## Importing SSL ertificate to IIS store

1. Go to IIS settings. Open Server Certificates.

ASP.NET .NET Authorizat	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Trust Levels	Application Settings	Connection Strings	Machine Key	Pages and Controls	Providers	Session State	SMTP E-mail	^
ASP	Authentic	CGI CGI	2 Compression	Default Document	Directory Browsing	Error Pages	FastCGI Settings	Handler Mappings	HTTP Respon	ISAPI and CGI Restri	ISAPI Filters	
Logging	MIME Types	Modules	Output Caching	Equest Filtering	Server Certificates	Worker Processes						
Manageme Configurat Editor	Feature Delegation	Shared Configurat	Web Platfor		Ť							~

2. Navigate to Actions section in the Server Certificates view. There is an Import... option.

	rtificatos					Actions
Server Cer	Tuncates					Import
Use this feature to reques	st and manage certificates that the Web	server can use with websit	es configured for SSL.			Create Certificate Request
Filter: new cert	🝷 ኛ Go 🕞 🕁 Show All 🛛 Group b	y: No Grouping 🔹				Complete Certificate Request
Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store	Create Domain Certificate
						Create Self-Signed Certificate
						Enable Automatic Rebind of Renewed Certificate
						😧 Help

3. Select a certificate (\*.pfx) that you want to import and enter your password if your certificate is password-protected.

Import Certificate	?	$\times$
<u>⊆</u> ertificate file (.pfx):		
C:\Program Files\WebSpellChecker\AppServ	/er\certific	
Password:		
•••••		
Select Certificate Store:		
Personal		$\sim$
Allow this certificate to be exported		
ОК	Cancel	

4. In case of the success operation, you will find a certificate listed on the list of Server Certificates.

## Server Certificates

Filter: Certificate	🕻 Go 🕞 😽 Show All 🛛 Group by:	No Grouping 🔹			
Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
Certificate_test	:		2/17/2021 2:00:00	E00CB966A700AAB215A5CE3	Personal

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

5. To check the common name (CN) of your certificate right-click on the certificate and select View...

## 

Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued	i To	Issued By	Expiration Date	Certificate Hash	Certificate Store
Certificate_test	m	Import		2/17/2021 2:00:00	E00CB966A700AAB215A5CE3	Personal
		Create Certificate Reque Complete Certificate Re Create Domain Certifica Create Self-Signed Certi View	st quest te ficate			
	× @	Export Remove Enable Automatic Rebin Help	d of Renewed Certificate			

On the pop-up with the Certificate infomation, open **Details** tab. Find the **Issuer** infomation.

:d

6. This is the CN name that you need to specify during the installaton of WebSpellChecker.

侵)

WebSpellChecker Setup	_
Configure Service SSL Certificate	

×

Export y	our SSL certificate f	rom Windows Certificate Store (recommended).
O Skip nov	v and configure late ation file.	r manually in the SSL tag of the AppServerX.xml
Apply a	ended). In this case	is used by your web or Java Application Server (not the connection with the service will be configured
via the I	astCGI protocol. rtificate Common Na	ame (the fully qualified HostName):
via the I Enter the Ce your_comm	astCGI protocol. rtificate Common Na on_name	ame (the fully qualified HostName):
via the I Enter the Ce your_comm Choose the	astCGI protocol. rtificate Common Na on_name Certificate Store	ame (the fully qualified HostName):
via the I Enter the Ce your_comm Choose the O	FastCGI protocol. rtificate Common Na on_name Certificate Store V	ame (the fully qualified HostName):
via the I Enter the Ce your_comm Choose the O	FastCGI protocol. rtificate Common Na on_name Certificate Store	ame (the fully qualified HostName):

Alternatively, if WebSpellChecker is already installed, you can update this directly in AppServerX.xml file.

```
<SSLCertificateSource>STORE</SSLCertificateSource>
    <SSLCertificateStoreSettings>
    <!-- The Common Name represents the server name protected by the SSL certificate (the fully qualified
HostName). -->
    <SSLCertificateCommonName>your_common_name</SSLCertificateCommonName>
    <!-- If specified, Windows machine certificate store is used. Otherwise, the user's certificate store is
used.
    The default value is true. -->
    <SSLCertificateUseMachineStore>true</SSLCertificateUseMachineStore>
    <!-- Possible values: MY (Personal), ROOT (Trusted Root Certification Authorities), TRUST (Enterprise
Trust),
    CA (Intermediate Certification Authorities), USERDS (Active Directory User Object). The default value is
MY. -->
<SSLCertificateStore>MY</SSLCertificateStore>
```