

Preparing IIS for the Reporting Web Site Installation

June 2011

In This Article:

- Installation Requirements
- Configuring Web Site IIS6
- Configuring Web Site IIS7
- Configuring Web Site 2008 Server
- Securing Report Folders
- Troubleshooting IIS

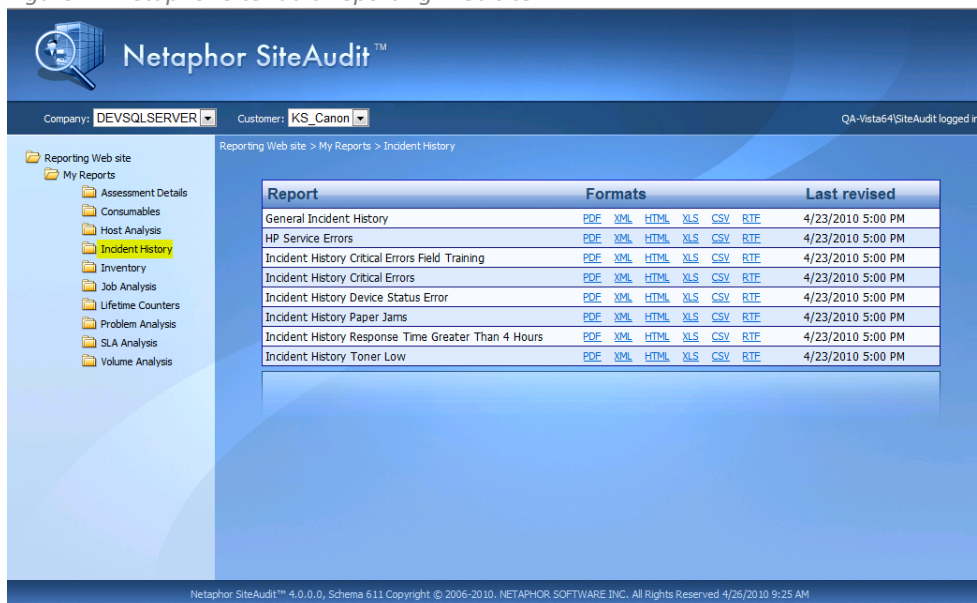
Since version 4.0, SiteAudit has included the ability to create reports from any SiteAudit view and publish the reports to a web site so that users can view reports using a browser. This article describes how to prepare for a Reporting Web site installation and how to troubleshoot basic IIS issues related to the Reporting Web site.

Feature Overview

The Reporting Web site is a new feature available since SiteAudit 4.0 that allows users to obtain SiteAudit reports over the Intranet or Internet. The Reporting Web site is an ASPX site installed on Microsoft IIS 6 or IIS 7. Authorized users can publish reports to the Reporting Web site directly from the SiteAudit Viewer and the reports can be accessed over the Web using Internet Explorer 7 or greater. Although the Reporting Web site runs perfectly on other browsers, only Internet Explorer is supported.

Figure 1 shows an example of the default Reporting Web site.

Figure 1 –Netaphor SiteAudit Reporting Web site



Preparing for the Reporting Web Site Deployment

The Reporting Web site is an ASPX site that runs on IIS6 or IIS7. The following sections describe how to configure IIS to work with the Reporting Web site

Prerequisites

To install and setup the reporting web site you will need the following:

- 1) SiteAudit v4.0 or later software
- 2) MS SQL Database Local or separate machine with access credentials
- 3) Internet Information Server (IIS) 6 or 7 or later
- 4) SiteAudit database

If a SiteAudit database does not already exist, it is recommended that a database be created using Microsoft SQL Management Studio.

Host Platform Support

Windows Vista/Windows 7 or Server 2003/08

Note: Windows XP and XP Pro are not supported by IIS 6 or 7

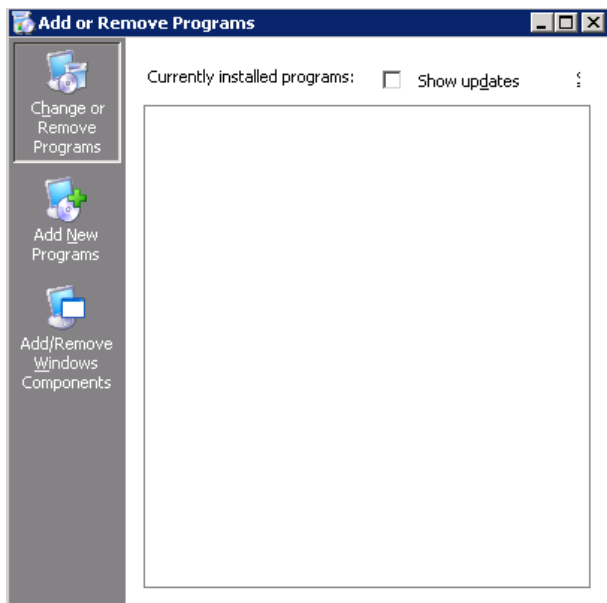
Viewing Platform

Browsers running on Windows XP/Vista/Windows 7 or Server 2003/08. Only IE7 and 8 are tested for compatibility although the Reporting Web site can be viewed using other browsers.

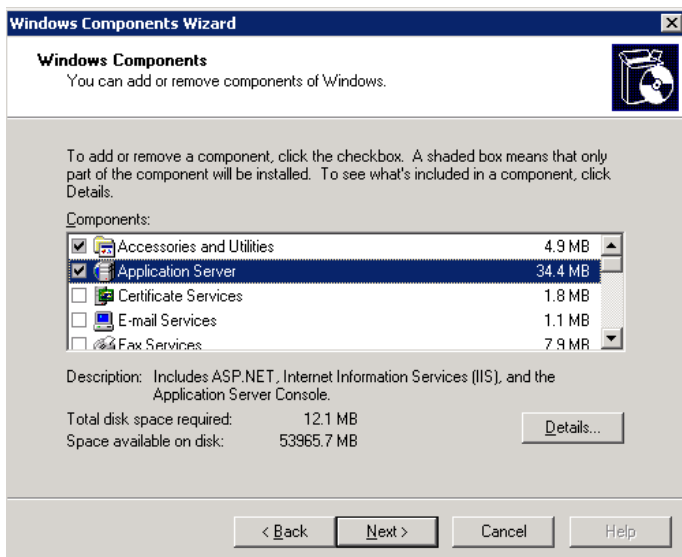
IIS 6 Installation

Prior to installing the SiteAudit Reporting Web site, IIS must already be installed. This section will describe the basic IIS components that need to be installed for correct functioning of the Reporting Web site (RWS).

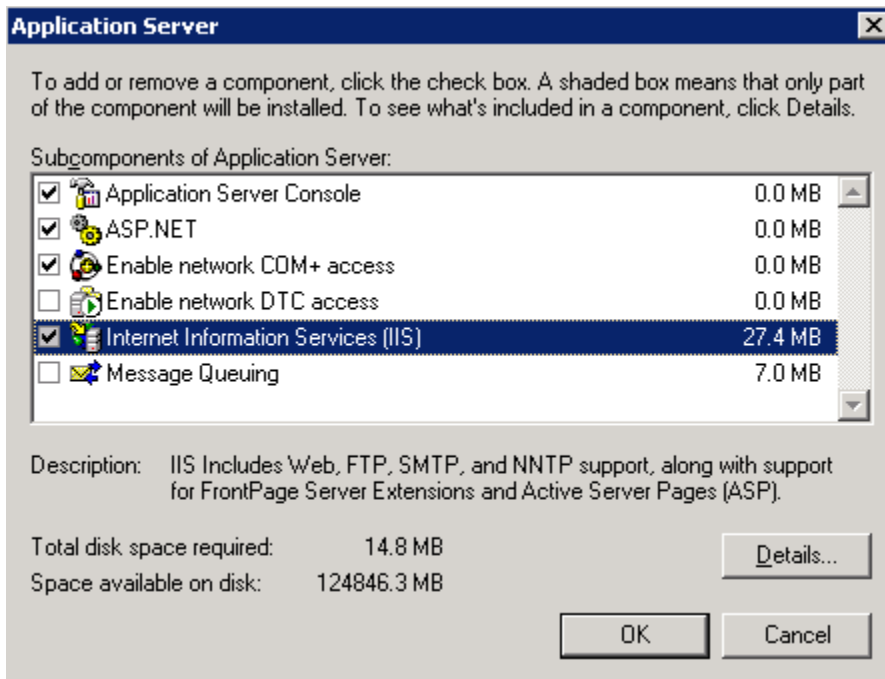
1. To install IIS, select **Add/Remove** programs from the Control Panel.
2. Select **Add/Remove Windows Components** from the buttons on the left panel



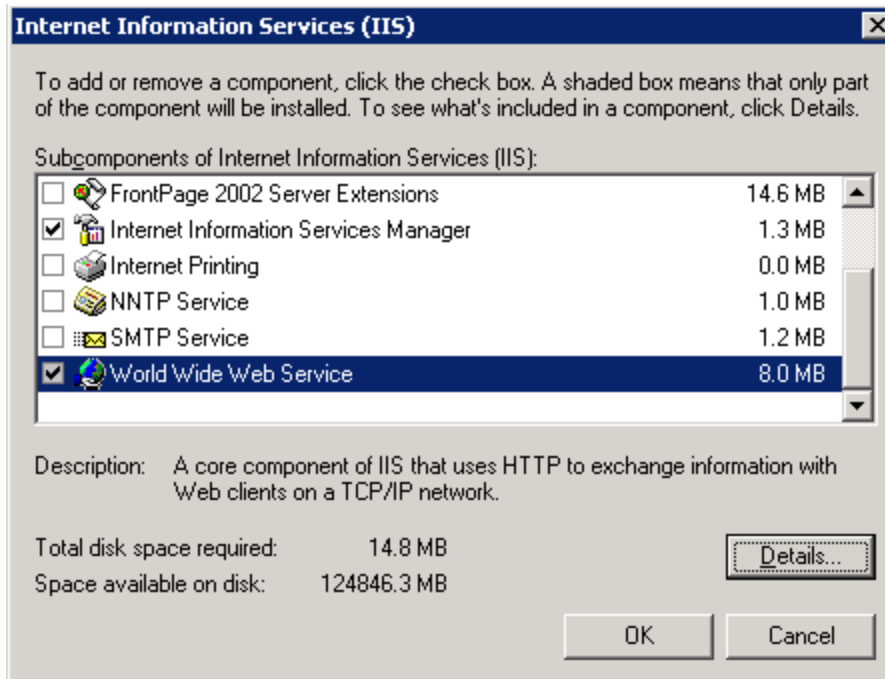
3. Select **Application Server** and click the **Details...** button



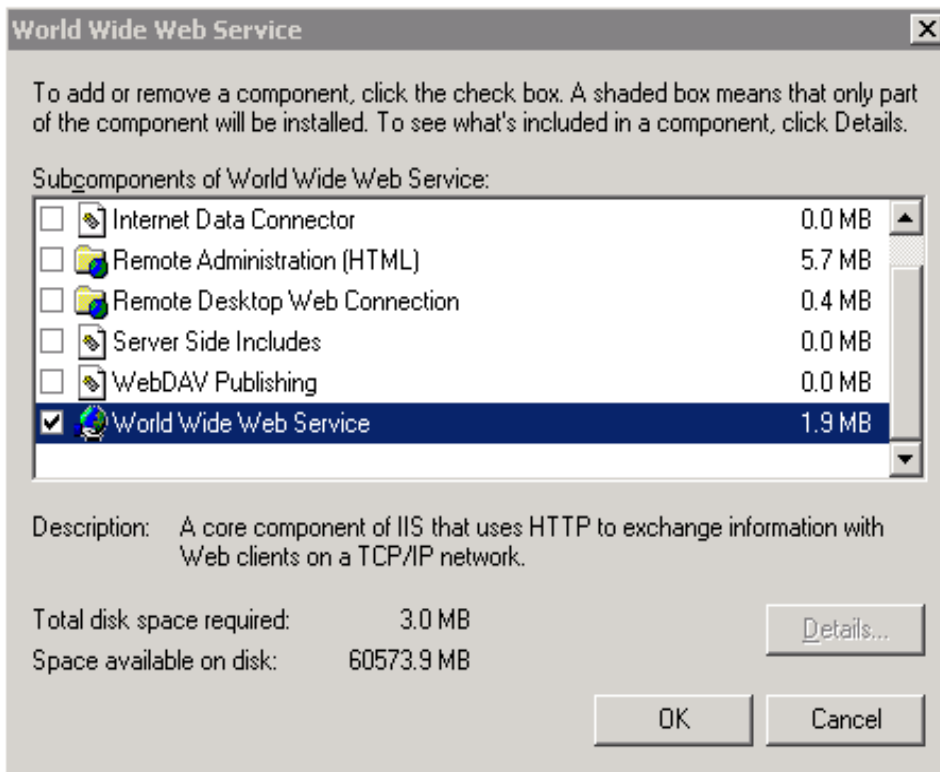
4. Make sure the boxes next to **ASP.NET** and **Internet Information Services (IIS)** are checked. Select **Internet Information Services (IIS)** and click the **Details...** button



5. Check the boxes next to **Internet Information Services Manager** and **World Wide Web Service**. Select **World Wide Web Service** and click the **Details...** button



6. Make sure **World Wide Web Service** is checked and click the **OK** button to close the dialog.



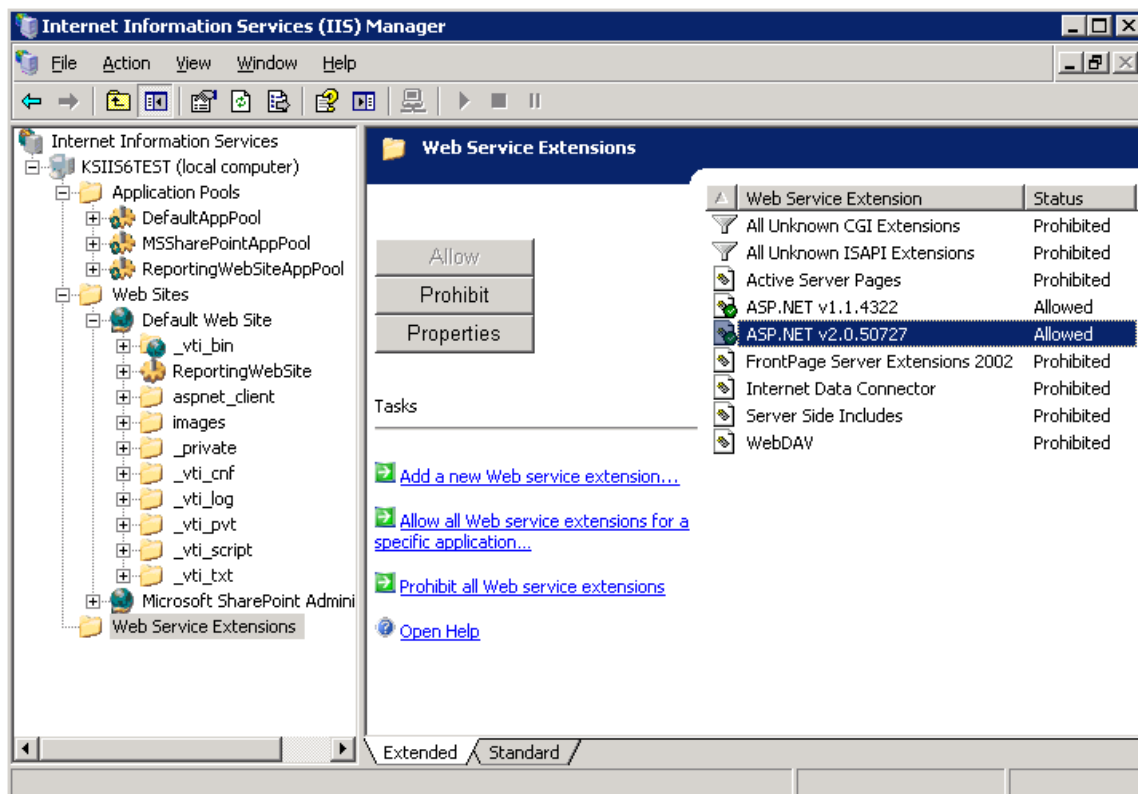
7. Close the dialogs and begin the installation of IIS. This often requires the operating system installation disk or access to the OS i386 folder.

It is safe to install the SiteAudit Reporting Web site after IIS has been installed. The following section describes how to configure IIS to work with the Reporting Web site.

IIS 6 Configuration for the Reporting Web Site

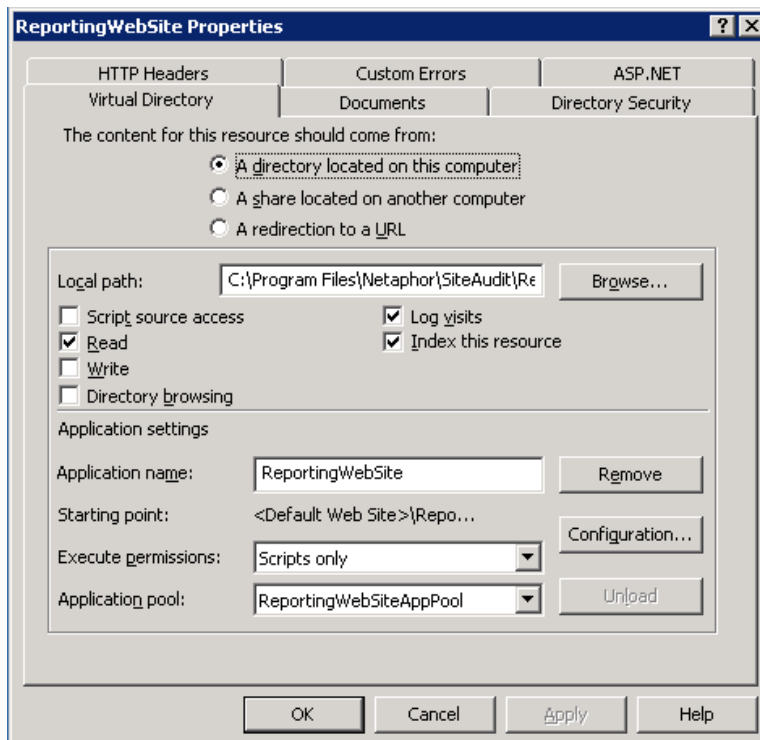
This section describes how to configure IIS to work with the Reporting Web site. Prior to installing the Reporting Web site, IIS must already be installed. Refer the section, **IIS 6 Installation**, for instructions on installing Internet Information Services (IIS).

1. Install the SiteAudit Reporting Web site. Refer to section, **Installing the Reporting Web Site**, for instructions.
2. Open **Internet Information Services (IIS) Manager** from the **Control Panel > Administrative Tools**.
3. Expand the local computer and select Web Service Extensions.

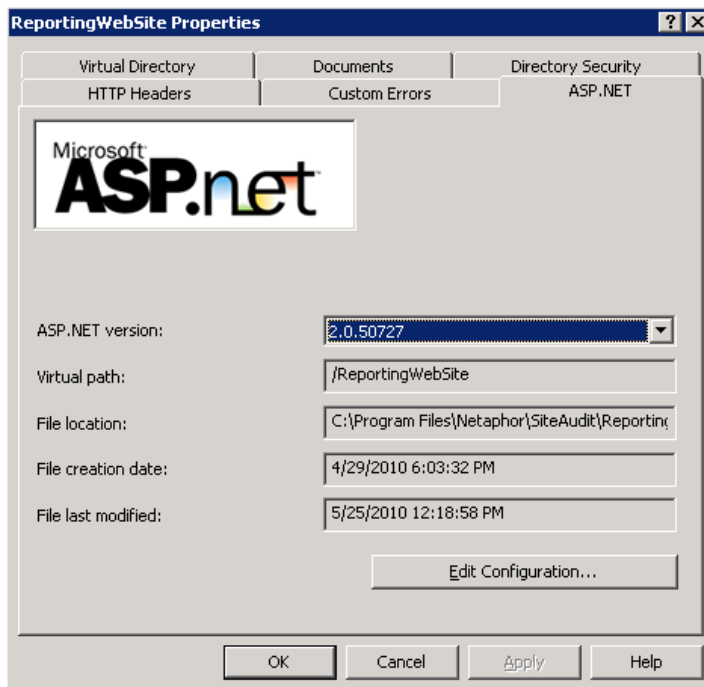


1. Make sure that the status for **ASP.NET v1.1.4322** and **ASP.NET v2.0.50727** is **Allowed**. The Reporting Web site requires **ASP.NET v2.0.50727**. If this component is not present in the Web Service Extensions, run the following command from a DOS prompt:
 - On 32-bit systems: `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis -i`
 - On 64-bit systems: `C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis -i`

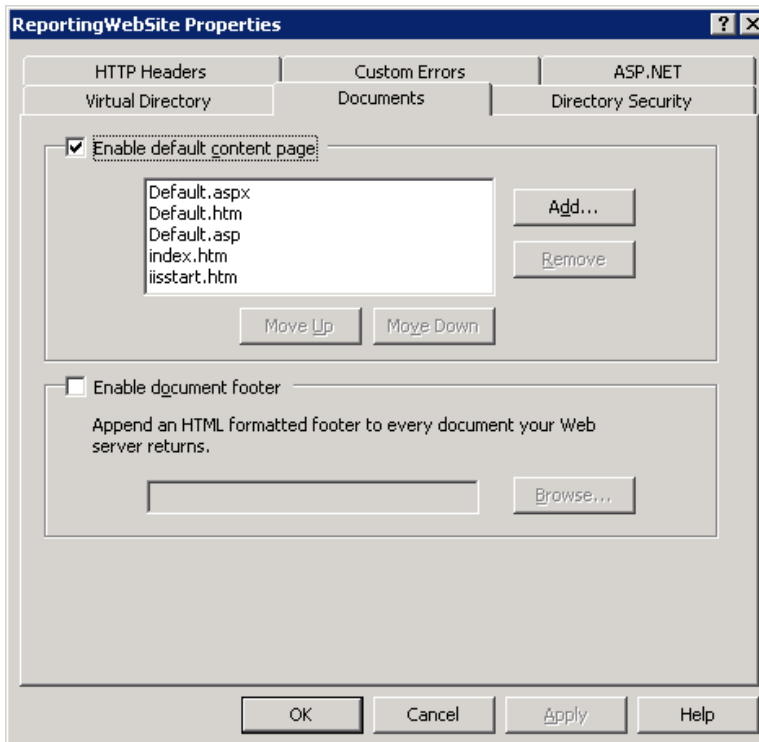
2. Configure the Reporting Web site virtual directory. From the IIS Manager, right-click on the **ReportingWebSite** (located under the Default Web Site) and select **Properties**.



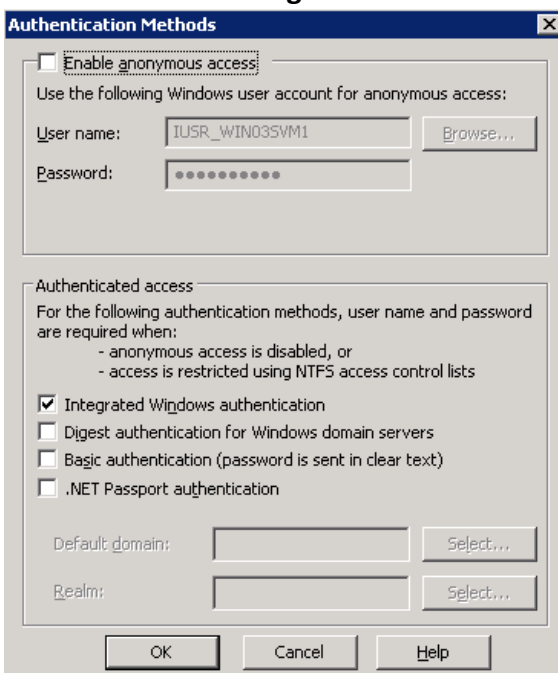
3. Select the ASP.NET tab and confirm that the **ASP.NET version is 2.0.50727**



4. Select the **Documents** tab and make sure that **Enable default content page** is checked and that the **Default.aspx** is included in the list



5. Select the **Directory Security** tab and make sure that **Enable anonymous access** is *not* checked and that **Integrated Windows authentication** is checked



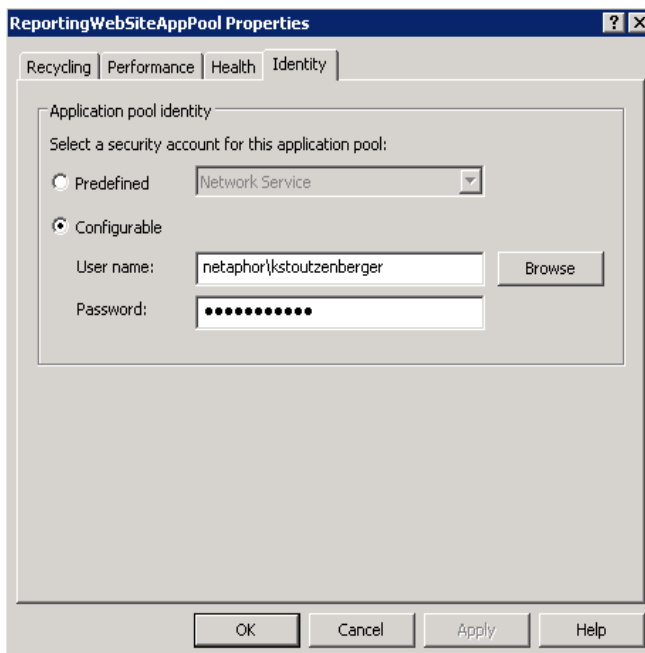
Configuring IIS 6 to Resolve Double Hop

If the SQL database is located on a machine other than the machine where the Reporting Web site is hosted, then a double hop problem can occur when using Windows authentication. Essentially, this means the credentials supplied by the client browser make it to the IIS server, but are not passed to the SQL server.

To resolve the double hop problem, one must configure the Reporting Web site application pool to use domain credentials that have access to the SQL server database. Users can then connect to the Reporting Web site using their own domain credentials. However, the Reporting Web site application will use the credentials supplied in the Application Pool when communicating with the SQL server. This section describes how to configure IIS 6 to work around the double hop problem.

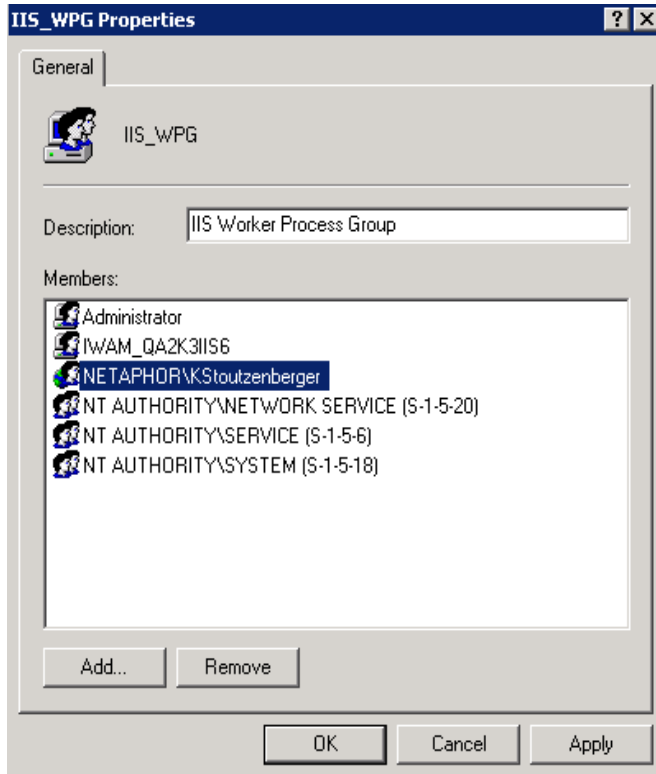
Configure the Application Pool

1. Open the Internet Information Services (IIS) Manager
2. Expand the local computer and **Application Pools** nodes
3. Right-click on the **ReportingWebSiteAppPool** node and select **Properties**
4. Select the **Identity** tab
5. Select the **Configurable** radio button and enter the domain credentials that has access to the remote SQL server database, then click the OK button



Add Application Pool user to the IIS_WPG group

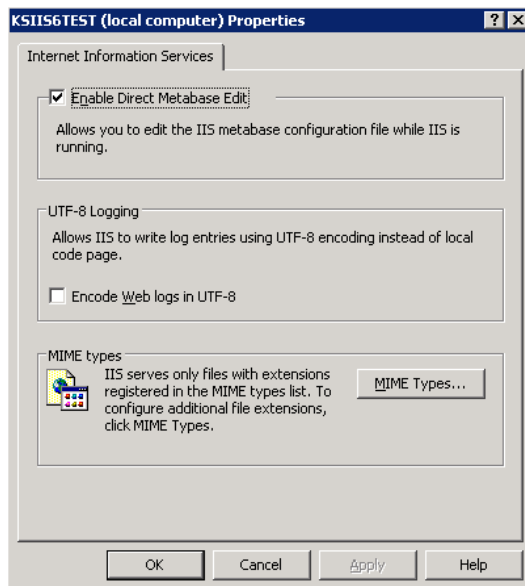
1. Select **Computer Management** from the **Control Panel > Administrative Tools**
2. Expand the **System Tools** and **Local Users and Groups** nodes
3. Select the **Groups** folder and double-click the **IIS_WPG** group
4. Add the user specified in the Application Pool



Force NTLM Authentication

Forcing NTLM authentication allows users to log onto the Reporting Web site using the site DNS name. This is typically only required if the server where IIS is installed does not do DNS or WINS resolution.

1. Open the Internet Information Services (IIS) Manager
2. Right-click on the local computer and select **Properties**
3. Select **Enable Direct Metabase Edit** check box, then click **OK**



4. Using Notepad, open **MetaBase.xml** document located at
`%systemroot%\system32\inetsrv`
5. Locate the section `<IISWebServer>` and add the following property and value:
NTAuthenticationProviders="NTLM"

Example

```
<IISWebServer Location = "/LM/W3SVC/1"
  AppPoolId="DefaultAppPool"
  DefaultDoc="Default.htm,Default.asp,index.htm,iisstart.htm,Default.aspx"
  NTAuthenticationProviders="NTLM"
  ServerAutoStart="TRUE"
  ServerBindings=":80:"
  ServerComment="Default Web Site"
  ServerSize="1">
</IISWebServer>
```

6. Save and close the MetaBase.xml file

Disable Impersonation

1. Using Notepad, open the **web.config** file for the Reporting Web site. This file is located in the root folder of the site, typically installed at **C:\Program Files\Netaphor\SiteAudit\ReportingWebSite**
2. Locate the identity tag and set impersonation to **false**.
<identity impersonate="false" />

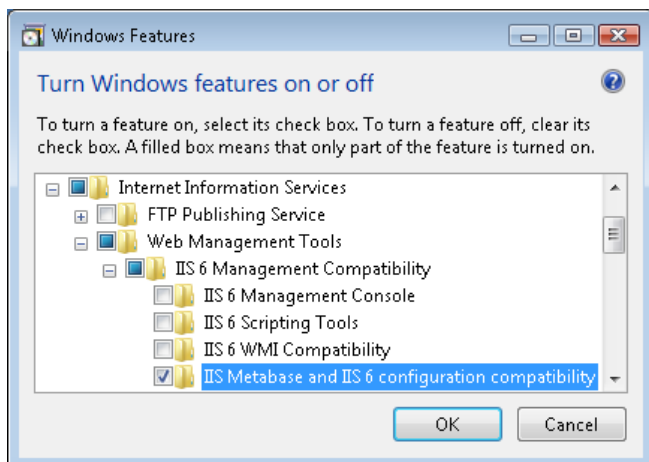
Reset IIS

Once all of the above steps have been executed for the IIS 6 double hop work-around, reboot the machine or reset IIS. To reset IIS, simply type the command, **iisreset** into the command prompt. This will stop and restart the IIS service.

Installing the Reporting Web Site on IIS 7

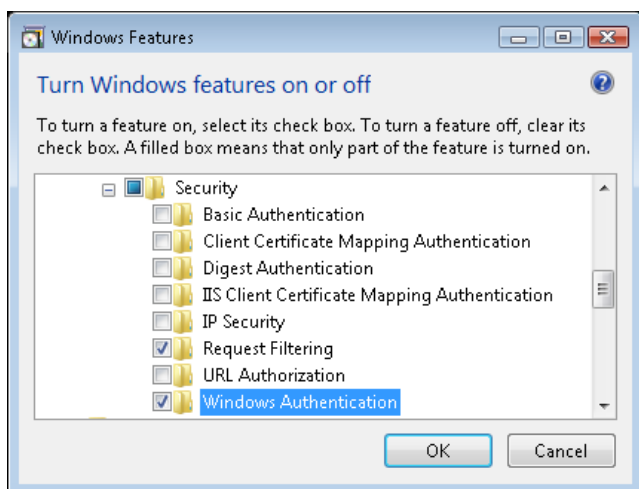
The following instructions indicate the components that must be installed on IIS 7 to support the Reporting Web site. If the IIS server is installed on Windows 2008 Server, please see the instructions for, *Installing the Reporting Web Site on IIS 7 (Server 2008)*, in the following section.

1. Install IIS if it has not already been installed. The Reporting Web site component will be disabled in the SiteAudit installer if IIS has not been installed.
2. Add Windows Features if they have not been installed already.
 - a. Add the "IIS Metabase and IIS 6 configuration compatibility" windows feature if it has not been added already.



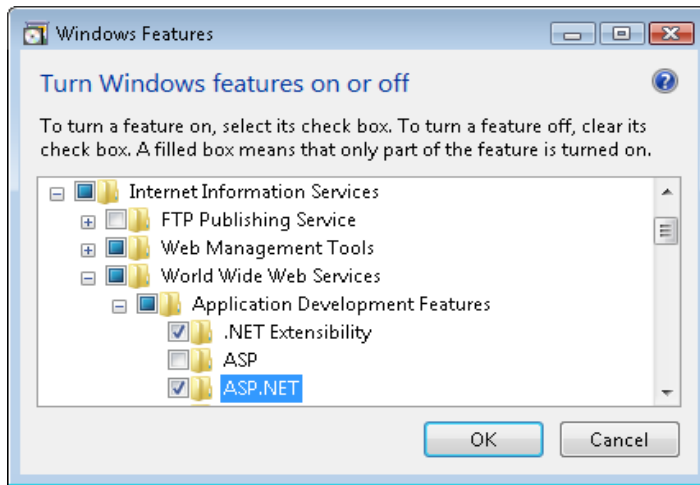
- b. Security Features.

Add the "**Windows Authentication**" windows feature if it has not been added already.

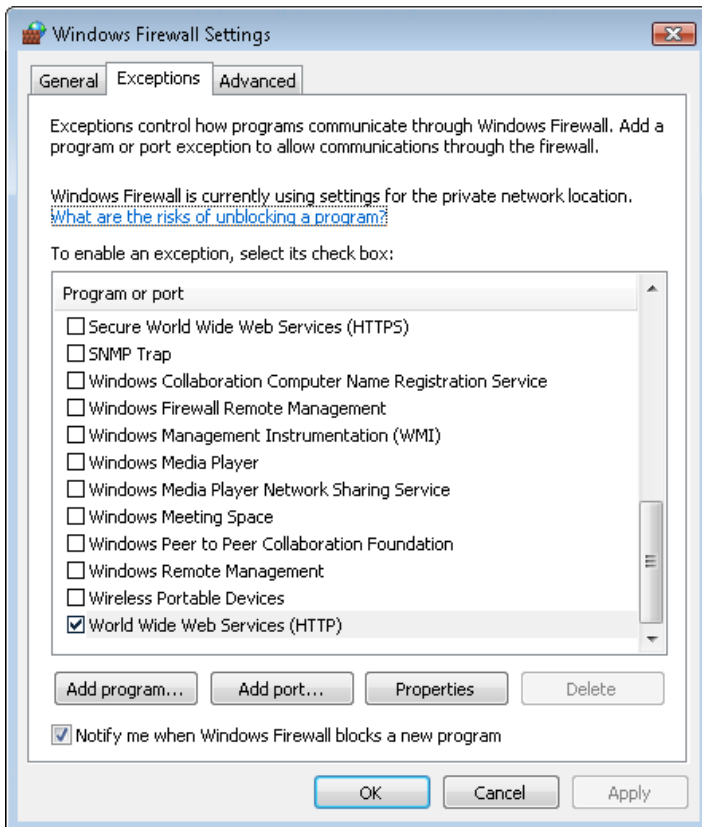


c. ASP.NET Feature.

Add the "ASP.NET" windows feature.



3. If Windows Firewall is disabled, this step can be skipped. If Windows Firewall is enabled, HTTP must be allowed through the firewall. In the Exceptions tab, make sure that "World Wide Web Services (HTTP)" is checked.

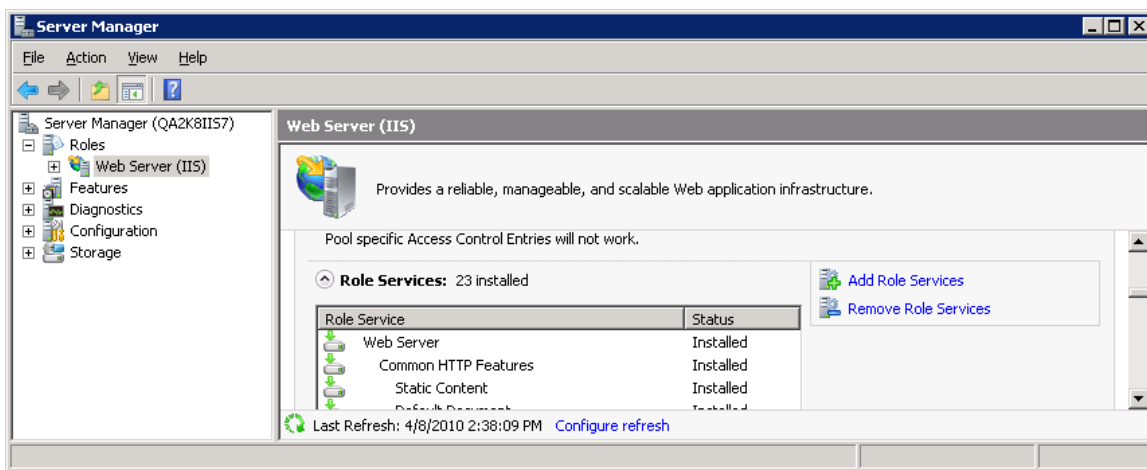


Installing the Reporting Web Site on IIS 7 (Server 2008)

Installing the Reporting Web Site on IIS 7 running on Windows Server 2008 is slightly different than when it is running on Windows Server 2003 or Vista. This section describes the configuration requirements for running the Reporting Web site on Windows Server 2008.

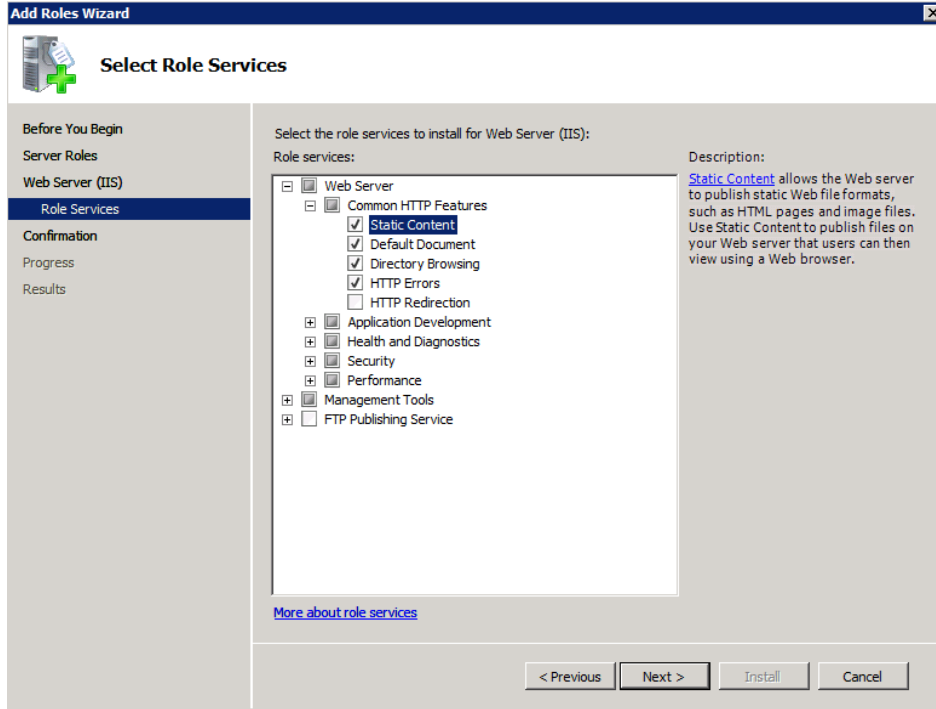
1. Install IIS if it has not already been installed. The Reporting Web site component will be disabled in the SiteAudit installer if IIS has not been installed.
2. Install the following Role Services if they have not been installed already.

From Control Panel's "Programs and Features", click on "Turn Windows features on or off". The Server Manager window will open. In the tree, select Server Manager - Roles - Web Server (IIS).

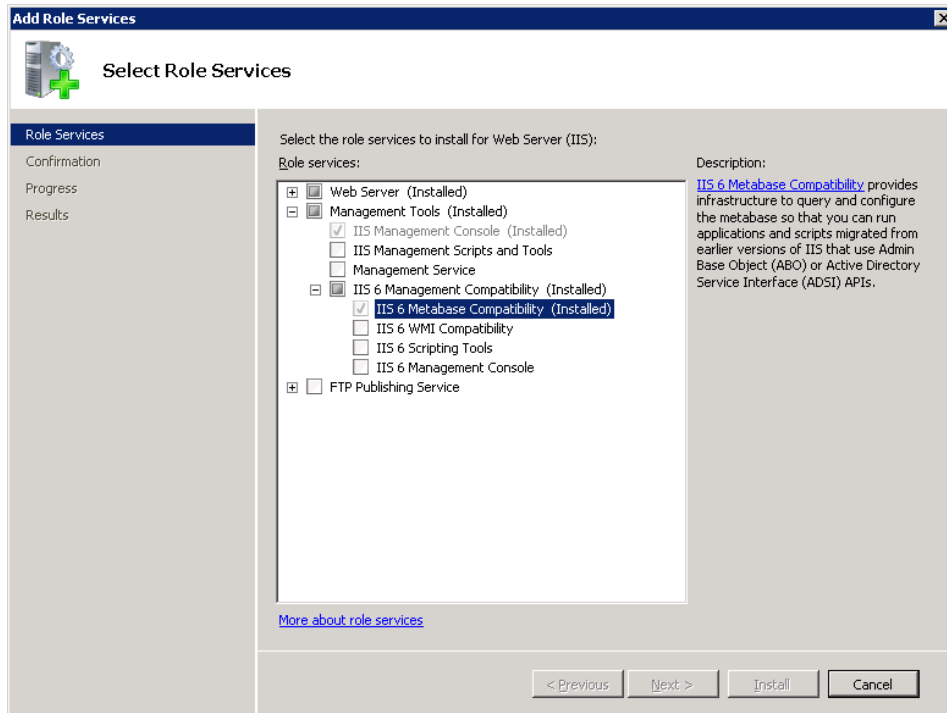


Click on the "Add Role Services" link to the right to open the "Add Role Services" window.

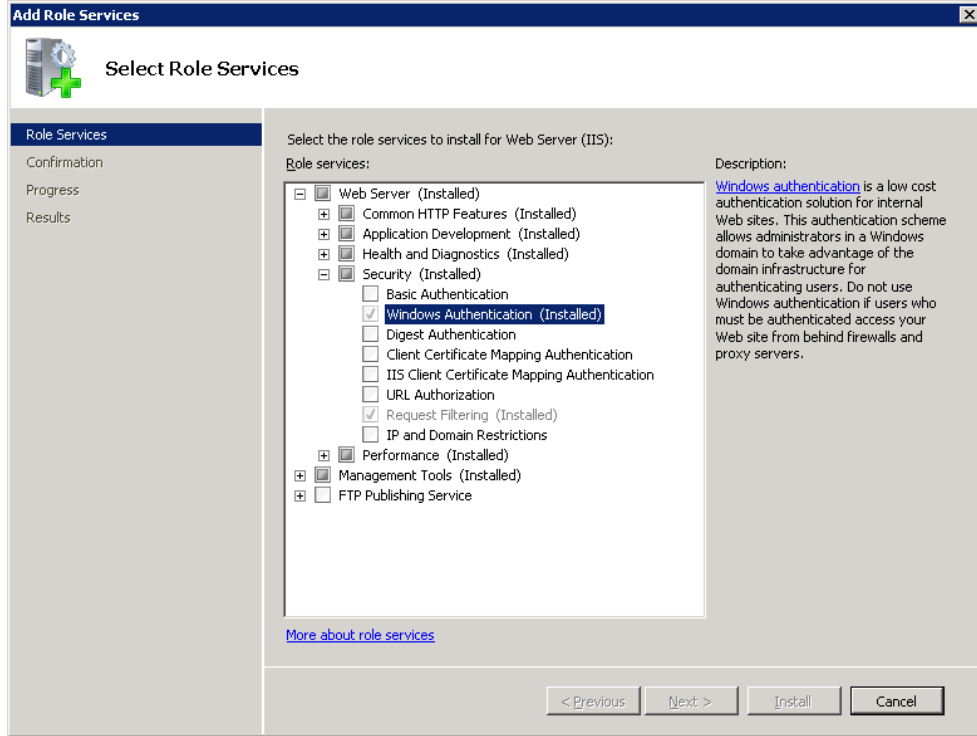
- a. Ensure that the following Common HTTP Features are enabled



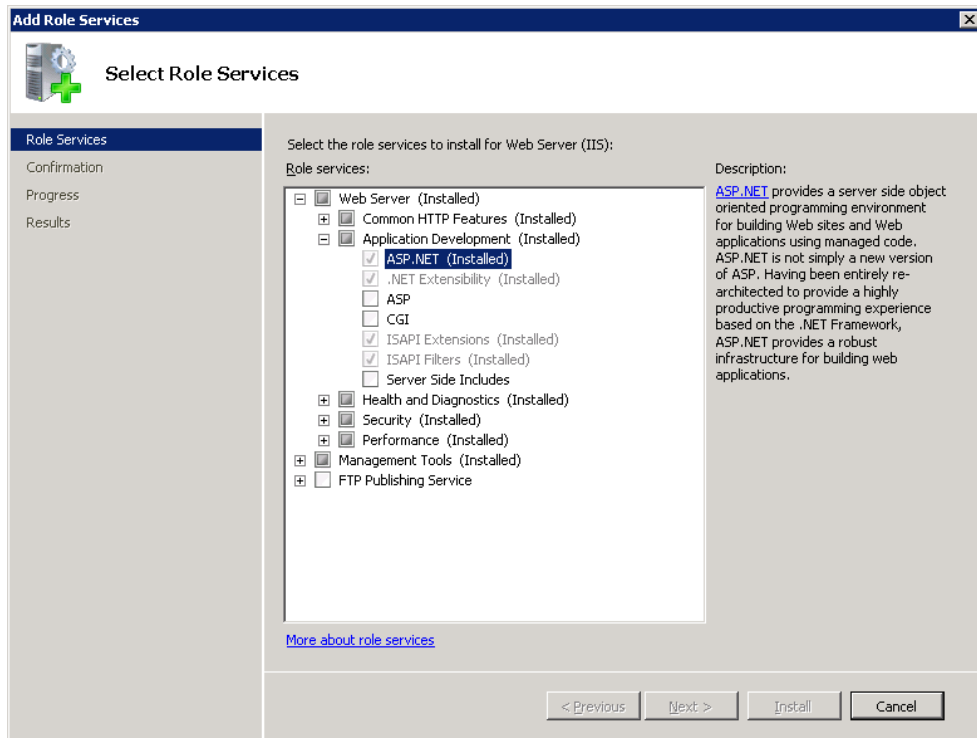
- b. Install the "IIS 6 Metabase Compatibility" role service if it has not been installed already.



- b. Install the "Windows Authentication" role service if it has not been installed already.



1. Install the "ASP.NET" role service if it has not been installed already.



3. If Windows Firewall is disabled, this step can be skipped. If Windows Firewall is enabled, HTTP must be allowed through the firewall. In the Inbound Rules, make sure that the "World Wide Web Services (HTTP Traffic-In)" rule is enabled

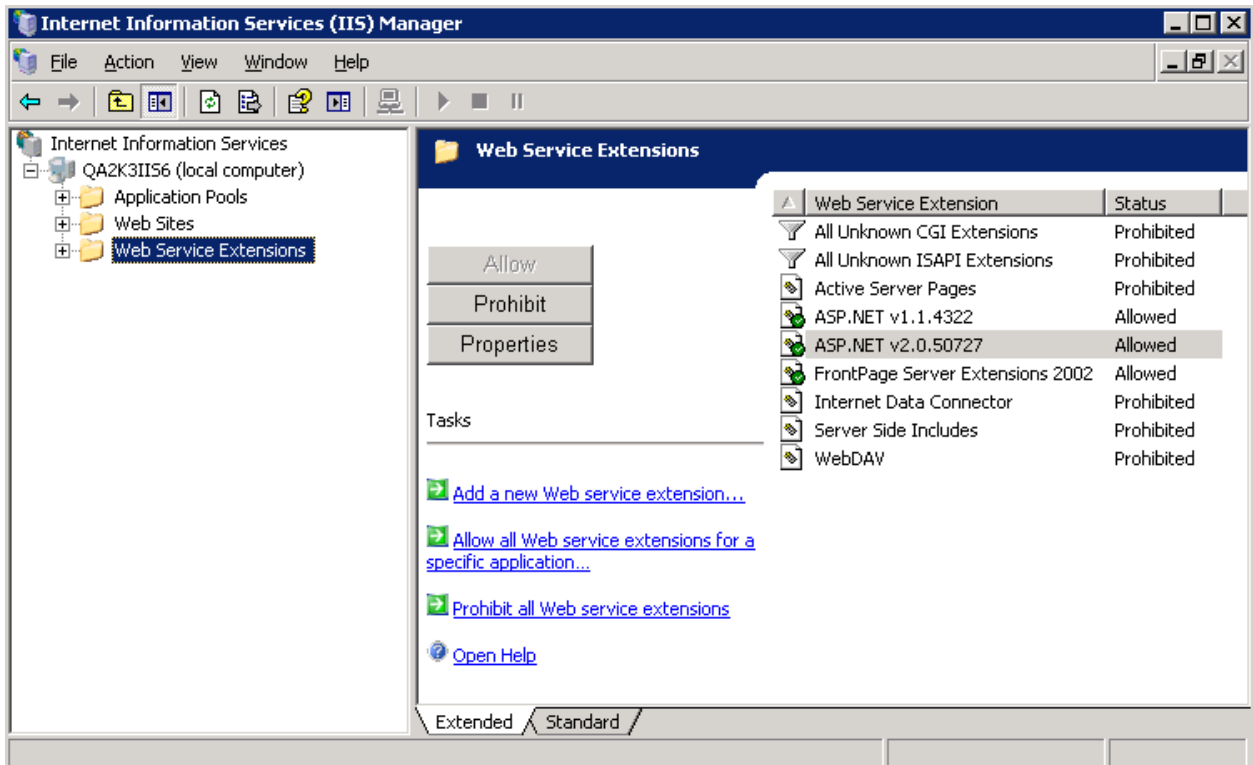
6. Enable the ASP.NET v2.0.50727 service extension.

Open the Internet Information Services (IIS) Manager. Click on the "Web Service Extensions" node. Verify that the extension "ASP.NET v2.0.50727" exists and the status is set to "Allowed".

If it does not exist in the list, run the following command from a DOS prompt:

On 32-bit systems: `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis -i`

On 64-bit systems: `C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis -i`



Securing Reporting Web Site Folders

By default, all users who have access to the Reporting Web site can see all folders and reports that exist. It is possible to limit access to the Reporting Web site folders to specific users and deny access to others. Folders are invisible to users who are denied access to them and visible to those who are permitted access. The folder security is handled in the web.config file located in the root folder of the Reporting Web site.

There is a section in the web.config called "location." This is where the administrator can define the path (the RWS folder) that requires special access privileges. A common technique is to create groups and assign users to the specific groups. Then allow or deny folder access to one or more groups. It is acceptable to allow or deny folder access to individuals as well.

In the example below, only users in the specified group will see the Inventory folder in the Reporting Web site. It will be hidden for all other users. Additionally, one can define specific users in the group who can access to the folder. An example user is: domain/username

```
<location path="MyReports/Inventory">
  <system.web>
    <authorization>
      <allow roles="RWSInventoryUsers" />
    </authorization>
  </system.web>
</location>
```

In the above example, the RWSInventoryUsers group contains the list of users who are permitted to view reports in the MyReports/Inventory folder. The Inventory folder will be hidden for all users who are not a member of the RWSInventoryUsers group.

This KB article provides additional details <http://support.microsoft.com/kb/316871>

System Configuration Scenarios

There are various ways in which the SiteAudit components can be distributed between machines. For instance, the SiteAudit Viewer and monitoring may run on one machine but the SiteAudit database may be hosted on a remote server. Additionally, the Reporting Web site can be installed on yet another server. It is also possible to install SiteAudit, the database, and the Web site on the same machine. This section explains these different scenarios.

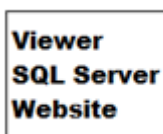
When configuring the environment for SiteAudit, all please make sure of the following:

- The SQL database can be accessed from the machine where the SiteAudit Viewer is installed.
- The SQL database can be accessed from the machine where the SiteAudit Monitoring runs.
- The SQL database can be accessed from the machine where the Reporting Web site runs
- The Reporting Web site can be accessed from the machine where SiteAudit Viewer is installed and from a remote client browser
- The SiteAudit schema must be the same for the SiteAudit Viewer, SiteAudit database, and the Reporting Web site for proper functionality. Reports cannot be viewed in the browser if the database has a different schema than the Reporting Web site.

When viewing web reports on the same machine that is hosting the Reporting Web Site, either run the web browser as administrator, or disable Protected Mode for Intranet Settings.

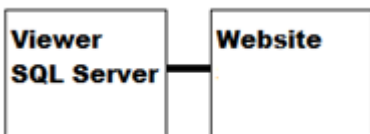
Scenario #1

The SiteAudit Viewer, SQL server, and the Reporting Web site are hosted on the same machine.



Scenario #2

SiteAudit Viewer and SQL server are installed on the same machine. The Reporting Web site is hosted on a separate machine.



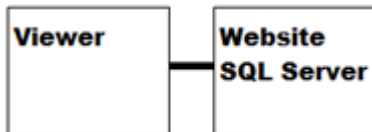
Scenario #3

SiteAudit Viewer and the Reporting Web site are on the same machine. The SQL server is hosted on a separate machine.



Scenario #4

The SiteAudit Viewer is installed on one machine and both the SQL server and Reporting Web site are hosted on a separate machine.



Scenario #5

The SiteAudit Viewer, the SQL server, and the IIS server hosting the Reporting Web site are all hosted on separate machines.



If Windows authentication is used and the credentials are not properly passed to the SQL server database, then a message may appear informing that the credentials are passed using an insecure mechanism. If this issue occurs, refer to the double-hop problem in the troubleshooting section located at the end of this document.

Troubleshooting IIS and Reporting Web Site Issues

This section provides troubleshooting tips for configuring IIS for the Reporting Web site. The first section deals with a general authentication error and the following sections deal with IIS6 and IIS7 issues.

Reporting Web Site Option Disabled in Installer

If IIS has not been installed on the machine where the installer is run, then the option to install the Reporting Web site will be disabled. Users must first install IIS prior to installing SiteAudit if the Reporting Web site is to be installed.

Page Cannot Be Found

Typically if the page cannot be found, there could be a couple different problems.

1. Confirm that the Firewall is configured to allow the port on with the Reporting Web site is running to pass. Typically this is port 80.
2. Verify that the Default.aspx page is in the list of content pages. This setting can be found in the web site properties, Documents tab.
3. Confirm that the web site is configured with ASP.NET 2.0.50727

Service Unavailable

The service unavailable error typically occurs when the user specified in the application pool identity is not a member of the IIS_WPG group. To resolve the issue, add the application pool user to this group.

Web.config Error when Loading Page

If a standard ASPX error page is displayed when loading a page and it references a problem with the web.config file, then it is likely that the correct version of ASP.NET is not installed. Be sure that **ASP.NET 2.0.50727** is configured for the Web site.

500 Internal Server Error: Login Failed for Anonymous User

Typically the error below occurs when a user tries to run a report on the Reporting Web site. This is an indication that impersonation is enabled on the Reporting Web site. Disable impersonation and confirm that the error no longer occurs.

We're sorry. We are unable to satisfy your request because Login failed for user 'NT AUTHORITY\ANONYMOUS LOGON'.

To disable impersonation, open the web.config file and set the identity impersonate to false.

```
<identity impersonate="false" />
```

500 Internal Server Error: Login Failed for Computer User

Typically the error below occurs when the application pool identity is set to NETWORK SERVICE and the SQL server is located on a remote computer. The error can also occur if the user specified in the application pool identity is not a member of the IIS_USR or IIS_WPG group, in the case of IIS 6. Refer to the Double Hop problem to resolve this issue.

We're sorry. We are unable to satisfy your request because Login failed for user 'NETAPHOR\QA-VISTA64\$'.

500.19 Internal Server Error:

This error can occur if there are problems with the web.config file. Typically, the error should provide a hint to the problem. For example, the following error indicates that the Default.aspx reference should not be added and indicates that the error exists on line #120. Removing the entry from the web.config file will resolve this error.

This problem typically occurs when the Reporting Web site is installed BEFORE IIS has been configured to include the Default.aspx page. To avoid this problem, configure IIS to include the Default.aspx start page BEFORE installing the Reporting Web site.

Error Summary

HTTP Error 500.19 - Internal Server Error

The requested page cannot be accessed because the related configuration data for the page is invalid.

ConfigCannot add duplicate collection entry of
Errortype 'add' with unique key attribute 'value'
set to 'Default.aspx'

Config File\\?
\\E:\Netaphor\ReportingWebSite\web.config

Config Source

```
119:         <files>
120:             <add value="Default.aspx" />
121:         </files>
```

Login Fails When using Web Site DNS Name but Works Using IP Address

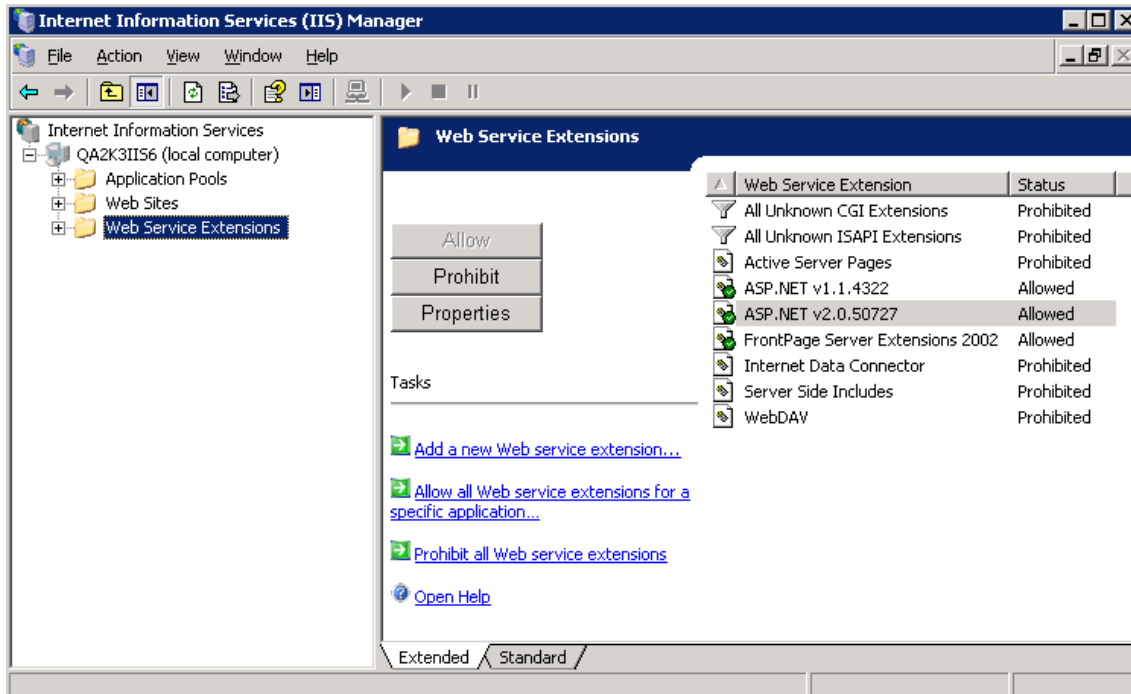
Typically when a user is able to log into the Reporting Web site using the IP address but is not able to log in when using the DNS name, it indicates that NTLM authentication is not being enforced. Refer to the section, **Force NTLM Authentication**, to force NTLM authentication.

404 Error Message

If a 404 error message appears when accessing the Reporting Web site, then make sure the ASP.NET Web Service Extension for v2.0 is installed. Once it has been installed, run the command below from the Command prompt.

On 32-bit systems: `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis -i`

On 64-bit systems: `C:\WINDOWS\Microsoft.NET\Framework64\v2.0.50727\aspnet_regiis -i`

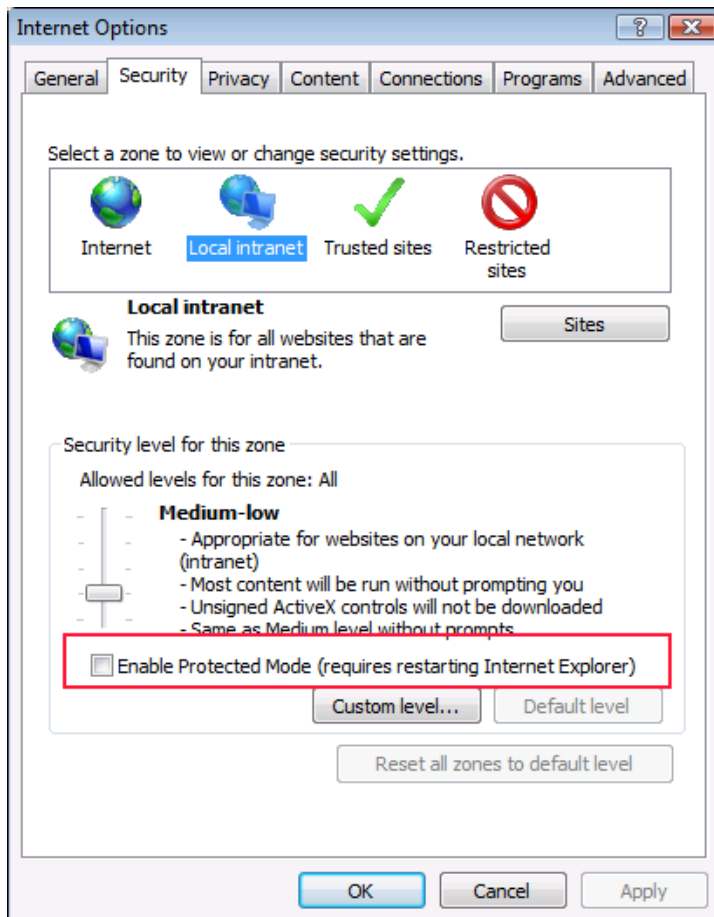


Configure User Access

All users who will access the Reporting Web site must be a member of the IIS_USR group. It is possible that users can access the site when not a member of this group but may be limited in what actions are permissible. Therefore it is recommended to always enter users into the IIS_USR group.

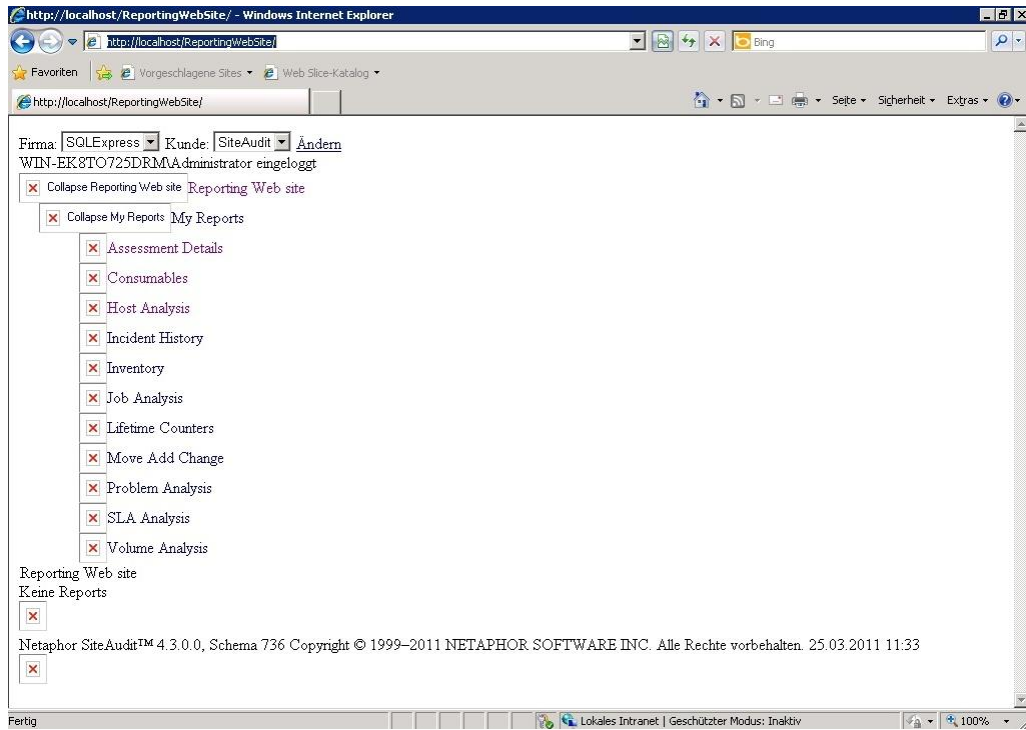
Access to Path Denied

If the Access to path denied error occurs when viewing a report, enable Intranet settings in Internet Explorer. This can be done by disabling the property, *Enable protected mode* in the Intranet settings.

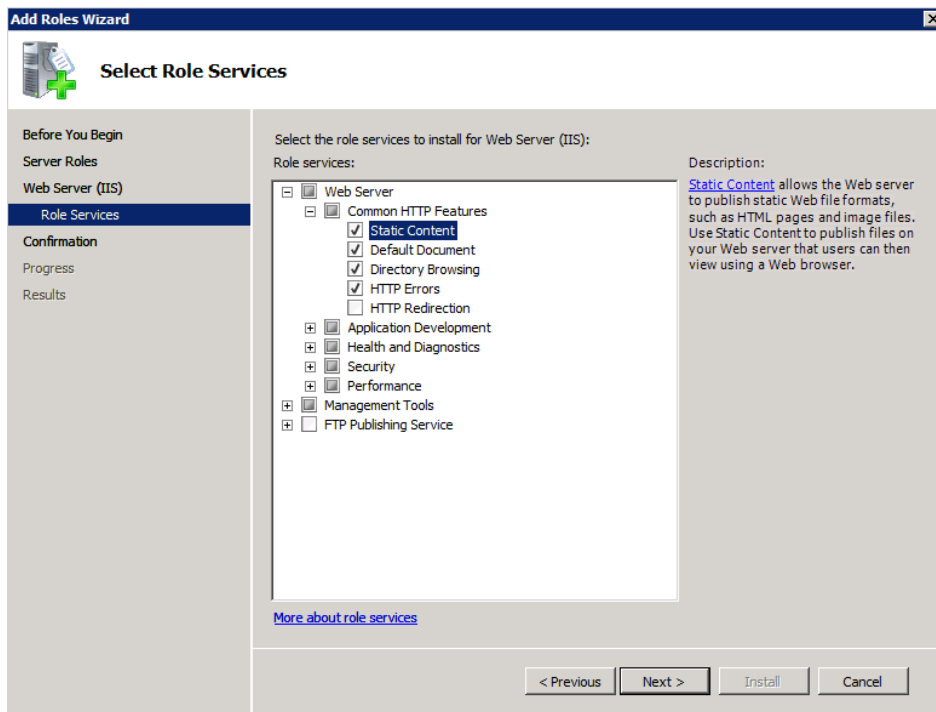


Images Do Not Appear on Reporting Web Site

If the images do not appear on the Reporting Web site, then the most likely problem is that the Static Content was not enabled in the Common Http Features.

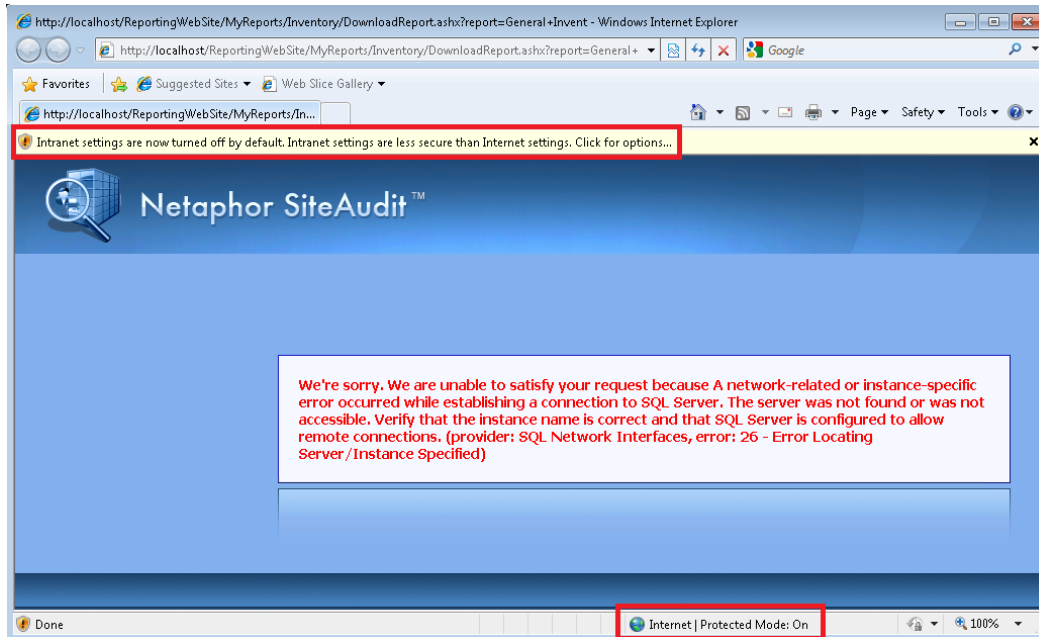


Ensure that the Static Content is checked as shown below



Error occurred while establishing a connection to SQL Server

This error can occur when web browser intranet settings are turned off, which is the case by default. To enable intranet settings, click on the yellow warning bar at the top of the web browser window and select *Enable Intranet Settings* from the dropdown. The text at the bottom of the web browser window will change from “*Internet | Protected Mode: On*” to “*Local intranet | Protected Mode: Off*”.



Using Alternative Credentials

Internet Explorer contains an advanced setting to always prompt users for credentials even if the user is logged into the machine using a domain account. To disable the prompt for domain users, disable *Always Prompt* in the advanced settings. Domain users will not be required to enter credentials when logging into the Reporting Web site.

It may be the case that a different user must log onto the Reporting Web site from a machine where a domain user has logged in. Enable the *Always Prompt* property so that the user can enter the appropriate credentials.

Windows Authentication Double-Hop Problem (IIS 7)

A double hop problem can exist when the SQL server is located on a different machine than the web server. If a user logs onto the web server using Windows authentication, the credentials

are not passed to the SQL server and thus it appears that the user is trying to log on using anonymous credentials. Instead of the Windows credentials being passed automatically to the server, users are prompted to enter their credentials and then warned that an insecure mechanism is used to pass the credentials.

Refer to the section, **Configuring IIS 6 to Resolve Double Hop**, to resolve double hop issues when using IIS 6.

The following sections describe how to troubleshoot to determine if a double-hop problem exists and how to work around the problem when using IIS 7.

Troubleshooting the Double-Hop Problem

Use the following method to determine if a double-hop problem may be causing authentication issues.

Quick Test

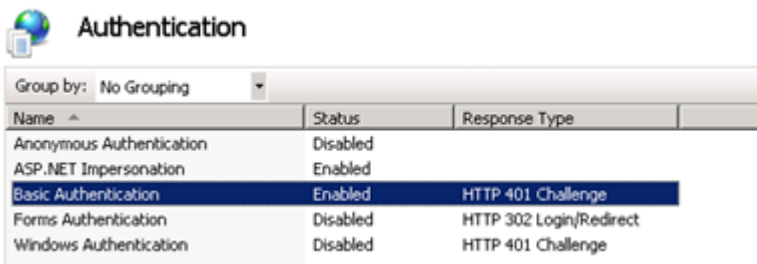
To quickly determine whether this is a permissions issue, follow these steps:

- Set the ASPX page security mechanism to use **Basic only**.
- Use a client to browse to the ASPX page, and then provide domain credentials when prompted.

If this works, you can conclude that the double-hop issue is probably the problem.

Workaround #1

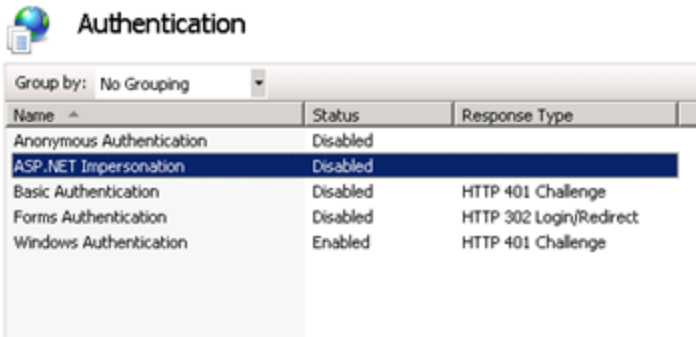
Use basic authentication between the browser and IIS. To do this, Windows Authentication must be disabled and Basic Authentication must be enabled on the IIS server



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Enabled	
Basic Authentication	Enabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Workaround #2

Disable ASP.NET impersonation and set the AppPool identity to an account that is known to have access to the SQL database:



It is also required to disable impersonation in the web.config file by modifying the identity tag as shown here: `<identity impersonate="false" />`

The following screenshot is an example of an Application Pool that has access to a remote SQL server database.

