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.

ie View Help Anections SERVER Home Start Age SERVER (DOMAINAdminister SERVER (DOMAINAdminister SERVER (DOMAINAdminister Asp. Net Asp. Net	🔛 🖂 🗄
Image: SERVER (DOMAINAdministe) Image: Server	
§ Sart Page • • • • • • • • • • • • • • • • • • •	Feature
ASP Authentic CGI Compression Default Directory Error Pages Failed FatCGI Handler HTTP HTTP ISAPI and ISAPI Filters Logging MIME Types Modules Output Request Reflected Response CGI Restrict	ige Server rt Application Pools Sites Jew Web Platform ponents
Worker	

- 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.

💐 Internet Information Services (IIS) I	Manager						- 🗆 ×
← → SERVER ►							📴 🛛 🟠 🔞 -
File View Help							
Connections	Server Certificat Use this feature to request and mark Filter:	tes mage cert Go - 🐙	ificates that the Web server can us Show All Group by: No Group	e with websites config ing •	ured for SSL.		Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate.
	Name WMSVC-SHA2	WMS	Issued By WMSvc-SHA2-WIN-10U475M	Expiration Date 9/26/2026 8:28:45	Certificate 6F2CCAA	Certricate Store Personal	Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate
< >>	🛐 Features View 🔀 Content View	/					9 <u>1</u>

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., <i>www.example.com</i>).
Organization:	Type your company's legally registered name (e.g., <i>YourCompany, Inc.</i>).
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 locate	ed.
State/province:	Type the state/province where your company is leg	ally located.
Country:	In the drop-down list, select the country where you legally located.	r company is
Request Certificate	?	×
Distinguishe	d Name Properties	

ommon name:	www.yourdomain.com
rganization:	Your Company, Inc.
rganizational unit:	П
ity/locality	Lehi
tate/province:	UT
ountry/region:	US v

Distinguished Name Properties

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

Cryntographic	In the d	rop-dowi	n list, select	Micro	osoft RS	A SCha	nnel
Ciyptographic	Crypto	graphic i	Provider,				
• • • •	1	1	• ••		1 •	• 1	

service provider: unless you have a specific cryptographic provider.

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

Request Certificate

Cryptographic Service Provider Properties	
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater length may decrease performance. Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider	the bit
Bit length:	
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.

Request Certificate		?	×
File Name			
Specify the file name for the certificate request. This information can be sent to a certification au signing.	thority for		
Specify a file name for the certificate request:			
C:\Users\Administrator\Desktop\csr.txt			
Previous Next Finish	C	ancel	

8. When you are done, click Finish.

 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.



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

 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.

← → SERVER ►												😈 🗟 😭 🔞
File View Help												
Connections 	Fiter ASP.NET ASP.NET NET Authorizat Co Session State SM	VER Hom	Go ← I Go ← I Aga .NET Error Pages	Show All	Revels	Application Settings	• E • Connection Strings	Machine Key	Pages and Controls	Providers	- • •	Actions Open Feature Manage Server Restart Stop View Application Pools View Sites Get New Web Platform Components Help
	IS ASP A HTTP Redirect	uthentic uthentic uthentic uthentic Respon	CGI CGI ISAPI and CGI Restri	Compression SAPI Filters	Default Document Logging	Directory Browsing	Error Pages	Failed Request Tra Uutput Caching	FastCGI Settings	Handler Mappings	•	
< >>	Features View	Content	View									•

- 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.

💐 Internet Information Services (IIS) N	Manager						- 🗆 ×
← → € + SERVER →							📴 🖂 🚱 🔹
File View Help							
File View Help Connections Start Page Start Page Application Pools Starts Start Star	Server Certifica Use this feature to request and m Filter:	tes anage cert Issued WMS	ificates that the Web server can us Show All Group by: No Group Issued By WMSvc-SHA2-WIN-10U475M	e with websites configu ing • Expiration Date 9/26/2026 8:28:45	rred for SSL. Certificate 6F2CCAA	Certificate Store Personal	Actions Import Create Certificate Request Create Domain Certificate Create Self-Signed Certificate Enable Automatic Rebind of Reneved Certificate Help
Ready							¶.:

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	

Select a cer inicate	In the drop down list select Web Hesting	
store	in the drop-down list, select web hosting.	
for the new		
certificate:		
Complete Certificate Request		?

 \times

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: 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.

Assign SSL Certificate

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.

← →	 Default We 	eb Site ►										🖬 🖂 🟠 🔞
File View Help												
Connections	Def Filter: ASP.NET .NET Authorizat Machine Key	INET Compilation Pages and Controls	• Site Ho • • Go • .NET Error Pages Providers	Show All	Group by: Ar	ea .NET Roles	• DD • .NET Trust Levels	.NET Users	Application Settings	Connection Strings	• •	Actions Actions Conservation Actions Actions
	ASP HTTP Respon Managemen	Authentic ISAPI Filters	CGI CGI Logging	Compression MIME Types	Default Document Modules	Directory Browsing Utput Caching	Error Pages	Failed Request Tra SSL Settings	Handler Mappings	HTTP Redirect	-	Browse Website Browse '*80 (http) Advanced Settings Configure Failed Request Tracing Limits Help

- 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.

Туре	Host Name	Port	IP Address	Binding Informa	Add
http		80	*		Edit
					Remove
					Browse
					Close

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., <i>yourdomain.com</i>).

		- C - C - C - C - C - C - C - C - C - C	D 1		
Δd	d	Site	 Bin 	d	ind
~~~		2110			

Type: https ~	IP address: All Unassigned		Port:	]
Host name:				
Require Server Nar	ne Indication			
SSL certificate:				
yourdomain.com		~	Select	View
			ОК	Cancel

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

Site Bindi	ngs				?	×
Type http	Host Name	Port 80	IP Address *	Binding Informa	Add	
https		443	*		Remove	
					biowse	
					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.

- 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.

💐 Internet Information Services (IIS) N	/lanager						- 🗆 ×
← → ♥ ► SERVER ►							😰 🖂 🟠 i 🔞 🗸
File View Help							
File View Help Connections Connections Start Page Start Page	Server Certifica Use this feature to request and m Filter.	tes Go - Issued WMS	ficates that the Web server can us (Show All Group by: No Group Issued By WMSvc-SHA2-WIN-10U475M	e with websites configu ing • Expiration Date 9/26/2026 8:28:45	ured for SSL. Certificate 6F2CCAA	Certificate Store Personal	Actions Import Create Certificate Request. Create Domain Certificate Request Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate Philp
< >>	🛅 Features View 牘 Content Vie	N					64

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., <i>your_domain_com.cer</i> ) 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 <b>Web Hosting</b> .

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.

×

?

e Bindir	ngs				? >
Туре	Host Name	Port	IP Address	Binding Informa	Add
http		80	*		Edit
					Remove
					Browse
					Class

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

Туре:	In the drop-down list, select <b>https</b> .
IP address:	In the drop-down list, select the IP address of the site or select <b>All Unassigned</b> .
Port:	Type port <i>443</i> . The port over which traffic is secure by SSL is port 443.
aa <b>.</b>	

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

Add Site Binding				?	×
Type: IP address: https v All Unassigned		Port: ~ 443	]		
Host name:					
Require Server Name Indication					
SSL certificate:					
yourdomain.com	$\sim$	Select	Vi	ew	
		ОК	C	ancel	
	_				

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.

- 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.

← → SERVER →												🕶 🚳 🟠 (
File View Help												
Connections           •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         •         <	SERV Filte: ASP.NET NET Authorizat C	VER Hom	• V Go • C	Show All ( .NET Globalization	Troup by: Ar	ea Application Settings	• = • Connection Strings	Machine Key	Pages and Controls	Providers	- • •	Actions Open Feature Manage Server Restart Start Stop View Application Pools View Sites Get New Web Platform Components Rep
		Authentic HTTP	CGI CGI	Compression	Default Document	Directory Browsing	Error Pages	Failed Request Tra Output	FastCGI Settings	Handler Mappings	•	
	Redirect Worker Processes	Respon	CGI Restri					Caching	Filtering	Certificates	¥	

- 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.

💐 Internet Information Services (IIS) N	Nanager						- 🗆 ×
← → ¶ → SERVER →							😐 🖂 🚱 •
File View Help							
Connections Connections Start Page Start Page Star	Server Certifica Use this feature to request and m Filter.	tes anage cert Issued WMS	ificates that the Web server can us Show All   Group by: No Group Issued By WMSvc-SHA2-WIN-10U475M	e with websites config ing Expiration Date 9/26/2026 8:28:45	ured for SSL. Certificate 6F2CCAA	Certificate Store Personal	Actions Import Create Certificate Request Create Demain Certificate Create Demain Certificate Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate Weip
Ready							• <u>1</u> .:

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	Click the box and browse to and select the .cer file								
authority's (e.g., <i>your_domain_com.cer</i> ) that DigiCert sent to you. response:									
Friendly name:	<ul><li>Type a friendly name for the certificate.</li><li>The friendly name is not part of the certificate; instead, it is used to identify the certificate.</li><li>We recommend that you add DigiCert and the expiration date to the end of your friendly name, for example: yoursite-digicert-(expiration date).</li><li>This information helps identify the issuer and expiration date for each certificate. It also helps distinguish multiple certificates with the same domain name.</li></ul>								
Select a certificate store for the new	In the drop-down list, select <b>Web</b> H	losting.							
for the new									
Complete Certificate Request		7 X							
complete certificate neques	•								
Specify Certi	ificate Authority Response								
Complete a previously cre response.	ated certificate request by retrieving the file that contair	is the certificate authority's							
File name containing the o	certification authority's response:								
C:\Users\Administrator\D	esktop\certs\your_domain_name.cer								
Friendly name:									
yourdomain.com									
Select a certificate store fo	r the new certificate								
Web Hosting									
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.

te Bindi	ngs				?
Туре	Host Name	Port	IP Address	Binding Informa	Add
http		80	*		Edit
					Remove
					Browse

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.

Require	After you enter the best name, sheek this box
Server	
Name Indication:	installed the first certificate and secured the primary site.

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

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

Add Site Binding				?	×
Type: https ∽	IP address: All Unassigned		Port:	]	
Host name:					
yourdomain2.com					
Require Server Nan	ne Indication				
SSL certificate:					
yourdomain2.com		~	Select	View	
		E	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, <u>DigiCert® SSL Installation Diagnostic Tool</u> can help you diagnose common problems.