Quest® InTrust 11.4.2

Leveraging Microsoft SQL Server Reporting Services Integration for

Advanced Reporting

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.**

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

InTrust Leveraging Microsoft SQL Server Reporting Services Integration for Advanced Reporting
Updated - September 2020
Version - 11.4.2

Contents

Microsoft SQL Server Reporting Services Integration Overview

InTrust provides two ways to take advantage of SQL Server Reporting Services:

- Automated report generation achieved by setting up task-based workflows in InTrust Manager
  The typical scenario is to configure a scheduled task that runs regularly and includes gathering events to an audit database (done by gathering jobs) and generating reports (done by reporting jobs).
- Interactive report viewing in Knowledge Portal
  This Web console enhances the Reporting Services user experience and streamlines on-demand reporting.

For details about automated workflows, see the Understanding Jobs and Tasks topic. For information about reporting jobs in particular, see the Reporting Job topic.

To get started with interactive reporting, see the Interactive Reporting topic.

Interactive Reporting

Knowledge Portal is a Web-based application that uses Microsoft SQL Server Reporting Service for report generation. You can connect to the Knowledge Portal from InTrust Manager, or from any computer where Internet Explorer runs.

This system is separate from InTrust reporting jobs. The purpose of Knowledge Portal is to provide interactive reporting capabilities, including report generation, custom report creation, scheduling reports and subscribing to them.

If you correctly specified Knowledge Portal's virtual directory during InTrust setup, Knowledge Portal is available in the **Data Analysis** node in the InTrust Manager treeview. You can view and edit the Knowledge Portal URL using the **Reporting_default_QRS** organization parameter via Organization Parameter Editor. When you select this node, the Knowledge Portal URL is opened in the new window, displaying its Welcome page.

To start working with InTrust reports, when on the **Reports** tabbed pane, click the **InTrust** report folder.

To learn more about the Knowledge Portal installation and usage, refer to the Knowledge Portal documentation. In particular, to learn how you can benefit from using the Knowledge Portal when analyzing data collected by InTrust, refer to Working with Reports in Knowledge Portal.

Setting Up Reporting Services Data Sources

When InTrust reports are installed during the InTrust setup, several predefined shared data sources are created. After installation, reports related to InTrust are linked to the following data sources:

- InTrust Configuration
- InTrust Audit
- InTrust Alerts

To view reports on the alerts, audit or configuration data, you should configure certain data source to point to a corresponding database. Initial association is made during the setup so that InTrust Audit data source points to the InTrust audit database specified during InTrust installation, and so on. However, you can associate your data sources with other databases.

Sample procedure described in this section helps you associate predefined InTrust Audit data source with your InTrust audit database. You can take similar steps for other data sources.

To associate a data source with an InTrust audit database:

1. Click **Data Sources** in the left pane and select **InTrust Audit** data source.
2. In the right pane, select **Modify Data Source** from the **Options** 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 necessary InTrust audit 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 **Log on as a service** right if the client computer is running Windows 2003 or later. If you select **Integrated Windows authentication**, the server will be accessed under the default account specified during the Knowledge Portal setup.

5. On the Select Database step, select the database you want to be associated with the InTrust Audit data source, for example, **IT_AuditDB**. If you want to create a new database, click New.
6. On the Select Products step, select **InTrust**, which is the product that collects data to this database.
7. Finish the wizard.

Security Considerations

You have three options related to credentials used for data source access:

- SQL Server authentication
  Select this to specify SQL Server credentials.
- Windows authentication
  Use this option if Reporting Services and the audit database reside on different computers. The credentials for database access must be specified explicitly in such a configuration.
- Integrated Windows authentication
  Use this option if Reporting Services are running on the SQL server that hosts the audit database.

It is important to understand that Reporting Services make a distinction between data source privileges and report privileges. The privileges of the account you use must be broad enough both for data source access and for report compilation.

Otherwise, for example, the reporting job may be able to read all of the necessary data in the audit database but may not be able to make a report with this data.

Reporting Services grant access privileges through roles. Configure roles directly in the Reporting Services Web interface.

To configure Reporting Services security settings

1. Open the SQL Server Reporting Services home page.
2. Navigate to the necessary item (report or report folder), and open the **Properties** tab.
3. Use the **Security** link to modify report access privileges and the **Data Sources** link to modify data source access privileges.

For more information about Knowledge Portal security configuration, see the Knowledge Portal User Guide.

Working with Reports in Knowledge Portal

This set of topics describes how you can use Knowledge Portal to work interactively with Quest InTrust reports.

Knowledge Portal is an add-on for Microsoft SQL Server Reporting Services (SSRS) that allows you to view and manage InTrust reports shipped in the Knowledge Packs. In particular, Knowledge Portal helps you do the following:

- View reports on data collected by InTrust
- Manage InTrust data sources
- Schedule automatic report generation and subscribe to reports delivered by email or made available in a shared folder
- Launch Report Builder to create custom reports on the predefined InTrust model
- Organize the structure of the folders that reports are stored in, and search through the reports for the ones you need
- Easily apply custom settings to multiple reports and folders
- Simplify report data filtering by using enhanced, user-friendly filter parameters
- Instruct reports to import the necessary data from an InTrust repository when they are being generated

Knowledge Portal can be installed as part of InTrust suite setup; for detailed instructions, refer to Installing the First Server in InTrust Organization.

This set of topics explains how you can:

- Install a Report Pack with InTrust reports
- Work with predefined reports from a Report Pack
- Create your own reports using Report Builder and predefined InTrust model

Installing InTrust Reports

When you run the InTrust setup suite, you are prompted to select features to install, in particular, the Knowledge Packs you need. Being a part of the Knowledge Pack, reports are installed automatically. However, you may need to install a particular Report Pack later on—for that, follow the procedure described in this section.

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

You must run Report Pack setup under an account the has the **System Administrator** role in SSRS.

To install a Report Pack

1. Launch the Report Pack setup from InTrust autorun, opening the Knowledge Packs tab and selecting the Report Pack you need.
2. Specify your name and organization.
3. Next, specify the URL of report server, for example, **http://my_sql_srv/report_server** or **https://my_sql_srv/report_server**.

4. To get data for reports provided in the Report Pack, you need to associate the data sources (Reporting Services entities) with the corresponding InTrust databases (for example, Audit database). This should be done on the Configure Data Sources step. Click **Configure** to provide the settings required for association.

> **NOTE:** If the data source has been already configured, you will see the corresponding notification in the Connection Settings for that data source listed on Configure Data Source step. The **Modify** button will be disabled. You can skip data source configuration in the setup and use Knowledge Portal to modify that data source later.

5. In the Data Source Configuration dialog, select the data source to configure (for example, InTrust Audit) and click **Modify**. The Data Source Configuration Wizard is started to help you with initial configuration of the data source.
6. On the Specify SQL Server step, enter the name of SQL Server where the Audit 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 at 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.

7. On the Specify Database step, you can either select a database from the list, or enter a name for a new database to create.
8. 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, and then use data source’s options in the Knowledge Portal to schedule the clean-up.

9. If you have InTrust Reports already installed on the specified report server, you will be prompted for their upgrade scenario. 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 **InTrust | InTrust for Servers and Applications**), in the folder named after this pattern: **Old<number>**. Here the **<number>** is incremented 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.

To install another Report Pack, follow the same steps. On steps 5 to 8, work with the corresponding data source (InTrust Audit) and associate it with the database you need (InTrust Audit database).

Viewing Reports

Select the desired report in the tree in the left pane. Report description and filters are displayed on the right.

Go through the filter tabs to configure filtering parameters you need. Filtering parameter types and their usage are described in the Filtering Reports section of the Knowledge Portal User Guide. When configuring the filters, you can select or clear the Apply filters from this tab check box to activate or deactivate the filters on the tab (by default, this check box is selected). After activating the filters, you can specify the values you need.

> **NOTES:**
>
> - A report can have mandatory filters or parameters (i.e., those that will be applied anyway, regardless of this option), for example, the **Show filters** parameter on the **Misc** tab (if a report has only one filter tab, it is named Filters, and all filters and controls are located there). Such filters and parameters are always displayed with a gray check box on the left (selected) and require a value to be specified.
> - If you are using a filter of the **Like** type, then you can use wildcards in the filter value. For instance, if you are filtering report data by domain and need to report on the domains **Accounting_NY**, **Sales_NY** and **IT_NY**, you can enter the following in the "Domain like:" filter:
> **%_NY**
> The **%** sign is used in Microsoft SQL Server Reporting Services to represent any set of characters (instead of the commonly used ***** symbol).

Every report has the default filter values stored in the SQL Server Reporting Services database; use the following commands to work with default filter settings:

- Save filters to defaults
Use this command from the **Manage Filters** menu to save the specified values as the default ones for all report users. This means that when any user opens this report, the filter values will be the ones you specified. If a user makes no changes to these filters, they will be applied to report at generation time.
- Load filters from defaults
Use this command from the **Manage Filters** menu to apply the default (predefined) filter values.

> **NOTE:** The **Save filters to defaults** and **Load filters from defaults** commands allow you to keep your user-defined filter values even if you deactivate the filter (by clearing the **Apply filters from this tab** option). You can deactivate the filter you configured, and save it to default - then, after you use the Load command, the value you specified will be shown as the default one (configuration will not be lost even though the filter remains inactive).

If you do not want filters to be shown within the generated report, then on the **Misc** filter tab (or **Filters** tab), in the **Show filters** list select **No**.

Making Changes to Reports

Generally, the Property Manager Wizard can be used to apply specific properties (settings) to the reports (for example, filter settings or subscription settings). However, best practices recommend that you customize the report copies rather than the original reports.

For example, you can click **Organize Reports** from the **Manage Folder** menu to copy the reports you need to the desired location, or add your favorite reports to **My Reports** folder using **Add to My Reports** command.

Report-Driven Data Import

When you work with reports in Knowledge Portal, there is a **Specific Actions** area in the right pane. Currently, the **Data Import** option is available in this area for most InTrust reports, but not all of them. Use it to configure import of data required for the selected InTrust report from an InTrust repository to an audit database.

This process is similar to the report-driven data import you set up for your reporting jobs; it uses not only the database connection account, but also an importing account—the one under which data is imported from the source repository to the database.

The authentication method and credentials for the database connection are specified in step 5 of the Report-Driven Data Import Wizard (see the procedure described below). The specifics of using the importing account and database connection account are described in the following table.

Authentication method selected	Importing account that will be used	Database connection account that will be used
SQL Server Authentication (with the specified credentials)	InTrust Server account (specified during InTrust setup; for details, refer to InTrust Installation Guide and User Guide)	Specified credentials
Windows Authentication (with the specified credentials)	Specified credentials; this account should be included in AMS Readers and granted Logon as a batch job privilege on the InTrust server	Specified credentials
Integrated Windows Authentication	Account specified for connection to InTrust Server (see step 3 of the procedure below).	Account specified for connection to InTrust Server (see step 3 of the procedure below).

To configure data import when generating reports interactively

1. In Knowledge Portal, click the **Reports** tab.
2. Select the InTrust report you need, and from **Specific Actions**, select **Run Data Import** to start the Report-Driven Data Import Wizard. Currently, this specific option is not available for all InTrust reports.
3. On the Specify InTrust Server step, specify the parameters of the InTrust server that will perform data import.
   Here you should supply the following:
   - InTrust server name
   - Connection protocol and connection port to be used
   - Credentials to be used when connecting to InTrust Server
4. Select the InTrust repository to import data from.

5. Specify the parameters of InTrust database the data will be imported to:
   The following is required:

   - Server—name of SQL Server hosting the InTrust audit database (this value is supplied automatically in accordance with current configuration)
   - Database—target database name (this value is supplied automatically in accordance with current configuration)
   - Authentication mode—select authentication method to be used for database connection, and supply access credentials. (For details, refer to the table above in this section.)

6. On the next step, set the **Computer** filter—events from the specified computers will be included in the data import.
7. Set the **Date/Time** filter to indicate the time period for which you want data.
8. Review the settings you have configured; now you can start data import.
9. Wait for the import process to complete.

On the final screen, review the results of data import; if needed, select **View the report after finishing**. Click **Finish** to close the wizard.

Creating Reports

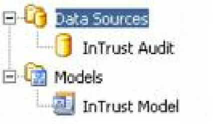
In addition to a number of predefined reports for products supplied in the Report Packs, the Knowledge Portal component provides for creation of custom reports. This process is based on using *report models*.

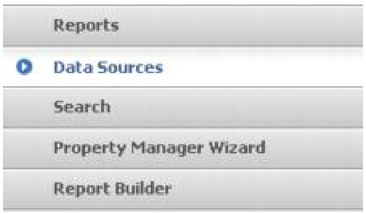
A report model helps Report Builder users to explore and select the data that they want to use from the underlying data source. Report models provide familiar business names for database fields and tables, logically grouped model items, and predefined relationships between items within the data source. They are used by the report server to automatically generate a query for retrieving the requested data, thus facilitating ad-hoc reporting.

In Knowledge Portal, predefined models are brought in by the Report Packs you install. Each model defines:

- What product provides data for the reports
- What data source this data should be obtained from

The InTrust model is installed automatically, and you can use this model to create the reports on audit data collected by InTrust. The available models are displayed when you are on the **Data Sources** tab:





To explore the InTrust model, click the **Report Builder** tab in Knowledge Portal. Report Builder is launched, and the model tree is displayed on the right pane.

> ! CAUTION: **Report Builder is available only if ASP .NET 2.0 is installed on the client computer you are using.**

Select the InTrust model from the models tree. From the panes on the left, you can select the objects you are interested in and the fields to obtain the data you need on these objects (such as Trusted Domain). To add an object or a field to your report, simply double-click this item in its pane.

You can use a full range of report building capabilities, as described in detail in Working with Report Builder (Ad Hoc Reports). See also Report Builder Help.

After you get back to Knowledge Portal, the report you create will appear in the reports tree in the left pane. By default, the report will use the data source prescribed by the model it was built on. You can use the **Change Data Source** option for your custom reports.

> i NOTES:
>
> - The **Customize Report View** option is unavailable for custom reports.
> - Unlike predefined reports whose filters can be changed when you view the reports, custom report's filters (i.e. parameters) are available for modification only via Report Builder. That is, to modify filters (parameters) for a custom report, you should select it in the tree, and click **Report Builder**. After you finish the modification, save the changes and go back to Knowledge Portal.

Perspectives and Entities

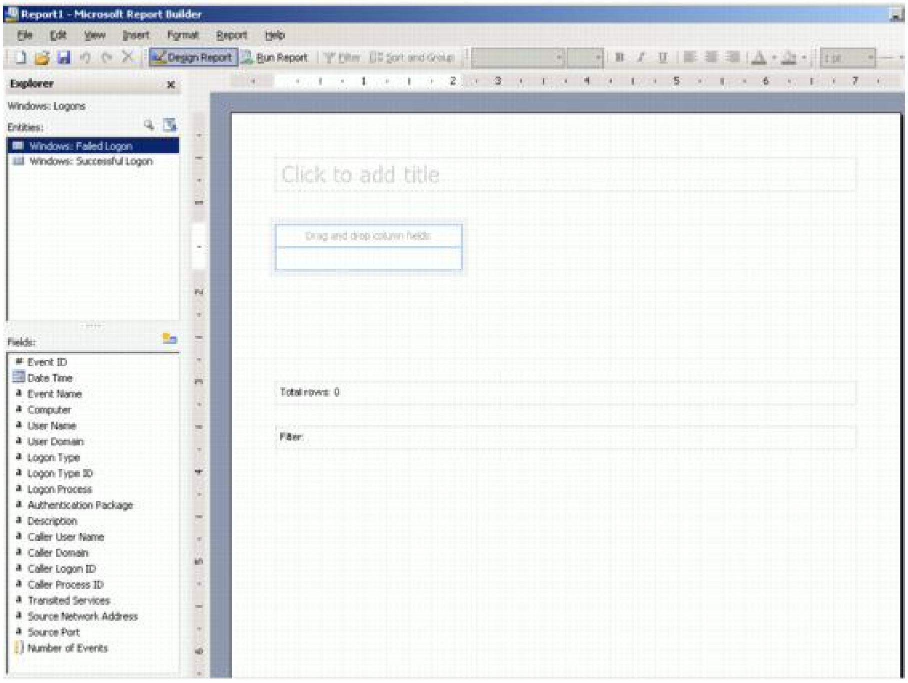
What is a Perspective?

Under the **InTrust Model** node, the following items are displayed:

- Generic Events
- Windows: Account Management
- Windows: Logons

These items are the perspectives of the InTrust model. A *perspective* is a subset of a model. For example, the whole **InTrust Model** allows you to create reports on any kind of events stored in InTrust Audit database, and its **Windows: Logons** perspective can be used to report on logon events.

After you select a model or any of its perspectives on the right and click **OK**, a number of entities and their fields are displayed in the left pane, as shown below:



What is an Entity?

In the most common case, an *entity* corresponds to a database table (or named query). For example, **Windows: Failed Logons** and **Windows: Successful Logons** are the entities of the selected **Windows: Logons** perspective. An entity consists of fields: for instance, the fields of the Failed Logons entity correspond to the event fields as they are presented in Event Viewer (such as Event ID or Date/Time).

Working with Models

To build a report using a model, drag and drop the fields you need, placing them into report layout area on the right.

In addition, you can use the Knowledge Portal to create new models and to change the data source for model-based reports.

To create a model

1. In Knowledge Portal, click the **Data Sources** tab, select **Models** node from the tree, and click **Create Model** from **New Model**. The New Model Wizard starts.
2. On the Select Model Type step, select the type of model you want to create (generally, the model type corresponds to the product that will provide data for reports built using the model).
3. On the Select Data Source step, select the data source that stores data for reports you will build on this model (each model is assigned one data source).
4. Finally, specify a name and description for the model. Review the settings and finish the wizard. Then the new model appears in the tree.

Each model is intended to work with a particular data source; to change the data source for model-based reports in bulk, you should take the steps described below.

To change the data source for multiple reports

1. Select the corresponding model in the tree.
2. Select **Change Data Source** from **Manage Model**.
3. Specify the data source that will provide data for the reports based on this model.

You can also change model and data source for a single model-based report.

To change the data source for a single report

1. Select the report you need from the report tree.
2. Select **Change Data Source** from **Manage Report**.
3. Specify the data source you want to use for selected report.

You can create a copy of existing model that you can use to create reports on the same product and the same data source as the original.

To create a copy of a model

1. Select the model you want to copy.
2. Select **Clone** from **Manage Model**.
3. Specify the new model's name and description.

Now you can create a custom report using any available model and Microsoft SQL Reporting Services report building capabilities.

Creating a Model-Based Report

1. Click the **Report Builder** tool button in the Knowledge Portal toolbar; in the models tree in Report Builder, select **InTrust**.
   Any custom report you create will get data from the data source assigned to the selected model.
2. From the panes on the left, select the objects you are interested in and the fields to obtain the data you need on these objects.
3. Drag and drop the objects or fields to the layout area. Refer to the examples below for details.
4. To add filters, click **Filter** in the Report Builder toolbar, and drag and drop the fields you want report data to be filtered by. Refer to the examples below for details.
5. Run your report or save it.

Saving a Report

When saving a report created with Report Builder, the report (RDL file) is saved to the default target location on report server where the Report Builder application runs. To make your custom report appear in the report tree in Knowledge Portal, specify **QKP\InTrust\Reports** as target location.

After you get back to the Knowledge Portal, the report you created will appear in the reports tree. By default, this report will use the data source prescribed by the model it was built on. You can use the **Change Data Source** option for your custom reports.

ℹ **NOTES:**

- The **Customize Report View** option is unavailable for custom reports.
- Unlike predefined reports whose filtering parameters can be changed when you view the reports, custom report's filtering parameters are available for modification only via Report Builder. That is, to modify filtering parameters for a custom report, you should to the following:
  1. Select report in the tree, and click **Report Builder**.
  2. Make the necessary changes to report filters.
  3. After you finish the modification, save the changes and go back to Knowledge Portal.

Two examples of custom report creation are provided in the following topics:

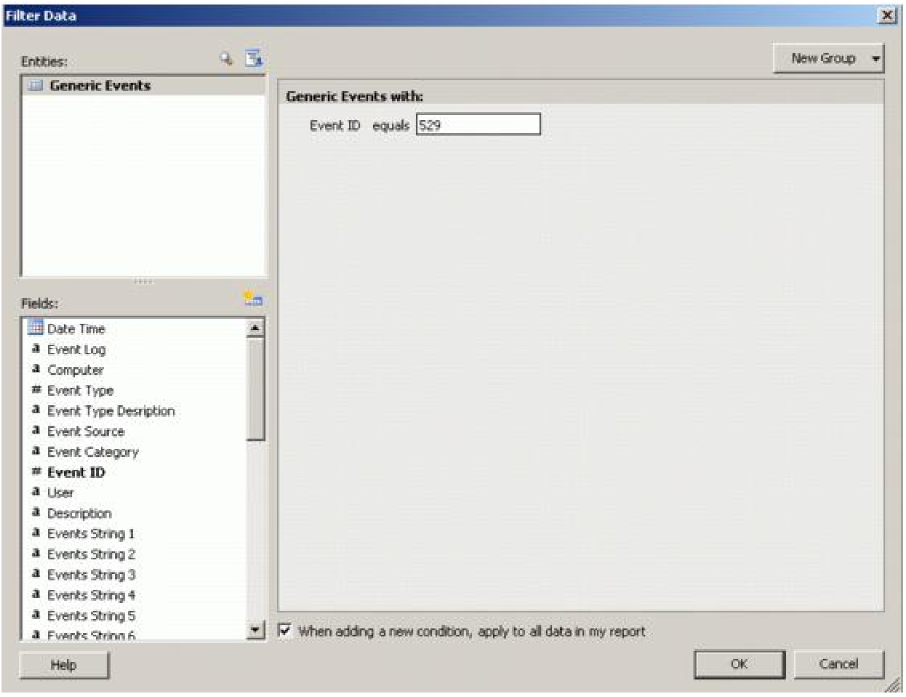
- Example 1: Creating a Report Based on the Generic Perspective
- Example 2: Creating a Summary Report on Group Membership Management

Example 1: Creating a Report Based on the Generic Perspective

To create a report on failed logons using the Generic perspective

1. In Report Builder, select the **InTrust** model, click **OK**, and select the **Generic Events** perspective. The entity and its fields are displayed on the left.
   The following entity fields will be used in this example to create a custom report on failed logons filtered by computer:
   - Event ID
   - Local Time
   - Computer (where the event was logged)
   - User
   - Events String 2—for User Name of the account who tried to log on
   - Events String 3—for Domain this user belongs to
   - Events String 7—for Workstation that was used
2. Drag and drop these fields to the report layout area.
3. Click the **Filter** button on the Report Builder toolbar.
4. In the Filter window, drag and drop the **Event ID** field from the Fields pane to the right pane.

5. To report on failed logon events (Event ID 529), set the filter equal to 529 by entering this number in the edit box.



Generic Events with:

Event ID equals 529

☑ When adding a new condition, apply to all data in my report

6. To prompt the user for the computer name to filter the report by, drag and drop the **Computer** field to the right pane and configure the parameter as prompted (by selecting this setting from the parameter's shortcut menu).

7. Click **OK**.

8. Run the report.

Example 2: Creating a Summary Report on Group Membership Management

You can use Report Builder to create summary reports with either a matrix (cross-tab) or a chart report layout:

- A matrix report layout template presents data in an intersecting format, with totals displayed in the center. It is also known as a cross-tab report.
- A chart report layout template presents data graphically in the form of bar, pie, and line charts.

In a summary report, you can drill down to the details of the selected total.

To help you add totals to a summary report, a special field (Number of <*type or name of the entity*>) is offered. For example, for the Group Membership Management entity this total will be named Number of Events. If this field is included in a report, a count of corresponding objects is displayed for the group the total refers to.

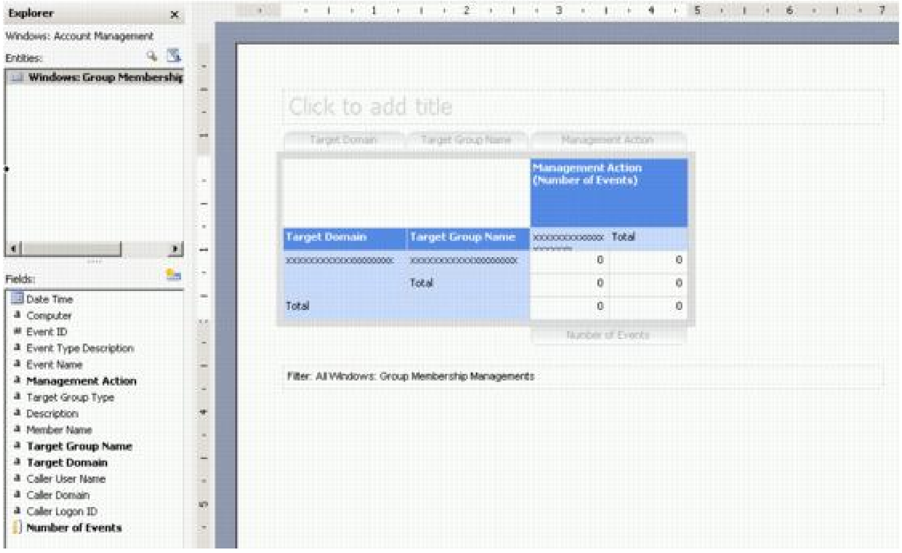
To create a report on group membership management

1. In Report Builder, select the **InTrust** model, and select its **Windows: Account Management** perspective.

2. From the Report layout options, **View| Task Pane**, select **Matrix (cross-tab)**. Click **OK**.

3. In the Entities pane, select **Windows: Group Membership Management** entity.

4. To group report data by the domain that target group belongs to, drag and drop the **Target Domain** field to the area marked as 'Drag and drop row groups'.
5. Drag and drop the **Target Group Name** field to place it next to Target Domain on the right.
6. Drag-and-drop the **Management Action** field to the area marked as 'Drag and drop column groups'. This filed is used to show addition or removal of group members.
7. To display the total count of management actions, drag and drop the **Number of Events** field to the area marked as 'Drag and drop totals'.



		Management Action (Number of Events)	
Target Domain	Target Group Name	xxxxxxxxxxxx	Total
xxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxxxx	0	0
	Total	0	0
Total		0	0

Filter: All Windows: Group Membership Managements

8. To add the drill-down capability from the totals to the details, right-click on the total field and select **Edit Formula**.
9. In the Define Formula dialog, replace the text in the right edit box with the following formula: *Count()*.
10. Drag the field (by which you want the total to be counted) to the right edit box, and place it into the formula. In this example, groups total will be counted by the **Management Action** field, so finally the formula should be *Count (Management Action)*.
11. Run the report.
12. Click on the total to view the detailed report.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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