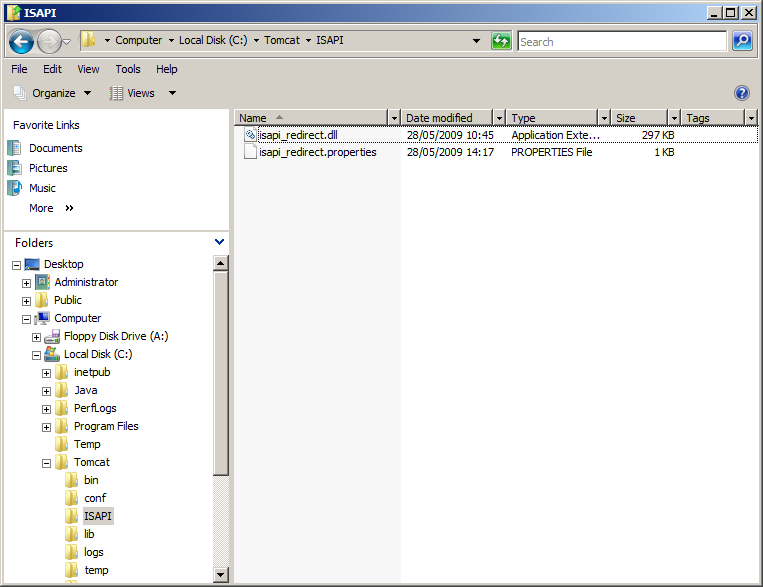
Tomcat 6.0, IIS7 and SSL

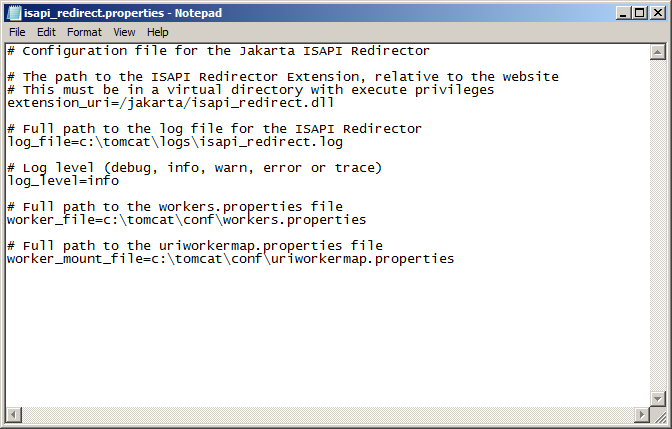
# Configure the JK 1.2 Connector

In this section we will configure the JK 1.2 Connector which will allow IIS to effectively act as a proxy and forward requests on to Tomcat. Start by creating a folder called ‘ISAPI’ under the Tomcat root folder. Then copy the isapi\_redirect-1.2.28.dll file into the ‘ISAPI’ folder and rename the file to isapi\_redirect.dll as shown here.



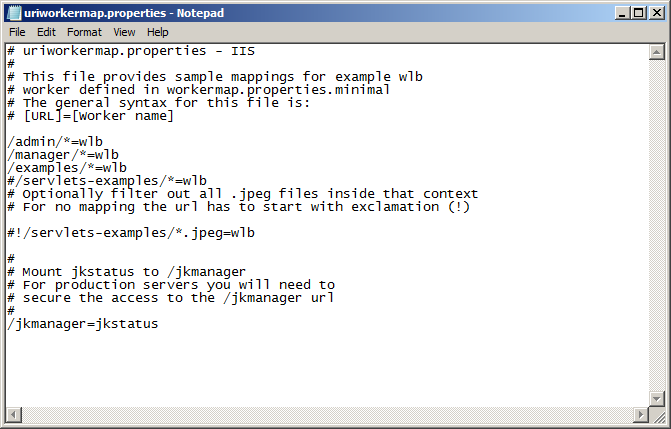
In order to configure the Tomcat connector you need to either add an entry in the Windows registry or you can use the isapi\_redirect.properties file. The isapi\_redirect.properties file tells the connector where to find its configuration files and also where the isapi\_redirect DLL file is located. If you have used the same directory structure as I have you can configure your isapi\_redirect.properties file as shown here.

The isapi\_redirect.properties file resides within the same directory that you placed the dll in, (**c:\tomcat\connector**).  workers.properties and uriworkmap.properties are placed inside the "conf" subdirectory, (for example, **c:\tomcat\connector\conf**).

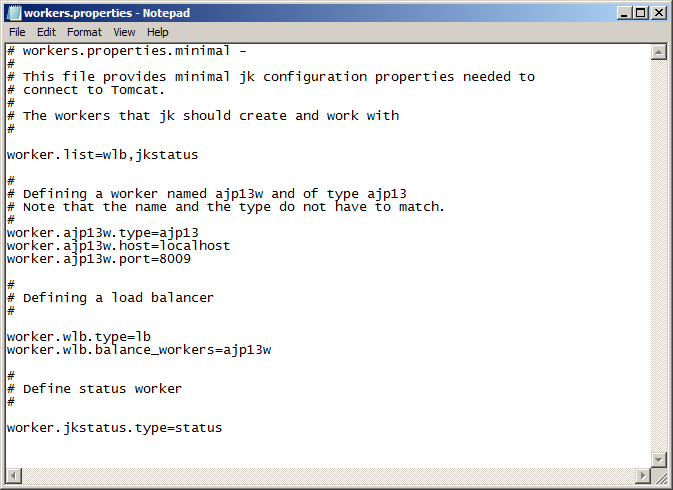


We also need to either update or create the two Tomcat connector configuration files (workers.properties and uriworkermap.properties) so that the connector knows how to handle the requests it receives. These configuration files are documented on the Tomcat web site here : [The Apache Tomcat Connector - Reference Guide](http://tomcat.apache.org/connectors-doc/index.html)

If you have just installed Tomcat with the sample applications then you can copy the sample uriworkermap.properties file shown here. Both config files need to placed in the Tomcat ‘conf’ folder which in this example is C:\Tomcat\conf

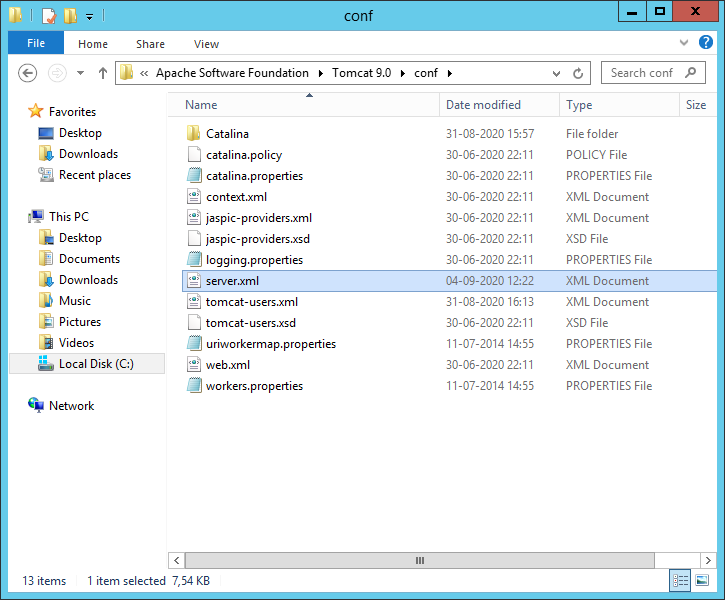


You can also copy the sample workers.properties file as shown below and save it to the C:\Tomcat\conf folder.

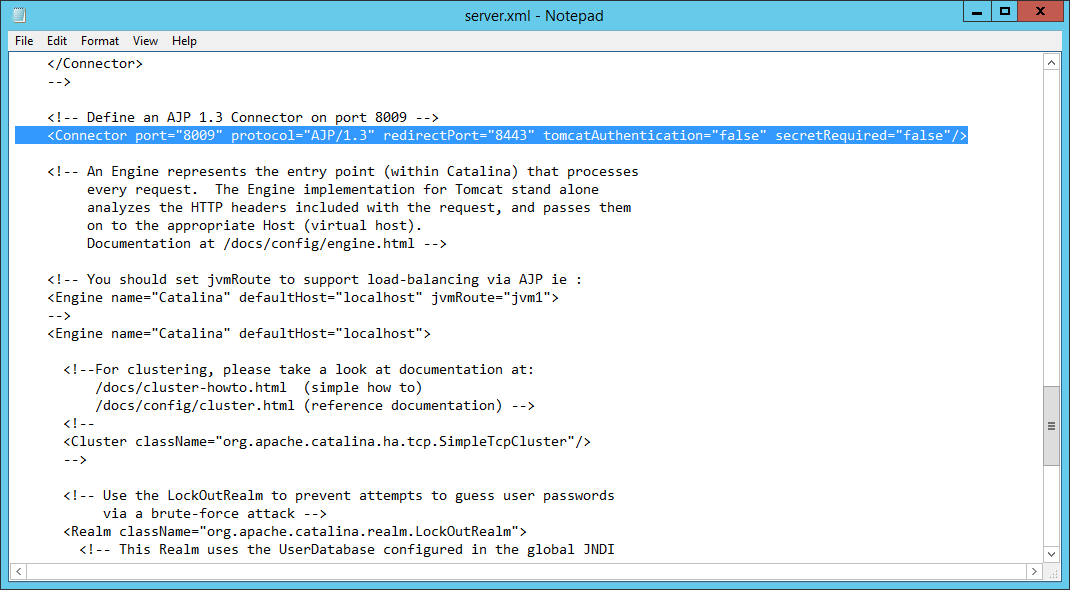


## Configure Tomcat server.xml

We also need to edit Tomcats server.xml file to enable the AJP connector port. The server.xml file is located in Tomcats /conf folder.



Open the server.xml file in a text editor and find the APJ connector port section



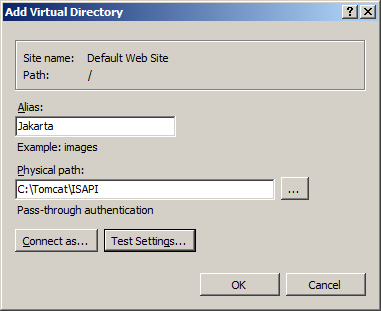
You should configure the connector like this:

<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" tomcatAuthentication="false" secretRequired="false"/>

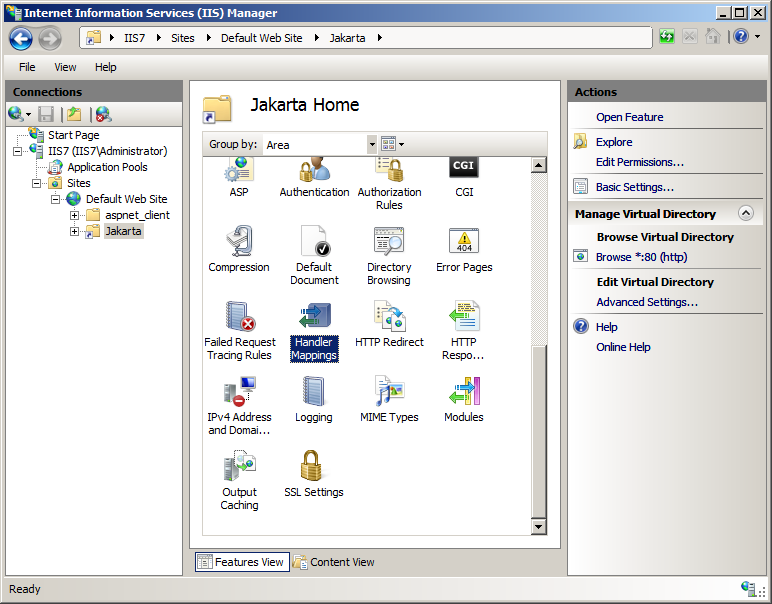
Save any changes you made and restart the Tomcat service.

## Configure the IIS Virtual Directory

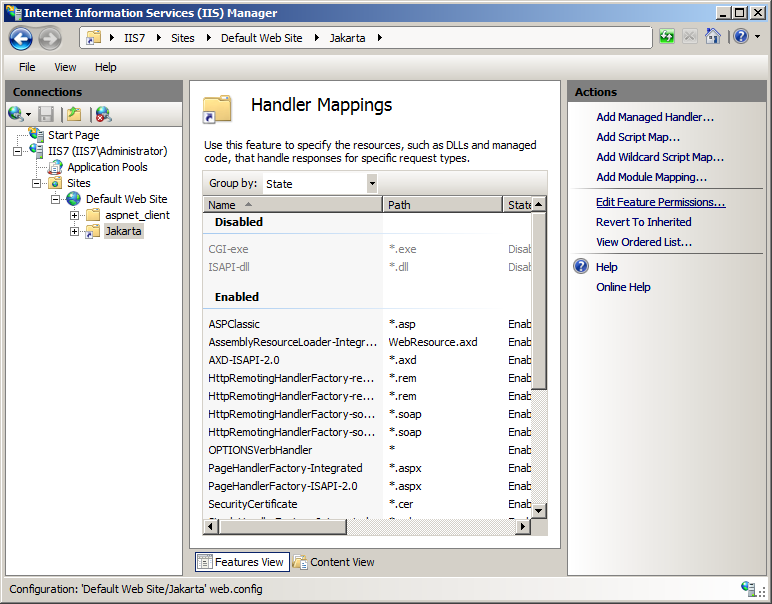
Now we need to configure IIS. Start by creating a virtual directory and give it an alias of ‘jakarta’ as shown here. Incidentally, you don’t have to call the virtual directory ‘jakarta’ - you can actually give it any name you like, just so long as the name you choose appears in the extension\_uri line of your isapi\_redirect.properties file.



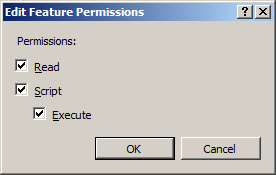
Next we need to configure the virtual directory to have execute permission. This was a simple tick-box option in IIS 6.0 but in IIS 7.0 we need to click on the Jakarta virtual directory and then double-click Handler Mappings.



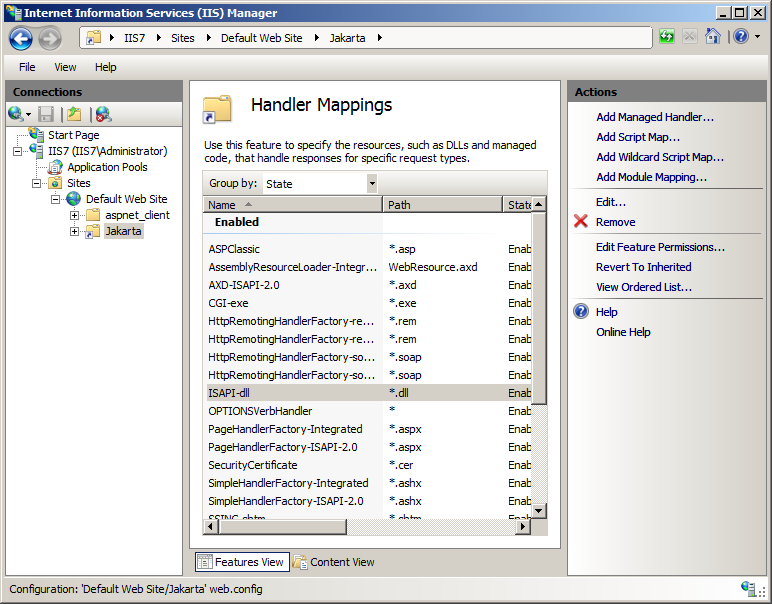
Within the Handler Mappings feature click Edit Feature Permissions in the Actions Pane.



Click Execute in the Edit Feature Permissions dialog box and click OK.

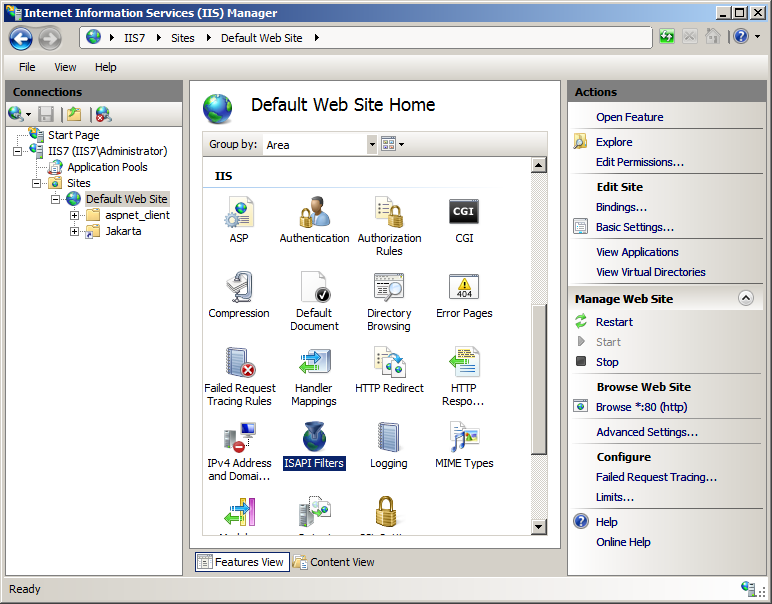


In the Handler Mappings feature you can now see that calls to ISAPI-dll files are enabled.

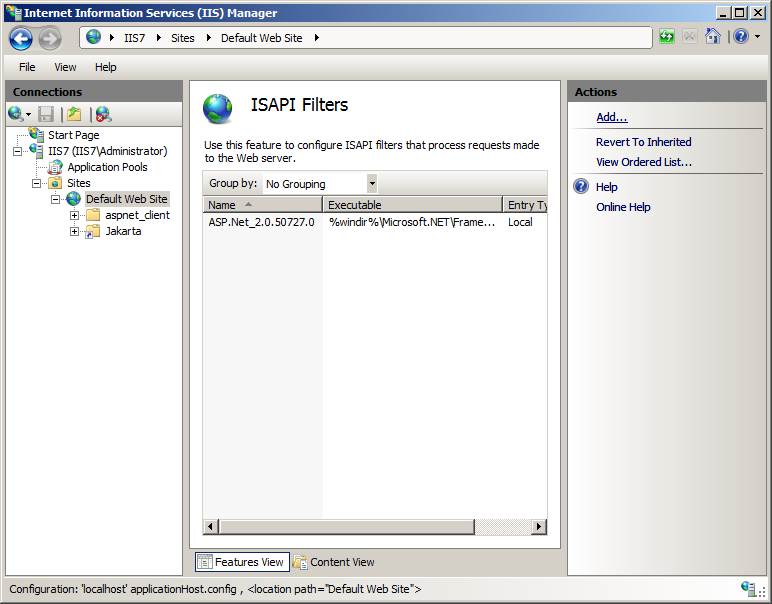


The next step is to add an ISAPI filter on the web site. To do this click on the web site and then double-click the ISAPI Filters feature.

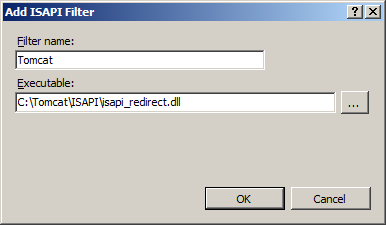
If the ISAPI Filters feature is not visible you must open the Server Manager and install the CGI, ISAPI Filters and restrictions features.



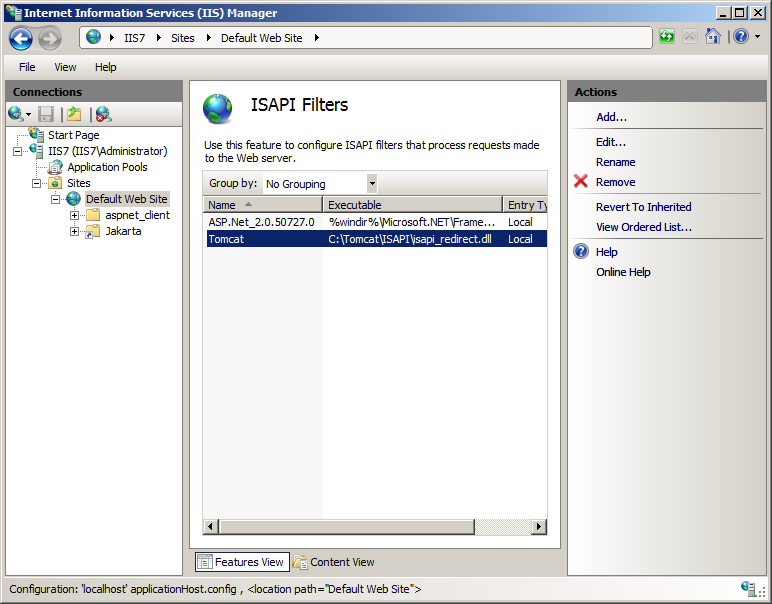
In the Actions pane click Add.



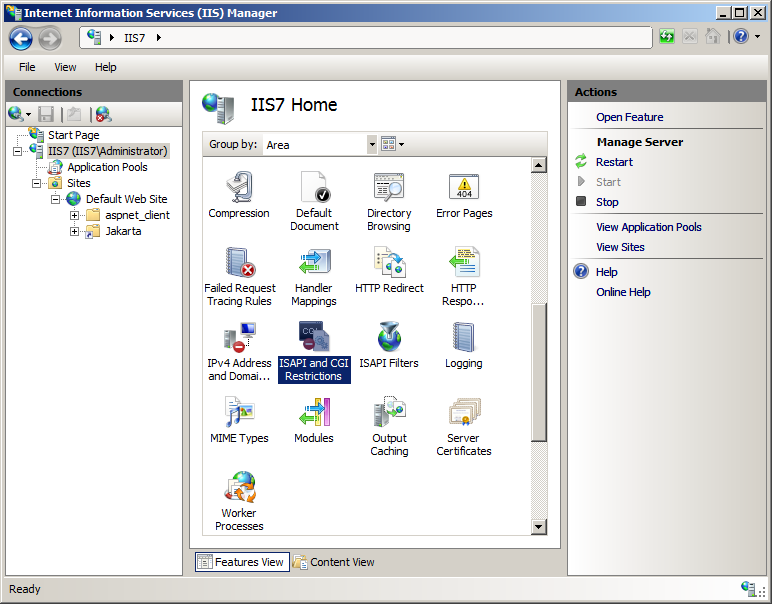
In the Add ISAPI Filter dialog box enter a name and the path to the isapi\_redirect.dll file and click OK.



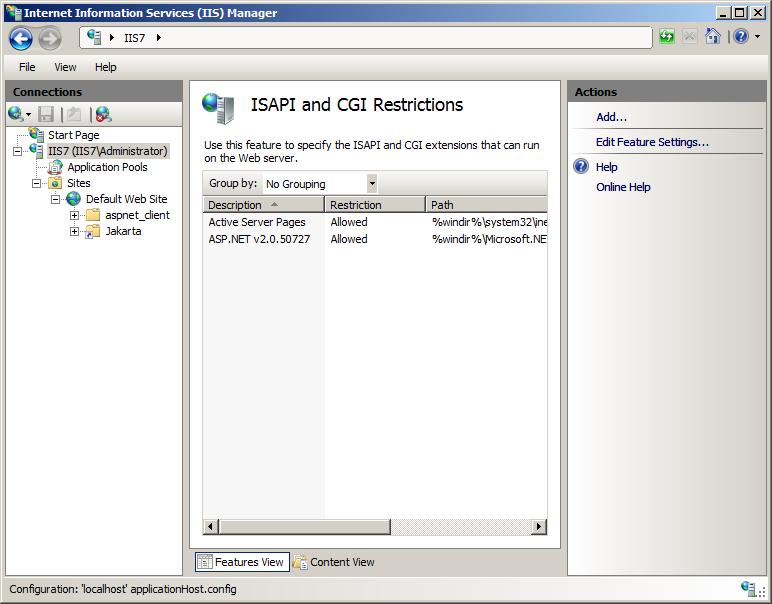
The Tomcat ISAPI filter should now appear in the ISAPI Filters list as shown here.



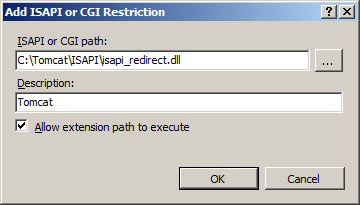
The final step we need to take is to configure the ISAPI and CGI Restrictions feature in IIS 7.0. This is analogous to adding or allowing a Web Service Extension in IIS 6.0. In IIS Manager navigate to the Server Home and then double-click on the ISAPI and CGI Restrictions feature.



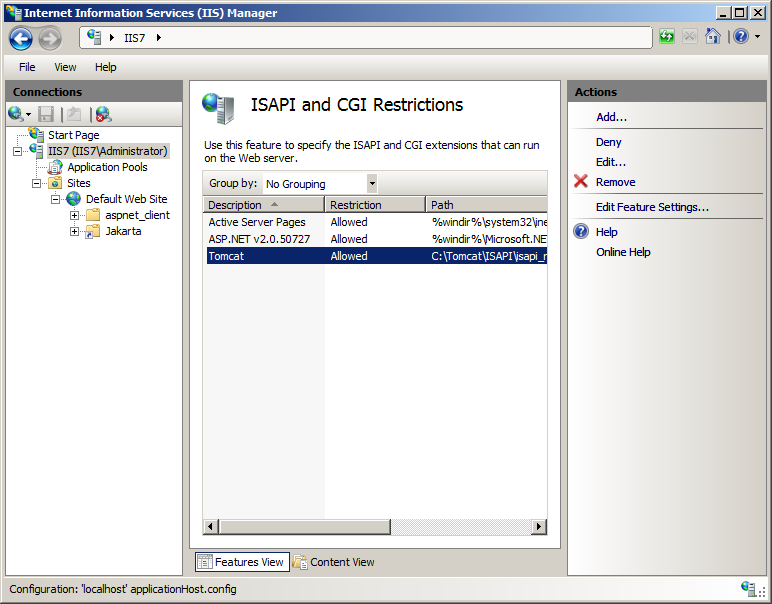
In the ISAPI and CGI Restrictions feature click Add on the Actions pane.



In the Add ISAPI or CGI Restriction dialog box enter a name and the path to the isapi\_redirect.dll file, tick the Allow extension path to execute option and click OK.



The Tomcat ISAPI extension should now appear in the list with a Restriction status of allowed as shown here.



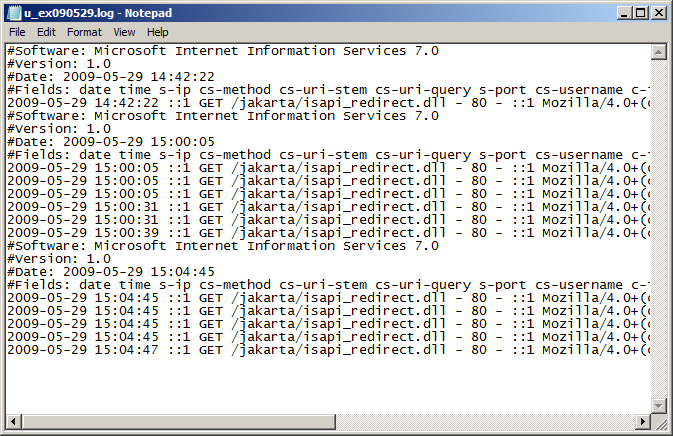
Everything we need to configure is now in place and we are ready to test. I started by requesting the ‘Hello World’ sample application from Tomcat directly on port 8080 with the result shown here.



The final step is to request the same ‘Hello World’ sample application using port 80 so that the request will be handled by IIS before being forwarded to Tomcat. If everything is configured correctly you should see the sample application load successfully as shown here.



If you now examine the IIS log file (which can be found in C:\inetpub\logs\LogFiles unless you moved it) you will see the request for the sample application being handled by IIS over port 80. One behaviour change that I have noticed is that the actual resource being requested isn’t logged with IIS 7.0 whereas it was in IIS 6.0, although I think this is likely to be a change in the bahviour of the ISAPI filter itself rather than any change in how IIS logs requests.

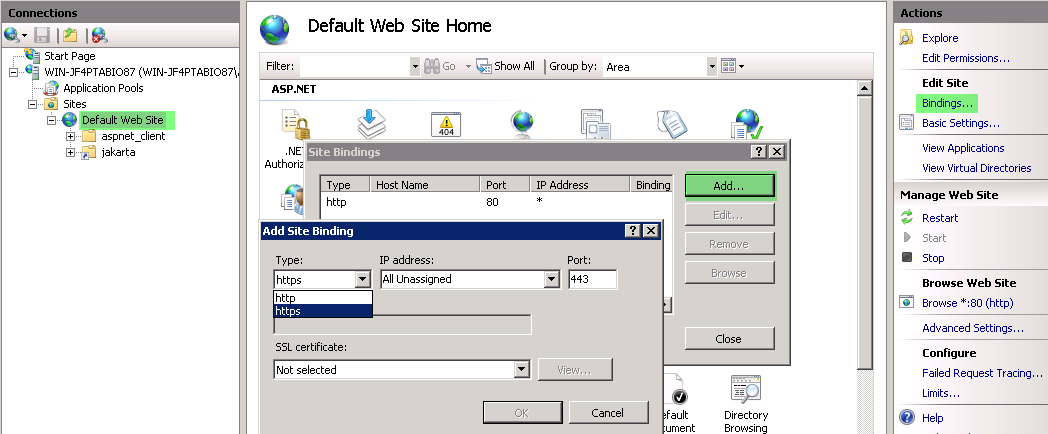


# Setup SSL

## Configure https in IIS

4. Select default website and click Bindings from the Actions bar. Then, Click Add

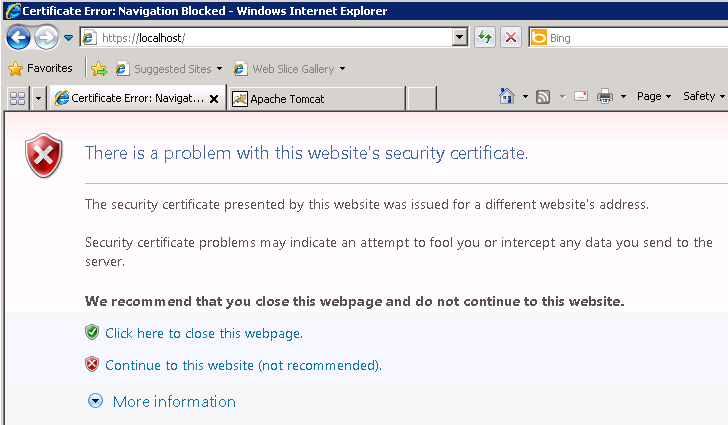
5. Select https from the Type

[](http://ashrafhossain.files.wordpress.com/2010/09/select-httpsbindings1.png)

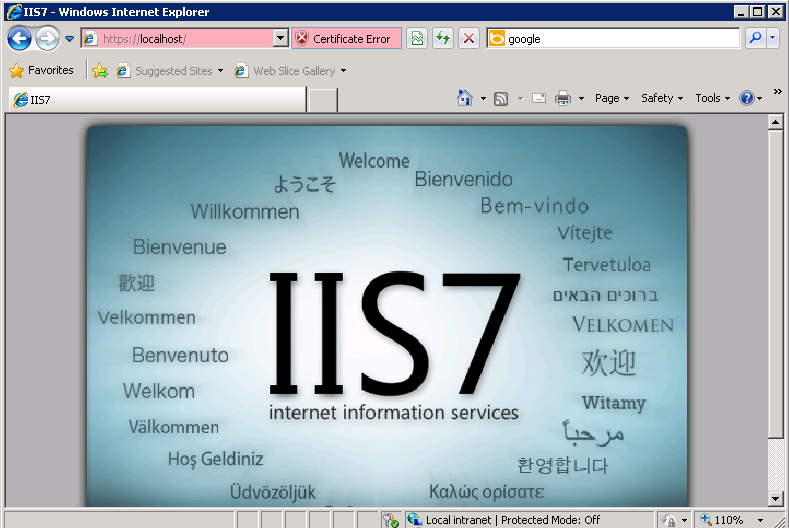
6. And Choose your SSL certificate 7. Click OK

## Test and Run

8. Restart IIS and test running [https://localhost](https://localhost/). It will show a problem loading the page.

[](http://ashrafhossain.files.wordpress.com/2010/09/https-prob.png)

Click “Continue to this website” and the site will appear in secure mode using https in lieu of [http.](http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol)

[](http://ashrafhossain.files.wordpress.com/2010/09/website-through-ssl.png)

## Configure https in Tomcat

Add require SSL to the Jakarta virtual directory. Click SSL settings and enable Require SSL.

### Configuring SSL with another port than 443

If you’ve selected to bind https to another port than 443 in your IIS website you have to tell Tomcat to use this port as well.

Edit the tomcat server.xml and change the SSL port from 8443 to the port you need.