

# SSL 证书 - IIS 10

## 证书安装指南



# IIS 10: Create CSR and Install SSL Certificate 创建 CSR 并安装 SSL 证书

在 Windows 服务器 2016 上创建 CSR 并安装 SSL 证书



应用此页面上的说明来使用 IIS 10 创建证书签名请求(CSR),然后在 Windows Server 2016 上安装 SSL 证书。

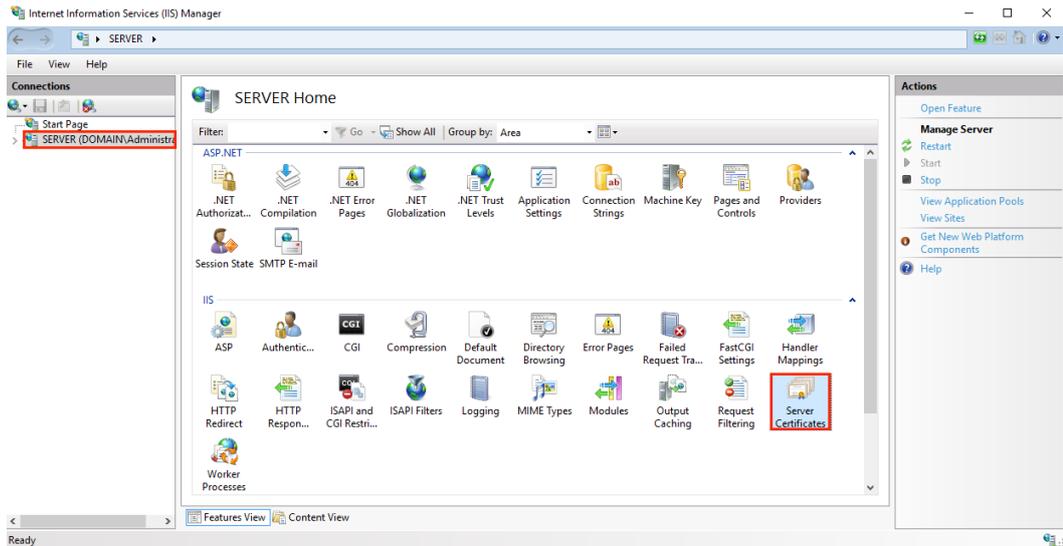
1. 要创建证书签名请求(CSR), 请参阅 [IIS 10: 如何在 Windows Server 2016 上创建 CSR](#)。
2. 要安装 SSL 证书, 请参阅 [IIS 10: 如何在 Windows Server 2016 上安装和配置 SSL 证书](#)。

如果您正在寻找更简单的方法来创建 CSR, 以及安装和管理您的 SSL 证书, 我们建议您使用适用于 Windows 的 DigiCert®证书实用程序。您可以使用 DigiCert Utility 生成 CSR 并安装 SSL 证书。请参阅 [Windows Server 2016: 使用 DigiCert Utility 创建 CSR 并安装 SSL 证书](#)。

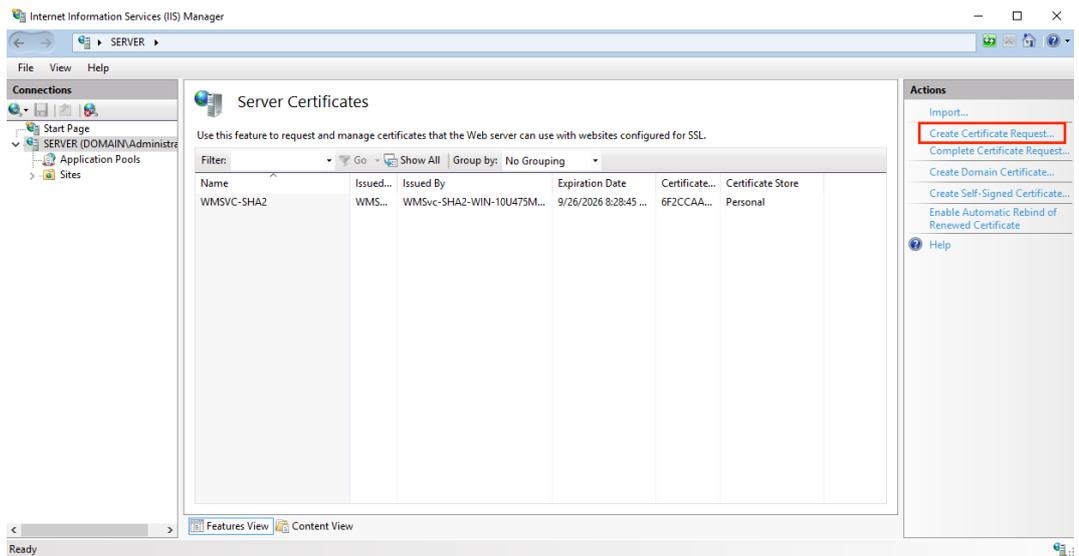
## 1.如何在 Windows Server 2016 上创建 CSR

### 使用 IIS 10 创建 CSR

1. 在 **Windows** 开始菜单中, 键入 **Internet 信息服务 (IIS) 管理器**并将其打开。
2. 在 **Internet 信息服务 (IIS) 管理器**的“**连接**”菜单树 (左窗格) 中, 找到并点击服务器名称。



3. 在服务器名称主页（中心窗格）的 **IIS** 部分中，双击“服务器证书”。
4. 在“服务器证书”页面（中心窗格）的“操作”菜单（右窗格）中，单击“创建证书申请...”链接。



5. 在“请求证书”向导的“可分辨名称属性”页面上，提供下面指定的信息，然后单击“下一步”：

**通用名称:** 输入完全限定的域名(FQDN) (例如:www.example.com)

**组织:** 输入您公司的合法注册名称 (例如: *YourCompany,Inc.*)

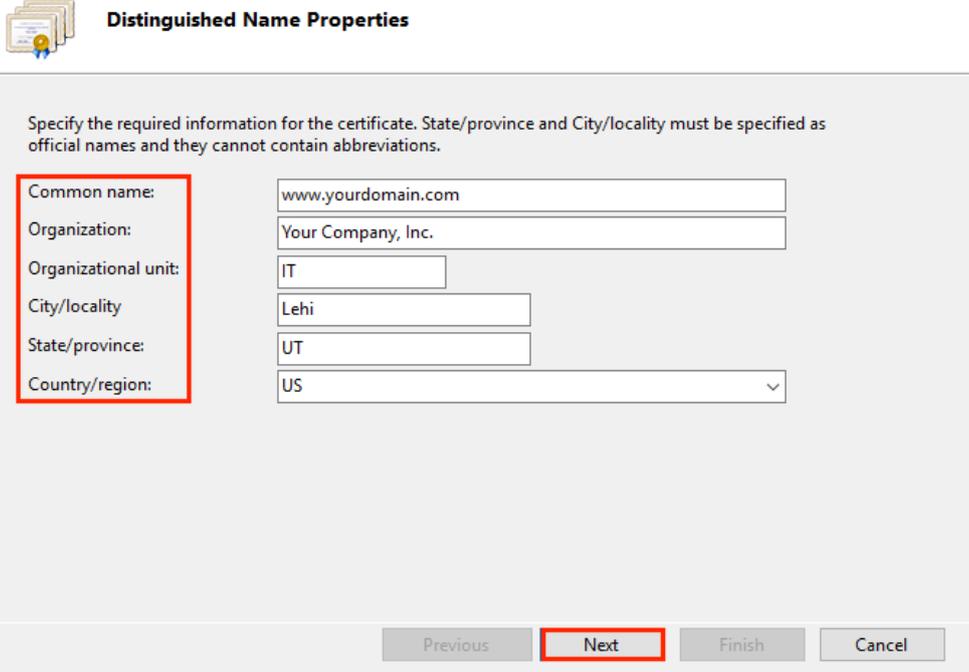
**组织单元:** 组织内部部门的名称。此条目通常会被列为“IT”, “Web Security”, 或者只是留空。

**城市/地区:** 输入贵公司合法所在的城市

**州/省:** 输入贵公司合法所在的州/省

**国家:** 在下拉列表中, 选择贵公司合法所在的国家/地区

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.

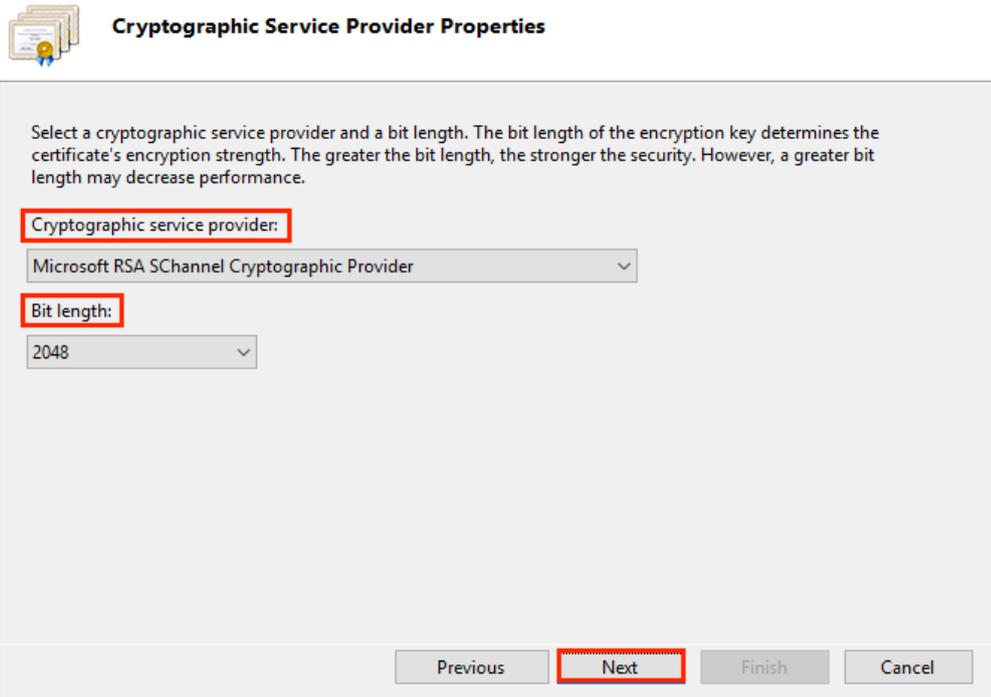
Common name:	www.yourdomain.com
Organization:	Your Company, Inc.
Organizational unit:	IT
City/locality:	Lehi
State/province:	UT
Country/region:	US

Previous **Next** Finish Cancel

6. 在“加密服务提供程序属性”页上, 提供以下信息, 然后单击“下一步”。

**加密服务提供者:** 在下拉列表中, 选择 **Microsoft RSA SChannel Cryptographic Provider**, 除非您有特定的加密提供程序。

**Bit length:** 在下拉列表中选择 **2048**, 除非您有特定原因选择更大的位长



**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.

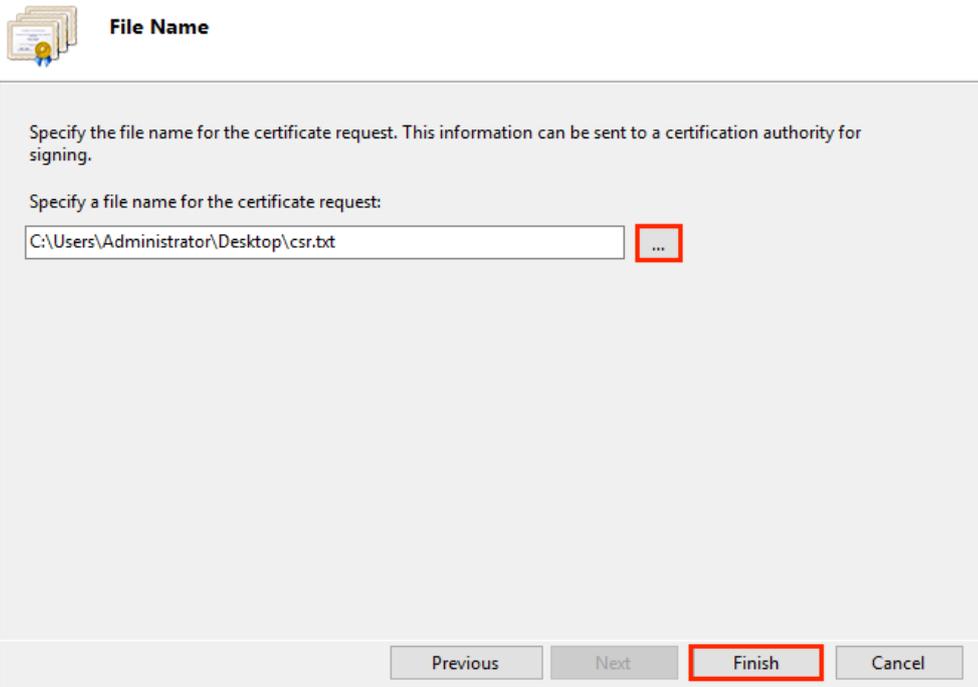
**Cryptographic service provider:**  
Microsoft RSA SChannel Cryptographic Provider

**Bit length:**  
2048

Previous Next Finish Cancel

7. 在“文件名”页面上的“为证书申请指定文件名”下，单击“...”框以浏览到要保存 CSR 的位置。

**注意：**请记住您选择的文件名以及保存 csr.txt 文件的位置。如果您只是输入文件名而不浏览某个位置，那么您的 CSR 将以 C:\Windows\System32 结尾。



**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. 完成后，单击“完成”。

9. 使用文本编辑器（如记事本）打开文件。然后，复制文本，包括----- **BEGIN NEW CERTIFICATE REQUEST** ----- 和----- **END NEW CERTIFICATE REQUEST** ----- 标签，并将其粘贴到 DigiCert 订购表中。

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJldGF0ZTER
MA8GA1UEBxMIW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHdtHk1RAoIVQCfjTwBwGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwqx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTMr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABAAAwDQYJ
KoZIHvcNAQEFBQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NhrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEb08GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAR3xlV8jHbcvZTcpx0Kbq6H1G
NLA4CXsOI4KGwu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGBnLPe4XMy7NPiEdzFnaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziunm1Df24NBt5tpCNzfGviKT6/RyfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

### 准备订购您的 SSL 证书

10. 从 DigiCert 收到 SSL 证书后，您可以安装它。

## 2. IIS 10：如何在 Windows Server 2016 上安装和配置 SSL 证书

如果您尚未创建 CSR 并订购了证书，请参阅 [IIS 10：如何创建 CSR Windows Server 2016](#)。

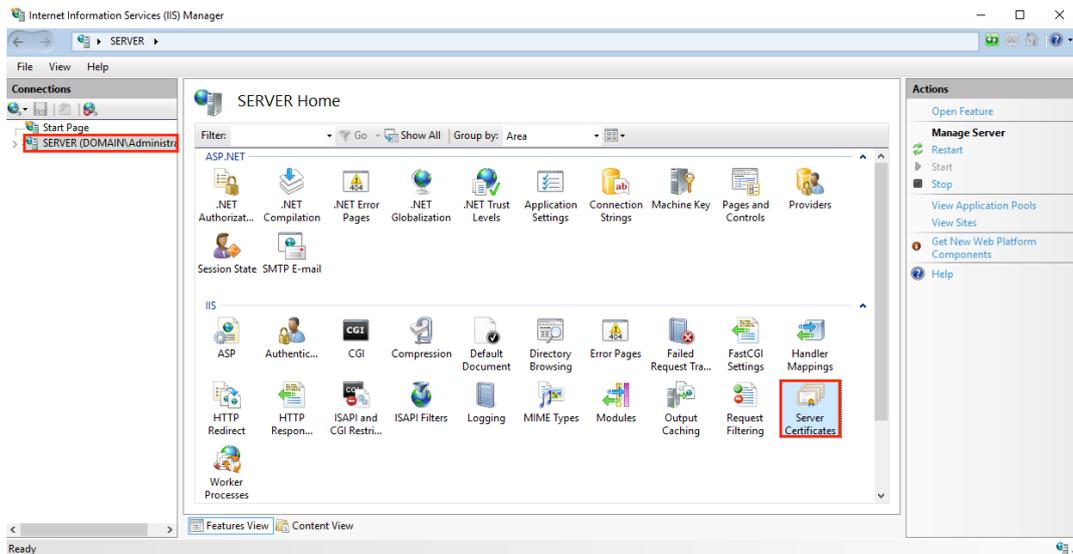
验证并颁发 SSL 证书后，您需要将其安装在生成 CSR 的 Windows 2016 服务器上。然后，您需要配置服务器以使用它。

- [（单个证书）如何安装和配置 SSL 证书](#)
- [（多个证书）如何使用 SNI 安装和配置 SSL 证书](#)

### （单个证书）如何安装 SSL 证书并配置服务器以使用它

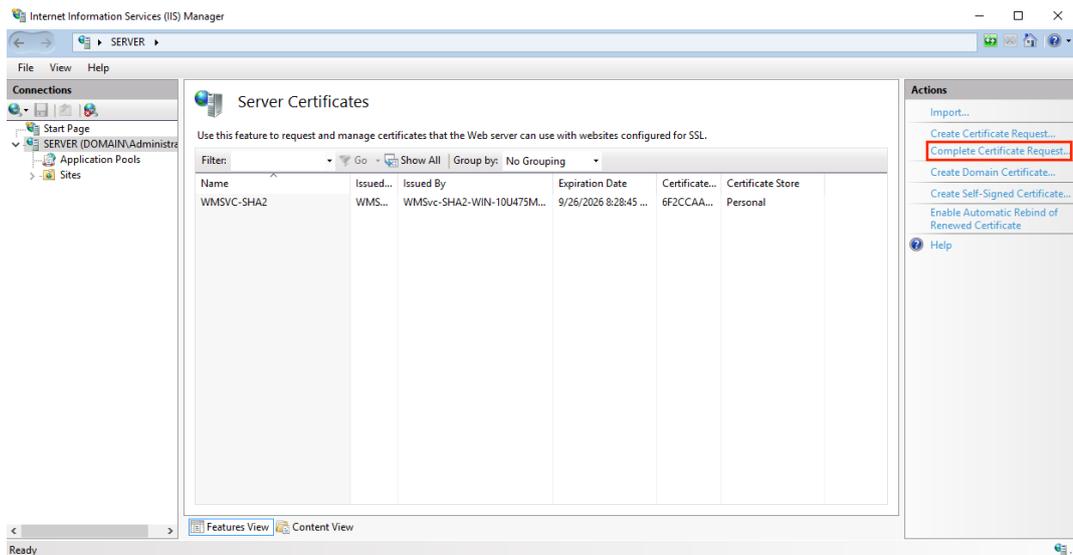
#### 安装 SSL 证书

1. 在创建 CSR 的服务器上，保存 SSL 证书。DigiCert 发送给您的 cer 文件（例如，*your\_domain\_com.cer*）。
2. 在 **Windows** 开始菜单中，键入 **Internet 信息服务 (IIS) 管理器** 并将其打开。
3. 在 **Internet 信息服务 (IIS) 管理器** 的“连接”菜单（左窗格）中，找到并单击服务器名称。



4.在服务器名称主页（中心窗格）的 IIS 部分中，双击“服务器证书”。

5.在“服务器证书”页面（中心窗格）的“操作”菜单（右窗格）中，单击“完成证书申请...”链接。



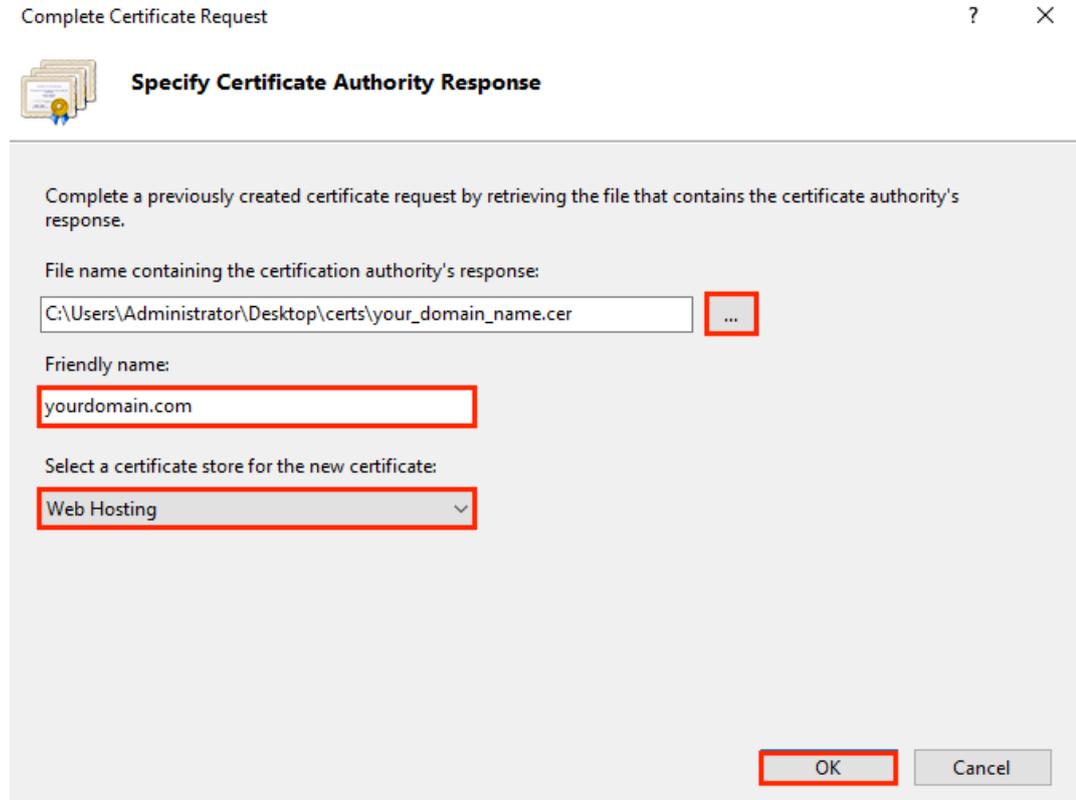
6.在“完成证书申请”向导的“指定证书颁发机构响应”页上，执行以下操作，然后单击“确定”：

文件名包含证书颁发机构的回复：单击...框并浏览并选择.cer 文件  
（比如：your\_domain\_com.cer）DigiCert 提供的

友好名称：键入证书的友好名称  
友好名称不是证书的一部分；相反，它用于识别证书。  
我们建议您将 DigiCert 和截止日期添加到友好名称的末尾，例如：yoursite-digicert -（截止日期）。

此信息有助于识别每个证书的颁发者和到期日期。它还有助于区分具有相同域名的多个证书。

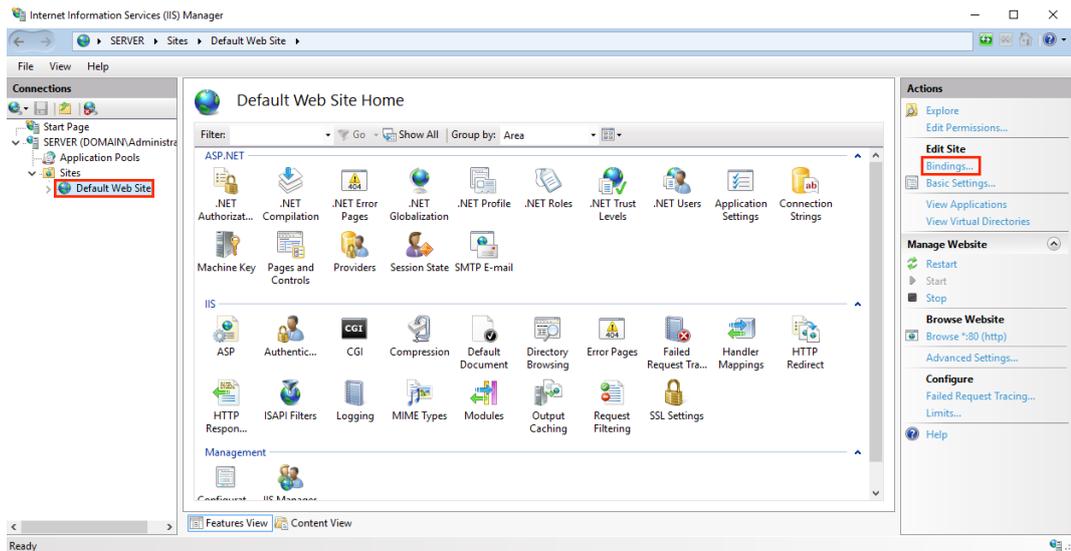
**选择证书库对于新证书:** 在下拉列表中, 选择“**虚拟主机**”。



7.现在您已成功安装 SSL 证书, 您需要将证书分配给相应的站点。

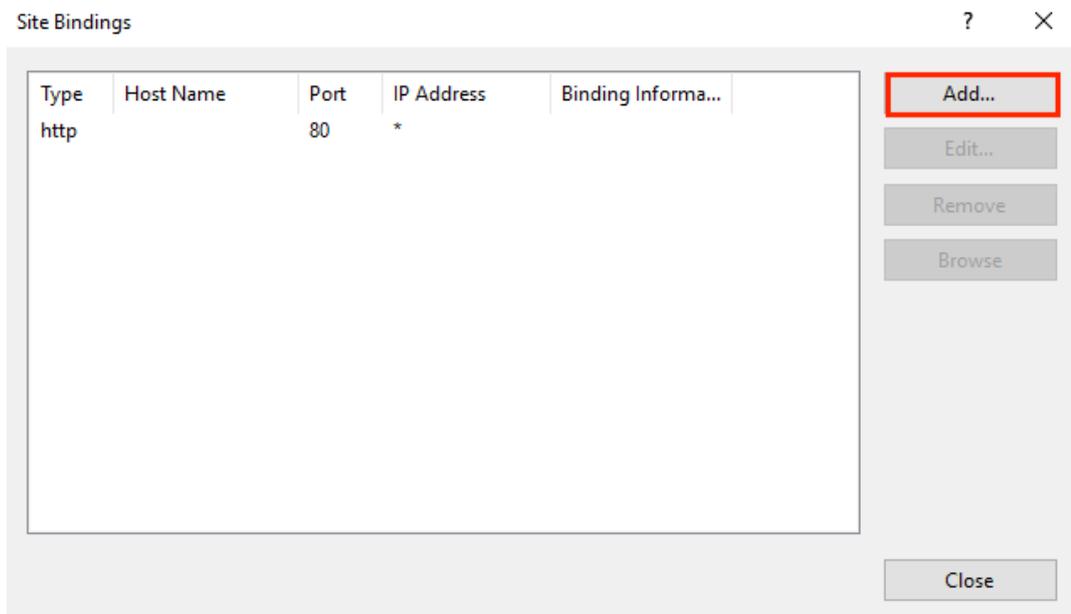
## 分配 SSL 证书

8. 在 **Internet 信息服务 (IIS) 管理器** 的“**连接**”菜单 (左窗格) 中, 展开安装证书的服务器的名称。然后展开“**站点**”, 然后单击要使用 SSL 证书进行保护的站点。



9. 在网站主页上的“操作”菜单（右侧窗格）中的“编辑网站”下，单击“绑定...”链接。

10. 在“站点绑定”窗口中，单击“添加”。



11. 在“添加网站绑定”窗口中，执行以下操作，然后单击“确定”：

**类型：** 在下拉列表中，选择 **https**。

**IP 地址：** 在下拉列表中，选择站点的 IP 地址或选择“全部未分配”。

**端口：** 输入端口 443。通过 SSL 保护流量的端口是端口 443

**SSL 证书：** 在下拉列表中，选择新的 SSL 证书（例如，*yourdomain.com*）。

Add Site Binding

Type: **https** IP address: **All Unassigned** Port: **443**

Host name:

Require Server Name Indication

SSL certificate:  
**yourdomain.com** Select... View...

OK Cancel

12. 您的 SSL 证书现已安装，并且网站已配置为接受安全连接。

Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
<b>https</b>		<b>443</b>	<b>*</b>	

Add... Edit... Remove Browse

Close

# (多个证书) 如何安装 SSL 证书并配置服务器以使用 SNI 使用它们

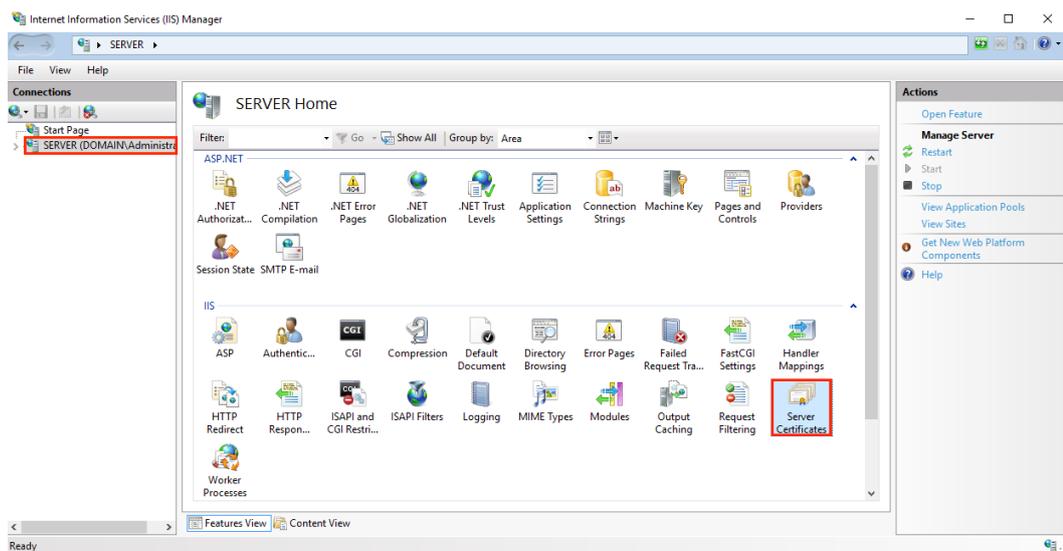
该指令说明了如何安装多个 SSL 证书并使用 SNI 进行分配。该过程分为以下两部分：

- [安装和配置您的第一个 SSL 证书](#)
- [安装和配置所有其他证书](#)

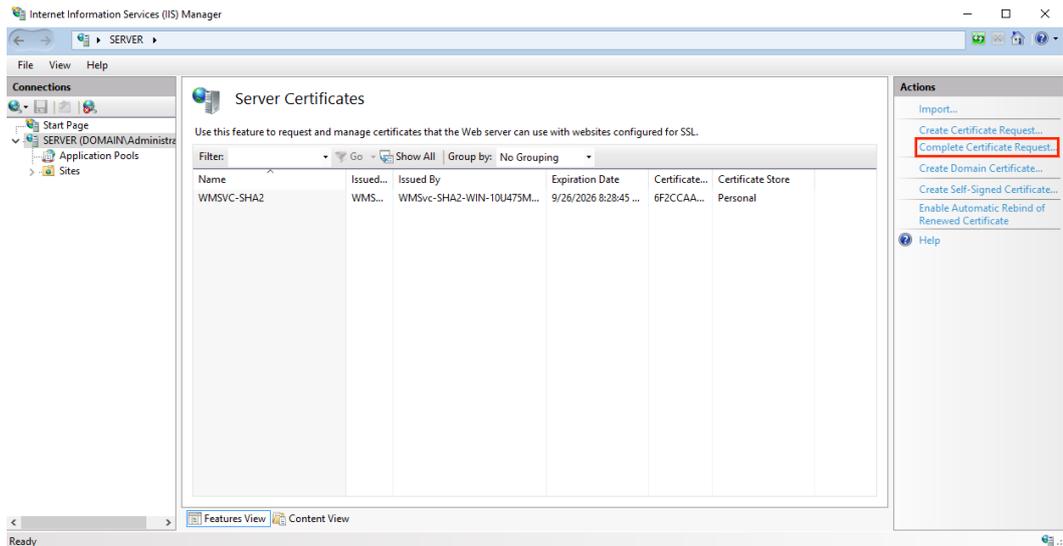
## 安装第一个 SSL 证书

对于第一个 SSL 证书，仅执行一次第一组指令。

1. 在创建 CSR 的服务器上，保存 SSL 证书。DigiCert 发送给您的.cer 文件（例如，`your_domain_com.cer`）。
2. 在 **Windows** 开始菜单中，键入 **Internet 信息服务 (IIS) 管理器** 并将其打开。
3. 在 **Internet 信息服务 (IIS) 管理器** 的“连接”菜单树（左窗格）中，找到并单击服务器名称



4. 在服务器名称主页（中心窗格）的 **IIS** 部分中，双击“**服务器证书**”。
5. 在“服务器证书”页面（中心面板）的“操作”菜单（右窗格）中，单击“完成证书申请...”链接。



6. 在“完成证书申请”向导的“指定证书颁发机构响应”页上，执行以下操作，然后单击“确定”：

**文件名包含证书颁发机构的回复：** 单击... 框并浏览并选择.cer 文件（例如，your\_domain\_com.cer）DigiCert 发送给您。

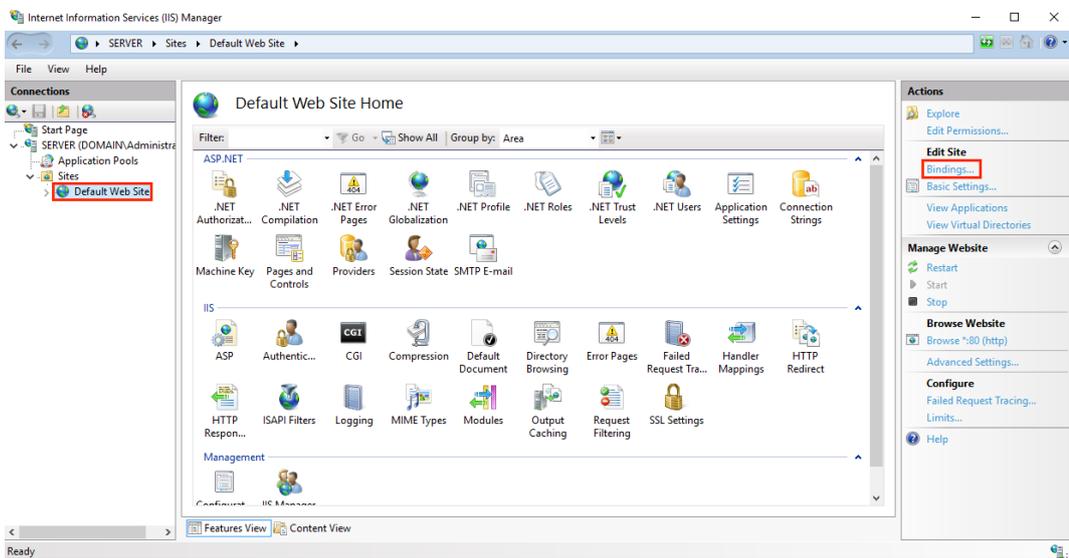
**友好名称：** 键入证书的友好名称。  
友好名称不是证书的一部分；相反，它用于识别证书。  
我们建议您将 DigiCert 和截止日期添加到友好名称的末尾，例如：yoursite-digicert - （截止日期）  
此信息有助于识别每个证书的颁发者和到期日期。它还有助于区分具有相同域名的多个证书。

**为新证书选择证书存储区：** 在下拉列表中，选择“虚拟主机”。



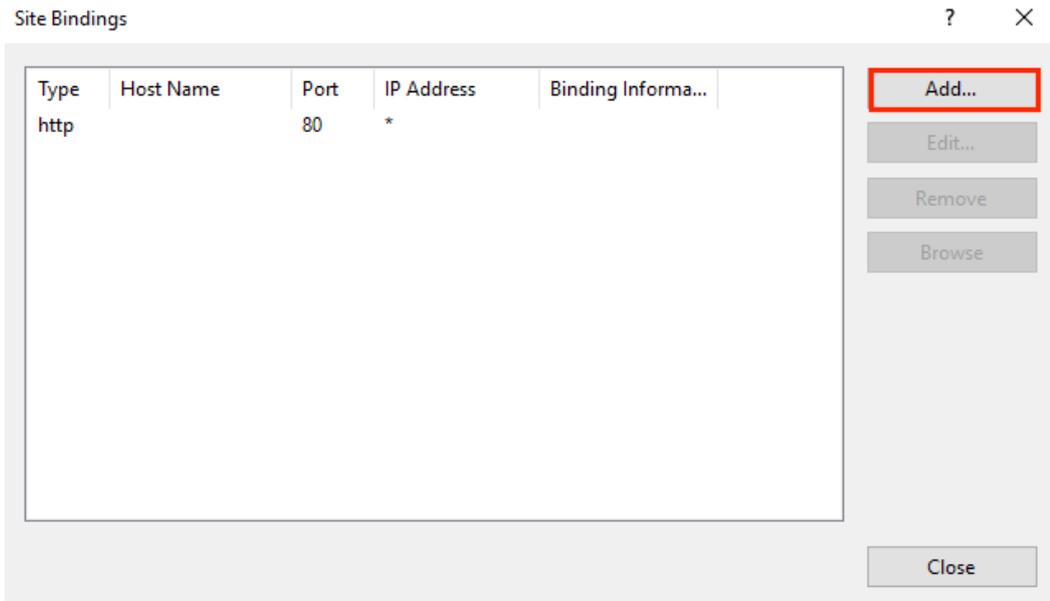
7. 现在您已成功安装 SSL 证书，您需要将证书分配给相应的站点。

8. 在 **Internet 信息服务 (IIS) 管理器** 的“连接”菜单树（左窗格）中，展开安装证书的服务器的名称。然后展开“站点”，然后单击要使用 SSL 证书进行保护的站点。



9. 在网站主页上的“操作”菜单（右侧窗格）中的“编辑网站”下，单击“绑定...”链接。

10. 在“站点绑定”窗口中，单击“添加”。



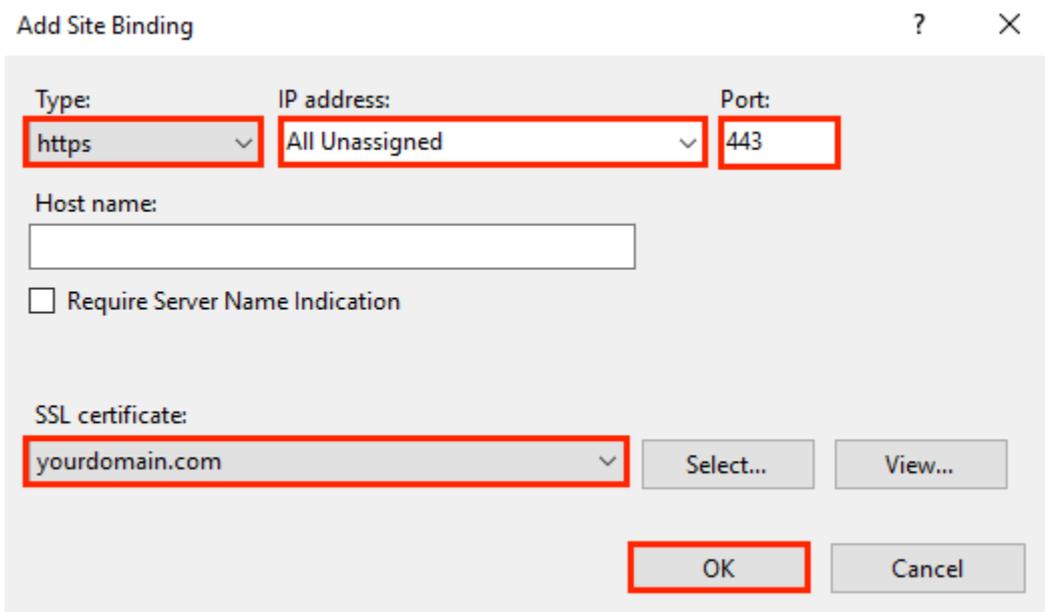
11. 在“添加网站绑定”窗口中，执行以下操作，然后单击“确定”：

**类型：** 在下拉列表中，选择 **https** 。

**IP 地址：** 在下拉列表中，选择站点的 IP 地址或选择“全部未分配”。

**端口：** 输入端口 **443**。通过 SSL 保护流量的端口是端口 443。

**SSL 证书：** 在下拉列表中，选择新的 SSL 证书（例如，*yourdomain.com*）。

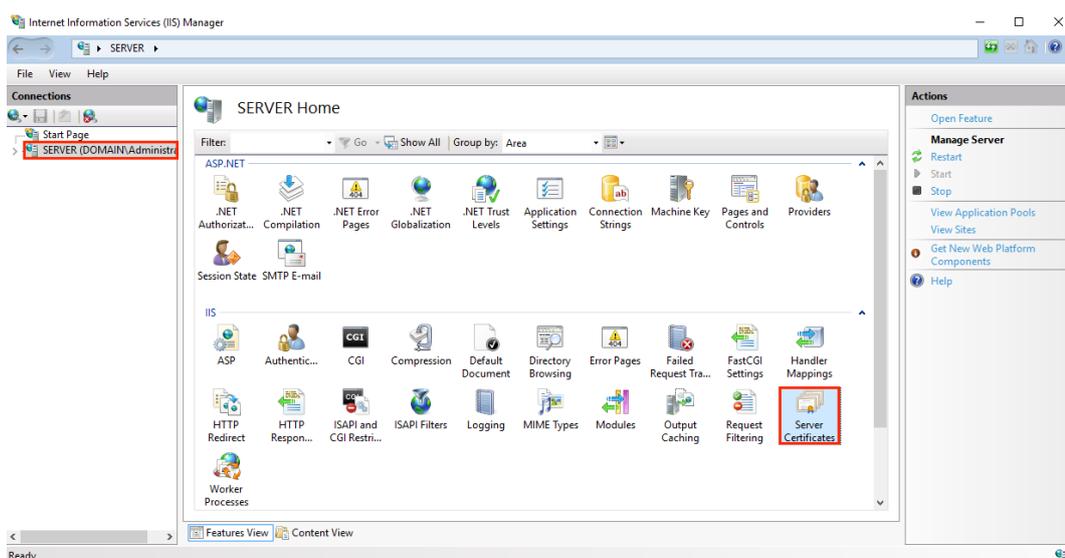


12. 您的第一个 SSL 证书现已安装，并且该网站已配置为接受安全连接。

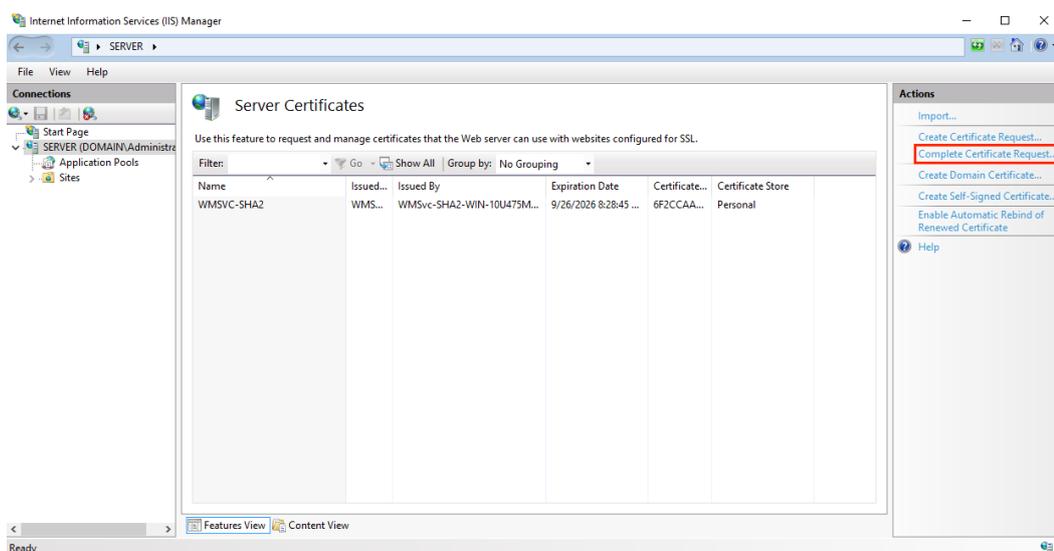
## 安装其他 SSL 证书

要安装和分配每个其他 SSL 证书，请根据需要重复以下步骤。

1. 在创建 CSR 的服务器上，保存 SSL 证书。DigiCert 发送给您的 cer 文件（例如，*your\_domain\_com.cer*）。
2. 在 **Windows** 开始菜单中，键入 **Internet 信息服务 (IIS) 管理器** 并将其打开。
3. 在 **Internet 信息服务 (IIS) 管理器** 的“连接”菜单树（左窗格）中，找到并单击服务器名称。



4. 在服务器名称主页（中心窗格）的 **IIS** 部分中，双击“服务器证书”。在服务器名称主页（中心窗格）的 **IIS** 部分中，双击“服务器证书”。
5. 在“服务器证书”页面（中心窗格）的“操作”菜单（右窗格）中，单击“完成证书申请...”链接。

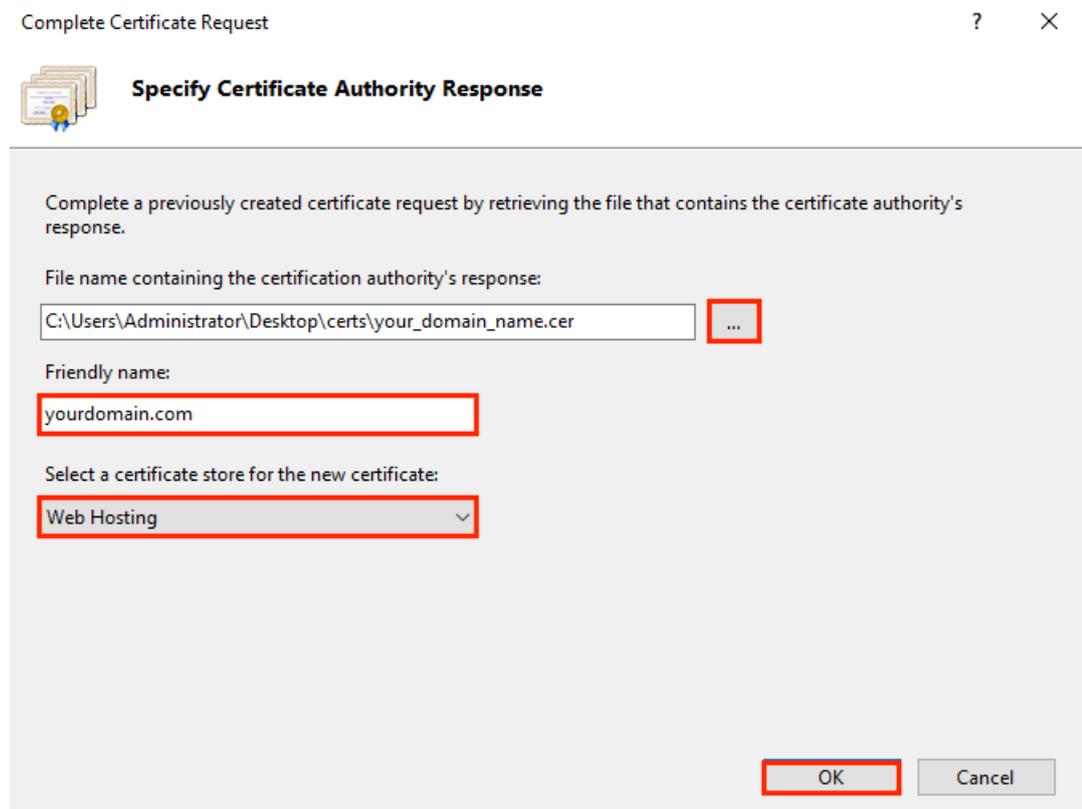


6. 在“完成证书申请”向导的“指定证书颁发机构响应”页上，执行以下操作，然后单击“确定”：

**文件名包含证书颁发机构的回复：** 单击...框并浏览并选择.cer 文件（例如，your\_domain\_com.cer）DigiCert 发送给您。

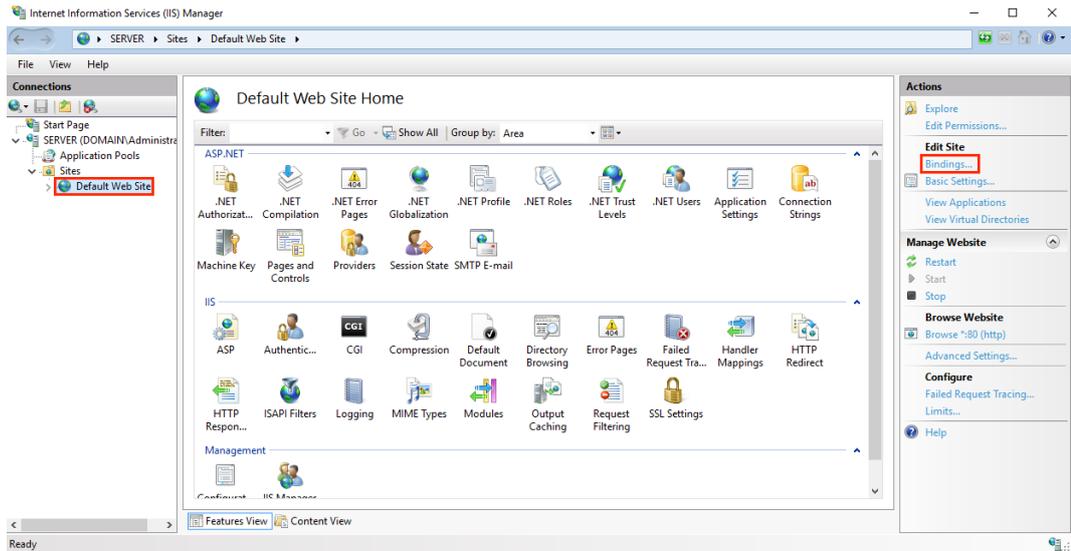
**友好名称：** 键入证书的友好名称。  
友好名称不是证书的一部分；相反，它用于识别证书。我们建议您将 DigiCert 和截止日期添加到友好名称的末尾，例如：yoursite-digicert -（截止日期）。  
此信息有助于识别每个证书的颁发者和到期日期。它还有助于区分具有相同域名的多个证书。

**为新证书选择证书存储：** 在下拉列表中，选择“虚拟主机”



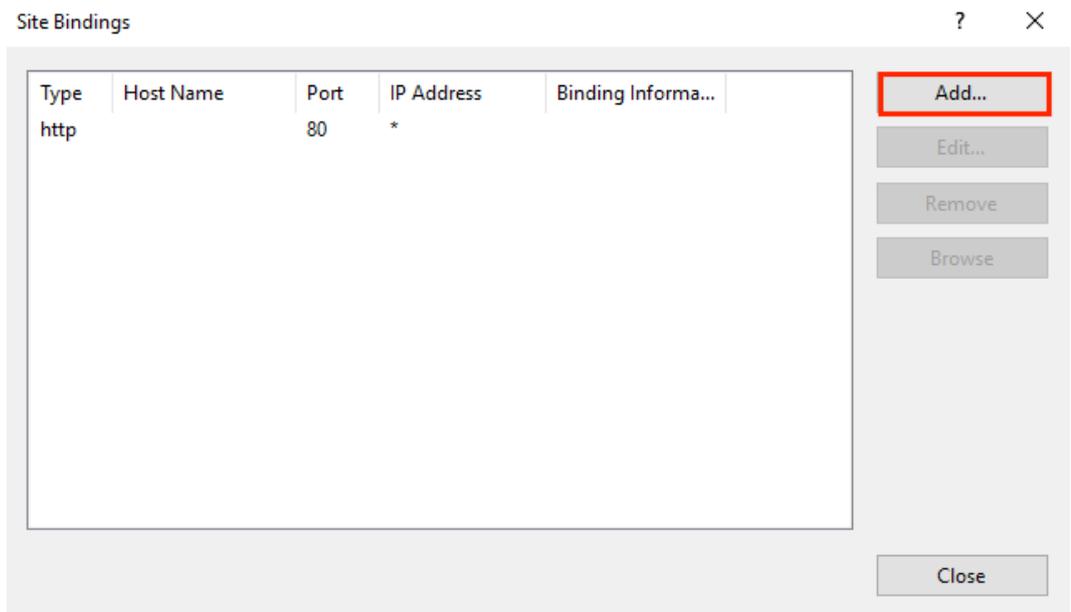
7. 现在您已成功安装 SSL 证书，您需要将证书分配给相应的站点。

8. 在 **Internet 信息服务 (IIS) 管理器** 的“连接”菜单树（左窗格）中，展开安装证书的服务器的名称。然后展开“站点”，然后单击要使用 SSL 证书进行保护的站点。



9.在网站主页上的“操作”菜单（右侧窗格）中的“编辑网站”下，单击“绑定...”链接。

10. 在“站点绑定”窗口中，单击“添加”。



11.在“添加网站绑定”窗口中，执行以下操作，然后单击“确定”：

**类型：** 在下拉列表中，选择 **https**。

**IP 地址：** 在下拉列表中，选择站点的 IP 地址或选择“全部未分配”。

**端口：** 输入端口 **443**。通过 SSL 保护流量的端口是端口 443。

**主机名：** 输入要保护的主机名。

输入主机名后，选中此框。

**需要服务器名称指示：** 在安装第一个证书并保护主站点之后，所有其他证书/站点都需要这样做。

**SSL 证书:** 在下拉列表中, 选择其他 SSL 证书 (例如, *yourdomain2.com*) 。

The screenshot shows the 'Add Site Binding' dialog box with the following configuration:

Type:	IP address:	Port:
https	All Unassigned	443

Host name: yourdomain2.com

Require Server Name Indication

SSL certificate: yourdomain2.com

Buttons: Select..., View..., OK, Cancel

12. 您已成功安装了另一个 SSL 证书, 并将网站配置为接受安全连接。

## 测试安装

如果您的网站可公开访问, [DigiCert@SSL 安装诊断工具](#)可以帮助您诊断常见问题。