Deltek

Deltek PM Compass 8.5

Advanced Administration Guide

May 16, 2025

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.

This edition published May 2025.

Contents

Overview 1
Secure your PM Compass Deployment 2
Configure HTTP Compression 50
Smart Client ClickOnce Deployment Options 54
Load Balancing 58
Configure Database Session State for PM Compass 61
Configure SQL Server Resource Governor to Manage PM Compass Workloads 64
Monitor Report Server Usage 72
Reporting Services Logging 75
Configure a Shared Location for Databases.enc 78

Overview

This guide is a supplement to the *Deltek PM Compass Installation Guide*. It provides additional insight into advanced administration topics for your Deltek application. The topics covered are for advanced deployments and may not be applicable to all installations of PM Compass.

The topics are outside the bounds of the Deltek Customer Success Agreement and are therefore **not** covered by your Support Contract. Contact Deltek Consulting Services Group for assistance with the implementation of this material for your specific environment.

Secure your PM Compass Deployment

Security is a critical part of any application. Applications must be secured against disclosure of confidential information, modification, destruction of data, misappropriation of resources, and compromise of accountability.

This topic includes some necessary steps that Deltek recommends for securing your PM Compass deployment.

If you are implementing PM Compass with any other application or product, Deltek recommends that you review the security best practices for those products as well.

Warning: Most of the steps in this topic require administrative rights on your servers, so be sure to log in with the proper account. Do not log in using the **DeltekPMCompass** local account because you will be deleting or disabling this account on all PM Compass servers.

Securing Client Access

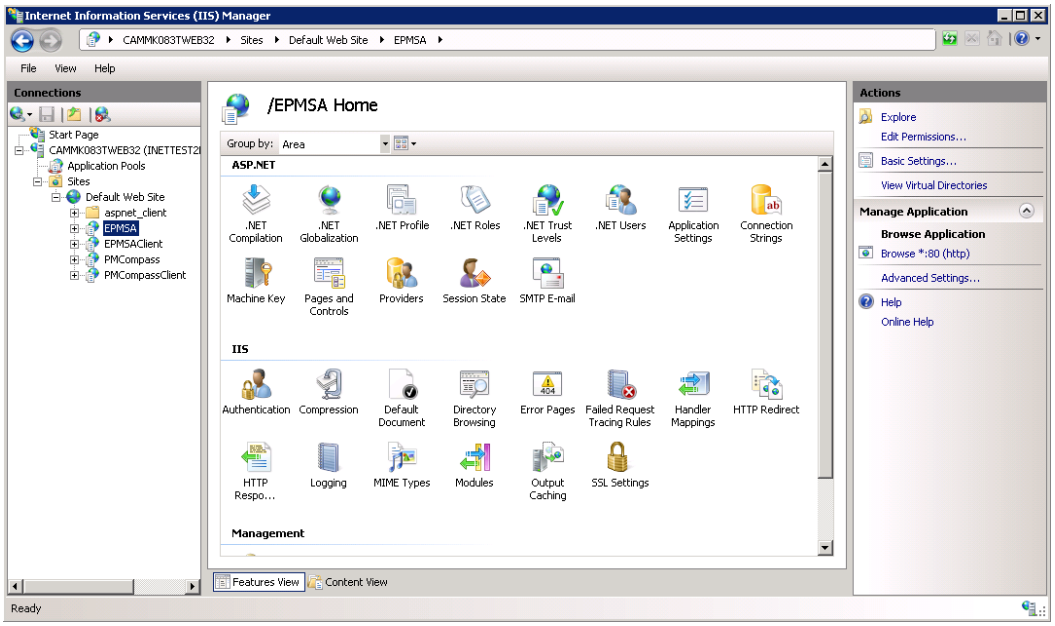
Configure the EPM SA and PMCompass IIS Applications to Use Windows Authentication

Warning: Do **not** modify the security settings for the EMPSAClient and PMCompassClient IIS applications. These applications represent the ClickOnce deployment and must use Anonymous Access.

To configure the EPM SA and PMCompass IIS applications to use Windows Integrated Authentication:

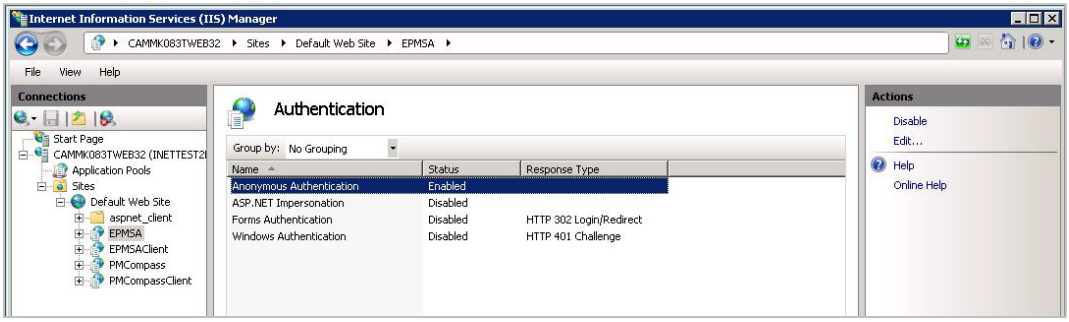
1. From within Internet Information Services (IIS), expand the web site where the EPM SA and PM Compass applications are installed.

2. In the Connections pane, select **EPMSA**.

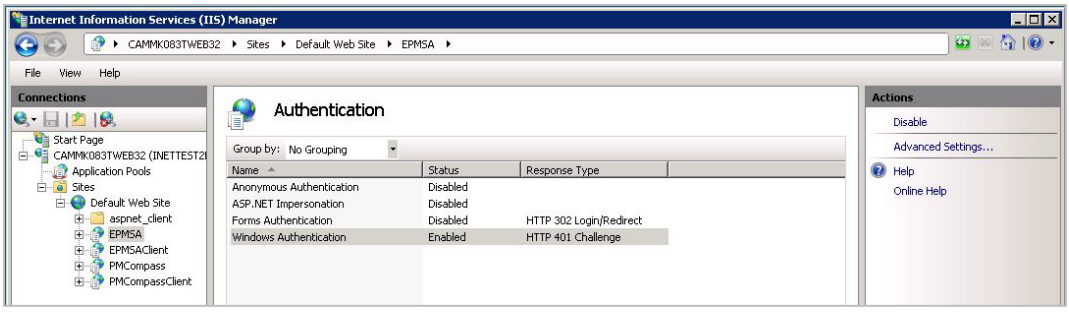


3. In the right pane of the Internet Information Services (IIS) Manager window, double-click **Authentication**.

4. In the Authentication pane, select **Anonymous Authentication** and click **Disabled** in the Actions pane.

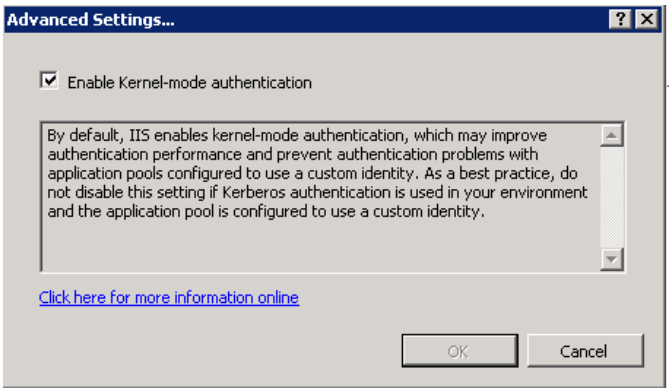


5. Select **Widows Authentication** and select **Enabled** in the Actions pane.



6. With **Windows Authentication** still selected, click **Advanced Settings** in the Actions pane.

7. On the Advanced Settings dialog box, confirm that the **Enable Kernel-mode authentication** option is selected then click **Cancel**.



> **Note:** Disabling Kernel Mode Authentication requires the creation of a Service Principal Name (SPN) for the Application Pool Identity. See Creating a Service Principal Name (SPN) for more information.

8. To configure the PMCompass IIS application to use Windows Integrated authentication, select **PMCompass** in the Connections pane and repeat steps 1-7 in this procedure.
9. Launch the EPM Security Administration and PM Compass applications.
10. On the EPM Security Administrator and Deltek PM Compass Login dialog boxes, you should see the **Windows Authentication** option selected.

    The **Windows Authentication** check box displays only if you have multiple databases configured in Weblink. If you have only one database, you are automatically logged onto PM Compass and the Login dialog box does not display.

Enable Windows Authentication in EPM SA and PM Compass

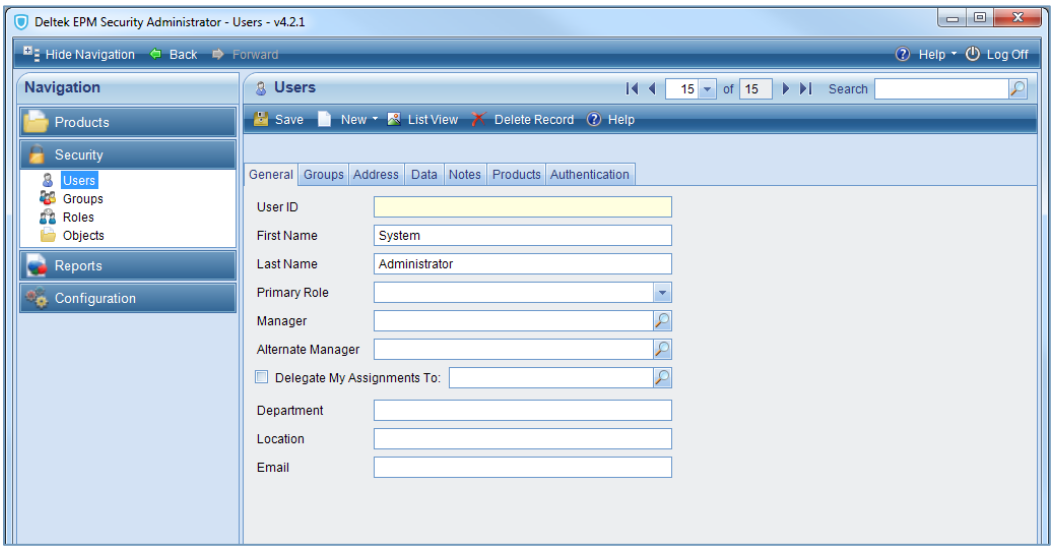
PM Compass supports Windows Integrated Security, which allows users to log in one time for both Windows and the PM Compass application. Integrated Security logs a user into PM Compass based on the user's Windows domain network login. If a user is not logged into the company network, the user will be prompted for a network ID and password before he or she can log in to PM Compass.

After the servers have been configured to support Windows Integrated Authentication, you must configure the logon accounts of your domain users within the EPM SA application.

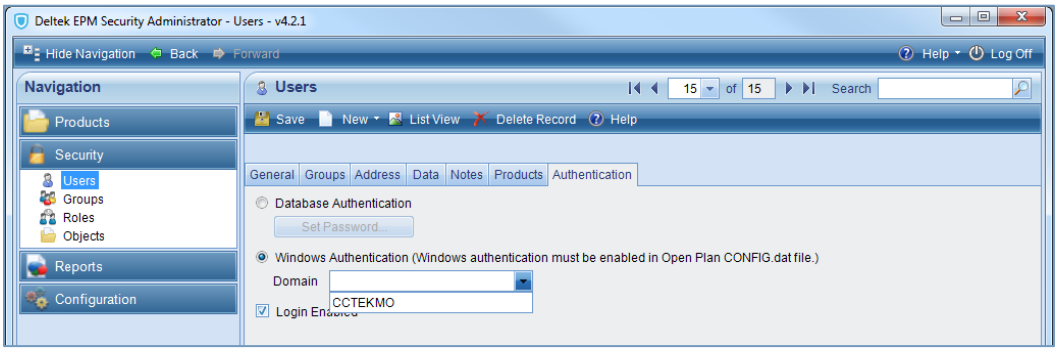
To configure a domain logon account for PM Compass:

1. Launch the EPM SA application (**http://<webserver>/epmsa**) and log on as a user with the appropriate security rights.

2. Click **Security » Users**, and then create a new user in the **Users** pane.
    a. Enter the domain user name of the user you are creating. This is the logon ID used by the user to log on to the Windows domain.
    b. Complete the information in the **Users** pane as required for this user.

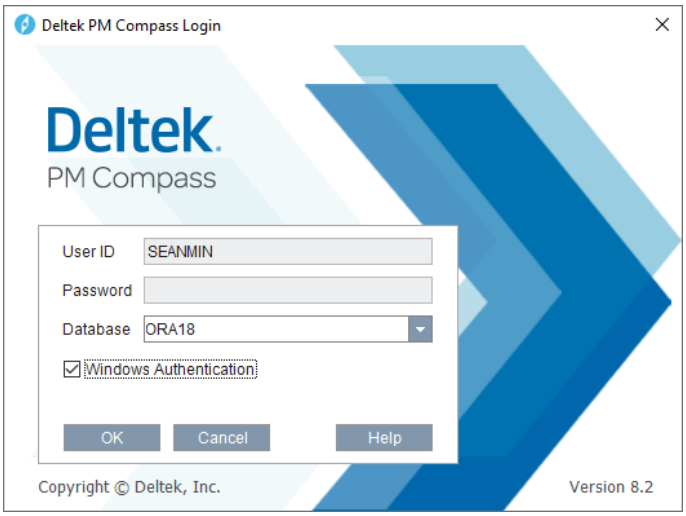


3. Click the Authentication tab, select the **Windows Authentication** option, and then select the domain for this user from the **Domain** drop-down list.



4. Save your changes.

5. When the user launches PM Compass or the EPM Security Administrator, the Login dialog box displays, showing the **Windows Authentication** option. Selecting this option populates the **User ID** field with their user name.

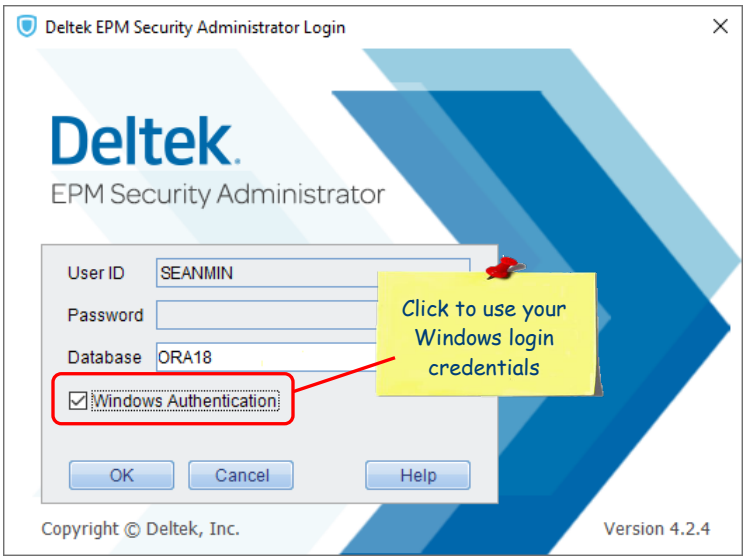


> **Warning:** When configured for Windows Integrated Authentication, the **Windows Authentication** check box is selected by default. The **Windows Authentication** check box displays only if you have multiple databases configured in Weblink. If you have only one database, you are automatically logged into PM Compass and the Login dialog box does not display.

6. If the user has been configured for Windows Integrated Authentication, they can click **Log In** to log on to the application. If not, they must clear the **Windows Authentication** check box and enter a valid PM Compass User ID and password.

Configure EPM Security Administrator and PM Compass to use Windows Authentication for Database Connections

When you enable Windows Authentication, the system uses the credentials that you used to log into Windows to access EPM SA and PM Compass. You must enable Windows Authentication on both the Web Server and in EPM SA.



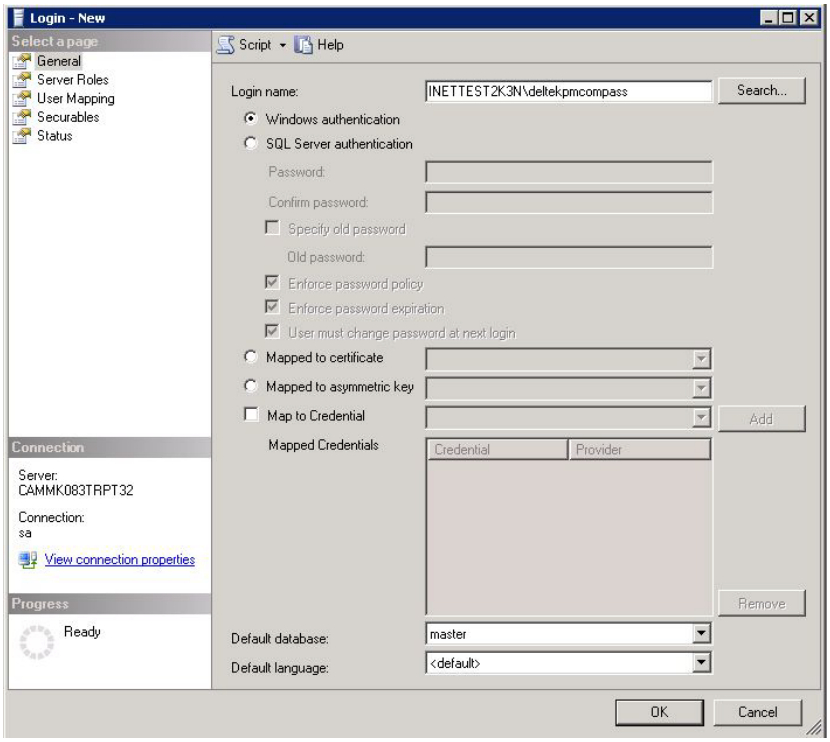
The first step toward using Windows Integrated Authentication for the database connections of the EPM Security Administrator and PM Compass is to grant the domain user account, which serves as the Application Pool Identity, the appropriate rights to the PM Compass database as well as to the Report Server and Session State databases (if needed).

Note: Oracle Servers — Windows Integrated Authentication for Oracle database connections is not supported in PM Compass.

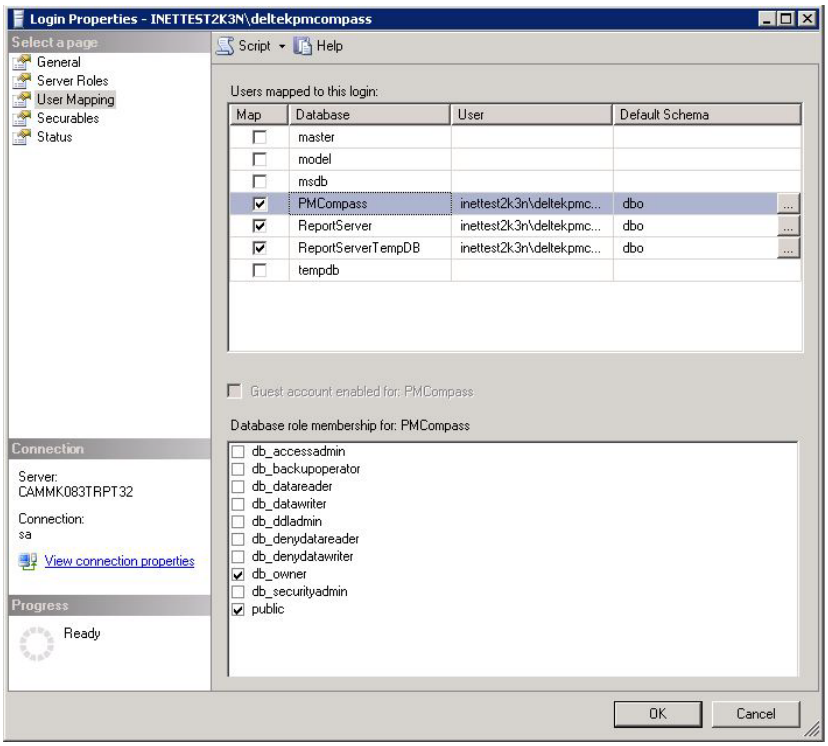
To configure the EPM Security Administrator and PM Compass to use Windows Integrated Authentication for database connections on SQL servers:

1. Identify the domain user account used as the Application Pool Identity in IIS. See Configuring the Application Pool Identity to be a Domain Account for more information.

2. In SQL Server Enterprise Manager, create an SQL logon account for this domain user account.



3. On the Login Properties dialog box, click **User Mapping** and grant the user **db_owner** rights to the PM Compass database as well as to the Report Server and Session State databases (if needed).



The SYSADMIN Account and Group in EPM Security Administrator

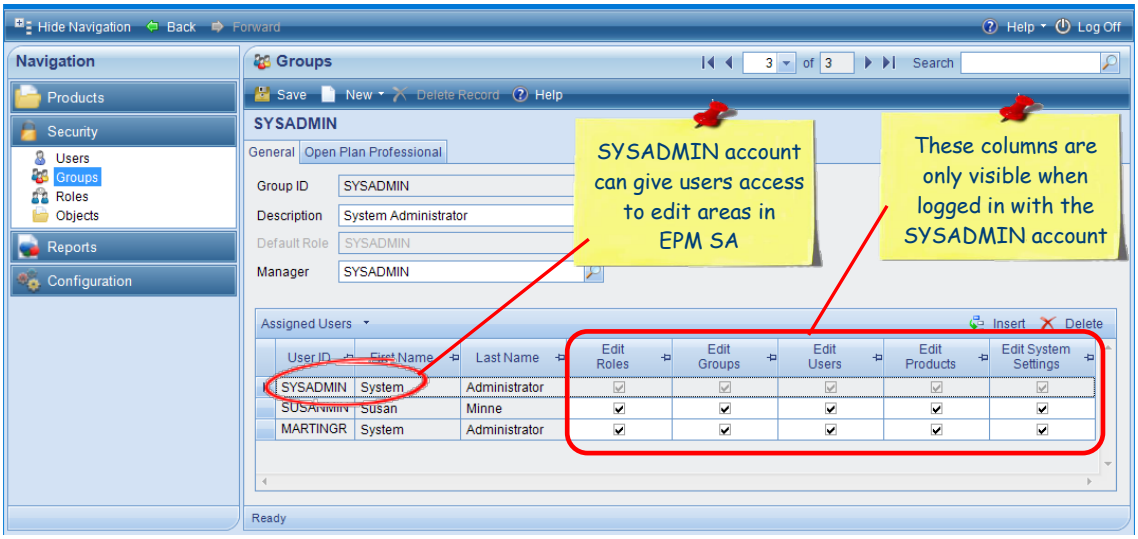
The Deltek EPM Security Administrator (EPM SA) allows you to define the security rights for Deltek Project Portfolio Management (PPM) applications. The EPM SA is installed when you install PM Compass.

In order to secure PM Compass, you should change your SYSADMIN account password and configure the users to log in using Windows Authentication.

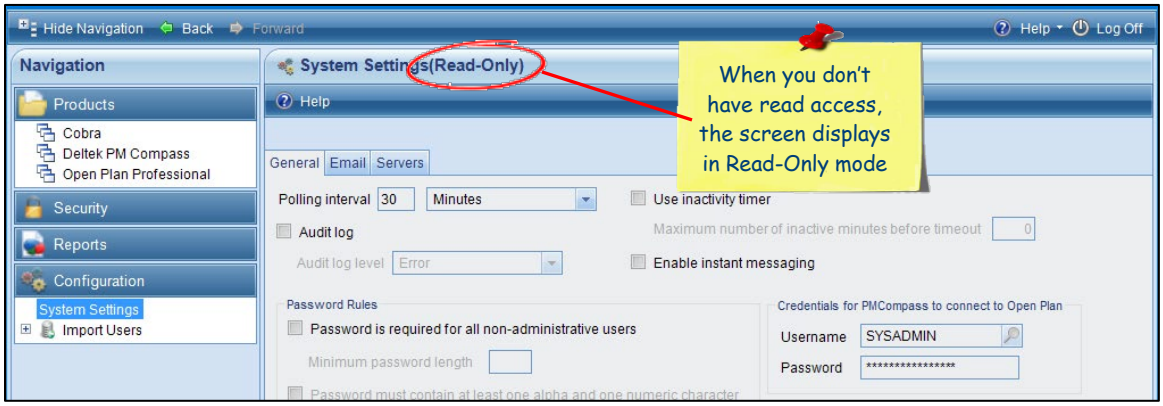
By default, in EPM SA, PM Compass creates a SYSADMIN account that is a member of the built-in SYSADMIN group. Only users who are assigned to this group can log into EPM SA. The SYSADMIN account and group cannot be deleted.

> **Note:** If you make a copy of the SYSADMIN group and add users, those users will not have access to EPM SA unless they are also added to the built-in SYSADMIN group.

The SYSADMIN account is the only User ID that can give other users access to edit EPM SA roles, groups, users, products, and system settings. None of the other users named in the Assigned Users grid have this ability and those columns in the grid are not visible to other users.



When a user who is part of the SYSADMIN group logs in to EPM SA with their own login / User ID, they have access to all of the features assigned to them by the SYSADMIN user. The areas to which they don't have edit rights display as **Read Only**.



Change the SYSADMIN Account Password

Security best practices recommend that you add users with Administrator-level access to the SYSADMIN group, change the SYSADMIN password, and then minimize use of the SYSADMIN account.

This encourages users to login using their own account instead of the built-in SYSADMIN account for better accountability.

To change the SYSADMIN password from the default "password":

1. Login to Deltek EPM Security Administrator.
2. On the Navigation menu, click **Security » Users**.
3. Use the navigation arrows or the Search field to locate the SYSADMIN account.
4. On the Authentication tab, click **Set Password**.
5. On the Set Password dialog box, enter a new password and confirm it.
6. Click **OK**.

The new password takes effect the next time you log into EPM Security Administrator.

Prevent Users from Logging into PM Compass using the SYSADMIN Credentials

There are two ways you can log in to the application — you can specify a username and password or you can log in using Windows Authentication where the application uses the domain credentials. If you want to limit users' ability to log in with credentials other than their own, you can enable Windows Authentication and not use the username and password option.

The default configuration for the SYSADMIN account is to login using the username and password. This account is a super-account and usage should be restricted. To prevent users from logging in to PM Compass using the SYSADMIN credentials, you can do the following:

- Create a SYSADMIN domain account and set the SYSADMIN account to Windows Authentication in EPM SA.
- Disable the PM Compass SYSADMIN account login.

See below for more information about both of these options.

Create a SYSADMIN domain account and set the SYSADMIN account to Windows Authentication in EPM SA

Create a Windows domain account for the SYSADMIN built-in account. When creating the domain account, the login must be in the format of SYSADMIN@domainname.com. The prefix (the wording before the "@domainname.com") and the User ID in EPM SA must match. That is, both should be **SYSADMIN**. When you create this account in Active Directory, it doesn't have to be a member of the Administrators group, it can be a regular user.

Setting up the SYSADMIN account as a Domain account satisfies SOX compliance requirements since a Domain Account password supports password complexity.

After creating the account, launch EPM SA, select the SYSADMIN built-in account, and set it to use **Windows Authentication**.

In order for the user to login using the SYSADMIN account, they have to logoff of their machine and log back in using the domain SYSADMIN account first and only then could they log into PM Compass with that account.

Disable the PM Compass SYSADMIN Account Login

To disable the SYSADMIN account for PM Compass login:

1. In EPM SA, click **Security » Users**.
2. Navigate to the SYSADMIN account.
3. On the Authentication tab, deselect **Login Enabled**.
4. Click **Save**.

When the **Login Enabled** option is deselected, the user cannot enter **SYSADMIN** / **<Password>** to log into PM Compass.

> **Note:** This does not affect access to EPM SA. To prevent users from accessing EPM SA using the SYSADMIN credentials, change the SYSADMIN password.

Configure Secure Sockets Layer (SSL)

Secure the PM Compass Web Server

To configure PM Compass for use with SSL, you must generate and acquire an SSL certificate from one of the following:

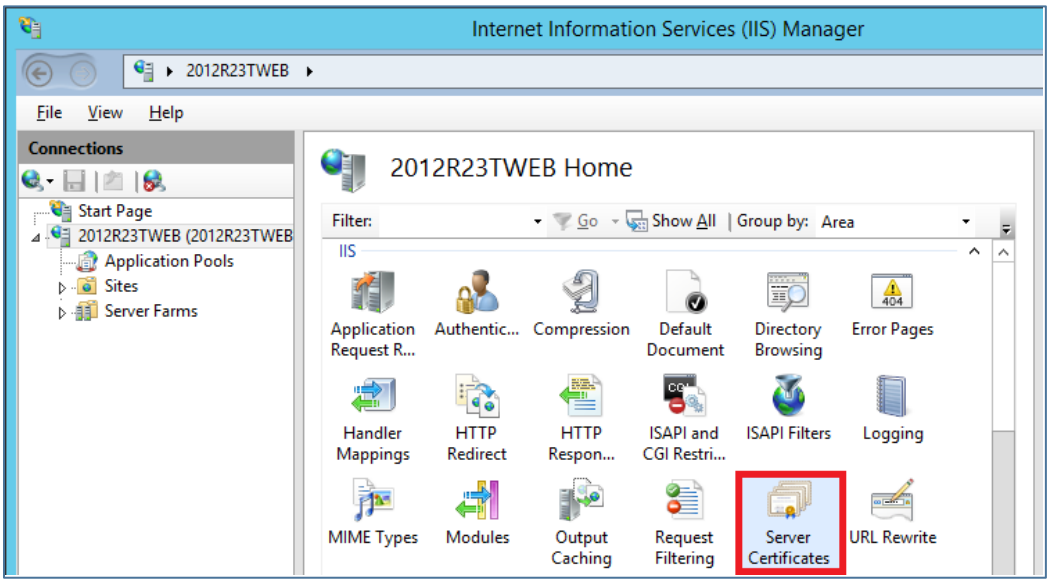
- Obtain an SSL certificate from an online certificate authority such as VeriSign, Thawte, or Comodo
- Have access to a domain or stand-alone certificate authority on your network

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

To secure the PM Compass web server:

1. Log on to the web server.
2. Click **Administrative Tools** » **Internet Information Services Manager**.
3. On the navigation pane on the left, select your server navigation menu.

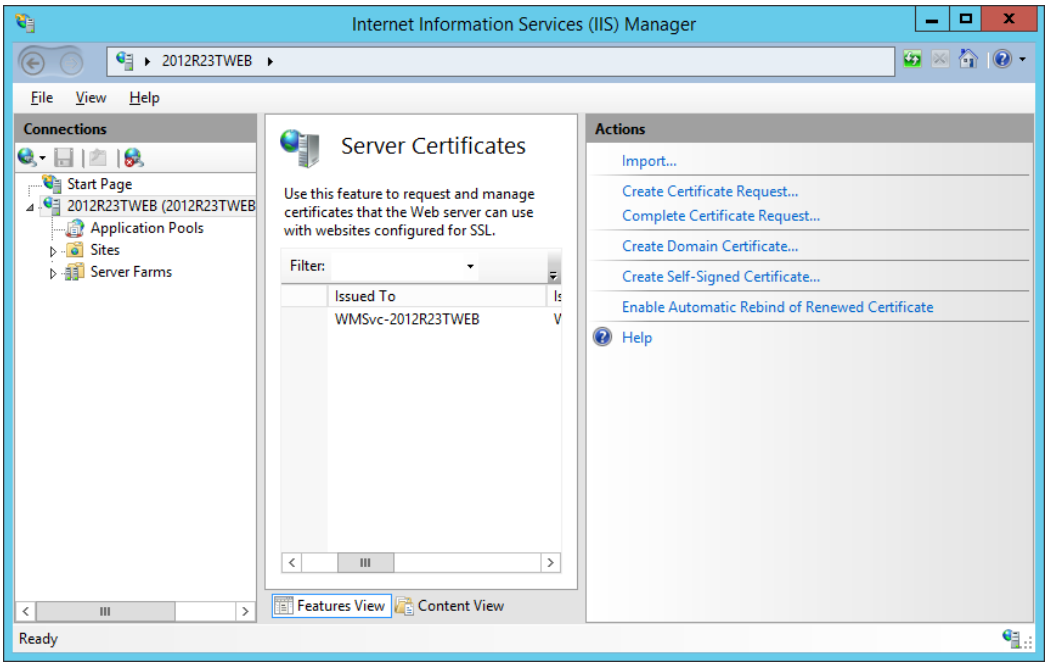
4. Double-click **Server Certificates**.



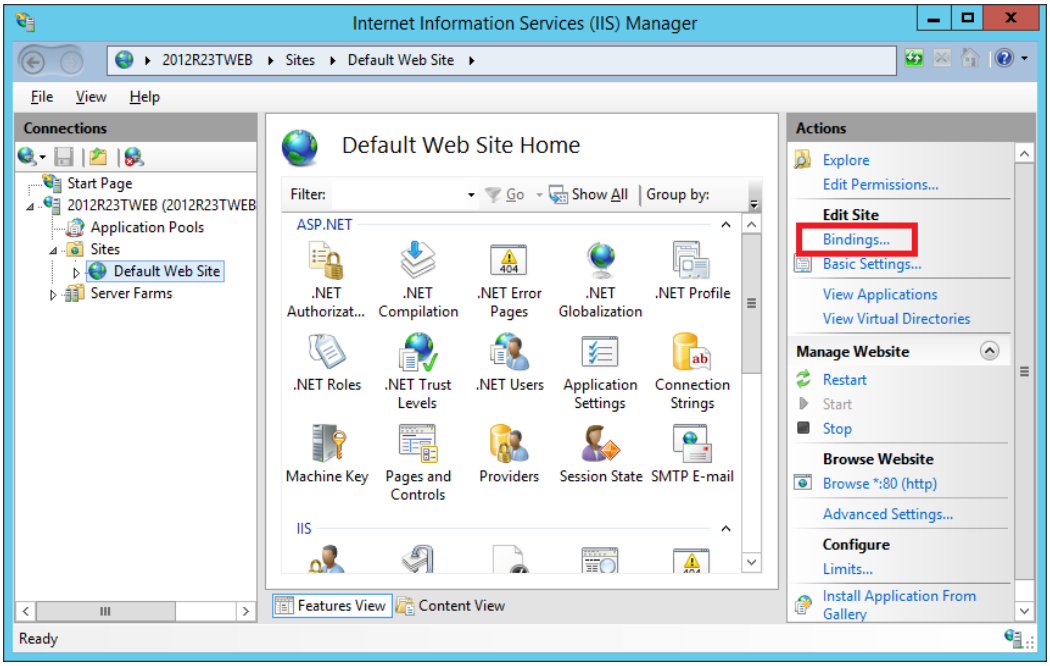
5. In the Server Certificate window Actions pane, select one of the following options:

   - **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) in order 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 Certificate Authority 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 in a non-production environment.

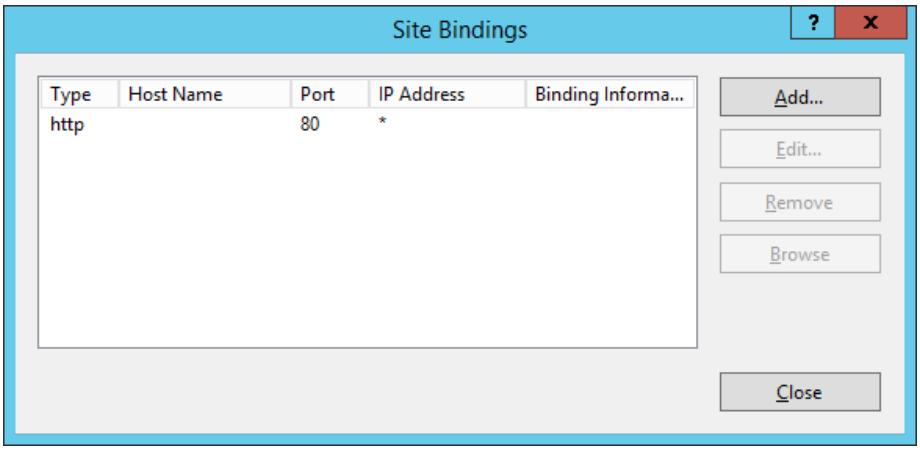
   After you obtain and import your SSL Certificate, you create an SSL binding for your web server.



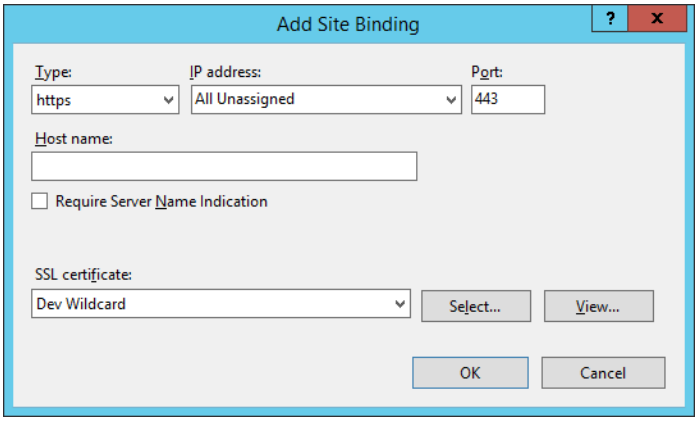
6. In the Connections pane, expand **Sites**, and select your web site.
7. In the Actions pane, click **Bindings**.



8. In the Site Bindings dialog box, click the **Add** button.



9. Complete the following in the Add Site Binding dialog box:
    a. In the **Type** field, select **https**. The **Port** field value automatically changes to **443**.
    b. In the **IP address** field, select your IP address or use the default setting **All Unassigned**.
    c. In the **SSL Certificate** field, select your certificate.
    d. 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 works correctly. After you have confirmed the https:// binding on port 443, remove the unencrypted binding running on port 80 and restart the Web server.

Update the PM Compass Application Server URL Definition with HTTPS

If you have configured your Web Server for SSL, you will need to complete two steps:

- Update the application URL defined in PM Compass
- Update the Open Plan Application Setting

Update the Application URL Defined in PM Compass

The application URL in the PM Compass Settings on the General tab here must be used to configure the Open Plan application setting for _PMCWEBSERVICEURL. In addition, you should access PM Compass using the same URL from a browser. For example: http://<pmcwebservername>/pmcompass. You can find the _PMCWEBSERVICEURL setting in Open Plan by clicking File » Preferences » Application, selecting the Advanced tab, and clicking Defaults.

Update the Open Plan Application Setting.

The **http** or **https** in the **_PMCWEBSERVICEURL** value must match the "**http**" or "**https**" option selected when you install the Open Plan Add-in on the Open Plan client machines. If they do not match, errors will occur when you launch the Open Plan Add-in. For example, if you specified that **http** is used to access PM Compass during the Open Plan Add-in installation, but the value of the **_PMCWEBSERVICEURL** starts with **https**, when you launch the Open Plan Add-in, you will encounter an error similar to the following: "A critical error occurred logging into the PM Compass Web Service. The provided URL scheme "http" is invalid; expected "https."

To add the PM Compass application server address to the Open Plan database:

1. Log into Open Plan as a member of the SYSADMIN group, or as the user **SYSADMIN**.
2. Click the Open Plan product icon in the top left corner and click **Preferences » Application** to display the Application Preferences dialog box.
3. On the Advanced tab, click **Defaults** to display the System Preferences Defaults dialog box.
4. Scroll down and look for the category titled **_PMCWEBSERVICEURL**.

   If this category does not exist, add it in the first blank row.
5. In the **Default Value** field, enter the PM Compass application server address.

   For example: **http://<pmcwebservername>/pmcompass** where **<pmcwebservername>** is replaced with the PM Compass Process Server name.

   The application URL on the PM Compass System Settings General tab must be used in this field.
6. Click **OK** to save your changes.

Secure SQL Server Reporting Services

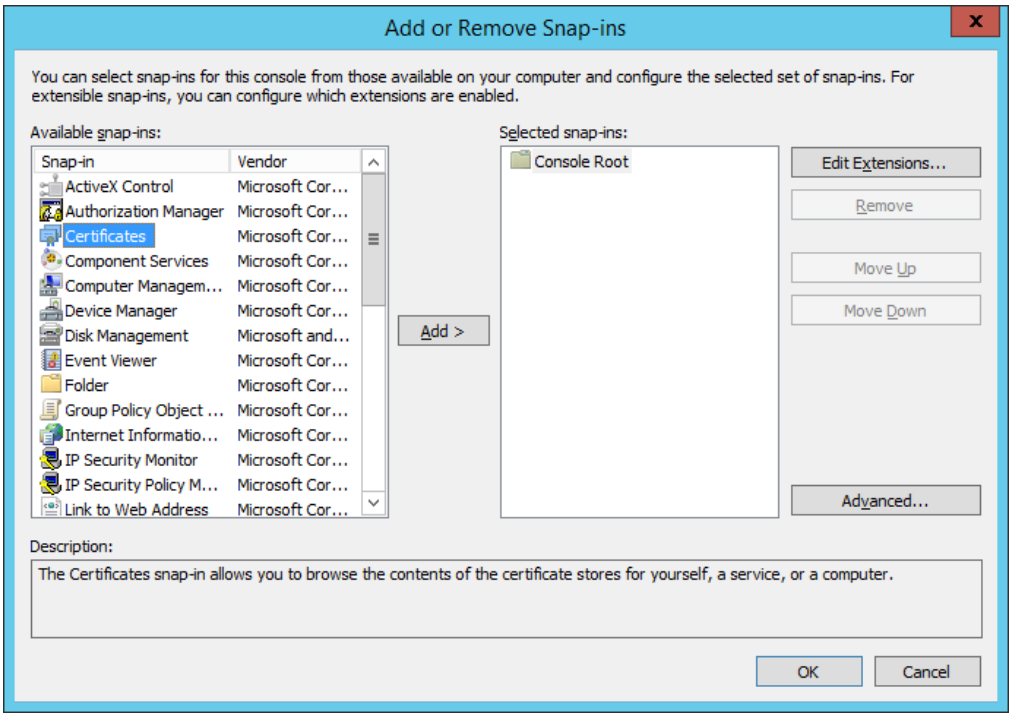
Configuring Reporting Services for SSL is slightly more involved than IIS. The Reporting Services Configuration Manager does not directly support the requesting and importing of the SSL certificate, as IIS does. To request and import the SSL Certificate on your Reporting Services server, you must use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

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

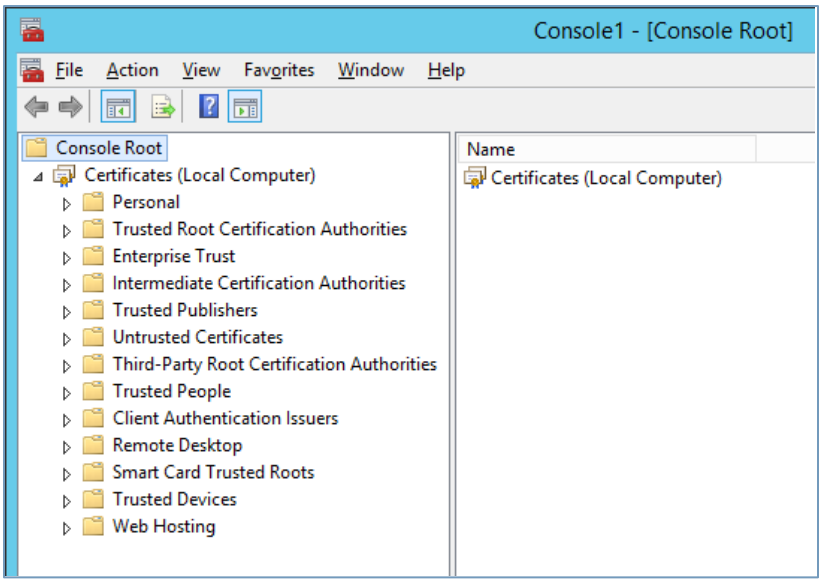
- You cannot run SSL for PM Compass without an SSL binding configured for Reporting Services.
- You cannot run PM Compass without SSL and still use SSL for Reporting Services.
- The Reporting Services web service URL in Weblink must reference the **Fully Qualified Domain Name** (FQDN) of the report server. 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)://pmcompass.companyname.com/reportserver.
- Wildcard certificates are not acceptable.

To secure SQL Server Reporting Services for PM Compass:

1. Click **Start » Run**.
2. In the **Open** field on the Run dialog box, enter **mmc,** and click **OK**.
3. On the MMC console, click **File » Add/Remove Snap-in**.
4. On the Add or Remove Snap-ins dialog box, select **Certificates** then click **Add**.

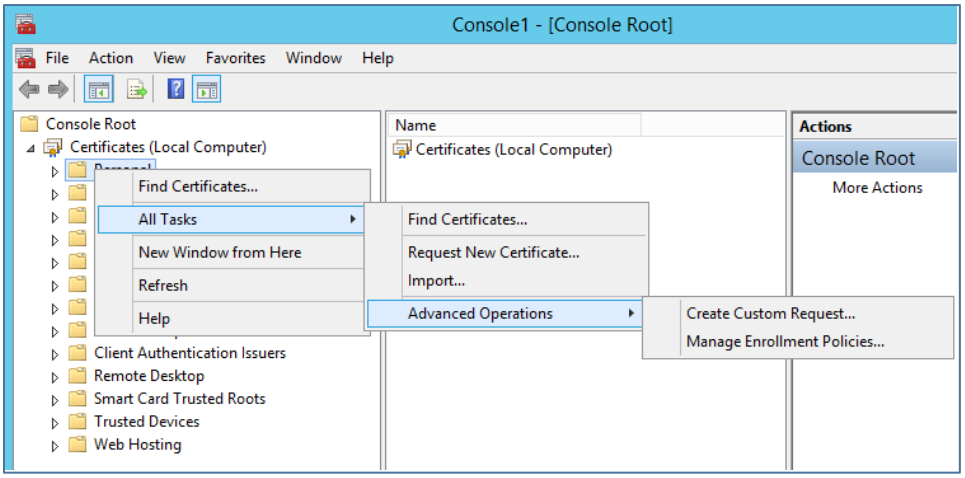


5. Select **Computer account** and click **Next**.
6. Select **Local Computer**.
7. Click **Finish**, and then click **OK**. You should now see the certificate store, as shown below.



Next, you need to request a new certificate or import an existing certificate.

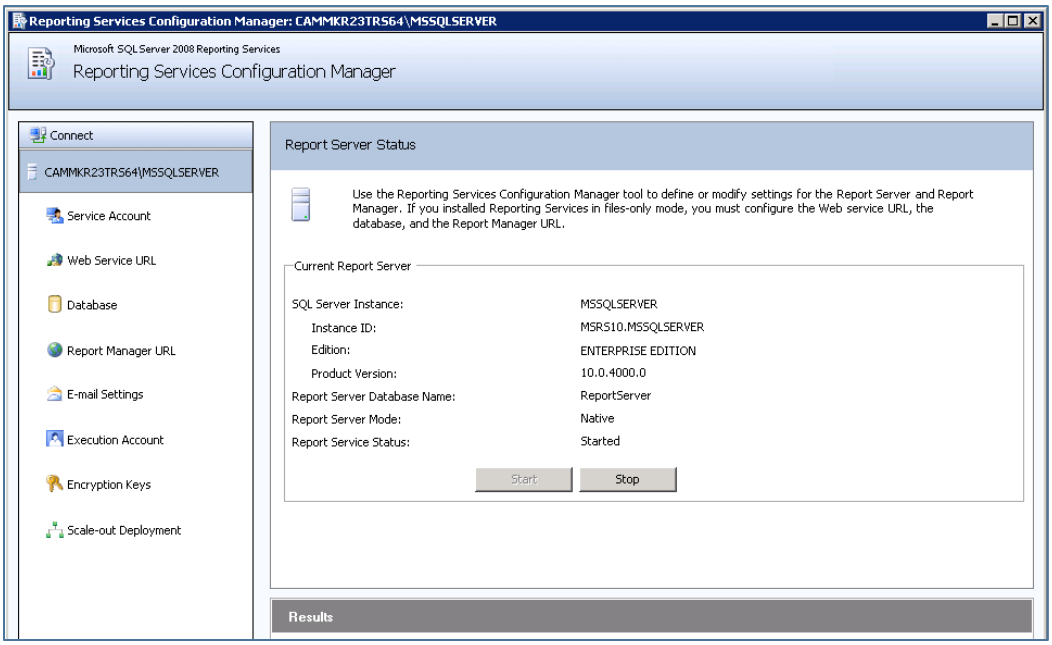
8. Right-click the **Personal** folder, and click **All Tasks** on the shortcut menu.



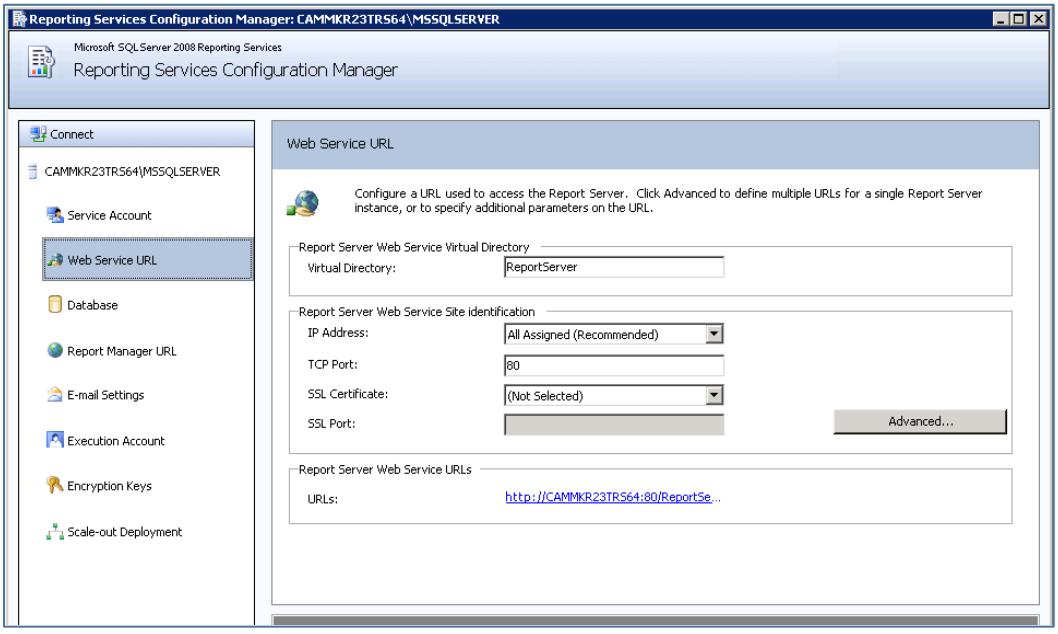
9. Take one of the following actions:
   - If you have a domain Certificate Authority (CA), click **Request New Certificate**.
   - If you need to request a certificate from a stand-alone CA or an online CA, click **Advanced Operations** and then click **Create Custom Request**.
10. After you have your SSL certificate, import it using the following steps:
    a. Right-click the **Personal** store folder, click **All tasks**, and click **Import**.
    b. On the Certificate Import Wizard, browse to the location of your SSL certificate and complete the import process.

The certificate is now registered with the server, but it still needs to be registered with SQL Reporting Services.

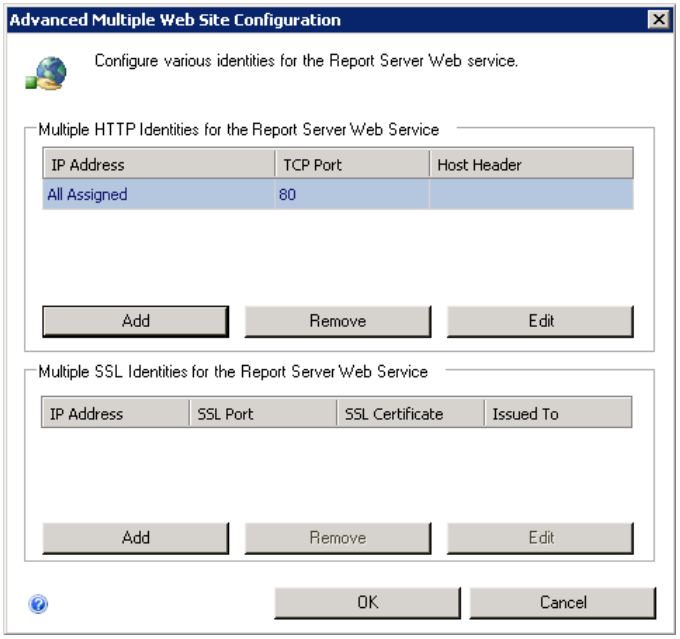
11. Click **Start » All Programs » Microsoft SQL Server » Configuration Tools** to open the Reporting Services Configuration Manager on the report server.



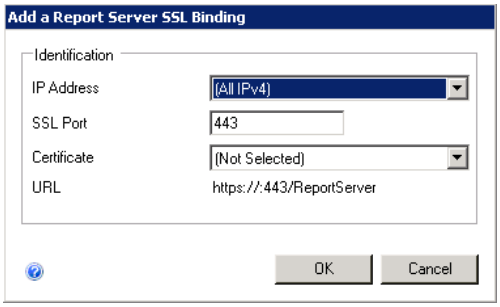
12. In the **Connect** pane, click **Web Service URL** to display the Web Service URL window.



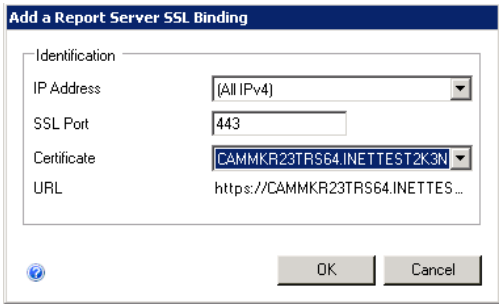
13. Click the **Advanced** button to display the Advanced Multiple Web Site Configuration dialog box.



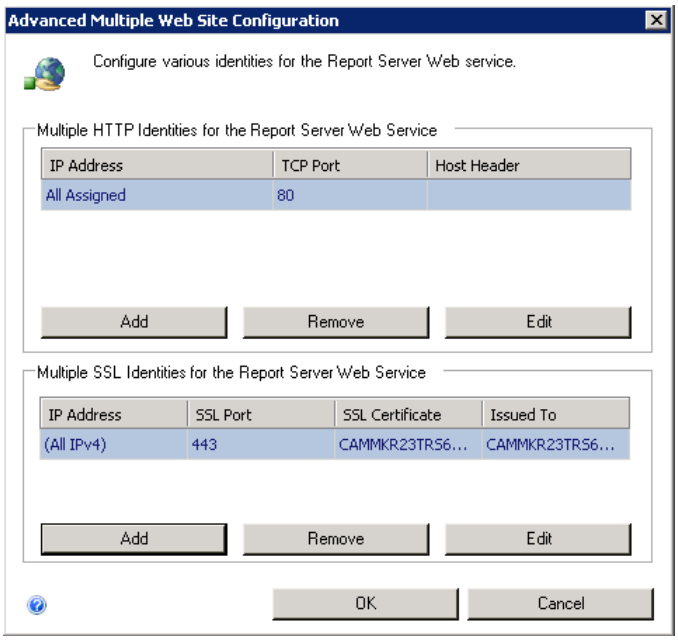
14. Under **Multiple SSL Identities for the Report Server Web Service**, click **Add** to display the Add a Report Server SSL Binding dialog box.



15. Select a specific **IP Address** (if appropriate).
16. In the **Certificate** field, select the certificate that you imported in the previous steps.



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

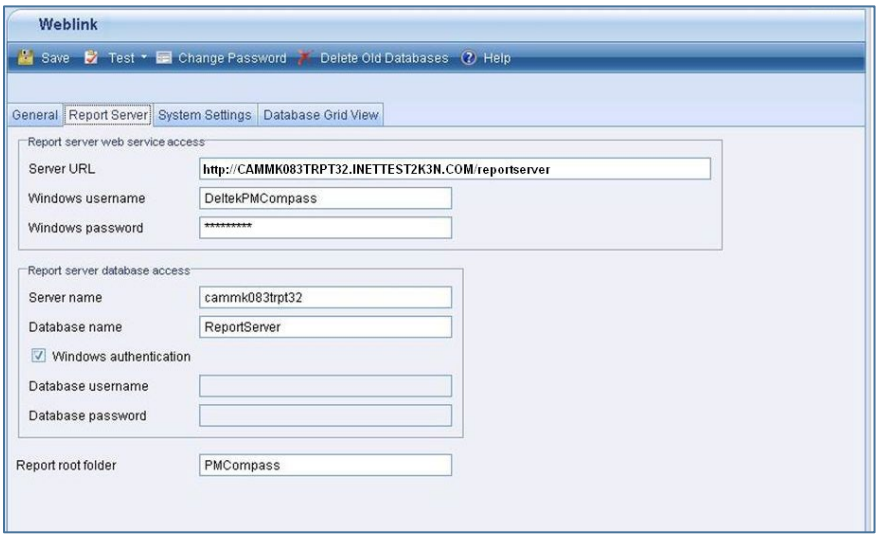


> **Note:** If you are going to run all communication to the report server via SSL then you should also remove the HTTP binding from the configuration

18. Repeat steps 12-17 for the Report Manager URL. The configuration of SSL for Reporting Services is complete.
19. On the Web Server, launch Weblink and log on. Select the appropriate database.
20. On the ReportServer page, verify if 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)://pmcompass.companydomain.com/reportserver

For example:



Test the SSL Configuration

Test PM Compass using SSL URLs to ensure the product is functioning correctly. You can do this by tracing a PM Compass SSL session using Fiddler (http://www.fiddlertool.com) or another HTTP tracing tool.

Change Default Account Settings Created By The Installer On All Logical Tiers

The default installation of Deltek PM Compass will create a local Windows user account on the PM Compass physical tiers (Database, Web/Application, Report, and Process Server) if you chose to create a local account on the **Specify Service/Identity Account Password** screen during installation.

This section guides you through making the necessary changes to secure your PM Compass deployment on the various physical tiers. Use it to change accounts so that they are unique to your firm and do not include any Deltek default user accounts or passwords.

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 DeltekPMCompass local Windows account is used for all the following:

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

If the account serves multiple roles, you may not need to delete or disable the accounts as many times as indicated in these instructions.

Secure the Web/Application Tier

The Web/Application tier installation creates a local Windows user account named **DeltekPMCompass**. This account is also added to the Local Administrators group and the IIS_IUSRS group. It is configured as

the Application Pool Identity of the DeltekPMCompassAppPool and is used as the service account for the Deltek PM Compass Process Server and Cobra Web Service service accounts.

To secure the Web/Application tier and customize the Application Pool Identity:

1. On the Web/Application tier, do one of the following:
   - If you are using a Windows domain:
     a. Create a domain user account or use an existing one.
     b. Add this user to the Local Administrators group and IIS_IUSRS group on the web/application server.
   - If you are not using a Windows domain, create a new local Windows user account and add that user to the same Windows groups.
2. Log on to the domain on the PM Compass Web/Application server using an Administrator account.
3. Click **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager** to open Internet Information Services.
4. Expand the Server name, and click **Application Pools**.
5. Select the **DeltekPMCompassAppPool**, and select **Advanced Settings** from the Action pane on the right-hand side.
6. Place your mouse pointer in the **Identity** field, and click the ellipses (…) button to set the identity.
7. Select the **Custom account** option, and click **Set**.
8. In the **User name** field on the Set Credentials dialog box, enter the Application Pool Identity in the form <Domain>\<Username>.
9. In the **Password** and **Confirm password** fields, enter the user's password.
10. Click **OK** three times to set the identity.

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

    > **Note:** See Database Tier for more information.

11. Click **Computer Management » Local Users and Groups » Users** and delete or disable the local Deltek PM Compass Windows user account on the web/application server.

Secure the Process Server Service

To secure the Process Server service:

1. On the Web/Application tier, do one of the following:
   - If you have a Windows Domain:
     a. Create or have a domain user account created.
     b. Use the Computer Management utility under Administrative Tools to add this user to the Local Administrators group on the Report server.

c. Click **Computer Management** » **Local Users and Groups** » **Administrators**, and 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. To change the service to run your new account, click **Start » Control Panel » Administrative Tools » Services**, and locate the Deltek PM Compass Process Server service.
3. Update the **Log On As** column to reflect the new user information that you created above.
4. Use the Computer Management utility from Administrative Tools to delete or disable the local **DeltekPMCompass** Windows user account on the Process server.

Secure the Cobra Web Service

To secure the Cobra Web Service service:

1. On the Web/Application tier, do one of the following:
   - If you have a Windows Domain:
     a. Create or have a Domain user account created.
     b. Use the Computer Management utility under Administrative Tools to add this user to the Local Administrators group on the Report server.
     c. Click **Computer Management** » **Local Users and Groups** » **Administrators**, and 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. To change the service to run your new account, click **Start » Control Panel » Administrative Tools » Services**, and locate the Deltek PM Compass Process Server service.
3. Update the **Log On As** column to reflect the new user information that you created above.
4. Use the Computer Management utility from Administrative Tools to delete or disable the local **DeltekPMCompass** Windows user account on the Process server.

Enable the Encryptrequests Setting

Enable the encryptrequests setting in web.config on the PM Compass server to encrypt the data communicated between the client and the Application server. This parameter must be applied to all servers in a load balanced environment.

To enable the encryptrequests setting in the web.config file:

1. On the Web server, add the following line in the web.config file under AppSettings section:

   <add key="EncryptRequests" value="Y" />

   By default the web.config file is located here: c:\Program Files\Deltek\PMCompass\Web
2. Restart the App server.

Additional Security Configurations

Additional security configurations provide a deeper level of encryption when data is transmitted between the PM Compass SmartClient and the web server. This encryption mechanism creates an additional layer

of protection above and beyond the traditional SSL encryption recommended for PM Compass implementations and prevents in-flight data transmission from being compromised.

The additional security enhancements are particularly important for companies that expose their instance of PM Compass outside their corporate firewall.

These settings are included and enabled on new PM Compass 8.2 and above installations. For upgrades, you will need to manually add them. If they are not specified in the **web.config** file, they are not used.

- **NonceKeyTimeout**: When the user logs into PM Compass, the system generates a one-time expiring nonce key. The key is used to ensure the attacker will not be able to reuse the login request after the data is sent to the server. The value is in seconds and the default is **10**. Setting it to **0** disables the timeout.

  This setting is added under `<appSettings>` tag

  ```
  <configuration>
      <appSettings>
          <add key="NonceKeyTimeout" value="10" />
      </appSettings>
  <configuration>
  ```

- **EncryptRequests**: This encryption mechanism is disabled by default. If you want to take advantage of this added security, you must enable it within the **web.config** configuration file on the PM Compass web server. To enable the encryption mechanism, you need to set the **web.config** setting **EncryptRequests** that is within the `<appSettings>` section to **Y**, as shown below. After you enable this setting, all client-server transmissions will utilize the new encryption mechanism.

  ```
  <configuration>
      <appSettings>
          <add key="EncryptRequests" value="N" />
      </appSettings>
  <configuration>
  ```

- **EnableHMAC**: When enabled, a hash key-based message authentication code (HMAC) is passed to the web server. The server computes for the hash key itself and compares whether the key sent by the client matches the key computed by the web server. If it succeeds, the client request proceeds. This feature is disabled by default.

  This ensures that requests sent by the client have not been modified and mitigates potential information calls. This setting is added under `<appSettings>` tag

  ```
  <configuration>
      <appSettings>
          <add key="EnableHMAC" value="Y" />
      </appSettings>
  <configuration>
  ```

- **X-Powered-By**: This is part of the response header sent by the server. It contains application framework information (for example, ASP.NET) used by the web server. To disable this setting, add the XML tag below under the `<configuration>` tag.

  ```
  <system.webServer>
      <httpProtocol>
  ```

```
            <customHeaders>
                <remove name="X-Powered-By" />
            </customHeaders>
        </httpProtocol>
    </system.webServer>
```

Secure the Database Tier

The Database tier installation creates a local Windows user account on the SQL Server named **DeltekPMCompass**. SQL Server has two modes of authentication:

- Windows Integrated
- Mixed Mode

To confirm the mode of authentication that you are using:

1. Click **Start » All Programs » Deltek PM Compass » Deltek PM Compass WebLink** to launch the WebLink utility on the Web/Application server.
2. If you have not set a password for WebLink, click **Change Password**, and enter a unique password.

   The **Change Password** button is visible only when accessing WebLink via localhost on the web/application server.
3. Login 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, you are using Windows Integrated Authentication.
   - If the **Windows Authentication** check box is cleared and a SQL username and password are filled in, you are using SQL Server or Mixed Mode authentication.

Windows Integrated Authentication

If you are using Windows Integrated Authentication for the SQL Server connection, the local Windows user account is created on the database tier. You need to update the database tier with the new user account that you created for the PM Compass Application Pool Identity in the Web/Application Tier section.

> **Attention:** For detailed information on configuring Windows Integrated Security for web/application and database connections, see Integrated Security Configuration for PM Compass.

To update the database tier with the new user account:

1. On the Database tier, do one of the following:
   - 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 the domain or local user account described above.

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.
3. Grant this new Windows login dbo (database owner) rights to your PM Compass database(s).
4. On the Web/Application server, launch the WebLink utility.
5. Login 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 you updated the database connection information correctly, click the **Test » Database Connection** to validate the connection.
8. Use the **Computer Management** utility under Administrative Tools to delete or disable the local **DeltekPMCompass** Windows user account on the Database server.
9. Use SQL Server Management Studio to delete or disable the **DeltekPMCompass** 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. The Deltek PM Compass installation does not create a SQL Server login account on your SQL Server.

To create the SQL Server login:

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 SQL Server Management Studio.
3. Grant the new login dbo (database owner) rights to your PM Compass database(s) and, if appropriate, the Reporting Services databases (ReportServer and ReportServerTempDB).
4. If you want to use a different account for 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. Login to WebLink, and select your database from the **Current Database** drop-down list.
6. On the General tab, enter the new SQL Server login username and password.
7. To ensure that you updated the database connection information correctly, click the **Test » Database Connection** to validate the connection.
8. Update the Report Server tab with the new connection information for the Report Server databases.

Secure the Report Tier

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

Note: When you created the database tier account, access rights were automatically given to the Report Server databases for the new user account.

To secure the Report tier and customize the Report tier account:

1. Do one of the following:
   - If you have a Windows Domain:
     a. Create or have a Domain user account created.
     b. Use the Computer Management utility under Administrative Tools to add this user to the Local Administrators group on the Report server.
     c. Click **Computer Management** » **Local Users and Groups** » **Administrators**, and 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 use Report Manager to grant this new account the necessary rights in Reporting Services.
2. Use http://<report_server>/reports to open Report Manager, replacing **<report_server>** with the name of your Report Server.

   To access Report Manager, you must already have been granted rights to the Report Server. You may also need to launch Internet Explorer using the **Run as Administrator** option.
3. Click the **Site Settings** link in the upper right corner and add the new account to the Administrators role.
4. Delete the **DeltekPMCompass** account from this role.
5. Click the Properties tab or the **Folder Settings** button (depending on your version of SQL Server).
6. Add your new account to the Content Manager Role.
7. Delete the **DeltekPMCompass** account from that role.
8. Use the Computer Management utility from Administrative Tools to delete or disable the local **DeltekPMCompass** Windows user account on the Report Server.

Secure the Process Server Tier

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

Note: 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 run.

In this procedure, you 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:

1. Select one of the following actions:
   - If you have a Windows Domain:
     a. Create or have a Domain user account created
     b. Use the Computer Management utility under Administrative Tools to add this user to the Local Administrators group on the Report server.
     c. Click **Computer Management** » **Local Users and Groups** » **Administrators**, and 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. To change the service to run your new account, click **Start » Control Panel » Administrative Tools » Services**, and locate the Deltek PM Compass Process Server service.
3. Update the **Log On As** column to reflect the new user information that you created above.
4. Use the Computer Management utility from Administrative Tools to delete or disable the local **DeltekPMCompass** Windows user account on the Process Server.

If You Have Multiple Servers

Your PM Compass 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 repeat the same steps on each physical server, using the same user account information that you used on the first server for that tier.

Integrated Security Configuration for PM Compass

PM Compass includes an option for Windows Integrated Authentication that allows users to log on once for both the Windows and the PM Compass applications. The use of Windows Integrated Security is configured for each user's PM Compass account by using the Windows domain network logon account as the user name for that particular user. This allows the user to be logged on automatically to PM Compass and EPM Security Administrator when logged onto the domain.

If they are not properly logged on to their domain, they will be asked for their network credentials before they can log on to PM Compass. For example, non-domain workstations and users connecting to the network via an Internet connection receive a domain authentication request before they are logged on to PM Compass.

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

Basic Domain and IIS Configuration

To configure Windows Integrated Authentication, several changes must be implemented both at the domain level and in IIS. This is in addition to the configuration of your domain user accounts in PM Compass.

These changes are as follows:

- A domain user account must be configured as the IIS Application Pool identity for the DeltekPMCompassAppPool in IIS. This domain account does not require any domain administrative rights.

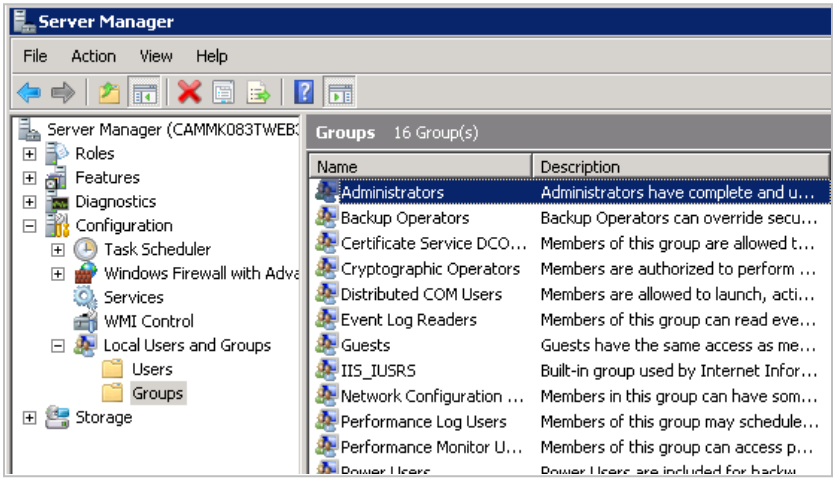
  By default, PM Compass creates a local windows account, DeltekPMCompass, to perform this function. However, a domain account is required to support trusted domains as well as the default IIS Windows Integrated Security configuration using Kernel Mode Authentication.

- The domain account used for the Application Pool Identity must have the following rights on the PM Compass 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 EPM SA and PM Compass IIS applications (virtual directories) must 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. Creating the SPN requires domain administrative rights.

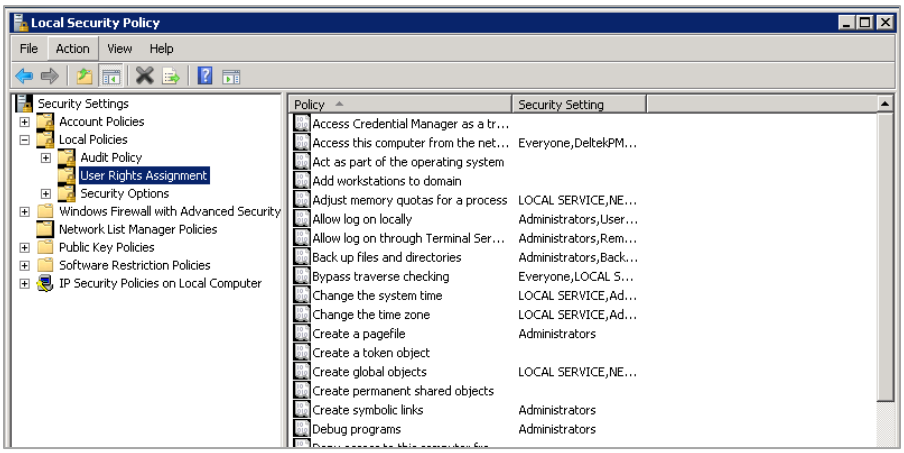
Configure the Application Pool Identity to be a Domain Account

To configure the Application Pool Identity to be a domain account:

1. Add the domain user to the local Administrators and IIS_IUSRS group via **Server Manager » Configuration » Local Users and Groups » Groups**.



2. Grant the domain user the necessary rights using the Local Security Policy tool (**Administrative Tools » Local Security Policy » Local Policies » User Rights Assignment**).

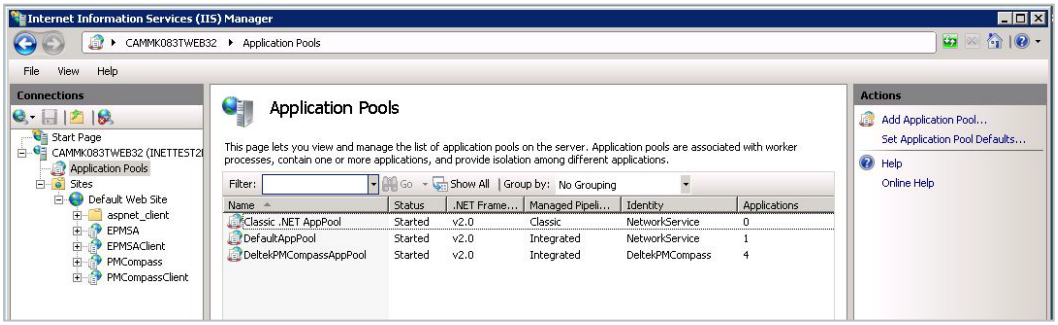


3. Now that you have created the domain account and given it rights, your next step is to change the Application Pool identity in IIS Manager.

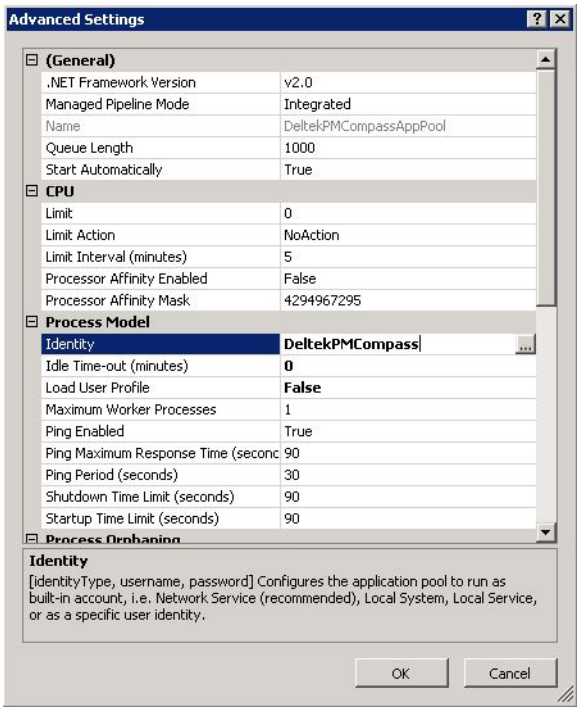
Change the Application Pool Identity

To change the Application Pool Identity:

1. Change the Application Pool Identity via **Administrative Tools » Internet Information Services » Application Pools**.

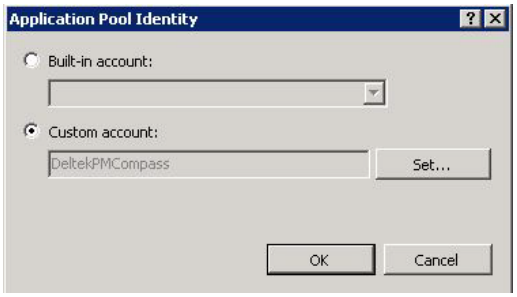


2. Right-click **DeltekPMCompassAppPool** and select **Advanced Settings** to display the Advanced Settings dialog box.

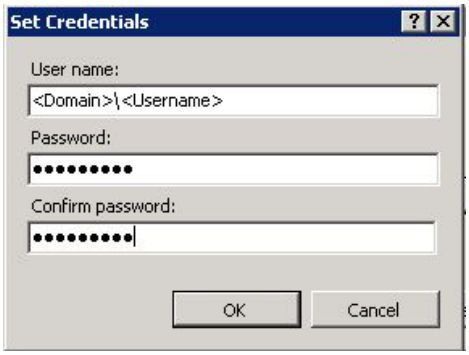


   a. In the **Identity** field, click the ellipsis.

   b. On the Application Pool Identity dialog box, select **Custom Account**, and click **Set**.



3. On the Set Credentials dialog box, enter the domain user name (domain\user name) and password, and click **OK**.

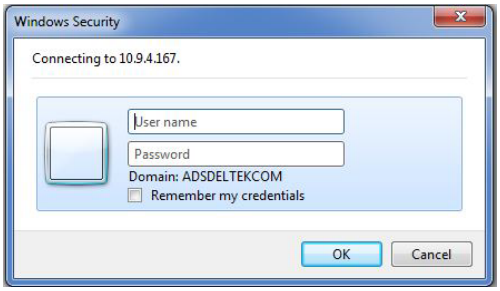


4. After the Application Pool Identity has been set, launch PM Compass on the Web/Application server to ensure that the application launches correctly. If PM Compass fails to launch, review the application event logs to identify the problem.

Important Information about Windows Integrated Authentication for Internet Users and Non-Domain Workstations

Domain users who are configured for Windows Integrated Authentication for PM Compass but who access the application either from a non-domain workstation or via the Internet will experience a slightly different authentication process as compared to users who are logging on to the application on a domain workstation on the corporate network.

1. The first difference is that when a domain user accessing the application either from a non-domain workstation or via the Internet clicks the URL to access PM Compass (**http://<webserver>/PMCompass**), IIS displays a prompt requesting the user's domain credentials.



This is normal because the users are not authenticated yet to access the domain and IIS is configured for Windows Integrated Authentication.

2. The second difference is that users will see a second authentication dialog box when the client-side application, after being downloaded via ClickOnce, makes its first call to the Web Server.

This second authentication dialog box displays because the client-side WinForm application is unable to use the previous credentials requested and processed by IIS.

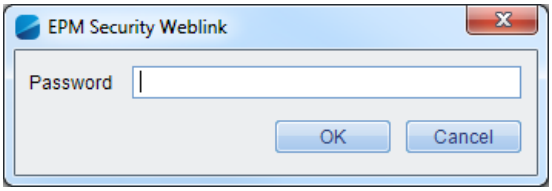
Configure Weblink to Use Windows Integrated Authentication for Database Connections

After the account has the necessary rights to the database, you must configure Weblink to use Windows Integrated Authentication for the various database connections.

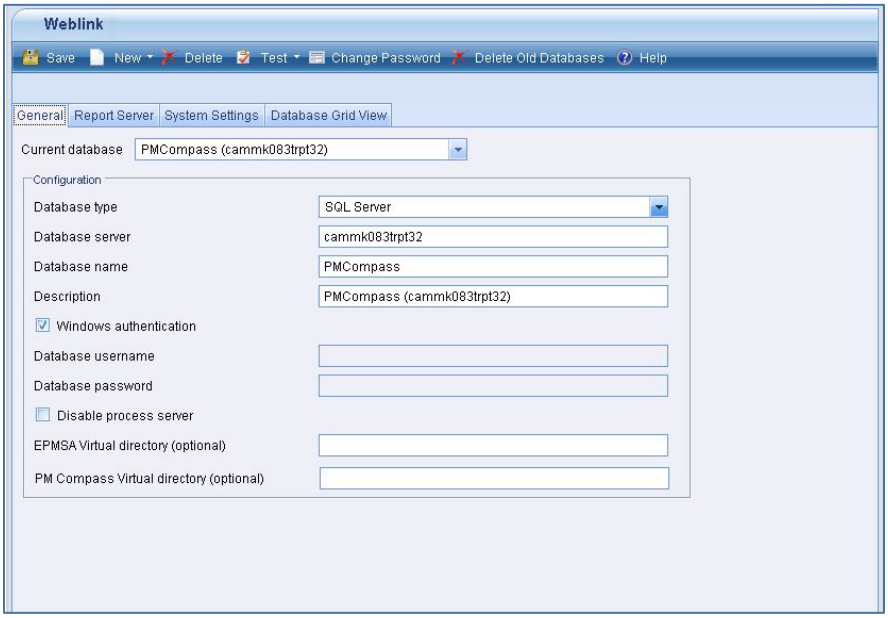
Note: Oracle Servers — Windows Integrated Authentication for Oracle database connections is not supported in PM Compass.

To configure Weblink to use Windows Integrated Authentication for database connections on SQL Servers:

1. Click **Start » All Programs » Deltek PM Compass » Deltek PM Compass WebLink** to launch the WebLink utility on the Web/Application server.
2. Enter the Weblink password.

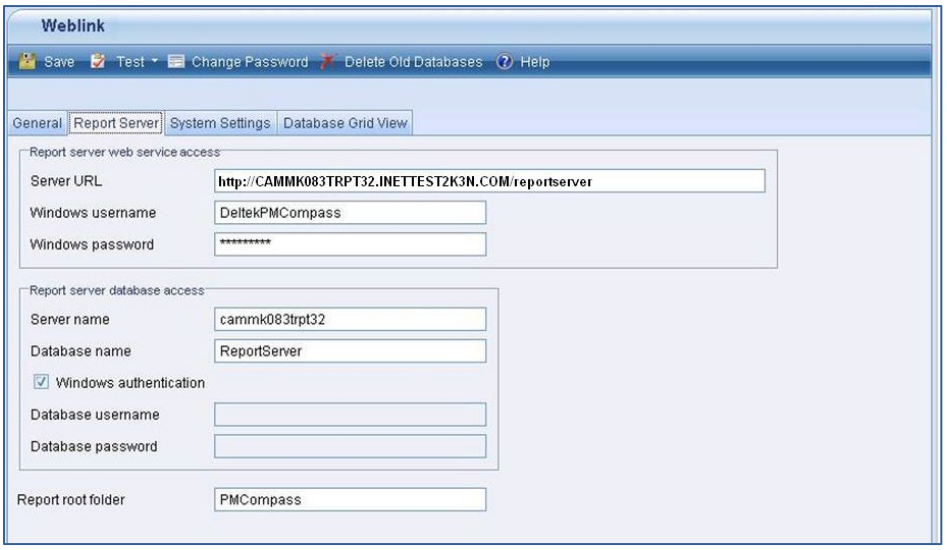


3. On the General tab:
   a. Select the database for which you want to enable Windows Integrated Authentication.
   b. Select **Windows authentication**. This option instructs Weblink to use the domain Application Pool Identity user account to connect to the database.

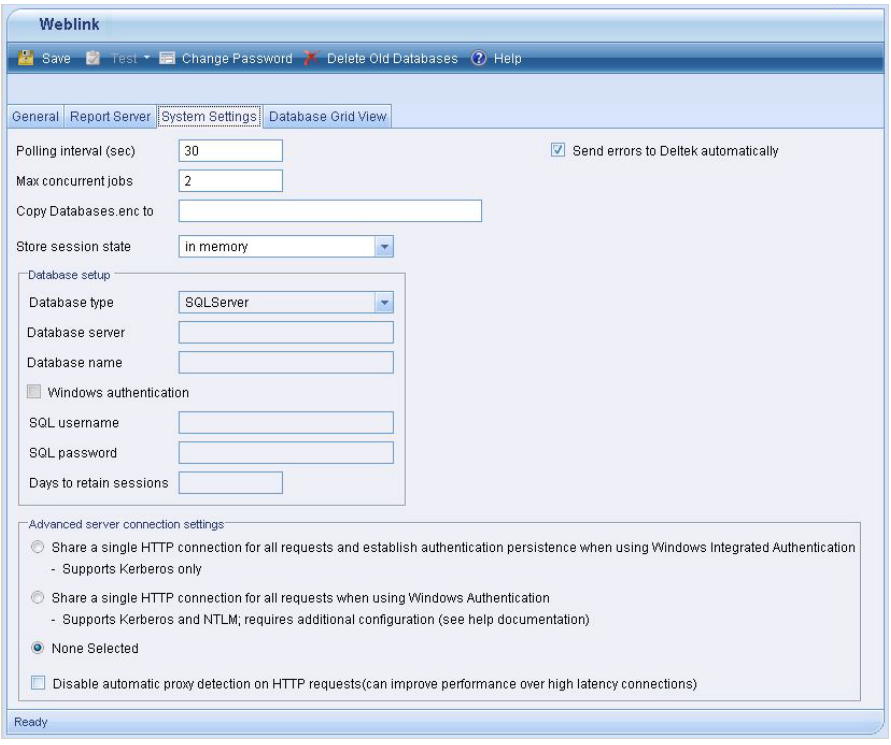


4. If needed, you can also enable Windows Integrated Authentication for the Report Server database connection. In this instance, the account requiring access may be a different account than the one used for the IIS Application Pool Identity. If this is the case, you must grant

db_owner rights to the Report Server databases and then select the **Windows authentication** option for the Report Server database.

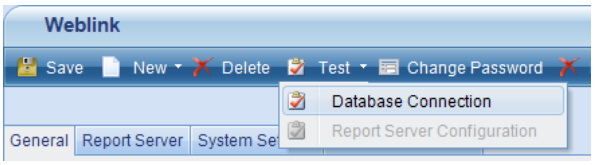


5. You can also enable Windows Integrated Authentication for the SQL Server Session state connection. This option instructs Weblink to use the IIS Application Pool Identity to make the database connection.



Note: For information about related settings in Weblink for configuring the **Advanced server connection settings** options, see the Weblink online help system.

6. On each of these tabs in Weblink, make sure you use the **Test** button to test the connection to ensure that everything is configured properly:

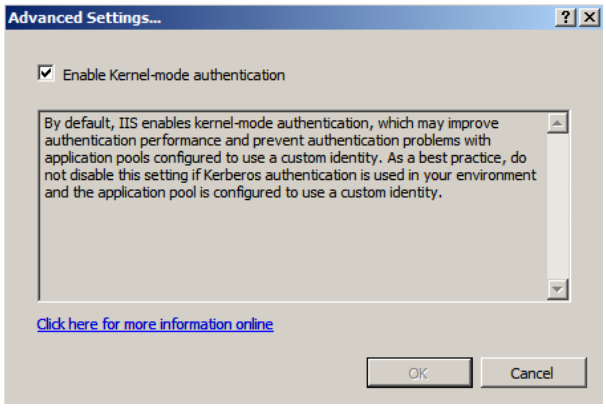


IIS Kernel Mode Authentication

When using Windows Integrated Authentication, the default configuration of IIS is to use Kernel Mode Authentication. If you need to disable Kernel Mode Authentication, follow the steps in this section.

To disable Kernel Mode Authentication:

1. Log on to the domain on the PM Compass Web/Application server using an Administrator account.
2. Click **Start » All Programs » Administrative Tools » Internet Information Services (IIS) Manager** to open Internet Information Services.
3. Expand the server name, expand **Sites**, and expand **Default Web Site** or whichever site PM Compass is installed.
4. Select the PM Compass virtual directory, and 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, click **Enable** on the **Actions** menu.
6. With **Windows Authentication** still selected, click **Advanced settings** on the **Actions** menu.
7. On the Advanced Settings dialog box, clear the **Enable Kernel-mode authentication** option to disable Kernel Mode Authentication.



Note: Disabling Kernel Mode Authentication requires the creation of a Service Principal Name (SPN) for the Application Pool Identity. See Creating a Service Principal Name (SPN) for more information.

Create a Service Principal Name (SPN)

In the default configuration wherein Kernel Mode Authentication is enabled, it is not advisable to create an SPN for the Application Pool Identity. Creating an SPN for the Application Pool Identity in this configuration will result in duplicate SPNs, preventing Windows Integrated Security from authenticating anyone to the Web site.

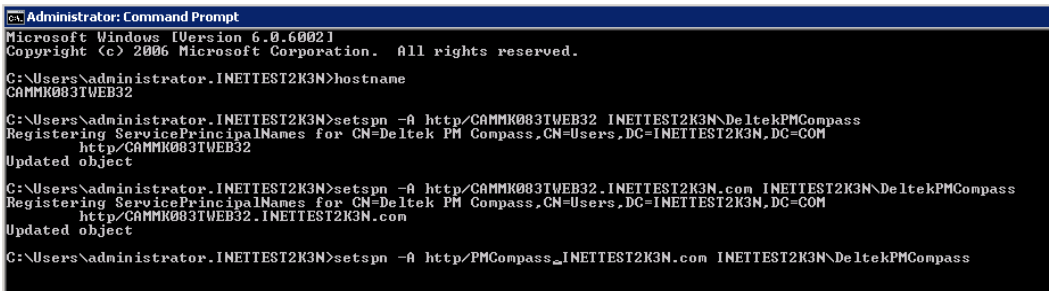
After Kernel Mode Authentication is disabled, use the procedure in this section to create an SPN for the Application Pool Identity of the DeltekPMCompassAppPool.

> **Note:** The setspn utility is installed by default on Windows Server 2008. It is not necessary to download and install it separately.

To create an SPN for the Application Pool Identity:

1. Make sure that you are logged onto the server with domain administrative rights.
2. Execute 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)

   See the examples in this screenshot:



> **Note:** For more information, refer to this Microsoft Knowledge Base article: http://support.microsoft.com/?id=871179.

Create a Reverse Proxy for SQL Reporting Services Using IIS Application Request Routing (ARR)

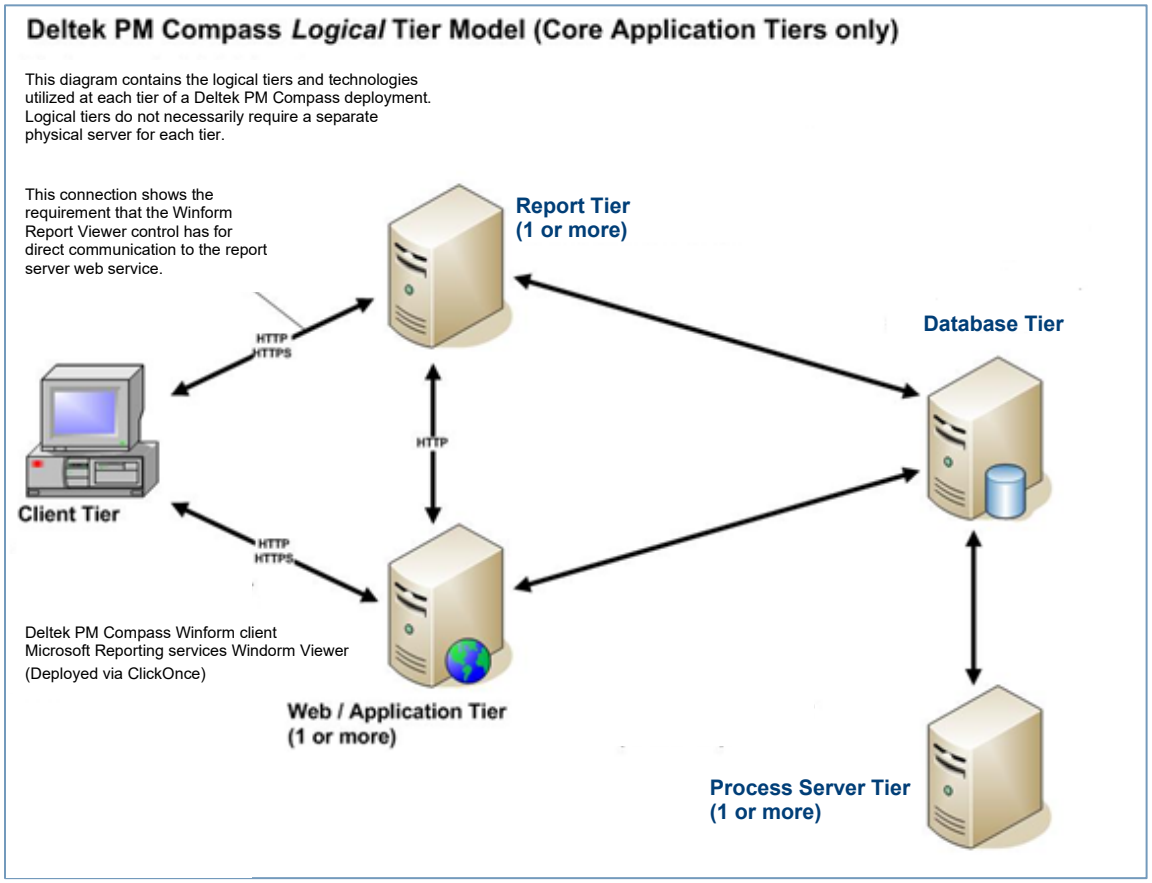
Why do I need a Reverse Proxy?

Deltek PM Compass 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 PM Compass 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 PM Compass web/application server in your deployment of PM Compass.

Typically this is not a problem when PM Compass is deployed inside the Intranet; however, when PM Compass 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 PM Compass 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 PM Compass, this deployment may require that the server hosting your database is made accessible to the internet, posing additional security risks. The architecture diagrams below depict the PM Compass logical tier diagrams with and without a reverse proxy.

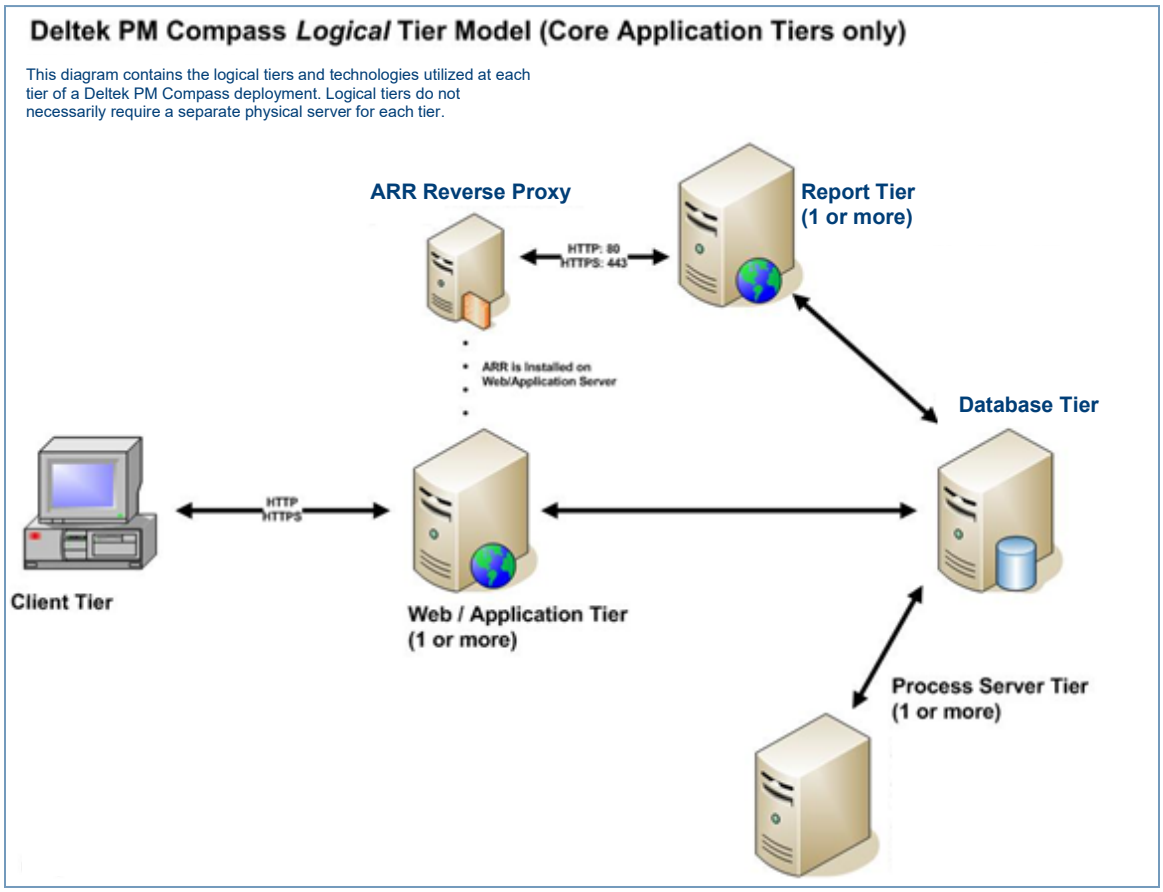
A reverse proxy utilizing Microsoft's Application Request Routing (ARR) extension for IIS allows the direct forwarding of requests through the PM Compass web server to the reporting services web service with responses back to your Internet clients. This configuration resolves all of the issues identified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

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 PM Compass web/application server.



A reverse proxy using Microsoft's Application Request Routing (ARR) extension for IIS allows the direct forwarding of requests through the PM Compass web server to the reporting services web service with responses back to your Internet clients.

This configuration requires that the server hosting the PM Compass web/application server be running Windows Server with IIS enabled.



Installation Steps

This section outlines the installation steps you need to follow. These instructions are specific to version 3.0 of Application Request Routing.

Prerequisites

The following pre-requisites must be met before installation:

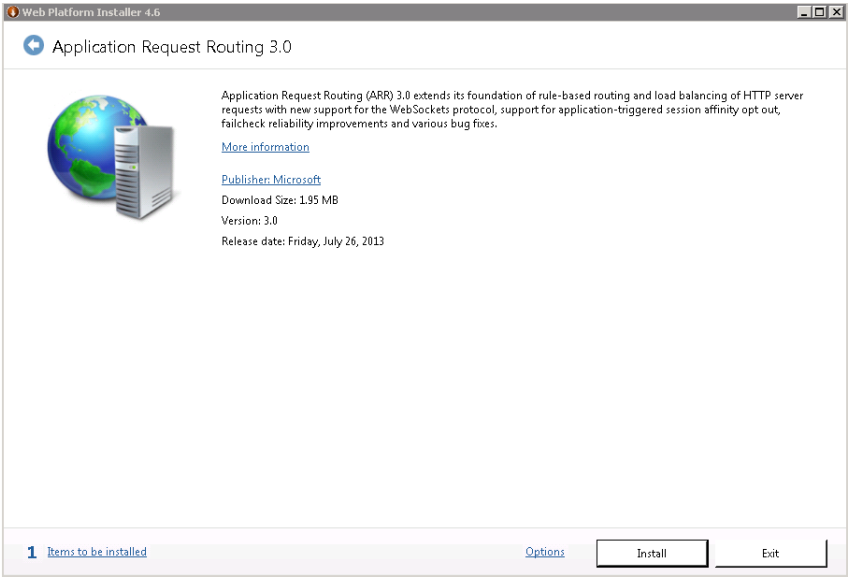
- The PM Compass Web/Application server must be running Windows Server 2012 R2 / IIS, Windows Server 2016 / IIS, or Windows Server 2019 / IIS.
- PM Compass must be installed.
- The IIS configuration must include the IIS role service “Management Service.”

Attention: Refer to the *Deltek Product Compatibility Matrix* document for complete information on the latest tested versions for the key technologies used by Deltek products.

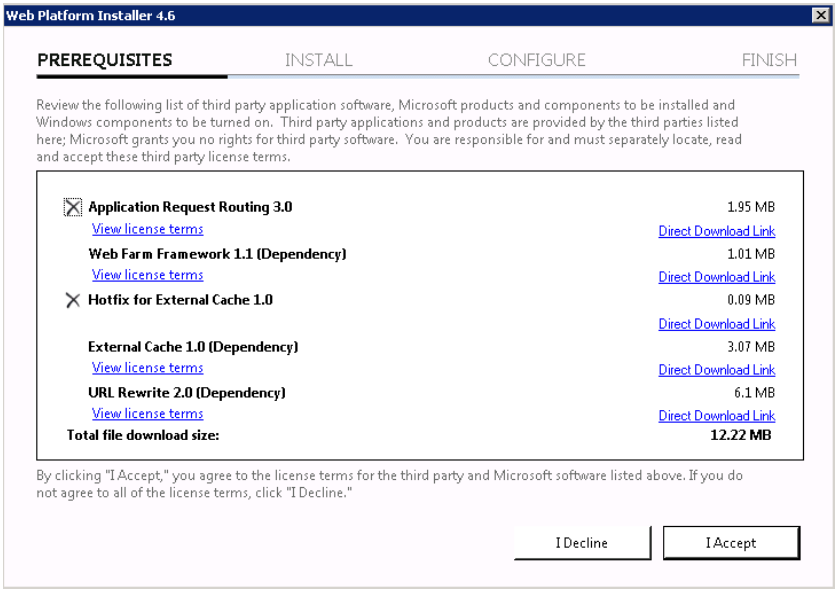
Install the Application Request Routing (ARR) Module on Your PM Compass Web/Application Server

To install ARR:

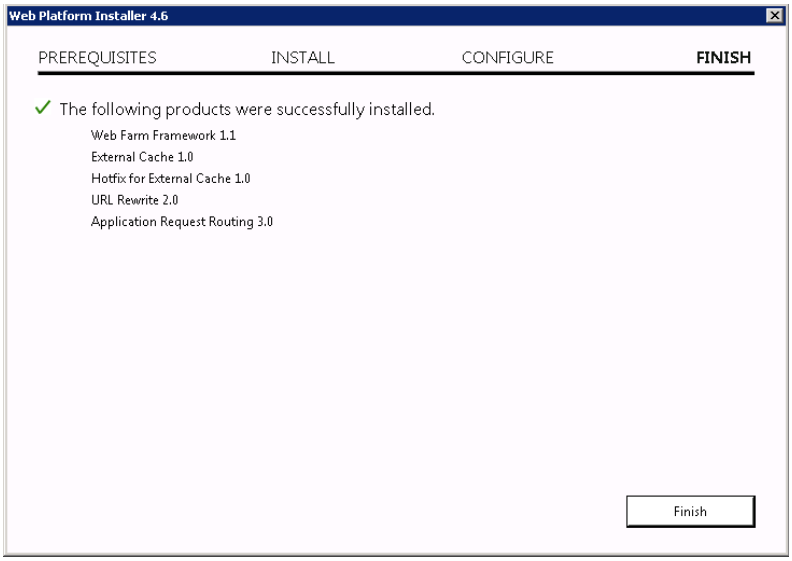
1. Go to the following URL to install ARR 3.0 via the Microsoft Web Platform installer: http://www.iis.net/downloads/microsoft/application-request-routing
2. Click **Install this Extension**.
3. On the Microsoft Web Platform Installer page, click **Install Now**.
4. On the File Download dialog box, click **Run** to run the **ARRv3_0.exe** file.
5. When the Web Platform Installer launches, choose to install Application Request Routing 3.0. The Web Platform Installer will ensure that all prerequisites required for the installation are also downloaded and installed.



6. Accept the license agreements.



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



Troubleshoot the Installation

To troubleshoot the installation process:

1. Open a command prompt and enter **cd %temp%**.
2. Use Notepad to open the **arr_setup.log** found in this folder. This log file identifies which components failed to install. Each component's installation log is also in this folder.

3. Make sure that the pre-requisite IIS components were installed and that the services were stopped. Then reinstall ARR. You can also extract and install the individual modules by entering the following from the **Start » Run** command:

   <Path to ARR Setup File>\ARR_x64_Version1.exe /T:<path to extract> /C

Configure Application Request Routing (ARR)

This section contains the following sub-procedures on how to configure Application Request Routing:

- Create the Reports and ReportServer folders
- Create the Application Pool
- Modify the Application Pool settings
- Create the IIS applications to act as proxies
- Add Rewrite Rules

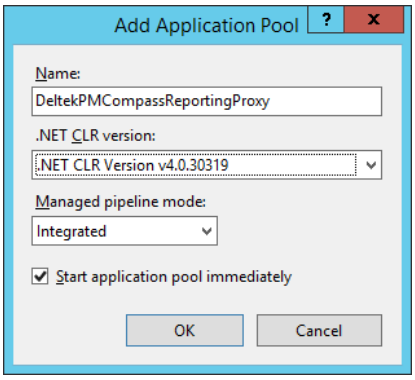
Create the Reports and ReportServer Folders

1. Open Windows Explorer.
2. Create two folders under **<drive>:\Program Files\Deltek\PMCompass\web** named:
   - Reports
   - ReportServer

   For example: c:\Program Files\Deltek\PMCompass\Reports.

Create a New Application Pool Called DeltekPMCompassReportingProxy

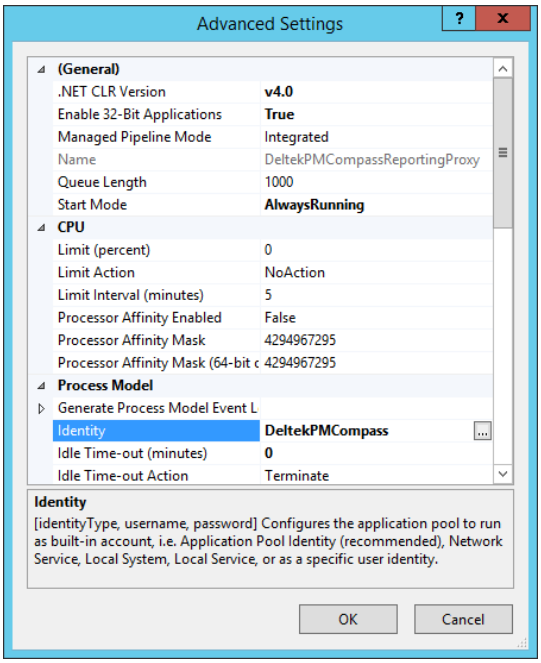
1. In IIS Manager, expand the server name.
2. Right-click **Application Pools**, and click **Add Application Pool** on the shortcut menu.
   - Enter the name and click **OK** to create the Application Pool.



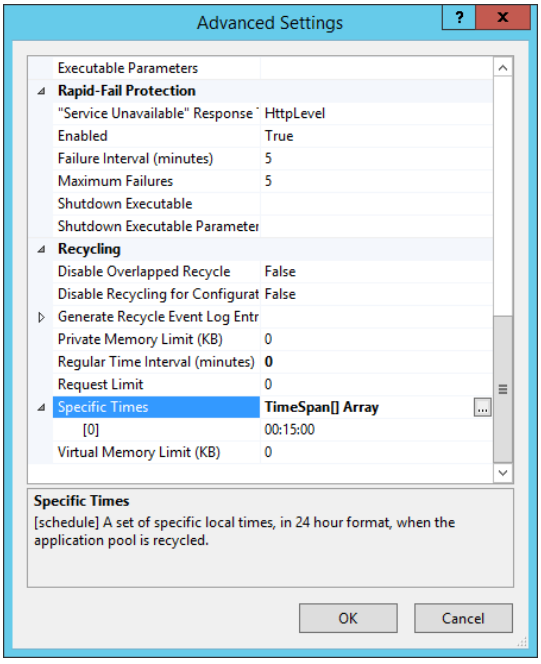
Modify the Settings of the Application Pool

1. Right-click the **DeltekPMCompassReportingProxy** Application Pool and click **Advanced Settings** on the shortcut menu.
   - Set **Enable 32 bit Applications** to **False**.
   - Configure the **Identity** to be the same account as your DeltekPMCompassAppPool. By default, this is the local Deltek PM Compass windows account.

- Set the **Idle Time-out (minutes)** to **0** (the default is 20).



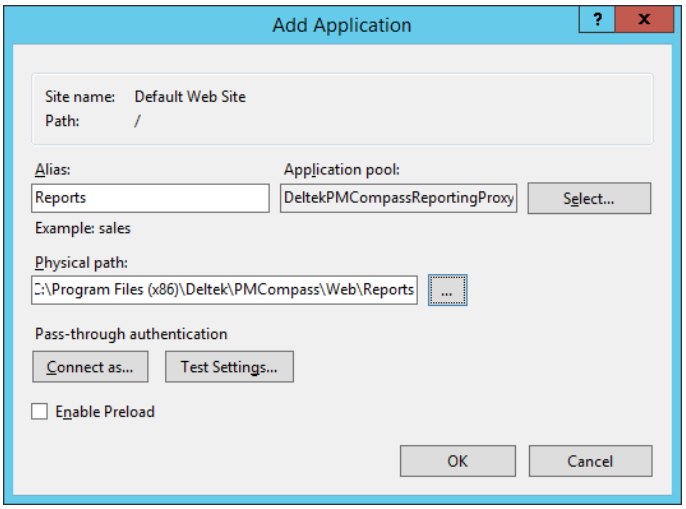
2. Scroll down for more settings.
   - Set **Regular Time Interval (minutes)** to **0** (the default is 1740).
   - Set **Specific Times** to **00:15:00** (the default is 00:00:00).



Create IIS Applications to Act as the Proxy for the Reports (SQL RS Report Manager) and ReportServer (SQL RS web service)

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

2. Right-click **Default Web Site** and click **Add Application** on the shortcut menu.
   - In the **Alias** field, enter **Reports**.
   - For **Application Pool**, configure it to use **DeltekPMCompassReportingProxy** and then enter (or browse to) the physical path you created.
   - Click **OK** to create the Reports Application.

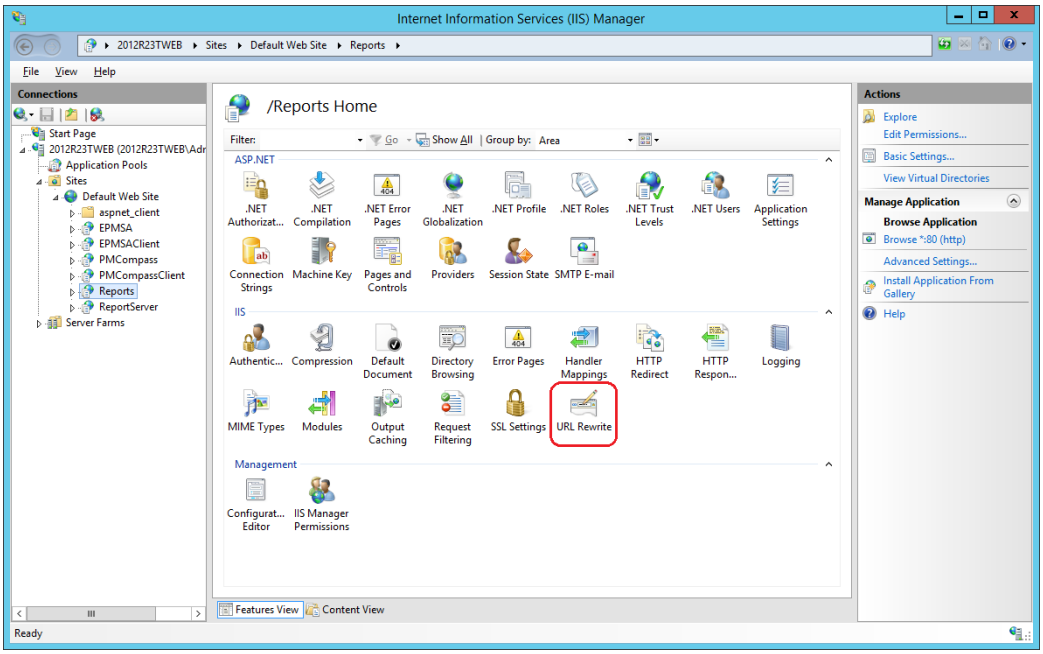


3. Repeat Step 2 to create the ReportServer Application. Be sure to enter **ReportServer** in the **Alias** field.

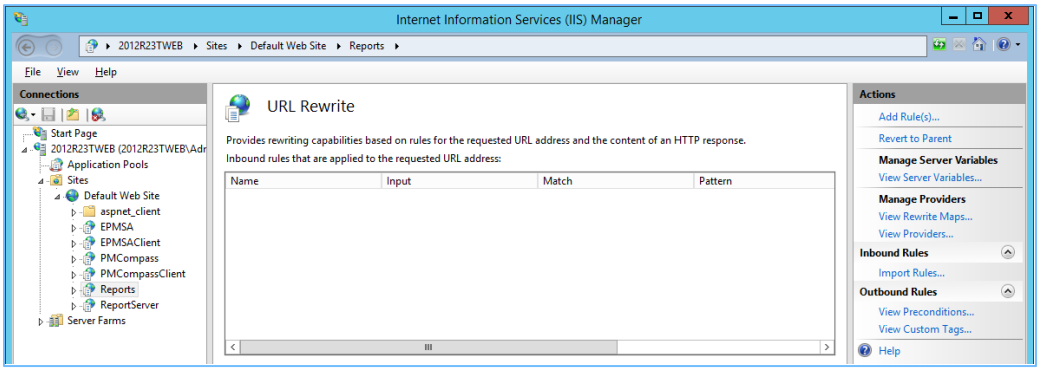
Add Rewrite Rules for Each Reporting Application

1. In Internet Services Manager, under **Default Web Site**, click the **Reports** application.
2. Double-click **URL Rewrite**.

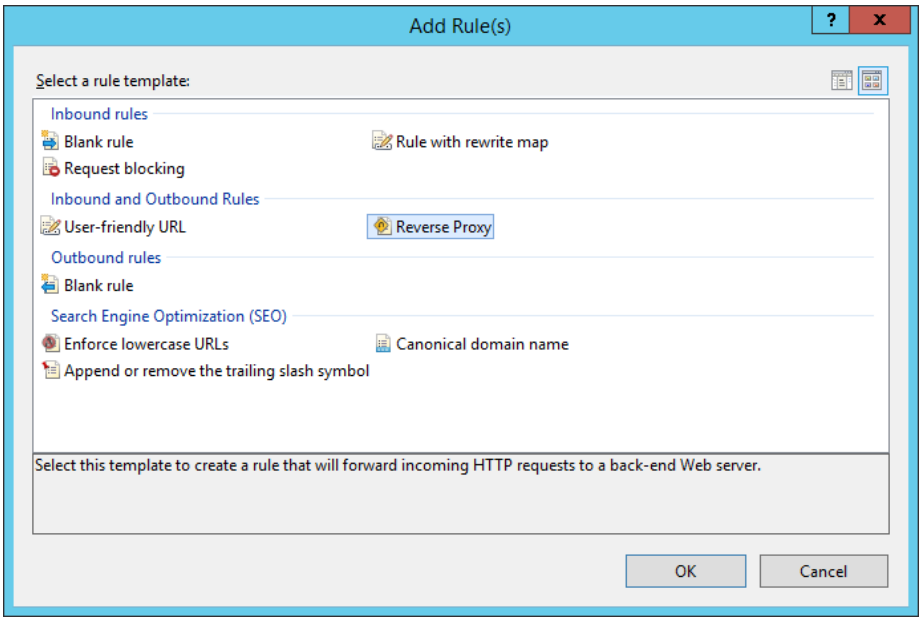
> **Note:** If you do not see the URL Rewrite module, it's possible that the Internet Services Manager was open when ARR was installed. Close and re-open Internet Services Manager.



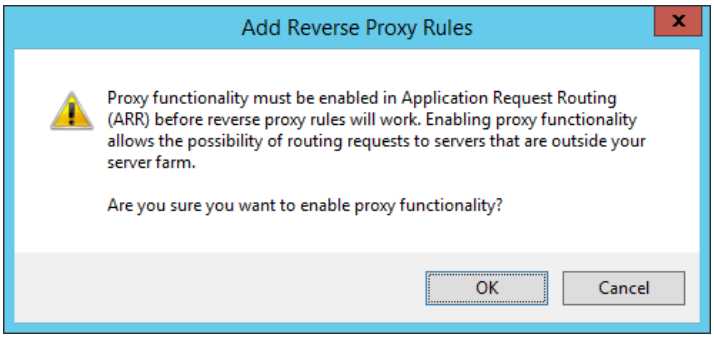
3. On the **Actions** menu, click **Add Rules**.



4. Select **Reverse Proxy**, and click **OK**.



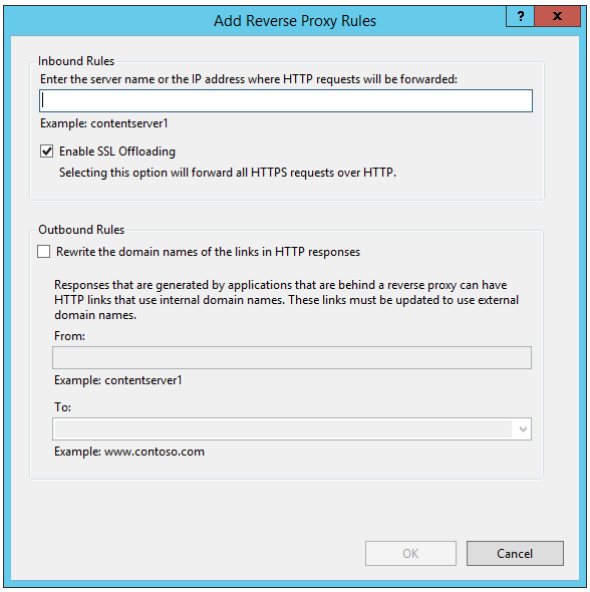
5. On the Add Reverse Proxy Rules dialog box, click **OK**.



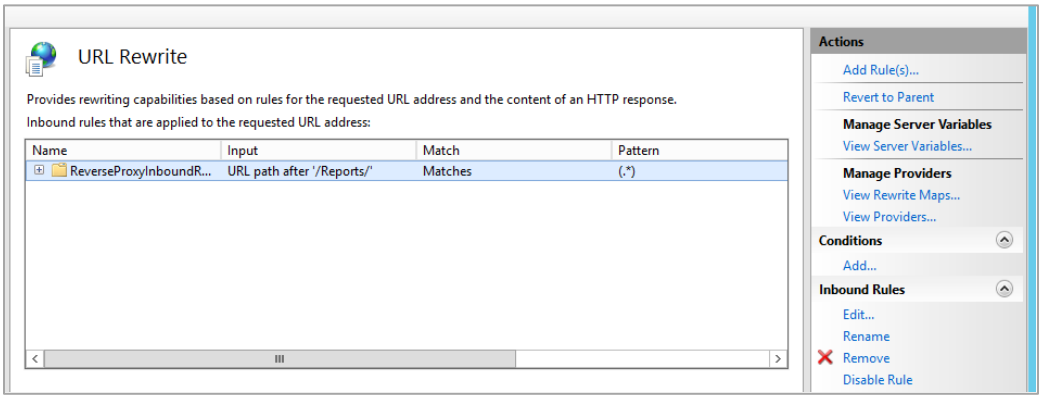
6. On the Add Reverse Proxy Rules dialog box, enter the name of your SQL Reporting Services server in the **Inbound Rules** text box.

   If your PM Compass server is configured for SSL, leave the **Enable SSL Offloading** option 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.



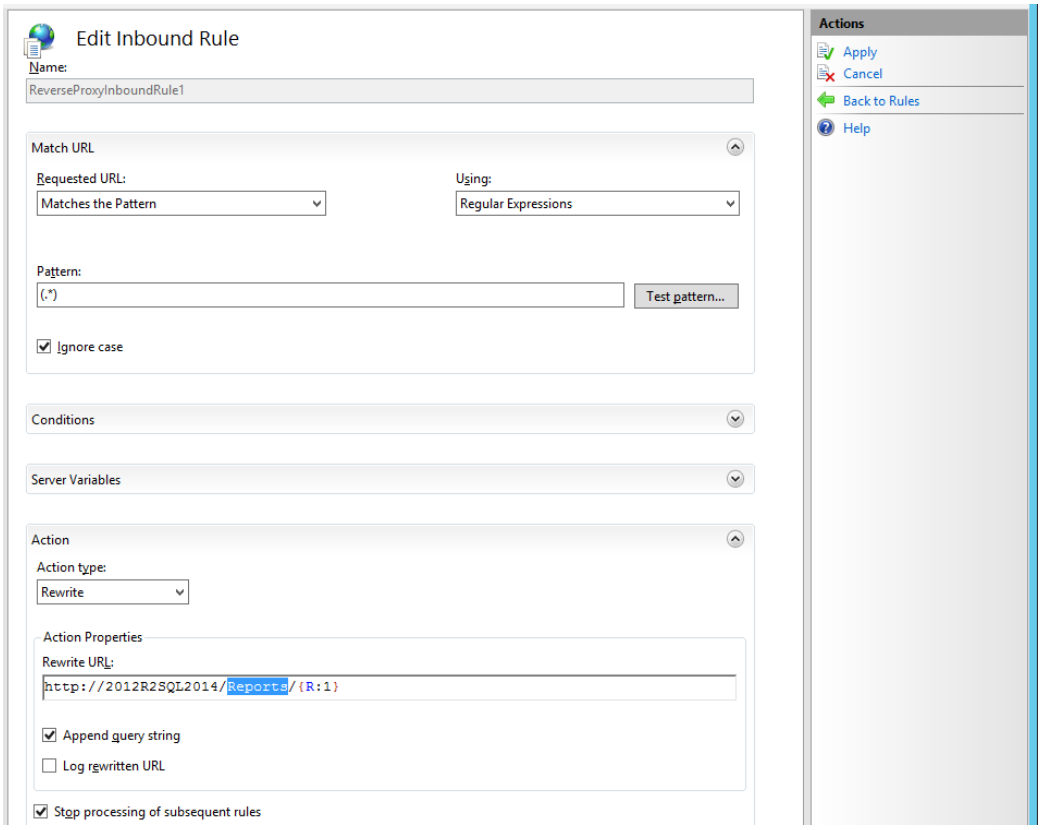
7. Click **OK** to create the reverse proxy rule.
8. Select the rule that was created and click **Edit** on the right, under **Inbound Rules**.



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

> **Note:** Make sure there is a slash between **Reports** and **{R:1}**.

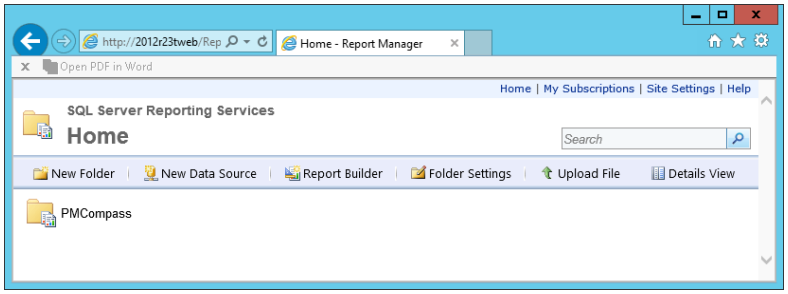


10. Repeat Steps 1 - 9 for the ReportServer virtual directory. Be sure to substitute **ReportServer** for **Reports** in Steps 1 and 9.

Test the Proxy Server

To test the proxy server:

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://<PMCompassWebServer>/Reports** where **<PMCompassWebServer>** is the name of the Web/Application server:



- **http://<PMCompassWebServer>/ReportServer** where **<PMCompassWebServer>** is the fully qualified domain name of the Web/Application server:

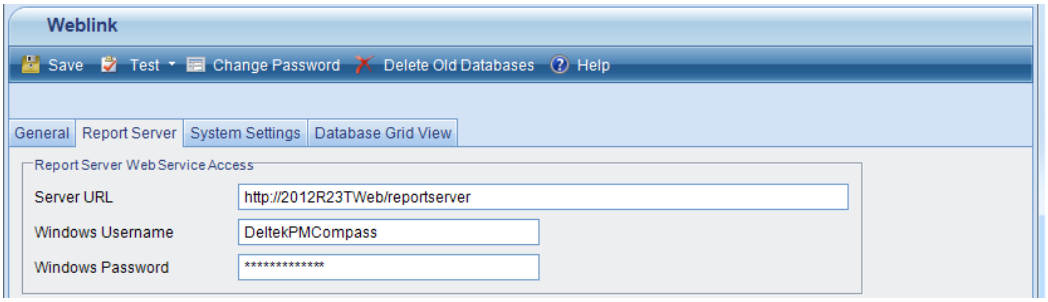
Configure PM Compass to Use the Reverse Proxy

After ARR is configured, modify Weblink to use the reverse proxy.

To modify Weblink:

1. On the Web/Application server, click **Start » All Programs » Deltek » PM Compass** to open Weblink.
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 PM Compass Web server.

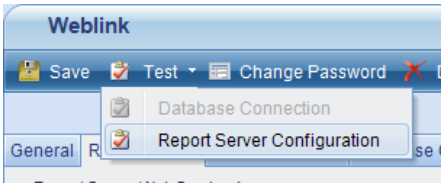
   Typically, the server URL is in the form http://<ReportServer>/ReportServer. Change this to http://<PMCompassWebServer>/ReportServer, where **<PMCompassWebServer>** is the exact, fully qualified domain name of the Web server (for example, pmcompass.companyname.com).



> **Note:** Deltek assumes that will secure the PM Compass Web server with an SSL certificate. In this configuration, it is not necessary to secure the SQL Reporting Services server with an SSL certificate. Therefore, the URL entered above should be http, not https. The proxy server will handle the forwarding of the https traffic to http.

4. Make sure to change all databases that will use the reverse proxy. No additional changes to the Weblink configuration are necessary.

5. Click **Test » Report Server Configuration** to test the configuration.



6. When the configuration tests successfully, save your changes.

Troubleshoot Configuration Issues

The following table lists common errors and their solutions.

Error	Description
HTTP 404 — When accessing PM Compass	Make sure the Load Balancing rule is configured to only work with *reports*.
HTTP 400 — The request cannot be routed because it has reached the Max-Forwards limit.	Make sure the SSRS server has been added to the Server Farm configuration.
HTTP 502 — Web server received an invalid response while acting as a gateway or proxy server.	Make sure the Proxy configuration under Server Farm has the **Reverse rewrite host in response headers** option selected.

Further assistance configuring reverse proxy is outside the scope of Technical Support. If more assistance is needed, it can be arranged through the Deltek Global Services consulting group, Customservices@Deltek.com. They will be glad to provide an estimate of the cost for this type of assistance, which is priced and charged separately.

Resources

See the following web sites for Application Request Routing (AAR) documentation:

- http://www.iis.net/extensions/ApplicationRequestRouting
- http://technet.microsoft.com/en-us/library/dd443531.aspx
- http://learn.iis.net/page.aspx/482/install-application-request-routing/

Configure HTTP Compression

Configuring HTTP compression for PM Compass can greatly reduce the size of http requests and responses between the client and web server, thereby improving application response time.

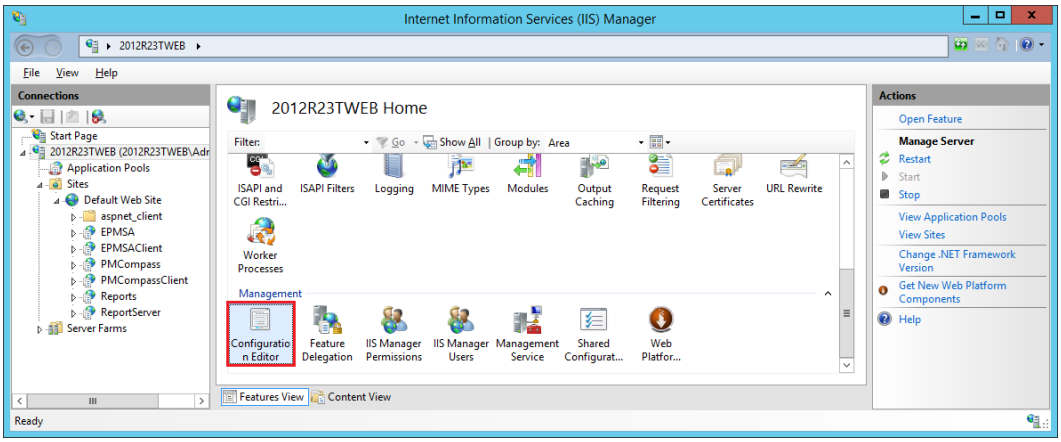
HTTP Compression is an available functionality built into Internet Information Services (IIS). By default, HTTP Compression is not enabled.

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 section 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:

1. Launch the **Server Manager**.
2. Click IIS.
3. In the left pane, locate **Roles and Features**, and check to see if these role services have been installed:

If not, select **Add Roles and Features** and install both the static and dynamic content compression 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:

1. Select one of the following actions:
   - If you want to enable compression at the server level, ensure that both static compression and dynamic compression are 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.

   > **Note:** 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**

> **Note:** 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.

> **Atention:** See http://www.iis.net/ConfigReference/system.webServer/serverRuntime for more information.

Test 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 **bold**:

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"** />

Smart Client ClickOnce Deployment Options

The Deltek Smart Client application uses the Microsoft .NET Framework ClickOnce deployment technology. The ClickOnce deployment technology makes it easy for administrators to deliver Windows-based applications to end-users by sending them a URL. When the user clicks on the URL, they are prompted to install the software. The application installs into the local user's profile (%LocalAppData%\Apps\2.0\ …) and does not require Administrator privileges. If the administrator updates the server, the next time the user launches the application, the update will automatically be applied.

ClickOnce Deployment Features

- Applications installed per-user, not per-computer.
- Administrator privileges not required.
- Applications not installed through the Add/Remove Programs feature.
- Nothing registers to the Global Assembly Cache (GAC).
- No ActiveX objects, plug-ins, or Java Applets.
- ClickOnce Cache Location: ..\Users\USERPROFILE_Name\AppData\Local\Apps\2.0 which can be accessed by typing in: %LocalAppData%\Apps\2.0.

Pre-Deploy PM Compass Smart Client to User Workstations

To reduce the size of the initial client-side download when a user launches PM Compass, you can pre-deploy the Smart Client files to specific locations on workstations for all users. This Hybrid Deployment Model installs the application:

- By looking in a specific folder on the workstation, and if the application is not found, and
- By downloading the file from the Application/Web Server.

Note: Hybrid Deployment Model (HDM) — ClickOnce only delivers about 15 files (enough to display the login page). After that, HDM takes over to deliver core application assemblies, hot fixes, language specific satellite assemblies and custom.

Files to be Deployed

The files that must be pre-deployed to the user workstations are located on the Application/Web server in this folder: **..\Program Files\Deltek\PMCompass\WebClient**. This is the same folder where PM Compass is installed.

- DeploymentManifest.xml
- DeltekPMCompassClient.zip: This file contains the Deltek PM Compass Smart Client components in a compressed format.

Workstation Deployment Location

The location to pre-deploy the files varies depending on the workstation operating system.

> **Note:** You must repeat the procedures in this section each time you upgrade your PM Compass Application/Web servers to a new version.
>
> By default, the Windows \ProgramData folder is hidden so you have to enable the **Show Hidden Files** option in Windows Explorer **Tools » Folder Options » View tab**.

Deploying on a Workstation

To deploy on a workstation:

1. Locate the **\ProgramData** directory and create the **\Deltek** directory.
2. Copy the **DeltekPMCompassClient.zip** and **DeploymentManifest.xml** files from the Application/Web Server into the Deltek directory.

Using PM Compass with Citrix or Remote Desktop (ClickOnce Bypass)

In some cases, the ClickOnce deployment behavior may not be supported. For example:

- Using it as a Seamless published application in Citrix

  Understanding Citrix XenApp and ClickOnce Applications — https://support.citrix.com/article/CTX125453

- Using it as a RemoteApp in Microsoft Remote Desktop Services (formerly known as Terminal Services)

  https://support.microsoft.com/en-us/help/2020945/clickonce-cannot-be-used-in-windows-terminal-server

- In some secure environments where ClickOnce deployment behavior is blocked.

In order to accommodate these scenarios, Deltek has created a procedure to bypass the browser based ClickOnce client deployment process for EPM SA and PM Compass. These deployments are composed of the same files that the regular ClickOnce deployment installs to the users profile on the local machine. However, instead of accessing a URL, the executable file for PM Compass or EPM SA is used. The files for this deployment are stored in the following location on the PM Compass Web/Application Server:

- **For PM Compass**: <PM Compass Installation folder>\PMCompass\ClickOnceBypassPMCompass
- **For EPM SA**: <PM Compass Installation folder>\EPMSA\ClickOnceBypassEPMSA

If the Administrator performing the installation chooses **Yes** at the “Will PM Compass be deployed with Citrix” prompt, the ClickOnceBypass folders will also be copied to the network share specified to be the Citrix shared folder during the web/application server installation.

The installer also updates the web.config file in the <PM Compass Installation folder>\PMCompass\Web folder by adding the following entry into the **<applicationSettings>** section

```
<add key="CitrixShareDirectory" value="\\UNCpath\folder" />
```

In order for the end-users to be able to use the application, the System Administrator can do one of the following:

- **Recommended**: Create or use an existing network shared folder to store the ClickOnce deployment files before installation. Specify the network folder at the Citrix prompt during installation so that the installer can copy the ClickOnceBypass folders into it.
- The installer places these folders into the network share specified during installation:
  - **ClickOnceBypassEPMSA**: Contains the EPM SA web client executable (DeltekEPMSA.exe) and other application files.

    Note: The installer updates the deltekepmsa.exe.config file in that folder with the name of your web server in the client endpoint address section. You can replace the server name with PMC Web Server DNS name, if one is used.

  - **ClickOnceBypassPMCompass**: Contains the PM Compass web client executable (DeltekPMCompass.exe) and other application files.

    Note: The installer updates the deltekpmcompass.exe.config file in that folder with the name of your web server in the client endpoint address section. You can replace the server name with PMC Web Server DNS name, if one is used.

- For Citrix or Remote Desktop Services deployments: If possible, have the network share exist on the Citrix servers, so that the installer can automatically copy the above folders into the location where you install your applications used for remote deployment, and publish the executable for PM Compass (deltekpmcompass.exe) and/or EPM SA (deltekepmsa.exe). This makes it possible to deploy PM Compass as a seamless published application or RemoteApp.

  Note: On Citrix, the network share may have to be located on the server in case the Citrix publishing feature does not allow referencing a UNC path to an executable on another server.

- Share the folder on the Web/Application Server (not recommended).

  Note: ClickOnceBypassPMCompass and ClickOnceBypassEPMSA folders are automatically updated. If you copy these folders to another location to use as a deployment, you must replace the shared files with the latest files from the ClickOnceBypassPMCompass and ClickOnceBypassEPMSA folders on the Web/Application Server. If you do not update the files, the users will not see any updates.

  This relates to deployment only. PM Compass still requires a connection to the Web/Application server when you use it.

To set this up:

1. Install PM Compass.
2. Ensure that after installation the ClickOnceBypassPMCompass and ClickOnceBypassEPMSA folders were installed into the central shared location.
3. Create a shortcut from the central shared location to launch **DeltekPMCompass.exe** (the PM Compass application) and **DeltekEPMSA.exe** (EPM Security Administrator).

4. Give the shortcut to end users. For Citrix/Remote Desktop deployments, publish the shortcut.
5. The folders are automatically updated with the latest client files during each cumulative update, or upgrade.
6. To support end-users running Open Plan on the Citrix box, install the Open Plan Add-in; choose **Yes** at the Citrix prompt, and specify the path to the network share. This will update the DeltekPMCompassChangeRequests.exe.config file with a setting in the **<applicationSettings>** section that alerts Open Plan to launch PM Compass from the ClickOnceBypassPMCompass folder on the network share instead of through a browser.

   Note: The setting in the DeltekPMCChangeRequests.exe.config file that tells Open Plan to launch PM Compass from the network share instead of from a browser:

   ```
   <applicationSettings>
     <DeltekPMCChangeRequests.My.MySettings>
       <setting name="PMCClientPath" serializeAs="String">
         <value>\\<FileServer>\<SharedFolder>\ClickOnceBypassPMCompass</value>
       </setting>
     </DeltekPMCChangeRequests.My.MySettings>
   </applicationSettings
   ```

Known Issues

PM Compass workflow emails contain a URL hyperlink that launches PM Compass and opens the record. This URL is configured in PM Compass (**Administration » System Settings » General Tab » Application URL field**).

When the user clicks on the URL in the PM Compass workflow email in a ClickOnce Bypass scenario, the links in the PM Compass workflow emails do not work. The browser tries to launch PM Compass directly from the users machine using the default ClickOnce deployment behavior. If your environment does not support ClickOnce deployment, the URL does not work. The user therefore has to start PM Compass manually from the location provided by the System Administrator (for example, within Citrix, RemoteApp or Shared Published executable) and navigate to the record.

Load Balancing

Configure load balancing according to your vendor's (for example, Microsoft Windows Server) recommendations. Make sure that you set the affinity to Single or Sticky (terminology depends on the vendor). This ensures that user sessions are maintained on the same server as long as a user remains logged on.

In addition, consider configuring the database session state for PM Compass and setting up a shared location for Databases.enc.

- **Configure Database Session State for PM Compass**: 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 PM Compass 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.

  One benefit of storing the session state in the database is that, when there is a Web Server failover, the work that was being performed at the time is not lost.
- **Configure a Shared Location for Databases.enc**: If your PM Compass deployment includes multiple web/application servers, or even just a dedicated Process Server, configuring a shared location for the databases.enc file eliminates the need to synchronize changes made to the databases.enc file across your servers.

Attention: For more information, see:

- Configure Database Session State for PM Compass
- Configure a Shared Location for Databases.enc

Loading Reports onto Load Balanced SSRS Servers

The Reports folder on the Web/Application server contains the report RDL files. RDL stands for Report Definition Language which is an XML schema that defines a report. PM Compass uses SSRS for managing reports. Before you can run a report in PM Compass, the report must be converted from the RDL file onto the the SSRS Web Service (Report Server).

Multiple SSRS servers in a load balanced environment all have a common URL but the .rdl files must be installed on each Server by running the Cumulative Update on each of your Web Servers. As long as you reload the reports after the Cumulative Update installation, it should update the central Report Server database, making it available for all servers.

Note: This batch file only updates standard reports. It does not update custom reports.

Before you begin

You have two options for loading reports after a Cumulative Update. You can either load them as part of the CU installation, or you can create and run a batch file.

Load Reports As Part of the CU Installation

1. Apply the Cumulative Update (CU) to all of your Web Servers.

2. For all Web Servers except the last one, select “No” when it asks you if you want to load reports.
3. When you apply the CU to the last Web Server, select “Yes” when it asks you if you want to load reports.

   The CU installer places all updated report .rdl files onto every Web Server and the reports are inserted into the Report Server database and available on all Report Servers.

Load Reports by Creating and Running the Batch File

1. Apply the Cumulative Update (CU) to all of your Web Servers.
2. Designate one Web Server to be your “Admin” web server. It should be the server on which you create and run the batch file.
3. On the Admin Web Server,create a batch file named, for example, **ManuallyLoadReports.bat**.
4. Paste the information below to the batch file.

   DeltekMakoCMD.exe LoadReports en-us "D:\Program Files\Deltek\PMCompass\Reports" PMCompass http://SSRS1/ReportServer VCAC Administrator Password

   Replace the above example text with the following:

Example Above	What You Should Use
DeltekMakoCMD.exe	DeltekMakoCMD.exe
LoadReports	LoadReports
en-us	en-us
“D:\Program Files\Deltek\PMCompass\Reports”	Specify the path to the PMC Reports folder containing the report RDL files
The details below (except for the password) can be found in WebLink on the Report Server tab.	
PMCompass	Specify the Report Root folder. By default it is named PMCompass.
http://SSRS1/ReportServer	▪ Specify the Report Server \ load balanced URL in the form of http://ReportServerName/ReportServer. ▪ If you are using an instance name, for example SQL2017, then the URL would be http://ReportServerName/ReportServer_SQL2017.
VCAC	▪ Specify the domain of the account specified in the Report Server Web Service. ▪ If you have installed PM Compass using a local account instead of a domain account, specify the local machine name.
Administrator	Specify the username (without the Domain).

Example Above	What You Should Use
Password	Specify the password.

5. Save the file into the <PM Compass Installation Directory> in Web\Bin.

   For example, if you installed PM Compass into D:\Program Files\Deltek\PMCompass, you would save the batch file in the "D:\Program Files\Deltek\PMCompass\Web\Bin" folder location.

6. (Optional) Create a shortcut for the batch file on the desktop.

7. Run the batch file.

   The batch file calls a file named **DeltekMakoCMD.exe** which is located in the <PM Compass Installation Directory> in Web\Bin. For example, if you installed PM Compass into D:\Program Files\Deltek\PMCompass, the file will be located in the D:\Program Files\Deltek\PMCompass\Web\Bin folder location.

Note: The above process works as long as you are using only one Report Server database with your load balanced Report Servers. After you run the steps one time, all the reports are uploaded into the SSRS database which is then available for all Report Servers

Warning: You must run the batch file every time you perform a CU installation. You should only run the batch file on the "Admin" web server.

Configure Database Session State for PM Compass

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 PM Compass 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.

Use Weblink to configure PM Compass to store session state information in a database. Deltek has developed its own session state model and does not rely on ASP.NET session state.

Note about Session State Database

Session state information is stored in a database table which is automatically configured by Weblink if you create it in the PM Compass database. However, if you want this database table stored in a database other than your PM Compass database, you need to create a separate database and login for this purpose. This is optional.

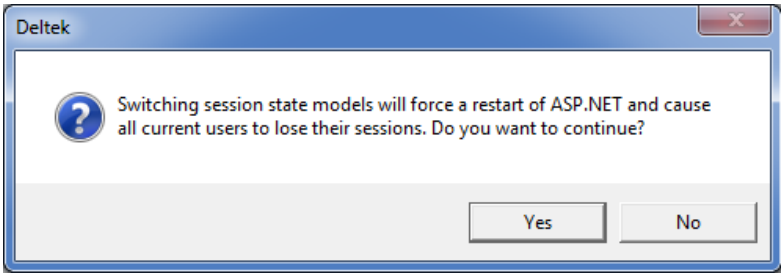
Configure PM Compass for Database Session State

Warning: Make sure that no one is logged in to PM Compass before making this change. Changing the session state invalidates all active user sessions.

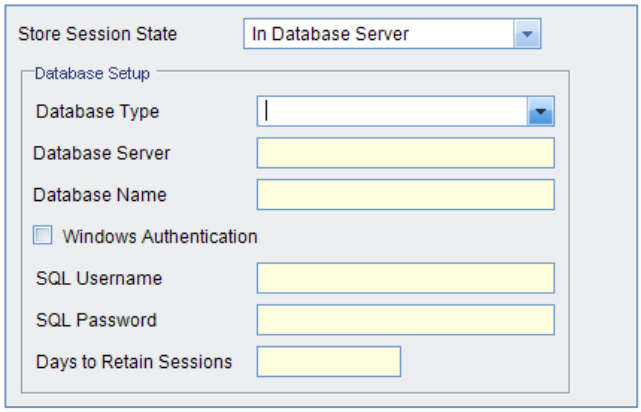
To configure PM Compass for database session State, complete the following steps on the Web/Application Server:

1. Launch and log on to Weblink. (The shortcut for Weblink is under the **Deltek PM Compass program group** in the Start menu.)
2. Click the System Settings tab.
3. In the drop-down field, change **in memory** to **in database Server**.

   The following message displays:



4. Click **Yes**. The Database setup dialog box displays:

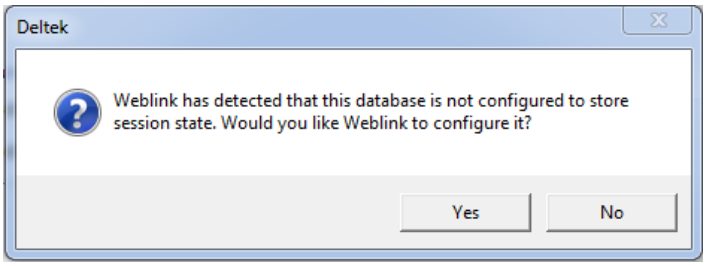


   - In Database type, select **SQL Server** or **Oracle**.
   - In the **Database server** field, enter the name of the database server where the session state database (or PM Compass) exists.
   - In the **Database name** field, enter the name of the session state database.
   - SQL Server only:
     - If you plan to use Windows Authentication for the database connection, select the **Windows Authentication** check box. If so, the **SQL Username** and **SQL Password** fields are disabled (shaded).

       Note: See Integrated Security Configuration for Deltek PM Compass for details on Windows authentication.

     - In the **SQL username** field, enter the SQL Login ID with rights to that database.
     - In the **SQL password** field, enter the password for the SQL Login ID that you entered in the previous step.
     - 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.

   The following message displays, prompting you to configure this database to store session state information:



7. Click **Yes** to create a table in the database called **FW_SessionState**. A message displays letting you know that Weblink has successfully configured the Server (database) to store PM Compass session state.

Verify the Configuration

To verify that session state is correctly being stored in the database for PM Compass:

1. Access your database server via a query utility.
2. Log on to PM Compass.
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.

```
Use <Session State Database>
Go
Select * from FW_SessionState
Go
```

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

Configure SQL Server Resource Governor to Manage PM Compass Workloads

> **Note: Prerequisite** — SQL Server Enterprise Edition.

With PM Compass, 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 takes up the majority of the resources (such as CPU or memory) of the SQL Server, thereby adversely impacting users.

For example, 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 running these reports and all other users experience dramatic slowdowns and timeouts using the software as a result. The only solution to the problem is to either allow the reports to complete (a process that could take hours) or 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 occurrences by ensuring that these disparate workloads don't monopolize resources on the database server. This topic provides the steps to configure the Resource Governor and provides suggestions on how to classify these workloads into separate resource pools.

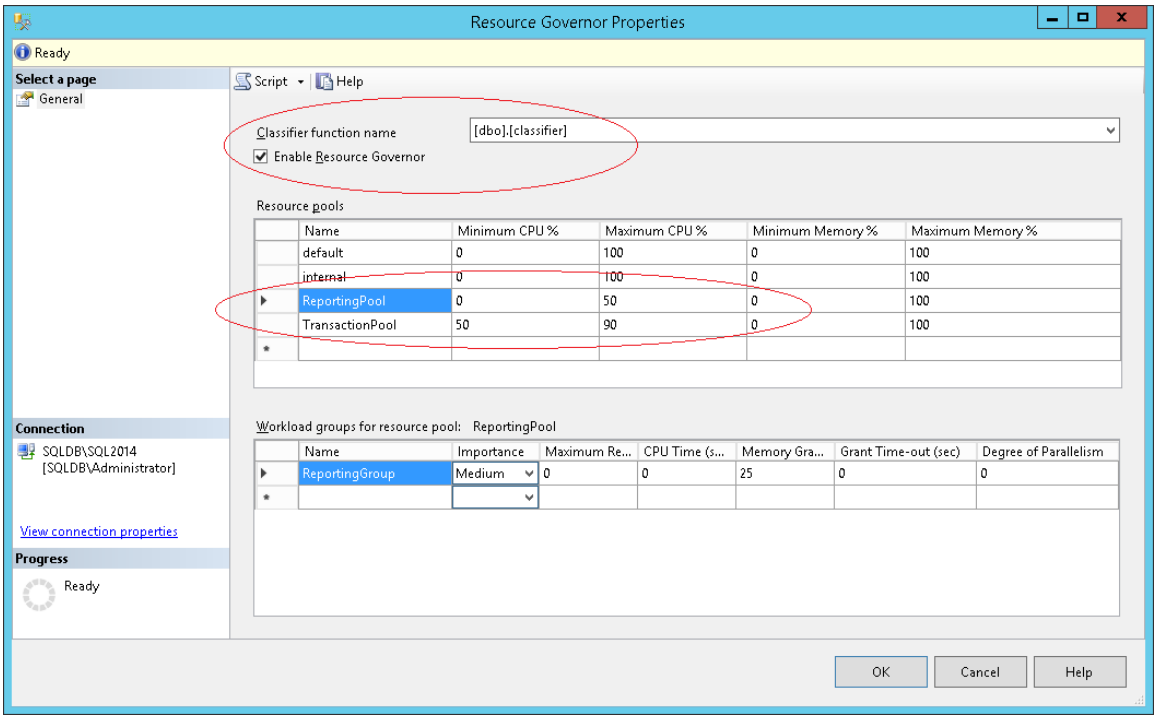
A SQL Server Classifier Function will be used to identify each workload which tells SQL Server which resource pool to place each connection in. You could use a variety of system functions to "classify" each connection. However, since all connections for PM Compass transaction processing are coming from the web/application server and that all report processing is coming from the report server, you can use the **client_net_address** from the **CONNECTIONPROPERTY** to classify each connection. The IP addresses for each of the servers to accomplish this classification assume that the Application Server and the Reporting Server are separate servers each with their own unique IP address.

> **Note:** Use the SQL Statements below to configure the Resource Governor replacing as appropriate the information that is highlighted in yellow.

```
--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 (PM Compass)
CREATE RESOURCE POOL ReportingPool
GO
CREATE RESOURCE POOL TransactionPool
GO
--Create Workload Groups for Reporting (SSRS) and Transactions (PM Compass)
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.

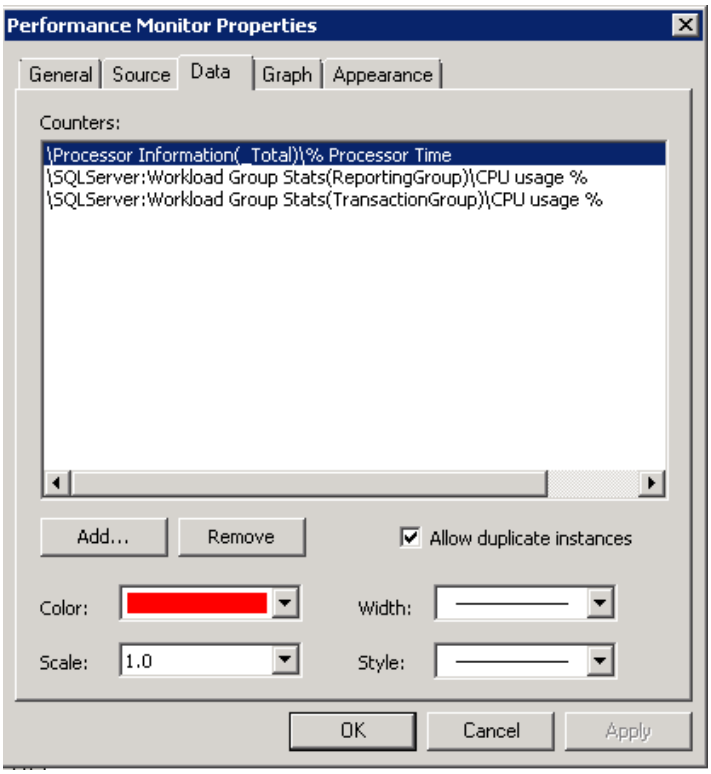
You can Install SQLCMD for your platform from the following link:

http://www.microsoft.com/en-us/download/search.aspx?q=install+sqlcmd

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

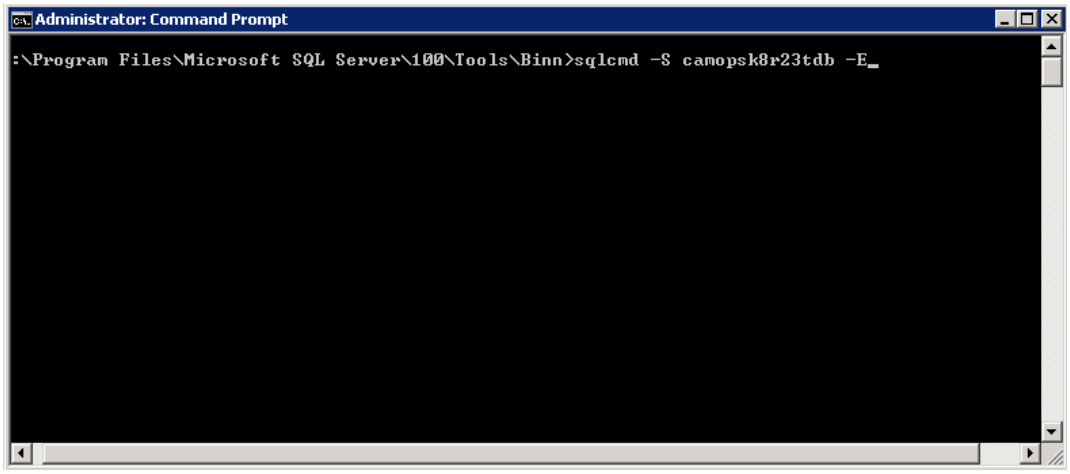
```
-- Here is a query that can be used to test (NOTE: osql doesn't seem to provide
necessary throughput)
SET NOCOUNT ON
DECLARE @i INT = 0
DECLARE @s NVARCHAR(500)
WHILE @i < 100000000
BEGIN
       SELECT @s = SUSER_NAME() + DB_NAME() + @@VERSION
       SET @i +=1
END
GO
```

Before executing the script, you should 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:



Monitor total CPU usage as well as the CPU usage for each Workload Group that you've 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 line graph.

1. Logon to the Application server.
2. Open a command prompt to the location of **SQLCMD**, and make a connection to your SQL Server:

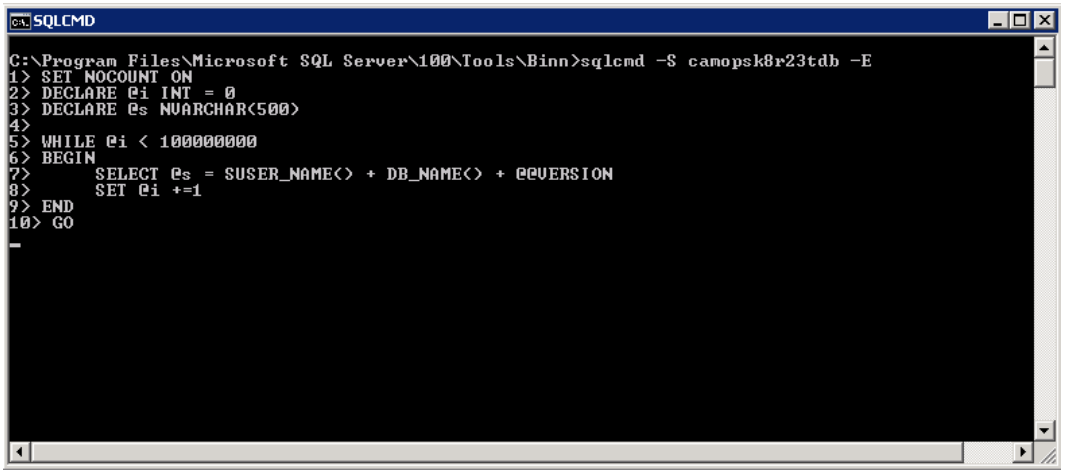


   - The **–S** switch specifies the name of the SQL Server machine.

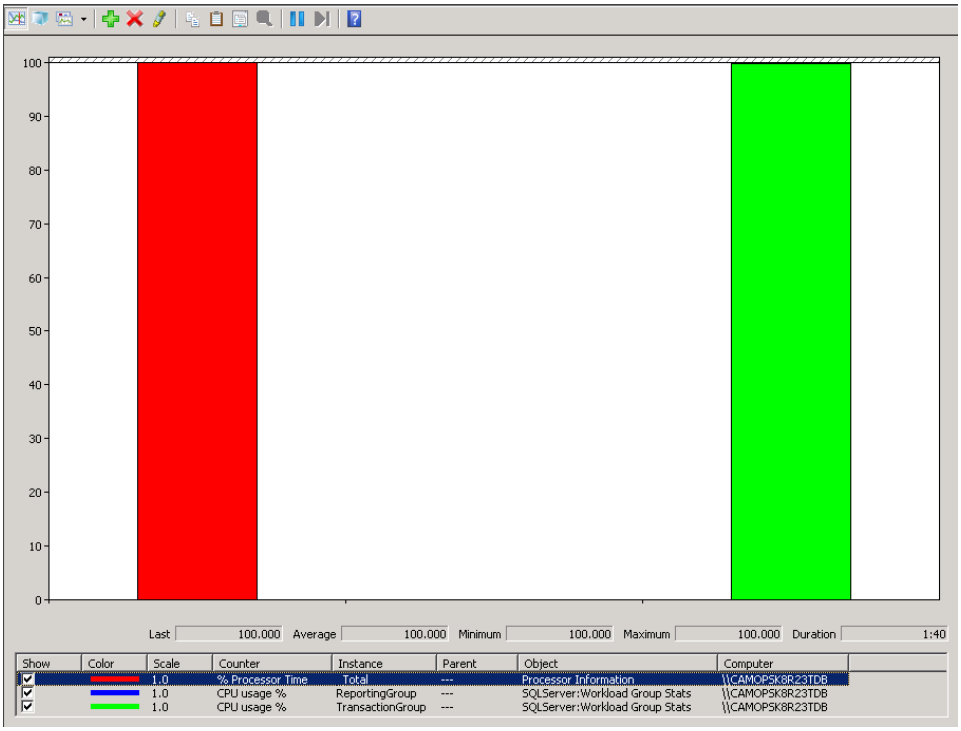
- The **–E** switch will use a Trusted Connection using the Windows credentials you are currently logged on as.

You can also specify a sql login id and password for the connection.

3. After the connection is made, paste the script into the command prompt window:



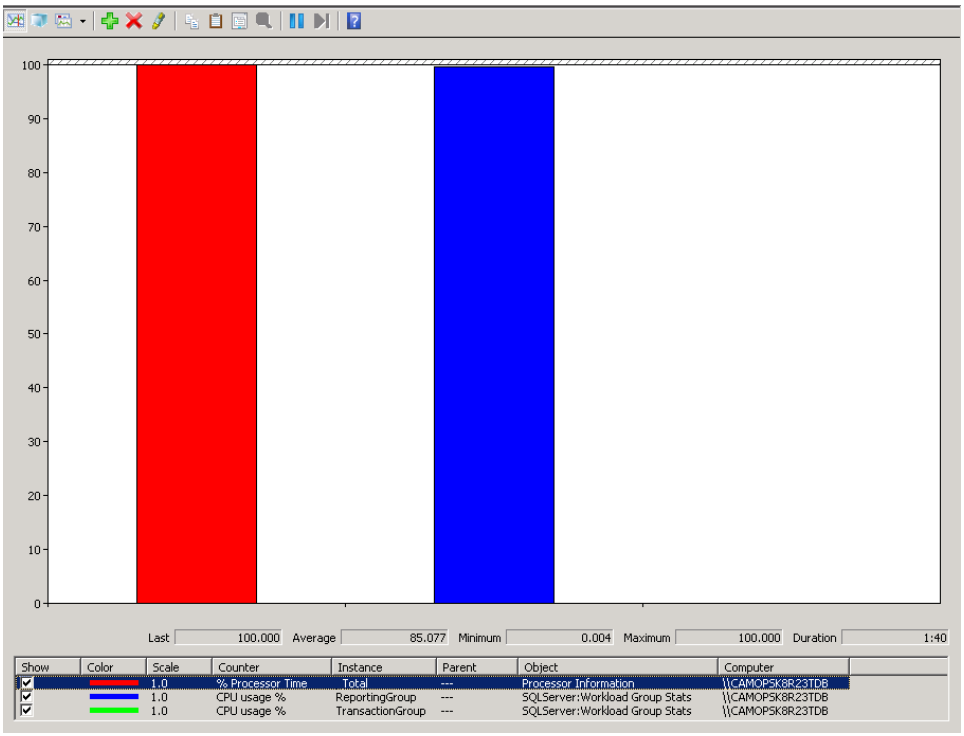
Executing this from the Application server will result in the following in Performance Monitor on the SQL Server:



Note that the Transaction Group is allowed to access all of the available CPU as there are currently no connections from the report server.

4. Use **CTRL-C** on the Application server to break out of running the script. The CPU usage should drop to zero.

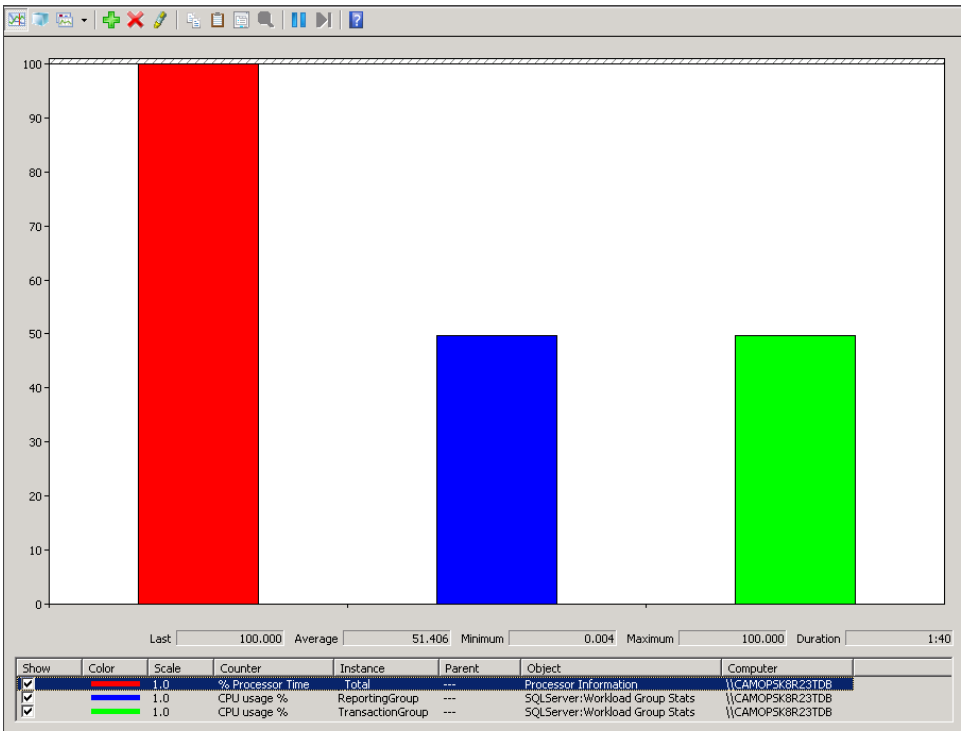
5. Log on to the Report server, open a command prompt window to SQLCMD, connect to the SQL Server, and execute the same test script. The results you will see are shown below:



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.

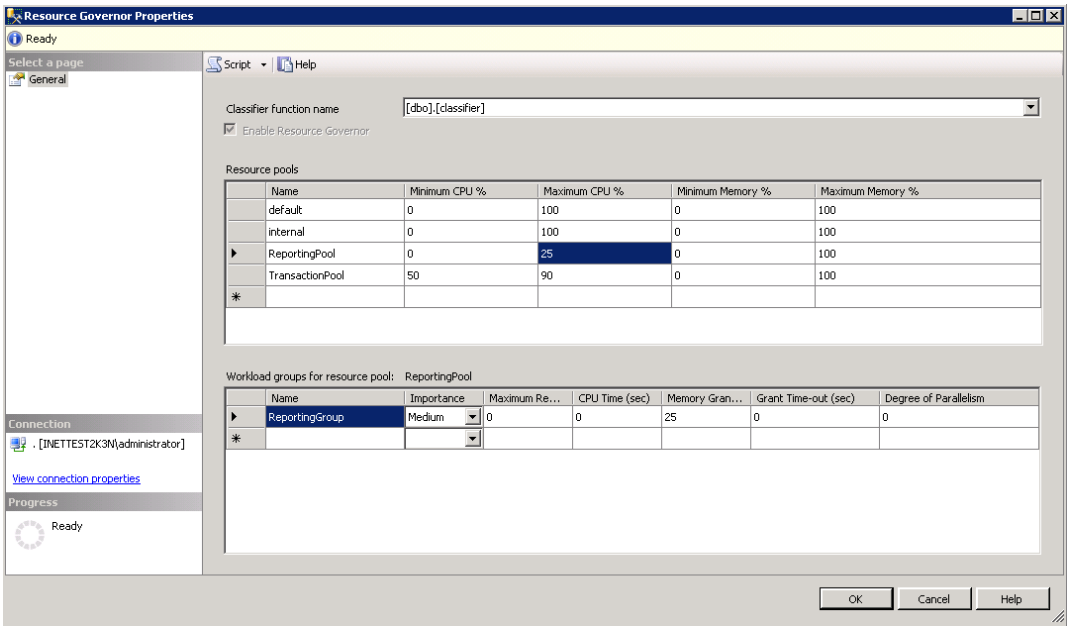
6. To see what happens when you execute the scripts from both servers at the same time, leave the script running on the Report server, then on the Application server, paste the script back into the command prompt window. The result will be similar to what is shown below, where both the

Transaction Group and the Reporting Group are effectively splitting the available CPU between them.

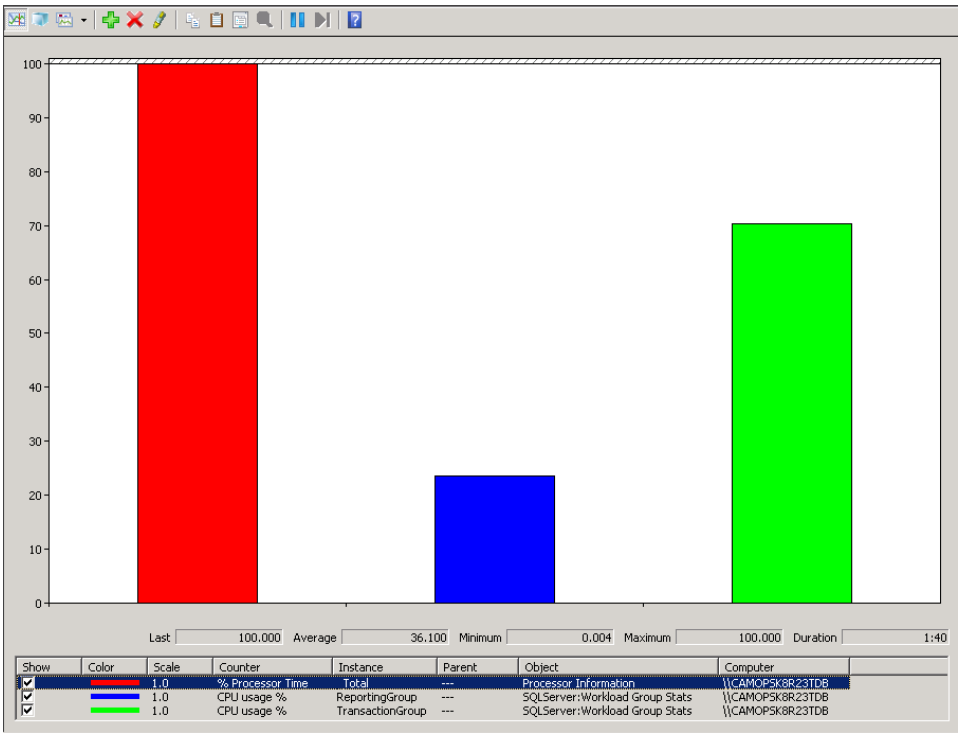


Under the current configuration, those reports would be able to access “up to” 50% of the available CPU on the SQL Server.

7. 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.

Monitor 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, there was an example about 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 which can be installed that provide a wealth of information about the usage of your report server.

Server Management Sample Reports Download and Installation Instructions

Attention: See the following link for sample reports and installation instructions: http://msftrsprodsamples.codeplex.com/wikipage?title=SS2008%21Server%20Management%20Sample%20Reports&referringTitle=Home

Reports

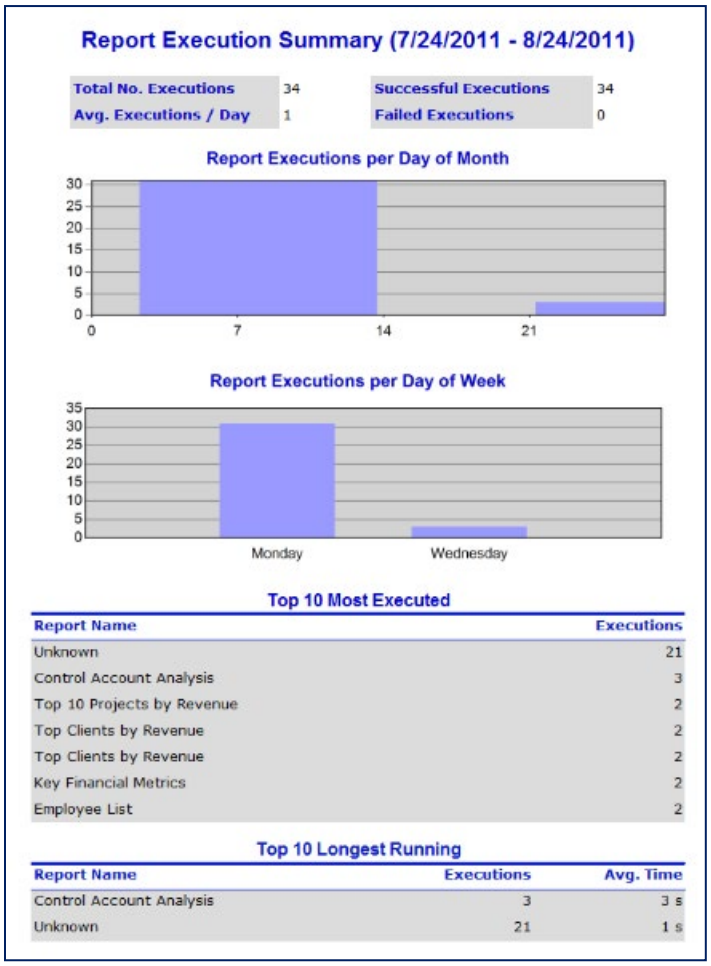
After you download and configure the sample reports, you can generate the following reports to provide information on your report server workload:

Report	Description
Execution Status Codes.rdl	This report 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	This report 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	This report shows the summary report execution information for a specific report within a specified date range.

The Report Execution Summary report may prove useful to you. It 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.



Report Execution Summary (7/24/2011 - 8/24/2011)

Total No. Executions	34	Successful Executions	34
Avg. Executions / Day	1	Failed Executions	0

Report Executions per Day of Month

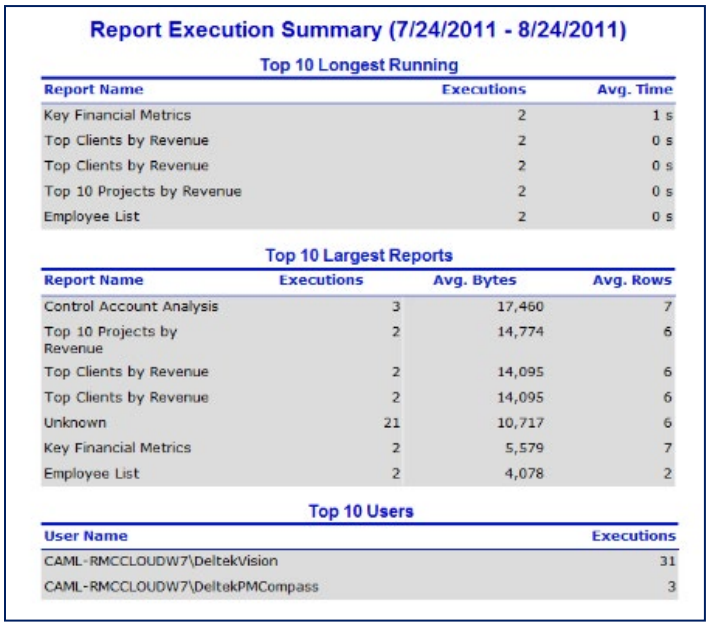
Report Executions per Day of Week

Top 10 Most Executed

Report Name	Executions
Unknown	21
Control Account Analysis	3
Top 10 Projects by Revenue	2
Top Clients by Revenue	2
Top Clients by Revenue	2
Key Financial Metrics	2
Employee List	2

Top 10 Longest Running

Report Name	Executions	Avg. Time
Control Account Analysis	3	3 s
Unknown	21	1 s



Report Execution Summary (7/24/2011 - 8/24/2011)

Top 10 Longest Running

Report Name	Executions	Avg. Time
Key Financial Metrics	2	1 s
Top Clients by Revenue	2	0 s
Top Clients by Revenue	2	0 s
Top 10 Projects by Revenue	2	0 s
Employee List	2	0 s

Top 10 Largest Reports

Report Name	Executions	Avg. Bytes	Avg. Rows
Control Account Analysis	3	17,460	7
Top 10 Projects by Revenue	2	14,774	6
Top Clients by Revenue	2	14,095	6
Top Clients by Revenue	2	14,095	6
Unknown	21	10,717	6
Key Financial Metrics	2	5,579	7
Employee List	2	4,078	2

Top 10 Users

User Name	Executions
CAML-RMCCLOUDW7\DeltekVision	31
CAML-RMCCLOUDW7\DeltekPMCompass	3

In addition, the following query 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/Pagination)')
AS varchar(200)),
  ScalabilityProcessing =
CAST(AdditionalInfo.query('data(/AdditionalInfo/ScalabilityTime/Processing)')
AS varchar(200)),
  EstMemPaginationKB =
CAST(AdditionalInfo.query('data(/AdditionalInfo/EstimatedMemoryUsageKB/Pagina
tion)') AS varchar(200)),
  EstMemProcessingKB =
CAST(AdditionalInfo.query('data(/AdditionalInfo/EstimatedMemoryUsageKB/Proces
sing)') 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

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.

Attention: 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:

1. Stop the RS service.
2. Modify the **ReportServer\bin\ReportServerService.exe.config** file.
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 of the rules are defined, the default trace level DefaultTraceSwitch defined in system.diagnostics/switches is used.

Attention: 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
- RunningJobs
- Processing
- ReportRendering
- HtmlViewer
- DataExtension
- EmailExtension
- ImageRenderer
- ExcelRenderer

- Notification
- Provider
- Schedule
- Subscription
- Security
- ServiceController
- DbCleanup
- Cache
- Chunks
- ExtensionFactory
- PreviewServer
- ResourceUtilities
- ReportPreview
- UI
- Crypto
- SemanticModelGenerator
- SemanticQueryEngine
- AppDomainManager
- HttpRuntime

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

Refer to the sections in **bold** 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,timetaken,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

Attention: For the Microsoft library article, 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.

Configure a Shared Location for Databases.enc

If your PM Compass deployment includes multiple web/application servers, or even just a dedicated process server, configuring a shared location for the **databases.enc** file eliminates the need to synchronize changes made to the **databases.enc** file across your servers.

To configure a shared path for the databases.enc file:

1. Ensure that the **databases.enc** file is synchronized across all servers.
2. Identify a server that can host the file share. This can be any server as long as it is located in the same data center as your PM Compass deployment.
3. Create a Windows file share on that server (for example, **\\server\share**).
4. Grant the service account(s) running the IIS Application Pool Identity and the Process Server service a minimum of modify rights to the share you created.
5. On all Web/Application Servers and Process Servers, modify the PM Compass **web.config** file (..\PMCompass\Web\web.config):
    a. Under **<appSettings>**, locate the **DatabasesEncDirectory** entry and uncomment it out. (It will be commented out by default.)
    b. For the setting value, enter the share path, not including the **databases.enc** file name. It should look similar to this, where **\\server\share** is the actual UNC path to your file share:

    <add key="DatabasesEncDirectory" value="\\server\share\" />
6. (The EPM SA application is installed only on the Web/Application tier so this step is only required to be performed on the Web/Application Servers.)

    On all Web/Application Servers, modify the EPM SA **web.config** file (..\EPMSA\Web\web.config)
    a. Under **<appSettings>**, add the **DatabasesEncDirectory** entry file as the first entry in the **<appSettings>** section.
    b. For the setting value, enter the share path, not including the **databases.enc** file name. It should look similar to this, where **\\server\share** is the actual UNC path to your file share:

    <add key="DatabasesEncDirectory" value="\\server\share\" />
7. Copy the **databases.enc** file to the share.
8. Rename the **databases.enc** file on all web/application and process servers to **databases.old**.
9. Restart IIS and the Process Server service on all applicable servers and run tests to ensure that PM Compass and Weblink can be accessed on all web/application servers and that the Process Server service is processing jobs correctly.
10. Make sure to check the Application Event Logs on all servers for any errors or warnings.

About Deltek

Better software means better projects. Deltek delivers software and information solutions that enable superior levels of project intelligence, management and collaboration. Our industry-focused expertise makes your projects successful and helps you achieve performance that maximizes productivity and revenue. www.deltek.com