

IIS Documentation Manual

05 BANANAL, Elmer Jr. Pasion

09 FERRER, Gavin Roy Llamido

23 AMBO, Melissa Denis

28 CUSTODIO, Danica Shiene Dela Masa

31 GONZALES, Darlene Joyce Buisan

33 LOPEZ, Kimberly Tangalin

37 PARIS, Lovelyn Degay

Table of Contents

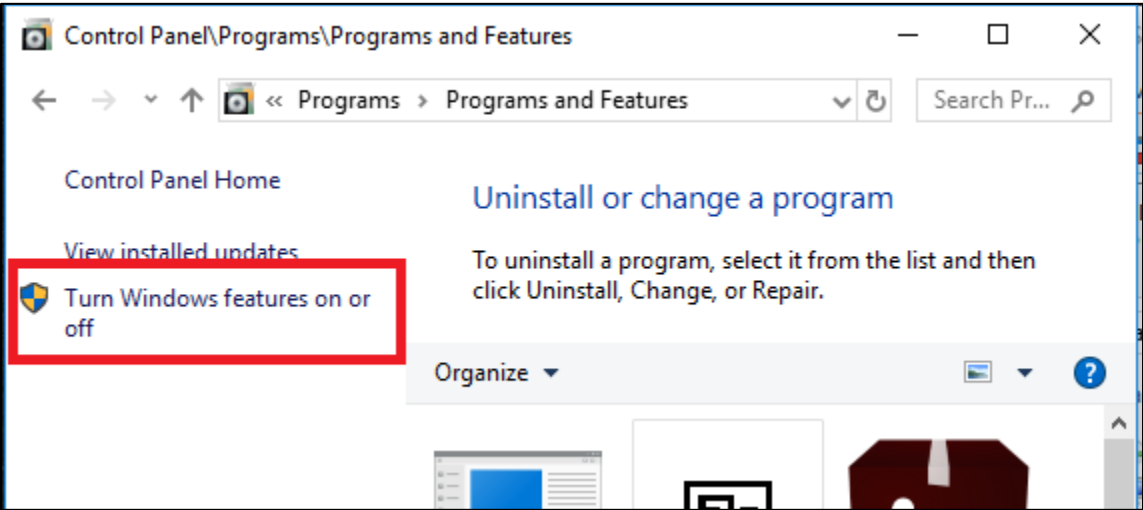
I.	Installation	3
II.	Hosting	5
III.	Compression	7
IV.	Content Negotiation	11
V.	Access	13
VI.	Secure	14
VII.	Server-Side Includes	16

IIS INSTALLATION

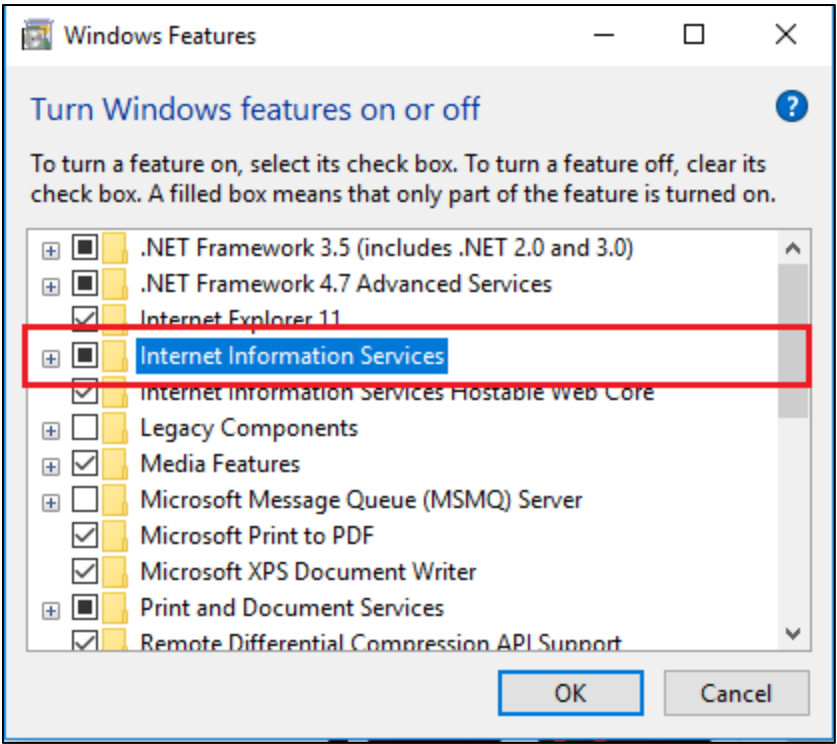
1. Since IIS is a readily available program in the Windows10 operating systems, the program’s installer does not require any downloading from the internet. If you are using a Windows10 operating system go to your Control Panel

PATH:Control Panel\Programs\Programs and Features

And click on “Turn Windows features on or off” option located in the left side panel

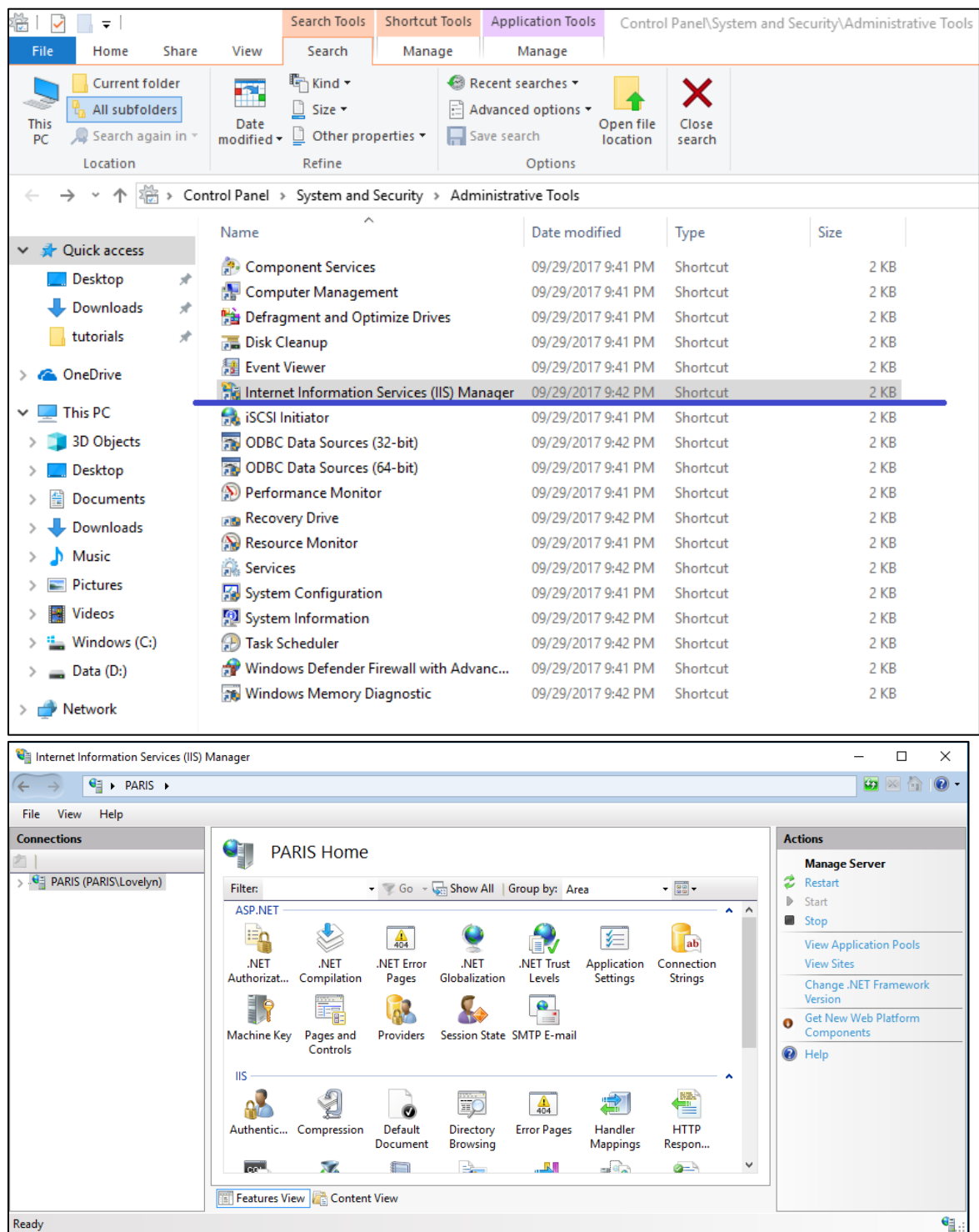


2. You will then be directed to list of programs from here on enable the Internet Information Services, and click the Ok button to save the changes.



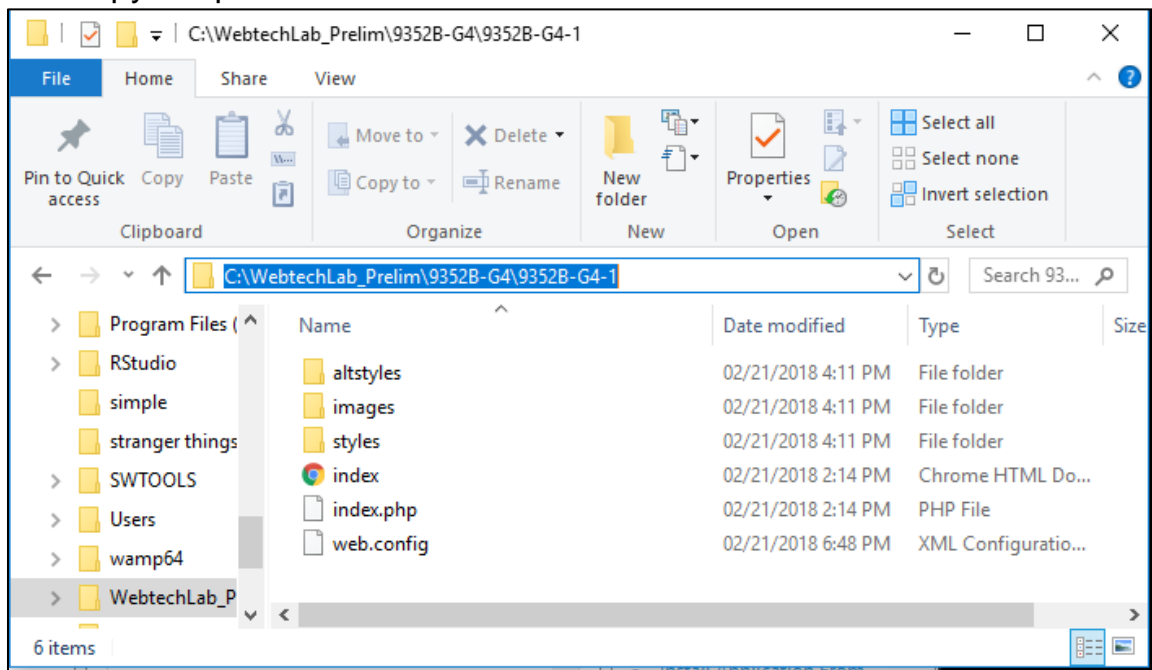
3. Afterwards you may now open the program by simply searching IIS in the start menu bar or go directly to its location

PATH: Control Panel\System and Security\Administrative Tools



HOSTING A WEBSITE IN IIS

- 1. Place the folder containing all the resources (html, css, etc.) in drive C://
And copy the path where the *index.html* file is located

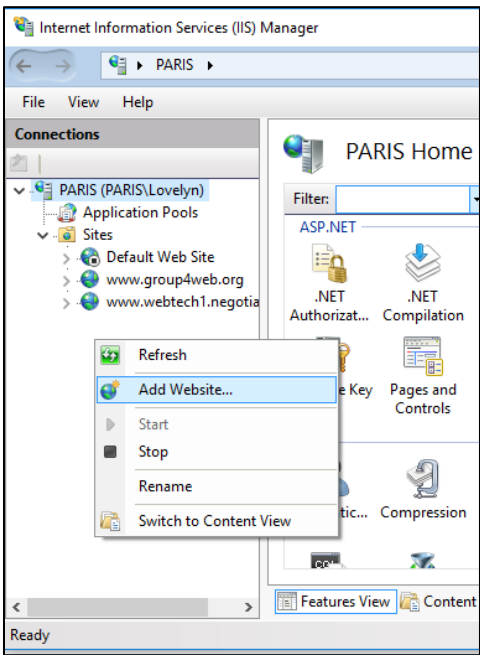


- 2. Run the command prompt and note the computer's IP address, by typing *ipconfig*

```
Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::d420:c6c6:18cc:fd06%8
IPv4 Address. . . . . : 192.168.64.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

- 3. Open the IIS program and right click on the *Connections* panel until an "Add a website" option appears.



4. Once clicked input the following values and click the Ok button

Add Website

Site name:

www.group4x.org

Application pool:

www.group4x.org

Select...

Content Directory

Physical path:

C:\WebtechLab_Prelim\9352B-G4\9352B-G4-1

...

Pass-through authentication

Connect as...

Test Settings...

Binding

Type:

http

IP address:

192.168.64.1

Port:

80

Host name:

www.group4x.org

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

OK

Cancel

5. Edit your system's host file located in:
PATH: C:\Windows\System32\drivers\etc
Use Notepad++ and allow System administration.
INPUT: <IP Address> <website url>
And save the changes in Administrator mode.

The screenshot shows a Windows File Explorer window with the address bar set to `C:\Windows\System32\drivers\etc`. The file list shows several files, including `hosts`, `hosts`, `Imhosts.sam`, `networks`, `protocol`, and `services`. The `hosts` file is selected. To the right, the contents of the `hosts` file are displayed in a text editor. The file contains comments and mappings. The last line, `192.168.64.1 www.group4x.org`, is highlighted with a red box.

```
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft
4 #
5 # This file contains the mappings of IP address
6 # entry should be kept on an individual line.
7 # be placed in the first column followed by the
8 # The IP address and the host name should be se
9 # space.
10 #
11 # Additionally, comments (such as these) may be
12 # lines or following the machine name denoted b
13 #
14 # For example:
15 #
16 # 102.54.94.97 rhino.acme.com
17 # 38.25.63.10 x.acme.com
18
19 # localhost name resolution is handled within I
20 # 127.0.0.1 localhost
21 # ::1 localhost
22
23 192.168.1.4 jetbrains
24 192.168.64.1 www.group4web.org
25 192.168.64.1 www.webtechl negotiate.org
26 192.168.64.1 www.group4x.org
```

6. Go to your web browser and type in the website's URL

6

IIS COMPRESSION

Compression takes files that are larger in size and compresses them to be smaller that will allow caching for faster web service

A.

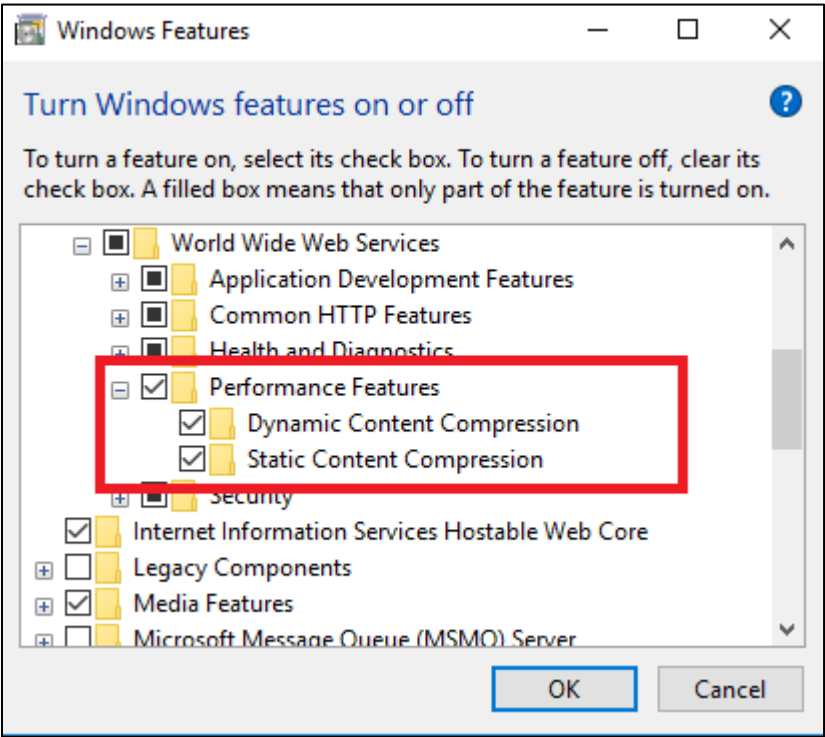
1. Check if the program feature for compression is activated or enabled by going back to the Control Panel for Programs and Features and Clicking on the “Turn the Windows features on and off”

From there scroll through the folders:

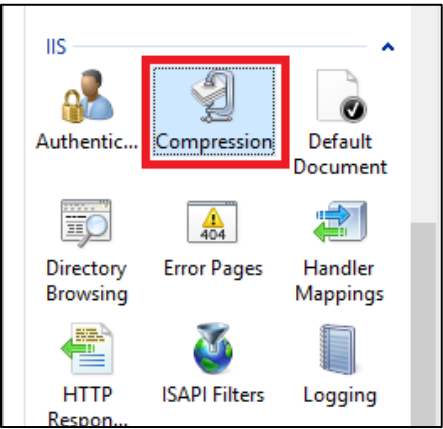
Internet Information Services > World Wide Web Services > Performance Features

And enable both types of content compression by select both checkboxes

- ✓ Dynamic Content Compression
- ✓ Static Content Compression

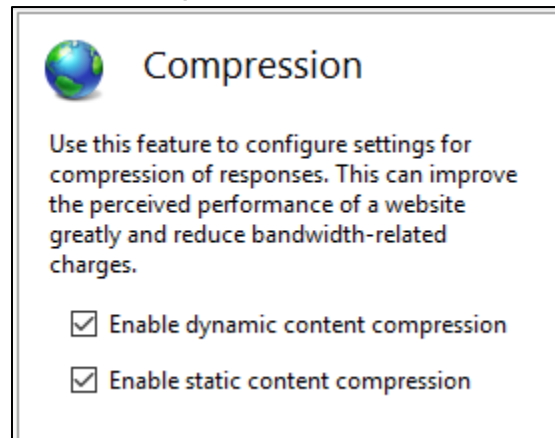


2. Afterwards go to the IIS program and click on the Compression icon

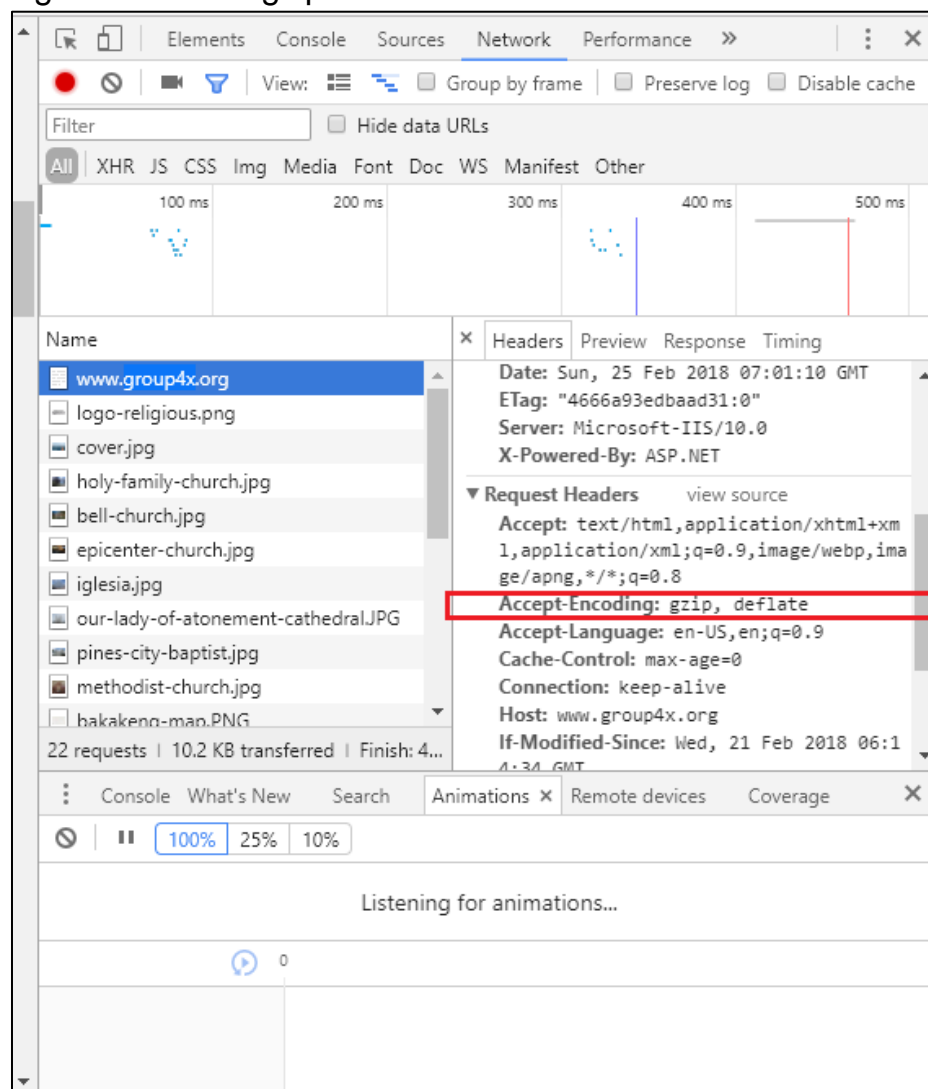


And enable both the static content compression and dynamic content compression by selecting the checkbox.

- ✓ Enable static content compression
- ✓ Enable dynamic content compression

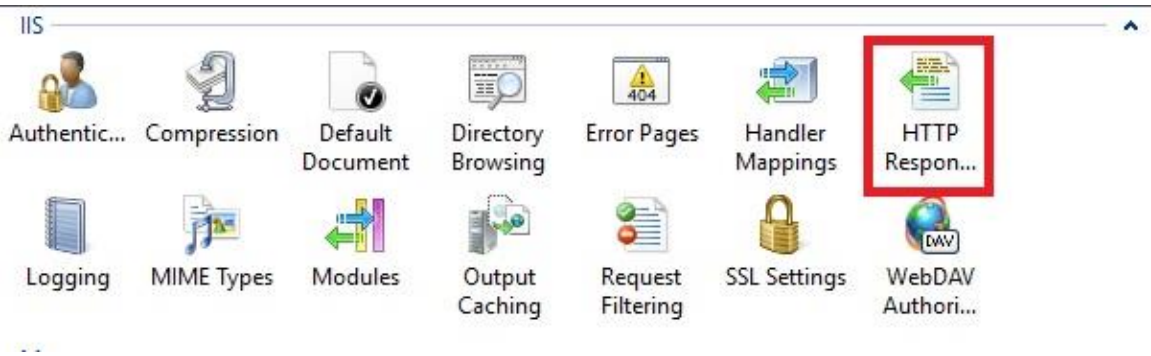


- It is also to be noted that since image file such as *.jpg and *.png are rasterized images they cannot be compressed from HTTP compression because these image files are already compressed.
3. To verify the changes, launch the website in a browser and inspect its elements. Refresh the page and open the headers of the html file in the Networks tab.
- An indication of the compression will show in the Accept-Encoding headers displaying the status of gzip and deflate.

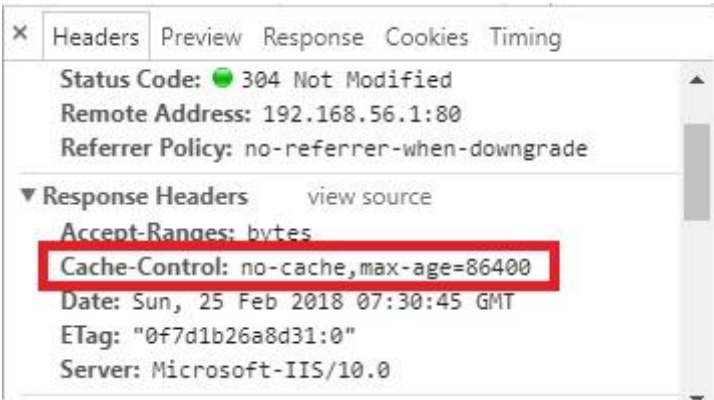
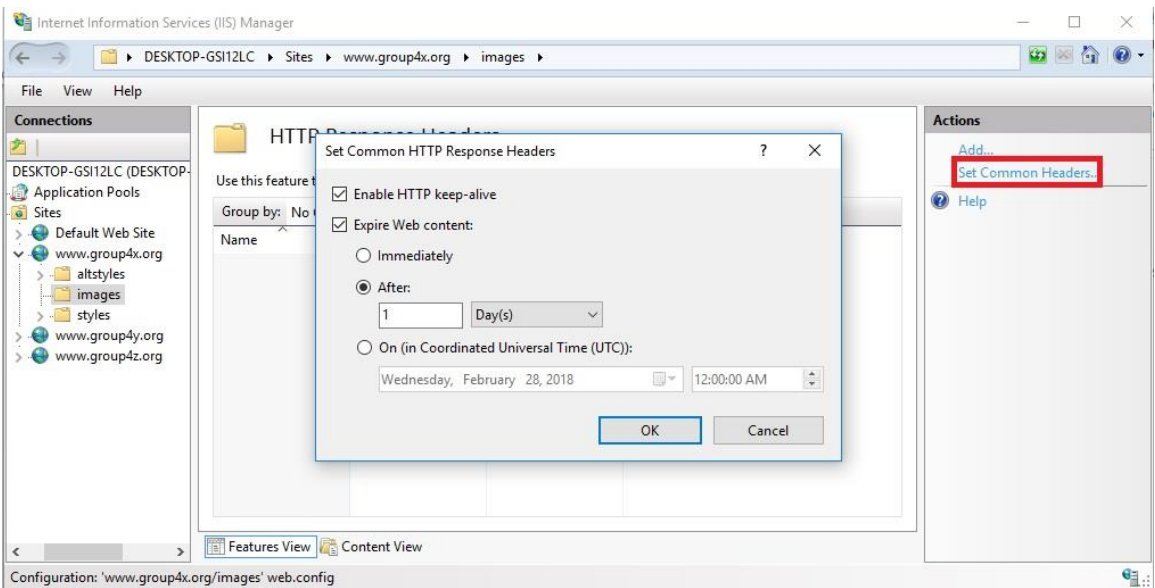


B.

1. To limit the clients access to the files in IIS you can set an expiration using the HTTP Response Headers feature. To check the Cache Control, click the “images” folder on the left tab and click “HTTP Response Headers”

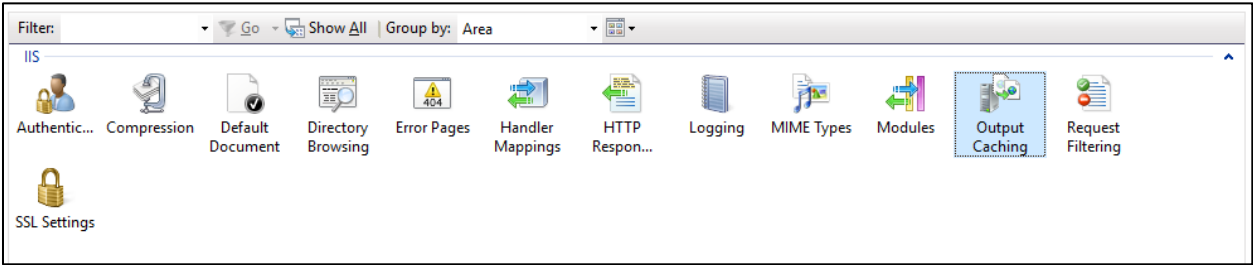


2. On the right tab, click the “Set common Headers” and set the followings settings shown on the figure. Then click restart. Access your browser and inspect its element and the Cache Control should be working
- ✓ Enable HTTP keep-alive
 - ✓ Expire Web Content
 - After
 - 1 Days

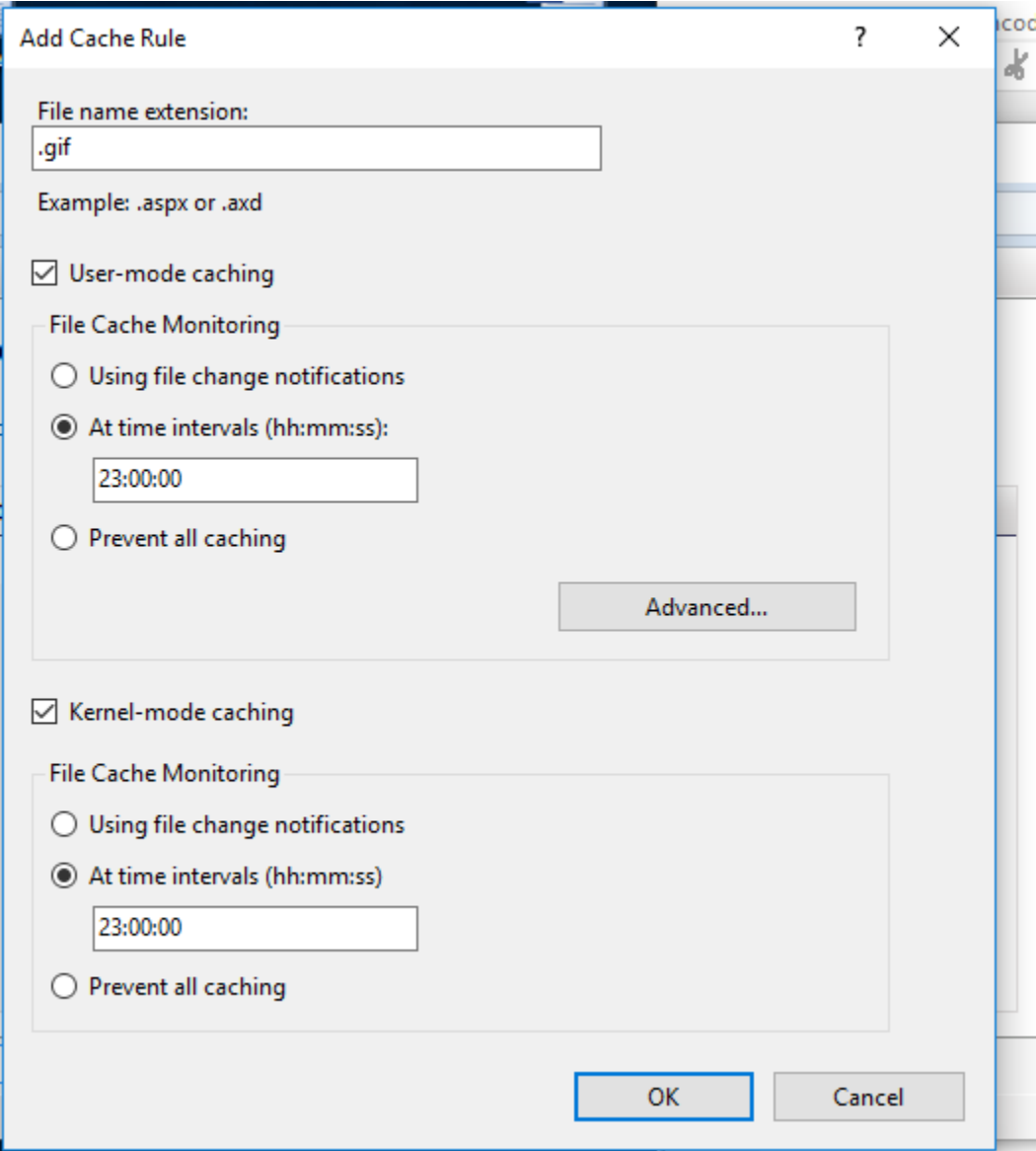


Caching

- 1. Click on Output Caching to add rules for caching

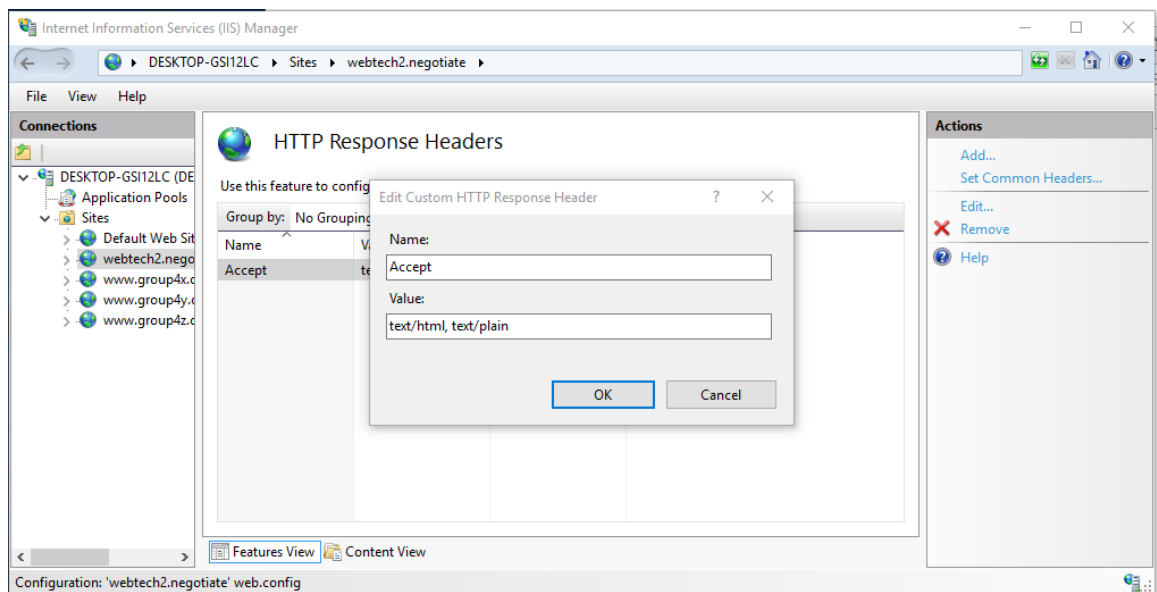


- 2. Fill up the File name extension box (i.e. .gif, .png, .jpg). Check on the User-mode caching box and check on the At time intervals radio button then change the time interval to 24 hours

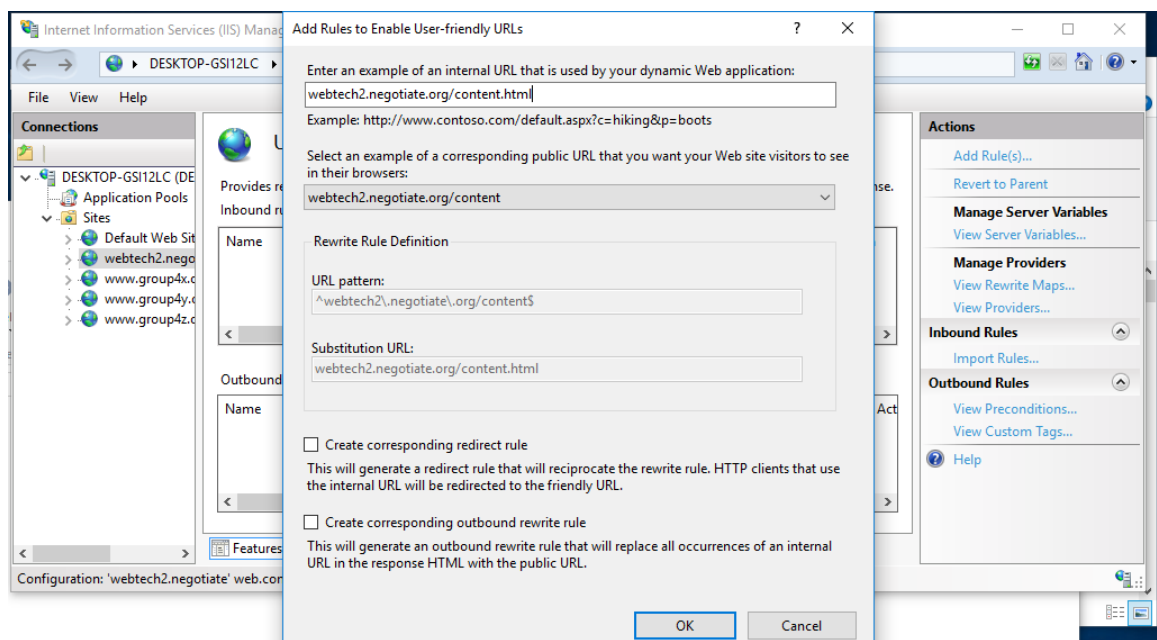


Content Negotiation

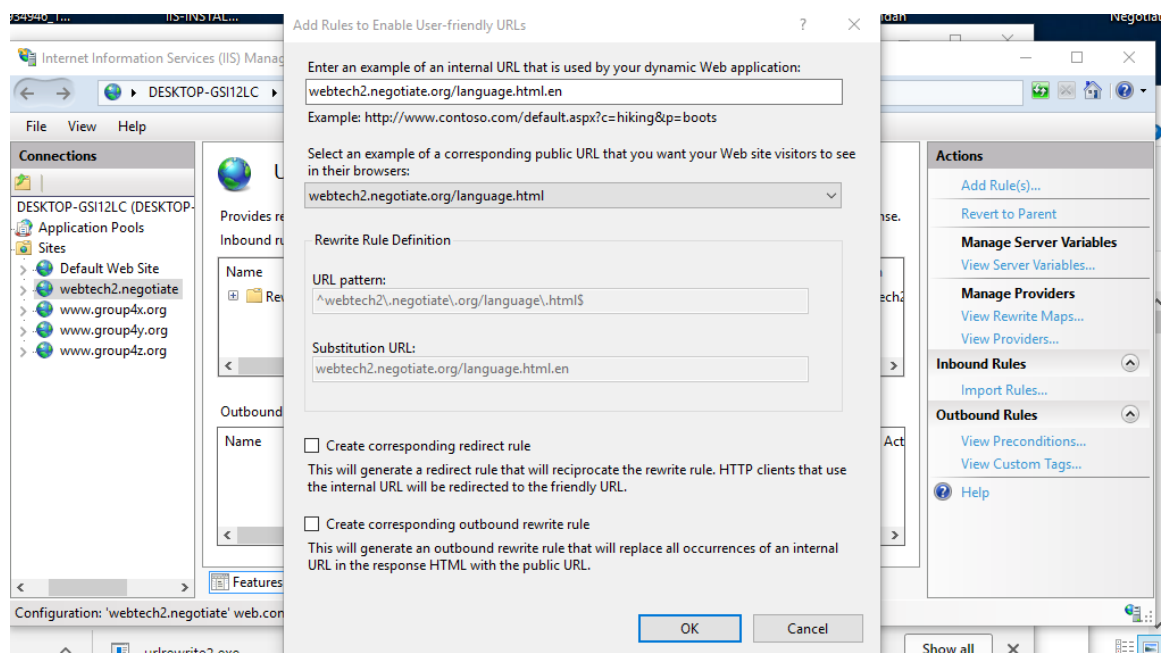
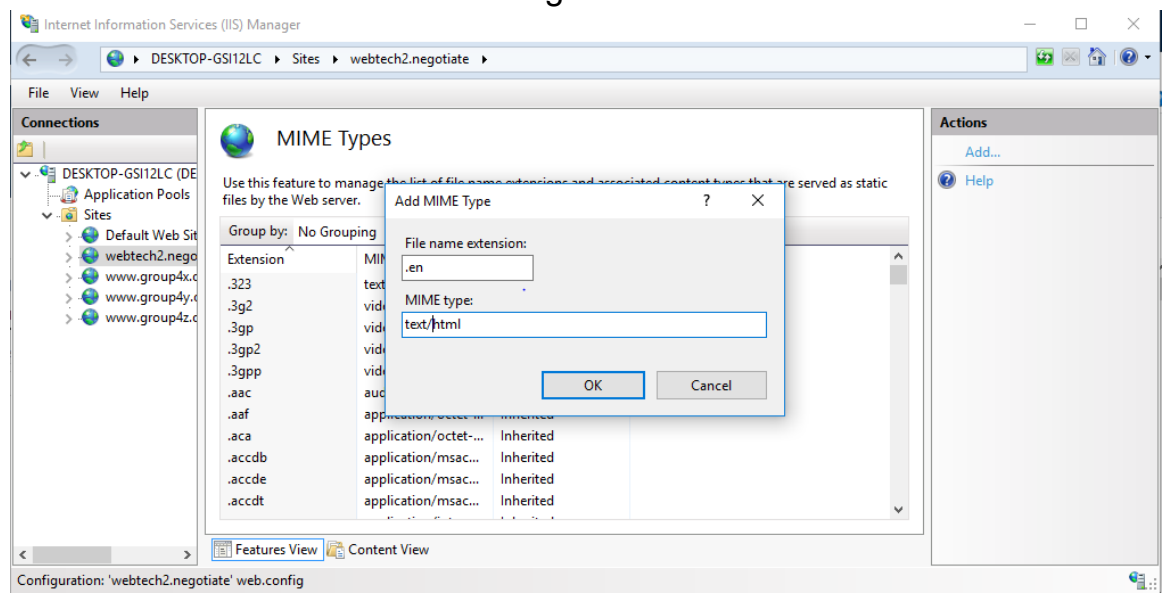
1. The Accept header sets the content that gets accepted. Click HTTP Response headers and “Set common headers” and enter the following details



2. Go URL Rewrite and enter the following. URL Rewrite will redirect the actual content. Click “Add rules..” and click “User-Friendly URL”

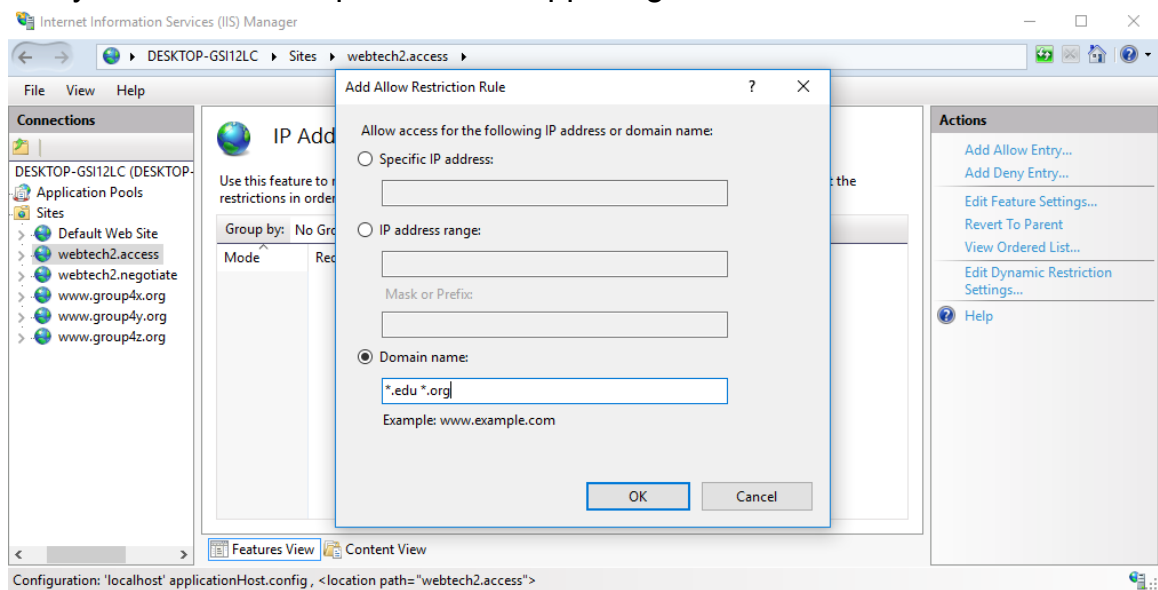


3. Next is to Click MIME types and click “Add” on the right tab and enter the following. IIS also negotiates with Languages. Next is to go to URL Rewrites and click “Add..” On the right tab.

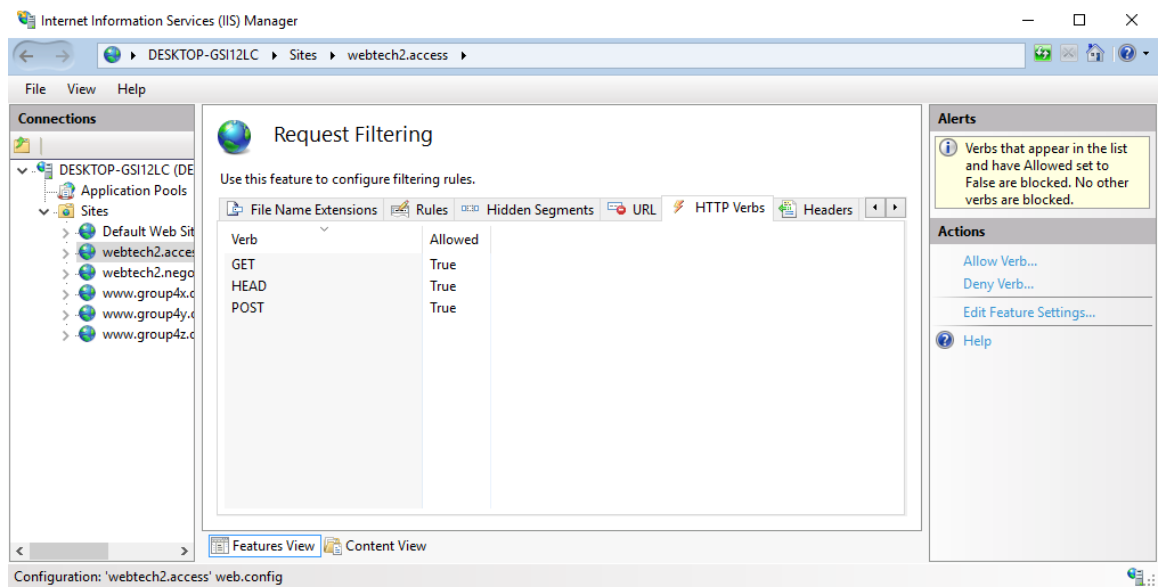


Access

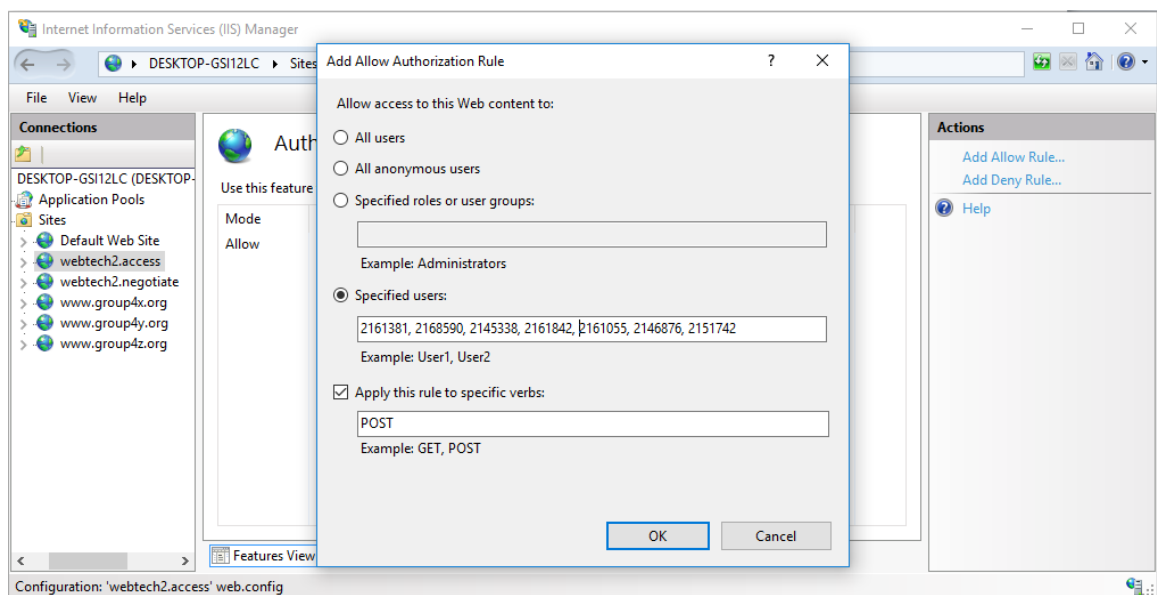
- 1. Restricting a certain domain can be configured using IIS. click on the IP Address and Domain Restrictions feature then click on Add Allow Entry...on the Action pane on the upper right side.



- 2. Go to the Request Filtering feature then HTTP Verbs tab. Click on “Allow Verb...” on the right tab. This configuration would set only GET, HEAD and POST



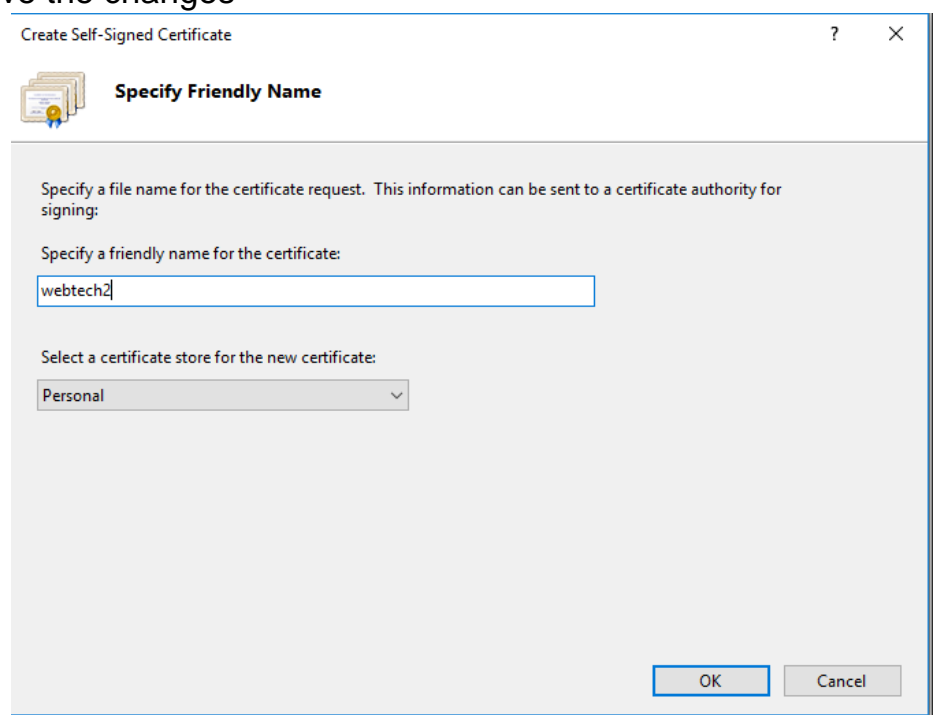
3. To specify rules, go to Authorization Rules feature and click “Add Allow Rule..”. Choose specified users. Add your groupmates id numbers as users.

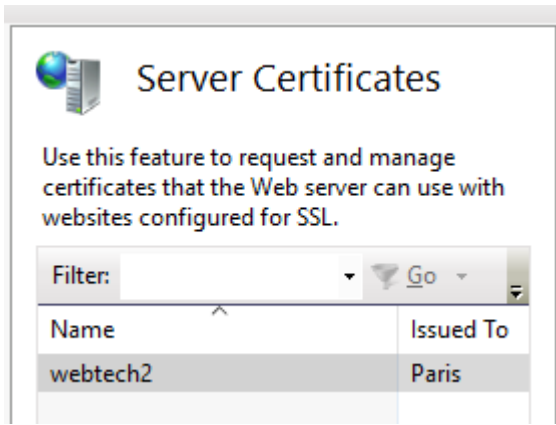


IIS CONFIGURATION FOR: *webtech2.secure.org*

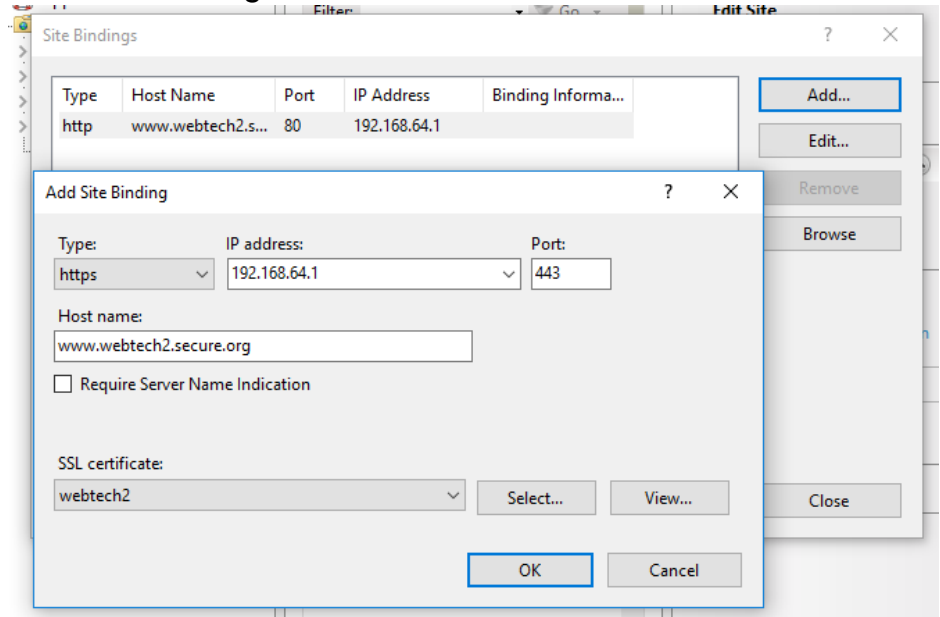
A.

1. Select the server at the Connections panel and click on the Server Certificates icon
2. From here select the Create Self-Signed Certificate Request... from the Actions panel and set the name of the certificate, indicate it as Personal and save the changes





- 3. Select the website to be certified and edit the Site Bindings, and switch the Type to https, input the sites IP address and the Host name select the SSL certificate to the self-signed certificate.



- 4. Open your browser and input the host name
- 5. Proceed with the site despite the error.

B. Open-ssl

- 1. Download and install open ssl
DOWNLOAD LINK: <https://slproweb.com/products/Win32OpenSSL.html>
It is recommended to download the 32-bit version because it is the most stable version to use.

Download Win32 OpenSSL today using the links below!

File	Type	Description
Win32 OpenSSL v1.1.0g Light	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.0g (Recommended for users by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win32 OpenSSL v1.1.0g	30MB Installer	Installs Win32 OpenSSL v1.1.0g (Recommended for software developers by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0g Light	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.0g (Only install this if you need 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.1.0g	33MB Installer	Installs Win64 OpenSSL v1.1.0g (Only install this if you are a software developer needing 64-bit OpenSSL for Windows. Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

- 2. After the installation go to the bin folder of the Open-SSL program located in
PATH: C:\Windows\System32\
And run command prompt in the bin directory

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.16299.248]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\OpenSSL-Win32\bin>
```

- 3. To create a rsa key input the following command:
openssl genrsa -out webtech2.key 2048

```
C:\OpenSSL-Win32\bin>openssl genrsa -out webtech2.key 2048
Generating RSA private key, 2048 bit long modulus
...+++
.....+++
e is 65537 (0x010001)
```

- 4. Input the next command that will create the .csr file
openssl req -new -key webtech2.key -out webtech2.csr -config .\openssl.cfg
Fill in the attributes:

```
Country Name (2 letter code) [AU]:PH
State or Province Name (full name) [Some-State]:Benguet
Locality Name (eg, city) []:Baguio City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:WebTech Group 4
Organizational Unit Name (eg, section) []:WebTech Group 4
Common Name (e.g. server FQDN or YOUR name) []:webtech2.serve.org
Email Address []:2145338@slu.edu.ph
```

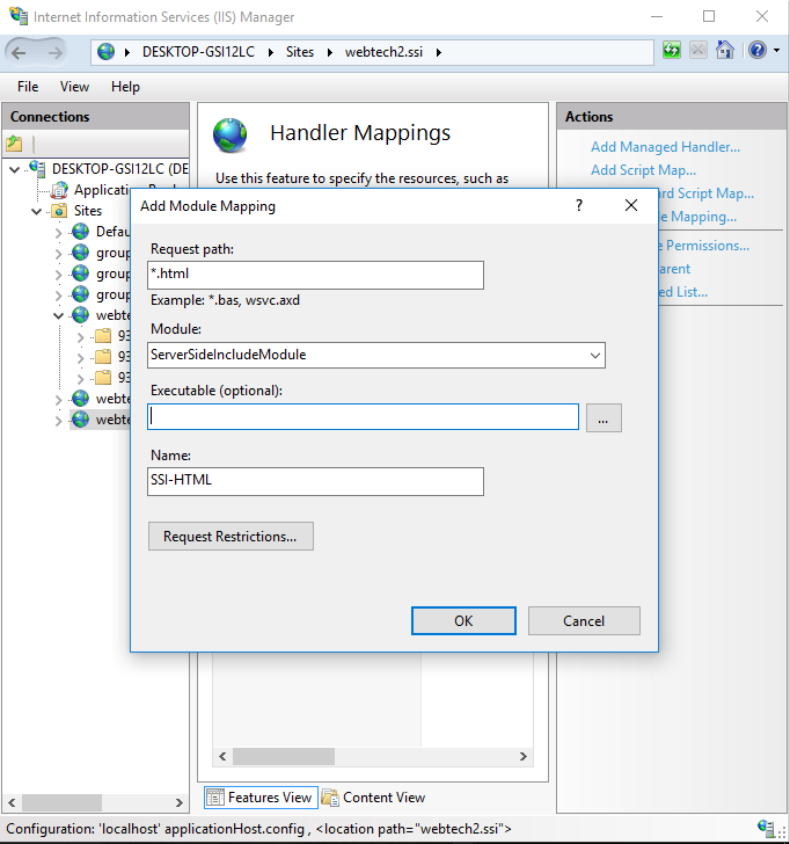
And the additional alternative attributes can either be left blank.

- 5. And generate the .pfx file by inputting:
openssl pkcs12 -inkey webtech2.key -in webtech2.cer -export -out webtech2.pfx

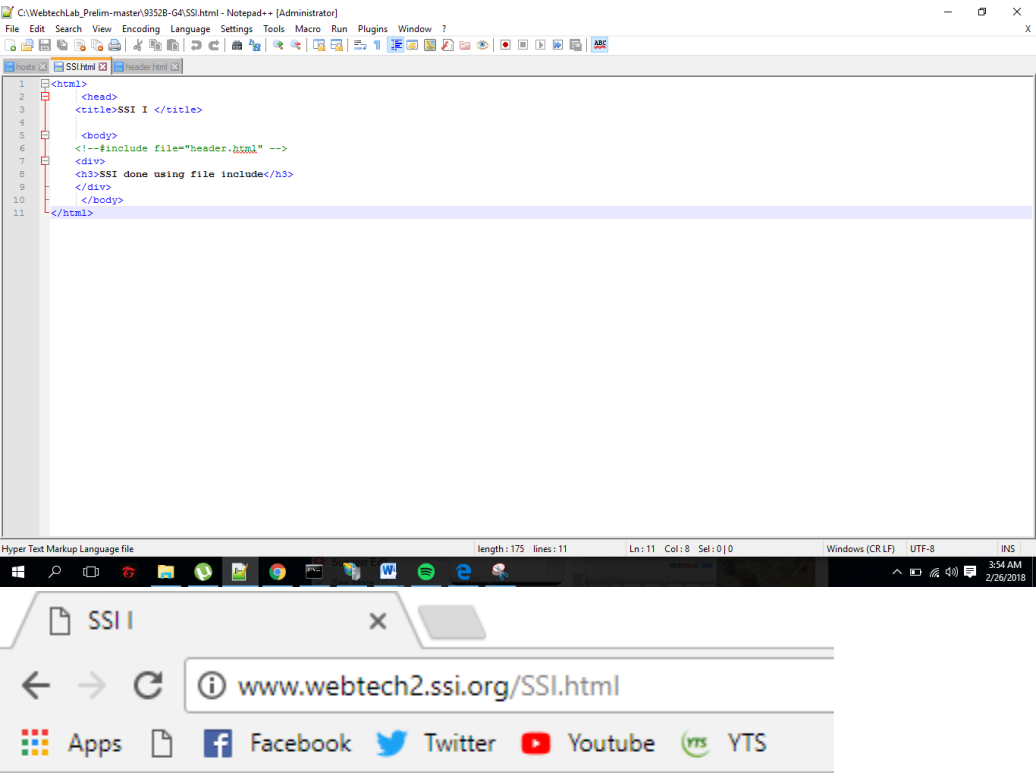
Server-side Includes (SSI)

- 1. Server-side Includes (SSI) on IIS can be done by adding the ServerSideIncludeModule using the Handler Mappings feature. go to the Handler Mappings feature while in the website you would want to apply it

to then click on Add Module Mapping...



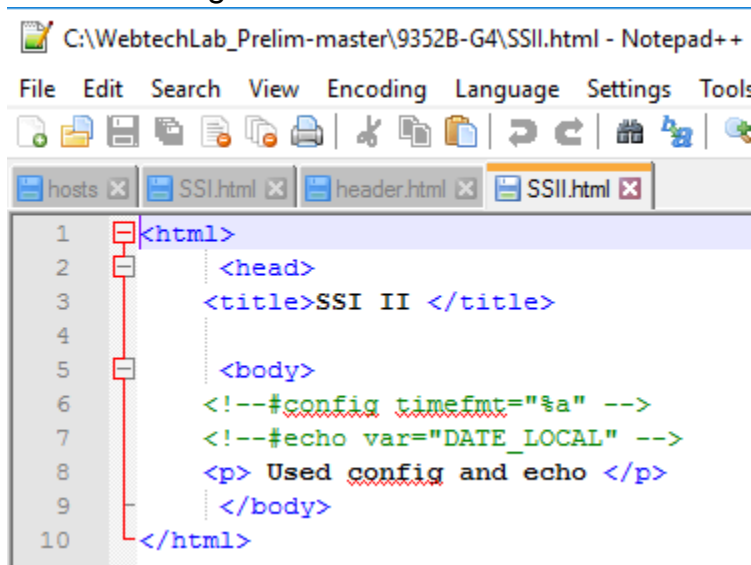
2. Create a html file that would be evaluated by the server. The include directive should have the header.html file to be accessed.



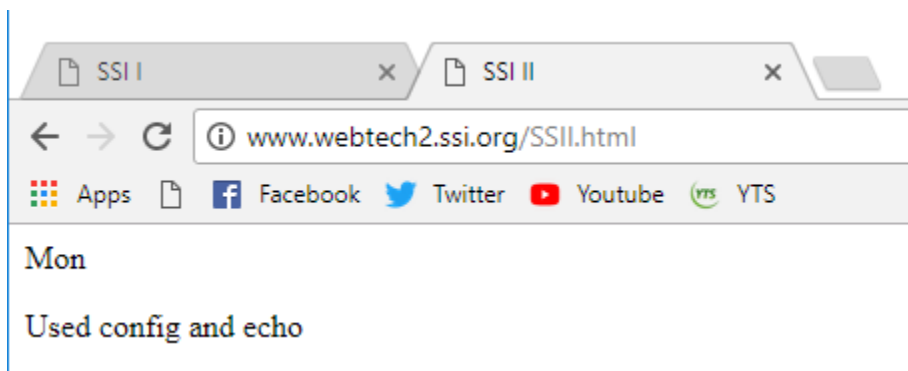
Hi this is my header!

SSI done using file include

3. When using the config directive, it would process what the server needs before loading.



```
1 <html>
2   <head>
3     <title>SSI II </title>
4
5   <body>
6     <!--#config timefmt="%a" -->
7     <!--#echo var="DATE_LOCAL" -->
8     <p> Used config and echo </p>
9   </body>
10 </html>
```



Web Certificates

1. Download and install openssl.
<https://slproweb.com/products/Win32OpenSSL.html>

Win32 OpenSSL v1.1.0g	30MB Installer	Installs Win32 OpenSSL v1.1.0g (Recommended for software developers by the creators of OpenSSL). Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
---------------------------------------	----------------	--

2. Open command prompt and go to **C:\OpenSSL-Win32\bin** then set a path of **OPENSSL_CONF=C:\OpenSSL-Win32\bin\cnf\openssl.cnf**. Type in the command prompt **openssl req -x509 -nodes -days 365 -keyout *key filename*.key -out *certificate filename*.crt** and fill out the information that will be incorporated to your certificate.

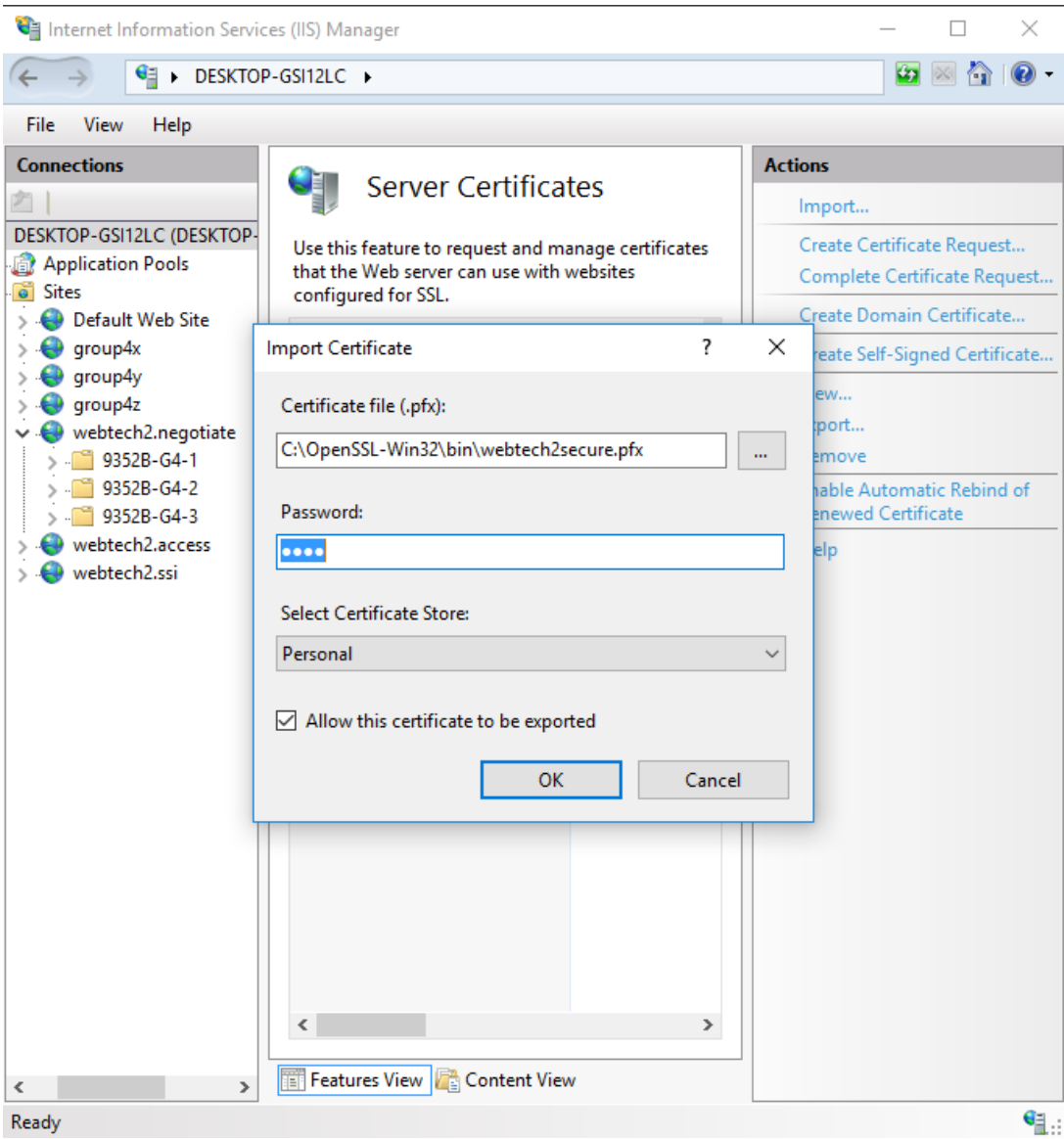
```
C:\Windows\System32\cmd.exe
C:\OpenSSL-Win32\bin>openssl req -x509 -nodes -days 365 -keyout "webtech2.secure".key -out "webtech2.secure".crt
req: Unknown digest x509-nodes-days
req: Use -help for summary.

C:\OpenSSL-Win32\bin>openssl req -x509 -nodes -days 365 -keyout "webtech2secure".key -out "webtech2secure".crt
req: Unknown digest x509-nodes-days
req: Use -help for summary.

C:\OpenSSL-Win32\bin>openssl req -x509 -nodes -days 365 -keyout webtech2secure.key -out webtech2secure.crt
Generating a 2048 bit RSA private key
.....+++++
writing new private key to "webtech2secure.key"
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:PH
State or Province Name (full name) [Some-State]:Benguet
Locality Name (eg, city) []:Baguio City
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SLU-SCIS
Organizational Unit Name (eg, section) []:Webtech Group 4
Common Name (e.g. server FQDN or YOUR name) []:webtech2.secure.org
Email Address []:2161381@slu.edu.ph

C:\OpenSSL-Win32\bin>
```

```
C:\OpenSSL-Win32\bin>openssl pkcs12 -inkey webtech2secure.key -in webtech2secure.crt -export -out webtech2secure.pfx
Enter Export Password:
Verifying - Enter Export Password:
```



3.