# Contents

## Introduction
- About GFI ReportCenter ................................................................. 5
- About the GFI EventsManager ReportPack ...................................... 6
- Components of the GFI EventsManager ReportPack ........................... 7
- Key features .................................................................................... 9

## Installation
- System requirements ........................................................................ 11
- Installation procedure ....................................................................... 11
- Launching the GFI EventsManager reports for GFI ReportCenter .......... 14
- Selecting a product ........................................................................... 14

## Getting started: Default reports
- Introduction ....................................................................................... 17
- Generating a default report .............................................................. 18
- Analyzing the generated report ....................................................... 20
- Adding default reports to the list of favorite reports ....................... 21

## Custom reports
- Introduction ....................................................................................... 23
- Creating a new custom report ......................................................... 23
- Configuring data filter conditions ................................................... 25
- Run a custom report ......................................................................... 30
- Editing a custom report ................................................................. 30
- Deleting a custom report ............................................................... 31
- Adding custom reports to the list of favorite reports ....................... 31

## Scheduling reports
- Introduction ....................................................................................... 33
- Scheduling a report ......................................................................... 33
- Configuring advanced settings ......................................................... 35
  - Configuring report export to file options ...................................... 36
  - Configuring report emailing options ........................................... 37
- Viewing the list of scheduled reports ............................................. 38
- Viewing the scheduled reports activity .......................................... 39
- Enable/disable a scheduled report ............................................... 40
- Editing a scheduled report ............................................................ 40
- Deleting a scheduled report .......................................................... 41
- Example: Scheduling a report ....................................................... 41

## Configuring default options
- Introduction ....................................................................................... 45
- Configuring database source ........................................................... 45
- Viewing the current database source settings .................................. 47
- Configuring default scheduling settings ........................................ 47
Appendix: GFI EventsManager Default Reports

Account Usage Reports ................................................................. 52
  Successful logons grouped by users ........................................... 52
  Successful logons grouped by computers .................................... 53
  Failed logons ........................................................................... 54
  Logoff events ........................................................................... 54
  Account Logons ......................................................................... 55
  Account lockouts ....................................................................... 56
  Successful logon count on each computer .................................... 56
Account Management Reports ..................................................... 57
  User account management .......................................................... 57
  Computer account management .................................................... 58
  Password changes ....................................................................... 59
  Security group management .......................................................... 60
Policy Changes Reports ............................................................... 62
  Domain policy changes ............................................................... 62
  Local audit policy changes ........................................................... 63
  User right assignment changes ..................................................... 64
  System access granted / removed .................................................. 65
  Encrypted Data Recovery policy .................................................... 65
  IPSec policy changes .................................................................. 66
  Kerberos policy changes ............................................................... 66
Object Access Reports ................................................................. 67
  Failed attempts to access to files and registry ............................. 67
  Successful attempts to access files and registry ............................ 67
  Object deleted ........................................................................... 68
Application Management Reports ................................................. 68
  Applications installed/removed ..................................................... 68
  Applications crashing or hanging ................................................... 69
Print Server Reports ..................................................................... 70
  Print activities ............................................................................. 70
Windows Event Log System Reports ............................................. 71
  Event Log health ........................................................................ 71
  Event Log cleared ....................................................................... 71
  Event Log service errors ............................................................... 72
Network Resource Access Reports (PCI requirement 10) ................... 72
  All individual access to cardholder data ....................................... 72
  All actions taken by any individual with root or administrative
  privileges .................................................................................... 73
  Access to all audit trails ............................................................... 73
  Invalid logical access attempts ...................................................... 74
  Use of identification and authentication mechanisms .................... 74
  Initialization of the audit logs ......................................................... 75
  Creation and deletion of system-level objects ................................. 75
  Time synchronization monitoring .................................................. 76
Events Trend Reports .................................................................... 76
  Generic events trend per hour ....................................................... 78
  Generic events trend per days ....................................................... 79
  Generic events trend per week ....................................................... 79
  Generic events trend per month ..................................................... 80
All critical messages reports .......................................................... 81
  All critical windows log events .................................................... 81
  All critical Syslog events .............................................................. 81
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>All critical W3C events</td>
<td>82</td>
</tr>
<tr>
<td>All critical Custom log events</td>
<td>83</td>
</tr>
<tr>
<td>All critical SNMP Traps Messages</td>
<td>83</td>
</tr>
<tr>
<td>All critical SQL Server Audit</td>
<td>84</td>
</tr>
<tr>
<td>Miscellaneous, Customizable reports</td>
<td>86</td>
</tr>
<tr>
<td>Generic Windows Event log report</td>
<td>86</td>
</tr>
<tr>
<td><strong>Troubleshooting</strong></td>
<td>87</td>
</tr>
<tr>
<td>Introduction</td>
<td>87</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td>87</td>
</tr>
<tr>
<td>Web Forum</td>
<td>87</td>
</tr>
<tr>
<td>Request technical support</td>
<td>87</td>
</tr>
<tr>
<td>Build notifications</td>
<td>88</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>89</td>
</tr>
</tbody>
</table>
Introduction

About GFI ReportCenter

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.
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)
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.

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
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>have installed a ReportPack.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Favorite Reports</strong> – 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Default Reports</strong> – 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Custom Reports</strong> – 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Scheduled Reports</strong> – 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Options</strong> – Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.</td>
<td></td>
</tr>
<tr>
<td><strong>Help</strong> – Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.</td>
<td></td>
</tr>
</tbody>
</table>
| **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. |   |
| **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). |   |
| **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.
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.

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.

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.
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.

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.
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.

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.

```
Specify custom date

Date Time
Select the date/time period on which to base the report

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

- Relative
  Today

- Day
  Saturday, July 01, 2006

1. Select the ‘Day’ option and expand the provided drop down.
2. Navigate to the required month (i.e. July) and select the required day (i.e. 1).
3. 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.
3. Select the ‘Date range’ option and specify the required parameters:
   - ‘From’ – 07/01/2006 00:00:00.
   **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

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**

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'.

3. Specify how the information will be sorted in your report.
4. Specify how the information will be grouped in your report.
5. Select the data source that will be used to generate the custom report (based on the date/time period).
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.
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:
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:
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.

<table>
<thead>
<tr>
<th>Filters applied</th>
<th>Data output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter 1 and Filter 2</td>
<td>The report will show: • All the events by users called ‘Jason’ on the computer called ‘TM_Admin1’.</td>
</tr>
<tr>
<td>Filter 1 or Filter 2</td>
<td>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).</td>
</tr>
</tbody>
</table>

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.
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.
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.
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

![Favorite reports navigation button]

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

4. Specify the report scheduling parameters (date/time/frequency). Click on Next to continue.
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:
<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Adobe Acrobat (.PDF)</td>
<td>Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.</td>
</tr>
<tr>
<td>2 MS Excel (.XLS)</td>
<td>Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.</td>
</tr>
<tr>
<td>3 MS Word (.DOC)</td>
<td>Use this format if you want to access this report using Microsoft Word.</td>
</tr>
<tr>
<td>4 Rich text format (.RTF)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Configuring report export to file options**

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

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

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:

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

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](image)

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

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’.

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.

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.
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.

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

11. From the ‘Advanced Settings’ dialog, click on the Settings button underneath the ‘Send by email’ option.
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:** ‘127.0.0.1’

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.

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.

![Database Source configuration dialog](image)

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](image)

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](image)

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

2. Configure 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](http://www.gfi.com/pages/regfrm.htm).

To input your GFI EventsManager license key:

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.
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 ReportPack:

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:
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

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

1. **Computer Name: CALDEV**

<table>
<thead>
<tr>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Account</th>
<th>Logs Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>12:22:12PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>9:26:32PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>12:22:12PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>9:26:32PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>12:22:12PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>9:26:32PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>12:22:12PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>9:26:32PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>12:22:12PM</td>
<td>6/16/2009</td>
</tr>
<tr>
<td>Successful Logon</td>
<td>529</td>
<td>Service</td>
<td>Caldev</td>
<td>Interactive</td>
<td>9:26:32PM</td>
<td>6/16/2009</td>
</tr>
</tbody>
</table>

2. **Computer Name: J NIVER**

<table>
<thead>
<tr>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Account</th>
<th>Logs Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
</table>

**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

Screenshot 48 - Sample report showing Failed logons

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Account</th>
<th>Logon Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CALLED/Host</td>
<td>E20</td>
<td>UP - Fail user name or password</td>
<td>failed</td>
<td></td>
<td>1:23 24DPM</td>
<td>9/1/2009</td>
</tr>
<tr>
<td></td>
<td>CALLED/Host</td>
<td>E20</td>
<td>UP - Fail user name or password</td>
<td>failed</td>
<td></td>
<td>1:23 24DPM</td>
<td>9/1/2009</td>
</tr>
<tr>
<td></td>
<td>CALLED/Host</td>
<td>E20</td>
<td>UP - Fail user name or password</td>
<td>failed</td>
<td></td>
<td>1:23 24DPM</td>
<td>9/1/2009</td>
</tr>
<tr>
<td></td>
<td>CALLED/Host</td>
<td>E20</td>
<td>UP - Account Disabled</td>
<td>failed</td>
<td></td>
<td>1:23 24DPM</td>
<td>9/1/2009</td>
</tr>
<tr>
<td></td>
<td>CALLED/Host</td>
<td>E20</td>
<td>UP - Logon Type Requested</td>
<td>failed</td>
<td></td>
<td>1:23 24DPM</td>
<td>9/1/2009</td>
</tr>
</tbody>
</table>

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

Screenshot 49 - Sample report showing Logoff events

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Account</th>
<th>Logon Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFT2005/SFTU201</td>
<td>E200</td>
<td>User Logoff</td>
<td></td>
<td>UserLogoff</td>
<td>1:01 24DPM</td>
<td>7/16/2009</td>
</tr>
<tr>
<td></td>
<td>SFT2005/SFTU201</td>
<td>E200</td>
<td>User Logoff</td>
<td></td>
<td>UserLogoff</td>
<td>1:01 24DPM</td>
<td>7/16/2009</td>
</tr>
<tr>
<td></td>
<td>SFT2005/SFTU201</td>
<td>E200</td>
<td>User Logoff</td>
<td></td>
<td>UserLogoff</td>
<td>1:01 24DPM</td>
<td>7/16/2009</td>
</tr>
<tr>
<td></td>
<td>SFT2005/SFTU201</td>
<td>E200</td>
<td>User Logoff</td>
<td></td>
<td>UserLogoff</td>
<td>1:01 24DPM</td>
<td>7/16/2009</td>
</tr>
<tr>
<td></td>
<td>SFT2005/SFTU201</td>
<td>E200</td>
<td>User Logoff</td>
<td></td>
<td>UserLogoff</td>
<td>1:01 24DPM</td>
<td>7/16/2009</td>
</tr>
</tbody>
</table>

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

NLM Logon attempts

The group is based on event 550 - Account Logons (50) - Account Logons failed. The event identifies the account name for the successful or unsuccessful logon attempts. If Windows 2000 domain is in use, the event is triggered for failed attempts.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Type</th>
<th>Description</th>
<th>Event Code</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>Account Logons</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
</tbody>
</table>

Failed authentication ticket requests

The analysis is based on event 550 - Account Logon failed. This event identifies the ticket that was requested to establish a connection to the domain controller. The event is triggered for failed attempts.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Type</th>
<th>Description</th>
<th>Event Code</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
</tbody>
</table>

NLM service ticket requests

The analysis is based on event 550 - Account Logon failed. This event identifies the ticket that was requested to establish a connection to the domain controller. The event is triggered for failed attempts.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Type</th>
<th>Description</th>
<th>Event Code</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
</tbody>
</table>

NLM failed events

The analysis is based on event 550 - Account Logon failed. This event identifies the ticket that was requested to establish a connection to the domain controller. The event is triggered for failed attempts.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Type</th>
<th>Description</th>
<th>Event Code</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
</tbody>
</table>

Terminal services account logon events

The analysis is based on event 551 - Account Logon from Terminal Services. This event is triggered when a user logs on through a Terminal Services session with a legacy OS.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Type</th>
<th>Description</th>
<th>Event Code</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
<tr>
<td>W2K8</td>
<td>AD</td>
<td>FTTM</td>
<td>550</td>
<td>02:44</td>
<td>11/02/2008</td>
</tr>
</tbody>
</table>

Screenshot 50 - Sample report showing account logons
Default Reports

Appendix: GFI EventsManager

Use this report to:
- Generate a list of all system logons.

**Account lockouts**

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Account</th>
<th>Logon Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>TESTSTATION</td>
<td>TEST01</td>
<td>s00001</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST02</td>
<td>s00002</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST03</td>
<td>s00003</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST04</td>
<td>s00004</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST05</td>
<td>s00005</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST06</td>
<td>s00006</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST07</td>
<td>s00007</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST08</td>
<td>s00008</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST09</td>
<td>s00009</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST10</td>
<td>s00010</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST11</td>
<td>s00011</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST12</td>
<td>s00012</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST13</td>
<td>s00013</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST14</td>
<td>s00014</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST15</td>
<td>s00015</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST16</td>
<td>s00016</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST17</td>
<td>s00017</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST18</td>
<td>s00018</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST19</td>
<td>s00019</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
<tr>
<td>TESTSTATION</td>
<td>TEST20</td>
<td>s00020</td>
<td>User Account Locked Out</td>
<td>Administrator</td>
<td>N/A</td>
<td>3:08:59PM</td>
<td>8/03/2008</td>
</tr>
</tbody>
</table>

Screenshot 51 - Sample report showing Account lockouts

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**

Chart displaying the distribution of successful logon events by user on a specific computer

Computer name

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**

- **User account created**
  - This report is based on event ID 54. Only authorized people and processes should create network accounts. Examine the user performing the attempt to verify whether an invalid attempt or process created an account. This event also details if administrators create accounts outside organizational policies.

- **User account deleted**
  - This report is based on event ID 55. Only authorized people and processes should delete network accounts. Search for these events and examine the user performing the attempt to verify if unauthorized people have deleted accounts.

- **User account changed**
  - This report is based on event ID 62. This event records changes made to security-related properties of user accounts.

**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

<table>
<thead>
<tr>
<th>Computer account created</th>
</tr>
</thead>
<tbody>
<tr>
<td>The report shows the computer accounts which were created. The report is based on the &quot;computer account created&quot; event which usually signals the fact that a new computer has joined a domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer account changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>The report shows the changes performed on the computer accounts. The report is based on the &quot;computer account changed&quot; event which shows changes performed to the authentication of the computer accounts. These include modifying the account, enabling/disabling the account, etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer account deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>The report shows the computer accounts which were deleted. The report is based on the &quot;computer account deleted&quot; event which usually signals the fact that a computer has left the domain.</td>
</tr>
</tbody>
</table>

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

**Change password attempts**

The section shows change password attempts based on the 527 event. Count the number of times that an attempt was made to change the password. The source IP address is not included in the event. Therefore, all attempts to change the password will be counted in this report. The failed attempts to change the password will be highlighted in the report.

**User account password set or reset**

The section shows events relating to the password change attempts. The events are grouped by user and computer. The events are also grouped by the user attempt to change the password. The events are grouped by the source IP address.

**Changes to dir. serv. restore mode passwords**

The section shows events relating to the change of Directory Services Restore Mode password. The events are grouped by user and computer. The events are also grouped by the user attempt to change the password.

---

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**

![Security group management diagram]

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

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**

<table>
<thead>
<tr>
<th>Privilege values and their short descriptions</th>
<th>Computer name</th>
<th>List of events with details related to audit policy changes, grouped by computer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use this report to:
- Identify audit policy changes
- Identify changes that were not made by authorized personnel.
User right assignment changes

Use this report to:
- Identify new privileges granted to a user account
- Identify privileges removed from a user account.
System access granted / removed

### Default Reports

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Action</th>
<th>Privilege</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>System access granted to account</td>
<td>Add</td>
<td>N/A</td>
<td>2/5/2010</td>
<td>8/10/2009</td>
</tr>
<tr>
<td>System access revoked from account</td>
<td>Remove</td>
<td>N/A</td>
<td>2/5/2010</td>
<td>8/10/2009</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Event Description</th>
<th>Action</th>
<th>Privilege</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted data recovery policy changed</td>
<td>Change</td>
<td>N/A</td>
<td>2/5/2010</td>
<td>8/10/2009</td>
</tr>
</tbody>
</table>

**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

Use this report to:
- Monitor IPsec policy changes
- Investigate occurrence of events outside system startups.

Kerberos policy changes

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

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Object Name</th>
<th>Object Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Event ID</th>
<th>Description</th>
<th>Object Name</th>
<th>Object Type</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
<tr>
<td>FSBVURN</td>
<td>GFIEventsManager Administrator</td>
<td>590</td>
<td>Object Open</td>
<td>REGISTRY\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Security\Logon\Eventing\Security</td>
<td>Key</td>
<td>08/24/2006</td>
<td></td>
</tr>
</tbody>
</table>

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.
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**

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Description</th>
<th>Event ID</th>
<th>Source</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(1) Product MyApp1 – Installation operation completed successfully.</td>
<td>11707</td>
<td>MInstaller</td>
<td>12:52:19PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(2) Product MyApp1 – Installation operation completed successfully.</td>
<td>11707</td>
<td>MInstaller</td>
<td>12:52:19PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(3) Product MyApp1 – Installation operation completed successfully.</td>
<td>11707</td>
<td>MInstaller</td>
<td>12:52:19PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(4) Product MyApp1 – Installation operation completed successfully.</td>
<td>11707</td>
<td>MInstaller</td>
<td>12:52:19PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(5) Product MyApp1 – Installation operation completed successfully.</td>
<td>11707</td>
<td>MInstaller</td>
<td>12:52:19PM</td>
<td>09/11/2008</td>
</tr>
</tbody>
</table>

**Applications successfully uninstalled**

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Description</th>
<th>Event ID</th>
<th>Source</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(1) Product MyApp1 – Removal completed successfully.</td>
<td>11724</td>
<td>MInstaller</td>
<td>12:53:29PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(2) Product MyApp1 – Removal completed successfully.</td>
<td>11724</td>
<td>MInstaller</td>
<td>12:53:29PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(3) Product MyApp1 – Removal completed successfully.</td>
<td>11724</td>
<td>MInstaller</td>
<td>12:53:29PM</td>
<td>09/11/2008</td>
</tr>
</tbody>
</table>

**Applications which failed to install**

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Description</th>
<th>Event ID</th>
<th>Source</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(1) MyApp2 – Installation operation failed.</td>
<td>11706</td>
<td>MInstaller</td>
<td>12:53:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(2) MyApp2 – Installation operation failed.</td>
<td>11706</td>
<td>MInstaller</td>
<td>12:53:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(3) MyApp2 – Installation operation failed.</td>
<td>11706</td>
<td>MInstaller</td>
<td>12:53:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(4) MyApp2 – Installation operation failed.</td>
<td>11706</td>
<td>MInstaller</td>
<td>12:53:15PM</td>
<td>09/11/2008</td>
</tr>
</tbody>
</table>

**Applications which failed to uninstall**

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Description</th>
<th>Event ID</th>
<th>Source</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(1) MyApp2 – uninstall failed.</td>
<td>11725</td>
<td>MInstaller</td>
<td>12:54:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(2) MyApp2 – uninstall failed.</td>
<td>11725</td>
<td>MInstaller</td>
<td>12:54:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(3) MyApp2 – uninstall failed.</td>
<td>11725</td>
<td>MInstaller</td>
<td>12:54:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(4) MyApp2 – uninstall failed.</td>
<td>11725</td>
<td>MInstaller</td>
<td>12:54:15PM</td>
<td>09/11/2008</td>
</tr>
<tr>
<td>CALDEV</td>
<td>N/A</td>
<td>(5) MyApp2 – uninstall failed.</td>
<td>11725</td>
<td>MInstaller</td>
<td>12:54:15PM</td>
<td>09/11/2008</td>
</tr>
</tbody>
</table>

Screenshot 68 - Sample report showing Applications installed/removed
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

<table>
<thead>
<tr>
<th>Computer</th>
<th>User</th>
<th>Description</th>
<th>Event ID</th>
<th>Source</th>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
</table>

Use this report to:

- Identify all faulty applications, including critical applications
- List of events showing applications which have crashed
- List of events showing applications which have hung
- List of events generated by 'DrWatson'
- 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**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>User</th>
<th>Printer Details</th>
<th>Action</th>
<th>Date/Time</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAU001V</td>
<td>N/A</td>
<td>Printer (1)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU002V</td>
<td>N/A</td>
<td>Printer (2)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU003V</td>
<td>N/A</td>
<td>Printer (3)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU004V</td>
<td>N/A</td>
<td>Printer (4)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU005V</td>
<td>N/A</td>
<td>Printer (5)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU006V</td>
<td>N/A</td>
<td>Printer (6)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU007V</td>
<td>N/A</td>
<td>Printer (7)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU008V</td>
<td>N/A</td>
<td>Printer (8)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU009V</td>
<td>N/A</td>
<td>Printer (9)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU010V</td>
<td>N/A</td>
<td>Printer (10)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU011V</td>
<td>N/A</td>
<td>Printer (11)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
<tr>
<td>CAU012V</td>
<td>N/A</td>
<td>Printer (12)</td>
<td>Install</td>
<td>1:40PM</td>
<td>OK</td>
</tr>
</tbody>
</table>

**Screenshot 70 - Sample report showing Print activities**

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

- **Event Log full**
  - Computer: NA
  - User: NA
  - Description: The Event log file is full.
  - Event ID: 8000
  - Source: EventLog
  - Time: 1:45:00PM
  - Date: 9/1/2008

- **Event log service started**
  - Computer: NA
  - User: NA
  - Description: The Event log service was started.
  - Event ID: 6005
  - Source: EventLog
  - Time: 1:47:00PM
  - Date: 9/1/2008

- **Event log service stopped**
  - Computer: NA
  - User: NA
  - Description: The Event log service was stopped.
  - Event ID: 6005
  - Source: EventLog
  - Time: 1:47:00PM
  - Date: 9/1/2008

- **Log file corrupt**
  - Computer: NA
  - User: NA
  - Description: The Event log file is corrupt, an event will be created.
  - Event ID: 6002
  - Source: EventLog
  - Time: 1:47:00PM
  - Date: 9/1/2008

- **Unexpected system shutdown**
  - Computer: NA
  - User: NA
  - Description: The system shutdown was not expected.
  - Event ID: 6008
  - Source: EventLog
  - Time: 1:47:00PM
  - Date: 9/1/2008

Screenshot 71 - Sample report showing Event Log health

- List of events generated when the event log is full
- List of events generated when the event log service is started
- List of events generated when the event log service is stopped
- List of events generated when the log file is corrupt
- 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

- **Event Log cleared**
  - Computer: SERVER
  - User name: NT AUTHORITY\SYSTEM
  - Caller user name: 0FITEMAS\FTVadminad
  - Time: 9:55:57PM
  - Date: 9/13/2006

Screenshot 72 - Sample report showing Event Log cleared

- 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

<table>
<thead>
<tr>
<th>Event Log service errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAIDEV N/A</td>
<td>Administrator removed from the VSC subsystem was excluded. The data is the lock. The data is the lock. The data is the lock. The data is the lock. The data is the lock.</td>
</tr>
<tr>
<td>CAIDEV N/A</td>
<td>Administrator removed from the VSC subsystem was excluded. The data is the lock. The data is the lock. The data is the lock. The data is the lock. The data is the lock.</td>
</tr>
<tr>
<td>CAIDEV N/A</td>
<td>Administrator removed from the VSC subsystem was excluded. The data is the lock. The data is the lock. The data is the lock. The data is the lock. The data is the lock.</td>
</tr>
</tbody>
</table>

Use this report to:

- Identify errors occurring in the auditing process.

## Network Resource Access Reports (PCI requirement 10)

### All individual access to cardholder data

<table>
<thead>
<tr>
<th>User Identification</th>
<th>Type of event</th>
<th>Time/Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
<td>[Image]</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>User Identifier</th>
<th>Type of Event</th>
<th>Date/Time</th>
<th>Source/Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Account Login</td>
<td>13:21:18AM</td>
<td>GFI EventsManager</td>
<td>Administrator Account Login</td>
</tr>
<tr>
<td>Administrator</td>
<td>Login/Logoff</td>
<td>13:21:18AM</td>
<td>GFI EventsManager</td>
<td>Administrator Login/Logoff</td>
</tr>
</tbody>
</table>

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 the PCI Data Security Standards document version 1.1.

Access to all audit trails

<table>
<thead>
<tr>
<th>User Identifier</th>
<th>Type of Event</th>
<th>Date/Time</th>
<th>Source/Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Account Login</td>
<td>13:21:18AM</td>
<td>GFI EventsManager</td>
<td>Administrator Account Login</td>
</tr>
<tr>
<td>Administrator</td>
<td>Login/Logoff</td>
<td>13:21:18AM</td>
<td>GFI EventsManager</td>
<td>Administrator Login/Logoff</td>
</tr>
</tbody>
</table>

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

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

Failed logins because of bad user name and password

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 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

<table>
<thead>
<tr>
<th>User Identification</th>
<th>Type of event</th>
<th>Data and time</th>
<th>Success or Failure of subject</th>
<th>Original System Object</th>
<th>Identify or name of affected state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>None</td>
<td>Jan 20, 2007 08:15:03 PM</td>
<td>Warning</td>
<td>GFI EventsManager</td>
<td>Audit Log</td>
<td>Initialized by root.</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Jan 20, 2007 08:15:03 PM</td>
<td>Warning</td>
<td>GFI EventsManager</td>
<td>Audit Log</td>
<td>The GDCG root initialized.</td>
</tr>
</tbody>
</table>

### Creation and deletion of system-level objects

<table>
<thead>
<tr>
<th>User Identification</th>
<th>Type of event</th>
<th>Data and time</th>
<th>Success or Failure of subject</th>
<th>Original System Object</th>
<th>Identify or name of affected state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>None</td>
<td>Dec 21, 2007 13:45:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Created</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Dec 21, 2007 13:45:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Deleted</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Dec 21, 2007 13:45:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Created</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Dec 21, 2007 13:45:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Deleted</td>
</tr>
</tbody>
</table>

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.

### List showing creation and deletion of system-level objects

<table>
<thead>
<tr>
<th>User Identification</th>
<th>Type of event</th>
<th>Data and time</th>
<th>Success or Failure of subject</th>
<th>Original System Object</th>
<th>Identify or name of affected state</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>None</td>
<td>Jan 20, 2007 08:15:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Created</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Jan 20, 2007 08:15:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Deleted</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Jan 20, 2007 08:15:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Created</td>
</tr>
<tr>
<td>NA</td>
<td>None</td>
<td>Jan 20, 2007 08:15:03 PM</td>
<td>Success</td>
<td>Windows</td>
<td>System accounts</td>
<td>Deleted</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>User/Computer</th>
<th>Time and Date</th>
<th>Source</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
<tr>
<td>VIRTUAL2009</td>
<td>2010-06-25 15:00:00</td>
<td>Server</td>
<td>Event Audited</td>
<td>The system time was changed</td>
</tr>
</tbody>
</table>

**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

Use this report to:
- Monitor system time changes
- Monitor the time synchronization process

**Screenshot 81 - Sample report showing time synchronization monitoring**

List showing time synchronization monitoring
- 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.

**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

**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
Use this report to:
- View trends on an hourly basis.
Generic events trend per days

Use this report to:
- View trends on an daily basis.

Generic events trend per week

Use this report to:
- View trends on a daily basis.
Default Reports

Appendix: GFI EventsManager

GFI EventsManager user manual

Use this report to:
- View trends on an weekly basis.

**Generic events trend per month**

Use this report to:
- View trends on a monthly basis.
All critical messages reports

All critical windows log events

<table>
<thead>
<tr>
<th>Event Source</th>
<th>Event Type</th>
<th>Event Message</th>
<th>Event Time</th>
<th>Event Source IP Address</th>
<th>Event Source Port</th>
<th>Event Source Domain</th>
<th>Event ID</th>
<th>Event Time</th>
<th>Event Source IP Address</th>
<th>Event Source Port</th>
<th>Event Source Domain</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Event Log</td>
<td>Event Triggered</td>
<td>Critical message detected</td>
<td>15:00</td>
<td>192.168.1.100</td>
<td>80</td>
<td>example.com</td>
<td>10001</td>
<td>15:00</td>
<td>192.168.1.100</td>
<td>80</td>
<td>example.com</td>
<td>10001</td>
</tr>
<tr>
<td>Windows Event Log</td>
<td>Event Triggered</td>
<td>Critical message detected</td>
<td>15:01</td>
<td>192.168.1.101</td>
<td>81</td>
<td>example.com</td>
<td>10002</td>
<td>15:01</td>
<td>192.168.1.101</td>
<td>81</td>
<td>example.com</td>
<td>10002</td>
</tr>
<tr>
<td>Windows Event Log</td>
<td>Event Triggered</td>
<td>Critical message detected</td>
<td>15:02</td>
<td>192.168.1.102</td>
<td>82</td>
<td>example.com</td>
<td>10003</td>
<td>15:02</td>
<td>192.168.1.102</td>
<td>82</td>
<td>example.com</td>
<td>10003</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Event Source</th>
<th>Event Type</th>
<th>Event Message</th>
<th>Event Time</th>
<th>Event Source IP Address</th>
<th>Event Source Port</th>
<th>Event Source Domain</th>
<th>Event ID</th>
<th>Event Time</th>
<th>Event Source IP Address</th>
<th>Event Source Port</th>
<th>Event Source Domain</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog Event Log</td>
<td>Event Triggered</td>
<td>Critical message detected</td>
<td>15:00</td>
<td>192.168.1.100</td>
<td>80</td>
<td>example.com</td>
<td>10001</td>
<td>15:00</td>
<td>192.168.1.100</td>
<td>80</td>
<td>example.com</td>
<td>10001</td>
</tr>
<tr>
<td>Syslog Event Log</td>
<td>Event Triggered</td>
<td>Critical message detected</td>
<td>15:01</td>
<td>192.168.1.101</td>
<td>81</td>
<td>example.com</td>
<td>10002</td>
<td>15:01</td>
<td>192.168.1.101</td>
<td>81</td>
<td>example.com</td>
<td>10002</td>
</tr>
<tr>
<td>Syslog Event Log</td>
<td>Event Triggered</td>
<td>Critical message detected</td>
<td>15:02</td>
<td>192.168.1.102</td>
<td>82</td>
<td>example.com</td>
<td>10003</td>
<td>15:02</td>
<td>192.168.1.102</td>
<td>82</td>
<td>example.com</td>
<td>10003</td>
</tr>
</tbody>
</table>

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.

Top 10 rules that were triggered:
1. Dnsd inbound UDP due to the security policy
2. Inboud TCP connection denied
3. Dnsd inbound UDP due to the security policy
4. Inboud TCP connection denied
5. Dnsd inbound UDP due to the security policy
6. Inboud TCP connection denied
7. Dnsd inbound UDP due to the security policy
8. Inboud TCP connection denied
9. Dnsd inbound UDP due to the security policy
10. Inboud TCP connection denied
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**

Use this report to:

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

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Priorities</th>
<th>Top 10 triggered rules and the number of events that have activated each particular rule.</th>
<th>Events that correspond to the current filtering conditions.</th>
</tr>
</thead>
</table>

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**
Appendix: GFI EventsManager

**Default Reports**

GFI EventsManager user manual

---

**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**
Top 10 rules that were triggered.

1. Top 10 triggered rules and the number of events that have activated each particular rule.

2. 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**

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.

![Screenshot 95 – Generic Windows Event log report](image)

<table>
<thead>
<tr>
<th>Computer</th>
<th>Event ID</th>
<th>Event ID</th>
<th>Event ID</th>
<th>Event ID</th>
<th>Event ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer 1</td>
<td>Event 1</td>
<td>Event 2</td>
<td>Event 3</td>
<td>Event 4</td>
<td>Event 5</td>
</tr>
</tbody>
</table>

All Windows events that correspond to the current filtering condition.
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

A
Account lockouts 56
Account Management Reports 17, 57
Account Usage Reports 17, 52
Application Management Reports 17, 68
Applications installed/removed 68
Audit policy changes 63

C
Computer account management 58
configuration settings 47
custom reports 8, 10, 23, 31, 33

D
data filters 10, 23
database source 45, 46, 47
default reports 8, 17, 18, 21
distribution of reports 9

E
e-mail settings 14
Encrypted Data Recovery policy 65
Event Log service errors 72
Events Trend Reports 77
export reports 9

F
Failed access to files and registry 67
Failed logons 54
favorite reports 8, 21, 31
filter conditions 25
framework 5, 6, 7, 9, 11

I
installation 9, 11, 14, 45, 49
IPsec policy changes 66

K
Kerberos policy changes 66

L
license 13, 39, 49, 50
Logoff events 54

N
navigation button 8, 18, 19, 21, 23, 28, 30, 31, 32, 36, 37, 38, 39, 40, 41, 42, 43, 45, 49, 50, 51

O
Object Access Reports 17, 67
Object deleted 68

P
Password changes 59
Policy Changes Reports 17, 63
Print activities 70
Print Server Reports 17, 70
product ReportPack 7
Product Selection drop down list 15, 49, 50, 51

R
Report scheduling 7, 9

S
sample database 14
schedule activity monitor 39
scheduled reports 8, 9, 38, 40
Security group management 60
Successful attempts to access files and registry 67
Successful logon count on each computer 56
Successful logons grouped by computers 53
Successful logons grouped by users 52
System access granted / removed 65
System requirements 11

T
Troubleshooting 87
U
User account management
57
user interface 7, 20, 38, 39, 45
User rights changes 64

W
Windows Event Log system
Reports 71
wizard 11, 14, 41