Miracle Service™

Configuring Microsoft®
Internet Information Service
(IIS6 & IIS7)

Configuring Microsoft® Internet Information Service (IIS6 & IIS7) Guide

Last revised: June 25, 2012

Configuring Microsoft®
Internet Information Service (IIS6 & IIS7)

Table of Contents

Configure Microsoft Internet Information Service (IIS6)

Step 1 – Start Internet Information Services

Start the Internet Information Services (IIS) application. It normally resides under administrative tools in your Control Panel.

Before starting the IIS you should check the properties of both the IIS Admin and World Wide Web Publishing Services in your Services Tool. It is recommended that you configure the Start-up Type as Automatic for both of these Services.
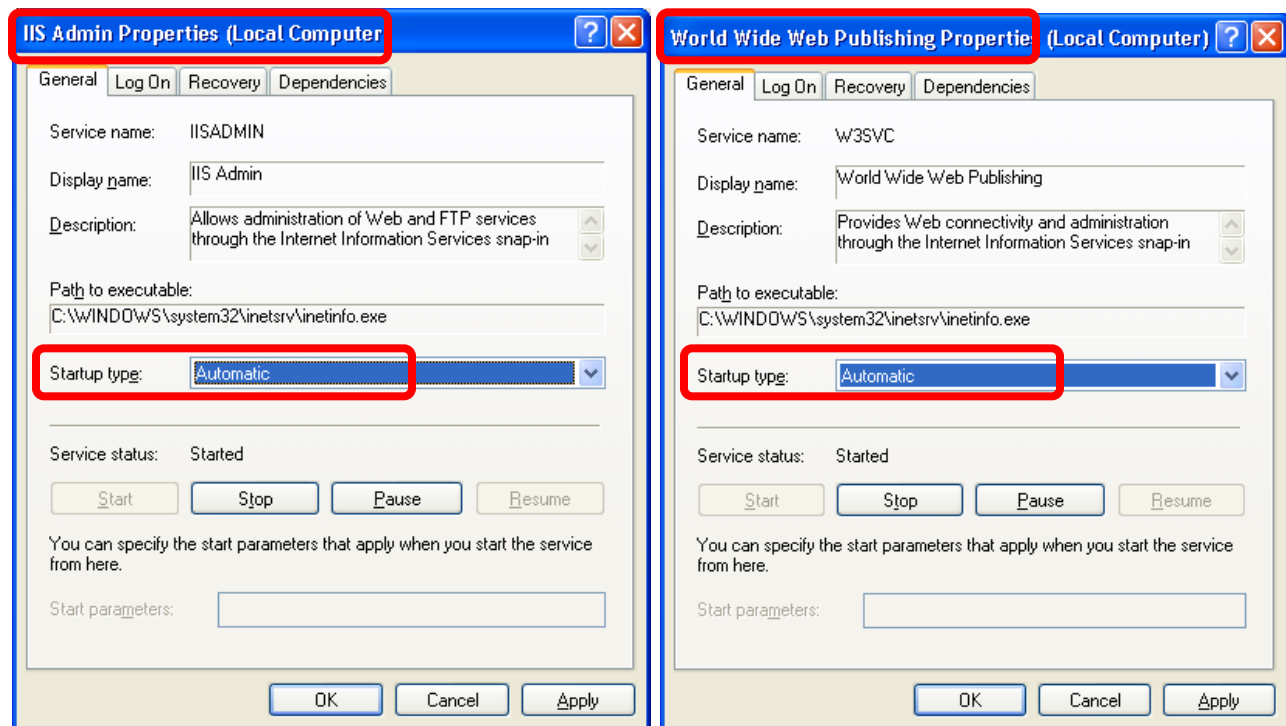
Once you have verified that the IIS Admin and World Wide Web Publishing Services are running and configured for Automatic Start-up Type, you can open your IIS Service. The IIS Service is located in your Control Panel under Administrative Tools. (Start – Control Panel – Administrative Tools)
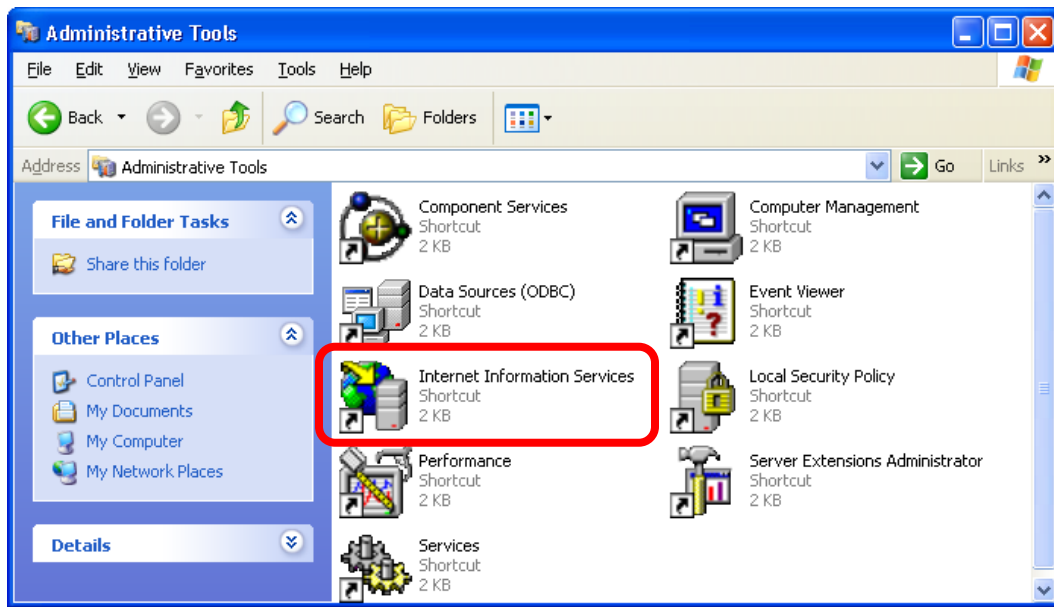
Step 2 – Share your Miracle Service Database Directory

Since the Miracle Service Directory (typically - C:\MiracleDB) will be shared with the Internet Information Service application, you must configure the Miracle Service directory Properties to allow the folder to be shared. To configure the Folder Properties, navigate to the database folder using Windows Explorer. Right click on the folder and select "Sharing and Security".
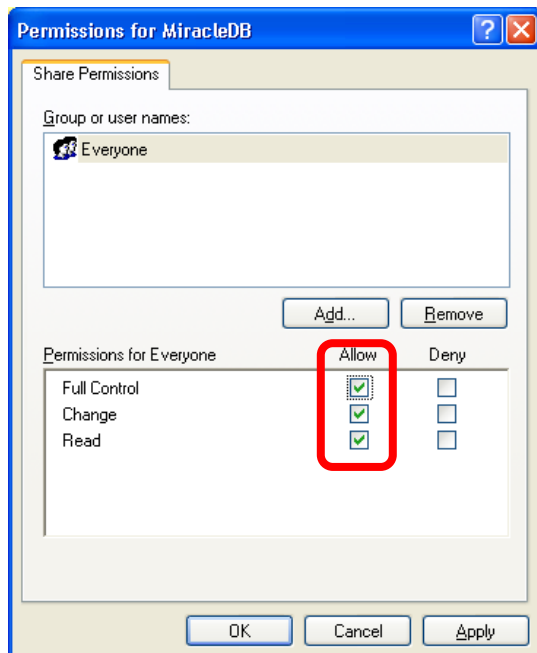
Once the Properties window is open, select the "Sharing" tab and "Share this folder".

Next click the "Permissions button." This will open the window used to define the level of permissions being granted. Select "Everyone" and the check "Full Control" under Allow.

The action should automatically check all of the Permission levels below Allow. This would allow Change and Read as well. If this does not happen automatically, manually check Change and Read under Allow as well.

Next Select the Security tab. This is where you will set-up sharing the folder with the Internet User for your Web Site.

Select 'Add…' to add a Group or user name. We will be adding the Internet User to this list.
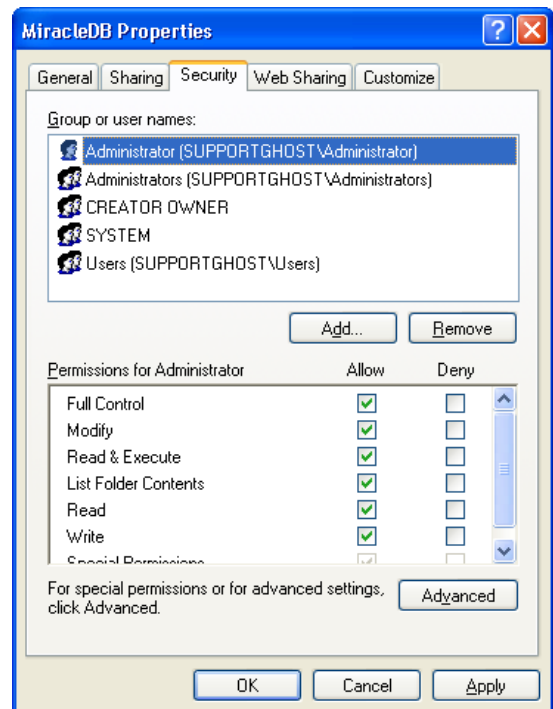
Select 'Advanced'

Locate the IUSR_*Computer* where the *Computer* is the name of the specific computer for the Web server user. If the web site is on a computer called WebServer, then you must locate the IUSR_WebServer.
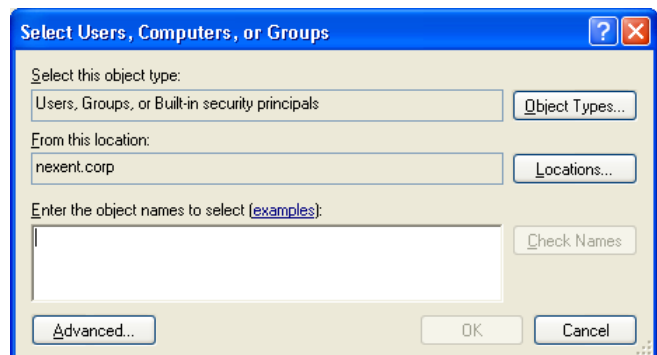
Scroll down the list until you have located the correct IUSR and then select the IUSR and select 'OK'.
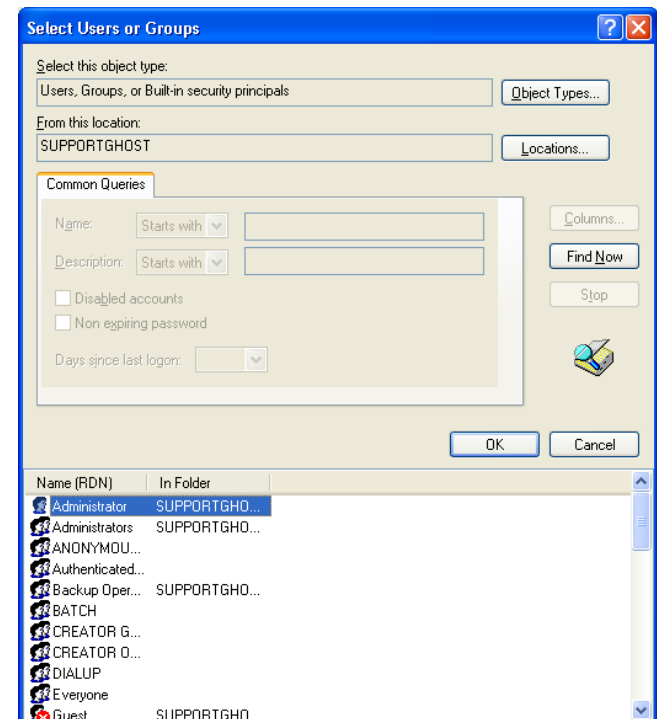
IIS7 and Server 2008 Special Considerations:
With IIS7 and Server 2008 there are 4 users that are important to configure. These are:
IUSR,
IIS_IUSR,
NETWORK, and
NETWORK SERVICE.

We recommend giving all of these users read and write access to the MiracleDB folder.

Click OK again on this screen.
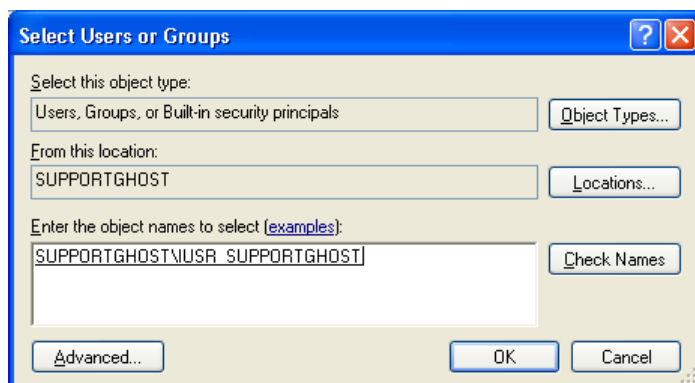
Check to ensure you have added the Internet Guest Account for the correct computer. Select this user to configure its Permissions.

Once you have selected the user it will be highlighted. Check 'Read' and 'Write' permissions for this user.

Click OK to complete the modification of the permissions.
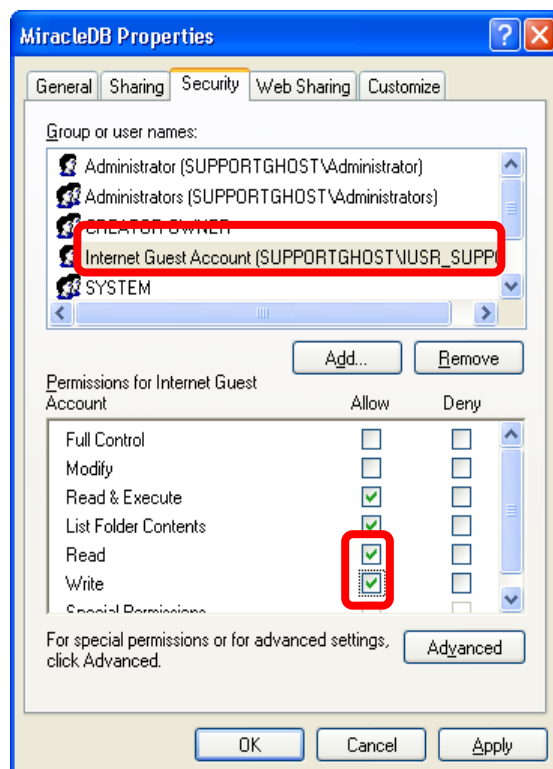
Step 3 – Configure the Security Settings on the MiracleDB Folder

Once the folder is shared select the Security tab to configure the same users to have sufficient security rights to also read and write to the files in the folder and all sub-folders and files.

Step 4 – Share your Inetpub Directory

The Inetpub folder must be shared so the Internet user can update the XML parameters file. In a Windows Explorer select the C:\Inetpub\wwwroot\MiracleService folder.
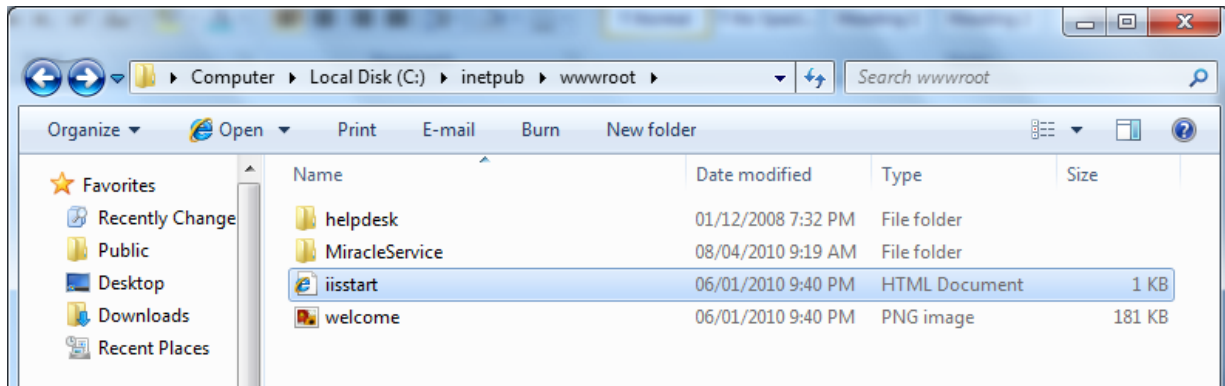
Right click and select Properties.
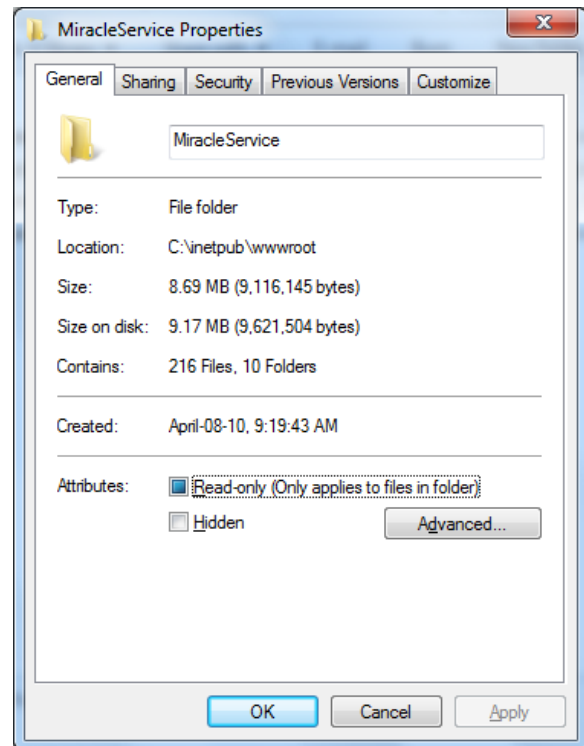
Select the Sharing Tab. And then "Advanced Sharing"
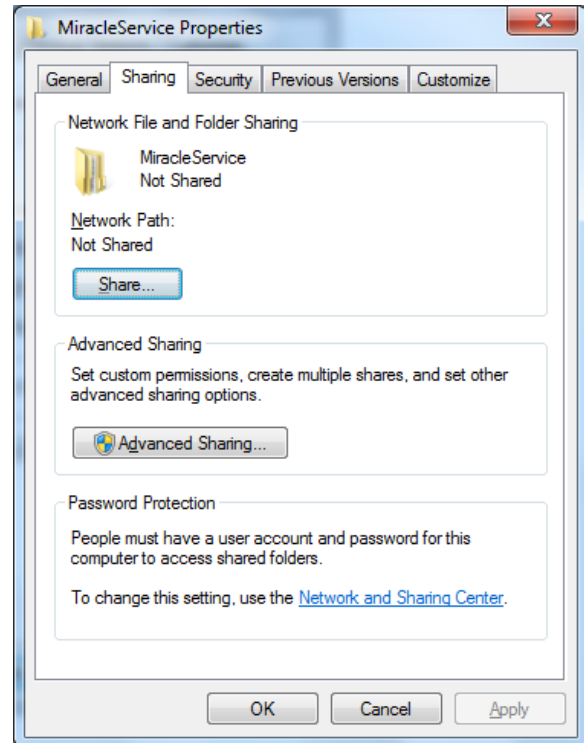
In the Advanced Sharing area you will want to configure the users that will require the rights to update the XML file. With IIS7 and Server 2008 there are 4 users that are important to configure. These are:

IUSR,
IIS_IUSR,
NETWORK, and
NETWORK SERVICE.

We recommend giving all of these users read and write access to the MiracleService folder. Through our experience we have discovered that combinations of these are often sufficient to set-up and have the Technician Portal function correctly; however, for completeness and to standardize these instructions we are including the recommendation on the full set.

Click the 'Advanced Sharing' and configure these users to have at least read / write access to this folder and all sub-folders.

Step 5 – Configure the Security Settings on the Inetpub Folder

Once the folder is shared select the Security tab to configure the same users to have sufficient security rights to also read and write to the files in the folder and all sub-folders and files.

Step 6 – Configure the Virtual Directory

A Virtual Directory was setup automatically during the installation process. At this time you need to verify the Properties of the directory. When you right click on the Virtual Directory you can select Properties. The following window appears.
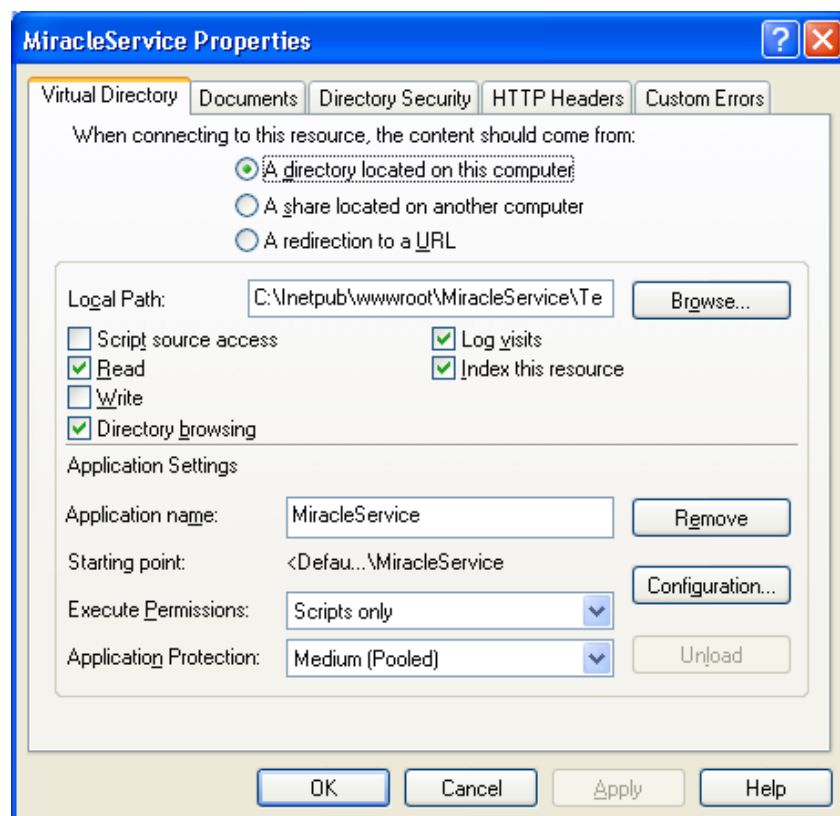

Select the "Configuration…" button and then the Options tab. Check to ensure that the Parent Paths is enabled. Also check the Default ASP language and the ASP Script Timeout is 90 seconds.

During the set-up you should consider the Session Timeout setting. The Timeout is defaulted at 20 minutes. After 20 minutes the session will timeout and the remote user will need to log back in to the portal. You should modify this to suit your business security concerns and impact on your technicians' data entry efforts.
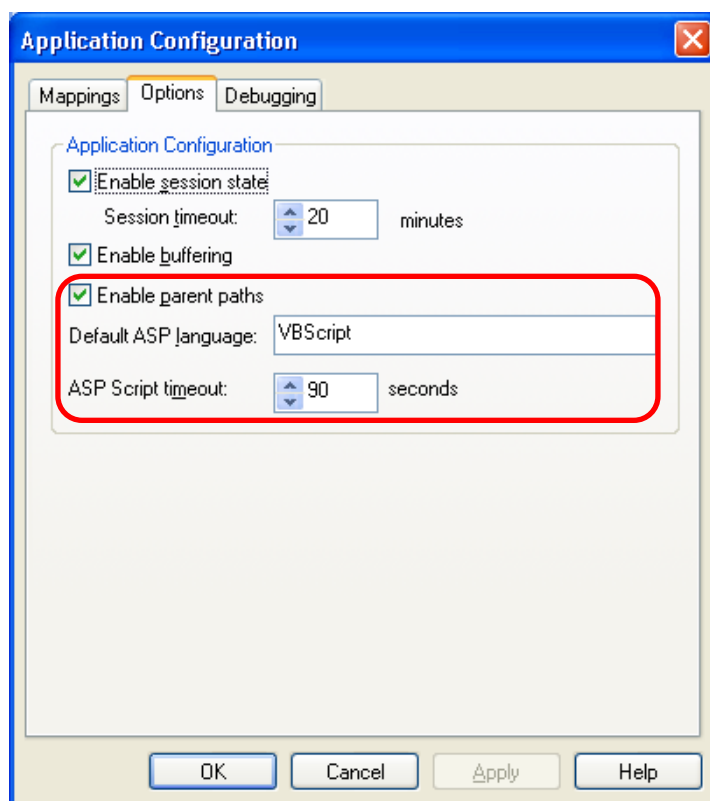
Configure Microsoft Internet Information Service (IIS7)

Configuring IIS7 is essentially the same as IIS6. While the user interface has changed considerably, the concepts are the same. The other issue with IIS7 is not all of the required feature come installed as standard. This means you will need to install the other necessary features. The following is an overview of some of the important features and changes.

Step 1 – Install the Required Features

To install the required features go to Programs and Features and run "Turn Windows features on or off".

In the feature list expand the Internet Information Services, then Web Management Tools and finally IIS6 Management Compatibility. Ensure IIS6 Management Compatibility is installed.
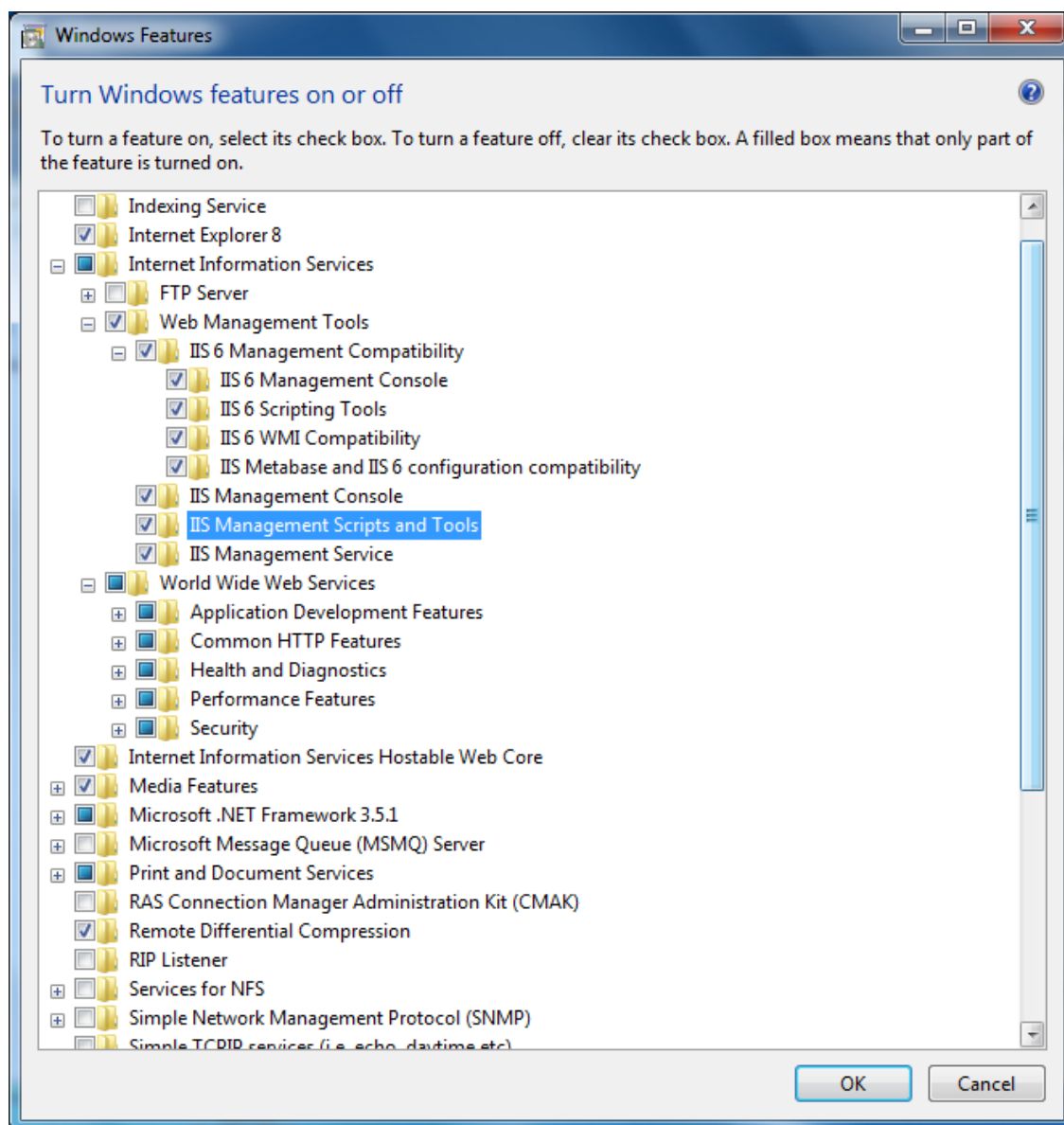
Next Expand the World Wide Web Services and then the Application Development Features. In this feature screen make sure that ASP and ASP.NET are installed. When you check ASP and ASP.NET the other features should automatically be checked. These include: .NET Extensibility, ISAPI Extensions and ISAPI Filters.
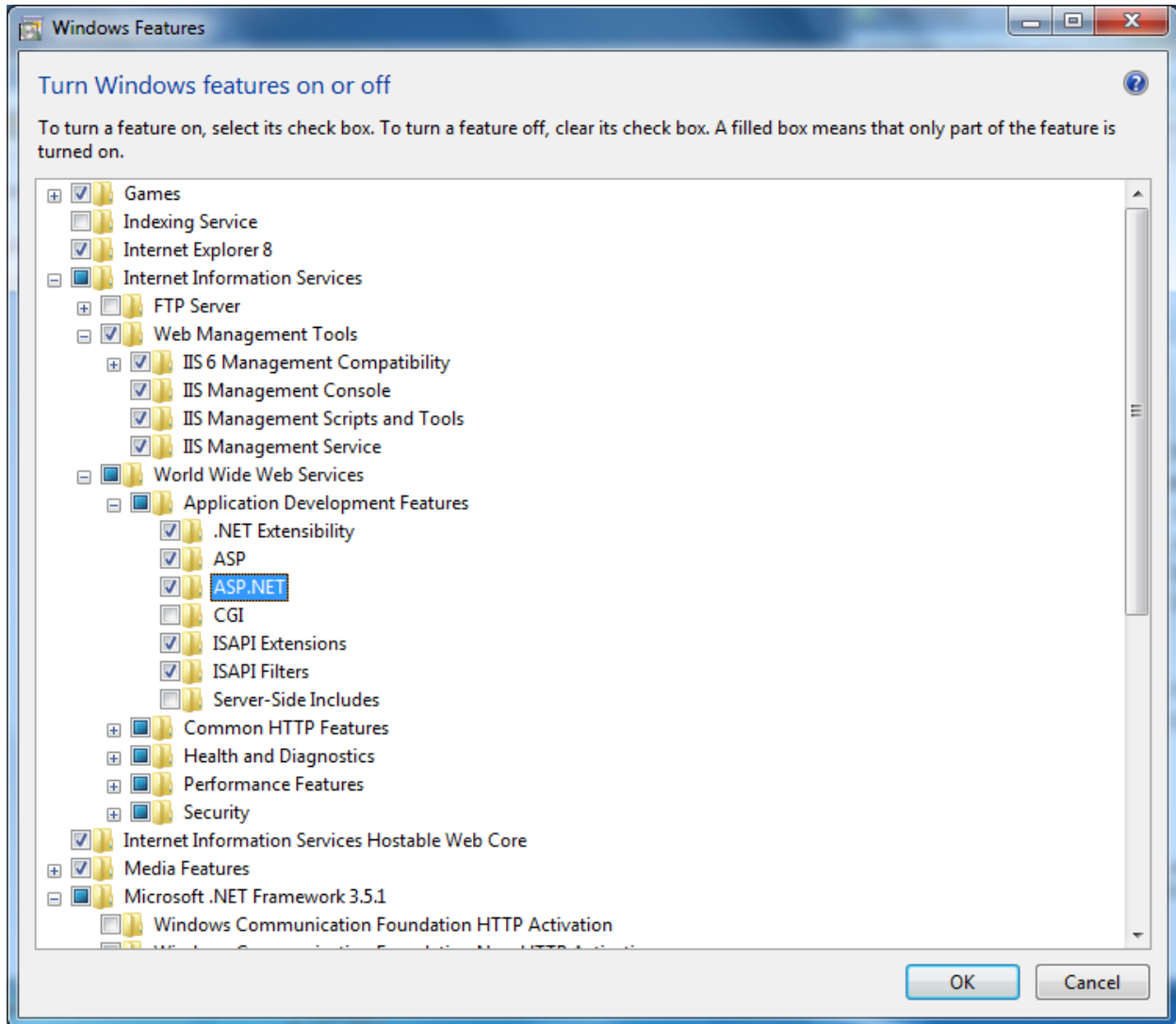
Step 2 – Configure Folder and Security Permissions

The folder and security permissions must be correctly configured for the IIS7 installation. It is essential the folder permissions are configured for the MiracleDB folder and the Inetpub\MiracleService folder as specified in Step 2, 3, 4 and 5 in the IIS6 Configuration steps shown previously in this document.

Step 3 – Configure the Virtual Directory

A Virtual Directory was setup automatically during the installation process. At this time you need to verify the Properties of the virtual directory. When you click on the Virtual Directory the following window appears.
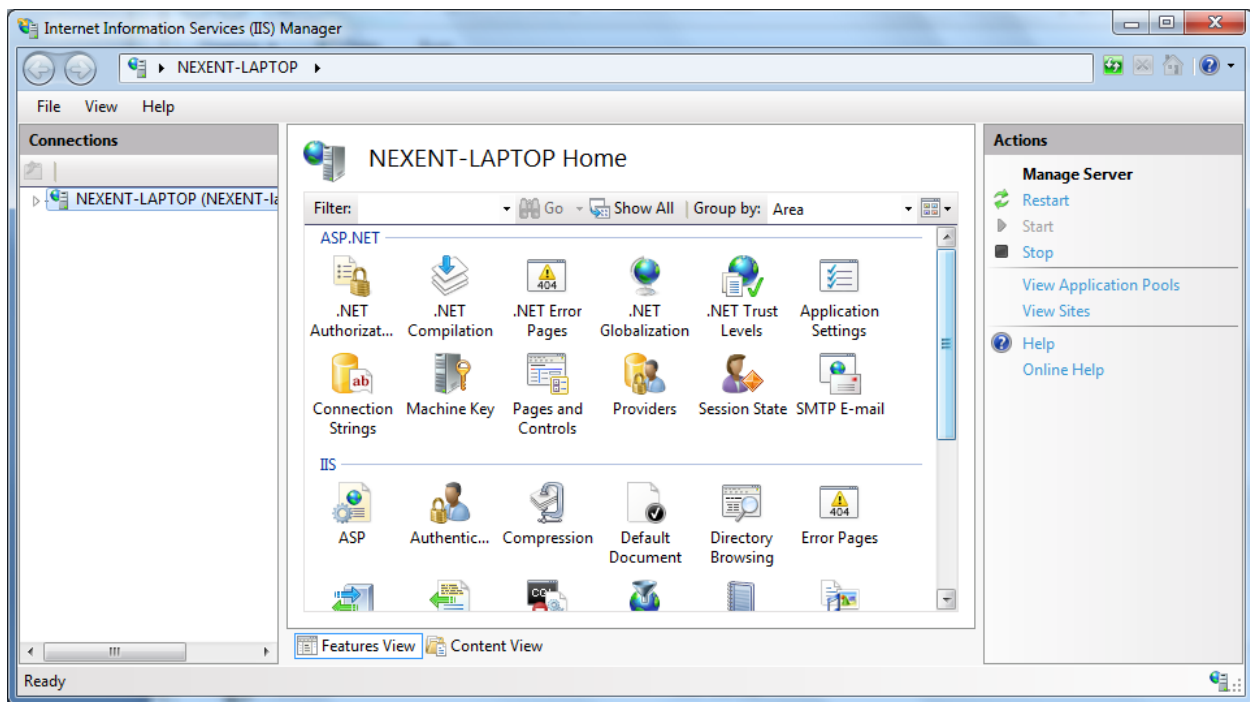
Double Click the ASP feature to open the ASP feature window.
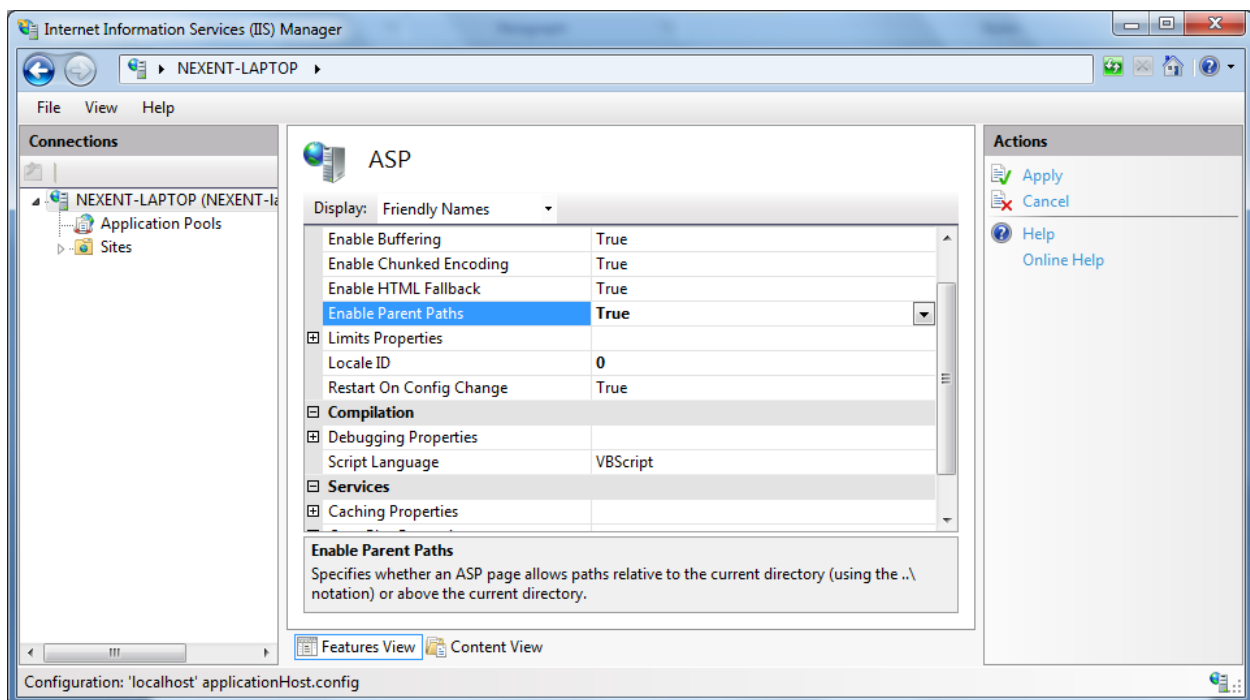
Set the Enable Parent Paths to True and click Apply.

Step 4 - Configure 32-Bit Enable Application Pool

Click the Application Pool (Default App Pool) and select the "Advanced Settings" in the Action pane on the right. Select 'True' for the Enable 32-Bit Applications.
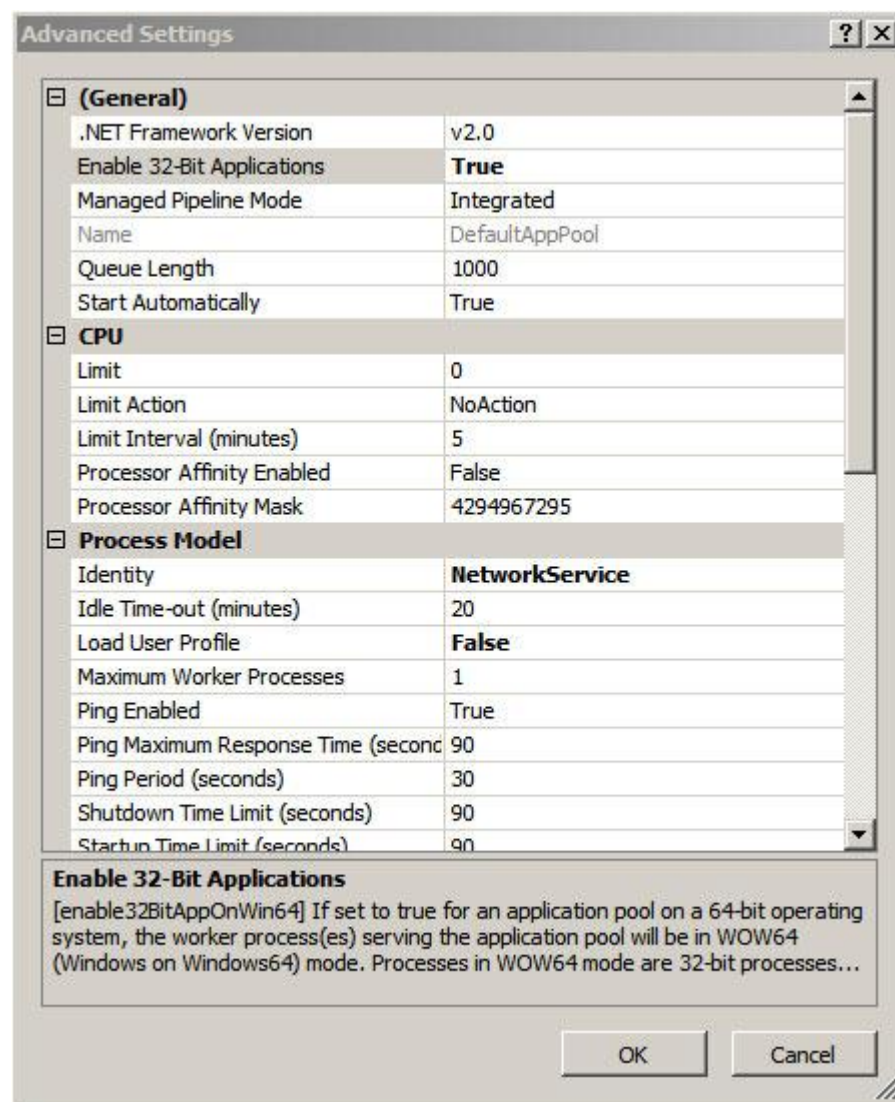
Step 5 – Configure the Default Documents

Double Click the Default Documents and modify the document list to remove all of the documents except 'default.asp'.

Step 6 – Other IIS7 Settings to Check

IIS7 has many features and settings and every server can be configured differently. Here are a few items to check and confirm the settings.

1) Ensure the Default Web Site is set to port 80.
   Click on the Default Web Site and then select the 'Binding' link in the Action pane in the right window. Verify the Port is set to port 80.

2) Confirm the Physical Path is correct.
Click on the Virtual Directory and select 'Basic Settings' in the right Action pane.
Review the path to ensure it is pointing to the correct location. It should typically be set to:

C:\Inetpub\wwwroot\MiracleService\TechnicianPortal

3) Convert the Virtual Directory to an Application
On some systems, it is necessary to convert the Virtual Directory to an application.

In the Internet Information Services (IIS) Manager select the Virtual Directory for the TechnicianPortal. Right click on this folder and if an option is available that says: "Convert to Application", select this option and allow IIS to convert the folder to an application. Note: if this option is not available and it only show "Add Application", do not run the Add Application function as it may duplicate this application.

4) For SBS 2008 it may be necessary to disable the compression application for the web environment as SBS 2008 only support a 64 Bit compression module. The following commands can be used to enable or disable the compression on a SBS 2008 server. Enter these commands at a command prompt with it running as administrator.

To Disable the compression:
%windir%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/httpCompression /-[name='xpress']

To Enable the compression:
%windir%\system32\inetsrv\appcmd.exe set config -
section:system.webServer/httpCompression
/+[name='xpress',doStaticCompression='false',dll='%windir%\system32\inetsrv\suscomp.
dll']

5) If you receive a HTTP 503 Error it may be necessary to manually configure some features of the web components as follows:

On SBS 2008 and other 64 bit editions of Windows 2008, additional steps are required after installation of Web Components. These steps ensure that the Web Components can run on the 64 bit system with other applications.

Warning:
  o **Back up files** before making changes.
  o Ensure that XML is correctly written. For general information about XML editing, see article Q12705.
  o Note that some lines below are wrapped for readability.

o Note that if you edit the lines referring to the "exppw" module, you MUST change both lines. If you do not, browsing to any page will fail with HTTP error 500.

To configure the Web Components:

1. Open a text editor or XML editor with elevated privileges (for instance, from the Start menu right-click Notepad and select *Run as Administrator*).

   In the file %windir%\system32\inetsrv\config\applicationhost.config:
   o change the line
   <add name="PasswordExpiryModule"
   image="C:\Windows\system32\RpcProxy\RpcProxy.dll" />

   to the following
   <add name="PasswordExpiryModule"
   image="C:\Windows\system32\RpcProxy\RpcProxy.dll"
   preCondition="bitness64" />
   o *Note that the "image" part of the entries will depend on your local installation and you should not change it*

2. **If Outlook Web Access is installed on the server**, perform the following additional steps *(note that the "path" part of the entries will depend on your local installation and you should not change it)*:

   In the file %windir%\system32\inetsrv\config\applicationhost.config:
   o change the line
   <filter name="Exchange OWA Cookie Authentication ISAPI Filter"
   path="C:\Exchange\ClientAccess\owa\auth\owaauth.dll"
   enabled="true" />

   to the following
   <filter name="Exchange OWA Cookie Authentication ISAPI Filter"
   path="C:\Exchange\ClientAccess\owa\auth\owaauth.dll"
   enabled="true" **preCondition="bitness64"** />

   o change the line
   <filter name="Exchange ActiveSync ISAPI Filter"
   path="C:\Exchange\ClientAccess\sync\bin\AirFilter.dll"
   enabled="true" />

   to the following
   <filter name="Exchange ActiveSync ISAPI Filter"
   path="C:\Exchange\ClientAccess\sync\bin\AirFilter.dll"
   enabled="true" **preCondition="bitness64"** />

- change the line
  ```
  <add name="exppw"
  image="C:\Program Files\Microsoft\Exchange
  Server\ClientAccess\Owa\auth\exppw.dll"  />
  ```

  to the following
  ```
  <add name="exppw"
  image="C:\Program Files\Microsoft\Exchange
  Server\ClientAccess\Owa\auth\exppw.dll"
  preCondition="bitness64" />
  ```

- change the line
  ```
  <add name="exppw" />
  ```

  to the following
  ```
  <add name="exppw" preCondition="bitness64" />
  ```

The following are some internet links that may provide more information and background on these settings:

http://forums.iis.net/t/1154189.aspx
http://www.m86security.com/kb/article.aspx?id=12671

Install XML Component

In order to process your web portal functional settings you will need to install a Microsoft XML parsing component.

Step 1 – Install XML Component

Download and run the msxml6.msi or msxml6_x64.msi file (depending on your operating system).

For further information regarding this component (MSXML 6.0) please see the following Microsoft article:

http://www.microsoft.com/en-us/download/details.aspx?id=3988

Step 2 – Set Directory Permission

The specified XML component requires read and write permissions to the directory that stores the XML configuration file (adminconfig.xml). This file is located in "c:\Inetpub\wwwroot\MiracleService\TECHNICIANPORTAL\Setup". To set the folder permissions right click on the "TECHNICIANPORTAL" folder and select "Sharing and Security". Select the "Security" tab and add the Internet user.
To review how to set read and write permissions for the Internet user please see "Step 2 - Share your Miracle Service Database Directory" from the "Web Server Files Installation and Setup" section above.

Establishing the Internet Connection

As mentioned in the Installation Overview, this manual is not intended to cover the set-up and configuration to establishing the web server's presence on the Internet. This is a relatively complex issue as corporate networks and router/firewall configurations are considerably different. However, in order for your technicians to be able to access your portal using either Internet Explorer or a Blackberry Browser, this is a critical step. The following covers the very basic issues that need to be addressed in a very simple network environment.

Public IP Address
e.g. 123.123.123.123

Server

Router

Port 80
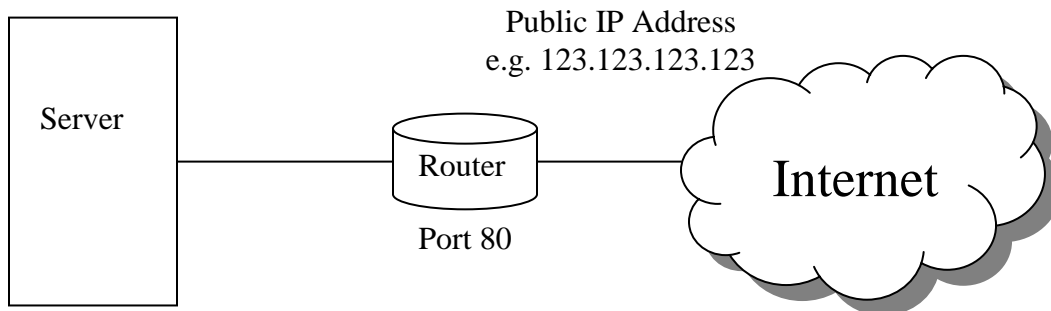
Internet

The Web Server is located on a server within your internal network. It is essential to connect the server to an external IP address to ensure your users can access the web server inside of your network. We recommend that you use knowledgeable network designers to set-up the internet connection, as there are important network security issues to consider. These issues are different for every corporate network environment.

To successfully connect the server to an external IP address you will probably need to configure your Firewall/Router. This typically requires you to establish IP Mapping. This maps your internet network IP address assigned to your server with a specific external Internet IP address. When establishing this connection your Firewall may also require you to set-up a policy to ensure only specific internet data traffic is allowed to pass to your server.

You will also need to configure the IIS server to recognize the connection by configuring the port assignment. This is part of the standard IIS configuration.

For more details on establishing a Web Server on the Internet we recommend you consult with a data network specialist.