GFI EventsManager 8 ReportPack

Manual

By GFI Software Ltd.



Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI SOFTWARE Ltd.

Version 8.1 - Last updated June 6, 2008

Contents

Introduction	5
About GFI ReportCenter	5
About the GFI EventsManager ReportPack	6
Components of the GFI EventsManager ReportPack	7
Key features	9
Installation	11
System requirements	11
Installation procedure	11
Launching the GFI EventsManager reports for GFI ReportCenter	14
Selecting a product	14
Getting started: Default reports	17
Introduction	17
Generating a default report	
Analyzing the generated report	20
Adding default reports to the list of favorite reports	21
Custom reports	23
Introduction	23
Creating a new custom report	23
Configuring data filter conditions	25
Run a custom report	30
Editing a custom report	
Deleting a custom report Adding custom reports to the list of favorite reports	31 31
Scheduling reports	33
	00
Introduction	
Configuring advanced settings	
Configuring advanced settings	36
Configuring report emailing options	
Viewing the list of scheduled reports	
Viewing the scheduled reports activity	
Enable/disable a scheduled report	40
Editing a scheduled report	40
Deleting a scheduled report	41
Example: Scheduling a report	41
Configuring default options	45
Introduction	45
Configuring database source	45
Viewing the current database source settings	47

General options

Entering your license key after installation	49
Viewing the current licensing details	
Viewing the product ReportPack version details	
Checking the web for newer builds	

Appendix: GFI EventsManager Default Reports

49

A	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
Α	Account Management Reports	57
	User account management	57
	Computer account management	58
	Password changes	59
	Security group management	60
F	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
C	Delect Access Reports	67
-	Failed attempts to access to files and registry	67
	Successful attempts to access files and registry	
	Object deleted	
Δ	Application Management Reports	
•	Applications installed/removed	
	Applications crashing or hanging	69
F	Print Server Reports	70
•	Print activities	
V	Vindows Event Log System Reports	71
-	Event Log health	
	Event Log cleared	
	Event Log service errors	
Ν	Vetwork Resouce Access Reports (PCI requirement 10)	
	All individual access to cardholder data	72
	All actions taken by any individual with root or administrative	
	privileges	73
	Access to all audit trails	
	Invalid logical access attempts	74
	Use of identification and authentication mechanisms	
	Initialization of the audit logs	75
	Creation and deletion of system-level objects	75
	Time synchronization monitoring	76
F	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
Δ	All critical messages reports	
/-	All critical windows log events	
	All critical System events	
		01

All critical W3C events	82
All critical Custom log events	
All critical SNMP Traps Messages	83
All critical SQL Server Audit	84
Miscellaneous, Customizable reports	86
Generic Windows Event log report	86

Troubleshooting

Introduction	
Knowledge Base	
Web Forum	
Request technical support	
Build notifications	

Index

87

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.



Figure 2 – Several ReportPacks plugged into the GFI ReportCenter framework

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

About the GFI EventsManager ReportPack

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

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

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

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

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

Components of the GFI EventsManager ReportPack

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

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

GFI ReportCenter framework

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



Screenshot 1 – The GFI ReportCenter management console

The GFI ReportCenter management console is organized as follows:

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

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

🙀 GFI EventsManager 8 Report Pack Setu	ip 📃 🗙
GFI Report Center Framework detection GFI Report Center framework was not found o	n the system
GFI EventsManager 8 Report Pack requires G order to run. You need to download and install in order to proceed. © Download and install the GFI Report Center © I will <u>m</u> anually install GFI Report Center fran	FI Report Center framework version 3.5 in the GFI Report Center framework version 3.5 er framework version 3.5 nework version 3.5 and restart this installation.
	< <u>B</u> ack <u>N</u> ext > Cancel

Screenshot 2 - GFI ReportCenter framework detection dialog

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

🙀 GFI EventsManager 8 Report Pack Setup	_ 🗆 ×
Check for latest build availability Check for a newer version of GFI EventsManager 8 Report Pack.	3. 100
This installation can check whether there is a newer build for GFI EventsManager 8 Report Pack downloadable from the GFI web site. This procedure will require an internet connection in order to connect to the GFI web site. © Kes, please check for a newer version of GFI EventsManager 8 Report Pack on the GFI eventsManager 8 Repo	ne GFI web
Site. Site. No thank you, do not check for a newer version and continue with the current inst Site.	allation.
< <u>B</u> ack <u>N</u> ext>	Cancel

Screenshot 3 - Check for latest build availability

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

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

🙀 GFI EventsManager	8 Report Pack Setup
License Key Enter the following info	mation to personalize your installation
Please enter your name use GFI EventsManage	e, company and license key. If you do not have a license key you can er 8 Report Pack as an evaluation version for the first 10 days.
<u>F</u> ull Name:	Jason Micallef
<u>C</u> ompany:	GFI Software Ltd.
License Key:	Evaluation
	< <u>B</u> ack <u>N</u> ext > Cancel

Screenshot 4 - Licensing details dialog

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

🙀 GFI EventsMan	ager 8 Report Pack Sel	tup	
Database selection Data source sett	o n ings for GFI EventsManager	8 Report P	ack
Specify the datal © Use sample o © Use SQL Ser	base source that will be used database wer database	l by the GF	I EventsManager 8 Report Pack.
Server and dat <u>S</u> erver:	abase selection SQLSERVER SMSSERVER SUE TMJASON_XP	×	Authentication method Use Windows authentication. Login using the following credentials (SQL Account): User: Sa Password: *********
Database:	EventsManager	< <u>B</u> a	ack <u>N</u> ext > Cancel

Screenshot 5 - SQL Server selection dialog

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

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

🙀 GFI Eventsi	lanager 8 Report Pack Setup	□ ×
Mail Settings Enteradmin	strator email and SMTP mail server settings	J))) J))) J))
Please ente EventsMana	the details of the SMTP server and email adress that are to be used by GFI ger 8 Report Pack for email reporting.	
<u>F</u> rom:	GFIReportCenter@127.0.0.1	
<u>Т</u> о:	administrator@localhost	
S <u>M</u> TP serve	r: 127.0.0.1 <u>P</u> ort: 25	
ⓒ SMTP s ◯ SMTP s	rrver does n <u>o</u> t require authentication. rrver requires <u>a</u> uthentication.	
SMTP <u>U</u> ser:		
SMTP Pa <u>s</u> s	vord: Verify Mail Settings	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Screenshot 6 - Email configuration dialog

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

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

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

Launching the GFI EventsManager reports for GFI ReportCenter

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

Selecting a product

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

Product Selection
ALL PRODUCTS
GFI EventsManager 8.0 ReportPack
ALLPRUDUCTS

Screenshot 7 – Product Selection drop down list

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

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

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

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

Getting started: Default reports

Introduction

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

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

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

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

Generating a default report

To generate a default report:

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



Screenshot 8 - Selecting the data set period

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

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

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

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

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

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

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

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

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

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 ▼ ▼ O Day 		
Saturday , July 01, 2006		
Sun Mon Tue Wed Thu Fri Sat Year: 2006 25 26 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 Today: 9/11/2006		

Screenshot 9 - Configuring custom date/time period

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

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

5. Click Finish to generate the report.

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

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

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

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

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.
C <u>R</u> elative Today
O Day Monday , September 11, 2006
C Month September Year: 2006
Date range
Erom: 7/ 1/2006 💌 00:00:00 🚔
<u>I</u> o: 7/10/2006 💌 23:59:59 🚔
< <u>B</u> ack <u>Einish</u> <u>Cancel</u>

Screenshot 10 - Configuring custom date/time period

- 3. Select the 'Date range' option and specify the required parameters:
- 'From' 07/01/2006 00:00:00.
- 'To' 07/10/2006 23:59:59.

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

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

Analyzing the generated report



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

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

Report browsing options

Browse the generated report page by page.

- Zoom in/Zoom out.
- Search the report for particular text or characters.
- Go directly to a specific page.
- Breakdown the report into a group tree (e.g. by date/time).
- Print report.

Report storage and distribution options

- Export the generated report to a specific file format.
- Distribute the generated report via email.

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

Adding default reports to the list of favorite reports



Screenshot 12 - Favorite Reports navigation button

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

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

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

3. Click Yes to confirm.

Custom reports

Introduction

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

Creating a new custom report

To create a custom report:

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

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

Custom Report Wizard
General settings Specify the title and the type of the report
Please specify the sorting condition that will be applied on the report. The available sorting conditions can vary, depending on the current report.
Date / time Ascending
You can specify the grouping conditions for this type of report. You can either choose not to group the records or select a grouping condition from the list below.
User
< <u>B</u> ack <u>Next</u> > <u>C</u> ancel

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

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

Custom Report Wizard
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.
C <u>R</u> elative Today
O Day Monday , September 11, 2006
C Month September Year: 2006
Date range
Erom: 7/ 1/2006 💌 13:00:00 🚔
<u>I</u> o: 7/ 1/2006 ▼ 17:00:00 ÷
< <u>B</u> ack <u>Next></u> <u>C</u> ancel

Screenshot 14 – Selecting the data source to use

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

Custom Report Wizard		
Data Filters Specify any filters that should be applied on the report		
Specify the filters which will be applie	ed to this report:	
Filters		Add
		Edit
	Add Filter Property	Remove
	Specify the filter condition to apply to the Filter condition:	he report:
	ОК	Cancel

Screenshot 15 – Specifying data filter conditions

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

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

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

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

Configuring data filter conditions

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

Custom Report Wizard	
Data Filters Specify any filters that should be applied on the report	D
+(+) -(-) Move Up Move Down Filters Add Edit Edit	
< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel	

Screenshot 16 - Custom Report Wizard: Filters dialog

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

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

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

Custom Report Wizard		
Data Filters Specify any filters that should be applied on the report		
+(+) -(-) Filters	Move Up Move Down	
	Add Filter Property X	
	Specify the filter condition to apply to the report: Filter condition:	
	Logical relation: is equal to Value:	
	TM_Jason Filter property condition when added: and	
	OK Cancel	

Screenshot 17 - Filter conditions configuration dialog

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

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

Example: Using multiple filters

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

Add Filter Property 🗙	Add Filter Property
Specify the filter condition to apply to the report:	Specify the filter condition to apply to the report:
Filter condition:	Filter condition:
Scomputer Name	😫 Account 🗨
Logical relation:	Logical relation:
is equal to	is equal to
Value:	Value:
TM_Admin1	Jason
Filter property condition when added:	Filter property condition when added:
and	and 🗾
	or
OK Cancel	OK Cancel

Screenshot 18 - Using multiple filters

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

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

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

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

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

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

To create this report:

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

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

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

Custom Report Wizard
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.
C <u>R</u> elative
Today
О <u>D</u> ау
Monday , September 11, 2006
July Year: 2006
○ D <u>a</u> te range
Erom: 9/11/2006 🔽 18:27:31 🚝
<u>I</u> o: 9/11/2006 🔽 18:27:31 😴
< <u>B</u> ack <u>Next></u> <u>C</u> ancel

Screenshot 19 – Selecting the data source to use

- 4. Select the 'Month' option and specify the following parameters:
- Month: 'July'.
- Year: '2006'.
- 5. Click on **Next** to proceed to the data filters dialog.

Custom Report Wizard	
Data Filters Specify any filters that should be applied on the report	
+(+) -(-) Move Up	Move Down
Filters Computer Name is equal to TM_Admin1 Admin1 Admin1	
Add Filter Property 🗙	Add Filter Property X
Specify the filter condition to apply to the report:	Specify the filter condition to apply to the report:
Eilter condition:	Eilter condition:
Secomputer Name	See Account
Logical relation:	Logical relation:
is equal to	is equal to
<u>V</u> alue:	Kalue:
TM_Admin1	Jason
Filter property condition when added:	Filter property condition when added:
and	and T
<u><u> </u></u>	<u>Q</u> K <u>C</u> ancel

Screenshot 20 - Filter conditions dialog(s)

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

- Filter condition: 'Computer Name'
- Condition: 'Equal to'
- Value: 'TM_Admin1'.
- 7. Click **OK** to finalize your filter configuration settings.

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

- Filter condition: 'Account'
- **Condition**: 'is equal to'
- Value: 'Jason'
- Filter Property condition ...: 'and'.
- 9. Click **OK** to finalize your filter configuration settings.
- 10. Click **Next** and specify the following parameters:
- Report Name: 'Failed logons in July 2006'
- **Report Title:** 'Failed logons by Jason on computer TM_Admin1'
- **Report Description**: 'This report shows the failed logons made by user Jason Micallef on computer TM_Admin1 during July 2006.'
- 11. Click **Next** to proceed to the final dialog.
- 12. Click Finish to finalize your custom report configuration settings.

Run a custom report

To run a custom report:

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

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

Editing a custom report

To edit the configuration settings of a custom report:

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



Screenshot 21 - Custom Report Wizard: Welcome dialog

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

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

Deleting a custom report

To delete a custom report:

1. Click on the Custom Reports navigation button.

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

3. Click **Yes** to confirm.

Adding custom reports to the list of favorite reports

Custom Reports		
GFI EventsManag	er 8.0 ReportPack	
	Run	
	Edit	
	Delete	
	Add To Favorites List	
	New	►

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.

Schedule Report Wizard
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.
 ► Helauve Today ▼ Today ▼ Today Today Taday This month Last seven days This month Last month
September 🔽 Year: 2006
Date range Erom: 9/11/2006 18:47:19 Io: 9/11/2006 18:47:19
< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

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

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

Schedule Report Wizard
Time Schedule Specify the time schedule to be used to automatically generate the report
Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.
O Generate this report (once) on the following day/time:
Date/Time: 9/11/2006 🔽 19:00:21
Generate this report every:
Interval: Days
Start date/time: 9/11/2006 Hours
Davs
< <u>B</u> ack <u>N</u> ext> <u>C</u> ancel

Screenshot 24 – Report Scheduling Wizard: Time schedule dialogue

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.
| Schedule Report Wizard |
|--|
| Advanced Settings Customize report distribution and storage options. |
| You can send the generated report by email to a target recipient list or save the generated report
in a folder on your file system. Click on the Settings button of the relevant section in the dialog to
further configure report sending/saving options. |
| Export to file |
| Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored. |
| Send by mail |
| Click on the Settings button to customize and configure the email settings which will be used for report distribution. |
| < <u>B</u> ack <u>N</u> ext > Cancel |

Screenshot 25 - Report Scheduling Wizard: Advanced Settings dialog

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

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

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

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

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

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

Configuring advanced settings

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

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

Report export formats

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

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

Configuring report export to file options

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

Expor	t to file
-	Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
	Settings

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

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

Report Storage Options	х
Folder Options	
You can override the default folder options for this scheduled report	
Qverride the default folder options for this report: C:\Program Files\GFI\ReportCenter	
Report format:	
Adobe Acrobat (*.pdf)	
Ok Cancel Apply	

Screenshot 27 - Advanced Settings: Export to file options

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

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

Configuring report emailing options

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

⊠ <u>S</u> end	l by mail
	Click on the Settings button to customize and configure the email settings which will be used for report distribution.
	Settings

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

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

Email Alerts Options	×
Email Options	1
You can override the default email options for this scheduled report	
☑ Override the default email options for this report:	
<u>I</u> o: administrator@localhost	
<u>C</u> C:	I
Erom: GFIReportCenter@127.0.0.1	I
Server: 127.0.0.1 Port: 25	I
SMTP Server requires login	
User name:	
Pass <u>w</u> ord:	I
Report format: Adobe Acrobat (*.pdf)	
Ok Cancel Apply	

Screenshot 29 - Report distribution options

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

- **Report format**: Reports are sent via email as attachments. Select the file format in which to send out your report.
- 4. Click **OK** to finalize your configuration settings.

Viewing the list of scheduled reports

GFI ReportCenter 3.5					_ 8 ×
<u>File T</u> ools <u>H</u> elp					
Panes 🗸		Schedule Name	Report Name	Last Generation	Next Generation
Product Selection		Schedule for report 'Failed logons'	Failed logons		9/11/2006 7:52:18 Pł
		Schedule for report 'Failed logon	Failed logons		9/12/2006 3:15:12 Pt
GFI EventsManager 8.0 ReportPack 💌					
Scheduled Reports					
GFI E ventsManager 8.0 ReportPack. Great Scheduled Reports List Scheduled Reports Activity					
🔆 Favorite Reports					
📓 Default Reports					
🕙 Custom Reports					
🙆 Scheduled Reports					
🟠 Options					
3 Help					
	•				Þ

Screenshot 30 - List of Scheduled reports

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

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

Viewing the scheduled reports activity

GFI ReportCenter 3.5				
<u>File T</u> ools <u>H</u> elp				
Panes 🎵	Date	Product Name	Туре 🛆	Description
Product Selection	9/11/2006 7:00:28 PM	GFI EventsManager 8.0 ReportPack	Information	Finished generating s
	9/11/2006 7:00:28 PM	GFI EventsManager 8.0 ReportPack	Information	Scheduled report exp
GFI EventsManager 8.0 ReportPack 💌	9/11/2006 7:00:20 PM	GFI EventsManager 8.0 ReportPack	Information	Generating schedule
	9/11/2006 7:00:20 PM	GFTE ventsManager 8.0 ReportPack	Information	Starting to generate :
Scheduled Reports				
🖃 🧾 GFI EventsManager 8.0 ReportPack				
Scheduled Reports Activity				
👷 Favorite Reports				
Default Reports				
🕙 Custom Reports				
🙆 Scheduled Reports				
🔞 Options				
(2) Help				
	•			Þ

Screenshot 31 - Schedule activity monitor

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

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

The activity monitor displays the following events:

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

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

Solution conditions include:

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

The activity monitor records and enumerates the following information:

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

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

Enable/disable a scheduled report

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

Indicates that the scheduled report is disabled.

Indicates that the scheduled report is enabled/pending.

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

Editing a scheduled report

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

1. Click on the Scheduled Reports navigation button.

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



Screenshot 32 - Scheduled Reports wizard

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

Deleting a scheduled report

To delete a scheduled report:

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

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

Example: Scheduling a report

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

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

To create the scheduled report:

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

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

Schedu	le Rep	ort Wizard					
Date S	Time Select the	e date/time perio	d on which to base	the report	t		
Rep perio	orts base od and w	ed on date and tir ill generate result	me will gather the e is based on informa	vents occ ation found	urred dur d within th	ing the sele his specified	cted time time interval.
0	<u>R</u> elative Today Today Yesterda Last sev This mor	ay en days nth					V
Ī	Septemi	Der		~	<u>Y</u> ear:	2006	
0	D <u>a</u> te ranj	ge					
ļ	Erom:	9/11/2006	19:05:02				
-	<u>T</u> o:	9/11/2006	19:05:02	× 7			
				< <u>B</u> ac	k	<u>N</u> ext >	<u>C</u> ancel

Screenshot 33 - Select events data period

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

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

Schedule Report Wizard
Time Schedule Specify the time schedule to be used to automatically generate the report
Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.
Generate this report (once) on the following day/time:
Date/Time: 9/11/2006 💌 19:16:57 🚔
Generate this report every:
Interval:
Start date/time: 9/11/2006 Hours
< <u>B</u> ack <u>N</u> ext > <u>C</u> ancel

Screenshot 34 – Specifying the scheduling options

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

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

Schedule Report Wizard
Advanced Settings Customize report distribution and storage options.
You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.
Send by mail
Click on the Settings button to customize and configure the email settings which will be used for report distribution.
< <u>B</u> ack <u>N</u> ext > Cancel

Screenshot 35 - Advanced Settings dialog

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

Report Storage Options
Folder Options
You can override the default folder options for this scheduled report
verride the default folder options for this report:
C:\Daily Reports
Report format:
Adobe Acrobat (*.pdf)
Adobe Acrobat (*.pdf) Microsoft Excel (*.xls) Microsoft Word (*.doc) Rich Text Format (*.rtf)
Ok Cancel Apply

Screenshot 36 - Advanced Settings: Export to file options

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

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

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



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

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

Email Alerts Options	×								
Email Options									
You can override the default email options for this scheduled report									
Qverride the default email options for this report:									
Io: administrator@localhost									
<u>C</u> C:									
Erom: GFIReportCenter@127.0.0.1									
Server: 127.0.0.1 Port: 25									
☐ S <u>M</u> TP Server requires login									
User name:									
Password:									
Report format:									
Adobe Acrobat (*.pdf)									
Ok Cancel Apply									

Screenshot 38 - Report distribution options

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

13. Specify the following parameters:

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

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

15. Click Next and specify the following parameters:

- Report Name: 'Daily failed logons report'
- **Report Title**: 'Daily failed logons report'
- **Report Description**: This report is generated on a daily basis at 20:00. It shows all failed logon events recorded throughout the day.
- 16. Click **Next** to proceed to the final dialog.
- 17. Click **Finish** to finalize your custom report configuration settings.

Configuring default options

Introduction

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



Screenshot 39 - Options navigation button and Tools menu

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

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

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

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

Configuring database source

To configure your database source:

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

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

Database Sou	ce	×
Database Sour	ce	
Database se	ttings	
	Database Type: MS SQL Server	
Please spe Server / MS	cify the name or IP of the machine containing the SQL SDE database to use:	
<u>S</u> erver:	(local)	
🗖 Use SG	L Server Authentication	
<u>∐</u> ser:		
Password:		
<u>D</u> B name:	EventsManager	
	OK Cancel Apply	

Screenshot 40 - Database source configuration dialog

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

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

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

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

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

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

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

Viewing the current database source settings



Screenshot 41 - Database source configuration settings

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

Configuring default scheduling settings

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

GFI ReportCenter 3.5							
<u>F</u> ile	<u>T</u> ools <u>H</u> elp						
	Default Scheduling Options						
	ESM ReportPack						

Screenshot 42 - Default Scheduling Options node

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

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

General options

Entering your license key after installation

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

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

To input your GFI EventsManager license key:



Screenshot 43 – Product Selection drop down list

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

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

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

Lic	ensing:	×]						
Ĩ	icensing								
	-Current li	icense key							
	A	ReportPack:							
		GFI EventsManager 8.0 ReportPack							
Licensing status:									
		Evaluation version							
		Evaluation status:							
		30 days evaluation, 0 days passed							
		License key:							
		Evaluation							
	New lice	nse key							
	(Enter your new ReportPack license key:							
	(H) 20								
L									
		OK Cancel Apply							

Screenshot 44 - Licensing dialog

- 4. Type in the GFI EventsManager license key.
- 5. Click on **OK** to finalize your entry.

Viewing the current licensing details

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

Viewing the product ReportPack version details

To view the version information of your product ReportPacks:

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

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

Checking the web for newer builds

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

🖶 Program Version Properties	×
General	
Version Information	
GFI EventsManager 8.0 ReportPack	
Copyright (c) 2000-2007 GFI Software Ltd.	
GFI EventsManager 8.0 ReportPack	
There is no newer build available.	
Version: 8.0 Build: 20070821	
Check for latest version on website	
OK Cancel Apply	

Screenshot 45 - Version Properties: Check for newer builds dialog

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

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

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

Appendix: GFI EventsManager Default Reports

Account Usage Reports

1 -> User Name: GFITEMASOFT\calin

Successful logons grouped by users

	Computer	Event ID	Description	A	ccount	Logon Type	Time	Date
	FSERVER	540	Successful Network Logon	calin		Network	2:06:56PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	2:13:42PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	2:13:58PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	2:13:59PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	2:13:59PM	6/27/2006
	FSERVER	528	Successfull Logon	calin		RemoteInteractive	2:22:39PM	6/27/2006
	FSERVER	528	Successfull Logon	calin		RemoteInteractive	2:24:38PM	6/27/2006
	FSERVER	528	Successfull Logon	calin		RemoteInteractive	2:26:27PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	2:31:50PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	2:35:06PM	6/27/2006
	FSERVER	528	Successfull Logon	calin		RemoteInteractive	11:57:64PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	11:57:65PM	6/27/2006
	FSERVER	540	Successful Network Logon	calin		Network	11:59:40PM	6/27/2006
-	FSERVER	540	Successful Network Logon	calin		Network	12:00:02AM	6/28/2006
$2 \rightarrow$	FSERVER	540	Successful Network Logon	calin		Network	12:23:17AM	6/28/2006
• •	FSERVER	528	Successfull Logon	calin		NetworkCleartext	12:50:11AM	6/28/2006
	FSERVER	528	Successfull Logon	calin		NetworkCleartext	1:05:27AM	6/28/2006
	FSERVER	528	Successfull Logon	calin		RemoteInteractive	7:07:09PM	7/6/2006
	FSERVER	540	Successful Network Logon	calin		Network	7:07:10PM	7/6/2006
	FSERVER	540	Successful Network Logon	calin		Network	6:28:37PM	7/19/2006
	FSERVER	540	Successful Network Logon	calin		Network	6:28:48PM	7/19/2008
	FSERVER	540	Successful Network Logon	calin		Network	1:56:18AM	7/25/2008
	FSERVER	540	Successful Network Logon	calin		Network	1:57:42AM	7/25/2008
	FSERVER	540	Successful Network Logon	calin		Network	1:57:42AM	7/25/2008
	FSERVER	540	Successful Network Logon	calin		Network	1:57:42AM	7/25/2006
	FSERVER	540	Successful Network Logon	calin		Network	1:57:42AM	7/25/2008
	FSERVER	540	Successful Network Logon	calin		Network	1:57:42AM	7/25/2008

Screenshot 46 - Sample report showing Successful logons grouped by users



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

Successful logons grouped by computers

liser	Event ID	Description	Account	Logon Type	Time	Date
NT AUTHORITY/NETWORK SEE	828	Successful Logon	NETWORK SERVICE	Service	12-27-23PM	9/11/20
CALDEV/Calin	528	Successful Logon	Calin	Interactive	12:28:14PM	9/11/20
CALDEMCalin	520	Successful Legen	Calin	Interactive	12-20-20PM	0/11/20
CALDEV/Calin	528	Successful Logon	Calin	Interactive	12:33:07PM	9/11/20
CALDEV/Calin	528	Successful Logon	Calin	Interactive	12-34-30PM	9/11/20
CALDEVICalia	520	Successful Logon	Calin	Saprise	12:39.47DM	0/11/20
uter Name: FSERVER						
User	Event ID	Description	Account	Logon Type	Time	Date
GFITEMASOFT\Administrator	540	Successful Network Logon	Administrator	Network	5:56:24PM	11/15/20
GFITEMASOFT\Administrator	540	Successful Network Logon	Administrator	Network	6:47:43PM	11/15/20
GFITEMASOFT\Administrator	540	Successful Network Logon	Administrator	Network	6:47:43PM	11/15/20
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:06:56PM	6/27/20
GFITEMASOFT\calin	540	Successful Network Logon	calin	Network	2:13:42PM	6/27/2
			ealin			8/27/2
GFITEMASOFT\calin	540	Successful Network Logon	cain	Network	2:13:58PM	0/2/12
GFITEMASOFT\calin GFITEMASOFT\calin	540 540	Successful Network Logon Successful Network Logon	calin	Network	2:13:58PM 2:13:59PM	6/27/2
GFITEMASOFT\calin GFITEMASOFT\calin GFITEMASOFT\calin	540 540 540	Successful Network Logon Successful Network Logon Successful Network Logon	calin calin	Network Network Network	2:13:59PM 2:13:59PM 2:13:59PM	6/27/2
GFITEMASOFT\calin GFITEMASOFT\calin GFITEMASOFT\calin GFITEMASOFT\calin	540 540 540 528	Successful Network Logon Successful Network Logon Successful Network Logon Successful Logon	calin calin calin	Network Network RemoteInteractive	2:13:58PM 2:13:59PM 2:13:59PM 2:22:39PM	6/27/20 6/27/20 6/27/20 6/27/20
GFITEMASOFT\calin GFITEMASOFT\calin GFITEMASOFT\calin GFITEMASOFT\calin GFITEMASOFT\calin	540 540 528 528	Successful Network Logon Successful Network Logon Successful Network Logon Successful Logon Successful Logon	calin calin calin calin	Network Network Network RemoteInteractive RemoteInteractive	2:13:58PM 2:13:59PM 2:13:59PM 2:22:39PM 2:24:38PM	6/27/2 6/27/2 6/27/2 6/27/2 6/27/2
GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin	540 540 528 528 528	Successful Network Logon Successful Network Logon Successful Network Logon Successful Logon Successful Logon	calin calin calin calin calin	Network Network RemoteInteractive RemoteInteractive RemoteInteractive	2:13:58PM 2:13:59PM 2:13:59PM 2:22:39PM 2:24:38PM 2:26:27PM	6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/
GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTicalin	540 540 528 528 528 528 540	Successful Network Logon Successful Network Logon Successful Logon Successful Logon Successful Logon Successful Logon	calin calin calin calin calin calin	Network Network RemoteInteractive RemoteInteractive RemoteInteractive Network	2:13:69PM 2:13:69PM 2:23:69PM 2:22:39PM 2:24:38PM 2:26:27PM 2:31:50PM	6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/
GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin	540 540 528 528 528 528 540 540	Successful Network Logon Successful Network Logon Successful Network Logon Successful Logon Successful Logon Successful Network Logon Successful Network Logon	cain cain cain cain cain cain cain	Network Network RemoteInteractive RemoteInteractive RemoteInteractive Network	2:13:60PM 2:13:50PM 2:22:30PM 2:24:30PM 2:26:27PM 2:31:50PM 2:35:00PM	6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/
GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin	540 540 528 528 528 528 540 540 540	Successful Network Logon Successful Network Logon Successful Network Logon Successful Logon Successful Logon Successful Network Logon Successful Network Logon Successful Network Logon	cain cain cain cain cain cain cain cain	Network Network RemoteInteractive RemoteInteractive RemoteInteractive Network Network RemoteInteractive	2:13:60PM 2:13:50PM 2:22:30PM 2:24:38PM 2:26:27PM 2:31:50PM 2:35:00PM 11:57:54PM	6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20
GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln GFITEMASOFToaln	540 540 528 528 528 528 540 540 528 540	Successful Network Logon Successful Network Logon Successful Logon Successful Logon Successful Logon Successful Network Logon Successful Network Logon Successful Logon Successful Network Logon	cain cain cain cain cain cain cain cain	Network Network RemoteInteractive RemoteInteractive RemoteInteractive Network Network RemoteInteractive Network	2:13:69PM 2:13:69PM 2:23:69PM 2:22:39PM 2:24:38PM 2:26:27PM 2:31:50PM 2:35:06PM 11:57:54PM 11:57:54PM	6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20
GPTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln GFTEMASOFToaln	540 540 528 528 528 528 540 540 528 540 528 540	Successful Network Logon Successful Network Logon Successful Network Logon Successful Logon Successful Logon Successful Logon Successful Network Logon Successful Network Logon Successful Network Logon	cain cain cain cain cain cain cain cain	Network Network RemoteInteractive RemoteInteractive RemoteInteractive Network RemoteInteractive Network Network	2:13:69PM 2:13:60PM 2:23:360PM 2:22:30PM 2:24:39PM 2:31:50PM 2:35:00PM 11:57:54PM 11:57:54PM 11:59:40PM	6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20
GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin GPTEMASOFToalin	540 540 528 528 528 528 540 540 528 540 528 540 540 540	Successful Network Logon Successful Network Logon Successful Logon Successful Logon Successful Logon Successful Network Logon Successful Network Logon Successful Network Logon Successful Network Logon	cain cain cain cain cain cain cain cain	Network Network Network RemoteInteractive RemoteInteractive RemoteInteractive Network Network Network Network Network	2:13:58PM 2:13:50PM 2:23:50PM 2:22:30PM 2:24:38PM 2:25:27PM 2:35:50PM 11:57:54PM 11:57:54PM 11:59:40PM 11:59:40PM	6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/
GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln GPTEMASOFToaln	540 540 528 528 528 528 540 540 540 540 540 540	Suddestull Network Logon Suddestull Network Logon Suddestull Logon Suddestull Logon Suddestull Logon Suddestull Logon Suddestull Network Logon Suddestull Network Logon Suddestull Network Logon Suddestull Network Logon Suddestull Network Logon	cain cain cain cain cain cain cain cain	Neteonik Neteonik RemoleInteractive RemoleInteractive RemoleInteractive Neteonik Neteonik Neteonik Neteonik Neteonik	2:13:69PM 2:13:69PM 2:22:39PM 2:22:39PM 2:26:67PM 2:35:60PM 11:57:64PM 11:57:64PM 11:57:64PM 11:57:64PM 11:57:64PM 12:00:02AM 12:23:17AM	6/27/2/ 6/27/2
GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin GFITEMASOFToalin	540 540 528 528 528 528 540 540 540 540 540 540 540 540 540	Suddeskulli Network, Logon Suddeskulli Network, Logon Suddeskulli Network, Logon Suddeskulli Logon Suddeskulli Logon Suddeskulli Network, Logon Suddeskulli Network, Logon Suddeskulli Network, Logon Suddeskulli Network, Logon Suddeskulli Network, Logon Suddeskulli Network, Logon	cain cain cain cain cain cain cain cain	Network Network Remote Interactive Remote Interactive Remote Interactive Network Network Network Network Network Network Network Network	2:13:68PM 2:13:69PM 2:23:69PM 2:22:39PM 2:24:38PM 2:24:38PM 2:33:50PM 11:57:64PM 11:57:64PM 11:57:64PM 11:59:40PM 12:20:02AM 12:20:27AM	6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/27/2/ 6/28/2/ 6/28/2/
GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin GFITEMASOFTealin	540 540 528 528 528 528 540 540 540 540 540 540 540 540 540 540	Suddeskuli Network Logon Suddeskuli Network Logon Suddeskuli Network Logon Suddeskuli Logon Suddeskuli Logon Suddeskuli Network Logon Suddeskuli Logon	cain cain cain cain cain cain cain cain	Neteonic Neteonic Remotelinteractive Remotelinteractive Remotelinteractive Neteonic Remotelinteractive Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic	2:13.36PM 2:13.46PM 2:23.36PM 2:22.36PM 2:24.38PM 2:24.38PM 2:25.06PM 11:57.56PM 11:57.56PM 11:57.56PM 11:57.56PM 12:20.02AM 12:20.02AM 12:20.11AM	6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/27/20 6/28/20 6/28/20 6/28/20 6/28/20
GRTETASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn GRTEMASOFTealn	540 540 528 528 528 540 540 540 540 540 540 540 540 540 540	Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Logon Suddeskulli Logon Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Network Logon Suddeskulli Logon	cain cain cain cain cain cain cain cain	Neteonic Neteonic Remotentineractive Remotentineractive Remotentineractive Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic Neteonic	2:13.36PM 2:13.56PM 2:13.56PM 2:22.36PM 2:24.36PM 2:24.36PM 2:35.06PM 11.57.54PM 11.57.54PM 11.57.54PM 11.57.54PM 11.59.40PM 12.23.17AM 12.23.17AM 12.23.17AM	627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 627/2 628/2 628/2 628/2 628/2 7/6/2

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.

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

Failed logons

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

Screenshot 48 - Sample report showing Failed logons

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

Use this report to:

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

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

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

Logoff events

	Computer	User	Event ID	Description	Account	Logon Type	Time	Date
	FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:58:27AM	7/25/2006
	FSERVER	GFITEMASOFT/calin	538	User Logoff	N/A	Network	1:57:13AM	7/25/2006
	FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:42AM	7/25/2006
	FSERVER	GFITEMASOFT/calin	538	User Logoff	N/A	Network	1:57:42AM	7/25/2006
U-	FSERVER	GFITEMASOFT/calin	538	User Logoff	N/A	Network	1:57:42AM	7/25/2006
	FSERVER	GFITEMASOFT\calin	538	User Logoff	N/A	Network	1:57:52AM	7/25/2006
	FSERVER	GFITEMASOFT/calin	538	User Logoff	N/A	Network	1:58:12AM	7/25/2006
	FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	Network	2:18:38AM	9/10/2006
	FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	RemoteInteractive	2:22:07AM	9/10/2006
	FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	Network	2:36:43AM	9/10/2006
	FSERVER	GFITEMASOFT\Administrator	538	User Logoff	N/A	Network	2:38:04AM	9/10/2006

Screenshot 49 - Sample report showing Logoff events



List of events showing all user logoff events.

Correlate these events with the successful logon events to determine the duration of each user session.

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

Account Logons

NTLM Logon attempts

The group is based on event880 – Account used for logon and 681 – Logon to account failed. The evens identify the account used for the successful or failed domain logon attempts. Event880 is logged on Windows 2000 domains both for successful and failed attempts. On Windows 2000 domains, event880 is logged on tyric successful attempts. Biology and the provide the successful and the successful attempts. Biology and the provide the successful attempts. Biology and the successful attempts. The successful attempts are successful attempts. Biology and the successful attempts are successful attempts. Biology and the successful attempts are successful attempts. Biology and the successful attempts are successful attempts and the successful attempt with a event Biology attempt with a event

	Computer	Туре	Description	Logon Account	Source Workstation	Error Code	Time	Date
VDC		Auditaliure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P M	9/10/2006
VDC		Auditualiure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P.M	9/10/2006
VDC		Auditualiure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P.0	9/10/2005
VDC		Audittaliure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P.0	9/10/2005
VDC		Auditraliure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P.0	9/10/2005
VDC		Auditraliure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P.M	9/10/2005
VDC		Auditaliure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P.M	9/10/2005
VDC		Auditaliure	Logon to account talled	Calh	CALDEV	3221225572	4:10:59P M	9/10/2005

Kerberos authentication ticket requests

The section is based on event 672 – authentication ticket request. This event enables the tracking of initial domain logons through the granting to the granting ticket granting ticket granting ticket (TG T). Windows 2003 domain records this event for both success and failure requests. The type field indicates whether the request was successful or on the Windows 2000 domains the event only records successful or ont in Windows 2000 domains the event only records successful or ont in Windows 2000 domains the Windows 2000 domains are the Windows 2000 domains are the Windows 2000 domains are the Windows 2000 domains the Windows 2000 domains are t

Computer	Type	User Name	Service Name	Client Address	Result Code	Time	Date
FSERVER	Auditsuccess	GFITEMASOFT.ROVESERVER\$	kırbılgit	127 0.0.1	NA	120805A.W	9/10/2006
FSERVER	Audits access	GFITEMASOFT.ROVESERVER\$	kıbigt	127 0.0.1	N/A	120806A.W	9/10/2005
FSERVER	Auditsuccess	GFITEMASOFT.ROVESERVER\$	kıtdığt	127 0.0.1	N/A	1208:17AM	9/10/2006
FSERVER	Audit tallure	G FITEMASO FTallia	kibigtG FITEMASO FT	127 0.0.1	N/A	12:13:26AM	9/10/2005
FSERVER	Auditaliure	G FITEMASO FTrailina	kibigtGFITEMASOFT	127 0.0.1	N/A	12:13:25A.M	9/10/2006
FSERVER	Audits uccess	G FITEMASO FT Administrator	kıtoligit	127 0.0.1	NA	12:31:46A.0	9/10/2005
FSERVER	Audits topess	GFITEMASOFTNUSR_FSERVER	kırbılgit	127 0.0.1	NA	12:41:55A.M	9/10/2006
FSERVER	Auditsuccess	GFITEMASOFTNUSR_FSERVER	kırbılgit	127 0.0.1	NA	1:38:53A.U	9/10/2006

Kerberos service ticket requests



The section is based on event 873 - A ticket grantingsenrice (TOS) ticket was requested. After a user's workstation requests a ticket grantingticket (TOB), the workstation immediatelyrequests a service ticket (TOB) so that the user can use the workstation. Windows 2003 domain records this event for both success and failure requests. The type field indicates worket muse there workstation or time workstation is based on event only records successful or not in Windows 2000 domains, the event only records successful erquests. For failed requests 2000 domains use the#77 event.

Computer	Туре	User Name	Service Name	Client Address	Failure Code	Time	Date
FSERVER	Auditsuccess	GFITEMASOFT.ROVAdministrator@GFITE MASOFT.RO	FSERVER\$	127 0.0.1	-	4:16:22AM	9/10/2005
FSERVER	Audits cooess	GFITEMASOFT.ROVAdministrator@GFITE MASOFT.RO	FSERVER\$	127 0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Audits uccess	GFITEMASOFT.ROVAdministrator@GFITE MASOFT.RO	FSERVER\$	127 0.0.1	-	4:16:22AM	9/10/2005
FSERVER	Auditsuccess	GFITEMASOFT.ROVAdministrator@GFITE MASOFT.RO	FSERVER\$	127 0.0.1	-	4:16:22AM	9/10/2005
FSERVER	Auditsuccess	GFITEMASOFT.ROVAdministrator@GFITE MASOFT.RO	FSERVER\$	127 0.0.1	-	4:16:22AM	9/10/2006
FSERVER	Auditsuccess	GFITEMASOFT.ROVAdministrator@GFITE MASOFT.RO	FSERVER\$	127 0.0.1	-	4:16:22A.M	9/10/2006
FSERVER	Auditsuccess	GFITEMASOFT.ROMORNERSCOFTEMAS OFT.RO	kıbılgit	127 00.1	-	4:16:25A.M	9/10/2006

Kerberos failed events

The section is based on events 676 - Pre-authenticationfailed,676 - Authentication Ticket Request failed,and 677 - Service ticket request failed Event675
 is recorded both in Windows 2000 and Windows 2003 domains. In a Windows 2000 domain, events 676 and 677 are logged for failed authentication/service
 ticket request

Computer	User Name	Description	Service Name	Client Address	Failure Code	Time	Date
FSERVER	G FITEMASO FT Administrator	Pre-artheritication tailed	kibigtGFITEMASOFT	127 00.1	B:18	4:16:20A.U	3/10/2005
FSERVER	G FITEMASO FT Administrator	Pre-arthentication talled	kibigtG FITEMASO FT	127 DD.1	Dc18	4:16:20A.M	9/10/2005
FSERVER	G FITEMASO FT Administrator	Pre-antientication tailed	kiblgtG FITEMASO FT	127 0.0.1	Dc18	4:16:2DAM	9/10/2005
FSERVER	G FITEMASO FT Administrator	Pre-autientication talled	kiblgtG FITEMASO FT	192.168.100.20	0.25	4:19:55A.M	9/10/2006
FSERVER	G FITEMASO FT Administrator	Pre-arthentication tailed	kiblgtG FITEMASO FT	192.168.100.20	0.25	4:19:55A.U	9/10/2005
FSERVER	G FITEMASO FT Administrator	Pre-autientication talled	kiblgtG FITEMASO FT	192.168.100.20	0:25	4:19:55A.U	9/10/2005
FSERVER	G FITEMASO FT Administrator	Pre-antiventication talled	krbigtGFITEMASOFT	192.168.100.20	Br25	420:17AM	9/10/2005

Terminal services account logon events

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

Computer	User Name	Description	Session Name	Client Name	Client Address	Time	Date
FSERVER	G FITEMASO FTradministrator	Session disconnected to winstation	R D P-Top#3	z	192.168.100.11	15191AM	8/21/2006
FSERVER	G FITEMASO FTradministrator	Session disconnected to winstation	R D P-Top#3	z	192.168.100.11	151D1AM	8/21/2006
FSERVER	G FITEMASO FTradministrator	Session reconnected to winstation	R D P-Top#4	z	192.168.100.11	1:53:15AM	8/21/2006
FSERVER	G FITEMASO FTradm in istrator	Session reconnected to winstation	R D P-Top#4	z	192.168.100.11	1:53:15AM	8/21/2006
FSERVER	G FITEMASO FTradm in istrator	Session disconnected to winstation	RDP-Top#4	z	192.168.100.11	23304PM	8/21/2006
FSERVER	G FITEMASO FTradin in istrator	Session disconnected to winstation	RDP-Top#4	z	192.168.100.11	23304PM	8/21/2006
FSERVER	G FITEMASO FTradm in istrator	Session reconnected to winstation	RDP-Top#5	z	192.168.100.11	234:11PM	8/21/2006
FSERVER	G FITEIII.ASO FTradm in istrator	Session reconnected to winstation	RDP-Top#S	z	192.168.100.11	234:11PM	8/21/2006

Screenshot 50 - Sample report showing account logons

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

Use this report to:

• Generate a list of all system logons.

Account lockouts

	Computer	User	Event ID	Description	Account	Logon Type	Time	Date
	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	12:01:42PM	8/17/2005
	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:34:59PM	9/1/2005
	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	3:35:44PM	9/1/2005
	TESTSTATION	TESTINGD/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:01:09PM	9/1/2005
	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:08:33PM	9/1/2005
• •	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:14:54PM	9/1/2005
	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:47:21PM	9/1/2005
	TESTSTATION	TESTING0/TESTSTATION\$	644	User Account Locked Out	Administrator	N/A	5:50:54PM	9/1/2005
	FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	pisu	N/A	2:28:04PM	6/27/2006
	FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Locked Out	Administrator	N/A	7:54:55PM	7/6/2006
	FSERVER	GFITEMASOFT\FSERVER\$	644	User Account Looked Out	Administrator	N/A	12:18:13AM	7/12/2006

Screenshot 51 - Sample report showing Account lockouts

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

Use this report to:

1

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

Successful logon count on each computer



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

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

Use this report to:

Graphically represent successful logons by users on each computer

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

Account Management Reports

User account management

0-			rations distribution			
0-						
	User account deleted	User acc	iount changed			
			User account chang	ed 40.7%		
			User account create	d 33.3%		
			User account delete	d 25.9%		
			Total:	100.0%		
	User account created					
liser account creat	ed.]		
The section is ha	sed on event 624. Only authorized or	onle and processes shou	id create network accounts. Exami	ne the user performing the attem	nt field to	
detect whether an guidelines.	authorized person or process create	ed an account. This event a	also detects if administrators creat	e accounts outside organizationa	al policy	
User creating the accoun	nt Computer Name	Attempt	Old Account Name	New Account Name	Time	Date
OF ITEMAS OF TVAdministrator	FSER//ER	Audt success	N/A	calin	3:12:46PM	9/16/2005
GF ITEMAS OF TVAdministrator	F\$ER/JER	Audit success	N/A	calin	3:12:52PM	9/16/2006
GF ITEMAS OF TVAdministrator	FSER/JER	Audit success	N/A	calin	3:13:42PM	9/16/2005
FITEMASOFTVAdministrator	FSERVER	Audit success	NA	calin	3:13:44PM	9/16/2006
FILEMAS UP Tradministrator	F SERVER	Audit success	N/A	cain perman	3:15:07PM	9/16/2005
FITEMAS OF Tradministrator	F SERVER F SERVER	Audit success	N/A	IUSK_FSERVER	2:51:20PM	6/10/2006
FITEMASOFTealo	ESERVER	Audt success	N/A	nimu	1:20:10PM	6/27/2006
FITEMASOFTicalin	FSERVER	Audit success	N/A	ofitest1	1:32:13PM	6/27/2006
User account dele	eted	seening and processes sho	uld delete network accounts. Sear	ch far thac a mante and avamina	the user	
performing the a	attempt field to detect if unauthorized p	people have deleted accou	uid delete network accounts. Sean ints.	ch for these events and examine	the user	
		Attempt	Target Account Name			
User deleting the account	at Computer Name			New Account Name	Time	Date
User deleting the account TESTINGONTESTISTATIONS	t Computer Name	Audt success	LNSS_MONITOR_USR	New Account Name	Time 12:24:32PM	Date 8/16/2006
User deleting the account restingenteststations restingenteststations	t Computer Name TESTSTATION TESTSTATION	Audt success Audt success	LNSS_MONITOR_USR LNSS_MONITOR_USR	New Account Name N/A	Time 12:24:32PM 12:24:32PM	Date 8/16/2005 8/16/2005
User deleting the account restingenteststations restingenteststations restingenteststations	t Computer Name TESTSTATION TESTSTATION TESTSTATION	Audt success Audt success Audt success	LNSS_MONITOR_USR LNSS_MONITOR_USR LNSS_MONITOR_USR	New Account Name N/A N/A N/A	Time 12:24:32PM 12:24:32PM 12:24:32PM	Date 8/16/2005 8/16/2005 8/16/2005
User deleting the account ESTINGO/TESTSTATIONS ESTINGO/TESTSTATIONS ESTINGO/TESTSTATIONS FITEMASOFT/Administrator	t Computer Name TESTSTATION TESTSTATION TESTSTATION FSERVER	Audt suocess Audt suocess Audt suocess Audt suocess Audt suocess	LNSS_MONITOR_USR LNSS_MONITOR_USR LNSS_MONITOR_USR calin	New Account Name	Time 12:24:32PM 12:24:32PM 12:24:32PM 3:12:51PM	Date 8/16/2005 8/16/2005 8/16/2005 9/16/2005
User deleting the account ESTINGONESTSTATIONS ESTINGONESTSTATIONS ESTINGONESTSTATIONS FITMASOFTNAMINIStrator FITMASOFTNAMINIStrator	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FSERVER FSERVER	Audt success Audt success Audt success Audt success Audt success Audt success	LNSS_MONITOR_USR LNSS_MONITOR_USR LNSS_MONITOR_USR calin calin	New Account Name N/A N/A N/A N/A	Time 12:24:32PM 12:24:32PM 3:12:51PM 3:12:51PM 3:12:50PM	Date 8/16/2005 8/16/2005 9/16/2005 9/16/2005
User deleting the account throotteststations throotteststations throotteststations theAsOFTVAdministrator TBA4SOFTVAdministrator TBA4SOFTVAdministrator TBA4SOFTVAdministrator	tt Computer Name TESTSTATION TESTSTATION TESTSTATION TESTSTATION FSERVER FSERVER FSERVER FSERVER	Audt success Audt success Audt success Audt success Audt success Audt success Audt success Audt success	LNSS_MONITOR_USR LNSS_MONITOR_USR LNSS_MONITOR_USR calin calin calin	New Account Name N/A N/A N/A N/A N/A	Time 12:24:32PM 12:24:32PM 3:12:51PM 3:12:51PM 3:13:43PM 3:13:43PM	Date 8/16/2005 8/16/2005 9/16/2005 9/16/2005 9/16/2005
User deleting the account TESTINGOVERTSTATIONS TESTINGOVERTSTATIONS OFTEMASOFTATIONS OFTEMASOFTAdministrator OFTEMASOFTAdministrator OFTEMASOFTAdministrator OFTEMASOFTAdministrator User account charn	t Computer Name TESTSTATION TESTSTATION TESTSTATION FSERVER FSERVER FSERVER FSERVER ISERVER IS	Audt success Audt success Audt success Audt success Audt success Audt success Audt success Audt success	LNSS_MONITOR_USR LNSS_MONITOR_USR cain cain cain cain cain	New Account Name Nia Nia Nia Nia Nia Nia Nia Nia	Time 12:24:32PM 12:24:32PM 3:12:51PM 3:12:51PM 3:13:50PM 3:13:40PM	Date 8/16/2005 8/16/2005 9/16/2005 9/16/2005 9/16/2005
User deleting the account тактиконстатитика тактиконстатитика тактиконстатитика отгламооптоннонитако отгламооптон	tt Computer Name TESTSTANDN TESTSTANDN TESTSTANDN FSERVER FSERVER FSERVER Starver Star	Audt zuocess Audt zuocess Audt zuocess Audt zuocess Audt zuocess Audt zuocess Audt zuocess Audt zuocess s changes made to securi	LNSS_MONTOR_USR LNSS_MONTOR_USR callo callo callo callo callo callo callo callo callo callo callo	New Account Name NA NA NA NA NA NA NA NA NA NA NA	Time 12:24:32PM 12:24:32PM 3:12:51PM 3:12:53PM 3:13:45PM 3:13:46PM	Date 9/16/2005 9/16/2005 9/16/2005 9/16/2005 9/16/2005
Вые disting the account техночестват какоон техночестват какоон техночестват какоон техночестват какоон оттемако Отчанизация Отчанизация Отчанизация Отчанизация Оттемако Отчанизация	tt Computer Name TESTSTATION TESTSTATION F	Audi suocess Audi suocess Audi suocess Audi suocess Audi suocess Audi suocess Audi suocess Is changes made to securi Attempt	Units Johnmong Unit Linits Johnmong Unit Linits Johnmong Unit Linits Johnmong Unit calls calls calls calls fly-reliated properties of user accou Target Account Name	New Account Name Noa	Time 12:24/32PM 12:24/32PM 3:12:51PM 3:12:51PM 3:12:50PM 3:13:46PM	Date 9/16/2005 9/16/2005 9/16/2005 9/16/2005 9/16/2005 Date
User deleting the account restinuous stratures to the international strature of the User account chan User changing the account EDISTATIONALFINIATION	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FESTIVATION FESTIVATION FESTIVATION TESTSTATION tt Computer Name TESTSTATION	Audt suncess Audt suncess Audt suncess Audt suncess Audt suncess Audt suncess is changes made to securi Audt suncess Audt suncess	Liss, scientroli, usi Liss, scientroli, usi Liss, scientroli, usi Liss, scientroli, usi anin anin anin anin anin by-related properties of user account Target Account Name SEM_MON_USER	New Account Name NA	Time 1224.02PM 1224.03PM 1224.03PM 1224.03PM 3.12.51PM 3.13.40PM 3.13.40PM 3.13.40PM 3.13.40PM 3.13.40PM 3.13.40PM	Date #/16/2005 #/16/2005 #/16/2005 #/16/2005 #/16/2005 Date #/14/2005
User deleting the account retrinoceter stratoris retrinoceter stratoris retrinoceter stratoris pri the stratoris pri the stratoris pri the stratoris pri the stratoris the section is but User changing the account EFISTATIONA-deviations EFISTATIONA-deviations	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FISTSTATION FISTSTATION FISTSTATION ASSED OF EVENT TESTSTATION TESTSTATION	Auft success Auft success	Units Johnmong Utits Luss Johnmong Utits Luss Johnmong Utits calls calls calls calls defined and the second second by related properties of user accou Target Account Name SELU_JOID_USER SELU_JOID_USER	New Account Name No	Time 12:24:32Mi 12:24:32Mi 12:24:32Mi 3:12:51Mi 3:12:51Mi 3:13:40PMi 3:13:40PMi 3:22:51Mi 3:32:51Mi 3:13:40PMi 3:13:40PMi 3:22:51PMi	Date 9/16/2005 9/16/2005 9/16/2005 9/16/2005 9/16/2005 0/16/2005 8/14/2005
User deleting the account TESTINOOTEST ATMONE TESTINOOTEST ATMONE TESTINOOTEST ATMONE OFTERADO TTACHINGTONE OFTERADO TTACHINGTONE OFTERADO TTACHINGTONE OFTERADO TTACHINGTONE OFTERADO TTACHINGTONE OFTERADO TTACHINGTONE User account chan User account chan User changing the account TESTISTATION/Administrator TESTISTATION/Administrator TESTISTATION/Administrator	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FESTSTATION FESTSTATION FESTSTATION FESTSTATION tt Computer Name tESTSTATION TESTSTATION TESTSTATION	Add success Add success Add success Add success Add success Add success add success is changes made to securi Add success Add success Add success Add success Add success	Liss, scientroli, use Liss, scientroli, use Liss, scientroli, use catin	New Account Name NA	Time 122432PM 122432PM 31232PM 31233PM 31343PM 31343PM 31344PM 31342PM 3134PM	Date \$/16/2005 \$/16/2005 \$/16/2005 \$/16/2005 Date \$/14/2005 \$/14/2005
User deleting the account reinvolver 174 and reinvolver 174 and of TBMAG TVAministrator of TBMAG TVAministrator of TBMAG TVAministrator of TBMAG TVAministrator of TBMAG TVAministrator User account chan User changing the account EISTSTATONA-Menistrator EISTSTATONA-MENISTRATOR EISTSTATONA-MENISTSTATONA-MENISTRATONA-MENISTRATONA-MENIST	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FISTSTATION FISTSTATION FISTSTATION ASSED ON EVENT FISTSTATION TESTSTATION TESTSTATION TESTSTATION TESTSTATION TESTSTATION	Auft success Auft success	Uns such more uns Luss such more uns Luss such more uns can can can can can can can for related properties of user accou Target Account Name SEM_Joor_USER SEM_Joor_USER	New Account Name No	Time 122432PM 123432PM 13345PM	Date 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005
User deleting the account TESTINGOUESTS ATMONE TESTINGOUESTS ATMONE OFTERMAD OT PARAMENTARIA OFTERMAD OT PARAMENTARIA OFTERMAD OT PARAMENTARIA OFTERMAD OT PARAMENTARIA OFTERMAD OT PARAMENTARIA THE SECTION Advantations TESTS TATION Advantation TESTS TA	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FESTSTATION FESTSTATION FESTSTATION FESTSTATION tt TESTSTATION TESTSTATIO	Auft succes Auft succes	Liss, scientroli, use Liss, scientroli, use Liss, scientroli, use catin	New Account Name N/A	Time 1224.02PM 1224.03PM 1224.03PM 1224.03PM 1224.03PM 122.03PM 0.12.03PM 0.12.04PM 0.12.04PM 0.12.04PM 0.12.04PM 0.12.04PM 0.12.04PM 0.12.02PM	Date 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.15/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005 0.14/2005
User deleting the account Testmoneter transmission Testmoneterstrations or Testado Thansmission or Testado Thansmission or Testado Thansmission or Testado Thansmission or Testado Thansmission or Testado Thansmission Dise changing the account Tests TafonAansmission TESTS Tafo	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FESTSTATION FESTSTATION FESTSTATION ASSED ON EVENT 642. This event record assed on event 642. This event record tt Computer Name TESTSTATION TESTSTATION TESTSTATION TESTSTATION TESTSTATION FESTSTATION	Auft success Auft success	Uns schumbe Uns Luss Johnno Uns Luss Johnno Uns cain cain cain cain cain cain cain cain	New Account Name N/A	Time 12.24327ki 12.24327ki 12.24327ki 12.24327ki 12.24327ki 12.2537ki 12.2537ki 13.3457ki 13.3457ki <td< td=""><td>Date 8/16/2006 8/16/2006 8/16/2006 9/16/2006 9/16/2006 9/16/2006 8/14/2006 8/14/2006 8/14/2006 8/14/2006 8/14/2006 8/14/2006</td></td<>	Date 8/16/2006 8/16/2006 8/16/2006 9/16/2006 9/16/2006 9/16/2006 8/14/2006 8/14/2006 8/14/2006 8/14/2006 8/14/2006 8/14/2006
User deleting the account TESTINGUESTIANOUS ESTINGUESTIANOUS OFTERMOST TANNOUS OFTERMOST TANNOUS OFTERMOST TANNOUS OFTERMOST TANNOUS THE SECTION TANNOUS THE SECTION TANNOUS TESTIANOUAPHINISTREE	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FESTSTATION FESTSTATION FESTSTATION tstate Computer Name tstatistation TESTSTATION TE	Auft succes Auft succes	Loss Johnmong Use Loss Johnmong Use Loss Johnmong Use Loss Johnmong Use Loss Johnmong Use Loss Johnmong Use tain calin c	New Account Name N/A	Time 12.24.03PH 12.24.03PH 12.24.03PH 12.24.03PH 12.25TH	Date 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026 9/15/2026
User deleting the account testinologistry and account testinologistry and account of ITBASIO THANSIANE OF ITBASIO THANSIANE OF ITBASIO THANSIANE User account chan User account chan User account chan User account chan ISTIATIONWARNING TESTIATIONWARNING TESTIATIONWARNING TESTIATIONWARNING TESTIATIONWARNING TESTIATIONWARNING TESTIATIONWARNING OF ITBASIO THANSIANE OF ITBASIO THAN	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FISTSTATION FISTSTATION FISTSTATION ASSED OF EVENT FISTSTATION TESTSTATION TESTSTATION TESTSTATION TESTSTATION TESTSTATION FISTSTATION FISTSTATIO	Auft success Auft success	Uns schumbe Uns Luss Johnnon Uns Luss Johnnon Uns cain cain cain cain cain cain cain cain	New Account Name N/A N/A	Time 12.24.02PH 12.24.02PH 12.24.02PH 3.12.01PH 3.12.01PH 3.13.40PH 3	Date 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/15/2005 9/17/2006 9/7/2006 9/7/2006
User deleting the account TESTINGUESTIANONS TESTINGUESTIANONS TESTINGUESTIANONS OFTEMANOTANING OFTEMANOTANING OFTEMANOTANING OFTEMANOTANING TESTIANONANING T	tt Computer Name TESTSTATION TESTSTATION TESTSTATION FESTSTATION FESTSTATION FESTSTATION feststate festore festore festore teststation tes	And succes And succes	Less Johnnon Uter Luss Johnnon Uter Luss Johnnon Uter Luss Johnnon Uter Luss Johnnon Uter all all all h-related properties of user accourt Target Account Name Stat John User Stat John User Stat John User Stat John User Stat John User all all all all all all all all all al	New Account Name N/A N/A	Time 12.24.02PM 12.24.02PM 12.24.02PM 12.24.02PM 12.25TM 12.25TM 12.25TM 12.25TM 12.25TM 12.35TM 12.35TM 12.35TM 12.35TM 12.35TM 12.325TM 32.250TM 31.552TM 31.5	Date 8/16/2026 8/16/2026 9/16/2026 9/16/2026 9/16/2026 9/16/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/14/2026 8/16/

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

- 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

		Comp	uter account management operatio	ns distribution		
	0 →	Computer account detieted Computer account created	Computer zoro dutoped	ter account changed 66.7% for account created 25.0% fer account diated 9.3% 100.0%		
Com	puter account creat The report shows the cr computer has joined a	ted omputer accounts which were of domain	created. The report is based on the "compute	r account created" event which usually signa	is the fact that a	
	Jser Name	Computer Name	Account created	Caller account	Time	Date
NT AUTHORITY VAN	DNYMOUS LOGON	FSERVER	GFITEMAS OF TVF SER VER\$	GFITEMAS OFT\FSERVER\$	3:07:49PM	9/16/200
GFITBMASOFTcalin		FSERVER	GFITEMAS OFT\CALDEV4	GFITEMAS OF Trealin	2:13:59PM	6/27/200
GETEMASUETVAdmi	histrator	FSERVER	GFTTEMAS OF Teasting.15%	GF ITEMAS OF Tradministrator	11:12:02PM	6/2//200
(i)	The report shows the cl performed by the admir	nanges performed on the comp instrator on the computer accou	outer accounts. The report is based on the "co ints. These include resetting the account, ena	omputer account changed" event which show bling/disabling the account, etc.	vs changes	Orto
	user name	Computer Name	Account changed	Caller account	Time	Date
NT AUTHORITY\SY:	JTBM	FSERVER	GFITEMAS OF THE SERVERS	GFITEMASOFTYFSERVER\$	1:28:12PM	0.000.000
NOT AN TRADUCTION AND	1154	FSERVER	OF ITEMMS OF THE SERVERS	OF ITEMAS OF THE SERVERS	0.00.40704	W20/20
NT AUTHORITY\SY:		E SERVER	OF ITEMAS OF TACAL DEVE	OF IT PAGE OF The align	2:03:48PM 2:13:50PM	9/20/20
NT AUTHORITY\SY: OFITEMASOFTicalin OFITEMASOFTicalin		FSERVER	OF ITEMAS OF T\CALDEV\$ GEITEMAS OF T\CALDEV\$	OF ITEMAS OF Trealin GEITEMAS OF Trealin	2:03:48PM 2:13:59PM 2:13:59PM	9/20/20 9/20/20 6/27/20 6/27/20
OFITEMASOFTvain GFITEMASOFTvain GFITEMASOFTvain GFITEMASOFTVain	nistrator	FSERVER FSERVER FSERVER	OF ITEMAS OF TIC ALD EV& OF ITEMAS OF TIC ALD EV& OF ITEMAS OF Titesting 1:5	OF ITEMAS OF Trealin OF ITEMAS OF Trealin OF ITEMAS OF Trealin	2:03:48PM 2:13:59PM 2:13:59PM 11:12:02PM	9/20/20 9/20/20 6/27/20 6/27/20 6/27/20
oFITEMASOFTxalin GFITEMASOFTxalin GFITEMASOFTxalin GFITEMASOFTXAlmi OFITEMASOFTXAlmi	nistrator	FSERVER FSERVER FSERVER FSERVER	OFITEMASOFTICALDEV GFITEMASOFTICALDEV GFITEMASOFTRessing.ts OFITEMASOFTRessing.ts	OF ITEMAS OF Treatin GF ITEMAS OF Treatin GF ITEMAS OF TrAdministrator OF ITEMAS OF TrAdministrator	2:03:48PM 2:13:59PM 2:13:59PM 11:12:02PM 11:12:40PM	6/27/20 6/27/20 6/27/20 6/27/20 6/27/20
NT AUTHORITY'SY: OFITEMASOFTicalin GFITEMASOFTicalin GFITEMASOFTIAdmi OFITEMASOFTIAdmi NT AUTHORITY'SY:	nistrator histrator iTEM	FSERVER FSERVER FSERVER FSERVER FSERVER	OF ITEMAS OF THE ALD EVE OF ITEMAS OF THE ALD EVE OF ITEMAS OF The sting 1:5 OF ITEMAS OF The sting 1:5 OF ITEMAS OF THE SERVER\$	OF ITEMAS OF Trealin OF ITEMAS OF Trealin OF ITEMAS OF TVAdministrator OF ITEMAS OF TVAdministrator OF ITEMAS OF TV5 SERVER\$	2:03:48PM 2:13:59PM 2:13:59PM 11:12:02PM 11:12:02PM 7:11:14PM	9/20/20 9/20/20 6/27/20 6/27/20 6/27/20 6/27/20 7/6/20
NT AUTHORITY(SY) OFITEMASOFTicalin OFITEMASOFTicalin OFITEMASOFTicalin OFITEMASOFTICAlmin NT AUTHORITY(SY) NT AUTHORITY(N)	nistrator nistrator STEM JNYMOUS LOGON	FSERVER FSERVER FSERVER FSERVER FSERVER	OFTEMASOFTICALDEVS OFTEMASOFTICALDEVS OFTEMASOFTICALDEVS OFTEMASOFTICALDEVS OFTEMASOFTICALS OFTEMASOFTICSERVERS	OFTIEMASOFT-calin GFTIEMASOFT-Valministrator OFTIEMASOFT-Valministrator OFTIEMASOFT-Valministrator OFTIEMASOFT-F\$SERVER\$ OFTIEMASOFT-F\$SERVER\$	2:03:49PM 2:13:59PM 11:12:02PM 11:12:02PM 11:12:40PM 7:11:14PM 9:45:04PM	9/20/20 9/20/20 6/27/20 6/27/20 6/27/20 6/27/20 8/26/20 8/16/20
NT AUTHORITYSY OFTEDAGOTTVAIN OFTEDAGOTTVAIN OFTEDAGOTTVAIN OFTEDAGOTTVAIN NT AUTHORITYSYS NT AUTHORITYSYS NT AUTHORITYSYS	Nistrator Nistrator STEM DIAYMOUS LOGON puter account delet) The report shows the cr computer was removed	FSERVER FSERVER FSERVER FSERVER FSERVER FSERVER ted omputer accounts which were of from a domain.	ormawsorncADBW ormawsorncADBW ormawsornempus ormawsornempus ormawsornesewers ormawsornesewers deleted. The report is based on the " compute	OFTBA4007Nuin OFTBA4007Nuininitator OFTBA4007Nuininitator OFTBA4007NSeininitator OFTBA4007NSERVERS OFTBA4007NSERVERS account deleted" events which usually sign	2:03:48PM 2:15:39PM 2:15:39PM 11:12:02PM 11:12:02PM 7:11:14PM 9:45:04PM	9/20/20 9/27/20 6/27/20 6/27/20 6/27/20 9/27/20 9/27/20 8/16/20
NT AUTHORITYSY: ОГГЕМАЗОГРазія ОГГЕМАЗОГРАЗІЯ ОГГЕМАЗОГРАЗІЯ ОГГЕМАЗОГРАЗІЯ NT AUTHORITYSY: NT AUTHORITYSY: Com	Netrator Nitrator STEM DIVINIOUS LOGON puter account dele) The report shows the cr computer was removed	FSERVER FSERVER FSERVER FSERVER FSERVER FSERVER Ed omputer accounts which were of thom a domain.	orrmawornce.dbr4 orrmawornce.dbr4 orrmawornce.br4 orrmaworns us orrmaworns servers orrmaworns servers orrmaworns servers deleted. The report is based on the " compute	OFTIMANOT Frain OFTIMANOT Frain OFTIMANOT Frain OFTIMANOT Frain OFTIMANOT Frain Activity of the second oftimanot frain services of the second oftimanot frain services of the second	2:03-497M 2:13:59PM 2:13:59PM 11:12:02PM 11:12:02PM 7:11:14PM 9:45:04PM	0/20/20 9/20/20 9/27/20 6/27/20 6/27/20 6/27/20 8/16/200
ит алтновитичи ог пракотрана ог пракотрана ог пракотрана ог пракотрана ит алтновитичи ит алтновитичи ог от объеко ог пракотрана ог пракотрана ог от объеко от объеко объеко от объеко об	Nistator Nistator STBA DNYMOUS LOGON puter account delet) The report shows the c computer was removed Joser Name	FSERVER FSERVER FSERVER FSERVER FSERVER Exerver ted omputer accounts which were of thom a domain.	orrmawornck.dbvA orrmawornck.dbvA orrmawornck.btvA orrmaworne.sts orrmaworne.sts orrmaworne.steves seleted. The report is based on the " compute sector of count deleted	OFTITMANOT Fruin OFTITMANOT Fruin OFTITMANOT Previolations OFTITMANOT Previolations oftitmanot previolation oftitmanot previolation oftitmanot previolation oftitmanot previolation of the second Optimized Constitution Optimized Constitution Optimized Constitution Optimized Constitution Optimized Constitution Optimized Constitution Optimized Constitution	2:03-497M 2:15:397M 11:12:407M 11:12:407M 7:11:147M 9:45:347M hal the fact that a	0/20/20 9/20/20 9/27/20 6/27/20 6/27/20 6/27/20 8/16/20 8/16/20 Date

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

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

Password changes



Change password attempts

The section shows password change attempts based on the 527 event. Compare the user trying to change the password with the Target Account Name to determine whether the account owner or someone else attempted to change the password. If the user trying to change the password does not equal the Target Account Name, someone other than the account owner tried to change the password. Check if the user trying to change the password is authorized to perform password changes. The failed attempts to change passwords are very important for security monitoring and may signal intruders trying to compromise user accounts. Therefore they are highlighted in light red in the report.

User trying to change password	Computer	Attempt	Target account	Time	Date
NT AUTHORITYANONYMOUS LOGON	FSERVER	Audit failure	calin	12:34:04PM	6/27/2006
NT AUTHORITYANONYMOUS LOGON	FSERVER	Audit failure	calin	12:34:14PM	6/27/2006
NT AUTHORITYANONYMOUS LOGON	FSERVER	Audit failure	calin	12:34:20PM	6/27/2006
NT AUTHORITYANONYMOUS LOGON	FSERVER	Audit success	calin	12:34:36PM	6/27/2006
GFITEMASOFTicalin	FSERVER	Audit failure	calin	1:56:17AM	7/25/2006
OFITEMASOFTicalin	FSERVER	Audit failure	calin	1:57:42AM	7/25/2006

User account password set or reset

The section, based on the 628 event, shows when a user or process resets an account password through an administrative interface such as Active Directory Users and Computers, rather than through a password change process. Only authorized people or processes should carry out this process, such as help desk or user self-service password reset.

User trying to change password	Computer	Attempt	Target account	Time	Date
GFITEMASOFT\Administrator	FSERVER	Audit success	calin	11:54:51AM	6/27/2006
GFITEMASOFT\calin	FSERVER	Audit success	calin	12:32:54PM	6/27/2006
GFITEMASOFTIcalin	FSERVER	Audit success	pisu	1:29:19PM	6/27/2006
GFITEMASOFTIcalin	FSERVER	Audit success	gfitest1	1:32:13PM	6/27/2006
GFITEMASOFTicalin	FSERVER	Audit success	CALDEVS	2:13:59PM	6/27/2006
GFITEMASOFTAdministrator	FSERVER	Audit success	testing.ts\$	11:12:02PM	6/27/2006
GFITEMASOFTAdministrator	FSERVER	Audit success	testing.ts\$	11:12:40PM	6/27/2006
TESTING0(TESTSTATION\$	TESTSTATION	Audit success	vmware_user	12:02:37PM	8/16/2005
TESTING0/TESTSTATION\$	TESTSTATION	Audit success	ymware_user	12:12:10PM	8/16/2005
TESTING@TESTSTATION\$	TESTSTATION	Audit success	vmware_user	11:26:25AM	9/9/2005
TESTING@TESTSTATION\$	TESTSTATION	Audit success	vmware_user	12:24:23PM	9/10/2005

Changes to dir. serv. restore mode passwords

The section, based on the 696 event, shows when someone attempts to change the Directory Services Restore Mode password on a domain controllier. Check Bource Machine and the user performing the attempt and investigate immediately.

-	User trying to change password	Computer	Attempt	Source machine	Time	Date
4 →	GFITEMASOFT\calin	FSERVER	Audit success	FSERVER	1:15:46PM	6/27/2006

Screenshot 55 - Sample report showing password changes

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

Use this report to:

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

Security group management



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

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



Security Enabled Universal Group changes

The section is based on events from 669 to 662. Examine for groups that have high privilege levels, such as Enterprise Admins or Scherna Admins, to ensure that no changes take place outside policy constraints.

	User parforming operation	Computer Name	Attempt	Changed group	Operation	Time	Date
	GFITEMASOFT\Administrator	FSERVER	Audit success	Enterprise Admins	Group created	3:17:56PM	9/16/2005
	GFITEMASOFT/Administrator	FSERVER	Audit success	Schema Admins	Group created	3:17:56PM	9/16/2005
	GFITEMASOFTVFSERVER\$	FSERVER.	Audit success	Sohema Admins	Group created	3:22:58PM	9/16/2005
	GFITEMASOFTVFSERVER\$	F SERVER	Audit success	Enterprise Admins	Group created	3:22:59PM	9/16/2005
•	GFITEMASOFT/calin	FSERVER	Audit success	GfiUtestGr	Group created	1:32:45PM	6/27/2006
7	GFITEM4S0FT/calin	FSERVER	Audit success	OfiUtest Gr	Member added: CN=gfitest1,CN=Users,DC=GfiTemasoft,DC=ro	1:32:45PM	6/27/2006
	GFITEMASOFTicalin	FSERVER	Audit success	GfiUtestGr	Group created	1:32:49PM	6/27/2006
	GFITEMASOFTicatin	FSERVER	Audit success	GfiUtestGr	Member removed: CN+gfitest1,CN+Users,DC+GfiTemasoft,DC+ro	1:32:49PM	6/27/2006
	GFITEMASOFTicalin	FSERVER	Audit success	GfiUtestGr	Group created	1:33:02PM	6/27/2006
	GFITBMASOFT/calin	FSERVER	Audit success	GfiUtestGr	Group deleted	1:33:08PM	6/27/2006

Security enabled group type changes

The section is based on the 668 event. It indicates changes to the group type. You should examine these events for groups that have high privilege levels to make sure that no changes take place outside policy constraints.

-	User parforming operation	Computer Name	Attempt	Changed group	Operation	Time	Date
	GFITEMASOFTVAdministrator	FSERVER	Audit success	Sohema Admins	Group type changed	3:17:56PM	9/16/200
	GFITEMASOFT/Administrator	FSERVER	Audit success	Enterprise Admins	Group type changed	3:17:56 PM	9/16/200
	GFITEMASOFT/calin	FSERVER	Audit success	test1	Group type changed	1:34:16PM	6/27/200

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

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

- 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

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

Local audit policy changes

		iv Ti as	he following report may co ssigned to an account. Be ne meaning of each privile	ontain information abou low you have a legend ge.	It the privileges which explains		
		Pr	ivilege value	Short description			
2→	Computer name: FS	So So So So So So So So So So So So So S	Tc-DPrivilege MachineAccountPrivilege BackupPrivilege BackupPrivilege CreatePageliePrivilege CreatePageliePrivilege CreateGabalPrivilege CreateGabalPrivilege DebugPrivilege BacmoteShutdownPrivilege BacmoteShutdownPrivilege SystemErvironmentPrivilege SystemErvironmentPrivilege SystemProfilePrivilege SystemProfilePrivilege TancOmmervirolege TancOmmervirolege TancOmmervirolege SystemProfilePrivilege Networkl.egenRight BatchLegenRight SarviceLegenRight	Act as part of the operation Add workstation to domain Adjust memory quotas for Backup files and directori Change the system time Create a pola objects Create global objects Cr	g system n a process es objects uthentication trivers lables unce tasks ce vice data nd folders the network		
	User Name	By User	Event Desc	ription	Privilege	Time	Date
	NT AUTHORITY'SYSTEM	WORKGROUP/FSERVER\$	Local audit policy changed	N/A		3:02:05PM	9/16/2005
	NT AUTHORITY'SYSTEM	WORKGROUP/FSERVER\$	Local audit policy changed	N/A		3:02:05PM	9/16/2005
	NT AUTHORITY'SYSTEM	N/A	Domain audit policy changed			3:09:24PM	9/16/2005
_ (3) →	NT AUTHORITY'SYSTEM	N/A	Domain audit policy changed			3:14:33PM	9/16/2005
-	GFITEMASOFTVAdministrator	N/A	Domain audit policy changed	-		3:17:56PM	9/16/2005
	NT AUTHORITY'SYSTEM	N/A	Domain audit policy changed			4:39:35PM	9/16/2005
	NT AUTHORITY'SYSTEM	GFITEMASOFT/FSERVER\$	Local audit policy changed	N/A		11:54:14AM	6/27/2006
	NT AUTHORITY'SYSTEM	N/A.	Domain audit policy changed	-		2:24:58PM	6/27/2006

Screenshot 59 - Sample report showing Local audit policy changes

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

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

User right assignment changes

t Selfa Seba Seba Secritical Secriti	Privilege chineAccountPrivilege exexpPrivilege termtimePrivilege atePagefilePrivilege ate Generativilege ate Generativilege ateGenerativilege ateGenerativilege ateGenerativilege ateGenerativilege ateGenerativilege attivePrivilege temErvilege temPrivilege cAgentPrivilege cAgentPrivilege cAgentPrivilege cAgentPrivilege cAgentPrivilege cortershipPrivilege conceshipPrivilege tortershipPrivilege	Act as part of th Add workstatio Adjust memory Backup files an Create anage Create a page Create a token Create perman Debug progran Bestore perman Debug progran Bestore perman Manage audit I Modify environ Perform volum Profile system Restore files or Synchronize di Take ownershi Access this con	ne operating system n to domain quotas for a process d directories tem time ille object bjects ent shared objects is system remotely client after authenticat ad device drivers ogs mental variables e maintenance tasks performance folders rectory service data	tion
	chLogonRight viceLogonRight rractiveLogonRight	Logon as batch Logon as servio Logon locally	p of files and folders nputer from the networ i job ce	rk
Computer name: FSERVER				
Assigned to GFITEMASOFTIWAM_FSERVER GFITEMASOF	By User Nadministrator F	Event Description Privilege assigned to user acco	n Privilege unt N/A	Tir 2
GFITEMASOFT/IWAM_FSERVER GFITEMASOF	Nadministrator F	Privilege assigned to user acco	unt N/A	2

 GPTEEMASOFTWAALFSERVER
 OPTEWASOFTwidministrator
 Philipge assigned to user account
 N/A
 2.61.46PM
 5/102005

 GPTEMASOFTWAALFSERVER
 OPTEWASOFTwidministrator
 Philipge assigned to user account
 N/A
 2.61.46PM
 5/102005

 GPTEMASOFTWAALFSERVER
 OPTEWASOFTwidministrator
 Philipge assigned to user account
 N/A
 2.61.46PM
 5/102005

 GPTEMASOFTIVALFSERVERS
 Philipge assigned to user account
 N/A
 2.61.46PM
 6/102005

 GPTEMASOFTipiu
 OPTEWASOFTISERVERS
 Philipge assigned to user account
 N/A
 1.49.26PM
 6/272005

 GPTEMASOFTipisu
 OPTEWASOFTISERVERS
 Philipge aremoved for user account
 N/A
 11.40.10PM
 6/272005

Screenshot 60 - Sample report showing user right assignment changes

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

Use this report to:

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

Date

System access granted / removed

\mathbf{U}	Computer name, FSERVER					
	Account modified	By User	Event Description	Privilege	Time	Date
	GFITEMASOFTIcalin	GFITEMASOFT\calin	System Access was granted to account	N/A	2:10:38PM	9/20/2005
	GFITEMASOFT/JUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:61:27PM	5/10/2008
2→	GFITEMASOFT/JUSR_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:28PM	5/10/2008
	GFITEMASOFT\WAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:42PM	5/10/2008
-	GFITEMASOFT/IWAM_FSERVER	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:51:43PM	5/10/2008
	GFITEMASOFT'IIS_WPG	GFITEMASOFT\administrator	System Access was granted to account	N/A	2:61:55PM	5/10/2006
	GFITEMASOFT/JUSR_FSERVER	GFITEMASOFT\FSERVER\$	System Access was granted to account	N/A	3:13:31PM	5/10/2008
	GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was granted to account	N/A	1:49:29PM	6/27/2006
	GFITEMASOFTIcalin	GFITEMASOFT\FSERVER\$	System Access was granted to account	N/A	2:31:50PM	6/27/2006
	GFITEMASOFT\pisu	GFITEMASOFT\FSERVER\$	System Access was removed for account	N/A	11:45:14PM	6/27/2008

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

0→	Computer name: FSERVE	2							
•	User Name	By User	Event Description	Privilege	Time	Date			
2→	NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Encrypted data recovery policy changed	N/A	3:00:30PM	9/16/2005			
Screenshot 62 - Sample report showing Encrypted Data Recovery policy									
1	Computer nar	ne							

List of encrypted data recovery policy events, grouped by computer

Use this report to:

2

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

IPsec policy changes

0 →	Computer name: CALDEV					
	User Name	By User	Event Description	Privilege	Time	Date
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:13PM	9/11/2008
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:13PM	9/11/2008
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:13PM	9/11/2008
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:32PM	9/11/2008
$2 \rightarrow$	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:44PM	9/11/2008
-	NT AUTHORITY'NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:44PM	9/11/2008
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:46PM	9/11/2008
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:46PM	9/11/2008
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:46PM	9/11/2006
	NT AUTHORITY/NETWORK SERVICE	N/A	IPSec pol. ag. serv.: Using the AD Storage policy.	N/A	12:10:49PM	9/11/2008

Screenshot 63 - Sample report showing IPsec policy changes

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

Use this report to:

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

Kerberos policy changes

0→	Computer name: FSERVER										
		User Name	By User	Event Description	Time	Date					
	$0 \rightarrow$	NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Kerberos policy changed	9:58:26PM	9/8/2006					
	• •	NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Kerberos policy changed	9:58:26PM	9/12/2006					
		NT AUTHORITY\SYSTEM	GFITEMASOFT\FSERVER\$	Kerberos policy changed	9:58:26PM	9/13/2006					

Screenshot 64 - Sample report showing Kerberos policy changes

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

- 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



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.

Computer User Event ID Description Object Name Object Type Time Date 11:42:17PM 6/27/20 GFITEMASOFT\Administrator REGISTRY/MACHINE/SYSTEM/CA Key INEUGI RY MACHINES YS EMICONTROLSEU I Services Eventogi Security IREGISTRY/MACHINE/SYSTEM/ControlSet001/Services/ Eventogi Security IREGISTRY/MACHINE/SYSTEM/ControlSet001/Services/ FSERVER GFITEMASOFT\Administrator 560 Object Open Key 11:44:37PM FSERVER GFITEMASOFT\calin 560 Object Open Key 12:00:11AM 6/28/2006 Eventiog\Security \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\ Evention\Security FSERVER GFITEMASOFT\calin 580 Object Open 12:01:07AM 8/28/2006 Eventiog/Security US > 1 EMIControlSet001/Services/ IREGISTRY1MACHINE/SYSTEM/ControlSet001/Services/ Eventiog/Security C:StyleSheets C:dot are FSERVER GFITEMASOFT\calin 550 Object Open Key 12:01:18AM 6/28/2006 GFITEMASOFT\calin GFITEMASOFT\calin FSERVER 560 Object Open File File 12-00-54AM Object Open Object Open FSERVER GFITEMASOFT\calin GFITEMASOFT\calin C:\dot.exe C:\dot.exe File 12:09:54AM C:\dot.exe File Key 12:12:21AM 12:47:40AM GFITEMASOFTicalin 560 Object Open GFITEMASOFTiAdministrator 560 Object Open FSERVER FSERVER GFITEMASOFT\Administrator 580 Object Open 8:37:17PM -> FSERVER GFITEMASOFT\Administrator 560 Object Open 10:12:35PM 7/2/2006 FSERVER GFITEMASOFT\Administrator 560 Object Open HINE\SYSTEM\ControlSet001\Services\ Key 8:16:37PM Eventlog/Security IREGISTRY/MACHINE\SYSTEM/ControlSet001\Services\ Key FSERVER GFITEMASOFT\Administrator 560 Object Open 10:45:18PM 7/25/2006 Eventlog\Security REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\ Key FSERVER GFITEMASOFT\Administrator 560 Object Open entlog/Security GISTRY/MACHINE/SYSTEM/ControlSet001/Services/ Key FSERVER GFITEMASOFT\Administrator 560 Object Open 11:56:49PM 7/27/2008 Eventlog\Security REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\ FSERVER GFITEMASOFT\Administrator 560 Object Open Key entlogiSecurity EGISTRY\MACHINE\SYSTEM\ControlSet001\Services\ Key FSERVER GFITEMASOFT\Administrator 560 Object Open 1:25:38AM 8/18/2006 ntlog/Security 319TEV/MACHINE/SYSTEM/ControlSet001/Services/ FSERVER GFITEMASOFT\Administrator 560 Object Open Kev 10:47:43PM 8/23/2006 FSERVER GFITEMASOFT\Administrator 550 Object Open GISTRYMA HINE\SYSTEM\ControlSet001\Services\ Key 10:47:43PM FSERVER GFITEMASOFT\Administrator 560 Object Open HINE\SYSTEM\ControlSet001\Services\ Key 1:23:17AM 8/24/2008 FSERVER GFITEMASOFT/Administrator 560 Object Open Key 1:16:22AM NE\SYSTEM\ControlSet001\Services\ FSERVER GFITEMASOFT\Administrator 560 Object Open Key 3:22:26AM 8/26/2006 INE\SYSTEM\ControlSet001\Services\ FSERVER GFITEMASOFT\Administrator 560 Object Open NE\SYSTEM\ControlSet001\Services\ Key 0:28:59AM 8/26/200

Successful attempts to access files and registry

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



Use this report to:

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

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

Object deleted

	Computer	User	Event ID	Description	Object Name	Object Type	Time	Date
	TESTSTATION	TESTSTATION\Administrator	564	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
	TESTSTATION	TESTSTATION\Administrator	584	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
	TESTSTATION	TESTSTATION\Administrator	584	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
	TESTSTATION	TESTSTATION\Administrator	584	Object Deleted	N/A	N/A	12:58:51PM	8/16/2005
	FSERVER	GFITEMASOFTicalin	504	Object Deleted	N/A	N/A	2:32:10PM	6/27/2006
	FSERVER	GFITEMASOFTicalin	584	Object Deleted	N/A	N/A.	2:34:08PM	6/27/2006
	FSERVER	GFITEMASOFTIcalin	584	Object Deleted	N/A	N/A	2:43:32PM	6/27/2006
$\mathbf{n} \rightarrow$	FSERVER	GFITEMASOFTIcalin	564	Object Deleted	N/A	N/A	2:45:01PM	6/27/2006
•	FSERVER	GFITEMASOFTicalin	504	Object Deleted	N/A	N/A	7:24:05PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	584	Object Deleted	N/A	N/A.	7:24:08PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	584	Object Deleted	N/A	N/A	7:24:08PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	564	Object Deleted	N/A	N/A	7:24:08PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	504	Object Deleted	N/A	N/A	7:24:08PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	584	Object Deleted	N/A	N/A.	7:24:08PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
	FSERVER	GFITEMASOFTIcalin	584	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
	FSERVER	GFITEMASOFT/calin	584	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	504	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
	FSERVER	GFITEMASOFTicalin	564	Object Deleted	N/A	N/A	7:24:48PM	7/6/2006
	FSERVER	GFITEMASOFT\calin	584	Object Deleted	N/A	N/A.	7:24:48PM	7/6/2006

Screenshot 67 - Sample report showing Objects deleted

List of events showing attempted and successful object deletions

Use this report to:

1

- 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

Applicatio	ons successfully inst	alled				
Computer	llser	Description	Event ID	Source	Time	Date
CALDEV	N/A	(1): Product My Application- Installation operation	11707	Msilnstaller	12:52:12PM	9/11/
CALDEV	N/A	 (1): Product My Application2 Installation operation 	11707	Msilnstaller	12:52:31PM	9/11
CALDEV	N/A.	(2): Product My Application2 Installation operation completed successfulls.	11707	Msilnstaller	12:52:31PM	9/11
CALDEV	N/A	(3): Product My Application - Installation operation completed successfulls.	11707	Msilnstaller	12:52:31PM	9/1
Applicatio	ons successfully uni	nstalled				
Computer	User	Description	Event ID	Source	Time	Date
CALDEV	N/A	(1): Product MyApp4 Removal completed successfully.	11724	Msilnstaller	12:53:37PM	9/1
CALDEV	N/A	(2): Product MyApp4 Removal completed successfully.	11724	Msilnstaller	12:53:37PM	9/1
CALDEV	N/A	(3): Product MyApp4 Removal completed successfully.	11724	Msilnstaller	12:53:37PM	9/1
CALDEV	N/A	(4): Product MyApp4 Removal completed successfully.	11724	Msilnstaller	12:53:37PM	9/1
CALDEV	N/A	(5): Product MyApp4 Removal completed successfully.	11724	Msilnstaller	12:53:37PM	9/1
Computer	Uror	Description	Event ID	Source	Time	Dest
CALDEV	N/A	(1): MyApp2 Installation operation failed.	11708	Msilnstaller	12:53:11PM	9/1
CALDEV	N/A	(2): MyApp2 Installation operation failed.	11708	Msilnstaller	12:53:11PM	9/1
CALDEV	N/A	(3): MyApp2 Installation operation failed.	11708	Msilnstaller	12:53:11PM	9/1
CALDEV	N/A	(4): MyApp2 Installation operation failed.	11708	Msilnstaller	12:53:11PM	9/1
CALDEV	N/A	(5): MyApp2 Installation operation failed.	11708	Msilnstaller	12:53:11PM	9/1
Applicatio	ns which failed to ur	ninstall				
Computer	User	Description	Event ID) Source	Time	Dat
CALDEV	N/A	(1): My App6 uninstall failed.	11725	Msilnstaller	12:54:13PM	9/1
CALDEV	N/A	(2): My App6 uninstall failed.	11725	Msilnstaller	12:54:13PM	9/1
CALDEV	N/A	(3): My App6 uninstall failed.	11725	Msilnstaller	12:54:13PM	9/1
CALDEV	N/A	(4): My App6 uninstall failed.	11725	Msilnstaller	12:54:13PM	9/1
CALDEV	N/A	(5): My App6 uninstall failed.	11725	Msilnstaller	12:54:13PM	9/1

Applications installed/removed

Screenshot 68 - Sample report showing Applications installed /removed

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

Use this report to:

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

Applications crashing or hanging

Computer		User	Description	Event I	D Source	Time	Date
CALDEV	N/A		Faulting application (1): My App, version(1): My	1000	Application Error	12:55:48PM	9/11/2
CALDEV	N/A		Faulting application (2): My App, version(2): My	1000	Application Error	12:55:46PM	9/11/2
CALDEV	N/A		App, faulting module(2): My App, version(2): My Faulting application (3): My App, version(3): My App, faulting module(3): My App, version(3): My	1000	Application Error	12:55:46PM	9/11/2
CALDEV	N/A		Faulting application (4): My App, version(4): My	1000	Application Error	12:55:46PM	9/11/2
CALDEV	N/A		Faulting application (5): My App, version(5): My App, faulting module(5): My App, version(5): My	1000	Application Error	12:55:46PM	9/11/
Applica	tions which	hanged					
Computer		User	Description	Event	ID Source	Time	Date
CALDEV	N/A		Hanging application(1): My App, version(1): My	1002	Application Hang	12:56:09PM	9/11/
CALDEV	N/A		App, nang module(1): My App, version(1): My App, Hanging application(2): My App, version(2): My	1002	Application Hang	12:56:09PM	9/11
CALDEV	N/A		App, hang module(2): My App, version(2): My App, Hanging application(3): My App, version(3): My App, hang module(3): My App, version(3): My App	1002	Application Hang	12:56:09PM	9/11
CALDEV	N/A		Hanging application (4): My App, version (4): My	1002	Application Hang	12:56:09PM	9/11
CALDEV	N/A		Hanging application(6): My App, version(6): My App, hang module(5): My App, version(5): My App,	1002	Application Hang	12:56:09PM	9/11
DrWats	on events						
Computer		User	Description	Event I	D Source	Time	Date
CALDEV	N/A		The application,(1): My App, generated an application emor	4097	DriWatson	12:56:21PM	9/11/
CALDEV	N/A		The application (2): My App, generated an application error	4097	Driwatson	12:56:21PM	9/11/
CALDEV	N/A		The application (3): My App, generated an application (3): My App, generated an	4097	DriWatson	12:56:21PM	9/11/
CALDEV	N/A		The application, (4): My App, generated an application error	4097	Driwatson	12:56:21PM	9/11/
			approximent case				

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

Use this report to:

• Identify all faulty applications, including critical applications

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

Print Server Reports

Print activities

	Printing act	vity					
	Computer	User	Description	Event ID	Source	Time	Date
	CALDEV	N/A	Printer (1): testwas created.	2	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer (2): testwas oreated.	2	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer (3): testwas created.	2	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer(4): testwas deleted.	3	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer(5): testwas deleted.	3	Print	1:46:27PM	9/11/2006
$ \rightarrow $	CALDEV	N/A	Printer(6): testwas deleted.	3	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer(7): test is pending deletion.	4	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer(8): test is pending deletion.	4	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer(9): test is pending deletion.	4	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer (10): testwas paused.	6	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer (11): testwas paused.	6	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer (12): testwas paused.	6	Print	1:46:27PM	9/11/2006
	CALDEV	N/A	Printer (13): testwas resumed.	7	Print	1:48:27PM	9/11/2006

Screenshot 70 - Sample report showing Print activities

List of events showing printing activity

Use this report to:

1

- 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 f	ull							
	Computer		User	Description	Event I	D	Source	Time	Date
	CALDEV	N/A		The (1): test log file is full.	6000	eventiog		1:47:05PM	9/11/2006
	CALDEV	N/A		The (2): test log file is full.	6000	eventiog		1:47:05PM	9/11/2008
•	CALDEV	N/A		The (3): test log file is full.	6000	eventiog		1:47:05PM	9/11/2006
()→	CALDEV	N/A		The (1): application log file is full.	6000	eventiog		1:54:21PM	9/11/2008
	CALDEV	N/A		The (2): application log file is full.	6000	eventlog		1:54:21PM	9/11/2006
	CALDEV	N/A		The (3): application log file is full.	6000	eventiog		1:54:21PM	9/11/2006
	CALDEV	N/A		The (1): system log file is full.	6000	eventiog		1:54:24PM	9/11/2006
	CALDEV	N/A		The (2): system log file is full.	6000	eventiog		1:54:24PM	9/11/2006
	CALDEV	N/A		The (3): system log file is full.	6000	eventiog		1:54:24PM	9/11/2006
	Event log se	ervice sta	arted						
	Computer		User	Description	Event I	D	Source	Time	Date
•	CALDEV	N/A		The Event log service was started.	6005	eventiog		1:47:05PM	9/11/2006
U →	CALDEV	N/A		The Event log service was started.	6005	eventiog		1:47:05PM	9/11/2006
	CALDEV	N/A.		The Event log service was started.	6005	eventiog		1:47:05PM	9/11/2006
	Event Log s	ervice st	topped						
	Computer		User	Description	Event I	D	Source	Time	Date
•	CALDEV	N/A		The Eventlog service was stopped.	6006	eventlog		1:47:05PM	9/11/2006
⊌ →	CALDEV	N/A		The Eventlog service was stopped.	6006	eventlog		1:47:05PM	9/11/2006
	CALDEV	N/A		The Eventlog service was stopped.	6006	eventlog		1:47:05PM	9/11/2006
	Log file cor	rupt							
	Computer		User	Description	Event	ID	Source	Time	Date
•	CALDEV	N/A		The (4): test log file is corrupted and will be cleared.	6002	eventiog		1:47:05PM	9/11/2006
4)→	CALDEV	N/A		The (5): test log file is corrupted and will be cleared.	6002	eventiog		1:47:05PM	9/11/2006
	CALDEV	N/A		The (6): test log file is corrupted and will be cleared.	6002	eventiog		1:47:05PM	9/11/2006
	Unovnoctor	devetor	shutdown						
	Unexpected	u system	Shutuovin						
	Computer	u system	User	Description	Event	D	Source	Time	Date
•	Computer	N/A	User	Description The previous system shutdown at(13): test on (13): test was unexpected	Event 6008	eventlog	Source	Time 1:47:05PM	Date 9/11/2006
6→	Computer CALDEV CALDEV	N/A N/A	User	Description The previous system shutdown at(13): test on(13): test was unexpected The previous system shutdown at(14): test on(14): test was unexpected.	Event 6008 6008	eventlog eventlog	Source	Time 1:47:05PM 1:47:05PM	Date 9/11/2006 9/11/2008

Screenshot 71 - Sample report showing Event Log health

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

Use this report to:

• Identify failures in the auditing process

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

Event Log cleared

	Computer	User name	Caller user name	Time	Date				
\mathbf{U}	FSERVER	NT AUTHORITY\SYSTEM	GFITEMASOFT\Administrator	9:55:57PM	9/13/2006				
Screenshot 72 - Sample report showing Event Log cleared									
1	List of events gene	rated when the event	log is cleared						

Use this report to:

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

Event Log service errors

	Computer	User	Description	Event ID	Source	Time	Date				
•	CALDEV	N/A	A driver packet received from the I/O subsystem was	6004	eventiog	1:56:57PM	9/11/2006				
0 →	CALDEV	N/A	invalid The data is the A driver packet received from the I/O subsystem was	6004	eventlog	1:56:57PM	9/11/2006				
	CALDEV	N/A	A driver packet received from the I/O subsystem was invalid. The data is the	6004	eventlog	1:56:57PM	9/11/2006				
Scree	Screenshot 73 - Sample showing Event Log service errors										
1	List of events showing event log service errors.										

Use this report to:

• Identify errors occurring in the auditing process.

Network Resouce Access Reports (PCI requirement 10)

All individual access to cardholder data

	User Identification	Type of event	Date a	ndtime	Success or Failure indication	Origination of	Identity or name of affected	Description
0→	GFITEMASOFTvcalin	Object Access	12:09:54 am	09/25/2006	Audit success	FSERMER	C:\cardholder	Object Open
	GFITEMASOFTvcalin	Object Access	12:09:54 am	09/25/2006	Audit success	FSERMER	C:\cardholder	Object Open
	GFITEMASOFTvcalin	Object Access	12:09:54 am	09/25/2006	Audit success	FSERVER	C:\cardholder	Object Open
		·						· ·

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

List of users who accessed cardholder data

Use this report to:

2

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

All actions taken by any individual with root or administrative privileges

	User Identification	Type of event	Date a	ndtime	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
0→	Administrator	Account Management	12:18:13 am	08/21/2006	Audit success	FSERMER	See the description field	User Account Locked Out (N/A)
	Administrator	Account Logon	12:31:46 am	08/21/2006	Audit success	FSERMER	See the description field	Authentication Ticket Granted
	Administrator	Object Access	12:47:40 am	08/21/2006	Audit success	FSERMER	See the description field	Object Open
	Administrator	Object Access	12:56:25 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
	Administrator	Object Access	1:16:22 am	08/21/2006	Audit success	FSERVER	See the description field	Object Open
	Administrator	Object Access	1:23:17 am	08/21/2006	Audit success	FSERMER	See the description field	Object Open
	Administrator	Object Access	1:25:38 am	08/21/2006	Audit success	FSERMER	See the description field	Object Open
	Administrator	Account Management	1:32:41 am	08/21/2006	Audit success	FSERVER	See the description field	User Account Locked Out (N/A)
	Administrator	Logon/Logoff	1:32:44 am	08/21/2006	Audit success	FSERMER	See the description field	Successfull Logon (N#4)
	Administrator	Account Logon	1:40:17 am	08/21/2006	Audit success	FSERMER	See the description field	Authentication Ticket Granted
	Administrator	Account Logon	1:50:43 am	08/21/2006	Audit success	FSERMER	See the description field	Authentication Ticket Granted
	Administrator	Logon/Logoff	1:51:01 am	08/21/2006	Audit success	FSERMER	See the description field	Winstation session disconnection
	Administrator	Logon/Logoff	1:51:01 am	08/21/2006	Audit success	FSERVER	See the description field	Winstation session disconnection
	Administrator	Logon/Logoff	1:53:15 am	08/21/2006	Audit success	FSERVER	See the description field	Winstation session connection
	Administrator	Account Logon	1:53:15 am	08/21/2006	Audit success	FSERMER	See the description field	Authentication Ticket Granted
	Administrator	Logon/Logoff	1:53:15 am	08/21/2006	Audit success	FSERMER	See the description field	Winstation session connection
	Administrator	Logon/Logoff	2:18:38 am	08/21/2006	Audit success	FSERMER	See the description field	User Logoff

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



List of actions taken by users with root or administrative privileges

Use this report to:

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

Access to all audit trails

	User Identification	Type of event	Date a	ndtime	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
0→	GFITEMASOFT\Administrator	System Event	9:55:57 pm	08/21/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
	GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/10/2006	Audit success	FSERMER	Security audit log	The audit log was cleared
	GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/20/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
	GFITEMASOFT\Administrator	System Event	9:55:57 pm	09/24/2006	Audit success	FSERVER	Security audit log	The audit log was cleared
	GFITEMASOFT\Administrator	System Event	9:66:67 pm	09/25/2006	Audit success	FSERMER	Security audatiog	The audit log was cleared

Screenshot 76 - Sample report showing access to all audit trails



List of audit trails

Use this report to:

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

Invalid logical access attempts

Account lockouts

 \bullet

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

Failed logons from reasons other than bad user name or password

User Identification	Type of event	Datea	andtime	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
CALDEVitest	Logon/Logoff	12:33:02 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDE/test	Logon/Logoff	12:33:02 pm	09/25/2006	Audit failure	CALDE/	CALDEV	LF: Account Disabled (test)
CALDEV#est	Logon/Logoff	12:33:02 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEVitest	Logon/Logoff	12:33:02 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEVitest	Logon/Logoff	12:33:02 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Account Disabled (test)
CALDEVitest	Logon/Logoff	12:34:34 pm	09/25/2006	Audit failure	CALDEV	CADEV	LF: Logon Type Rejected (test)
CALDEVitest	Logon/Logoff	12:34:34 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEVitest	Logon/Logoff	12:34:34 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEVitest	Logon/Logoff	12:34:34 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Logon Type Rejected (test)
CALDEV/test	Logon/Logoff	12:34:34 pm	09/25/2006	Audit failure	CALDEV	CADEV	LF: Logon Type Rejected (test)

Screenshot 77 - Sample report showing invalid logical access attempts

	List of invalid	d logical	access	attempts
--	-----------------	-----------	--------	----------

Use this report to:

2

 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 logons because of bad user name and password

User Identification Type of event Date and time Successor Origination of Ignitude individual (ignation of all verification) Identify a factor of all verification Description CALDEVdat/tidt Logon/Logitt 1227:53 pm 04/25/2000 Audit failure CALDEV CALDEV CALDEV CALDEV CALDEV CALDEV CF.Bed username/password (dot/fid/) CALDEVdat/tidt Logon/Logitt 1227:53 pm 04/25/2000 Audit failure CALDEV CALDEV CF.Bed username/password (dot/fid/) CALDEVdat/tidt Logon/Logitt 1227:53 pm 04/25/2000 Audit failure CALDEV CALDEV LF: Bed username/password (dot/fid/) CALDEVdat/tidt Logon/Logitt 1227:53 pm 04/25/2000 Audit failure CALDEV CALDEV LF: Bed username/password (dot/fid/) CALDEVdat/tidt Logon/Logitt 122:7:53 pm 04/25/2000 Audit failure CALDEV CALDEV LF: Bed username/password (dot/fid/) CALDEVdat/tidt Logon/Logitt 122:83 pm 04/25/2000 Audit failure CALDEV CALDEV LF: Bed username/password (ebd/fid/) <								
CALDEV/subfisht Logon/Log/ft 12.27.51 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/subfisht Logon/Log/ft 12.27.53 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/subfisht Logon/Log/ft 12.27.53 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/subfisht Logon/Log/ft 12.27.53 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/staffisht Logon/Log/ft 12.27.53 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/staffisht Logon/Log/ft 12.29.09 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/staffisht Logon/Log/ft 12.29.09 pm 09/25/2000 Ault failure CALDE/ CALDE/ LF: Bad user name/password (bothsoft) CALDEV/staffisht Logon/Log/ft 12.29.09 pm 09/25/2000	User Identification	Type of event	Datea	andtime	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
CALDE/Vest Logon/Logoff 12:27:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest/titiet Logon/Logoff 12:27:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest/titiet Logon/Logoff 12:27:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest/titiet Logon/Logoff 12:27:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest Logon/Logoff 12:27:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest Logon/Logoff 12:28:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest Logon/Logoff 12:28:30 pn 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfath) CALDE/Vest Logon/Logoff 12:28:30 pn 09/25/2008 Audit failu	CALDEValisatifisati	Logon/Logoff	12:27:53 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/ password (drsdffsdf)
CALDE/Vest Logon/Logoff 12:27:50 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:27:50 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:27:50 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:27:50 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:23:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:23:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:23:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bothfod) CALDE/Vest Logon/Logoff 12:23:09 pm 00/25/2000 Audit failure CALDE/ </td <td>CALDEVatisatifisati</td> <td>Logon/Logoff</td> <td>12:27:53 pm</td> <td>09/25/2006</td> <td>Audit failure</td> <td>CALDEV</td> <td>CALDEV</td> <td>LF: Bad user name/password (drsdffsdf)</td>	CALDEVatisatifisati	Logon/Logoff	12:27:53 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (drsdffsdf)
CALDE/Vest Logon/Logoff 12:27:59 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodffod) CALDE/Vest Logon/Logoff 12:27:59 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodffod) CALDE/Vest Logon/Logoff 12:27:59 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodffod) CALDE/Vest Logon/Logoff 12:28:09 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodffod) CALDE/Vest Logon/Logoff 12:28:09 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod) CALDE/Vest Logon/Logoff 12:28:09 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod) CALDE/Vest Logon/Logoff 12:28:09 pr 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod) CALDE/Vest Logon/Logoff 12:28:09 pr 09/25/2008 Audit failure CALDE/	ALDEValisatifisati	Logon/Logoff	12:27:53 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (drsdffsdf)
CALDE/Vest Logon/Logoff 12:27:30 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodfidd) CALDE/Vest Logon/Logoff 12:28:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodfidd) CALDE/Vest Logon/Logoff 12:28:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bodfidd) CALDE/Vest Logon/Logoff 12:28:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod) CALDE/Vest Logon/Logoff 12:28:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod) CALDE/Vest Logon/Logoff 12:28:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod) CALDE/Vest Logon/Logoff 12:28:09 pm 00/25/2000 Audit failure CALDE/ CALDE/ LF: Bad user name/password (bod)	CALDEValisatifisati	Logon/Logoff	12:27:53 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (drsdffsdf)
CALDE/Veet Logon/Logoff 12:23:09 pr 09/25/200 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDE/Veet Logon/Logoff 12:23:09 pr 09/25/200 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDE/Veet Logon/Logoff 12:23:09 pr 09/25/200 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDE/Veet Logon/Logoff 12:23:09 pr 09/25/200 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDE/Veet Logon/Logoff 12:23:09 pr 09/25/200 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDE/Veet Logon/Logoff 12:23:09 pr 09/25/200 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set)	CALDEValisatifisati	Logon/Logoff	12:27:53 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (drsdffsdf)
CALDEV/test Logon/Logoff 12:28:09 pm 09:255/200 Audit failure CALDEV CALDEV LF: Bad user name/password (set) CALDEV/test Logon/Logoff 12:28:09 pm 09:255/200 Audit failure CALDEV CALDEV LF: Bad user name/password (set) CALDEV/test Logon/Logoff 12:28:09 pm 09:255/200 Audit failure CALDEV CALDEV LF: Bad user name/password (set) CALDEV/test Logon/Logoff 12:28:09 pm 09:255/200 Audit failure CALDEV CALDEV LF: Bad user name/password (set)	CALDEVitest	Logon/Logoff	12:28:09 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/ password (test)
CALDEV/test Logon/Logoff 12:28:09 pm 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDEV/test Logon/Logoff 12:28:09 pm 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set) CALDEV/test Logon/Logoff 12:28:09 pm 09/25/2008 Audit failure CALDE/ CALDE/ LF: Bad user name/password (set)	CALDEVitest	Logon/Logoff	12:28:09 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)
CALDEVtext Logon/Logoff 12:28:09 pm 09/25/2006 Audit failure CALDEV CALDEV LF: Bad user name/ password (text)	CALDEVitest	Logon/Logoff	12:28:09 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)
	CALDEVitest	Logon/Logoff	12:28:09 pm	09/25/2006	Audit failure	CALDEV	CALDEV	LF: Bad user name/password (test)

IPSec security events

User Identification	Type of event	Dates	andtime	Success or Failure indicator	Origination of	Identity or name of affected	Description
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDE/	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK SERVICE	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service
NT AUTHORITY\NETWORK	Policy Change	12:10:13 pm	09/25/2006	Audit success	CALDEV	Security	IPSec Policy Agent service

Screenshot 78 - Sample report showing identification and authentication mechanisms

List of identification and authentication mechanisms

Use this report to:

2

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

Initialization of the audit logs

	User Identification	Type of event	Date and time		Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
0→	N#A.	None	1:22:18 pm	05/15/2007	Warning	Comp-Alina	Audit Log	The (1): ev.evt log file is full.
	NA	None	1:22:18 pm	05/15/2007	Warning	Comp-Alina	Audit Log	The (1): ev.evt log file is full.
	Event Log service s	tarted						
	User Identification	Type of event	Date a	indtime	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
	User Identification	Type of event	Date a 12:18:14 pm	ndtime 05/15/2007	Success or Failure indication Information	Origination of event COMP-AUNA	Identity or name of affected data, resource or componen Eventlog	Description The Event log service was stated.
	User Identification NA NA	Type of event None None	Date a 12:18:14 pm 12:18:14 pm	o5/15/2007 05/15/2007	Success or Failure indication Information	Origination of event COMP-AUNA COMP-AUNA	Identity or name of affected data, resource or componen Eventlog Eventlog	Description The Event log service was statted. The Event log service was statted.
	User Identification NA NA NA	Type of event None None None	Date a 12:18:14 pm 12:18:14 pm 1:22:18 pm	ond ti me 05/15/2007 05/15/2007 05/15/2007	Success or Failure indication Information Information Warning	Origination of event COMP-AUNA COMP-AUNA COMP-AUNA	Identity or name of affected data, resource or componen Event log Event log event log	Description The Event log service was stanted. The Event log service was stanted. The Event log service was stanted.
	User Identification NA NA NA NA	Type of event None None None None	Date a 12:18:14 pm 12:18:14 pm 1:22:18 pm 1:22:18 pm	ndtime 05/15/2007 05/15/2007 05/15/2007 05/15/2007	Success or Failure indicator Information Information Warning Warning	Origination of event COMP-AUNA COMP-AUNA COMP-AUNA	Identity or name of affected data, resource or componen EventLog EventLog eventLog eventLog	Description The Event log service was stanted. The Event log service was stanted. The Event log service was stanted. The Event log service was stanted.
	User Identification NA NA NA NA	Type of event None None None None None	Date a 12:18:14pm 12:18:14pm 1:22:18pm 1:22:18pm 9:02:53pm	nd time 05/15/2007 05/15/2007 05/15/2007 05/15/2007 05/16/2007	Success or Failure indication Information Information Warning Warning Information	Drigination of event COMP.4UNA COMP.4UNA COMP.4UNA COMP.4UNA COMP.4UNA	Identity or name of affected data, resource or componen Eventing eventing eventing eventing Eventing Eventing	Description The Event log service was stanted. The Event log service was stanted.



Use this report to:

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

Creation and deletion of system-level objects

User Identification	Type of event	Dates	andtime	Success or	Origination of	Identity or name of affected	Description
				Failure indication	event	data, resource or component	٩
VIRTUALD 0M1\\2003DC1\$	Directory Service Access	4:31:10 pm	04/17/2007	Audit success	V2003DC1	%{4ae49748-6aa4-4366-aff2-274 ea3e5a019%}	Object Operation
VIRTUALD 0M1\\2003DC1\$	Directory Service Access	10:45:21 am	04/26/2007	Audit success	V2003DC1	DC=VirtualDom1,DC=ts	Object Open
VIRTUALD 0M1\\2003DC1\$	Directory Service Access	11:22:30 am	04/26/2007	Audit success	V2003DC1	%{4ae49748-6aa4-4365-aff2-274 ea3e5a019%}	Object Operation
VIRTUALD 0M1\\2003DC1\$	Directory Service Access	3:00:16 pm	05/15/2007	Audit success	V2003DC1	DC=\/irtualDom1,DC=ts	Object Open
COMP-ALINA\aina	Object Access	11:03:27 am	05/16/2007	Audit success	Comp-Alina	Policy\Secrets\L\$ASP.NETAuto Ge nKeys2.0.50727.210	Diject Operation
COMP-ALINA\aina	Object Access	11:05:48 am	05/16/2007	Audit success	Comp-Alina	Policy\Secrets\L\$ASP.NETAutoGe nKeys2.0.50727.210	Object Operation
Windows File Pro	tection Service - att	tempt to rep	lace protecte	d file			
Windows File Pro	tection Service - att	tempt to rep Date	lace protecte and ti me	d file	Origination of	f Identity or name of affected	d Description
Windows File Pro	tection Service - att	tempt to rep Date	lace protecte and time	d file Success or Failure indicatio	Origination of n event	Identity or name of affected data, resource or component	d Description
Windows File Pro User Identification NA	tection Service - att Type of event None	Date 4:11:41 pm	and time	d file Success or Failure indication Information	Origination of n event COMP-AUNA	Identity or name of affected data, resource or componen (1): event	si Description File replacement was attempted on the prot system fle(1):event.
Windows File Pro User Identification	tection Service - att Type of event None	Date 4:11:41 pm	lace protecte and time 05/15/2007	d file Success or Failure indication Information	Origination of n event COMP-AUNA	Identity or name of affected data, resource or componer (1): ev.et	d Description The replacement was attempted on the prot system Bi(1) event. This File was restored to the original version cystem staffly.
Windows File Pro User Identification NA	tection Service - att	Date 4:11:41 pm 4:11:41 pm	lace protecte and time 05/16/2007 05/16/2007	d file Success or Failure indication Information	Origination of event COMP-AUNA COMP-AUNA	Identity or name of affected data, resource or componer (1): event (2): event	Description Foreplacement was attempted on the path system fiel() reveet. This file was prevented to the path system state, was attempted on the path system fiel() verset.
Windows File Pro User Identification NA	tection Service - att	Date 4:11:41 pm 4:11:41 pm	lace protecte and time 05/16/2007 05/16/2007	d file Success or Failure indication Information	Origination of event COMP-AUNA COMP-AUNA	data, resource or componer (1): event (2): event	Description Pereplacement was attempted on the pot system fie(1) event. This file was restored to the original version system study. File replacement setup. This file was restored to the original version system study. This file was restored to the original version system study.
Windows File Pro	Type of event None None None	Cate 4:11:41 pm 4:11:41 pm 4:11:41 pm	lace protecte and time 05/16/2007 05/16/2007	d file Success or Failure indicato Information	Origination of event COMP-AUNA COMP-AUNA COMP-AUNA	Identity or name of affected data, resource or componen (1): event (2): event	Description Pereplacement was attempted on the pro- system fie(1) event. This file was restored to the original version aystam study. The replacement was attempted on the pro- system study. This file was restored to the original version system study. The replacement was attempted on the pro- system study. The replacement was attempted on the pro- system field was restored to the pro-
Windows File Pro	tection Service - att Type of event None None	Cate 0ate 4:11:41 pm 4:11:41 pm 4:11:41 pm	lace protecte and time 05/16/2007 05/16/2007	d file Success or Failure indicato Information Information	Comp-Alina COMP-Alina COMP-Alina COMP-Alina	I dentity or name of affectes data, resource or compose (1); event (2); event (3); event	Description File replacement was attempted on the pat- system fie(1) evexet. This file was rescreted to the original version system stably. File replacement was attempted on the pat- system fie(2) evexet. This file was rescreted to the original version system stably.
Windows File Pro	Type of event None None None	Date 0:1:41 pm 4:11:41 pm 4:11:41 pm	lace protecter and time 05/15/2007 05/15/2007 05/15/2007	d file Success or Failure indicated Information Information Information Information	Origination of event COMP-AUNA COMP-AUNA COMP-AUNA COMP-AUNA	Gentity or name of affectes data, resource or componen (1): event (2): event (3): event (4): event	Description Description The replacement was attempted on the prot system fiel(1) event. This flue was recreated to the original version system study. The replacement was attempted on the prot system fiel(2) event. This flue was recreated to the original version system fiel(2) event. This flue was recreated to the original version system fiel(2) event. This flue was restored to the original version system fiel(2) event. This flue was restored to the original version system fiel(2) event. This flue was restored to the original version system fiel(2) event. This flue was restored to the original version system fiel(2) event. This flue was restored to the original version system fiel(2) event.

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

List showing creation and deletion of system-level objects

Use this report to:

2

 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 systemlevel objects' for Windows-based systems presented in the format required by point 10.2.3 of the PCI Data Security Standards document version 1.1.

Time synchronization monitoring

	User Identification	Type of event	Date a	andtime	Success or Failure indication	Origination of event	Identity or name of affected data, resource or component	Description
2 →	VIRTUALD 0M1\\2003DC1\$	System Event	10:39:54 am	04/26/2007	Audit success	V2003DC1	System time	The system time was changed
	VIRTUALD 0M1\\2003DC1\$	System Event	2:59:21 pm	05/15/2007	Audit success	V2003DC1	System time	The system time was changed
	COMP-ALINA/aina	System Event	4:47:11 pm	05/15/2007	Audit success	COMP-AUNA	System time	The system time was changed
	COMP-ALINA\aina	System Event	4:47:11 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA\aina	System Event	4:47:14 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA\aina	System Brent	4:47:14pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA\aina	System Event	4:47:35 pm	05/15/2007	Audit success	Comp-Auna	System time	The system time was changed
	COMP-ALINA/alina	System Event	4:47:35 pm	05/15/2007	Audit success	COMP-AUNA	System time	The system time was changed
	COMP-ALINA\aina	System Event	4:47:42 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA\aina	System Brent	4:47:42 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA\aina	System Event	5:47:01 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA/alina	System Event	6:47:01 pm	05/15/2007	Audit success	COMP-AUNA	System time	The system time was changed
	COMP-ALINA\alina	System Event	5:47:01 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed
	COMP-ALINA\aina	System Event	5:47:01 pm	05/15/2007	Audit success	Comp-Alina	System time	The system time was changed



User Identification	Type of event	Date a	Date and time Success or		Origination of Identity or name of affected		Description	
				Failure indication	event	data, resource or componen	4	
NA	None	12:18:58 pm	05/15/2007	Information	Comp-Alina	W32Time	The time service is now synchronizing the system time with the time	
							source developerstemasof9.ts (nto di192.168.100.54/123.>192.168.100.3/123)	
NA	None	12:18:58 pm	05/15/2007	Information	Comp-Alina	W32Time	The time service is now synchronizing the system time with the time	
							source developerstemasof9.ts (ntp.d)192.168.100.54:123->192.168.100.3:123).	
NA	(1204)	4:48:34 pm	05/15/2007	Error	Comp-Alina	W32Time	The time sample was rejected because Duplicate timestamps were received from this peer.	

Screenshot 81 - Sample report showing time synchronization monitoring

2	List showing time synchronization monitoring
---	--

Use this report to:

- Monitor system time changes
- Monitor the time synchronization process

Events Trend Reports

Use the reports in this category to:

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

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

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

- Directory Services log
- File Replication Service log.

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



Screenshot 82 - Sample extract from Events Trend Reports: 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



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

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

Generic events trend per hour

5



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

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

Use this report to:

• View trends on an hourly basis.

Generic events trend per days



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

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

Use this report to:

• View trends on an daily basis.

Generic events trend per week



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

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

Use this report to:

• View trends on an weekly basis.

Generic events trend per month



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

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

Use this report to:

• View trends on a monthly basis.

All critical messages reports

All critical windows log events

	Computer	User	Event ID	Source	Description	Type	Time	Date
	FSERVER	GFITEMASOFTcalls	540	Security	Seccess thi Network Logon (calls)	And/ts rooms s	12:00:02AM	8212006
	FSERVER	G FITEMASO FTeals	560	Security	ObjectOpe	And its notes s	12:00:11AM	8212006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpes	Audits rocess	12:01:07AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpe	Audits access	12:01:18AM	8212006
	FSERVER	NT AUTHORITY/SYSTEM	672	Security	Antientication Ticket Granted	Andits access	12:08:06AM	8/21/2006
	FSERVER	NT AUTHORITYGYSTEM	672	Security.	Artiertication Ticket Granted	Andits nocess	12:06:06AM	8212006
•	FSERVER	NT AUTHORITY/GYSTEM	672	Security	Antientication Ticket Granted	Andits nooness	12:08:17AM	8212006
$0 \rightarrow$	FSERVER	GFITEMASOFTcalls	560	Decently.	ObjectOpe	And its notes a	12:09:54AM	8212006
•	FSERVER	G FITEMASO FTealls	560	Security	ObjectOpe	Andits recess	12:09:54AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpes	Audits access	12:09:54AM	8212006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpes	Audits rooks	12:12:21AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpes	Audits access	12:12:21AM	8212006
	FSERVER	NT AUTHORITY/SYSTEM	672	Security	Antientication Ticket Granted	Audit failure	12:13:25AM	8/21/2006
	FSERVER	NT AUTHORITYGYSTEM	672	Security.	Artice stication Ticket Granted	Auditalium	12:13:26AM	8212006
	FSERVER	NT AUTHORITY/GYSTEM	644	Security	User Account Looked Ont (Adm in Istrator)	And its recess	12:18:13AM	8212006

Screenshot 89 - All critical Windows log events

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

Use this report to:

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

All critical Syslog events



Screenshot 90 - All critical Syslog log events

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

Use this report to:

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

All critical W3C events



Microsoft Internet Information	192.168.10.1	N/A	GET	200 (0K)	R1	STEEPIN	8/24/2005
Services6.0 Microsoft Internet Information	192.168.10.1	N/A	GET	200 (DK)	R2	610012PH	8/24/2006
Services6.0 Microsoft Internet Information	192.168.10.1	N/A	GET	200 (DK)	R2	60002PM	8/24/2006
Services6.0 Microsoft Internet Information	192.168.10.1	N/A	GET	200 (DK)	R2	50004PM	8/24/2005
Services6.0 Microsoft Internet Information	192.168.10.1	N/A	GET	200 (0k)	R2	SEEDERFIN	8/24/2006
Services6.0 Microsoft Internet Information	192,168,10,1	N/A	GET	200 (DK)	Rule 1	510106PM	8/24/2005
Services6.0 Microsoft Internet Information	192 168 10.1	N/A	GET	200 (0k)	Rule 1	5.00.08P III	8/24/2006
Services6.0 Microsoft Internet Information	102 168 101	N/A	GET	200 (04)	Rule 2	5.00:10P II	8/24/2006
Services6.0 Microsoft Internet Information	102 169 101	N/A	GET	200 (04)	Rula 2	500:10P.II	8/24/2006
Services6.0	102.100.10.1	N/A	OFT	200 (01)	Rule 2	600-128.0	BOLOTE
Microsoft internet information	192.108.10.1	N/A	GET	200 (0K)	Rule 2	V10.12P M	010100

Screenshot 91 - All critical W3C log events

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

Use this report to:

Time Date

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

Top 10 rules triggered ule1 Please follow the nextpages for more details. R.tk certly protection agent has stopped ESTSTATIO NА 1000 tor has started Rek 1 PointDecently 3.0 12 43 167 NА R182 ESTSTATIO teority30 139297 CD LOVO ROM D_/stem NA Rik2 Finned Deten Class Rek 1 System Class Rek 1

All critical Custom log events

Screenshot 92 - All critical custom logs events

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

Use this report to:

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

All critical SNMP Traps Messages



Classification: Critical

	Trap Data	Trap OID	Community String	SNMP Version	Rule Name	Time	Date
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/200
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/20
I/A		43.5.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/20
UA.		43.5.1.2.1.11	public	1	New processing rule	2:14:31PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/20
WA.		43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/20
UA.		43.5.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/20
I/A		43.5.1.2.1.11	public	1	New processing rule	2:14:32PM	9/24/20
e/A		43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/20
e/A		43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:33PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/20
e/A		43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/20
e/A		43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/20
(/A		43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:34PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:35PM	9/24/20
UA.		43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/20
(/A		43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/20
I/A		43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/20
WA.		43.6.1.2.1.11	public	1	New processing rule	2:14:36PM	9/24/20

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



Şerver: SERVER ᢒ→ Classification: Unclassified

Event Class	Application Name	Database Name	Login Name	Time	Date	Text Data
Audii Objeci Permission Eveni	Microsofi SQL Senier Managemeni Sludio	13	sa	12:00:00 pm	01/10/2008	SELECT db_name() AS (Dalablase_Name), bluame AS (Name).
30, L.S.Im IComple led	Microsofi 30, L Sener Managemen i Sludio	13	sa	12:00:00 pm	01/10/2008	s bilmanne AS (Sichema), SELECT db_manne() AS (Dalabase_Name), bilmanne AS (Manne).
SQ L:BaichComple ied	Microsofi SQL Senier Managemeni Skullo	R/A	sa	12:00:00 pm	01/10/2008	s bilmanne AS (Sicherma), SELEOT db_manne() AS (Dababase_Nanne), bilmanne AS (Nanne),
SQL:BaichSiaring	Microsofi 30, L Senier Managemen i Studio	N/A	sa	12:00:00 pm	01/10/2008	sbiname AS[Exchema], SELECT @@LOCK_TMEOUT
80 L.Sim Kilaring	Microsofi SQL Server Managementi Studio	13	sa	12:00:00 pm	01/10/2008	SELECT OO LOCK_TMEOUT
30 L:Sim iComple led	Microsofi SQL Server Managemen i Studio	13	sa	12:00:00 pm	01/10/2008	SELECT OC LOC K_TIMEOUT
SQ L:BalchComple led	Microsofi SQL Server Managementi Studio	N/A	sa	12:00:00 pm	01/10/2008	SELECT OO LOC K_TMEOUT
30 L:BaichStarling	Microsofi SQL Server Managementi Studio	N/A.	sa	12:00:00 pm	01/10/2008	use (g3)
30 L.Sim iSlarling	Microsofi SQL Server Managementi Studio	13	sa	12:00:00 pm	01/10/2008	use (g3)
30 L:Sim Compleied	Microsofi SQL Server Managementi Studio	13	sa	12:00:00 pm	01/10/2008	use (g3)
30 L:BaichComple led	Microsofi SQ L Sener Managementi Studio	N/A	58	12:00:00 pm	01/10/2008	use (g3)
SQL:BaichSiarling	Microsofi SQ L Senier Managemeni Studio	N/A	sa	12:00:00 pm	01/10/2008	SELECT db_mame()AS[Dalablasse_Name], w.mame AS[Name],
		-				suname AS (Schema),
Satismisianing	Managemeni Studio	13	sa	12300300 pm	01/10/2008	db_name() AS (Dalabase_Name),

Screenshot 94 - All critical SQL Server Audit

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

Use this report to:

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

Miscellaneous, Customizable reports

	Computer	User	Event ID	Source	Description	Type	Time	Date
	FSERVER	GFITEMASOFTcalls	540	Security	Seccess fill Network Logoe (calle)	Andits rocess	12:00:02AM	8/21/2006
	FSERVER	GFITEMASOFTealls	560	Security	ObjectOpes	Andits rocess	12:00:11AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpes	Andits scoress	12:01:07AM	8/21/2006
	FSERVER	GFITEMASOFTealle	560	Security	ObjectOpes	Andits scoress	12:01:18A.M	8/21/2006
	FSERVER	NT AUTHORITY/SYSTEM	672	Security	Artientication TicketGranted	Andits nocess	12:08:05A.M	8/21/2006
	FSERVER	NT AUTHORITYGYSTEM	672	Security	Arbertoator Tidet Granted	Andits rocess	12:08:05A.M	8/21/2006
	FSERVER	NT AUTHORITY/SYSTEM	672	Security	Arbertcator TicketGranted	Andits scoress	12:08:17AM	8/21/2006
≁	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpea	Andits rocess	12:09:54AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpes	Andits scoress	12:09:54AM	8/21/2006
	FSERVER	GFITEMASOFTealls	560	Security	ObjectOpes	Andits rocess	12:09:54AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	560	Security	ObjectOpea	Andits scoress	12:12:21AM	8/21/2006
	FSERVER	GFITEMASO FTcalls	560	Security	ObjectOpes	Andits scoress	12:12:21AM	8/21/2006
	FSERVER	NT AUTHORITY/SYSTEM	672	Security	Arbertcator TicketGranted	Anditibiling	12:13:25A.M	8/21/2006
	FSERVER	NT AUTHORITY/SYSTEM	672	Security	Arbentoaton Tidet Granted	Addtallere	12:13:25A.M	8/21/2006
	FSERVER	NT AUTHORITY/SYSTEM	644	Security	User Account Locked Ont (Administrator)	Andits access	12:18:13AM	8/21/2006
	FSERVER	GFITEMASOFTcalls	540	Security	Seccess fill Network Logos (calls)	Andits rooms	12:23:17AM	8/21/2006

Generic Windows Event log report

Screenshot 95 – Generic Windows Event log report

1 All Windows events that correspond to the current filtering condition

Use this report to:

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

Troubleshooting

Introduction

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

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

Knowledge Base

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

Web Forum

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

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: <u>http://support.gfi.com/supportrequestform.asp</u>. 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: <u>http://www.gfi.com/company/contact.htm</u>.

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: <u>http://customers.gfi.com</u>.

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: <u>http://www.gfi.com/pages/productmailing.htm</u>.

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

С

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

Ε

email 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

Κ

Kerberos policy changes 66

L

license 13, 39, 49, 50 Logoff events 54

Ν

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

0

Object Access Reports 17, 67 Object deleted 68

Ρ

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

Т

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