

IBM Business Analytics Proven Practices: Configure Microsoft Internet Information Services 7.x for IBM Cognos 10

Product(s): IBM Cognos 10 BI; Area of Interest: Infrastructure

Bastian Kiessling
Ryan Laginski
Roger Östlund

April 16, 2015
(First published December 02, 2011)

How to set up IBM Cognos 10 with Internet Information Services (IIS) 7.x. This document applies to IIS 7.x installed on a Windows 2008 Server (GA or R2) and all versions of IBM Cognos 10 Business Intelligence and/or Enterprise Planning. The only gateway implementations covered in this document are ISAPI and CGI as those are the only ones supported by IIS.

[View more content in this series](#)

Introduction

Purpose

This document will assist the reader in setting up IBM Cognos 10 with Internet Information Services (IIS) 7.x.

The document is structured in consecutive sections of which some are optional. The optional sections describe how to enable features which are not required but nice-to-have when running IBM Cognos 10 on IIS 7.x. All steps of any section not explicitly labelled optional must be implemented for the set-up to be successful.

Applicability

This document applies to IIS 7.x installed on a Windows 2008 Server (GA or R2) and all versions of IBM Cognos 10 Business Intelligence and/or Enterprise Planning. The only gateway implementations covered in this document are ISAPI and CGI as those are the only ones supported by IIS.

Exclusions and Exceptions

This document will not cover configuring single sign-on (SSO) for IBM Cognos 10 based on IIS authentication. For information about this topic, please refer to the IBM Cognos 10 Information Center, IBM Cognos Technotes and resources published on the developerWorks web site.

Assumptions

This document assumes IIS 7.x has previously been added to the Windows 2008 Server roles and all necessary options have been selected to successfully run a website. For details, see Appendix A.

This document also assumes the IBM Cognos 10 Gateway install component has been successfully installed to the same machine as IIS.

Configuring An Application Pool

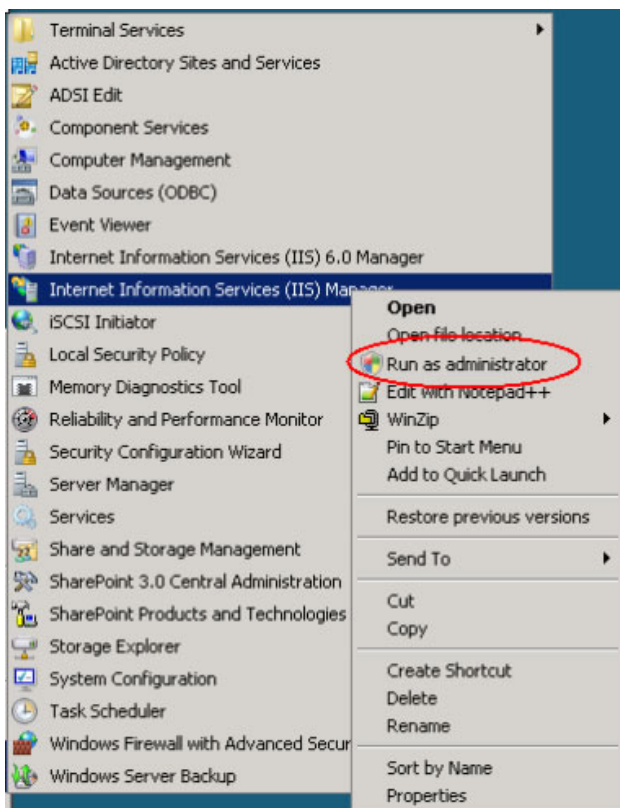
IBM Cognos 10 gateway modules will need to be executed in the context of an IIS 7.x application pool. While it's most convenient to simply use the **Default Application Pool**, it's strongly recommended to define an additional separate application pool for IBM Cognos 10. This application pool can be shared by many IBM Cognos products such as IBM Cognos 10 BI, IBM Cognos Enterprise Planning, IBM Cognos TM1 Web or IBM Cognos Executive Viewer.

Setting up the Application Pool container

The initial steps are to setup an Application Pool for the IBM Cognos gateway modules to reside in.

1. Open the Internet Information Services Manager by clicking **Start > Administrative Tools**, right-click **Internet Information Services (IIS) Manager** and select **Run as administrator**.

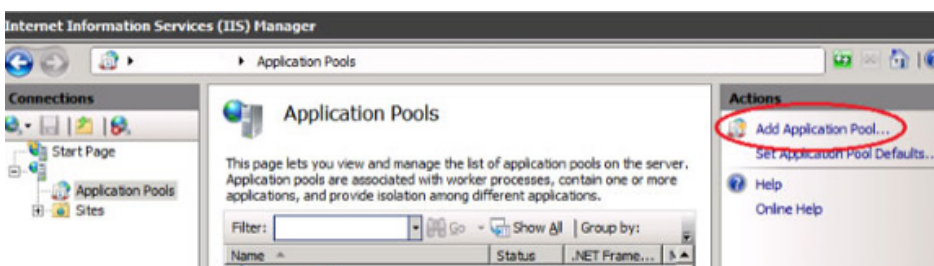
Figure 1: Launching Internet Information Services (IIS) Manager as Administrator



NOTE: There may be an entry in the Start menu titled **Internet Information Services (IIS) 6.0 Manager**. Please use the **Internet Information Services (IIS) Manager** only.

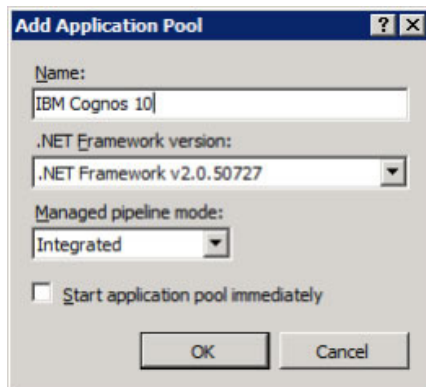
2. Expand on the <server name> which is located under the Start Page, then expand on **Application Pools**.
3. Click on **Add Application Pool...** from the **Actions** pane on the far right.

Figure 2: Adding an application pool



4. Provide the required details in the **New Application Pool** dialog.
 - In the **Name:** field, provide a name such as **IBM Cognos 10** for the new application pool. Do not use cgi-bin or isapi as a name, as these are reserved.
 - Leave the **.Net Framework version:** and **Managed pipeline mode:** fields as the default.
 - Un-check the **Start application pool immediately** field.

Figure 3: The Add Application Pool dialog asking for name, .NET Framework version and pipeline mode



5. Click **OK** to create the application pool.

In IBM Cognos 10.2 a 64-bit gateway is now available but is disabled by default. In IBM Cognos 10.2.1 and 10.2.2 the 64-bit gateway is the default gateway. The following steps are broken into two sections, 32-bit installs and 64-bit installs. It is possible to install IBM Cognos 10 in 64-bit but keep the gateway in 32-bit mode.

If the IBM Cognos version is 10.2.0 or 10.1.1, use the 32-bit section even if IBM Cognos and/or the operating system is 64-bit. If the IBM Cognos version is 10.2 or higher, use the 32-bit section if installed to a 32-bit environment and use the 64-bit section if installed into a 64-bit environment. If the IBM Cognos version is 10.2.1 or 10.2.2 use the 64-bit section of this document.

Configuring a 32-bit Gateway

This section applies to all versions of IBM Cognos 10.1.0 and 10.1.1 or 32-bit versions of IBM Cognos 10.2 and higher.

1. Once back in the IIS Manager's left explorer pane, select the newly created application pool and click **Advanced Settings...** under the **Edit Application Pool** section within the **Actions** tool pane on the far right.

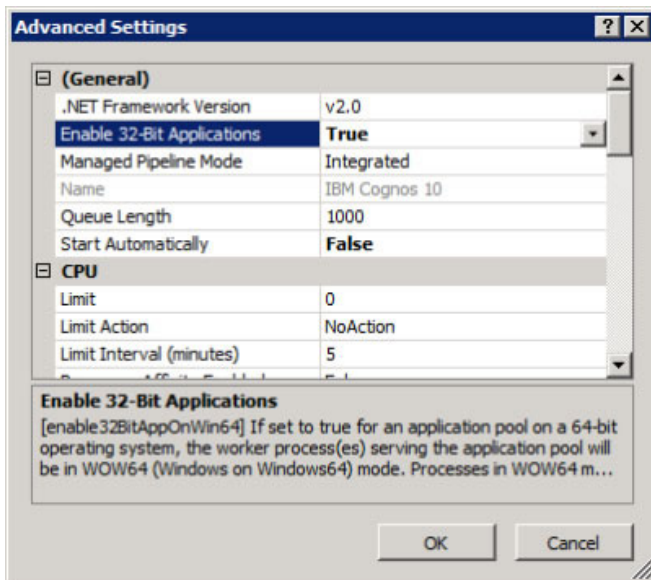
Figure 4: Select the Advanced Settings action for an application pool



2. If applicable, enable 32-bit applications. For Windows 2008 (R2) 64-bit, the application pools will use 64-bit operating mode by default. However, IBM Cognos 10.1.0 and 10.1.1 Gateway modules are 32-bit even in 64-bit installs of IBM Cognos 10. Therefore on 64-bit platforms

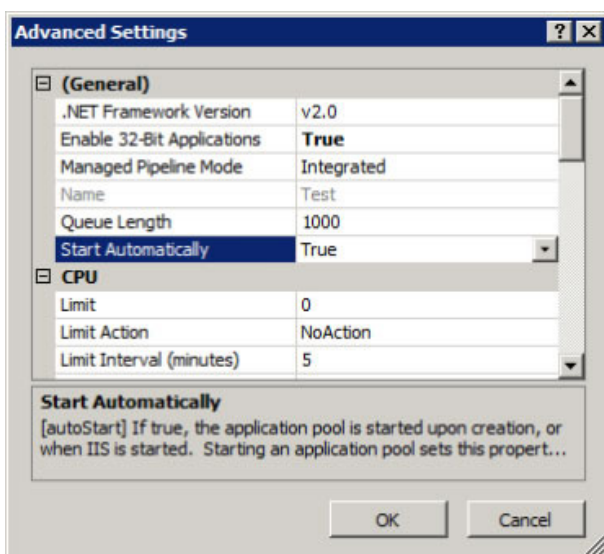
the application pool must be configured for 32-bit mode to execute the IBM Cognos Gateway modules. For 64-bit installs of IIS, select the **Enable 32-Bit Applications** setting and set the value to **True**. For 32-bit installs of IIS, this option will not be available.

Figure 5: The Advanced Settings dialog showing the advanced properties of an application pool



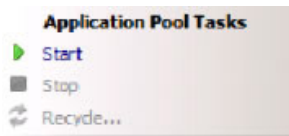
3. Change the **Start Automatically** setting to **True**.

Figure 6: The Advanced Settings dialog of an application pool showing the Start Automatically option



4. Click **OK**.
5. Again, in the IIS Manager's left explorer pane select the newly created application pool and under **Application Pool Tasks** within the **Actions** tool pane on the right, click **Start**.

Figure 7: Start the Application Pool

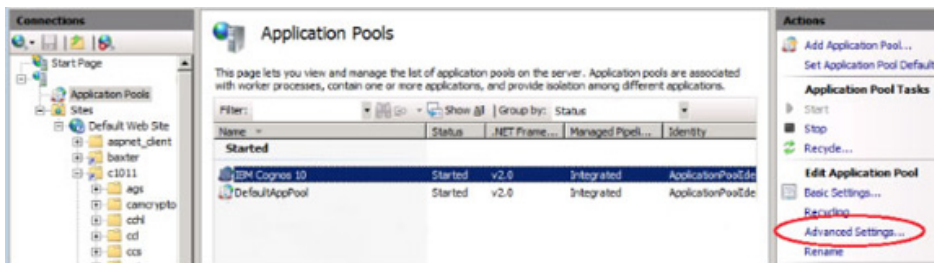


Configuring a 64-bit Gateway

This section applies to 64-bit versions of IBM Cognos 10.2 and higher.

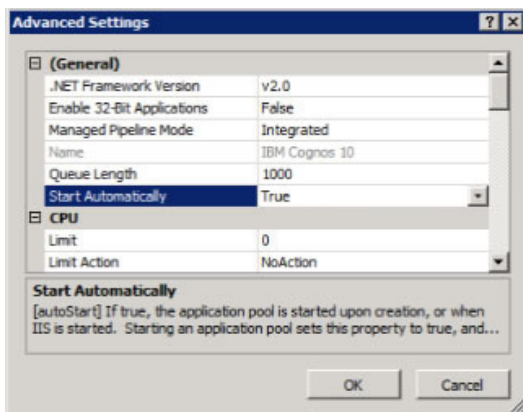
1. Once back in the IIS Manager's left explorer pane, select the newly created application pool and click **Advanced Settings...** under the **Edit Application Pool** section within the **Actions** pane on the far right.

Figure 8: Advanced Settings for an application pool



2. Change the **Start Automatically** setting to **True**.

Figure 9: The Advanced Settings dialog of an application pool showing the Start Automatically option



3. By default, the IBM Cognos Gateway binaries are 32-bit in order to preserve backwards compatibility for upgraded environments. The following steps are required to enable 64-bit.
 - Open a Command Prompt and navigate to the IBM Cognos install directory, then to cgi-bin. For example, D:\ibm\cognos\c10\cgi-bin.
 - Run the command `copyGateMod.bat 64bit`.
 - A list of files that were copied will scroll across the screen.

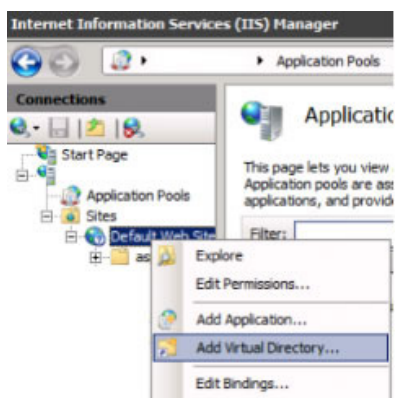
- If there is a need to revert back to the 32-bit gateway, use the command `copyGateMod.bat 32bit`.

Create The IBM Cognos 10 Virtual Directory

IIS, like any other web server, serves its contents to clients by exposing a virtual directory tree. For IBM Cognos 10 one will have to create a new virtual directory. This virtual directory will determine the path (or alias) element to be used in the URL, right after the web server host name or address. The product documentation states **ibmcognos** as the default virtual directory name (for example, `http://>server</ibmcognos`), however any other string can be used.

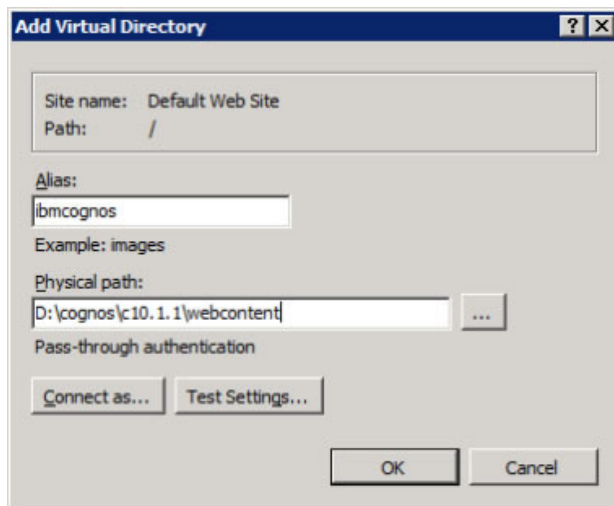
1. In the IIS Manager's left explorer pane, expand **Sites** and **Default Web Site**.
2. Right-click the **Default Web Site** and select **Add Virtual Directory...**

Figure 10: Adding a virtual directory



3. Provide the required details for the **Add Virtual Directory** dialog.
 - In the **Alias:** field, provide a name for the virtual directory, such as **ibmcognos**. The remainder of this document will use **ibmcognos** as the virtual directory name.
 - In the **Physical path:** field, specify the location of the **webcontent** sub-directory within the IBM Cognos 10 Gateway install. If necessary, use the button with the ellipsis to browse for the directory.

Figure 11: Add Virtual Directory dialog with required alias and physical path



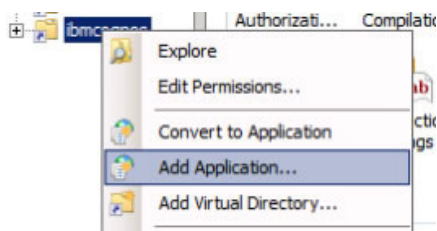
4. Click **OK** to save the changes.

Create an Application for cgi-bin

Creating an IIS Application for cgi-bin will map the IBM Cognos gateway modules to the application pool that was previously created in the [Configuring an Application Pool](#) section.

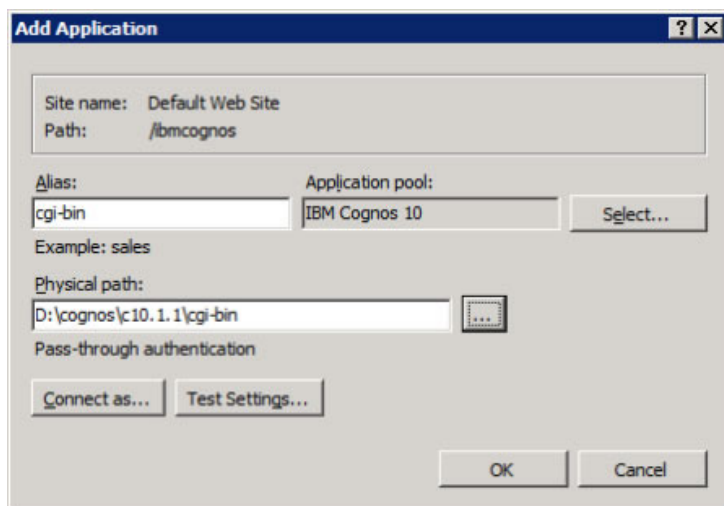
1. In the IIS Manager's left explorer pane find the virtual directory created earlier in the section titled [Create the IBM Cognos 10 Virtual Directory](#). The default virtual directory name is **ibmcognos**.
2. Right-click on the virtual directory and select **Add Application...**

Figure 12: Right-Click on the Virtual Directory to add application



3. Provide the required details in the Add Application dialog.
 - In the **Alias:** field, specify a value of **cgi-bin**. This is a mandatory value and cannot be any other value.
 - In the **Physical path:** field, specify the location of the **cgi-bin** sub-directory within the IBM Cognos 10 Gateway install. If necessary, use the button with the ellipsis to browse for the directory.
 - In the **Application pool:** field, select the application pool created in the **Configuring an Application Pool** section by clicking on the **Select...** button.

Figure 13: Add Application dialog with the required alias, physical path and application pool



4. Click OK to save the changes.

Configuring IIS 7 for IBM Cognos ISAPI

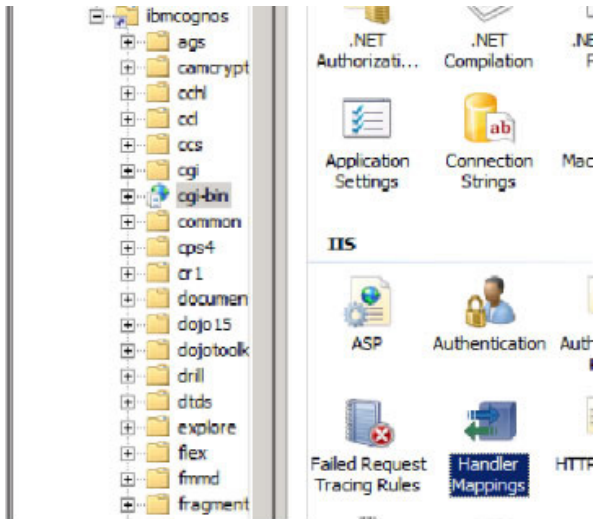
IBM Cognos 10 offers two implementations of gateway modules to be used with IIS, ISAPI and CGI. It is considered to be best practice to use ISAPI with IIS since this provides better performance and resource allocation over CGI. Therefore this section describes the setup of the ISAPI module and the next section describing CGI setup is optional. Use CGI on IIS only if required.

For the ISAPI module to work there are two steps. First, a module mapping must be configured which routes requests calling **cognosisapi.dll** to the executable. Second, the module must be added as an allowed extension so IIS does not block its execution.

Setting up Module Mapping for ISAPI

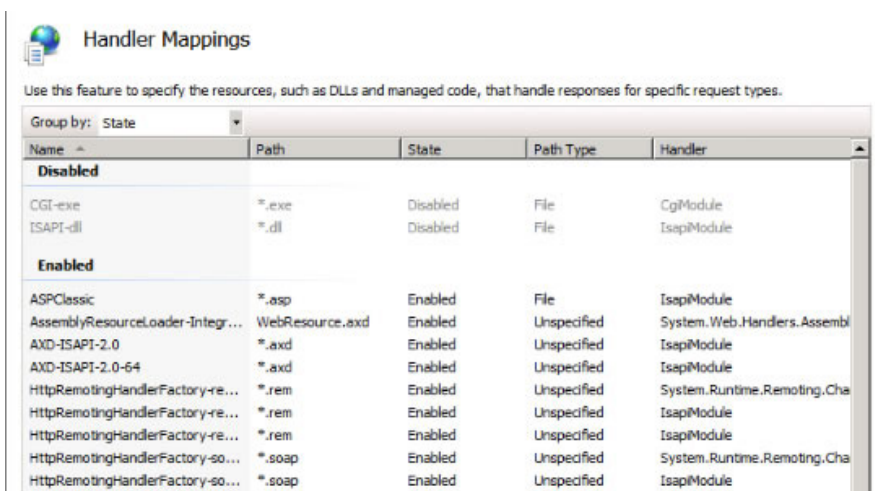
1. Select the **cgi-bin** application from the **Default Web Site > ibmcognos** tree in the left pane of IIS Manager and select the **Features View** from the lower bar in the middle pane.
2. Double-click on **Handler Mappings** in the middle pane. This will bring up the list of handler mappings for this application in the middle pane.

Figure 14: Handler Mappings under the Feature View of cgi-bin application



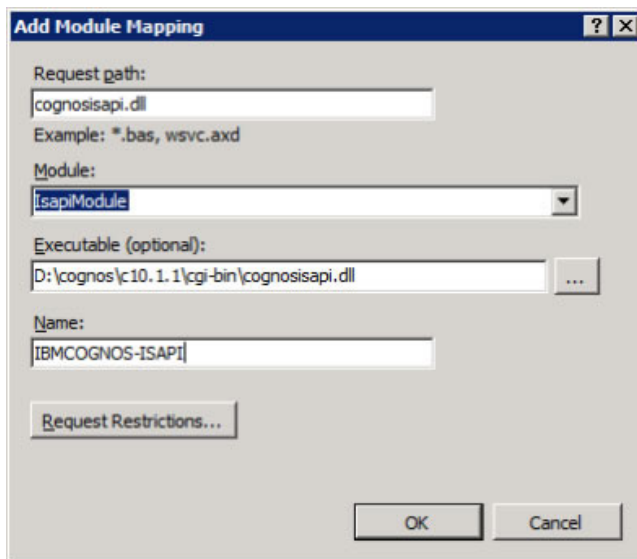
Note that by default ISAPI and CGI are listed as **Disabled**. Also note that CGI is for .EXE file extensions only.

Figure 15: Default view of Handler Mappings with CGI and ISAPI disabled



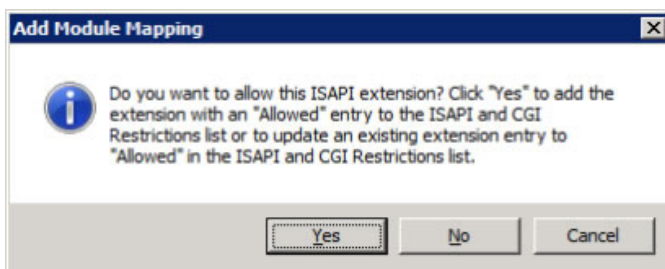
3. In the far right Actions pane click **Add Module Mapping...** to add the ISAPI mapping.
4. Provide the required details to the **Add Module Mapping** dialog.
 - In the **Request path:** field, specify the value **cognosisapi.dll**. This is a mandatory value and cannot be any other value.
 - In the **Module:** field, select **IsapiModule** from the drop down list.
 - In the **Executable (optional):** field, specify the path to the **cognosisapi.dll** within the IBM Cognos Gateway install. This file will be in <COG_ROOT>/cgi-bin, where <COG_ROOT> refers to the IBM Cognos BI installation directory. For example, D:\cognos\c10\cgi-bin.
 - In the **Name:** field, specify a name for this module (for example, **IBMCOGNOS-ISAPI**).

Figure 16: The Add Module Mapping dialog with required request path, module, executable and name




5. Click **OK**.
6. A dialog will appear to confirm that this new ISAPI extension should be allowed. Click **Yes**.

Figure 17: The Add Module Mapping prompt that will appear after creating the ISAPI module mapping



7. Back at the **Handler Mappings** screen, the newly added handler (in this example **IBMCOGNOS-ISAPI**) will appear under the **Enabled** section.

Figure 18: The list of handler mappings now showing the enabled ISAPI module mapping

 **Handler Mappings**

Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Group by: State				
Name	Path	State	Path Type	Handler
Disabled				
CGI-exe	*.exe	Disabled	File	CgiModule
ISAPI-dll	*.dll	Disabled	File	IsapiModule
Enabled				
ASPClassic	*.asp	Enabled	File	IsapiModule
AssemblyResourceLoader-Integr...	WebResource.axd	Enabled	Unspecified	System.Web.Handlers.Assembl
AXD-ISAPI-2.0	*.axd	Enabled	Unspecified	IsapiModule
AXD-ISAPI-2.0-64	*.axd	Enabled	Unspecified	IsapiModule
HttpRemotingHandlerFactory-re...	*.rem	Enabled	Unspecified	System.Runtime.Remoting.Cha
HttpRemotingHandlerFactory-re...	*.rem	Enabled	Unspecified	IsapiModule
HttpRemotingHandlerFactory-re...	*.rem	Enabled	Unspecified	IsapiModule
HttpRemotingHandlerFactory-so...	*.soap	Enabled	Unspecified	System.Runtime.Remoting.Cha
HttpRemotingHandlerFactory-so...	*.soap	Enabled	Unspecified	IsapiModule
HttpRemotingHandlerFactory-so...	*.soap	Enabled	Unspecified	IsapiModule
IBMCOGNOS-ISAPI	cognosisapi.dll	Enabled	Unspecified	IsapiModule
OPTIONSVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule

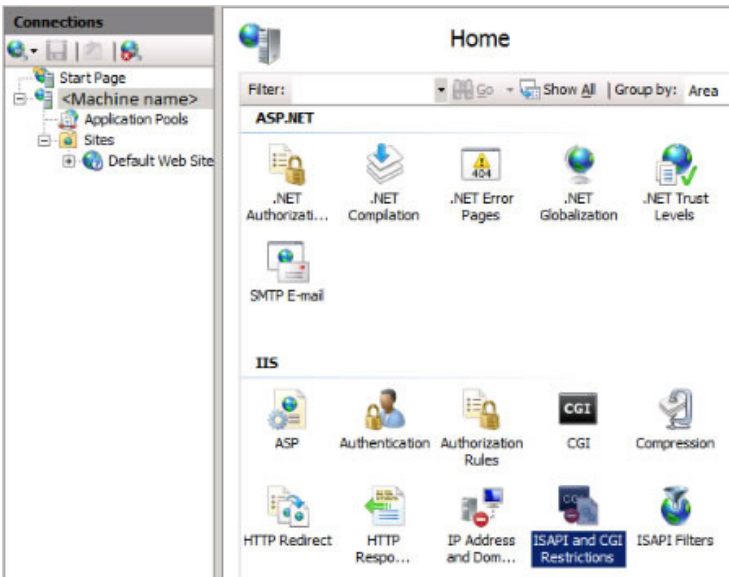
Setting the ISAPI Restrictions for the Web Server

1. In the IIS Manager, select the **Web Server** from the tree view on the left.

2. In the middle pane, select the **Features View** tab at the bottom.

3. Double-click on the **ISAPI and CGI Restrictions** feature. This will bring up the list of defined restrictions in the middle pane of IIS Manager.

Figure 19: Location of the ISAPI and CGI Restrictions



4. Ensure that the entry for **cognosisapi.dll** is set to **Allowed** within the list. This entry should have been inserted automatically by the steps from the **Setting up Module Mapping in**

ISAPI. It will have no description and one has to identify it based on the value shown in the **Path** column.

Figure 20: List of defined ISAP and CGI restrictions, showing the newly created ISAPI module being allowed

ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Group by: No Grouping		
Description	Restriction	Path
[No Description]	Allowed	D:\cognos\c10.1.1\cgi-bin\cognosisapi.dll

If the restriction entry for the

cognosisapi.dll is missing continue to Step 5 otherwise skip to the next section.

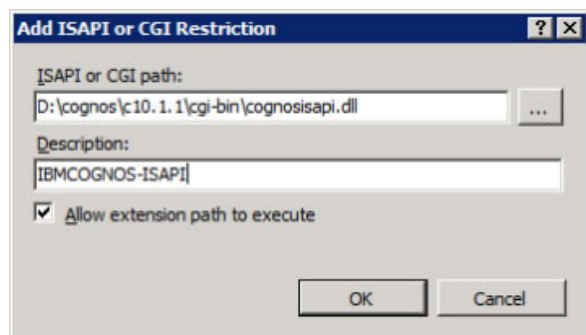
5. In the far right Actions pane, click **Add...**

6. Provide the required details to the **Add ISAPI or CGI Restriction** dialog.

- In the **ISAPI or CGI path:** field, specify the path to the **cognosisapi.dll** within the IBM Cognos Gateway install. This value will normally be <COG_ROOT>\cgi-bin\cognosisapi.dll. For example, D:\cognos\c10\cgi-bin\cognosisapi.dll.
- In the Description: field, enter a description of the restriction, such as **IBMCOGNOS-ISAPI**.

7. Check the **Allow extension path to execute** checkbox.

Figure 21: Add ISAPI or CGI Restriction dialog with checked option to allow the extension path to execute



Testing the ISAPI installation

There are several ways to call the IBM Cognos 10 ISAPI Gateway.

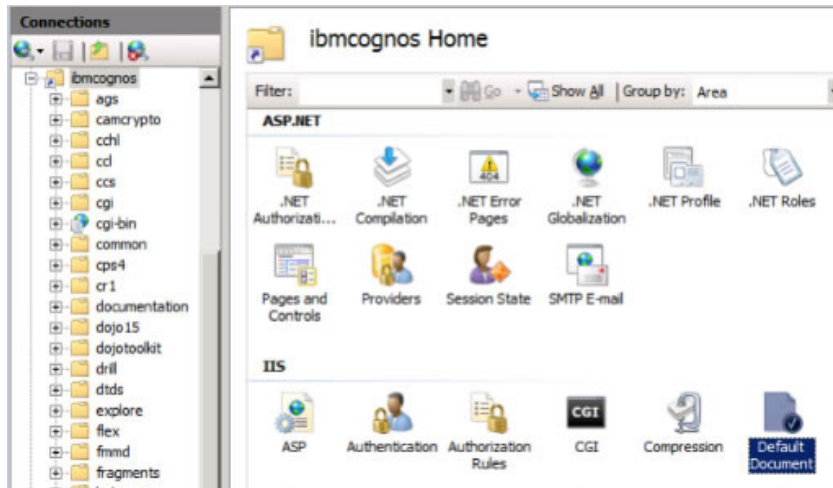
- Call `http://<webserver>/<alias>`
- Call `http://<webserver>/<alias>/isapi`
- Call `http://<webserver>/<alias>/cgi-bin/cognosisapi.dll`

By default, only the third option will work without any additional configuration. For convenience reasons, administrators usually prefer to use the first URL because it is the shortest to type. However, that URL is also the most general one to use and is not specific to any particular Gateway implementation. To implement the first option for ISAPI, the following the steps below are

required to load the default document from the specified paths. The second URL is prepared to call the ISAPI Gateway but it also needs to be enabled.

1. In IIS Manager, in the left explorer pane select the virtual directory for IBM Cognos 10 that was created earlier in **Create the IBM Cognos 10 Virtual Directory** section.
2. In the middle pane, switch to **Features View**.
3. Double-click **Default Document**.

Figure 22: Location of the default document



4. In the far right Actions pane, click **Add**.
5. Type **default.htm** and click **OK** to save.

This will make default.htm a default document to serve if the directory is accessed without specifying a particular document, as is the case here. The default.htm file contains JavaScript code that will perform a redirect to the IBM Cognos 10 Gateway module after showing a splash screen. The default.htm in the second URL form, `http://<webserver>/<alias>/isapi`, will redirect to the ISAPI module by default. The default.htm in the first URL form, `http://<webserver>/<alias>`, will redirect to CGI by default.

After enabling the URLs, accessing either URL should present the IBM Cognos 10 log-in screen or, if anonymous authentication is enabled for IBM Cognos 10, IBM Cognos Connection. In the case where IBM Cognos 10 is not started, an error message stating that the IBM Cognos 10 Gateway could not contact the IBM Cognos 10 BI server will appear.

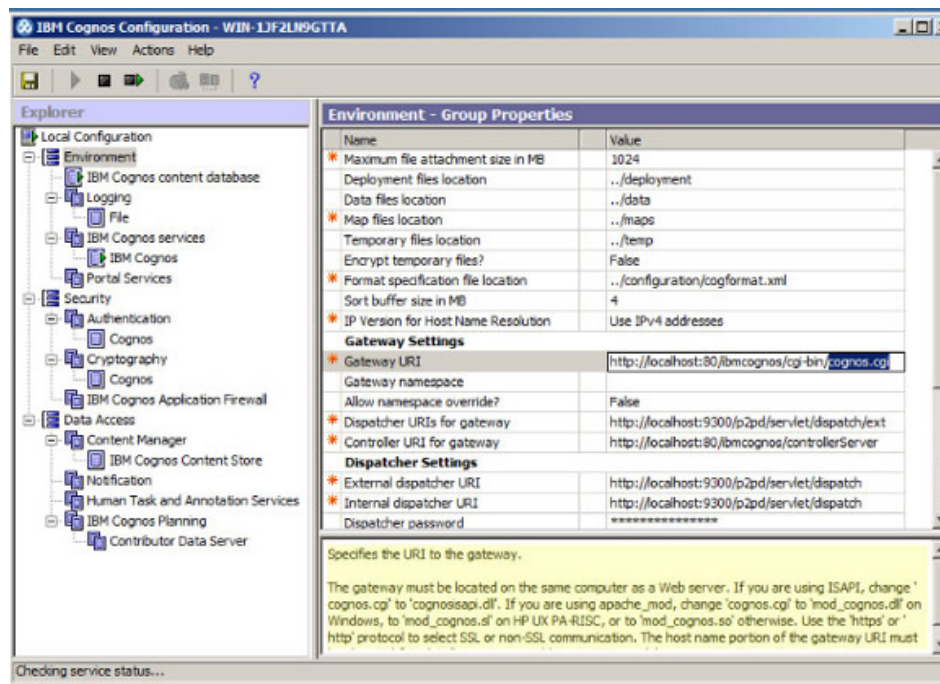
Making the ISAPI Gateway the default

To make the ISAPI Gateway module the default for the IBM Cognos 10 BI system, there are two more steps required. The first step is to change the Gateway URI configuration setting using IBM Cognos Configuration and the second step is to adjust the default.htm file for the `/<alias>` virtual directory.

Repeat the following for all installs of IBM Cognos 10 Application Tier or Content Manager.

1. Open **IBM Cognos Configuration**, select the **Environment** element in the left Explorer pane and click on the **Gateway URI** field.

Figure 23: IBM Cognos Configuration showing the properties of the Environment element including the Gateway URI



2. Edit the Gateway URI field to reflect the actual URI used to call the ISAPI Gateway. As a best practice, use a fully qualified domain naming scheme such as `http://<server>.<domain>.<suffix>:<port>/<alias>/cgi-bin/cognosisapi.dll` for the server name. An example URI might be `http://myserver.domain.com:80/ibmcognos/cgi-bin/cognosisapi.dll`.

If enabled earlier, the default.htm file for the `http://<webserver>/<alias>` URL must be edited to change the redirect target from CGI to ISAPI. Be aware that editing default.htm has implications as there can be only one redirect to one particular IBM Cognos 10 Gateway module. If the CGI gateway is required as well, a decision will need to be made as to which redirect (either CGI or ISAPI) will be the default. It is most likely that users will prefer the shorter URL for accessing the system, so although there is a particular URL for accessing the ISAPI module (`http://<webserver>/<alias>/isapi`), it is recommended that default.htm be edited to redirect to ISAPI if ISAPI is to be the default.

On the IBM Cognos 10 Gateway install,

1. Open **<COG_ROOT>\webcontent\default.htm** in a text editor. For example, `D:\cognos\c10\webcontent\default.htm`.
2. Find the line that reads

```
window.setTimeout("window.location.replace('cgi-bin/cognos.cgi?b_action=xts.run&m=portal/main.xts&startwel=yes')", 5);
```


and change **cognos.cgi** to **cognosisapi.dll**.

```
window.setTimeout("window.location.replace('cgi-bin/cognosisapi.dll?b_action=xts.run&m=portal/main.xts&startwel=yes')",5);
```

This will make **http://<webserver>/<alias>** work like **http://<webserver>/<alias>/isapi**, redirecting to the ISAPI Gateway after showing a splash screen.

Configuring IIS 7 for IBM Cognos CGI (optional)

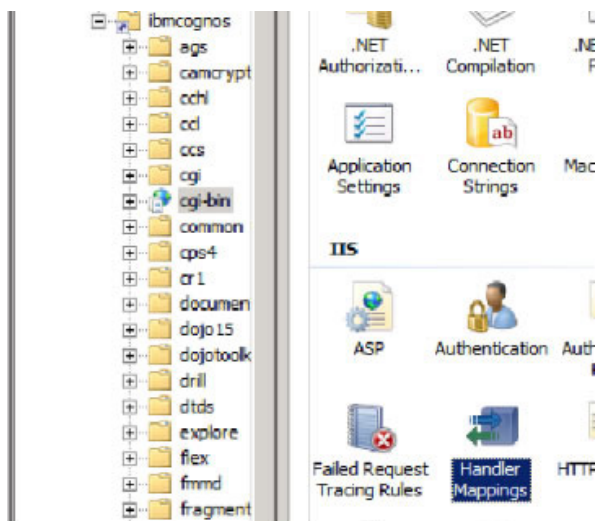
Although it is considered best practice to use the IBM Cognos 10 ISAPI Gateway module for Microsoft IIS, the IBM Cognos 10 CGI Gateway module can be enabled as well. Be aware that CGI modules spawn a new worker process for each session which makes them unsuitable for high load production environments.

As with the ISAPI module, a module mapping needs to be defined first and then the module must be allowed to execute in IIS.

Setting up Module Mapping for CGI

1. Select the **cgi-bin** application from the **Default Web Site > ibmcognos** tree in the left pane of IIS Manager and select the **Features View** from the lower bar in the middle pane.
2. Double-click on **Handler Mappings** in the middle pane. This will bring up the list of handler mappings for this application in the middle pane.

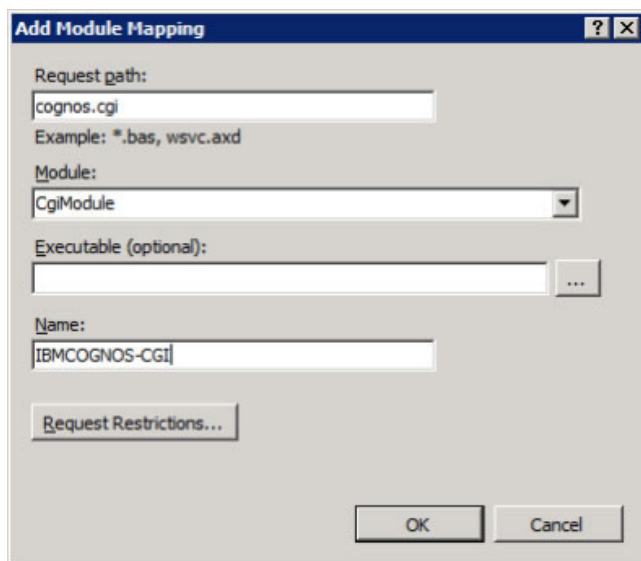
Figure 24: Location of Handler Mappings within the cgi-bin application



3. In the far right **Actions** pane, click **Add Module Mapping...** to add the CGI mapping.
4. Provide the required details for the **Add Module Mapping** dialog.
 - In the **Request path:** field, specify a value of **cognos.cgi**. This is a mandatory value and cannot be any other value.
 - In the **Module:** field, select **cgiModule** from the dropdown list. Note that the use of **fastCGIModule** is not supported.
 - The **Executable (optional):** field should be left blank.

- In the **Name:** field, enter a name for this module, such as **IBMCOGNOS-CGI**.

Figure 25: The Add Module Mapping dialog showing the required request path, module and name




The 'Add Module Mapping' dialog box is shown. It contains the following fields and controls:

- Request path:** A text box containing 'cognos.cgi'. Below it is an example: 'Example: *.bas, wsvc.axd'.
- Module:** A dropdown menu with 'CgiModule' selected.
- Executable (optional):** A text box with a browse button ('...').
- Name:** A text box containing 'IBMCOGNOS-CGI'.
- Request Restrictions...** button.
- OK** and **Cancel** buttons at the bottom.

5. Click **OK** to save. Back at the Handler Mapping page, **IBMCOGNOS-CGI** will appear under the **Enabled** section.

Figure 26: The list of handler mappings now showing the enabled CGI module mapping

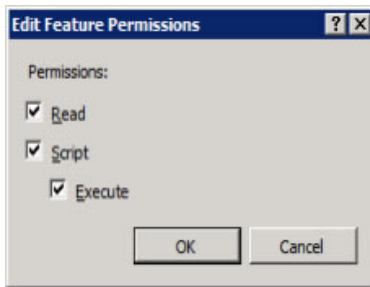
 **Handler Mappings**

Use this feature to specify the resources, such as DLLs and managed code, that handle responses for specific request types.

Name	Path	State	Path Type	Handler
HttpRemotingHandlerFactory-so...	*.soap	Enabled	Unspecified	IsapiModule
HttpRemotingHandlerFactory-so...	*.soap	Enabled	Unspecified	IsapiModule
IBMCOGNOS-ISAPI	cognosisapi.dll	Enabled	Unspecified	IsapiModule
OPTIONSVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule
PageHandlerFactory-Integrated	*.aspx	Enabled	Unspecified	System.Web.UI.PageHandler
PageHandlerFactory-ISAPI-2.0	*.aspx	Enabled	Unspecified	IsapiModule
PageHandlerFactory-ISAPI-2.0-64	*.aspx	Enabled	Unspecified	IsapiModule
SecurityCertificate	*.cer	Enabled	File	IsapiModule
SimpleHandlerFactory-Integrated	*.ashx	Enabled	Unspecified	System.Web.UI.SimpleHandk
SimpleHandlerFactory-ISAPI-2.0	*.ashx	Enabled	Unspecified	IsapiModule
SimpleHandlerFactory-ISAPI-2.0-64	*.ashx	Enabled	Unspecified	IsapiModule
SSINC-shhtm	*.shhtm	Enabled	File	ServerSideIncludeModule
SSINC-shhtml	*.shhtml	Enabled	File	ServerSideIncludeModule
SSINC-stm	*.stm	Enabled	File	ServerSideIncludeModule
StaticFile	*	Enabled	File or Folder	StaticFileModule,DefaultDocu
TraceHandler-Integrated	trace.axd	Enabled	Unspecified	System.Web.Handlers.TraceI
TRACEVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule
WebAdminHandler-Integrated	WebAdmin.axd	Enabled	Unspecified	System.Web.Handlers.WebA
WebDAV	*	Enabled	Unspecified	WebDAVModule
WebServiceHandlerFactory-Inte...	*.asmx	Enabled	Unspecified	System.Web.Services.Protoc
WebServiceHandlerFactory-ISAP...	*.asmx	Enabled	Unspecified	IsapiModule
WebServiceHandlerFactory-ISAP...	*.asmx	Enabled	Unspecified	IsapiModule
IBMCOGNOS-CGI	cognos.cgi	Enabled	Unspecified	CgiModule

6. With the newly created mapping selected, click **Edit Feature Permissions** from the far right Actions pane.
7. In the **Edit Feature Permissions** dialog, check the **Execute** checkbox to enable CGI execution.

Figure 27: The Edit Feature Permissions dialog showing the execute permission enabled

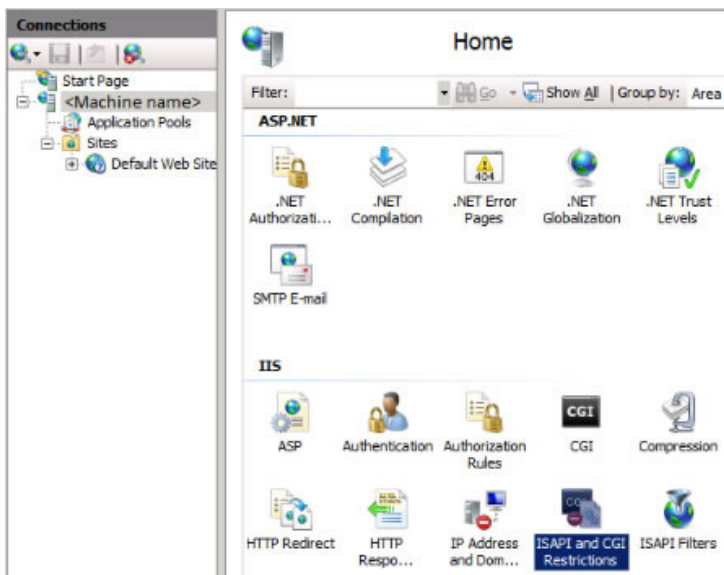


8. Click **OK**.

Setting the CGI Restrictions for the Web Server

1. In the IIS Manager, select the Web Server, in the tree view on the left and in the content pane, select the Features View tab at the bottom.
2. Double-click on the ISAPI and CGI Restrictions feature. This will bring up the list of defined restrictions in the middle pane of IIS Manager.

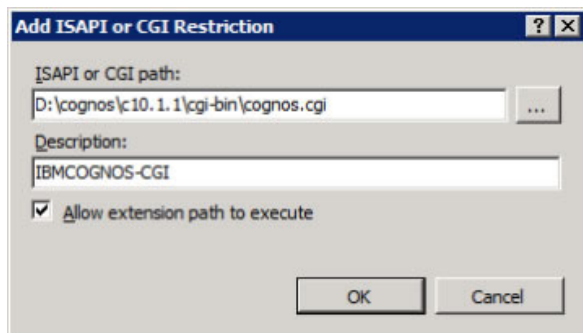
Figure 28: Location of the ISAPI and CGI Restrictions



3. In the far right **Actions** pane, click **Add...**
4. Provide the required details in the **Add ISAPI or CGI Restriction** dialog.
 - In the **ISAPI or CGI Path:** field, specify the path to the **cognos.cgi** file within the IBM Cognos Gateway install. This file can be found in the <COG_ROOT>\cgi-bin directory. If browsing for the file, change the file type to **All files (*.*)**, since .cgi is not a default suffix.

- In the **Description:** field, specify a description of the restriction, such as **IBMCOGNOS-CGI**.
- Ensure that the check-box for **Allow extension path to execute** is checked.

Figure 29: The Add ISAPI or CGI Restriction dialog with the required ISAPI or CGI path, description and allow extension path to execute settings



Testing the CGI installation

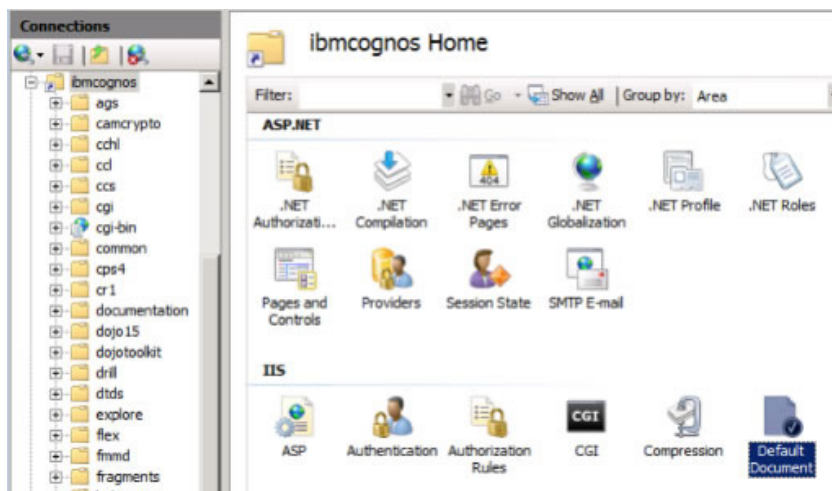
There are two ways to call the IBM Cognos 10 CGI Gateway module,

- By calling `http://<webserver>/<alias>`
- By calling `http://<webserver>/<alias>/cgi-bin/cognos.cgi`

Note: If the steps in the earlier section titled **Making the ISAPI Gateway the default** have been implemented (recall that this was editing the `default.htm` located in the `/<alias>` path), the first URL will re-direct to the ISAPI module and will not call the CGI module.

By default only the second URL will work. For convenience reasons, administrators often desire to use the first URL which is the shortest to type. However, that URL is the most general one to use and is not specific to any particular Gateway implementation. To enable the CGI URL, the following steps will be required to make IIS load a default document from the specified paths.

1. In IIS Manager, in the left explorer pane select the virtual directory for IBM Cognos 10 that was created earlier in **Create the IBM Cognos 10 Virtual Directory** section.
2. In the middle pane, switch to **Features View**.
3. Double-click **Default Document**.

Figure 30: Location of the default document

4. In the far right **Actions** pane, click **Add...**
5. Type **default.htm** and click **OK** to save.

This will make the file default.htm the default document to serve if the directory is accessed without specifying a particular document. The default.htm file contains JavaScript code to perform a redirect to the IBM Cognos 10 Gateway module after showing a splash screen. By default, the redirect will be to the CGI module so unless the default.htm was previously edited, no further changes are required.

Accessing either URL should present the IBM Cognos 10 log-in screen or, if anonymous authentication is enabled for IBM Cognos 10, IBM Cognos Connection. In the case where IBM Cognos 10 is not started, an error message stating that the IBM Cognos 10 Gateway could not contact the IBM Cognos 10 BI server will appear.

Updating The Module Mapping Parameter

An IBM Cognos 10 Gateway requires an additional parameter to be configured for the ISAPI and/or CGI module mapping handlers. This is required so that IBM Cognos Administration and IBM Cognos Mobile function correctly. This section describes how to add this configuration item.

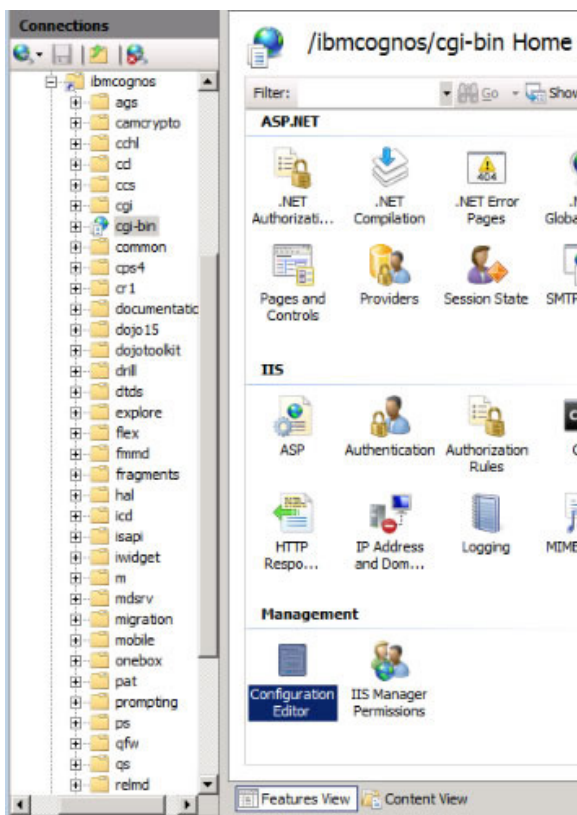
Setting allowPathInfo in the Module Mapping Handlers

IBM Cognos 10 requires the allowPathInfo=true parameter to be added to the ISAPI and/or CGI module mapping handler. This parameter controls how the handler will populate the standard CGI environment variable PATH_INFO for the mapped module. By default, IIS sets it to the full URL but this is not compliant with the CGI specification. However some applications, in particular Active Server Pages, expect it to be the full URL. The IBM Cognos 10 Gateway modules comply with the CGI specification and expect it to contain the last part of the URL only, for example “cognos.cgi” instead of “<alias>/cgi-bin/cognos.cgi”. This is why this additional parameter must be added.

1. Navigate to the **cgi-bin** virtual directory located under the virtual directory that was created earlier in the section titled **Create the IBM Cognos 10 Virtual Directory**.

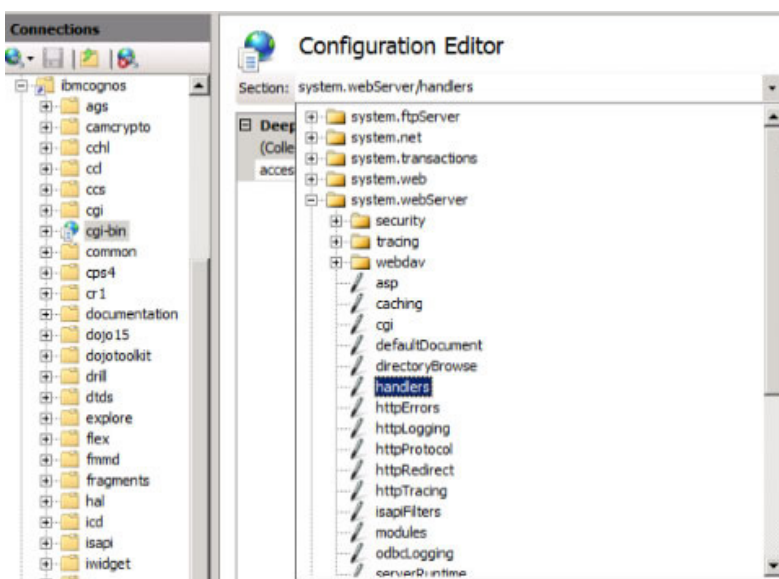
2. In the **Features View**, double click **Configuration Editor** in the **Management** subsection.

Figure 31: Location of the Configuration Editor



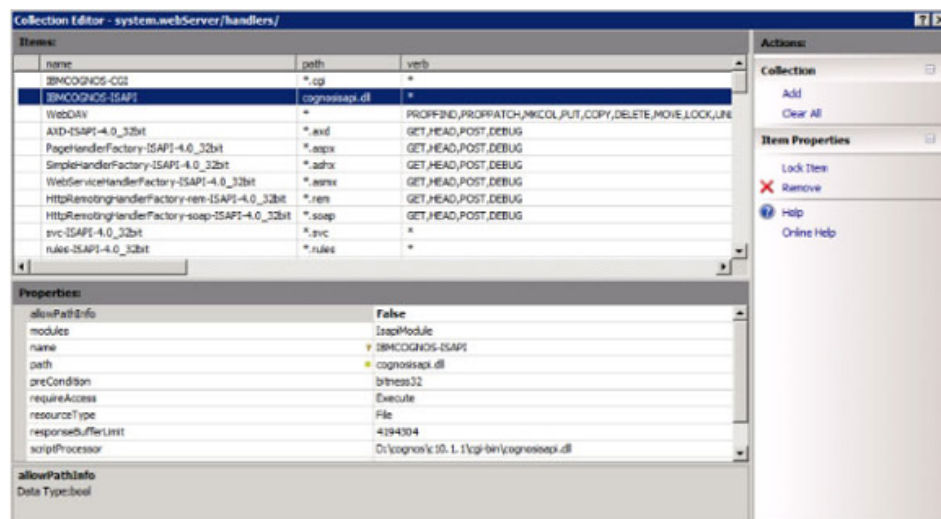
3. Locate the **Section** dropdown. Click the dropdown to expand the various sections, expand **system.webServer** and select **handlers**.

Figure 32: Selecting the handlers section in Configuration Editor



4. Click on the **(Collections)** row, then click on **Edit Items** within the **Action** pane on the far right.
5. Within the **Items** pane of **Collection Editor**, click on the handler that was created in the **Configuring IIS 7 for IBM Cognos ISAPI** section. In this document the handler's name is **IBMCOGNOS-ISAPI**.

Figure 33: Updating the allowPathInfo for each module mapping



6. Within the **Properties** pane, locate the **allowPathInfo** property and change it from **False** to **True**.
7. Close the Collection Editor window, then under the **Actions** pane at the far right, click **Apply**.

If the [Configuring IIS 7 for IBM Cognos CGI](#) section was used to enable CGI, repeat steps 5 through 7 for the IBMCOGNOS-CGI handler.

Testing allowPathInfo

Log in to IBM Cognos Connection as a member of the System Administrator role and bring up IBM Cognos Administration. If IBM Cognos Administration comes up without error, the configuration is correct.

If allowPathInfo is not set correctly, IBM Cognos Administration will not be accessible and will display the error “PF-SRV-6116 Unable to process the document, target is not valid or the target was not received” at the top of the page. Possible resolutions to this error are discussed towards the end of this document in the section titled **Troubleshooting**.

Figure 34: Error PF-SRV-6116 as displayed when calling IBM Cognos Administration if the allowPathInfo configuration is not set correctly

PF-SRV-6116 Unable to process the document, target is not valid or the target was not received.
[Details](#) | [Retry](#) | [Hide this message.](#)

Note: For IBM Cognos Mobile, after the log-in screen, a pop-up containing the text “No Operation Specified” will occur.

Performance Tips (Optional)

To help performance there are a few tweaks one can add to the IIS configuration. The first recommendation is to use ISAPI gateway as the default module. The second recommendation is to define the content expiration so that unchanged static web content will be taken from the local browser cache instead requesting it from the server. The third recommendation is to define connection time-out to a finite value so that connections get dropped earlier when being idle for too long.

Use the ISAPI Gateway

The IBM Cognos ISAPI gateway module is native IIS code, which provides better resource management and performance. The CGI Module is a separate process that IIS needs to spawn on each request, which leads to slightly longer request times and in high-load environments, more resources consumed than ISAPI. Refer back to the section titled Configuring IIS 7 for IBM Cognos ISAPI on setting up the ISAPI Gateway as the default.

Content Expiration

For IBM Cognos Business Intelligence for reporting, it is recommended that content expiry be set on the **<COG_ROOT>/webcontent/pat/images** virtual directory.

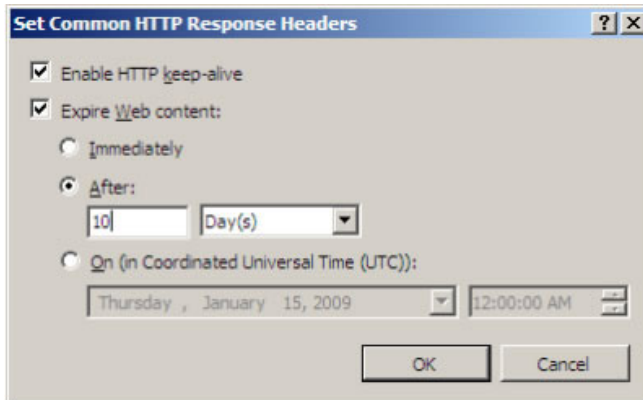
Each time a user opens Report Studio, the web browser checks with the web server to determine if images are current. With over 600 images, this can result in excess network traffic. You can postpone this check until a specified date by using the content expiry feature of the web server.

For additional information on setting content expiry, see the documentation for your web server.

Be aware that when IBM Cognos is upgraded, Report Studio users may have to clear their web browser cache to get the latest images.

1. In IIS Manager's left pane, select the **IBM Cognos 10** virtual directory by clicking on it. During the course of this document we used **ibmcognos** as the name of the virtual directory.
2. Change to **Features View** at the bottom of the middle pane, then double-click **HTTP Response Headers**.
3. In the far right Actions pane click **Set Common Headers**.
4. In the **Set Common HTTP Response Headers** dialog, check the **Expire Web Content:** checkbox, click the **After:** radiobutton and set the expiration period to 10 days. Lower values mean that content will expire earlier which leads to more requests, and higher values will cause less requests.

Figure 35: The Set Common HTTP Response Headers dialog with the adjusted web content expiry set to 10 days



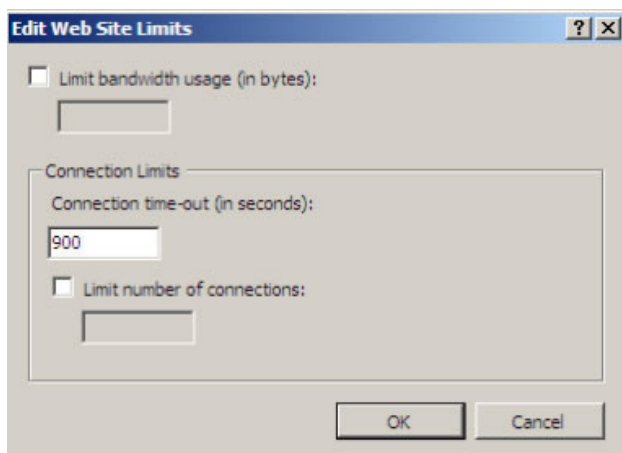
5. Click **OK**.

Connection Time-out

Connection Time-out can assist limiting the resources taken by idle connections. It can help reduce memory footprint and number of open idle ports.

1. In IIS Manager's left pane select the web site used to serve IBM Cognos Gateway content (likely named **Default Web Site**) by clicking on it.
2. In the far right Actions pane in the **Configure** section click on **Limits**.
3. In the Edit Web Site Limits dialog, set the **Connection time-out (in seconds):** field to a value of **900**.

Figure 36: The Edit Web Site Limits dialog showing the connection time-out set to 900 seconds



Configuring WebDAV (Optional)

Web-based Distributed Authoring and Versioning (WebDAV) is a protocol based on HTTP which allows clients to read, write and modify files served by a web server and save them back to the server.

IBM Cognos 10 uses this protocol to allow browsing for images in studios when a report author wants to add images to reports and analyses. Out of the box, IBM Cognos BI provides sample image files that are used by the product samples and these images will be used to demonstrate how to set up WebDAV. These sample image files are located underneath the virtual directory configured for the IBM Cognos 10 Gateway.

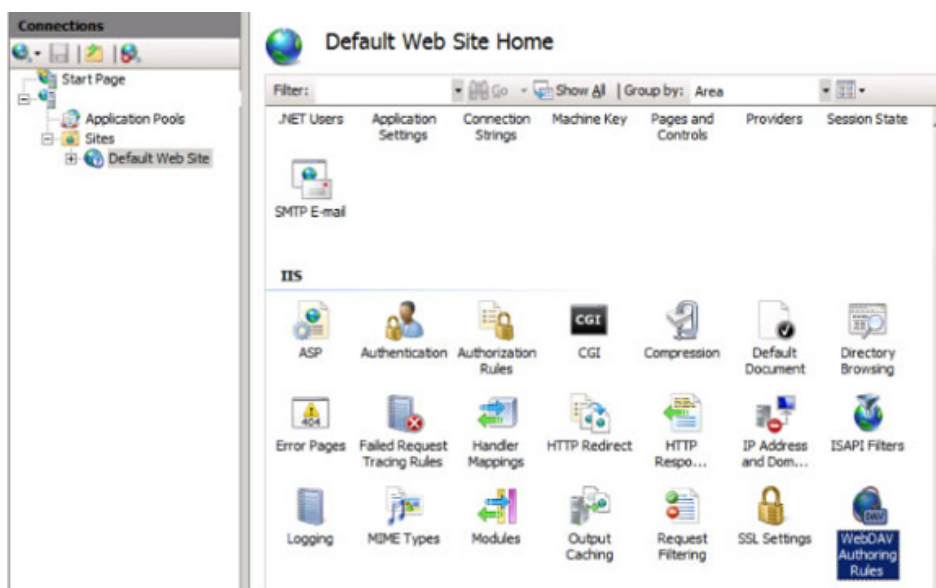
By default WebDAV is disabled in IIS and has to be explicitly enabled. In addition, authorization must be defined to ensure only the desired path of the virtual directory structure of the web server gets exposed and only authorized users are allowed to access files.

To use WebDAV, the **WebDAV Publishing Role Service** must be installed. Refer to Appendix A for details.

Enable WebDAV

1. In IIS Manager's left pane select the web site hosting the image files by clicking on it. For example, **Default Web Site**.
2. Change to **Features View** at the bottom of the middle pane, then click **WebDAV Authoring Rules**.

Figure 37: Location of WebDAV Authoring Rules



3. In the far right Action pane, click **Enable WebDAV**.

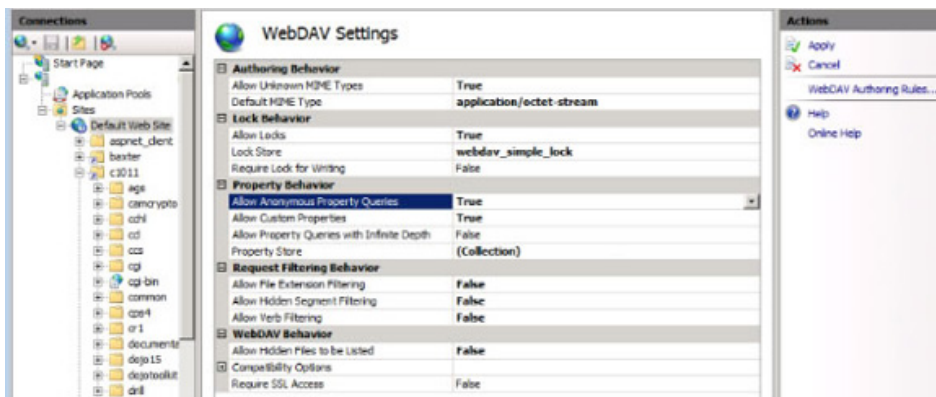
Enable Allow Anonymous Property Queries

By default, only authenticated users can query file properties. This option is required for Report Studio to successfully browse for images.

1. In the far right Action pane, click **WebDAV Settings...**
2. Under the **Property Behavior** section, locate **Allow Anonymous Property Queries**.

3. Change the value from **False** to **True**.

Figure 38: Enabling the Allow Anonymous Property Queries



4. Click **Apply** under the Actions pane on the far right.

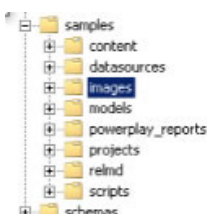
Define WebDAV access

The next step is to configure IIS authentication and authorization for the folders containing images. If the IBM Cognos 10 BI samples have been installed, there will be a folder of sample images at <COG_ROOT>/webcontent/samples/images which is accessible through IIS as <alias>/samples/images. We will use this folder to demonstrate the approach. Repeat it for any other folder containing images, even when in different virtual directories than the IBM Cognos 10 BI one.

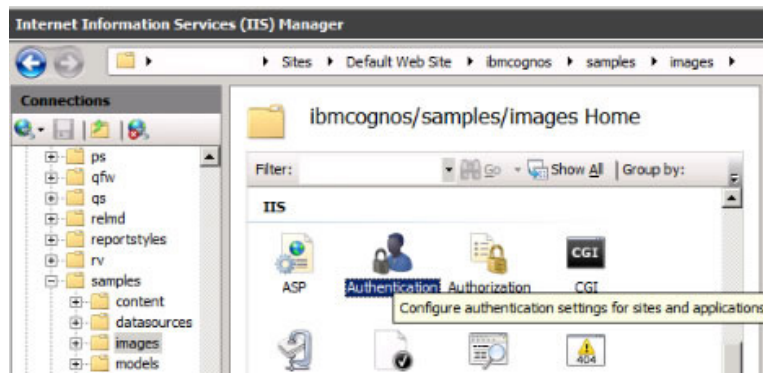
Note that in this very simple demonstrative example, we're enabling WebDAV access for anonymous users and on all files as read-only. Discuss with your Windows Administrator about which users or groups should have which access. The same applies for the authentication method. To have file access secured by Windows security, Windows authentication must be configured. However, this is out of the scope of this document.

1. In IIS Manager's left explorer pane, find the <alias>/samples/images folder and select it by clicking on it.

Figure 39: Location of the images folder underneath the IBM Cognos 10 alias/samples



2. In the lower middle pane of IIS Manager, switch to **Feature View** and double-click on **Authentication**. This will display the configured authentication methods for this virtual folder in the middle pane.

Figure 40: Location of Authentication

3. In the middle pane, select **Anonymous Authentication** by clicking on it.
4. If the Status column states **Disabled**, in the far right Actions pane click **Enable** to enable anonymous authentication for this folder.

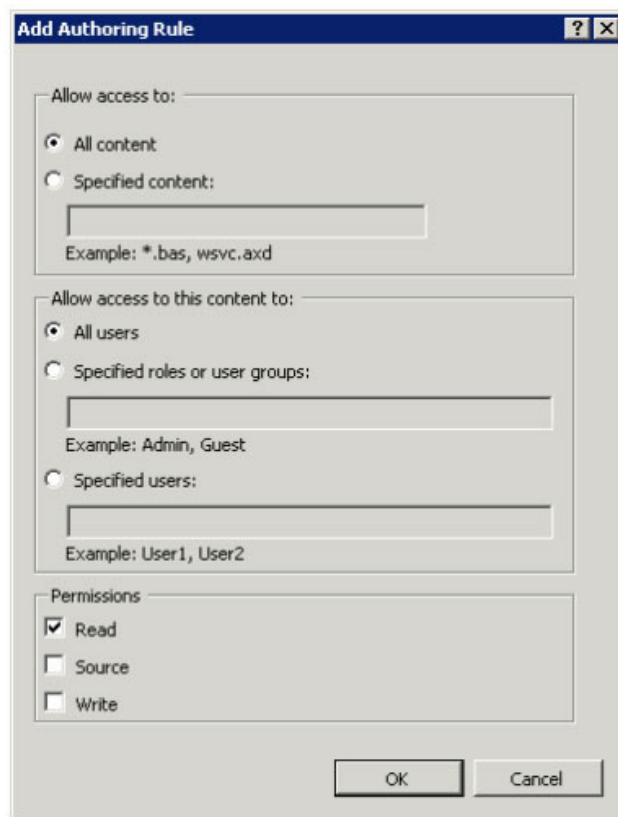
Figure 41: Enabling anonymous authentication

Authentication		
Group by: No Grouping		
Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

This will allow anyone access to the folder without authentication. Be aware that IIS uses the special **local IIS user account** for file access in this configuration. The files in the <COG_ROOT>/webcontent/samples/images folder therefore must be accessible for this account for this to work.

5. In IIS Manager's left explorer pane, find the **<alias>/samples/images** and select it again by clicking on it.
6. Click on **WebDAV Authoring Rules** in the middle pane, showing the **Features View** for this folder.
7. In the far right Actions pane, click on **Add Authoring Rule...**
8. In the **Add Authoring Rule** dialog, do the following:
 - In the **Allow access to:** section, click the **All content** radiobutton.
 - In the **Allow access to this content to:** section, click the **All users** radiobutton.
 - In the **Permissions:** section, click to check the **Read** checkbox.

Figure 42: Add Authoring Rules dialog with required options to define WebDAV access



9. Click **OK** to save the changes.

At this point, it should be possible to see the image files when browsing in one of the IBM Cognos 10 studios such as Report Studio.

Enable Secure Socket Layer (SSL) communication

For sake of completeness this document will provide the pointers and steps required to configure the IBM Cognos 10 Gateway for SSL. This task has several steps which are,

1. Request a web server certificate for SSL.
2. Install the web server certificate to the web server.
3. Amend IBM Cognos Configuration settings on all affected installs of IBM Cognos 10.
4. Import a certificate required for establishing trust into IBM Cognos 10 trust store(s).

The first two steps are outside of the IBM Cognos domain and must be implemented by the web server administrator or someone with Public Key Infrastructure (PKI) knowledge. There are some best practices to follow though.

- The web server certificate should not be self-signed - that is the certificate's subject and issuer shouldn't be identical. These certificates are not insecure and are not trusted by IBM

Cognos. They should be used for test or troubleshooting only as they are unsuitable by modern security standards for production systems. Self-signed certificates must bear the CA:True X.509 extension to work with IBM Cognos since they are server certificate and CA certificate in one.

The best practice is to set up your own Certifying Authority (CA) and have it sign the web server certificate with its CA certificate. Microsoft Server 2008 contains the Active Directory Certificate Services which can be used for this purpose. A free and widely adopted standard tool is OpenSSL which exists for many platforms and various guides can be found online.

- The web server certificate subject Distinguished Name (DN) (the identity used by the web server) must be the server name and should be specified using a Fully Qualified Domain Naming (FQDN) scheme such as CN=<serverhost>.<domain>.<suffix>, ...<other optional DN attributes>. This is because browsers will compare the certificate subject to the URL used to call the server and issue a warning or reject the certificate if they don't match up.

The best practice is to use FQDN for either certificates and any URI used to call the IBM Cognos 10 Gateway. The Gateway URI specified in IBM Cognos Configuration should always use a FQDN - "localhost" is not feasible.

- SSL implements, amongst other things, encrypted communication. The protocol and method used for the encryption is called the cipher and is based on a key which, depending on its length in bits, is considered to be either weak or strong. Recent web servers should use strong ciphers, which is keys with a length of 128bits and higher.

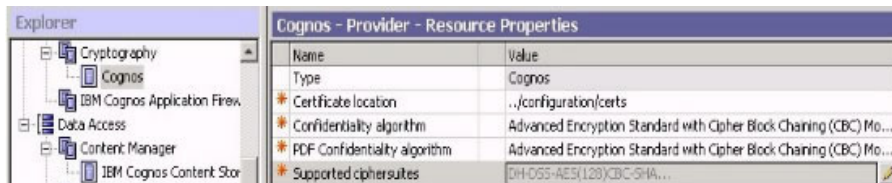
The web server should be configured to disallow weak ciphers for security reasons. IIS 7.x only supports strong ciphers and therefore adheres to this best practice out of the box. IBM Cognos 10 does support strong ciphers out of the box and they are enabled for the supported ciphersuites option in IBM Cognos Configuration by default.

For details on how to configure IIS 7.x for SSL consult the following link on the Microsoft IIS 7 web site, <http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis-7-and-above/>.

Steps 3 and 4 are covered in the *IBM Cognos 10 Installation and Configuration Guide*. While the general steps provided in the *IBM Cognos 10 Installation and Configuration Guide* apply to the setups described in this document as well, there are several things to consider.

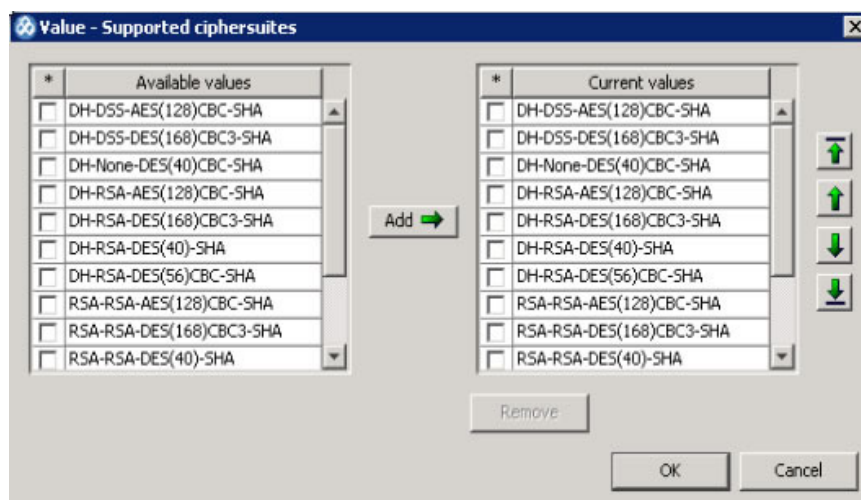
- The import of the CA certificate (or the self-signed certificate with CA:True extension) must be implemented on any IBM Cognos 10 install which references the IBM Cognos 10 Gateway. This includes Application Tier installs and Content Manager installs, not only for IBM Cognos 10 BI but also for IBM Cognos Planning, IBM Cognos PowerPlay and other tools of the IBM Cognos 10 suite.
- In addition to changing the value of the Gateway URI in IBM Cognos Configuration, one must ensure the strong ciphers are enabled for SSL as well. To do this, in IBM Cognos Configuration check the **Supported ciphersuites** property at **Security > Cryptography > Cognos**.

Figure 43: IBM Cognos Configuration showing the supported ciphersuites



Click on the **Edit** symbol to display the list of enabled ciphersuites. The dialog will display two lists - on the left will be one labeled **Available values** and on the right one labeled **Current values**. Current values should contain all entries from Available values. If not, add ciphers from the Available values list by checking them and click the **Add** button in the middle between the two lists. Click **OK** to save the changes.

Figure 44: List of supported ciphersuites



- If using other IBM Cognos client tools to connect to this IBM Cognos 10 Gateway (for example, IBM Cognos TM1 Architect or Web, IBM Cognos Executive Viewer or IBM Cognos Planning) these tools must establish trust to the web server certificate as well by importing the CA certificate into their respective trust stores. It's a good idea to inform the administrator of these IBM Cognos products that additional configuration steps are required. Not all of these tools use their own trust stores but leverage the machine trust store of the Windows box they run on. They should implement the step described next.
- For Internet Explorer clients, the CA certificate which signed the web server certificate should be imported as a trusted root certification authority. Consult your Windows administrator for details. By employing your favorite search engine, the internet will provide more verbose guides for this task.

Troubleshooting

HTTP Error 404.0 – File Not Found

The HTTP error 404.0 is returned whenever IIS cannot find a file at the specified path.

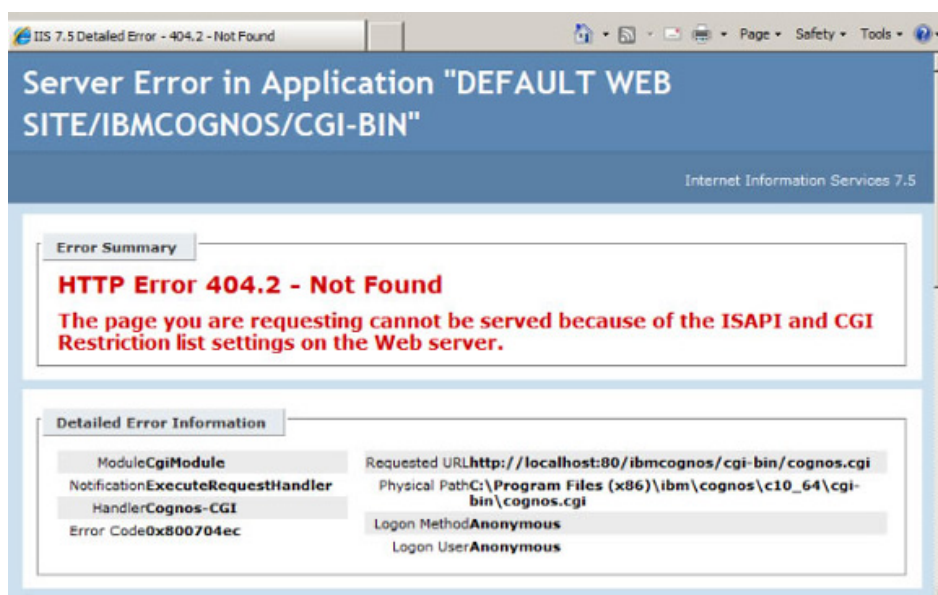
Possible solutions are,

- The application cgi-bin has not been setup or is not at the correct level as a child to the main IBM Cognos 10 alias (virtual directory).
- Type in the URI or the virtual directory name.
- IIS is not started.

HTTP Error 404.2 – Not Found

Hitting the IBM Cognos 10 Gateway URI leads to “HTTP 404.2 - The page you are requesting cannot be served because of the ISAPI and CGI Restriction list settings on the Web server.”

Figure 45: Internet Explorer displaying the HTTP 404.2 - Not found error



Possible solutions are,

- Re-check the ISAPI restrictions.
- Verify the URI, it is possible that it is redirected or calling the wrong IBM Cognos 10 Gateway module.

HTTP Error 503 – Service Unavailable

The service is unavailable when accessing an IBM Cognos 10 Gateway URI.

A possible solution is to ensure the Application Pool hosting the IBM Cognos 10 Gateway modules is started.

HTTP 500 – Internal server error

An internal server error usually means there is a problem with the resource you are looking for and it cannot be displayed.

To diagnose the error:

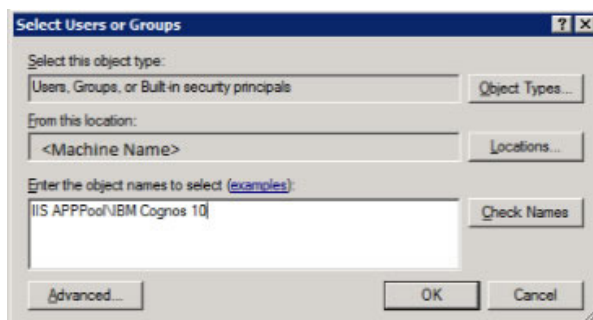
1. Navigate to the created **cgi-bin** application.
2. In the middle pane, double-click **Error Pages** within the **IIS** section.
3. In the far right pane, click **Edit Feature Settings...**
4. Change the **Error Responses** to **Detailed errors**.
5. Click **OK**.

Once the issue has been determined, it is recommended to revert this setting back to Detailed errors for local requests and custom error pages for remote requests.

Possible causes and solutions are,

1. Ensure the application pool has file system access to cgi-bin. It is possible that the file system has been locked down, preventing the IIS process from accessing the required module handlers. To add the application pool user into Windows Explorer file folder security:
 - For Windows 2008 and lower: Check the **Identity** of the application pool (typically **Network Service**) and ensure that identity has **Full Control** over cgi-bin.
 - For Windows 2008 SP2+ or Windows 2008 R2 and higher: A **unique identity** is created for each application pool. The name of the identity is the application pool name itself. To add this identity in the file system security, click Locations, change the domain to local machine name. Then type **IIS APPPool\<apppoolname>** in the **Enter the object names to select** field. Click **Check Names** to resolve the ID.

Figure 46: Allowing the IIS application pool ID access to the IBM Cognos install at the file system level



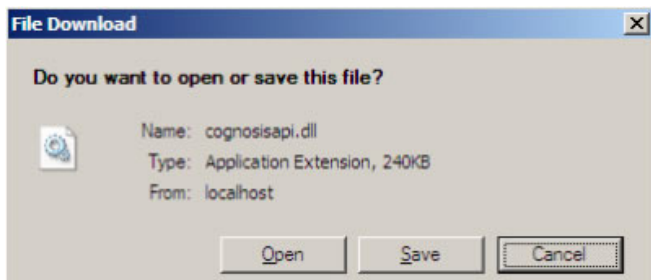
For more information refer to <http://www.iis.net/learn/manage/configuring-security/application-pool-identities>.

2. Ensure that the correct bitness is used on the application pool. If the 32-bit Gateway is installed within cgi-bin but the application pool is configured for 64-bit or vice versa, an HTTP 500 error will occur. Review the **Setting up the Application Pool container section** to correct the installation.

File download dialog appears when accessing the ISAPI module

A file download dialog box, asking whether to open, save or cancel pops up when accessing the IBM Cognos 10 ISAPI Gateway module.

Figure 47: File Download dialog presented by IIS when using ISAPI URL

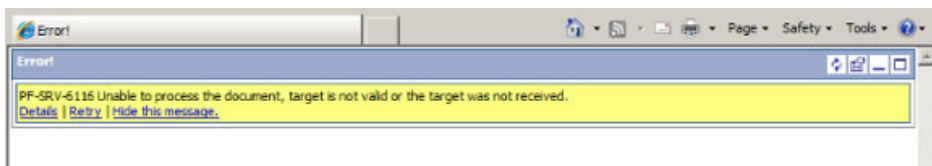


A possible solution is to check the **Edit Feature Permission** for the ISAPI handler mapping. It must be set to **Execute**.

PF-SRV-6116 when starting IBM Cognos Administration

When invoking IBM Cognos Administration, the error PF-SRV-6116 is displayed in a yellow box at the top of the page and the remainder of the browser window remains plain white.

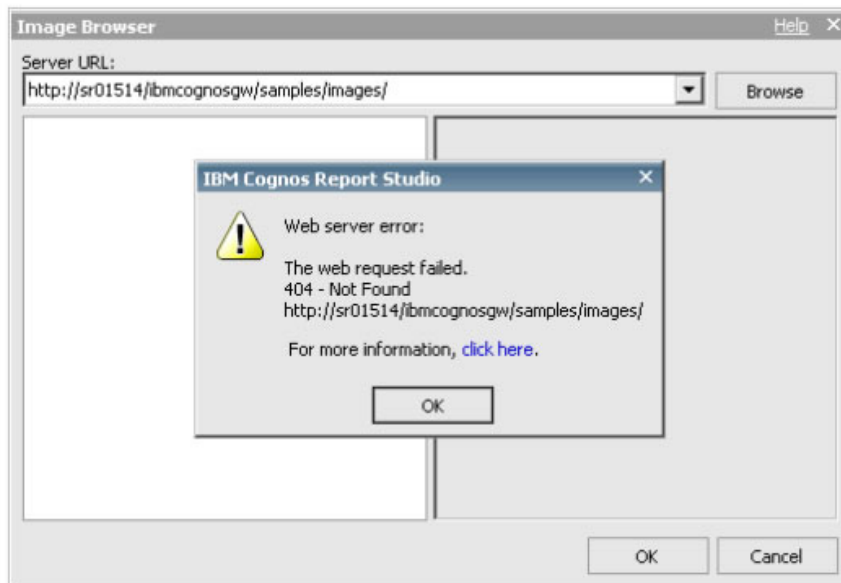
Figure 48: Error PF-SRV-6116 in IBM Cognos Administration



Error when browsing for images in Report Studio

When browsing for images in Report Studio the following error comes up in a dialog box,

```
Web Server error:  
The web request failed.  
404 - Not Found  
<url>
```

Figure 49: Web Server error dialog when browsing for images in Report Studio

Possible solutions are,

- Ensure WebDAV is configured for IIS. Refer to the **Configuring WebDAV (optional)** section.
- If the URL points to <alias>/samples/images, make sure the IBM Cognos 10 BI samples have been installed. The sample images are not part of the base IBM Cognos 10 BI install.

Appendix A – IIS Installation Requirements

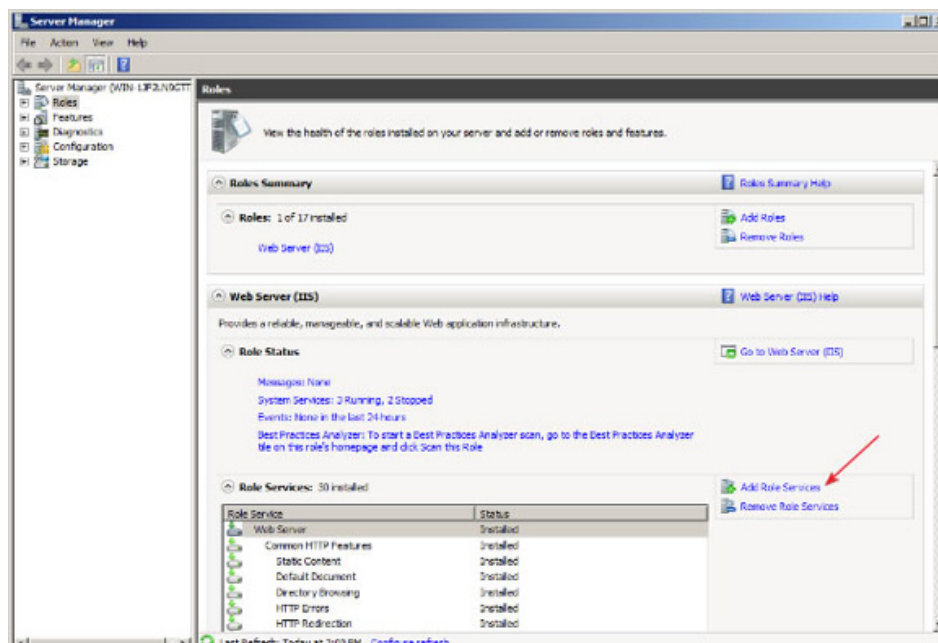
Before being able to set up IBM Cognos 10 with IIS 7.x, the following installation prerequisites regarding IIS7.x must be fulfilled:

- The **Web Server** role must have been added to the Microsoft Server 2008 (R2).
- In addition, the following **Role Services** for the Web Server role must be installed:
 - Common HTTP Features with the following sub-components
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Management Tools with the following sub-components
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
- For cognos.cgi usage, the **CGI Role** service must be installed.
- For cognosisapi.dll usage, the **ISAPI Extensions Role** service must be installed.
- For WebDAV use, the **WebDAV Publishing Role service** must be installed.

To verify the installed Role Services, as a local administrator click **Start > Administrative Tools > Server Manager**. The **Roles** screen now should now be available.

In the section of the Roles screen for **Web Server (IIS)**, a **Role Services** sub-category which lists all installed role services. If any of the **Role Services** listed above is missing, click **Add Role Services** and install the missing services. This may require a restart of the IIS server.

Figure 50: Server Manager displaying the installed server roles and corresponding role services



Appendix B – Disabling Windows 2008 security features for troubleshooting

Microsoft Windows 2008 (R2) introduced several new security features which allows for the hardening of a machine. Among these features are User Account Control (UAC), Internet Explorer Enhanced Security Configuration (IE ESC) and Data Execution Prevention (DEP).

Each of those features affects IBM Cognos 10 components executing on the server. If problems occur, these security features could be temporarily disabled by an Administrator. Some behaviors which might require one to temporarily disable a security feature for the purpose of ruling it out as the root cause are:

- DEP - Issues with application pools such as CGI or ISAPI; calls do not complete or crash.
- IE ESC - Internet Explorer blocking access to the Gateway URI; Error messages when accessing the Gateway URI; redirects are not working.
- UAC - Need to run some executable as an administrator but the administrator credentials cannot be shared. Ask the administrator to disable UAC temporarily during setup/configuration.

Disabling any of these features should be done temporarily for troubleshooting purposes only. It is strongly advised to leave them all in place to adhere to security practices and standards as IBM

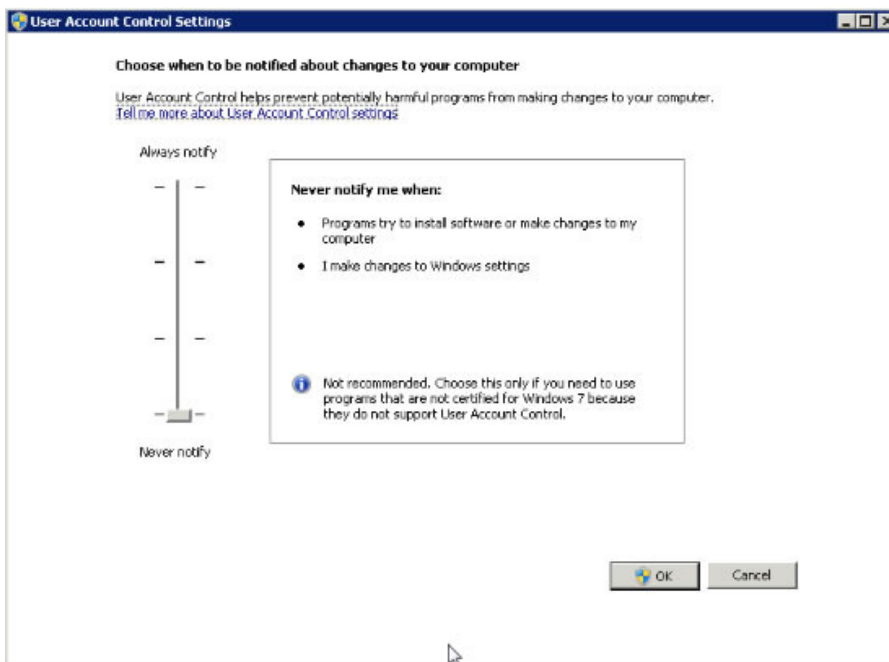
Cognos 10 is 100% compatible with all of these features. Be aware that disabling any of those features may impose a security risk to the server and may violate corporate security policies. For details on each of the features, please refer to the Microsoft Windows 2008 TechNet pages at [http://technet.microsoft.com/en-us/library/cc754279\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754279(Ws.10).aspx).

Disable UAC

As a local Administrator,

- From the **Start Menu**, select **Control Panel** and select **User Accounts**.
- In User Accounts page, click on **Change User Account Control Settings**.
- In the User Account Control Settings screen, move the slider control to **Never notify**, the lowest possible setting.

Figure 51: The User Account Control settings dialog with the slider control to specify the notification level



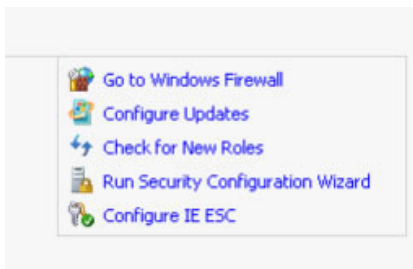
- Click **OK** to save the changes.

Turn off IE Enhanced Security Configuration (IE ESC)

To disable IE ESC, as an administrator,

- From the **Start Menu**, select **Administrative Tools** and then select **Server Manager**.
- In the Server Manager left explorer pane, select the root element labelled **Server Manager <hostname>** by clicking on it.
- In the Server Manager right pane, context dependent options will be presented. Click on **Configure IE ESC**.

Figure 52: Server Manager's options pane listing the supported configuration options, such as Firewall Configuration and Configure IE ESC



- This will present the **Internet Explorer Enhanced Security Configuration** dialog. Change the status of the IE ESC for Administrators and Users to Off by clicking the associated radio buttons and click **OK** to save the changes.

Figure 53: IE Enhanced Security Configuration Dialog showing the status of IE ESC for administrators and regular users



Turn off DEP on server

To disable DEP, as an administrator,

- From the **Start Menu**, select **Computer** and then select **Properties**.
- In the **System Properties** window, click **Advanced System Settings** in the left options pane.
- In the **Advanced System Properties** dialog, select the **Advanced** tab.

- On the Advanced tab, click **Settings** in the **Performance** section.
- From the **Performance Options** dialog, select the **Data Execution Prevention** tab.
- Select the first option **Turn on DEP for essential Windows programs and services only**.
- Click **OK** to save the changes.

Figure 54: The Data Execution Prevention tab showing the two options for enabling DEP for essential Windows programs and services only



More information about IBM Cognos BI version 10 can be found in the [Related topics](#) section below.

Related topics

- [Supported Environments](#)
- [Information Center](#)
- [A Redbook about IBM Cognos 10](#)
- [Customizing the IBM Cognos 10 Login Page](#)
- [The official IIS7 site](#)

© Copyright IBM Corporation 2011, 2015

(www.ibm.com/legal/copytrade.shtml)

[Trademarks](#)

(www.ibm.com/developerworks/ibm/trademarks/)