GFI EventsManager 8 ReportPack

Manual

By GFI Software Ltd.

http://www.gfi.com
E-Mail: info@gfi.com

Version 8.1 – Last updated June 6, 2008

Contents

Introduction

About GFI ReportCenter

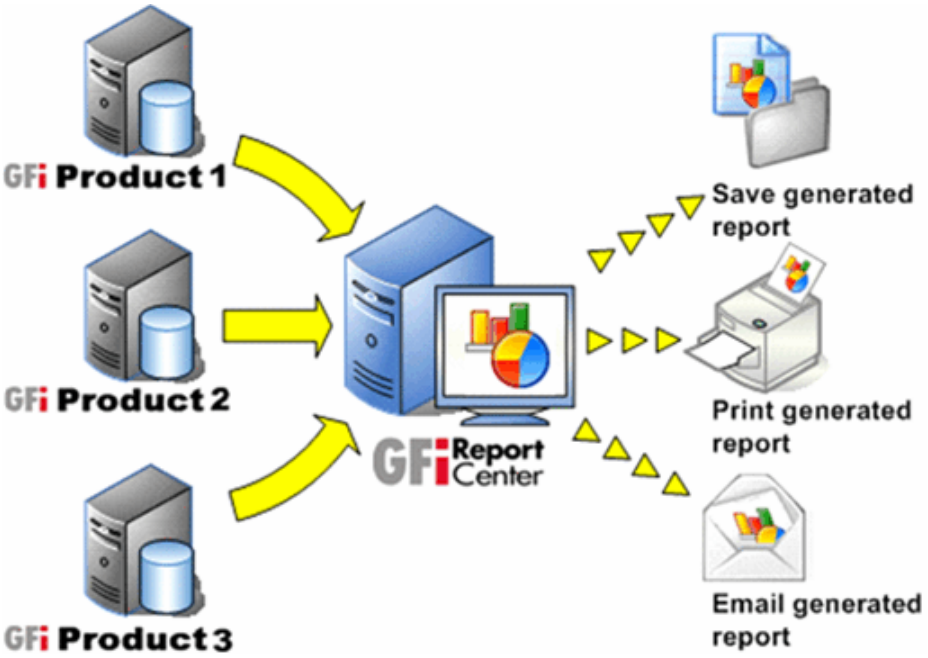


Figure 1 - Centralized reporting framework

GFI ReportCenter is a centralized reporting framework that allows you to generate various reports using data collected by different GFI products. GFI releases specialized reports for each of its products, referred to as a ReportPack; for example, the GFI EventsManager ReportPack. A ReportPack can be purchased as an add-on to the GFI product.

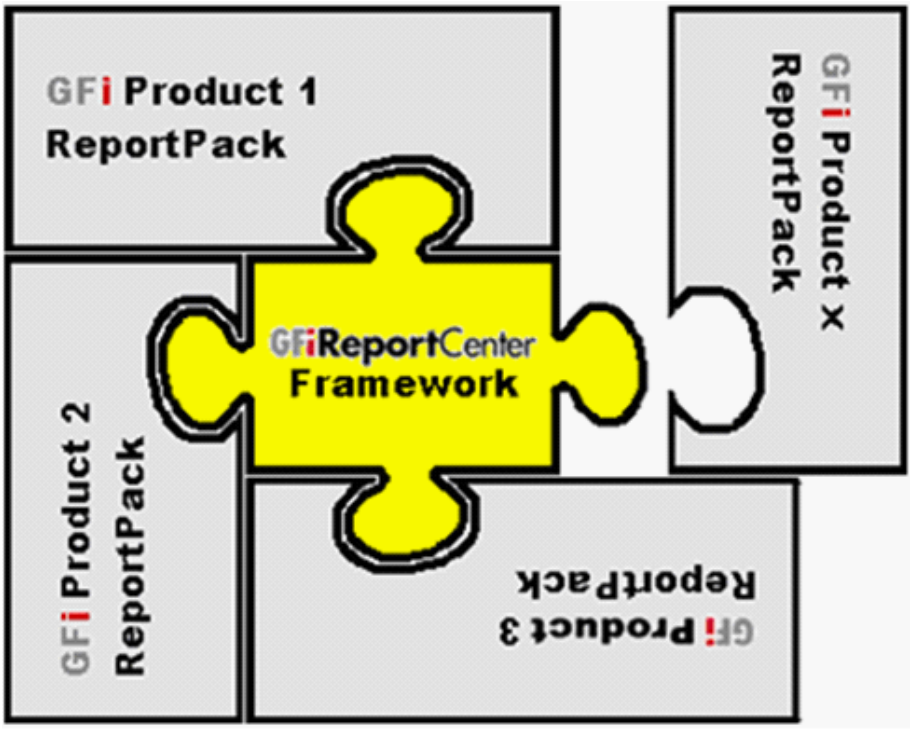


Figure 2 – Several ReportPacks plugged into the GFI ReportCenter framework

A ReportPack plugs into the GFI ReportCenter framework; allowing you to generate, analyze, export and print the information generated through these reports.

About the GFI EventsManager ReportPack

The GFI EventsManager ReportPack is a full-fledged reporting companion to GFI EventsManager. It allows you to generate graphical IT-level, technical and management reports based on the hardware and software events recorded by GFI EventsManager. Hardware and software event sources include any networked component that can generate Syslog messages or record/log events to Windows and/or W3C event logs. These include computers, network devices, PABXs, and third party software solutions.

From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI EventsManager ReportPack provides you with the easy-to-view information required, to fully understand the events activity on your corporate network.

The GFI EventsManager ReportPack allows for the creation of various graphical and text based reports related to:

- Account Usage
- Account Management
- Policy Changes
- Object Access
- Application Management
- Print Server
- Windows Event Log system
- Network Resource Access (PCI Requirement 10)

- Events Trend
- All critical messages
- Miscellaneous, customizable reports.

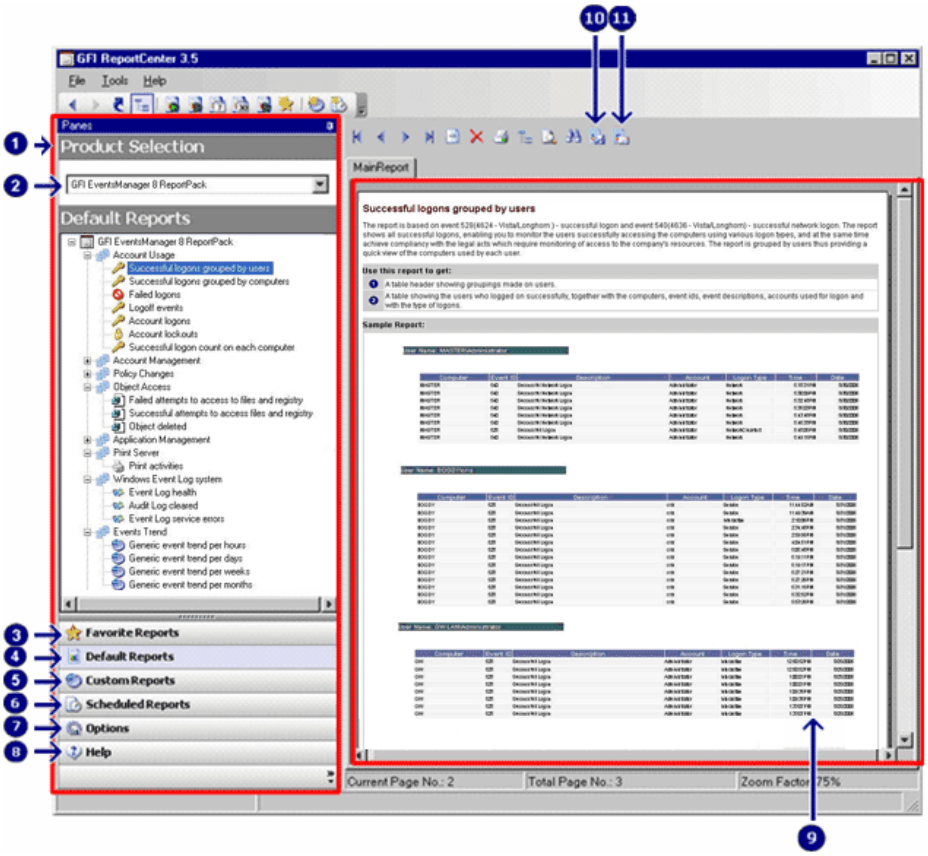
Components of the GFI EventsManager ReportPack

When you install the GFI EventsManager ReportPack, the following components are installed:

- GFI ReportCenter framework
- GFI EventsManager default reports
- Report scheduling service.

GFI ReportCenter framework

The GFI ReportCenter framework is the management console through which you can generate the specialized product reports which are shipped with a product ReportPack. The GFI ReportCenter framework offers a common application interface through which you can navigate, generate, customize and schedule reports.



Screenshot 1 – The GFI ReportCenter management console

The GFI ReportCenter management console is organized as follows:

1	**Navigation Pane** – Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
2	**Product Selection drop-down list** – Use this drop-down list to select the GFI product for which to generate reports. The Product Selection drop-down list displays all the products for which you

	have installed a ReportPack.
3	**Favorite Reports** – Use this navigation button to access your favorite/most used reports. For more information on how to add reports to this list refer to the 'Adding default reports to the list of favorite reports' and 'Adding custom reports to the list of favorite reports' sections in this manual.
4	**Default Reports** – Use this navigation button to access the default list of reports which can be generated for the selected product. For more information on default reports refer to the 'GFI EventsManager default reports' section in this manual.
5	**Custom Reports** – Use this navigation button to access the list of customized reports which can be generated for the selected product. For more information on how to create custom reports refer to the 'Custom reports' chapter in this manual.
6	**Scheduled Reports** – Use this navigation button to access the list of scheduled reports for automatic generation and distribution. For more information on how to create scheduled reports refer to the 'Scheduling reports' chapter in this manual.
7	**Options** – Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.
8	**Help** – Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
9	**Report Pane** - Use this multi-functional pane to: • View and analyze generated reports • Maintain the scheduled reports list • Explore samples and descriptions of default reports.
10	**Export** – Use this button to export generated reports to various formats including HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC), and Rich Text Format (RTF).
11	**Send email** – Use this button to instantly distribute the last generated report via email.

GFI EventsManager default reports

The GFI EventsManager default reports are a collection of specialized pre-configured reports which plug into the GFI ReportCenter framework. These reports present the events recorded by GFI EventsManager and allow for the generation of both graphical and tabular IT-Level, technical and management reports. Default reports can also serve as the base template for the creation of customized reports which fit specific network-reporting requirements.

Report scheduling service

The report scheduling service controls the scheduling and automatic distribution of reports by email. Reports generated by this service can also be saved to a specific hard disk location in a variety of formats which include DOC, PDF, RTF and HTML.

Key features

Centralized reporting

GFI ReportCenter is a one-stop, centralized reporting framework which enables the generation and customization of graphical and tabular reports for a wide array of GFI Products.

Wizard assisted configuration

Wizards are provided to assist you in the configuration, scheduling and customization of reports.

Report scheduling

With GFI ReportCenter you can schedule reports to be generated on a pre-defined schedule as well as at specified intervals. For example, you can schedule lengthy reports to be generated after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Distribution of reports via email

GFI ReportCenter allows you to automatically distribute generated reports via email. In scheduled reports, this can be achieved automatically after the successful generation of a scheduled report.

Report export to various formats

By default, GFI ReportCenter allows you to export reports to various formats. Supported formats include HTML, PDF, XLS, DOC and RTF. When scheduling reports, you can optionally configure the preferred report output format. Different scheduled reports can also be configured to output generated reports to different file formats.

Default reports

The GFI EventsManager ReportPack ships with a default set of graphical and tabular reports. These reports can be generated without any further configuration effort immediately after the installation. The

default reports in this ReportPack are organized into different report-type categories:

- Account Usage
- Account Management
- Policy Changes
- Object Access
- Application Management
- Print Server
- Windows Event Log system
- Network Resource Access (PCI requirement 10)
- Events Trend
- All critical messages
- Miscellaneous, customizable reports.

Report customization

The default reports that ship with every ReportPack can serve as the base template for the creation of customized reports. Report customization is achieved by building up custom data filters which will analyze the data source and filter the information that matches specific criteria. In this way, you create reports tailored to your reporting requirements.

Favorites

GFI ReportCenter allows you to create bookmarks to your most frequently used reports – both default and custom.

Printing

By default, all reports generated by GFI ReportCenter are printer friendly and can be printed through the windows printing services provided by the system where GFI ReportCenter is installed.

Installation

System requirements

Install the GFI EventsManager ReportPack on a computer that meets the following requirements:

- Microsoft Windows 2008, 2003 (SP2), 2000 (SP4), XP (SP2), VISTA
- .NET framework 2.0
- Internet Explorer 5.1 or higher
- GFI EventsManager 8.x

NOTE: The GFI EventsManager ReportPack only allows you to generate reports for data contained in the SQL Server database backend of GFI EventsManager.

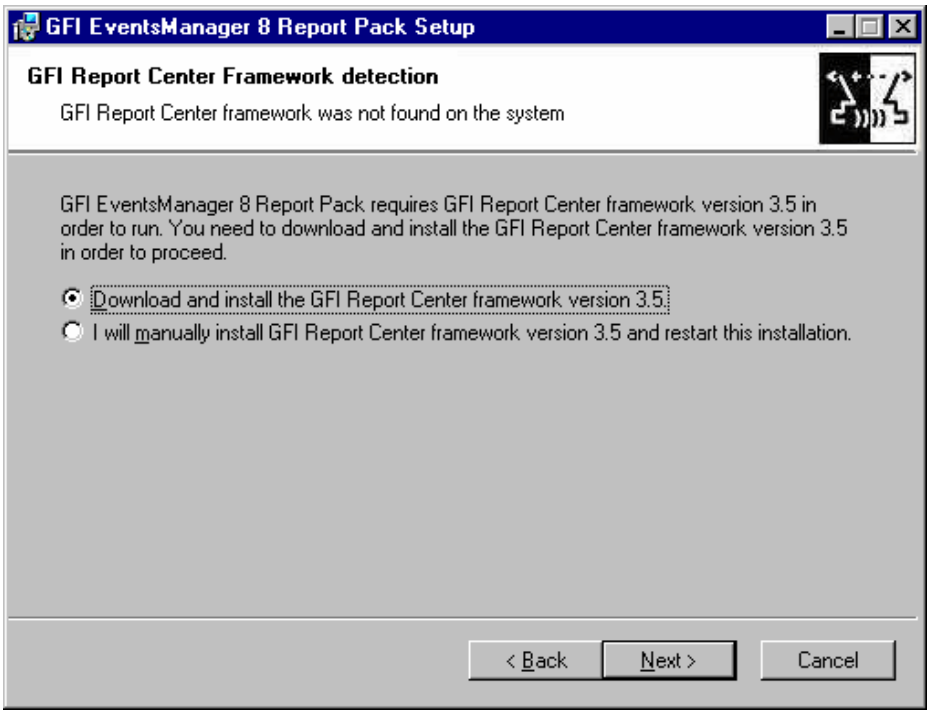
Installation procedure

The GFI EventsManager ReportPack includes an installation wizard which will assist you through the installation process. During the installation process this wizard will:

- Verify that you are running the latest version of the GFI ReportCenter framework; if you are installing the framework for the first time or the currently installed framework version is outdated, the installation wizard will automatically download the latest one for you.
- Automatically install all the required components distributed including the GFI ReportCenter framework, the GFI EventsManager default reports and the Report Scheduling service.

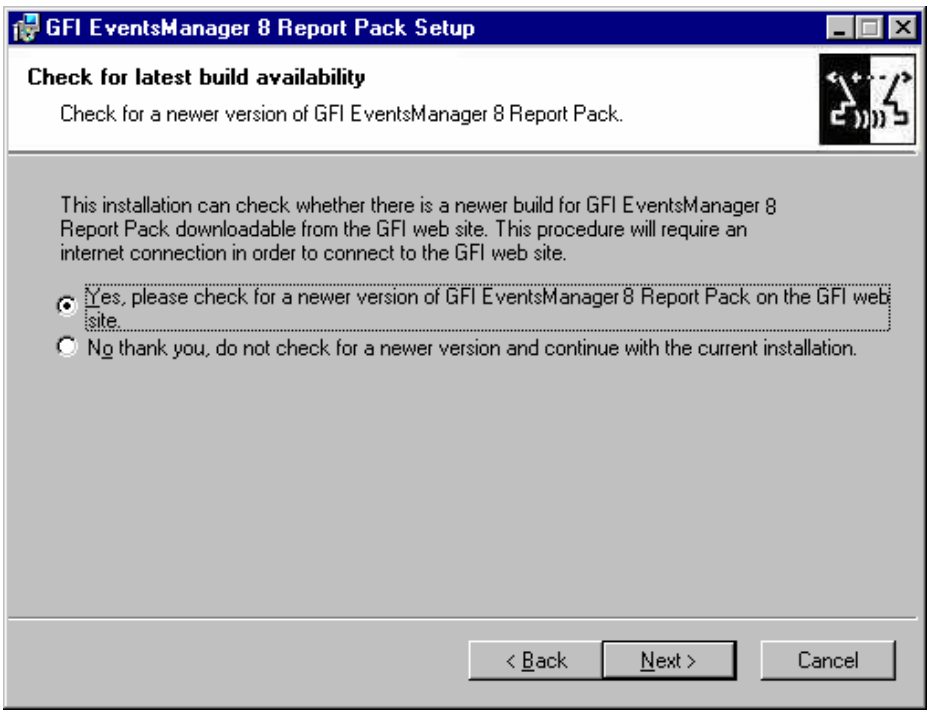
To start the installation:

1. Double-click on **eventsmanager8rp.exe**. As soon as the welcome dialog is displayed, click **Next** to start the installation.



Screenshot 2 - GFI ReportCenter framework detection dialog

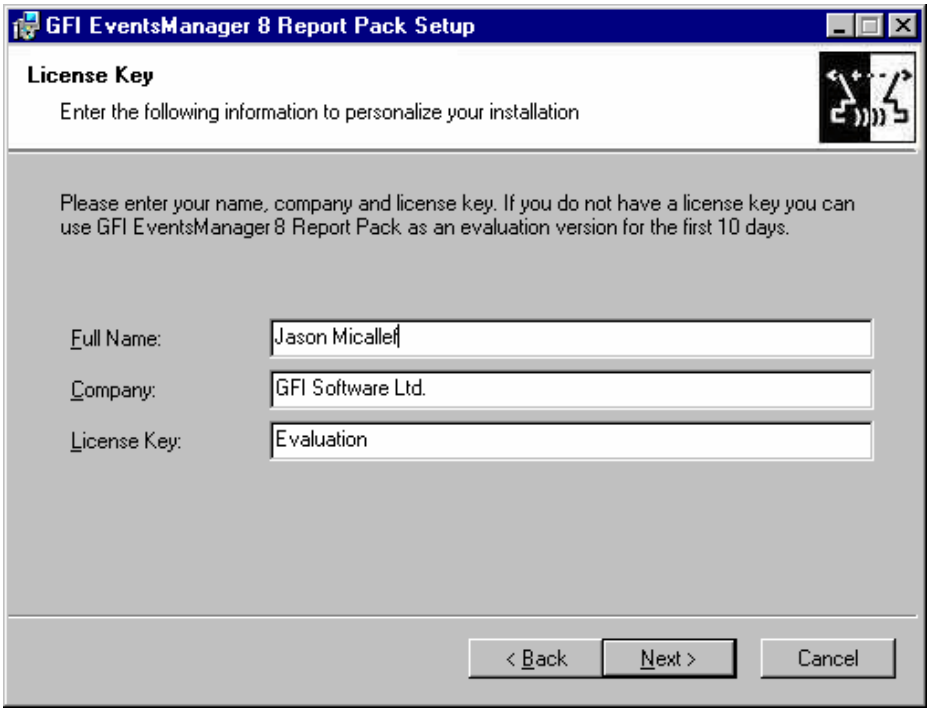
2. If the current version of your GFI ReportCenter framework is not compatible with the GFI EventsManager ReportPack, you will be prompted to download and install an updated version. To automatically achieve this, leave the dialog options as default and click on the **Next** button.



Screenshot 3 - Check for latest build availability

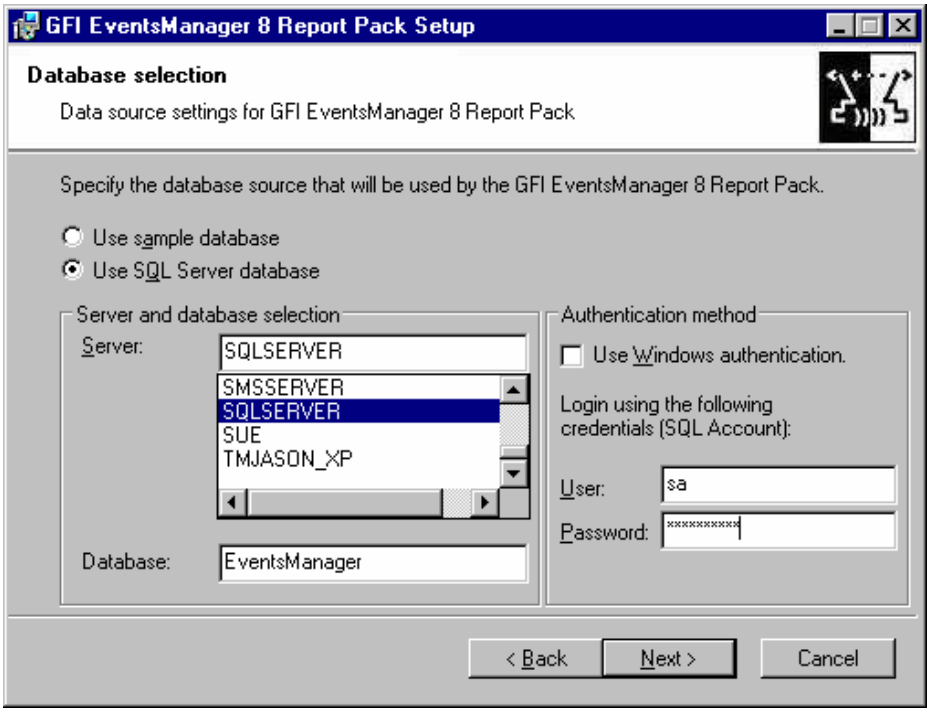
3. Choose whether you want the installation wizard to search for a newer build of the GFI EventsManager ReportPack on the GFI website. Then, click on the **Next** button to proceed with the installation.

4. In the license dialog, read the licensing agreement carefully. Select the '*I accept the Licensing agreement'* option and click on **Next** to continue.



Screenshot 4 - Licensing details dialog

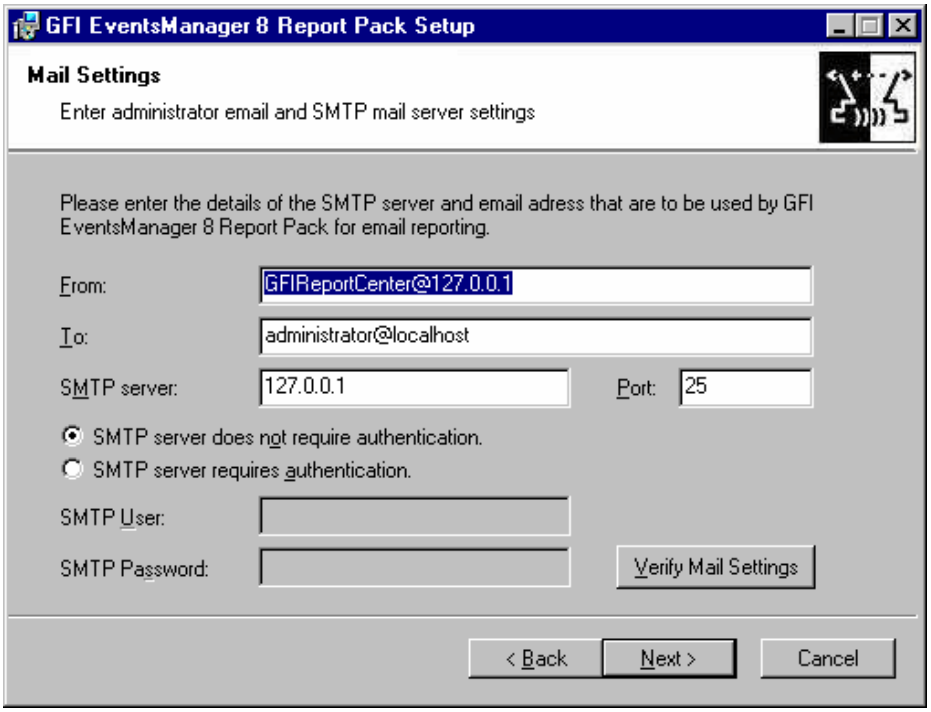
5. Specify the full user name, the company name and the GFI EventsManager license key. If you will be evaluating the product for 10 days, leave the evaluation key as default (i.e. "Evaluation"). Click on **Next** to continue.



Screenshot 5 – SQL Server selection dialog

6. Specify the details of the SQL Server which is hosting your GFI EventsManager database backend.

NOTE: For evaluation purposes you can also use the sample database that is distributed with this installation. When the GFI EventsManager ReportPack installation is complete, the sample database configuration guide is launched.



Screenshot 6 - Email configuration dialog

7. Specify the default email settings that will be used for report distribution.

8. Specify the product installation path or click **Next** to leave as default. The installation will need approximately 100 MB of free disk space.

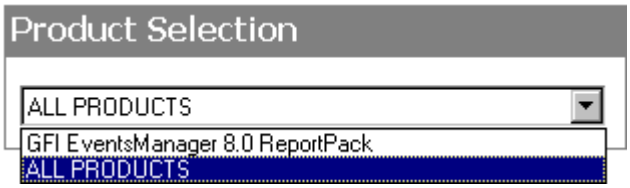
9. The installation wizard is now ready to copy the required files and finalize the installation. To proceed click on the **Next** button.

Launching the GFI EventsManager reports for GFI ReportCenter

Following the installation, launch the GFI EventsManager Reports for GFI ReportCenter from **Start ► Programs ► GFI ReportCenter ► EventsManager 8 ReportPack.**

Selecting a product

When more than one product ReportPack is installed, use the **Product Selection** drop down list to select the GFI product ReportPack to be used.



Screenshot 7 – Product Selection drop down list

For example, to run the reports provided in the GFI EventsManager ReportPack:

1. Launch GFI ReportCenter from **Start ► Program Files ► GFI ReportCenter.**

2. Select 'GFI EventsManager 8 ReportPack' from the **Product Selection** drop down list.

NOTE: Select the 'ALL PRODUCTS' option to display and navigate all the ReportPacks that are currently installed in GFI ReportCenter.

Getting started: Default reports

Introduction

After installing the GFI EventsManager ReportPack, a number of specialized pre-configured reports can immediately be generated on the data stored in the database backend of GFI EventsManager. These default reports are organized into the following categories:

- **Account Usage Reports:** Use the reports in this category to identify user logon issues. The event details shown in these reports include successful/failed user logons and locked user accounts.
- **Account Management Reports:** Use the reports in this category to generate a graphical overview of important events that took place across your entire network. The event details shown in these reports include changes in user and computer accounts as well as changes in security group policies.
- **Policy Changes Reports:** Use the reports in this category to identify policy changes effected on your network.
- **Object Access Reports:** Use the reports in this category to identify object access issues. The event details shown in these reports include successful/failed object access and objects which have been deleted.
- **Application Management Reports:** Use the reports in this category to identify faulty applications and application installation and removal issues. The event details shown in these reports include applications which have been installed or removed as well as applications which are crashing and hanging.
- **Print Server Reports:** Use the reports in this category to display details related to printing events. Details provided in these reports include documents that have been printed, the users that triggered the printing event and the date/time when the printing operation took place.
- **Windows Event Log System Reports:** Use the reports in this category to identify audit failures and important Windows event log issues. Details provided in these reports include the starting and stopping of event log services, clear log operations as well as errors generated during event logging.
- **Network Resource Access (PCI requirement 10):** Use the reports in this category to display information that will help you meet the requirements outlined by the PCI Data Security Standards document, version 1.1.

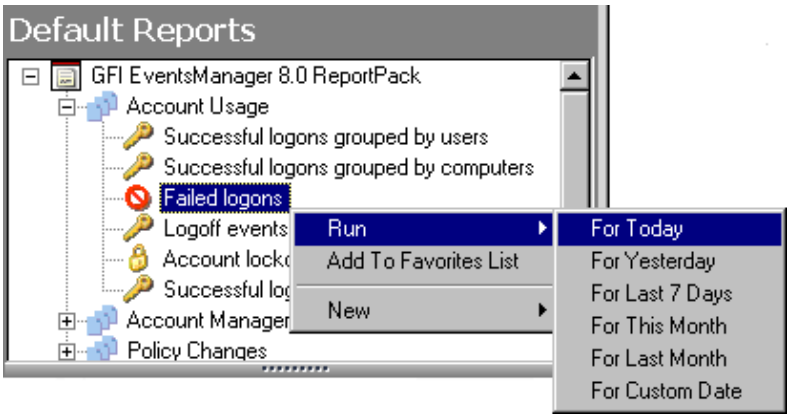
- **Events Trend Reports:** Use the reports in this category to display statistical information related to event generation. Charts provided enumerate the 10 computers and users with most events. Other reports provide event counts on a network-wide basis as well as on a computer by computer basis. Reports in this category can be generated for each main time period – by hour, day, week or month.
- **All critical reports:** Use the reports in this category to display information related to critical Windows events, Syslog, W3C, Custom Events, SNMP Traps and SQL Server Audit events. The charts provided enumerate the 10 most critical events.
- **Miscellaneous, Customizable reports:** Use the reports in this category to generate reports that offer broad customization. These can be used to generate reports based on any Windows event log, using filtering conditions and grouping modes which are not covered by the other default reports.

GFI EventsManager default reports are accessed by clicking on the **Default Reports** navigation button provided in the management.

Generating a default report

To generate a default report:

1. Click on the **Default Reports** navigation button to bring up the list of default reports available.



Screenshot 8 – Selecting the data set period

2. Right-click on the report to be generated, select **Run** and specify the event date/time period that will be covered by the report.

Example 1: Generating a "Failed logons" report based on yesterday's data.

This example demonstrates how to generate a failed logons report based on the events that were recorded yesterday:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

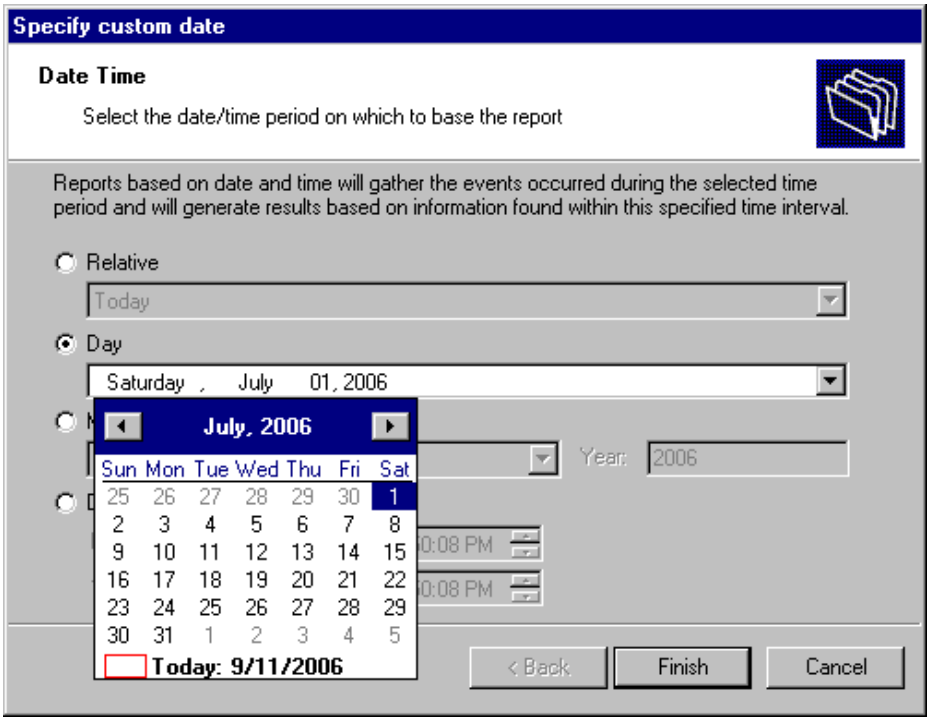
2. Right-click on **Failed logons** and select **Run ► For Yesterday**.

Example 2: Generating a "Failed logons" report based on that data collected on a particular day.

This example demonstrates how to generate a failed logons report based on the events that were recorded on July 1, 2006.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on **Failed logons** and select **Run ► For Custom Date**.



Screenshot 9 - Configuring custom date/time period

3. Select the 'Day' option and expand the provided drop down. This will bring up the date selection calendar.

4. Navigate to the required month (i.e. July) and select the required day (i.e. 1).

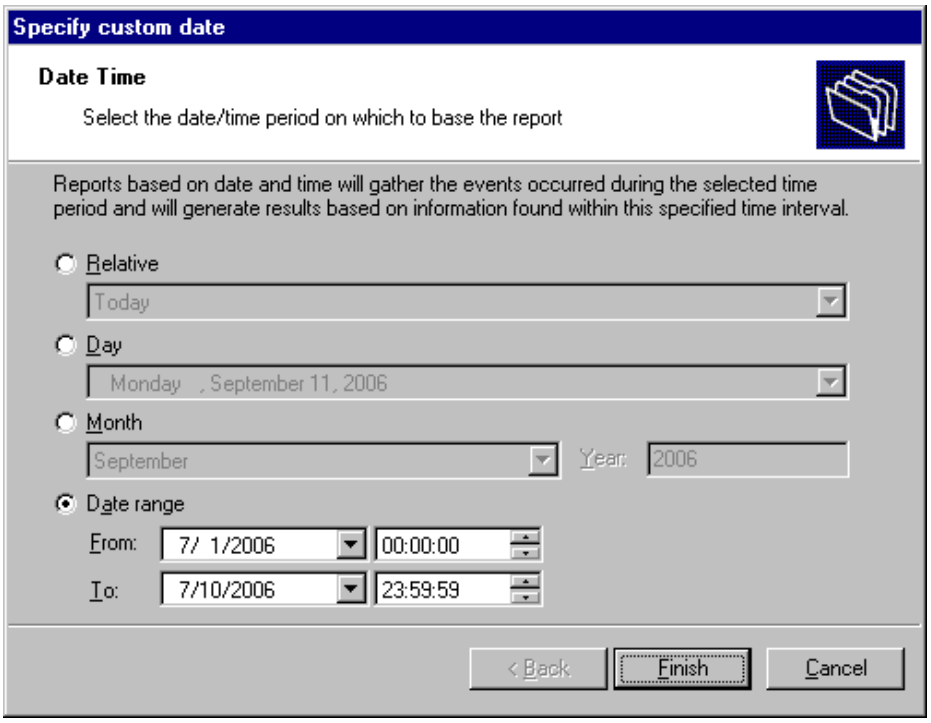
5. Click **Finish** to generate the report.

Example 3: Generating a "Failed logons" report based on data collected over a specific date/time period.

This example demonstrates how to generate a failed logons report based on the events recorded between July 1, 2006 and July 10, 2006.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on **Failed logons** and select **Run ► For Custom Date**.



Screenshot 10 - Configuring custom date/time period

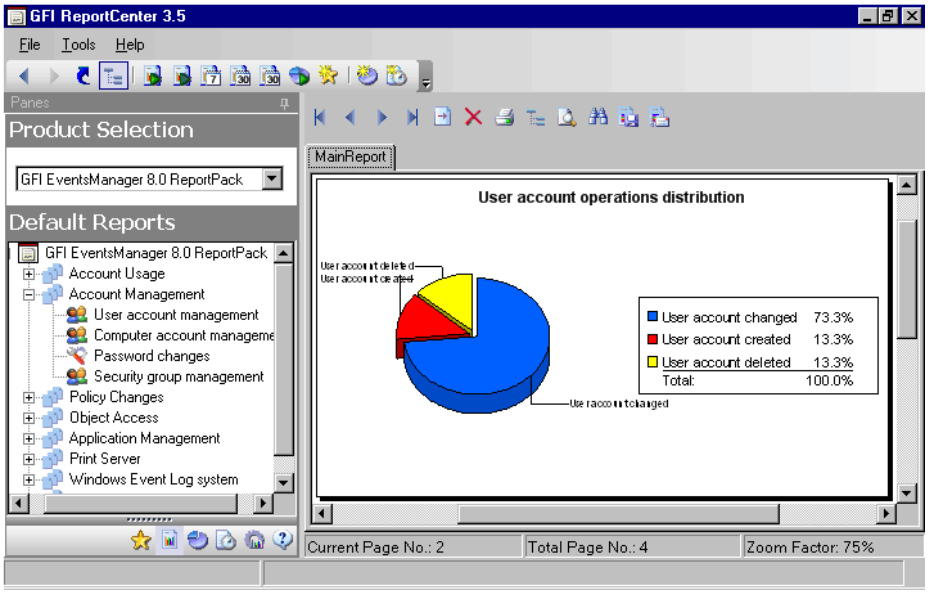
3. Select the 'Date range' option and specify the required parameters:

- 'From' – 07/01/2006 00:00:00.
- 'To' – 07/10/2006 23:59:59.

NOTE: Date and time format are based on the regional settings configured on your computer.

4. Click **Finish** to generate the report.

Analyzing the generated report



Screenshot 11 – Generated reports are displayed in the right pane of the management console

Generated reports are shown in the right pane of the GFI ReportCenter. Use the toolbar at the top of the report pane to access common report related functions:

Report browsing options

Browse the generated report page by page.

Zoom in/Zoom out.

Search the report for particular text or characters.

Go directly to a specific page.

Breakdown the report into a group tree (e.g. by date/time).

Print report.

Report storage and distribution options

Export the generated report to a specific file format.

Distribute the generated report via email.

NOTE: For information on how to configure report storage and distribution options refer to the 'Configuring Advanced Settings' section in this manual.

Adding default reports to the list of favorite reports

Screenshot 12 – Favorite Reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a default report to the list of favorite reports:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.

2. Right-click on the default report that you to be added to favorites and select **Add to favorites list**.

3. Click Yes to confirm.

Custom reports

Introduction

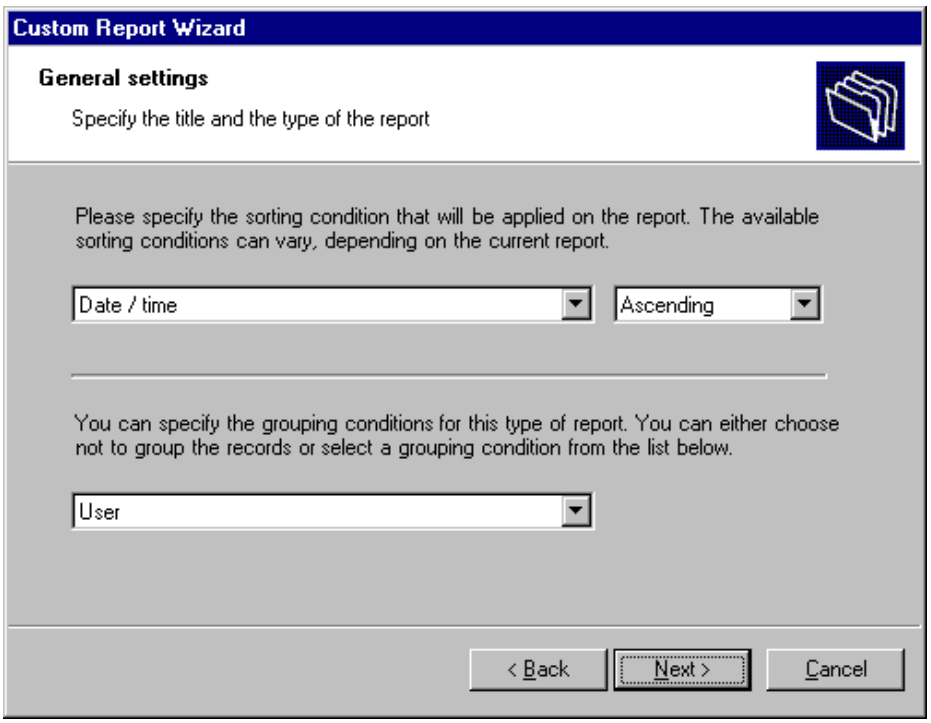
GFI ReportCenter allows you to create custom reports which are tailored to your reporting requirements. This is achieved by building up custom data filters which will analyze the data source and filter out the information that matches the specified criteria.

Creating a new custom report

To create a custom report:

1. Click on the **Default Reports** navigation button.

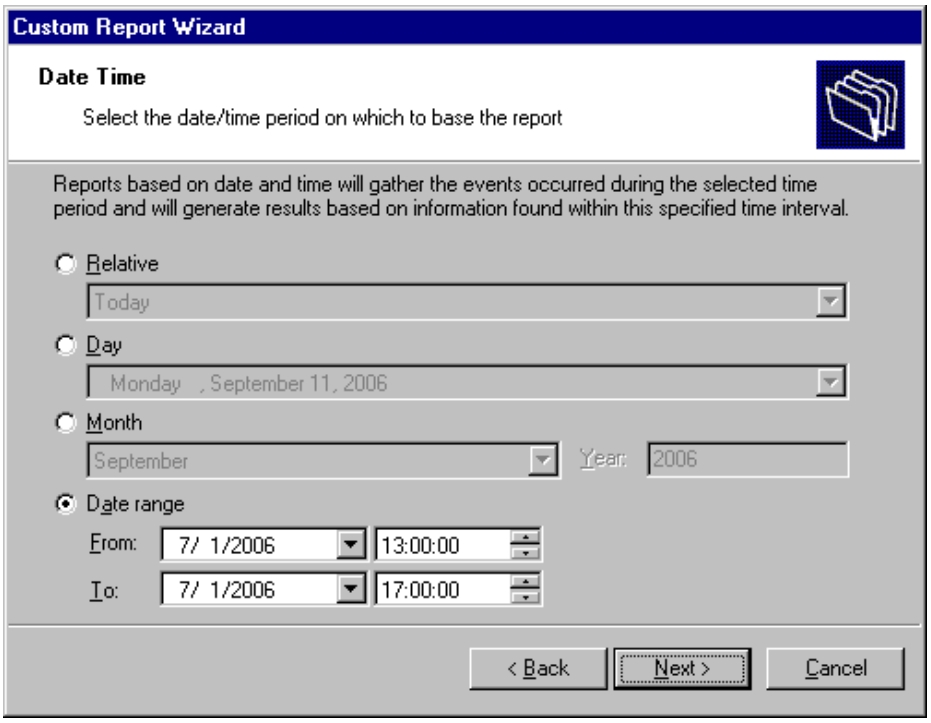
2. Right-click on the default report to be used as template and select **New ► Custom Report**. This will bring up the 'Custom Report Wizard'.



Screenshot 13 - Sorting and grouping conditions to be applied to the report

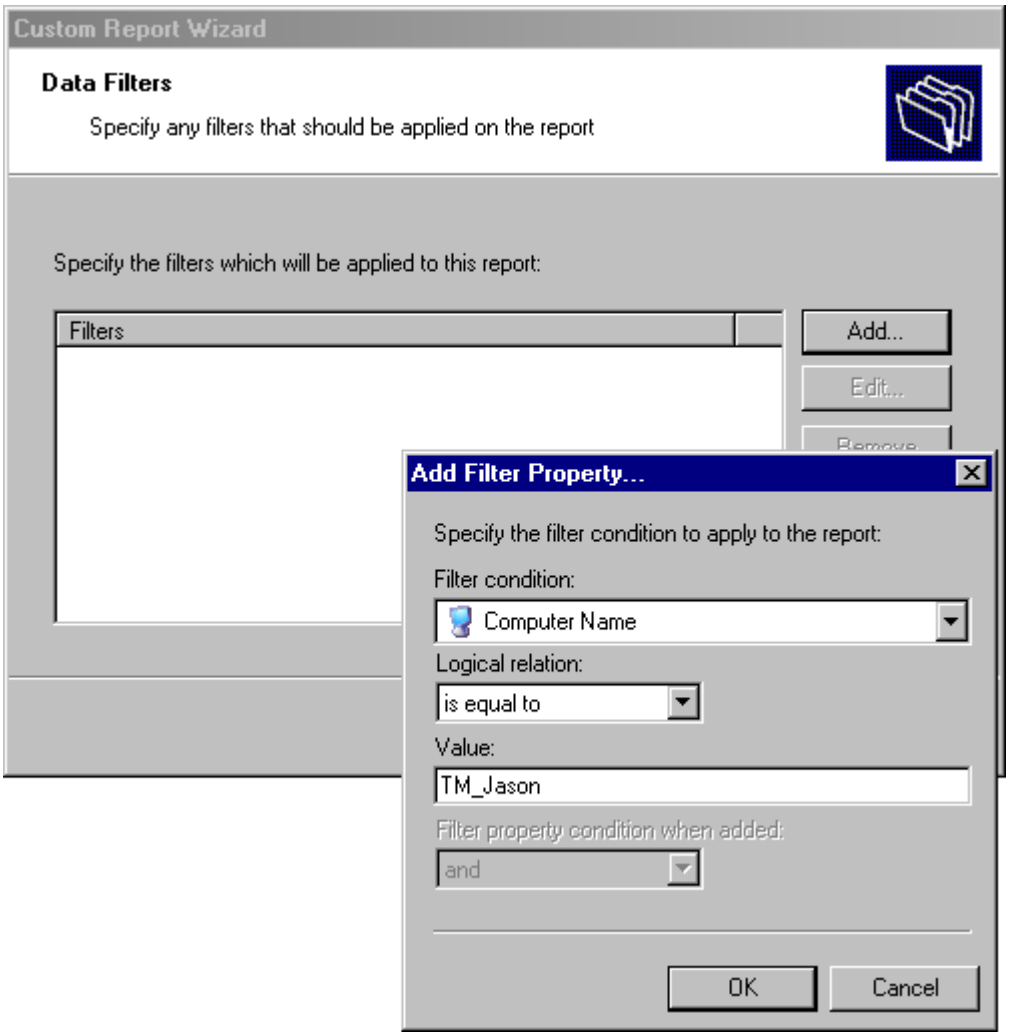
3. Specify how the information will be sorted in your report.

4. Specify how the information will be grouped in your report.



Screenshot 14 – Selecting the data source to use

5. Select the data source that will be used to generate the custom report (based on the date/time period).



Screenshot 15 – Specifying data filter conditions

6. Configure the data filter conditions that will be applied against the selected data source. Click on **Next** to continue.

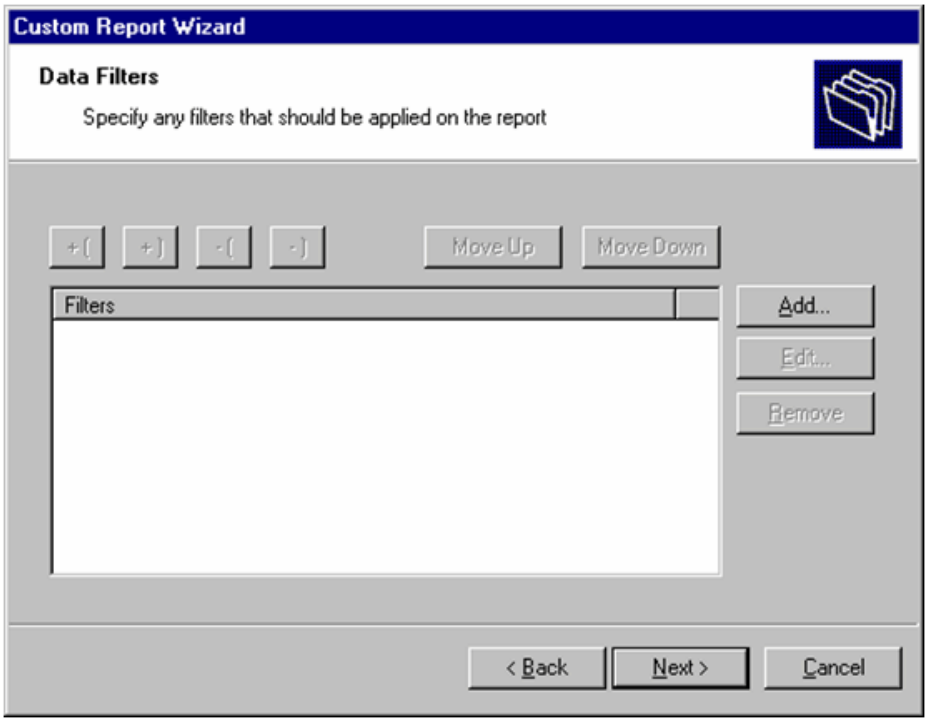
NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this manual.

7. Specify a name and description for the customized report. Click on **Next** to continue.

8. Click on **Finish** to finalize your configuration settings.

Configuring data filter conditions

Use data filter conditions to specify which events will be included in the report. Only the events which match the specified criteria will be processed and presented within the report.

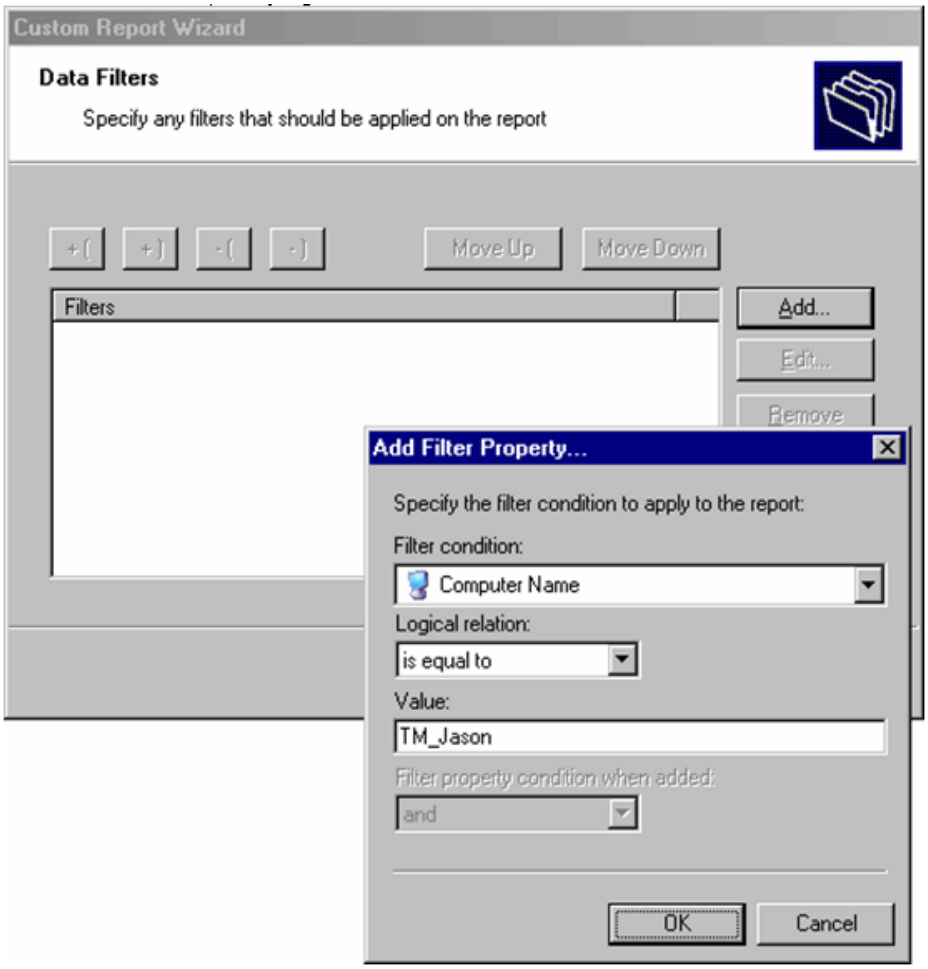


Screenshot 16 - Custom Report Wizard: Filters dialog

Click on the **Add…** button to bring up the 'Edit filter properties' dialog and configure the following conditions:

- '*Filter condition*' – Specify the data source area on which the filter will focus (for example, select 'Computer Name' to filter the events data related to a particular computer).
- '*Condition*' – Specify the condition comparison parameter.
- '*Value*' – Specify the string to which source data will be compared.

For example to generate a report which contains only information related to a workstation called "TM_Jason", configure your filter parameters as shown below:



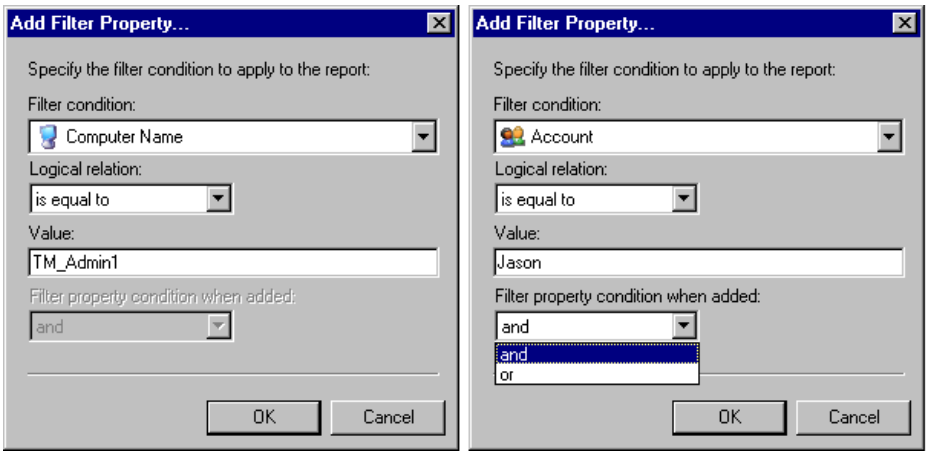
Screenshot 17 - Filter conditions configuration dialog

For more specific reports, you can limit the range of information to be displayed by tightening your conditions/search criteria. This is achieved by configuring and applying multiple data filters against the selected data source. When more than one filter is used, specify how these filters will be logically linked. This is achieved by selecting a logical grouping condition from 'Filter property condition…' drop down list.

- Select **And** to include ALL the scan data information that satisfies ALL of the conditions specified in the filters.
- Select **Or** to include ALL the scan data information that matches at least one of the specified filter conditions.

Example: Using multiple filters

Consider the situation where a custom report has 2 filters configured as follows:



Screenshot 18 - Using multiple filters

Parameters	Filter 1	Filter 2
Filter condition	Computer Name	User Name
Logical relation	Is equal to	Includes
Value	'TM_Admin1'	'Jason'

The data which will be included in this custom report will vary according to how these filters will be applied against your data. This is defined through the 'Filter property condition…' drop-down.

Filters applied			Data output
Filter 1	and	Filter 2	The report will show: • All the events by users called 'Jason' on the computer called 'TM_Admin1'.
Filter 1	or	Filter 2	The report will show: • All the events generated by users called 'Jason' – (no matter on which computer the connections were made) AND • All events related to the computer called 'TM_Admin1' – (no matter who the users are).

Example: Creating a custom report based on data collected during a particular month

This example demonstrates how to generate a failed logon report called 'Failed logons in July 2006'. This report will be based on the events:

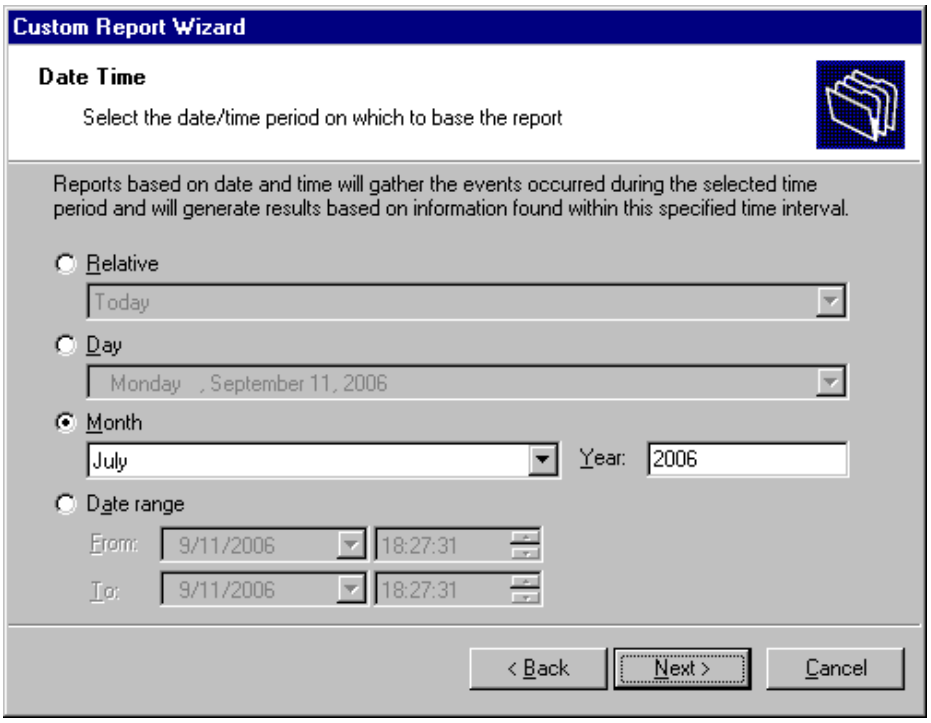
- Collected from the computer called 'TM_Admin1'
- Generated by the user account 'Jason'
- Recorded during the month of 'July 2006'.

To create this report:

1. Click on the **Default Reports** navigation button.

2. Right-click on the report to be customized and select **New ► Custom Report**. This will bring up the 'Custom Reports Wizard'.

3. As soon as the welcome dialog is displayed, click **Next**.

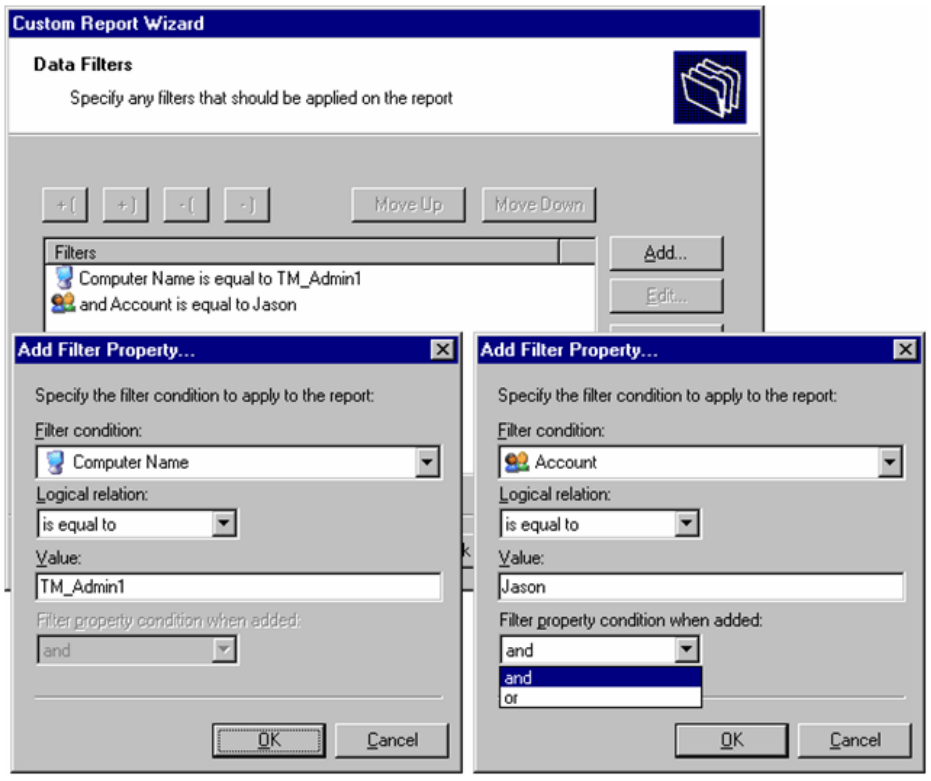


Screenshot 19 – Selecting the data source to use

4. Select the *'Month'* option and specify the following parameters:

- **Month**: '*July*'.
- **Year**: '*2006*'.

5. Click on **Next** to proceed to the data filters dialog.



Screenshot 20 - Filter conditions dialog(s)

6. Click on the **Add…** button and configure the parameters of filter 1 as follows:

- **Filter condition**: 'Computer Name'
- **Condition**: 'Equal to'
- **Value**: 'TM_Admin1'.

7. Click **OK** to finalize your filter configuration settings.

8. Click again on the **Add…** button and configure the parameters of filter 2 as follows:

- **Filter condition**: *'Account'*
- **Condition**: *'is equal to'*
- **Value**: *'Jason'*
- **Filter Property condition**…: *'and'.*

9. Click **OK** to finalize your filter configuration settings.

10. Click **Next** and specify the following parameters:

- **Report Name**: *'Failed logons in July 2006'*
- **Report Title:** *'Failed logons by Jason on computer TM_Admin1'*
- **Report Description***: 'This report shows the failed logons made by user Jason Micallef on computer TM_Admin1 during July 2006.'*

11. Click **Next** to proceed to the final dialog.

12. Click **Finish** to finalize your custom report configuration settings.

Run a custom report

To run a custom report:

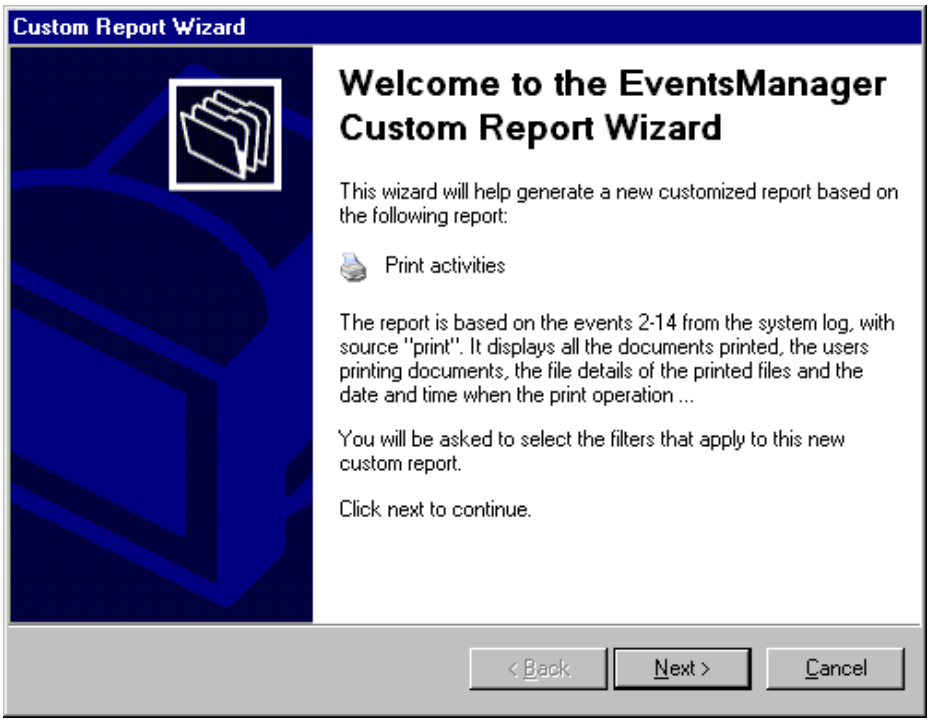
1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report to be generated and select **Generate**.

Editing a custom report

To edit the configuration settings of a custom report:

1. Click on the **Custom Reports** navigation button.



Screenshot 21 - Custom Report Wizard: Welcome dialog

2. Right-click on the custom report to be modified and select **Edit**. This will bring up the 'Custom Reports Wizard' through which you can make the required changes.

NOTE: For more information on how to configure the parameters of a custom report refer to the 'Creating a custom report' section in this chapter.

Deleting a custom report

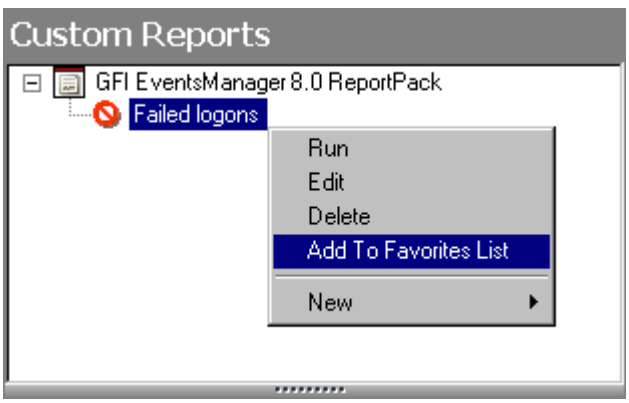
To delete a custom report:

1. Click on the **Custom Reports** navigation button.

2. Right-click on the custom report to be permanently removed from the list and select **Delete**.

3. Click **Yes** to confirm.

Adding custom reports to the list of favorite reports



Screenshot 22 - Favorite reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a custom report to the list of favorite reports:

1. Click on the **Custom Reports** navigation button to bring up the list of available reports.

2. Right-click on the custom report to be added to favorites and select **Add to Favorites List**.

3. Click Yes to confirm.

Scheduling reports

Introduction

GFI ReportCenter allows you to generate reports on a pre-defined schedule as well as at specified intervals. This way you can automate the generation of reports that are required on regular basis/ periodically.

Further to this, GFI ReportCenter can also be configured to automatically distribute scheduled reports via email. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format (e.g. PDF) in which the report will be attached to the email.

Use the report scheduling feature to automate your report generation requirements. For example, you can schedule lengthy reports after office working hours and automatically email them to the intended recipients. This way, you maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

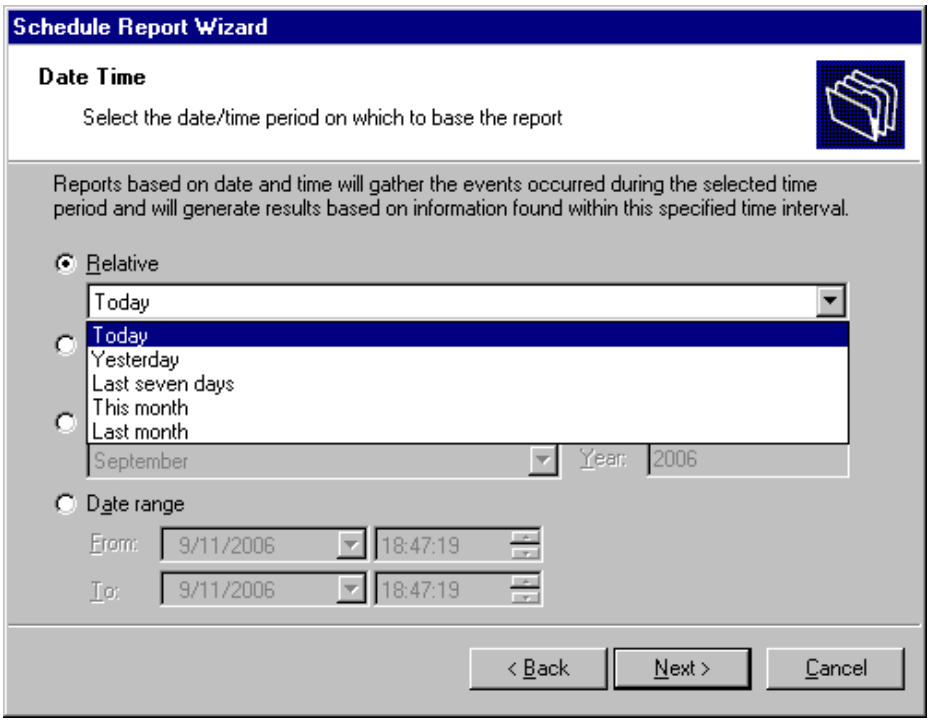
Both default and custom reports can be scheduled for automatic generation.

Scheduling a report

To schedule a report:

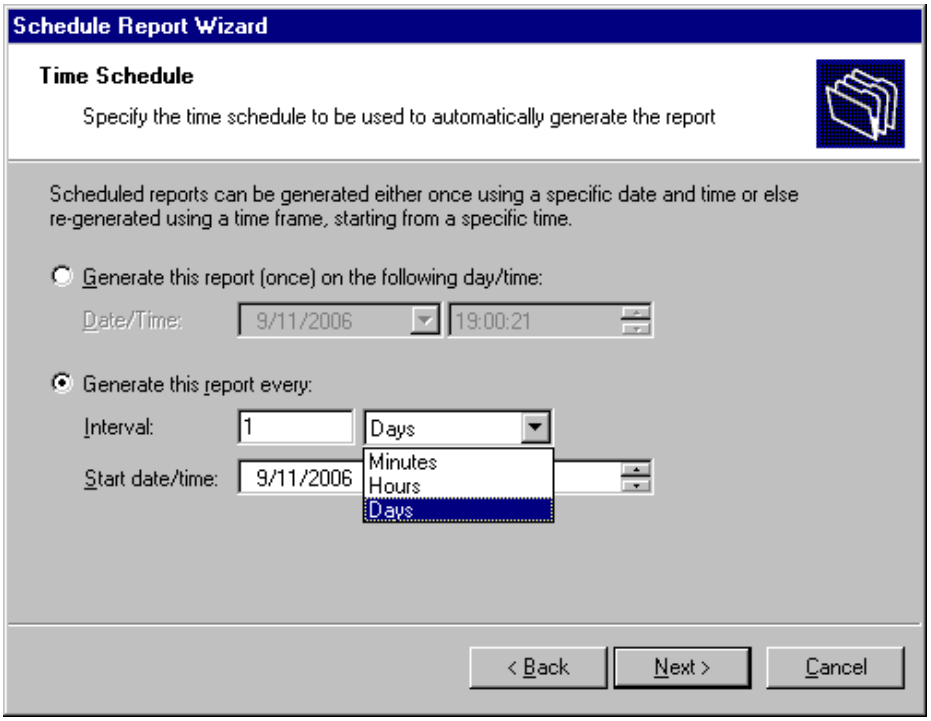
1. Click on the **Default/Custom Reports** option pane.

2. Right-click on the report to be scheduled and select **New ► Scheduled report**. This will bring up the 'Scheduled Report Wizard'. Click on **Next** to continue.



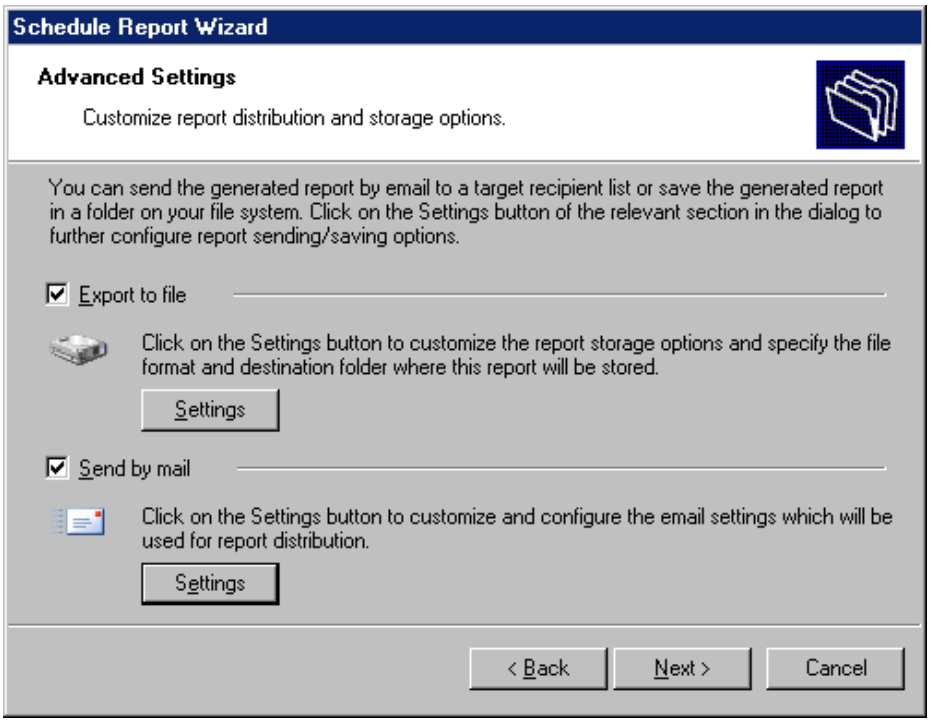
Screenshot 23 - Report Scheduling Wizard: Data-set selection dialog

3. Select the events data period to be covered by this report.



Screenshot 24 – Report Scheduling Wizard: Time schedule dialogue

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.



Screenshot 25 – Report Scheduling Wizard: Advanced Settings dialog

5. To export the generated report to file, select the *'Export to file'* option. To customize the report export configuration settings click on the **Settings** button underneath this option.

NOTE: For information on how to configure export-to-file settings refer to the 'Configuring report export to file options' section in this chapter.

6. To automatically distribute generated reports via email, select the *'Send by mail'* option. To customize the email settings used for report distribution click on the **Settings** button underneath this option.

NOTE: For information on how to configure email settings refer to the 'Configuring report emailing options' in this chapter.

7. Specify a name and description for this scheduled report. Click on **Next** to continue.

8. Click on **Finish** to finalize your settings.

Configuring advanced settings

GFI EventsManager ReportPack allows you to export scheduled reports to a specific file format as well as to automatically distribute these reports via email. This is achieved using either a set of parameters (e.g. recipient's email addresses) which are specified on the fly during scheduled report configuration or using the default set of report export and distribution parameters configured during the ReportPack installation.

NOTE: The Report Scheduling Wizard is by default configured to use the default set of report export and distribution parameters.

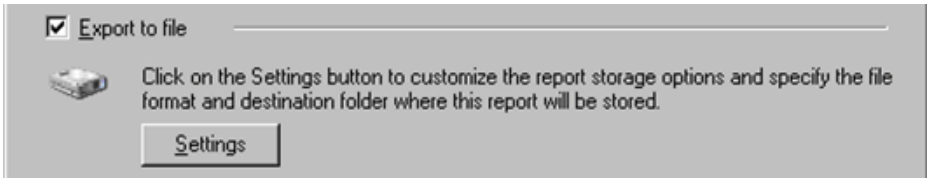
Report export formats

Scheduled reports can be exported in a variety of formats. Supported file formats include:

	Format	Description
1	Adobe Acrobat (.PDF)	Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.
2	MS Excel (.XLS)	Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.
3	MS Word (.DOC)	Use this format if you want to access this report using Microsoft Word.
4	Rich text format (.RTF)	Use this format to save the report in a format that is small in size and which allows accessibility through different word processors in different operating systems.

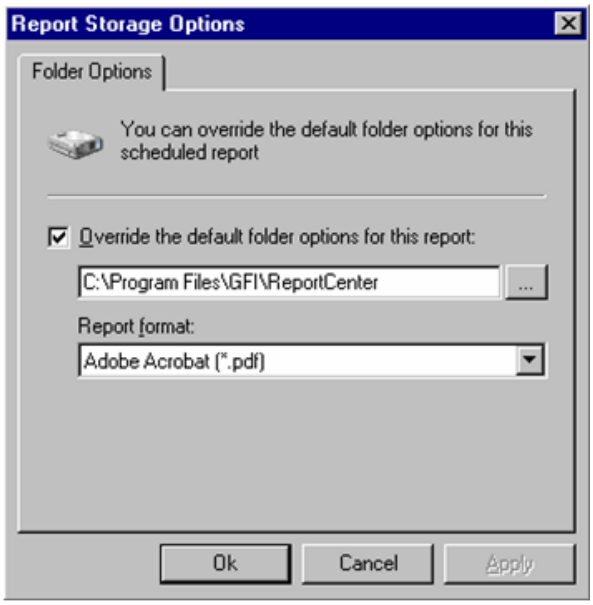
Configuring report export to file options

To configure the report export to file settings of a scheduled report do as follows:



Screenshot 26 - Advanced Settings dialog: Export to file settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Export to file'* option.



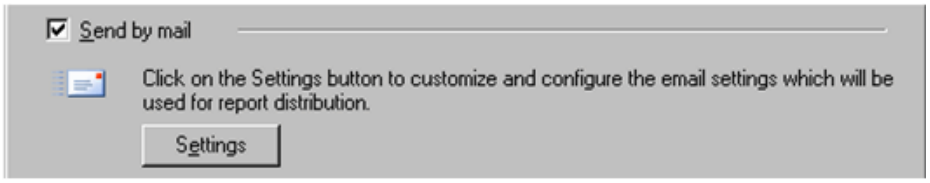
Screenshot 27 - Advanced Settings: Export to file options

2. Select the option *'Override the default folder options for this report:'*
3. Specify the complete path where the exported report will be saved.
4. Specify the file format in which the exported report will be saved.
5. Click **OK** to finalize your configuration settings.

NOTE: For information on how to configure the default export to file settings refer to the 'Configuring default scheduling options' section in this manual.

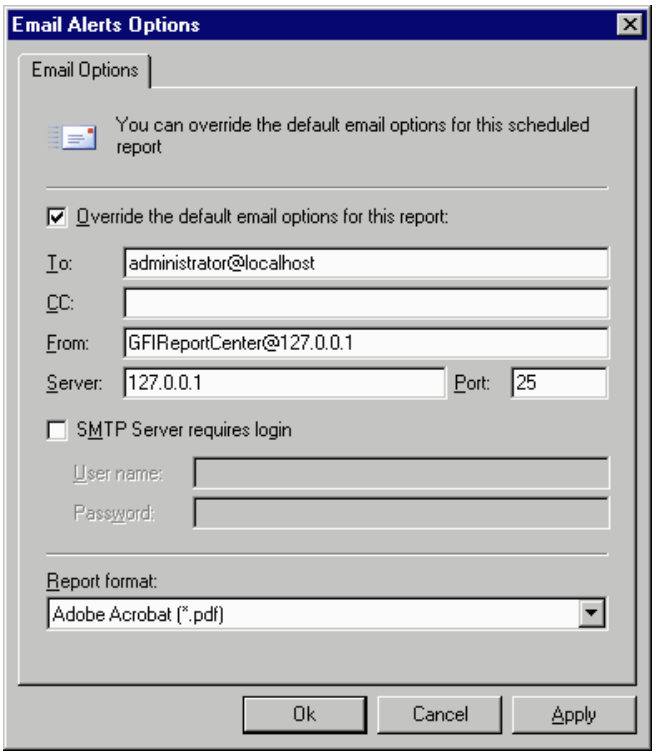
Configuring report emailing options

To configure the report emailing options of a scheduled report do as follows:



Screenshot 28 - Advanced Settings dialog: Send by email settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Send by email'* option.



Screenshot 29 - Report distribution options

2. Select the option *'Override the default email options for this report:'*

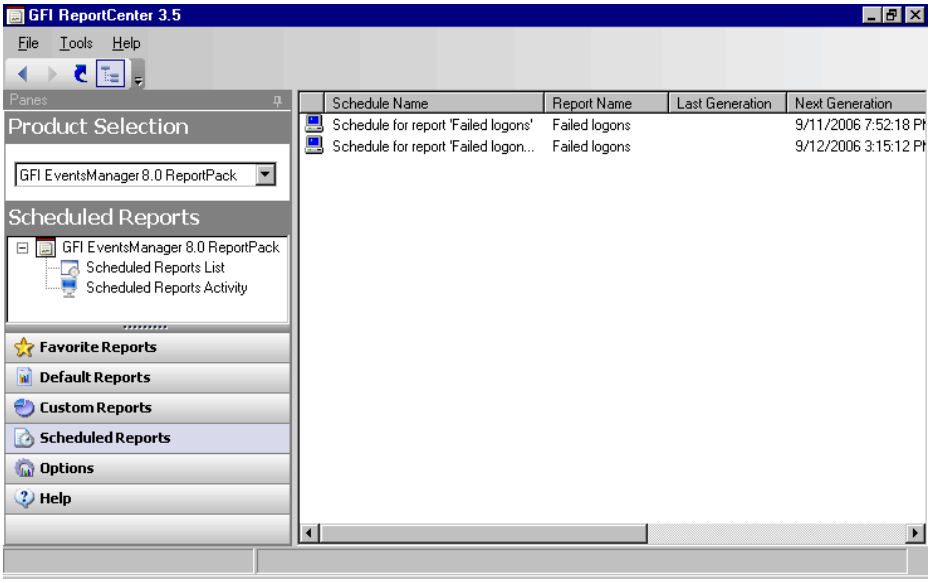
3. Specify the following parameters:

- **To/CC**: Specify the email address(es) where the generated report will be sent.
- **From**: Specify the email account that will be used to send the report.
- **Server**: Specify the name/IP of your SMTP (outbound) email server. If the specified server requires authentication, select the option 'SMTP Server requires login' and specify the logon credentials in the *'User name'* and *'Password'* fields.

- **Report format**: Reports are sent via email as attachments. Select the file format in which to send out your report.

4. Click **OK** to finalize your configuration settings.

Viewing the list of scheduled reports

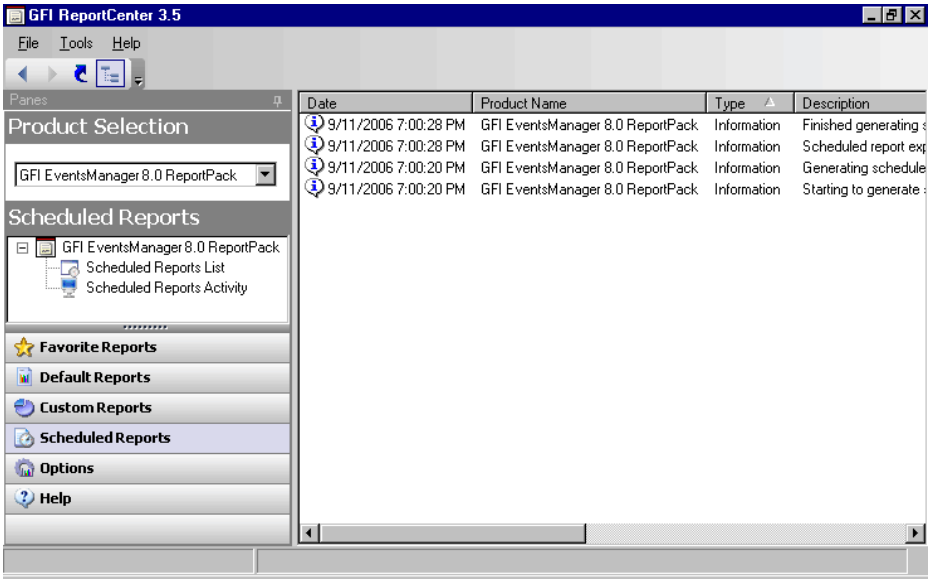


Screenshot 30 - List of Scheduled reports

Click on the **Scheduled Reports** navigation button to show the list of scheduled reports which are currently configured for automatic generation. This information is displayed in the right pane of the management console and includes the following details:

- **Schedule Name:** The custom name that was specified during the creation of the new scheduled report.
- **Report Name:** The names of the default or custom report(s) that will be generate.
- **Last Generation***:* Indicates the date/time when the report was last generated.
- **Next Generation:** Indicate the date/time when the report is to be next generated.
- **Description**: The description that you have entered for each schedule.

Viewing the scheduled reports activity



Screenshot 31 - Schedule activity monitor

GFI ReportCenter also includes a schedule activity monitor through which you can view events related to all scheduled reports that have been executed.

To open the schedule activity monitor, click on the **Scheduled Reports** navigation button and select the **Scheduled Reports Activity** node. This will bring up the activity information in the right pane of the GFI ReportCenter management console.

The activity monitor displays the following events:

- **Information**: The scheduled report was successfully executed and sent by email and/or saved to disk.

- **Warning**: The scheduled report was not executed because product license is invalid or has expired.

- **Error**: The scheduled report was not executed due to a particular condition/event. Typical conditions include:

- Errors when attempting to save the generated report to a specific folder (for example, out of disk space).
- Errors when attempting to send the generated report via email (for example, the SMTP server configured in the GFI ReportCenter settings is not reachable).

The activity monitor records and enumerates the following information:

- **Date:** The date and time when the scheduled report was executed.
- **Product name**: The name of the GFI product to which the report belongs.
- **Type:** The event classification - error, information, or warning.
- **Description:** Information related to the state of a scheduled report that has been executed. The format and contents of the activity description vary, depending on the event type.

NOTE: The description is often the most useful piece of information, indicating what happened during the execution of a scheduled report or the significance of the event.

Enable/disable a scheduled report

Scheduled reports can be enabled or disabled as required. Use the **Scheduled Reports** navigation button to view the list of scheduled reports as well as to identify their current status. The status of scheduled reports is shown through the icon included on the left hand side of each schedule:

 - Indicates that the scheduled report is disabled.

 - Indicates that the scheduled report is enabled/pending.

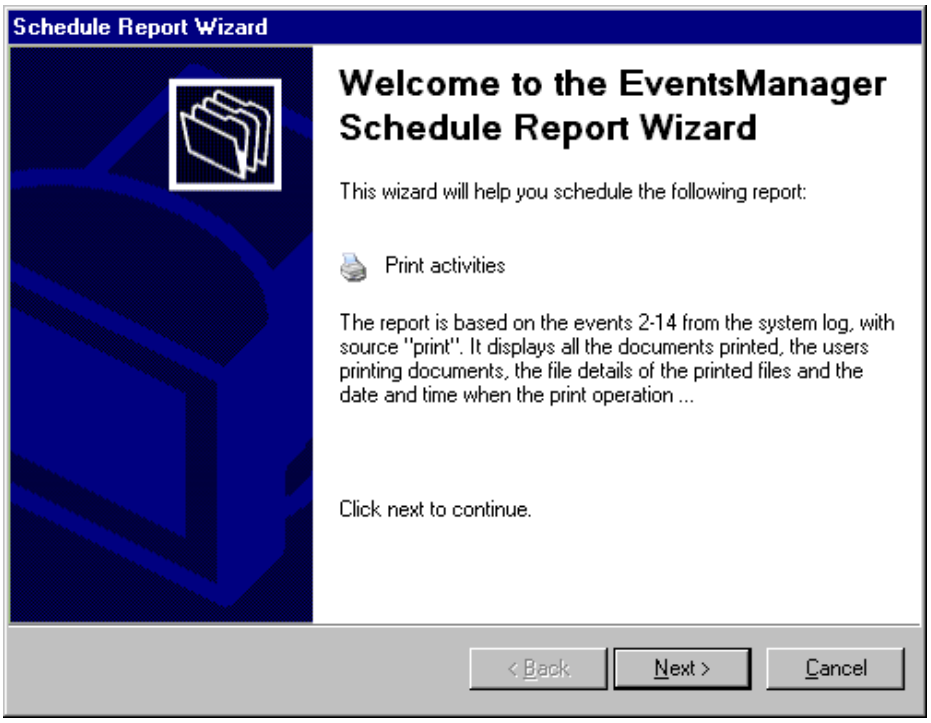
To enable or disable a scheduled report, right-click on the respective report and select **Enable/Disable** accordingly.

Editing a scheduled report

To make changes to the configuration settings of a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be re-configured and select **Properties**. This will bring up the 'Scheduled Reports Wizard'.



Screenshot 32 - Scheduled Reports wizard

3. Click on **Next** and perform the required changes. For information on how to configure the parameters of a scheduled report refer to the 'Creating a scheduled report' section in this chapter.

Deleting a scheduled report

To delete a scheduled report:

1. Click on the **Scheduled Reports** navigation button.

2. Right-click on the scheduled report to be permanently removed from the list and select **Delete**.

Example: Scheduling a report

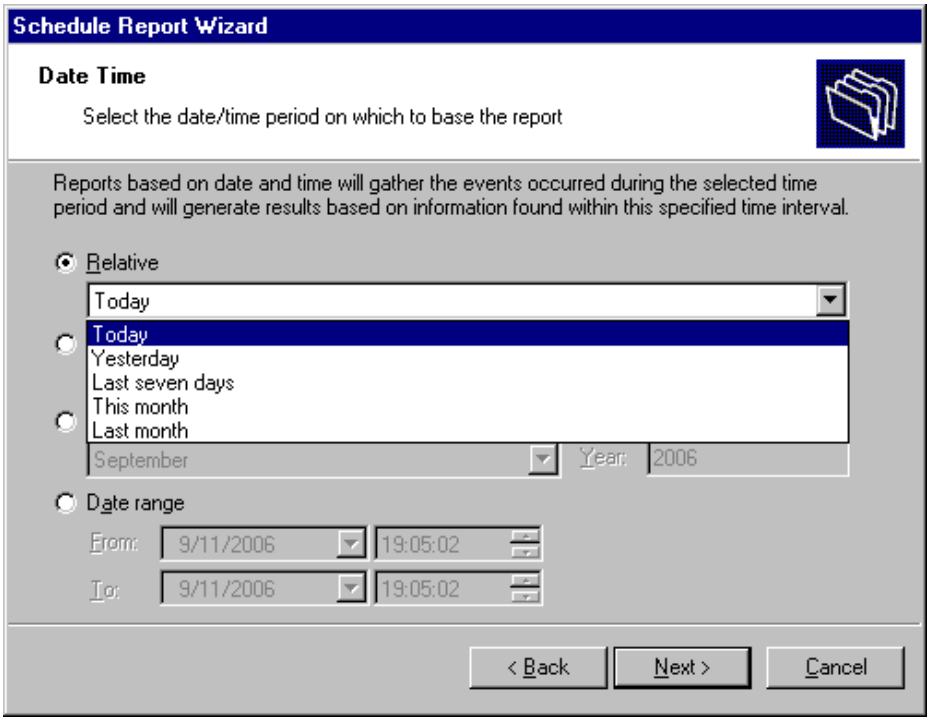
This example demonstrates how to schedule a failed logons report which will:

- Generate the first report on 09/11/2006 at 20:00.
- Continue generating the same report on a daily basis.
- Export the generated report(s) to folder 'C:\Daily Reports' in PDF format.
- Email the generated report using the following custom parameters:
  - Send from email account: 'RC_Admin@gfi.com'
  - Send to email account: 'IT_manager@gfi.com'
  - SMTP server details: '120.11.120.11.

To create the scheduled report:

1. Click on the **Default Reports** navigation button.

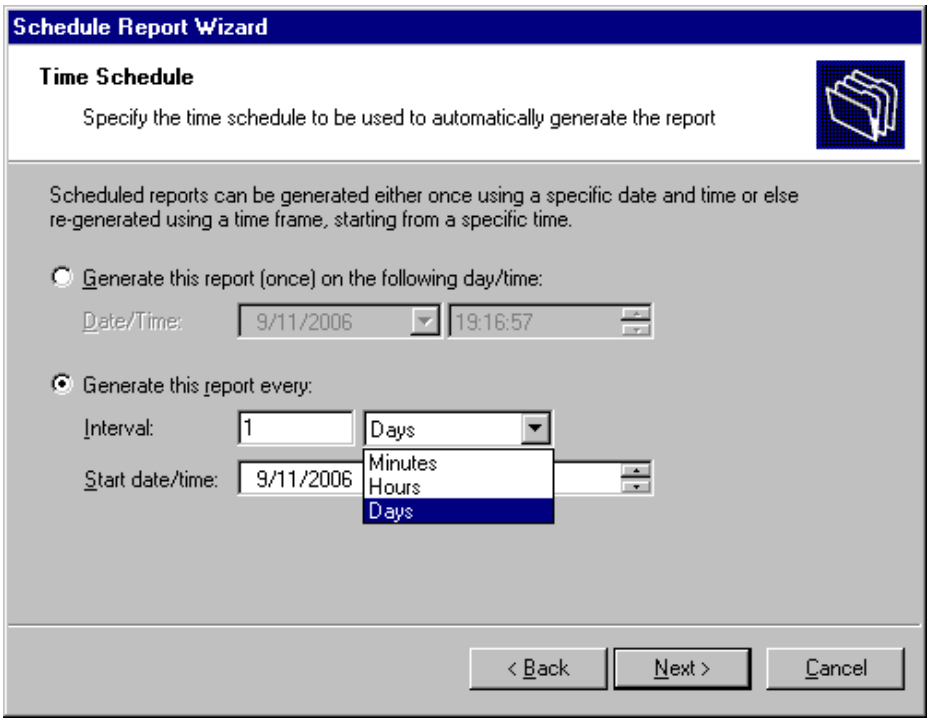
2. Right-click on 'Failed logons' and select **New ► Scheduled Report**. As soon as the welcome dialog is displayed click **Next**.



Screenshot 33 - Select events data period

3. Select the option ***'Relative'*** and from the provided drop down list select *'Today'*. Click on **Next** to proceed to the next dialog.

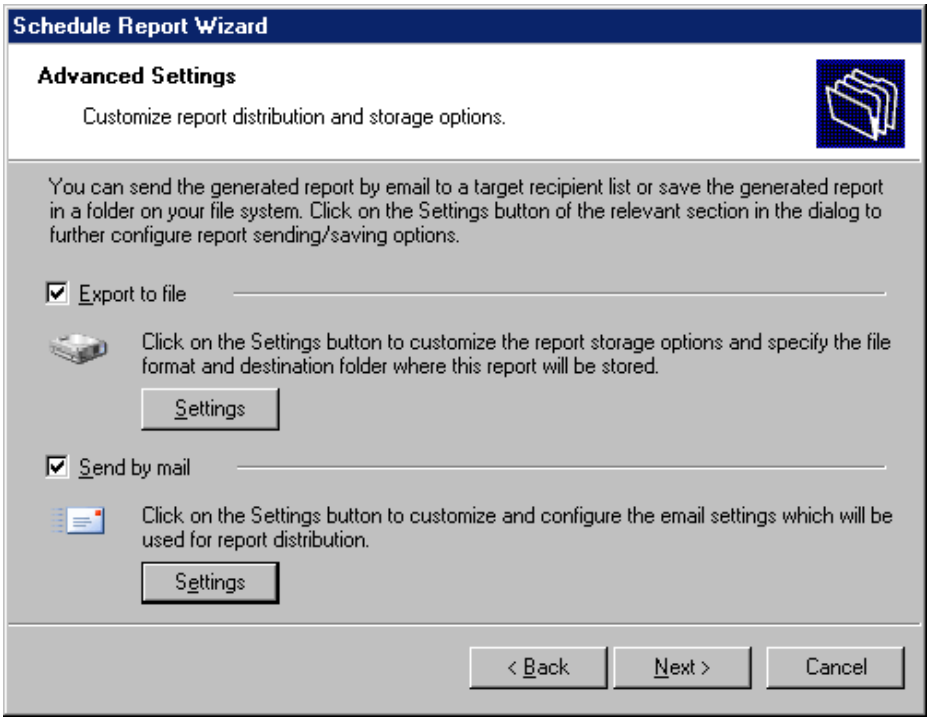
4. Since no data filters will be applied in this example, click **Next** to proceed to the next dialog.



Screenshot 34 – Specifying the scheduling options

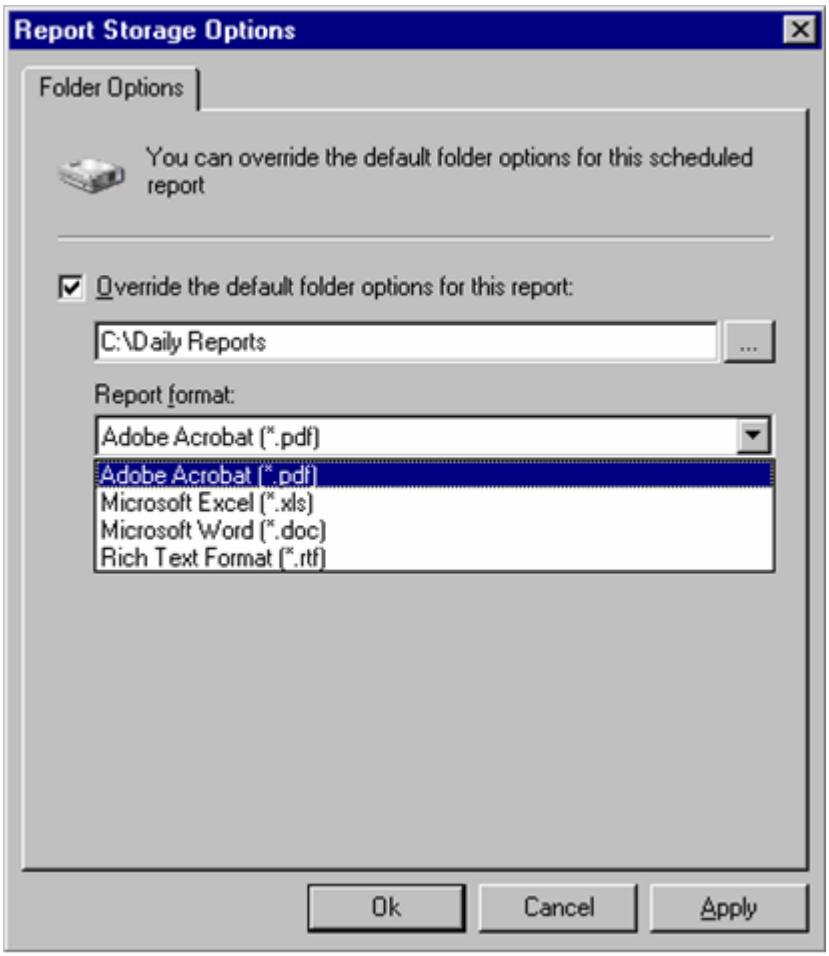
5. To generate this report on daily basis, select the option *'Generate this report every:'* and set the interval to *'1 Day'* .

6. Set the start date to *'09/11/2006'* and time to *'20:00'*. Click **Next** to continue.



Screenshot 35 - Advanced Settings dialog

7. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Export to file'* option.

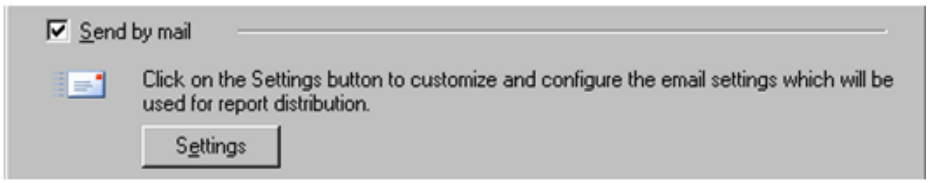


Screenshot 36 - Advanced Settings: Export to file options

8. Select the option *'Override the default folder options for this report:'*

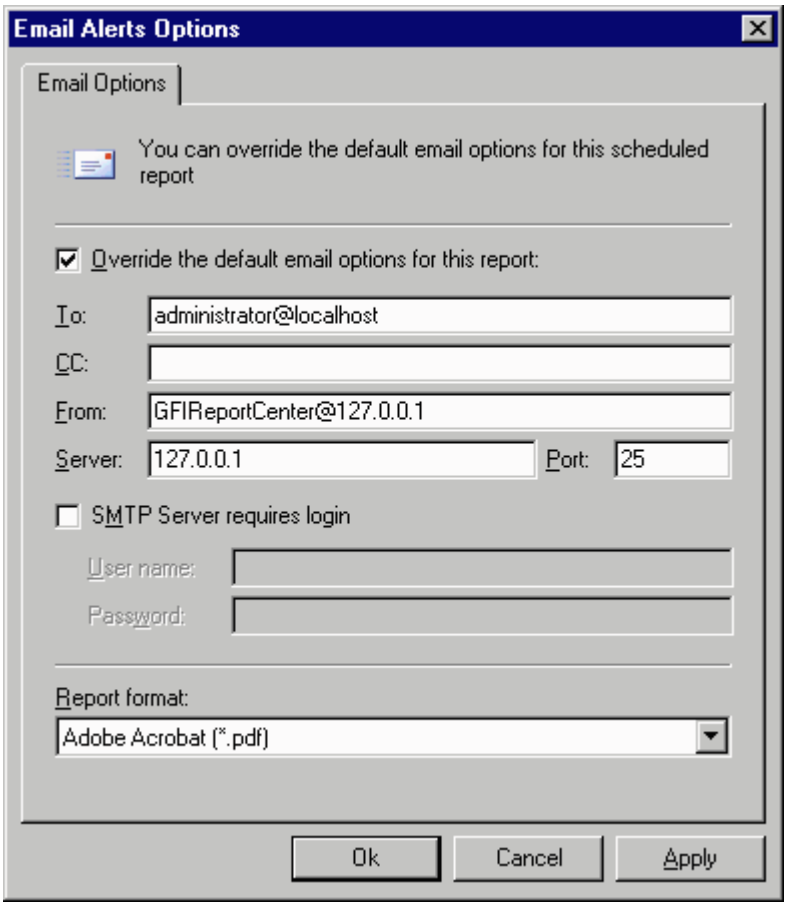
9. Specify the complete path where this report will be saved i.e. *'C:\Daily Reports'*.

10. From the report format drop down select '*PDF'* and click **OK**.



Screenshot 37 - Advanced Settings dialog: Send by email settings button

11. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the *'Send by email'* option.



Screenshot 38 - Report distribution options

12. Select the option *'Override the default email options for this report:'*

13. Specify the following parameters:

- **To:** *'RC_Admin@gfi.com'*
- **From:** *'IT_manager@gfi.com'*
- **Server:** *'120.11.120.11'.*

14. From the report format drop down select *'PDF'* and click **OK** to finalize your email settings.

15. Click **Next** and specify the following parameters:

- **Report Name**: '*Daily failed logons report'*
- **Report Title**: *'Daily failed logons report'*
- **Report Description**: This report is generated on a daily basis at 20:00. It shows all failed logon events recorded throughout the day.

16. Click **Next** to proceed to the final dialog.

17. Click **Finish** to finalize your custom report configuration settings.

Configuring default options

Introduction

The GFI EventsManager ReportPack allows you to configure a default set of parameters which can be used when generating reports. These parameters are first set during installation. However, you can still reconfigure any of these parameters via the **Options** navigation button and the **Tools** menu provided in the GFI ReportCenter management console.

Screenshot 39 - Options navigation button and Tools menu

Through the **Options** navigation button you can configure the following parameter:

- **Database source:** Use this node to specify the database backend from where the ReportPack will extract the required reporting data.

Through the **Tools** menu you can configure the following parameters:

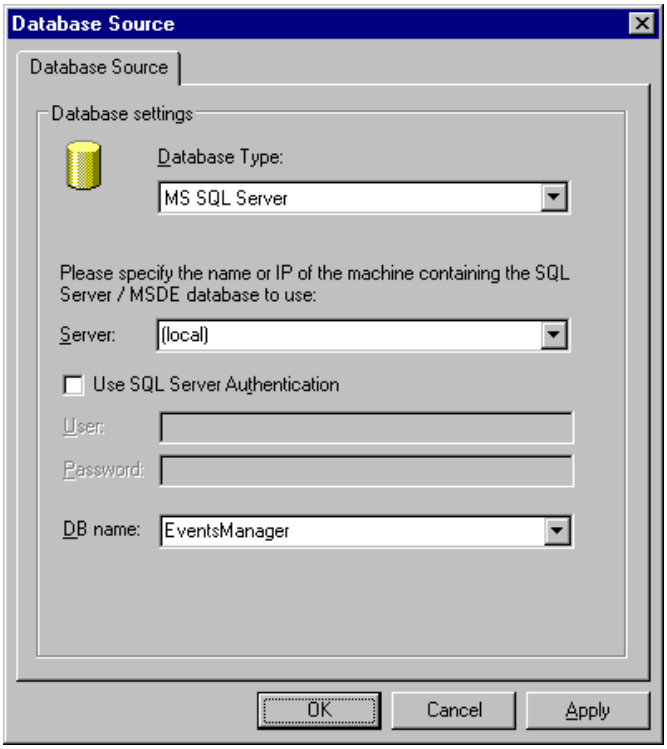
- **Default scheduling settings:** Use this menu option to configure the default export to file parameters and report emailing parameters of scheduled reports.

Configuring database source

To configure your database source:

1. Click on the **Options** navigation button.

2. Right-click on the **Database Source** node and select **Set Database Source…** This will bring up the database source configuration dialog.



Screenshot 40 - Database source configuration dialog

3. Select the database type (e.g. MS SQL Server) from the provided list of supported databases.

NOTE: GFI EventsManager database backend supports only MSDE/MS SQL Server.

4. Specify the name or IP address of your MSDE/MS SQL Server database backend.

5. To use the credentials of an SQL Server account, select the *'Use SQL Server authentication'* option and specify the user name and password in the provided fields.

NOTE: By default, the GFI EventsManager ReportPack uses Windows logon credentials to authenticate to the SQL Server.

6. Specify the name of the database to be used by the database backend.

7. Click on **OK** to finalize your configuration settings.

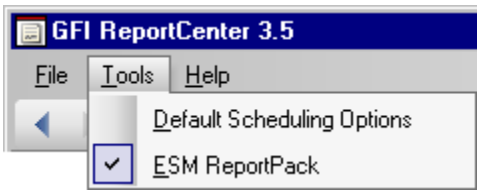
Viewing the current database source settings

Screenshot 41 - Database source configuration settings

After configuration, you can view the current database source settings by clicking on the **Database Source** node.

Configuring default scheduling settings

To configure the default settings to be used by scheduled reports:



Screenshot 42 - Default Scheduling Options node

1. From the pull-down menu, click on the **Tools ► Default Scheduling Options**.

2. Configuration the required parameter as described in the 'Configuring Advanced Settings' section of the Scheduling Reports chapter.

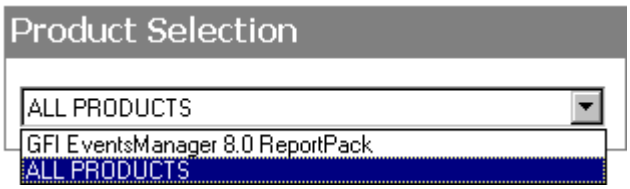
General options

Entering your license key after installation

If you have purchased GFI EventsManager, enter your License key using the **Options** ► **Licensing** node (no re-installation/re-configuration required)

NOTE: Entering the License Key should not be confused with the process of registering your company details on our website. This is important since it allows us to give you support and notify you of important product news. You may register and obtain your GFI customer account from: http://www.gfi.com/pages/regfrm.htm.

To input your GFI EventsManager license key:

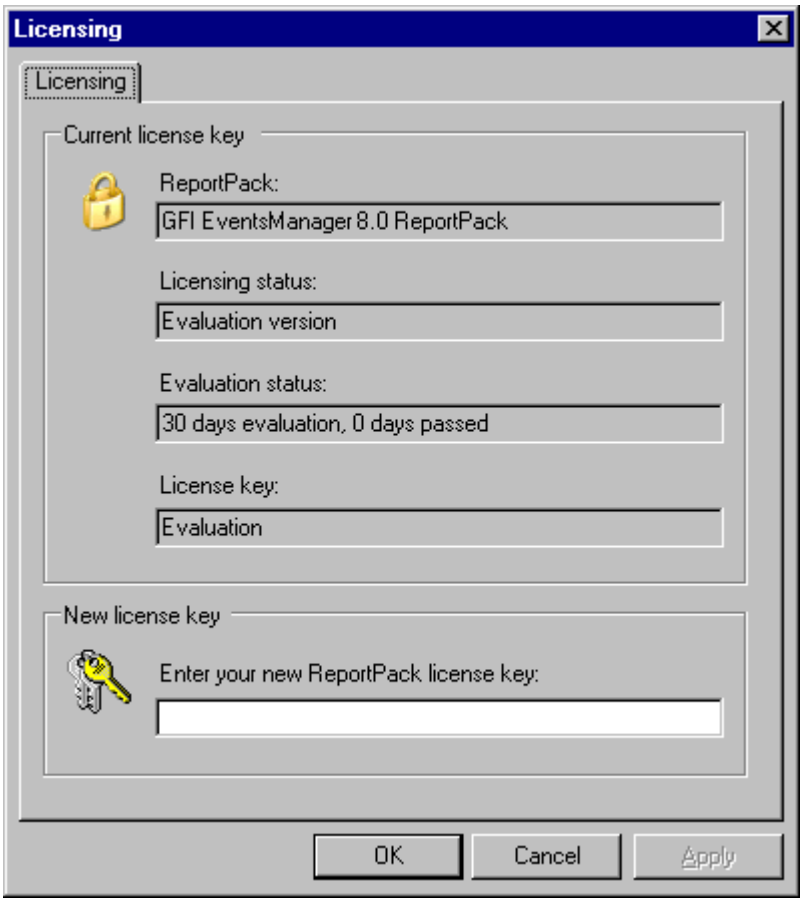


Screenshot 43 – Product Selection drop down list

1. Select the respective product (e.g. *'GFI EventsManager 8 ReportPack'*) from the **Product Selection** drop down list.

2. Click on the **Options** navigation button.

3. Right-click on the **Licensing** node and select **Set Licensing…**. This will bring up the 'Licensing' dialog.



Screenshot 44 - Licensing dialog

4. Type in the GFI EventsManager license key.

5. Click on **OK** to finalize your entry.

Viewing the current licensing details

To view your current licensing details, click on the **Options** navigation button and select the **Licensing** node. The licensing details will be displayed in the right pane of the management console.

Viewing the product ReportPack version details

To view the version information of your product ReportPacks:

1. Select the product ReportPack from the **Product Selection** drop down list.

2. Click on the **Options** navigation button and select the **Version Information** node. The version details will be displayed in the right pane of the management console.

Checking the web for newer builds

Periodically GFI releases product and ReportPack updates which can be automatically downloaded from the GFI website. To check if a newer built is available for download:

Screenshot 45 - Version Properties: Check for newer builds dialog

1. Select the respective product (for example, GFI EventsManager 8 ReportPack) from the **Product Selection** drop down list.

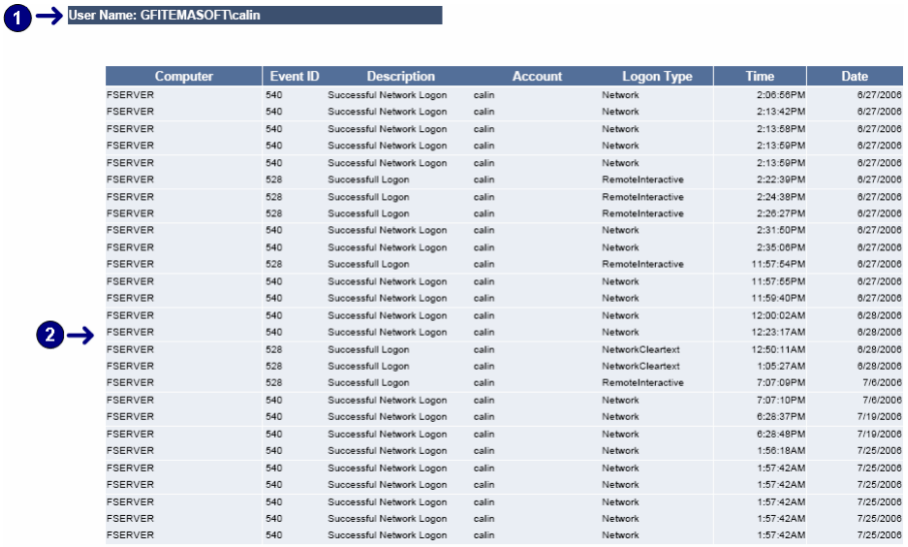
2. Click on the **Options** navigation button.

3. Right-click on the **Version Information** node and select **Checking for newer builds…**

Appendix: GFI EventsManager Default Reports

Account Usage Reports

Successful logons grouped by users



Computer	Event ID	Description	Account	Logon Type	Time	Date
FSERVER	540	Successful Network Logon	calin	Network	2:06:56PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	2:13:42PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	2:13:58PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	2:13:59PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	2:13:59PM	6/27/2006
FSERVER	528	Successfull Logon	calin	RemoteInteractive	2:22:39PM	6/27/2006
FSERVER	528	Successfull Logon	calin	RemoteInteractive	2:24:38PM	6/27/2006
FSERVER	528	Successfull Logon	calin	RemoteInteractive	2:26:27PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	2:31:50PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	2:35:06PM	6/27/2006
FSERVER	528	Successfull Logon	calin	RemoteInteractive	11:57:54PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	11:57:55PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	11:59:40PM	6/27/2006
FSERVER	540	Successful Network Logon	calin	Network	12:00:02AM	6/28/2006
FSERVER	540	Successful Network Logon	calin	Network	12:23:17AM	6/28/2006
FSERVER	528	Successfull Logon	calin	NetworkCleartext	12:50:11AM	6/28/2006
FSERVER	528	Successfull Logon	calin	NetworkCleartext	1:05:27AM	6/28/2006
FSERVER	528	Successfull Logon	calin	RemoteInteractive	7:07:09PM	7/6/2006
FSERVER	540	Successful Network Logon	calin	Network	7:07:10PM	7/6/2006
FSERVER	540	Successful Network Logon	calin	Network	6:28:37PM	7/19/2006
FSERVER	540	Successful Network Logon	calin	Network	6:28:48PM	7/19/2006
FSERVER	540	Successful Network Logon	calin	Network	1:56:18AM	7/25/2006
FSERVER	540	Successful Network Logon	calin	Network	1:57:42AM	7/25/2006
FSERVER	540	Successful Network Logon	calin	Network	1:57:42AM	7/25/2006
FSERVER	540	Successful Network Logon	calin	Network	1:57:42AM	7/25/2006
FSERVER	540	Successful Network Logon	calin	Network	1:57:42AM	7/25/2006
FSERVER	540	Successful Network Logon	calin	Network	1:57:42AM	7/25/2006

Screenshot 46 - Sample report showing Successful logons grouped by users

1	Username
2	List of events showing all successful logons by a specific user.

Use this report to:

- Generate a list of all successful user logons, grouped by user
- Monitor all access to network resources.

Successful logons grouped by computers

User	Event ID	Description	Account	Logon Type	Time	Date
NT AUTHORITY\NETWORK SER\	528	Successfull Logon	NETWORK SERVICE	Service	12:27:23PM	9/11/2006
CALDEV\Calin	528	Successfull Logon	Calin	Interactive	12:28:14PM	9/11/2006
CALDEV\Calin	528	Successfull Logon	Calin	Interactive	12:29:20PM	9/11/2006
CALDEV\Calin	528	Successfull Logon	Calin	Interactive	12:33:07PM	9/11/2006
CALDEV\Calin	528	Successfull Logon	Calin	Interactive	12:34:39PM	9/11/2006
CALDEV\Calin	528	Successfull Logon	Calin	Service	12:38:47PM	9/11/2006

User	Event ID	Description	Account	Logon Type	Time	Date
GFITEMASOFT\Administrator	540	Successful Network Logon	Administrator	Network	5:56:24PM	11/15/2005
GFITEMASOFT\Administrator	540	Successful Network Logon	Administrator	Network	6:47:43PM	11/15/2005
GFITEMASOFT\Administrator	540	Successful Network Logon	Administrator	Network	6:47:43PM	11/15/2005
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:06:56PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:13:42PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:13:58PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:13:59PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:13:59PM	6/27/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	RemoteInteractive	2:22:39PM	6/27/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	RemoteInteractive	2:24:38PM	6/27/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	RemoteInteractive	2:26:27PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:31:50PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:35:08PM	6/27/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	RemoteInteractive	11:57:54PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	11:57:55PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	11:59:40PM	6/27/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	12:00:02AM	6/28/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	12:23:17AM	6/28/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	NetworkCleartext	12:50:11AM	6/28/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	NetworkCleartext	1:05:27AM	6/28/2006
GFITEMASOFT\calin	528	Successfull Logon	calin	RemoteInteractive	7:07:09PM	7/6/2006
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	7:07:10PM	7/6/2006

Screenshot 47 - Sample report showing Successful logons grouped by computers

1	Computer name
2	List of events showing all successful logons on a specific computer. Events are grouped by computer, providing an overview of the logon activity in each domain.

Use this report to:

- Generate a list of all successful user logons, grouped by computer
- Monitor all access to network resources.

Failed logons

Computer	User	Event ID	Description	Account	Logon Type	Time	Date
CALDEV	CALDEV\drsdffsdf	529	LF: Bad user name/ password	drsdffsdf	Interactive	12:27:53PM	9/11/2006
CALDEV	CALDEV\test	529	LF: Bad user name/ password	test	Interactive	12:28:09PM	9/11/2006
CALDEV	CALDEV\test	529	LF: Bad user name/ password	test	Interactive	12:29:13PM	9/11/2006
CALDEV	CALDEV\test	531	LF: Account Disabled	test	Interactive	12:33:02PM	9/11/2006
CALDEV	CALDEV\test	534	LF: Logon Type Rejected	test	Interactive	12:34:34PM	9/11/2006

Screenshot 48 - Sample report showing Failed logons

1	List of events showing all failed logons, including user account and reason for failure

Use this report to:

- Generate a list of all failed logons
- Investigate multiple logon failures.

NOTE 1: Logon failure due to a disabled account may signal attempted abuse by former internal users, such as ex-employees.

NOTE 2: Logon failure due to account expiry may signal attempted abuse by contractors or temporary internal users.

Logoff events

Computer	User	Event ID	Description	Account	Logon Type	Time	Date
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:56:27AM	7/26/2006
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:13AM	7/26/2006
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:42AM	7/26/2006
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:42AM	7/26/2006
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:42AM	7/26/2006
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:52AM	7/26/2006
FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:58:12AM	7/26/2006
FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	Network	2:18:38AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	RemoteInteractive	2:22:07AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	Network	2:36:43AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	Network	2:38:04AM	9/10/2006

Screenshot 49 - Sample report showing Logoff events

1	List of events showing all user logoff events. Correlate these events with the successful logon events to determine the duration of each user session.

Use this report to:

- Generate a list of all user logoff events
- Determine the duration of a user session.

Account Logons

NTLM Logon attempts

The group is based on event 680 – Account used for logon and 681 – Logon to account failed. The evens identify the account used for the successful or failed domain logon attempts. Event 680 is logged on Windows 2003 domains both for successful and failed attempts. On Windows 2000 domains, event 680 is logged only for successful attempts while event 681 is logged for failed attempts.

Computer	Type	Description	Logon Account	Source Workstation	Error Code	Time	Date
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006
VDC	Audit failure	Logon to account failed	Calin	CALDEV	3221225572	4:10:59PM	9/10/2006

Kerberos authentication ticket requests

The section is based on event 672 – authentication ticket request. This event enables the tracking of initial domain logons through the granting of ticket granting tickets (TGT). Windows 2003 domain records this event for both success and failure requests. The type field indicates whether the request was successful or not. In Windows 2000 domains, the event only records successful requests. For failed requests in Windows 2000 domains use the 676 event.

Computer	Type	User Name	Service Name	Client Address	Result Code	Time	Date
FSERVER	Audit success	GFITEMASOFT.RO\FSERVER$	krbtgt	127.0.0.1	N/A	12:08:06AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\FSERVER$	krbtgt	127.0.0.1	N/A	12:08:06AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\FSERVER$	krbtgt	127.0.0.1	N/A	12:08:17AM	9/10/2006
FSERVER	Audit failure	GFITEMASOFT\alina	krbtgt\GFITEMASOFT	127.0.0.1	N/A	12:13:26AM	9/10/2006
FSERVER	Audit failure	GFITEMASOFT\alina	krbtgt\GFITEMASOFT	127.0.0.1	N/A	12:13:26AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT\Administrator	krbtgt	127.0.0.1	N/A	12:31:46AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT\IUSR_FSERVER	krbtgt	127.0.0.1	N/A	12:41:56AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT\IUSR_FSERVER	krbtgt	127.0.0.1	N/A	1:38:53AM	9/10/2006

Kerberos service ticket requests

The section is based on event 673 - A ticket granting service (TGS) ticket was requested. After a user's workstation requests a ticket granting ticket (TGT), the workstation immediately requests a service ticket (TGS) so that the user can use the workstation. Windows 2003 domain records this event for both success and failure requests. The type field indicates whether the request was successful or not. In Windows 2000 domains, the event only records successful requests. For failed requests in Windows 2000 domains use the 677 event.

Computer	Type	User Name	Service Name	Client Address	Failure Code	Time	Date
FSERVER	Audit success	GFITEMASOFT.RO\Administrator@GFITEMASOFT.RO	FSERVER$	127.0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\Administrator@GFITEMASOFT.RO	FSERVER$	127.0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\Administrator@GFITEMASOFT.RO	FSERVER$	127.0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\Administrator@GFITEMASOFT.RO	FSERVER$	127.0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\Administrator@GFITEMASOFT.RO	FSERVER$	127.0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\Administrator@GFITEMASOFT.RO	FSERVER$	127.0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audit success	GFITEMASOFT.RO\fserver$@GFITEMASOFT.RO	krbtgt	127.0.0.1	-	4:16:26AM	9/10/2006

Kerberos failed events

The section is based on events 675 - Pre-authentication failed, 676 - Authentication Ticket Request failed, and 677 – Service ticket request failed. Event 675 is recorded both in Windows 2000 and Windows 2003 domains. In a Windows 2000 domain, events 676 and 677 are logged for failed authentication/service ticket request.

Computer	User Name	Description	Service Name	Client Address	Failure Code	Time	Date
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	127.0.0.1	0x18	4:16:20AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	127.0.0.1	0x18	4:16:20AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	127.0.0.1	0x18	4:16:20AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	192.168.100.20	0x25	4:19:55AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	192.168.100.20	0x25	4:19:55AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	192.168.100.20	0x25	4:19:55AM	9/10/2006
FSERVER	GFITEMASOFT\Administrator	Pre-authentication failed	krbtgt\GFITEMASOFT	192.168.100.20	0x25	4:20:17AM	9/10/2006

Terminal services account logon events

The section is based on events 682 and 683 from the Account Logon category. The 682 event is recorded when a user has reconnected to a disconnected Terminal Services session. The 683 event is recorded when a user disconnected a Terminal Services session without logging off.

Computer	User Name	Description	Session Name	Client Name	Client Address	Time	Date
FSERVER	GFITEMASOFT\administrator	Session disconnected from winstation	RDP-Tcp#3	Z	192.168.100.11	1:51:01AM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session disconnected from winstation	RDP-Tcp#3	Z	192.168.100.11	1:51:01AM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session reconnected to winstation	RDP-Tcp#4	Z	192.168.100.11	1:53:15AM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session reconnected to winstation	RDP-Tcp#4	Z	192.168.100.11	1:53:15AM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session disconnected from winstation	RDP-Tcp#4	Z	192.168.100.11	2:33:04PM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session disconnected from winstation	RDP-Tcp#4	Z	192.168.100.11	2:33:04PM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session reconnected to winstation	RDP-Tcp#5	Z	192.168.100.11	2:34:11PM	8/21/2006
FSERVER	GFITEMASOFT\administrator	Session reconnected to winstation	RDP-Tcp#5	Z	192.168.100.11	2:34:11PM	8/21/2006

Screenshot 50 - Sample report showing account logons

1	List showing the NTLM logon attempts
2	List showing the Kerberos authentication ticket requests
3	List showing the Kerberos service ticket requests
4	List showing the Kerberos failed events
5	List showing the Terminal Services account logon events

Use this report to:

- Generate a list of all system logons.

Account lockouts

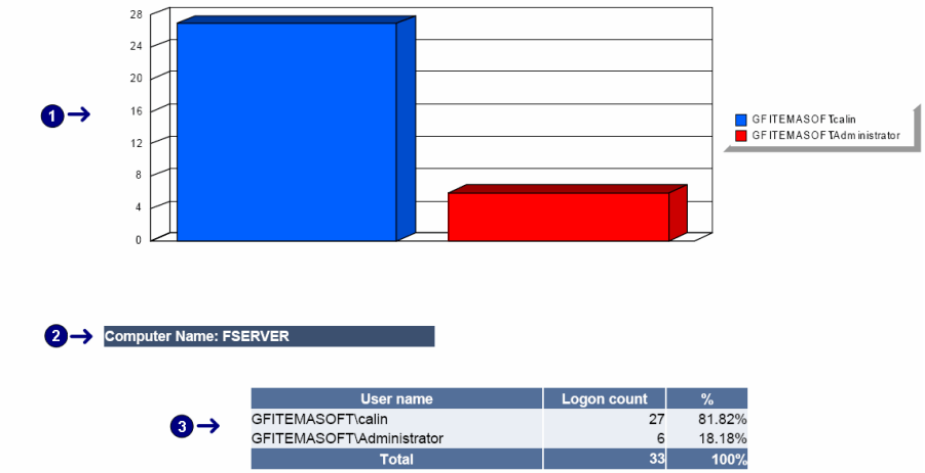
Screenshot 51 - Sample report showing Account lockouts

1	List of events showing all user accounts which have been locked out

Use this report to:

- Generate a list of all user accounts which have been locked out
- Identify possible attacks against the default Administrator account.

Successful logon count on each computer



Screenshot 52 - Sample report showing Successful logon count on each computer

1	Chart displaying the distribution of successful logon events by user on a specific computer
2	Computer name
3	List of events showing all successful user logon events on a specific computer

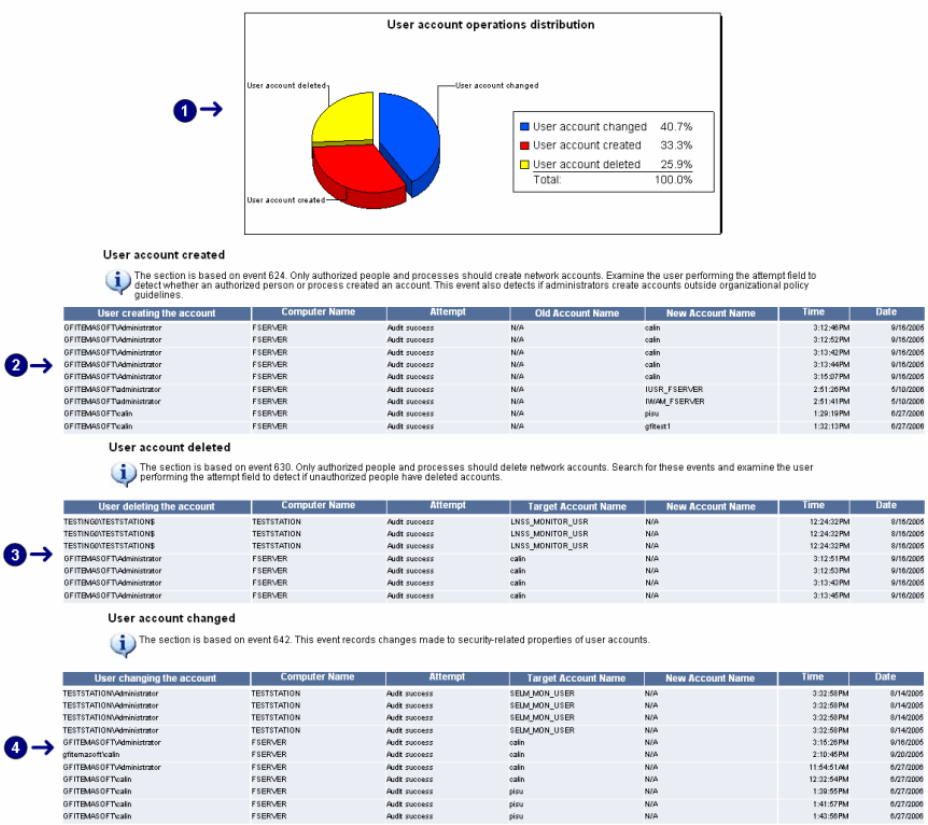
Use this report to:

- Graphically represent successful logons by users on each computer

- Generate statistical information of successful logons by users on each domain / computer.

Account Management Reports

User account management



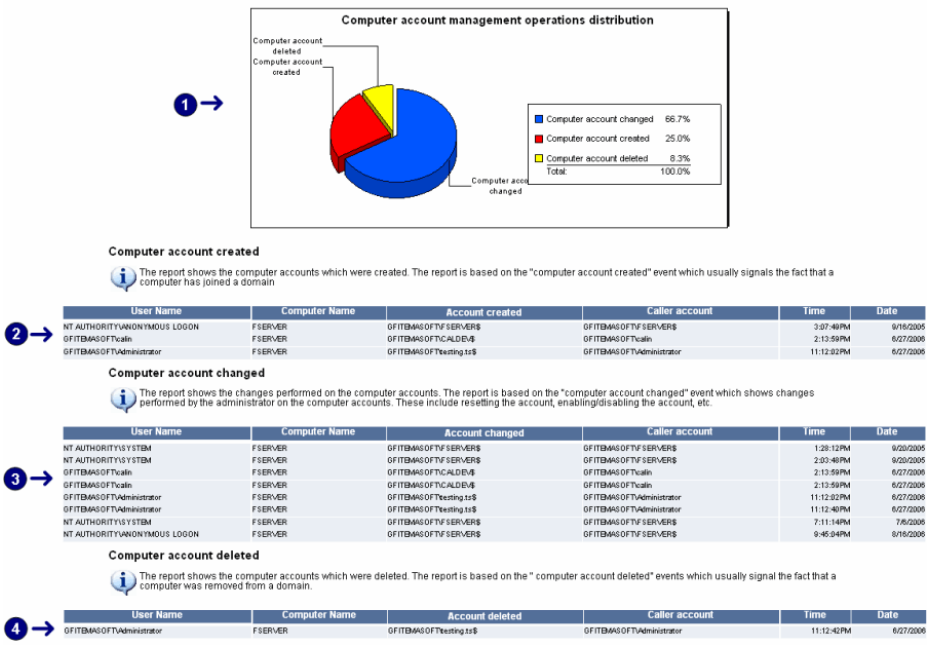
Screenshot 53 - Sample report showing User account management

1	Chart displaying user accounts created, deleted and changed
2	List of events showing user accounts created
3	List of events showing user accounts deleted
4	List of events showing user accounts amended

Use this report to:

- Discover irregular or unusual network account activity
- Identify administrators who abuse privileges to create or modify accounts
- Identify patterns of account activity that do not conform to corporate security policy.

Computer account management



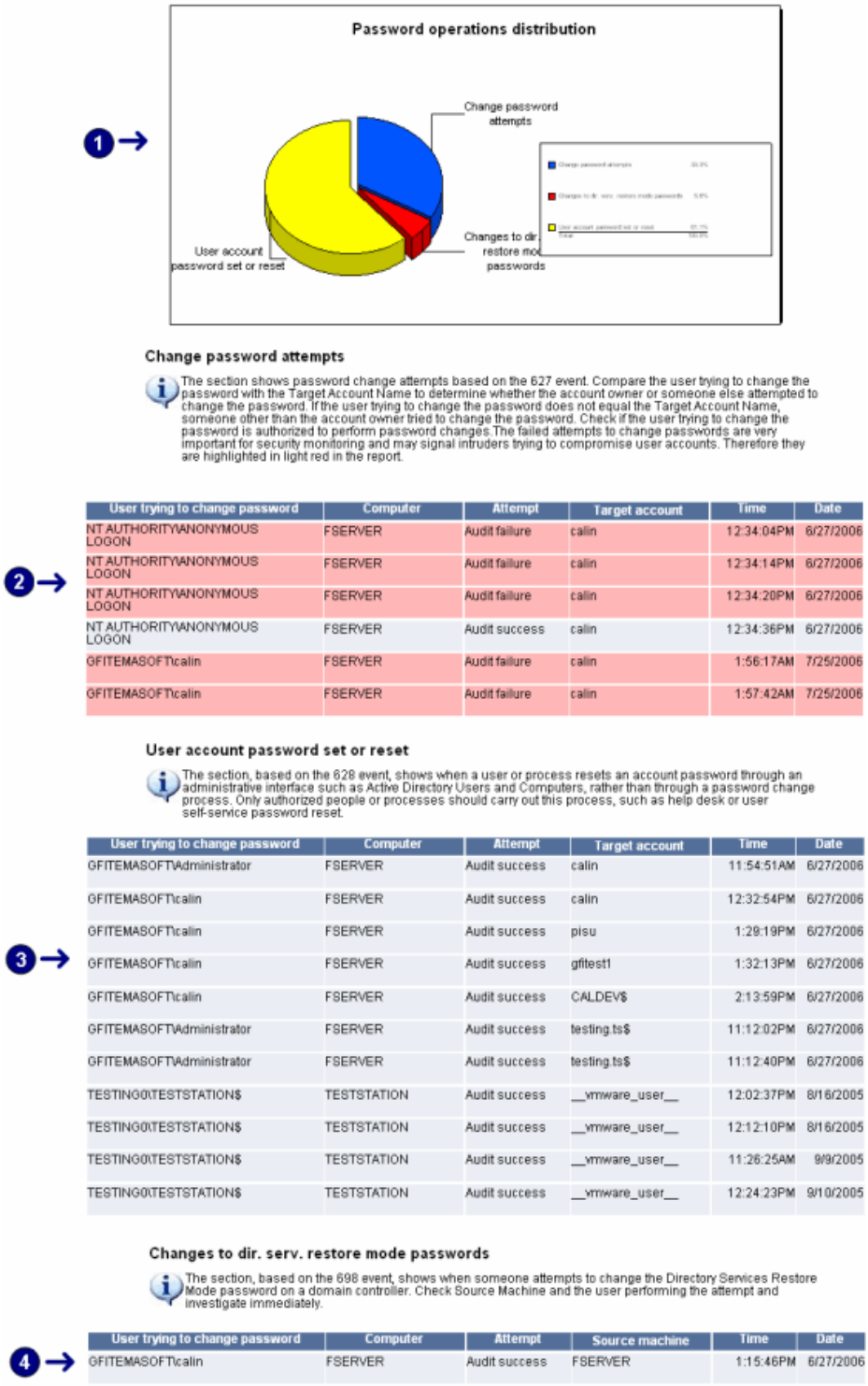
Screenshot 54 - Sample report showing Computer account management

1	Chart displaying computer accounts created, deleted and changed
2	List of events showing computer accounts created
3	List of events showing computer accounts deleted
4	List of events showing computer accounts amended

Use this report to:

- Audit computer access to the network and to domain resources
- Obtain information on computer domain membership.

Password changes



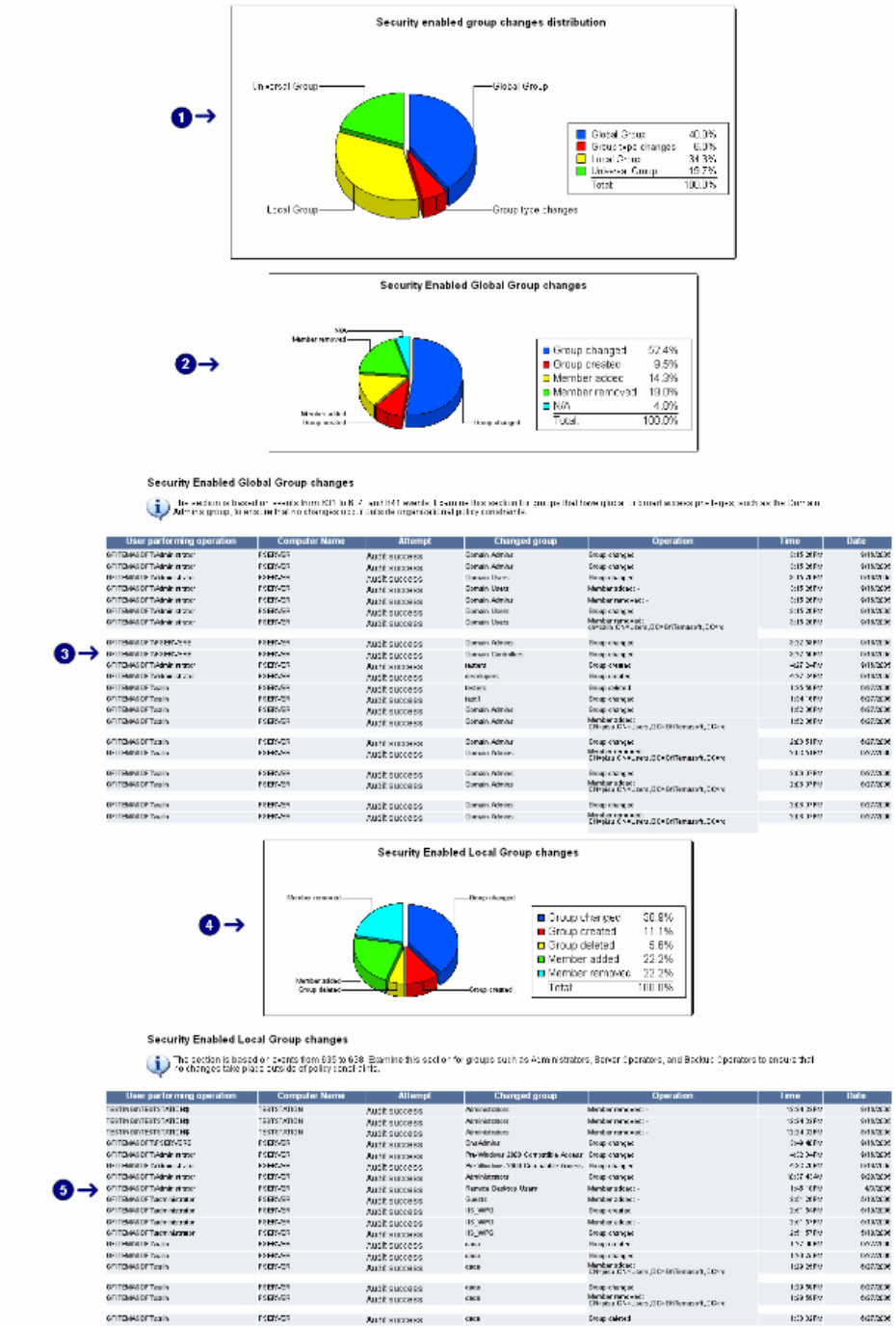
Screenshot 55 - Sample report showing password changes

1	Chart displaying attempts made to change or reset passwords
2	List of events showing password change attempts
3	List of events showing passwords set or reset
4	List of events showing attempts to change the Directory Services Restore Mode password on a domain controller

Use this report to:

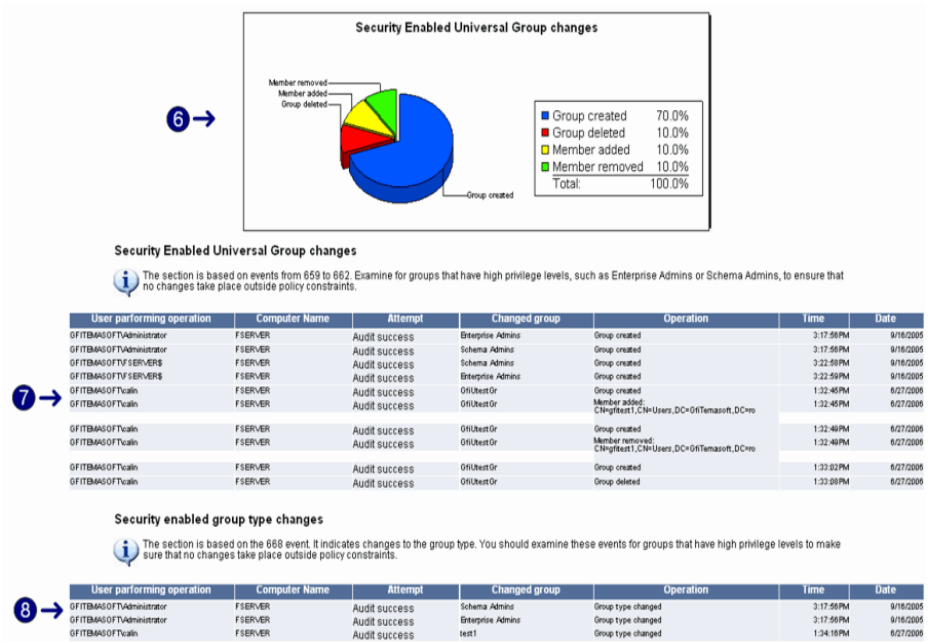
- Identify password changes that do not conform to corporate security policy.

Security group management



Screenshot 56 - Sample showing extracts from the Security group management report

1	Chart displaying distribution of security enabled group changes according to group type
2	Chart displaying distribution of events related to security enabled global group changes
3	List of events with details related to security enabled global group changes
4	Chart displaying distribution of events related to security enabled local group changes
5	List of events with details related to security enabled local group changes



Screenshot 57 - Sample showing extracts from the Security group management report

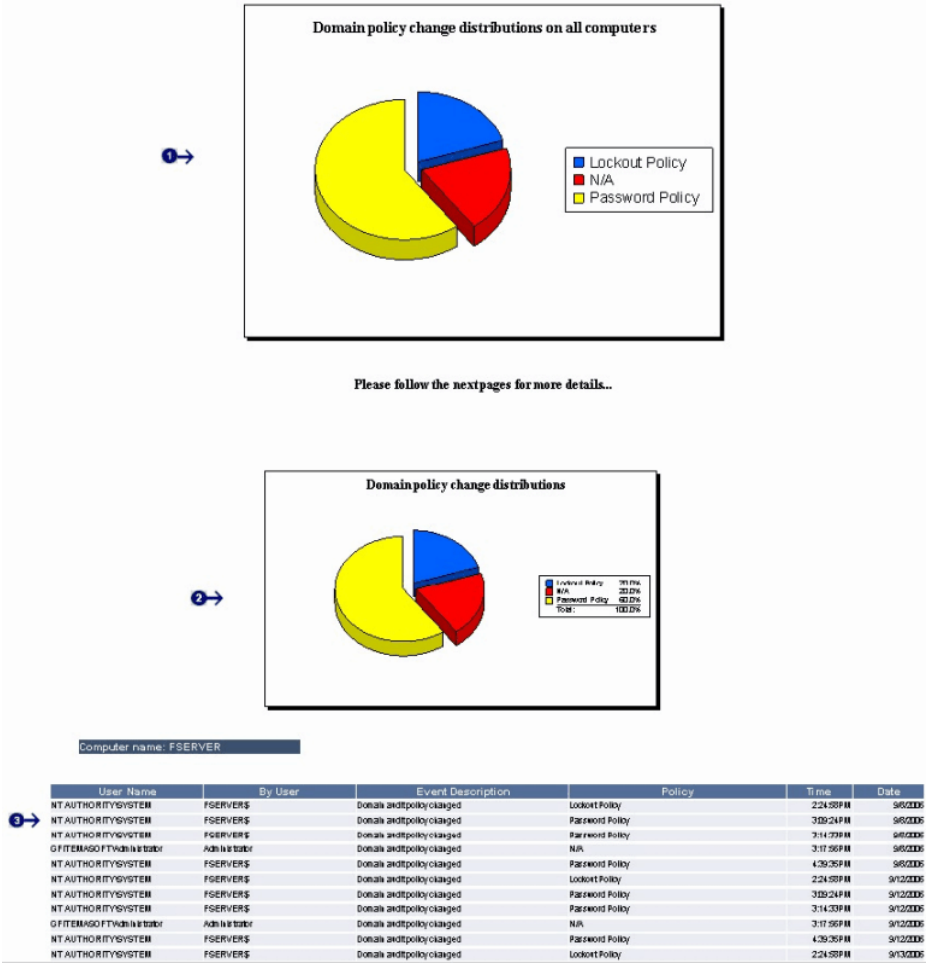
6	Chart displaying distribution of events related to security enabled universal group changes
7	List of events with details related to security enabled local group changes
8	List of events with details related to changes in group type

Use this report to:

- Identify user account group memberships that do not conform to corporate security policy
- Identify user account group membership changes that do not conform to corporate security policy.

Policy Changes Reports

Domain policy changes



Screenshot 58 – Sample report showing Domain policy changes

1	Distribution of the domain policy changes for all the computers
2	Distribution of the domain policy changes per computer
3	Policy change event details

Use this report to:

- Identify domain policy changes
- Identify changes that were not made by authorized personnel.

Local audit policy changes

Screenshot 59 - Sample report showing Local audit policy changes

1	Privilege values and their short descriptions
2	Computer name
3	List of events with details related to audit policy changes, grouped by computer

Use this report to:

- Identify audit policy changes
- Identify changes that were not made by authorized personnel.

User right assignment changes

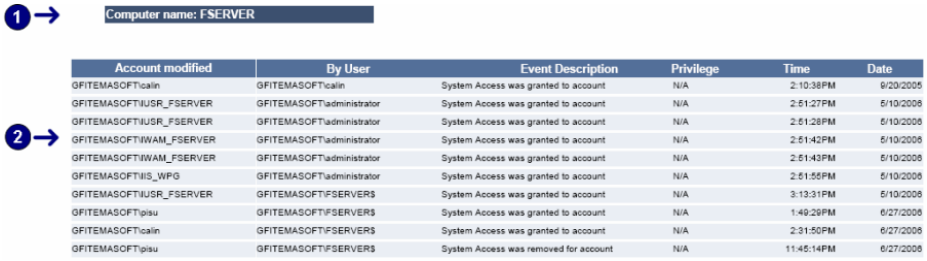
Screenshot 60 - Sample report showing user right assignment changes

1	Privilege values and their short descriptions
2	Computer name
3	List of events with details related to user rights changes, grouped by computer

Use this report to:

- Identify new privileges granted to a user account
- Identify privileges removed from a user account.

System access granted / removed



Account modified	By User	Event Description	Privilege	Time	Date
GFITEMASOFT\calin	GFITEMASOFT\calin	System Access was granted to account	N/A	2:10:38PM	9/20/2005
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:27PM	5/10/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:28PM	5/10/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:42PM	5/10/2006
GFITEMASOFT\IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:43PM	5/10/2006
GFITEMASOFT\IIS_WPG	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:55PM	5/10/2006
GFITEMASOFT\IUSR_FSERVER	GFITEMASOFT\FSERVER$	System Access was granted to account	N/A	3:13:31PM	5/10/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER$	System Access was granted to account	N/A	1:49:29PM	6/27/2006
GFITEMASOFT\calin	GFITEMASOFT\FSERVER$	System Access was granted to account	N/A	2:31:50PM	6/27/2006
GFITEMASOFT\pisu	GFITEMASOFT\FSERVER$	System Access was removed for account	N/A	11:45:14PM	6/27/2006

Screenshot 61 - Sample report showing System access granted / removed

1	Computer name
2	List of events with details related to system access granted or revoked, grouped by computer

Use this report to:

- Identify users granted access to a system
- Identify users whose access to a system has been revoked.

Encrypted Data Recovery policy

User Name	By User	Event Description	Privilege	Time	Date
NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER$	Encrypted data recovery policy changed	N/A	3:09:30PM	9/16/2005

Screenshot 62 - Sample report showing Encrypted Data Recovery policy

1	Computer name
2	List of encrypted data recovery policy events, grouped by computer

Use this report to:

- Monitor encrypted data recovery policy events
- Investigate occurrence of events that do not conform to corporate security policy.

IPsec policy changes

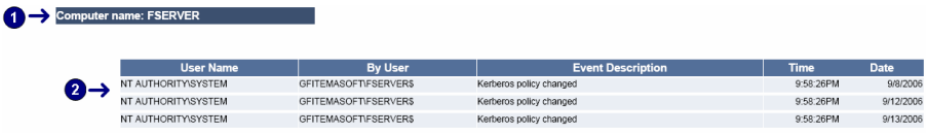
Screenshot 63 - Sample report showing IPsec policy changes

1	Computer name
2	List of events with details related to IPsec policy changes, grouped by computer.

Use this report to:

- Monitor IPsec policy changes
- Investigate occurrence of events outside system startups.

Kerberos policy changes



Screenshot 64 - Sample report showing Kerberos policy changes

1	Computer name
2	List of events with details related to Kerberos policy changes, grouped by computer.

Use this report to:

- Monitor Kerberos policy changes
- Identify changes that were not made by authorized personnel
- Identify changes that do not conform to corporate security policy.

Object Access Reports

Failed attempts to access to files and registry

Computer	User	Event ID	Description	Object Name	Object Type	Time	Date
FSERVER	GFITEMASOFT\pisu	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	3:06:00PM	8/27/2006

Screenshot 65 - Sample repot showing failed attempts to access to files and registry

1	List of events showing failed object access attempts on files and registry

Use this report to:

- Identify requests for object access which have been rejected
- Identify which users are trying to access resources to which they have not been granted privileges.

NOTE: File auditing should be enabled on the required files and registry values of interest.

Successful attempts to access files and registry

Computer	User	Event ID	Description	Object Name	Object Type	Time	Date
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	11:42:17PM	6/27/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	11:44:37PM	6/27/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	12:00:11AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	12:01:07AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	12:01:18AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	C:\StyleSheets	File	12:09:54AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	C:\dot.exe	File	12:09:54AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	C:\dot.exe	File	12:09:54AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	C:\dot.exe	File	12:12:21AM	6/28/2006
FSERVER	GFITEMASOFT\calin	560	Object Open	C:\dot.exe	File	12:12:21AM	6/28/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	12:47:40AM	6/29/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	8:37:17PM	6/29/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	10:12:35PM	7/2/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	8:16:37PM	7/26/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	10:46:18PM	7/26/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	11:56:49PM	7/27/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	11:56:49PM	7/27/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	9:46:25PM	8/17/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	1:25:38AM	8/18/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	10:47:43PM	8/23/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	10:47:43PM	8/23/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	1:23:17AM	8/24/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	1:16:22AM	8/26/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	3:22:28AM	8/26/2006
FSERVER	GFITEMASOFT\Administrator	560	Object Open	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\Eventlog\Security	Key	6:28:59AM	8/26/2006

Screenshot 66 - Sample report showing Successful attempts to access files and registry

1	List of events showing successful object access attempts on files and registry

Use this report to:

- Identify requests for object access which have been authorized
- Determine which users are accessing sensitive information.

NOTE: File auditing should be enabled on the required files and registry values of interest.

Object deleted

Computer	User	Event ID	Description	Object Name	Object Type	Time	Date
TESTSTATION	TESTSTATION\Administrator	564	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
TESTSTATION	TESTSTATION\Administrator	564	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
TESTSTATION	TESTSTATION\Administrator	564	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
TESTSTATION	TESTSTATION\Administrator	564	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	2:32:16PM	6/27/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	2:34:06PM	6/27/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	2:43:32PM	6/27/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	2:45:01PM	6/27/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:05PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:06PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:06PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:06PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:06PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:06PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
FSERVER	GFITEMASOFT\calin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006

Screenshot 67 - Sample report showing Objects deleted

1	List of events showing attempted and successful object deletions

Use this report to:

- Identify users deleting objects
- Investigate attempts to identify possible attacks on resources
- Identify successful delete operations that do not conform to corporate security policy.

Application Management Reports

Applications installed/removed

Applications successfully installed

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	(1): Product: My Application-- Installation operation completed successfully.	11707	MsiInstaller	12:52:12PM	9/11/2006
CALDEV	N/A	(1): Product: My Application2 -- Installation operation completed successfully.	11707	MsiInstaller	12:52:31PM	9/11/2006
CALDEV	N/A	(2): Product: My Application2 -- Installation operation completed successfully.	11707	MsiInstaller	12:52:31PM	9/11/2006
CALDEV	N/A	(3): Product: My Application2 -- Installation operation completed successfully.	11707	MsiInstaller	12:52:31PM	9/11/2006

Applications successfully uninstalled

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	(1): Product MyApp4 -- Removal completed successfully.	11724	MsiInstaller	12:53:37PM	9/11/2006
CALDEV	N/A	(2): Product MyApp4 -- Removal completed successfully.	11724	MsiInstaller	12:53:37PM	9/11/2006
CALDEV	N/A	(3): Product MyApp4 -- Removal completed successfully.	11724	MsiInstaller	12:53:37PM	9/11/2006
CALDEV	N/A	(4): Product MyApp4 -- Removal completed successfully.	11724	MsiInstaller	12:53:37PM	9/11/2006
CALDEV	N/A	(5): Product MyApp4 -- Removal completed successfully.	11724	MsiInstaller	12:53:37PM	9/11/2006

Applications which failed to install

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	(1): MyApp2 -- Installation operation failed.	11708	MsiInstaller	12:53:11PM	9/11/2006
CALDEV	N/A	(2): MyApp2 -- Installation operation failed.	11708	MsiInstaller	12:53:11PM	9/11/2006
CALDEV	N/A	(3): MyApp2 -- Installation operation failed.	11708	MsiInstaller	12:53:11PM	9/11/2006
CALDEV	N/A	(4): MyApp2 -- Installation operation failed.	11708	MsiInstaller	12:53:11PM	9/11/2006
CALDEV	N/A	(5): MyApp2 -- Installation operation failed.	11708	MsiInstaller	12:53:11PM	9/11/2006

Applications which failed to uninstall

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	(1): My App6 -- uninstall failed.	11725	MsiInstaller	12:54:13PM	9/11/2006
CALDEV	N/A	(2): My App6 -- uninstall failed.	11725	MsiInstaller	12:54:13PM	9/11/2006
CALDEV	N/A	(3): My App6 -- uninstall failed.	11725	MsiInstaller	12:54:13PM	9/11/2006
CALDEV	N/A	(4): My App6 -- uninstall failed.	11725	MsiInstaller	12:54:13PM	9/11/2006
CALDEV	N/A	(5): My App6 -- uninstall failed.	11725	MsiInstaller	12:54:13PM	9/11/2006

Screenshot 68 - Sample report showing Applications installed /removed

1	List of events showing applications which have been successfully installed
2	List of events showing applications which have been successfully uninstalled
3	List of events showing failed attempts to install applications
4	List of events showing failed attempts to uninstall applications

Use this report to:

- Identify applications which have been successfully installed or uninstalled
- Identify failed attempts to install or uninstall applications
- Identify installed applications that do not conform to corporate security policy
- Identify removals of applications that have not been authorized
- Investigate whether failures to install or uninstall applications were attempts to:
    - use unapproved applications
    - deploy rogue or malicious programs on the company network.

Applications crashing or hanging

Applications which crashed

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	Faulting application (1): My App, version(1): My App, faulting module(1): My App, version(1): My	1000	Application Error	12:55:46PM	9/11/2006
CALDEV	N/A	Faulting application (2): My App, version(2): My App, faulting module(2): My App, version(2): My	1000	Application Error	12:55:46PM	9/11/2006
CALDEV	N/A	Faulting application (3): My App, version(3): My App, faulting module(3): My App, version(3): My	1000	Application Error	12:55:46PM	9/11/2006
CALDEV	N/A	Faulting application (4): My App, version(4): My App, faulting module(4): My App, version(4): My	1000	Application Error	12:55:46PM	9/11/2006
CALDEV	N/A	Faulting application (5): My App, version(5): My App, faulting module(5): My App, version(5): My	1000	Application Error	12:55:46PM	9/11/2006

Applications which hanged

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	Hanging application (1): My App, version(1): My App, hang module(1): My App, version(1): My App,	1002	Application Hang	12:56:09PM	9/11/2006
CALDEV	N/A	Hanging application (2): My App, version(2): My App, hang module(2): My App, version(2): My App,	1002	Application Hang	12:56:09PM	9/11/2006
CALDEV	N/A	Hanging application (3): My App, version(3): My App, hang module(3): My App, version(3): My App,	1002	Application Hang	12:56:09PM	9/11/2006
CALDEV	N/A	Hanging application (4): My App, version(4): My App, hang module(4): My App, version(4): My App,	1002	Application Hang	12:56:09PM	9/11/2006
CALDEV	N/A	Hanging application (5): My App, version(5): My App, hang module(5): My App, version(5): My App,	1002	Application Hang	12:56:09PM	9/11/2006

DrWatson events

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	The application,(1): My App, generated an application error	4097	DrWatson	12:56:21PM	9/11/2006
CALDEV	N/A	The application,(2): My App, generated an application error	4097	DrWatson	12:56:21PM	9/11/2006
CALDEV	N/A	The application,(3): My App, generated an application error	4097	DrWatson	12:56:21PM	9/11/2006
CALDEV	N/A	The application,(4): My App, generated an application error	4097	DrWatson	12:56:21PM	9/11/2006
CALDEV	N/A	The application,(5): My App, generated an application error	4097	DrWatson	12:56:21PM	9/11/2006

Screenshot 69 - Sample report showing Applications crashing or hanging

1	List of events showing applications which have crashed
2	List of events showing applications which hanged
3	List of events generated by 'DrWatson'

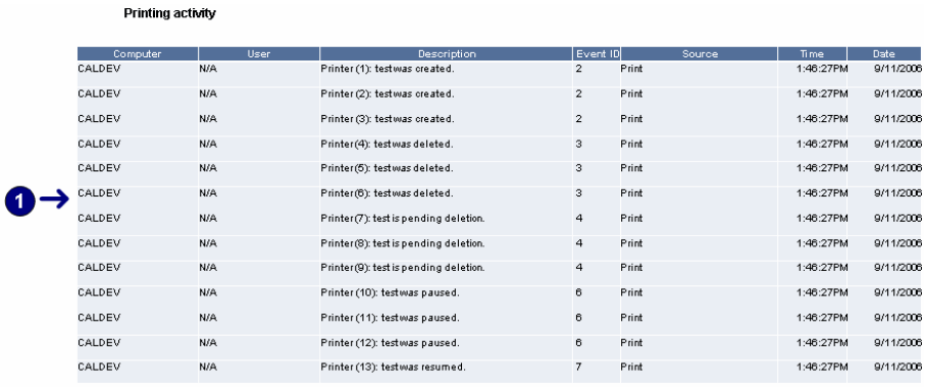
Use this report to:

- Identify all faulty applications, including critical applications

- Investigate whether the events are a result of attacks which have managed to disable or affect the functionality of the target computers.

Print Server Reports

Print activities



Printing activity

Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	Printer (1): testwas created.	2	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (2): testwas created.	2	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (3): testwas created.	2	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (4): testwas deleted.	3	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (5): testwas deleted.	3	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (6): testwas deleted.	3	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (7): test is pending deletion.	4	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (8): test is pending deletion.	4	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (9): test is pending deletion.	4	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (10): testwas paused.	6	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (11): testwas paused.	6	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (12): testwas paused.	6	Print	1:46:27PM	9/11/2006
CALDEV	N/A	Printer (13): testwas resumed.	7	Print	1:46:27PM	9/11/2006

Screenshot 70 - Sample report showing Print activities

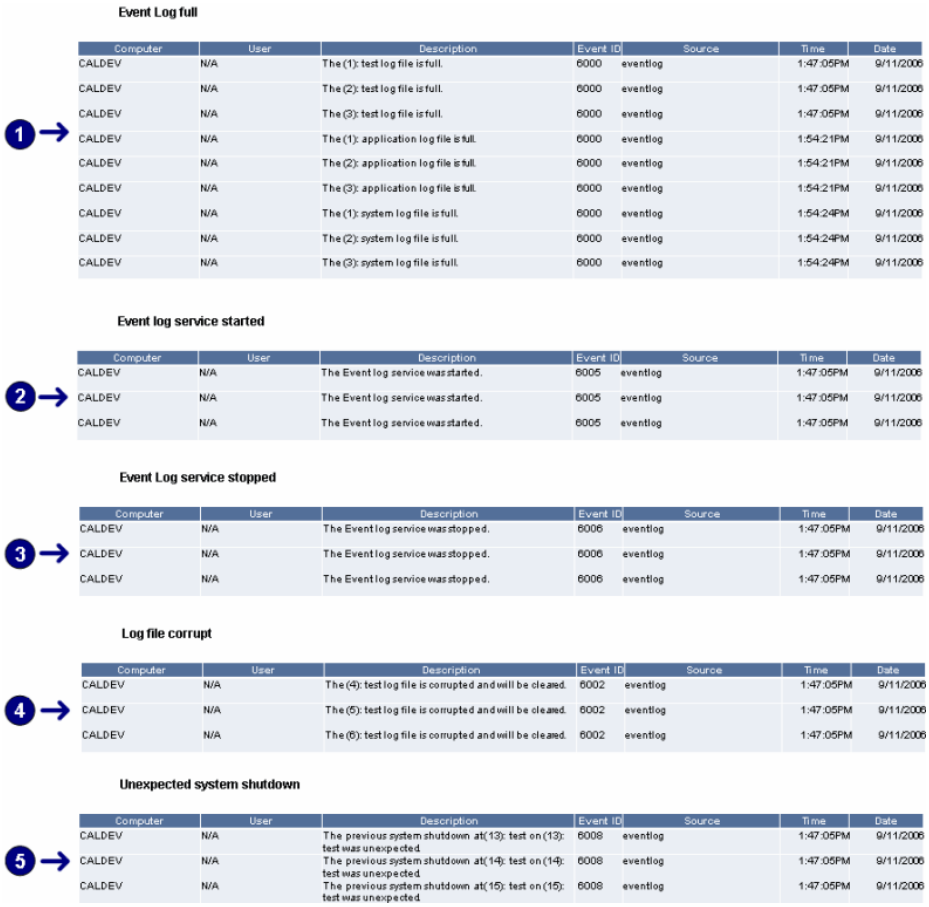
1	List of events showing printing activity

Use this report to:

- Identify all the documents printed over the network
- Identify which users have been using printing resources
- List file details of the printed files and the date and time when the print operation took place.

Windows Event Log System Reports

Event Log health



Screenshot 71 - Sample report showing Event Log health

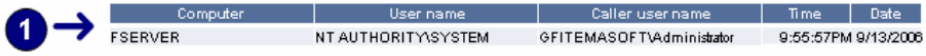
1	List of events generated when the event log is full
2	List of events generated when the event log service is started
3	List of events generated when the event log service is stopped
4	List of events generated when the log file is corrupt
5	List of events generated on unexpected system shutdown

Use this report to:

- Identify failures in the auditing process

NOTE: Failures in the auditing process may be exploited by attackers and usually lead to loss of audit entries.

Event Log cleared



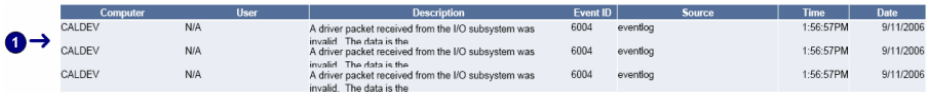
Screenshot 72 - Sample report showing Event Log cleared

1	List of events generated when the event log is cleared

Use this report to:

- Identify which users cleared the security event log without being authorized to do so
- Identify clearing events that do not conform to corporate security policy.

Event Log service errors



Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	A driver packet received from the I/O subsystem was invalid. The data is the	6004	eventlog	1:56:57PM	9/11/2006
CALDEV	N/A	A driver packet received from the I/O subsystem was invalid. The data is the	6004	eventlog	1:56:57PM	9/11/2006
CALDEV	N/A	A driver packet received from the I/O subsystem was invalid. The data is the	6004	eventlog	1:56:57PM	9/11/2006

Screenshot 73 - Sample showing Event Log service errors

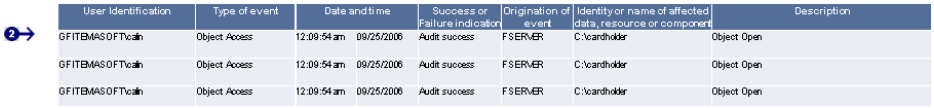
1	List of events showing event log service errors.

Use this report to:

- Identify errors occurring in the auditing process.

Network Resouce Access Reports (PCI requirement 10)

All individual access to cardholder data



User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
GFITEMASOFT\calin	Object Access	12:09:54 am	09/25/2006	Audit success	FSERVER	C:\cardholder	Object Open
GFITEMASOFT\calin	Object Access	12:09:54 am	09/25/2006	Audit success	FSERVER	C:\cardholder	Object Open
GFITEMASOFT\calin	Object Access	12:09:54 am	09/25/2006	Audit success	FSERVER	C:\cardholder	Object Open

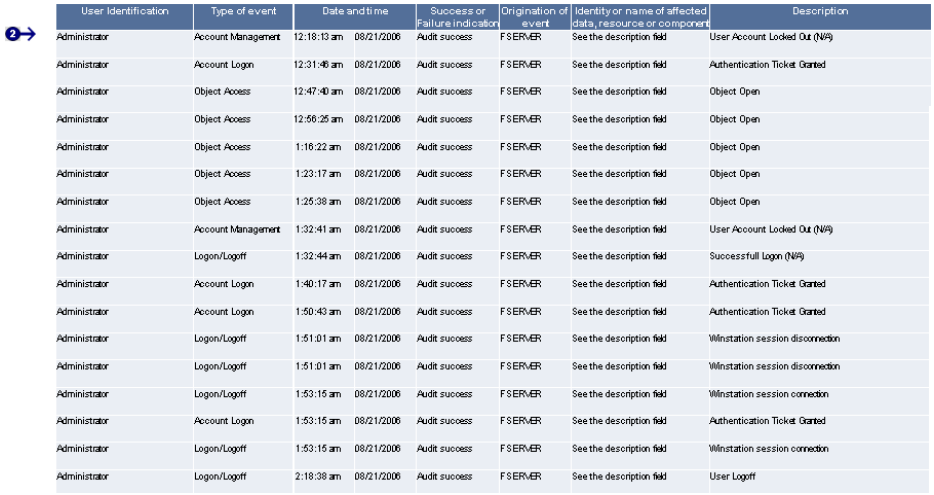
Screenshot 74 - Sample report showing all individual access to cardholder data

2	List of users who accessed cardholder data

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – 'Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data' for Windows-based systems presented in the format required by point 10.2.3 of of the PCI Data Security Standards document version 1.1.

All actions taken by any individual with root or administrative privileges



User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
Administrator	Account Management	12:18:13 am	08/21/2006	Audit success	FSERVER	See the description field	User Account Locked Out (N/A)
Administrator	Account Logon	12:31:46 am	08/21/2006	Audit success	FSERVER	See the description field	Authentication Ticket Granted
Administrator	Object Access	12:47:40 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
Administrator	Object Access	12:56:25 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
Administrator	Object Access	1:16:22 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
Administrator	Object Access	1:23:17 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
Administrator	Object Access	1:25:38 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
Administrator	Account Management	1:32:41 am	08/21/2006	Audit success	FSERVER	See the description field	User Account Locked Out (N/A)
Administrator	Logon/Logoff	1:32:44 am	08/21/2006	Audit success	FSERVER	See the description field	Successfull Logon (N/A)
Administrator	Account Logon	1:40:17 am	08/21/2006	Audit success	FSERVER	See the description field	Authentication Ticket Granted
Administrator	Account Logon	1:50:43 am	08/21/2006	Audit success	FSERVER	See the description field	Authentication Ticket Granted
Administrator	Logon/Logoff	1:51:01 am	08/21/2006	Audit success	FSERVER	See the description field	Winstation session disconnection
Administrator	Logon/Logoff	1:51:01 am	08/21/2006	Audit success	FSERVER	See the description field	Winstation session disconnection
Administrator	Logon/Logoff	1:53:15 am	08/21/2006	Audit success	FSERVER	See the description field	Winstation session connection
Administrator	Account Logon	1:53:15 am	08/21/2006	Audit success	FSERVER	See the description field	Authentication Ticket Granted
Administrator	Logon/Logoff	1:53:15 am	08/21/2006	Audit success	FSERVER	See the description field	Winstation session connection
Administrator	Logon/Logoff	2:18:38 am	08/21/2006	Audit success	FSERVER	See the description field	User Logoff

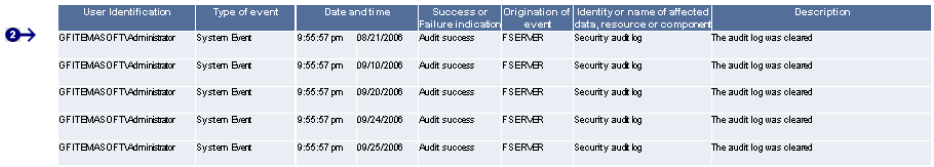
Screenshot 75 - Sample report showing all actions taken by any individual with root or administrative priveleges

2	List of actions taken by users with root or administrative privileges

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – 'Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges' for Windows-based systems presented in the format required by point 10.2.3 of of the PCI Data Security Standards document version 1.1.

Access to all audit trails



User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
GFITEMASOFT\Administrator	System Event	9:55:57 pm	08/21/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/10/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/20/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/24/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/25/2006	Audit success	FSERVER	Security audit log	The audit log was cleared

Screenshot 76 - Sample report showing access to all audit trails

2	List of audit trails

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – 'Implement automated audit trails for all system components to reconstruct the following events: Access to all audit trails' for Windows-based systems presented in the format required by point 10.2.3 of the PCI Data Security Standards document version 1.1.

Invalid logical access attempts

❶→ **Account lockouts**

❷→

User Identification	Type of event	Date and time	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
GFITEMASOFT\FSERVER$	Account Management	12:18:13 am 08/21/2006	Audit success	CRISTI	FSERVER$	User Account Locked Out (Administrator)
GFITEMASOFT\FSERVER$	Account Management	1:32:41 am 08/21/2006	Audit success	FSERVER	FSERVER$	User Account Locked Out (Administrator)
GFITEMASOFT\FSERVER$	Account Management	2:26:04 pm 08/21/2006	Audit success	CALDEV	FSERVER$	User Account Locked Out (pisu)
GFITEMASOFT\FSERVER$	Account Management	7:54:55 pm 08/21/2006	Audit success	FSERVER	FSERVER$	User Account Locked Out (Administrator)
GFITEMASOFT\FSERVER$	Account Management	12:18:13 am 09/10/2006	Audit success	CRISTI	FSERVER$	User Account Locked Out (Administrator)
GFITEMASOFT\FSERVER$	Account Management	1:32:41 am 09/10/2006	Audit success	FSERVER	FSERVER$	User Account Locked Out (Administrator)
GFITEMASOFT\FSERVER$	Account Management	2:26:04 pm 09/10/2006	Audit success	CALDEV	FSERVER$	User Account Locked Out (pisu)
GFITEMASOFT\FSERVER$	Account Management	7:54:55 pm 09/10/2006	Audit success	FSERVER	FSERVER$	User Account Locked Out (Administrator)

Failed logons from reasons other than bad user name or password

User Identification	Type of event	Date and time	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
CALDEV\test	Logon/Logoff	12:33:02 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEV\test	Logon/Logoff	12:33:02 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEV\test	Logon/Logoff	12:33:02 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEV\test	Logon/Logoff	12:33:02 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEV\test	Logon/Logoff	12:33:02 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEV\test	Logon/Logoff	12:34:34 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEV\test	Logon/Logoff	12:34:34 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEV\test	Logon/Logoff	12:34:34 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEV\test	Logon/Logoff	12:34:34 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEV\test	Logon/Logoff	12:34:34 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)

Screenshot 77 - Sample report showing invalid logical access attempts

2	List of invalid logical access attempts

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – ‘Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts’ for Windows-based systems presented in the format required by point 10.2.3 of the PCI Data Security Standards document version 1.1.

Use of identification and authentication mechanisms

❶→ **Failed logons because of bad user name and password**

❷→

User Identification	Type of event	Date and time	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
CALDEV\dsdffsdf	Logon/Logoff	12:27:53 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (dsdffsdf)
CALDEV\dsdffsdf	Logon/Logoff	12:27:53 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (dsdffsdf)
CALDEV\dsdffsdf	Logon/Logoff	12:27:53 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (dsdffsdf)
CALDEV\dsdffsdf	Logon/Logoff	12:27:53 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (dsdffsdf)
CALDEV\dsdffsdf	Logon/Logoff	12:27:53 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (dsdffsdf)
CALDEV\test	Logon/Logoff	12:28:09 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)
CALDEV\test	Logon/Logoff	12:28:09 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)
CALDEV\test	Logon/Logoff	12:28:09 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)
CALDEV\test	Logon/Logoff	12:28:09 pm 09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)

IPSec security events

User Identification	Type of event	Date and time	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm 09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service

Screenshot 78 - Sample report showing identification and authentication mechanisms

2	List of identification and authentication mechanisms

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – 'Implement automated audit trails for all system components to reconstruct the following events: Use of identification and authentication mechanisms' for Windows-based systems presented in the format required by point 10.2.3 of the PCI Data Security Standards document version 1.1.

Initialization of the audit logs

User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
N/A	None	1:22:18 pm	05/15/2007	Warning	COMP-ALINA	Audit Log	The (1): ev.evt log file is full.
N/A	None	1:22:18 pm	05/15/2007	Warning	COMP-ALINA	Audit Log	The (1): ev.evt log file is full.

Event Log service started

User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
N/A	None	12:18:14 pm	05/15/2007	Information	COMP-ALINA	Event Log	The Event log service was started.
N/A	None	12:18:14 pm	05/15/2007	Information	COMP-ALINA	Event Log	The Event log service was started.
N/A	None	1:22:18 pm	05/15/2007	Warning	COMP-ALINA	eventlog	The Event log service was started.
N/A	None	1:22:18 pm	05/15/2007	Warning	COMP-ALINA	eventlog	The Event log service was started.
N/A	None	9:02:53 am	05/16/2007	Information	COMP-ALINA	Event Log	The Event log service was started.

Screenshot 79 - Sample report showing initialization of audit logs

2	List showing initialization of audit logs

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – 'Implement automated audit trails for all system components to reconstruct the following events: Initialization of audit logs' for Windows-based systems presented in the format required by point 10.2.3 of the PCI Data Security Standards document version 1.1.

Creation and deletion of system-level objects

User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
\VIRTUALDOM1\W2003DC1$	Directory Service Access	4:31:10 pm	04/17/2007	Audit success	\V2003DC1	%{fae49748-6aa4-43b5-aff2-274ea3e5a019%}	Object Operation
\VIRTUALDOM1\W2003DC1$	Directory Service Access	10:45:21 am	04/26/2007	Audit success	\V2003DC1	DC=VirtualDom1,DC=ts	Object Open
\VIRTUALDOM1\W2003DC1$	Directory Service Access	11:22:30 am	04/26/2007	Audit success	\V2003DC1	%{fae49748-6aa4-43b5-aff2-274ea3e5a019%}	Object Operation
\VIRTUALDOM1\W2003DC1$	Directory Service Access	3:00:16 pm	05/15/2007	Audit success	\V2003DC1	DC=VirtualDom1,DC=ts	Object Open
COMP-ALINA\alina	Object Access	11:03:27 am	05/16/2007	Audit success	COMP-ALINA	Policy\Secrets\L$ASP.NET_Auto GenKeys\2.0.50727.210	Object Operation
COMP-ALINA\alina	Object Access	11:05:48 am	05/16/2007	Audit success	COMP-ALINA	Policy\Secrets\L$ASP.NET_Auto GenKeys\2.0.50727.210	Object Operation

Windows File Protection Service - attempt to replace protected file

User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
N/A	None	4:11:41 pm	05/15/2007	Information	COMP-ALINA	(1): ev.evt	File replacement was attempted on the protected system file (1): ev.evt. This file was restored to the original version to maintain system stability.
N/A	None	4:11:41 pm	05/15/2007	Information	COMP-ALINA	(2): ev.evt	File replacement was attempted on the protected system file (2): ev.evt. This file was restored to the original version to maintain system stability.
N/A	None	4:11:41 pm	05/15/2007	Information	COMP-ALINA	(3): ev.evt	File replacement was attempted on the protected system file (3): ev.evt. This file was restored to the original version to maintain system stability.
N/A	None	4:11:41 pm	05/15/2007	Information	COMP-ALINA	(4): ev.evt	File replacement was attempted on the protected system file (4): ev.evt. This file was restored to the original version to maintain system stability.

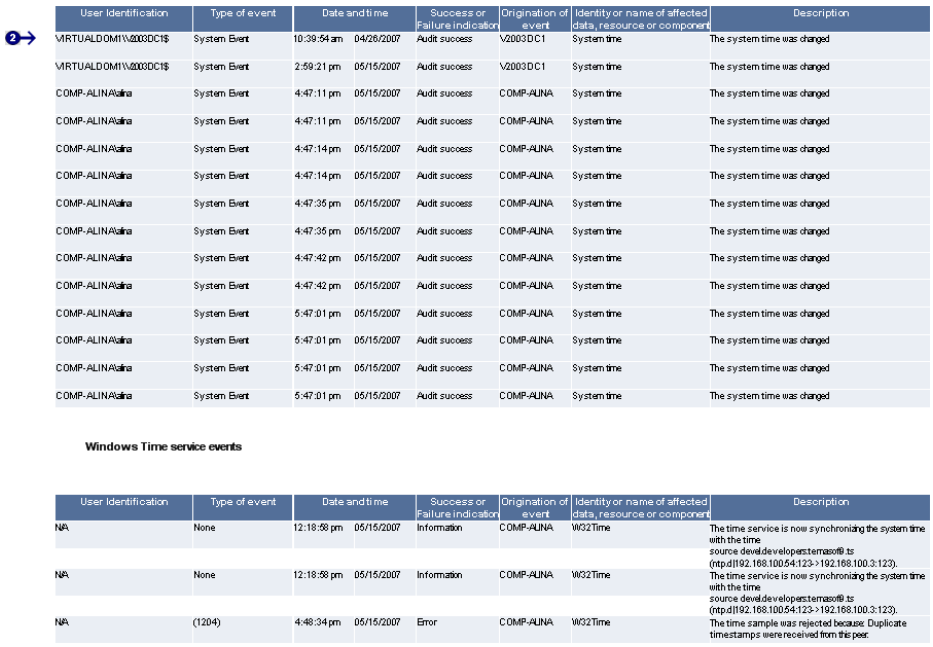
Screenshot 80 - Sample report showing creation and deletion of system-level objects

2	List showing creation and deletion of system-level objects

Use this report to:

- Display the data which forms the scope of PCI requirement 10.2 – 'Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects' for Windows-based systems presented in the format required by point 10.2.3 of the PCI Data Security Standards document version 1.1.

Time synchronization monitoring



User Identification	Type of event	Date and time	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
\VIRTUALDOM1\W2003DC1$	System Event	10:39:54 am 04/26/2007	Audit success	W2003DC1	System time	The system time was changed
\VIRTUALDOM1\W2003DC1$	System Event	2:59:21 pm 05/15/2007	Audit success	W2003DC1	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:11 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:11 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:14 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:14 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:36 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:36 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:42 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	4:47:42 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	5:47:01 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	5:47:01 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	5:47:01 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed
COMP-ALINA\alina	System Event	5:47:01 pm 05/15/2007	Audit success	COMP-ALINA	System time	The system time was changed

Windows Time service events

User Identification	Type of event	Date and time	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
N/A	None	12:18:58 pm 05/15/2007	Information	COMP-ALINA	W32Time	The time service is now synchronizing the system time with the time source devel.developerstemasoft®.ts (ntp.d|192.168.100.54:123->192.168.100.3:123).
N/A	None	12:18:58 pm 05/15/2007	Information	COMP-ALINA	W32Time	The time service is now synchronizing the system time with the time source devel.developerstemasoft®.ts (ntp.d|192.168.100.54:123->192.168.100.3:123).
N/A	(1204)	4:48:34 pm 05/15/2007	Error	COMP-ALINA	W32Time	The time sample was rejected because: Duplicate timestamps were received from this peer.

Screenshot 81 - Sample report showing time synchronization monitoring

2	List showing time synchronization monitoring

Use this report to:

- Monitor system time changes
- Monitor the time synchronization process

Events Trend Reports

Use the reports in this category to:

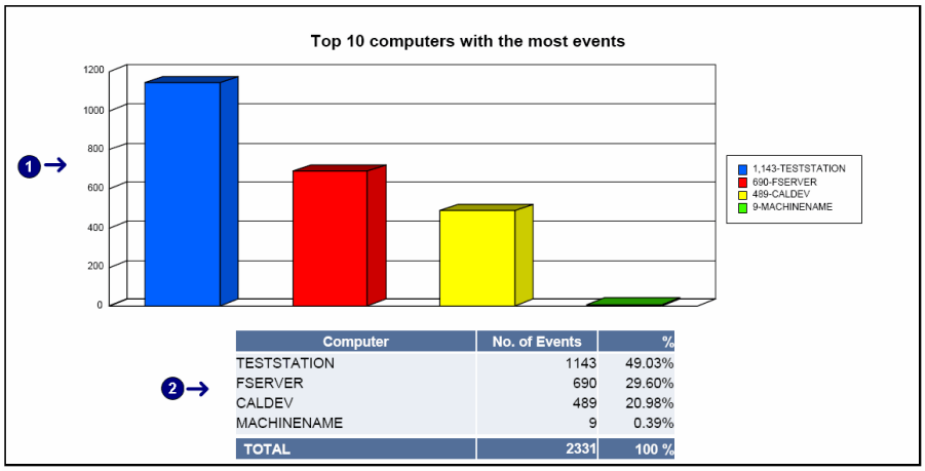
- Identify the top 10 computers, those with the highest number of events
- Identify the top 10 users, those having generated the highest number of events
- Determine the events trend on all computers
- Determine the events trend on a computer by computer basis.

The reports in this category are based on events from the following sources:

- Security log
- Application log
- System log
- DNS Server log

- Directory Services log
- File Replication Service log.

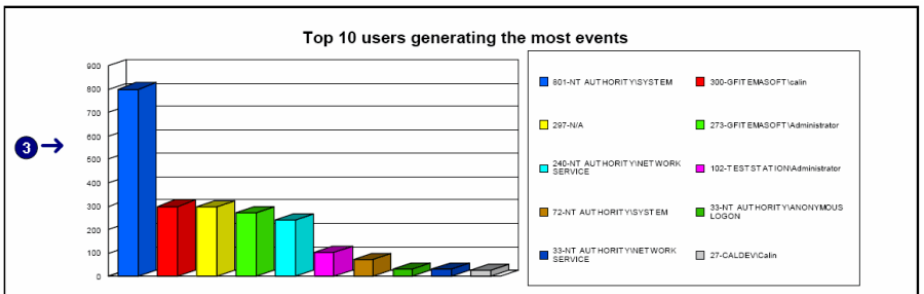
NOTE: The layout shown in the sample extracts below is common to all reports in the **Events Trend Reports** category. Sections which are specific to individual reports within this category are shown further down.



Computer	No. of Events	%
TESTSTATION	1143	49.03%
FSERVER	690	29.60%
CALDEV	489	20.98%
MACHINENAME	9	0.39%
TOTAL	2331	100 %

Screenshot 82 - Sample extract from Events Trend Reports: Top 10 computers with most events

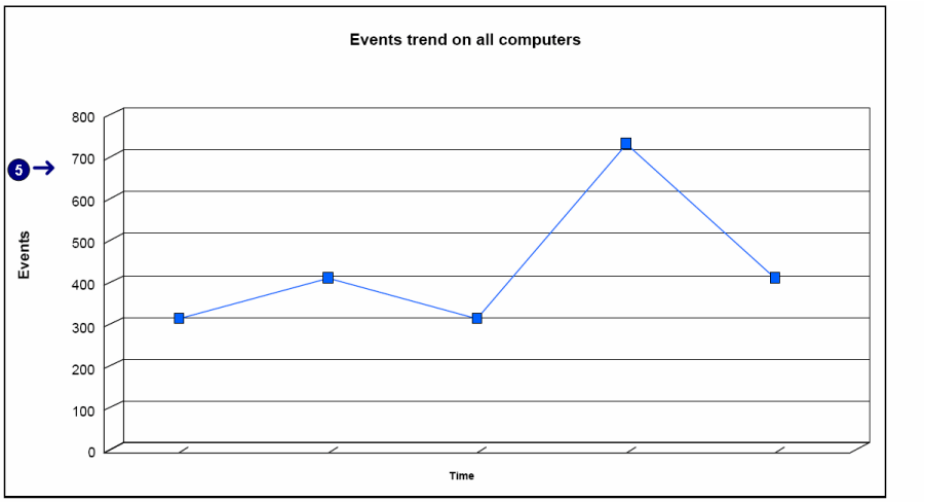
1	Chart showing the top 10 computers with most events
2	Table displaying statistical information on the top 10 computers with most events



Computer	User name	No. of Events	%
TESTSTATION	NT AUTHORITY\SYSTEM	801	36.78%
FSERVER	GFITEMASOFT\calin	300	13.77%
CALDEV	N/A	297	13.64%
FSERVER	GFITEMASOFT\Administrator	273	12.53%
TESTSTATION	NT AUTHORITY\NETWORK SERVICE	240	11.02%
TESTSTATION	TESTSTATION\Administrator	102	4.68%
FSERVER	NT AUTHORITY\SYSTEM	72	3.31%
FSERVER	NT AUTHORITY\ANONYMOUS LOGON	33	1.52%
CALDEV	NT AUTHORITY\NETWORK SERVICE	33	1.52%
CALDEV	CALDEV\Calin	27	1.24%
TOTAL		2178	100 %

Screenshot 83 - Sample extract from Events Trend Reports: Top 10 users with most events

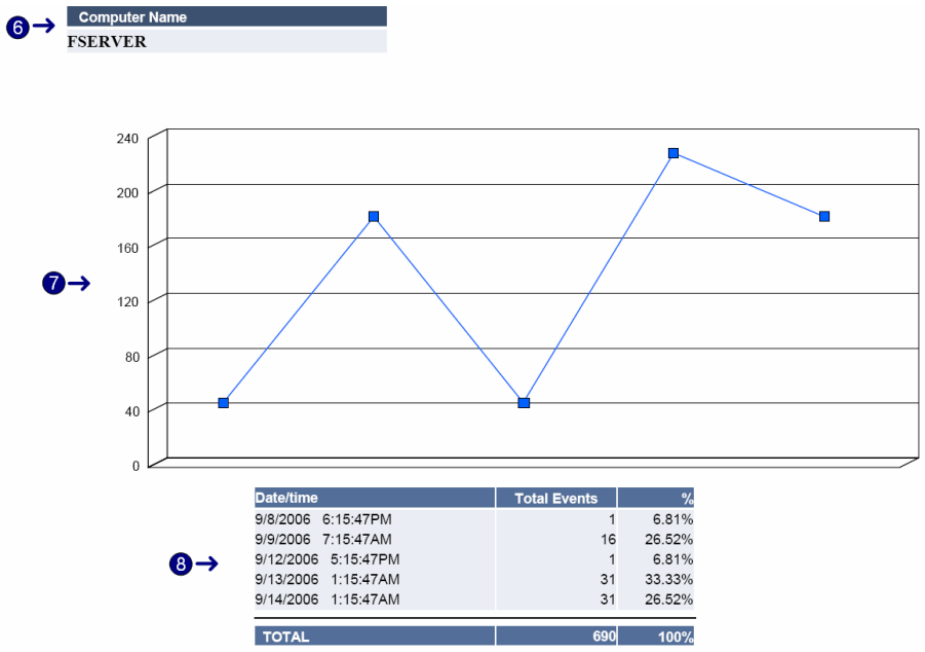
3	Chart showing the top 10 users generating the most events
4	Table displaying statistical information on the top 10 users generating the most events



Screenshot 84 - Sample extract from Events Trend Reports: Events trend on all computers

5	Chart displaying the events trend on all computers. The minimum time interval on this chart can be of one hour.

Generic events trend per hour



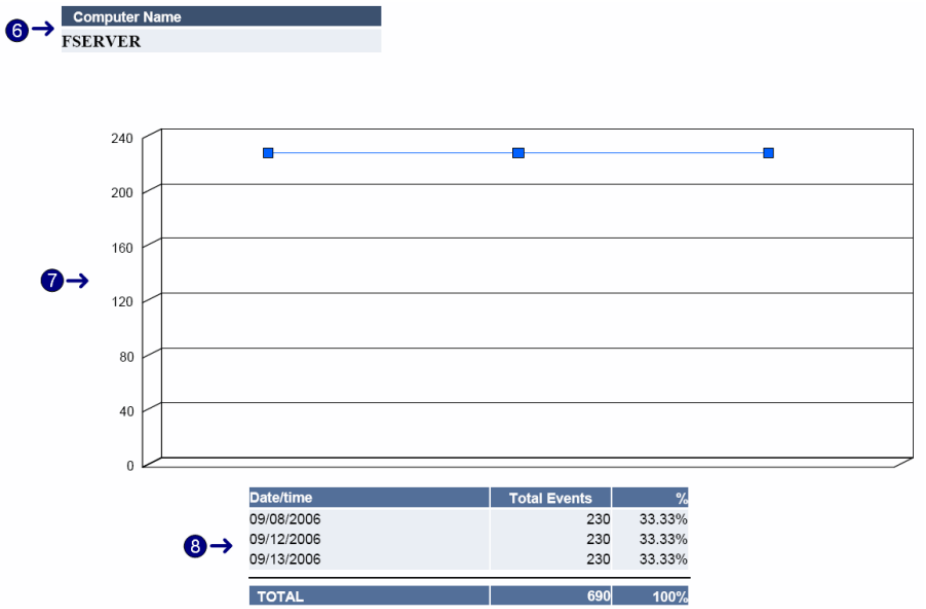
Screenshot 85 - Sample extract from Events Trend Reports: Generic events trend per hour

6	Computer name
7	Chart displaying the events trend for a computer on an hourly scale
8	Table of statistical information showing the events trend for a computer on an hourly basis

Use this report to:

- View trends on an hourly basis.

Generic events trend per days



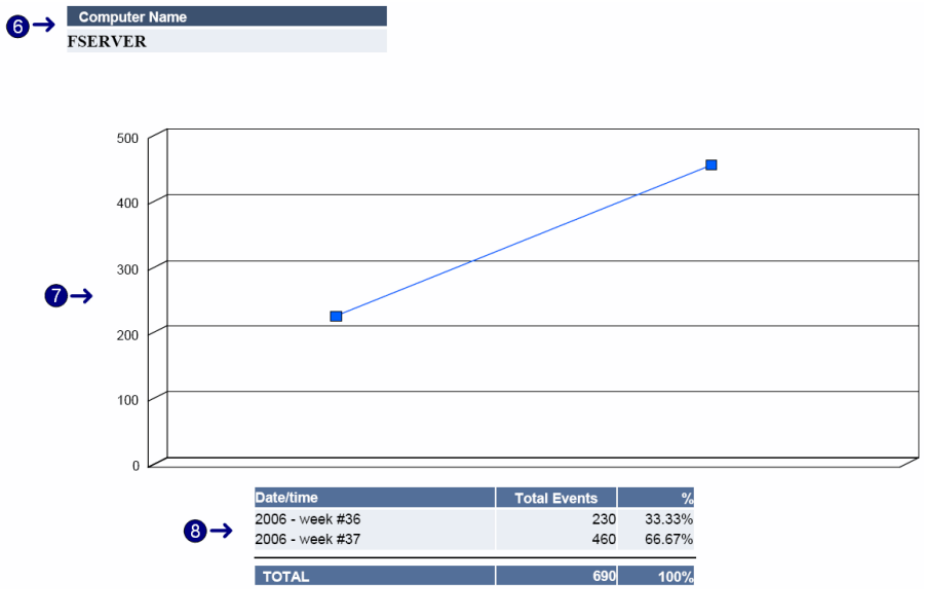
Screenshot 86 - Sample extract from Events Trend Reports: Generic events trend per day

6	Computer name
7	Chart displaying the events trend for a computer on a daily scale
8	Table of statistical information showing the events trend for a computer on a daily basis

Use this report to:

- View trends on an daily basis.

Generic events trend per week



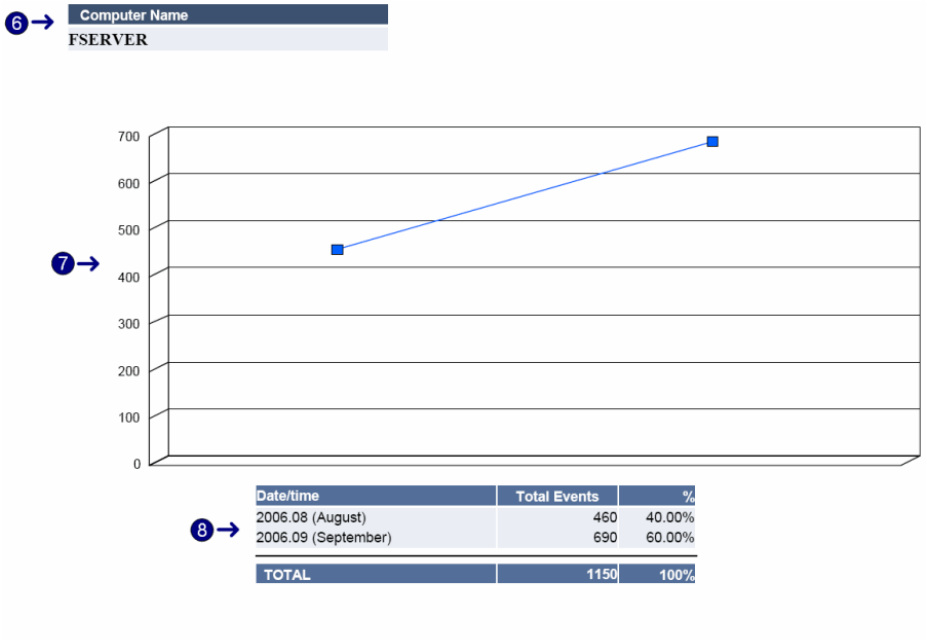
Screenshot 87 - Sample extract from Events Trend Reports: Generic events trend per week

6	Computer name
7	Chart displaying the events trend for a computer on a weekly scale
8	Table of statistical information showing the events trend for a computer on a weekly basis

Use this report to:

- View trends on an weekly basis.

Generic events trend per month



Screenshot 88 - Sample extract from Events Trend Reports: Generic events trend per month

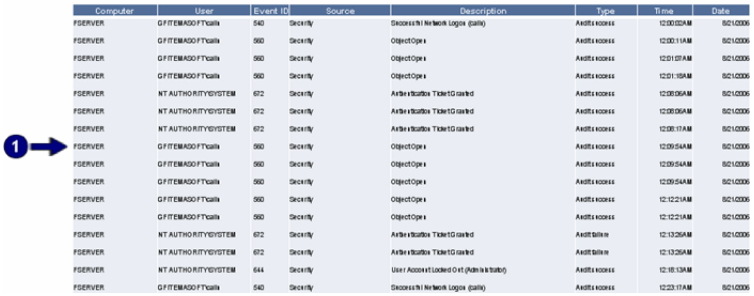
6	Computer name
7	Chart displaying the events trend for a computer on a monthly scale
8	Table of statistical information showing the events trend for a computer on a monthly basis

Use this report to:

- View trends on a monthly basis.

All critical messages reports

All critical windows log events



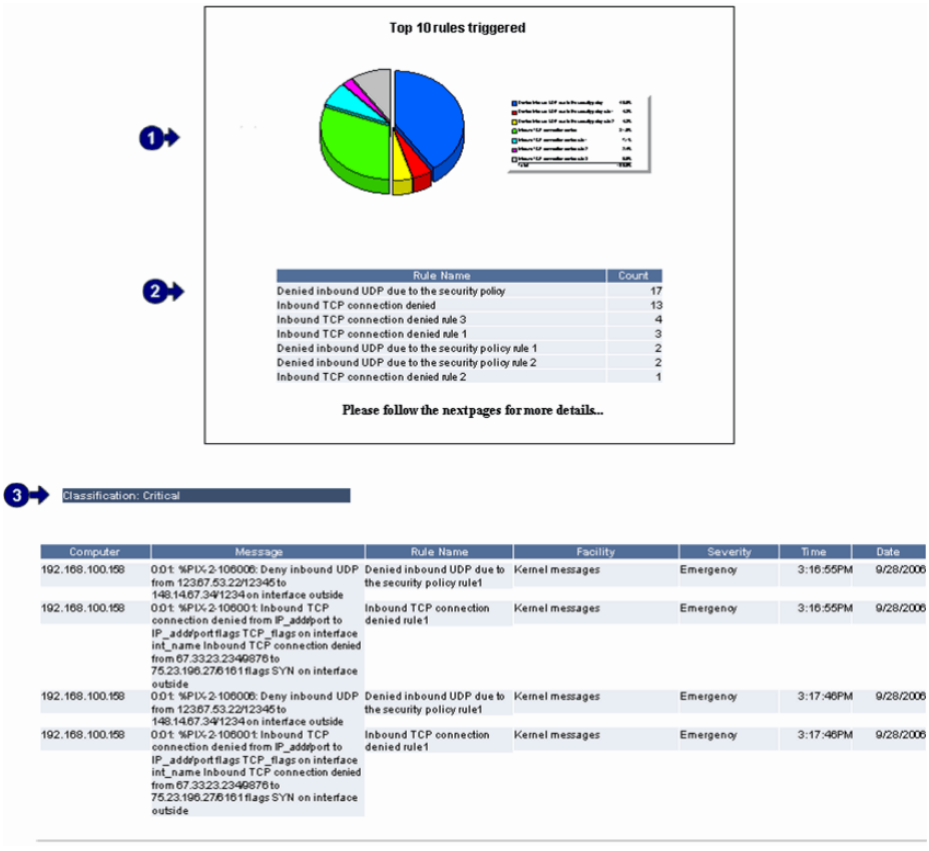
Screenshot 89 - All critical Windows log events

1	Top 10 rules that were triggered.
2	Top 10 triggered rules and the number of events that have activated each particular rule.
3	Events that correspond to the current filtering conditions.

Use this report to:

- View the most important events that require immediate attention.
- The top 10 rules that were triggered most frequently by these events.

All critical Syslog events



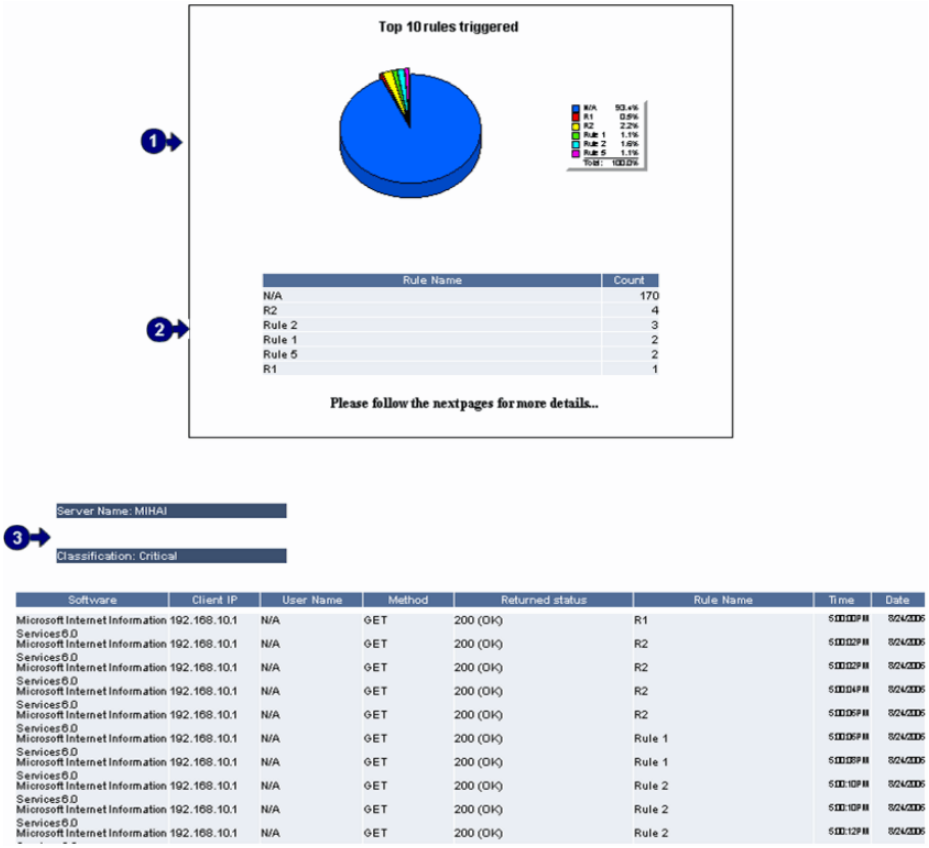
Screenshot 90 - All critical Syslog log events

1	Top 10 rules that were triggered.
2	Top 10 triggered rules and the number of events that have activated each particular rule.
3	Events that correspond to the current filtering conditions.

Use this report to:

- View the most Syslog important events that require immediate attention.
- The top 10 rules that were triggered most frequently by these Syslog events.

All critical W3C events



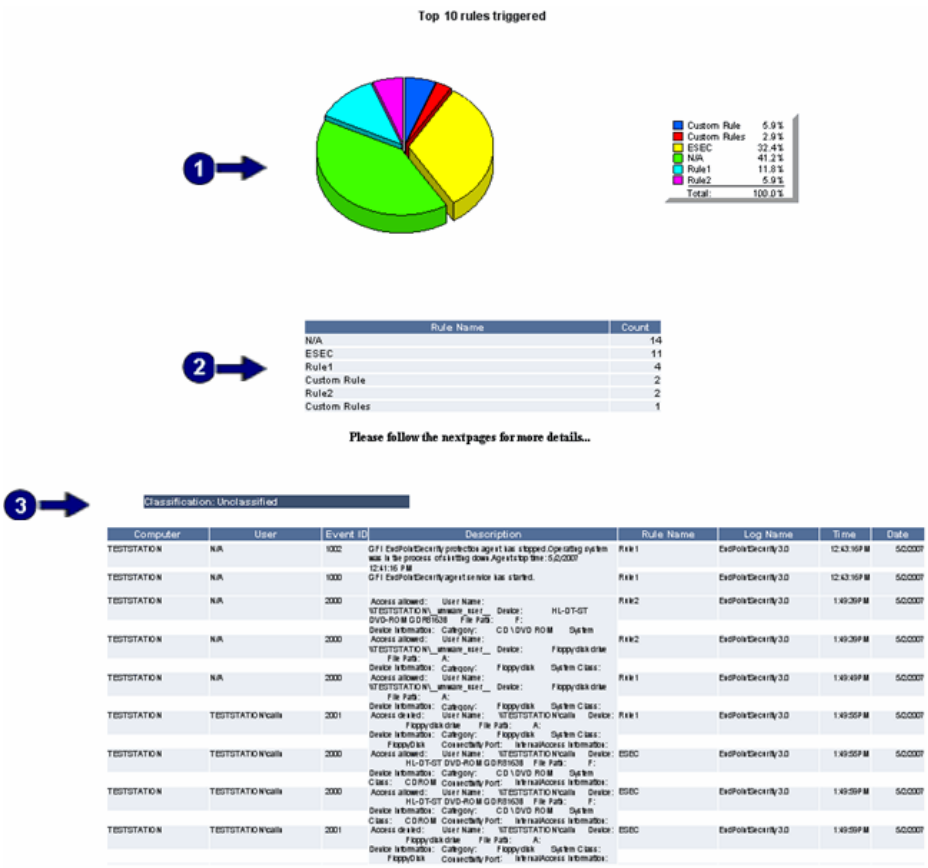
Screenshot 91 - All critical W3C log events

1	Top 10 rules that were triggered.
2	Top 10 triggered rules and the number of events that have activated each particular rule.
3	Events that correspond to the current filtering conditions.

Use this report to:

- View the most W3C important events that require immediate attention.
- The top 10 rules that were triggered most frequently by these W3C events.

All critical Custom log events



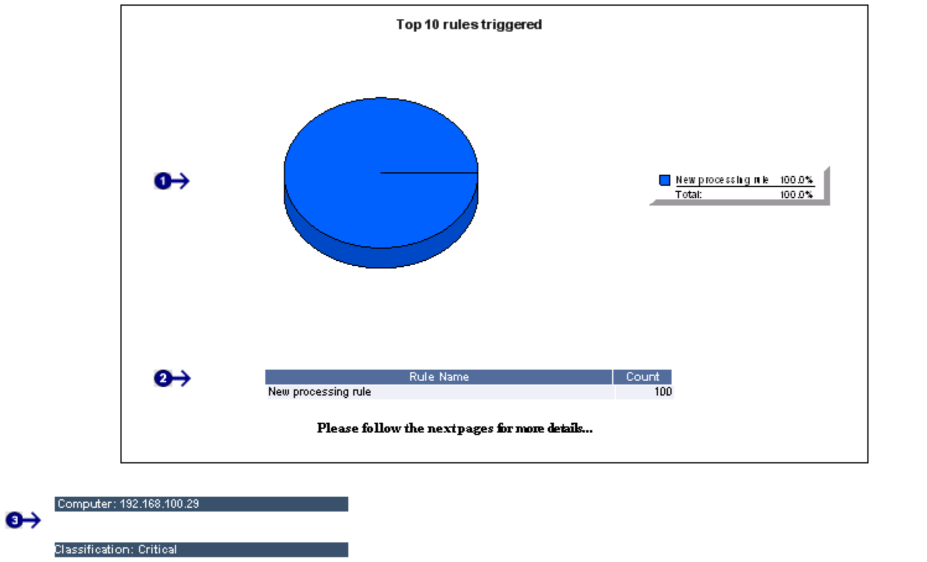
Screenshot 92 - All critical custom logs events

1	Top 10 rules that were triggered.
2	Top 10 triggered rules and the number of events that have activated each particular rule.
3	Events that correspond to the current filtering conditions.

Use this report to:

- View the most important custom log events that require immediate attention.
- The top 10 rules that were triggered most frequently by these custom log events.

All critical SNMP Traps Messages



Trap Data	Trap OID	Community String	SNMP Version	Rule Name	Time	Date
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/2007
N/A	43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/2007

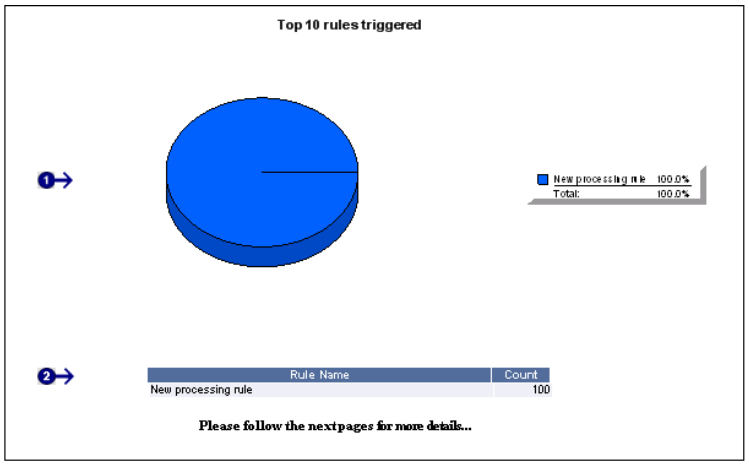
Screenshot 93 - All critical SNMP Traps Messages

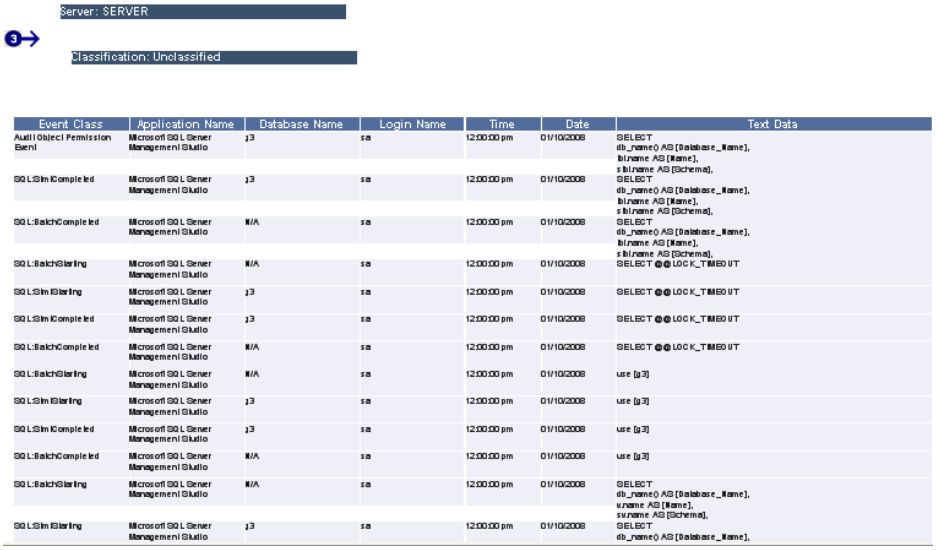
1	Top 10 rules that were triggered.
2	Top 10 triggered rules and the number of events that have activated each particular rule.
3	Events that correspond to the current filtering conditions.

Use this report to:

- View the most important SNMP Trap events that require immediate attention.
- The top 10 rules that were triggered most frequently by SNMP Trap events.

All critical SQL Server Audit





Screenshot 94 - All critical SQL Server Audit

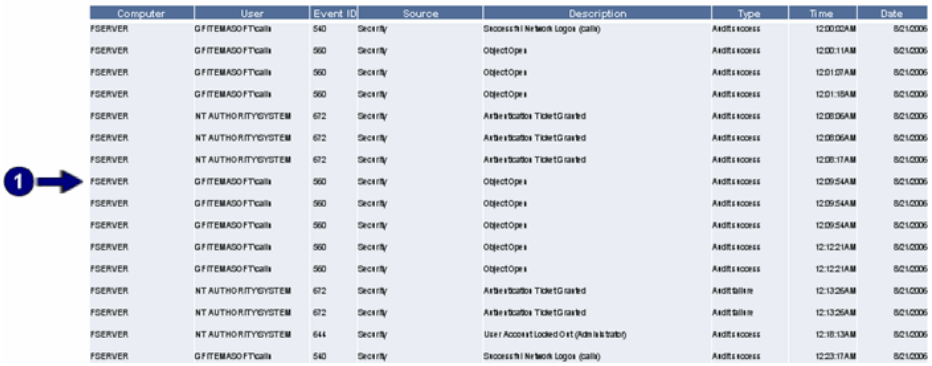
1	Top 10 rules that were triggered.
2	Top 10 triggered rules and the number of events that have activated each particular rule.
3	Events that correspond to the current filtering conditions.

Use this report to:

- View the most important SQL Server Audit events that require immediate attention.
- The top 10 rules that were triggered most frequently by SQL Server Audit events.

Miscellaneous, Customizable reports

Generic Windows Event log report



Computer	User	Event ID	Source	Description	Type	Time	Date
FSERVER	GFITEMASOFT\calls	540	Security	Successful Network Logon (calls)	Audit success	12:00:00AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:00:11AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:01:07AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:01:16AM	8/21/2006
FSERVER	NT AUTHORITY\SYSTEM	672	Security	Authentication Ticket Granted	Audit success	12:08:06AM	8/21/2006
FSERVER	NT AUTHORITY\SYSTEM	672	Security	Authentication Ticket Granted	Audit success	12:08:06AM	8/21/2006
FSERVER	NT AUTHORITY\SYSTEM	672	Security	Authentication Ticket Granted	Audit success	12:08:17AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:09:54AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:09:54AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:09:54AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:12:21AM	8/21/2006
FSERVER	GFITEMASOFT\calls	560	Security	Object Open	Audit success	12:12:21AM	8/21/2006
FSERVER	NT AUTHORITY\SYSTEM	672	Security	Authentication Ticket Granted	Audit failure	12:13:26AM	8/21/2006
FSERVER	NT AUTHORITY\SYSTEM	672	Security	Authentication Ticket Granted	Audit failure	12:13:26AM	8/21/2006
FSERVER	NT AUTHORITY\SYSTEM	644	Security	User Account Locked Out (Administrator)	Audit success	12:18:13AM	8/21/2006
FSERVER	GFITEMASOFT\calls	540	Security	Successful Network Logon (calls)	Audit success	12:23:17AM	8/21/2006

Screenshot 95 – Generic Windows Event log report

1	All Windows events that correspond to the current filtering condition

Use this report to:

- Generate event logs customized to your exact specifications
- Filter out Windows Events by criteria such as computer name, user, Event ID, rule name and more.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual – most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: http://www.gfi.com/pages/productmailing.htm.

Index

U

W