电子证书（伺服器）用户指南

Microsoft IIS 10.0 适用

修订日期：2025 年 4 月

目录

A. 电子证书（伺服器）申请人指引

香港邮政核证机关在收到及批核电子证书（伺服器）申请后，会向获授权代表发出主旨为 “Submission of Certificate Signing Request (CSR)” 的电邮，要求获授权代表到香港邮政核证机关的网站提交 CSR。

本用户指南旨在提供参考给电子证书（伺服器）申请人如何使用 Microsoft Internet Information Server (IIS) 10.0 产生配对密码匙和证书签署要求(CSR)的详细步骤。包含公匙的 CSR 将会提交到香港邮政核证机关以作证书签署。

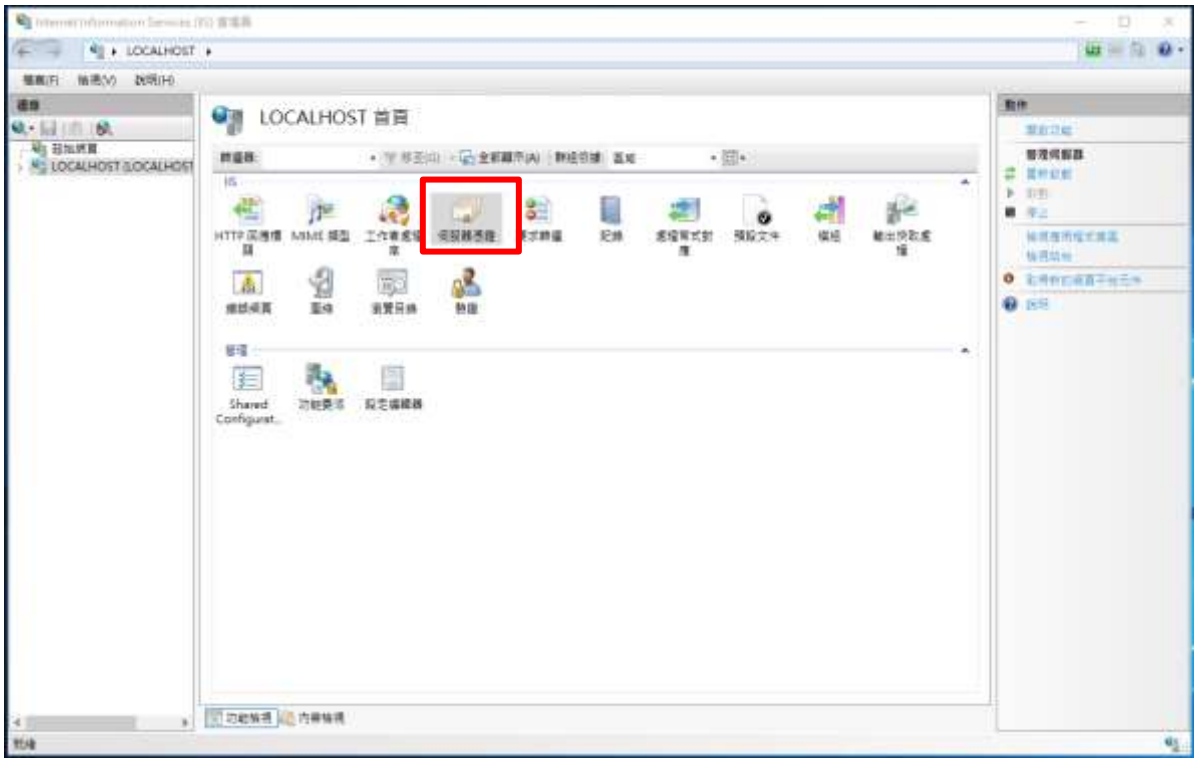
如阁下在证书签发后遗失密码匙，您将不能安装或使用该证书。因此强烈建议阁下于**提交证书签署要求(CSR)前**及**完成安装伺服器证书后**均为密码匙进行备份。有关备份及还原密码匙的方法，请参阅以下部分的详细步骤：

新申请及续期申请

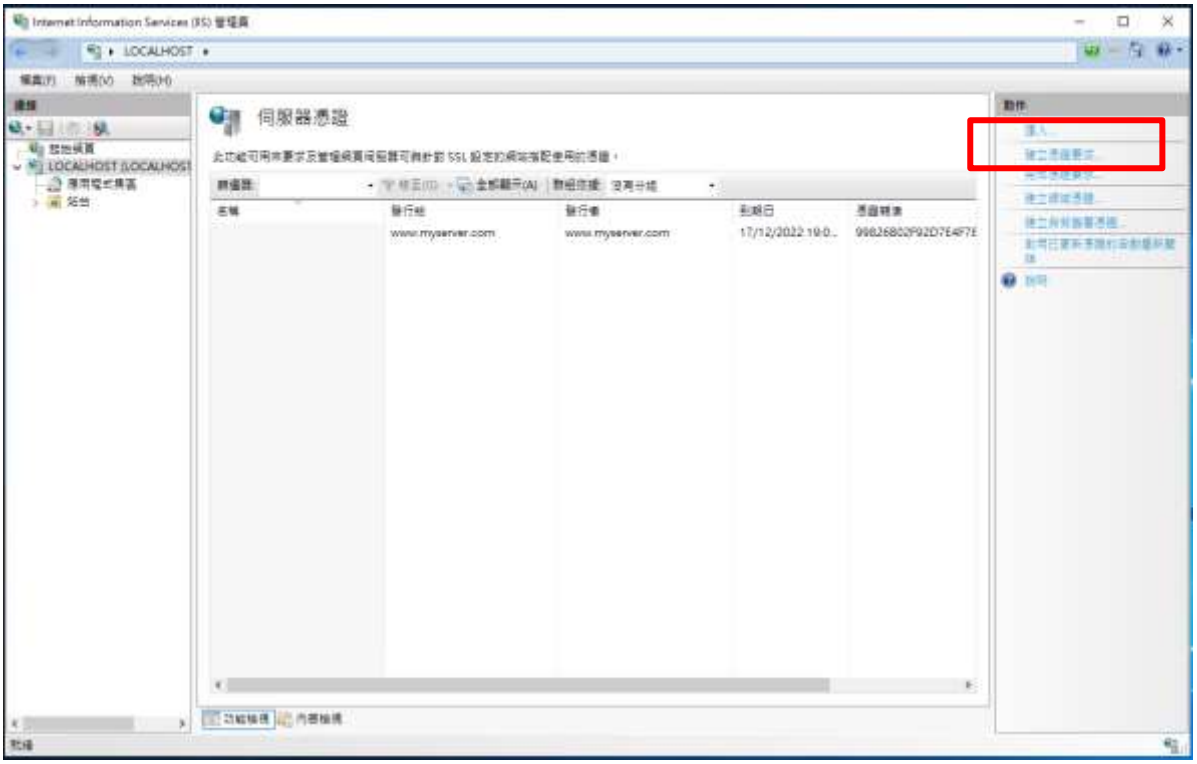
首次及续期申请电子证书（伺服器），请参阅以下部分的详细步骤：

B. 产生证书签署要求(CSR)

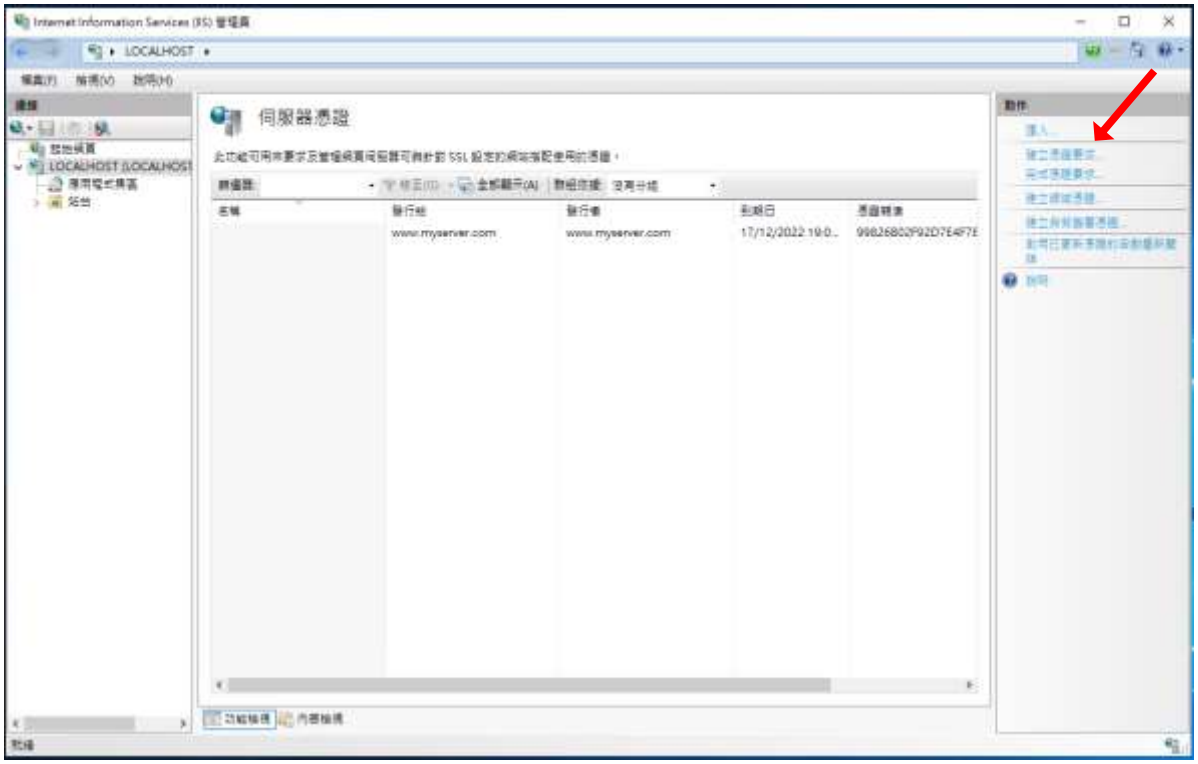
1. 按[开始]>[系统管理工具]>[Internet Information Services (IIS) 管理员]来启动网际网路资讯服务 (IIS) 管理员。
2. 在 [Internet Information Services (IIS) 管理员]视窗内，展开[网站]及选择您的网站，然后按[伺服器凭证]。



3. 在右手边[动作]一栏内，按[建立凭证要求]。



*注意：*新申请及续期申请电子证书（伺服器）的步骤相同，即使是续期电子证书，请不要使用[更新]，要选择[建立凭证要求]。



4. 输入您的一般名称和组织，以及组织单位，並选择 “HK” 作为 [国家 (地区)]， 输入 “Hong Kong” 作为[县市/位置] 及[省份]，然后按[下一步]。

注意：请确定于「发给」一欄显示正确的登记域名(即伺服器名称)及「国家(地区)」一欄显示「HK」。

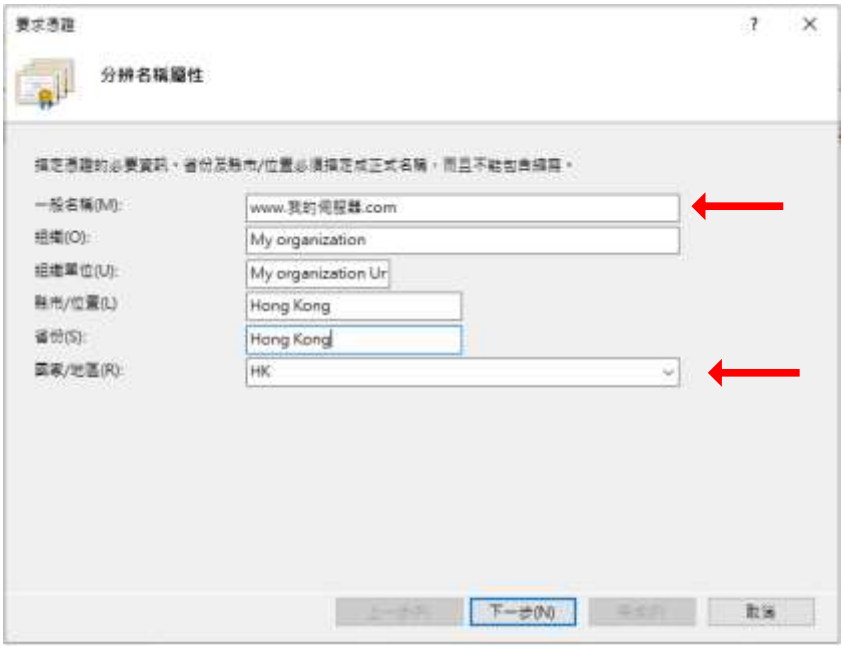
注意：若申请电子证书（伺服器）“多域版”或延伸认证电子证书（伺服器）“多域版”,请在「一般名称」一欄中，输入与申请表格中所填写的「用作电子证书主体名称的伺服器名称」相同的登记伺服器名称。而「电子证书主体别名内的额外伺服器名称」，则无需在产生证书签署要求(CSR)过程中输入，香港邮政核证机关系统在签发证书时，会根据申请表格所申请的资料自动填写。

若申请电子证书（伺服器）“通用版”，请在「通用名称」一欄中，输入与申请表格中所填写的「有通配符的电子证书伺服器名称」相同的登记伺服器名称(伺服器名称的最左部份需包括有通配符「」的部份)。例如 *.myserver.com。*

注意：若申请中文伺服器名称的电子证书（伺服器）

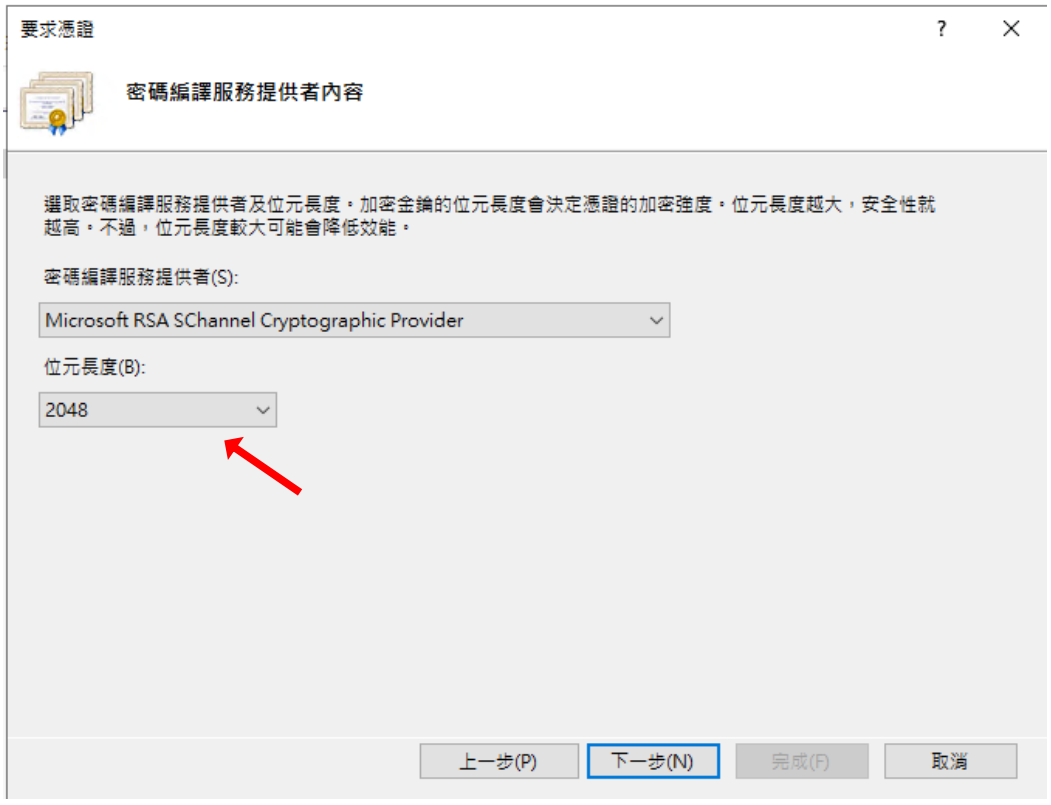
选项 1：请在「通用名称」一欄中，输入与申请表格中所填写的「用作电子证书主体名称的伺服器名称」相同的登记伺服器名称。

选项 2: 请使用国际网域名称转换工具把中文网域名称转换成 ASCII 字元，并可以在"通用名称" 一欄中输入转换后的名称。

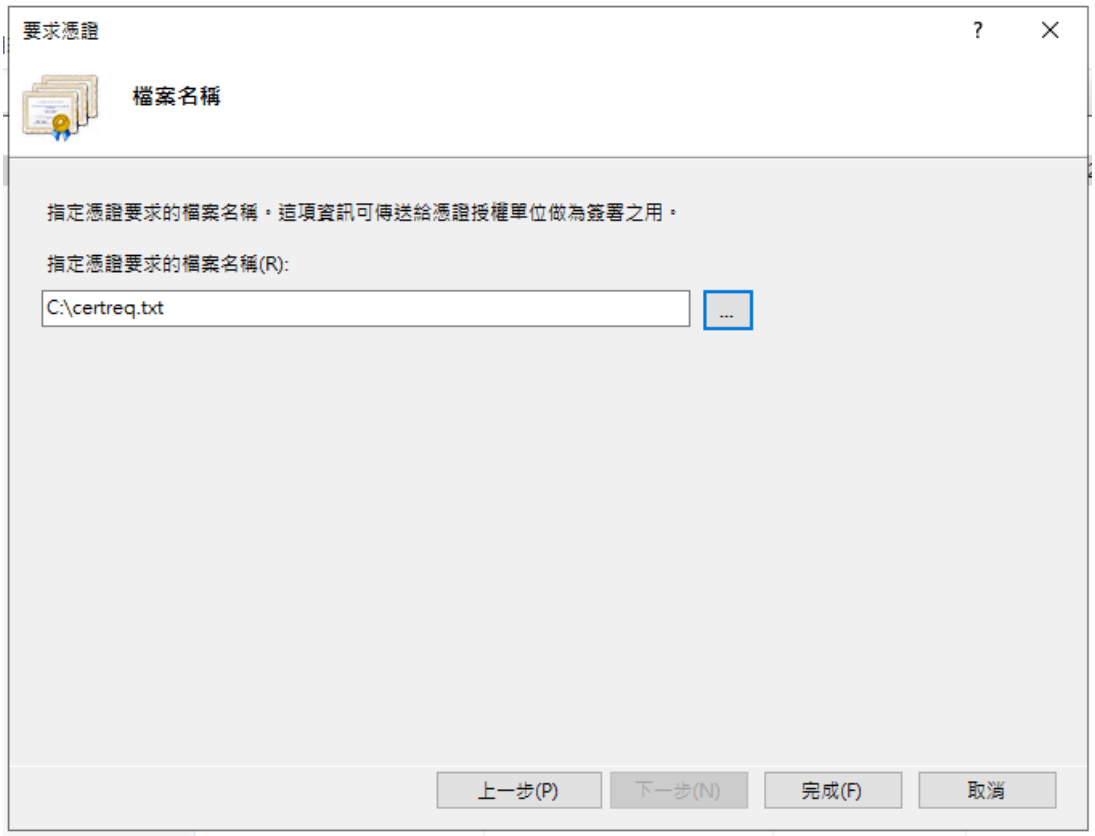


5. 选择“Microsoft RSA SChannel Cryptographic Provider”作为[密码编译服务提供者]及选择“2048”作为密码匙的[位元长度]，然后按[下一步]。

注意: 小于2048 位元的密码匙或未能提供足够保密程度; 相反大于2048 位元有可能与某些浏览器不兼容。建议选择长度为 2048 位元的密码匙，从而提供较佳的保密程度。

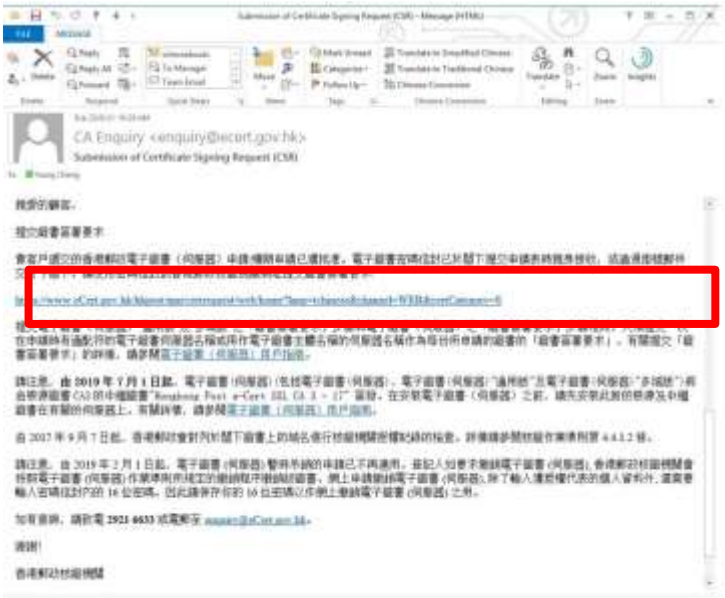


6. 输入新凭证名称 (或接受预设) 及按[完成]来关闭精灵。



C. 提交证书签署要求(CSR)

1. 在香港邮政核证机关发出主旨为 “Submission of Certificate Signing Request (CSR)” 的电邮内按一下超连结以连线至香港邮政核证机关的网站。



2. 输入[伺服器名称]、印于密码信封面的[参考编号](九位数字)及印于密码信封内的[电子证书密码](十六位数字)，然后按[提交]。

3. 按[提交]确认申请资料。(如发现资料不正确，请电邮至 enquiry@eCert.gov.hk 联络香港邮政核证机关。)

注意：若电子证书申请表格上提供了机构中文名称和/或分部中文名称，如要发出一张主体名称为机构中文名称的电子证书(伺服器)，请按[确认使用中文]键繼續。

4. 用文字编辑器(例如：记事本)开启早前产生的证书签署要求(CSR)及复 制全部内容包括 “-----BEGIN NEW CERTIFICATE REQUEST-----” 及 “-----END NEW CERTIFICATE REQUEST-----”。(您可参考 B 部的步骤 6 的凭证要求档案的位置。)

5. 在方格内贴上内容，然后按[提交]。

6. 按 [**接受**] 确认接受此证书。

7. 下载 Hongkong Post e-Cert (Server)证书。

注意：

1. *您也可以从搜寻及下载证书网页下载您的电子证书（伺服器）。*
   https://www.ecert.gov.hk/tc/sc/index_sc.html
2. *由 2019 年 7 月 1 日起，电子证书（伺服器）将由根源证书Root CA3 的中继证书"Hongkong Post e-Cert SSL CA 3 - 17" 签发。*

   持有 2019 年 7 月 1 日或以后签发的电子证书（伺服器）的登记人，须进行以下改动，以便安装了由根源证书Root CA3 签发的电子证书（伺服器）的网站继续受到一般网页浏览器的信任：

   安装由根源证书Root CA3 签发的中继证书"Hongkong Post e-Cert SSL CA 3 - 17"。下载地址如下：

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

   安装由根源证书 GlobalSign Root CA - R3 签发的交叉证书"Hongkong Post Root CA 3"。

   下载地址如下：

   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt
3. *由2022年1月21日起，延伸认证电子证书（伺服器）将由根源证书Root CA3的中继证书"Hongkong Post e-Cert EV SSL CA 3 - 17" 签发。*

   持有2022年1月21日或以后签发的延伸认证电子证书（伺服器）的登记人，须进行以下改动，以便安装了由根源证书Root CA3签发的延伸认证电子证书（伺服器）的网站继续受到一般网页浏览器的信任：

   安装由根源证书Root CA3签发的中继证书"Hongkong Post e-Cert EV SSL CA 3 - 17"。下载地址如下：

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

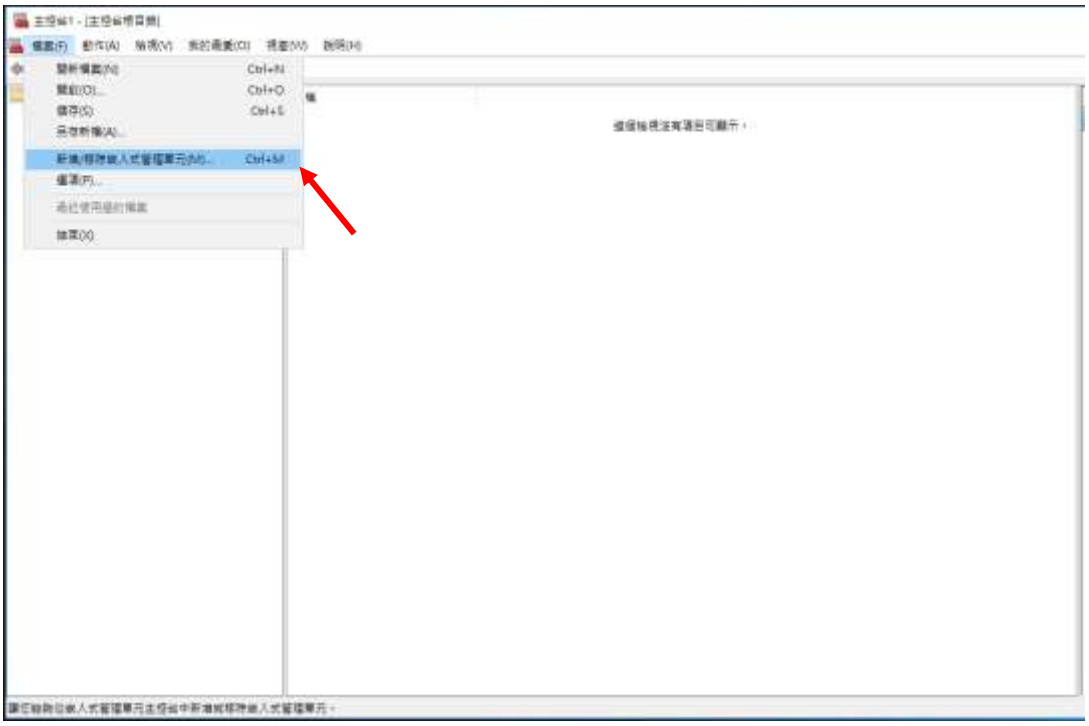
   安装由根源证书 GlobalSign Root CA - R3 签发的交叉证书"Hongkong Post Root CA 3"。

   下载地址如下：

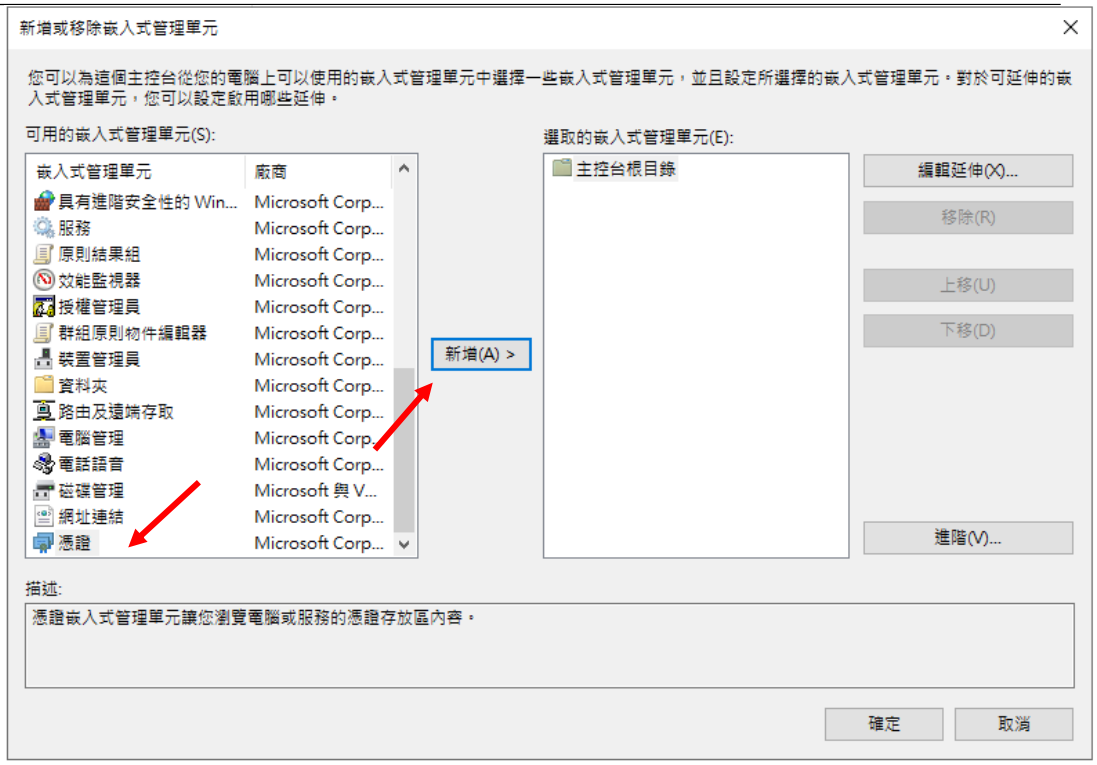
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. 安装中继 / 交叉证书

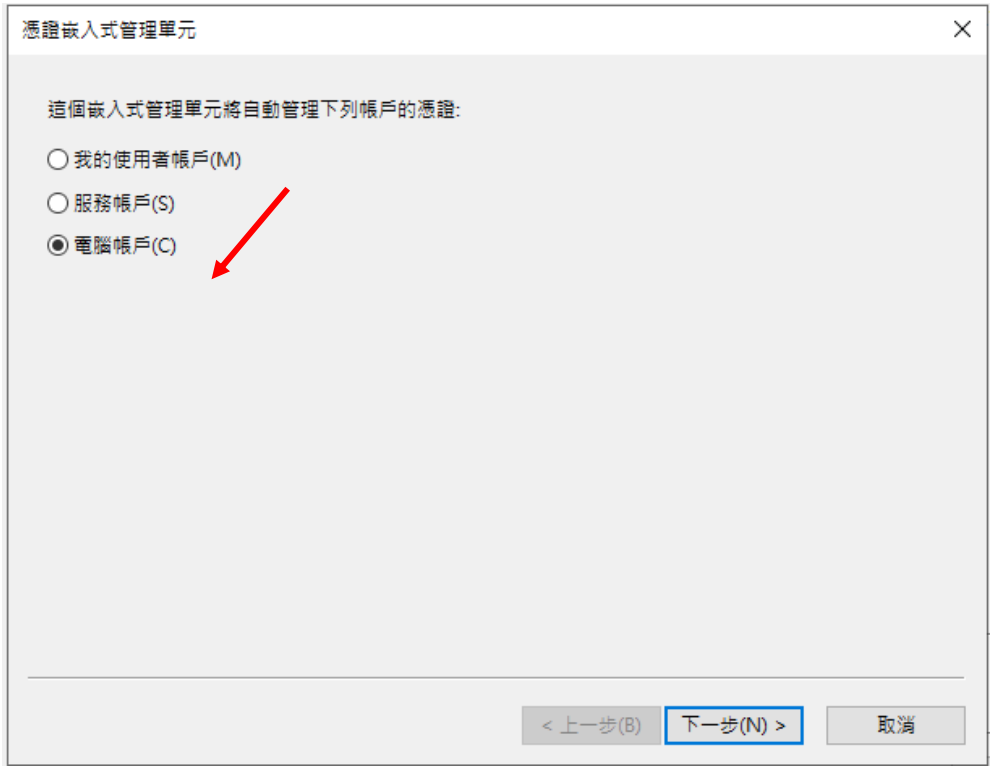
1. 按[开始]>[执行]，然后输入 “mmc” 及按[确定] 来启动 Microsoft Management Console (MMC)，然后从[档案]选单中选取[新增/移除嵌入式管理单元]。



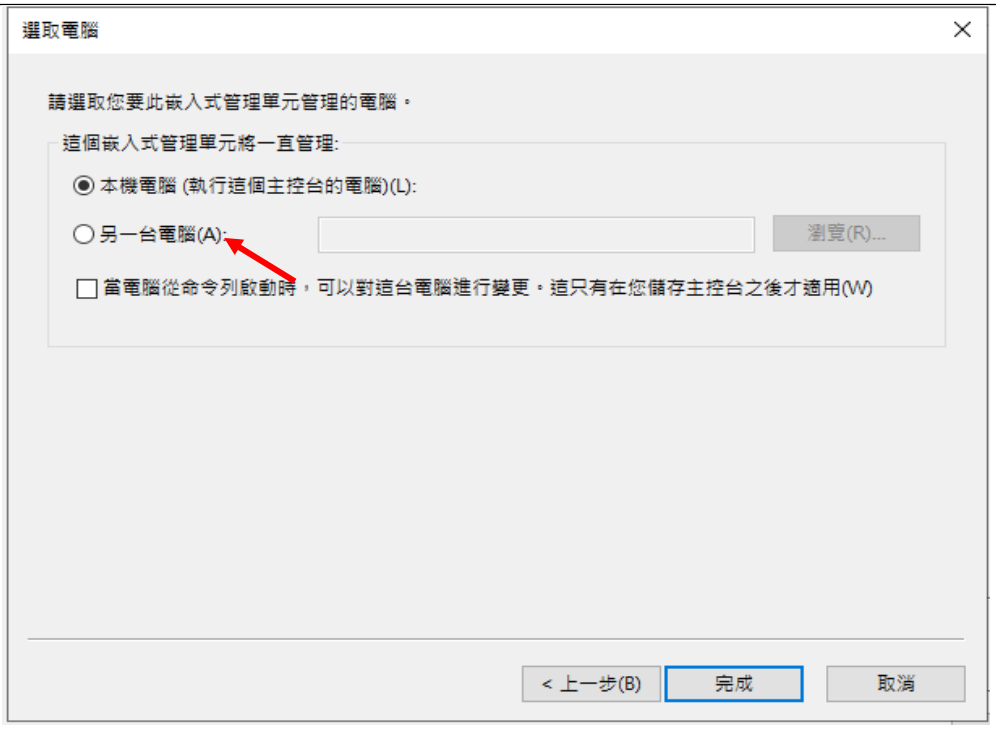
2. 选择[凭证]，然后按[新增]。



3. 选择[电脑帐户]，然后按[下一步]。



4. 选择[本机电脑]，然后按[完成]。

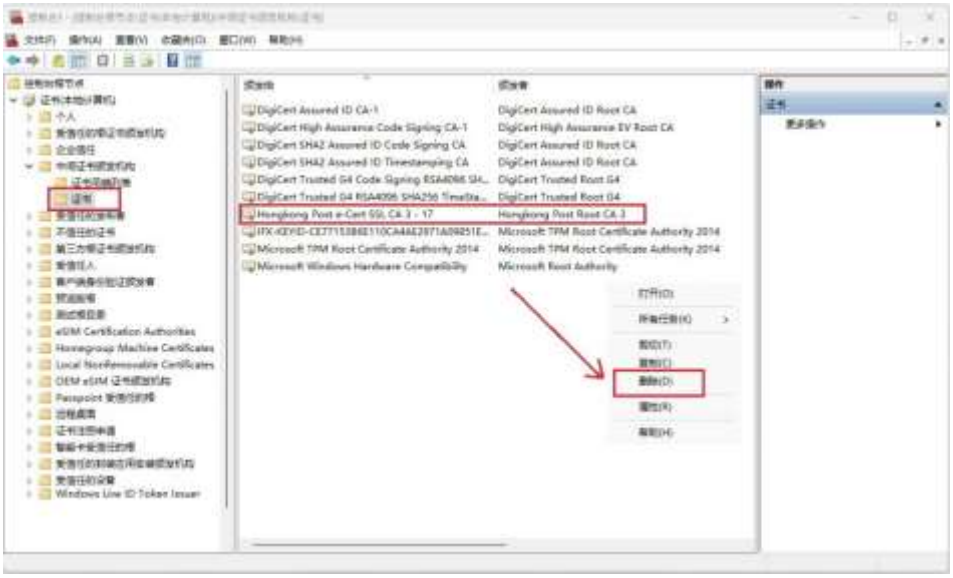

選取電腦
請選取您要此嵌入式管理單元管理的電腦。
這個嵌入式管理單元將一直管理:
本機電腦 (執行這個主控台的電腦)(L):
另一台電腦(A):
瀏覽(R)...
當電腦從命令列啟動時，可以對這台電腦進行變更。這只有在您儲存主控台之後才適用(W)
< 上一步(B)
完成
取消

以下内容以 “**Hongkong Post e-Cert SSL CA 3 - 17**” 中继证书为例子。

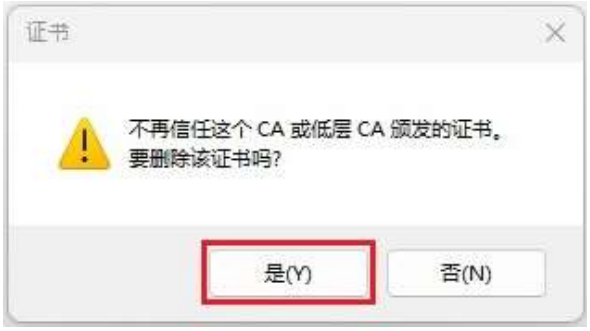
*注意：由 2025 年 5 月 1 日起，电子证书（服务器）会以新中继证书签发。在安装 2025 年 5 月 1 日或之后发出的电子证书（伺服器）时，**请先移除旧有中继证书（如适用）**，**然后在相关伺服器上安装新的中继证书**。*

移除旧有中继证书（如适用）

展开[中继证书颁发机构]，选择[证书]，及以滑鼠右键按一下旧有中继证书[Hongkong Post e-Cert SSL CA 3 - 17]，然后选择[删除]。



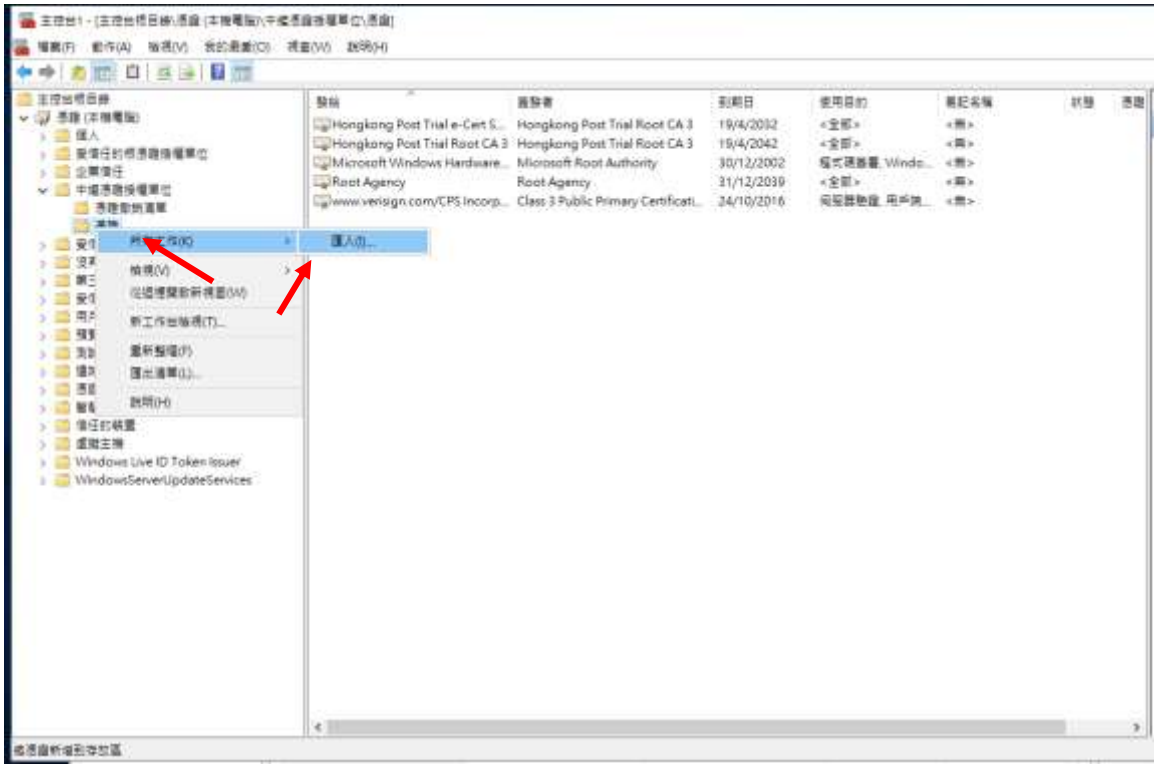
选择［是］确定删除。



以下内容以 “Hongkong Post e-Cert SSL CA 3 - 17” 中继证书为例子。

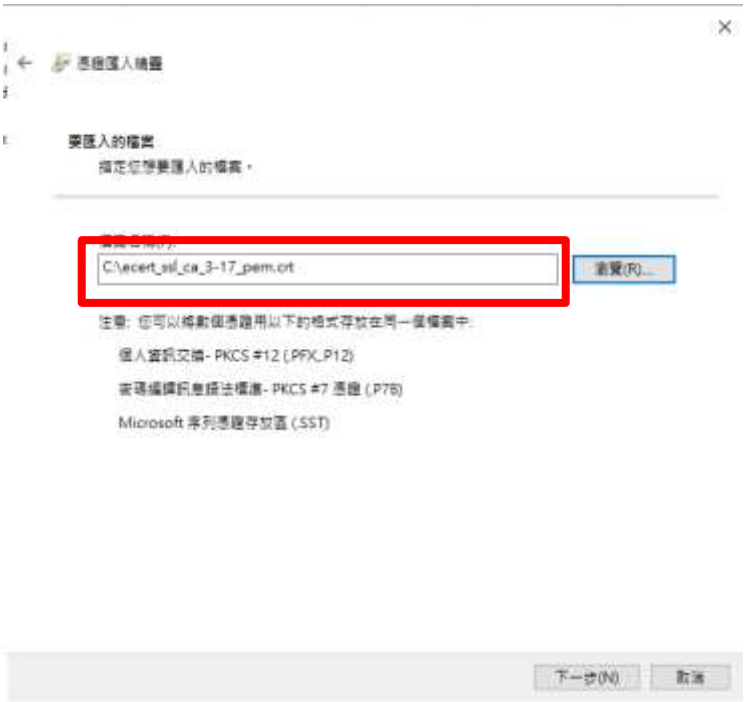
安装中继 / 交叉证书

5. 展开[中继凭证授权]及以滑鼠右键按一下[凭证]，然后选择[所有工作]>[汇入]。

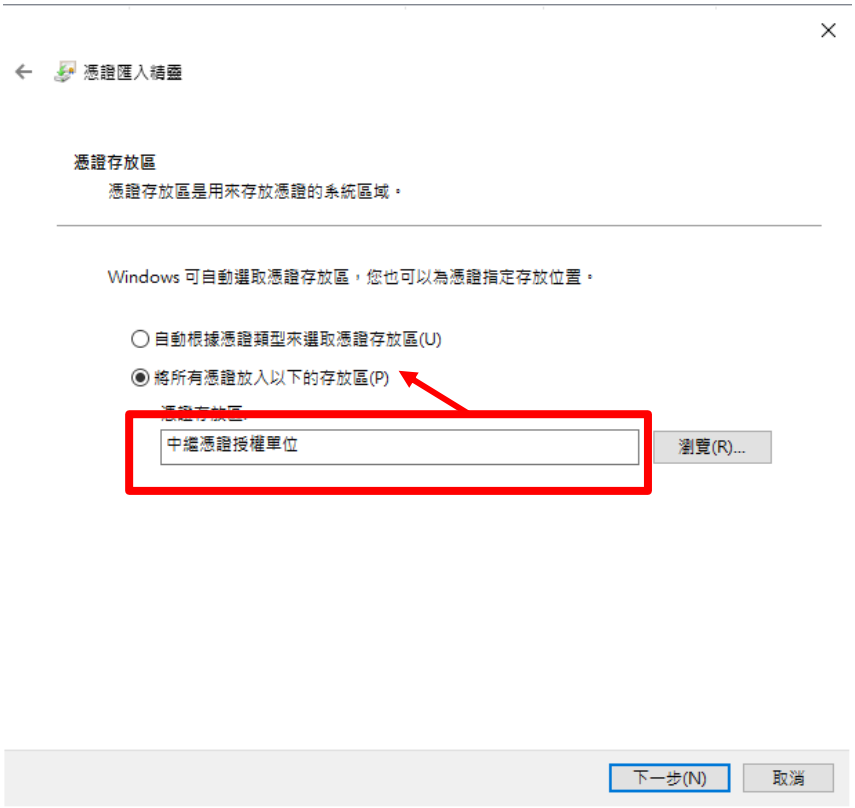


6. 在[凭证汇入精灵]内，按[下一步]继续。

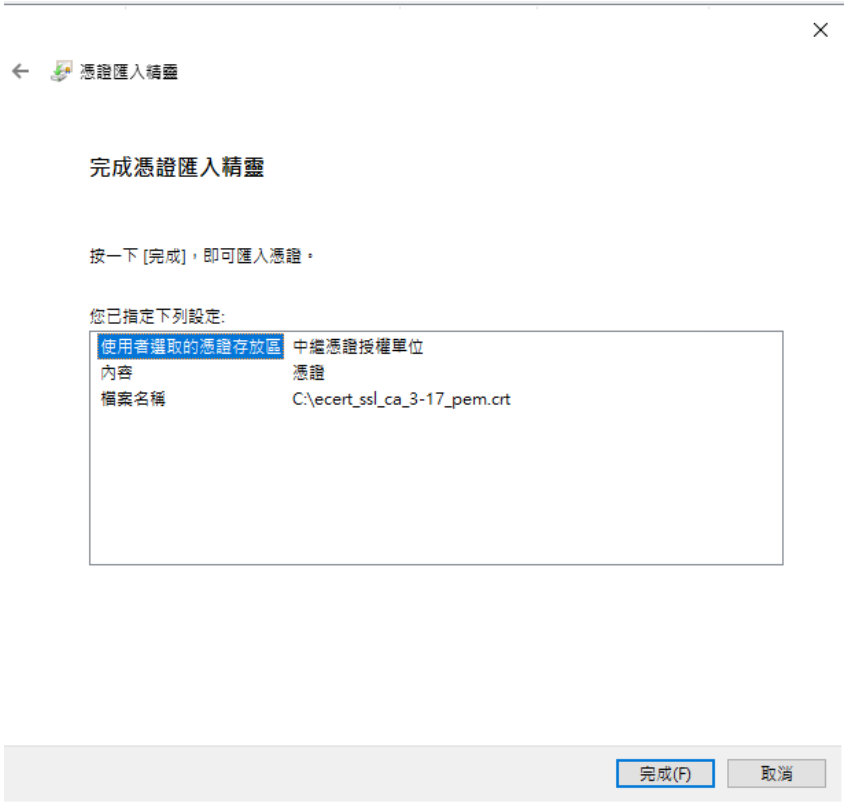
7. 按[浏览]指定早前于 C 部的步骤 7 下载的 “**Hongkong Post e-Cert SSL CA 3 – 17** ” 中继证书 (ecert_ssl_ca_3-17_pem.crt)，然后按[下一步]。



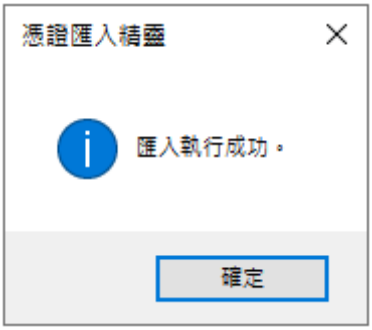
8. 选择[将所有凭证放入以下的存放区]，并选择中继证书颁发机构单位为证书存储，然后按[下一步]。

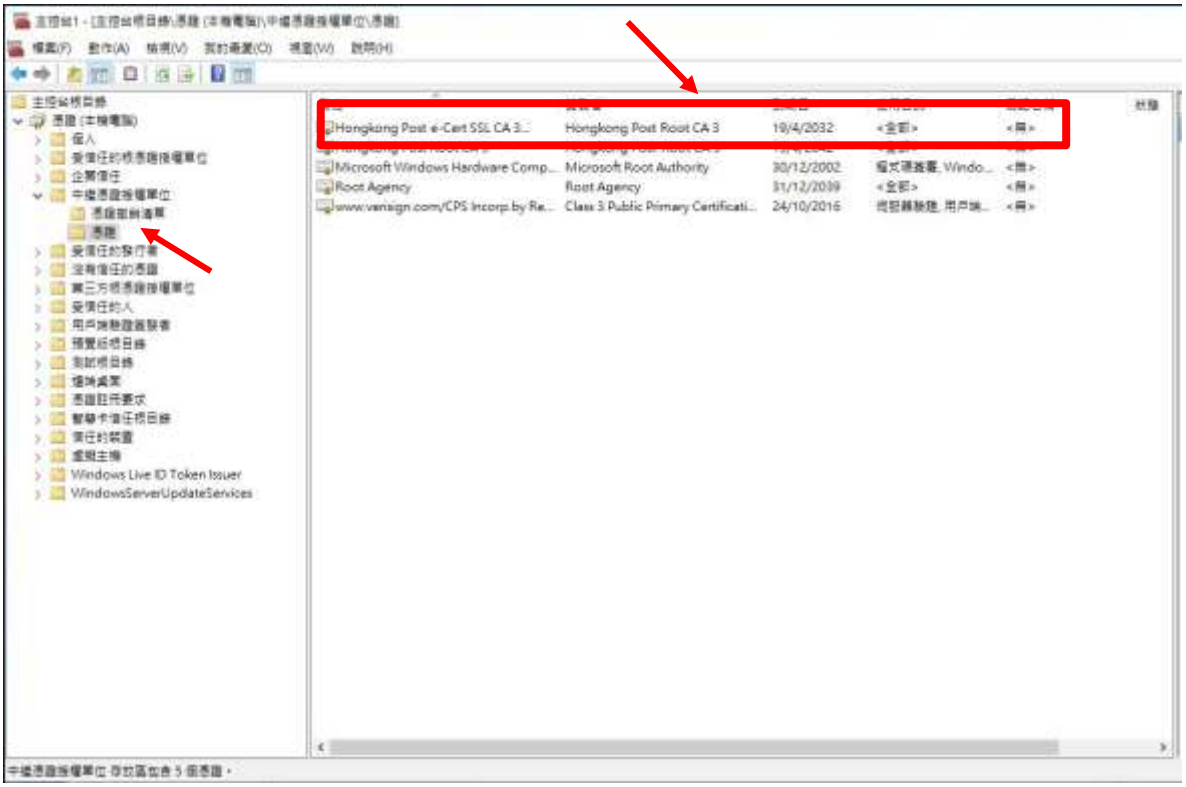


9. 按[完成]来关闭精灵。



10. 按[确定]来完成。



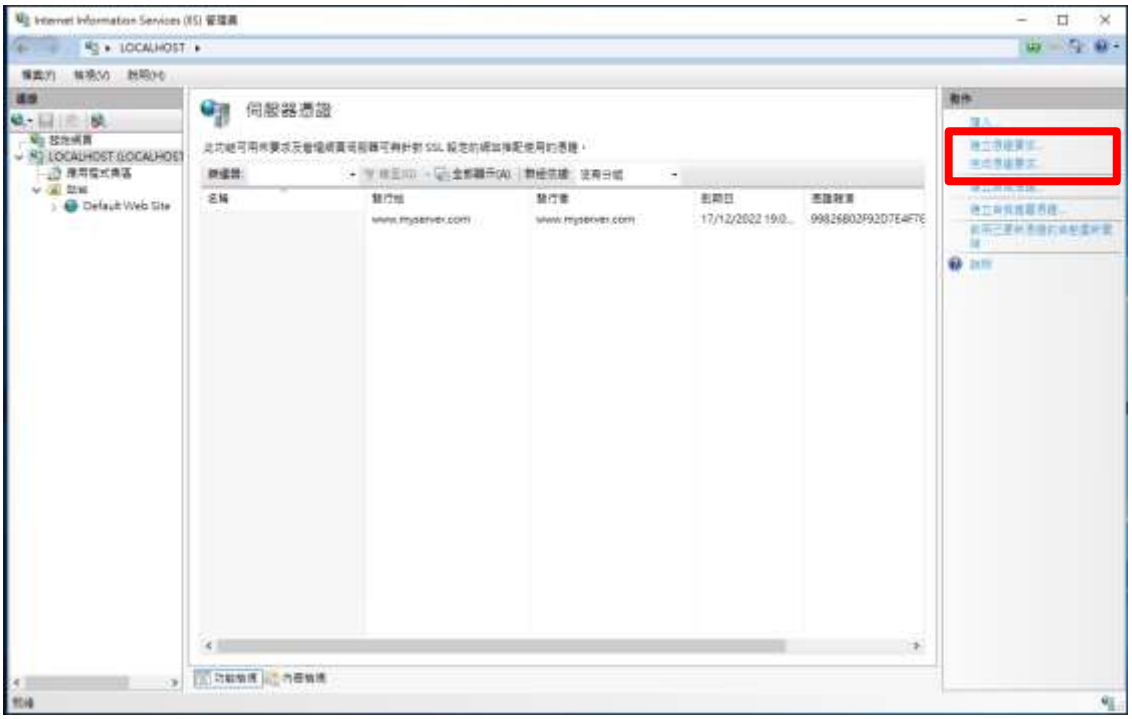


图表 1: “Hongkong Post e-Cert SSL CA 3 – 17”已成功安装

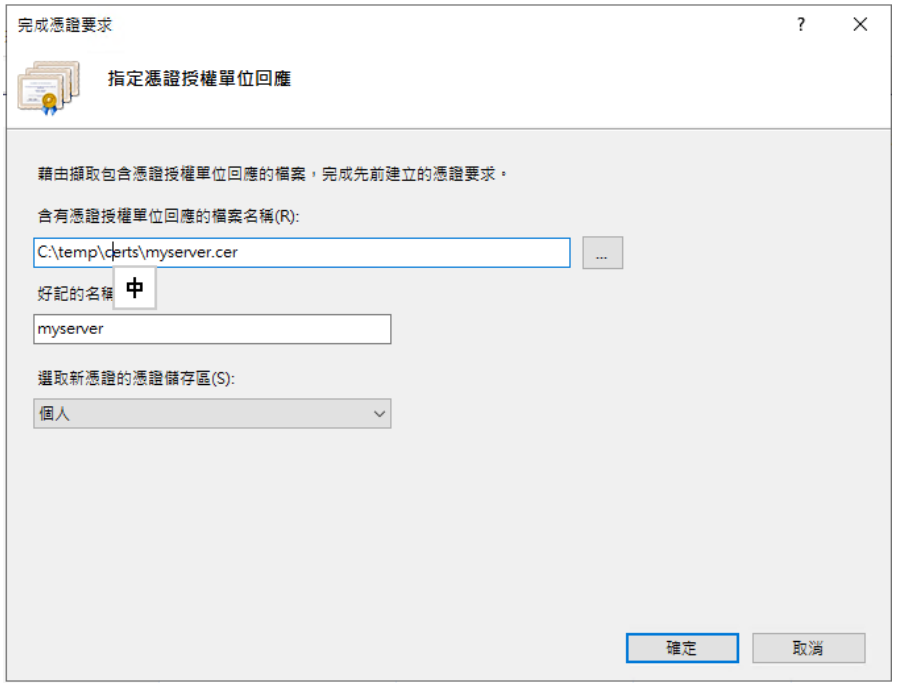
重复步骤 5 到步骤 10 以安装通过 C 部分步骤 7 下载的交叉证书 (root_ca_3_x_gsca_r3_pem.crt)。

E. 安装伺服器证书

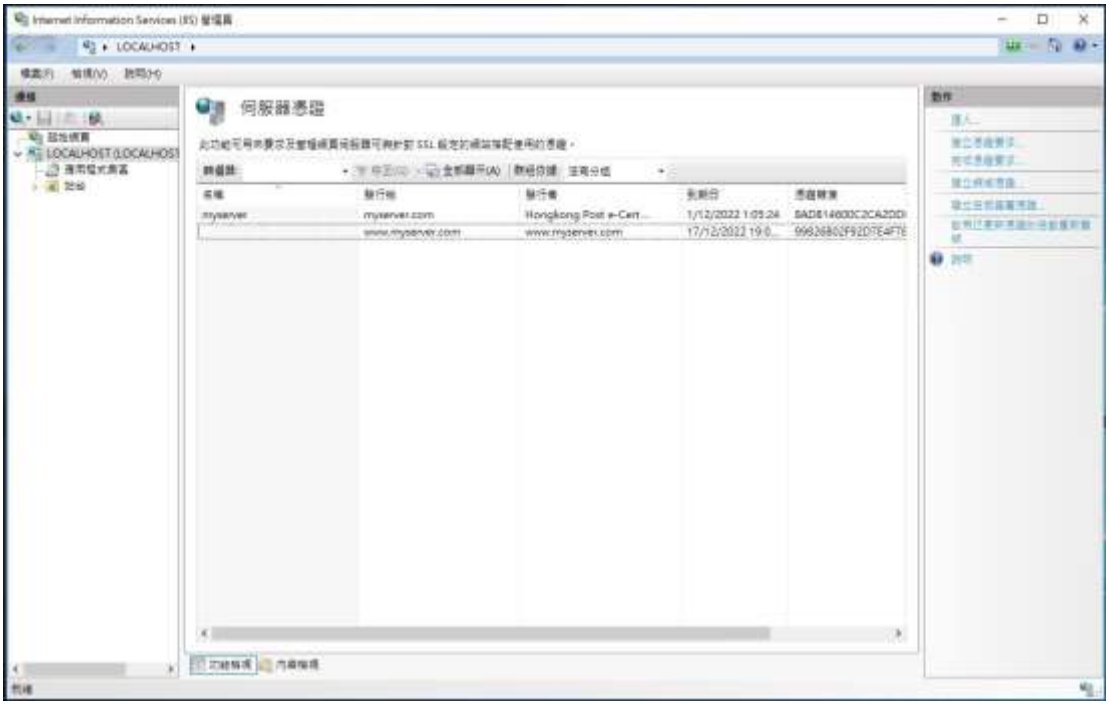
1. 在 [Internet Information Services 管理员]视窗内，选择您的网站，然后按[伺服器凭证]。在右手边动作一栏内，按[完成凭证要求]。



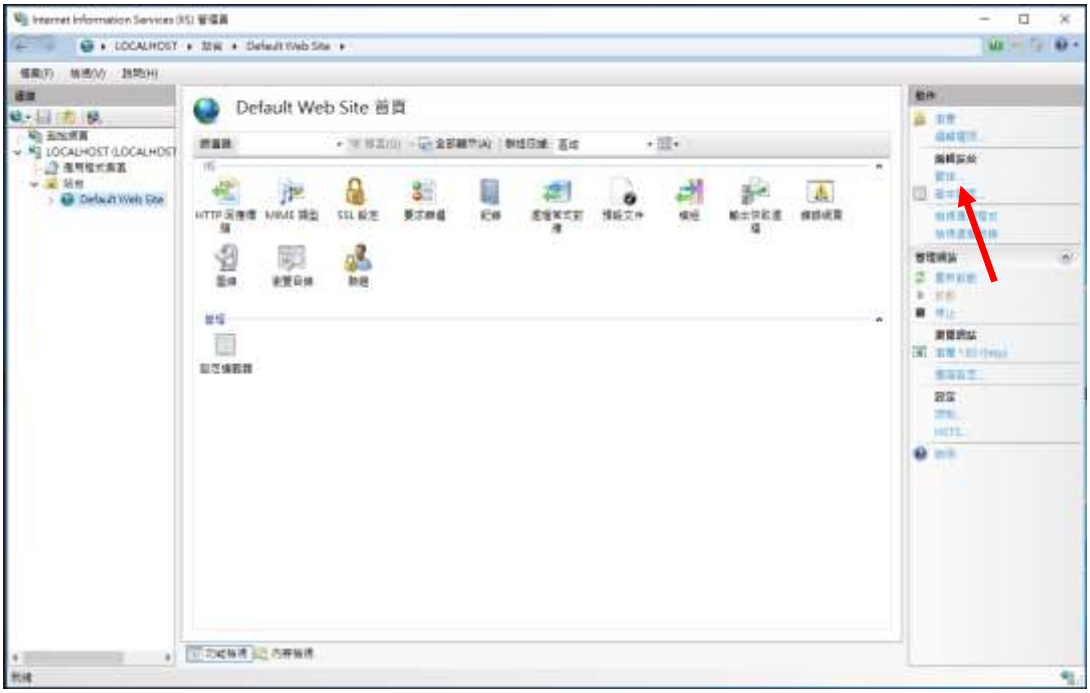
2. 按[浏览]指定早前于 C 部的步骤 7 下载的 “Hongkong Post e-Cert (Server)” 证书及输入[好记的名称]，然后按[确定]。



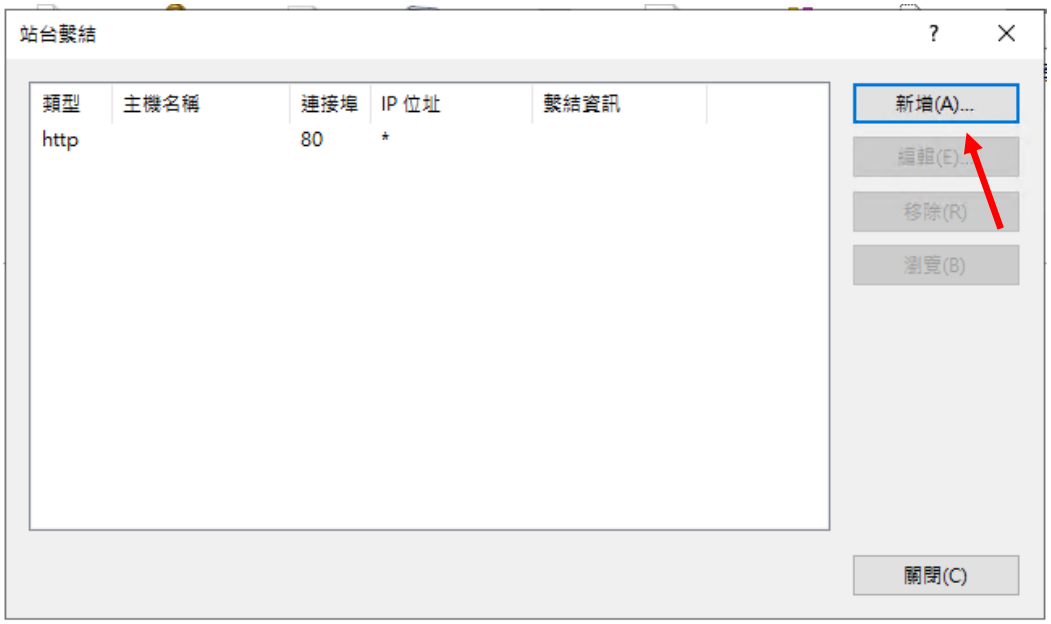
3. “Hongkong Post e-Cert (Server)” 证书已成功安装。



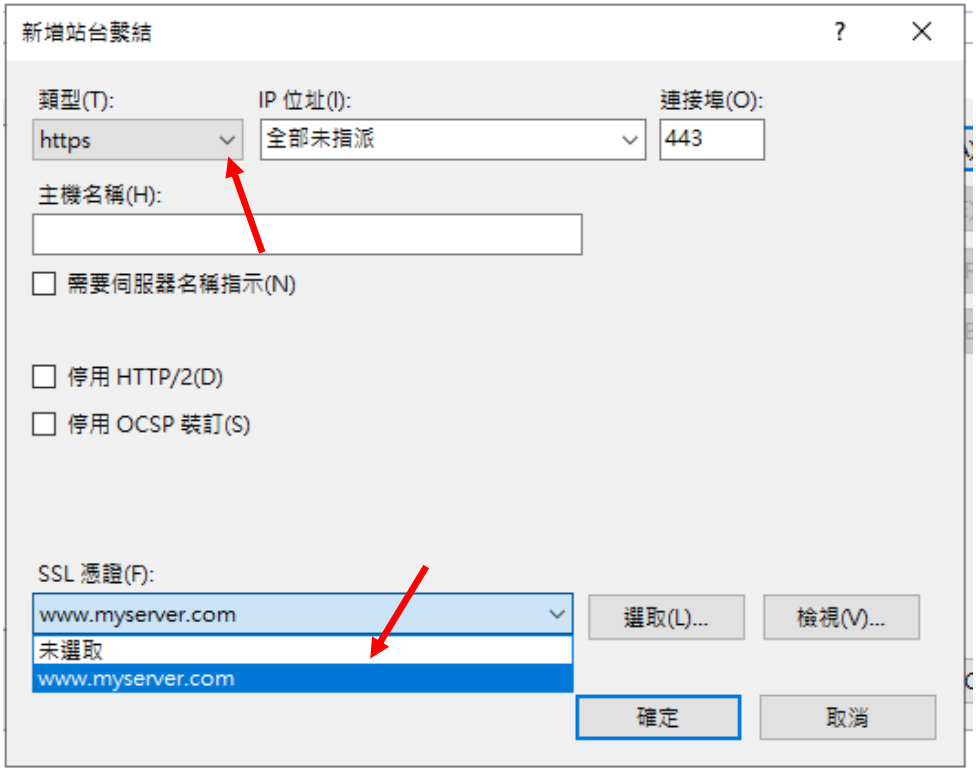
4. 选择你需要系结的网站 ，然后按[系结]。



5. 按[新增]。

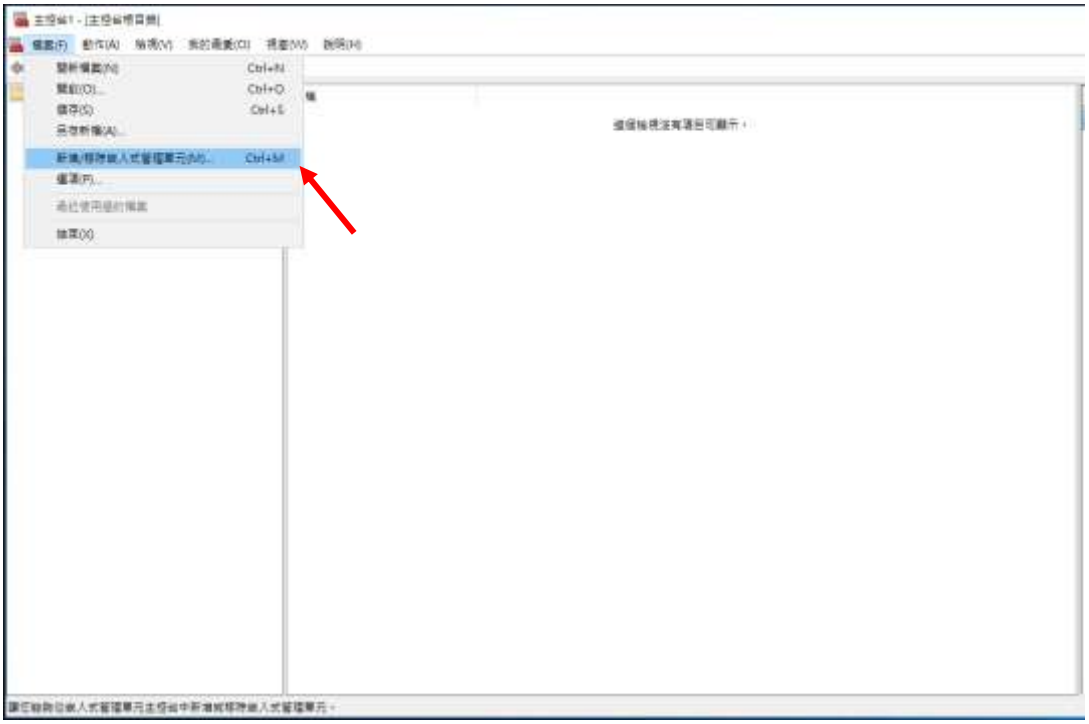


6. 选取[https]及相对应的 SSL 凭证及确定。

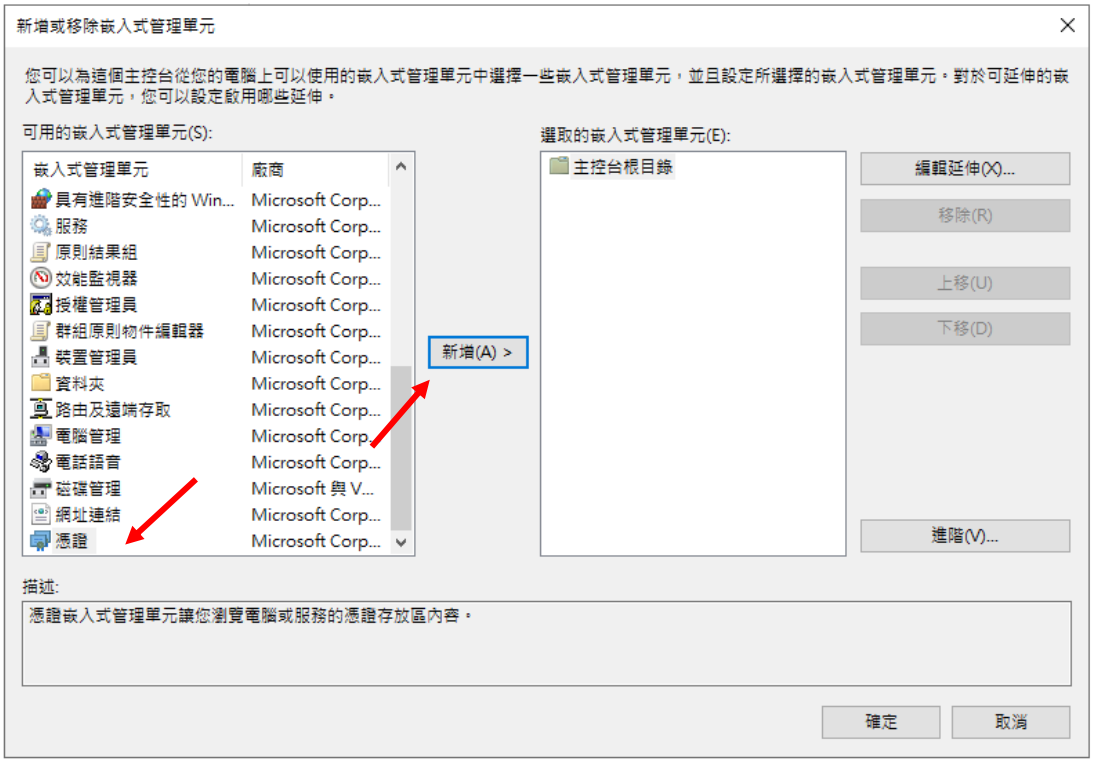


F. 备份密码匙

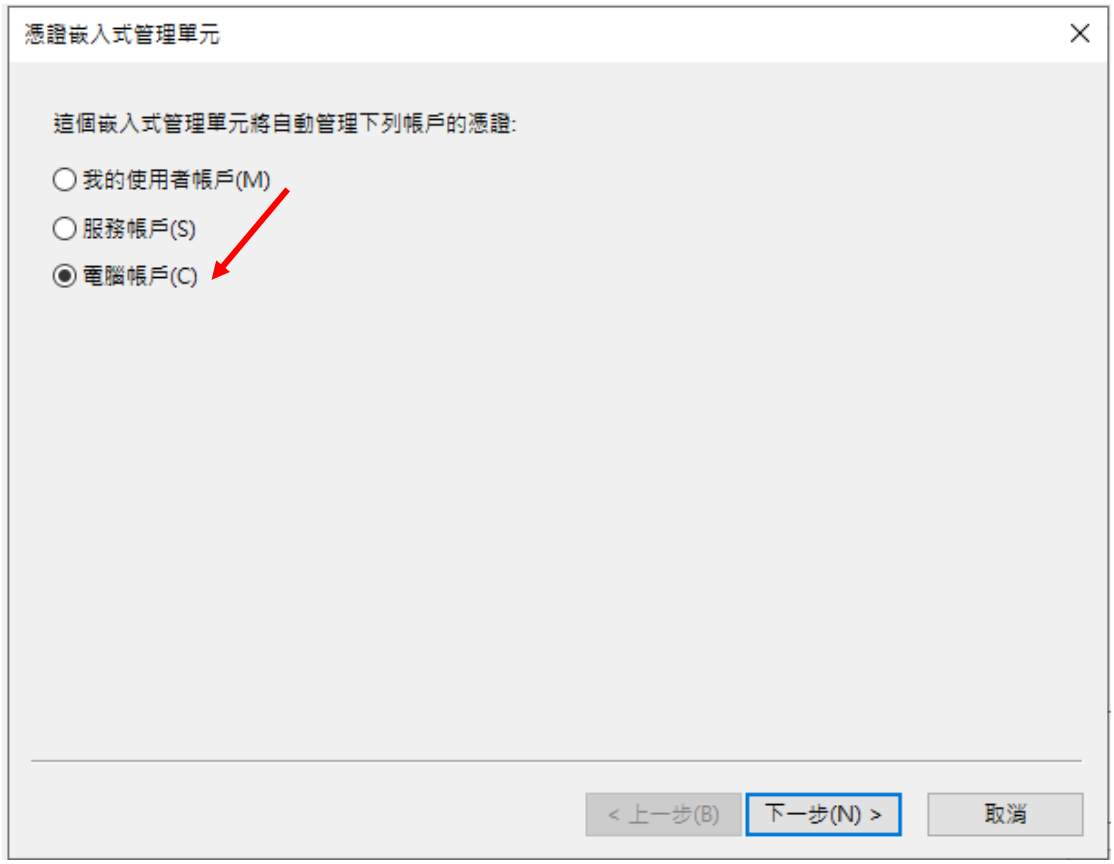
1. 按[开始]>[执行]，然后输入 “mmc” 及按[确定]来启动 Microsoft Management Console (MMC)，然后从[档案]选单中选取[新增/移除嵌入式管理单元]。



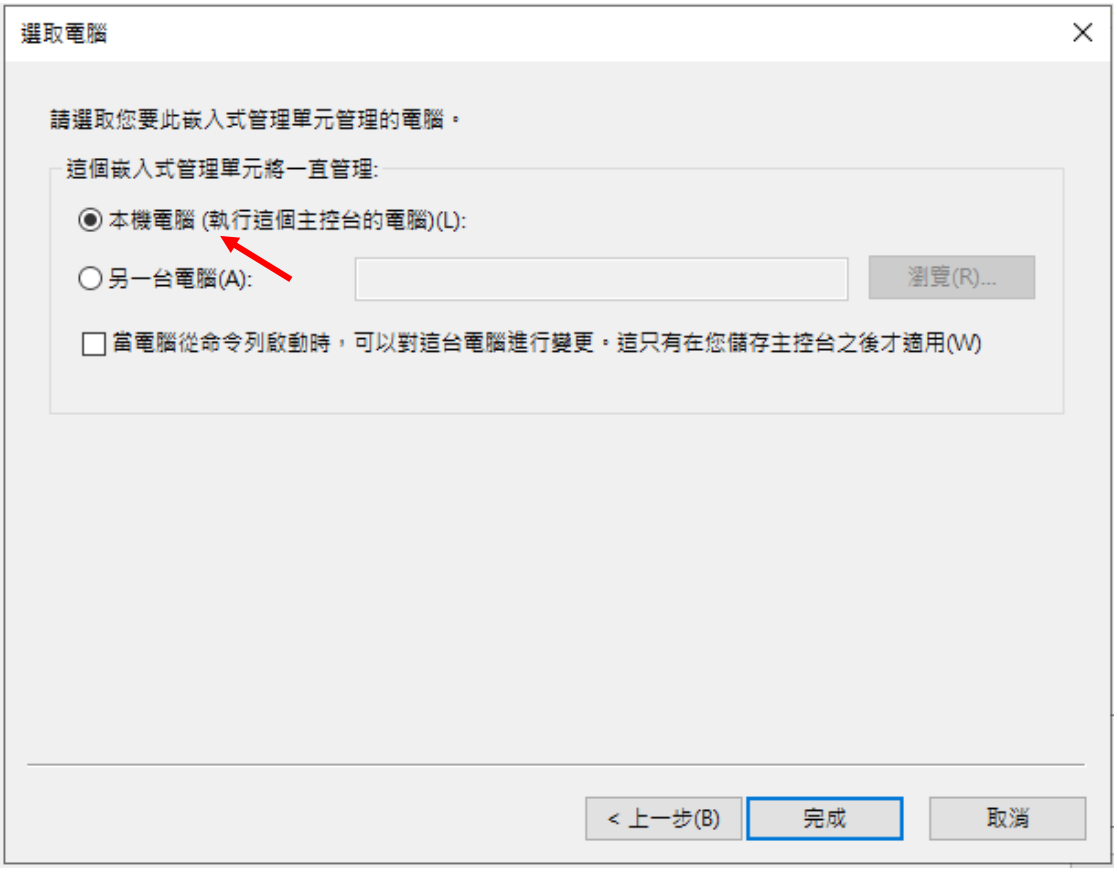
2. 选择[凭证]，然后按[新增]。



3. 选择[电脑帐户]，然后按[下一步]。

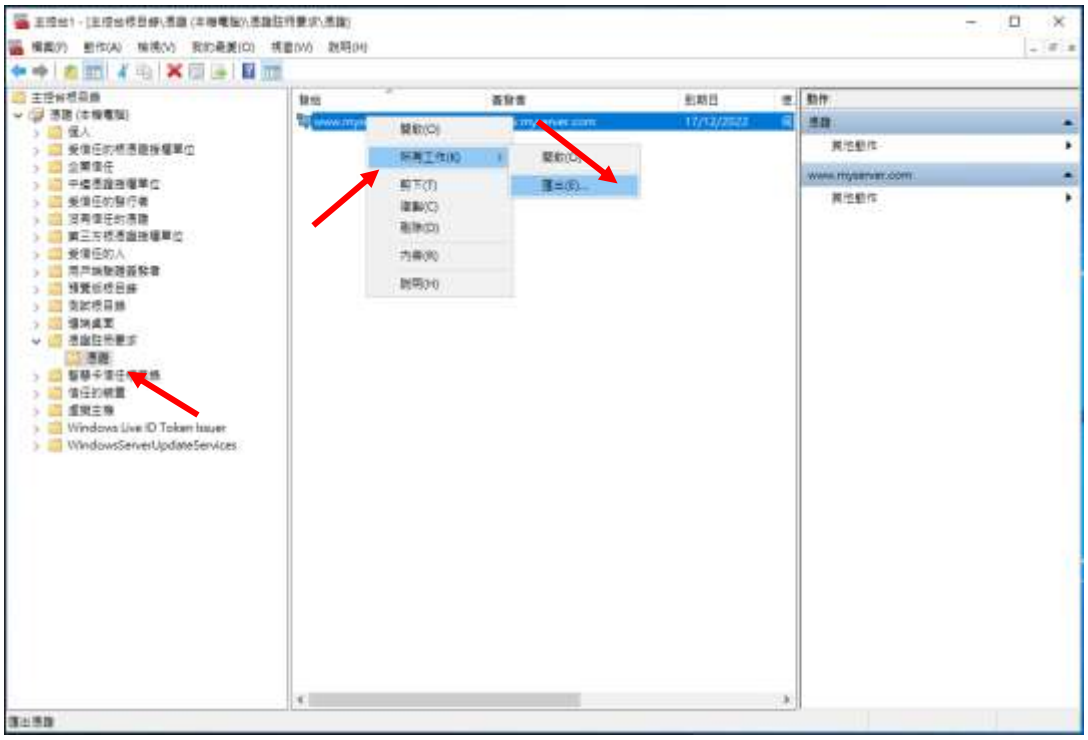


4. 选择[本机电脑]，然后按[完成]。

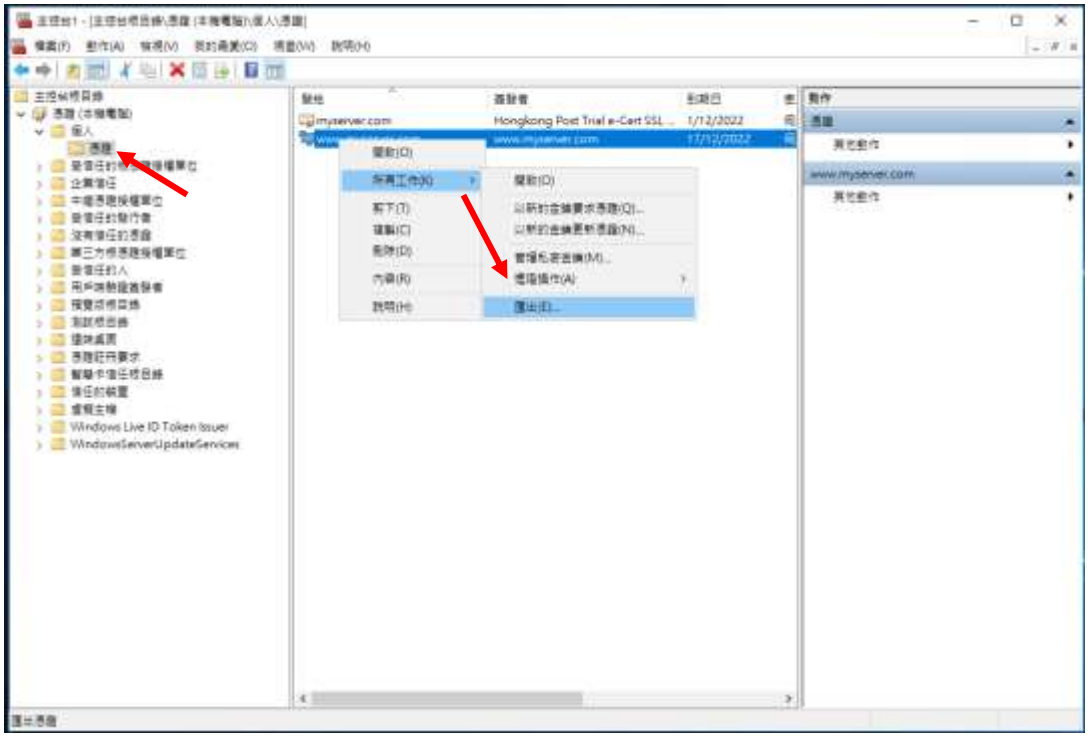


5. 备份密码匙

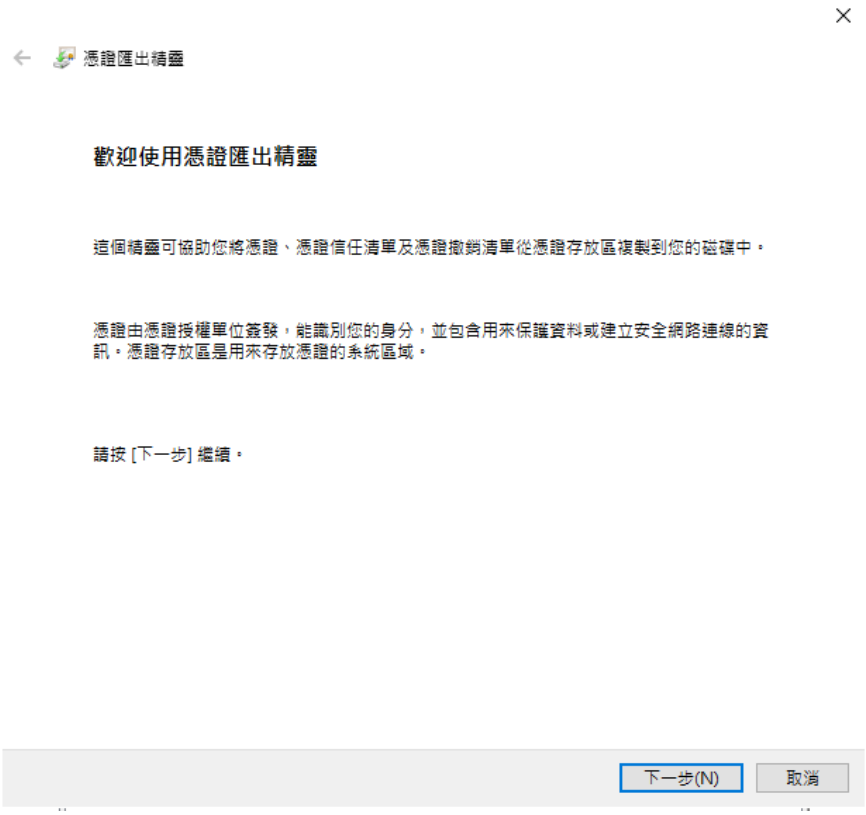
- 备份凭证注册要求的密码匙，请展开[凭证注册要求](或于某些系统称为[REQUESTS])。）。按一下[凭证]，选择你刚建立的凭证注册要求，然后以滑鼠右键选择[所有工作]>[汇出]。



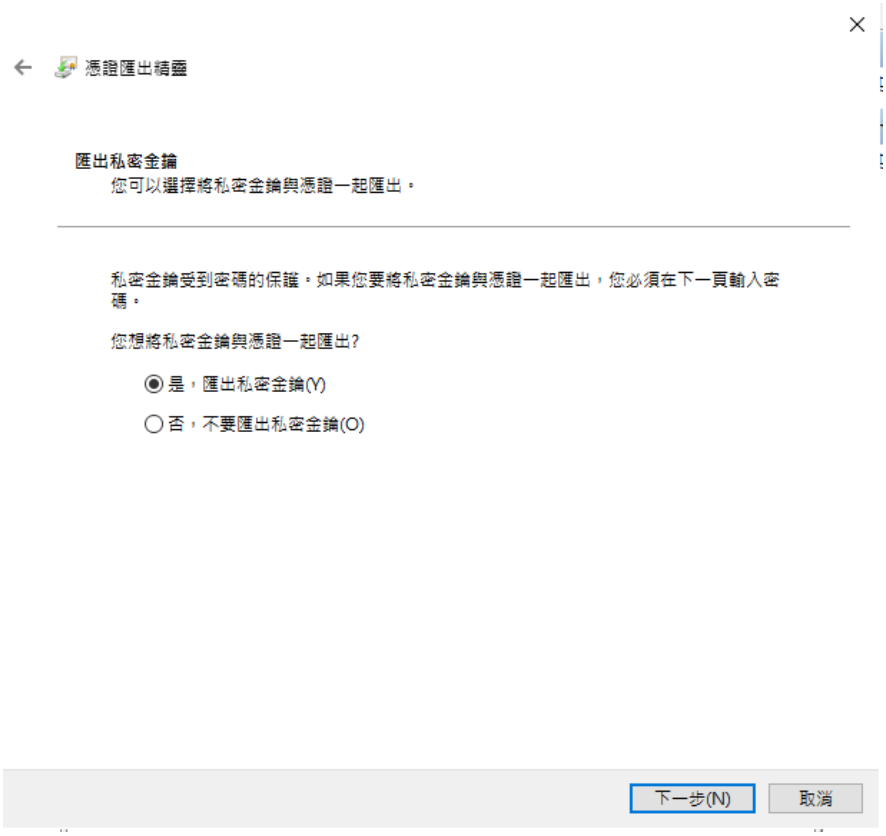
- 备份现有证书的密码匙，展开[个人]及以滑鼠右键按一下[凭证]，选择你需要备份的证书，然后以滑鼠右键按一下[所有工作]>[汇出]。



6. 在[凭证汇出精灵]内，按[下一步]继续。



7. 选择[是，汇出私密金钥] ，按[下一步]继续。

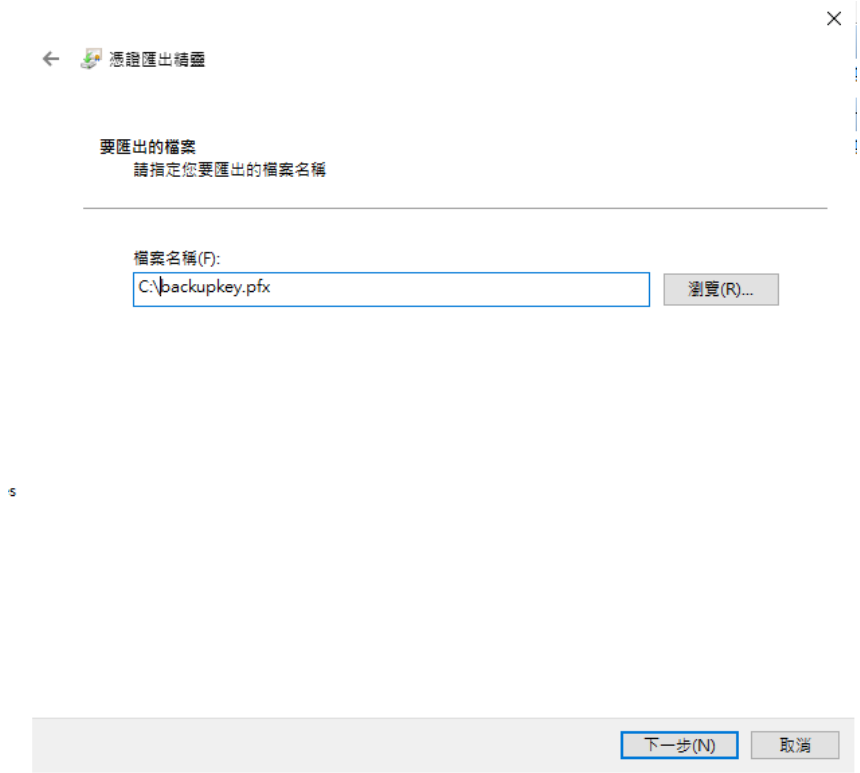


8. 选择[个人资讯交换 – PKCS #12 (.PFX)(P)]，只选取[如果可能的话，包含凭证路径中的所有凭证(U)]及[启用凭证隐私权(E)]，然后按[下一步]。

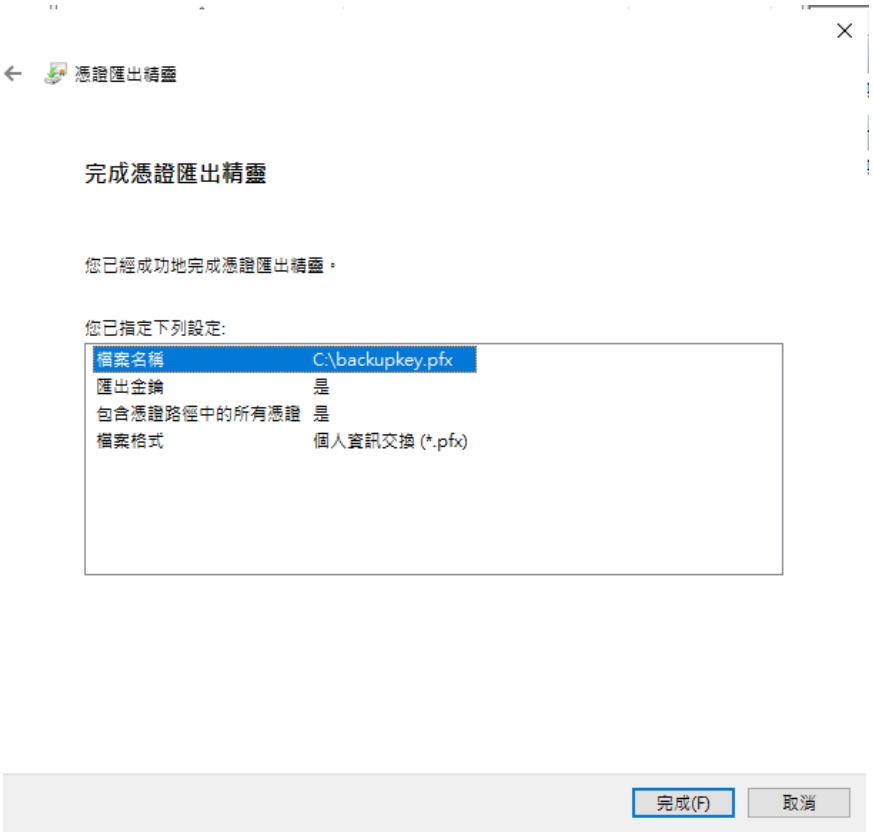
9. 输入密码匙的密码，然后按[下一步]。

注意：请紧记这个重要的密码。如果您忘记这密码，您将不能还原您的密码匙。

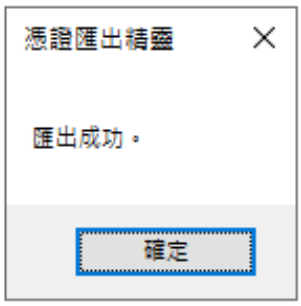
10. 按[浏览]指定密码匙的备份档案，然后按[下一步]。（此档案的副档名预设值为 pfx）。



11. 按[完成]来关闭精灵。

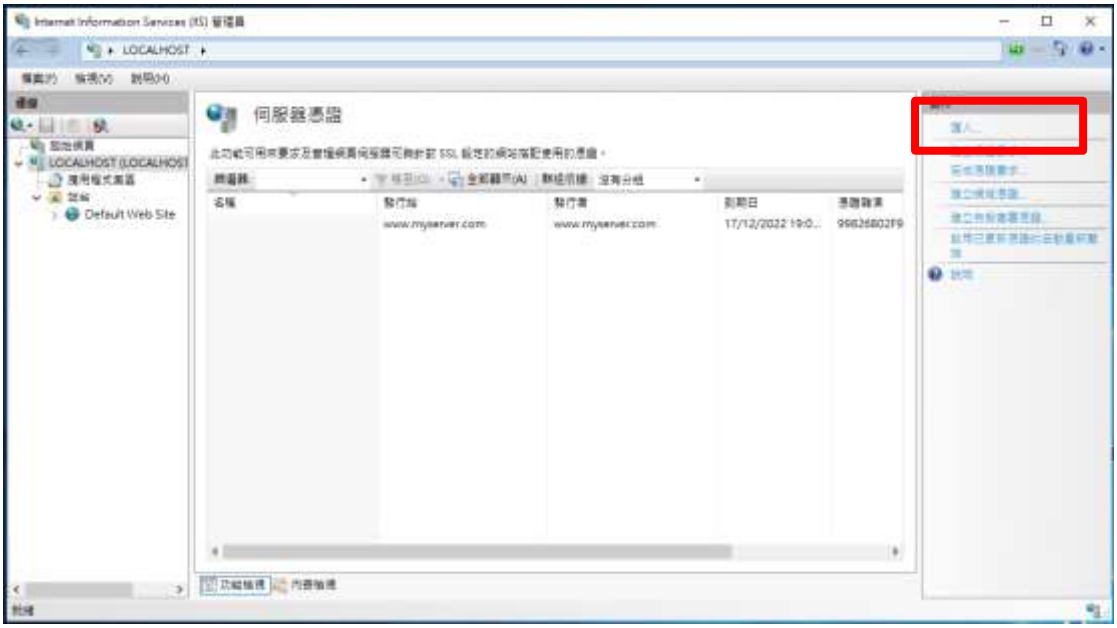


12. 按[确定]来完成。



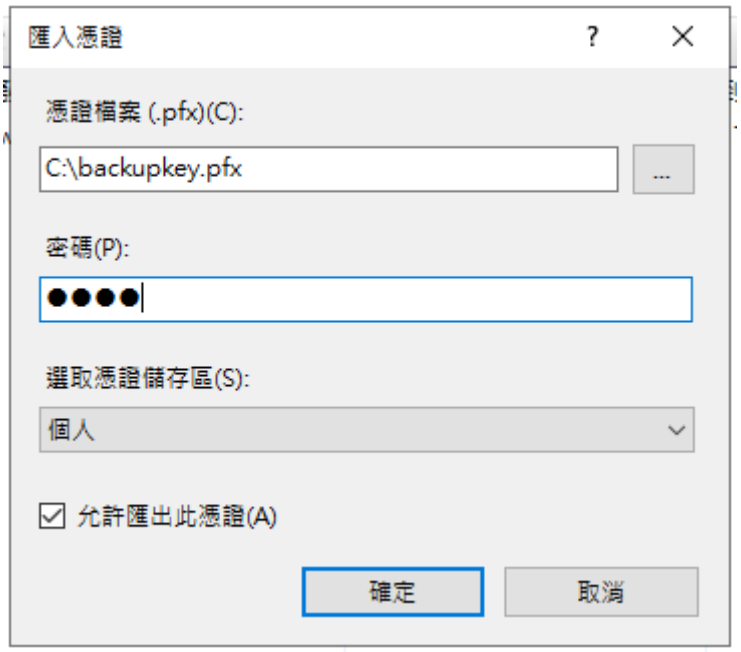
G. 还原密码匙

1. 按[开始]>[控制台]>[所有控制台项目]>[系统管理工具]>[Internet Information Services (IIS) 管理员]来启动网际网路资讯服务 (IIS) 管理员。
2. 选择你的网站，然后按[伺服器凭证]。
3. 在右手边动作一栏内，按[汇入]。



4. 输入包含凭证的档案名称及路径及凭证的密码，然后按[确定]。

> 注意：你可以取消选取[允许汇出此凭证]使不允许汇出凭证。或为使您将來可以进行备份或传输您的凭证，可选取[允许汇出此凭证]使凭证可汇出。



5. 电子证书（伺服器）证书已成功汇入。