Configuring Tomcat-Connector for IIS 7.0 (Windows Server 2008)

* Created by Joseph Clark [Atlassian], last modified by Husein Alatas [Atlassian] on Sep 25, 2012

This page is part of the installation guide for the **Confluence SharePoint Connector**. It tells you how to configure access to Confluence using Integrated Windows Authentication via IIS.

This section of the guide describes the steps necessary to set up an IIS website that will perform authentication using NTLM or Kerberos, and then forward the authenticated requests to the Confluence instance. You will do this by installing a custom ISAPI filter in IIS that understands how to use the AJP protocol (Apache JServ Protocol) to communicate with Confluence.

Si può leggere una spiegazione ulteriore e dettagliata al seguente link: Autenticazione integrata IIS

On this page:

Installation

Step 1. Install and Configure the AJP Connector

1. Download the latest Tomcat Connector ISAPI Filter binaries from the download page on apache.org, ensuring that you select the version that is appropriate for your operating system and CPU architecture. At the time this installation guide was written, the latest version was jk-1.2.31. Use the table below to help identify the correct download version for your server.

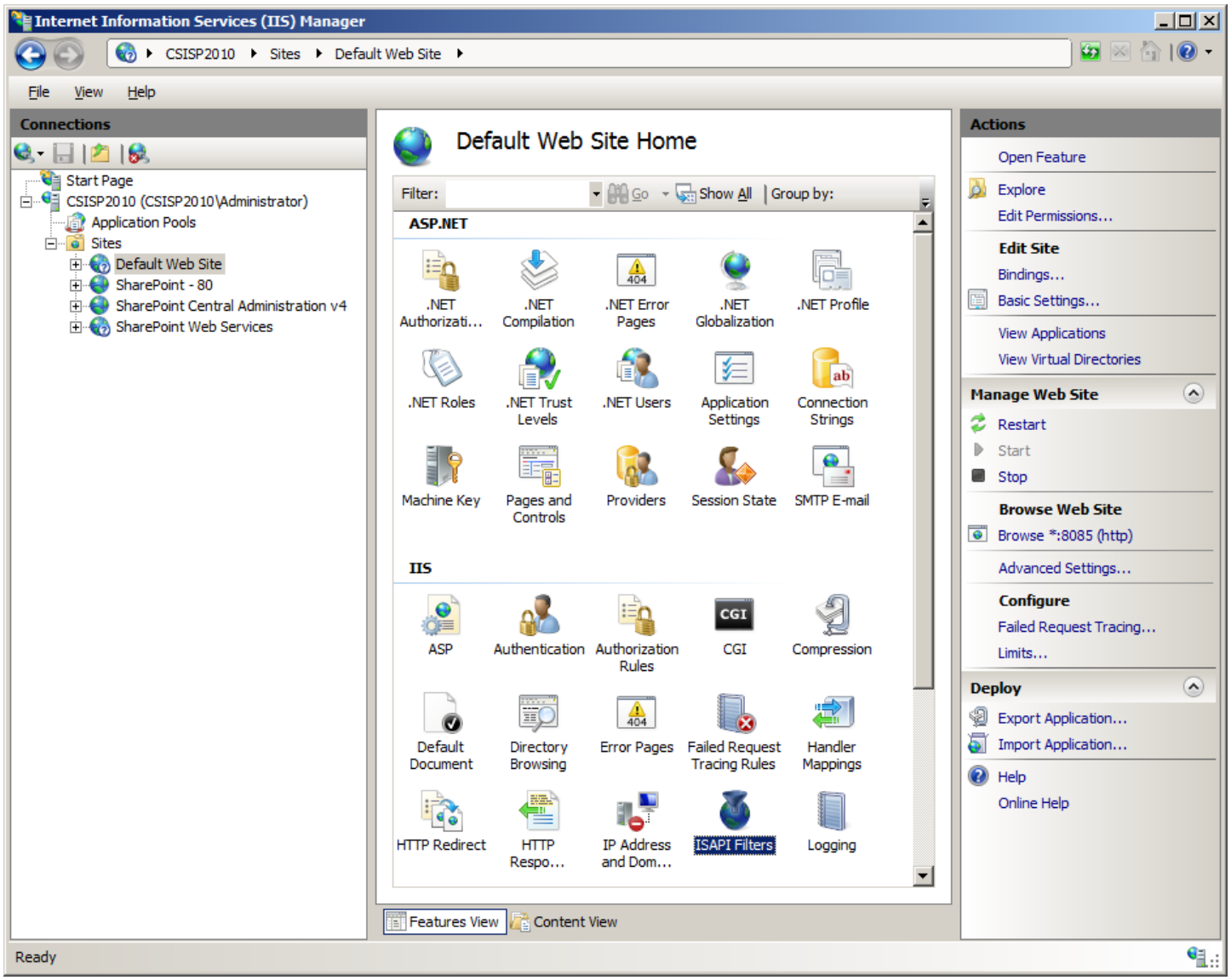
Operating System	Download Link
Windows Server 2008 x86 (32-bit)	win32
Windows Server 2008 x64 (64-bit)	win64-amd64

1. Download the **tomcat_iis_connector.zip** from links below. It contains the configuration files necessary for the ISAPI filter to run and communicate with your Confluence server.
2. Extract the downloaded zip file and place the contents in a folder alongside the downloaded binary file in a convenient location on your server. The default location is `C:\tomcat_iis_connector`.
3. Rename the downloaded binary file to **isapi_redirect.dll** (that is, remove the version number from the file name).
4. If you extracted the AJP Connector to a directory other than the default (`C:\tomcat_iis_connector`), then edit the **isapi_redirect.properties** file and ensure that the **log_file**, **worker_file**, **worker_mount_file** and **rewrite_rule_file** properties point to the correct locations.
5. If your Confluence server is not running on the same server as IIS (for example, if Confluence is running on a non-Windows server), then edit the **worker.properties.minimal** file in the **conf** directory so that the **worker.worker1.host** property points to the IP address or host name of your Confluence server.
6. If you wish to change the default port for Confluence's AJP Connector, then edit the **worker.properties.minimal** file in the **conf** directory and change the **worker.worker1.port** property to specify the required port number. The default port used in this guide for Confluence's AJP Connector is **8009**.

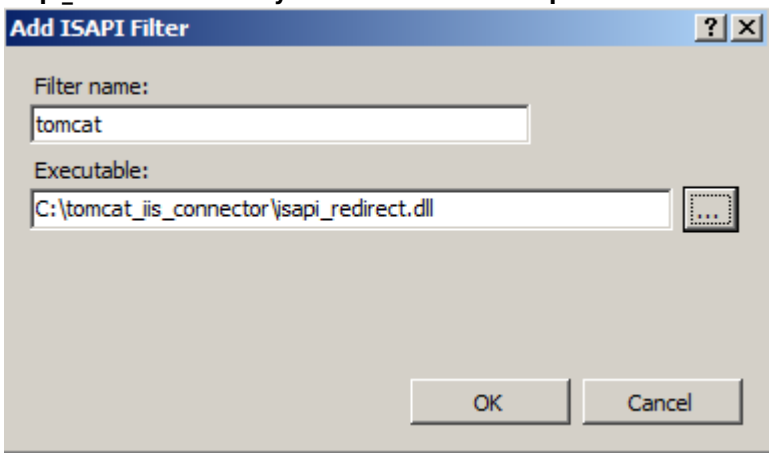
Step 2. Add ISAPI Filter

1. Open the **Internet Information Services (IIS) Manager**.
2. In the '**Connections**' panel, ensure that the IIS Web Site that will be used to proxy Confluence requests is selected.
3. Double-click the '**ISAPI Filters**' icon in '**Features View**'.

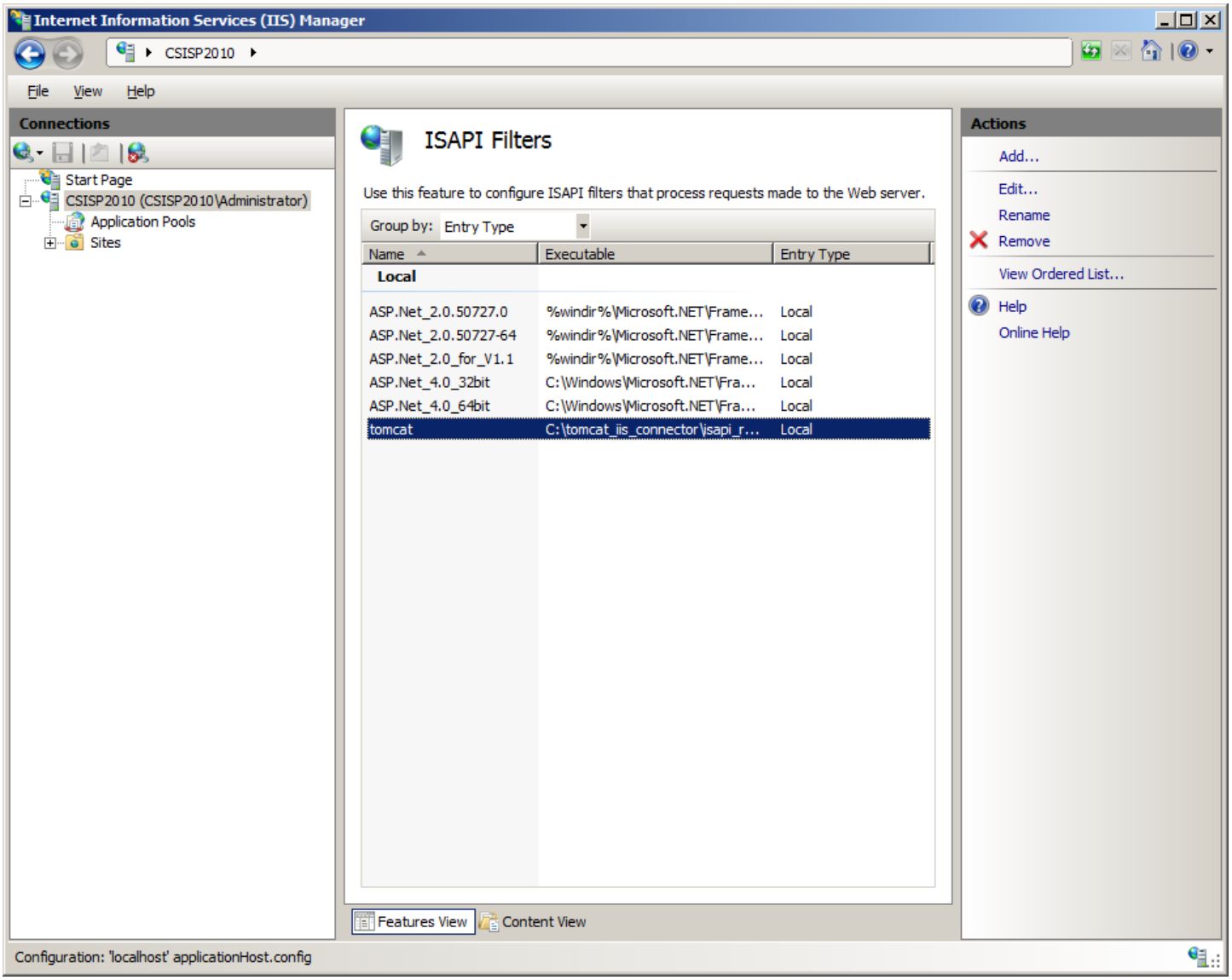
ATTENZIONE AI 64 BIT – In a 64 Bit environment - at least for IIS 7 - the used IIS Application Pool should have "Enable 32-bit Applications" set to "False". Otherwise the redirector will not be called and returns an http code 404. If you think, the 32bit version of isapi_redirect.dll would do the job instead, you will get an http code 500, because the library is not loadable into a 64 Bit IIS.



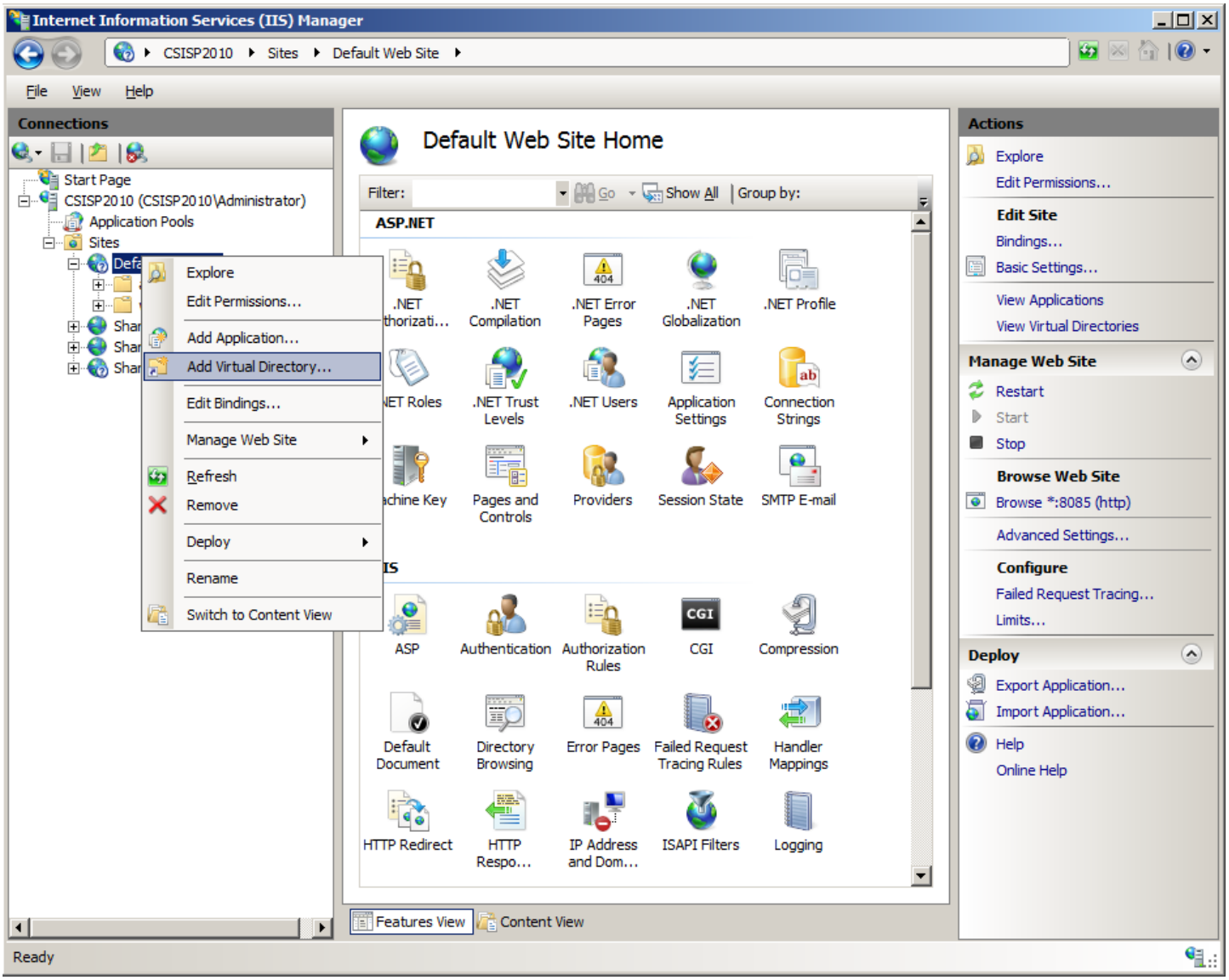
- In the 'Actions' **panel on the right, select** 'Add'**. - Set the** 'Filter name' **to 'tomcat' and set the** 'Executable' **to the isapi_redirect.dll that you downloaded in step 1.**



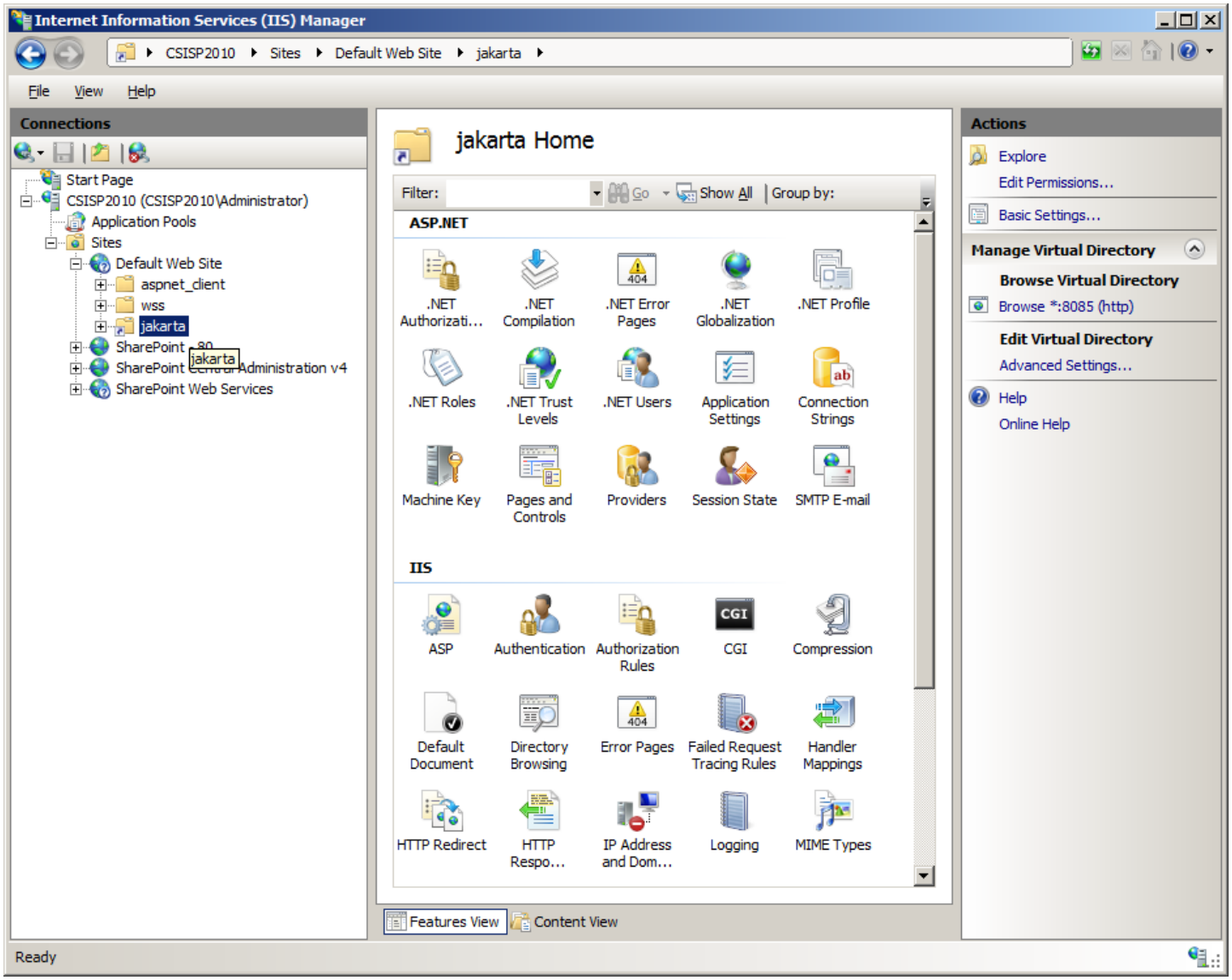
- Click 'OK'**. - The new filter should now be listed in the ISAPI Filters list for the website.**



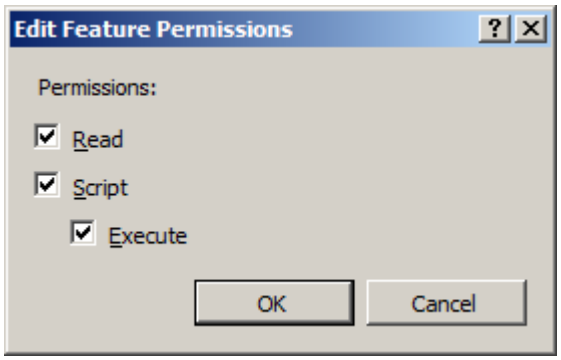
==== Step 3. Add Virtual Directory ==== Now you will add a virtual directory in the IIS website to host the ISAPI Filter. - In the 'Connections' **panel, ensure that the correct IIS Web Site is selected. - Right-click the IIS Web Site and select** 'Add Virtual Directory'**.**



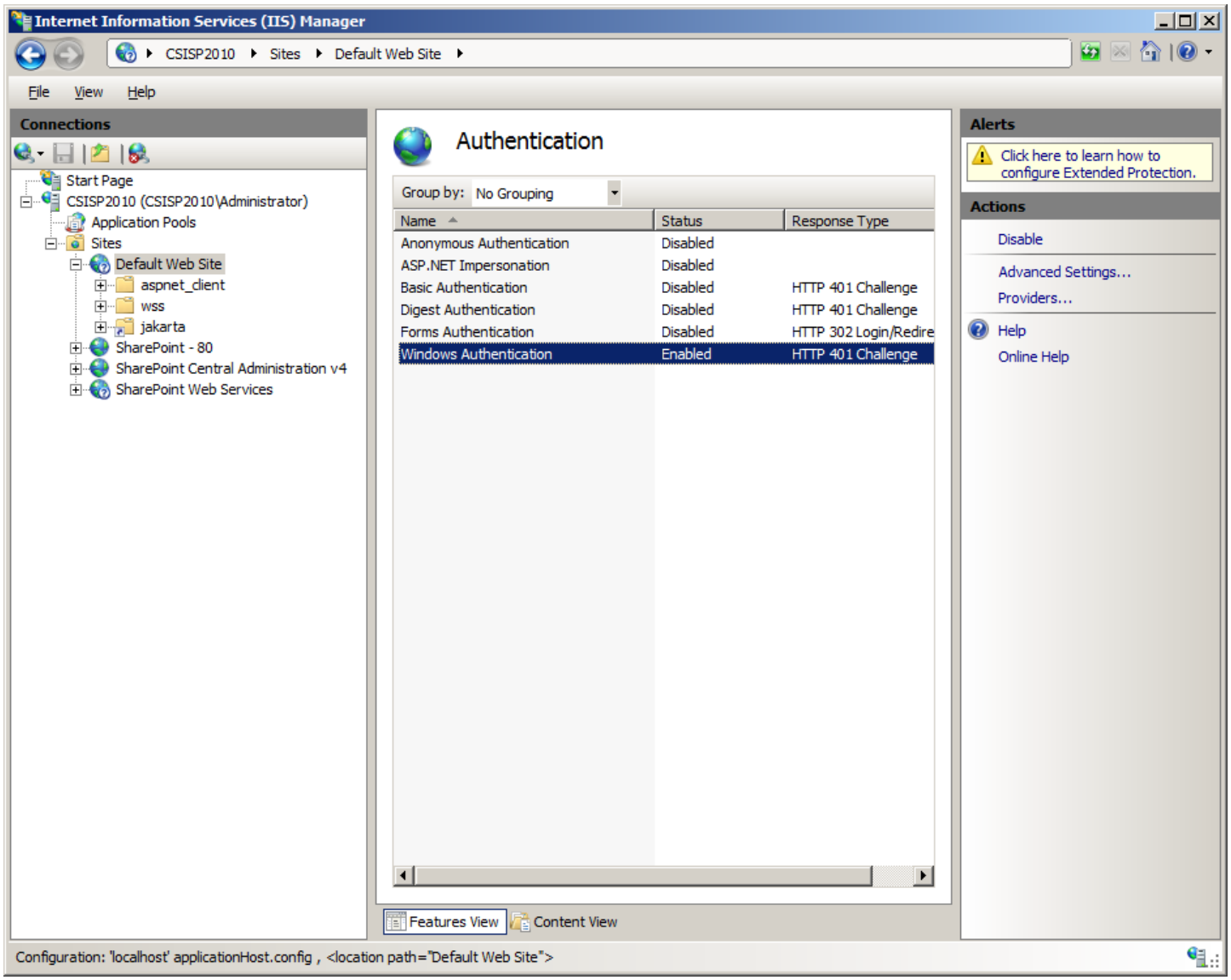
- Set the 'Alias' **to 'jakarta'. - Set the** 'Physical Path' **to the directory where you extracted the ISAPI Filter in step 1 (such as,** `C:\tomcat_iis_connector`**). - Click** 'OK'**. - Verify that a 'jakarta' virtual directory is now present under the selected website.**

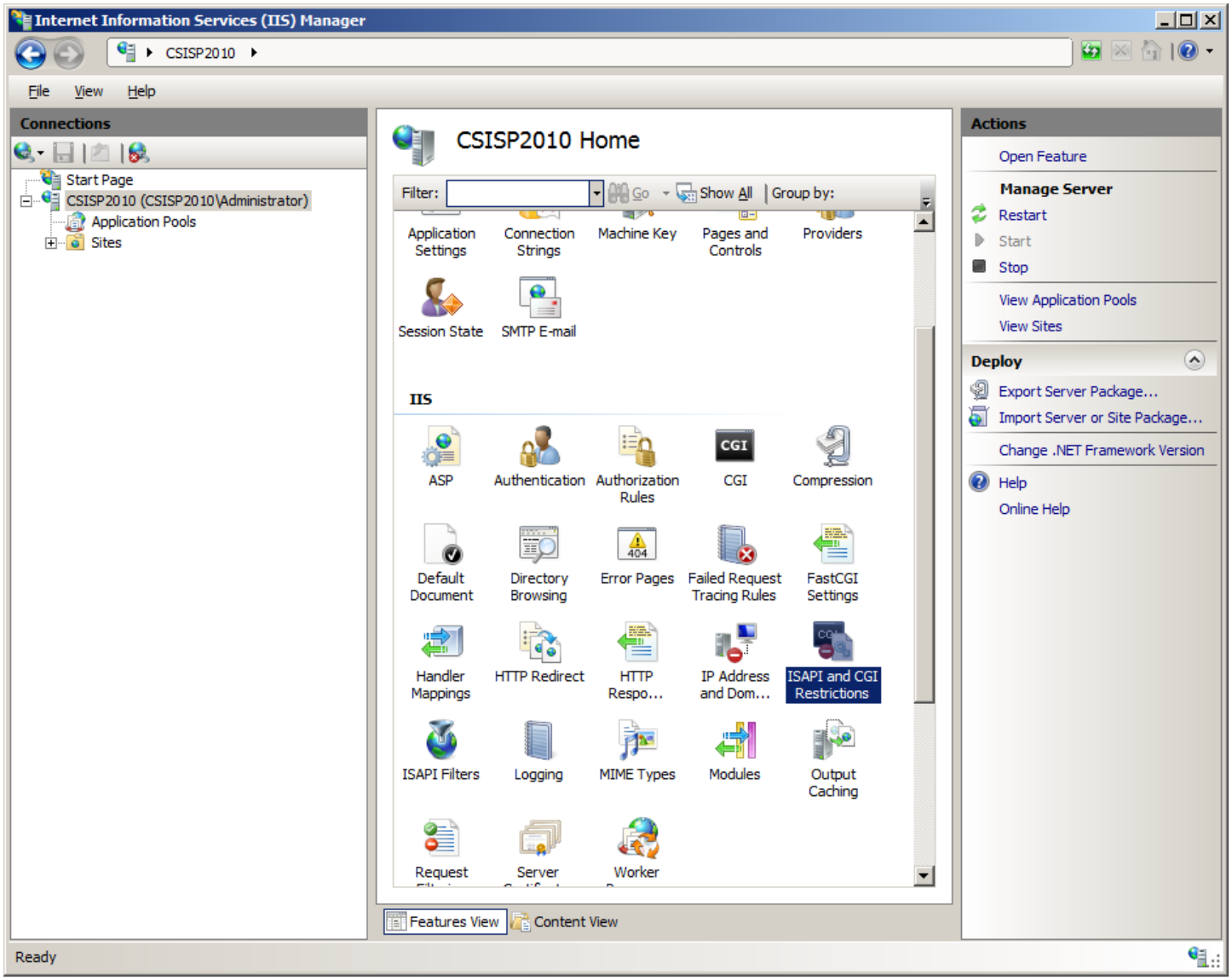


- Next, select the 'jakarta' **virtual directory in the** 'Connections' **panel. - Double-click the** 'Handler Mappings' **icon in** 'Features View'**. - Click the** 'Edit Feature Permissions' **link in the** 'Actions' **panel. - Ensure that the** 'Execute' **option is selected.**

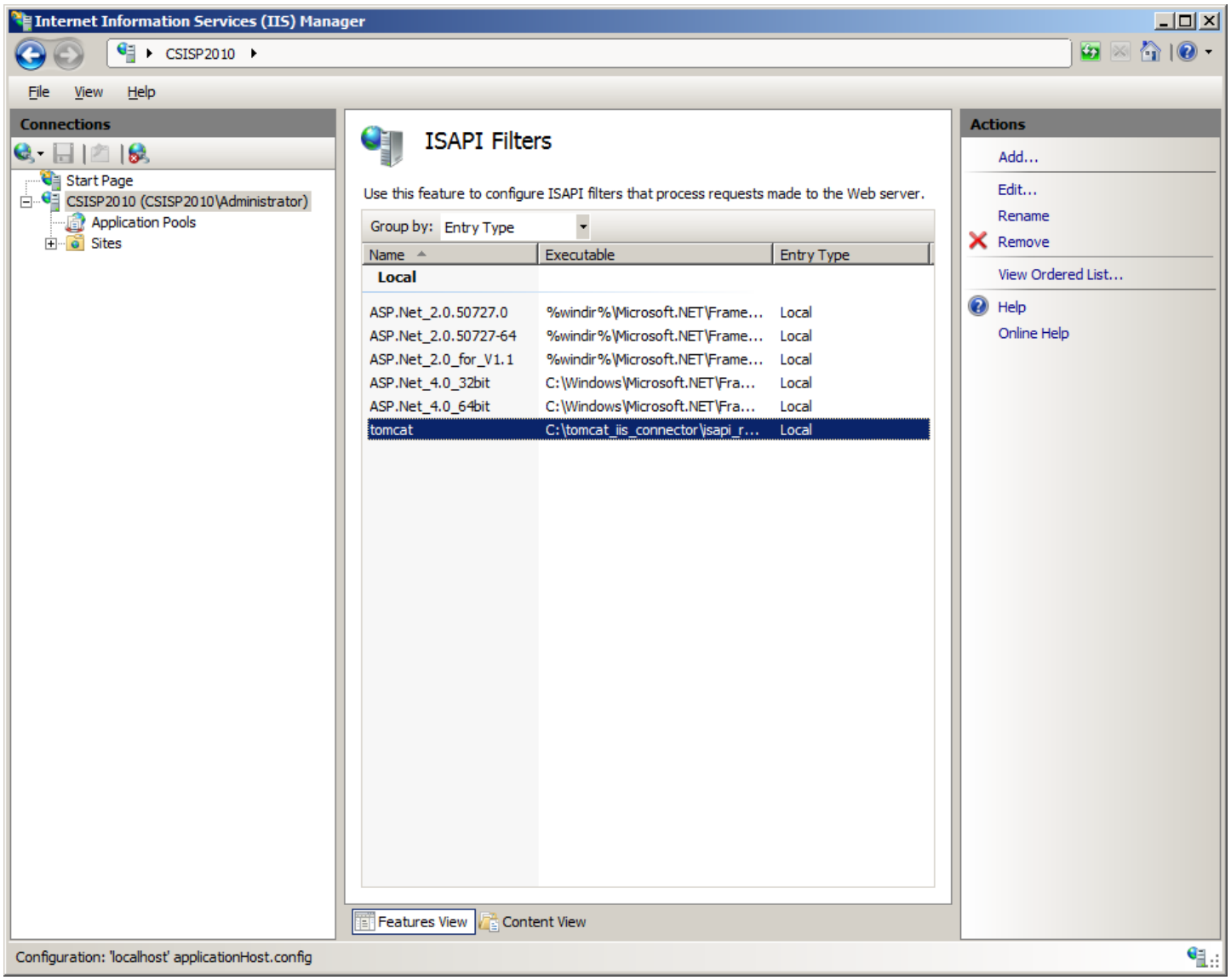


- Click 'OK'**. ==== Step 4. Enable Integrated Windows Authentication ==== This step involves modifying the security of the IIS Web Site to use NTLM or Kerberos authentication. - Select the IIS Web Site modified in step 3 and double-click the** 'Authentication' **icon in** 'Features View'**. - Use the** 'Disable' **and** 'Enable' **items in the** 'Actions' **panel to ensure that** 'Windows Authentication' **is the only authentication method listed in the table as** 'Enabled'**.**

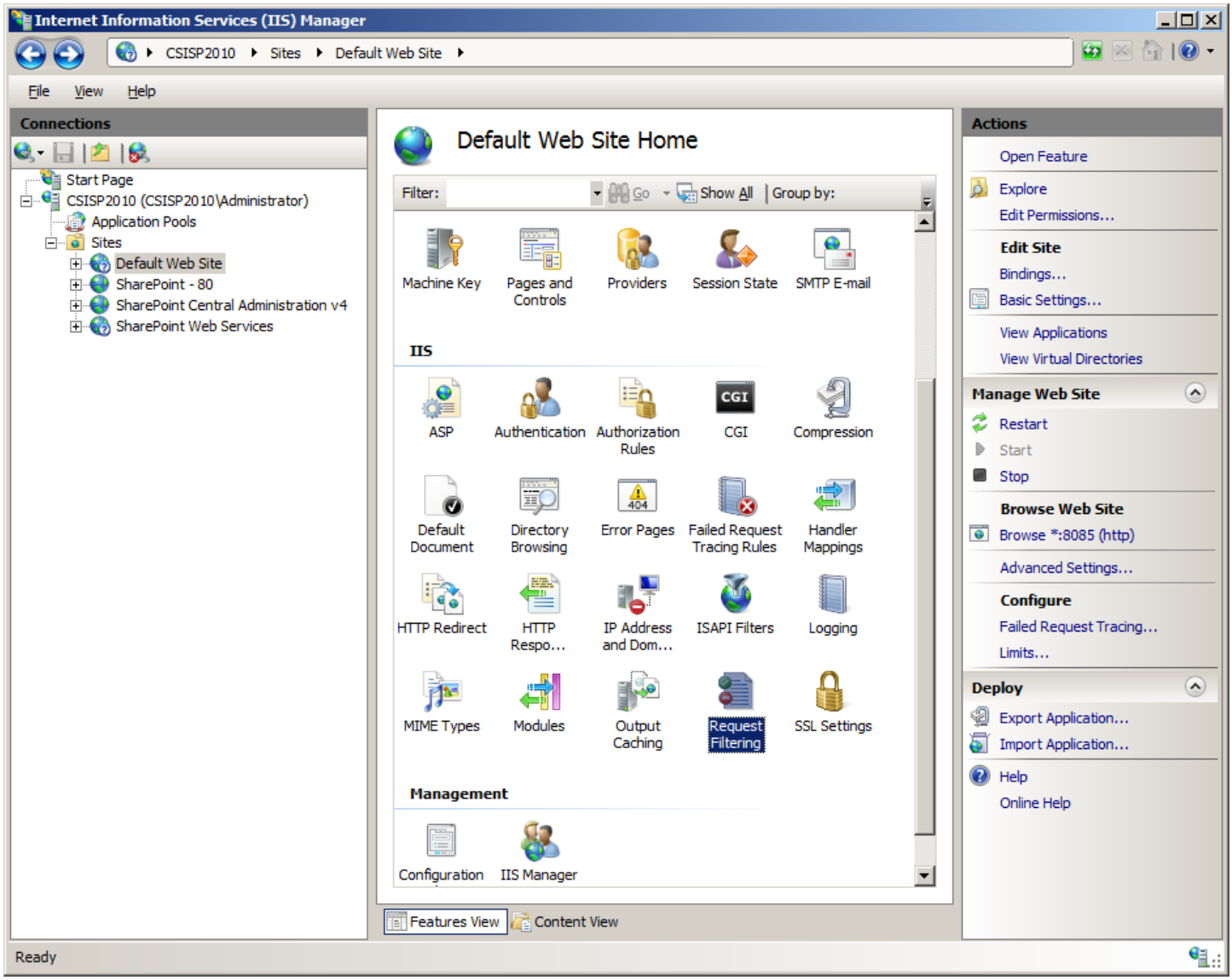

Internet Information Services (IIS) Manager
CSISP2010 ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
CSISP2010 (CSISP2010\Administrator)
Application Pools
Sites
Default Web Site
aspnet_client
wss
jakarta
SharePoint - 80
SharePoint Central Administration v4
SharePoint Web Services
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication Disabled
ASP.NET Impersonation Disabled
Basic Authentication Disabled HTTP 401 Challenge
Digest Authentication Disabled HTTP 401 Challenge
Forms Authentication Disabled HTTP 302 Login/Redire
Windows Authentication Enabled HTTP 401 Challenge
Features View
Content View
Alerts
Click here to learn how to configure Extended Protection.
Actions
Disable
Advanced Settings...
Providers...
Help
Online Help
Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">
==== Step 5. Register the ISAPI Extension ==== Now you will register the isapi_redirect.dll as an authorised ISAPI Extension. - In the 'Connections' panel, ensure that the local IIS Server is selected. - Double-click the 'ISAPI and CGI Restrictions' icon in 'Features View'.



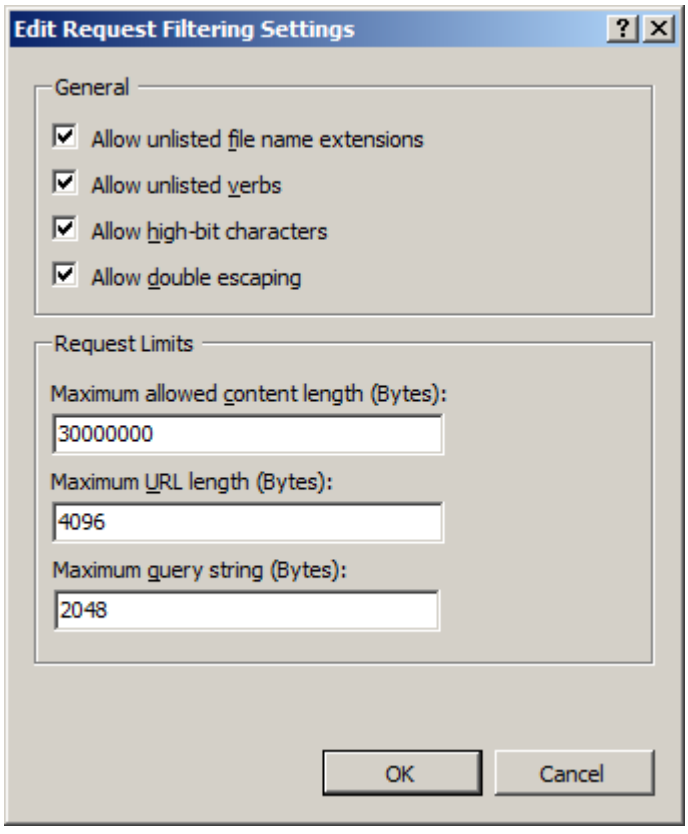
- Click 'Add' **in the** 'Actions' **panel. - Set the** 'ISAPI or CGI path' **to the isapi_redirect.dll you downloaded in step 1. - Set the** 'Description' **to 'tomcat'. - Ensure that the** 'Allow extension path to execute' **is selected.**



- Click 'OK'**. - Verify that the new ISAPI restriction is listed in the table with a restriction of** 'Allowed'**. ==== Step 6. Allow Double Escaping ==== By default, IIS 7 prohibits any URL that contains a '+' character in the URL from being served. This is referred to as 'double escaping'. In Confluence, any page with a space in the title will be served from a URL with spaces replaced by the '+' sign (such as, 'http://confluence/display/spacekey/This+Page+Has+Spaces+In+The+Title'). You will need to disable this security feature in IIS 7 in order for the ISAPI filter to correctly process any Confluence page URLs. - In the** 'Connections' **panel, ensure that the IIS Web Site that will be used to proxy Confluence requests is selected. - Double-click the** 'Request Filtering' **icon in** 'Features View' **(If the** Request Filtering **icon is not displayed, you may need to download the IIS Administration Pack first).**



- Click the 'Edit Feature Settings' **link in the** 'Actions' **panel. - Ensure that the** 'Allow double escaping' **option is selected. - Modify "Maximum allowed content length (bytes)" to the maximum size of attachments you want that your installation allows. ie 104857600 for 100MB.**



- Click 'OK**'.