電子證書（伺服器）用戶指南

Microsoft IIS 10.0 適用

修訂日期：2025 年 4 月

目錄

A. 電子證書（伺服器）申請人指引

香港郵政核證機關在收到及批核電子證書（伺服器）申請後，會向獲授權代表發出主旨為 “Submission of Certificate Signing Request (CSR)” 的電郵，要求獲授權代表到香港郵政核證機關的網站提交 CSR。

本用戶指南旨在提供參考給電子證書（伺服器）申請人如何使用 Microsoft Internet Information Server (IIS) 10.0 產生配對密碼匙和證書簽署要求(CSR)的詳細步驟。包含公匙的 CSR 將會提交到香港郵政核證機關以作證書簽署。

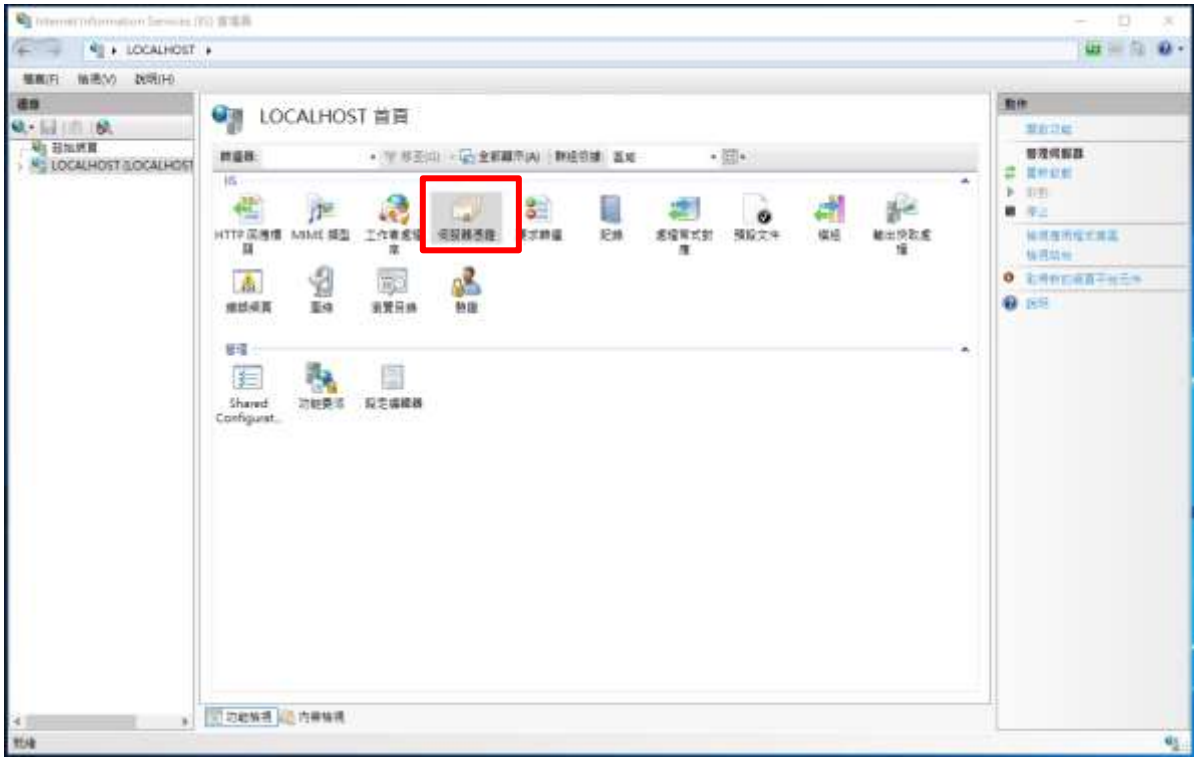
如閣下在證書簽發後遺失密碼匙，您將不能安裝或使用該證書。因此強烈建議閣下於**提交證書簽署要求(CSR)前**及**完成安裝伺服器證書後**均為密碼匙進行備份。有關備份及還原密碼匙的方法，請參閱以下部分的詳細步驟：

新申請及續期申請

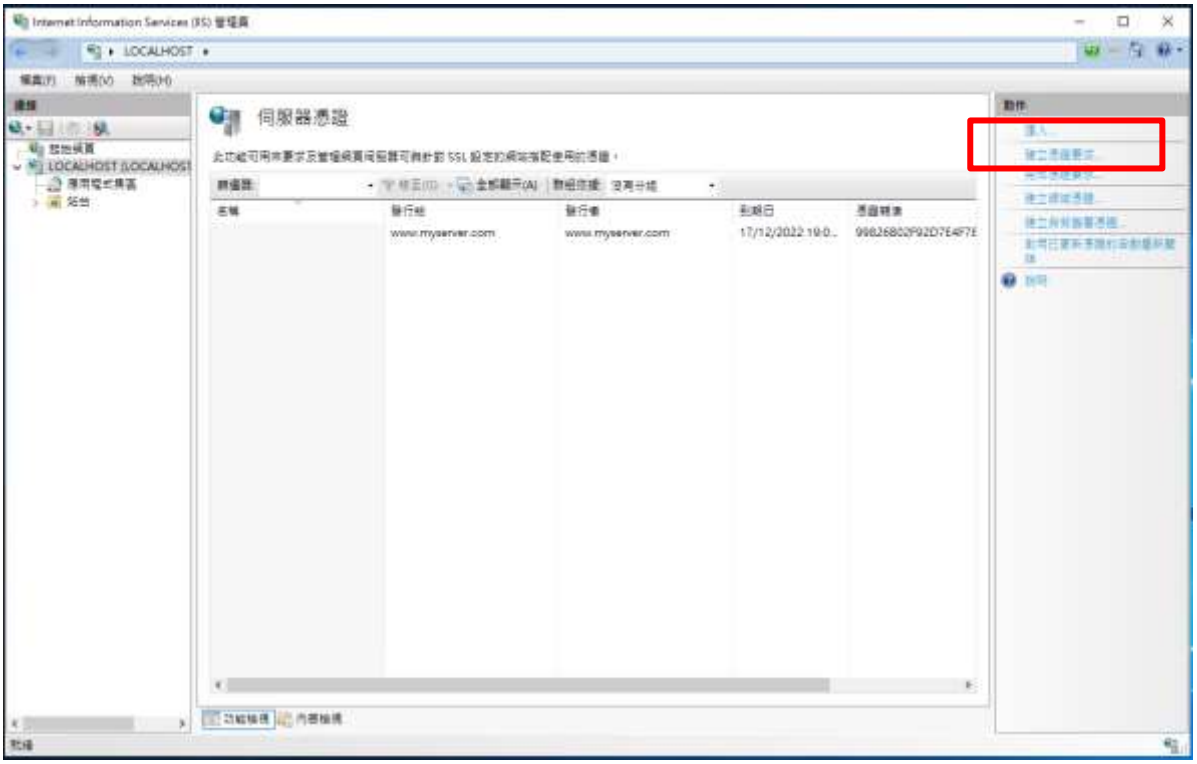
首次及續期申請電子證書（伺服器），請參閱以下部分的詳細步驟：

B. 產生證書簽署要求(CSR)

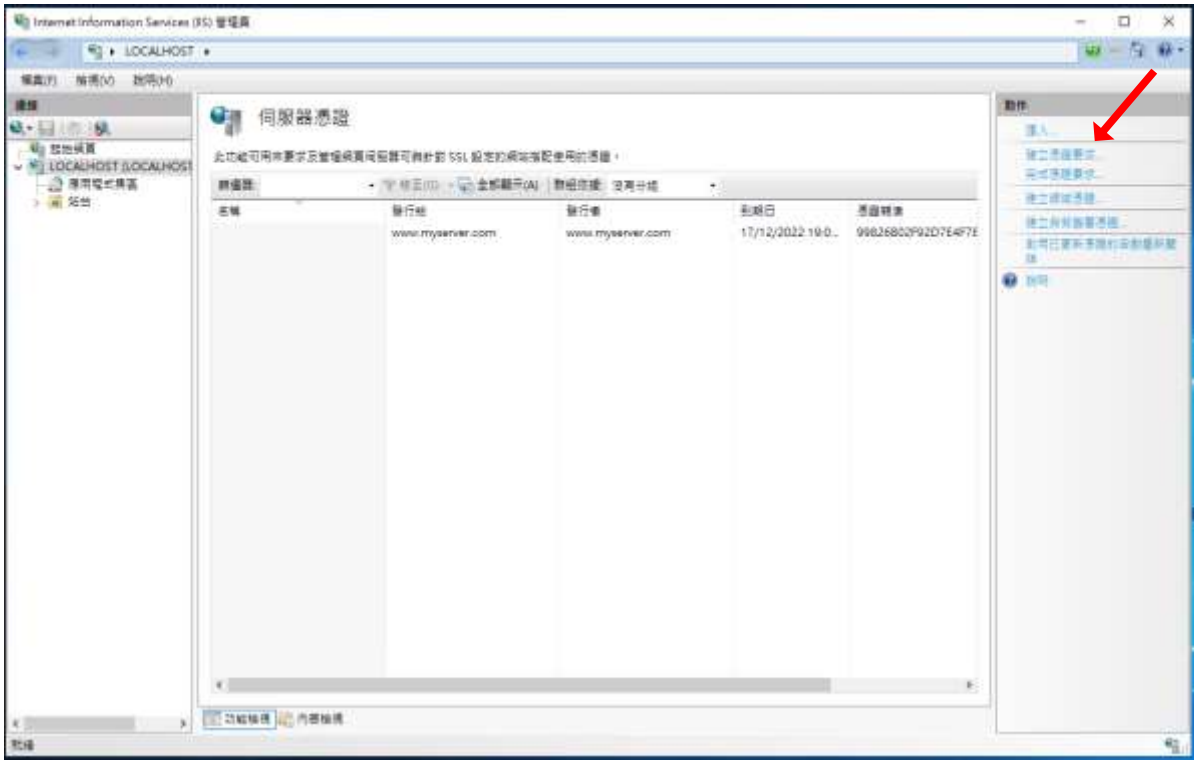
1. 按[開始]>[系統管理工具]>[Internet Information Services (IIS) 管理員]來啟動網際網路資訊服務 (IIS) 管理員。
2. 在[Internet Information Services (IIS) 管理員]視窗內，展開[網站]及選擇您的網站，然後按[伺服器憑證]。



3. 在右手邊[動作]一欄內，按[建立憑證要求]。



*注意：*新申請及續期申請電子證書（伺服器）的步驟相同，即使是續期電子證書，請不要使用[更新]，要選擇[建立憑證要求]。



4. 輸入您的一般名稱和組織，以及組織單位，並選擇“HK”作為[國家 (地區)]，輸入“Hong Kong”作為[縣市/位置]及[省份]，然後按[下一步]。

注意：請確定於「發給」一欄顯示正確的登記域名(即伺服器名稱)及「國家(地區)」一欄顯示「HK」。

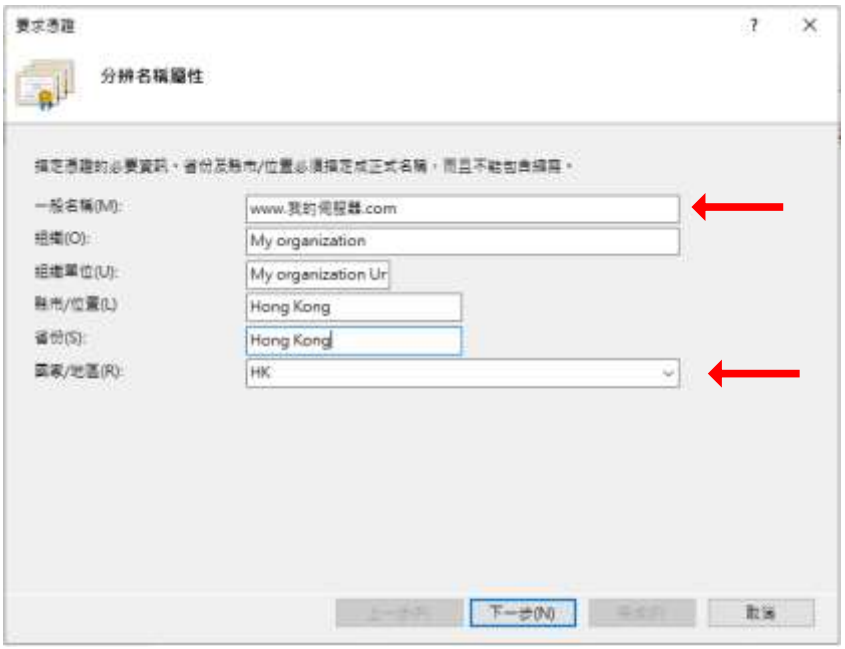
注意：若申請電子證書（伺服器）“多域版”或延伸認證電子證書（伺服器）“多域版”，請在「一般名稱」一欄中，輸入與申請表格中所填寫的「用作電子證書主體名稱的伺服器名稱」相同的登記伺服器名稱。而「電子證書主體別名內的額外伺服器名稱」，則無需在產生證書簽署要求(CSR)過程中輸入，香港郵政核證機關系統在簽發證書時，會根據申請表格所申請的資料自動填寫。

*若申請電子證書（伺服器）“通用版”，請在「通用名稱」一欄中，輸入與申請表格中所填寫的「有通配符的電子證書伺服器名稱」相同的登記伺服器名稱(伺服器名稱的最左部份需包括有通配符「＊」的部份)。例如 *.myserver.com。*

注意：若申請中文伺服器名称的電子證書（伺服器）

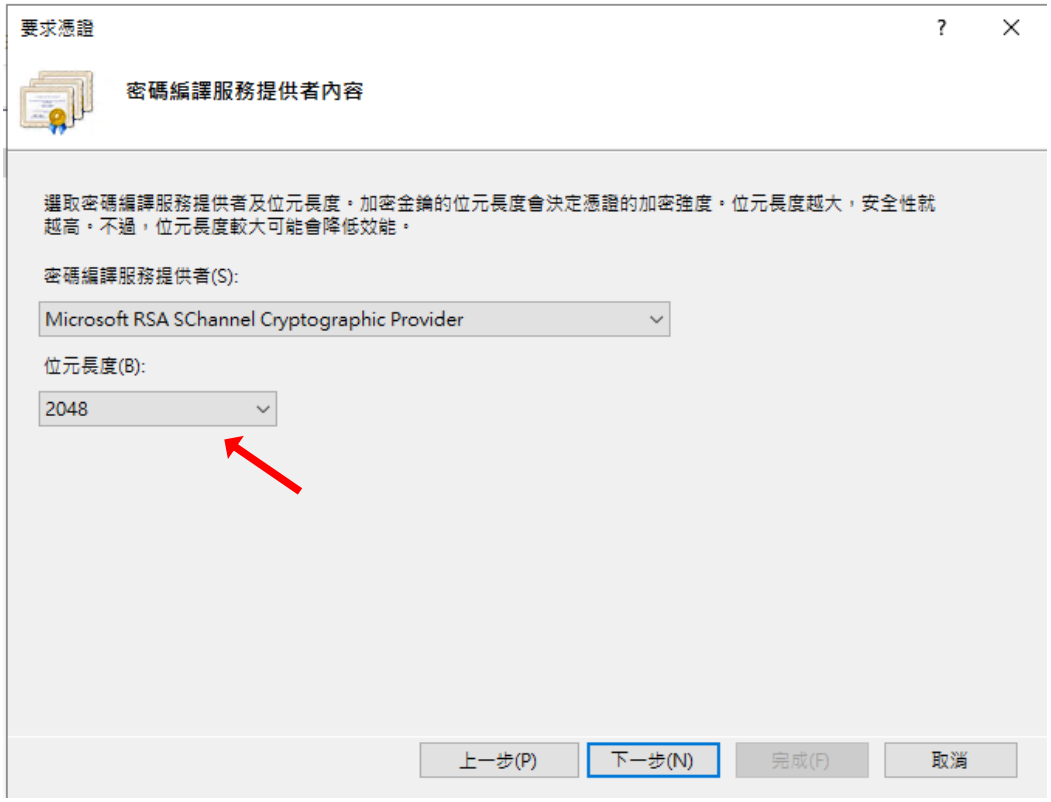
選項 1：請在「通用名稱」一欄中，輸入與申請表格中所填寫的「用作電子證書主體名稱的伺服器名稱」相同的登記伺服器名稱。

選項 2: 請使用國際網域名稱轉換工具把中文網域名稱轉換成 ASCII 字元，並可以在"通用名稱"一欄中輸入轉換後的名稱。

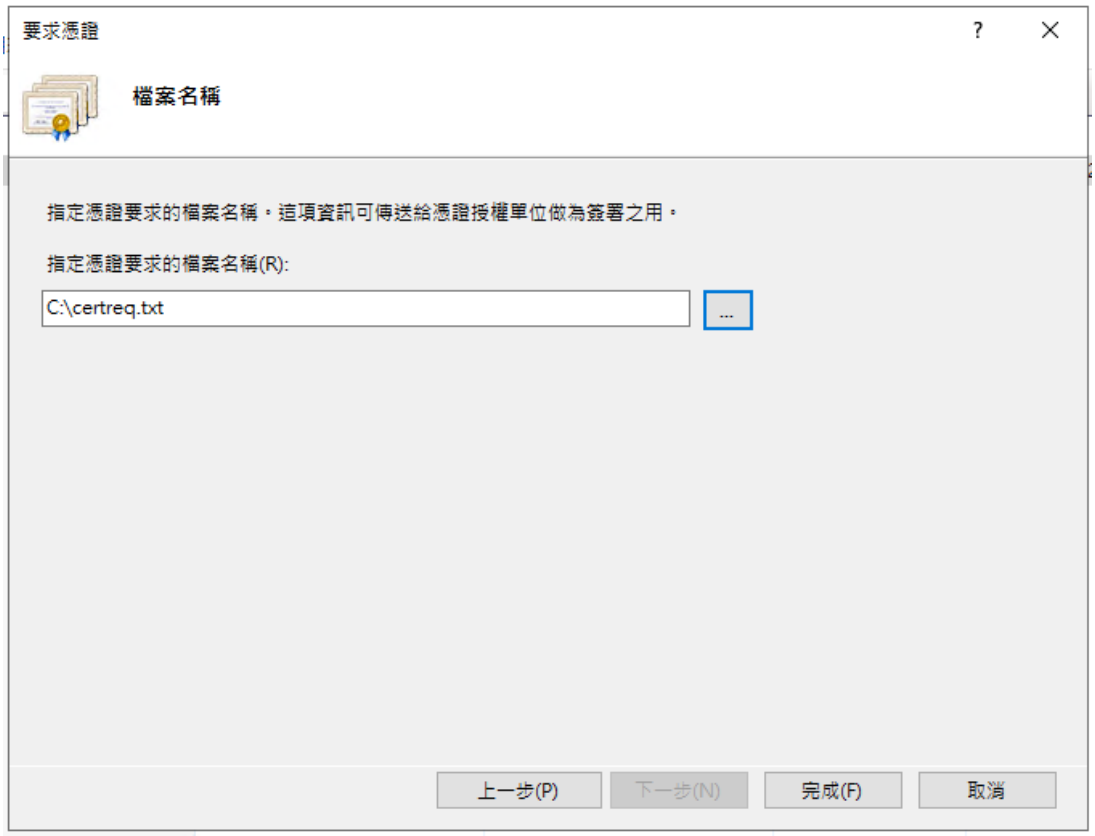


5. 選擇 “Microsoft RSA SChannel Cryptographic Provider” 作為[密碼編譯服務提供者]及 “2048” 作為密碼匙的[位元長度]，然後按[下一步]。

注意:小於 2048 位元的密碼匙或未能提供足夠保密程度，相反大於 2048 位元有可能與某些瀏覽器不兼容。建議選擇長度為 2048 位元的密碼匙，從而提供較佳的保密程度。

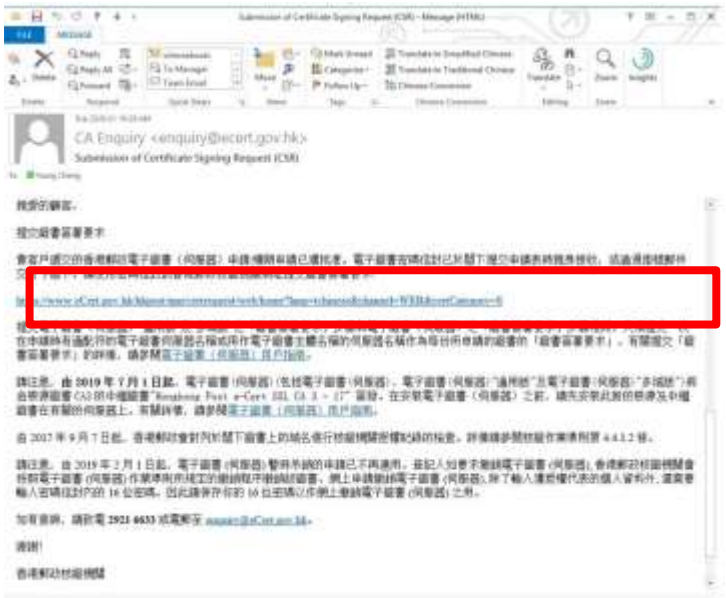


6. 輸入新憑證名稱 (或接受預設) 及按[完成]來關閉精靈。



C. 提交證書簽署要求(CSR)

1. 在香港郵政核證機關發出主旨為 “Submission of Certificate Signing Request (CSR)” 的電郵內按一下超連結以連線至香港郵政核證機關的網站。



2. 輸入[伺服器名稱]、印於密碼信封面的[參考編號](九位數字)及印於密碼 信封內的[電子證書密碼](十六位數字)，然後按[提交]。

3. 按[提交]確認申請資料。(如發現資料不正確，請電郵至 enquiry@eCert.gov.hk 聯絡香港郵政核證機關。)

注意：若電子證書申請表格上提供了機構中文名稱和/或分部中文名稱，如要發出一張主體名稱為機構中文名稱的電子證書(伺服器)，請按[確認使用中文]鍵繼續。

4. 用文字編輯器(例如：記事本)開啟早前產生的證書簽署要求(CSR)及複製全部內容包括 "-----BEGIN NEW CERTIFICATE REQUEST-----" 及 "-----END NEW CERTIFICATE REQUEST-----"。(您可參考 B 部的步驟 6 的憑證要求檔案的位置。)

5. 在方格內貼上內容，然後按[提交]。

6. 按 [接受] 確認接受此證書。

7. 下載 Hongkong Post e-Cert (Server)證書。

注意：

1. *您也可以從搜尋及下載證書網頁下載您的電子證書（伺服器）。*
   https://www.ecert.gov.hk/tc/sc/index_c.html
2. *由 2019 年 7 月 1 日起，電子證書（伺服器）將由根源證書Root CA3 的中繼證書"Hongkong Post e-Cert SSL CA 3 - 17" 簽發。*

   持有 2019 年 7 月 1 日或以後簽發的電子證書（伺服器）的登記人，須進行以下改動，以便安裝了由根源證書Root CA3 簽發的電子證書（伺服器）的網站繼續受到一般網頁瀏覽器的信任：

   安裝由根源證書Root CA3 簽發的中繼證書"Hongkong Post e-Cert SSL CA 3 - 17"。下載地址如下：

   http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt

   安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書"Hongkong Post Root CA 3"。

   下載地址如下：

   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt
3. *由2022年1月21日起，延伸認證電子證書（伺服器）將由根源證書Root CA3的中繼證書"Hongkong Post e-Cert EV SSL CA 3 - 17" 簽發。*

   持有2022年1月21日或以後簽發的延伸認證電子證書（伺服器）的登記人，須進行以下改動，以便安裝了由根源證書Root CA3簽發的延伸認證電子證書（伺服器）的網站繼續受到一般網頁瀏覽器的信任：

   安裝由根源證書 Root CA3簽發的中繼證書"Hongkong Post e-Cert EV SSL CA 3 - 17"。下載地址如下：

   http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt

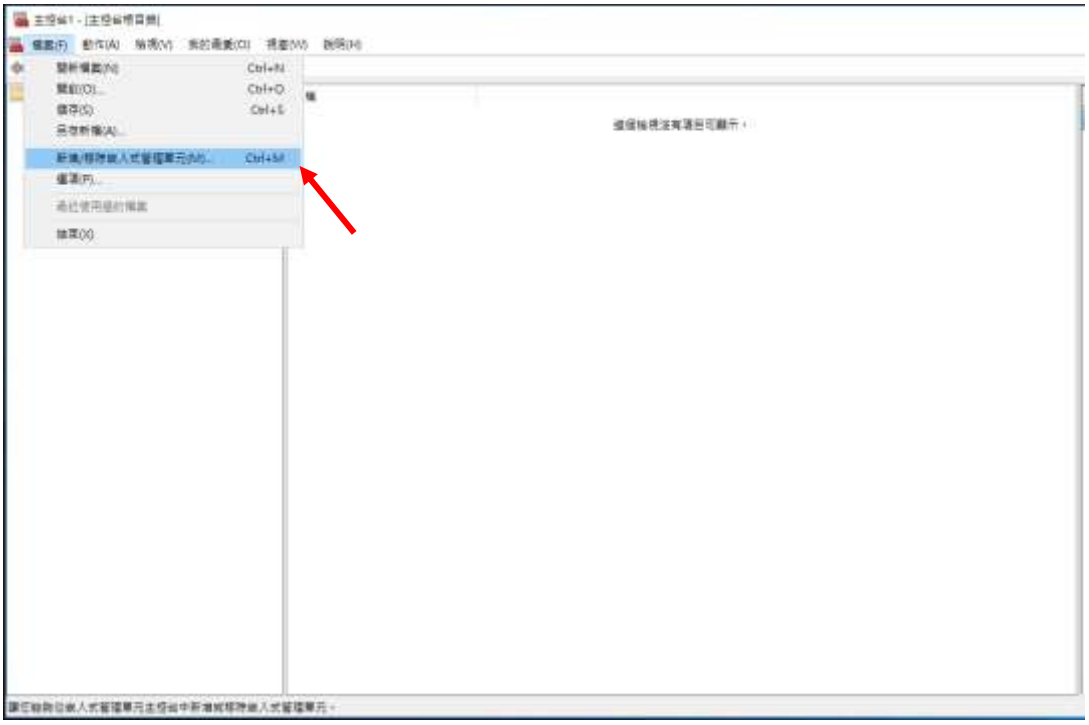
   安裝由根源證書 GlobalSign Root CA - R3 簽發的交叉證書"Hongkong Post Root CA 3"。

   下載地址如下：

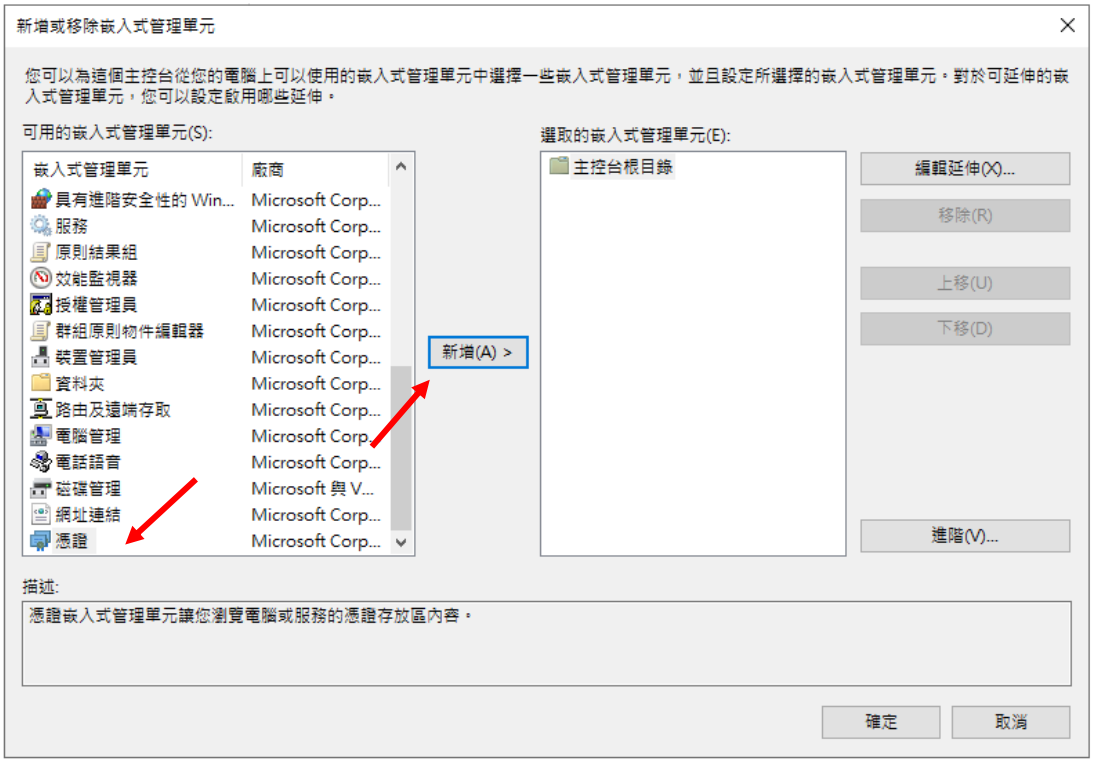
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. 安裝中繼 / 交叉證書

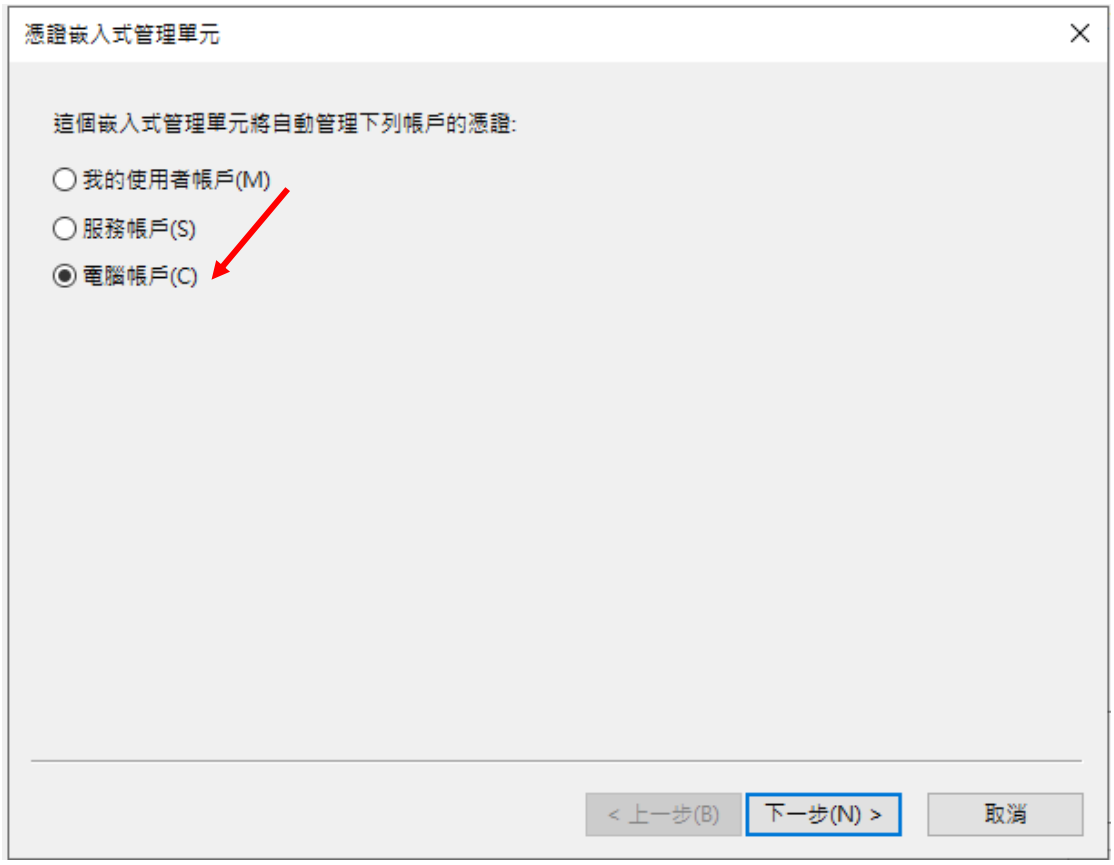
1. 按 [開始] > [執行]，然後輸入 “mmc” 及按[確定] 來啟動 Microsoft Management Console (MMC)，然後從[檔案]選單中選取[新增/移除嵌入式管理單元]。



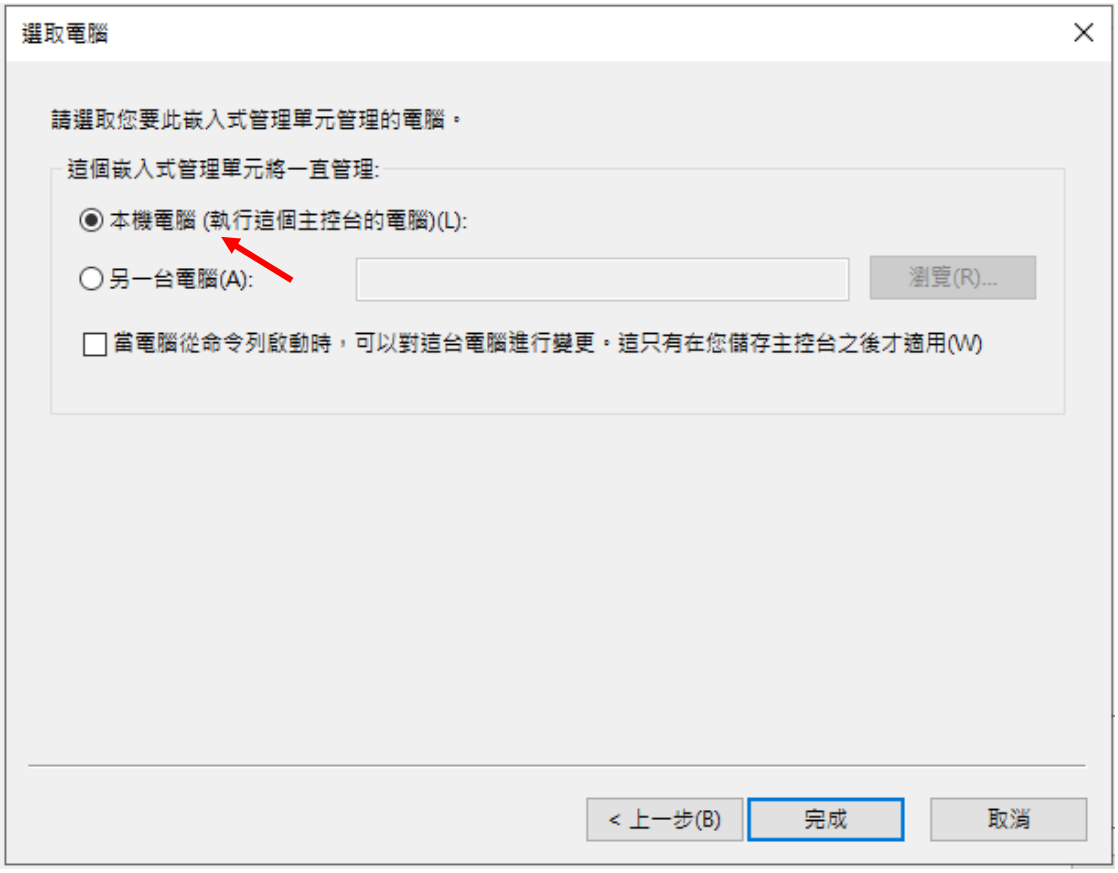
2. 選擇[憑證]，然後按[新增]。



3. 選擇[電腦帳戶]，然後按[下一步]。



4. 選擇[本機電腦]，然後按[完成]。



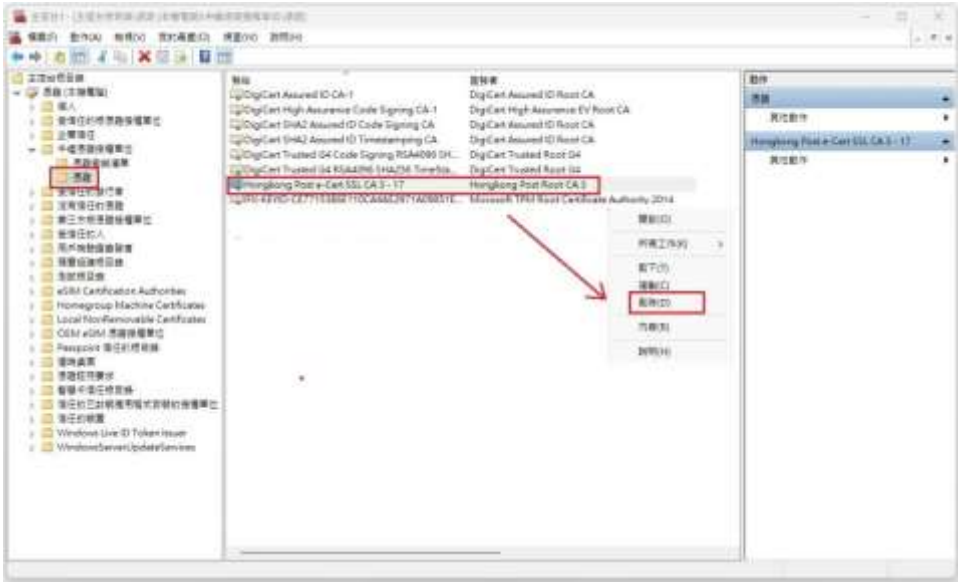
以下內容以 **"Hongkong Post e-Cert SSL CA 3 - 17"** 中繼證書為例子。

注意：

*由 2025 年 5 月 1 日起，電子證書（伺服器）會以新中繼證書簽發。在安裝 2025 年 5 月 1 日或之後發出的電子證書（伺服器）時，**請先移除舊有中繼證書（如適用），然後在相關伺服器上安裝新的中繼證書**。*

移除舊有中繼證書（如適用）

展開 [中繼憑證授權單位]，選擇 [憑證]，及以滑鼠右鍵按一下選擇舊有中繼證書[Hongkong Post e-Cert SSL CA 3 - 17]，然後選擇 [刪除]。

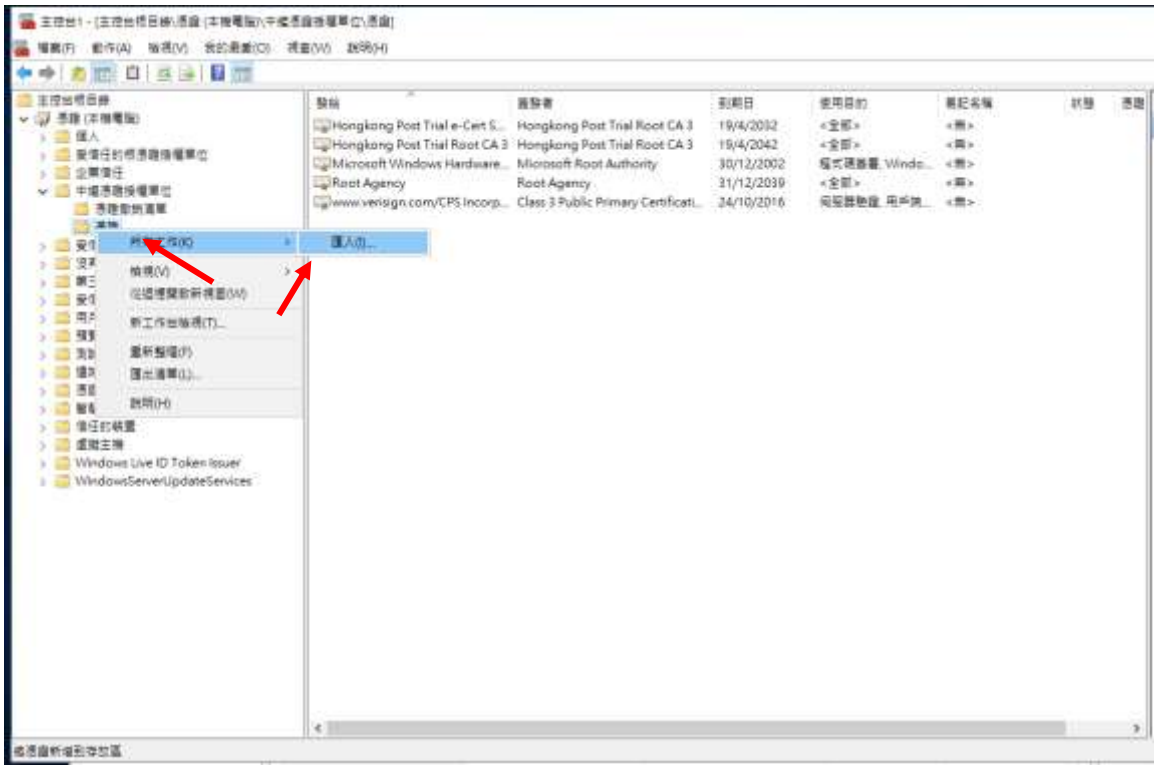


選擇 [是] 確定刪除。

以下內容以 **"Hongkong Post e-Cert SSL CA 3 - 17"** 中繼證書為例子。

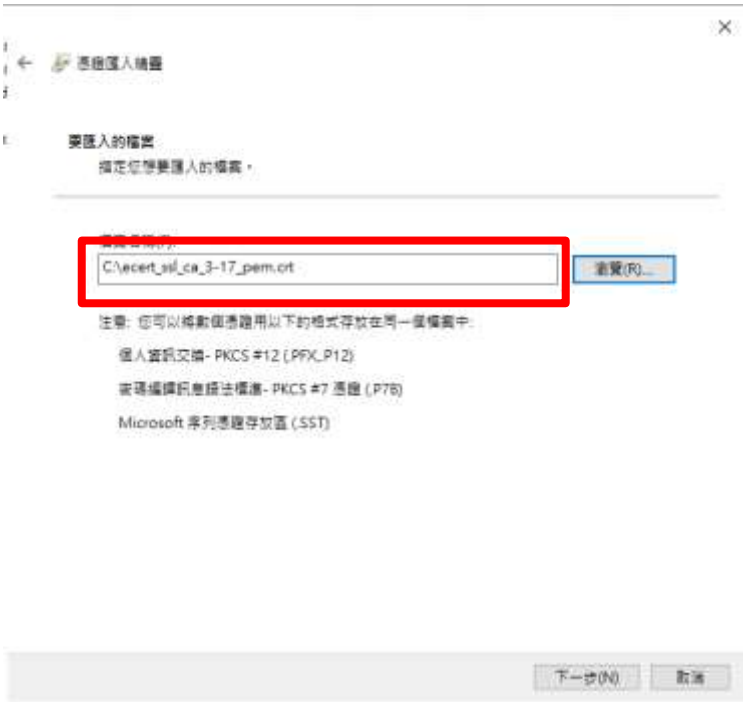
安裝中繼 / 交叉證書

5. 展開[中繼憑證授權]及以滑鼠右鍵按一下[憑證]，然後選擇[所有工作]>[匯入]。

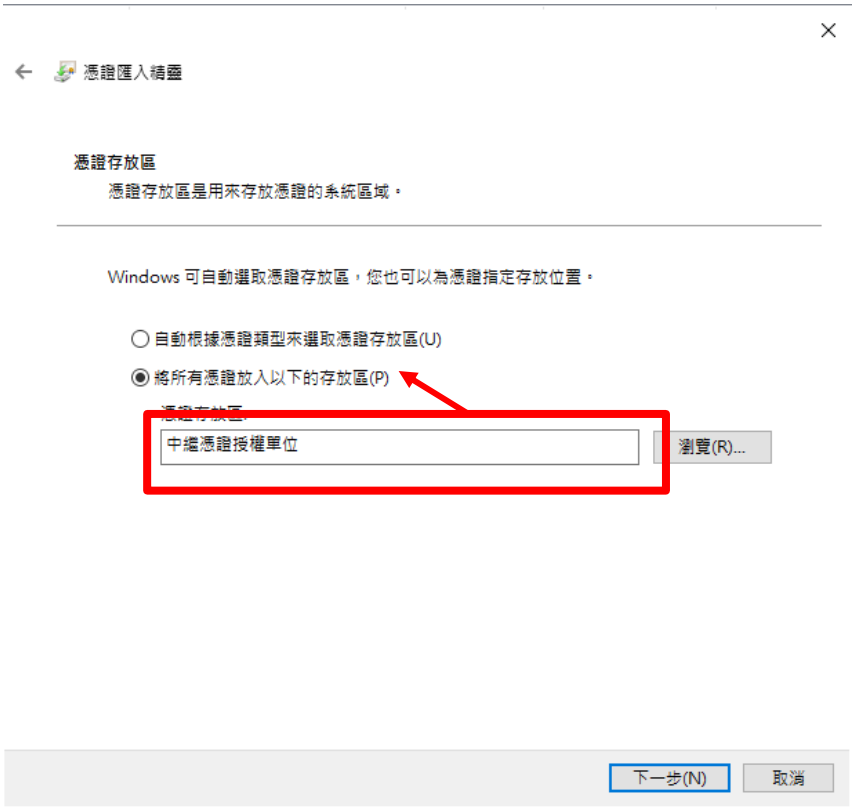


6. 在[憑證匯入精靈]內，按[下一步]繼續。

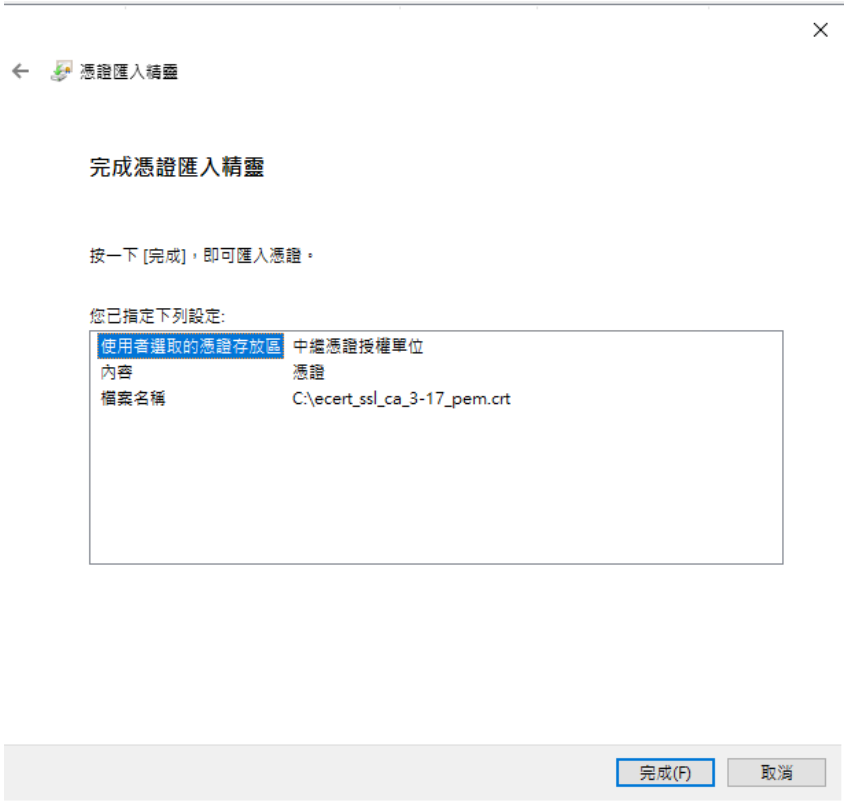
7. 按[瀏覽]指定早前於 C 部的步驟 7 下載的 "**Hongkong Post e-Cert SSL CA 3 – 17**" 中繼證書 (ecert_ssl_ca_3-17_pem.crt)，然後按[下一步]。



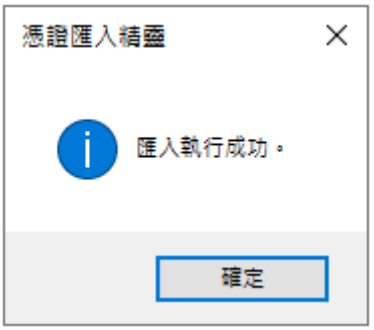
8. 選擇[將所有憑證放入以下的存放區]，並選擇中繼憑證授權單位為憑證存放區，然後按[下一步]。

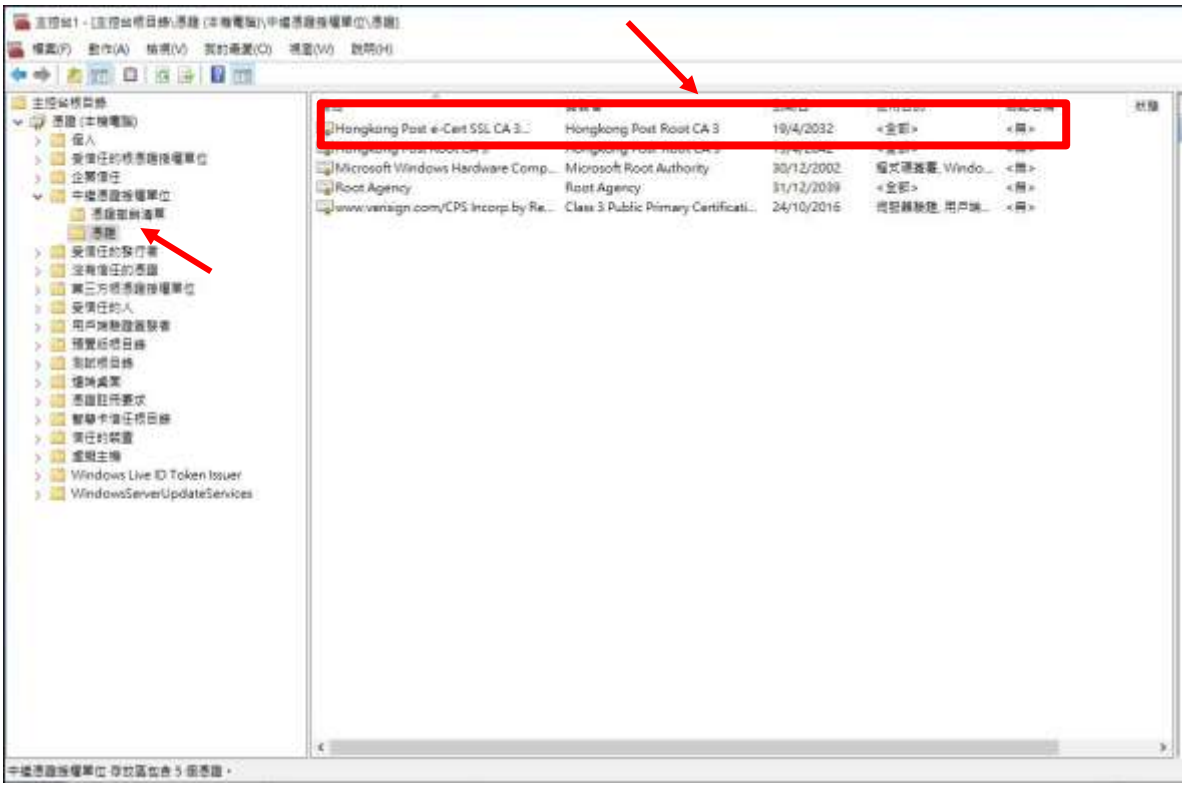


9. 按[完成]來關閉精靈。



10. 按[確定]來完成。



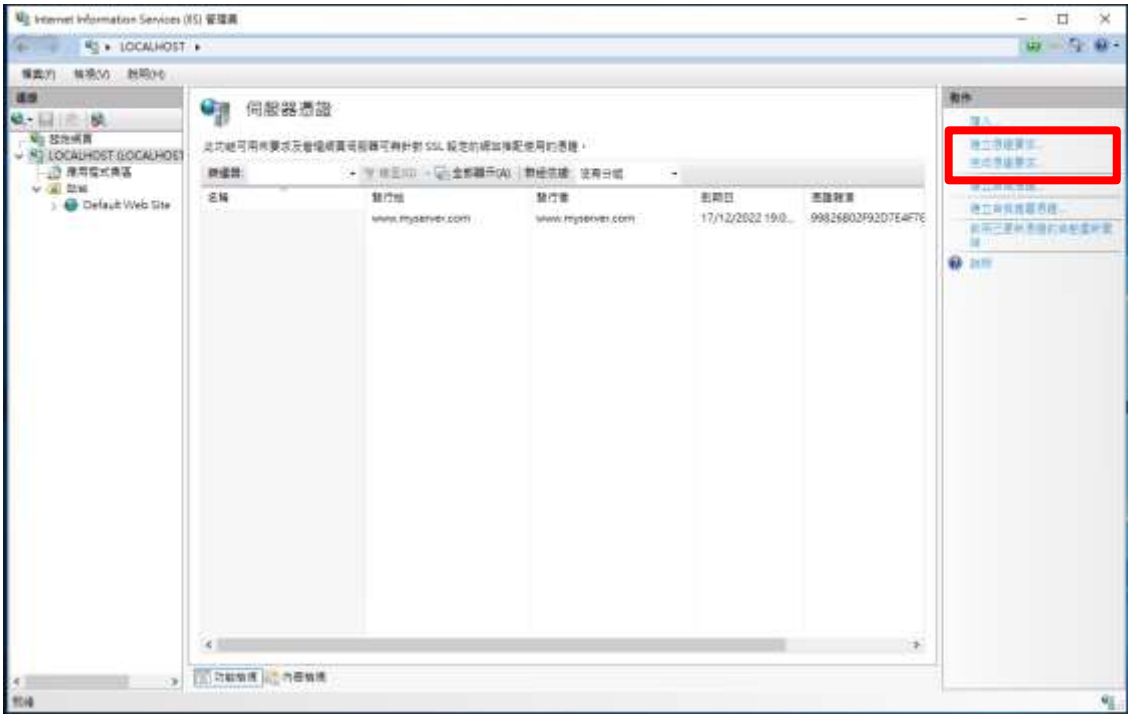


圖表 1: “Hongkong Post e-Cert SSL CA 3 – 17” 已成功安裝

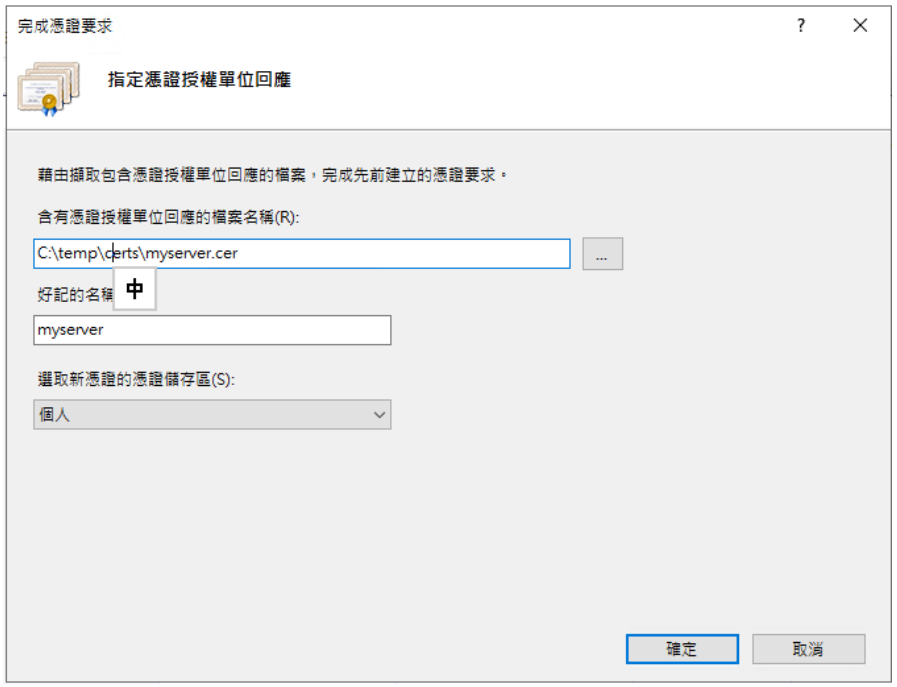
重複步驟 5 到步驟 10 以安裝通過 C 部分步驟 7 下載的交叉證書 (root_ca_3_x_gsca_r3_pem.crt)。

E. 安裝伺服器證書

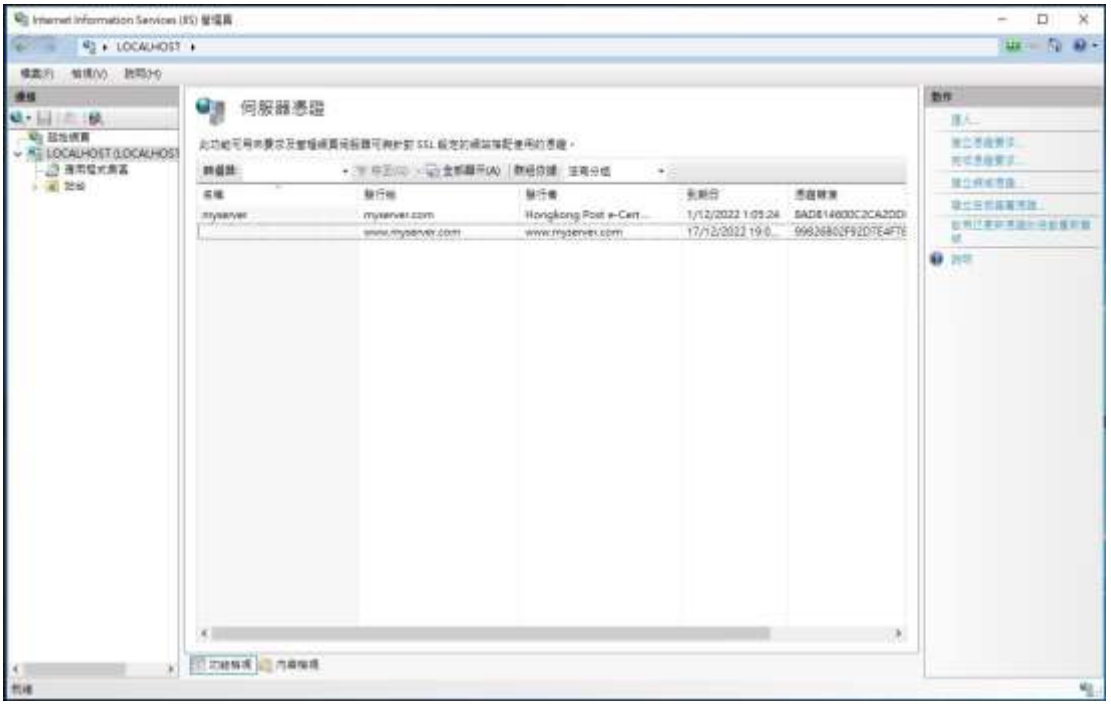
1. 在[Internet Information Services 管理員]視窗內，選擇您的網站，然後按[伺服器憑證]。在右手邊動作一欄內，按[完成憑證要求]。



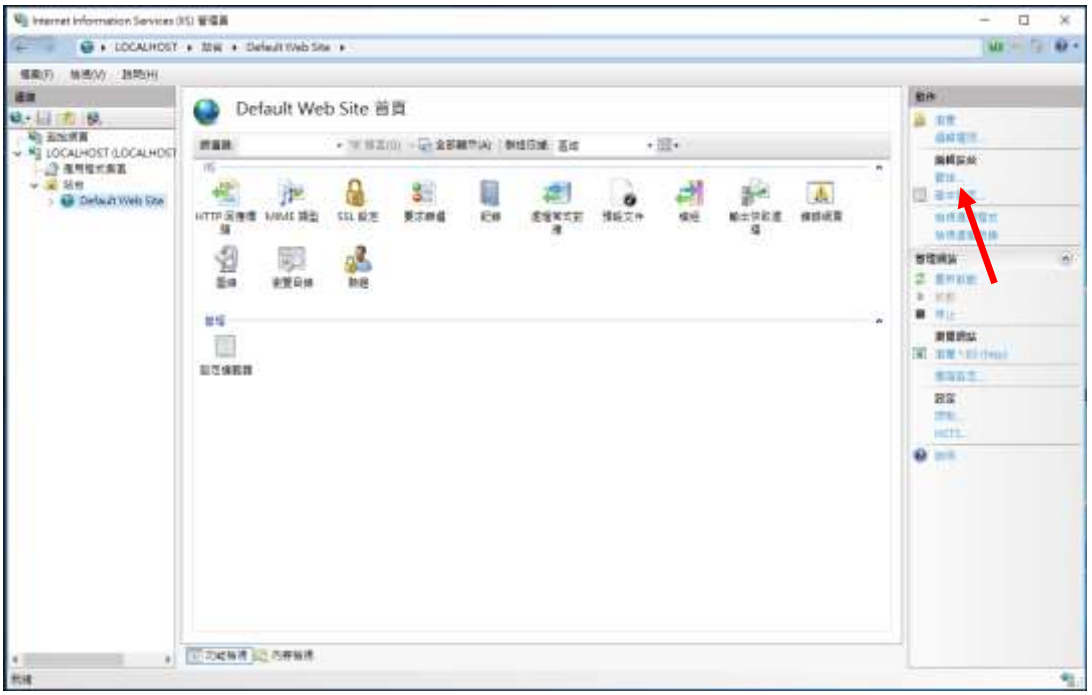
2. 按[瀏覽]指定早前於 C 部的步驟 7 下載的 “Hongkong Post e-Cert (Server)” 證書及輸入[好記的名稱]，然後按[確定]。



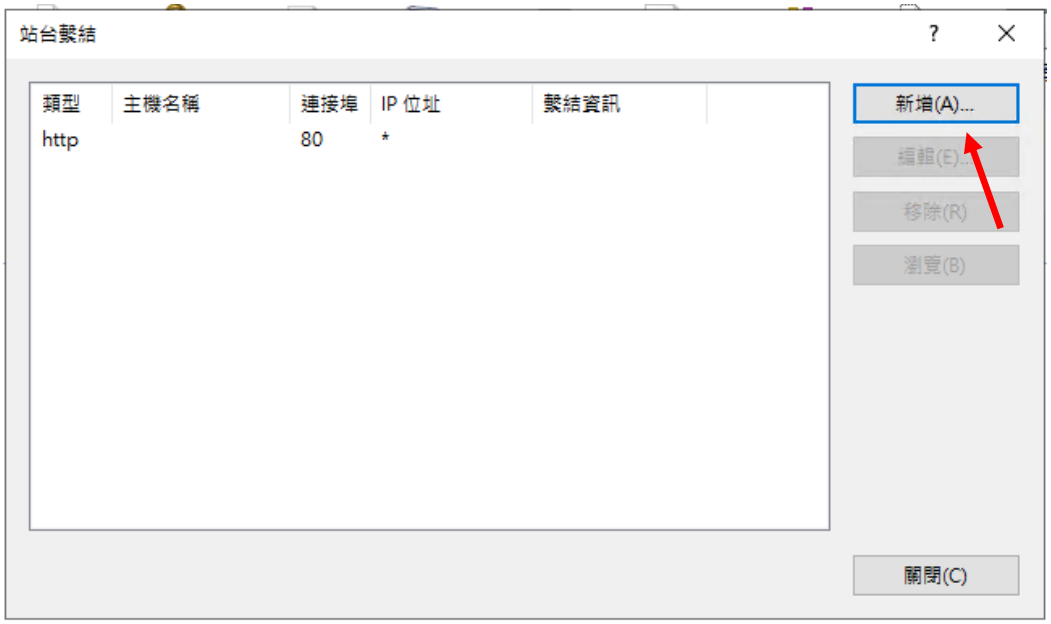
3. “Hongkong Post e-Cert (Server)” 證書已成功安裝。



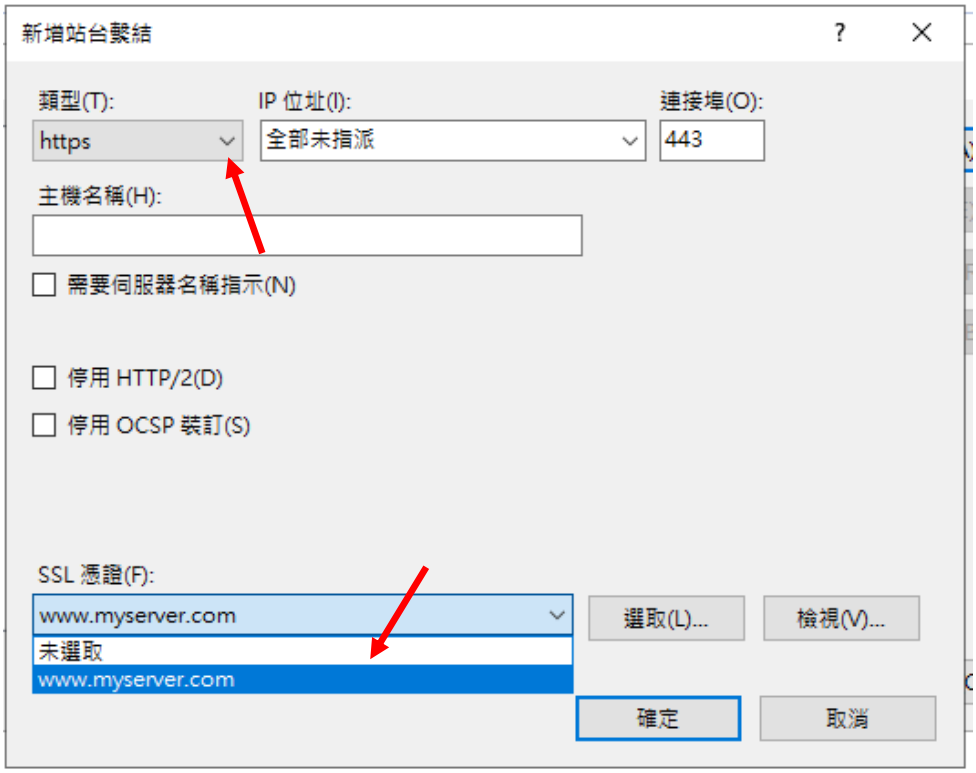
4. 選擇你需要繫結的網站，然後按[繫結]。



5. 按[新增]。

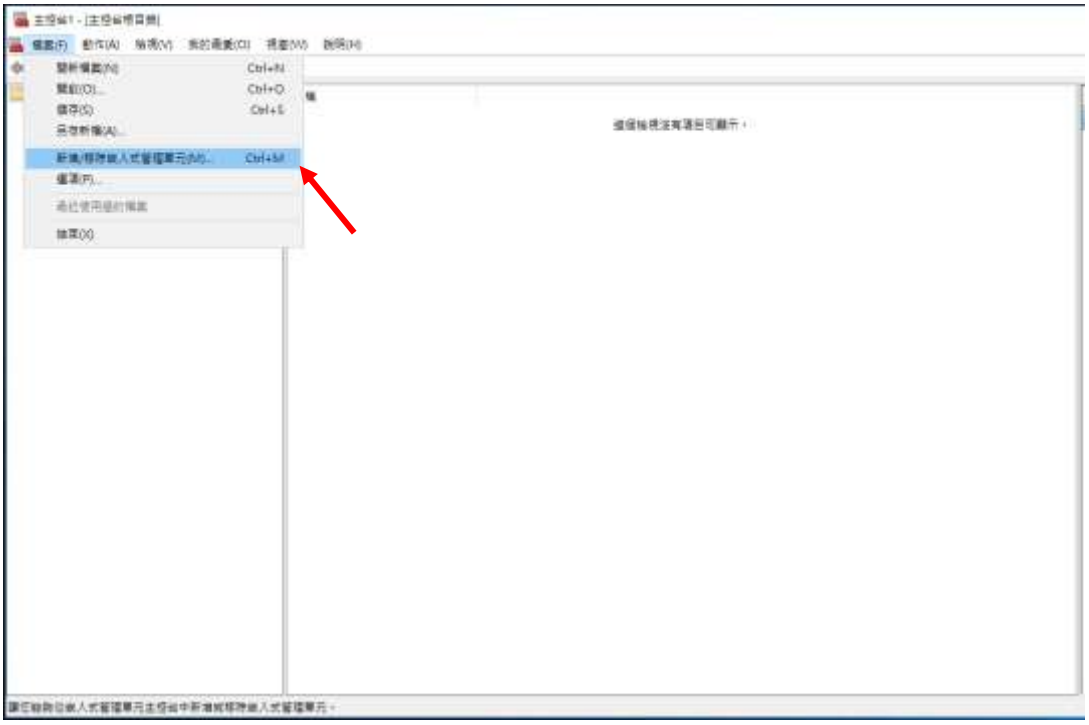


6. 選取[https]及相對應的 SSL 憑證及確定。

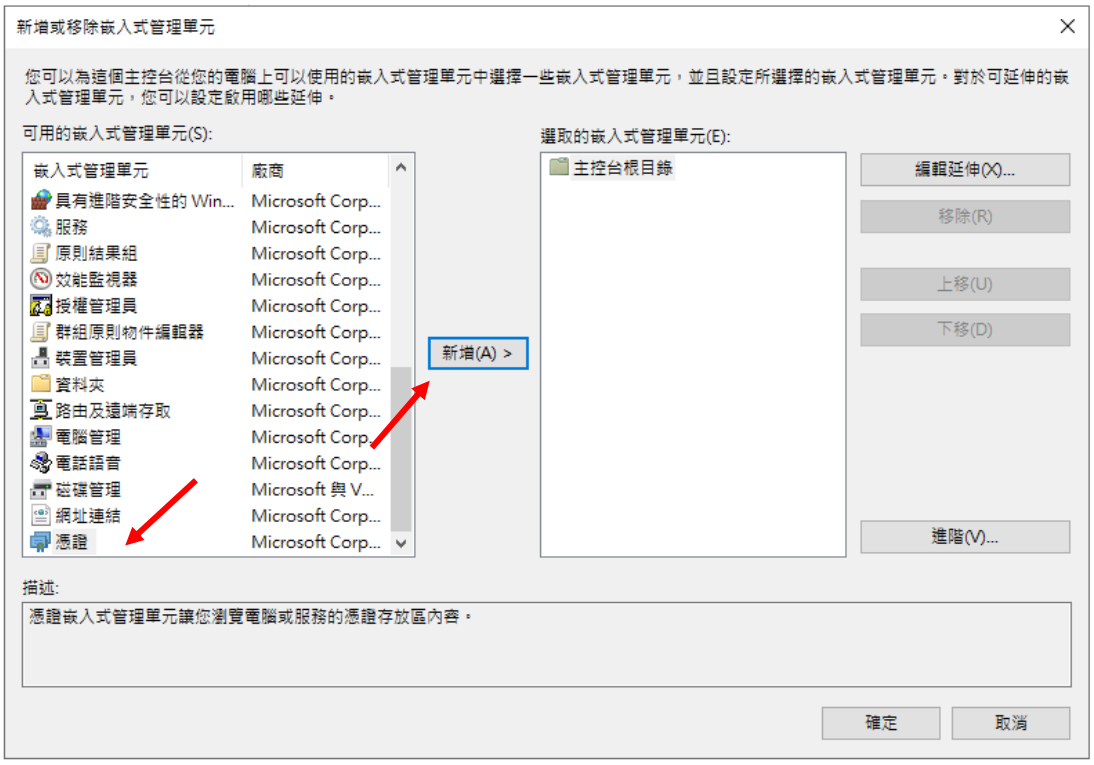


F. 備份密碼匙

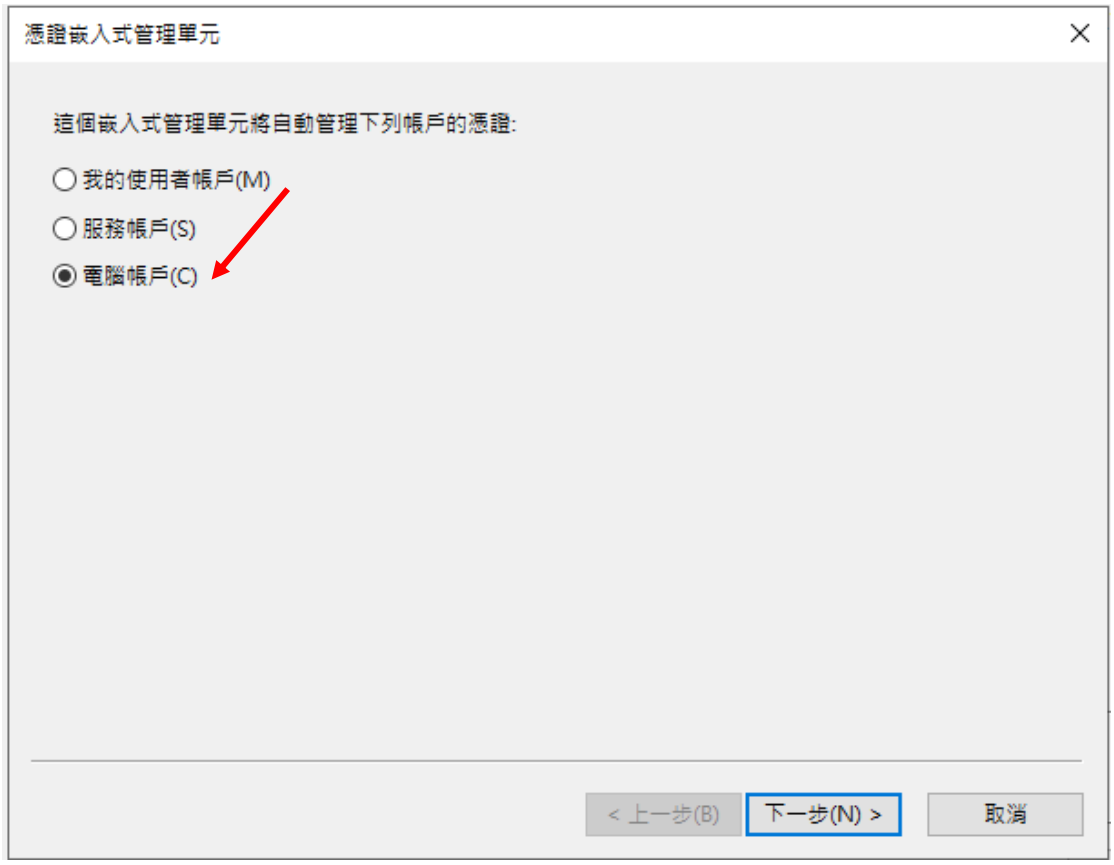
1. 按[開始]>[執行]，然後輸入 “mmc” 及按[確定]來啟動 Microsoft Management Console (MMC)，然後從[檔案]選單中選取[新增/移除嵌入式管理單元]。



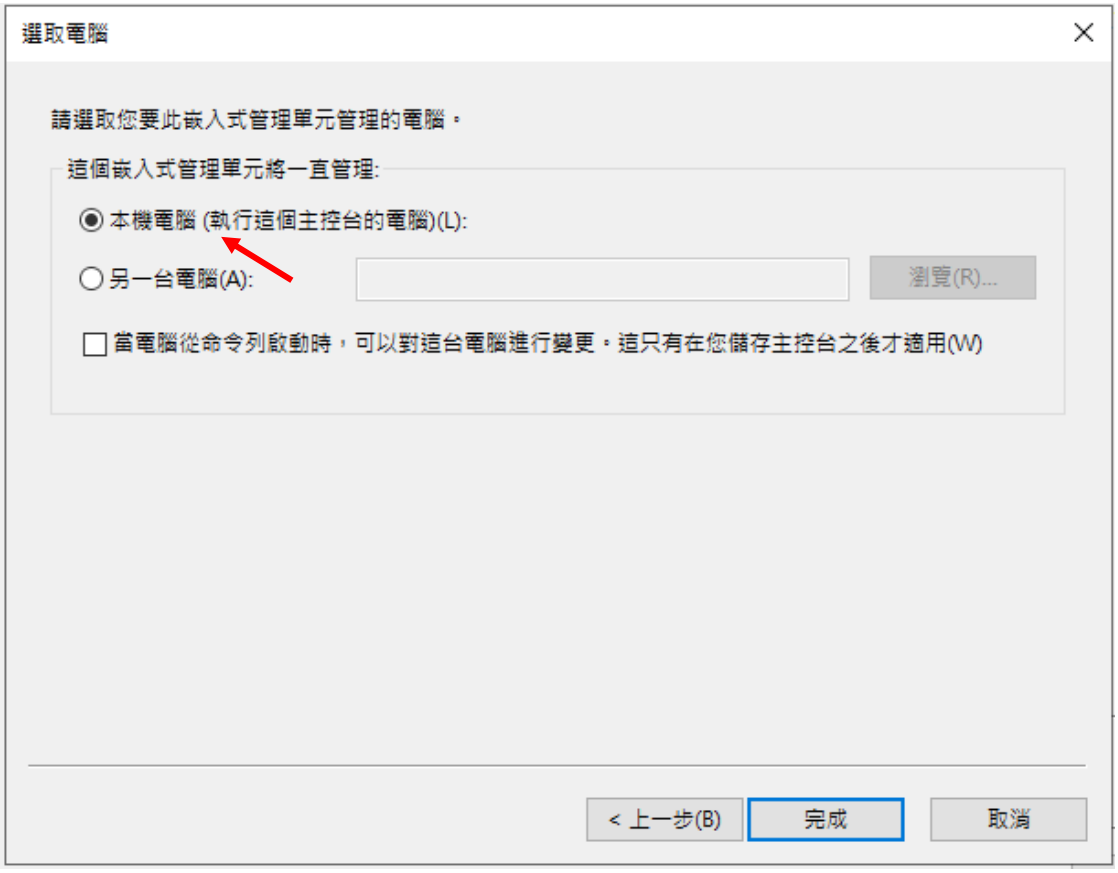
2. 選擇[憑證]，然後按[新增]。



3. 選擇[電腦帳戶]，然後按[下一步]。

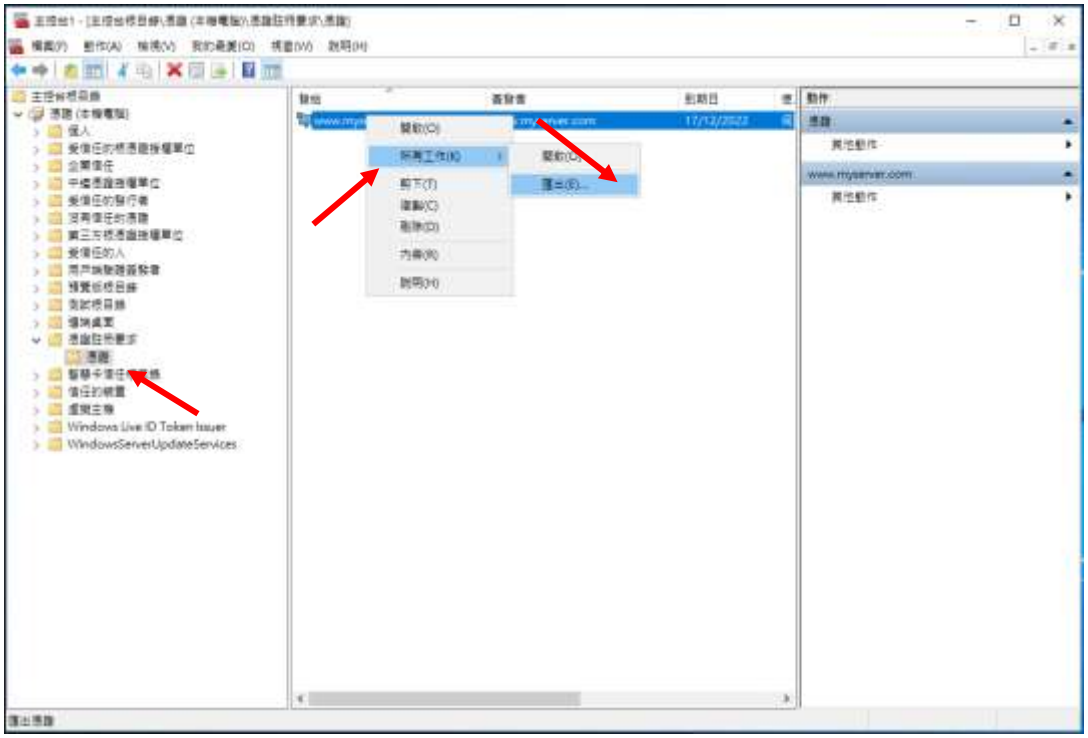


4. 選擇[本機電腦]，然後按[完成]。

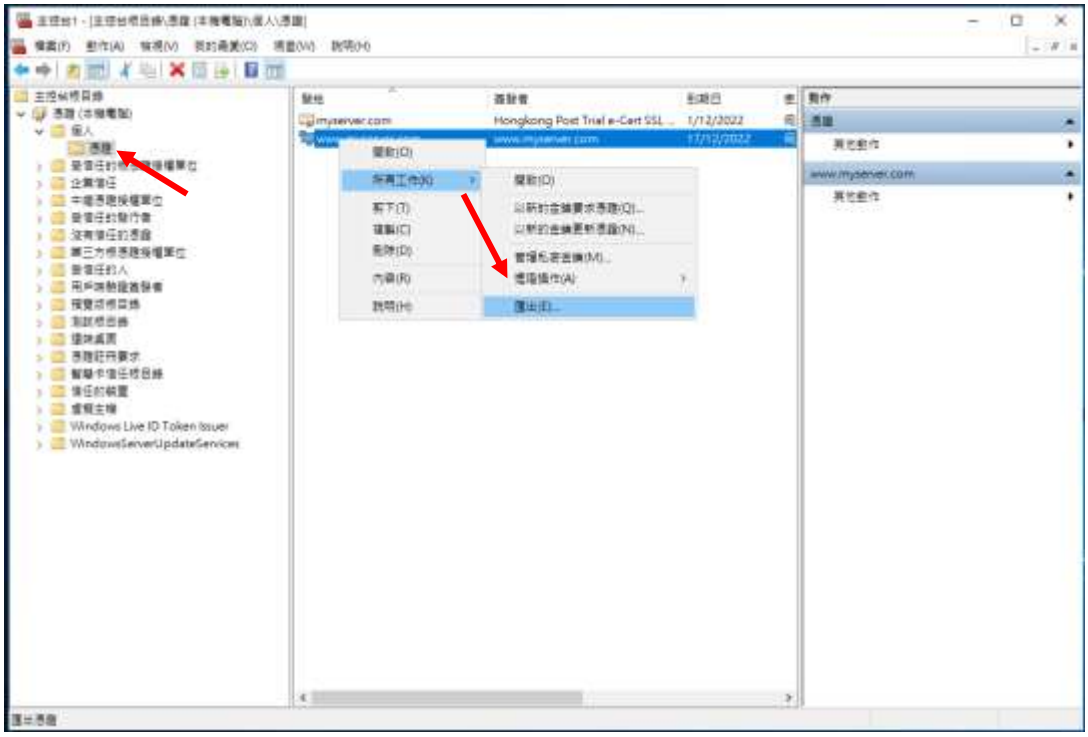


5. 備份密碼匙

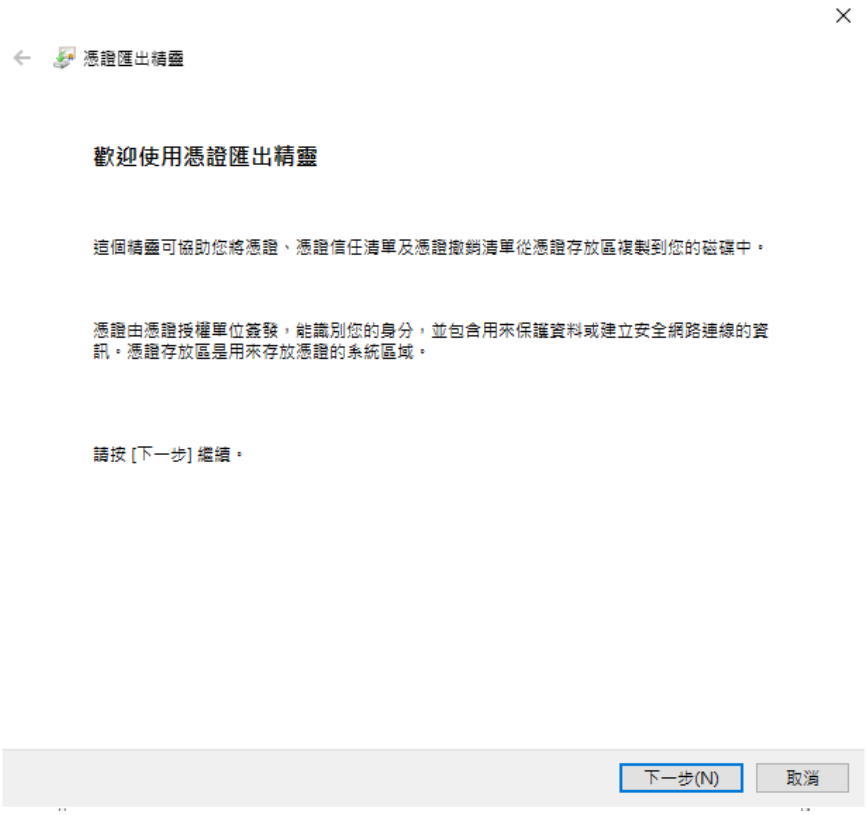
- 備份憑證註冊要求的密碼匙，請展開[憑證註冊要求](或於某些系統稱為[REQUESTS])。) 。按一下[憑證]，選擇你剛建立的憑證註冊要求，然後以滑鼠右鍵選擇[所有工作]>[匯出]。



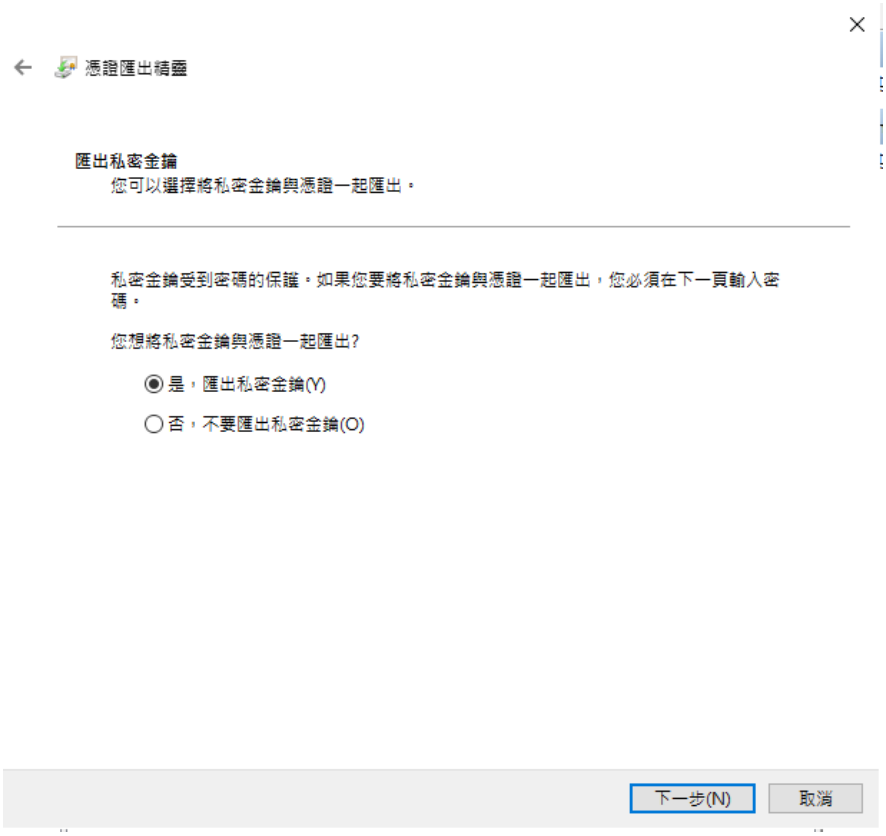
- 備份現有證書的密碼匙，展開[個人]及以滑鼠右鍵按一下[憑證]，選擇你需要備份的證書，然後以滑鼠右鍵按一下[所有工作]>[匯出]。



6. 在[憑證匯出精靈]內，按[下一步]繼續。



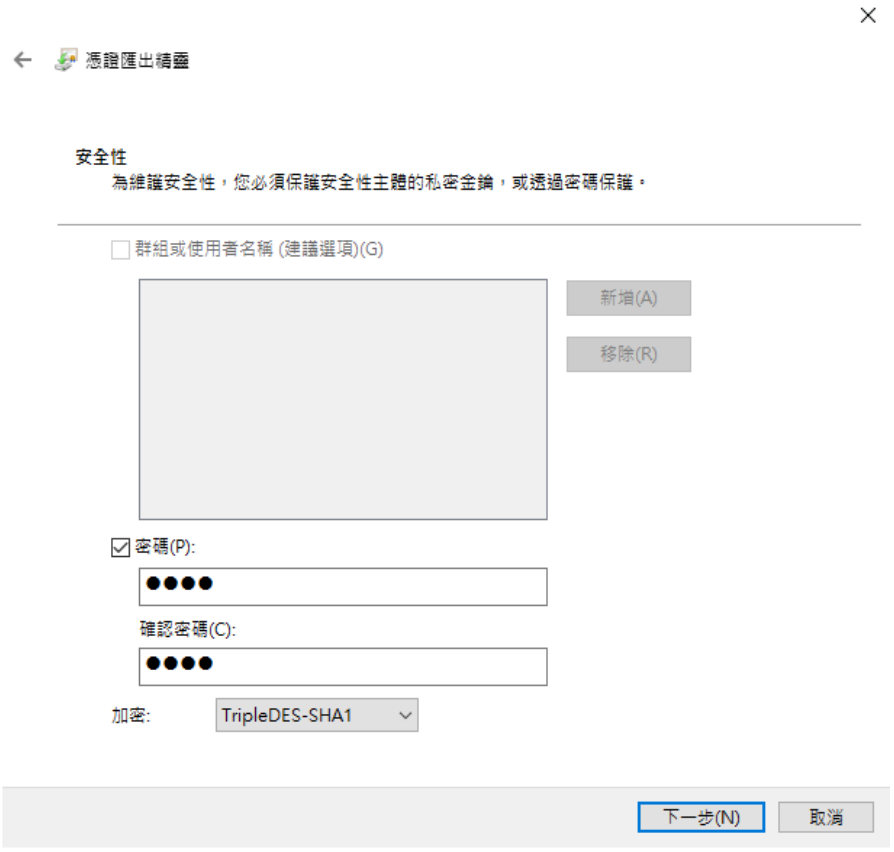
7. 選擇[是，匯出私密金鑰] ，按[下一步]繼續。



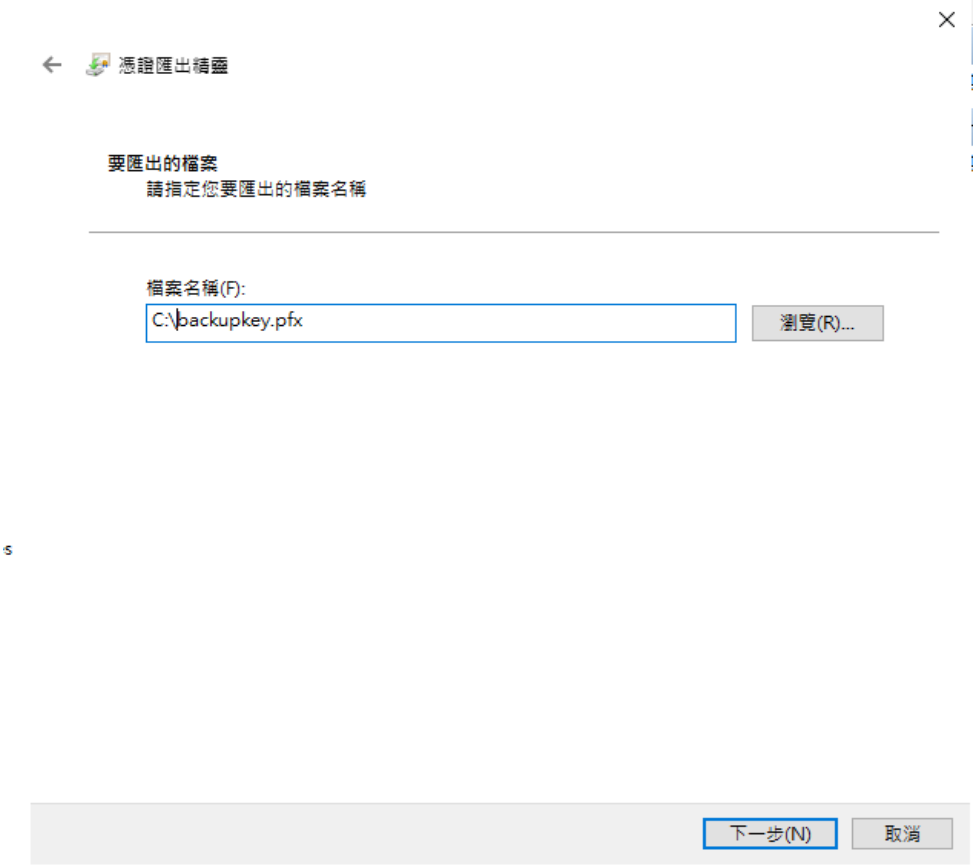
8. 選擇[個人資訊交換 – PKCS #12 (.PFX)(P)] ，只選取[如果可能的話，包含憑證路徑中的所有憑證(U)]及[啟用憑證隱私權(E)]，然後按[下一步]。

9. 輸入密碼匙的密碼，然後按[下一步]。

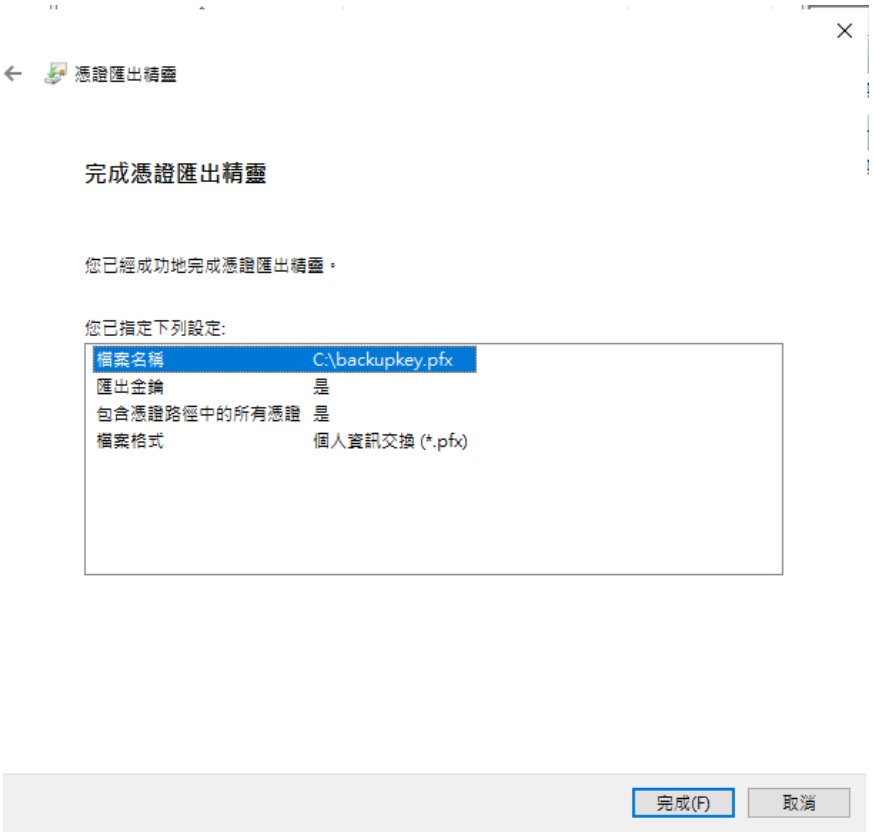
注意：請緊記這個重要的密碼。如果您忘記這密碼，您將不能還原您的密碼匙。



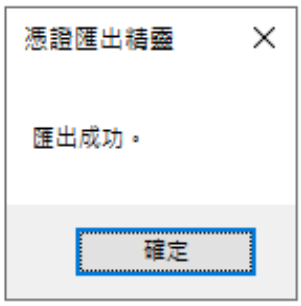
10. 按[瀏覽]指定密碼匙的備份檔案，然後按[下一步]。（此檔案的副檔名預設值為 pfx）。



11. 按[完成]來關閉精靈。

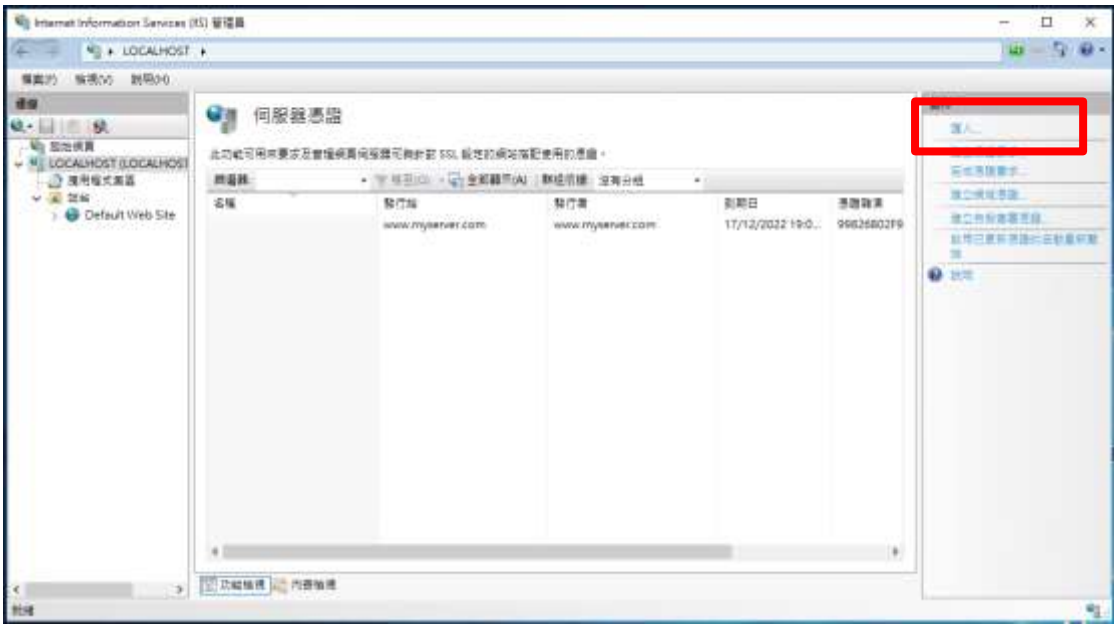


12. 按[確定]來完成。



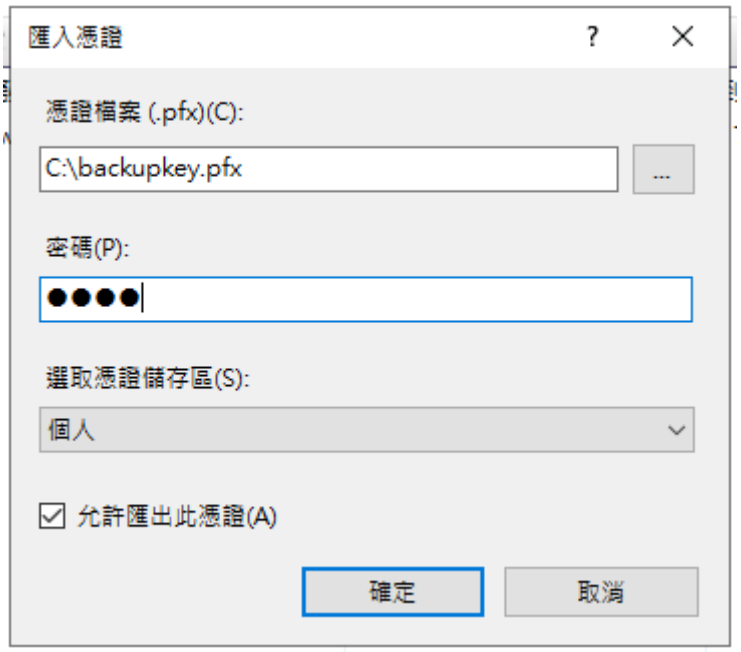
G. 還原密碼匙

1. 按[開始]>[控制台]>[所有控制台項目]>[系統管理工具]>[Internet Information Services (IIS) 管理員]來啟動網際網路資訊服務 (IIS) 管理員。
2. 選擇你的網站，然後按[伺服器憑證]。
3. 在右手邊動作一欄內，按[匯入]。



4. 輸入包含憑證的檔案名稱及路徑及憑證的密碼，然後按[確定]。

> 注意：你可以取消選取[允許匯出此憑證]使不允許匯出憑證。或為使您將來可以進行備份或傳輸您的憑證，可選取[允許匯出此憑證]使憑證可匯出。



5. 電子證書（伺服器）証書已成功匯入。