

SSL Certificate – IIS10

Installation Guide



IIS 10: Create CSR and Install SSL Certificate

Creating a CSR and installing your SSL certificate on your Windows server 2016



Use the instructions on this page to use IIS 10 to create your certificate signing request (CSR) and then to install your SSL certificate on your Windows server 2016.

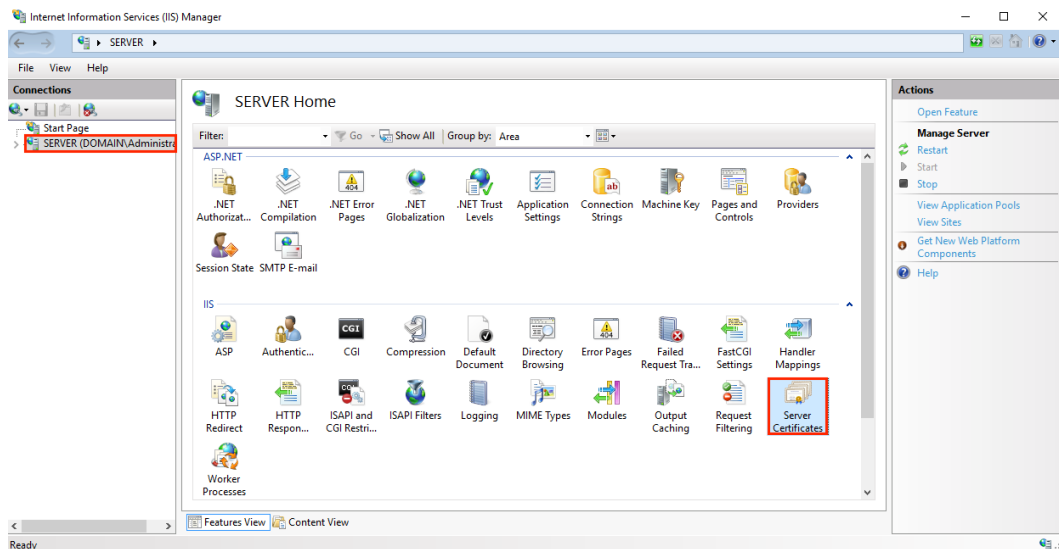
1. To create your certificate signing request (CSR), see [IIS 10: How to Create Your CSR on Windows Server 2016](#).
2. To install your SSL certificate, see [IIS 10: How to Install and Configure Your SSL Certificate on Windows Server 2016](#).

If you are looking for a simpler way to create CSRs, and install and manage your SSL Certificates, we recommend using the DigiCert® Certificate Utility for Windows. You can use the DigiCert Utility to generate your CSR and install your SSL certificate. See [Windows Server 2016: Create CSR & Install SSL Certificate with DigiCert Utility](#).

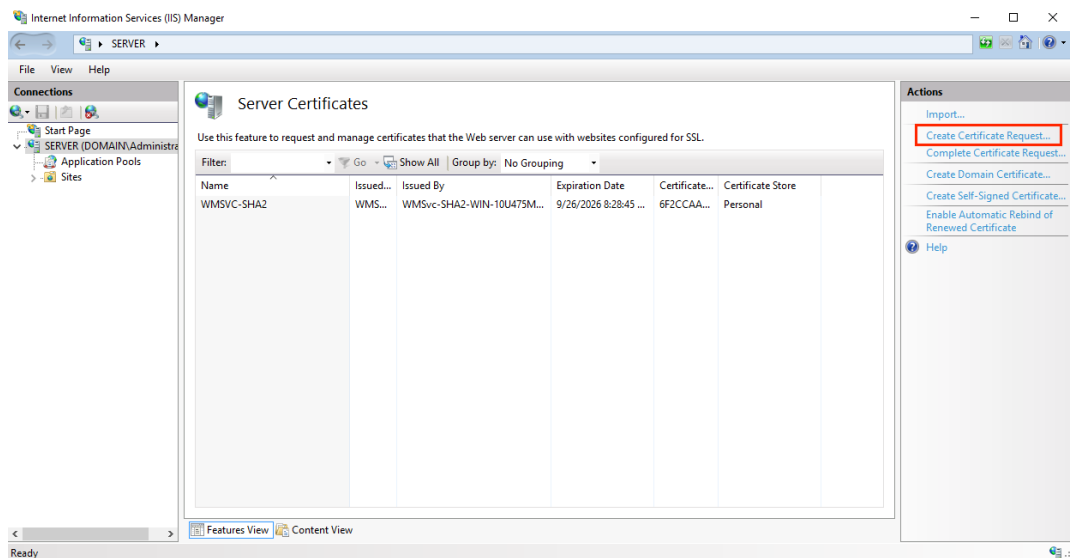
1. IIS 10: How to Create Your CSR on Windows Server 2016

Using IIS 10 to Create Your CSR

1. In the **Windows** start menu, type **Internet Information Services (IIS) Manager** and open it.
2. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), locate and click the server name.



3. On the server name **Home** page (center pane), in the **IIS** section, double-click **Server Certificates**.
4. On the **Server Certificates** page (center pane), in the **Actions** menu (right pane), click the **Create Certificate Request...** link.



5. In the **Request Certificate** wizard, on the **Distinguished Name Properties** page, provide the information specified below and then click **Next**:

Common name: Type the fully-qualified domain name (FQDN) (e.g., *www.example.com*).

Organization: Type your company's legally registered name (e.g., *YourCompany, Inc.*).


Organizational unit: The name of your department within the organization. Frequently this entry will be listed as "IT", "Web Security," or is simply left blank.

City/locality: Type the city where your company is legally located.

State/province: Type the state/province where your company is legally located.

Country: In the drop-down list, select the country where your company is legally located.

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. On the **Cryptographic Service Provider Properties** page, provide the information below and then click **Next**.

Cryptographic service provider: In the drop-down list, select **Microsoft RSA SChannel Cryptographic Provider**, unless you have a specific cryptographic provider.

Bit length: In the drop-down list select **2048**, unless you have a specific reason for opting for larger bit length.

**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. On the **File Name** page, under **Specify a file name for the certificate request**, click the ... box to browse to a location where you want to save your CSR.

Note: Remember the filename that you choose and the location to which you save your csr.txt file. If you just enter a filename without browsing to a location, your CSR will end up in C:\Windows\System32.

**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. When you are done, click **Finish**.

9. Use a text editor (such as Notepad) to open the file. Then, copy the text, including the **-----BEGIN NEW CERTIFICATE REQUEST-----** and **-----END NEW CERTIFICATE REQUEST-----** tags, and paste it into the DigiCert order form.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICvDCCAAQCAQAwdzELMAkGA1UEBhMCVVMxEjAQBgNVBAgTCVlvdXJldGF0ZTER
MA8GA1UEBxMIWW91ckNpdHkxCzAJBgNVBAsTAk1UMRowGAYDVQQKExFZb3VyQ29t
cGFueSwgSW5jLjEYMBYGA1UEAxMPd3d3LmV4YW1wbGUuY29tMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA379BFFxfACdXsUk2wrQka/nAlKbo+I9DAW32
+/SRxj/KtXVddscKW1obHGpMKPw4meJqOpQwJkIChYjSUQSpPKzdGpccDMf/eoF0
J7EaQ2szLv9AqdRQw2Aaek8SmocVmd3LxEOX4VvALBOMLHVrB5/vhYfGECLJbc3l
RdEbdXyHdTHk1RAoIVQCfjTwBWGNAD337vmHW7Q0R6FYUoa4fcJh7Rv6jHSyqwqx
7pVfaDbZPuTgUhw7wksKNFxccG0xcTmr/+GrciHEuZ0chq86CBP9RIyLpp2+RMSf
m6rMEYm9o65j7vEYaKEJU0JtA5MIz/ZjaXfS1LjXurLU0nCOQQIDAQABAAAwDQYJ
KoZIHvcNAQEFAAQADggEBAK159goyAYOpcnrQ2EvCGlizrK1kS3D8JjnAiP1NhrjB
/qdTYR+/8Dr/hMcwU5ThGAVf68eMkk6tUNwAdpZ9C904Js2z+ENEbO8GA0Fc4rw
ix7vb15vSXe3shGijRGIzzHVGRoR3r7xQtIuMaDAr3xlV8jHbcvZTcpx0Kbq6H1G
NLA4CXsOI4KGWu4FXfSzJEGb3gEJD8HaMP8V8er5G0owv/g/9Z/1/b0g97kAcUwk
M2eDsvPhMx/pENGbnLPe4XMy7NPiEdzfNaYtUy2BDcXj3ZQEWxRWk1ERgg9/YcWI
obf5ziuNm1Df24NBt5tpCNzfGvIKT6/RyfWg3dMaKxc=
-----END NEW CERTIFICATE REQUEST-----
```

Ready to order your SSL certificate

10. After you receive your SSL certificate from DigiCert, you can install it.

2. IIS 10: How to Install and Configure Your SSL Certificate on Windows Server 2016

If you have not yet created a CSR and ordered your certificate, see [IIS 10: How to Create Your CSR Windows Server 2016](#).

After we validate and issue your SSL certificate, you need to install it on the Windows 2016 server where the CSR was generated. Then, you need to configure the server to use it.

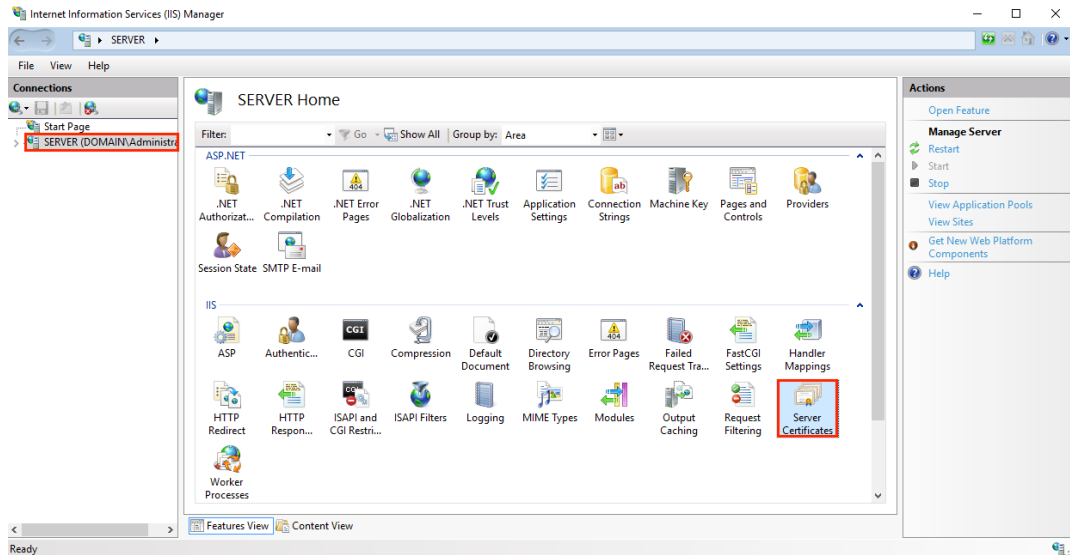
- [\(Single Certificate\) How to install and configure your SSL certificate](#)
- [\(Multiple Certificates\) How to install and configure your SSL certificates using SNI](#)

(Single Certificate) How to install your SSL certificate and configure the server to use it

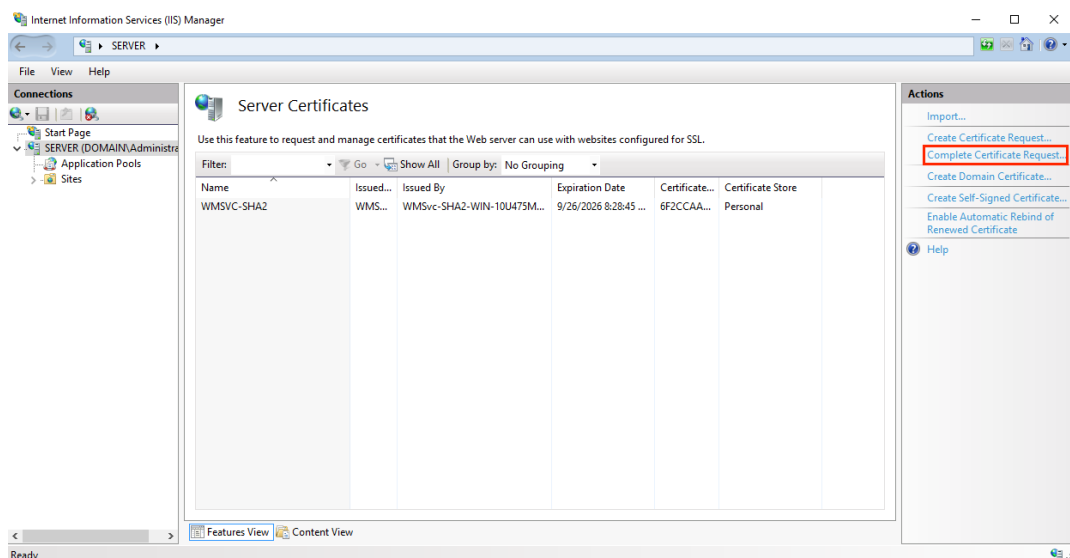
Install SSL Certificate

1. On the server where you created the CSR, save the SSL certificate .cer file (e.g., *your_domain_com.cer*) that DigiCert sent to you.

2. In the **Windows** start menu, type **Internet Information Services (IIS) Manager** and open it.
3. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), locate and click the server name.



4. On the server name **Home** page (center pane), in the **IIS** section, double-click **Server Certificates**.
5. On the **Server Certificates** page (center pane), in the **Actions** menu (right pane), click the **Complete Certificate Request...** link.



6. In the **Complete Certificate Request** wizard, on the **Specify Certificate Authority Response** page, do the following and then click **OK**:

File name
containing the

Click the **...** box and browse to and select the **.cer** file

**certificate
authority's
response:**

(e.g., *your_domain_com.cer*) that DigiCert sent to you.


Friendly name:

Type a friendly name for the certificate.
The friendly name is not part of the certificate; instead, it is used to identify the certificate.
We recommend that you add DigiCert and the expiration date to the end of your friendly name, for example: yoursite-digicert-(expiration date).
This information helps identify the issuer and expiration date for each certificate. It also helps distinguish multiple certificates with the same domain name.

**Select a certificate
store
for the new
certificate:**


In the drop-down list, select **Web Hosting**.

Complete Certificate Request ? X

 **Specify Certificate Authority Response**

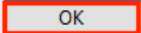
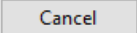
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:



Friendly name:

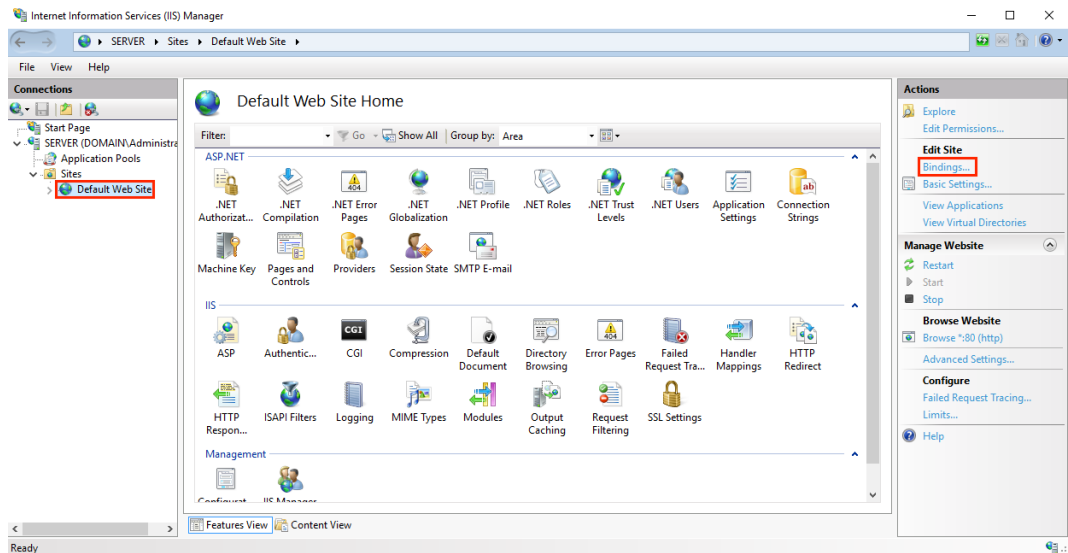
Select a certificate store for the new certificate:

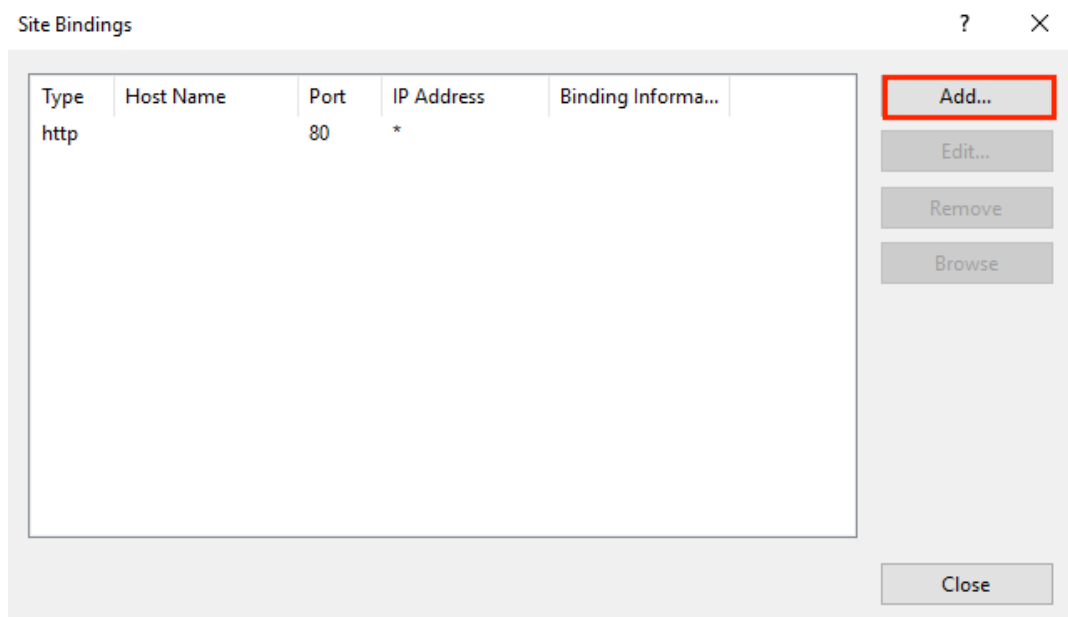
- Now that you've successfully installed your SSL certificate, you need to assign the certificate to the appropriate site.

Assign SSL Certificate

- In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), expand the name of the server on which the certificate was installed. Then expand **Sites** and click the site you want to use the SSL certificate to secure.



9. On the website **Home** page, in the **Actions** menu (right pane), under **Edit Site**, click the **Bindings...** link.
10. In the **Site Bindings** window, click **Add**.



11. In the **Add Site Bindings** window, do the following and then click **OK**:
 - Type:** In the drop-down list, select **https**.
 - IP address:** In the drop-down list, select the IP address of the site or select **All Unassigned**.
 - Port:** Type port **443**. The port over which traffic is secure by SSL is port 443.
 - SSL certificate:** In the drop-down list, select your new SSL certificate (e.g., *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. Your SSL certificate is now installed, and the website configured to accept secure connections.

Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	*	

Add... **Edit...** **Remove** **Browse**

Close

(Multiple Certificates) How to install your SSL certificates and configure the server to use them using SNI

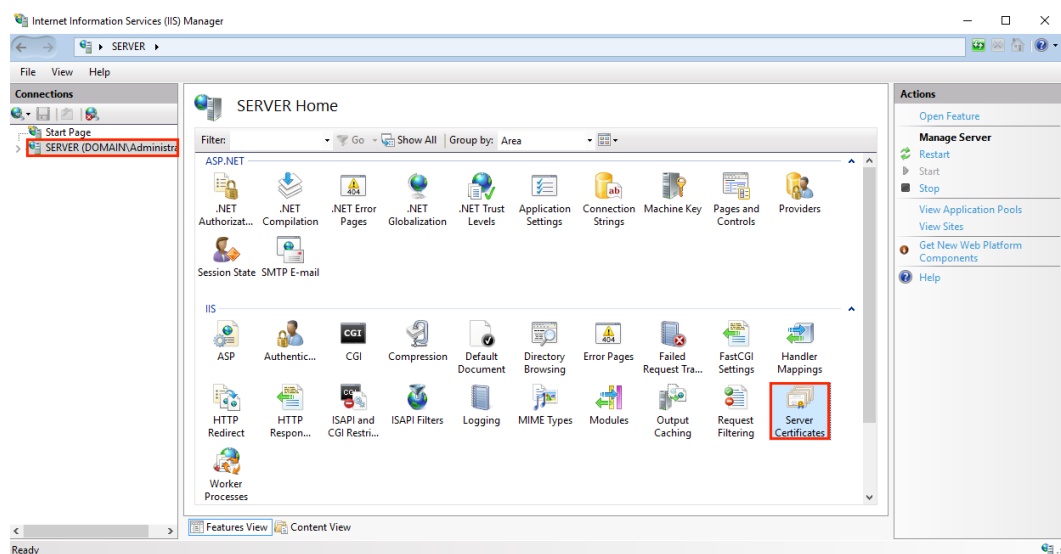
This instruction explains how to install multiple SSL certificates and assign them using SNI. The process is split into two parts as follows:

- [Installing and Configuring Your First SSL Certificate](#)
- [Installing and Configuring All Additional Certificates](#)

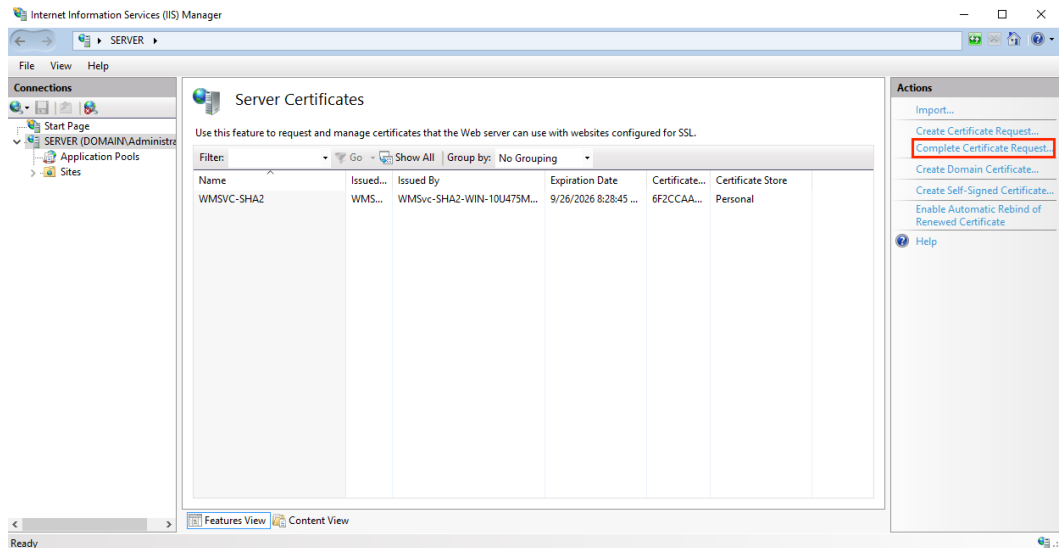
Install First SSL Certificate

Do this first set of instructions only once, for the first SSL certificate.

1. On the server where you created the CSR, save the SSL certificate .cer file (e.g., *your_domain_com.cer*) that DigiCert sent to you.
2. In the **Windows** start menu, type **Internet Information Services (IIS) Manager** and open it.
3. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), locate and click the server name.



4. On the server name **Home** page (center pane), in the **IIS** section, double-click **Server Certificates**.
5. On the **Server Certificates** page (center pane), in the **Actions** menu (right pane), click the **Complete Certificate Request...** link.



6. In the **Complete Certificate Request** wizard, on the **Specify Certificate Authority Response** page, do the following and then click **OK**:

File name containing the certificate authority's response:

Click the ... box and browse to and select the .cer file
(e.g., *your_domain_com.cer*) that DigiCert sent to you.

Friendly name:

Type a friendly name for the certificate.
The friendly name is not part of the certificate; instead, it is used to identify the certificate.
We recommend that you add DigiCert and the expiration date to the end of your friendly name, for example: *yoursite-digicert-(expiration date)*.
This information helps identify the issuer and expiration date for each certificate. It also helps distinguish multiple certificates with the same domain name.

Select a certificate store for the new certificate:

In the drop-down list, select **Web Hosting**.



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

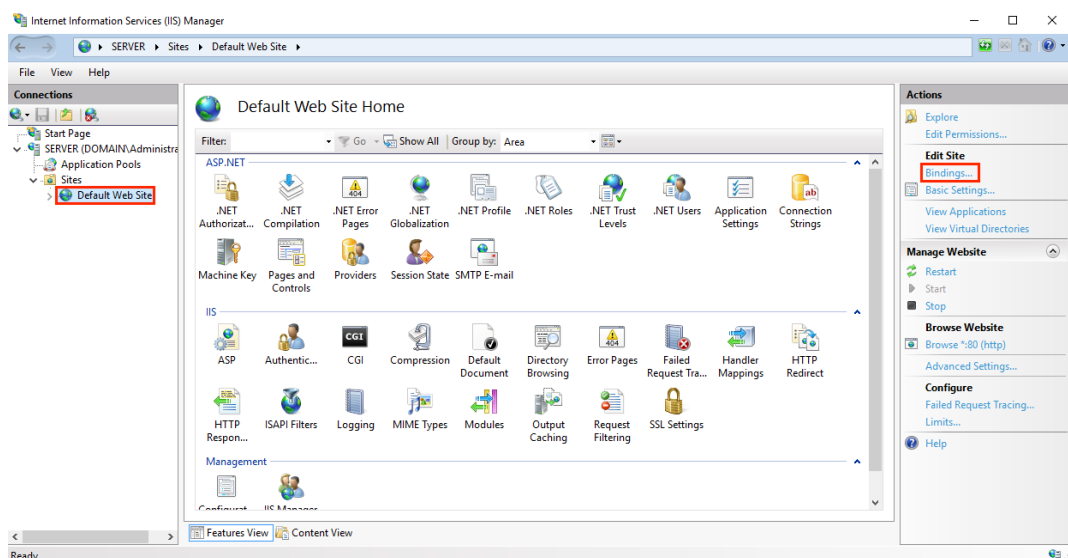
Select a certificate store for the new certificate:

Web Hosting

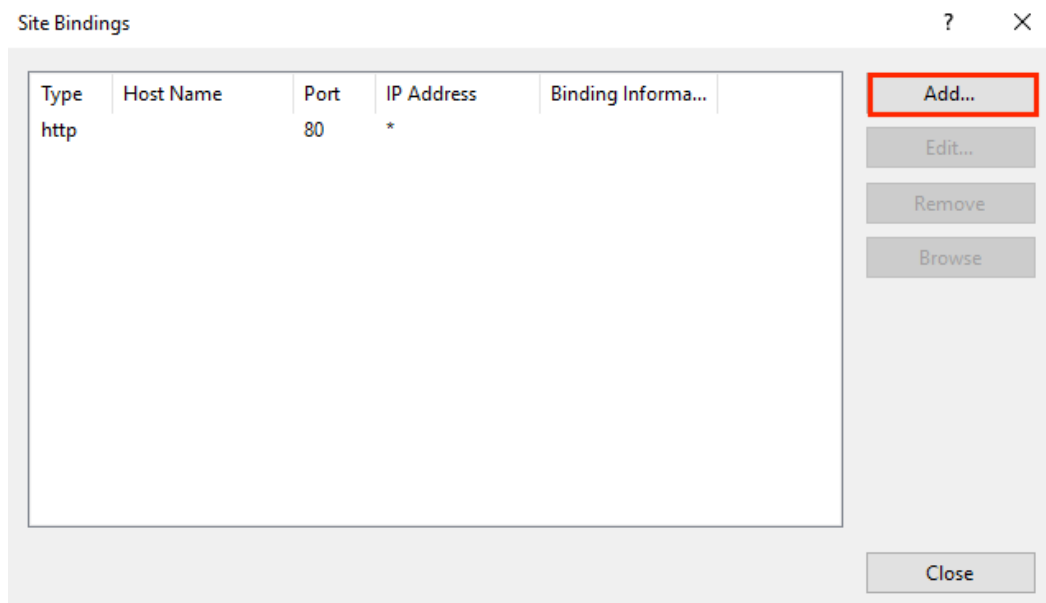
OK

Cancel

7. Now that you've successfully installed your SSL certificate, you need to assign the certificate to the appropriate site.
8. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), expand the name of the server on which the certificate was installed. Then expand **Sites** and click the site you want to use the SSL certificate to secure.



9. On the website **Home** page, in the **Actions** menu (right pane), under **Edit Site**, click the **Bindings...** link.
10. In the **Site Bindings** window, click **Add**.



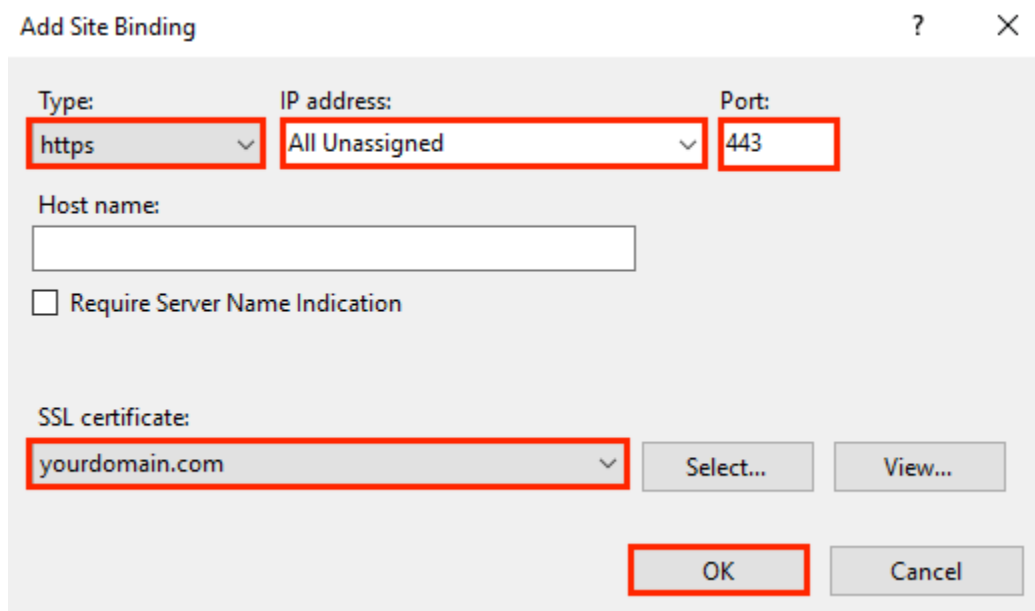
11. In the **Add Site Bindings** window, do the following and then click **OK**:

Type: In the drop-down list, select **https**.

IP address: In the drop-down list, select the IP address of the site or select **All Unassigned**.

Port: Type port **443**. The port over which traffic is secure by SSL is port 443.

SSL certificate: In the drop-down list, select your new SSL certificate (e.g., *yourdomain.com*).

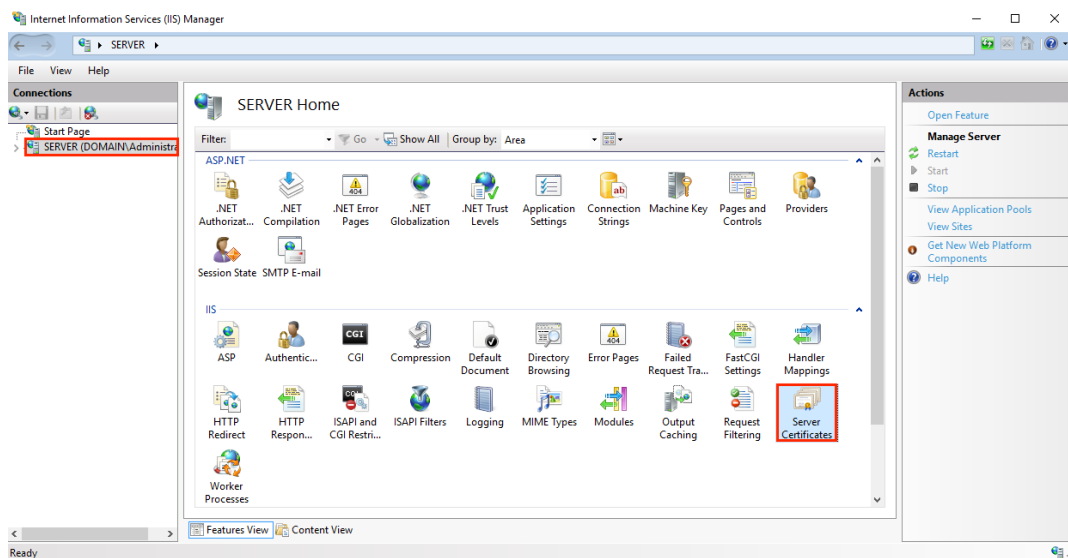


12. Your first SSL certificate is now installed, and the website configured to accept secure connections.

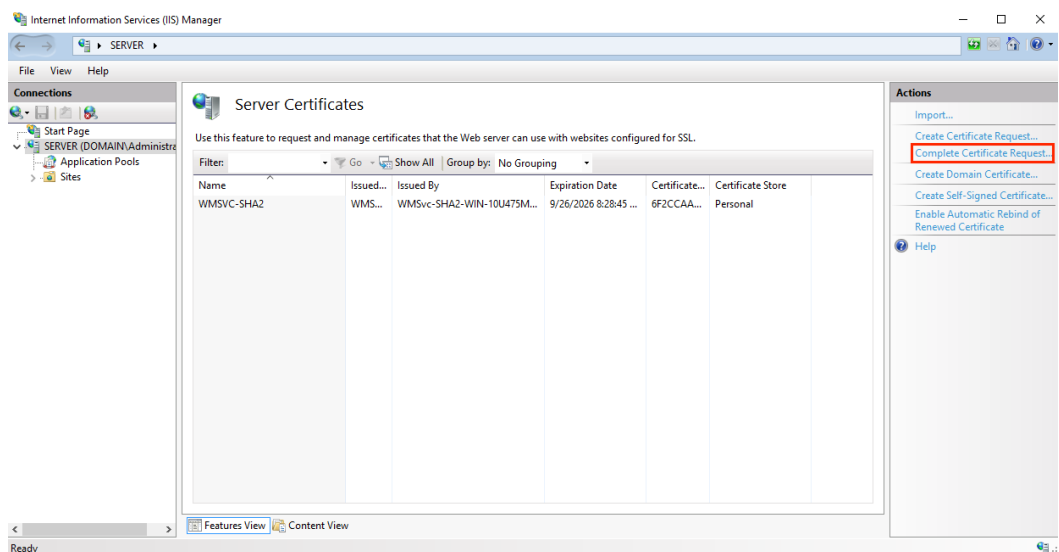
Install Additional SSL Certificates

To install and assign each additional SSL certificate, repeat the steps below, as needed.

1. On the server where you created the CSR, save the SSL certificate .cer file (e.g., *your_domain_com.cer*) that DigiCert sent to you.
2. In the **Windows** start menu, type **Internet Information Services (IIS) Manager** and open it.
3. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), locate and click the server name.



4. On the server name **Home** page (center pane), in the **IIS** section, double-click **Server Certificates**.
5. On the **Server Certificates** page (center pane), in the **Actions** menu (right pane), click the **Complete Certificate Request...** link.



6. In the **Complete Certificate Request** wizard, on the **Specify Certificate Authority Response** page, do the following and then click **OK**:

File name containing the certificate authority's response:

Click the ... box and browse to and select the .cer file
(e.g., *your_domain_com.cer*) that DigiCert sent to you.


Friendly name:

Type a friendly name for the certificate.
The friendly name is not part of the certificate; instead, it is used to identify the certificate.
We recommend that you add DigiCert and the expiration date to the end of your friendly name, for example: *yoursite-digicert-(expiration date)*.
This information helps identify the issuer and expiration date for each certificate. It also helps distinguish multiple certificates with the same domain name.

Select a certificate store for the new certificate:

In the drop-down list, select **Web Hosting**.

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:

...

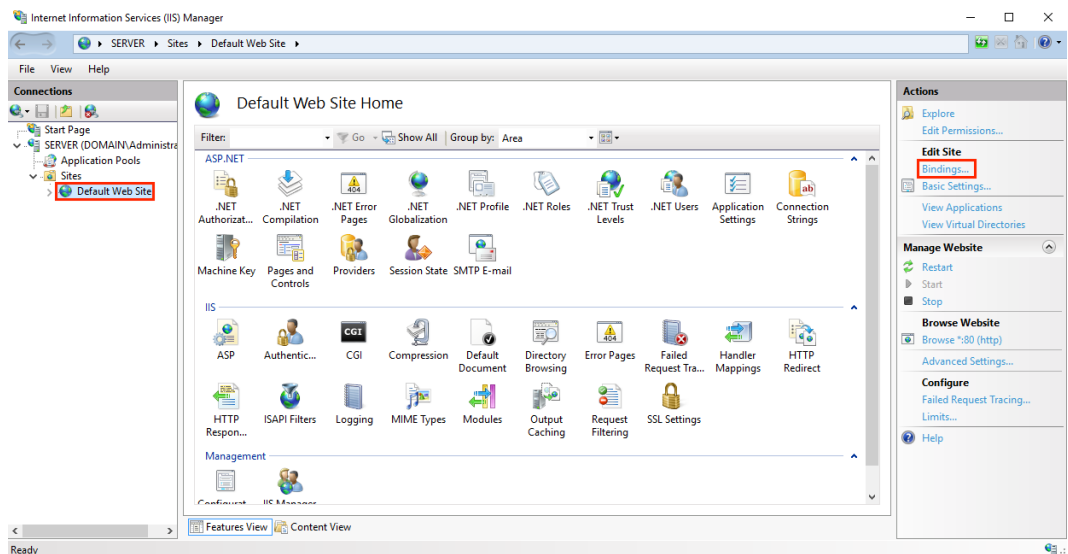
Friendly name:

Select a certificate store for the new certificate:

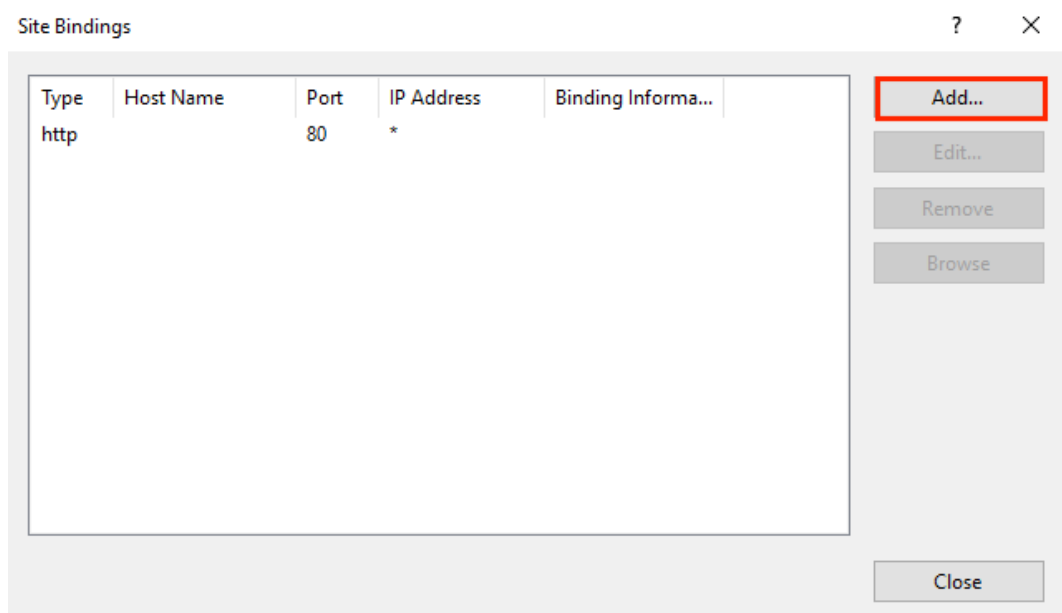
OK Cancel

7. Now that you've successfully installed your SSL certificate, you need to assign the certificate to the appropriate site.

8. In **Internet Information Services (IIS) Manager**, in the **Connections** menu tree (left pane), expand the name of the server on which the certificate was installed. Then expand **Sites** and click the site you want to use the SSL certificate to secure.



9. On the website **Home** page, in the **Actions** menu (right pane), under **Edit Site**, click the **Bindings...** link.
10. In the **Site Bindings** window, click **Add**.



11. In the **Add Site Bindings** window, do the following and then click **OK**:

Type: In the drop-down list, select **https**.

IP address: In the drop-down list, select the IP address of the site or select **All Unassigned**.

Port: Type port **443**. The port over which traffic is secure by SSL is port 443.

Host name: Type the host name that you want to secure.

Require Server After you enter the host name, check this box.

Name This is required for all additional certificates/sites, after you've installed the first certificate and secured the primary site.

SSL certificate: In the drop-down list, select an additional SSL certificate (e.g., *yourdomain2.com*).

Add Site Binding

Type: https IP address: All Unassigned Port: 443

Host name: yourdomain2.com

☒ Require Server Name Indication

SSL certificate: yourdomain2.com Select... View...

OK Cancel

12. You have successfully installed another SSL certificate and configured the website to accept secure connections.

Test Installation

If your website is publicly accessible, [DigiCert® SSL Installation Diagnostic Tool](#) can help you diagnose common problems.