

Generate PFX File in Windows Server:

	C				Actions	
Server	Certificates				Import	
Jse this feature to i	request and manage c	ertificates that the Web server (an use with	ı websites	Create Certificate Request	
onfigured for SSL.					Complete Certificate Reques	
Filter:	▪ 🐺 Go →	🔙 Show All Group by: No	Grouping	-	Create Domain Certificate	
Name	Issued To	Issued By	Expiratio	n Date	Create Self-Signed Certificate	
cloudekonom	CloudEkonom	CloudEkonom	28.03.201	8 2:00:00	View	
sslmarket-pt-17	www.sslmarket.pt	RapidSSL SHA256 CA - G2		0 1.50.50 port		
				este Certificat	te Request	
			Co	implete Certif	icate Request	
				eate Domain (Certificate	
					-d Codificate	
				eate seit-sign	gned Certificate	
			Vie	2VV		
			Export Renew Remove			
			En	able Automat	tic Rebind of Renewed Certificate	
			🕜 He	lp		
<				>		

Importing from a .pfx File:

- 1. On the Start menu click **Run** and then type *mmc*.
- 2. Click File > Add/Remove Snap-in.
- 3. Click **Certificates > Add**.
- Select Computer Account and then click Next. Select Local Computer and then click Finish. Then close the add standalone snap-in window and the add/remove snap-in window.
- 5. Click the + to expand the certificates (local computer) console tree and look for the personal directory/folder. Expand the certificates folder.
- 6. Right-click on the certificate you want to backup and select **ALL TASKS > Import**.
- Follow the certificate import wizard to import your primary certificate from the .pfx file.
 When prompted, choose to automatically place the certificates in the certificate stores based on the type of the certificate.



Enabling a New Certificate on a Server:

- 1. On the Start menu, click Administrative Tools > Internet Information Services (IIS) Manager.
- 2. In the IIS Manager, click the server name.
- 3. Expand the sites folder.
- 4. Select the site that you want to secure (usually the default website).
- 5. On the actions menu in the edit site section, click **Bindings**.

Number Information Services (II	5) Manager	
(3) (8) WIN-4PL9715YGXF	X Sites Default Web Site	😥 🖂 🔂 I 😥 🕶
Ele <u>Vi</u> ew <u>H</u> elp		
Ele Yew Help Connections Start Page Start Page WIN-4PL9715YGXR (WIN-4PL97) Application Pools Sites Ele Default Web Site	Oefault Web Site Ho Group by: Area ASP.NET Image: Complication NET Image: Complication .NET Image: Complication .NET Roles Image: Complication .NET Roles Image: Complication .NET Roles Image: Complication Application Connection Settings Connection Providers Session State	Actions Actions Actions Explore Edit Permissions Edit Site Bindings Basic Settings Basic Settings Wew Applications View Virtual Directories Manage Web Site Restart Start Start Stop Browse Web Site ev Browse *:80 (http) Browse *:443 (https) Advanced Settings ate Configure
	Features View 💦 Content View	e Heb
Ready 🖞 digicert		• <u>•</u> ••••••••••••••••••••••••••••••••••

6. In the site bindings window, click **Add**. If a binding for https already exists, select the https binding, and click **Edit**.

Site Bindir	ıgs				? ×
Type http	Host Name	Port 80	IP Address *	Bind	<u>A</u> dd
					Edit Remove
•				F	Browse
G digi ce	erť				Close



7. Fill out the information in the add site binding window. In the type drop-down choose https. Set the IP address to the IP address of the site or choose all unassigned. The port for SSL traffic is usually 443. Enter the recently imported certificate in the SSL Certificate field.

Add Site Binding						
Type: IP address: https All Unassigned Host name: Image: Imag	P <u>o</u> rt:					
SSL certificate:	<u>▼</u> <u>V</u> iew					
G digi cert	OK Cancel					

8. Click **OK.** Your SSL Certificate is now installed, and the website is configured to accept secure connections. You may have to restart IIS or the server for it to recognize the new certificate.

Si	te Bindi	ngs				<u>?×</u>
	Type http	Host Name	Port 80	IP Address *	Bind	<u>A</u> dd
	https		443	*		Edit
	•				Þ	Browse
5	digic	erť				Close