

# SSL 證書 - IIS 10

證書安裝指南



# IIS 10: Create CSR and Install SSL Certificate 創建 CSR 並安裝 SSL 證書

在 Windows 服務器 2016 上創建 CSR 並安裝 SSL 證書



應用此頁面上的說明來使用 IIS 10 創建證書簽名請求(CSR),然後在 Windows Server 2016 上安裝 SSL 證書。

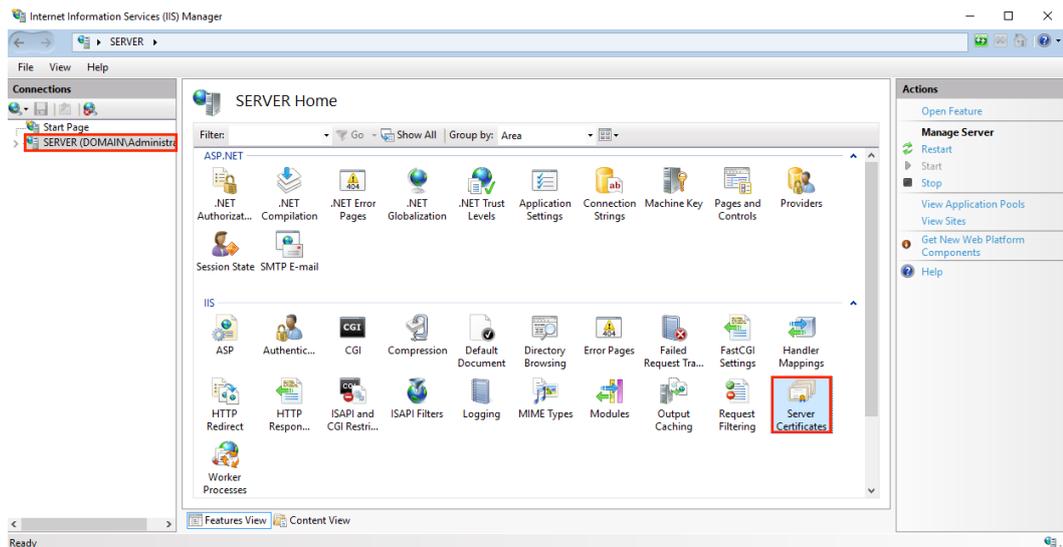
1. 要創建證書簽名請求(CSR) , 請參閱 [IIS 10: 如何在 Windows Server 2016 上創建 CSR](#) 。
2. 要安裝 SSL 證書, 請參閱 [IIS 10: 如何在 Windows Server 2016 上安裝和配置 SSL 證書](#)。

如果您正在尋找更簡單的方法來創建 CSR, 以及安裝和管理您的 SSL 證書, 我們建議您使用適用於 Windows 的 DigiCert®證書實用程式。您可以使用 DigiCert Utility 生成 CSR 並安裝 SSL 證書。請參閱 [Windows Server 2016: 使用 DigiCert Utility 創建 CSR 並安裝 SSL 證書](#)。

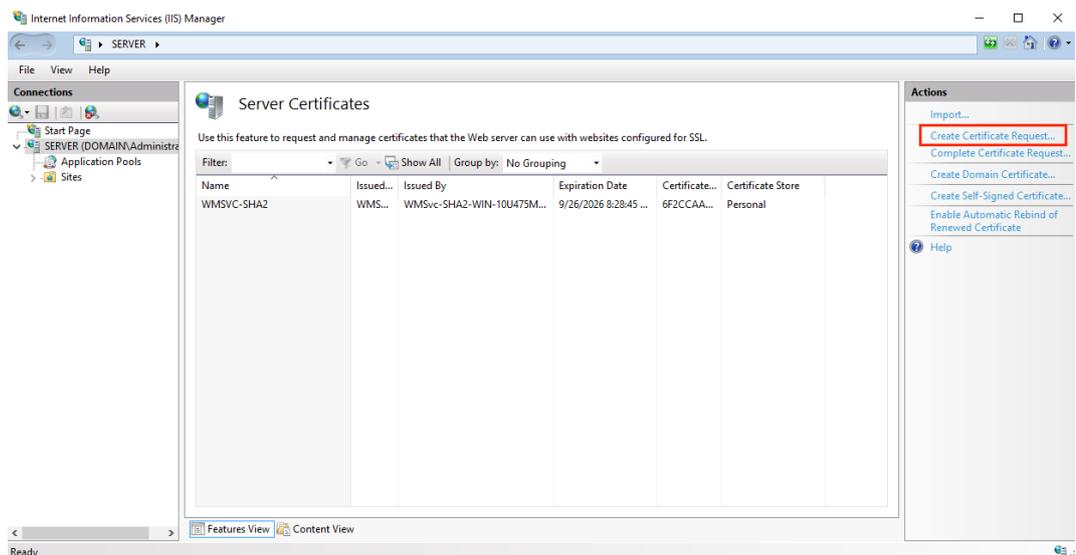
## 1. 如何在 Windows Server 2016 上創建 CSR

### 使用 IIS 10 創建 CSR

1. 在 Windows 開始功能表中, 鍵入 **Internet 資訊服務 (IIS) 管理器** 並將其打開。
2. 在 **Internet 資訊服務 (IIS) 管理器** 的「**連接**」功能表樹 (左窗格) 中, 找到並按一下伺服器名稱。



3. 在伺服器名稱主頁（中心窗格）的 IIS 部分中，按兩下「伺服器憑證」。
4. 在「伺服器憑證」頁面（中心窗格）的「操作」功能表（右窗格）中，按一下「創建證書申請...」連結。



5. 在「請求證書」嚮導的「可分辨名稱屬性」頁面上，提供下面指定的資訊，然後按一下「下一步」：

- 通用名稱:** 輸入完全限定的功能變數名稱(FQDN) (例如:www.example.com)
- 組織:** 輸入您公司的合法註冊名稱 (例如: *YourCompany,Inc.*)
- 組織單元:** 組織內部部門的名稱。此條目通常會被列為「IT」,「Web Security」,或者只是留空。
- 城市/地區:** 輸入貴公司合法所在的城市

州/省: 輸入貴公司合法所在的州/省

國家: 在下拉清單中, 選擇貴公司合法所在的國家/地區

Request Certificate ? X

 **Distinguished Name Properties**

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name:	<input type="text" value="www.yourdomain.com"/>
Organization:	<input type="text" value="Your Company, Inc."/>
Organizational unit:	<input type="text" value="IT"/>
City/locality	<input type="text" value="Lehi"/>
State/province:	<input type="text" value="UT"/>
Country/region:	<input type="text" value="US"/>

Previous **Next** Finish Cancel

6. 在「密碼編譯服務提供者屬性」頁上, 提供以下資訊, 然後按一下「下一步」。

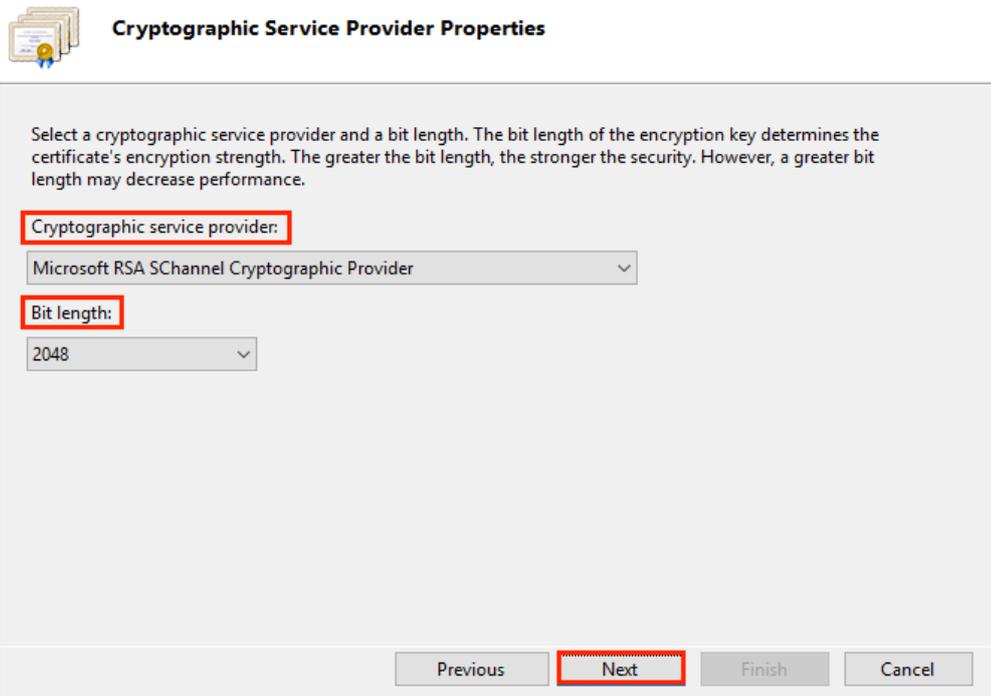
加密服務提供者:

在下拉清單中, 選擇**微軟 RSA S 通道加密供應商**,

unless you have a specific cryptographic provider. 在下拉清單中, 選擇 **Microsoft RSA SChannel Cryptographic Provider**, 除非您有特定的加密提供程式。

位長:

在下拉清單中選擇 **2048**, 除非您有特定原因選擇更大的位長



**Cryptographic Service Provider Properties**

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

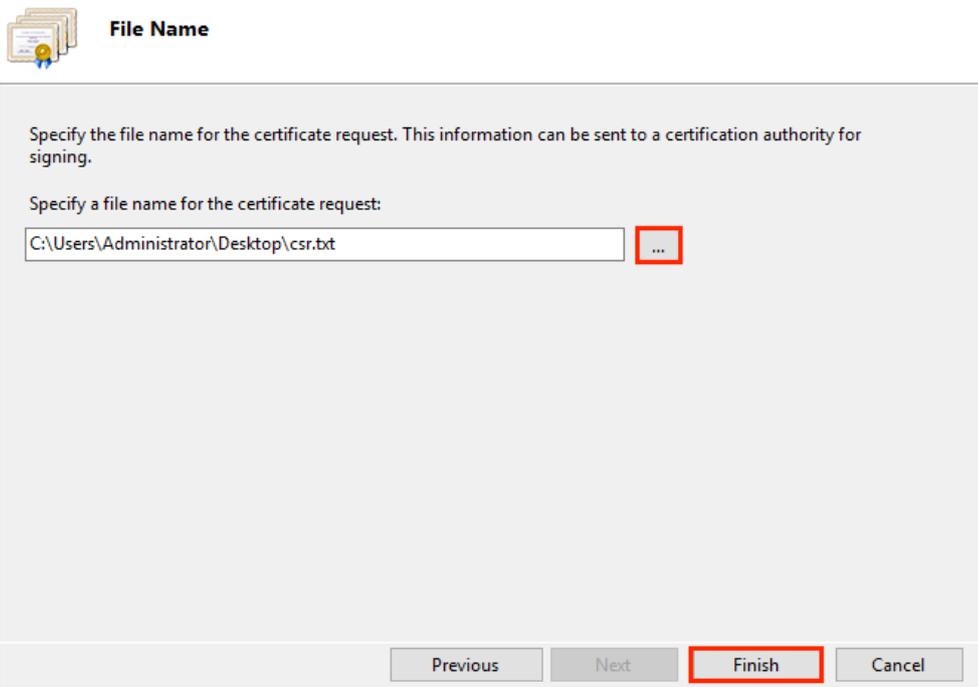
**Cryptographic service provider:**  
Microsoft RSA SChannel Cryptographic Provider

**Bit length:**  
2048

Previous **Next** Finish Cancel

7. 在「檔案名」頁面上的「為證書申請指定檔案名」下，按一下「...」框以流覽到要保存 CSR 的位置。

**注意：**請記住您選擇的檔案名以及保存 csr.txt 檔的位置。如果您只是輸入檔案名而不流覽某個位置，那麼您的 CSR 將以 C: \ Windows \ System32 結尾。



**File Name**

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:  
C:\Users\Administrator\Desktop\csr.txt

...

Previous Next **Finish** Cancel

8. 完成後，按一下「完成」。

9. 使用文字編輯器（如記事本）打開檔。然後，複製文本，包括-----開始新證書請求-----和-----結束新證書請求-----標籤，並將其粘貼到迪吉切特訂購表中。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAaQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCV1vdXJtZGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAK1UMRowGAYDVQQKEXFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdrQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc31
RdEbdKyHDtHklRAoIVQCfjTwBWNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwqx
7pVfaDb2PuTgUhw7wksKNFxcG0xcTmr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYakeJUOJtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABoAAwDQYJ
KoZIHvcNAQEFBQADggEBAAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NhrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIZzHVGRoR3r7xQtIuMaDar3x1V8jHbcvZTepX0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPIEdzFnaYtUy2BDcXj3ZQEwXRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGviKT6/Ryfwg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

### 準備訂購您的 SSL 證書

10. 從 DigiCert 收到 SSL 證書後，您可以安裝它。

## 2. IIS 10：如何在 Windows Server 2016 上安裝和配置 SSL 證書

如果您尚未創建 CSR 並訂購了證書，請參閱 IIS 10：如何創建 CSR Windows Server 2016。

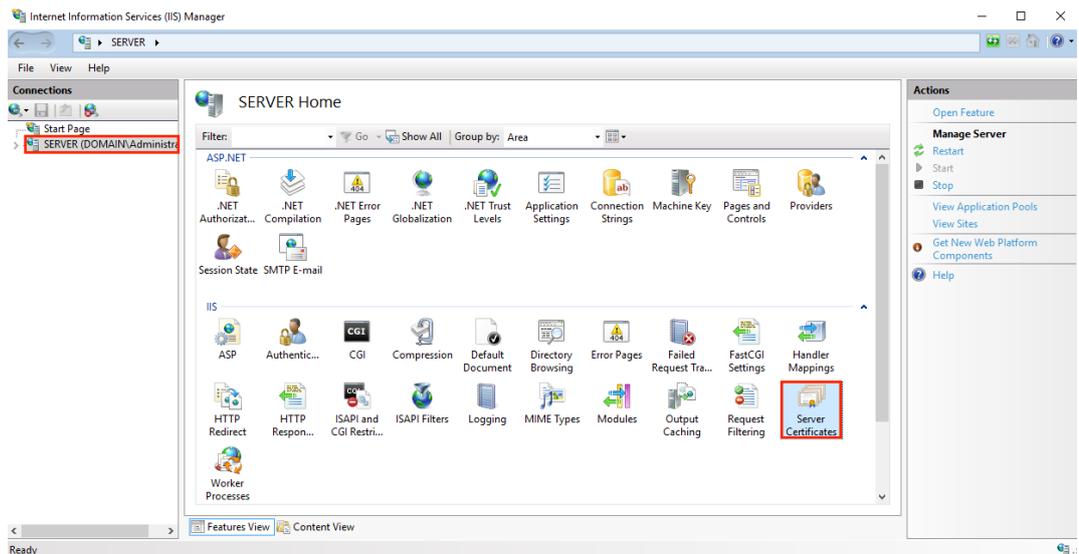
驗證並頒發 SSL 證書後，您需要將其安裝在生成 CSR 的 Windows 2016 伺服器上。然後，您需要佈建伺服器以使用它。

- [（單個證書）如何安裝和配置 SSL 證書](#)
- [（多個證書）如何使用 SNI 安裝和配置 SSL 證書](#)

### （單個證書）如何安裝 SSL 證書並佈建伺服器以使用它

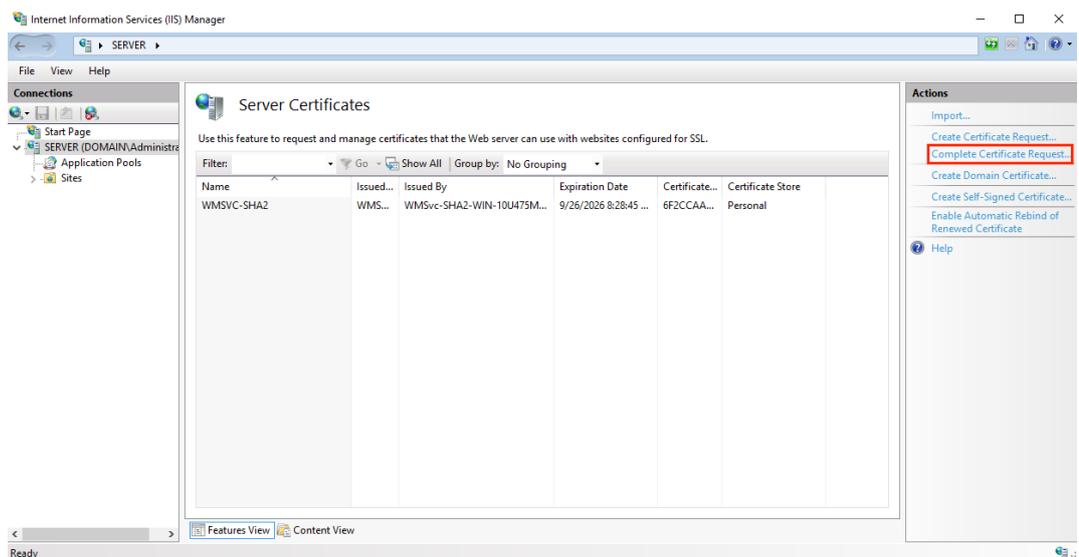
#### 安裝 SSL 證書

1. CSR 的服務器上，保存 SSL 證書。DigiCert 發送給您的 cer 文件（例如，your\_domain\_com.cer）。
2. 在 Windows 開始功能表中，鍵入 *Internet 資訊服務 (IIS) 管理器* 並將其打開。
3. 在 *Internet 資訊服務 (IIS) 管理器* 的「連接」功能表樹（左窗格）中，找到並按一下伺服器名稱。



4.在伺服器名稱主頁（中心窗格）的 IIS 部分中，按兩下「伺服器憑證」。

5.在「伺服器憑證」頁面（中心窗格）的「操作」功能表（右窗格）中，按一下「完成證書申請...」連結。



6.在「完成證書申請」嚮導的「指定憑證授權單位回應」頁上，執行以下操作，然後按一下「確定」：

**檔案名包含憑證授權單位的回復：** 單擊...框並瀏覽並選擇.cer 文件

**易記名稱：** 鍵入證書的友好名稱

易記名稱不是證書的一部分；相反，它用於識別證書。

我們建議您將 DigiCert 和截止日期添加到易記名稱的末尾，例如：yoursite-digicert -（截止日期）。

此資訊有助於識別每個證書的頒發者和到期日期。它還有助於區分具有相同功能變數名稱的多個證書。

選擇證書庫對於新  
證書： 在下拉清單中，選擇「虛擬主機」。

Complete Certificate Request

? X



### Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\Users\Administrator\Desktop\certs\your\_domain\_name.cer

Friendly name:

yourdomain.com

Select a certificate store for the new certificate:

Web Hosting

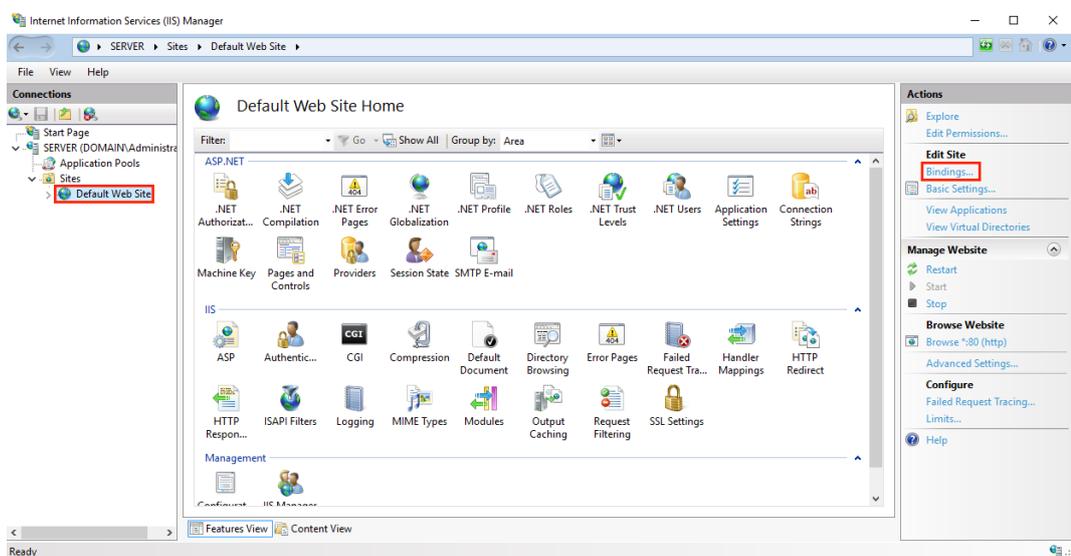
OK

Cancel

7.現在您已成功安裝 SSL 證書，您需要將證書分配給相應的網站。

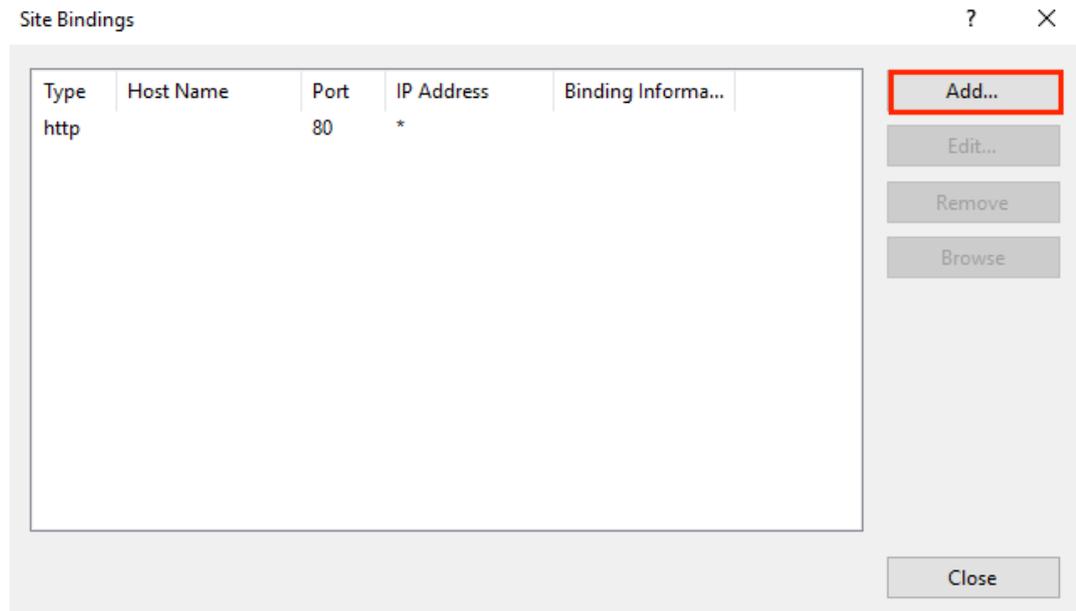
## 分配 SSL 證書

8. 在 Internet 資訊服務 (IIS) 管理器的「連接」功能表樹 (左窗格) 中，展開安裝證書的伺服器的名稱。然後展開「網站」，然後按一下要使用 SSL 證書進行保護的網站。



9.在網站主頁上的「操作」功能表（右側窗格）中的「編輯網站」下，按一下「綁定...」連結。

10.在「網站綁定」視窗中，按一下「添加」。



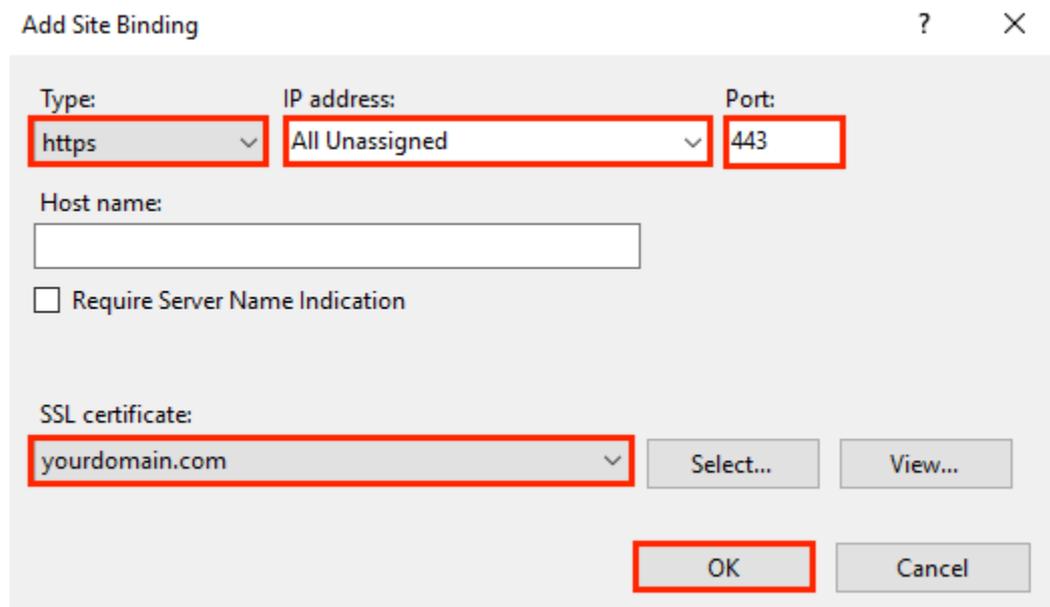
11.在「添加網站綁定」視窗中，執行以下操作，然後按一下「確定」：

**類型：** 在下拉清單中,選擇 **HTTPS**。

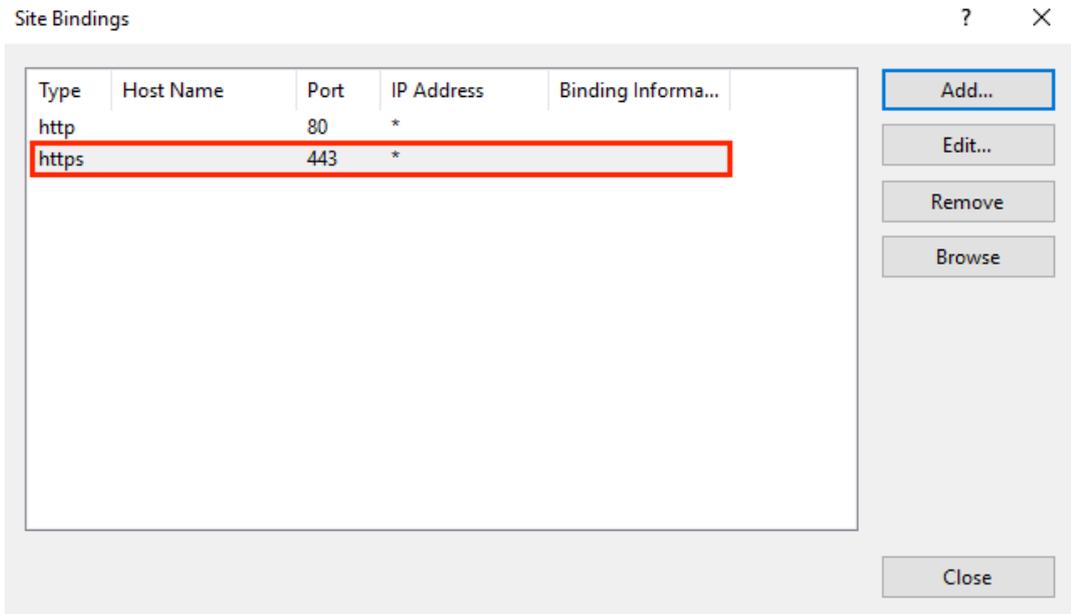
**IP 地址** 在下拉清單中,選擇網站的 IP 位址或選擇"所有未分配"。

**端口：** 輸入端口 **443**。通過 SSL 保護流量的端口是端口 443

**SSL 證書** 在下拉清單中，選擇新的 SSL 證書（例如，*yourdomain.com*）。



12. 您的 SSL 證書現已安裝，並且網站已配置為接受安全連線。



# (多個證書) 如何安裝 SSL 證書並佈建服務器以使用 SNI 使用它們

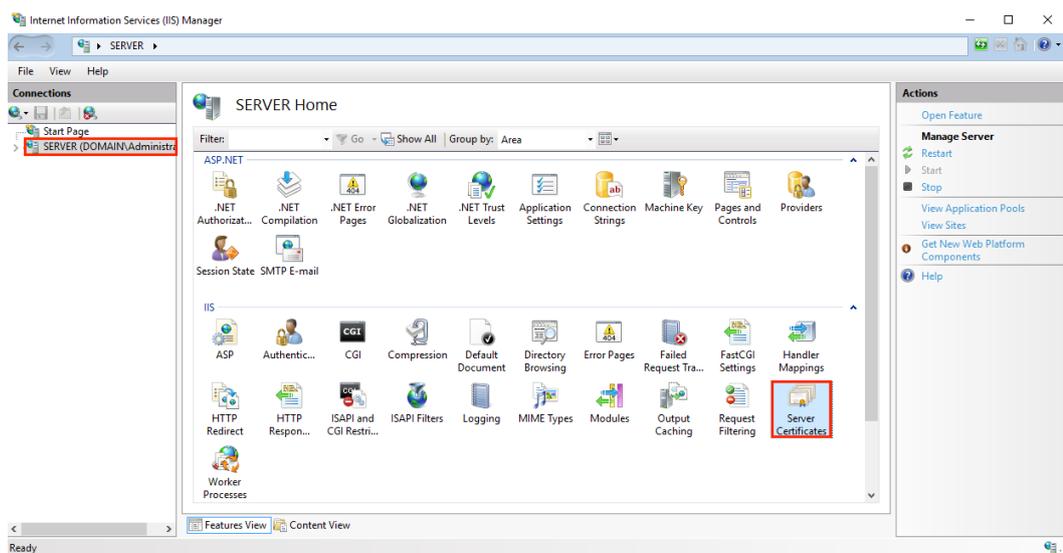
該指令說明了如何安裝多個 SSL 證書並使用 SNI 進行分配。該過程分為以下兩部分：

- [安裝和配置您的第一個 SSL 證書](#)
- [安裝和配置所有其他證書](#)

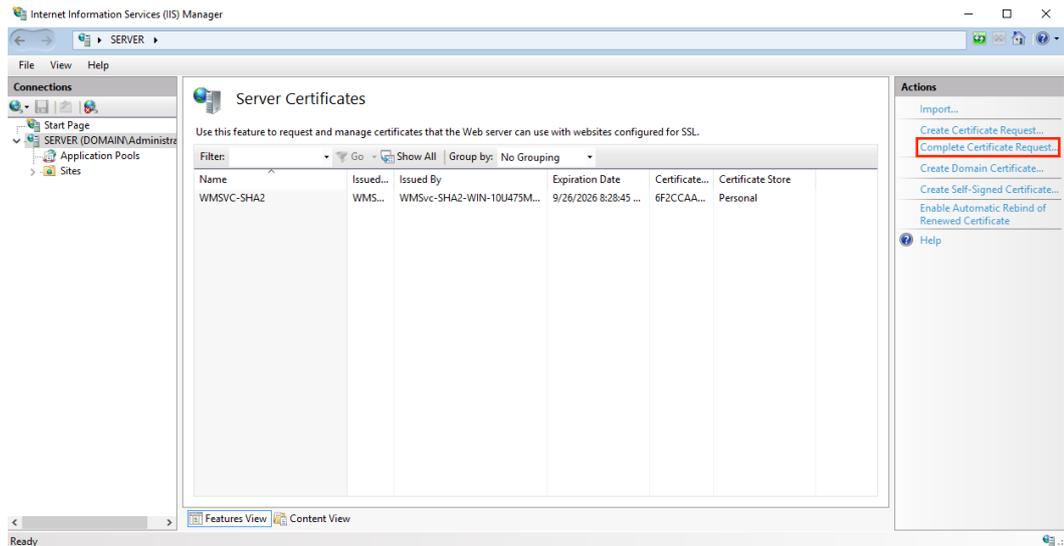
## 安裝第一個 SSL 證書

對於第一個 SSL 證書，僅執行一次第一組指令。

1. 在創建 CSR 的服務器上，保存 SSL 證書。DigiCert 發送給您的 cer 文件（例如，your\_domain\_com.cer）。
2. 在 **Windows** 開始功能表中，鍵入 **Internet 資訊服務 (IIS) 管理器** 並將其打開。
3. 在 **Internet 資訊服務 (IIS) 管理器** 的「**連接**」功能表樹（左窗格）中，找到並按一下伺服器名稱



4. 在伺服器名稱主頁（中心窗格）的 **IIS** 部分中，按兩下「**伺服器憑證**」。
5. 在「**伺服器憑證**」頁面（中心面板）的「**操作**」功能表（右窗格）中，按一下「**完成證書申請...**」連結。



6. 在「完成證書申請」嚮導的「指定憑證授權單位回應」頁上，執行以下操作，然後按一下「確定」：

**檔案名包含憑證授** 單擊... 框並瀏覽並選擇.cer 文件

**權單位的回復：** (例如, your\_domain\_com.cer) DigiCert 發送給您。

**易記名稱：** 鍵入證書的易記名稱。

易記名稱不是證書的一部分;相反, 它用於識別證書。

我們建議您將 DigiCert 和截止日期添加到易記名稱的末尾, 例如: yoursite-digicert - (截止日期)

此資訊有助於識別每個證書的頒發者和到期日期。 它還有助於區分具有相同功能變數名稱的多個證書。

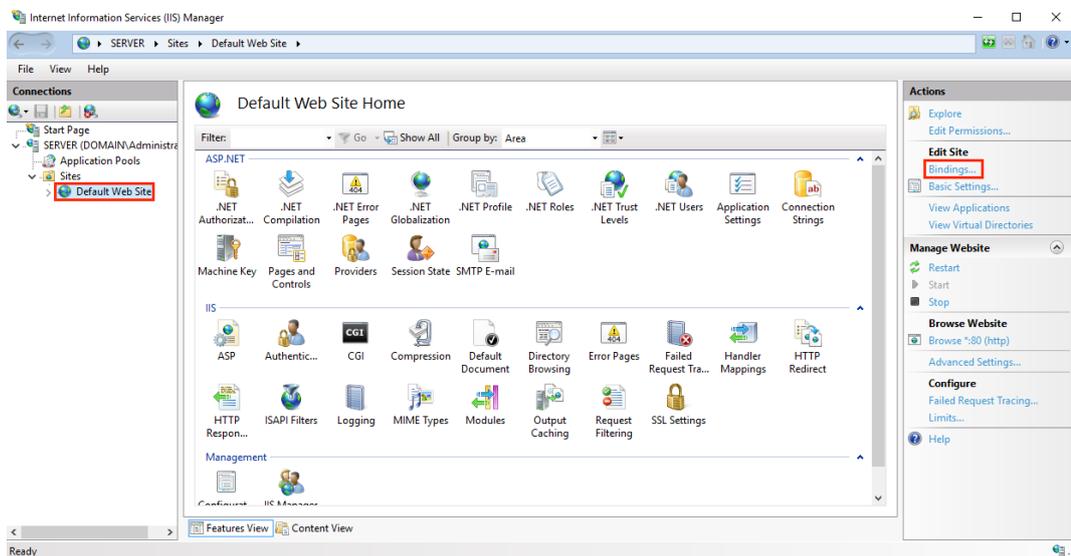
**為新證書選擇證書**

**存儲區：** 在下拉清單中, 選擇「虛擬主機」。



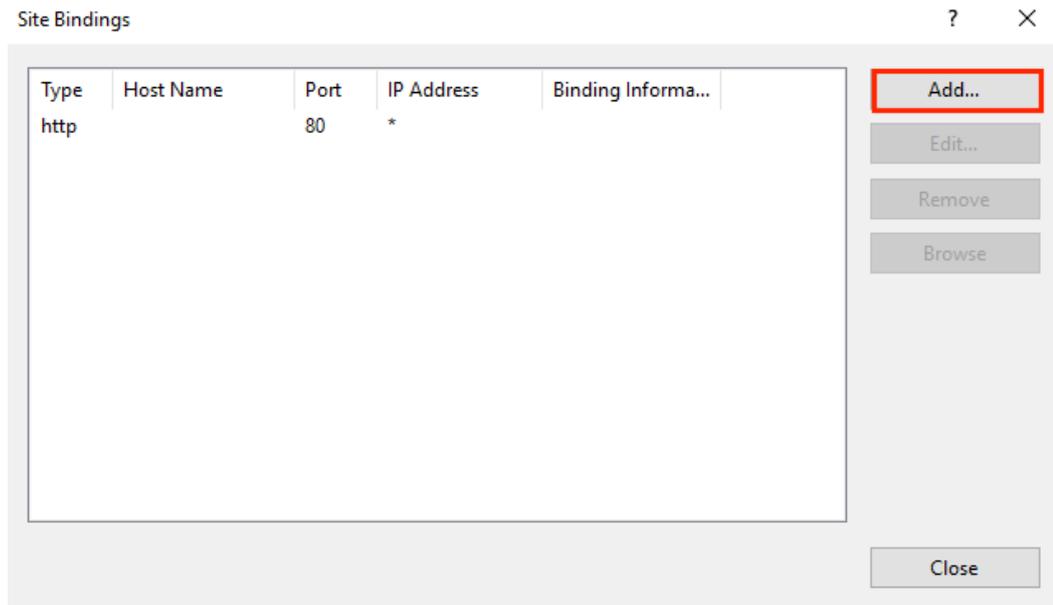
7. 現在您已成功安裝 SSL 證書，您需要將證書分配給相應的網站。

8. 在 **Internet 資訊服務 (IIS) 管理器** 的「**連接**」功能表樹 (左窗格) 中，展開安裝證書的伺服器的名稱。然後展開「**網站**」，然後按一下要使用 SSL 證書進行保護的網站。



9. 在網站主頁上的“**操作**”菜單 (右側窗格) 中的“**編輯網站**”下，單擊“**綁定...**”鏈接。

10. 在“站點綁定”窗口中，單擊“添加”。



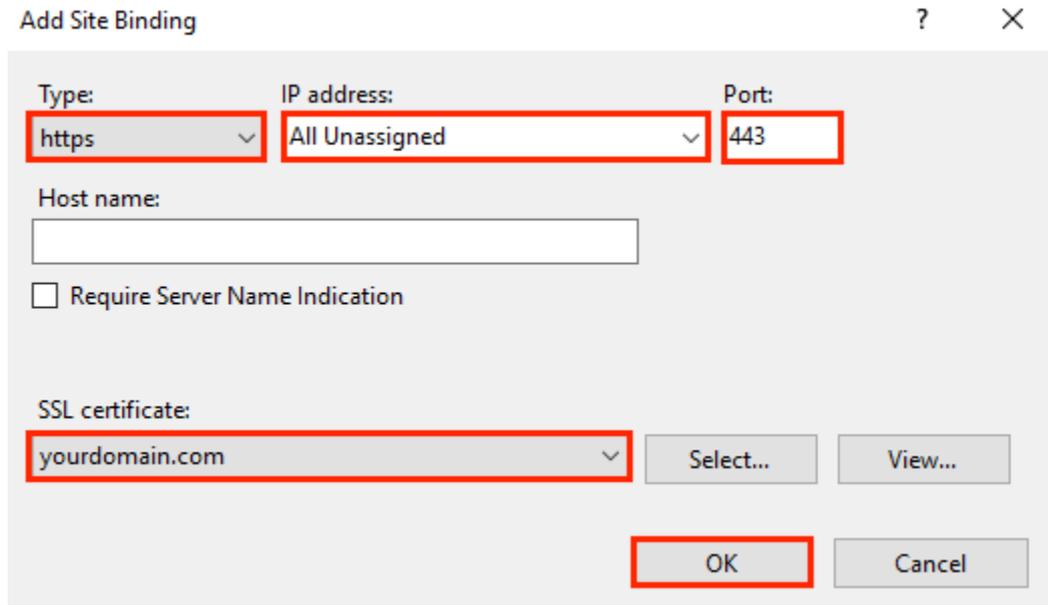
11. 在「添加網站綁定」視窗中，執行以下操作，然後按一下「確定」：

**類型：** 在下拉清單中，選擇 **HTTPS**。

**IP 地址** 在下拉清單中，選擇網站的 IP 位址或選擇「全部未分配」。

**端口：** 輸入端口 **443**。通過 SSL 保護流量的端口是端口 443。

**SSL 證書** 在下拉清單中，選擇新的 SSL 證書（例如，*yourdomain.com*）。

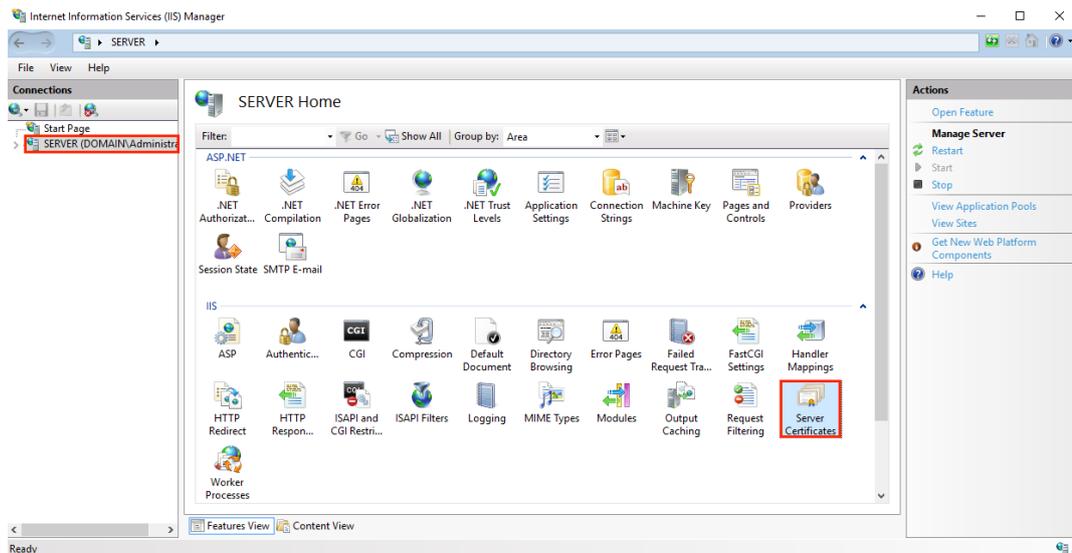


12. 您的第一個 SSL 證書現已安裝，並且該網站已配置為接受安全連線。

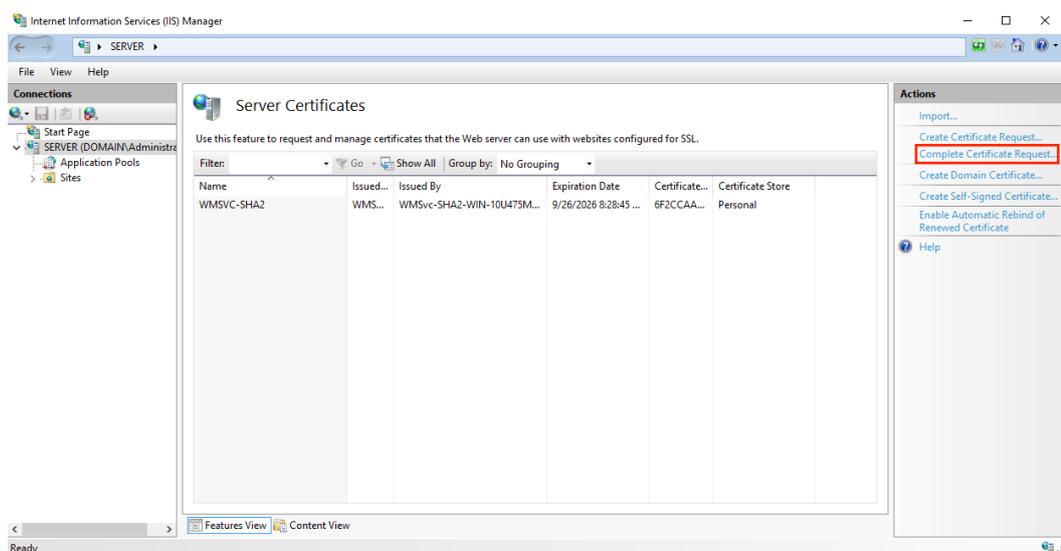
## 安裝其他 SSL 證書

要安裝和分配每個其他 SSL 證書，請根據需要重複以下步驟。

1. 在創建 CSR 的服務器上，保存 SSL 證書。DigiCert 發送給您的 cer 文件（例如，your\_domain\_com.cer）。
2. 在 **Windows** 開始功能表中，鍵入 **Internet 資訊服務 (IIS) 管理器** 並將其打開。
3. 在 **Internet 資訊服務 (IIS) 管理器** 的「連接」功能表樹（左窗格）中，找到並按一下伺服器名稱。



4. 在伺服器名稱主頁（中心窗格）的 **IIS** 部分中，按兩下「**伺服器憑證**」。在伺服器名稱主頁（中心窗格）的 **IIS** 部分中，按兩下「**伺服器憑證**」。
5. 在「**伺服器憑證**」頁面（中心窗格）的「**操作**」功能表（右窗格）中，按一下「**完成證書申請...**」連結。



6. 在「完成證書申請」嚮導的「指定憑證授權單位回應」頁上，執行以下操作，然後按一下「確定」：

**檔案名包含憑證授權單位的回復：** 單擊...框並瀏覽並選擇.cer 文件（例如，your\_domain\_com.cer）DigiCert 發送給您。

**易記名稱：** 鍵入證書的易記名稱。  
易記名稱不是證書的一部分；相反，它用於識別證書。  
我們建議您將 DigiCert 和截止日期添加到易記名稱的末尾，例如：yoursite-digicert - （截止日期）。  
此資訊有助於識別每個證書的頒發者和到期日期。它還有助於區分具有相同功能變數名稱的多個證書。

**為新證書選擇憑證存放區：** 在下拉清單中，選擇「虛擬主機」



Complete Certificate Request

**Specify Certificate Authority Response**

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:  
C:\Users\Administrator\Desktop\certs\your\_domain\_name.cer

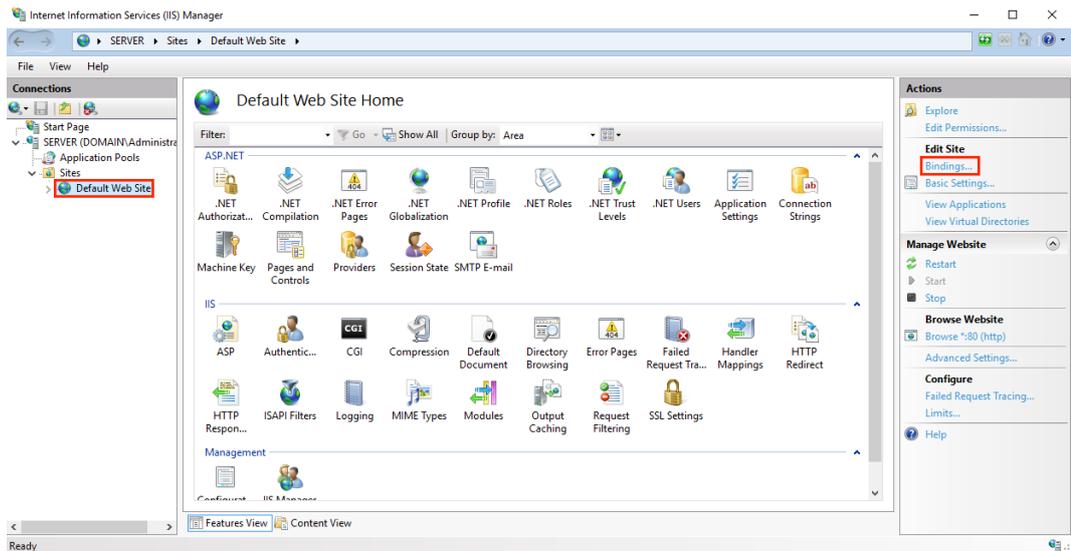
Friendly name:  
yourdomain.com

Select a certificate store for the new certificate:  
Web Hosting

OK Cancel

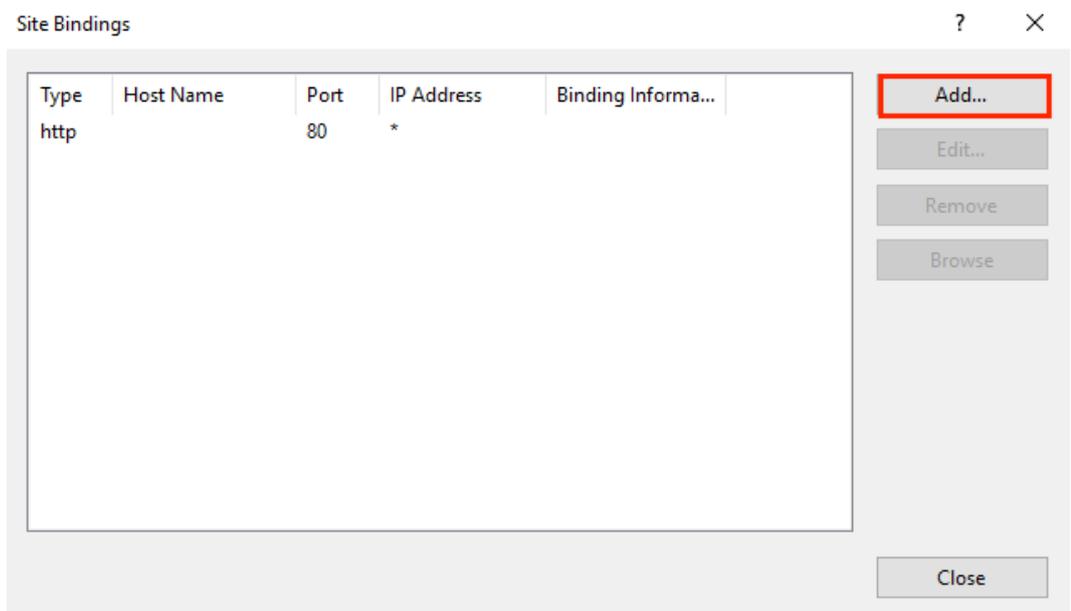
7. 現在您已成功安裝 SSL 證書，您需要將證書分配給相應的網站。

8. 在 Internet 資訊服務 (IIS) 管理器的「連接」功能表樹（左窗格）中，展開安裝證書的伺服器的名稱。然後展開「網站」，然後按一下要使用 SSL 證書進行保護的網站。



9 在網站主頁上的“操作”菜單（右側窗格）中的“編輯網站”下，單擊“綁定...”鏈接。

10.在「網站綁定」視窗中，按一下「添加」。



11.在「添加網站綁定」視窗中，執行以下操作，然後按一下「確定」：

**類型：** 在下拉清單中，選擇 **HTTPS**。

**IP 地址** 在下拉清單中，選擇網站的 IP 位址或選擇「全部未分配」。

**端口：** 輸入端口 **443**。通過 SSL 保護流量的端口是端口 443。

**主機名稱：** 輸入要保護的主機名稱。

輸入主機名稱後，選中此框。

**需要伺服器名稱指示：** 在安裝第一個證書並保護主網站之後，所有其他證書/網站都需要這樣做。

**SSL 證書** 在下拉清單中，選擇其他 SSL 證書（例如，*yourdomain2.com*）。

Add Site Binding ? X

Type:	IP address:	Port:
https	All Unassigned	443

Host name:  
yourdomain2.com

Require Server Name Indication

SSL certificate:  
yourdomain2.com

Select... View...

OK Cancel

12. 您已成功安裝了另一個 SSL 證書，並將網站配置為接受安全連線。

## 測試安裝

如果您的網站可公開訪問，[DigiCert®SSL 安裝診斷工具](#)可以說明您診斷常見問題。