Quest

Quest Knowledge Portal 2.9

Installation Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Knowledge Portal Installation Guide
Updated - July 2017
Version - 2.9

Contents

Introducing Quest Knowledge Portal

Microsoft SQL Server Reporting Services

Quest Knowledge Portal (QKP) was built on Microsoft SQL Server Reporting Services (SSRS) basis, further extending its functionality to meet Quest products users' needs.

Microsoft SQL Server Reporting Services is a server-based reporting platform that allows you to create and manage tabular, matrix, graphical, and free-form reports on data stored in the data sources (databases). You can also create ad hoc reports using predefined models and data sources. Reports that you create can be viewed and managed over your Internet or intranet connection using Microsoft Internet Explorer.

The reports you build using Reporting Services surpass traditional reporting by including interactive and Web-based features, such as:

- Drill-down and drill-through reports that enable navigation through layers of data
- Free-form reports that support content in vertical, nested, and side-by-side layouts, along with links to Web-based content or resources
- Secure, centralized access to reports over remote or local Web connections
- Automated delivery of reports through subscriptions

Knowledge Portal

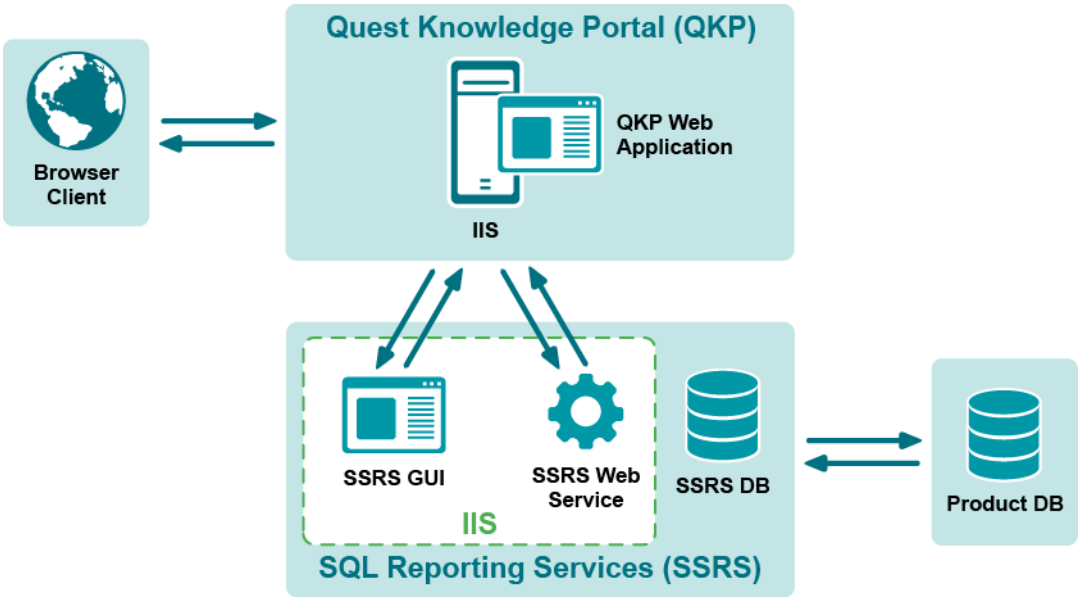
Knowledge Portal extends Microsoft SQL Server Reporting Services capabilities to provide easy report management and delivery.

Knowledge Portal enables you to:

- View the reports on data collected by Quest products
- Easily apply filters to the reports
- Facilitate data source management
- Subscribe to the reports
- Search through the report names and descriptions for the ones you need
- Create custom reports using Report Builder and predefined report models
- Organize the structure of the folders that reports are stored in

- Easily apply the necessary properties (settings) to reports and folders
- Modify report presentation on the fly (sorting order, fields visibility)

Knowledge Portal architecture is shown in the figure below.



What's Inside

The following components are involved in Knowledge Portal operation:

1. Product database—SQL Server database storing data collected by the product (InTrust, Reporter, etc.); reports are generated on that data and RDL files (report definitions)
2. SSRS DB—Reporting Services database storing information required for reporting (for example, .RDL files defining report structure)
3. SSRS Web Service—main service that is responsible for report generation and delivery
4. SSRS GUI—Report Manager, a component of Reporting Services that provides for configuration of reporting process (delivery options, scheduling, etc.) and report management (filtering, properties configuration, etc.)
5. Knowledge Portal—web application designed to simplify report management tasks, providing user-friendly interface and enhanced functionality (for example, arrangement of reports and folders, property application for multiple reports, etc.). In fact, this is an add-in for SSRS; for some tasks, users are redirected to SSRS GUI (like exploring filtering parameters, changing data source name, etc.). Reports and other predefined product-specific objects are brought in by Report Packs (for example, Reporter Report Pack).
6. Browser—Microsoft Internet Explorer used on the client computers to work with Knowledge Portal.

Knowledge Portal operation takes place as follows:

1. Browser client interacts with the Knowledge Portal interface: a user connects toKnowledge Portal, selects a report to open, and clicks View Report.
2. Knowledge Portal web application sends a request to SSRS web service—for this, an appropriate SSRS role is required for the account under which Knowledge Portal is running.
3. SSRS web service turns to the database, gets the required data, and fills in the report fields, and returns the generated report to the Knowledge Portal web application to be finally displayed to the end user. To access the database, it is recommended to use the credentials stored on server. For details, refer to the Configuring Access Rights topic.
4. Ready reports are delivered to users through scheduled subscriptions (sent by email, or stored to a file share)

Installation

System Requirements

Before installing Knowledge Portal, ensure that your system meets the following minimum hardware and software requirements.

Server Side

Platform	Intel x86, Itanium 64-bit, x64
Memory	512 MB or more (1 GB recommended)
Hard disk space	Min 50 MB
Operating system	Any of the following: • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 • Microsoft Windows Server 2003 with or without SP1 • Microsoft Windows Server 2003 R2
Additional software	Web server based on Microsoft Internet Information Services (IIS) 5.0 or higher, with ASP.NET 4.0 Microsoft.NET Framework 4.0 Microsoft SQL Server Reporting Services—any of the following versions:

	• 2016 • 2014 • 2012 • 2008 R2 • 2008 • 2005

Before you install Knowledge Portal on a computer running Windows Server 2012, you must do the following:

1. Open Server Manager and select **Local Server** from the left pane.
2. Then click **Manage** from the toolbar an select **Add Roles and Features**.
3. The Add Roles and Features wizard opens. On the **Select role services** screen, select **Web Server Role (IIS) | Role Services**.
4. In the feature list, expand **Web Server (IIS) | Web Server | Security** and select the **Basic Authentication** and **Windows Authentication** features.
5. Then expand **Web Server (IIS) | Web Server | Application Development** and select the **ASP.NET 4.0** feature.
6. Complete the wizard.

If you plan to use a web server based on Microsoft IIS 6.0, make sure ASP extensions are allowed.

If you plan to use a web server based on Microsoft IIS 7.0, do the following:

1. In the Control Panel, click **Programs**.
2. Select **Programs and Features | Turn Windows Features on or off.**
3. In the Windows Features dialog, select the **Internet Information Services | Web Management Tools | IIS 6 Management Compatibility** feature.

Before you install Knowledge Portal on a computer running Windows Server 2008, turn off User Account Control (UAC). Otherwise, the component will not install. Also, UAC must not be activated while Knowledge Portal is running.

You can use a local or remote installation of Microsoft SQL Server Reporting Services. For details, see the Connection to Knowledge Portal and Product Database topic.

Client Side

Platform	Intel x86
Screen resolution	Minimum 800x600 (1024x768 recommended)
Color depth	16 bit
Operating system	Any of the following: • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012

	• Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 • Microsoft Windows Server 2003 R2 • Microsoft Windows Server 2003 with or without SP1 • Microsoft Windows XP SP1, SP2
Additional software	Microsoft Internet Explorer 7.0 or later

Minimal Rights and Permissions

1. To install Knowledge Portal, the user account under which the setup is launched must have the following permissions:
    - Must be a member of the local **Administrators** group on the computer where the setup is run.
    - Must have the **System Administrator** role for the Microsoft SQL Server Reporting Services.
2. To install the Report Packs, the user account under which the Report Pack setup is launched must have **System Administrator** role for the SSRS.
3. To start the Knowledge Portal, a user must have the **Read** permission for **%WinDir%**.

NOTE: Generally, for the account that will be used to access the Knowledge Portal, Data Source properties are used to assign the required credentials (see the Configuration topic for details). This account must belong to the same domain where SSRS hosting the Knowledge Portal is installed, otherwise membership in the Authenticated Users group (for SSRS domain) is required.

4. To view reports and data sources, the user account must have:
    - **View Folders** and **View Reports** permissions on the **Home** folder and on the necessary subfolders (where the user's reports are stored) of the **\QKP** folder in SQL Reporting Services.
    - **View Data Sources** permission on the **\QKP\SharedDatasources** folder in SQL Reporting Services.
    - **View Resources** permission on **\QKP\<Product>\SharedResources** folder in SQL Reporting Services. (for the **<Product>** folder, substitute the folder of the Quest product Report Pack you use; this can be, for example, Reporter, or InTrust), and on the **\QKP\SharedResources** folder.
5. To create a report with Report Builder, a user will need the **Execute Report Definition** permission on the site level. To save a newly created report in the .RDL file on SSRS, **Manage Reports** permission on target folder with reports is also required.
6. To modify a report (for example, customize report view, or edit report in Report Builder or Microsoft Visual Studio), a user will need **Manage Reports** permission on this report (stored in the corresponding folder with reports under **\QKP**).
7. To work with models and model-based reports, **View Models** and **View Resources** permission on the **\QKP\SharedDatasources** folder in SQL Reporting Services is required.

NOTE: If you have no need for such granular rights assignment, the user account can be assigned the following SSRS roles:

- **Content Manager** role for the **QKP\SharedDatasources** folder and for the folder where the report is located (under the **\QKP** folder) in SQL Reporting Services.
- **Browser** role for the **Home** folder in SQL Reporting Services. However, some additional permissions are required for users who need to work with models and model-based reports (view reports and change their settings) but who have only the Browser role for these reports - **Manage Models** permission on the **\QKP\SharedDatasources** folder in SQL Reporting Services.
- The **Publisher** and **Content Manager** roles can provide the **Manage Reports** permission.

Rights and roles are assigned as explained in the Configuring Access Rights topic.

Checking for Reporting Services on SQL Server

To install Knowledge Portal and the Report Packs, you have to check whether the Reporting Services is installed and configured on your SQL Server, as explained below.

To check whether Reporting Services is running locally

1. Go to **Programs |Microsoft SQL Server | Configuration Tools** and launch the **Reporting Services Configuration** utility.
2. The utility displays the SSRS service status and checks whether all required configuration data is specified. It also displays SSRS virtual directories (Report Server virtual directory and Report Manager virtual directory).
3. If these virtual directories are other than the default, you will have to specify them during the Knowledge Portal setup.

To check whether Reporting Services is running remotely

1. In the Internet Explorer address bar, type:
   `http://<your_sql_server_name>/reports`
2. Check whether the SSRS Report Manager window is displayed. If not, you need to investigate and resolve the problem locally. The cause may be one of the following:
   - SSRS service is not running
   - SSRS Report Manager uses a different virtual directory
   - Your account does not have enough access rights.

If you are already using SQL Server, Reporting Services is a part of your SQL Server deployment. Otherwise, see the New Installation (Reporting Services) MSDN article for details.

Installing Knowledge Portal

CAUTION: **Knowledge Portal can be installed either on the computer where SSRS is running or on a dedicated computer.**

To install Knowledge Portal

1. Run the Knowledge Portal Setup.
2. Specify your full name and organization.
3. Specify the installation folder and make sure to select the Knowledge Portal.
4. Select the country where you are performing installation. This specifies whether or not you are participating in the Quest Software Improvement Program by default. Depending on your choice, you may be asked whether you want to opt in; for some countries, participation will be enabled automatically.

NOTE: The Quest Software Improvement Program involves Quest automatically receiving anonymous usage statistics from the Quest software you install. No personal identifying data (such as account names) is included in this feedback. The purpose is to determine which features are most popular and find out how their use can be streamlined.

The following information is transmitted:

- Hardware configuration
- Which product features are used
- External IP addresses

Participation in the program is voluntary. For details about opting into and out of the initiative, see the Installing and Configuring InTrust Components topic in the InTrust Deployment Guide.

5. Specify the site and virtual directory where to install the Knowledge Portal.
6. Next, select the report server that you want to associate Knowledge Portal with. Setup automatically selects one of the available report servers. If the automatic choice is not suitable for you, select another report server by clicking the button next to the **Report Server Web Service URL** box.

If setup fails to detect reporting servers that should be available, try editing your Windows Firewall configuration to allow WMI connections. For that, do one of the following:

- In the Group Policy Object Editor MMC snap-in, set **Local Computer Policy | Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall | Domain Profile | Windows Firewall:Allow inbound remote administration exception** to **Allow**.
- In the Windows Firewall Settings dialog box, go to the Exceptions tab, and enable the exception for **Windows Management Instrumentation (WMI)** in the list of options.

7. Specify the default user name and password that will be used for:
   - Connecting to the SQL Server hosting the product databases
   - Searching for accounts in Active Directory when granting access rights to report users

NOTE: This user account should be granted the **Log on as a service** right on Windows 2003-based computers where Knowledge Portal is installed.

8. Click **Next** and wait for the installation to complete.

Installing Report Packs

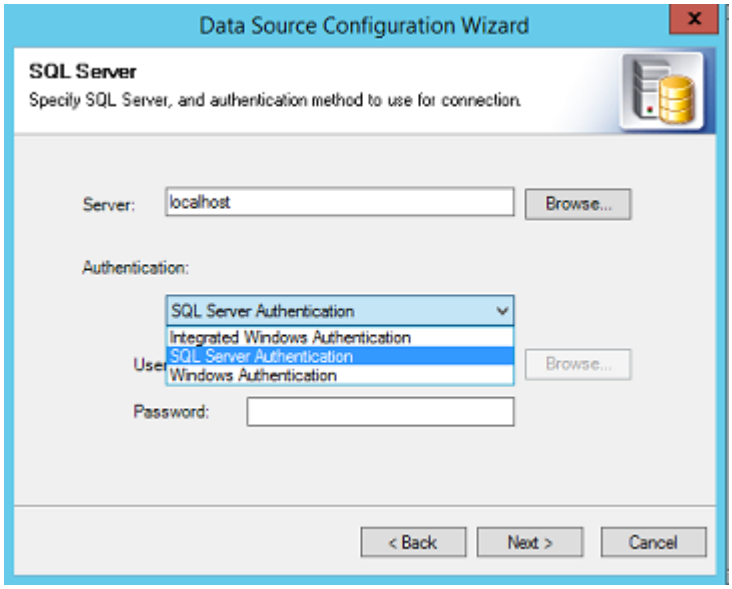
Report Packs can be installed on the same computer with the Knowledge Portal, or on the different computer.

To install a Report Pack

1. Run the Report Pack setup.
2. Next, specify the URL of report server, for example:
   `http://my_sql_srv/report_server`
   –or–
   `https://my_sql_srv/report_server`
3. To get data for reports provided in the Report Pack, you need to associate the Data Sources (Reporting Services entities) with the corresponding product databases. This should be done on the Configure Data Sources step. Click **Configure** to provide the settings required for association.

> **NOTE:** You can skip data source configuration in the setup; then you will have to configure your data sources later, as described in the Configuring Data Sources topic.

4. In the Data Source Configuration dialog, select the data source to configure and click **Modify**. The Data Source Configuration Wizard is started to help you with initial configuration of the data source.
5. On the Specify SQL Server step, enter the name of SQL Server where the product database resides, or click **Browse** to select server from the list of available SQL Servers. Specify authentication method to use for connection.



Connection settings will be applied to this data source and used when getting data for the reports and also when removing the temporary tables from the database. (By default, a special Temporary Tables Clean-up job is configured during the setup to periodically clean up the databases from temporary tables that are created during report generation. For details, refer to the Knowledge Portal User Guide.)

> **NOTE:** To schedule this job, you should select **SQL Server Authentication** or **Windows Authentication**. If **Integrated Windows Authentication** is used, the clean-up job cannot be scheduled.

6. On the **Specify Database** step, you can either select a database from the list, or enter a name for a new database to create.
7. Click **Next** and wait for connection test to complete. Click **OK** to finish data source configuration.

NOTE: For Temporary Tables Clean-up job schedule to be applied, make sure SQL Server Agent is running. If not, start the Agent, then connect to the Knowledge Portal, select the necessary data source and use the **Manage Data Source** menu command to schedule the clean-up.

To install another Report Pack, follow the same steps. On steps 5–8, select the corresponding data source and associate it with the database you need.

Starting Knowledge Portal

After you install the Knowledge Portal and the Report Packs, you can start it, for example, by selecting **Programs | Quest | Knowledge Portal | Knowledge Portal** in the Start menu.

Also, you can connect to the Knowledge Portal by typing its URL in the Internet Explorer address bar in the following format:

```
http://<portal_server_name>/<QKP_virtual_folder>
```

-or-

```
https://<portal_server_name>/<QKP_virtual_folder>
```

For example:

```
http://myreportserver/QuestKnowledgePortal
```

When supplying the URL, you can enter the path to Knowledge Portal's sub-entity (for example, InTrust) you want to be displayed as the root node of the treeview. For that, use the following format when entering the URL:

```
http://<portal_server_name>/<QKP_virtual_folder>/?path=<path_to_QKP_sub-entity>
```

-or-

```
https://<portal_server_name>/<QKP_virtual_folder>/?path=<path_to_QKP_sub-entity>
```

For example:

```
http://myreportserver/QuestKnowledgePortal/?path=/QKP/InTrust
```

Knowledge Portal main page is displayed; to work, for example, with InTrust reports, select InTrust in the tree on the left, and browse for the report you need. To work with the data sources, click the corresponding tab.

Upgrade

Upgrading Knowledge Portal

Seamless upgrade from the following Knowledge Portal versions is supported:

- 2.8
- 2.7
- 2.6

To upgrade Knowledge Portal, run the setup and follow the steps of the wizard (described in the Installing Knowledge Portal topic).

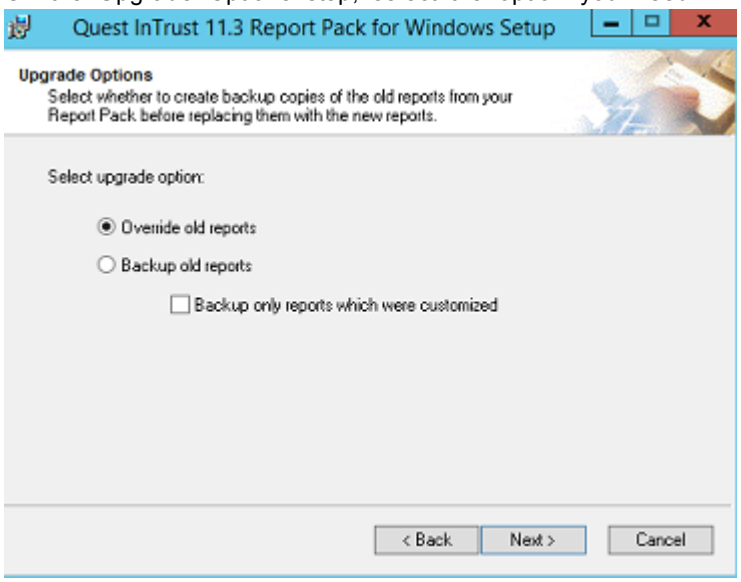
Upgrading Report Packs

Upgrades to Report Packs released prior to Knowledge Portal 2.7 will be available after the release of the corresponding product (following the Knowledge Portal release).

You can install new Report Packs (without removing the old ones) as described in the following procedure.

To upgrade the Report Pack

1. Run the Report Pack setup and follow the steps of the wizard.
2. On the Upgrade Options step, select the option you need:



- **Override old reports**
  Select this option if you want old reports to be replaced with the new ones. No backup copies of the old reports will be kept.
- **Backup old reports**
  Select this option if you want to install new reports, keeping backup copies of the old reports. These copies will be stored in the same location where the corresponding new reports are kept (for example, in the **InTrust| InTrust for Servers and Applications**), in the folder named like **Old<*number*>**. Here the ***<number>*** is increased by 1 after each Report Pack upgrade.

If you want to create the backup copies only of those reports that were customized, select the corresponding check box.

NOTE: You can select the **Backup only reports which were customized** option only if you run the setup locally on the computer where the earlier version of the Report Pack was installed.

Configuration

Configuring Data Sources

Data sources are databases that store the information used in the reports. Knowledge Portal uses the concept of shared data sources defined by Microsoft SQL Server Reporting Services. For more information about shared data sources, see Microsoft SQL Server Reporting Services documentation, for example, the Shared Data Sources and Report-Specific Data Sources MSDN article.

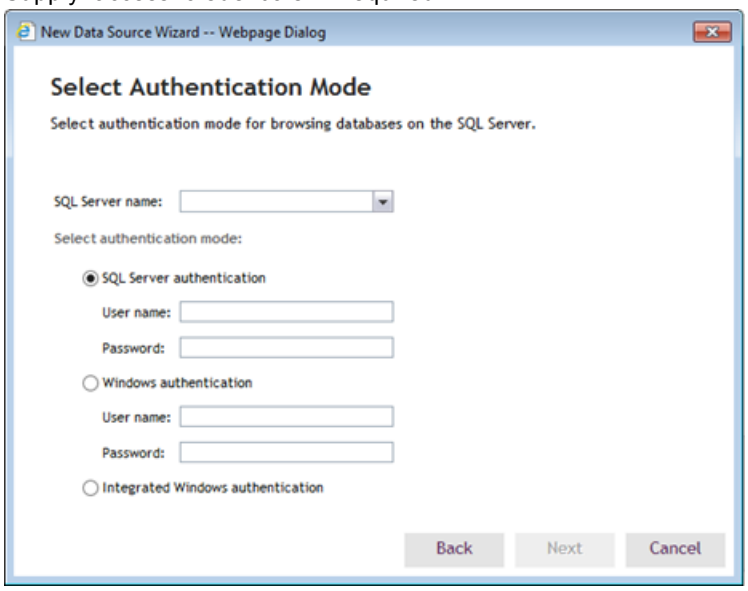
During the Report Pack setup process, predefined data sources are configured to point to corresponding databases. After installation, they are available when you click **Data Sources** in the Knowledge Portal.

If the data sources were not configured during the Report Pack setup, you should do it manually before you start generating reports. Sample procedure described in this section helps you associate predefined data source with your database. You can take similar steps to associate other data sources with the product databases.

To associate a data source with the product database

1. Click **Data Sources** in the left pane and select the required data source.
2. In the right pane, select **Modify Data Source** from the **Manage Data Source** menu to start the wizard.
3. On the Specify Data Source Name step, click **Next**.

4. On the Select Authentication Mode step of the wizard, specify the SQL Server where the product database resides, and select authentication method to be used for database access. Supply access credentials if required.



NOTE: To use **Windows authentication**, make sure the account you supply has the **Logon as a service right** if the client computer is running Windows 2003 or later.

If you select **Integrated Windows authentication**, the SQL server will be accessed under the account of user currently logged on. (For details, see the Configuring Access Rights topic). In this case, however, the Temporary Tables Clean-up job cannot be scheduled.

5. On the Select Database step, select the database you want to be associated with the data source, for example, **Test_DB**.
6. On the Select Products step, select the product that collects data to this database.
7. Finish the wizard.

Configuring Access Rights

It is recommended that you study this section to understand which accounts should be provided with which access rights.

To generate a report using the Reporting Services and fill it in with data stored in SQL Server database, a user should be able to operate as follows:

- Use one account (ACCOUNT1) to access the Reporting Services and work with reports (forms that data is presented in)—that is, to create, delete, edit, and organize reports. This account works within Reporting Services security context.
- Use another account (ACCOUNT2) to render data from the data source associated with the report—that is, to read data from the database, probably, create some temporary tables and clean them up, and so on. This account works within SQL Server security context.

NOTE: Usually, this account is configured by the Knowledge Portal administrator and stored securely on server.

So, to successfully generate a report and fill it with data, these accounts should be granted appropriate permissions in both of the following ways:

- Via the **Reporting Services role** assigned to ACCOUNT1 in the report's security settings (described below), in order to work with data presentation form (report)
- Via the **SQL Server database role** assigned to ACCOUNT2 by your database administrator, for working with the data itself (data source).

NOTE: You can use SSRS site-wide security settings, for example, to provide System User role to the users who need to work with Report Builder, and item-level security - to grant the necessary permissions on certain items (reports, folders, etc.) Refer to Using Role-Based Security for more information.

For different deployment scenarios and authentication methods to be used, refer to the Connection to Knowledge Portal and Product Database topic.

For minimal rights, permissions, and roles required for working with the Knowledge Portal, refer to the Minimal Rights and Permissions topic.

Using Shared Data Sources

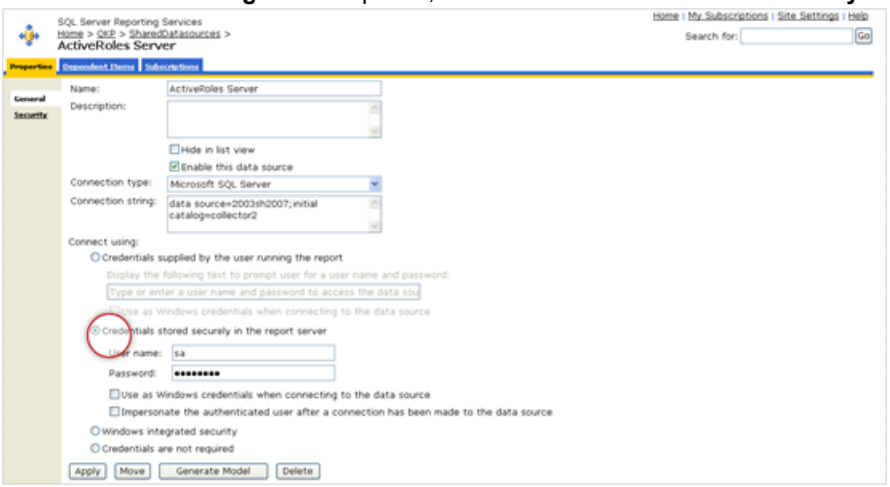
To simplify database access provisioning for ACCOUNT2, it is recommended that you configure the reports in the Report Pack to use credentials stored on server. For that, you can use the SSRS Report Manager, or Knowledge Portal Property Manager Wizard.

To configure report's data source using Report Manager

1. In Knowledge Portal, select a report in the reports tree.
2. Click **Change Report Properties** from the **Manage Report** options in the right pane. You are taken to Report Manager displaying report Properties page.
3. Click **Data Sources**, and for all data sources on that tab, select **A shared data source** option:

4. If no data source is specified, browse for the one you need.
5. Click **Apply**, then click **Back** to return to the Knowledge Portal.
6. Click the Data Sources tab, and select the necessary data source. Click **Change Data Source Properties** from the **Manage Data Source** menu options in the right pane. You are taken to Report Manager displaying data source **Properties**.

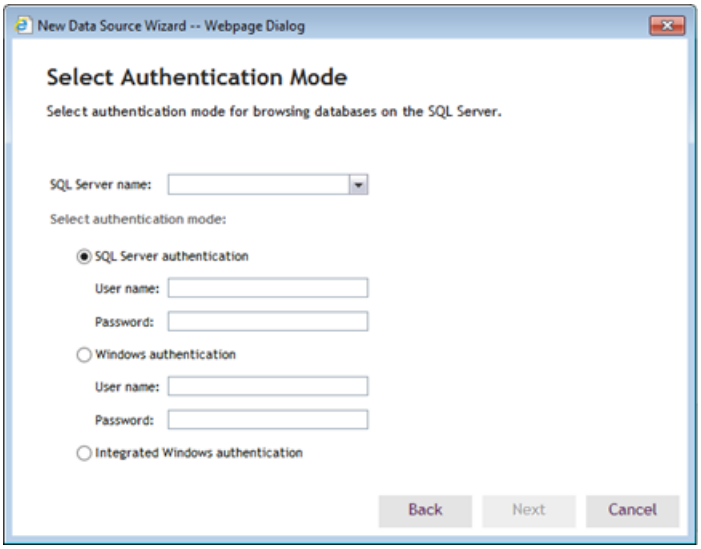
7. In the **Connect using** list of options, select **Credentials stored securely in the report server**:



8. Supply the user name and password to be used; if needed, select the check boxes with the corresponding options.
9. Click **Apply**, then click **Back** to return to Knowledge Portal.

Connection to Knowledge Portal and Product Database

Depending on the deployment scenario you select, different authentication types can be used when you configure connection settings. In particular, when configuring a data source, you will be prompted for authentication method, as shown below:



The following options are available:

- SQL Server authentication, which means that:
    a. Credentials of user currently logged on will be used to access the Knowledge Portal (ACCOUNT1 described above)
    b. SQL Server will be accessed under the account you specify during data source configuration (ACCOUNT2)
- Windows authentication, which means that:
    a. Credentials of user currently logged on will be used to access the Knowledge Portal (ACCOUNT1)
    b. SQL Server will be accessed under the account you specify during data source configuration (ACCOUNT2)
- Integrated Windows authentication, which means that credentials of the user currently logged on will be used to access both the Knowledge Portal and SQL Server (by default, without prompting for login name and password), that is, ACCOUNT1 and ACCOUNT2 are the same.

NOTE: To schedule a special clean-up job that will periodically remove the unnecessary temporary tables from the data source, you should use **SQL Server Authentication**, or **Windows Authentication**. If **Integrated Windows Authentication** is used, the clean-up job cannot be scheduled.

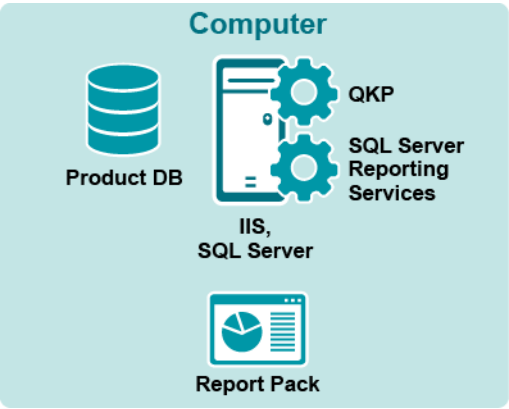
To access data stored in the product database, the account under which SSRS connects to SQL server should have a corresponding database role (typically, created by the product Report Pack's setup) or sufficient rights assigned.

- Scenario 1: All in One Place
- Scenario 2: SSRS Detached from SQL Server
- Scenario 3: Separate Knowledge Portal, SQL Server, SSRS
- Using Integrated Windows Authentication

Scenario 1: All in One Place

For evaluation purposes, you can make one computer to host all the required components, including:

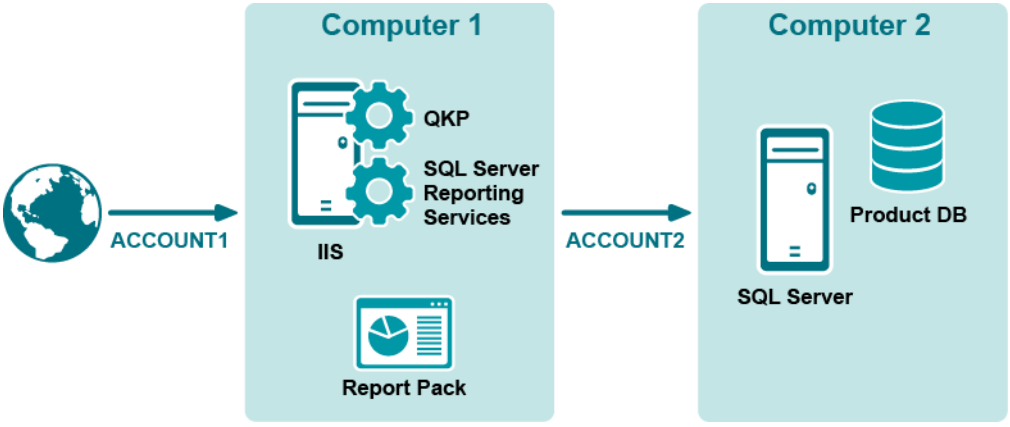
- SQL Server (where the product database are stored)
- SQL Server Reporting Services
- Knowledge Portal (QKP)
- Report Pack(s)



In this case, you can use any authentication method; Integrated Windows authentication does not require any additional configuration.

Scenario 2: SSRS Detached from SQL Server

The most typical deployment scenario (recommended) is to co-locate SQL Server Reporting Services and the Knowledge Portal—this will simplify security configuration. Product database can be located on a dedicated SQL Server.



Here a user will access the Knowledge Portal and SSRS under ACCOUNT1, and data from the product database is obtained using ACCOUNT2.

> **TIP:** It is recommended that your reporting server use SSL and HTTPS protocol for client-server communication, as described below.

You can use the Knowledge Portal Property Management Wizard to grant ACCOUNT1 access to the necessary reports, or do this within SSRS Report Manager. For details, see the Access to Reports and Folders topic.

To provide for database access under ACCOUNT2, it is recommended to use the credentials stored in the report server, as described above.

When selecting authentication mode, any of the options described above can be used:

- SQL Server authentication
- Windows authentication
- Integrated Windows authentication (with NTLM protocol, or with Kerberos protocol (default)).

If you want to use a single account instead ACCOUNT1 and ACCOUNT2 (that is, the credentials of the user currently logged on will be used to access the Knowledge Portal and the database), you can select Windows authentication, or Integrated Windows authentication. However, to use Integrated Windows authentication with Kerberos authentication protocol, take the following steps:

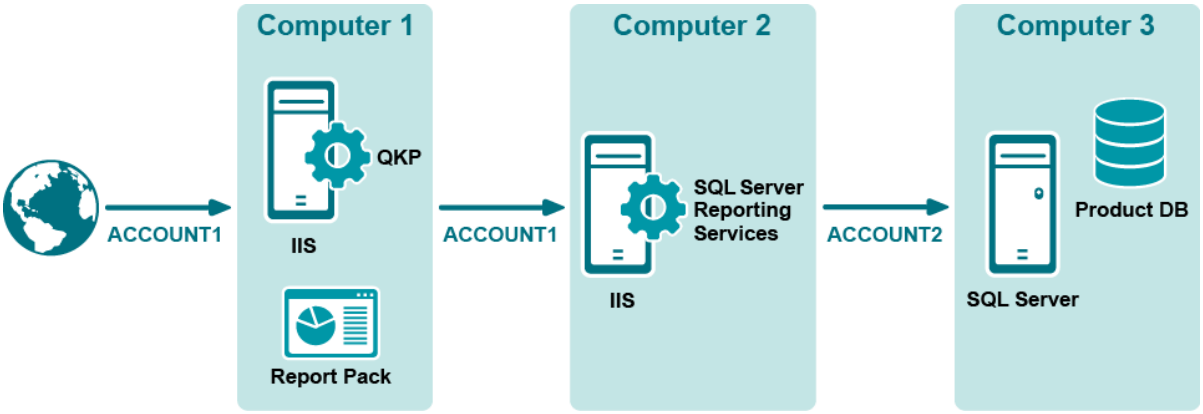
1. In **Active Directory Users and Computers** MMC snap-in, select the user account under which the product database will be accessed.
2. Select **Properties** and click the **Account** tab.
3. Make sure the **Account is sensitive and cannot be delegated** option is cleared.
4. Select **Account is trusted for delegation**.
5. Select the computer where the SSRS and Knowledge Portal are installed.

6. Select **Properties** and click the **General** tab.
7. Select **Trust computer for delegation**.

NOTE: If Integrated Windows authentication is used for database access, then temporary table clean-up job cannot be scheduled for the corresponding data source. To provide for this job scheduling, use other authentication method.

Scenario 3: Separate Knowledge Portal, SQL Server, SSRS

As shown in the figure below, SQL Server Reporting Services and the Knowledge Portal can be installed separately.



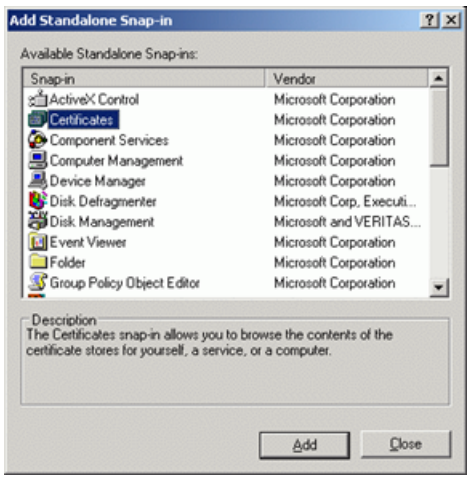
In this case it is recommended that you use either SQL Server authentication or Windows authentication method.

In case of remote SSRS installation, users are prompted for login name and password each time they connect to the Knowledge Portal (on Computer 1). These credentials are transmitted to SSRS (on Computer 2) as plain text. To secure them, you have to ensure that the following are true:

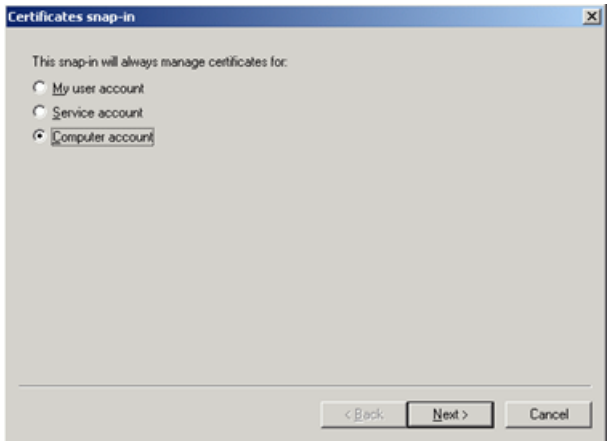
1. Your SSRS deployment is configured to use SSL (Secure Socket Layer)
2. The HTTPS protocol is used for communication (that is, the link to SSRS you specify during the setup must begin with https://).

To provide a certificate for trusted connection over HTTPS with remote SSRS

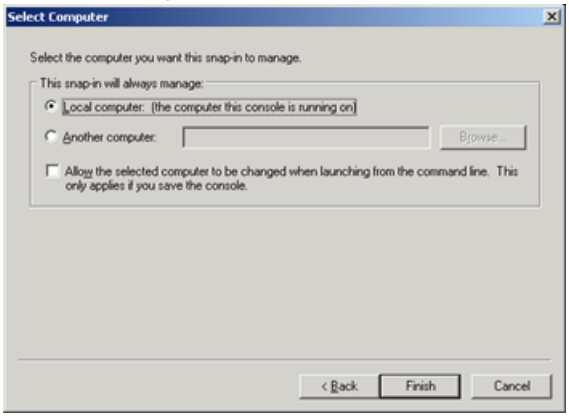
1. Run Microsoft Management Console and use the Add/Remove Snap-In command to add the Certificates snap-in:



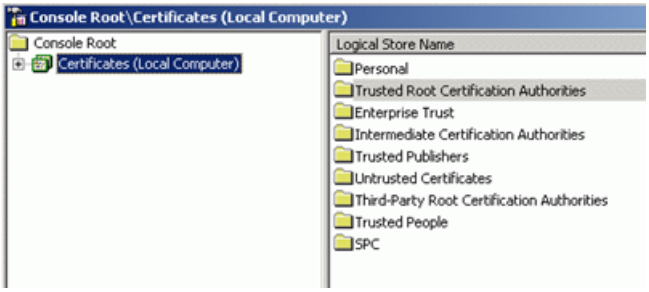
2. Select the **Certificates** snap-in from the list, click **Add**. Then select the **Computer account** option and click **Next**:



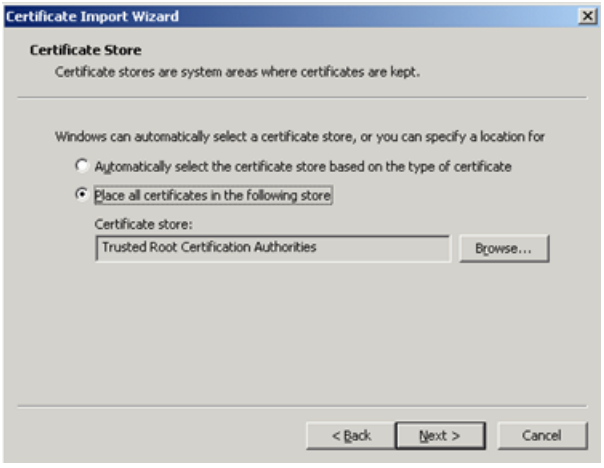
3. Select the computer to be managed (the one where SSRS is installed):
   - If SSRS is installed on the local computer, select **Local computer**.
   - If SSRS is installed on a remote computer, select **Another computer** and browse for SSRS server you need.



1. Click **Finish** and then close the Add/Remove Snap-In dialog by clicking **OK**.
2. In the **Certificates** snap-in, right-click **Trusted Root Certification Authorities**.



3. From its shortcut menu, select **All Tasks| Import**.
4. On the File to Import step of the Certificate Import Wizard, specify the certificate for the required holder (that is, for the Web server where the SSRS is installed).
5. On the **Certificate Store** step, select the **Place all certificates in the following store** option, and leave the default store (**Trusted Root Certification Authorities**):



6. Complete the wizard.

Using Integrated Windows Authentication

If you want to use Integrated Windows authentication, make sure it uses Kerberos authentication protocol, and take the following steps to make such authentication work properly:

1. In the **Active Directory Users and Computers** MMC snap-in, select the user account under which the product database will be accessed.
2. Select **Properties** and click the **Account** tab.
3. Make sure the **Account is sensitive and cannot be delegated** option is cleared.
4. Select **Account is trusted for delegation**.
5. Select the computer where the SSRS and Knowledge Portal are installed.
6. Select **Properties** and click the **General** tab.
7. Select **Trust computer for delegation**.

Access to Reports and Folders

Report security settings allow you to provide report users with access rights to the particular reports or folders they need.

> **NOTE:** Security settings are inherited from the report folder, so you may want to proceed with the report folder rather than with individual reports.

There is a special role named "QKP—Traverse Folders" that allows users to view child folders or reports using their full path in the folder hierarchy, but prevents these users from viewing parent folders contents.

To apply security settings (i.e., configure access rights) for multiple reports, the Property Manager Wizard can be used. To apply security settings to a single report, use the **Change Security Settings** command from **Manage Report** menu and make the necessary changes with Report Manager.

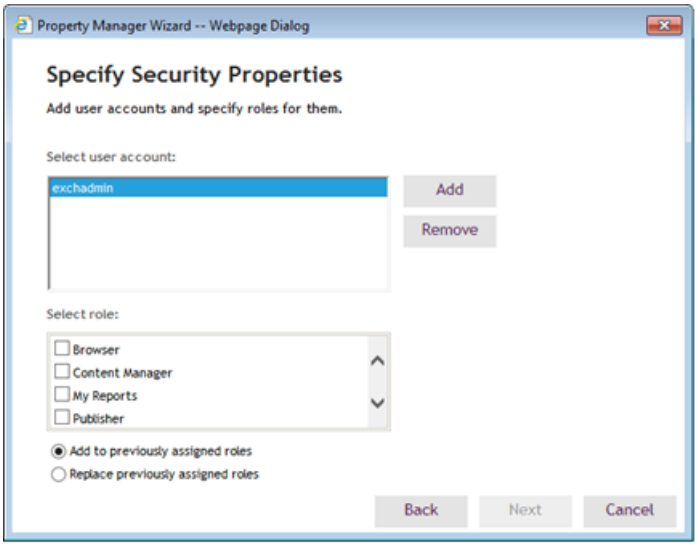
> **NOTE:** Custom roles (like 'QKP - Traverse Folders') can be created and automatically included into roles list in Report Manager only in SSRS 2005. To work with custom roles in SSRS 2008, follow the instructions provided in the How to: Create, Delete, or Modify a Role (Management Studio) MSDN article.

To specify security settings for multiple reports

1. Start the wizard by clicking on the **Property Manager Wizard** tab in the toolbar.
2. On the **Select Property Application Mode** step, select the **Apply specific values** option.
3. Select the reports or folders you want.

> **NOTE:** For the certain reports or folders to be displayed properly, you may need to assign the **QKP—Traverse Folders** role (or the one with not less privileges for viewing the reports) to user who is to get access to these reports or folders in the reports tree. Remember that this predefined role is displayed in SSRS 2005 Report Manager only.

4. On the Select Properties to Apply step, select **Security properties**.
5. On the Specify Security Properties step, specify accounts and roles for them to grant the users access to the reports or folders they need:
    a. Click **Add** to add an account to the list. On the Select User or Group dialog, enter the first letters of the account name to look for, and click **Search**.
    b. In the list of accounts found, select the account you need, and **click** OK.
    c. Select the account you need, and from the list of SSRS roles, select the role or roles to be assigned to this account.



NOTE: To exclude an account from role assignment, select it in the list, and click **Remove**.

If you select to **Replace previously assigned roles**, then security settings being configured will take precedence over the ones you might have set for selected reports and user accounts with Reporting Services (as described below).

6. Finish the wizard.

To specify security settings for a single report

1. Select the required report or folder in the Knowledge Portal, and select **Change Security Settings** from the **Manage Report** menu. You are taken to Reporting Services Report Manager.

2. Click **Edit Item Security** to specify roles for the user accounts as needed.
3. When finished, click **Back** to return to Knowledge Portal.

Example

We assume that InTrust Audit data source is associated with the the **ITAudit_DB** database on the SQL Server named **SQLSRV**. To provide a sample user account **Alex** from the **IT** domain with access to the 'Group Membership Management' report, you need to check the following:

1. Within SSRS, this user (or the group this user belongs to) has the **Browser** role for the report and its parent folders (up to the root folder).
2. The account specified in the InTrust Audit data source properties for the 'Group Membership Management' report was granted access to the **ITAudit_DB** database on **SQLSRV** server.

This can be achieved by taking the steps described below.

To provide an account with access rights required for report generation

1. In Knowledge Portal, click the **Reports** tab in the left pane and navigate to the 'Group Membership Management' report.
2. Select the **Change Security Settings** command from the **Manage Report** menu options.
3. On the **Properties** tab in Report Manager, click **Edit Item Security** to assign the **IT\Alex** account the **Browser** role to currently selected report. Refer to Report Manager Help if necessary.
4. When finished, click **Back** to return to Knowledge Portal.
5. In Knowledge Portal, click the **Data Sources** tab.
6. Select the InTrust Audit data, and click **Modify Data Source** from the **Manage Data Source** menu options.
7. On the **Select Authentication Mode** step of the wizard, select the **Windows Integrated authentication** option.
8. Finish the wizard.

NOTE: Remember to assign sufficient access rights to the user account that will access the **ITAudit_DB** database.

To test access rights, you can connect to the Knowledge Portal under the sample **IT\Alex** account, click the **Reports** tab, select the 'Group Membership Management' report and click **View Report** option. The report should be generated and displayed in the right pane.

Role-Based Security

SQL Server Security Model

The SQL Server security model involves security policy and authentication, roles, permissions, and passwords. In particular, fixed database roles allow the database administrator to assign certain groupings of database administrative permissions. Instead of giving a user full database owner functionality, fixed database roles allow the DBA to assign only the database-level permissions to be granted to the user.

For example, if the DBA wants to give a particular user the ability to create objects in the database, the DBA could just add that database user account to the **db_ddladmin** fixed database role.

Role	Description
db_owner	Performs all maintenance and configuration activities in the database.
db_accessadmin	Adds or removes access for Windows users, groups, and SQL Server logins.
db_datareader	Reads all data from all user tables.
db_datawriter	Adds, deletes, or changes data in all user tables.
db_ddladmin	Runs any Data Definition Language (DDL) command in a database.
db_securityadmin	Modifies role membership and manages permissions.
db_backupoperator	Backs up the database.
db_denydatareader	Cannot read any data in user tables within a database.
db_denydatawriter	Cannot add, modify, or delete data in any user tables or views.

SQL Server roles for the accounts used to work with reports are a part of system requirements; they are provided by your database administrator.

Reporting Services Security Model

Knowledge Portal is based on the Reporting Services and uses its security model to allow authorized users work with exactly the reports they need.

SQL Server Reporting Services implements a flexible, role-based security model to protect reports and reporting resources. To provide an account with access rights to a report or folder, you can assign it an SSRS role.

NOTE: Custom roles (like 'QKP - Traverse Folders') can be created and automatically included into roles list in Report Manager only in SSRS 2005. To work with custom roles in SSRS 2008, follow the instructions provided in the How to: Create, Delete, or Modify a Role (Management Studio) MSDN article.

The following predefined roles are available:

Role	Description
Browser	Use to view folders, reports, and to subscribe to reports.
Content Manager	Use to manage all aspects of content, including creating folders, reports, and data sources.
My Reports	Use to publish reports, create folders, and manage resources in the My Reports folder.
QKP—Traverse Folders	Allows users to access child folders using their full path in the folder hierarchy but prevents these users from viewing parent folders contents.
Publisher	Use to publish reports.
Report Builder	Use to view report definitions (RDL).

To learn more about role-based security in SSRS, refer to the Using Role-Based Security MSDN article.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product