Deltek Vision® 7.1

Advanced Technical Administration Guide

February 5, 2014

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

Contents

Overview

This guide is a supplement to the *Deltek Vision Technical Installation Guide*.

Topics covered in this supplement are for advanced deployments and may not be applicable to all installations of Vision.

Procedures included in this guide explain how to:

- Create a reverse proxy for SQL Reporting Services Using IIS 7.0 Application Request Routing (ARR).
- Configure HTTP compression to improve application response time.
- Configure the Secure Sockets Layer (SSL).
- Pre-deploy the Vision Smart Client to user workstations.
- Configure integrated security.
- Configure database session state.
- Secure your product deployment.

Consulting Is Available

This document provides additional insight into advanced technical administration topics for your Deltek application. These advanced topics are outside the bounds of the Deltek Customer Care Agreement and therefore are **not** covered by your Support Contract.

If you would like Deltek to provide additional insight into, or assistance with, the implementation of this material for your specific environment, experts within our Consulting Group are available to provide the specialized help that you need.

Adding Custom Notes to This Guide

If you would like to add custom notes to this guide that are specific to your company, Adobe® Reader® X provides this ability. If you do not already use Adobe Reader X, you can download it here free from Adobe.

To add a custom note using Adobe Reader X, complete the following steps:

1. On the Reader toolbar, click **Comment** at far right.
2. In the **Annotations** pane that displays, click ☐ **Sticky Note**. The cursor changes to match the button.
3. Position the cursor at the location in the guide where you want the note to appear, and click. A note icon is inserted at the location and a text box pops up.
4. Enter your information in the text box.
5. Continue adding notes as needed.
6. Save the document.

> Deltek recommends that you save the document to a slightly different filename so as to keep the original from being overwritten.

When reading the document, cursor over a note icon to see the information. Double-click a note icon to edit the information.

If You Need Assistance

If you need assistance installing, implementing, or using Vision, Deltek makes a wealth of information and expertise readily available to you.

Customer Services

For over 20 years, Deltek has maintained close relationships with client firms, helping with their problems, listening to their needs, and getting to know their individual business environments. A full range of customer services has grown out of this close contact, including the following:

- Extensive self-support options through the Customer Care Connect Web portal.
- Phone and email support from Customer Care analysts
- Technical services
- Consulting services
- Custom programming
- Classroom, on-site, and Web-based training

Find out more about these and other services from the Customer Care Connect site.

Customer Care Connect Site

The Deltek Customer Care Connect site is a support Web portal for Deltek customers who purchase an Ongoing Support Plan (OSP).

The following are some of the many options you have at the Customer Care Connect site:

- Download the latest versions of your Deltek products
- Search Deltek's knowledge base
- Ask questions, exchange ideas, and share knowledge with other Deltek customers through the Deltek Connect Customer Forums
- Display or download product information, such as release notes, user guides, technical information, and white papers
- Submit a support case and check on its progress
- Transfer requested files to a Customer Care analyst
- Use Quick Chat to submit a question to a Customer Care analyst online
- Subscribe to Deltek communications about your Deltek products and services
- Receive alerts of new Deltek releases and hot fixes

If you need assistance using the Customer Care Connect site, the online help available on the site provides answers for most questions.

Access Customer Care Connect

To access the Customer Care Connect site, complete the following steps:

1. Go to http://support.deltek.com.

2. Enter your Customer Care Connect **Username** and **Password**.

3. Click **Log In.**

> If you do not have a username and password for the Customer Care Connect site, contact your firm's Vision Administrator.
>
> If you forget your username or password, you can click the **Account Assistance** button on the login screen for help.

Additional Documentation

The following table lists the additional Deltek documentation available for this release. Except where noted, all the user guides and quick reference guides listed in this table are available for download from the Deltek Customer Care Connect site.

Deltek Vision Guides	
Deltek Vision Getting Started and Concepts Guides	
Deltek Vision Getting Started Guide	This guide contains information about the Vision Web interface and all the Vision applications, with tips for navigating through the system, using the dashboard, and finding and opening records.
Deltek Vision Concepts Guide	This guide describes the concepts underlying the basic accounting, project control, and customer relationship management (CRM) functions of the Vision application.
Deltek Vision Installation and Implementation Guides	
Deltek Vision Technical Installation Guide	This guide provides IT staff and system administrators with instructions for installing the Vision application.
Deploying Deltek Vision at a Hosting Provider	This guide contains instructions for deploying Deltek Vision at a hosting provider.
Deltek Vision Implementation Guide	This guide contains information about configuring and setting up Vision applications and features.
Deltek Vision Migration Guides	
Deltek Advantage to Deltek Vision Migration Guide	This guide contains information about migrating from Advantage to Vision, including the steps in the migration process and an overview of Vision features.
Deltek FMS to Deltek Vision Migration Guide	This guide contains information about migrating from FMS to Vision, including the steps in the migration process, discussions of the key migration decisions, and procedures

Deltek Vision Guides	
	for verifying the converted data.
Deltek Sema4 to Deltek Vision Migration Guide	This guide contains information about migrating from Sema4 to Vision, including the steps in the migration process and an overview of Vision features.
Deltek Vision Quick Reference Cards	
Deltek Vision Quick Reference Cards	Quick reference cards provide snapshots of specific business processes or Vision forms, with tips for entering data and using application toolbars. The following quick reference cards are available: ▪ Accounts Payable (Create a Voucher from a Purchase Order) ▪ Create Client from Vendor Utility ▪ Dashboard ▪ Desktop and Microsoft Office Integration ▪ Expense Report ▪ Navigation Tree Designer ▪ Project Planning ▪ Purchasing (Create a Standard Purchase Order) ▪ Resource Management (Generic Resource Assignments and Resource Utilization) ▪ Screen Designer ▪ SF330 Proposals ▪ Template Based E-mails ▪ Timesheet ▪ User Options ▪ Visualization
Deltek Vision Document Management Guide	
Deltek Vision Document Management Installation Guide	This guide contains detailed information on the prerequisites, general configuration, and installation procedures required to use the Vision Document Management application.
Deltek Vision Interface to Microsoft Project	
Deltek Vision Interface to Microsoft Project 2010	This guide describes how the manual scheduling feature in Microsoft Project 2010 impacts the two-way interface between Deltek Vision and Microsoft Project 2010.
Deltek Vision Performance Management Guides	

Deltek Vision Guides	
Deltek Vision Performance Management Technical Installation Guide	This guide provides instructions on how to install and configure the Analysis Cubes components of the Deltek Vision Performance Management module.
Deltek Vision Performance Management Content and Functionality Overview	This guide provides an overview of Vision Performance Management functionality and the pre-built visualizations that are included with it.
Deltek Vision Reporting Guides	
Deltek Vision Custom Reports and Microsoft® SQL Server Reporting Services	This guide provides instructions for creating, delivering, and generating Vision custom reports with Microsoft SQL Server Reporting Services and its report writing tools.
Deltek Vision Microsoft SQL Server Reporting Services Licensing FAQ	This guide explains the Microsoft SQL Server Reporting Services licensing implications for Vision.
Deltek Vision Connect for Microsoft Outlook Guides	
Deltek Vision Connect for Microsoft Outlook Installation Guide	This guide contains an overview of Vision Connect for Microsoft Outlook, as well as technical installation, setup, and maintenance information.
Deltek Vision Customizing Configuration Settings for Connect for Microsoft Outlook	**This guide was formerly titled Deltek Vision Connect for Microsoft Outlook Presets Configuration Guide** The guide is intended for system administrators, IT staff, or custom developers. It provides instructions on how to create presets to: configure default behavior for converting Microsoft Outlook contacts; control the display of the Synchronization Control Panel when issues occur during synchronization; and implement default and custom synchronization filters.
Deltek Vision Connect for Microsoft Outlook Frequently Asked Questions	This document contains frequently asked questions (FAQs) on topics regarding deployment, customization, environment, usage, and functionality.
Deltek VisionXtend Guides	
Deltek VisionXtend Web Services and APIs for Deltek Vision	This guide explains how to use the Deltek VisionXtend platform to integrate Vision with other applications, access web services, implement data validation routines, and establish workflow procedures using the Microsoft .NET Framework.
Deltek VisionXtend Test Client Application for Vision Web APIs/Web Services	This guide provides information about the Web Services Test Client application that is included with the Vision Utilities software.

Deltek Vision Guides	
Deltek Vision Navigator Guides	
Deltek Vision Navigator Installation Guide	This guide contains technical installation, setup, and maintenance information for Vision Navigator.
Deltek Vision Navigator Integration Guide	This guide provides technical information for using Vision Navigator with Deltek Vision.
Deltek Vision Project Connect Guides	
Deltek Vision Project Connect Installation and Administration Guide	This guide contains detailed information on installing and administering Project Connect for integrating Microsoft Project with Deltek Vision.
Deltek Vision Project Connect User's Guide for Microsoft Project 2010	This guide contains information for integrating for integrating Microsoft Project 2010 with Deltek Vision.
Deltek Vision Project Connect User's Guide for Microsoft Project 2007	This guide contains information for integrating for integrating Microsoft Project 2007 with Deltek Vision.

Chapter 1: Creating a Reverse Proxy for SQL Reporting Services Using Application Request Router (ARR)

Why Do I Need a Reverse Proxy?

Deltek Vision uses the Microsoft SQL Reporting Services WinForm report viewer control to render reports. This control requires a direct connection to the server running the SQL Reporting Services web service. Due to the nature of the Deltek Vision and SQL Reporting Services logical tier architectures and the available editions and licensing requirements of SQL Reporting Services, it is likely that the SQL Reporting Services web service will not be installed on the Vision web/application server in your deployment of Deltek Vision.

Typically this is not a problem when Vision is deployed inside the Intranet. However, when Vision is deployed where it is accessible directly via the Internet, the infrastructure requirements needed to support the configuration become complex because it is necessary to have multiple points of entry (one each for the Vision web server and SQL Reporting web service), multiple firewall configurations, and potentially the need to have multiple public DNS records with your Internet Service Provider (ISP). To complicate matters, if you have a two tier deployment of Deltek Vision, this deployment may require that the server hosting your database is made accessible to the Internet, posing additional security risks. The architecture diagrams in the next section depict the Deltek Vision logical tier diagrams with and without a reverse proxy.

A reverse proxy utilizing Microsoft's Application Request Routing (ARR) extension for IIS allows the direct forwarding of requests through the Vision web server to the reporting services web service with responses back to your Internet clients. This configuration resolves all of the issues identified in the previous paragraph but does require that the server hosting the Vision web/application server be running Windows Server 2008 / IIS 7.0 or Windows Server 2008 R2 / IIS 7.5 or Windows Server 2012 / IIS 8.0.

The primary intent of a reverse proxy is to shield the SQL server from access via the Internet. Specifically, this is for two tier deployments where the SQL database and report server are on the same physical machine. Deltek does **not** recommend the use of the reverse proxy for a large number of users due to the potential performance impact that the reverse proxy component may introduce to the Vision web/application server.

With the release of Vision 7.2, Deltek supports the use of Application Request Routing 3.0 for Vision 7.0 SP1 and higher. If you are running Vision on Windows Server 2008 / IIS 7.0 or Windows Server 2008 R2 / IIS 7.5 and already have ARR 2.0 or 2.5, an ARR upgrade is not necessary. ARR 3.0 support is intended for new installations on Windows Server 2012 / IIS 8.0, but is also supported for new installations on Windows Server 2008 / IIS 7.0 and Windows Server 2008 R2 / IIS 7.5.

Install ARR

Follow the steps below to install ARR. These installation instructions are specific to version 3.0 of ARR.

Prerequisites

The following pre-requisites must be met before installation:

- The Vision web/application server must be running Windows Server 2008 / IIS 7.0 or Windows Server 2008 R2 / IIS 7.5 or Windows Server 2012 / IIS 8.0.

7. When the Web Platform Installer has finished downloading and installing all components, click **Finish,** then **Exit,** on the Web Platform Installer main page.
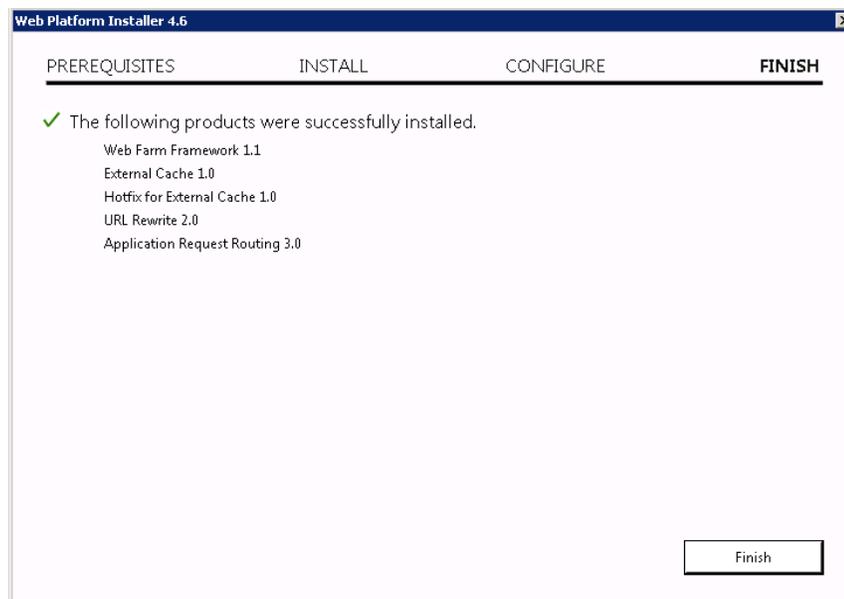
Configure ARR

To configure Application Request Routing, complete the following steps:

1. Open Windows Explorer and create two folders under <drive>:\Program Files\Deltek\Vision\Web\, named:

    ▪ Reports

    ▪ ReportServer

    For example, enter: c:\Program Files\Deltek\Vision\Web\Reports).

    For x64 operating systems, the path is Program Files (x86).

2. Create a new Application Pool called **DeltekVisionReportingProxy**:

   a. In IIS Manager, expand the server name.

   b. Right-click **Application Pools**, then select **Add Application Pool**.

   c. Enter the name and click **OK** to create the Application Pool.
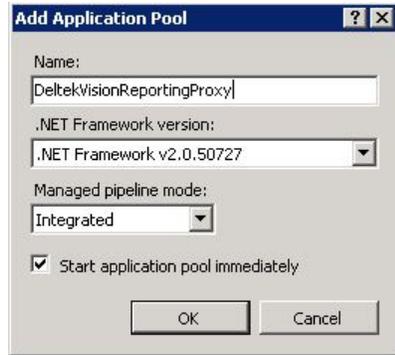
3. Modify the Application Pool settings:

   a. Right-click the **DeltekVisionReportingProxy** Application Pool and select **Advanced Settings**.

   b. If on an x64 server, set **Enable 32 bit applications** to **True**.

   c. Configure the **Identity** to be the same account as your DeltekVisionAppPool. By default, this is the local DeltekVision Windows account.
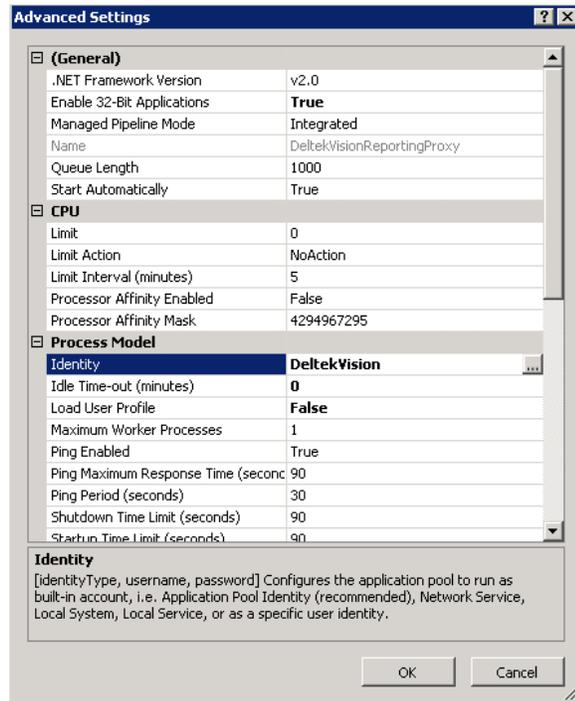
   d. Set the **Idle Time-out** to **0** (the default is 20)

   e. Scroll down to see more Advanced Settings.
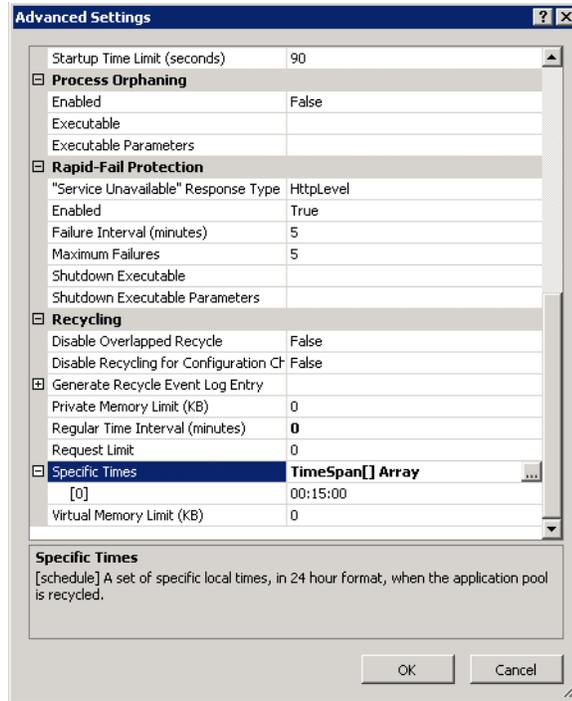
f. Set **Regular Time Interval (minutes)** to **0** (the default is 1740).

g. Set **Specific Times** to **00:15:00** (the default is 00:00:00).

4. Create IIS Applications to act as the Proxy for the Reports (SQL RS Report Manager) and ReportServer (SQL RS web service):

a. In IIS Manager, expand **Sites**.

b. Right-click **Default Web Site** and then select **Add Application**.

c. In the **Alias** field, enter **Reports** and then configure it to use the DeltekVisionReportingProxy and enter (or browse to) the physical path that you created in step 1.

d. Click **OK** to create the Reports Application.
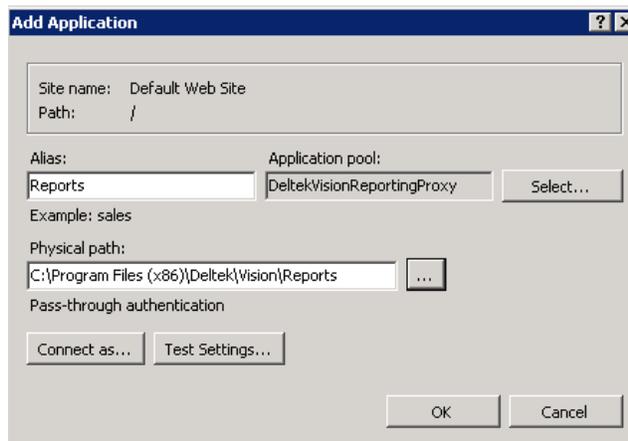
5. Set up the ReportServer Application.

a. Right-click **Default Web Site** and then select **Add Application**.

b. In the **Alias** field, enter **ReportServer** and then configure it to use the DeltekVisionReportingProxy and enter (or browse to) the physical path you created in step 1.

c. Click **OK** to create the ReportServer Application.

6. Add **Rewrite Rules** for each reporting application.

a. Under **Default Web Site**, click the **Reports Application**.

b. Double-click **URL Rewrite**.

> If you do not see the URL Rewrite module, it's possible that Internet Services Manager was open when ARR was installed. Close and re-open Internet Services Manager.
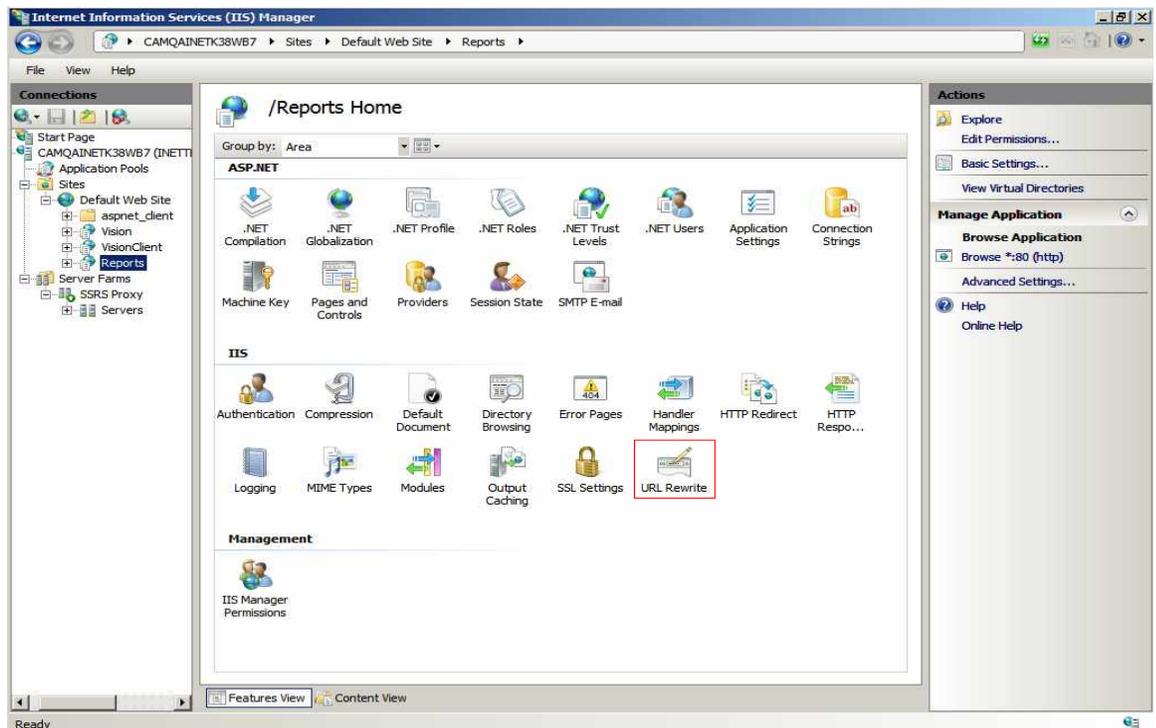
c. Click **Actions » Add Rules**.
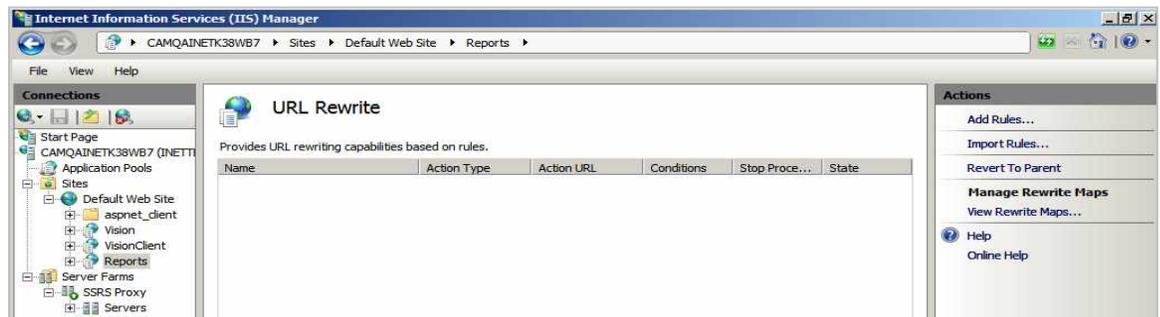
d. Select **Reverse Proxy** and click **OK**.
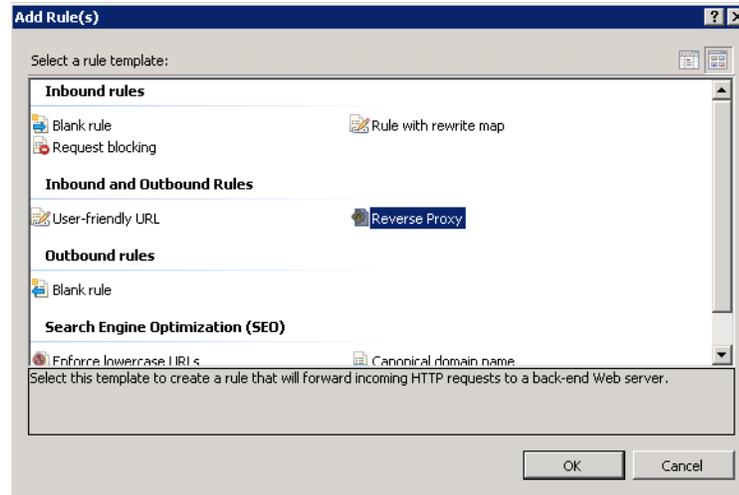
e. When the following prompt displays, click **OK**.
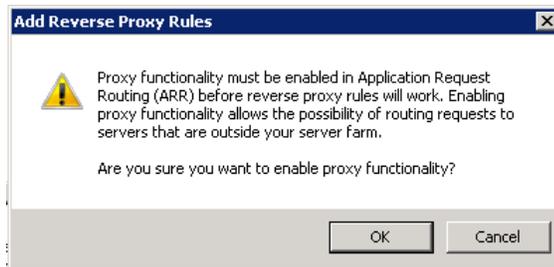
f. On the Add Reverse Proxy Rules dialog box, enter the name of your SQL Reporting Services server in the **Inbound Rules** text box.
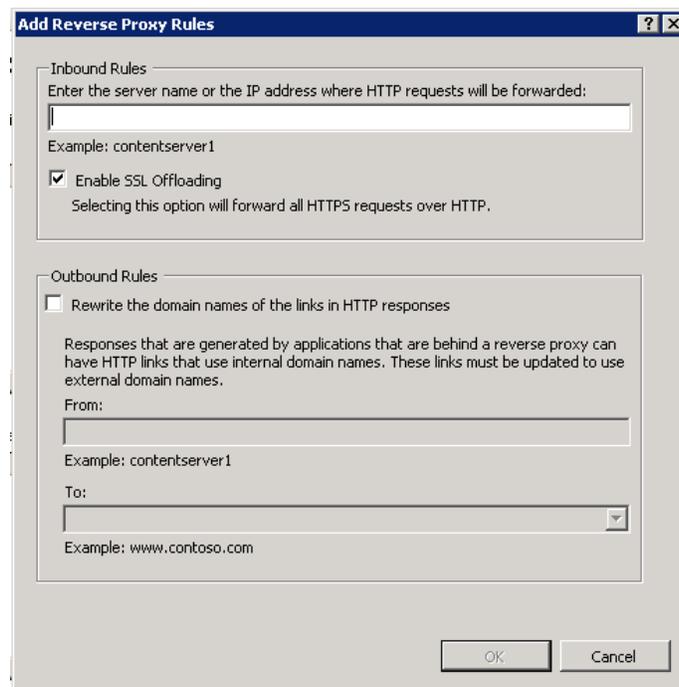
If your Vision server is configured for SSL, keep **Enable SSL Offloading** selected (this is the default). With SSL Offloading enabled, it is not necessary for an SSL

certificate to be installed on the SQL Reporting Services server. The SSL certificate on the web/application server will ensure that reporting functionality is encrypted between client and server.

g. Click **OK** to create the reverse proxy rule.

h. Select the rule that was created and click the **Edit** link on the right, under **Inbound Rules**.
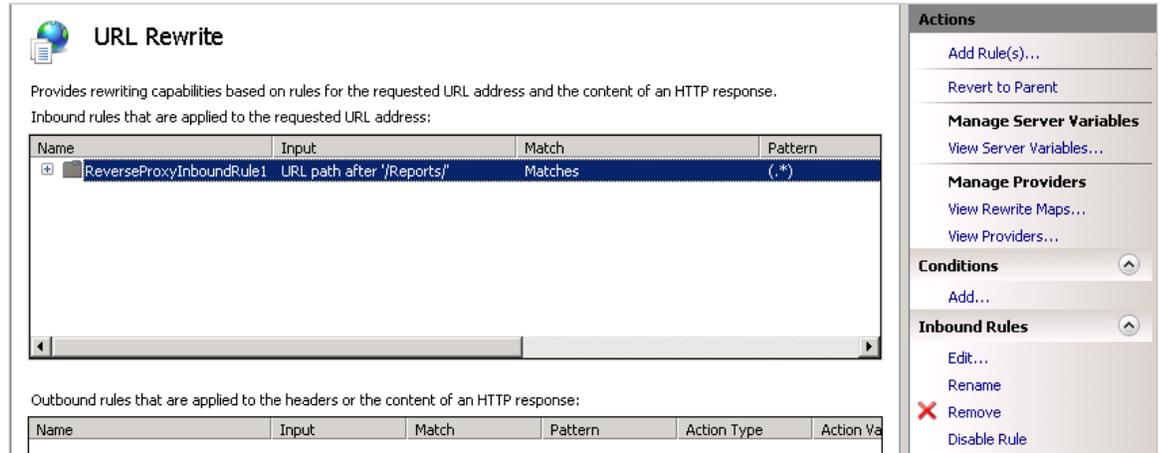
i. By default, the rewrite rule only includes the base URL for the server name entered. Edit the URL under **Rewrite URL** to have the correct Reporting Services application. The correct URL will be:

http://<reportserver>/Reports/{R:1}

	Make sure there is a slash between Reports and {R:1}.
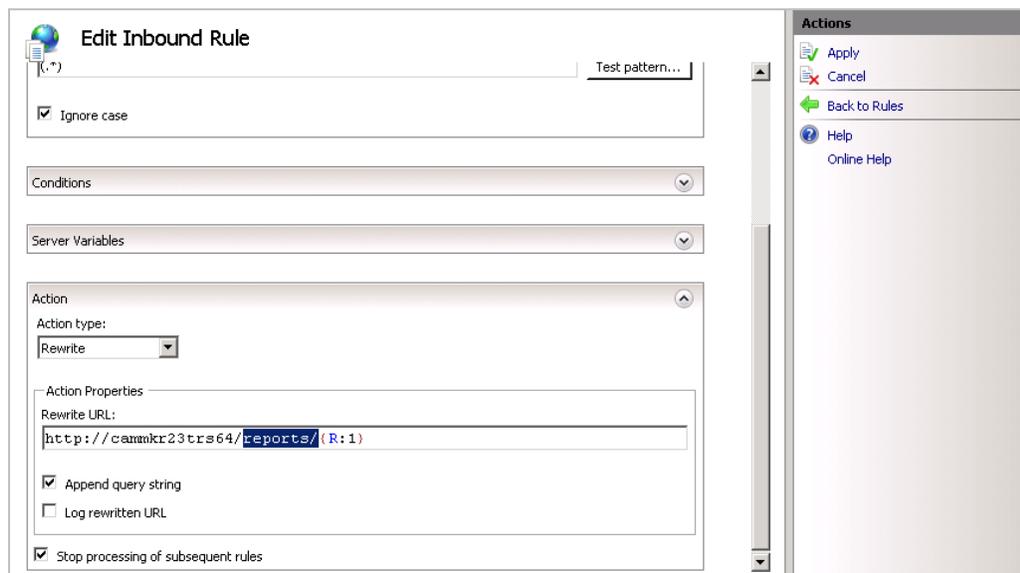
7. Repeat steps 6a through 6g for the ReportServer virtual directory.

a. Under **Default Web Site**, click the **ReportServer Application**.

b.   Double-click **URL Rewrite**.

c.   Click **Actions » Add Rules**.

d.   Select **Reverse Proxy** and click **OK**.

e.   When prompted about enabling proxy functionality, click **OK**.

f.   On the Reverse Proxy Rules dialog box, enter the name of your SQL Reporting Services server in the **Inbound Rules** text box.

g.   Click **OK** to create the reverse proxy rule.

8.   Select the rule that was created and click the **Edit** link on the right under **Inbound Rules**. By default, the rewrite rule only includes the base URL for the server name entered.

9.   Edit the URL under **Rewrite URL** to have the correct Reporting Services application. The correct URL will be:

http://<reportserver>/ReportServer/{R:1}

Test the Proxy Server

To test the proxy server, complete the following steps:

1.   Open Internet Explorer and browse to the following URLs. If ARR has been configured properly, your request will be proxied to the SQL Reporting Services server.

   ▪ **http://<VisionWebServer>/Reports**

   where "VisionWebServer" is the Fully Qualified Domain Name of the web/application server:
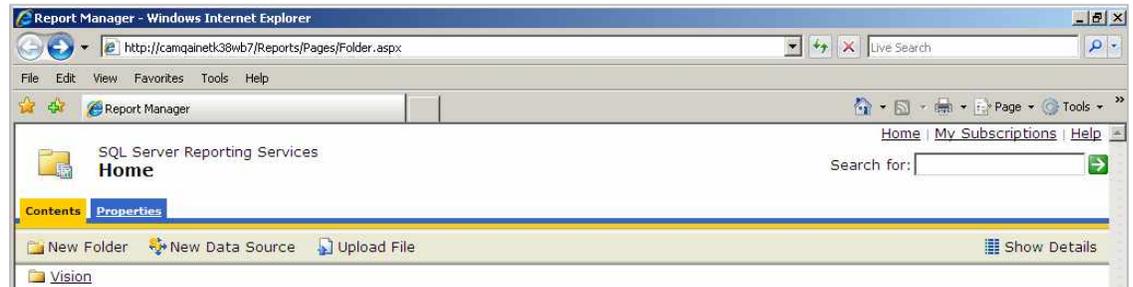
   ▪ **http://<VisionWebServer>/ReportServer**

   where "VisionWebServer" is the Fully Qualified Domain Name of the Web/Application server:

Configure Vision to Use the Reverse Proxy

To modify Weblink to use the Reverse Proxy, complete the following steps:

1. To open Weblink, click **Start » All Programs » Deltek Vision** if on the Web/Application server or via **http://<VisionWebServer>/Vision/Weblink.htm**.

2. Enter the password to access Weblink.

3. Click the Report Server tab and modify the Server URL to be the URL to access the new ReportServer virtual directory that you created on the Vision Web Server.

4. Typically, the Server URL is in the form **http://<ReportServer>/ReportServer**.Change this to **http://<VisionWebServer>/ReportServer**.

    No additional changes are necessary to the Weblink configuration. Be sure to change all databases that will use the reverse proxy.
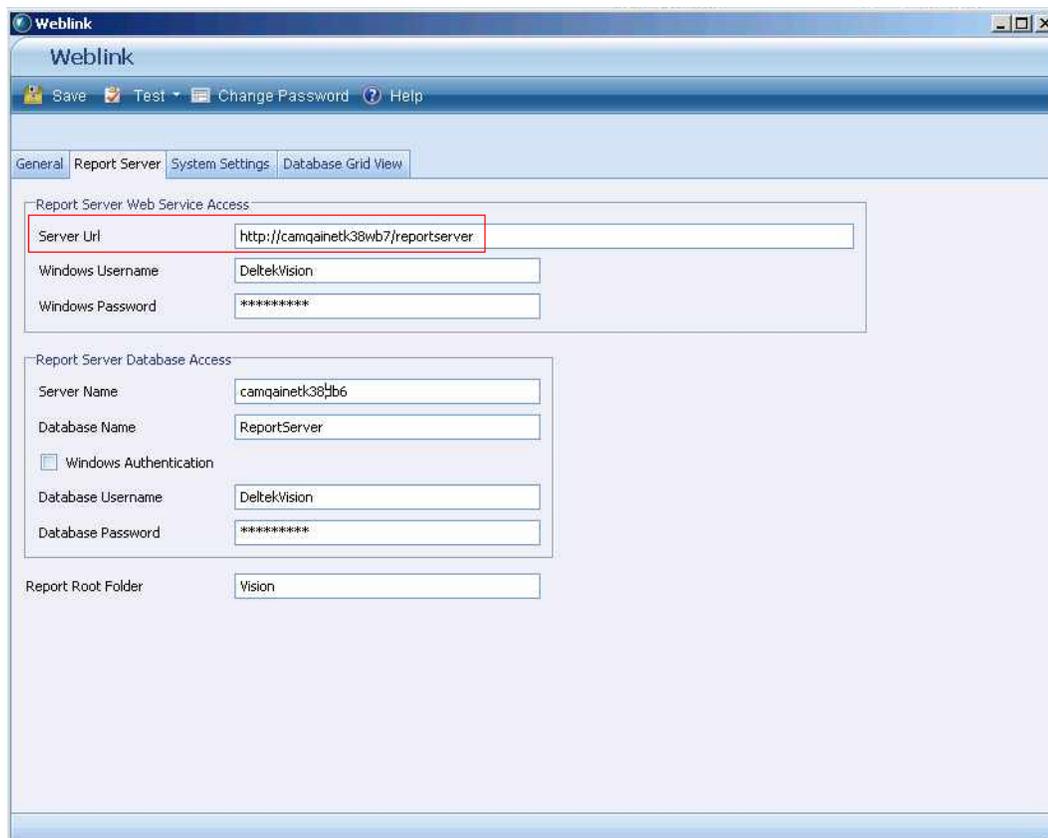
    It is expected that you secure the Vision Web server with an SSL certificate. In this configuration, it is not necessary to secure the SQL Reporting Services server with an SSL certificate so the URL entered above should be http, not https. The proxy server will handle the forwarding of the https traffic to http.

5. To test the Report Server configuration, click **Test » Report Server Configuration**.
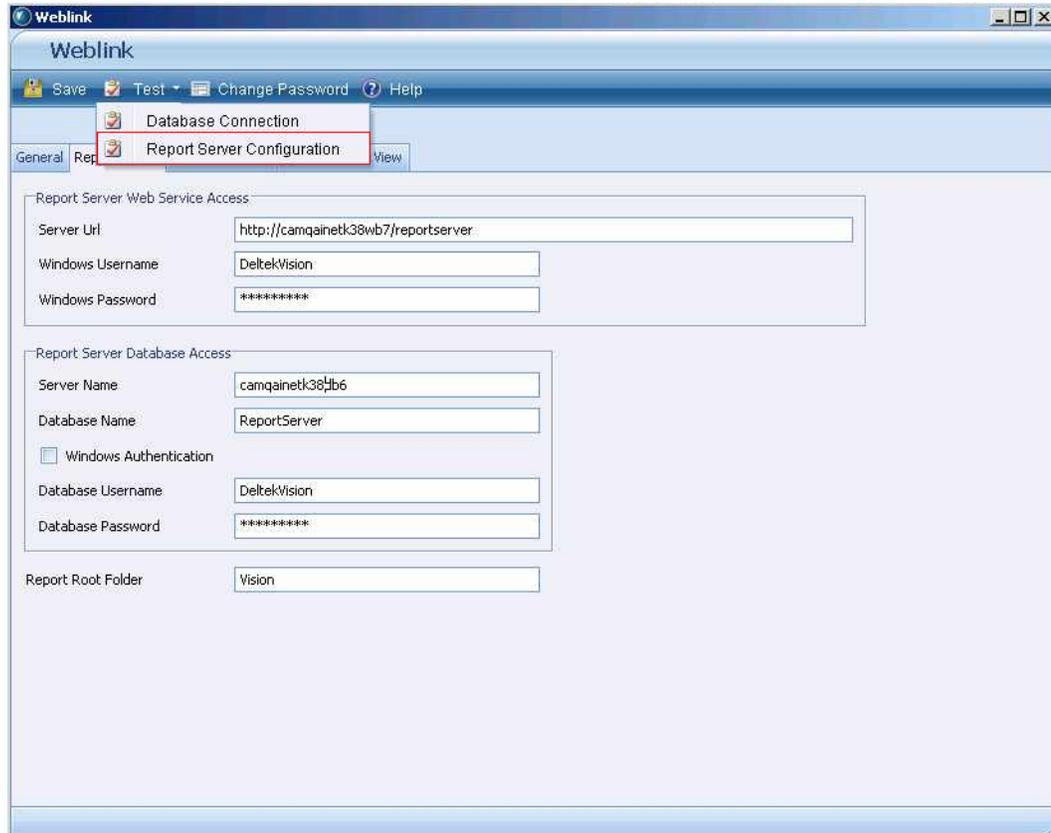
6. After the configuration tests successfully, save your changes.

Troubleshooting

If you need assistance, contact the Deltek Global Services consulting group, customservices@deltek.com. The consulting group will provide an estimate of the cost for the assistance you need.

ARR Documentation

For additional documentation, go to http://www.iis.net/extensions/ApplicationRequestRouting

Chapter 2: Configuring HTTP Compression

Configuring HTTP compression for Vision can greatly reduce the size of http (hypertext transfer protocol) requests and responses between the client and web server, which improves application response time.

HTTP Compression is an available functionality built into Internet Information Services (IIS). By default, however, HTTP Compression is not enabled.

This section explains how to install and configure HTTP Compression.

Three Configuration Methods for HTTP Compression

You can configure HTTP Compression using one of three methods. This document focuses on the first of the three methods. However, you can use the modified entries and settings from applicationhost.config, described at the end of this section, if you want to use the other methods.

- Use the **appcmd** IIS command line administrative utility. You must run this utility via an elevated command prompt such as "Run as Administrator."

- Modify the **applicationhost.config** file directly. Deltek does **not** recommend that you modify the applicationhost.config file directly unless you are familiar with XML formatting. Be sure to make a backup of applicationhost.config before you make any changes.

- Use the **Configuration Editor** via the Internet Information Services administrative utility:
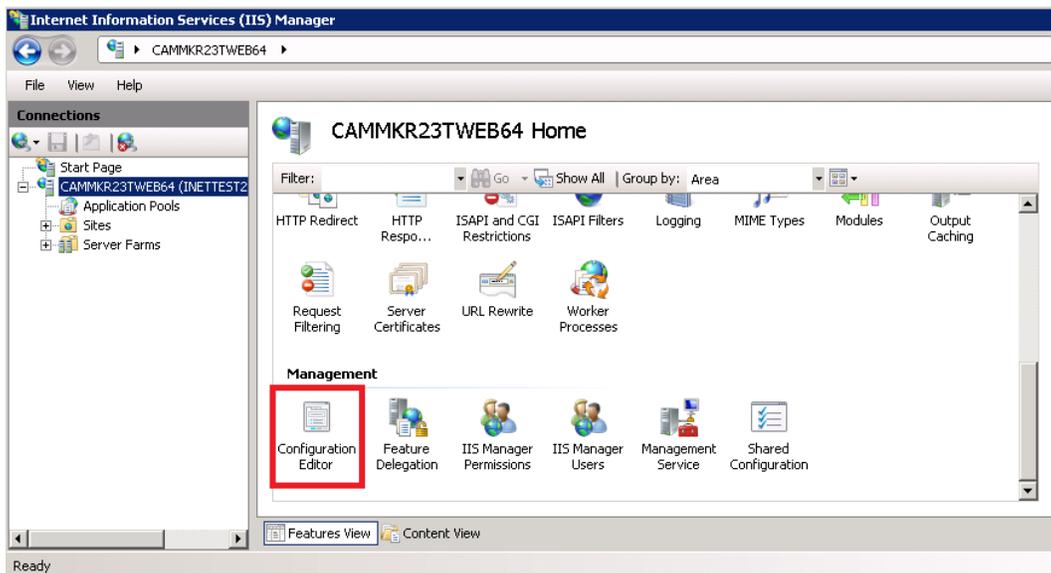
Install HTTP Compression IIS Role Services

To install HTTP Compression IIS Role Services, complete the following steps:

1. Launch the **Server Manager**.

2. Click **Roles**.

3. Under Web Server (IIS), locate **Role Services** and check to see whether these role services have been installed:

4. If not, select **Add Role Services** and install both role services.

Alternate Procedure

Alternatively, you can install these role services using the Windows Package Manager (pkgmgr) from an administrative command prompt (for example, "Run as Administrator"):

start /w pkgmgr /iu:IIS-WebServerRole;IIS-Performance;IIS-HttpCompressionStatic;IIS-HttpCompressionDynamic

Configure HTTP Compression

To configure HTTP Compression, complete the following steps:

1. Select one of the following actions:

    ▪   If you want to enable compression at the server level, ensure that both static and dynamic compression is enabled via an elevated command prompt:

        C:\Windows\System32\Inetsrv\Appcmd.exe set config -section:urlCompression -doStaticCompression:true -doDynamicCompression:true

    ▪   If you want to enable compression for a particular web site, use the following command and replace "Site Name" with the name of the web site:

        C:\Windows\System32\Inetsrv\Appcmd.exe set config "Site Name" -section:urlCompression -doStaticCompression:true -doDynamicCompression:true

2. Set the static and dynamic compression levels via an elevated command prompt:

    C:\Windows\System32\Inetsrv\Appcmd.exe set config -section:httpCompression -[name='gzip'].staticCompressionLevel:9 -[name='gzip'].dynamicCompressionLevel:4

    The default dynamic compression level is zero.

    > Dynamic compression can significantly impact CPU resources. Refer to the following blog post for information and recommendations on setting compression levels. The command above uses the recommendations from this blog:
    >
    > http://weblogs.asp.net/owscott/archive/2009/02/22/iis-7-compression-good-bad-how-much.aspx

3. Configure the content types that you want to compress. The default configuration compresses most static and dynamic content types used by the application.

    However, you must configure specific content types to compress the ClickOnce content types.

    C:\Windows\system32\inetsrv\appcmd set config /section:httpCompression /+dynamicTypes.[mimeType='application/octet-stream',enabled='true'] /commit:apphost

    C:\Windows\system32\inetsrv\appcmd set config /section:httpCompression /+dynamicTypes.[mimeType='application/x-ms-application',enabled='true'] /commit:apphost

C:\Windows\system32\inetsrv\appcmd set config /section:httpCompression /+dynamicTypes.[mimeType='application/x-ms-manifest',enabled='true'] /commit:apphost

> ClickOnce content types are considered dynamic. If you add them under the <statictypes> section, ClickOnce files are not compressed.
>
> See the following Microsoft support article for additional guidance on setting content types:
>
> http://support.microsoft.com/kb/969062

Additional Settings that May Impact HTTP Compression

You should test to ensure that HTTP Compression is working as expected before modifying these settings. Refer to the following section to determine if these settings are necessary in your environment.

The following additional settings may impact the functionality of HTTP Compression:

C:\Windows\system32\inetsrv\appcmd.exe set config -section:system.webServer/serverRuntime /frequentHitThreshold:1 /commit:apphost

C:\Windows\system32\inetsrv\appcmd.exe set config -section:system.webServer/serverRuntime /frequentHitTimePeriod:00:01:00 /commit:apphost

The default values are **2** and **00:00:10**, respectively.

> For more information, see http://www.iis.net/ConfigReference/system.webServer/serverRuntime.

Testing the HTTP Compression Configuration

Fiddler HTTP Debugging Proxy (http://www.fiddlertool.com) is a good tool for determining whether or not HTTP Compression is working as expected.

HTTP Compression sections/settings in Applicationhost.config

The configuration of HTTP Compression that is documented above modifies three primary sections in applicationhost.config. These sections are shown below and the specific settings that are modified are shown in red:

1. <urlCompression doStaticCompression="true" doDynamicCompression="true" />

2. <httpCompression directory="%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files">

    <scheme name="gzip" dll="%Windir%\system32\inetsrv\gzip.dll" staticCompressionLevel="9" dynamicCompressionLevel="4" />

    <staticTypes>

      <add mimeType="text/*" enabled="true" />

      <add mimeType="message/*" enabled="true" />

      <add mimeType="application/x-javascript" enabled="true" />

      <add mimeType="application/atom+xml" enabled="true" />

```
        <add mimeType="application/xaml+xml" enabled="true" />

        <add mimeType="*/*" enabled="false" />

    </staticTypes>

    <dynamicTypes>

        <add mimeType="text/*" enabled="true" />

        <add mimeType="message/*" enabled="true" />

        <add mimeType="application/x-javascript" enabled="true" />

        <add mimeType="application/octet-stream" enabled="true" />

        <add mimeType="application/x-ms-application" enabled="true" />

        <add mimeType="application/x-ms-manifest" enabled="true" />

        <add mimeType="*/*" enabled="false" />

    </dynamicTypes>

  </httpCompression>
```

3. `<serverRuntime frequentHitThreshold="1" frequentHitTimePeriod="00:01:00" />`

Chapter 3: Configuring the Secure Sockets Layer (SSL)

Securing the Vision Web Server

To configure Vision for use with SSL, you must either:

- Obtain an SSL certificate from an online certificate authority such as Verisign, Thawte, or Comodo, *or*

- Have access to a domain or stand-alone certificate authority on your network.

The procedure below includes steps for creating and completing the certificate request process.

To secure the Vision web server, complete the following steps:

1. Log on to the web server.

2. From Administrative Tools, open **Internet Information Services Manager**.

3. From the navigation pane at left, select your server navigation menu.

4. Double-click **Server Certificates**.
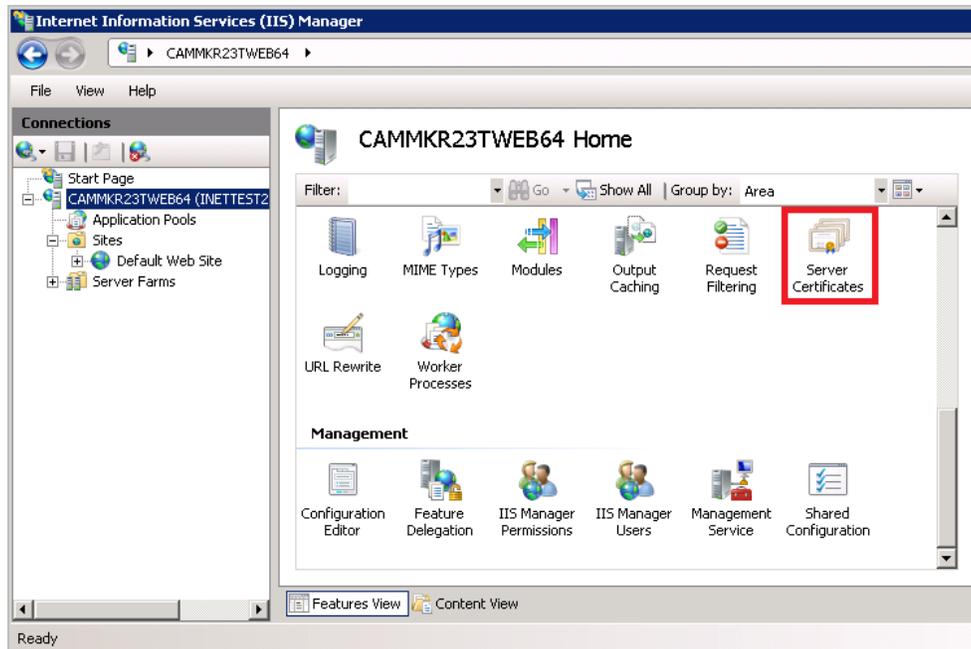
The Server Certificates window displays.
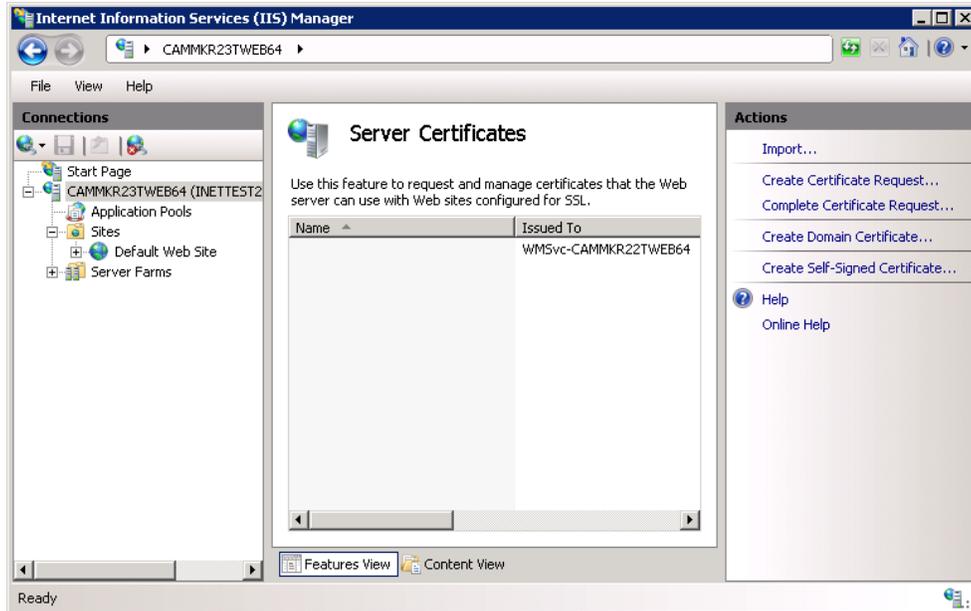
5. In the Actions pane, select one of the following options:

   ▪ **Import** — If you already have a certificate for your server, select this action to import that certificate.

   ▪ **Create Certificate Request** — Select this action to launch a wizard that guides you in creating a text file to submit to your Certificate Authority (CA), to obtain the actual SSL certificate for your web server.

   ▪ **Complete Certificate Request** — If you used **Create Certificate Request** to request a certificate, select this action to complete your request and install your certificate.

   ▪ **Create Domain Certificate** — If you have a CA on your domain, select this action to request your certificate.

   ▪ **Create Self-Signed Certificate** — Select this action to test SSL functionality or troubleshoot SSL certificate issues.

   After you obtain and import your SSL Certificate, you create an SSL binding for your web server.

6. Expand **Sites** and select your web site.

7. In the Actions pane, click **Bindings**.
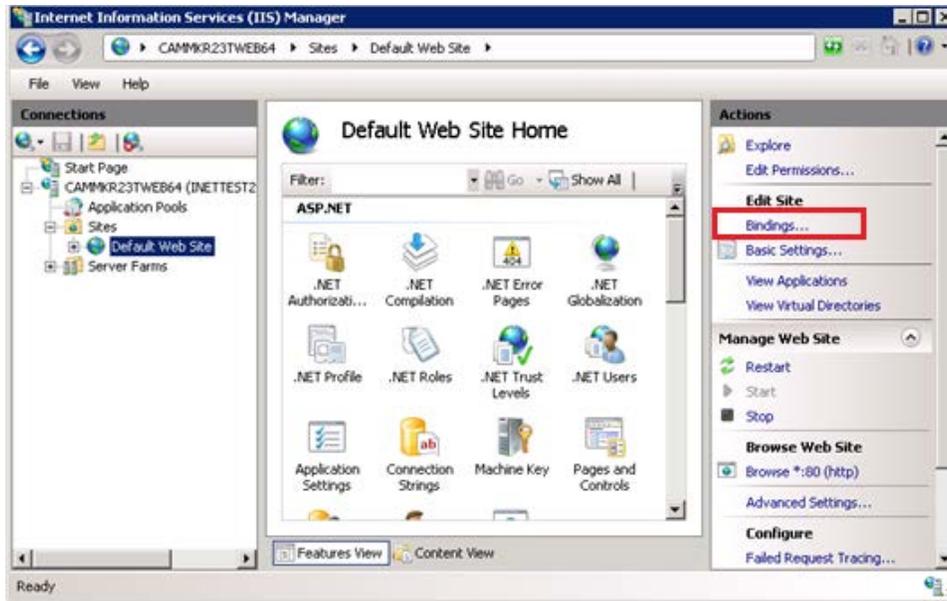
The Site Bindings dialog box displays.
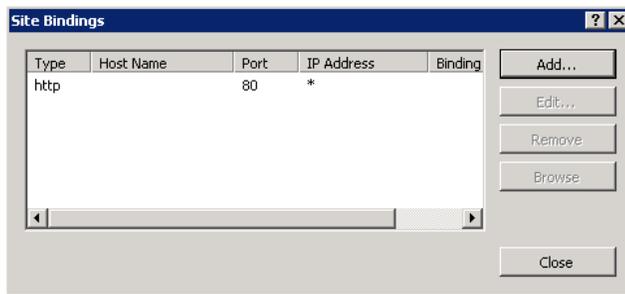
8. Click the **Add** button. The Add Site Binding dialog box displays.

9. From the **Type** drop-down list, select **https**. The **Port** value automatically changes to **443**.

10. From the **IP address** drop-down list, select your IP address or use the default setting, **All Unassigned**.

11. From the **SSL Certificate** drop-down list, select your certificate.

12. Click **OK**.

Test the SSL Certificate and Binding

To test your new SSL certificate and binding, access your web site using **https://** as the URL prefix and then make sure that everything is working correctly.

Securing SQL Server Reporting Services

The Reporting Services Configuration Manager does not directly support the requesting and importing of the SSL certificate, as IIS does. To request and import the SSL Certificate on your Reporting Services server, you must use the Certificates MMC (Microsoft Management Console) snap-in, which is outlined below.

The SSL architecture of Vision is such that if you are using SSL for Vision, you **must** use SSL for Reporting Services.

▪ You cannot run SSL for Vision without an SSL binding configured for Reporting Services.

▪ You cannot run Vision without SSL and still use SSL for Reporting Services.

▪ The Reporting Services web service URL in Weblink must reference the **Fully Qualified Domain Name** (FQDN) of the report server. This is specified in the SSL certificate. If the report server previously referenced a local netbios name, that must be changed to the FQDN. The FQDN name must be in the following format:

http(s)://vision.companyname.com/reportserver

▪ Wildcard certificates are not acceptable.

To secure SQL Server Reporting Services for Vision, complete the following steps:

1. Click **Start » Run**.

2. In the **Open** field on the Run dialog box, enter **mmc** and then click **OK**. The MMC console launches.

3. Click **File » Add/Remove Snap-in**. The Add or Remove Snap-ins dialog box displays.

4. Select **Certificates** and click **Add**.
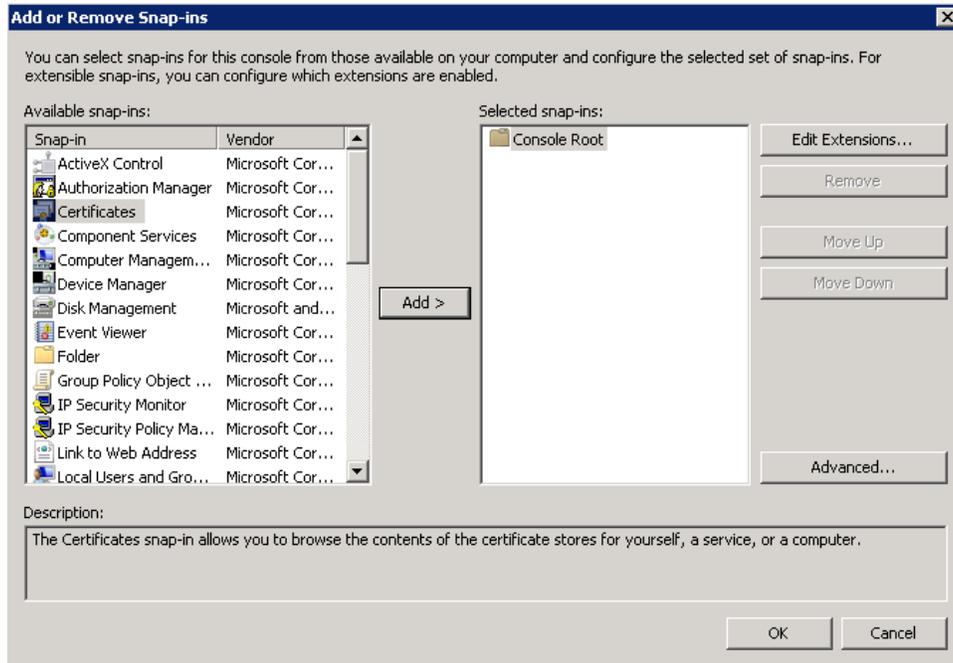
5. Select **Computer account** and then click **Next**.

6. Select **Local Computer**.

7. Click **Finish** and then click **OK**. You should now see the certificate store, as shown below.
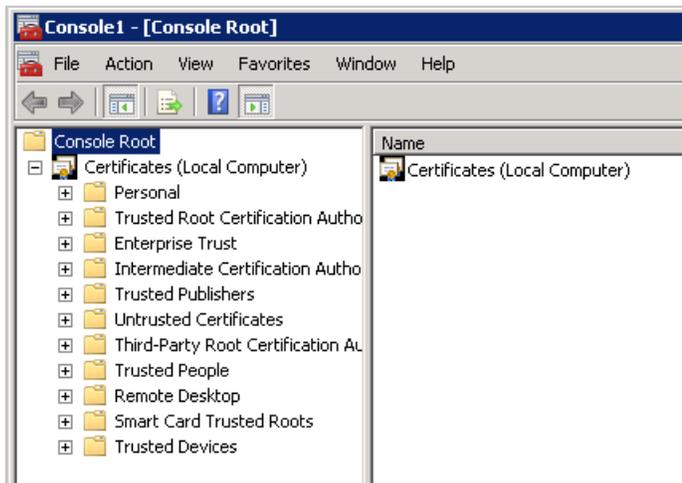
Next you need to request a new certificate or import an existing certificate.

8. Right-click the **Personal** folder and select **All Tasks**.
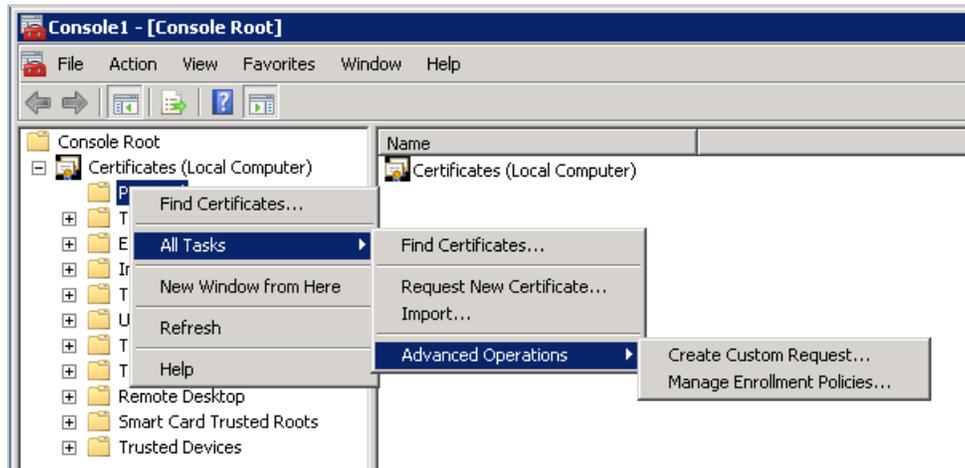
9. Select one of the following actions:

    ▪   If you have a domain Certificate Authority (CA), select **Request New Certificate**.

    ▪   If you need to request a certificate from a stand-alone CA or an online CA, select **Advanced Operations** and **Create Custom Request**.

10. After you have your SSL certificate, import it using the following steps:

    a. Right-click the **Personal** folder.

    b. Select **All Tasks**.

    c. Select **Import** to launch the Certificate Import Wizard.

    d. Browse to the location of your SSL certificate and complete the import process. The following sample certificate was imported from a domain CA
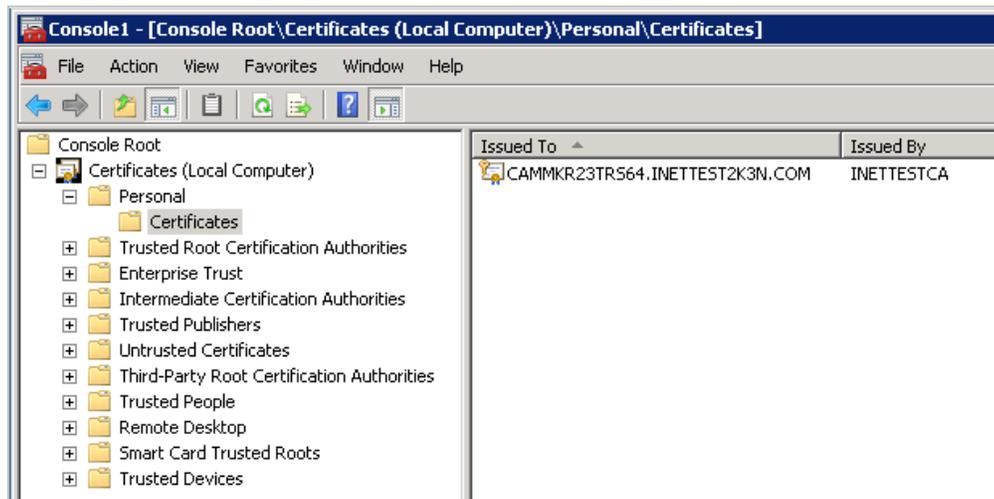
    At this point the certificate is registered with the server. The next step is to register the certificate with SQL Reporting Services.

11. Click **Start » All Programs » Microsoft SQL Server » Configuration Tools** to open the Reporting Services Configuration Manager on the Report Server.
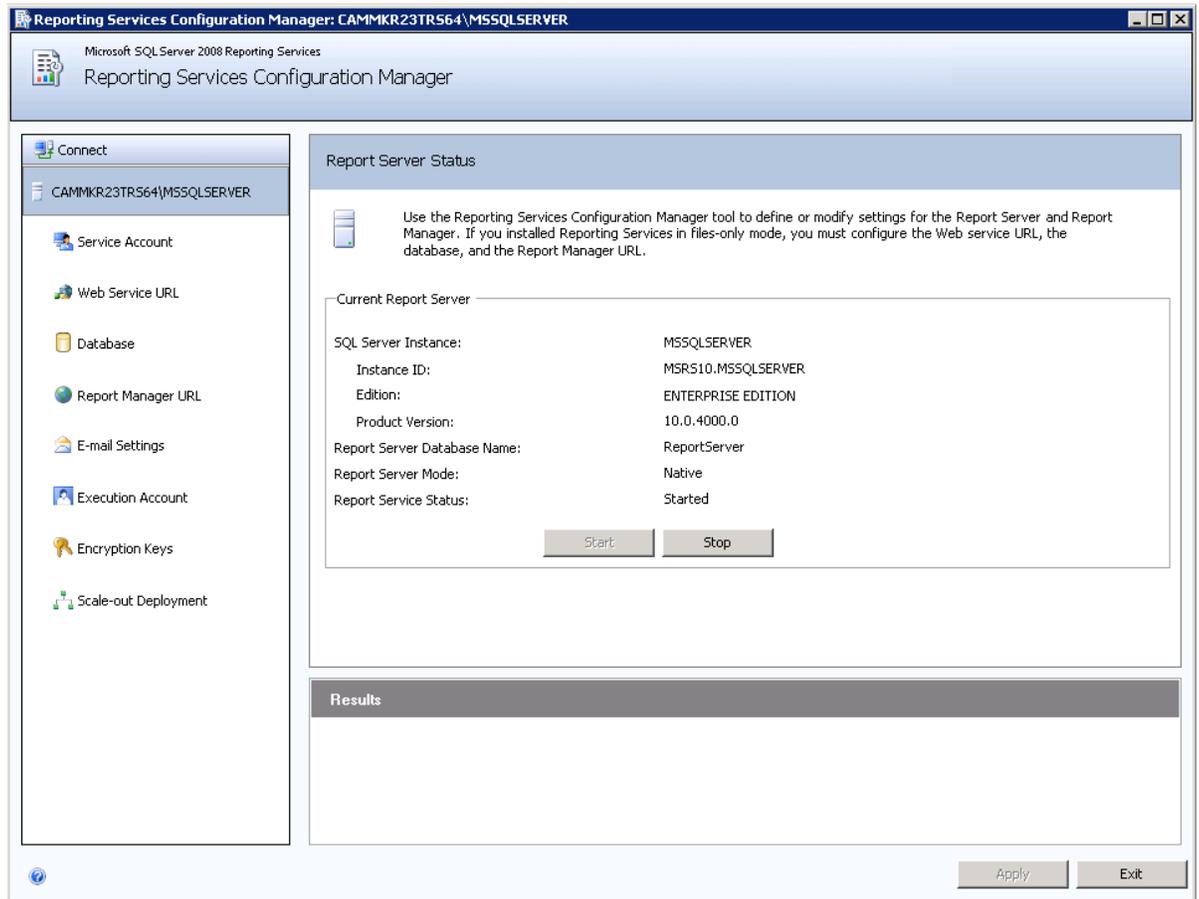
The next steps are to create the SSL bindings for the Web Service URL and the Report Manager URL.

12. Under **Connect**, click **Web Service URL**. The Web Service URL window displays.
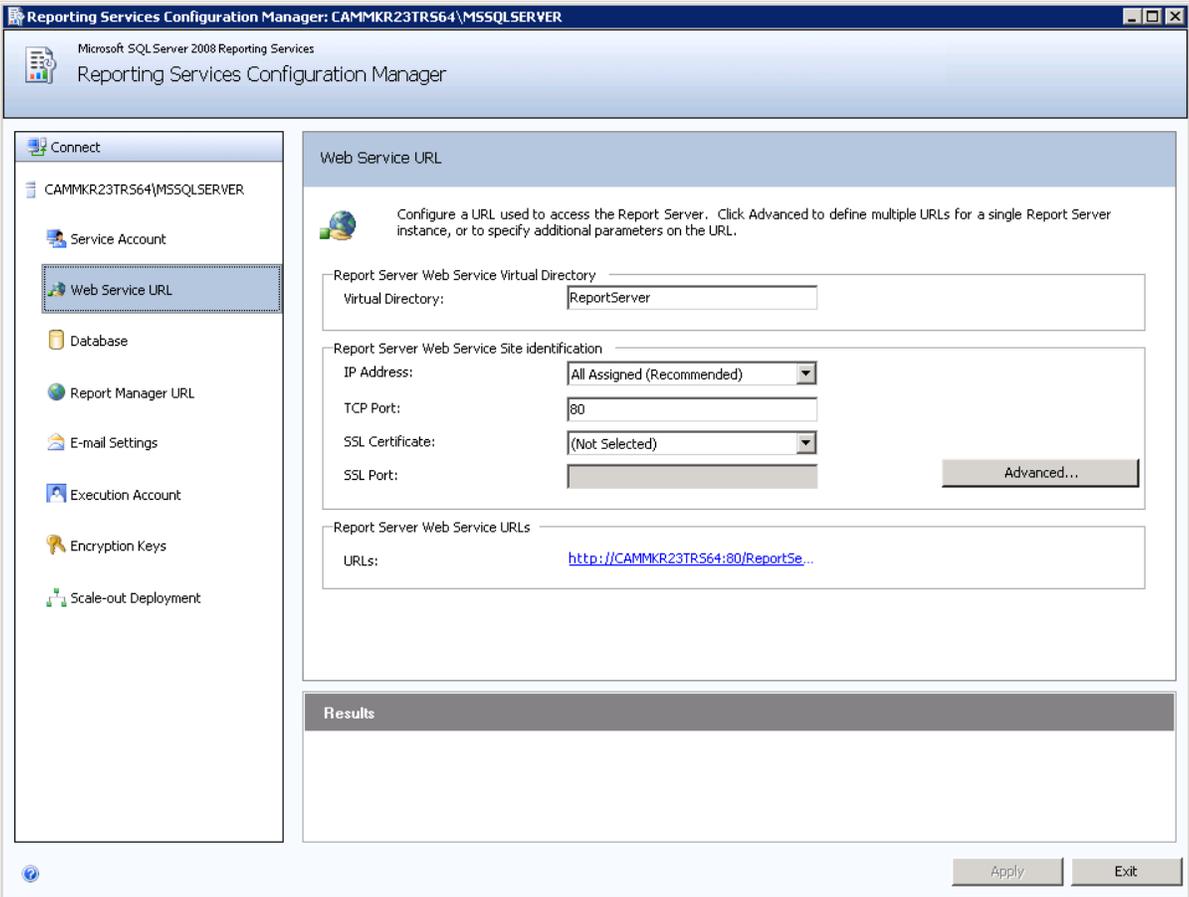
13. Click the **Advanced** button. The Advanced Multiple Web Site Configuration dialog box displays.
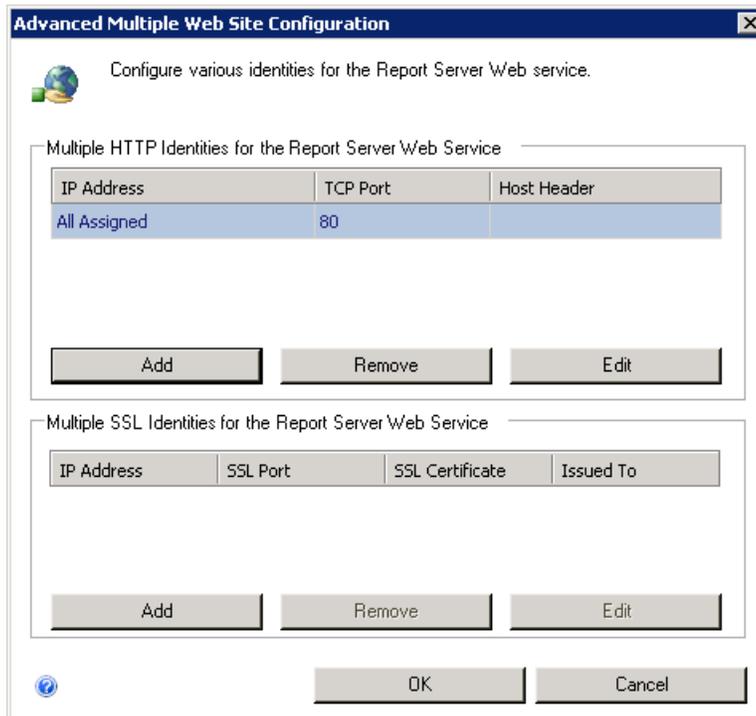
14. Under **Multiple SSL Identities for the Report Server Web Service**, click **Add**. The Add a Report Server SSL Binding dialog box displays.
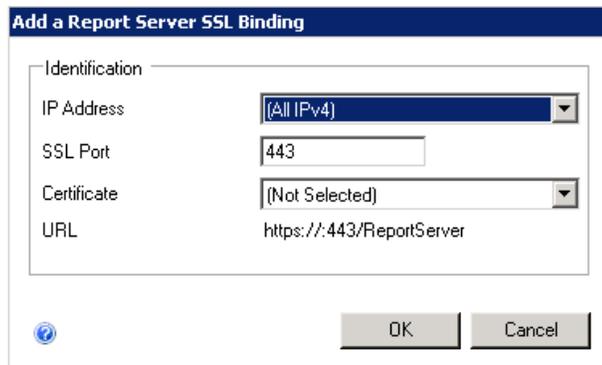
15. Select a specific **IP Address** (if appropriate).

16. Click the drop-down list for the **Certificate** option. The certificate you imported in the previous steps should now be visible. Select the certificate now.

17. Click **OK** to add this URL to the system.

> If all communication to the report server will be done via SSL then you should also remove the HTTP binding from the configuration.

18. Repeat these steps for the Report Manager URL.

19. On the Web Server, launch Weblink and log in. Select the database.

20. On the ReportServer page, verify the URL contains a reference to the **Fully Qualified Domain Name** (FQDN) of the report server. This is specified in the SLL certificate. If the report server previously referenced a local netbios name, that must be changed to the FQDN. The FQDN name must be in the following format:

    http(s)://vision.companyname.com/reportserver.

Testing the SSL Configuration

Test Vision using SSL URL's to ensure the product is functioning correctly. To do this, trace a Vision SSL session using Fiddler (http://www.fiddlertool.com) or another HTTP tracing tool.

Chapter 4: Pre-Deploying Deltek Vision Smart Client to User Workstations

The ClickOnce deployment technology is used for delivering Windows-based applications to the user. The Deltek Vision Smart Client application uses this technology to check for new updates on the application/web server each time the application is launched, and automatically installs them into the local user's profile (%USERPROFILE%\Local Settings\Apps\2.0\...).

To reduce the size of the initial client-side download when a user launches Vision, you can pre-deploy the Smart Client files to specific locations on workstations for all Windows XP and Vista users. This "Hybrid Deployment Model" installs the application by first looking in a specific folder on the workstation and, if not found, then downloading the file from the application/web server.

> Hybrid Deployment Model (HDM) – ClickOnce delivers about 15 files (enough to display the login page). After that, HDM takes over to deliver core application assemblies, hotfixes, language-specific satellite assemblies, and custom items.

ClickOnce Deployment Features

- Applications are installed per-user, not per-computer
- Administrator privileges are not required
- Applications do not have to be installed through add/remove programs
- Nothing registered to the GAC (Global Assembly Cache)
- No ActiveX objects, Plug-ins, or Java Applets
- ClickOnce Cache Location
  - Windows XP – "\Documents and Settings\USERPROFILE_Name\Local Settings\Apps\2.0"
  - Windows Vista /7– "\Users\USERPROFILE_Name\AppData\Local\Apps\2.0"

Files to be Deployed

You must repeat the process below each time that you upgrade your Vision Application/Web Servers to a new release.

The files that must be pre-deployed to the user workstations are located on the application\web server in the *"\Program Files\Deltek\Vision\WebClient"* folder (where Vision 7.0 is installed):

- DeploymentManifest.xml
- One or more zip files (as listed in the DeploymentManifest.xml)

You must copy all of the zip files, plus the DeploymentManifest.xml, to the workstation.

The dates on the time stamp for each zip file must match the date and time shown in the DeploymentManifest.xml.

Workstation Deployment Location

The location to pre-deploy the above files depends on the workstation operating system. Refer to the following procedures based on your operating system.

By default, the "\Documents and Settings" folder on XP and the "\ProgramData" folder on Vista are hidden. You may need to enable the **Show Hidden Files** option in Windows Explorer.

Windows XP Operating System

To deploy on a workstation with the Windows XP operating system, complete the following steps:

1. Locate the \Documents and Settings\All Users\Application Data\ directory and create the Deltek directory.

2. Copy the DeploymentManifest.xml file and **all** zip files from the Vision\WebClient directory on the application\web server into the Deltek directory. The dates on the time stamp for each zip file must match the date and time shown in the DeploymentManifest.xml.
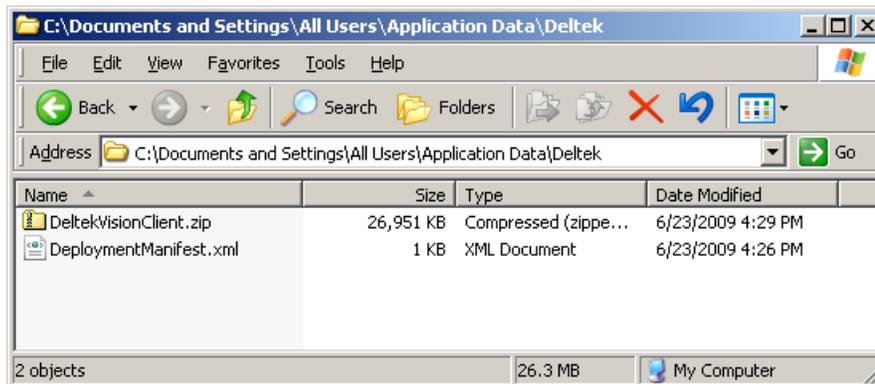
Windows Vista/7 Operating System

To deploy on a workstation with the Windows Vista/7 operating system, complete the following steps:

1. Locate the \ProgramData\ directory and create the Deltek directory.

2. Copy the DeploymentManifest.xml file and **all** zip files from the application\web server into the Deltek directory.
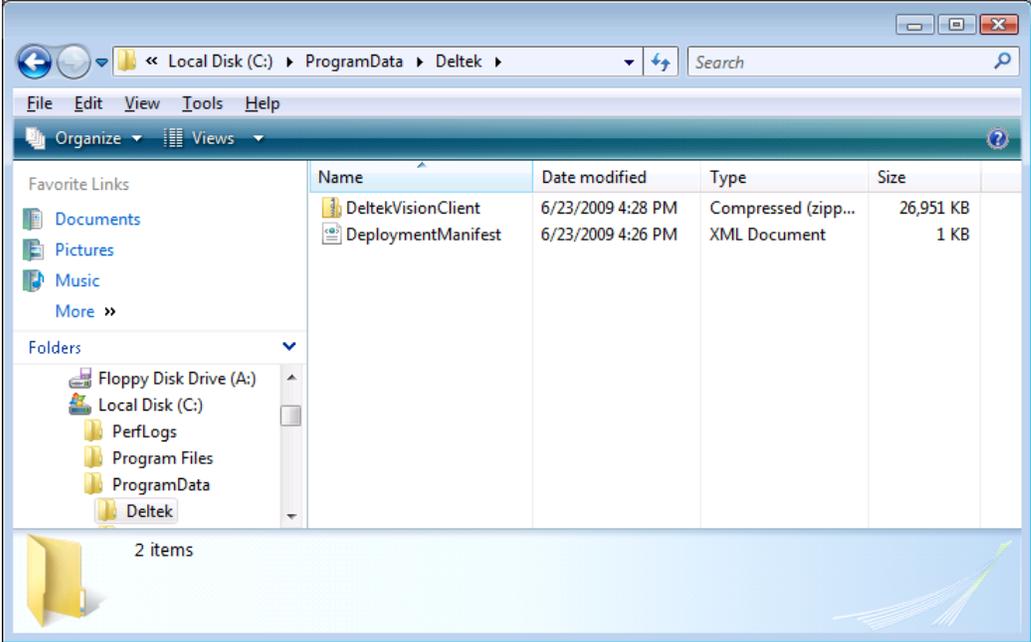
You must repeat this process each time you upgrade your Vision Application/Web Servers to a new release.

Chapter 5: Integrated Security Configuration for Vision

Vision includes an option for Windows Integrated Authentication, which allows users to log in one time for both Windows and the Vision application. You configure the use of Windows Integrated Security for each user's Vision account by using the Windows Domain network login as the username for that user. This allows the user to be logged in automatically to the Vision application as long as they are logged in to the domain. If the user is not properly logged in to their domain, the user is prompted for network credentials before they can log in to Vision. For example, non-domain workstation and users connecting to the network via an Internet connection will receive a domain authentication challenge before they are logged in to Vision.

The use of Integrated Security in IIS **requires** a CAL (Client Access License) for each user that will access that Web server. This is a Microsoft, not Deltek, licensing requirement.

Required Configuration Changes

To configure Windows Integrated Authentication, there are several changes that are required at the domain level and in IIS. These are in addition to configuring your domain user accounts in Vision. These changes are as follows:

- A domain user account must be configured as the IIS Application Pool identity for the DeltekVisionAppPool in IIS. The domain account does not require domain administrative rights. By default, the Vision installation creates a local windows account "DeltekVision" to serve this function. However, a domain account is required in order to support trusted domains as well as the default IIS 7.0/7.5 Windows Integrated Security configuration of using Kernel Mode Authentication.

- The domain account used for the Application Pool Identity needs the following rights on the Vision Web/Application server:

    - The account must be a member of the following local groups:

        - Administrators group

    - IIS_IUSERS group

    - The account requires the following local security policy rights:

        - Allow log on locally

        - Log on as a service

        - Log on as a batch job

- The Vision IIS Application (virtual directory) needs to be changed from using Anonymous Access to Windows Integrated Security.

- Kernel Mode Authentication requires that a Service Principal Name (SPN) be created for the domain user account that is the Application Pool Identity. The creation of the SPN requires domain administrative rights. See page 48 for more information.

Configure the Application Pool Identity

To configure the Application Pool Identity to be a domain account, complete the following steps:

1. Click **Server Manager » Configuration » Local Users and Groups » Groups** and add the domain user to the local Administrators and IIS_IUSRS group.
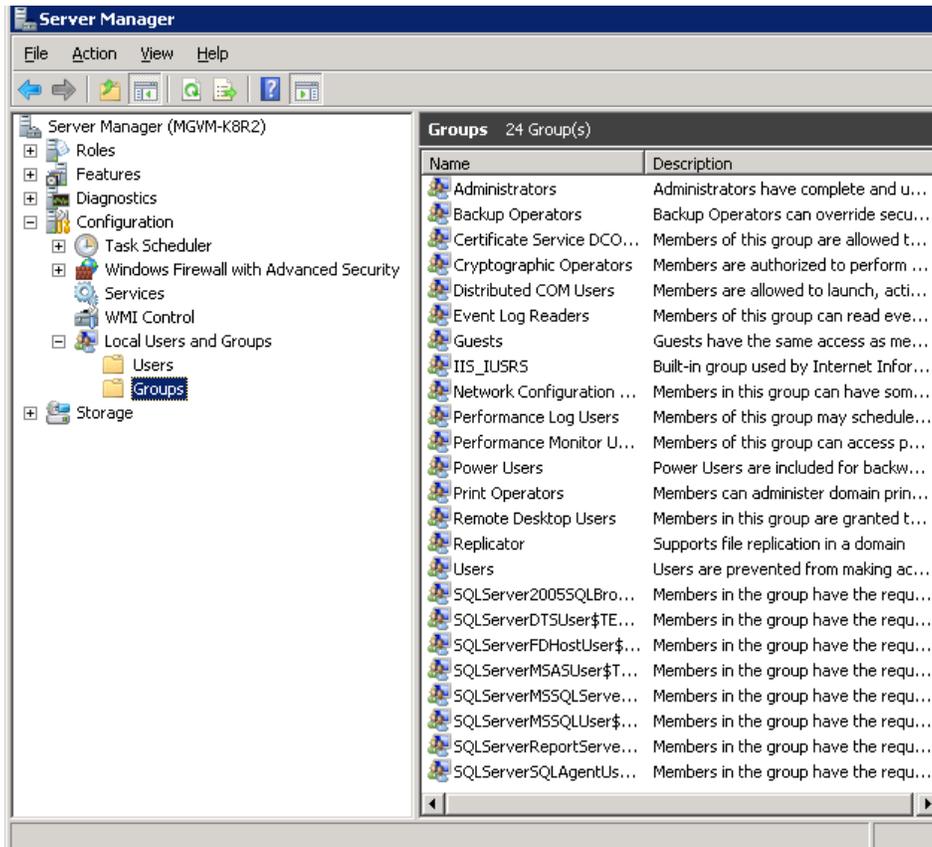
2. In Administrative tools, click **Security Settings » Local Policies » User Rights Assignment** to grant the domain user the necessary rights.
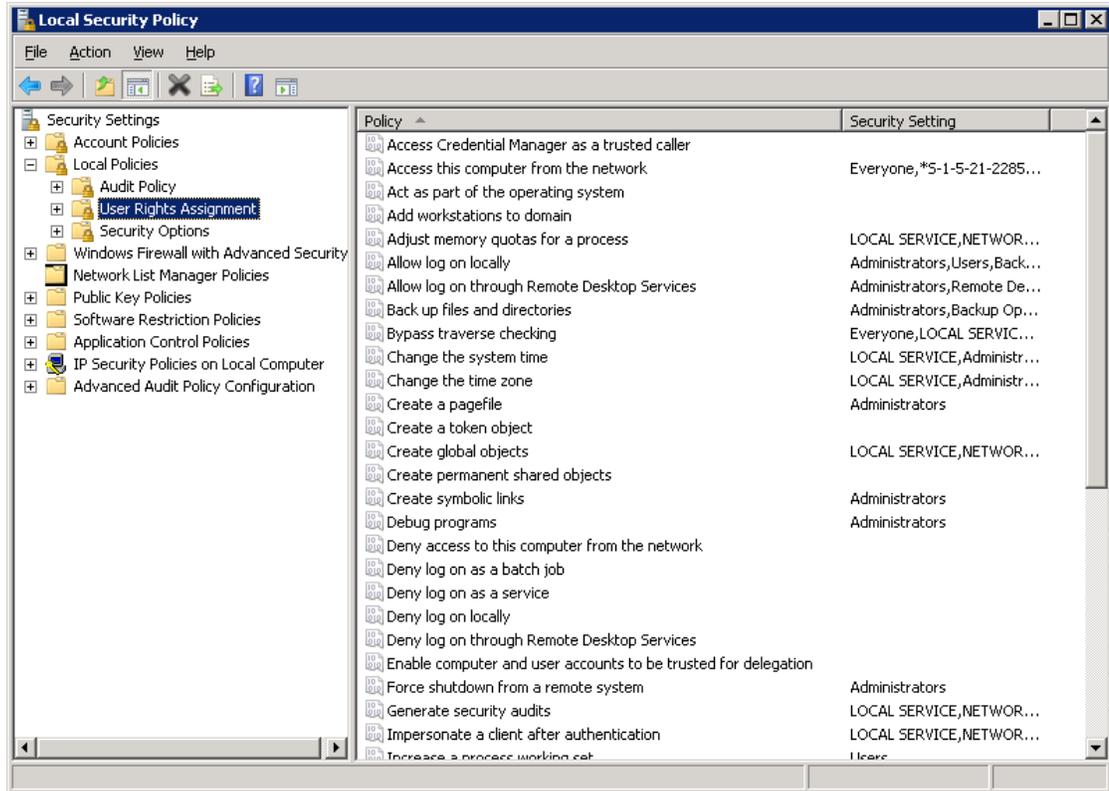
3. Click **Administrative Tools » Internet Information Services » Application Pools** and change the application pool identity.
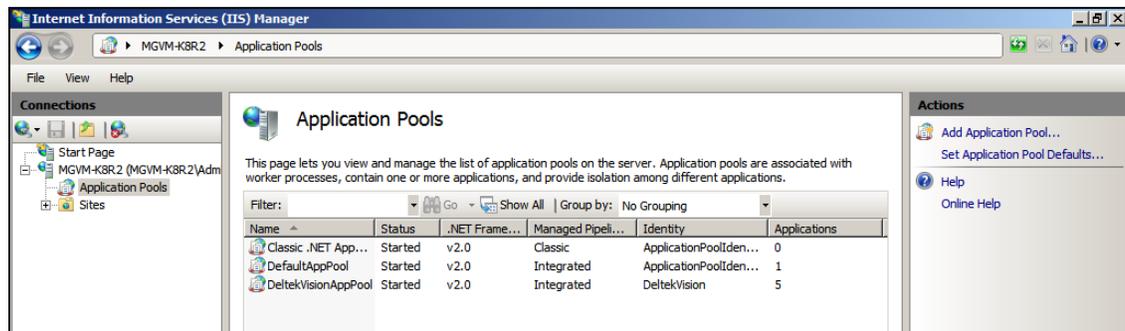
4. Right-click **DeltekVisionAppPool** and choose **Advanced Settings**.
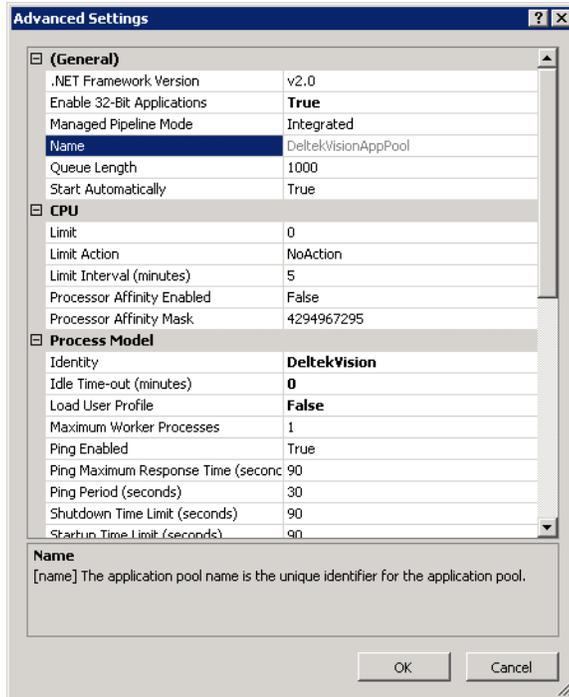
5. In the **Process Model » Identity** field, click the ellipses (**…**). The Application Pool Identity dialog box displays. Select **Custom Account**.

6. Click **Set**. The Set Credential dialog box displays.
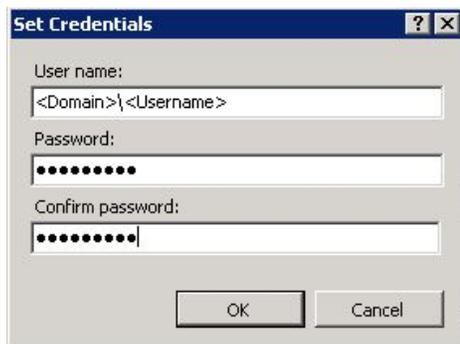
7. In the **Username** field, enter the domain and user name in the following format: **Domain\Username**, and click **OK**.

8. Launch Vision on the Web/Application server to ensure that the application launches correctly. If not, review the application event logs for an indication of the problem.

Configure Vision IIS to Use Windows Integrated Authentication

Do **not** make any modifications to the security settings for the VisionClient IIS Application. The Application represents the ClickOnce deployment and must remain using Anonymous Access.

To configure Vision IIS to use Windows Integrated Authentication, complete the following steps:

1. From within Internet Information Services, expand the web site where the Vision Application is installed.

2. Select the Vision application:
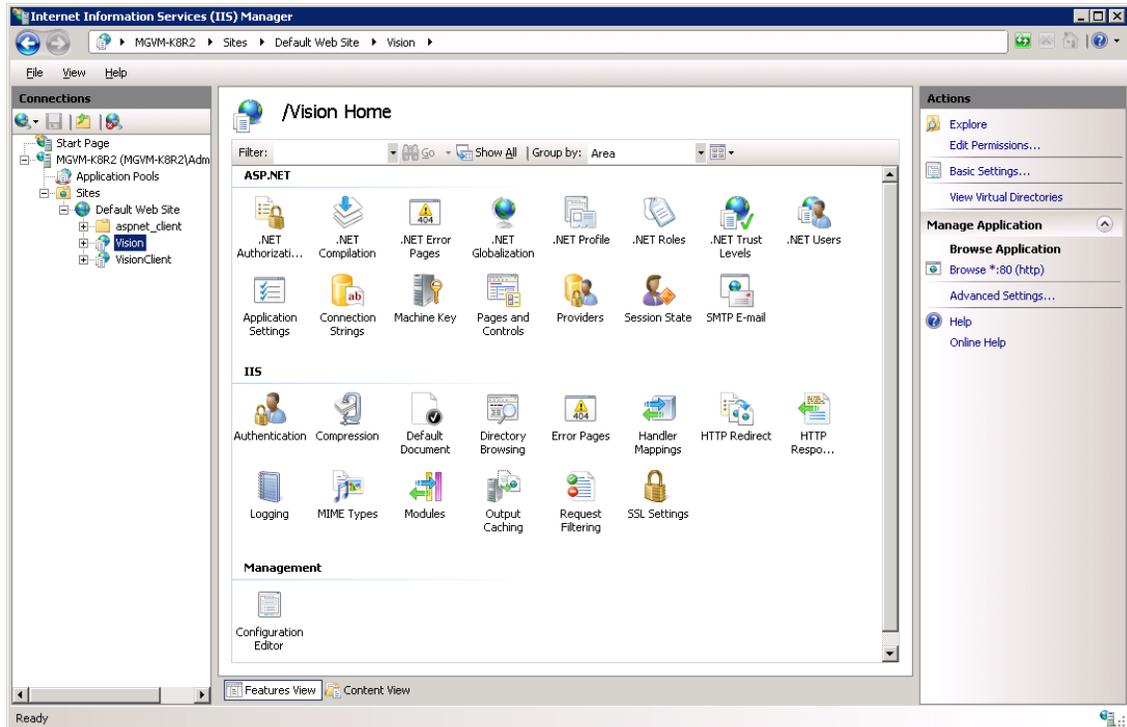
3. Double-click the **Authentication** icon under IIS.
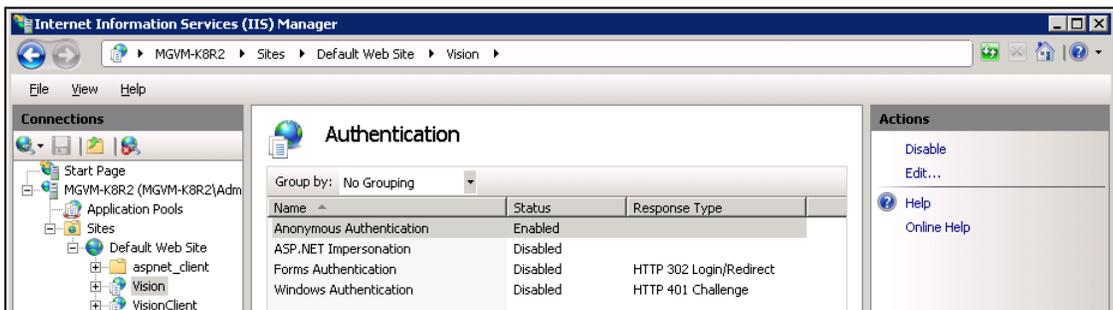
4. Select **Anonymous Authentication**, and click **Disable** on the Actions pane.

5. Select **Widows Authentication**, and click **Enable** on the Actions pane.
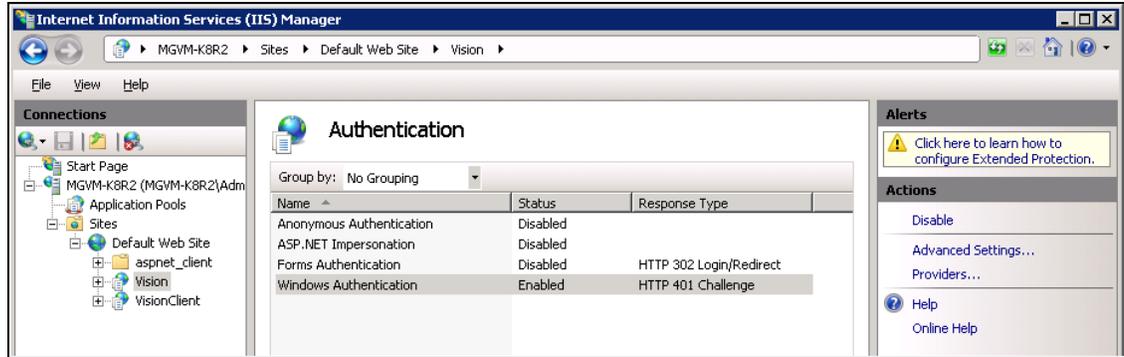
6. With Windows Authentication still selected, click **Advanced Settings**. Ensure that the **Enable Kernel-mode authentication** option is checked and click **Cancel**.
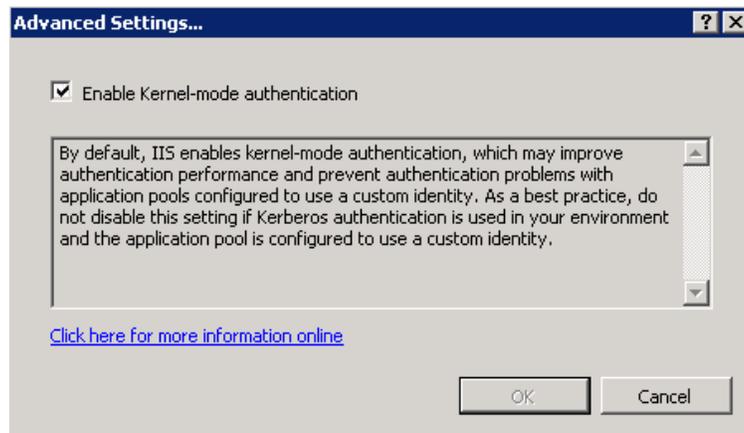
The default configuration is to have **Enable Kernel-mode authentication** selected. If you clear **Enable Kernel-mode authentication**, you must create a Service Principal Name, which is documented later in this section. The default setting is acceptable for application authentication; however, if you wish to use windows authentication for your database connection, you must complete the Configure Windows Integrated Authentication for Internet Users (and Non-Domain Workstations) procedure on page 43.

7. Launch the Vision application. On the login page you should see the **Windows Authentication** option.

The **Windows Authentication** option only displays if you have multiple databases configured in the weblink. If there is only one database, the user is automatically logged into Vision, and this screen does not display.
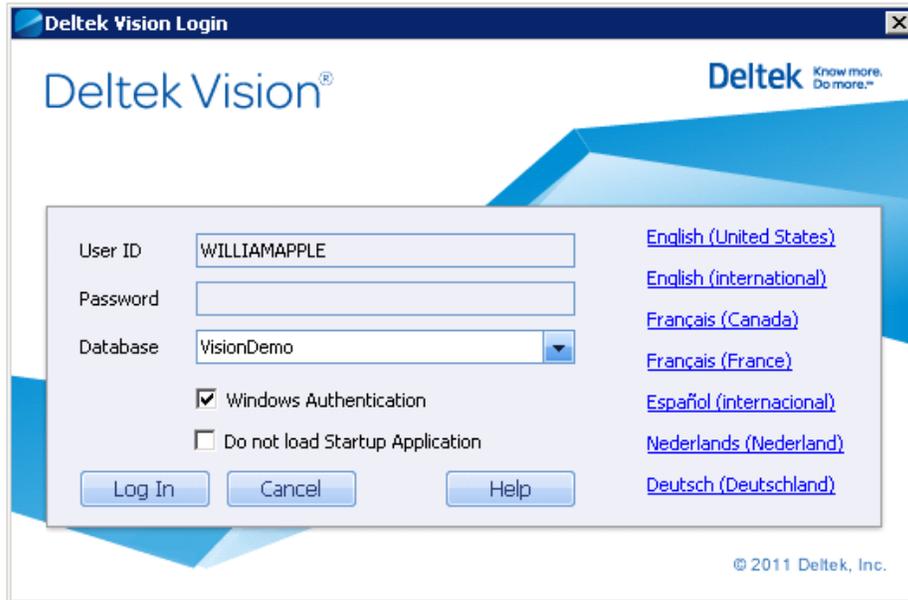
Configure Vision for Windows Integrated Authentication

After the servers are configured to support Windows Integrated Authentication, you must configure Vision application domain users with their domain logins.

Weblink has options on the System Settings Tab that may alleviate performance issues when using Windows Integrated Authentication. Details for these configuration settings are documented in the Weblink help. Test changes to these settings thoroughly before you implement the changes in a production environment.

To configure a domain login for Vision, complete the following steps:

1. Launch the Vision application and log in as a user with the appropriate security rights.

2. Click **Configuration » Security » Users and Passwords** and create a new user.
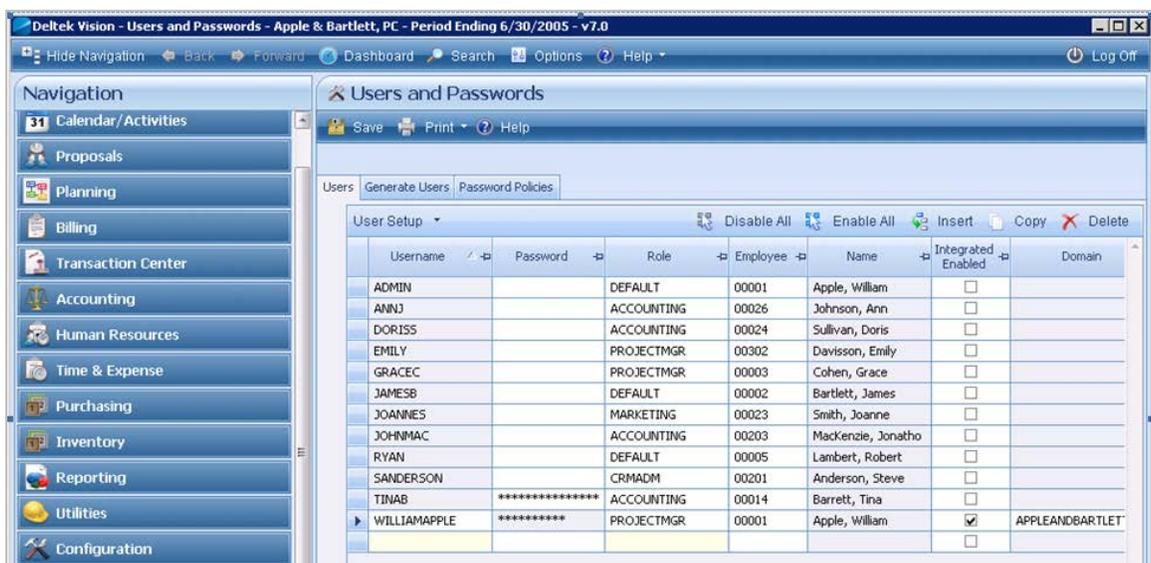
3. Enter the domain username for the user you want to create (for example, the login ID used to log in to the windows domain).

4. Complete the additional information as required for this user.

5. Select the **Integrated Enabled** option.

6. From the **Domain** drop-down list, select the domain for this user.

7. Save your changes.

8. When the user launches Vision, the login screen displays with the User ID populated with their username, and the **Windows Authentication** option selected.

    ▪ When configured for Windows Integrated Authentication, the option is not selected by default. After a login with **Windows Authentication** selected, the option is remembered for subsequent logins.

    ▪ If there is only one database defined in Weblink and the application is configured for Windows Integrated Authentication, the user is automatically logged into the application.
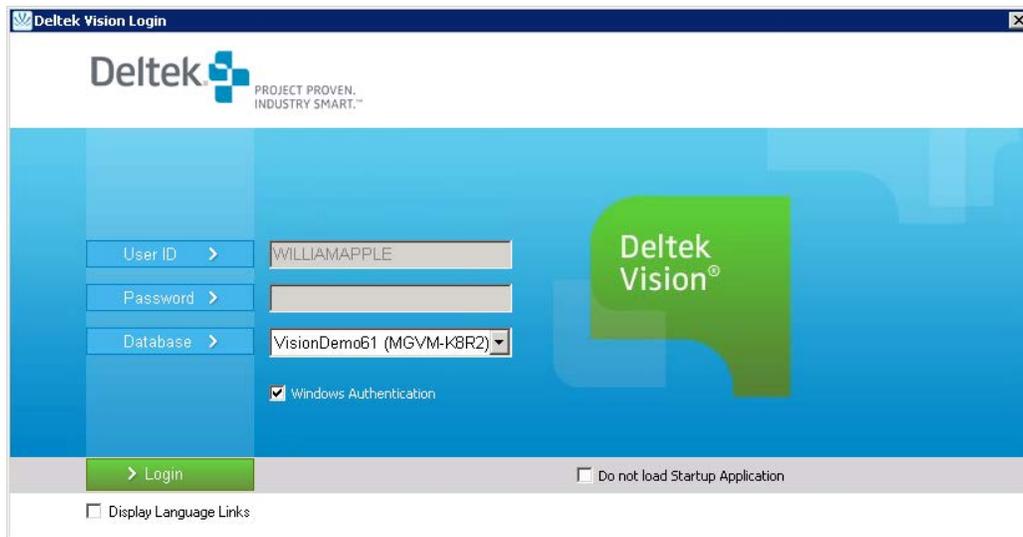
9. If configured for Windows Integrated Authentication, the user clicks **Log In** to complete the login process. If not, the user must clear the **Windows Authentication** option and enter a valid Vision username/password.

Configure Windows Integrated Authentication for Internet Users (and Non-Domain Workstations)

Domain users configured for Windows Integrated Authentication but accessing the application from a non-Domain workstation or via the Internet require a different authentication process.

To configure Integrated Authentication for Internet users, complete the following steps:

1. Launch the Vision application. The Windows Security prompt displays.

2. Enter the domain credentials by IIS.
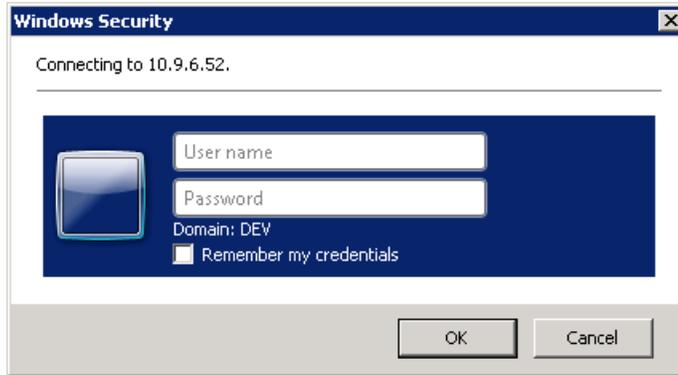
This is expected because they are not authenticated to the domain and IIS is configured for Windows Integrated Authentication so that only authenticated users can access without a challenge.

3. Click **OK**. The Windows Login Credentials dialog box displays.

4. Enter values in the **Username**, **Password**, and **Domain** fields. This is necessary because the client side Winforms application is not able to use the previous credentials requested by, and processed by, IIS.

Configure Windows Authentication for the Vision Database Connection

The first step to using Windows Integrated Authentication for the Vision database connection is to grant the domain user account the appropriate rights to the Vision database (and the Report Server and Session State databases, as needed).

To establish rights for SQL Server, complete the following steps:

1. Identify the domain user account that is being used as the Application Pool Identity in IIS. See step 3 in the **To configure the Application Pool Identity to be a domain account** procedure on page 37.

2. In SQL Server Enterprise Manager, create a SQL login for this domain user account:
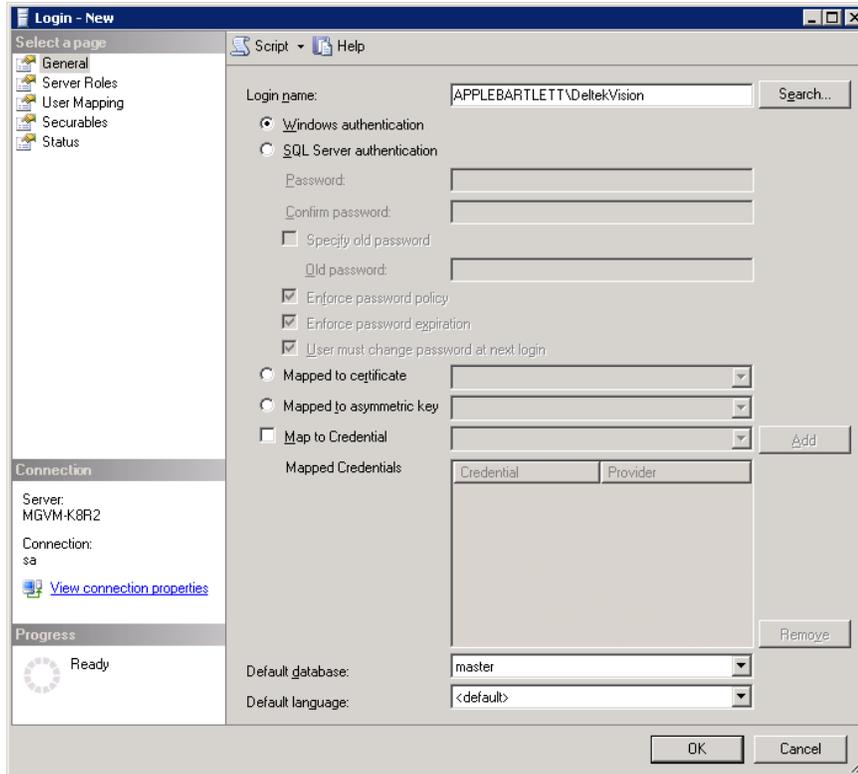
3. Click **User Mapping** and grant db_owner rights to the Vision database (and the Report Server and Session State databases):
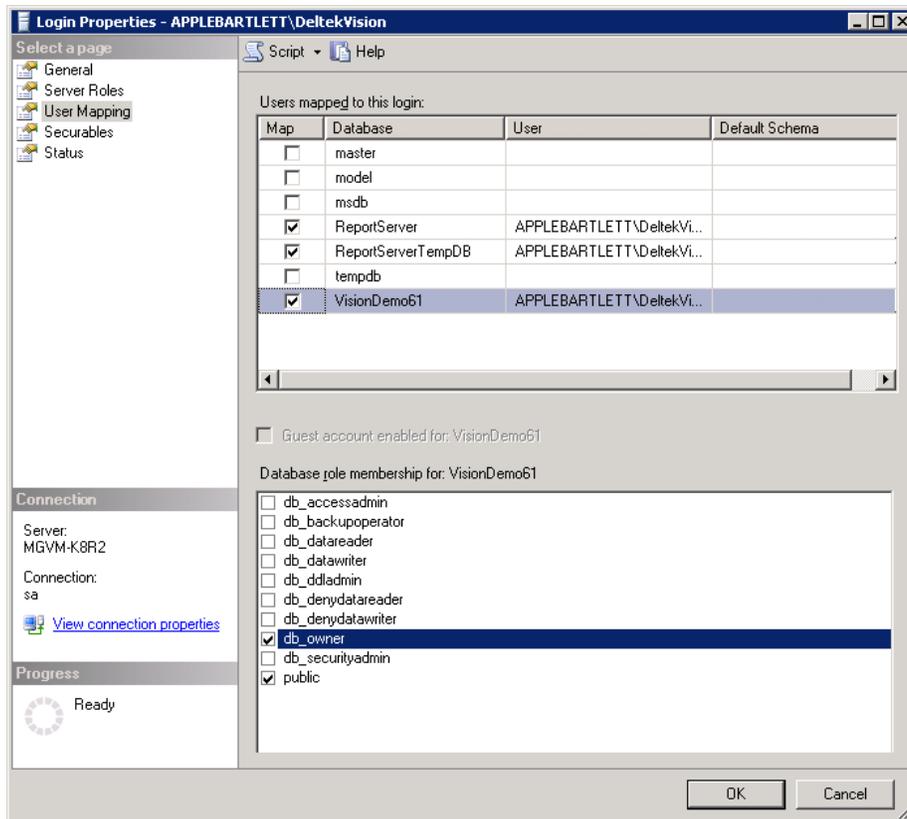
4. Modify Weblink to use Windows Integrated Authentication for the various database connections. Complete steps 5 through 10 to enable these settings.

5. Launch Weblink. Enter the Weblink password when prompted.
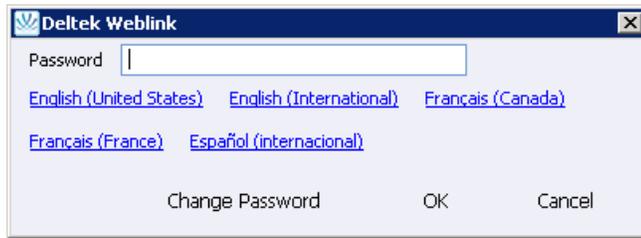
6. Click **OK**. The Weblink screen displays.
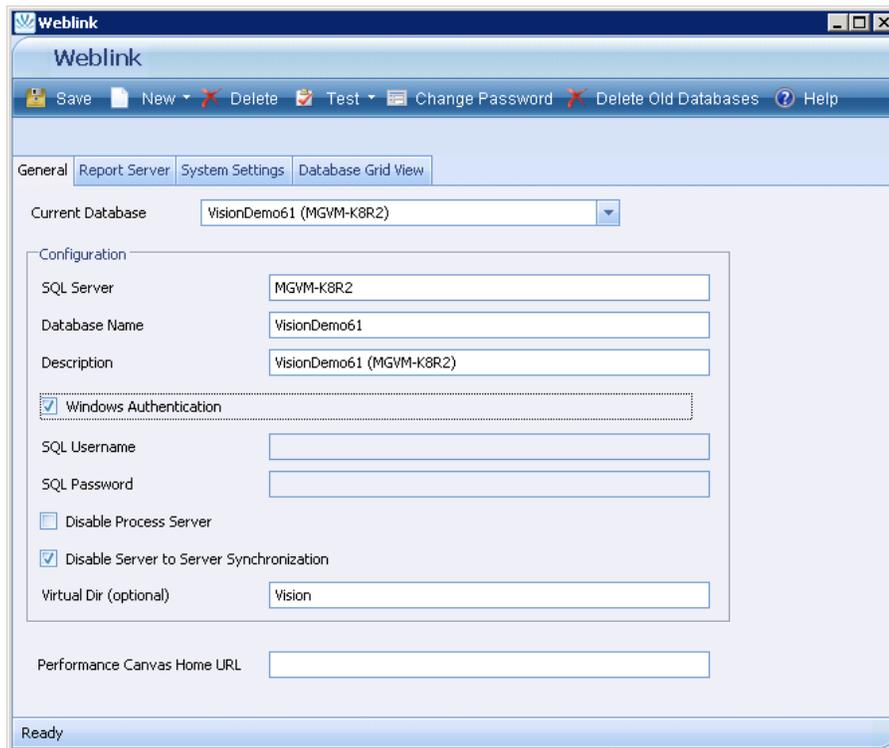
7. From the **Current Database** drop-down list, select the database to which you want to connect.

8. Select the **Windows Authentication** option to use the domain Application Pool Identity user account to connect to the database.

9. If necessary, you can also enable Windows Authentication for the Report Server database connection. In this situation, the account requiring access may differ from the one used for the IIS Application Pool Identity. The account that will be used to make this connection is shown on this page as the **Windows Username** under the Report Server URL. If this is a different account than the IIS Application Pool Identity, you must grant db_owner rights to the Report Server databases and then select the Windows Integrated option for the Report Server database authentication.
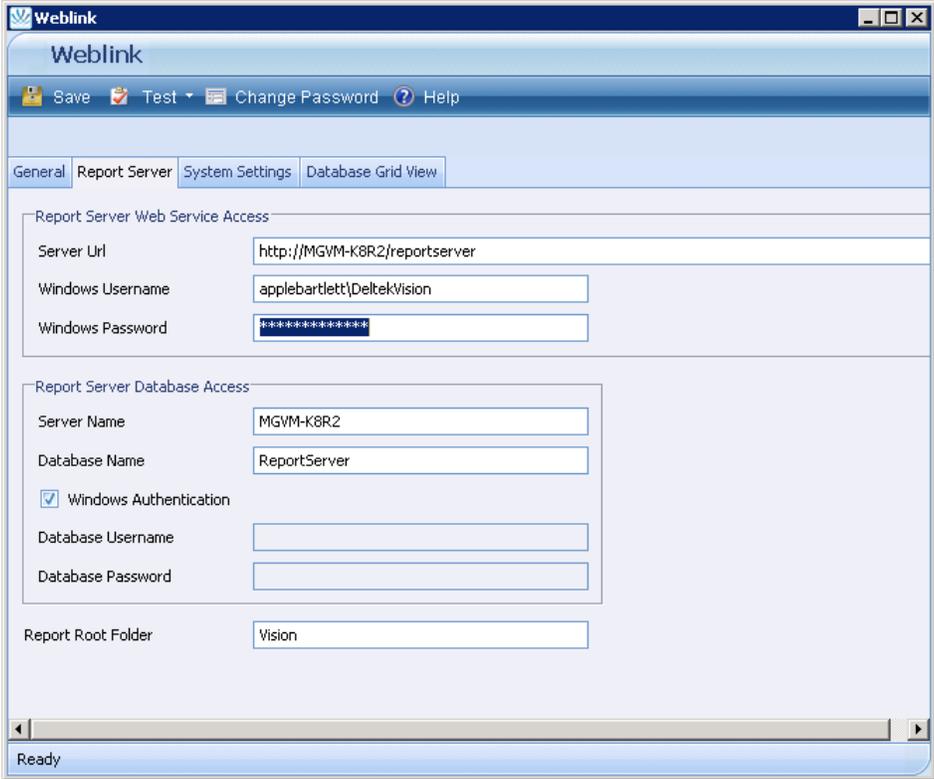
Optionally, if using SQL Server Session state, you can also enable Windows Authentication for that connection. This will use the IIS Application Pool Identity to make the database connection:
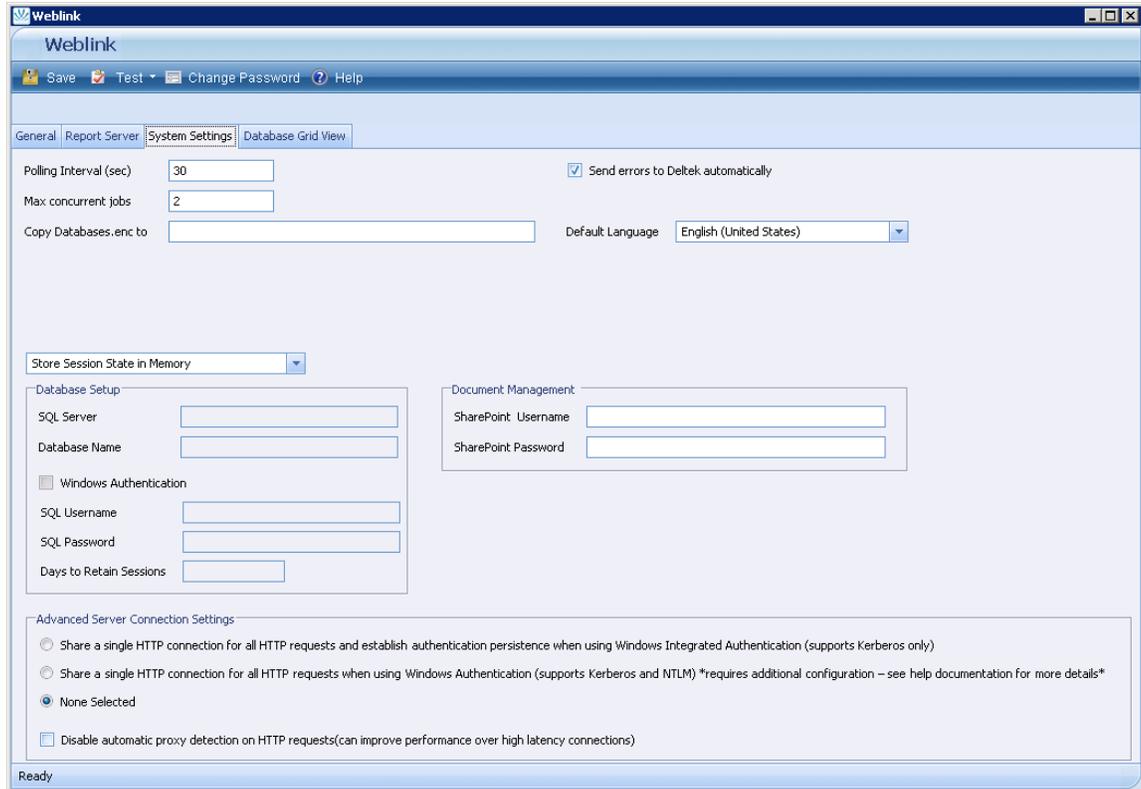
Weblink has options on the System Settings Tab that may alleviate performance issues when using integrated authentication. Details for these configuration settings are documented in the Weblink help. Changes to these settings should be thoroughly tested before implementing in a production environment.

10. On each of these tabs in Weblink, you must select the test button to test the connection to ensure that everything is configured properly:
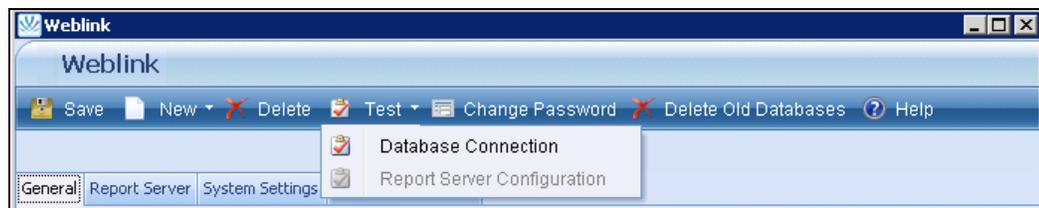
Configure a Service Principal Name

To disable Kernel Mode Authentication, you must create a Service Principal Name (SPN) for the domain user account that is the Application Pool Identity. The creation of the SPN requires domain administrative rights.

IIS 7.0 Kernel Mode Authentication

The default configuration of IIS 7.0/7.5 when using Windows Integrated Authentication is to use Kernel Mode Authentication. If you must disable Kernel Mode Authentication, follow the steps in this section to establish a Service Principal Name (SPN) for the Application Pool Identity.

In a default configuration of IIS 7.0/7.5, Kernel Mode Authentication is enabled.

To identify if Kernel Mode Authentication is enabled, complete the following steps.

1. Using an Administrator account, log on to Vision Web/application server domain.

2. Open Internet Information Services: **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager**.

3. Expand the server name, expand **Sites**, and select **Default Web Site** (or the site where Vision is installed).

4. Select the Vision virtual directory and then double-click **Authentication** in the Features view.

5. Select **Windows Authentication** and verify that the status is **Enabled** (Anonymous Access should be **Disabled**). If it is not, select **Enable** from the Actions menu.

6. With **Windows Authentication** still selected, click **Advanced settings** on the Action menu. The Advanced Settings dialog box displays:
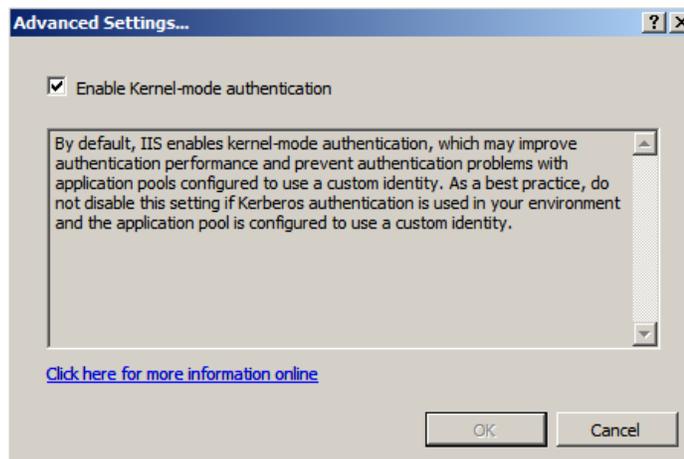
Kernel Mode Authentication Implementation

The default configuration works for the Vision Windows Integrated Authentication application and database connections.

To disable Kernel Mode Authentication, remove the **Enable Kernel Mode Authentication** selection under the Advanced Settings of the Windows Authentication feature for the Vision virtual directory. Disabling Kernel Mode Authentication requires that a Service Principal Name be established for the Application Pool Identity. The following section provides more information on SPNs.

Service Principal Names

Under the default configuration with Kernel Mode Authentication enabled, it is not necessary to create a Service Principal Name for the Application Pool Identity. The default SPNs created are sufficient.

If you do create an SPN for the Application Pool Identity, there will be a duplicate SPN issue that prevents Windows Integrated Security from authenticating anyone to the Web site.

When Kernel Mode Authentication is disabled, complete the following steps to create a Service Principal Name for the Application Pool Identity of the DeltekVisionAppPool.

Hybrid Deployment Model (HDM) – ClickOnce delivers about 15 files (enough to display the login page). After that, HDM takes over to deliver core application assemblies, hotfixes, language-specific satellite assemblies, and custom items.

> The setspn utility is installed by default on Windows Server 2008. You do not need to download and install it separately.

To create the Service Principal Name, complete the following steps:

1. Log in to the server with domain administrative rights and complete the following commands:

   - setspn –A http/<name of server> ApplicationPoolIdentity (Domain\Username)

   - setspn –A http/<fully qualified name of server> ApplicationPoolIdentity (Domain\Username)

   or, if appropriate, the DNS name of the server:

   - setspn –A http/<DNS name of server> ApplicationPoolIdentity (Domain\Username)

   For example:

> Refer to the following related Microsoft Knowledge Base article if you need additional details:
>
> http://support.microsoft.com/?id=871179

Chapter 6: Configuring Database Session State for Vision

Session state information is typically stored in memory on the web server in the IIS Application Pool process serving the application (w3wp.exe). Database session state is normally not a consideration unless you will be load balancing multiple front-end Vision Web/Application servers and you would like to isolate your user's session information from a failure or error on one web server where their session information may be lost.

Configuring Deltek Vision to store session state information in a database is a process configured using the Weblink utility. You should also be aware that Deltek has written our own session state model and does not rely on ASP.NET session state.

Create the Session State Database (Optional)

Session state information is stored in a database table which is automatically configured by Weblink if you will be creating it in the Vision database. However, if you would like this database table stored in a database other than your Vision database, you must create a separate database and login for this purpose.

Configure Vision for Database Session State

Important! Make sure that no one is logged in to Vision before making this change. Changing the session state invalidates all active user sessions.

To configure Vision for database session state, complete the following steps on the Web/Application Server:

1. Launch and log in to the Vision Weblink utility. (The shortcut for Weblink is under the Deltek Vision program group on the Start Menu).

2. Click the System Settings Tab.

3. In the drop-down field, change **Store Session State in Memory** to **Store Session State in SQL Server**. The following message displays:
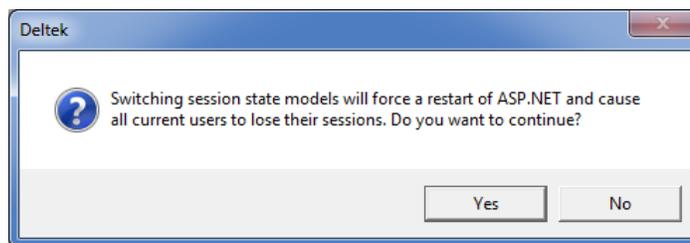
4. Click **Yes**. The Database Setup dialog box displays.

5. In the **SQL Server f**ield, enter the name of the database Server where the session state database (or <Product> exists.

6. In the **Database Name** field, enter the name of the session state database.

7. If you plan to use Windows Authentication for the database connection, select the **Windows Authentication** check box. If you do so, the SQL Username / SQL Password are disabled (shaded).

> See "Chapter 5: Integrated Security Configuration for Deltek Vision" for details on Windows authentication.

2. In the **SQL username** field, enter the SQL Login ID with rights to that database.

3. In the **SQL password** field, enter the password for the SQL Login ID that you entered in the previous step.

4. In the **Days to retain sessions** field, enter the number of days that you want to retain sessions.

5. Click **Test Database Connection** to validate the connection information entered.

6. Click **Apply** to save your changes.

   A message displays that prompts you to configure this database to store session state information.

   Click **Yes** to create a table in the database called **SessionState**. A message displays to tell you that Weblink has successfully configured the Server (database) to store Vision session state.

Verifying the Configuration

To verify that session state is correctly being stored in the database for Vision, complete the following steps:

1. Access your database server via a query utility

2. Log in to Vision.

3. Run the following query in Query Analyzer to verify that a row has been added to the table. There will be one row for every user logged in.

   Sessions will remain in the table for the number of days specified in the **Number of Days to retain Sessions** field on the Database Setup dialog box.

Use <Session State Database>
Go
Select * from SessionState
Go

Chapter 7: Securing Your Deltek Vision Deployment

The default installation of Deltek Vision creates a variety of user accounts on the various Vision physical tiers (Database, Web/Application, Report and Process Server). These user accounts include local Microsoft Windows user accounts and SQL Server Login IDs (for both Windows and Mixed Mode authentication).

Deltek has created a utility called the Deltek Vision Resource Kit. This utility is installed on each tier, and provides you with quick access to technical administrative functions commonly used to support your Deltek Vision installation. Among its many functions is the ability to create or change a variety of user account information on the various tiers. You can use the Resource Kit to make most of these security account customizations. Where the Resource Kit is not the appropriate tool, this document provides the necessary manual instructions.

Most of these changes require Administrative rights on your servers, so be sure to log in with the proper account. Do **not** log in using the DeltekVision local account, because you will be deleting or disabling this account on all Vision servers.

This document guides you through making the necessary changes on the various physical tiers. It is designed to instruct you on changing all of these accounts so that they are unique to your firm and do not include any Deltek default user accounts or passwords.

If You Have Deployed Several Logical Tiers with the Same Windows Account

You may have deployed several logical tiers all using the same Windows account and all located on the same physical server. For example, in a single-server installation, the DeltekVision local Windows account is used as:

- The Application Pool Identity
- The Reporting Services access account
- The Process Server service account *and*
- A Windows SQL Login account

You may not need to delete or disable the accounts as many times as indicated in these instructions, if the account is serving multiple roles.

The Web / Application Tier

The Web/Application tier installation creates a local Windows user account named **DeltekVision**. This account is also added to the Local Administrators group and the IIS_IUSRS (or IIS_WPG in IIS 6.0) group and is configured as the Application Pool Identity of the DeltekVisionAppPool.

To secure the Web/Application tier and customize the Application Pool Identity, complete the following steps:

1. Change the Application Pool Identity.

2. Select one of the following actions:

   - If you are using a Windows domain, create a Domain user account, or use an existing one. Then add this user to the Local Administrators group and IIS_IUSRS (or IIS_WPG) group on the Web/Application server.

   - If you are not using a Windows Domain, you need to create a new local Windows user account and add that user to the same Windows groups. Continue with step 3.

3. Click **Start » All Programs » Deltek Vision » Deltek Vision Resource Kit** to launch the Deltek Vision Resource Kit on the Web/Application server.

   On Windows Server 2008, you need to right-click the short-cut and select **Run as Administrator** unless Windows User Account Control (UAC) is disabled.

4. Click the Web/Application Server tab and enter the appropriate username, password, and domain information in the **DeltekVisionAppPool Account** section, shown below.

   - If you are using a local Windows user account, the Domain is the machine name of the Web/Application server.

   - If you are not using a local Windows user account, enter the Domain credentials of the user you created above, in the **Username** and **Password** fields and then select your domain from the **Domain** drop-down list.

5. Click the **Set DeltekVisionAppPool Identity** button.

   This process may take several minutes. After this process is complete, if you are using Windows Integrated Authentication for the SQL Server connection, you need to add the Domain user to the Local User (not Administrators) group on the SQL server and grant this new Domain user dbo (database owner) rights to your Vision database(s).

6. Change the Process Server service account. See "Process Server Tier," on page 61, for the procedure. By default, the Process Server service is installed on every Web/Application server, as well as on any server installed as a Dedicated Process Server.

7. Click **Computer Management » Local Users and Groups » Users** and then delete or disable the local Deltek Vision Windows user account on the Web/Application server.
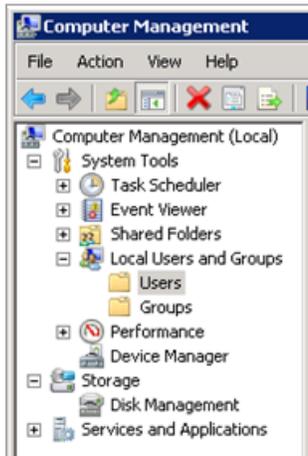
Database Tier

The Database tier installation creates a local Windows user account on the SQL Server named **DeltekVision** as well as a SQL Server Login ID, also named **DeltekVision**.

SQL Server has two modes of authentication:

- Windows Integrated
- Mixed Mode

If you are unsure which mode of authentication you are using, complete the following steps:

1. Click **Start » All Programs » Deltek Vision » Weblink** to launch the Deltek Vision Weblink utility on the Web/Application server.

2. If you have not set a password for Weblink, click the Change Weblink Password tab and enter a unique password. The Change Password tab is visible only when accessing Weblink via localhost on the Web/Application server.

3. Log in to Weblink and select your database from the **Current Database** drop-down list.

4. Review the information on the General tab to identify your method of SQL authentication:

- If the **Windows Authentication** check box is selected, then you are using Windows Integrated Authentication.

- If the **Windows Authentication** check box is cleared and a SQL username and password is filled in, then you are using SQL Server or Mixed Mode authentication.

Windows Integrated Authentication

The local Windows user account is created on the Database tier for those implementations that will be using Windows Integrated Authentication for the SQL Server connection.

> See Chapter 5 for detailed information on configuring Windows Integrated Security for the Web/Application and Database connections.

If you are using Windows Integrated Authentication for the SQL Server connection, you need to update the database tier with the new user account that you've created for the Vision Application Pool Identity in the Web/Application Tier section.

To update the database tier with the new user account, complete the following steps:

1. Select one of the following options:

    ▪   If you are using a Domain user account for the IIS Application Pool Identity, add this Domain user to the Local Users (not Administrators) group on the SQL Server.

    ▪   If you are using a Local user account as the IIS Application Pool Identity, use the **Computer Management** utility from Administrative Tools to create a local user on the database server with the **same username and password** as you used on the Web/Application server.

    Administrative rights to your database server are not necessary for this functionality.

2. Create a new Windows login in SQL Server for the Domain or Local user account that is being used for the IIS Application Pool Identity. Create the new SQL Login using SQL Server Management Studio from the Security->Logins folder, as shown in the screen below.
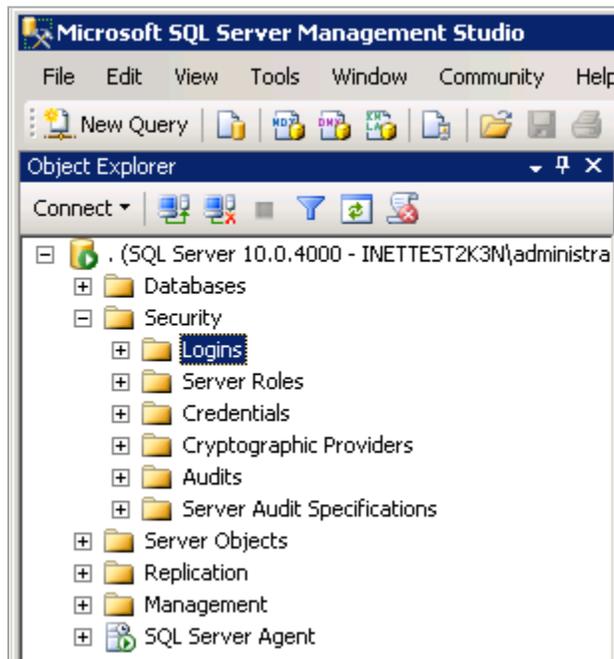
> The creation of Windows Login accounts in SQL Server has not been added to the functionality of the Resource Kit as of this publication.

3. Grant this new Windows login dbo (database owner) rights to your Vision database(s).

4. On the Web/Application server, launch the Weblink utility.

5. Log in to Weblink and select your database from the **Current Database** drop-down list.

6. If it is not already selected, select the **Windows Authentication** check box.

7. To ensure that the database connection information was updated correctly, click the **Test Database Connection** button to validate the connection.
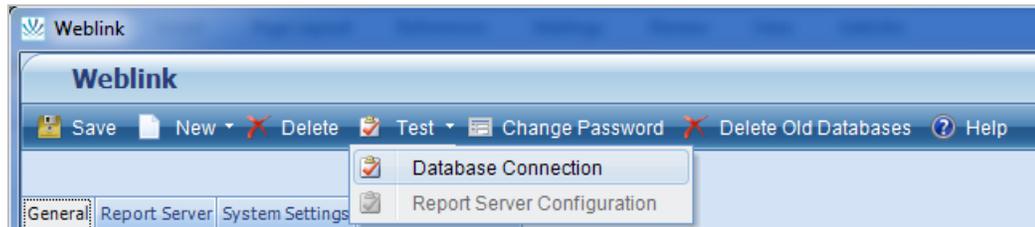
8. Use the **Computer Management** utility under Administrative Tools to delete or disable the local DeltekVision Windows user account on the Database server.

9. Use SQL Server Management Studio to delete or disable the DeltekVision Windows Login ID from within SQL Server. Deleting the Windows User Account does not remove it from SQL Server. However, disabling it disables the account in SQL Server.

Mixed Mode Authentication

If you are using Mixed Mode Authentication for the SQL Server database connection, you need to create a unique SQL Server login.

To create the SQL Server login, complete the following steps:

1. If you haven't already done so, secure the **sa** account with a unique password using SQL Server Management Studio from the Security - Logins folder.

2. Create a unique SQL Server login ID and password using either the Resource Kit or SQL Server Management Studio.

3. Grant the new login dbo (database owner) rights to your Vision database(s) and, if appropriate, the Reporting Services databases (ReportServer and ReportServerTempDB).

    Although the Resource Kit updates the General tab for your Vision database, it currently does not update the Report Server database user ID/password on the Report Server tab of Weblink. You need to perform this update manually.

4. If you want to use a different account for the report server database access, create a second SQL login in SQL Server Management Studio and manually update the Report Server tab in Weblink with the new connection information. Be sure to test the connection before saving your changes.

5. If you are using the Resource Kit, follow the steps below:

    On Windows Server 2008, right-click the shortcut and select **Run as Administrator** unless Windows User Account Control (UAC) is disabled.

    a. Launch the Resource Kit on the Web/Application server (**not** the Database server, because we also need to update Weblink during this process and the Resource Kit on the web/application server can accomplish both jobs).

    b. Click the Database tab. You will be prompted to log in to your SQL server.

c.   Enter the following information:

- The name of the SQL Server, if it is not pre-populated

- The username **sa**

- The correct password.

- Select the **Windows Authentication** check box if the account you are logged in to has rights to both the Vision Web/Application and Database servers.

d.   Click the General tab and enter a unique SQL login ID and password in the **Create SQL Account for Deltek Vision** area.

e.   Select the database(s) to which this account should have dbo rights.

f.   Click the **Create SQL Logon** button. This process creates a new SQL Login ID on the database server and grants that login database owner (dbo) rights to the databases selected.

6.   After the new SQL login has been created, you must associate that new login with Weblink so that the new account is used:

a.   Using the Resource Kit, on the **Database, General tab, Associate Logins with Databases.enc** section, select the new SQL login ID you just created from the **Username** drop-down in the **SQL Logon** field.

b.   Enter the unique password for that login and select the check box for the database(s) to be updated.

c.   Click the **Associate SQL Logon** button.

7.   To verify that Weblink has been updated properly, click the General Tab in the Resource Kit and then click the link to launch Weblink. Although the Resource Kit updates the General tab for your Vision database, it currently does not update the Report Server database user ID/password on the Report Server tab of Weblink. You need to perform this update manually.

8.   Log in to Weblink and select your database from the **Current Database** drop-down list.

9.   To ensure that the database connection information was updated correctly, click the **Test Database Connection** button to validate the connection.

10. Update the Report Server tab with the new connection information for the Report Server databases.

11. Use SQL Server Management Studio to delete or disable the DeltekVision SQL login ID that the installation created on the Database server.

Report Tier

The Report tier installation creates a local Windows user account on the Report Server (SQL Reporting Services server) named **DeltekVision**. This Windows user account is also granted System Administrator and Content Manager Rights in SQL Reporting Services.

You already accomplished customization of the account granted access to the Report Server databases by completing the steps for database tier procedure.

You cannot use the Resource Kit to customize the Report Server.

To secure the Report tier and customize the Report tier account, complete the following steps:

1. Select one of the following actions:

   - If you have a Windows Domain, create or have a Domain user account created, and use the **Computer Management** utility under Administrative Tools to add this user to the Local Administrators group on the Report server. Select **Computer Management**, **Local Users and Groups**, **Administrators**, and then add the new Windows account.

   - If you are not using a Windows Domain, you need to create a new local Windows user account and add that user to the Local Administrators group.

   The next step is to grant this new account the necessary rights in Reporting Services using Report Manager.

2. Open Report Manager using **http://<report_server>/reportsError! Hyperlink reference not valid.**, replacing <report_server> with the name of your Report Server.

   You must already have been granted rights to the Report Server in order to access Report Manager. You may also need to launch Internet Explorer using the **Run as Administrator** option.

   The Report Manager web application displays:
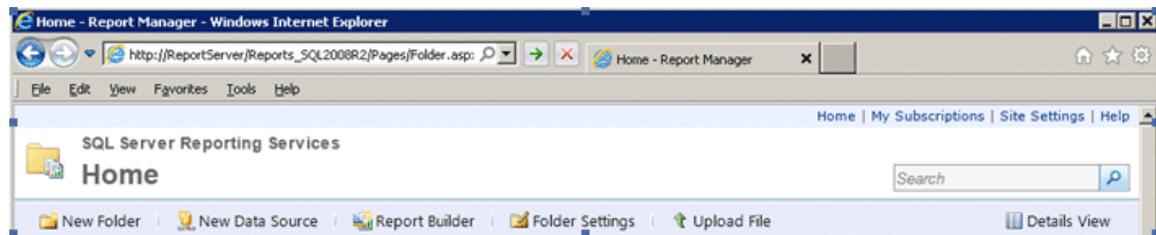
3. Click the **Site Settings** link in the upper right corner and add the new account to the Administrators role.

4. Delete the **DeltekVision** account from this role.

5. Click the Properties tab in SQL 2008 or the **Folder Settings** button in SQL 2008 R2 and SQL 2012.

6. Add your new account to the Content Manager Role.

7. Delete the **DeltekVision** account from that role.

8. Use the **Computer Management** utility from Administrative Tools to delete or disable the local DeltekVision Windows user account on the Report Server.

Process Server Tier

The Process Server tier installation creates a local Windows user account on the Process Server named **DeltekVision**.

By default, the Process Server service is installed on every Web/Application server, as well as on any server installed as a Dedicated Process Server. Therefore, you should perform the following steps on every Web/Application server as well as on every dedicated Process Server where the process server service will be run.

In this procedure, you will change the Process Server Service Account (Windows account on the Process Server tier).

To secure the Process Server tier and customize the Process Server service, complete the following steps:

1. Select one of the following actions:

   - If you have a Windows Domain, create or have a Domain user account created. Use the **Computer Management** utility under Administrative Tools to add this user to the Local Administrators group on the Report server. Select **Computer Management**, **Local Users and Groups**, **Administrators**, and then add the new Windows account.

   - If you are not using a Windows Domain, you need to create a new local Windows user account and add that user to the Local Administrators group.

2. Launch the Deltek Vision Resource Kit on the Process Server if you are changing the service account on a dedicated Process Server. Otherwise, launch the Resource Kit on the Web/Application Server.

3. Click **Start » All Programs » Deltek Vision » Deltek Vision Resource Kit**.

4. Click the Process Server tab and enter the user information in the **Service Account** section.

5. Select one of the following actions:

   - If you are using a local account, enter a unique local Windows username and password and select the **Create Local Account if it does not exist** check box.

   - If you are not using a local account, enter the Domain credentials that you created earlier in the **Username** and **Password** fields, and select your domain from the **Domain** drop-down list.

6. Click the **Set Process Server Identity** button. This process will take several minutes. When it is complete, you can see that the new account is now running the Deltek Process Server service.

7. To see this, click **Start » Control Panel » Administrative Tools » Services** and locate the Deltek Vision Process Server service. Make sure that the **Log On As** column reflects the new user information that you entered above.

> If for some reason the Resource Kit does not restart the service, it may be because the new service account was not granted the **Log on as a Service** Local Security Policy right.
>
> To correct this, click **Start » Control Panel » Administrative Tools » Services**. Then double-click the Deltek Vision Process Server service, click the Log On tab, and enter and confirm the password for the new user at whom the service is running. You should see a message indicating that the user was granted this right and you can start the service.

8. Use the **Computer Management** utility from Administrative Tools to delete or disable the local DeltekVision Windows user account on the Report server.

If You Have Multiple Servers

Your Deltek Vision installation should now be secured with customized username and password information unique to your firm on every tier. If you have multiple Web/Application, Report, or Process Servers, make sure that you run through the above steps on each physical server using the same user account information you used on the first server for that tier.

Chapter 8: Configuring SQL Server Resource Governor to Manage Vision Workloads

Prerequisites: SQL Server Enterprise Edition

With Vision, transaction processing and report processing can and will occur simultaneously on the same physical database in SQL Server. There may be times when either transaction or report processing take up the majority of the resources (such as CPU or memory) of the SQL Server, thereby adversely impacting users.

For example, assume a user needs to run a complex report. The report must be run separately for each of the firm's offices. To save time, the user submits all of the reports to run simultaneously, unaware of the potential impact to the system. As a result of the complex query processing of the reports, the CPU on the SQL Server is effectively monopolized by running these reports. As a result, all other users experience dramatic slowdowns and timeouts using the software. The only solutions to the problem are to allow the reports to complete (a process that could take hours) or to stop the SQL Server query processes that are executing the report queries.

SQL Server (Enterprise Edition only) includes a feature called the **Resource Governor**, which can help to alleviate these problems by ensuring that these disparate workloads don't monopolize resources on the database server. This chapter provides the steps to configure the Resource Governor and provides suggestions on how to classify these workloads into separate resource pools.

Important! This document was written using test results from SQL Server 2008. The Resource Governor feature is not routinely tested or directly supported by Deltek, but is presented as a possible solution for workload-based performance issues. The Resource Governor's features and functions may or may not work with future versions of SQL Server. Please refer to the available Microsoft documentation for additional configuration options and changes in functionality based on your specific version of SQL Server: http://technet.microsoft.com/en-us/library/bb933866(v=sql.100).aspx.

A SQL Server Classifier Function is used to identify each workload, telling SQL Server how to assign each connection to a resource pool. You could use a variety of system functions to "classify" each connection. However, since we know that all connections for Vision transaction processing are coming from the web/application server and that all report processing is coming from the report server, we can use the 'client_net_address' from the CONNECTIONPROPERTY to classify each connection. The IP addresses for each of the serversused in this classification assume that the Application Server and the Reporting Server are separate servers each with its own unique IP address.

Use the SQL Statements below to configure the Resource Governor, replacing the information that is highlighted in yellow as appropriate.

```
--Connect to the master database
USE MASTER
GO
--Enable Resource Governor. To disable execute, ALTER RESOURCE GOVERNOR DISABLE
ALTER RESOURCE GOVERNOR RECONFIGURE
GO
--Create Resource Pools for Reporting (SSRS) and Transactions (Vision)
CREATE RESOURCE POOL ReportingPool
GO
CREATE RESOURCE POOL TransactionPool
GO
--Create Workload Groups for Reporting (SSRS) and Transactions (Vision)
CREATE WORKLOAD GROUP ReportingGroup
USING ReportingPool
GO
CREATE WORKLOAD GROUP TransactionGroup
USING TransactionPool
GO
--Create the Classifier Function which is used to "Classify" the requests.
--This function determines which pool to place the request in based on the IP
address of the server.
CREATE FUNCTION classifier()
RETURNS SYSNAME with SCHEMABINDING
BEGIN
        DECLARE @retval SYSNAME
        IF ConnectionProperty('client_net_address') = '<WebApp_IP>'
                SET @retval = 'TransactionGroup'
        ELSE IF ConnectionProperty('client_net_address') = '<Report_IP>'
                SET @retval = 'ReportingGroup'
        RETURN @retval
END
GO
--Set the classifying function for use with the Resource Governor
ALTER RESOURCE GOVERNOR WITH (CLASSIFIER_FUNCTION=dbo.classifier)
GO
ALTER RESOURCE GOVERNOR RECONFIGURE
GO
--Set CPU limits for each Resource Pool. NOTE: These are not "hard" limits.
ALTER RESOURCE POOL TransactionPool
WITH (MIN_CPU_PERCENT=50, MAX_CPU_PERCENT=90)
GO
ALTER RESOURCE POOL ReportingPool
WITH (MAX_CPU_PERCENT=50)
GO
ALTER RESOURCE GOVERNOR RECONFIGURE
GO
```

After you run the above statements successfully, you can see the following configuration when you view the properties of the Resource Governor:
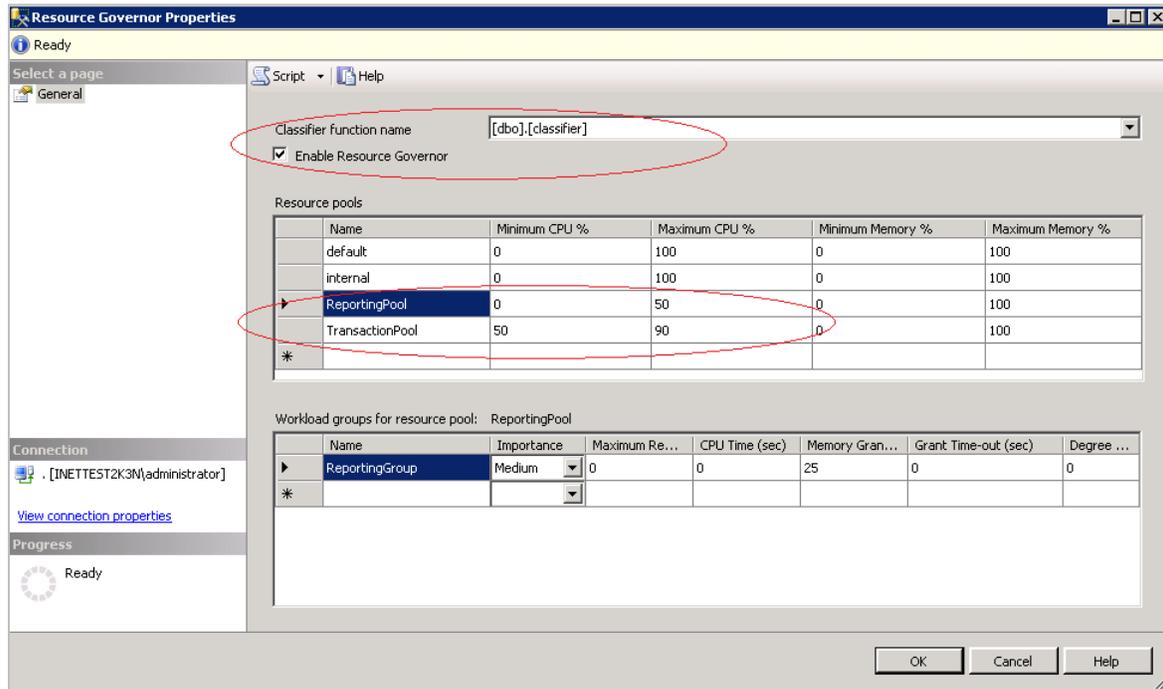
In addition, you can modify the percentages for each resource pool as well as configuring additional parameters including memory and the maximum number of requests. Deltek recommends that you configure and test the Resource Governor in a test environment to ensure the configuration works as anticipated. To test this, execute the following query by installing the SQL Server tools on the Application and Report server. The query must be executed from the IP addresses of the servers associated with the classifer function or the requests will not be classified correctly.

You can Install SQLCMD for your platform from the following link:

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8824

> The SQL Native Client software is a pre-requisite component as is Windows Installer 4.5.

```
-- Here is a query that can be used to test (NOTE: osql doesn't seem to provide
necessary throughput)
SET NOCOUNT ON
DECLARE @i INT = 0
DECLARE @s NVARCHAR(500)
WHILE @i < 100000000
BEGIN
        SELECT @s = SUSER_NAME() + DB_NAME() + @@VERSION
        SET @i +=1
END
GO
```

Before executing the script, configure Performance Monitor on the database server so that you can review the results of executing the query. The specific counters to add are shown below:
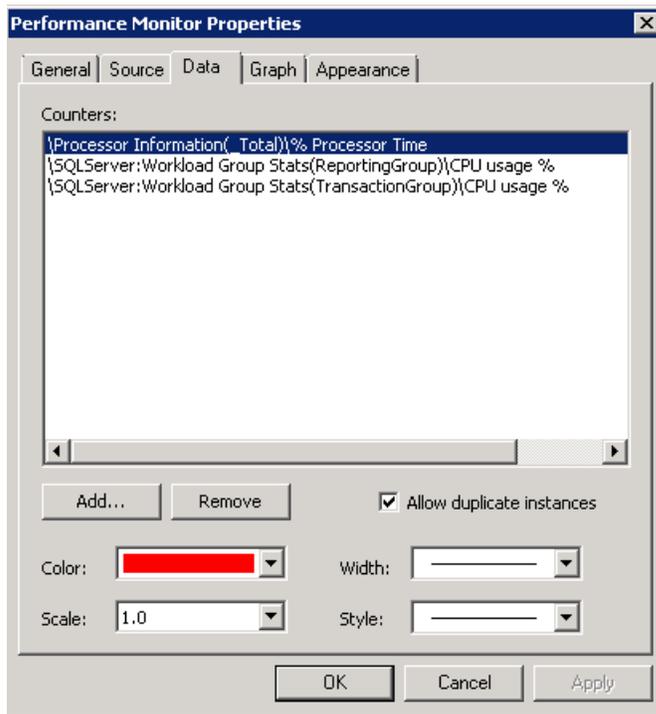
You will want to monitor total CPU usage as well as the CPU usage for each Workload Group that you have established. The results are also best viewed as a Histogram bar graph, which you can select by clicking the Graph tab above and changing from the default of a line graph.

In order to execute the script above, logon to the Application server and open a command prompt to the location of SQLCMD and make a connection to your SQL Server:
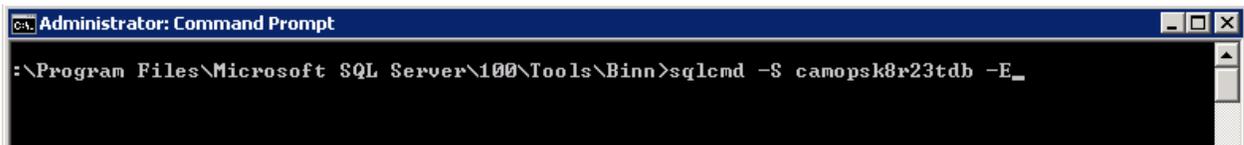
The –S switch specifies the name of the SQL Server machine and the –E will use a Trusted Connection using the Windows credentials you are currently logged on as. You can also specify a sql login id and password for the connection.

After the connection is made, paste the script above into the command prompt window:
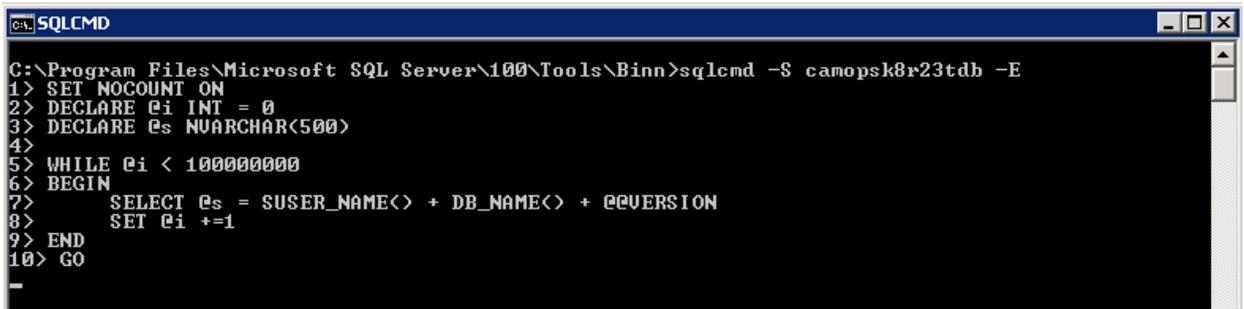
Executing this from the Application server will result in the following in Performance Monitor on the SQL Server:
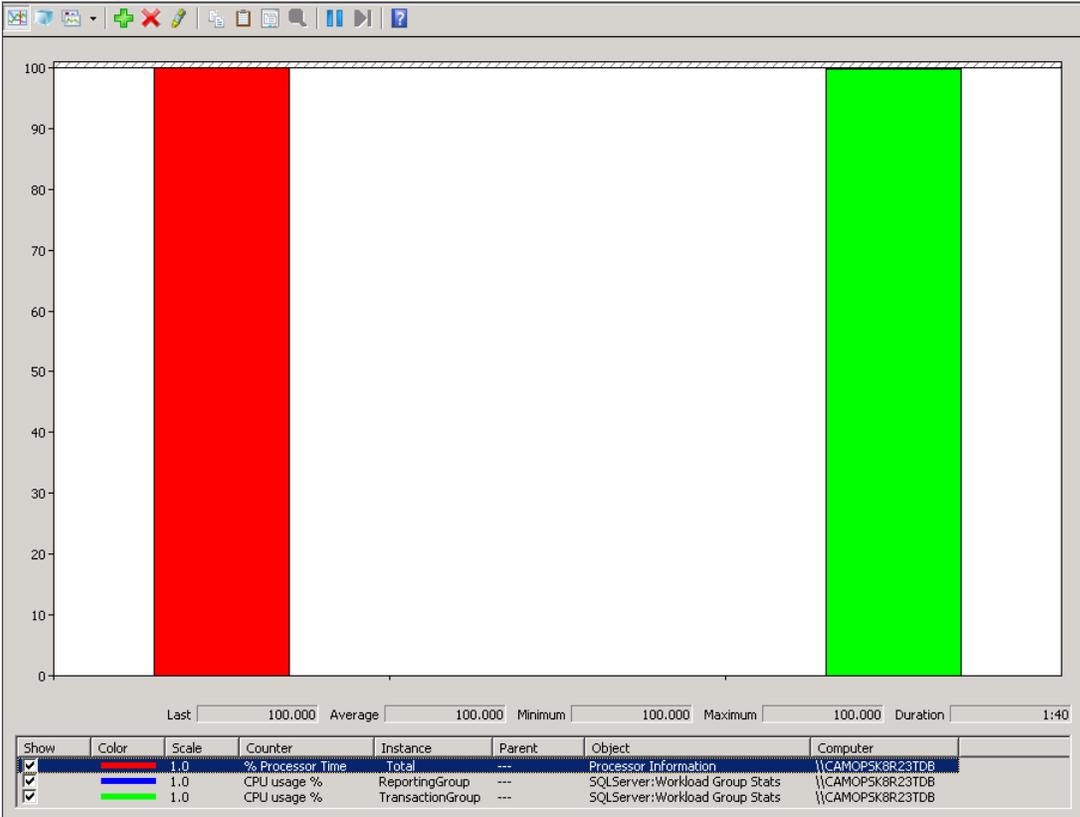
Note that the Transaction Group is allowed to access all of the available CPU as there are currently no connections from the report server.

Next, on the Application server use CTRL-C to break out of running the script. The CPU usage should drop to zero.

Log on to the Report server, open a command prompt window to SQLCMD, connect to the SQL Server and execute the same test script. The results you will see are shown below:
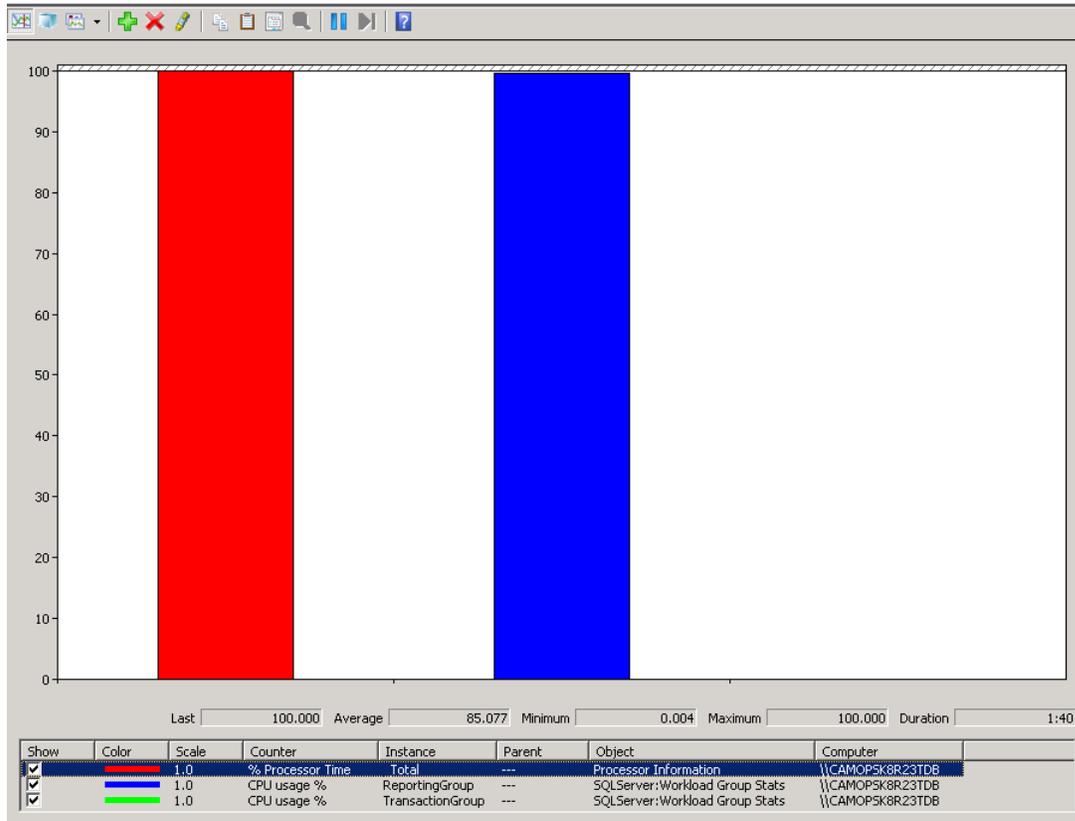
You might have expected that the Reporting Group would only be able to access 50% of the available CPU. However, if there is less than 50% CPU usage being used by the Transaction Group, the Reporting Group can use more, up to 100% of the availble CPU to finish it's work quicker.

Next, let's see what happens when we execute the scripts from both servers at the same time. Leave the script running on the Report server and back on the Application server, paste the script back into the command prompt window. The result will be similar to below, where both the Transaction Group and the Reporting Group are effectively splitting the available CPU between them.
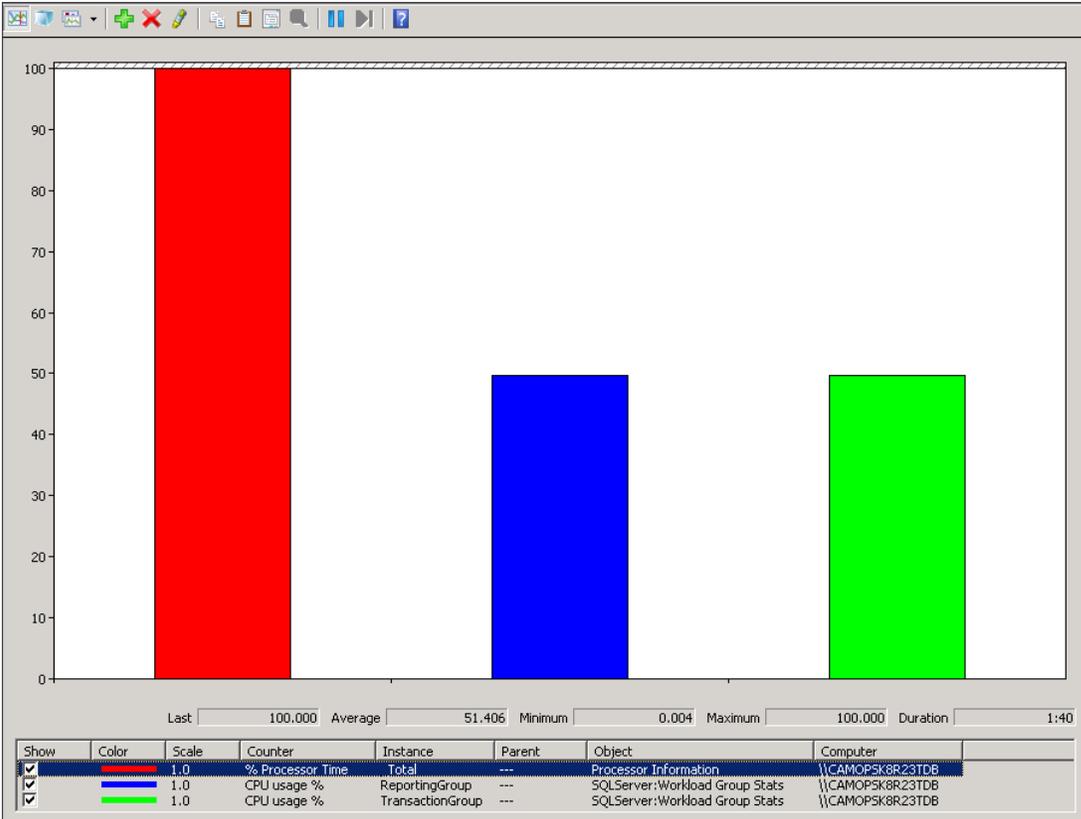
Based on the example at the beginning of this section, where a user executing multiple resource-intensive reports simultaneously, those reports would be able to access "up to" 50% of the available CPU on the SQL Server under the current configuration.

Let's reconfigure the Reporting Group to only allow up to 25 % by changing the Maximum CPU % in the Resource Governor properties for the Reporting Group.
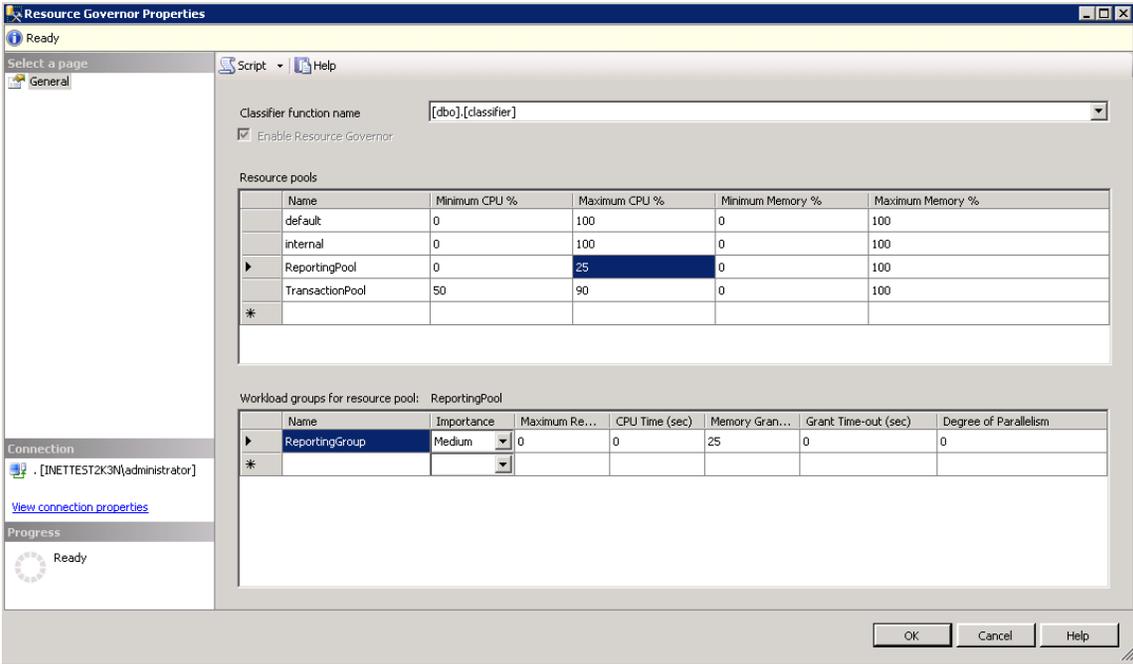
Executing the script on both servers again will yield the following results:
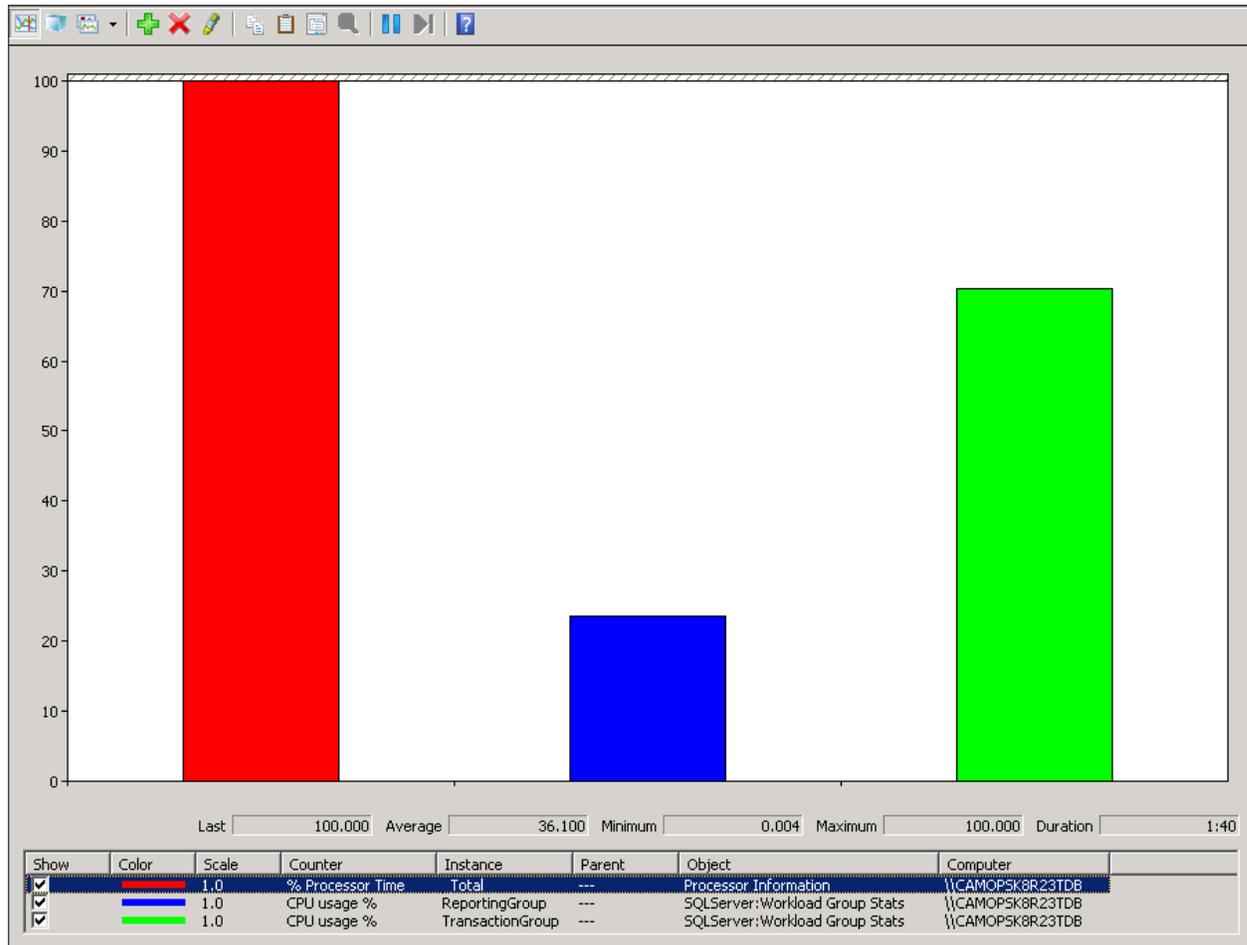
The Resource Governor will help to stop one or more types of transactions (if classified properly) from monopolizing the resources of your SQL Server and allow your applications to continue to work. The end result in this situation may be that reports take longer to run but at least your application will continue to function.

Another way to manage these issues is to identify the resource intensive reports in your organization (refer to the next chapter, on using the Reporting Services Execution Log and Management Reports for more information) and train your users to schedule these reports to run off hours using the process server. If this is not an option in your environment, then the Resource Governor may help to keep everything running.

Chapter 9: Monitoring Report Server Usage

Understanding how reports are run in your organization can be very helpful in identifying areas in which performance might be improved. In the previous chapter, about the SQL Server Resource Governor, we provided an example to show how a single user running reports can dramatically impact the performance of the system as a whole. The information presented in this chapter will provide you with the tools that can help you identify those types of users and/or the reports that are taking up valuable system resources.

Microsoft provides a set of sample reports that you can install, which provide a wealth of information about the usage of your report server.

Server Management Sample Reports Download and Installation Instructions

See the following link for sample reports and installation instructions:

http://msftrsprodsamples.codeplex.com/wikipage?title=SS2008%21Server%20Management%20Sample%20Reports&referringTitle=Home

Reports

After you download and configure the sample reports, you can generate the following reports to provide information on your report server workload:

Report	Description
Execution Status Codes.rdl	Shows the success and failure rates for all report executions occurring within a specified date range. It also shows which failure codes occurred and which reports failed to process.
Execution Summary.rdl	Shows overall report execution statistics for a specified date range. It shows the number of reports processed each day, the top 10 most requested reports, and the top 10 longest-running reports.
Report Summary.rdl	Shows summary report execution information for a specific report within a specified date range.

The Report Execution Summary report may prove useful to you. This report provides the following information on reports in the timeframe specified:

- Top 10 Longest Running Reports
- Top 10 Most Executed Reports
- Top 10 Largest Reports

Because all reporting is done under the credentials of a single report server user, the information for the Top 10 Users will not be accurate.
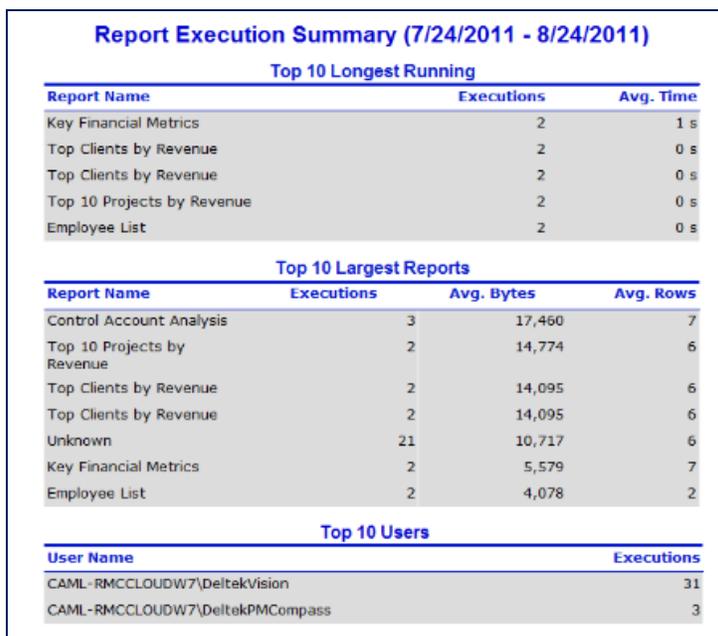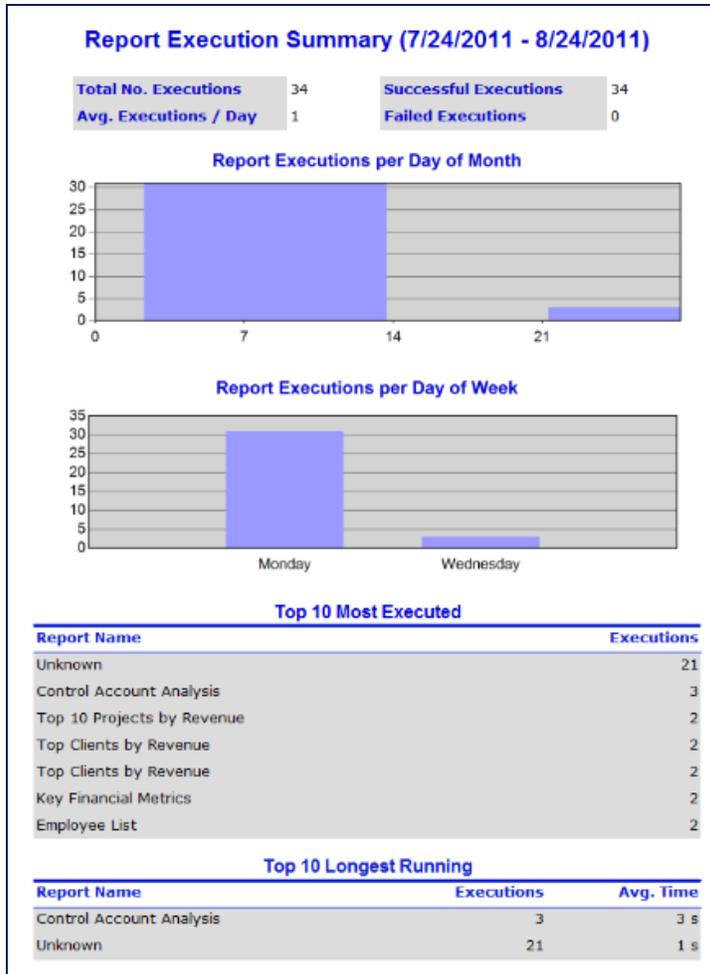
In addition, the following query (http://thefirstsql.com/2010/10/21/sql-server-reporting-services-performance-monitoring/) provides detailed information on specific report executions:

```
USE ReportServer
GO
SELECT TOP 100
  Report = REVERSE(LEFT(REVERSE(ReportPath),CHARINDEX('/',
REVERSE(ReportPath),1)-1)),
  Username,
  Parameters,
  TimeStart,
  TotalDurationMS = DATEDIFF(ms, TimeStart, TimeEnd),
  DurationDataRetrievalMS = TimedataRetrieval,
  DurationProcessingMS = TimeProcessing,
  DurationRendering = TimeRendering,
  [RowCount],
  ReportSizeKB = CAST(ByteCount/1024.0 AS decimal(18, 2)),
  ProcessingEngine =
CAST(AdditionalInfo.query('data(/AdditionalInfo/ProcessingEngine)') AS
varchar(200)),
  ScalabilityPagination =
CAST(AdditionalInfo.query('data(/AdditionalInfo/ScalabilityTime/Paginat
ion)') AS varchar(200)),
  ScalabilityProcessing =
CAST(AdditionalInfo.query('data(/AdditionalInfo/ScalabilityTime/Process
ing)') AS varchar(200)),
  EstMemPaginationKB =
CAST(AdditionalInfo.query('data(/AdditionalInfo/EstimatedMemoryUsageKB/
Pagination)') AS varchar(200)),
  EstMemProcessingKB =
CAST(AdditionalInfo.query('data(/AdditionalInfo/EstimatedMemoryUsageKB/
Processing)') AS varchar(200)),
  DBQueryTimes =
CAST(AdditionalInfo.query('data(/AdditionalInfo/DataExtension/SQL)') AS
varchar(200))
FROM ExecutionLog2 WITH (NOLOCK)
WHERE ReportPath <> 'Unknown'
ORDER BY TimeStart DESC
```

The **EstMemProcessingKB** value can help identify reports that use a significant amount of memory on the Reporting Services server. See the following blog post for detailed information about each column in this query:

http://blogs.msdn.com/b/robertbruckner/archive/2009/01/05/executionlog2-view.aspx

Chapter 10: Reporting Services Logging

Reporting Services has several different types of logging to help debug various reporting services issues. You can enable two kinds of logging:

- Trace logging, which provides more detailed logging on errors or warnings seen in the Reporting Services logs.

- HTTP logging, which helps identify issues with http related issues for Report Manager or the Report Server web service.

> For more information, see the Microsoft library article: http://msdn.microsoft.com/en-us/library/ms157403.aspx.

How to Enable Reporting Services Trace Logging

To configure trace logging, complete the following steps:

1. Stop the RS service.

2. Modify the ReportServer\bin\ReportServerService.exe.config file, as shown on page 75.

3. Restart the RS service.

   The trace level rules are as follows for a particular component and are defined in the ReportServerService.exe.config file:

   - If there is a component-wide trace level defined in RSTrace/Components, then it takes precedence.

   - If the trace level is defined for **all**, it uses that level (for example, **all:3**).

4. If neither 1 nor 2 is defined, the default trace level DefaultTraceSwitch defined in system.diagnostics/switches is used.

> For more information, see the Microsoft library article: http://msdn.microsoft.com/en-us/library/ms156500.aspx.

Components for Which You Can Enable Tracing

You can enable tracing for the following components:

- Library
- ConfigManager
- WebServer
- NtService
- Session
- BufferedResponse
- RunningRequests
- DbPolling
- Notification

- Provider

- Schedule

- Subscription

- Security

- ServiceController

- DbCleanup

- Cache

- Chunks

- ExtensionFactory

- RunningJobs

- Processing

- ReportRendering

- HtmlViewer

- DataExtension

- EmailExtension

- ImageRenderer

- ExcelRenderer

- PreviewServer

- ResourceUtilities

- ReportPreview

- UI

- Crypto

- SemanticModelGenerator

- SemanticQueryEngine

- AppDomainManager

- HttpRuntime

Changes for the ReportServer\bin\ReportServerService.exe.config File

Refer to the highlighted sections below:

<configuration>

  <configSections>

    <section name="RStrace"
type="Microsoft.ReportingServices.Diagnostics.RSTraceSectionHandler,Microsoft.ReportingServices.Diagnostics" />

  </configSections>

  <system.diagnostics>

    <switches>

```
<add name="DefaultTraceSwitch" value="3" />

  </switches>

</system.diagnostics>

 <RStrace>

      <add name="FileName" value="ReportServerService_" />

      <add name="FileSizeLimitMb" value="32" />

      <add name="KeepFilesForDays" value="14" />

      <add name="Prefix" value="tid, time" />

      <add name="TraceListeners" value="debugwindow, file" />

      <add name="TraceFileMode" value="unique" />

      <add name="HttpTraceFileName" value="ReportServerService_HTTP_" />

      <add name="HttpTraceSwitches" value="date,time,
clientip,username,serverip,serverport,host,method,uristem,uriquery,protocolstatus,bytesreceived,t
imetaken,protocolversion,useragent,cookiereceived,cookiesent,referrer" />

      <add name="Components"
value="all:3,http:3,Library:4,EmailExtension:4,Subscription:4,Schedule:4,Notification:4,DbPolling:
4,NtService:4" />

  </RStrace>
```

Errors in the Reporting Services Log File

Several lines from a reporting services log file showing errors are shown below:

session!ReportServer_0-1!e10!09/11/2011-13:14:51:: i INFO: LoadSnapshot: Item with session: pvon0l55nrycom3uczjnho45, reportPath: , **userName: KL\deltekadmin not found in the database**

library!ReportServer_0-1!e10!09/11/2011-13:14:51:: e ERROR: **Throwing Microsoft.ReportingServices.Diagnostics.Utilities.ExecutionNotFoundException: Execution 'pvon0l55nrycom3uczjnho45' cannot be found,** ;

Info: Microsoft.ReportingServices.Diagnostics.Utilities.ExecutionNotFoundException: Execution 'pvon0l55nrycom3uczjnho45' cannot be found

The sections (or "Components") that can be traced are identified at the beginning of each log entry and appended with an exclamation point. For example, if you want verbose logging for the errors in the example above, you would enable library and session verbose logging as follows:

<add name="Components" value="all:3,Library:4,Session:4" />

Enable Reporting Services HTTP Logging

For the Microsoft library article about this, see the following link:

http://msdn.microsoft.com/en-us/library/bb630443.aspx

The Reporting Services windows service runs its own http.sys listener to accept standard http/https requests on standard http ports (80/443). Unlike Internet Information Services, http logging is not enabled by default but can be enabled following the steps in the linked MSDN article above to assist in troubleshooting http and authentication related issues.

You can also use Fiddler trace the http requests from client to report server to assist in troubleshooting these kinds of issues. Obtain Fiddler and information from http://www.fiddler2.com.

Chapter 11: Deltek Vision Transaction Document Management

Vision Transaction Document Management (TDM) uses Microsoft SQL Server FILESTREAM technology to store and retrieve documents in a SQL Server database. Deltek has chosen to configure FILESTREAM functionality and to store these documents in a separate database rather than in your Vision transactional database. These documents include transaction-related supporting documents as well as Adobe InDesign templates.

The following instructions will assist you in configuring FILESTREAM and Vision TDM.

> Your separate Vision and FILESTREAM (TDM) databases must be backed up on the same schedule so that they will be in sync if a restore is needed.

Prerequisites

Install or upgrade to Vision 7.1.

> If your Vision Application server is running Windows Server 2008 as the operating system, and your SQL Server is running 2008 R2 as its operating system, a Microsoft hotfix is required. To obtain this hotfix and contact Microsoft Support, refer to the following KB article:
>
> http://support.microsoft.com/kb/2255379

Installation Overview

Refer to the following steps to configure Vision TDM with SQL Server FILESTREAM:

- Identify the SQL Server to host the FILESTREAM database
- Enable FILESTREAM
- Identify the Physical Disk Location of the FILESTREAM Data
- Create the FILESTREAM Database

Identify the SQL Server to Host the FILESTREAM Database

In many Vision configurations, the SQL Server that hosts the Vision transaction database will also host the FILESTREAM database. However, Vision TDM has been developed to allow the FILESTREAM database to exist on a separate SQL Server instance. It is recommended that you review the FILESTREAM Best Practices section below before making the decision on where to enable FILESTREAM.

FILESTREAM Best Practices

The following article provides detailed information on FILESTREAM best practices:

http://msdn.microsoft.com/en-us/library/dd206979(v=sql.105).aspx

Some examples of FILESTREAM Best Practices noted in the MSDN article are listed below:

- Disable short file names on FILESTREAM computer systems because they take significantly longer to create. To disable short file names, use the Windows **fsutil** utility.
- Regularly defragment FILESTREAM computer systems.

- Use 64-KB NTFS clusters. Compressed volumes must be set to 4-KB NTFS clusters.

- Disable indexing on FILESTREAM volumes and use the Windows **fsutil** utility to set **disablelastaccess**.

- Disable antivirus scanning of FILESTREAM volumes, if possible. If antivirus scanning is necessary, avoid setting policies that will automatically delete offending files.

Enable FILESTREAM on SQL Server

You must enable FILESTREAM on the SQL Server intended to host the FILESTREAM database before you can create the database. Because FILESTREAM is not enabled by default, you must enable FILESTREAM during the SQL Server installation or after SQL Server is installed. Refer to the appropriate section for your installation.

Enable FILESTREAM during SQL Server Installation

To enable FILESTREAM during SQL Server installation, complete the following steps:

1. Open the Database Engine Configuration.

2. Click the FILESTREAM tab and ensure that the **Enable FILESTREAM for Transact-SQL access, Enable FILESTREAM for file I/O streaming access** and **Allow remote clients to have streaming access to FILESTREAM data** options are selected.

> By default, the Windows share name that will be created for FILESTREAM access will be the SQL Server instance name (default SQL instances are named MSSQLSERVER). Deltek recommends that you follow the default selections.

3. Click **Next** to continue.
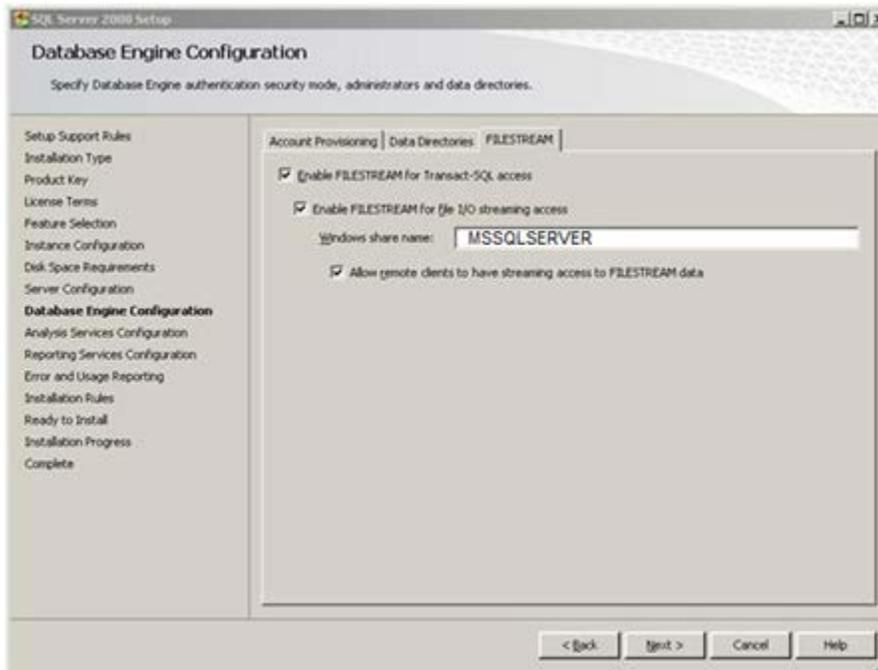
Enable FILESTREAM after SQL Server is installed

To enable FILESTREAM after installaing SQL Server, complete the following steps:

1. On the database server, open the SQL Server Configuration Manager.

2. Right-click your SQL Server service, and click **Properties** on the shortcut menu.

3. Click the FILESTREAM tab and ensure all three options are selected.

> By default, the Windows share name will be the SQL Server instance name (default SQL instances are named MSSQLSERVER). Deltek recommends that you follow the default selections.
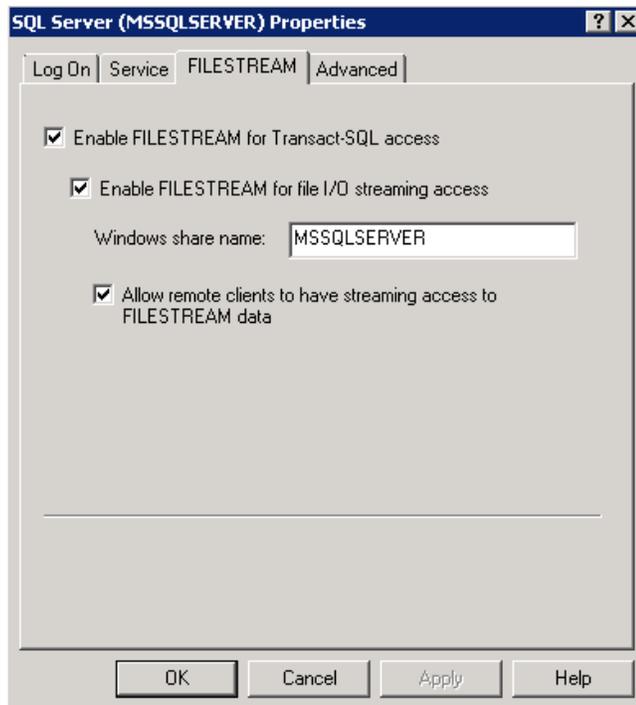
4. Click **OK.**

Additionally, complete the following configuration settings in SQL Server properties:

1. Open SQL Server Management Studio.

2. Right-click the server and select **Properties**.

3. Select the **Advanced** page.

4. Check to ensure that the **Running Values** are displaying that the **Filestream Access level** is set to **Full access enabled**.
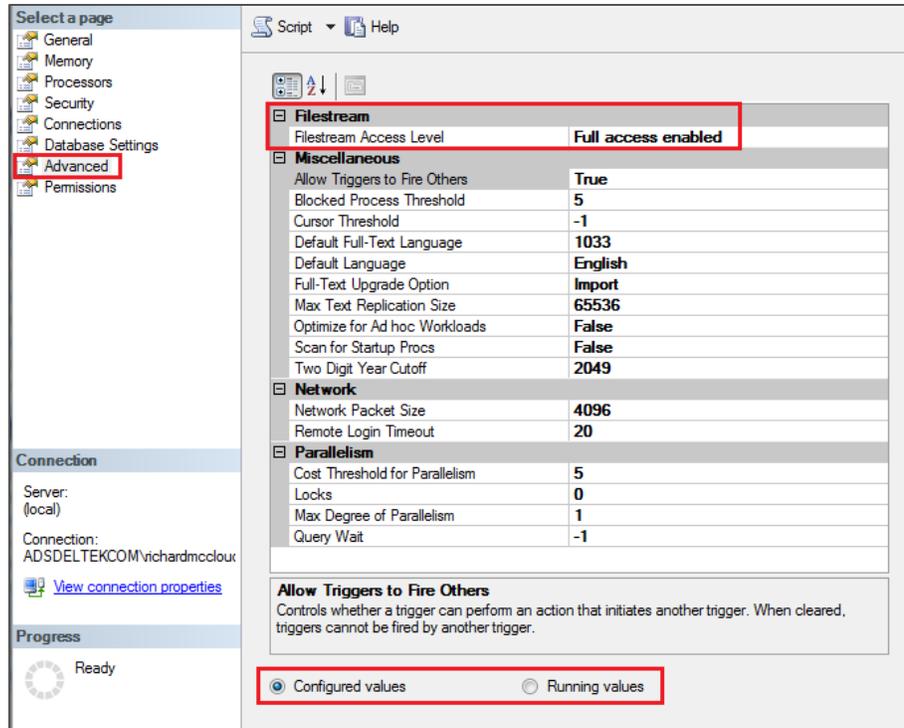
5. Click **OK** and restart the SQL Server service.

Identify the Physical Disk Location of the FILESTREAM Data

Prior to creating the FILESTREAM database, you must determine where the FILESTREAM data will be stored. By default, the FILESTREAM data is stored in a folder and sub-folders in your SQL Server Data folder. Depending on your SQL Server installation and disk configuration, it may be more advantageous to place this data on a separate physical disk, partition, RAID array, and so on.

> Refer to the "FILESTREAM Best Practices" section for more information.

Create the FILESTREAM Database

To create the FILESTREAM database, complete the following:

1. Open the SQL Server Management Studio (SSMS).

2. Right-click the Databases folder, and click **New Database** on the shortcut menu.

3. Enter a name for the database.

    The name of the FILESTREAM database **must** be your Vision database name plus **FILES** appended to it. For example, if your Vision database is **VisionDemo71**, then your FILESTREAM database will be **VisionDemo71FILES**.
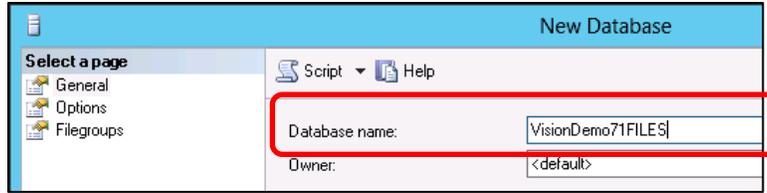
4. Select the Filegroups page from the left menu.

5. Click the **Add** button to add a new Filegroup.

6. Enter a name for the filegroup.

    The name of the Filegroup **must** be your Vision FILESTREAM database name plus **_FS** appended to it. For example, if your Vision FILESTREAM database is **VisionDemo71FILES**, then the name of the Filegroup will be **VisionDemo71FILES_FS**. This name is necessary for the Weblink utility to correctly create the FILESTREAM database objects (tables, indexes, and so on).
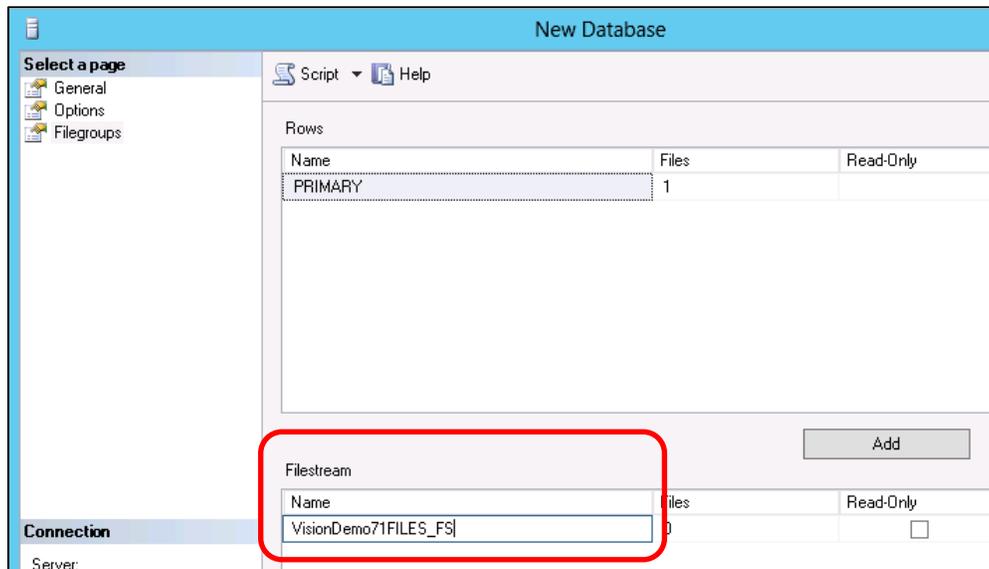
7. Select the General page from the left menu.

8. Click the **Add** button to add the FILESTREAM data file.

9. Enter the following information for the FILESTREAM data file:

    ▪ **File Type** — Select **Filestream Data**.

    ▪ **Logical Name** — For consistency, name this the same name as the Filegroup (for example, **VisionDemo71FILES_FS**).
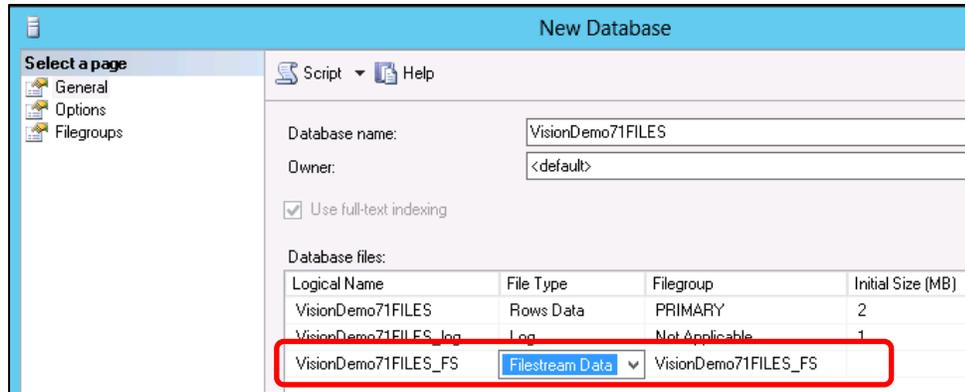
- **Path** — Select the physical path to the FILESTREAM data.

> Refer to the "Identify Physical Disk Location of the FILESTREAM Data" section for more information.
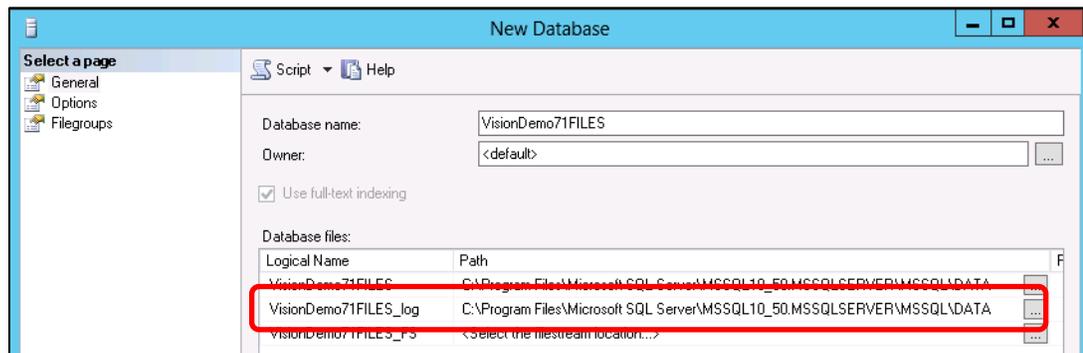
> The other fields applicable to the SQL Server Data and Log files are not applicable for FILESTREAM data.

Configure Database Access for FILESTREAM Database

In addition to configuring SQL Server to support FILESTREAM, you must make changes to your Vision configuration to properly support Vision TDM.

IIS Application Pool Configuration

The FILESTREAM database connection is only supported using Windows Integrated Authentication. In Vision, the identity of the DeltekVisionAppPool is the account that will make this connection to the FILESTREAM-enabled TDM database. You will need to ensure that the Application Pool is running as a Windows account (domain or local), and that this account has db_owner rights to the FILESTREAM database.

> Although the FILESTREAM database connection requires Windows Integrated Authentication, you do not need to make any changes to the database connection for your Vision transaction database to support FILESTREAM. For example, if you are using a SQL Login to access your Vision database, no changes are needed.

> If using a local account, the same Windows account name (with the same password) must exist on both the Vision Web/Application server and the FILESTREAM enabled SQL Database server in order for Vision to access the FILESTREAM Windows file share.

Configure and Validate the FILESTREAM Database with Weblink

After the FILESTREAM database has been created and the IIS Application Pool identity has been granted db_owner rights to the FILESTREAM database, you will use the Weblink Utility to create the FILESTREAM database schema.
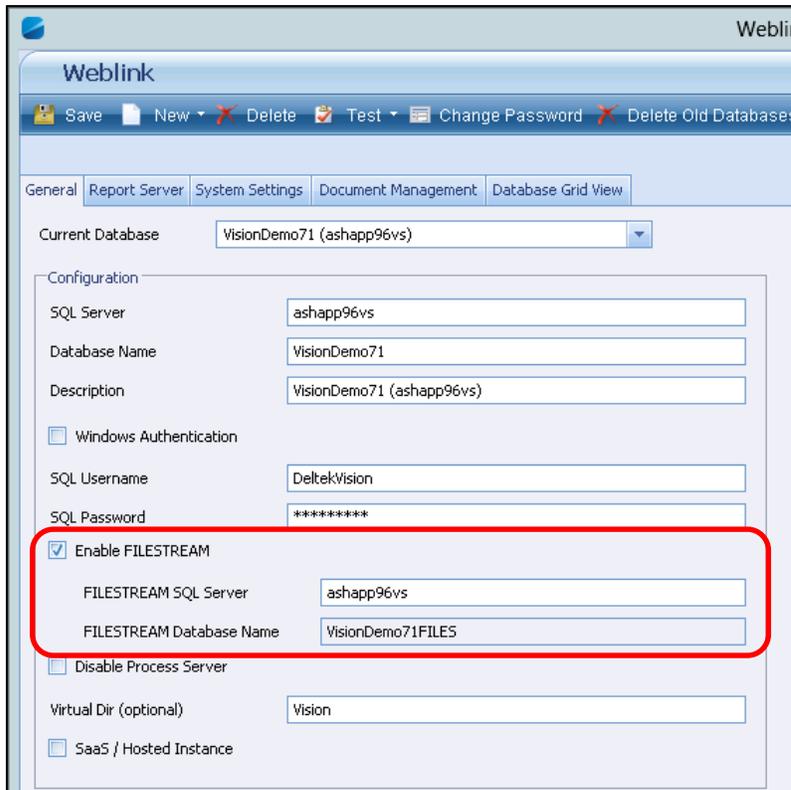
To configure the database schema and verify the configuration, complete the following steps:

1. Launch and log in to the Weblink utility on the Vision Web/Application server.

2. From the **Current Database** drop-down list, select your Vision database that will be used with Vision TDM.

3. Select the **Enable FILESTREAM** check box. You will be presented with the following message.

By default, Weblink will prefill the name of the SQL Server being used for the Vision database and the name of the FILESTREAM database (required and grayed out). If you are hosting the FILESTREAM database on a different instance of SQL Server, click **No**, and modify the name of the FILESTREAM SQL Server. As indicated in the message, you can re-test (and create the FILESTREAM database schema) by clicking the **Test Connection** button in the Weblink menu after you have made the necessary changes.

> Your FILESTREAM database can exist on a different SQL Server instance. Refer to the "Identify the SQL Server to Host the FILESTREAM Database" section for more information.

4. Click **Yes** to validate the configuration. The following message displays:
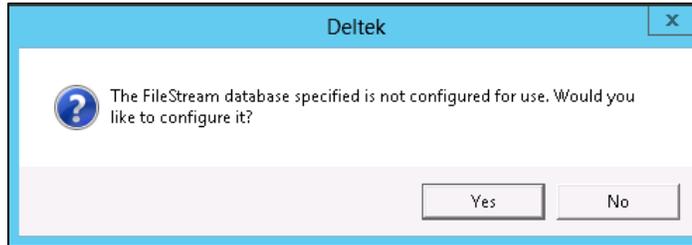
5. Click **Yes** to create the FILESTREAM database objects (Tables, Indexes, and so on). When the objects have been created, the following message displays:
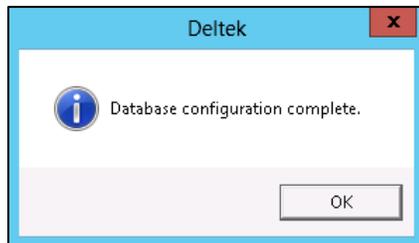
Files Administration Utility in Vision

The Vision Files Administration utility allows you to search for and view files that were uploaded into Vision. This includes supporting documents that were uploaded for Vision transactions as well as InDesign templates that were imported or created using the Vision Merge Templates application.

To view the documents that have been uploaded using the Files Administration utility, complete the following steps:

1. Open the Vision application.

2. ON the **Vision Utilities** menu, click **Files Administration**.

3. On the Files Administration dialog box, use the **Date Range** fields to select the start and end dates to define the date range to search. Vision defaults to use the past three days.

4. Click **Refresh Files List** to populate the Files grid. Records that match the start and end date criteria display.

5. To further refine your results set, complete one or more of the following:

    ▪   Enter specific text that you want to find. Vision searches the **File Name** and **Description** fields to locate the matching text.

- Open the lookup, and select a User ID.

- Use the drop-down list to select a Vision Application. This drop-down list displays the applications that allow supporting documents.

6. Click **Refresh Files List** to activate the search. The Files grid updates to list all documents that match the specified criteria.

7. Click the **File Name** link to open the associated PDF.

> If you receive an error message stating that the file is missing, the Vision and TDM databases are not in sync. Refer to the "Data Synchronization Issue" section for additional information.

Data Synchronization Issue

The Databases Out of Sync dialog box displays when the files in the Vision and FILESTREAM databases are not synchronized. This file mismatch can occur when there is a database backup or restore on one database, but not the other. In this situation, the **File Name** link cannot open the selected file. Click **OK** to return to the Files Administration utility. Then contact your system administrator for details.

Troubleshooting FILESTREAM

Refer to the following list of potential problems, causes, and solutions for issues with FILESTREAM.

Problem 1

You test the database connection for the first time in Weblink, and Weblink cannot create the FILESTREAM database objects.
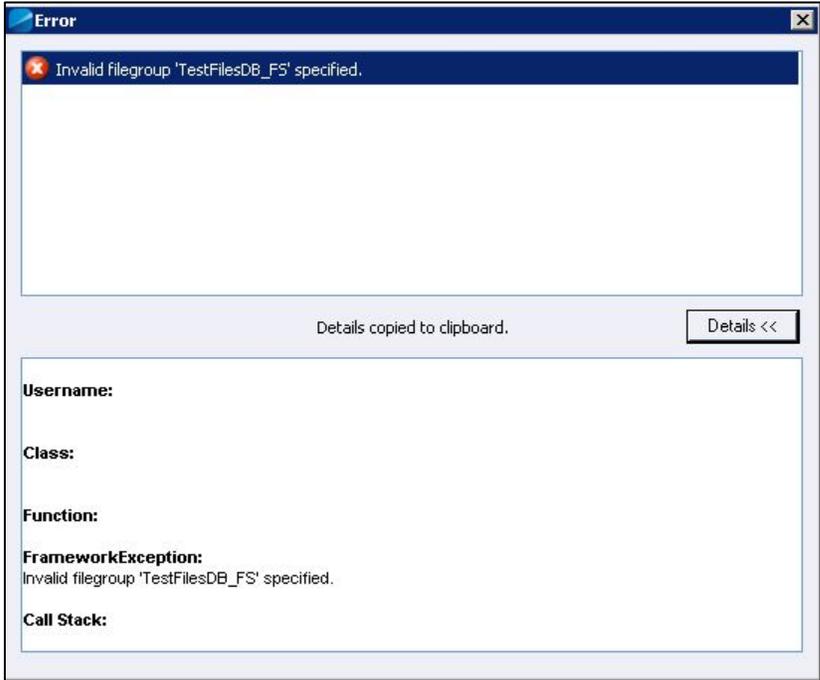
Possible Cause	The FILESTREAM filegroup name is not in the required format: **[VisionFILESTREAMDBName]_FS**.
Solution	Reformat the FILESTREAM filegroup name.

Problem 2

You receive a "FILESTREAM data cannot be placed on empty filegroup" error.
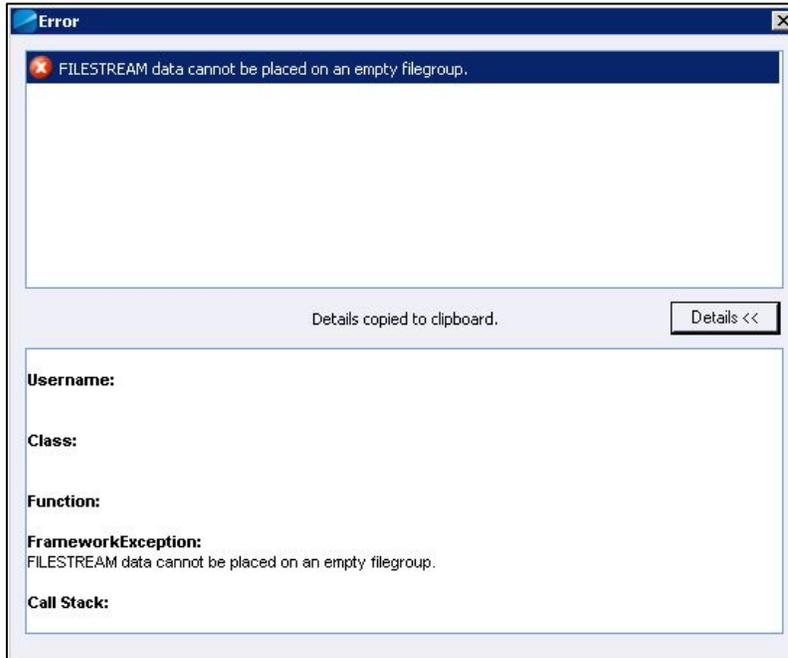
Possible Cause	The FILESTREAM filegroup is not configured.
Solution	Configure the FILESTREAM filegroup, and confirm that the FILESTREAM filegroup name is in the required format: **[VisionFILESTREAMDBName]_FS**.

Problem 3

Vision displays the following message when users attempt to upload documents where FILESTREAM functionality is required.
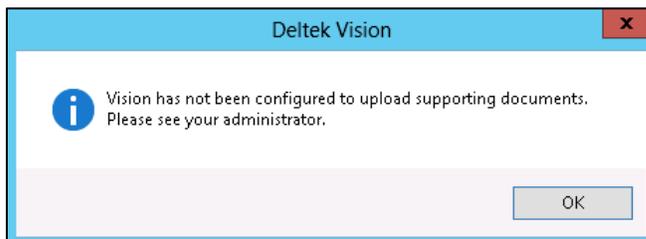
Possible Cause	The **Enable FILESTREAM** option is not selected in Weblink and/or FILESTREAM is not configured properly (unable to connect to FILESTREAM database or FW_Files table not created).
Solution	Confirm that the **Enable FILESTREAM** option is selected in Weblink and that FILESTREAM is configured properly.

Problem 4

When testing the FILESTREAM configuration Weblink, the following error displays.

Possible Cause	The FILESTREAM database has not been created or has not been created with the required naming format, or the Identity of the DeltekVisionAppPool in IIS has not been granted db_owner rights to the FILESTREAM database.
Solution	Confirm that the FILESTREAM database exists and has been properly named and that the IIS Application Pool Identity has the required database rights.

Using FILESTREAM with Other SQL Server Features

Refer to the following article for detailed information on using FILESTREAM with other SQL Server options:

http://msdn.microsoft.com/en-us/library/bb895334(v=sql.105).aspx

FILESTREAM and SQL 2012 Availability Groups

http://msdn.microsoft.com/en-us/library/hh510261.aspx

TDE (Transparent Data Encryption)

FILESTREAM can be used with TDE; although, the FILESTREAM data is not encrypted.

Log Shipping

Log shipping supports FILESTREAM. Both the primary and secondary servers must be running SQL Server 2008, or later, and have FILESTREAM enabled.

Database Mirroring

Database mirroring does not support FILESTREAM. A FILESTREAM filegroup cannot be created on the principal server. Database mirroring cannot be configured for a database that contains FILESTREAM filegroups.

Failover Clustering

For failover clustering, FILESTREAM filegroups must be put on a shared disk. FILESTREAM must be enabled on each node in the cluster that will host the FILESTREAM instance.

SQL Server Express

SQL Server Express supports FILESTREAM. The 4-GB database size limit does not include the FILESTREAM data container.

How to Use FILESTREAM in a Firewall-Protected Environment

To use FILESTREAM in a firewall-protected environment, both the client and server must be able to resolve DNS names to the server that contains the FILESTREAM files. FILESTREAM requires the Windows file-sharing ports 139 and 445 be open.

The "client" in your Vision TDM deployment is the web/application server, so if your Vision deployment has a firewall between the web/application server and the FILESTREAM database server, then the ports referenced above must be open between the servers.

Queries to Join the Vision Transaction DB and FILES DB

The following query will obtain the file sizes in the FILES database by joining two [Vision] and [Vision]Files databases. This will work if the databases are on the same SQL Server:

```
SELECT DATALENGTH(a.FileData) as FileSize, b.FileName, b.ContentType FROM
[VisionDBName]FILES.dbo.FW_Files a inner join [VisionDBName].dbo.FW_Files b ON
a.FileID=b.FileID
```

The following query will obtain the file sizes in the FILES database by joining two [Vision] & [Vision]Files databases. This will work if the databsaes are on Linked SQL Servers:

```
SELECT DATALENGTH(a.FileData) as FileSize, b.FileName, b.ContentType FROM
[FILESTREAMDBServer].[VisionDBName]FILES.dbo.FW_Files a inner join
[VisionDBName].dbo.FW_Files b ON a.FileID=b.FileID
```

> You must create the link between the servers first. See SQL Server Books Online for information on how to create Linked Servers: http://msdn.microsoft.com/en-us/library/ms130214(v=sql.105).aspx

Chapter 12: Configure an Alternate Database for Vision Reporting

When you use Vision Reporting, Vision creates two different workloads on your SQL Server Database Engine: Transactional and Reporting. These workloads are necessary for proper functionality, but they also require a tremendous amount of resources on your SQL Server.

Vision 7.1 provides the following method to offload the reporting workload to a different SQL Server, which will help reduce the drain on your SQL Server resources:

- Configure a copy of your Vision database for access, and configure the connection string information in Weblink on the Report Server tab in the **Alternate Database for Reporting** section.

The following reports will use the alternate database:

- Dashboard reports

- Reports in the Reporting menu applications (minus Purchasing reports)

- The reports that will use the alternate database will do so whether previewed, directly printed, emailed, run via the process server, or otherwise processed.

All other reports, including posting logs, billing (interactive and batch) reports, timesheet and expense reports, and so on will continue to run their queries against the Vision transaction database.

> Visualization reports do not use SQL Reporting Services and are not applicable to this feature.

Alternate Database for Reporting

The primary benefit of using the **Alternate Database for Reporting** configuration in Weblink is that it can be used with any version or edition of SQL Server.

> With SQL Express, the Alternate Database for Reporting must be located on the same SQL Express instance as the transaction database. This is a limitation of SQL Express because Reporting Services for SQL Express can only use Local databases.

When using the Alternate Database for Reporting configuration in Weblink, consider the following:

- Find an appropriate method to create the copy of the database on the second SQL Server (for example, transactional replication, log shipping, database backup/restore, or third party tools that support SQL Server snapshot backup).

> Deltek has not completed testing and does not provide support for the underlying database copy/synchronization methodology you choose.

- Ensure that the database copy used for reporting is kept in sync with the transaction database. Not keeping the databases in sync will result in stale data for reporting purposes.

- Ensure that the SQL login used for authentication has read-only access to the database.

Refer to the following are links to Microsoft documentation that will help you choose an appropriate database replication/synchronization methodology:

> Deltek does not provide support for the underlying database copy/synchronization methodology you choose.

- Transactional Replication:

  http://msdn.microsoft.com/en-us/library/ms151198.aspx

- Log Shipping:

  http://msdn.microsoft.com/en-us/library/ms187103.aspx

- Backup/Restore:

  http://msdn.microsoft.com/en-us/library/ms187048.aspx

- Third Party Tools that support Snapshot Backups:

  http://msdn.microsoft.com/en-us/library/ms189548(v=sql.105).aspx

> SQL Server Database Mirroring is not supported for the Alternate Database for Reporting functionality as the mirrored database is not accessible for read-only queries. Also, Database Mirroring does not support SQL Server FILESTREAM, which is required for Vision Transaction Document Management (TDM).

Configure the Alternate Database for Reporting in Weblink

To configure an alternate database for reporting, complete the following steps:

1. Identify and implement a methodology to create a copy of your Vision transaction database on a second SQL Server. For testing purposes, you can perform a backup/restore.
2. Identify and implement a methodology to ensure that the data is synchronized between the databases within a timeframe differential suitable to your business needs.
3. Create a login that has read-only rights to this database copy. This can be accomplished by granting db_datareader rights, rather than db_owner rights, for the SQL Server login that is used for the alternate database for reporting.
4. Launch the Vision Weblink Utility and select the Vision transaction database entry that you will configure for an alternate reporting database.
5. Click the Report Server tab.
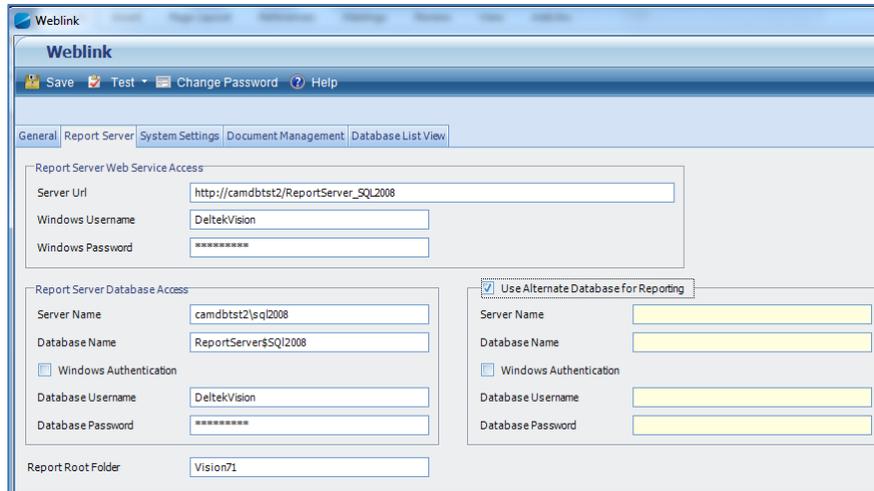
6. Select the **Use Alternate Database for Reporting** option. When you click **OK**, Vision displays the following message:
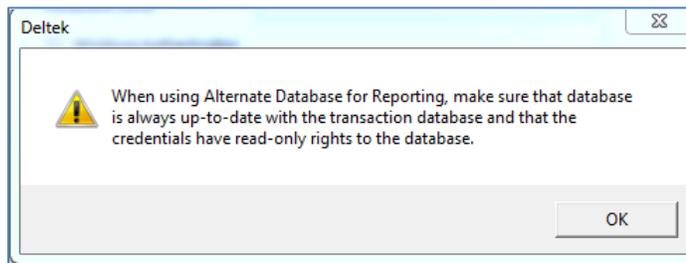
7. Click **OK** to continue. Complete the following fields to enter the connection string information for the alternate database:

Field	Description
Server Name	Enter the name of the SQL Server hosting the alternate database.
Database name	Enter the name of the alternate database.
Windows Authentication	Select this check box if using Windows Authentication for the database connection. The identity of the DeltekVisionAppPool will need read-only rights to the alternate database.
Database Username/Password	If not using Windows Authentication, enter the SQL server login with read-only rights to the alternate database.

8. From the Weblink menu, click **Test » Alternate Database for Reporting** to validate the connection.

Troubleshooting

Identify the Connection String Used for a Report

After configuring the **Alternate Database for Reporting** or **Availability Group** options, you must validate that the reports are running against the correct database.

Preview the Report

To acquire the connection string by previewing the report, complete the following steps:

1. Click the construction hat icon in the Reporting toolbar.

> You may not see it if the report is not maximized

2. From the **View Report Information** drop-down list, select **Report Data Source**.
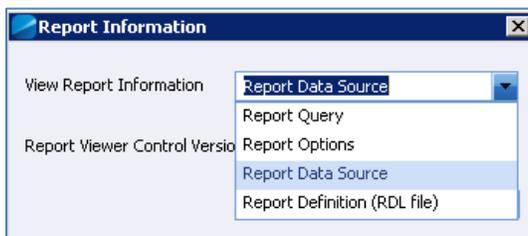
3. Click the **View** button.

4. You will be prompted to Open or Save the XML file.
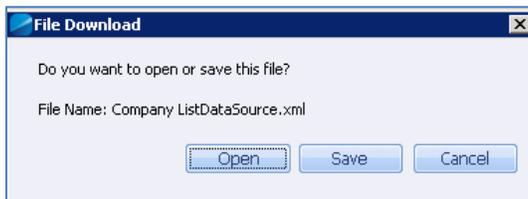
5. Click **Open** and the file will open with the application configured to open XML files. On most computers that will be your default browser.

The following is displayed:
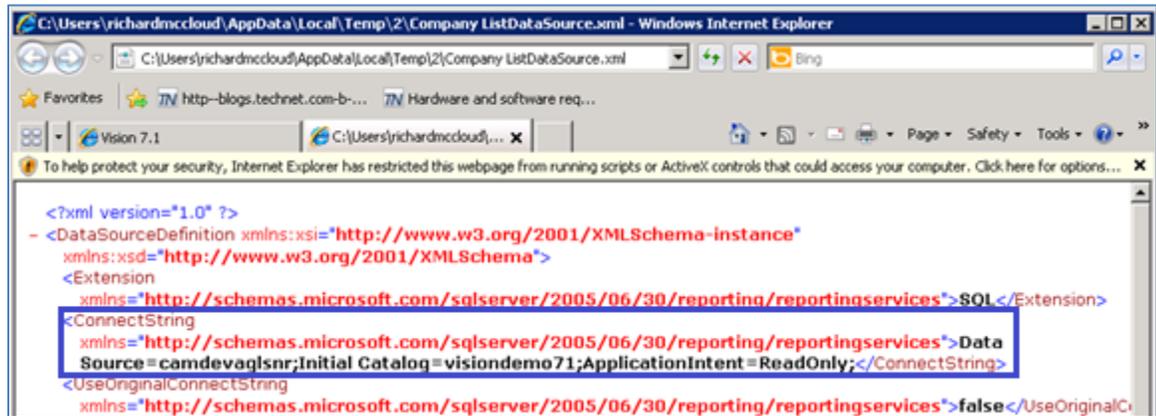
6. Review the ConnectString element for the following attributes:

- **Data Source** — This is either the database server specified in the Alternate Database for Reporting configuration or the Availability Group listener if using Availability Groups

- **Initial Catalog** — This is either the database name specified for the Alternate Database for Reporting configuration or the Vision database name if using Availability Groups

- **ApplicationIntent=ReadOnly** — Only displays when using Availability Groups and if the report was run against the Read Only reporting database.

Issue

The following error will display if the SQL login used for the Vision database does not have the **View Definition** or **View Server State** permissions.

See **Database Login Configuration**.

FrameworkException:

The user does not have permission to perform this action.

Call Stack:

{\b Query: }

select synchronization_health from sys.dm_hadr_availability_group_states

Chapter 13: Configure Microsoft SQL 2012 Availability Groups

With the release of Deltek Vision 7.1, support for Microsoft SQL 2012 AlwaysOn Availability Groups has been added. A SQL 2012 Availability Group provides an all-inclusive High Availability and Disaster Recovery solution for SQL Server databases, which encompasses many features. The specific feature of Availability Groups directly supported by Vision is called Readable Secondary Replicas/Read Only Routing. This configures a readable replica of your transaction database that you can use to offload report queries from the primary transaction database

This chapter focuses specifically on the SQL 2012 Availability Group features supported by Vision.

> For support of all the other features, please refer to the Microsoft documentation:
>
> http://msdn.microsoft.com/en-us/library/ff877884.aspx
>
> Additionally, the following AlwaysOn Architecture Guides provide a wealth of insight into designing the solution:
>
> http://blogs.msdn.com/b/sqlalwayson/archive/2012/07/03/alwayson-architecture-guides.aspx

Prerequisites

Refer to the MSDN documentation for Prerequisites, Restrictions, and Recommendations for AlwaysOn Availability Groups:

http://msdn.microsoft.com/en-us/library/edbab896-42bb-4d17-8d75-e92ca11f7abb

Specific prerequisites for Vision are listed below:

- Deltek Vision 7.1

- The Enterprise Edition of SQL Server 2012 SP1 + CU1

- At least two SQL Server 2012 nodes

- The Enterprise Edition of Windows Server 2008 Sp2 or Windows Server 2008 R2 Sp1 or the Standard Edition of Windows Server 2012. The specific operating system feature that is required to support Availability Groups is Windows Server Failover Clustering.

- A Windows file share on a server other than the SQL Servers to which the SQL service accounts have write access. This is required for configuration of the Availability Groups.

- A .NET 3.5 SP1 Hotfix may be required on the Vision web/application servers. Refer to the following Microsoft KB article:

    http://support.microsoft.com/kb/2654347

- Windows Server 2008 Enterprise SP2 (x86 or x64) or Windows Server 2008 R2 Enterprise SP1 (x64 only). The Enterprise Edition of the operating system is required due to the need for the Windows Server Failover Clustering feature

- Install the following features on ALL nodes:
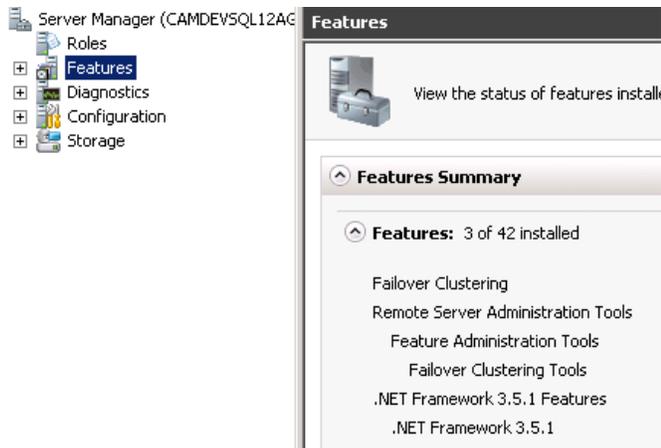
- Create a file share on a different server that the service accounts on all nodes can access

- .NET 3.5 Sp1 Hotfix may be required http://support.microsoft.com/kb/2654347

Create the Windows Server Failover Cluster (WSFC)

The WSFC will cluster applications and services. Your specific configuration may be different depending on your intended use of SQL 2012 Availability Groups. For example, you may want to use a SQL Server Failover Cluster Instance (FCI) in addition to using Availability Groups. One of the primary differences in the cluster configuration of an FCI versus an Availability Group is the need to provide shared storage.

> Refer to the Microsoft documentation for in depth details of configuring Windows Server Failover Clustering for your intended use.

When configuring Windows Server Failover Cluster:

- A Cluster virtual network will be created. You will need an IP address and DNS name for the Cluster and also the server names of the nodes that will be members of the cluster.

- No shared storage is needed, so you can clear the check box to add available storage.

- A static IP or DHCP can be used for the Cluster Network. Deltek recommends a static IP for production environments. The example provided below will be using DHCP.

- A DNS name will be created automatically, or you can create a DNS entry before configuring the cluster.

- You will need domain rights as the process creates a computer account in the domain for the cluster virtual network.

- There are two virtual networks created, one for the Windows Server Failover Cluster and one for the Availability Group listener. Use a unique name for the cluster which is not SQL-specific but will be easily identifiable as the Windows Cluster.

- When Vision connects to the SQL Server, it will not be connecting to the WSFC name. Vision will connecti to the Availability Group Listener (created later). The WSFC is enabled for the fail-over functionality of availability groups.

Installing and Configuring WSFC

Use the following procedures to install and configure Windows Server Failover Clustering.

> Depending on your operating system, the steps in the procedures may vary slightly. The procedures in this section are based on Windows Server 2012 Standard Edition.

Install Failover Clustering Feature

To install the failover clustering feature, complete the following steps:

1. Open the Server Manager utility.

2. Access the **Local Server**, and scroll down to **Roles and Features**.

3. From the **Tasks** drop-down list, select **Add Roles and Features**.

4. In the Add Roles and Features wizard, click **Next** until you get to the Select Features page.

5. Select the **Failover Clustering** option.

6. If prompted, click **OK** to install any dependent features.

7. Complete the Wizard to perform the installation.

8. If prompted, reboot the server.

Configure Failover Clustering using Failover Cluster Manager

To configure failover clustering, complete the following steps:

1. From Administrative Tools, open the Failover Cluster Manager.

2. Under **Management**, click **Create Cluster**. The Create Cluster Wizard will guide you through the process.

3. On the Select Servers page of the wizard, browse to or enter the names of the servers that will be part of the cluster to the configuration.
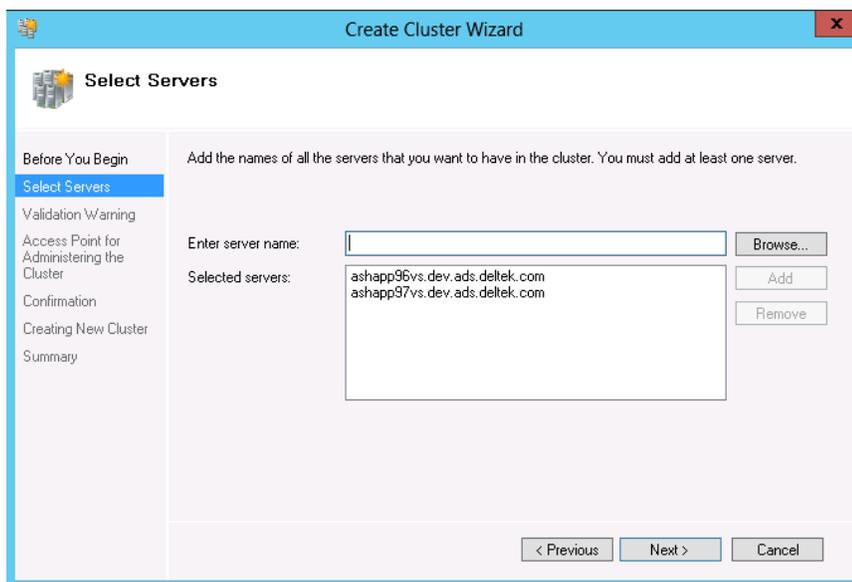
4. On the Validation Warning page, select **Yes** to run the Cluster Validation tests, and click **Next**.
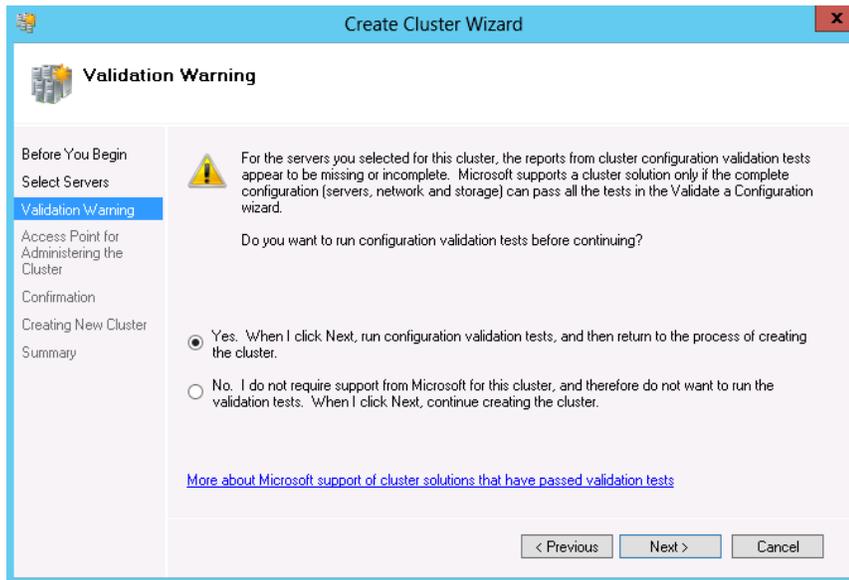
This process creates a report that will identify any problems that need to be addressed before creating the cluster.

5. When the validation is complete, you must provide a name for the cluster.
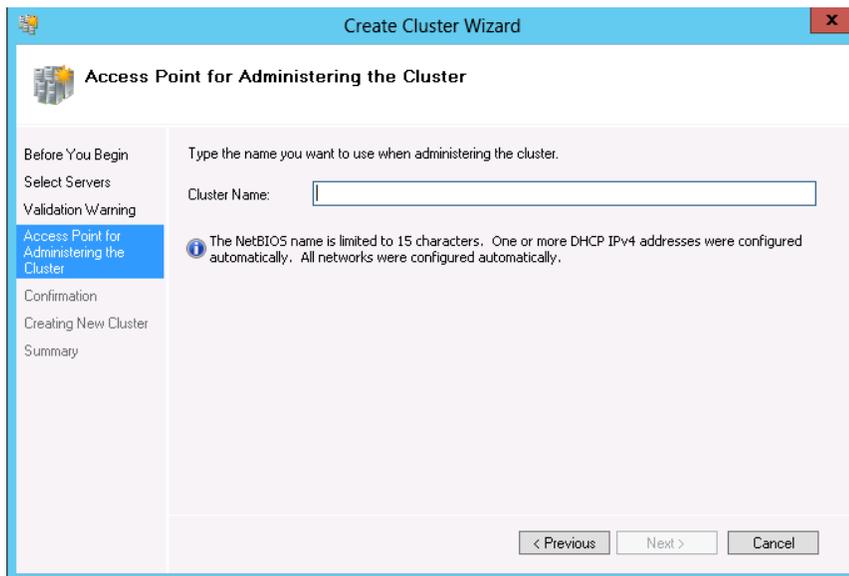
6. Click **Next** to create the cluster.
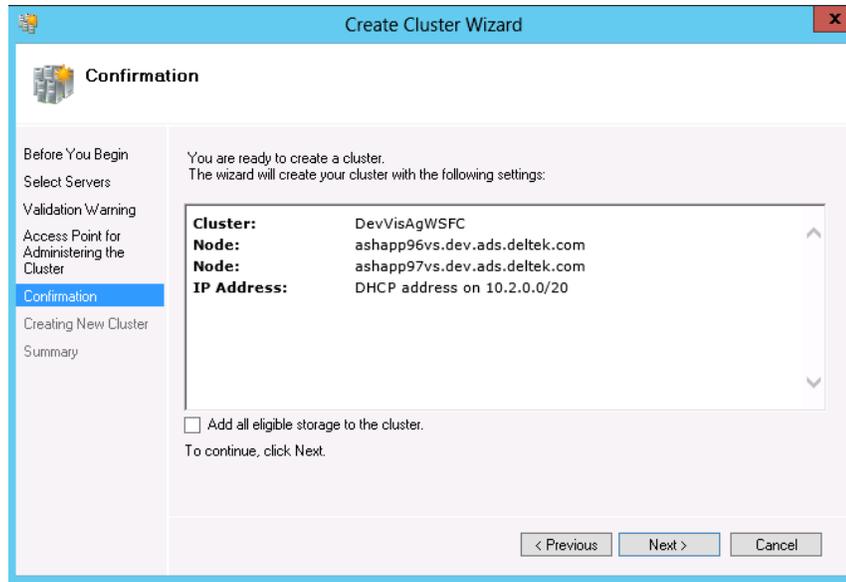
If you are configuring a WSFC that does not require shared storage, you can clear the **Add all eligible storage to the cluster** option.

Install SQL Server 2012 on Each Node

After configuring the WSFC, you must perform the SQL Server 2012 installation on each node in the cluster.

Installation Requirementsa nd Notes

- SQL Server Enterprise Edition is required for Availability Groups.

- If only configuring Availability Groups (not FCI), you must perform a New SQL Server stand-alone installation, not a New SQL Server failover cluster installation on each node. If you choose a SQL Server Cluster installation, it may fail the pre-requisites of shared storage as this is not a requirement of Availability Groups. However, it may be a requirement for your specific configuration.

- Only the SQL Database Engine can use Availability Groups. Even though the Availability Groups use a WSFC, this is not a true cluster and will not provide fault tolerance for other SQL Server services (Analysis Services or Reporting Services) if installed.

- Analysis Services must be part of an actual Failover Cluster Instance (FCI) where SQL is installed using New SQL Server failover cluster installation in order to be fault tolerant.

- A FCI may be used together with an availability group to enhance the availability of an availability replica. However, to prevent potential race conditions in the WSFC cluster, automatic failover of the availability group is not supported to or from an availability replica that is hosted on a FCI.

- Reporting Services uses a Scale-out Deployment, which is not a cluster.

- You can use the same service accounts on each node or different service accounts but all accounts must have rights to the file share as outlined in the Prerequisites section.

- FILESTREAM functionality can be used with the Availability Groups and will require that FILESTREAM be enabled on all fail-over nodes.

> For more information, see http://msdn.microsoft.com/en-us/library/hh510261.aspx.

- Although not a specific requirement, you should consider mirroring the SQL Server installation on each node including installation and data paths and also the instance name.

- For proper failover support, the failover nodes should be of comparable hardware resources.

- Refer to the MSDN documentation for Prerequisites, Restrictions, and Recommendations for AlwaysOn Availability Groups, http://msdn.microsoft.com/en-us/library/edbab896-42bb-4d17-8d75-e92ca11f7abb

After installing SQL Server on all nodes in the cluster, restore your Vision transaction database and configure the SQL Reporting Services databases (ReportServer and ReportServerTempDB) on the Primary node in the cluster.

Database Login Configuration

For the Vision and Reporting Services databases that are part of an Availability Group to be immediately available in the event of an Availability Group failover, you must complete these steps on all failover nodes. The following rights need to be granted to the login used to access the databases (Vision and Reporting Services databases) that are part of the availability group:

Permission	Required for
Dbo (Database Owner?) rights to all databases in the AG	All databases in the Availability Group
View Any Definition	Availability Groups
View Server State	Availability Groups
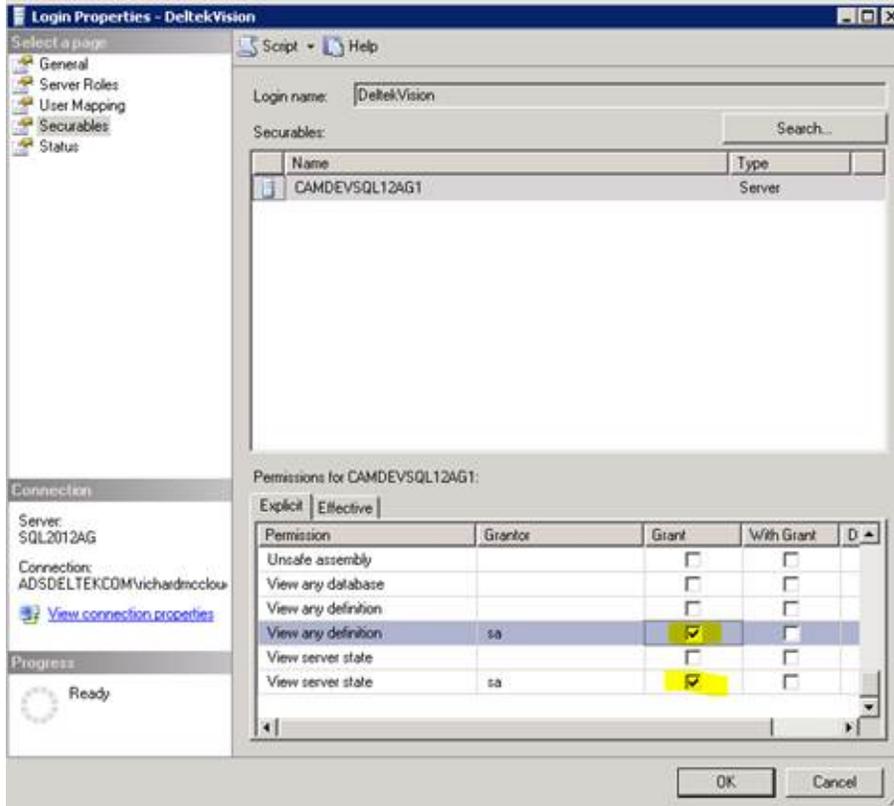
When you backup and restore a database to another server, the Login on Server A has a different SID (Security Identifier) than the same login on Server B. This issue is typically resolved using the sp_change_users_login stored procedure. However, since the database on the Secondary Replica will be in read only mode, you cannot fix the login.

You can resolve this issue by using the sp_help_revlogin stored procedure, which can be found in the following Microsoft Support article:

http://support.microsoft.com/kb/918992

Once the procedure is created in the master database, execute it to get the list of SQL Logins with their associated SID and the CREATE statement to create the login on the secondaries:

```
CREATE LOGIN [DeltekVision] WITH PASSWORD =
0x0200E0E05D60876CCE39BD9209515FB63C5589D6C939F3AB56A6CE9DBFBF49A9410F66F098408
27135F800725E25A77714FDFA31FB6C18BCB46561217947C3749F0380A18AF5 HASHED, SID =
0x0124F12258D9BD49BE649C2D7A6DA838, DEFAULT_DATABASE = [master], CHECK_POLICY =
OFF, CHECK_EXPIRATION = OFF
```

Run this CREATE statement on all secondary replicas prior to configuring the Availability Groups.

Create Availability Groups

You must create the Availability Group on each individual node.

To create the Availability Group, completet he following steps:

1. Open the SQL Server Configuration Manager.

2. On the SQL Service Properties page, enable the Availability Groups for each node. In this example, AGCLUSTER is the name of the WSFC cluster VIP, not the Availability Group VIP.
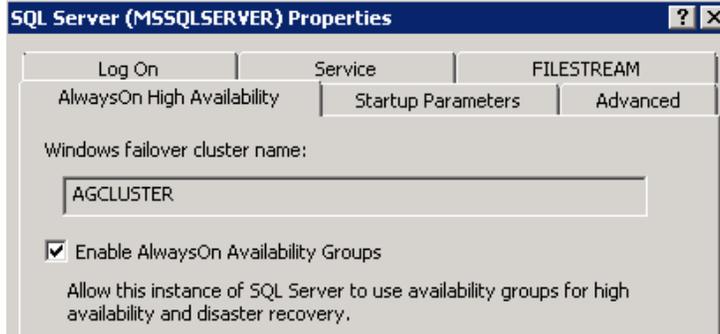
3. Select the databases to be included in the availability group (all of these databases will failover together if there is a failover).

4. Decide on the databases to be included in the availability group (all of these databases will failover together if there is a failover). At a minimum, include the Vision and Reporting Services databases (ReportServer and ReportServerTempDB).

   The database must be in FULL recovery mode and a FULL database backup must have been taken on the database prior to going through the Availability Group wizard.

   For more information of performing backups and restores of databases in FULL recovery model, refer to the following MSDN documentation:

   http://msdn.microsoft.com/en-us/library/ms187048(v=sql.105).aspx

5. In SMS, start the Availability Group Wizard.

6. Expand **AlwaysOn High Availability**, right-click **Availability Groups**, and click **New Availability Group Wizard** on the shortcut menu.
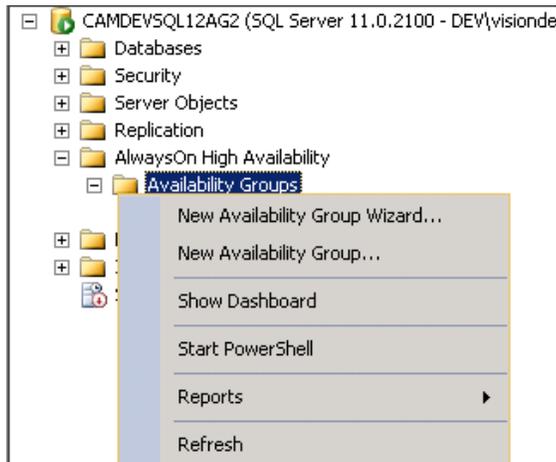
7. Select a name for the Availability Group.

   This is not the name clients will use to connect (VIP), but you can use the same name for the AG Listener which is the VIP. The name should be descriptive of the databases it includes (for example, VisionAG) because multiple Availability Groups can exist on the same servers.

8. Select the databases you want to be part of the Availability Group. The wizard will tell you whether or not they meet the requirements (for example, FULL recovery and FULL backup taken)

9. Specify the AG configuration (nodes, failover mode, and synchronization mode).

Refer to the following settings to complete the fields on this form:

Field	Setting
Server Instance	Four allowed
Initial Role	Primary or Secondary
Automatic Failover	Can only configure two nodes
Synchronous Commit — Synchronous versus asynchronous commit indentifies relative amount of data loss in the event of a failure versus the performance of the synchronization.	Can configure a maximum of three.
Readable Secondary — Sets the access rights for the Server Instance (for read-only reportingand so on).	**No** — Connections are not allowed to secondary replicas. **Yes** — Connections are allowed in read-only mode. **Read-intent only** — Connections using the **ApplicationIntent=ReadOnly** keyword are used for Read Only Routing.

> **Read-intent only** is used for the Read Only Routing feature of Availability Groups. This is described later in this document, and it defines the specific functionality supported by Vision.

10. Click the Endpoints tab. The Endpoint for each instance is created automatically.

Backup Preferences determine whether or not backups can be taken from the replicas other than the Primary (another feature of Availability Groups).

11. Click the Listener tab. You use this tab to create the AG Listener.

12. From the **Network Mode** drop-down list, select the type of listener: **Static IP** or **DHCP**. The port will be the same as the one used by the SQL Server port (default is 1433).

13. Click **Next**.

14. On the Data Synchronization Preference screen, enter the shared path or use the **Browse** button to select the location that all nodes/SQL service accounts can access. This determines how the databases are going to synchronize to the replicas.

Read Only Routing Configuration

Vision architecture changes have been specifically made to support the Read Only Routing feature. This feature allows certain report queries to be run against the read only copy of the Vision transaction database on a Secondary Replica of the Availability Group. The benefit of this feature is that it allows much of the Vision reporting workload to be offloaded from the database

on the Primary replica to the Secondary Replica, which frees resources for the transaction workload.

> For more information about Read Only Routing, read the following MSDN article:
>
> http://msdn.microsoft.com/en-us/library/hh710054(v=sql.110).aspx

- Read Only Routing requires that the connection string uses the **ApplicationIntent=ReadOnly** keyword. The Vision Reporting architecture has been specifically modified to allow for this change in the connection string when the database configuration specified in Weblink is configured to use Availability Groups.

- With this keyword and the proper configuration (queries below), the Availability Group will automatically route connections with this keyword to the read only secondaries configured for **Read-intent only**.

> A .NET 3.5 Sp1 Hotfix may be required on the Vision web/application servers. Refer to the following Microsoft KB article:
>
> http://support.microsoft.com/kb/2654347

- Even though you have configured the Availability Group for Read-intent onl" secondaries, there are manual queries required to configure the Read Only Routing aspect of the configuration.

Read Only Routing Queries

There are two queries required to modify the Availability Group configuration to support Read Only Routing:

- Configure the Read Only Routing URL
- Configure Read Only Routing lists

Configure Read Only Routing URL

Read Only Routing URLs are different than the Availability Group Endpoints, which were automatically configured earlier. In the Availability Group configuration above, there are two nodes, each configured to allow Read-intent only connections when that node is in secondary mode. (A node in Secondary mode is promoted to Primary when a failover occurs.)

- The following query identifies existing Read only routing URLs

```
select read_only_routing_url from sys.availability_replicas

Query Result:
read_only_routing_url
tcp://CAMDEVSQL12AG1:1433
tcp://CAMDEVSQL12AG2:1433
```

- The following blog post identifies a script that can be run against each replica to calculate the read-only routing URL:

http://blogs.msdn.com/b/mattn/archive/2012/04/25/calculating-read-only-routing-url-for-alwayson.aspx.

Example output from script is below:

```
Read-only-routing url script v.2012.1.24.1
```

```
This SQL Server instance version is [11.0.2100.60]
This SQL Server instance is a standard (not clustered) SQL Server
instance.
This SQL Server instance is enabled for AlwaysOn.
This SQL Server instance is NOT a Sql Azure instance.
This SQL Server instance DAC (dedicated admin) port is 1434
This SQL Server instance is listening to all IP addresses (default mode).
This SQL Server instance is listening on fixed tcp port(s) (it is not
configured for dynamic ports), this is a recommended configuration when
using read-only routing.
This SQL Server instance resides in domain 'dev.ads.deltek.com'
This SQL Server instance FQDN (Fully Qualified Domain Name) is
'CAMDEVSQL12AG1.dev.ads.deltek.com'
This SQL Server instance port is 1433
************************************************************************
The read_only_routing_url for this SQL Server instance is
'tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433'
************************************************************************
```

- The following statements configure the Read only routing URL for each node:

```
ALTER AVAILABILITY GROUP [SQL12AG1]
MODIFY REPLICA ON N'CAMDEVSQL12AG1' WITH
(SECONDARY_ROLE(READ_ONLY_ROUTING_URL=N'tcp://CAMDEVSQL12AG1.dev.ads.delt
ek.com:1433'))
ALTER AVAILABILITY GROUP [SQL12AG1]
MODIFY REPLICA ON N'CAMDEVSQL12AG2' WITH
(SECONDARY_ROLE(READ_ONLY_ROUTING_URL=N'tcp://CAMDEVSQL12AG2.dev.ads.delt
ek.com:1433'))
```

Where

- `[SQL12AG1]` is the name of the Availability Group (not the listener).

- `CAMDEVSQL12AG1` is the node 1 and `CAMDEVSQL12AG2` is node 2.

- `tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433` is the read only routing URL for node 1 and `tcp://CAMDEVSQL12AG1.dev.ads.deltek.com:1433` is the read only routing URL for node 2.

Configure Read Only Routing Lists

The Read Only Routing Lists provide a priority order for the routing of Read-intent only connections among nodes in the Availability Group configured for Read Only Routing

- The following query identifies existing Read Only Routing lists:

```
select g.name, r1.replica_server_name, l.routing_priority,
r2.replica_server_name, r2.read_only_routing_url
from sys.availability_read_only_routing_lists as l
join sys.availability_replicas as r1 on l.replica_id = r1.replica_id
join sys.availability_replicas as r2 on l.read_only_replica_id =
r2.replica_id
join sys.availability_groups as g on r1.group_id = g.group_id
```

```
Query Result:
```

name	replica_server_name	routing_	replica_server_name	read_only_routing_url

		priority		
SQL12AG1	CAMDEVSQL12AG2	1	CAMDEVSQL12AG1	tcp://CAMDEVSQL12AG1:1433
SQL12AG1	CAMDEVSQL12AG1	1	CAMDEVSQL12AG2	tcp://CAMDEVSQL12AG2:1433

- The following statements configure the Read Only Routing Lists for this configuration:

```
ALTER AVAILABILITY GROUP [SQL12AG1]
MODIFY REPLICA ON N'CAMDEVSQL12AG1' WITH (PRIMARY_ROLE
(READ_ONLY_ROUTING_LIST = (N'CAMDEVSQL12AG2',N'CAMDEVSQL12AG1')))

ALTER AVAILABILITY GROUP [SQL12AG1]
MODIFY REPLICA ON N'CAMDEVSQL12AG2' WITH (PRIMARY_ROLE
(READ_ONLY_ROUTING_LIST = (N'CAMDEVSQL12AG1',N'CAMDEVSQL12AG2')))
```

Where

- [SQL12AG1] is the name of the Availability Group (not the listener)

- CAMDEVSQL12AG1 is the node 1 and CAMDEVSQL12AG2 is node 2.

Monitoring Availability Groups

The following tools are available for monitoring the status of your Availability Group:

- Availability Group Dashboard

- System and Dynamic Management Views (DMV's)

- System Monitor (PerfMon)

- Windows Powershell

Availability Group Dashboard

To display the Availability Group Dashboard, complete the following the steps:

1. Launch SQL Server Management Studio and connect to the primary replica.

2. Right-click the Availability Group folder, and click **Show Dashboard** on the shortcut menu.

System and Dynamic Management Views (DMV's)

The following MSDN article provides a variety of System Views and DMV's that can be used to monitor the health and status of the WSFC and Availability Groups:

http://msdn.microsoft.com/en-us/library/ff878305.aspx

System Monitor (PerfMon)

There are a variety of System Monitor counters that can be used to monitor the performance of the Availability Groups. [Refer to the following for more information on the available counters and how to use them:

http://technet.microsoft.com/en-us/library/ff877954.aspx

Windows PowerShell

The following links are a four-part MSDN series on using PowerShell to monitor Availability Groups:

- http://blogs.msdn.com/b/sqlalwayson/archive/2012/02/13/monitoring-alwayson-health-with-powershell-part-1.aspx

- http://blogs.msdn.com/b/sqlalwayson/archive/2012/02/13/monitoring-alwayson-health-with-powershell-part-2.aspx

- http://blogs.msdn.com/b/sqlalwayson/archive/2012/02/13/monitoring-alwayson-health-with-powershell-part-3.aspx

- http://blogs.msdn.com/b/sqlalwayson/archive/2012/02/15/the-always-on-health-model-part-4.aspx

Flexible Failover Policy

The Failover feature of Availability Groups is controlled using the Failover Policy. For more Information on this feature, read the following:

http://msdn.microsoft.com/en-us/library/hh710061(v=sql.110).aspx

Failover Condition Level and Health Check Timeout

Transact-SQL Value	Level	Automatic Failover Initiated When…
1	One	On server down. The SQL Server service stops because of a failover or restart.
2	Two	On server unresponsive. Any condition of lower value is satisfied, the SQL Server service is connected to the cluster and the health check timeout threshold is exceeded, or the current primary replica is in a failed state. This is the default level.
3	Three	On critical server error. Any condition of lower value is satisfied or an internal critical server error occurs.
4	Four	On moderate server error. Any condition of lower value is satisfied or a moderate Server error occurs.
5	Five	On any qualified failure conditions. Any condition of lower value is satisfied or a qualifying failure condition occurs.

- Failover condition is determined by WSFC executing sp_server_diagnositcs at regular intervals

- The following query identifies the existing Failover Policy:

```
select name,failure_condition_level,health_check_timeout from
sys.availability_groups
```

```
Query Result:
```

name	failure_condition_level	health_check_timeout
SQL12AG1	3	30000

- The following statements configure the Failover Policy for this configuration:

```
ALTER AVAILABILITY GROUP AG1 SET (FAILURE_CONDITION_LEVEL = 1); //default
is 3
ALTER AVAILABILITY GROUP AG1 SET (HEALTH_CHECK_TIMEOUT = 60000);
//default is 30000
```

Configure Vision and Reporting Services to Use Availability Group Listener

For the final steps to configure Vision and Reporting Services to correctly use the Read Only Routing feature in Availability Group configuration, you must configure the following to use the Availability listener:

- Report Server Configuration Tool to configure Reporting Services
- Weblink utility for your Vision database

Configure Vision for Availability Groups

To configure Vision to use the Availability Group configured in the preceding sections, complete the following steps:

1. Launch the Weblink utility, and select your Vision transaction database that is part of the Availability Group.

   When you select your Vision database, Weblink issues a query to identify the Availability Group that Vision is part of. It also selects the **Use Availability Group** option and populates the name of the **Availability Group** (this is not the listener name).

> It is important to note that although you are modifying the server connection information for the Vision database, the Vision FILESTREAM database (if applicable), and the Reporting Services database to use the Availability Group listener, this only ensures that these connects can still connect to the new Primary node in the event of a failover.
>
> The only features that use the Vision database on the Secondary (Read Only) Replica are the database queries for the specific reports outlined earlier in this document. This includes reports in the Reporting Applications menu (minus purchasing reports) and the Dashboard reports.

2. In order to use Availability Groups, complete the following:

   a. Select the **Use Availability Groups** option.

   b. Change the **SQL Server** name to be the Availability Group listener name.

   c. If using FILESTREAM and the FILESTREAM database is part of the Availability Group (which it should be if located on the same SQL Server as Vision), confirm that the **FILESTREAM SQL Server** is using the Availability Group listener name.

   d. On the Report Server tab, confirm that the Server Name specified in the Report Server Database Access is using the Availability Group listener name.

Configure Reporting Services to Use the Availability Group Listener

If Reporting Services has not yet been configured, follow the steps in the *Deltek Vision Technical Administration Guide* to configure Reporting Services. When entering in the Database Server name to use for the Report Server databases, use the Availability Group Listener.

If Reporting Services is already configured to use the Primary Node server name, you must complete the following:

1. Open the Reporting Services Configuration Manager.

2. Select the Database menu.

3. Click the **Change Database** button.

4. Select the **Choose an existing report server database** option, and click **Next**.

5. On the **Connect to the Database Server** screen, change the **Server Name** to be the Availability Group listener, and click **Next**.
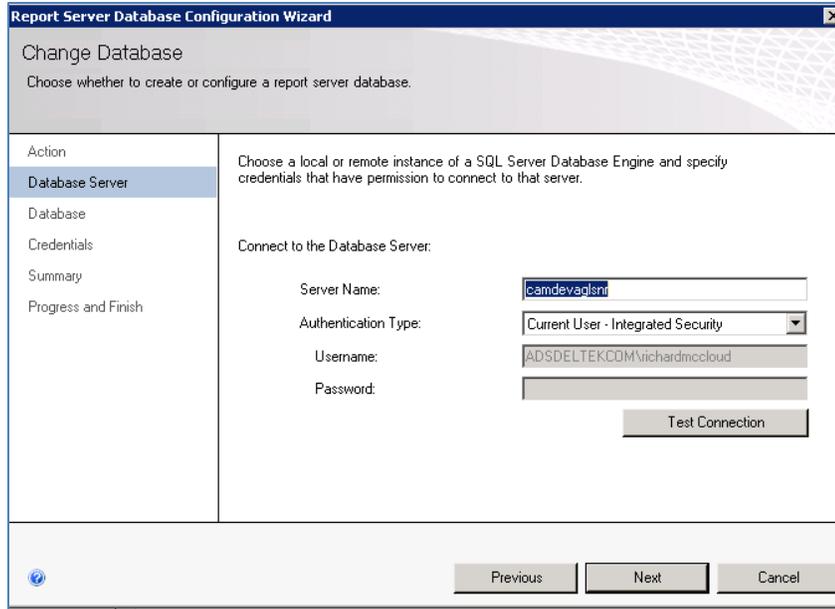
6. Select the existing ReportServer database from the drop-down list and click **Next** to complete the re-configuration.

Troubleshooting

Issue:

If the **Use Availability Groups** check box does not display for your Vision database when selected in Weblink, execute the following query to see if it returns anything:

```
SELECT e.name, s.database_name
FROM sys.availability_groups_cluster AS e
 INNER JOIN sys.availability_databases_cluster AS s
 ON e.group_id = s.group_id
```

It should return a result set similar to the following.

Issue:

When using Availability Groups, a system health check query is run to determine the health of the Availability Group. If the result of this query returns 0 or 1 (as indicated in the table below), then the system will fall back to running all reports against the Primary Replica and the Read Only Routing will effectively be disabled.

select synchronization_health from sys.dm_hadr_availability_group_states

Synchronization Health

Value	Description
0	Not healthy. None of the availability replicas have a healthy **synchronization_health** (2 = HEALTHY).
1	Partially healthy. The synchronization health of some, but not all, availability replicas is healthy.
2	Healthy. The synchronization health of every availability replica is healthy.

Deltek is the leading global provider of enterprise software and information solutions for professional services firms, government contractors, and government agencies. For decades, we have delivered actionable insight that empowers our customers to unlock their business potential. Over 14,000 organizations and 1.8 million users in approximately 80 countries around the world rely on Deltek to research and identify opportunities, win new business, optimize resource, streamline operations, and deliver more profitable projects. Deltek – Know more. Do more.®

deltek.com

Deltek Know more. Do more.™