

## Installing an SSL Certificate in Windows Server 2008 (IIS 7.0)

Microsoft's new server platform, Windows Server 2008 uses Internet Information Services (IIS) 7.0. This new version makes big changes in the way that SSL certificates are generated, primarily making it much easier than previous versions of IIS. In addition to the new method of requesting and installing SSL certificates, IIS 7 includes the ability to:

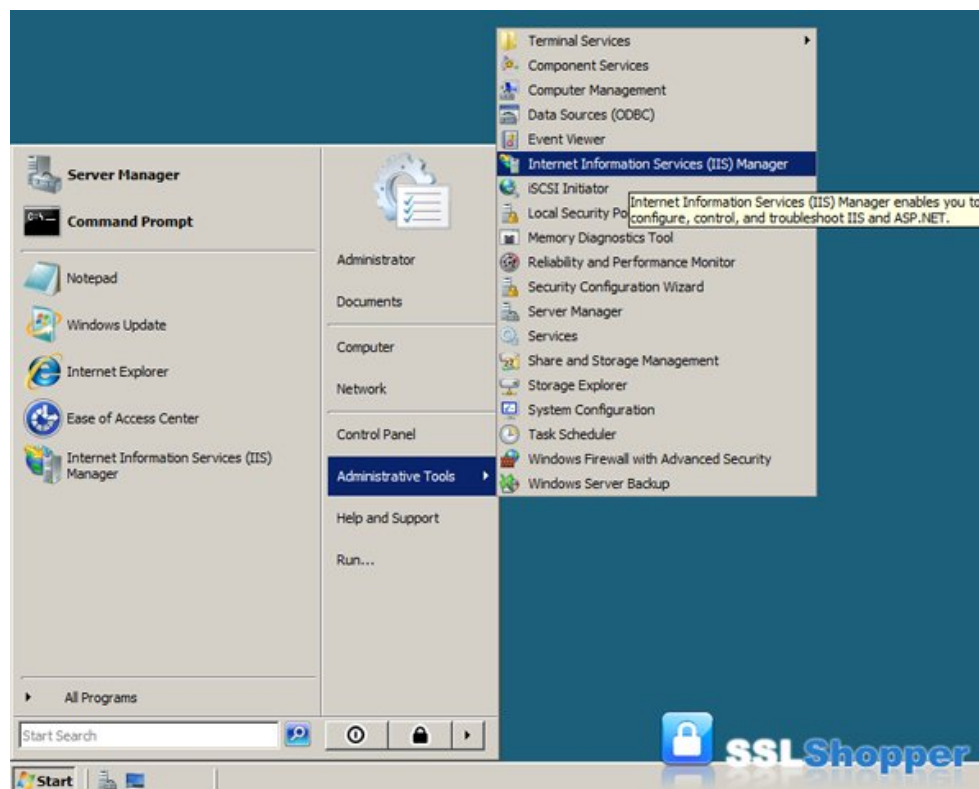
- Request more than one SSL certificate at a time
- Import, export, and renew SSL certificates easily in IIS
- Quickly create a [self-signed certificate](#) for testing

This article will walk you through the process of ordering an SSL certificate from a commercial [certificate authority](#) and installing it on an IIS 7 Windows Server 2008 machine.

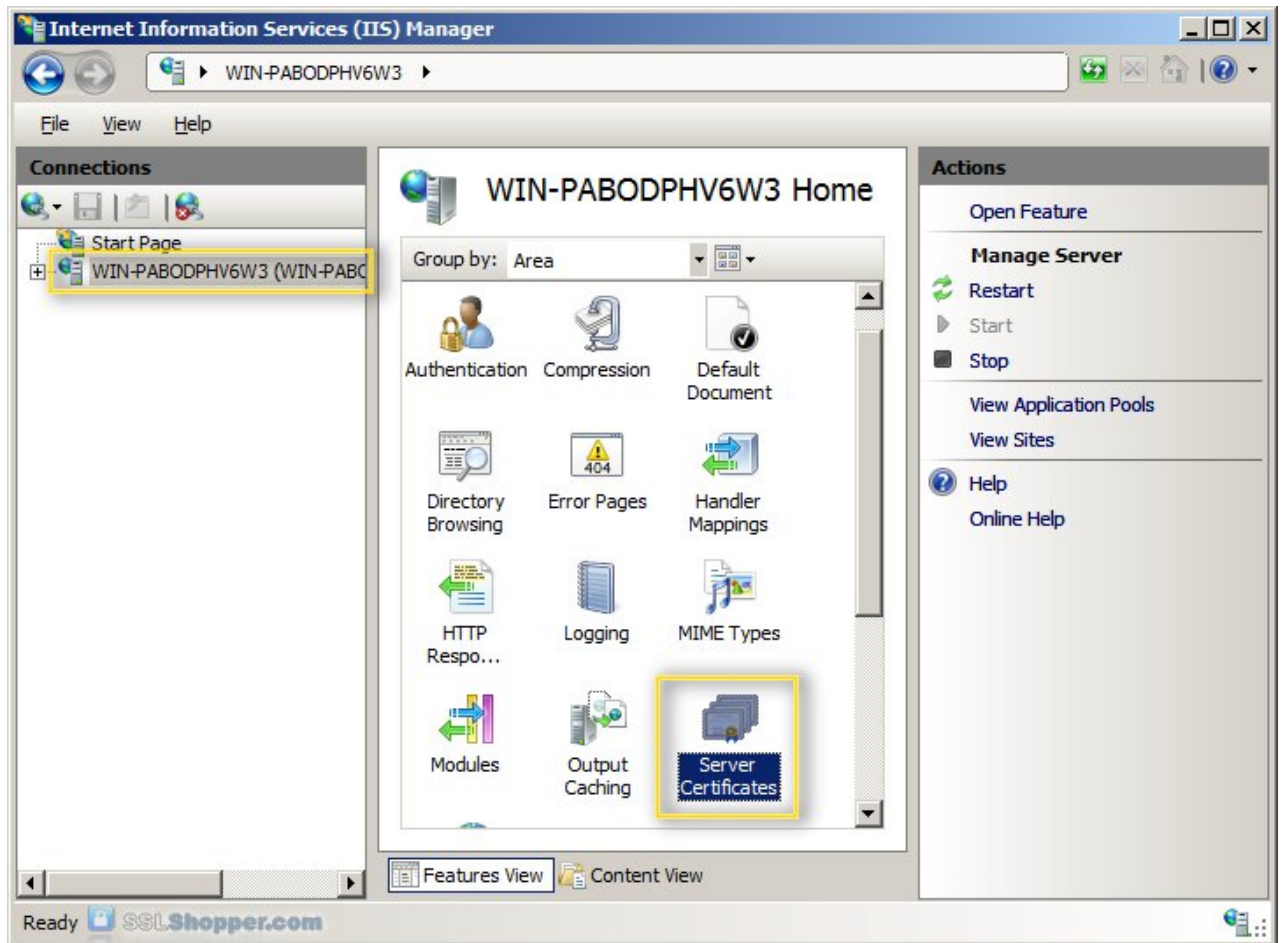
### Create the Certificate Signing Request

The first step in ordering an SSL certificate is generating a [Certificate Signing Request](#). This is very easy to do in IIS7 using the following instructions. [Click here to hide or show the images](#)

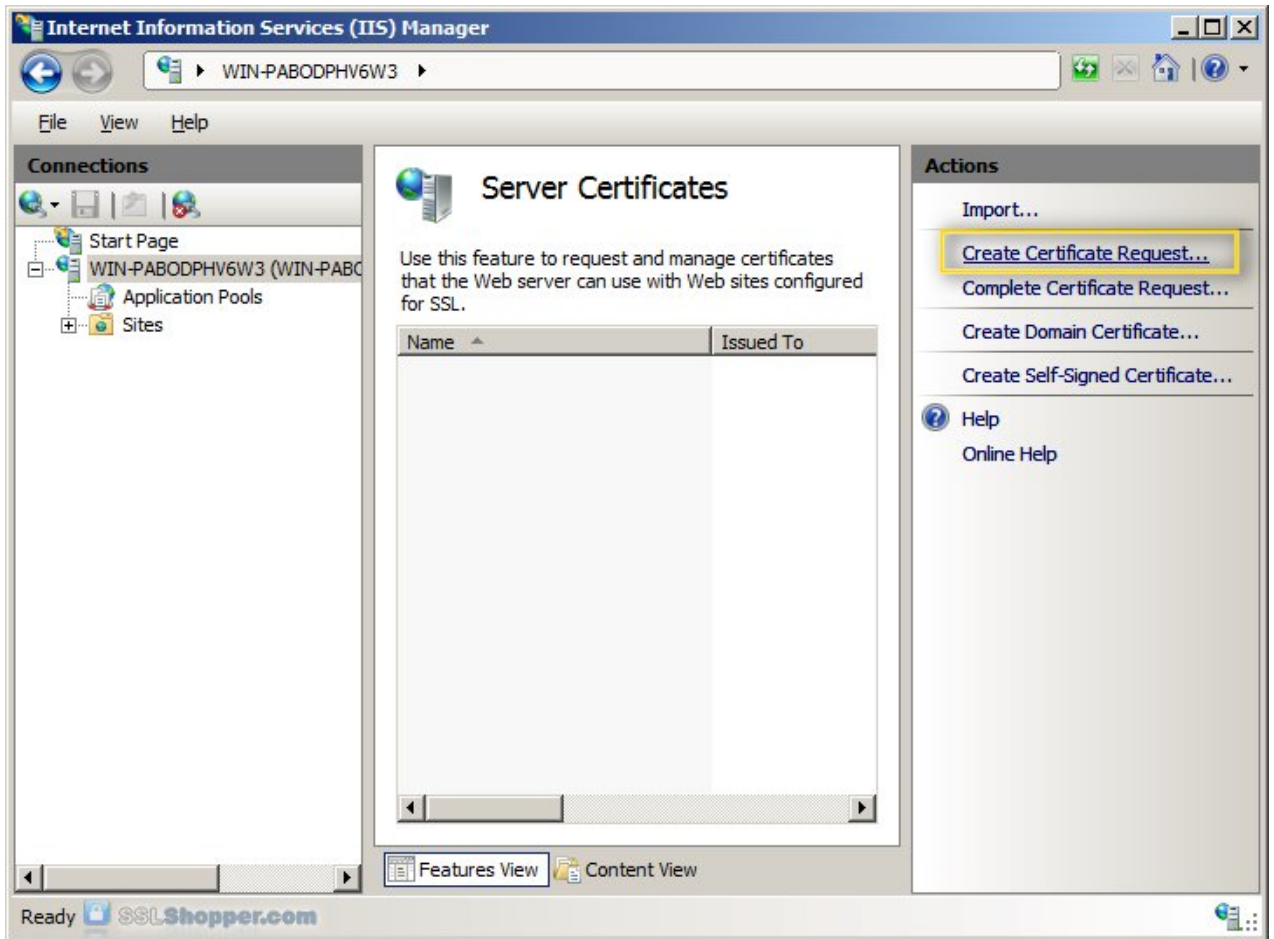
1. Click on the Start menu, go to Administrative Tools, and click on Internet Information Services (IIS) Manager.



2. Click on the name of the server in the Connections column on the left. Double-click on Server Certificates.



3. In the Actions column on the right, click on Create Certificate Request...



4. Enter all of the following information about your company and the domain you are securing and then click Next.

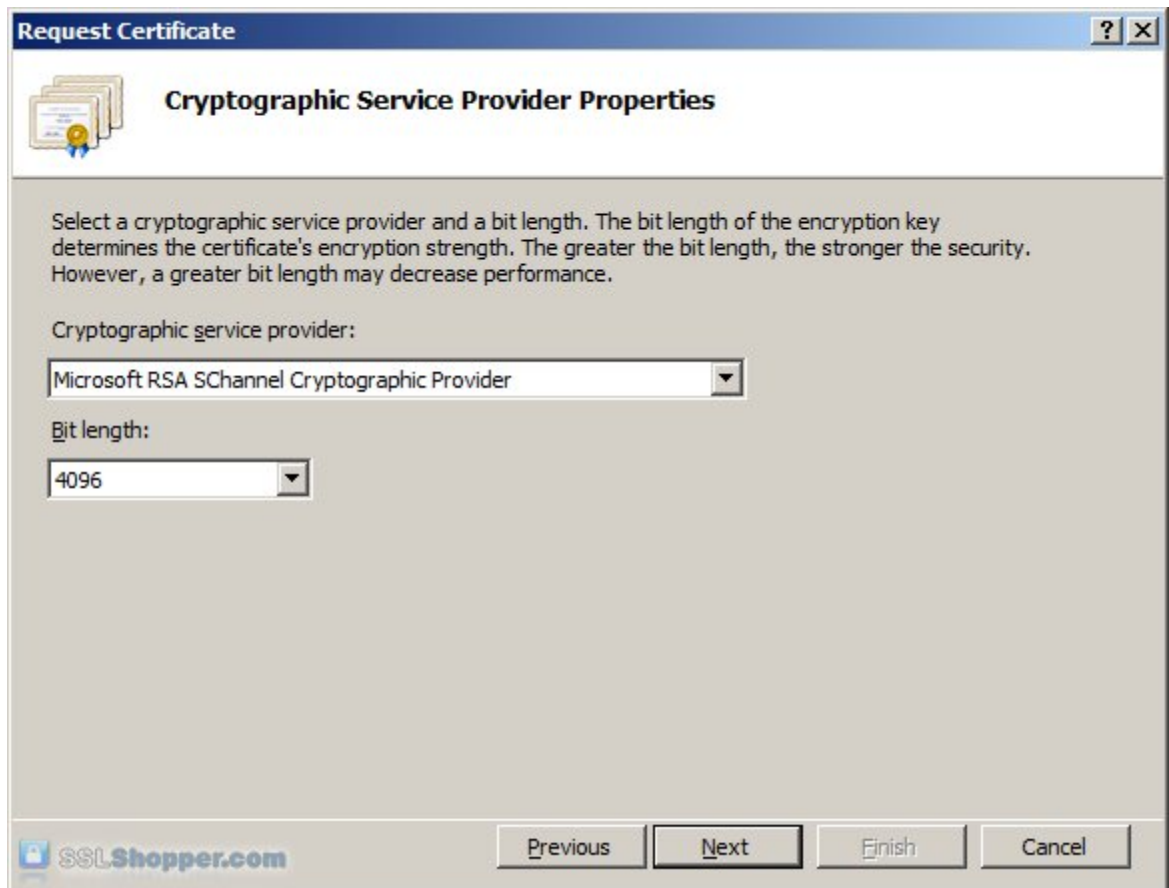
The screenshot shows the 'Request Certificate' dialog box with the 'Distinguished Name Properties' tab selected. The dialog contains the following text: 'Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.' Below this text are several input fields:

Common name:	google.com
Organization:	Google, Inc.
Organizational unit:	Web
City/locality:	Mountain View
State/province:	California
Country/region:	US

At the bottom of the dialog, there are four buttons: 'Previous', 'Next' (highlighted), 'Finish', and 'Cancel'. The status bar at the bottom shows 'SSLShopper.com'.

Name	Explanation	Examples
Common Name	The fully qualified domain name (FQDN) of your server. This must match exactly what you type in your web browser or you will receive a <a href="#">name mismatch error</a> .	*.google.com mail.google.com
Organization	The legal name of your organization. This should not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Google Inc.
Organizational Unit	The division of your organization handling the certificate. (Most CAs don't validate this field)	IT Web
City/Locality	The city where your organization is located.	Mountain View
State/province	The state/region where your organization is located. This shouldn't be abbreviated.	California
Country/Region	The two-letter ISO code for the country where your organization is location.	US GB

5. Leave the default Cryptographic Service Provider. Increase the Bit length to 2048 bit or higher. Click Next.



**Request Certificate**

**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.

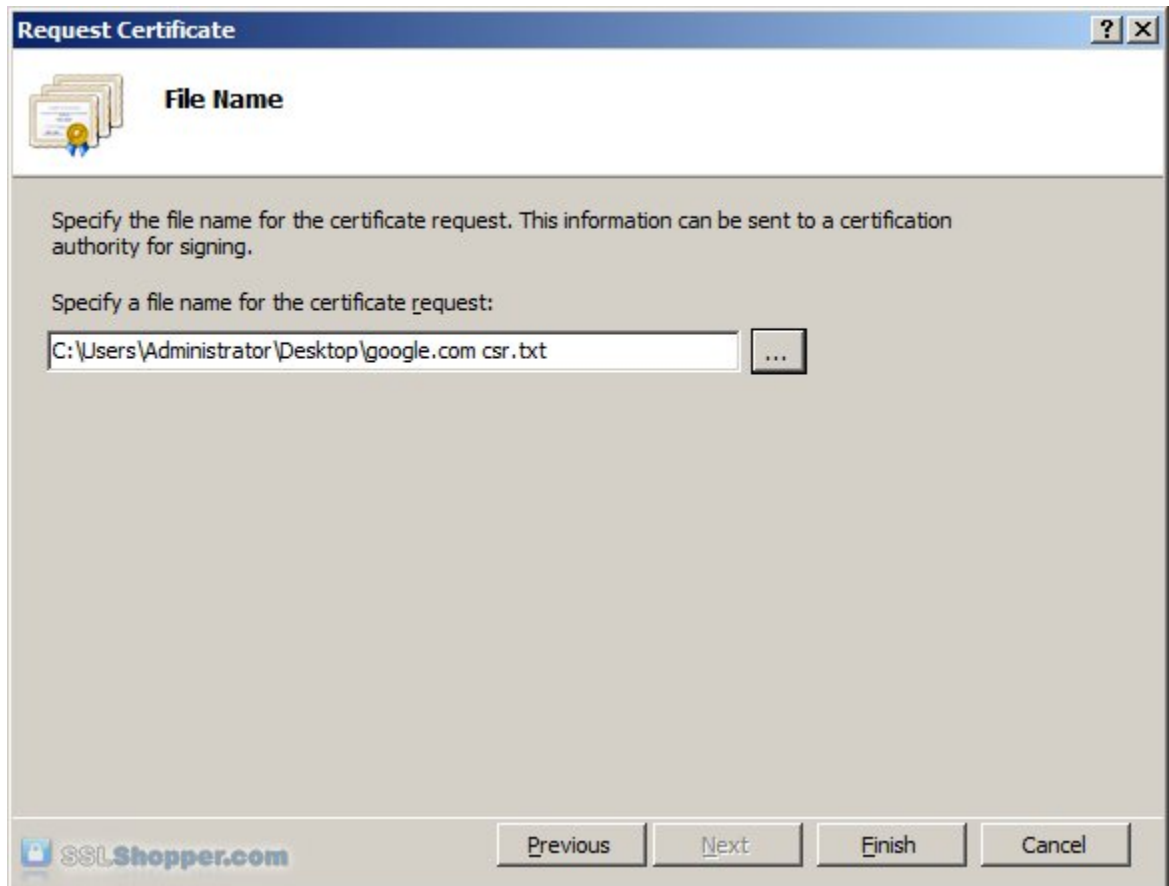
Cryptographic service provider:

Bit length:

SSLShopper.com

Previous Next Finish Cancel

6. Click the button with the three dots and enter a location and filename where you want to save the CSR file. Click Finish.

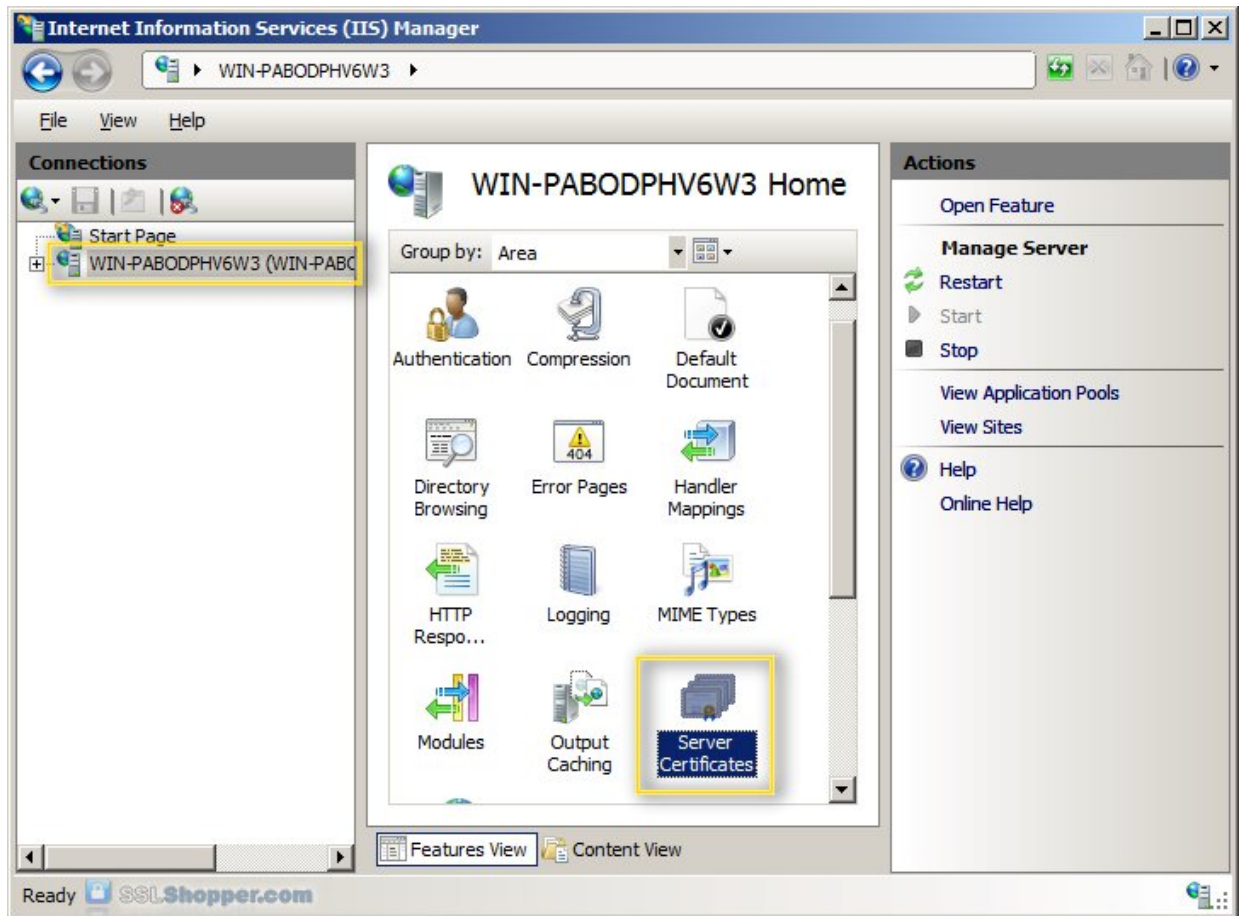


Once you have generated a CSR you can use it to order the certificate from a [certificate authority](#). If you don't already have a favorite, you can [compare SSL](#) features from each provider using our SSL Wizard or by comparing [cheap SSL certificates](#), [Wildcard Certificates](#), or [EV certificates](#). Once you paste the contents of the CSR and complete the ordering process, your order is validated, and you will receive the SSL certificate file.

### Install the Certificate

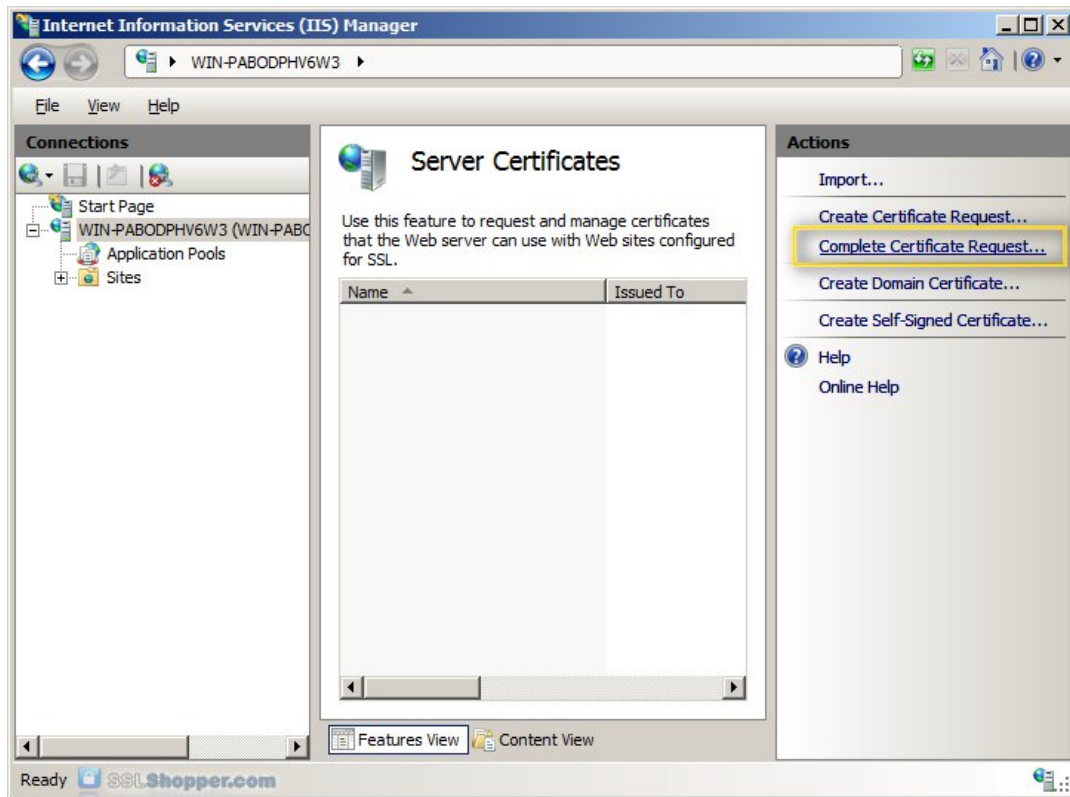
To install your newly acquired SSL certificate in IIS 7, first copy the file somewhere on the server and then follow these instructions:

1. Click on the Start menu, go to Administrative Tools, and click on Internet Information Services (IIS) Manager.
2. Click on the name of the server in the Connections column on the left. Double-click on Server Certificates.



3. In the Actions column on the right, click on Complete Certificate Request...

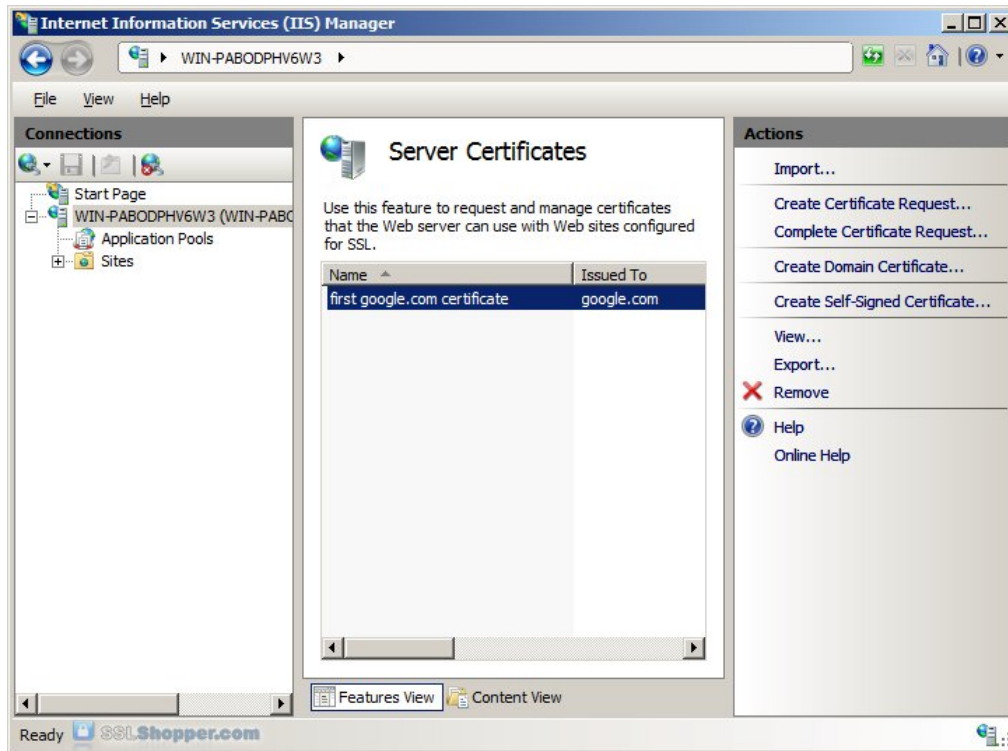




4. Click the button with the three dots and select the server certificate that you received from the certificate authority. If the certificate doesn't have a .cer file extension, select to view all types. Enter any friendly name you want so you can keep track of the certificate on this server. Click OK.



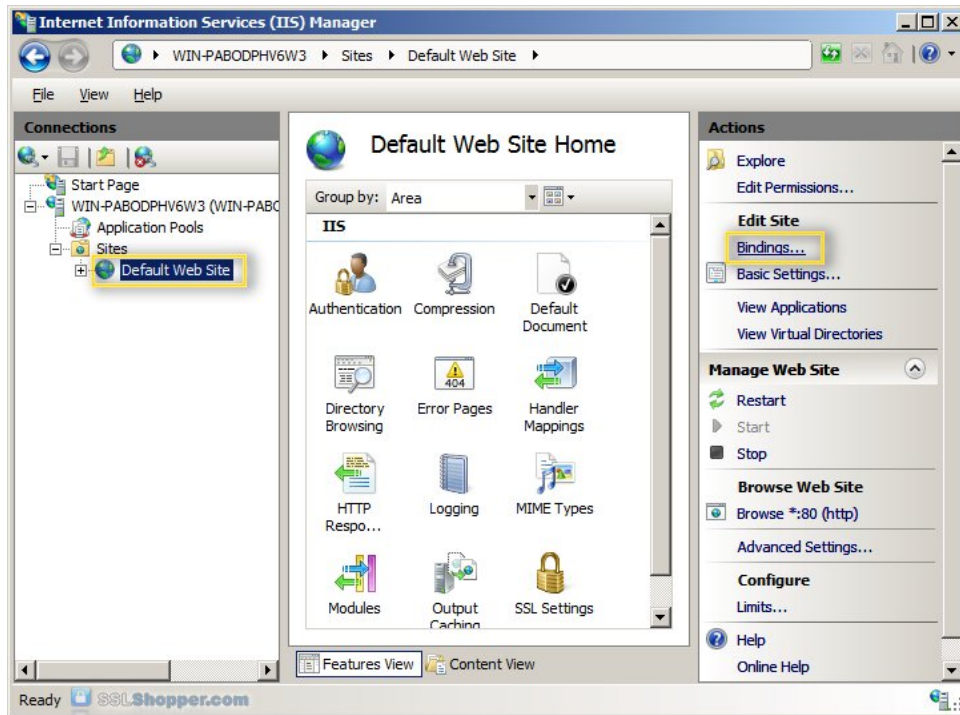
5. If successful, you will see your newly installed certificate in the list. If you receive an error stating that the request or private key cannot be found, make sure you are using the correct certificate and that you are installing it to the same server that you generated the CSR on. If you are sure of those two things, you may just need to create a new Certificate Request and reissue/replace the certificate. Contact your certificate authority if you have problems with this.



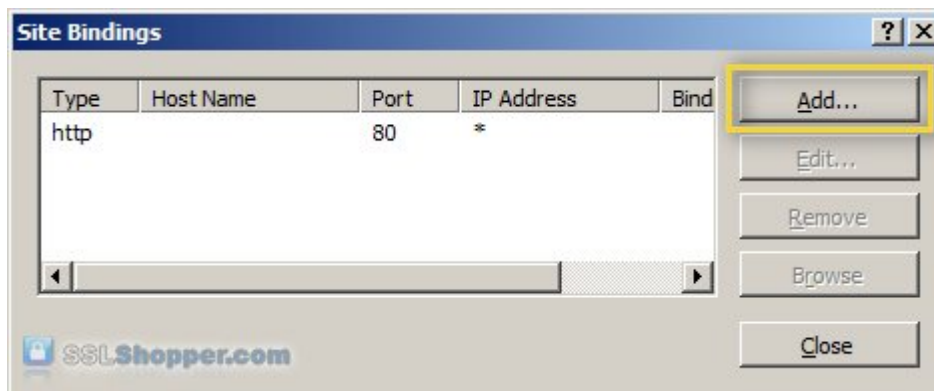
Bind the Certificate to a website

1. In the Connections column on the left, expand the sites folder and click on the website that you want to bind the certificate to. Click on Bindings... in the right column.





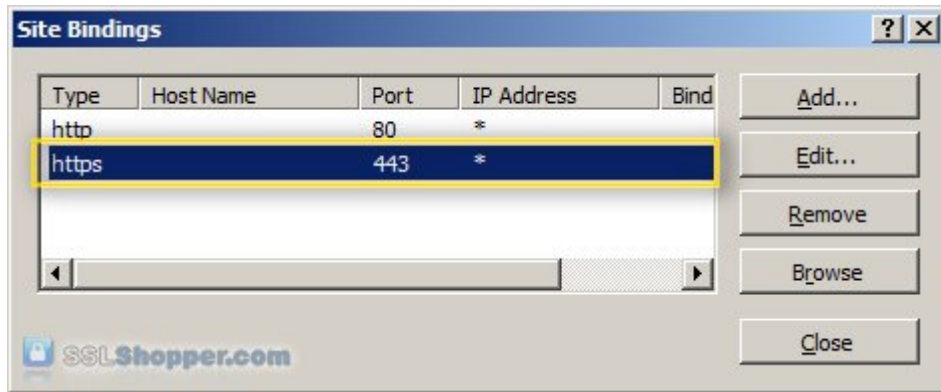
2. Click on the Add... button.



3. Change the Type to https and then select the SSL certificate that you just installed. Click OK.



4. You will now see the binding for port 443 listed. Click Close.



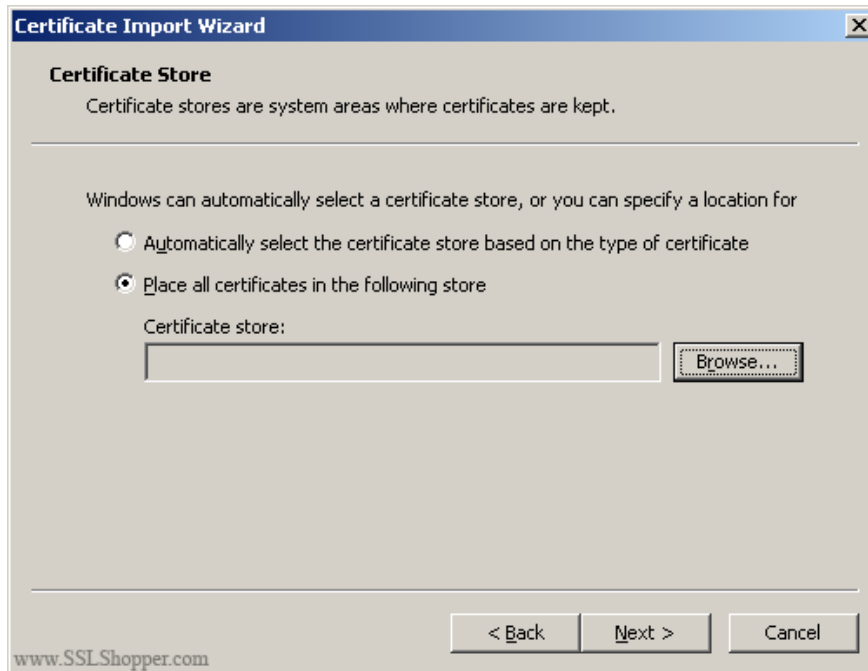
### Install any Intermediate Certificates

Most SSL providers issue server certificates off of an Intermediate certificate so you will need to install this Intermediate certificate to the server as well or your visitors will receive a [Certificate Not Trusted Error](#). You can install each Intermediate certificate (sometimes there is more than one) using these instructions:

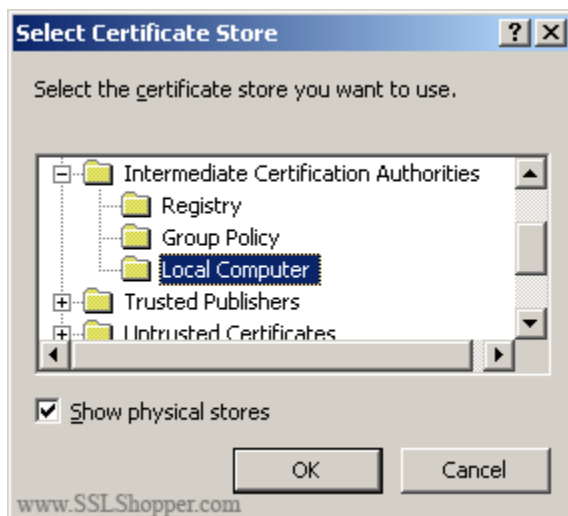
1. Download the intermediate certificate to a folder on the server.
2. Double click the certificate to open the certificate details.
3. At the bottom of the General tab, click the Install Certificate button to start the certificate import wizard. Click Next.



4. Select Place all certificates in the following store and click Browse.



5. Check the Show physical stores checkbox, then expand the Intermediate Certification Authorities folder, select the Local Computer folder beneath it. Click OK. Click Next, then Finish to finish installing the intermediate certificate.



You may need to restart IIS so that it starts giving out the new certificate. You can verify that the certificate is installed correctly by visiting the site in your web browser using https instead of http or using our [SSL Checker](#).

## IIS7 Redirect HTTP to HTTPS

Redirecting all traffic from HTTP to HTTPS in IIS7 will make sure your users always access the site securely. There are many different ways to set up an IIS7 Redirect from HTTP to HTTPS and some are better than others. The ideal HTTP to HTTPS redirect would do the following:

- Gently redirect users to HTTPS so users don't have to type in "https" in the URL
- Redirect users to the specific page that they were going to go to on HTTP (page.htm)
- Save any variables passed in the query string (?page=2)
- Work in all browsers
- Transfer PageRank to the redirected page by using a 301 redirect, maintaining SEO
- Allow specific parts of a site to force SSL but allow HTTP on other parts of the site
- Redirect users from mydomain.com to www.mydomain.com

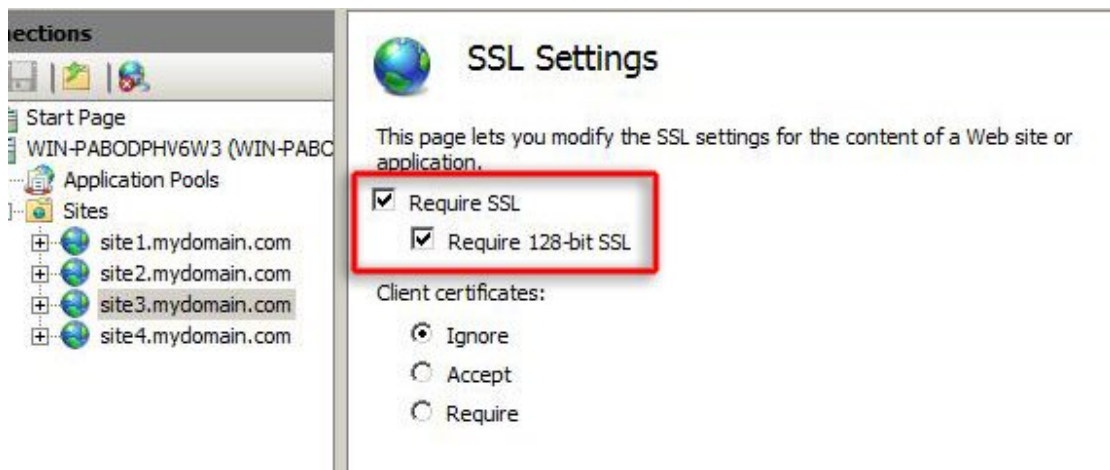
Unfortunately, there isn't an easy way to satisfy all of these requirements, and most methods only satisfy a few of them. The best method of doing an HTTP to HTTPS redirect I've seen involves using [ASP.Net to do the HTTP to HTTPS redirection](#).

But most people don't need all of those features, so I have listed two of the best methods of redirecting HTTP to HTTPS in IIS 7. They are easy to set up and effective in most situations.

### Method 1 – Using Microsoft URL Rewrite Module

For this method of redirecting from HTTP to HTTPS, you will need to do the following;

1. Install the [Microsoft URL Rewrite Module](#)
2. [Install your SSL certificate in IIS 7](#) and bind it to your website
3. Make sure Require SSL is NOT checked under SSL Settings for your website (uncheck the boxes that are checked in this screenshot)



4. Copy and paste the following code between the <rules> and </rules> tags in your web.config file in your website root directory.

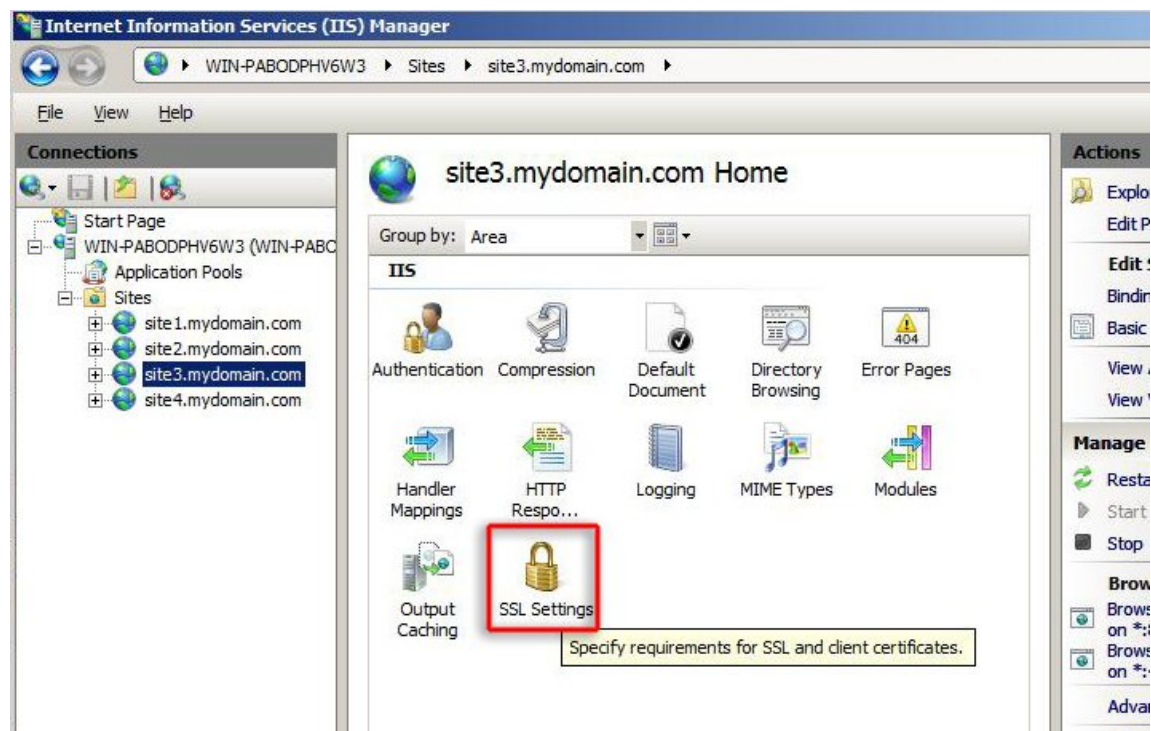
```
<rule name="HTTP to HTTPS redirect" stopProcessing="true">
  <match url="(.*)" />
  <conditions>
    <add input="{HTTPS}" pattern="off" ignoreCase="true" />
  </conditions>
  <action type="Redirect" redirectType="Found" url="https://{HTTP_HOST}/{R:1}" />
</rule>
```

5. Test the site by going to <http://www.yoursite.com> and making sure it redirects

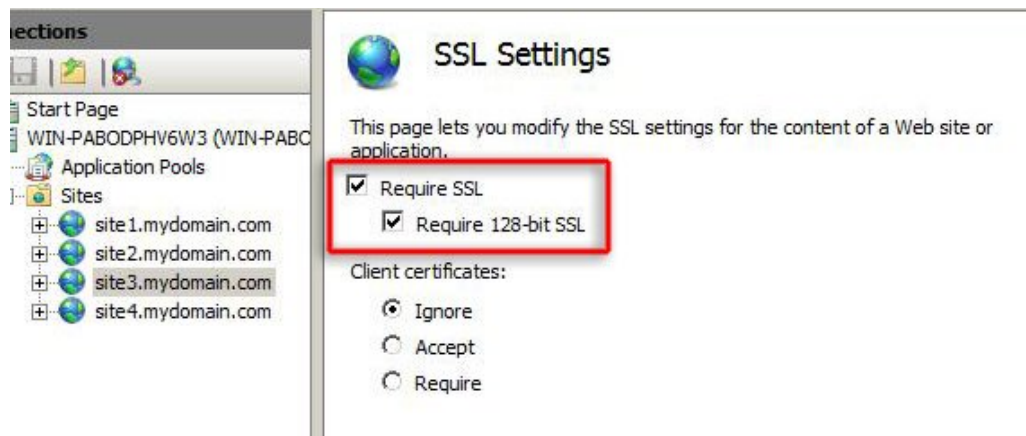
## Method 2 – Setting up a Custom Error Page

The second method of setting up an IIS7 redirect HTTP to HTTPS is to Require SSL on the site or part of the site and set up a custom 403.4 error page. To do this, just following these steps:

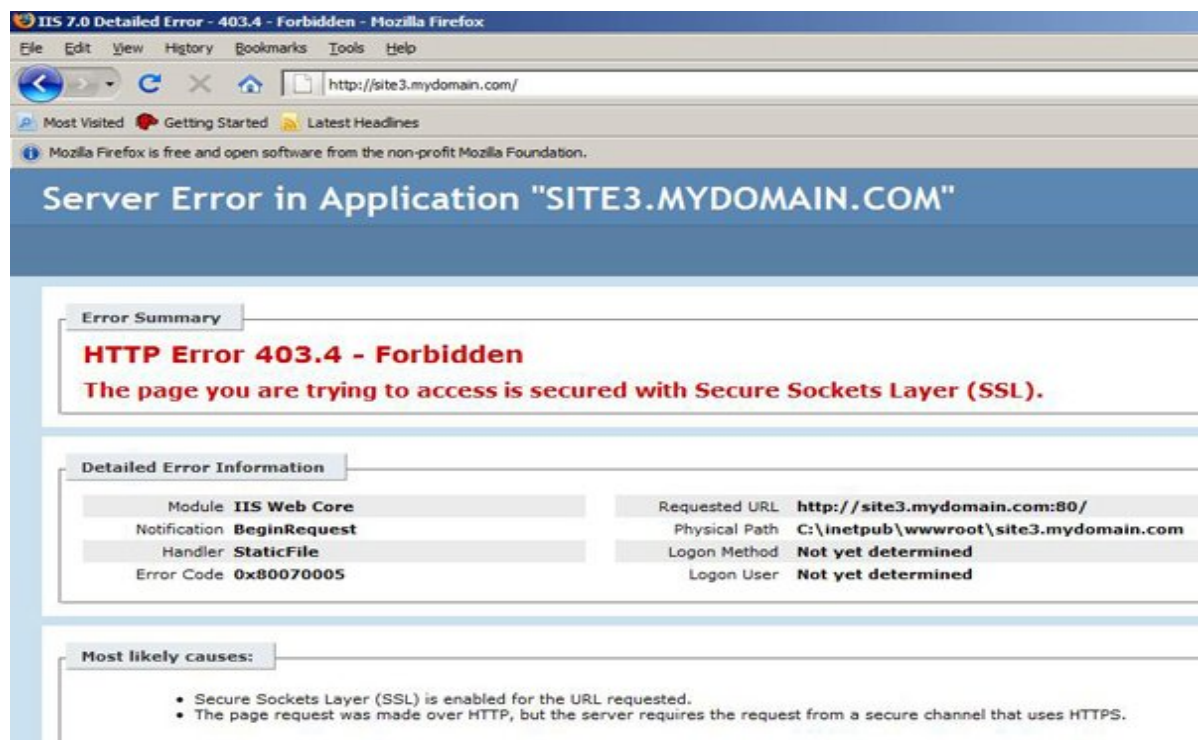
1. [Install your SSL certificate in IIS 7](#) and bind it to your website
2. In IIS, click on the site name, and go to the SSL Settings section



3. Check Require SSL and Require 128-bit SSL and click Apply



4. After doing this, users will normally receive this error:



5. Create a new text file and paste the following into it:

```
<html>
<head><title>Redirecting...</title></head>
<script language="JavaScript">
function redirectHttpToHttps()
{
    var httpURL= window.location.hostname + window.location.pathname +
window.location.search;
    var httpsURL= "https://" + httpURL;
```

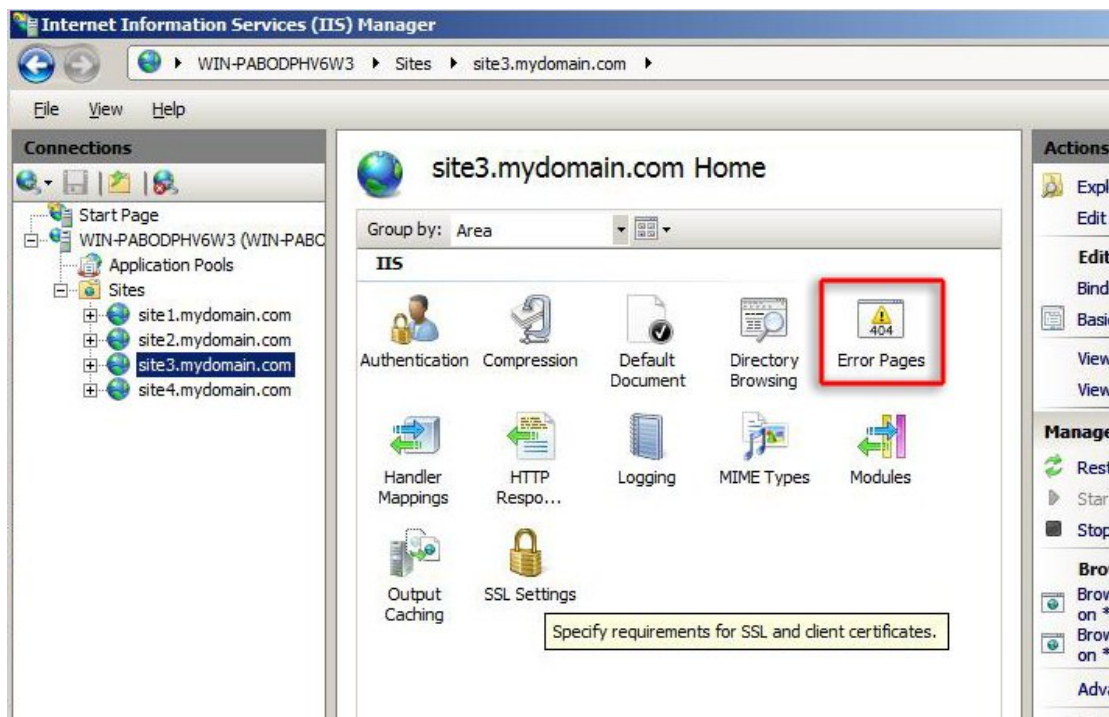


```

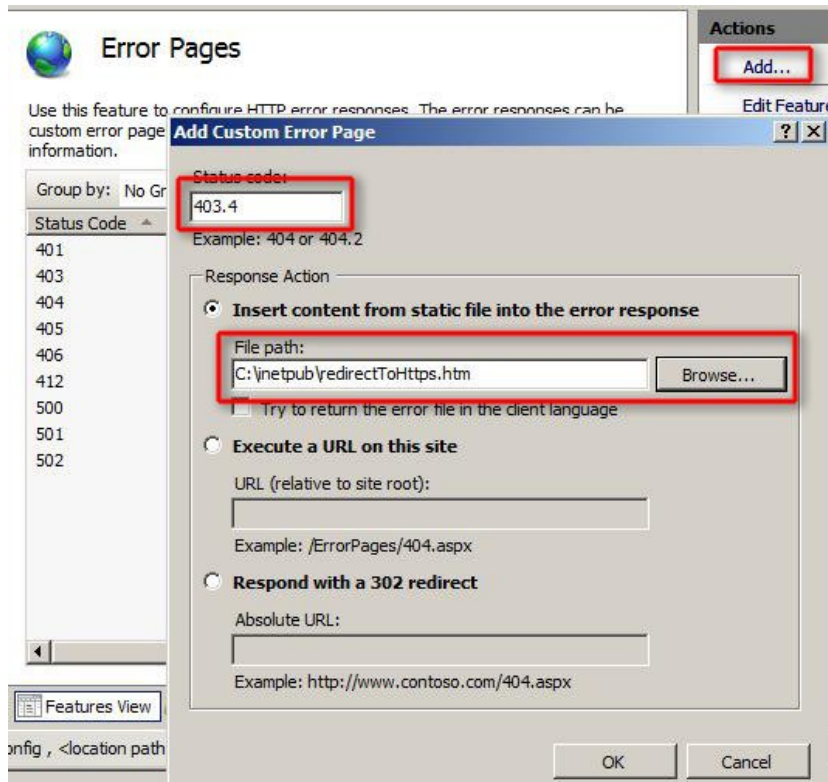
    window.location = httpsURL;
}
redirectHttpToHttps();
</script>
<body>
</body>
</html>

```

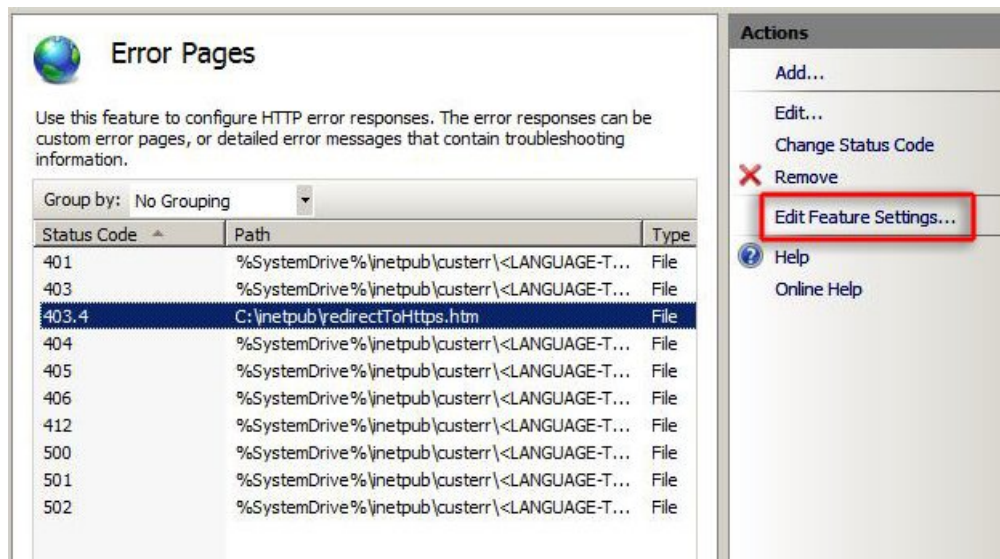
6. Save the file as redirectToHttps.htm in your C:\inetpub directory
7. Back in IIS, click on the site name and double-click the Error Pages option



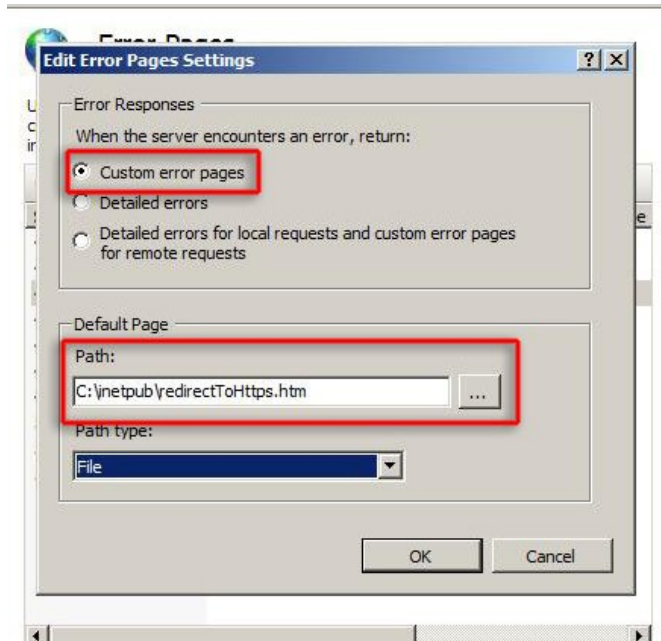
8. Click Add... and enter 403.4 as the Status code. Browse for the redirectToHttps.htm file you just created and click OK



9. Select the error code and press Edit Feature Settings...



10. Click the Custom error pages option and again browse for the redirectToHttps.htm file



11. Test the site by going to <http://www.yoursite.com> and making sure it redirects

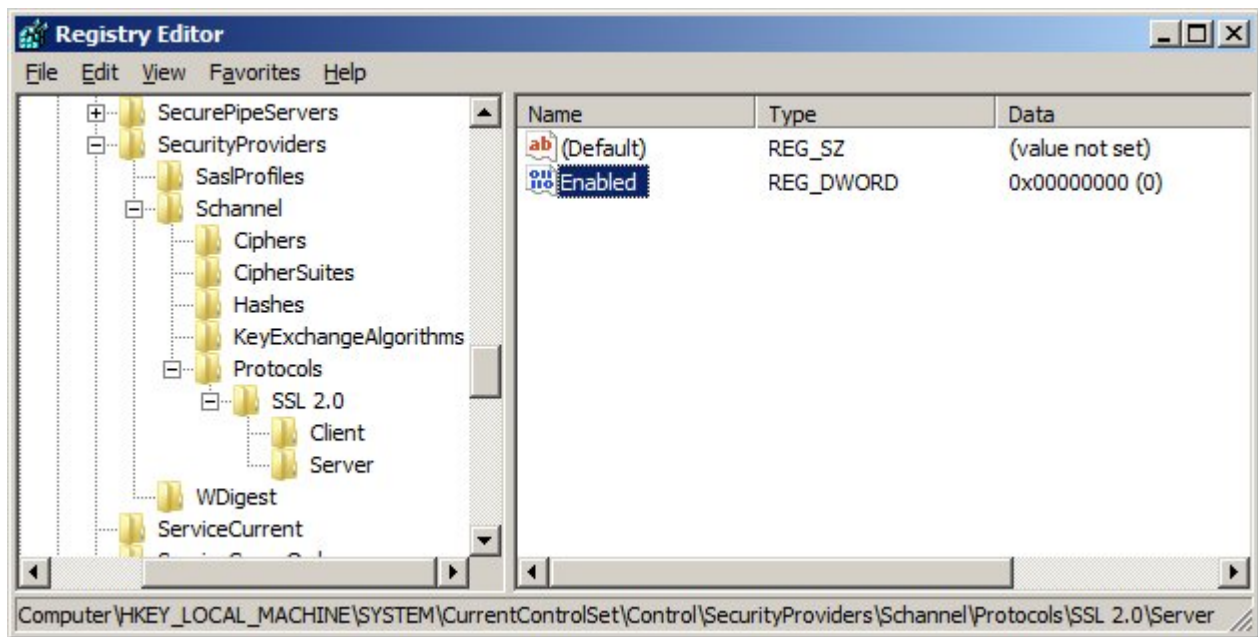
A caveat of using a custom error page to do an IIS7 redirect from HTTP to HTTPS is that the web browser must have JavaScript enabled for the redirection to work.

## How to Disable SSL 2.0 and SSL 3.0 in IIS 7

Windows Server 2008 using IIS 7 allows SSL 2.0 and SSL 3.0 by default. Unfortunately, this means you will fail a [PCI Compliance scan](#) by default. To properly secure your server and ensure that you pass your PCI-DSS scans, you will need to disable SSL 2.0 and disable weak ciphers. In order to disable SSL 2.0 and SSL 3.0 in IIS 7 and make sure that the stronger TLS 1.0 is used, follow these instructions:

1. Click Start, click Run, type regedit, and then click OK.
2. In Registry Editor, locate the following registry key/folder:  
  
HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANN  
EL\Protocols
3. Right-click on the SSL 2.0 folder and select New and then click Key. Name the new folder Server.
4. Inside the Server folder, click the Edit menu, select New, and click DWORD (32-bit) Value.
5. Enter Enabled as the name and hit Enter.
6. Ensure that it shows 0x00000000 (0) under the Data column (it should by default). If it doesn't, right-click and select Modify and enter 0 as the Value data.

7. Now to disable SSL 3.0, right-click on the SSL 3.0 folder and select New and then click Key. Name the new folder Server.
8. Inside the Server folder, click the Edit menu, select New, and click DWORD (32-bit) Value.
9. Enter Enabled as the name and hit Enter.
10. Ensure that it shows 0x00000000 (0) under the Data column (it should by default). If it doesn't, right-click and select Modify and enter 0 as the Value data.
11. Restart the computer.
12. Verify that no SSL 2.0 or SSL 3.0 ciphers are available at [ServerSniff.net](http://ServerSniff.net) or the [Public SSL Server Database](http://PublicSSLServerDatabase)



Note: This process is essentially the same on an IIS 6 (Windows Server 2003) machine. Normally, the Server key under SSL 2.0 will already be created so you will just need to create a new DWORD value under it and name it Enabled.

For more information, read Microsoft's Knowledge base [article on how to disable SSL 2.0 and other protocols in IIS 7](http://support.microsoft.com/kb/924451).

### [Compare SSL Certificates](#)

### Disable Weak Ciphers In IIS 7.0

In addition to disabling SSL 2.0, you can disable some weak ciphers by editing the registry in the same way. To speed up the process, you can paste the following in to a text file and name it disableWeakCiphers.reg, then double-click it.

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]

"Enabled"=dword:00000000

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client]

"DisabledByDefault"=dword:00000001