下方文字方框輸入憑證中心 根憑證(root 檔案) 文本資訊

(依據憑證類型不同，請與匯智索取)

4 再次進入 Install Trusted Root Certificate into Key Ring

5 於跳出之下方文字方框輸入憑證中心 根憑證(cross 檔案) 文本資訊

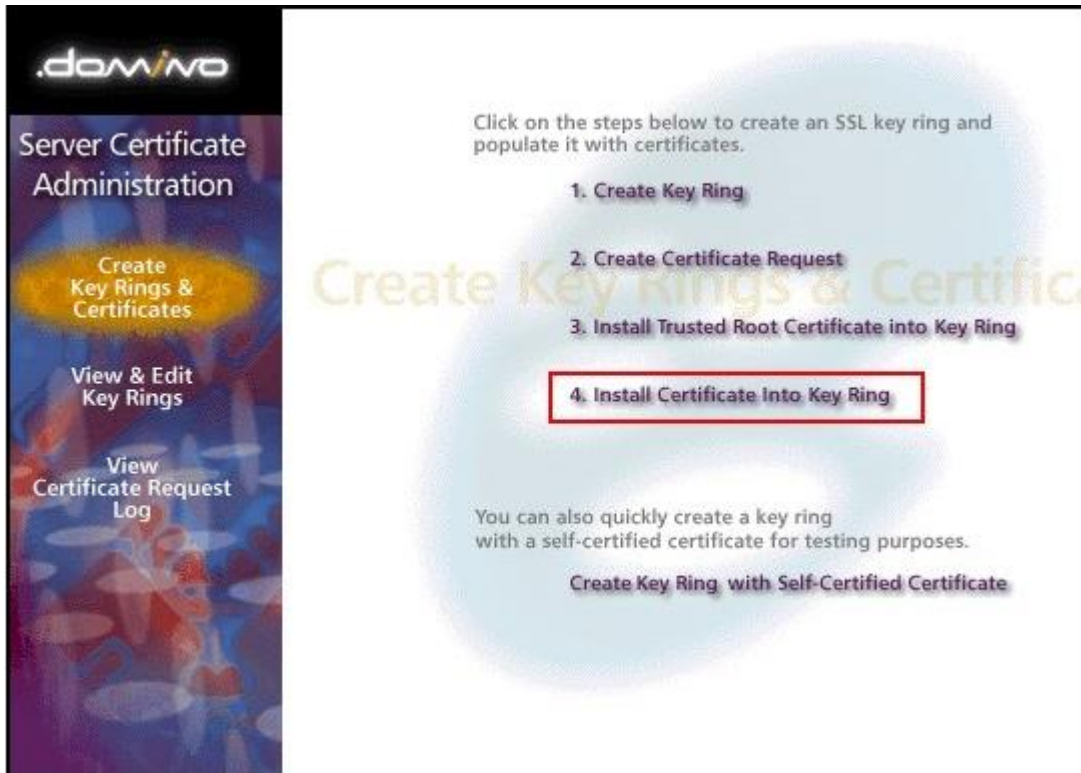
(依據憑證類型不同，請與匯智索取)

6 再次進入 Install Trusted Root Certificate into Key Ring

7 於跳出之下方文字方框輸入憑證中心 根憑證(intermedia 檔案) 文本資訊

(依據憑證類型不同，請與匯智索取)

8 進入 Install Certificate into Key Ring



9 於 certificate Source 選擇 Clipboard

10 於跳出之下方文字方框輸入憑證中心 憑證(cert 檔案) 文本資訊

(此訊息請參閱您的憑證開通信件)

五、檢查憑證安裝是否正確

您可以透過此驗證工具來確認憑證是否已經正確掛載：

GeoTrust：<http://geotrust.cloudmax.com.tw/OpenSSL/checkservercert.asp>

GlobalSign：<https://globalsign.sslabs.com/>