



*Evaluation Guide*

# **GFI** *EventsManager*<sup>™</sup>

*Learn how to get the most from your 30-day trial of GFI EventsManager.*



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

GFI and GFI EventsManager are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI EventsManager is copyright of GFI Software Ltd. - 1999-2017 GFI Software Ltd. All rights reserved.

Document Version: 13.1.0

Last updated (month/day/year): 06/16/2017

# Contents

<b>1 Why monitor and analyze your data?</b>	<b>4</b>
1.1 Before starting the evaluation	4
1.2 How GFI EventsManager works	4
1.2.1 Stage 1: Event Collection	4
1.2.2 Stage 2: Event Processing	5
<b>2 Evaluating GFI EventsManager</b>	<b>6</b>
2.1 Configuring GFI EventsManager for evaluation	6
2.1.1 Observing operational history logs of the localhost	6
2.2 Using the Quick Launch Console	6
2.3 How to configure Alerting Options	7
2.4 How to process events for the Local computer	8
2.5 How to process events for the Local domain	9
2.6 How to process events for Selected machines	10
2.7 Monitoring your network with GFI EventsManager	12
2.7.1 Events Processing Rules	12
2.7.2 Alerts	12
2.7.3 Dashboard	13
2.7.4 Events browser	15
2.7.5 Reporting	15
2.8 Using GFI EventsManager to demonstrate compliance	16
2.9 Using GFI EventsManager for forensic analysis	17
<b>3 Advanced features of GFI EventsManager</b>	<b>18</b>
3.1 How to customize events processing rules	18
3.2 How to get systems information not present in log data	19
3.3 How to detect possible hacker activities	19
3.4 How to detect events that refer to administrators	20
3.5 How to anonymize personal data from events	21
3.6 How to create custom reports	21

# 1 Why monitor and analyze your data?

The enormous volume of system event logs generated daily is of growing importance to organizations that must record information for forensic and compliance purposes. It is essential to perform real-time network-wide event log monitoring, analysis and reporting to address any incidents or security concerns and combat threats to business continuity.

GFI EventsManager assists with this monumental task by automatically and centrally monitoring and managing event logs - supporting a wide range of event types generated both by applications and devices from top vendors as well as for custom ones.

GFI EventsManager can help you:

- » Boost your security by monitoring security-relevant activity, mechanisms and applications.
- » Cut costs and increase productivity by automating IT management
- » Understand what is happening in your IT environment
- » Benefit from network uptime and identify problems through real-time alerts and dashboard
- » Protect your network by detecting and analyzing security incidents through event log data analysis
- » Achieve regulatory compliance with SOX, PCI DSS, HIPAA etc

## 1.1 Before starting the evaluation

Register to download and evaluate GFI EventsManager free for 30 days at: [http://go.gfi.com/?pageid=esm\\_trial](http://go.gfi.com/?pageid=esm_trial)

During evaluation our support and sales teams are ready to assist you with any questions you may have. The easiest way to get in touch with our representatives is to use the contact details shown on the GFI website: <https://www.gfi.com/contact-us> or directly via Support at <http://kb.gfi.com/supportcontact>.

## 1.2 How GFI EventsManager works

The operational functionality of GFI EventsManager is divided in the following stages:

- » Stage 1: Event Collection
- » Stage 2: Event Processing

### 1.2.1 Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of two event collection engines: The **Event Retrieval Engine** and the **Event Receiving Engine**.

Engine	Description
<b>The Event Retrieval Engine</b>	Used to collect Windows® Event Logs and Text Logs from networked event sources. During the Event Collection process this engine will: 1. Log-on to the event source(s) 2. Collect events from the source(s) 3. Send collected events to GFI EventsManager Server 4. Log-off from the event source(s). The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console

Engine	Description
<b>The SQL Server® Listener</b>	The listener receives trace messages from the scanned Microsoft® SQL Server® in real time. On receipt, GFI EventsManager processes the message immediately.
<b>The Oracle Retrieval Engine</b>	The Oracle Retrieval Engine connects periodically to Oracle servers and collects audits from a specific auditing table. Similar to the Microsoft® Windows® Event Retrieval Engine, GFI EventsManager processes events generated by the Oracle server.
<b>Log Receiving Engine</b>	<p>The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured.</p> <p>By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are however customizable via the GFI EventsManager management console.</p>

## 1.2.2 Stage 2: Event Processing

During this stage, GFI EventsManager runs a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

- » Analyze collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- » Filter events that match specific conditions
- » Trigger email, SMS and network alerts on key events
- » Trigger remediation actions such as the execution of executable files or scripts on key events
- » Optionally archive collected events in the database backend.

### Important

Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to the following article: [http://go.gfi.com/?pageid=esm\\_process\\_rights](http://go.gfi.com/?pageid=esm_process_rights)

## 2 Evaluating GFI EventsManager

Installing GFI EventsManager is easy. Follow the guidelines in our [Getting Started with GFI EventsManager](#) to review system requirements and learn how to prepare your environment and deploy the product.

After installing GFI EventsManager, go through the following topics to learn how to configure GFI EventsManager for first time use. Here you will find information on how to browse events and observe history logs through the Quick Launch Console:

### 2.1 Configuring GFI EventsManager for evaluation

GFI EventsManager has many features that apply to several log types. Event logs from the localhost are collected and processed automatically upon first startup of GFI EventsManager. For best results, you should enable Audit Policy on all categories on the machines listed below. More information can be obtained using this link:

[http://go.gfi.com/?pageid=esm\\_adminguide#cshid=AuditPolicy](http://go.gfi.com/?pageid=esm_adminguide#cshid=AuditPolicy).

- » The local machine or a workstation (a Windows 7 machine is recommended)
- » A Windows server in your network (ensure the GFI EventsManager service account you specified during the installation has admin rights on that machine)

#### 2.1.1 Observing operational history logs of the localhost

To confirm that event logs of the localhost are being processed:

1. Open GFI EventsManager and from **Status** tab click **> Job Activity**.

Operational History

Export data

Tell me more

	Date/Time	Machine	Source	Job ID	Log format	Message
	2012/08/24 12:18:11.2...	localhost	Processor service	N/A	monitoring	Finished processing 1 monitoring events from machine localhost - 1 events were archived.
	2012/08/24 12:18:11.1...	localhost	Processor service	N/A	monitoring	Processing 1 monitoring events from machine localhost.
	2012/08/24 12:18:04.0...	localhost	Processor service	N/A	monitoring	Finished processing 1 monitoring events from machine localhost - 1 events were archived.
	2012/08/24 12:18:03.9...	localhost	Processor service	N/A	monitoring	Processing 1 monitoring events from machine localhost.
	2012/08/24 12:17:57.6...	localhost	Processor service	N/A	monitoring	Finished processing 1 monitoring events from machine localhost - 1 events were archived.
	2012/08/24 12:17:57.5...	localhost	Processor service	N/A	monitoring	Processing 1 monitoring events from machine localhost.
	2012/08/24 12:17:50.7...	localhost	Processor service	N/A	monitoring	Finished processing 1 monitoring events from machine localhost - 1 events were archived.
	2012/08/24 12:17:50.7...	localhost	Processor service	N/A	monitoring	Processing 1 monitoring events from machine localhost.
	2012/08/24 12:17:30.0...	localhost	Processor service	N/A	monitoring	Finished processing 1 monitoring events from machine localhost - 1 events were archived.
	2012/08/24 12:17:30.0...	localhost	Processor service	N/A	monitoring	Processing 1 monitoring events from machine localhost.
	2012/08/24 12:17:25.9...	localhost	Processor service	N/A	monitoring	Finished processing 1 monitoring events from machine localhost - 1 events were archived.
	2012/08/24 12:17:23.4...	localhost	Processor service	N/A	monitoring	Processing 1 monitoring events from machine localhost.

Screenshot 1: Operational history logs of the localhost

2. Check that there is activity logs under the **Operational History** section.

#### Note

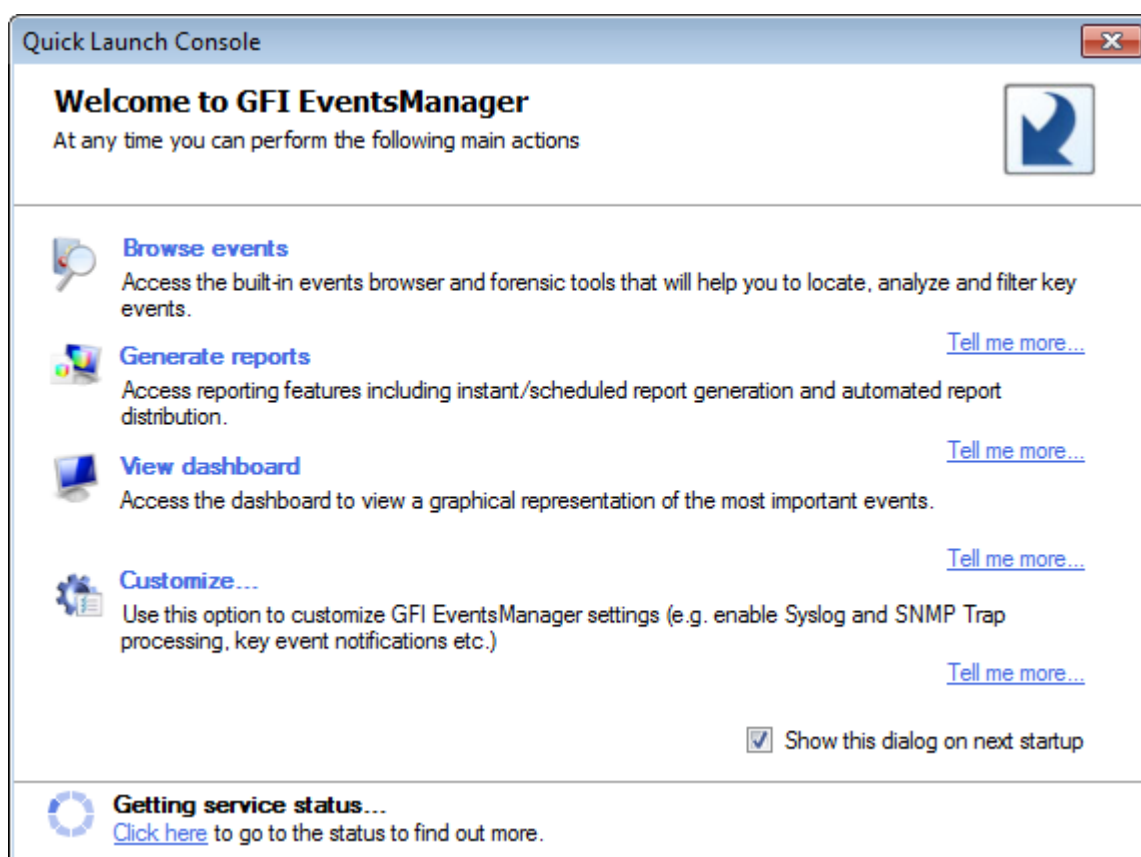
If the installation is functioning properly, this section is instantly populated.

### 2.2 Using the Quick Launch Console

When the Management Console is opened, the Quick Launch Console is automatically displayed.





#### Note

To stop the console from opening automatically, unselect **Show this dialog on next startup**.



Screenshot 2: GFI EventsManager Quick Launch Console

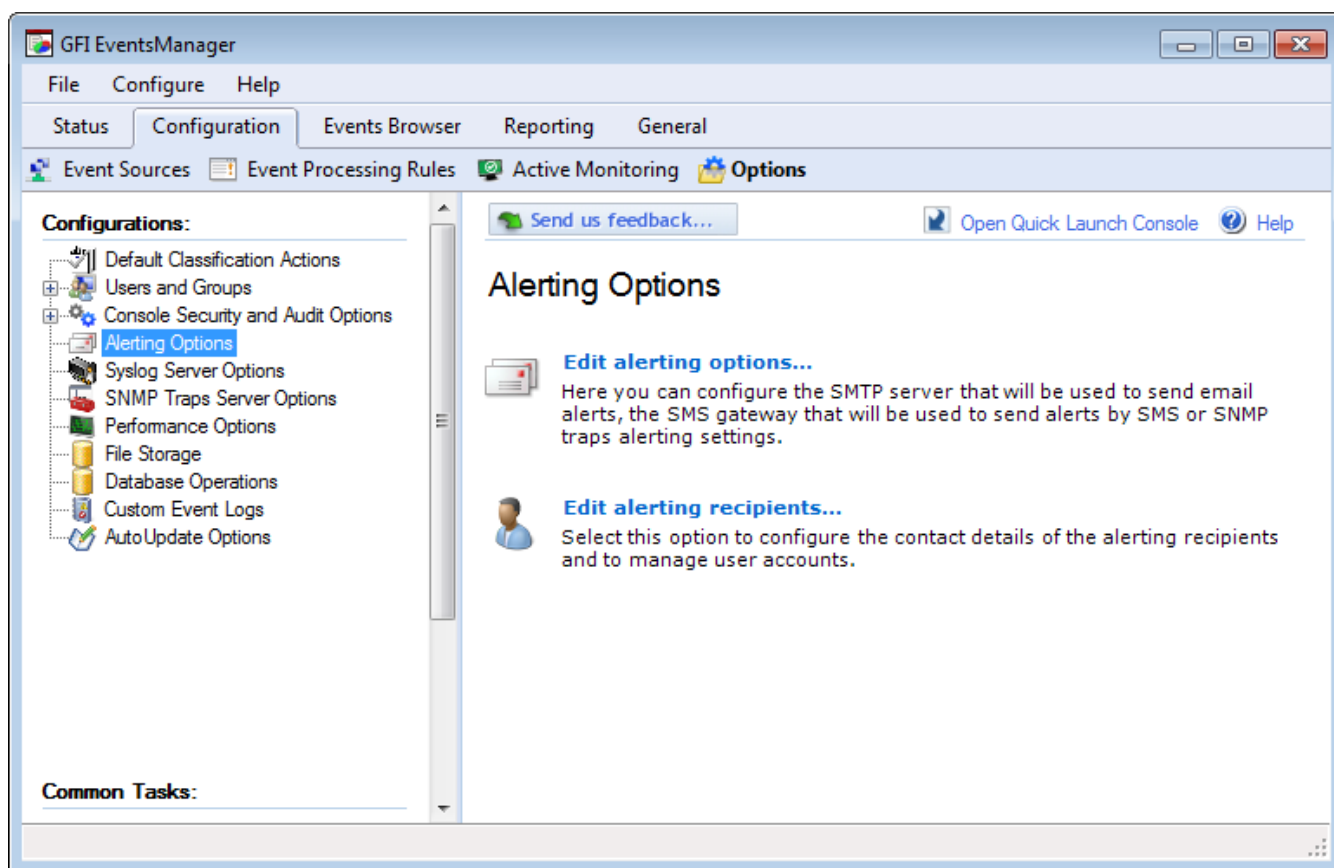
The following table describes the available options of the Quick Launch Console:

Icon	Description
	<b>Browse events</b> Access the built-in events and forensic tools that will help you locate, analyze and filter key events.
	<b>Generate reports</b> Access reporting features including instant/scheduled report generations and automated report distribution.
	<b>View dashboard</b> Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager.
	<b>Customize</b> Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, system checks, key events notifications, and more.

## 2.3 How to configure Alerting Options

To complete the setup configure alerting options to be notified in real time when important events occur. Alerting options enable you to configure what alerts are triggered when particular event(s) are collected. For example, you can configure GFI EventsManager to send an email and SMS alert to one or more recipients when a Critical event is processed.

To configure these options click: **Configuration>Options>Alerting Options**.



Screenshot 3: Configuring Alerting Options

## 2.4 How to process events for the Local computer

This option enables you to automatically add the localhost as an event source and start processing logs generated by it.

To process events from the local computer:

1. Open the GFI EventsManager Quick Launch Console. In the welcome page, click **Process events - Local computer**.
2. After the localhost logs start processing, you can:

Icon	Description
	<b>Browse events</b> Access the built-in events and forensic tools that will help you locate, analyze and filter key events.
	<b>Generate reports</b> Access reporting features including instant/scheduled report generations and automated report distribution.
	<b>View dashboard</b> Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager.
	<b>Customize</b> Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, system checks, key events notifications, and more.

### Note

To confirm that logs are successfully processed, go to **Status** tab > **Job Activity** and check that there are activity logs under the **Operational History** section.

## 2.5 How to process events for the Local domain

This option enables you add one or more computers that are on the same domain or workgroup as GFI EventsManager. The Automatic Network Discovery wizard enables you to select the type of event sources you want to add and then lists the sources that are detected.

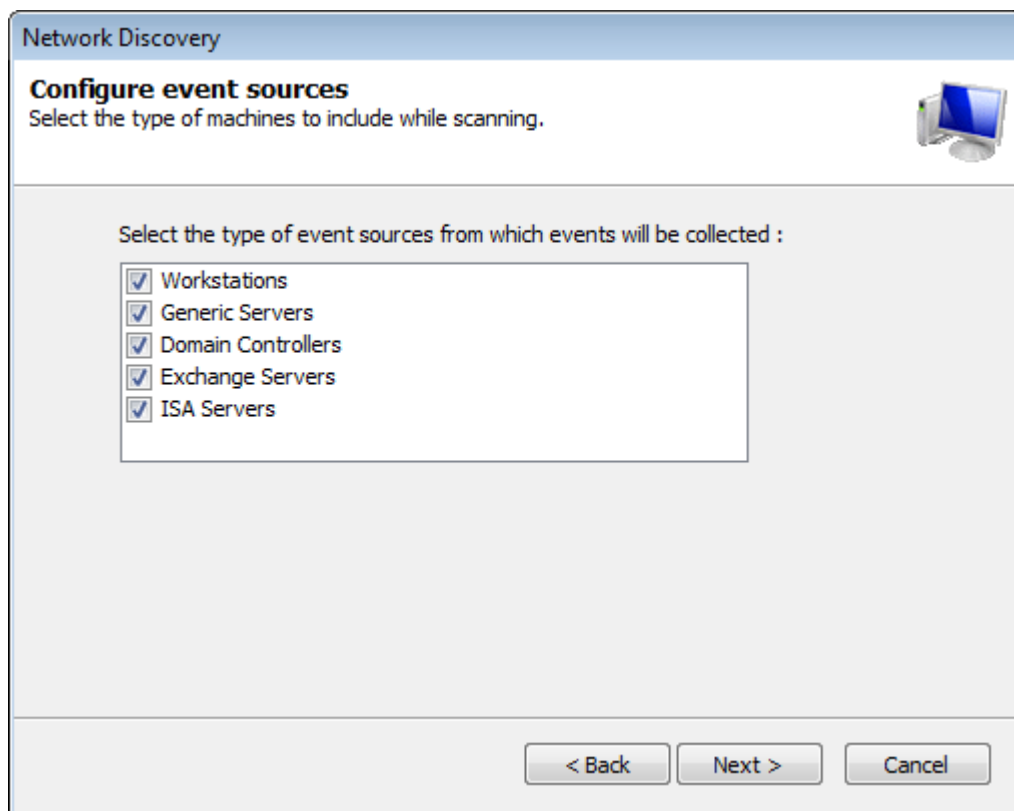
To process event from computers on the same domain/workgroup:

1. Open the GFI EventsManager Quick Launch Console. In the welcome page, click **Process events - Local domain**. This opens the **Automatic Network Discovery** wizard.

### Note

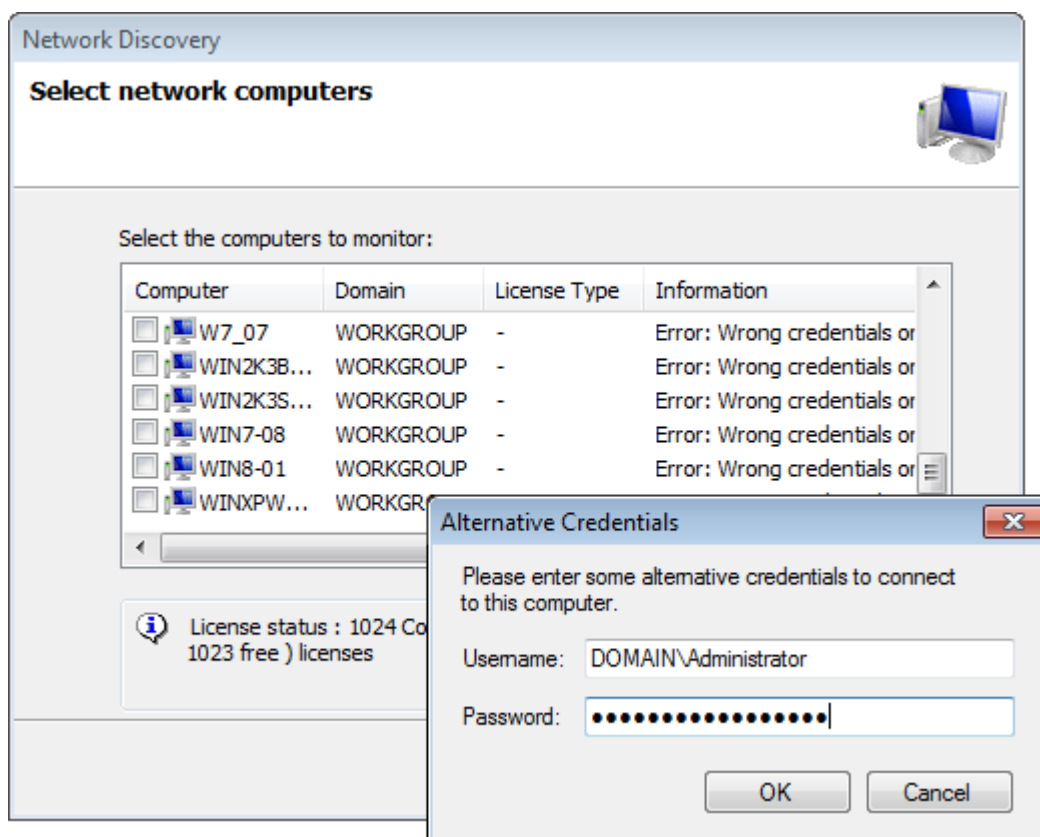
The wizard can also be launched from **Configuration** tab > **Event Sources**. From the left pane, right-click **All event sources** and select **Scan local domain**.

2. Click **Next** at the wizard welcome screen.



Screenshot 4: Select event source types to detect on your network

3. Select the type of event sources that the wizard will attempt to detect on your network. Click **Next**.



Screenshot 5: Search network progress

### Note

If GFI EventsManager detects computers that cannot be logged onto using the supplied credentials, it enables you to specify alternate logon credentials for each computer you select.

4. Select a computer from the list and key in the username and password. Click **OK** to close the **Alternative Credentials** dialog. Repeat this step until all the required sources are added.

5. Click **Next** and **Finish**.

### Note

To automatically add new computers that are joined to the same domain/workgroup as GFI EventsManager, you must configure Synchronization Options.

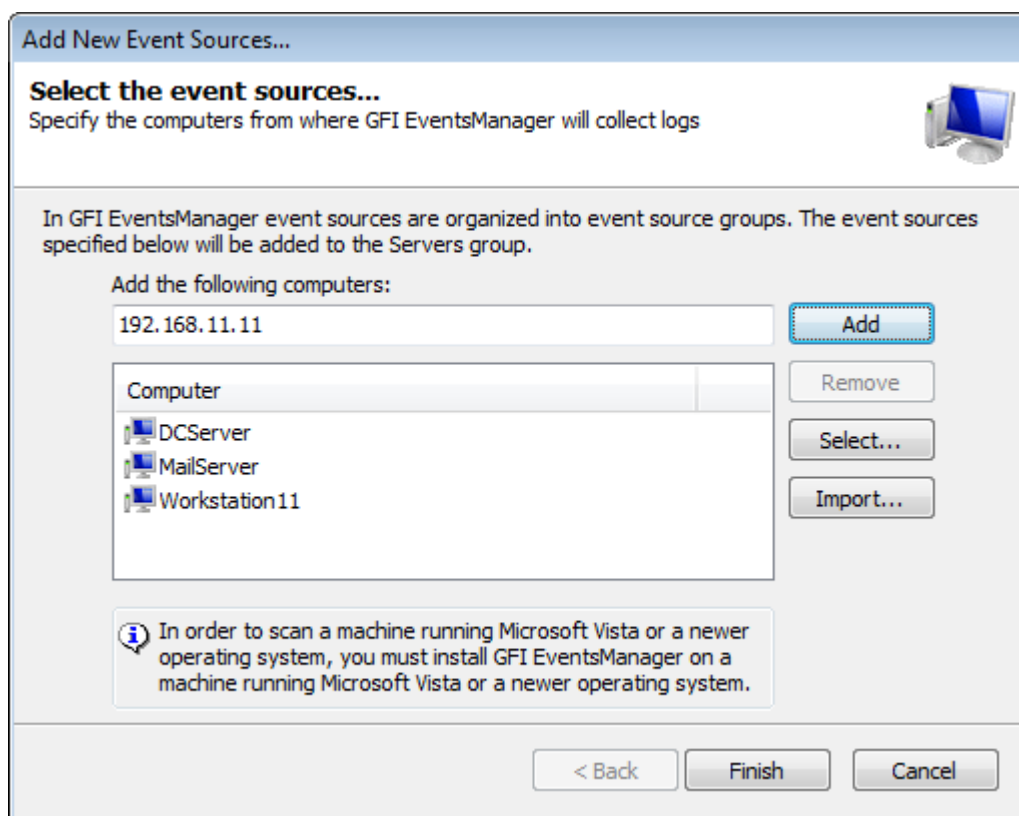
## 2.6 How to process events for Selected machines

This option enables you to add specific computers manually, by:

- » Keying in computer names and IPs
- » Selecting computers from reachable domains and workgroups
- » Importing computers from a text file containing a single computer name per line.

To process events of selected machines:

1. Open the GFI EventsManager Quick Launch Console. In the welcome page, click **Process events - Selected machines**.
2. This opens the **Add New Event Source** dialog.



Screenshot 6: Add new event source wizard

3. The following table describes the available options:

Option	Description
<b>Add</b>	Key in the computer name or IP address in the <b>Add the following computers</b> field. Click <b>Add</b> to add the specified computer to the <b>Computer</b> list. Repeat this step until you add all the event sources to the selected group. <div> <p><b>Note</b></p> <p>Since Syslog and SNMP traps use IP addresses to determine the source of an event, it is recommended to use the source IP address instead of the computer name when adding Syslog and SNMP Traps sources.</p> </div>
<b>Remove</b>	Select one or more computers from the <b>Computer</b> list and click <b>Remove</b> to delete them from the list.
<b>Select...</b>	Click <b>Select...</b> to launch the <b>Select Computers...</b> dialog: <ol style="list-style-type: none"> <li>From the <b>Domain</b> drop-down menu, select the domain you want to scan for available sources and click <b>Search</b>.</li> <li>From the search results list, select the computers you want to add.</li> <li>Click <b>OK</b> to close the <b>Select Computers...</b> dialog and return to the <b>Add New Event Sources...</b> dialog.</li> </ol>
<b>Import...</b>	Click <b>Import...</b> to import computers from a text file. Ensure that the text file contains only one computer name or IP address per line.

4. Click **Finish** to finalize your settings. GFI EventsManager immediately attempts to scan the added event sources, using the default logon credentials.

#### Note

If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add events sources. To launch **Network Discovery Wizard**, right-click **All event sources** from the event sources tree and select **Scan local domain**.

### Note

To confirm that logs are successfully processed, go to **Status** tab > **Job Activity** and check that there are activity logs under the **Operational History** section.

## 2.7 Monitoring your network with GFI EventsManager

GFI EventsManager can help monitor your network and detect various events, including: security incidents, downtimes, system health problems and configuration problems. GFI EventsManager offers five main features and locations to help you stay in touch with the main events occurring in your network.

### 2.7.1 Events Processing Rules

Events processing rules are checks that are run against event logs when they are collected. Based on the conditions configured in a rule, events processing rules help you:

- » **Classify processed events** - assign a severity rating to collected logs. This enables you to trigger actions or notifications if a certain severity log is processed. By default, events are classified using five main ratings, however, more ratings can be added
- » **Filter out noise (repeated events) or unwanted events** - remove duplicate logs or logs that are not important for you and archive important event data only. This reduces database growth and saves storage space
- » **Trigger Email, SMS and Network alerts on key events** - send notifications to configured recipients upon detection of certain events. You can configure an event processing rule to send notifications to recipients when the rule conditions are met
- » **Attempt remedial actions** - run executable files, commands and scripts upon detection of specific events. This enables you to automatically perform remedial actions to mitigate or completely eliminate a detected problem
- » **Filter events that match specific criteria** - remove event logs that are not important for you. Example, you can run a rule which filters out low severity or duplicate events
- » **Archive filtered events** - event archiving is based on the severity of the event and on the configuration settings of the event processing rules. Example: you can configure GFI EventsManager to archive only events that are classified as critical or high in severity and discard all the rest.

### 2.7.2 Alerts

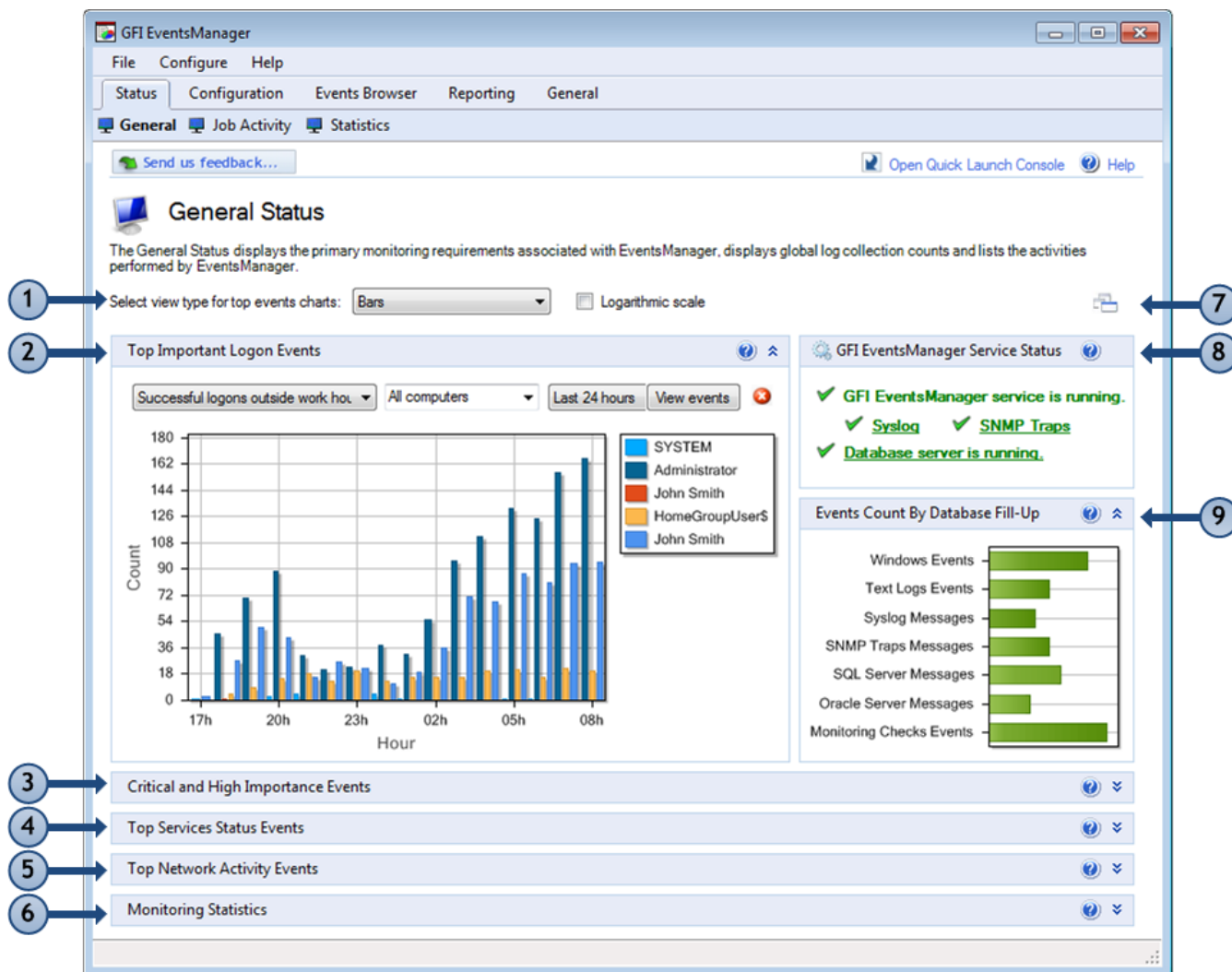
Alerting options enable you to configure what alerts are triggered when particular event(s) are encountered. For example, you can configure GFI EventsManager to send an email and SMS alert to one or more recipients when a **Critical** event is processed.

## 2.7.3 Dashboard

This General Status view is used to:

- » View the status of the GFI EventsManager event processing engine
- » Access statistical information such as the number of logon events, critical events and service status events.

To access the **General** view, go to **Status** tab > **General**.



Screenshot 7: GFI EventsManager Status: General view

The General view consists of the sections described below:

Section	Description
1	Use this section to select the chart type for top events.
2	<p>The <b>Top Important Log Events</b> section provides statistical information about:</p> <ul style="list-style-type: none"> <li>» Top 10 successful Logon events outside working hours</li> <li>» Top 10 important Logon events during working hours</li> <li>» Top 10 failed Logon events.</li> </ul> <p>Events in this section are filtered by:</p> <ul style="list-style-type: none"> <li>» <b>Machine:</b> Select a machine or key in a machine name in the drop down list</li> <li>» <b>Period:</b> The time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).</li> </ul>

Section	Description
3	<p>The <b>Critical and High Importance Events</b> section provides statistical/graphical information about critical events collected from all event sources. Here you can also view the vulnerability results monitored by GFI LanGuard. This graph shows the rules that collected and processed events for a particular period. From the drop down lists, select the type of information to display. Select from:</p> <ul style="list-style-type: none"> <li>» <b>Grouping:</b> Determines how events are grouped; such as Events, Computers, Computer groups, Events/Computers or Events/Computer groups</li> <li>» <b>Event type:</b> Select the type of data to display (Windows®, Text Logs, Syslog, SNMP, Active Monitoring Logs, SQL and Oracle audit)</li> <li>» <b>Alert type:</b> Specify the alert severity; such as All alerts, Critical or High</li> <li>» <b>Period:</b> Specify the time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).</li> </ul> <p><b>NOTE</b></p> <p>For detailed information about the different types of important events shown in this view, download the Microsoft® Security Monitoring and Attack Detection Planning Guide from <a href="http://go.gfi.com/?pageid=esm_smad_plan">http://go.gfi.com/?pageid=esm_smad_plan</a>.</p>
4	<p>The <b>Top Service Status Events</b> displays the top 10 services that caused the selected event. A service can generate events when:</p> <ul style="list-style-type: none"> <li>» Terminated with an error</li> <li>» Failed to load</li> <li>» Failed to start</li> <li>» Timed out</li> <li>» Stopped</li> <li>» Started.</li> </ul> <p>The graph shows the frequency of these events sorted by service type and/or by computer generating the event. Select a machine or service from the drop down lists or key in the required criteria to customize the graph results.</p> <p><b>Note</b></p> <p>To collect services information, event sources must have Audit system events policy enabled.</p>
5	<p>The <b>Top Network Activity Events</b> section displays details of the top 10 network activities (inbound and outbound) for computers running Microsoft® Windows® Vista or later. Network activity consists of all type of traffic generated by various protocols including SMTP, HTTP, FTP and MSN traffic. The network activities displayed can be filtered by:</p> <ul style="list-style-type: none"> <li>» Applications</li> <li>» Source Addresses</li> <li>» Destination Addresses</li> <li>» Computers</li> <li>» Ports</li> <li>» Users.</li> </ul> <p>Select parameters from the drop down lists or key in the values to filter the type of chart displayed.</p> <p><b>Note</b></p> <p>To collect network activities, event sources must have Object auditing and Process tracking enabled.</p>
6	<p>The <b>Monitoring Statistics</b> section displays status information about active Active Monitoring you are running on event sources. The information displayed in this section is refreshed every 20 seconds and you provides the:</p> <ul style="list-style-type: none"> <li>» Check name</li> <li>» Success/Fail count</li> <li>» Number of generated events</li> <li>» Check date and time</li> <li>» Check type.</li> </ul> <p>Select a row and click <b>View Events</b> to view the pertaining logs that were generated when the check failed/succeeded.</p>
7	<p>Click the <b>Arrange Window</b> icon to automatically fit all graphs in the management console.</p>

Section	Description
8	<p>The GFI EventsManager <b>Service Status</b> is used to view:</p> <ul style="list-style-type: none"> <li>» The operational status of GFI EventsManager service/event processing engine</li> <li>» The operational status of the Syslog server</li> <li>» The operational status of the SNMP Traps server</li> <li>» The operational status of the database server currently in use by GFI EventsManager.</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>» Click the service name to edit the service settings.</li> <li>» Click <b>Database server is running</b> to switch between different databases.</li> </ul>
9	<p>The <b>Events Count By Database Fill-Up</b> displays:</p> <ul style="list-style-type: none"> <li>» The horizontal bars represent the number of events stored in the database backend, sorted by event log type</li> <li>» The date and time of the last backup</li> <li>» The date and time of the next scheduled backup.</li> </ul> <p>The bar color turns from green to red as the database is populated with events.</p>

### Note

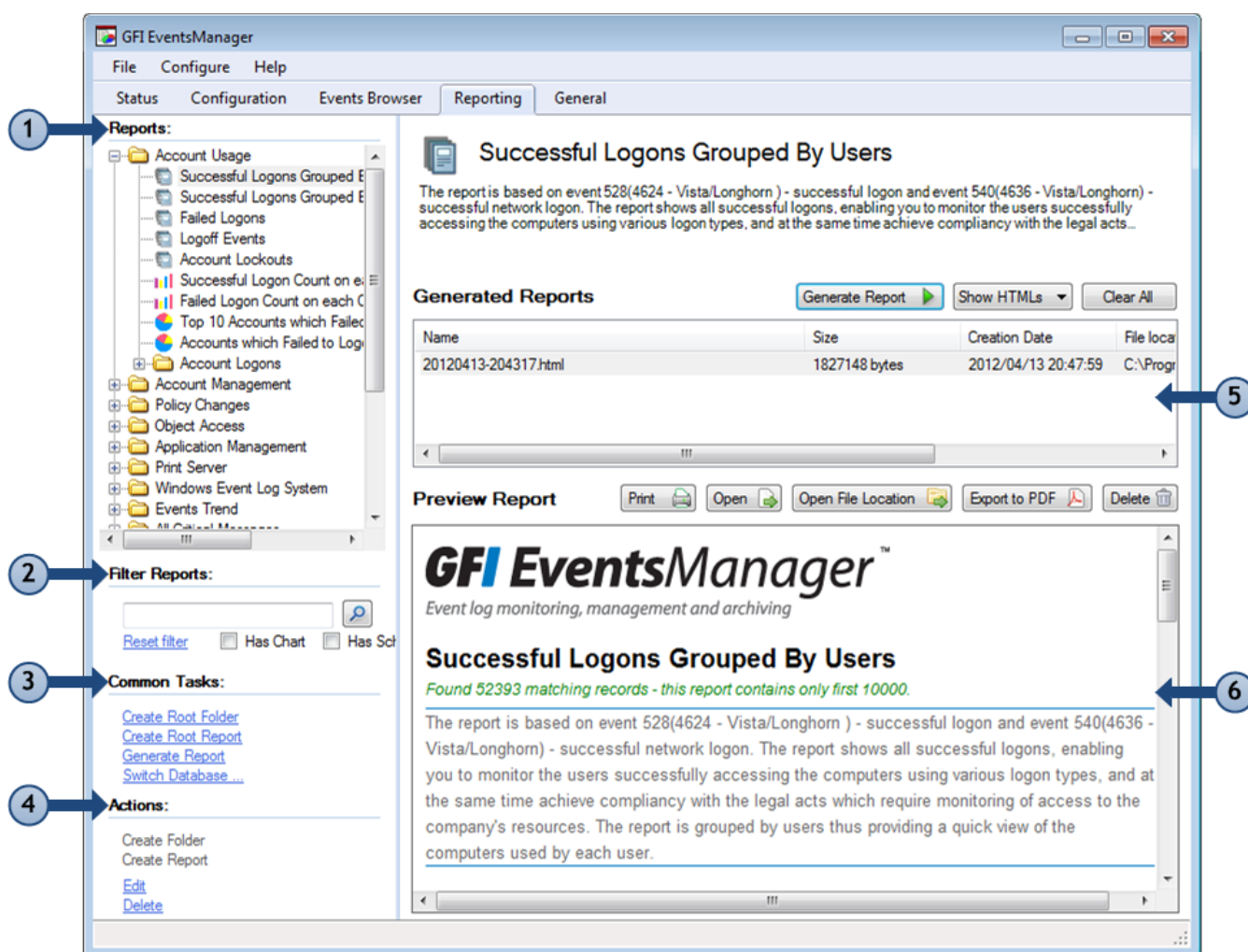
Double-click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph. Use the **Export to image** button to export the graph.

## 2.7.4 Events browser

The Events Browser is equipped with tools for event analysis and forensic investigation. It also enables you to easily browse through multiple events databases as well as export events to encrypted databases for legal compliance purposes. The Events Browser allows you to monitor the most important events from a common location. For more information refer to the **Using the Events Browser** section in the **Administrator Guide**.

## 2.7.5 Reporting

The Reporting tab enables you to generate various reports about important events that occur on your network.



Screenshot 8: Navigating the Reporting UI

The Reporting tab consists of the sections described below:

Section	Description
1	The <b>Reports</b> section contains all the predefined reports that ship with the product. Use this section to organize and generate various reports from technical to executive type.
2	Find reports rapidly, using the available filtering options. Through <b>Filter Reports</b> options, you are able to search for reports that contain charts and are generated based on a schedule.
3	The <b>Common Tasks</b> section enables you to quickly launch typical operations such as creating folder and report views to organize reports and generating reports.
4	From <b>Actions</b> , create, edit or delete reports according to your needs.
5	Use the <b>Generated Reports</b> section to view the history of a selected report (from Section 1). This enables you to regenerate and export the report to HTML and/or PDF.
6	The <b>Preview Report</b> section provides a view of a selected, generated report. Use the control buttons to Print, Open, Export or Delete reports directly from this section.

## 2.8 Using GFI EventsManager to demonstrate compliance

Most of the regulations' logs are deemed instrumental for tracking the activity occurring on systems that process personal data. Consequently, most of the regulations require that logs are regularly archived and reviewed . GFI

EventsManager helps you demonstrate regulatory compliance through four main features:

Feature	Achieving Compliance
<b>Event reporting</b>	GFI EventsManager is automatically configured with general and predefined reports covering common compliance acts, such as: HIPAA, FISMA, GLBA, Payment Cards Industry Data Security Standard (PCI DSS) and Code of Connection.
<b>Event processing rules</b>	Dedicated rules used to identify and categorize Windows events that are relevant for different PCI DSS requirements.
<b>Event archival</b>	The GFI EventsManager storage engine archives event data in files that can be compressed and encrypted. Your event data can be stored locally or in a central location.
<b>Event consolidation</b>	GFI EventsManager provides three layers of consolidation for your log data: <ul style="list-style-type: none"><li>» Encrypted storage</li><li>» Controlled and audited access to the log data</li><li>» Hash values for log data to detect outside tampering</li></ul>

At this stage of the evaluation it is recommended that you to go to the **Reporting** tab:

- » Select the report set applicable to your regulation and run a few reports.
- » If you don't find a dedicated report set for your regulation, check the general reports and select the ones that match your requirements. For example, **Account Usage reports** that show Logon/Logoff information are useful for most compliance acts.

#### NOTE

If you need to comply with the Payment Card Industry Data Security Standard (PCI-DSS), review GFI white papers on PCI DSS Compliance at [http://go.gfi.com/?pageid=EM\\_PCIDSS](http://go.gfi.com/?pageid=EM_PCIDSS). This offers very detailed information on how GFI can assist with each PCI requirement.

## 2.9 Using GFI EventsManager for forensic analysis

GFI EventsManager enables you to perform thorough investigations when incidents occur. This is done using the drill-down, filtering and sorting capabilities available from the **Events Browser**.

At this stage we recommend you become familiar with the views and filters in the browser by following these steps:

- » From the **Windows Events** view and sort events by clicking the column names in the grid.
- » From the **Properties** panel on the right side of the window, select **Fields** view. Click any field value to drill-down event data.
- » Create a custom view, right click on a value and select **Create Query From Field**.
- » To customize the view, open **Properties** and choose **Edit**. Check the fields available for you.

## 3 Advanced features of GFI EventsManager

This section provides you with information about configuring advanced features of GFI EventsManager. For more detailed information, refer to the [Administrator Guide](#).

### 3.1 How to customize events processing rules

Processing rules present information about event logs. They can help you identify and categorize events and trigger alerts or other actions for some of them. You will need to know how the rules work to master and configure them correctly:

- » Once defined, rules need to be manually assigned to event sources .
- » Rules have priorities (the order in which they are evaluated).
- » When an event is collected from a source, each rule assigned to that event source is evaluated against that event in order of priority.
- » When an event matches a rule, the actions of that rule are triggered and no additional rules will be evaluated for that event.

See this short video to familiarize yourself with these rules:

- » <https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-eventsmanager/videos/event-processing-rules>

Try out some of these rules:

1. Go to **Configuration > Event Processing Rules** tab.
2. Create a new folder (for example: **My rule folder**) and create a new rule set (for example: **My rule set**) within that folder.
3. Add a new rule to the rule set (for example: **Rule One**) that applies to Windows Security events with a specific event ID.
4. Set the rule to classify the matching events as **High**.
5. Create another rule called **Rule Two** with the same filter as **Rule One**; however, set this one to classify the events as **Medium**.

Assign these rules to your local machine:

1. Go to **Configuration > Event Sources** tab.
2. Choose the **All event sources** node from the tree and locate your local machine
3. Open the machine **Properties** and go to the **Windows event log**.
4. Uncheck the **Inherit Settings** option and add **Security Log** to the log list. Choose **Process using these Rule Sets** and check **My rule folder**.

#### NOTE

Wait until more events are generated and check the browser. You should see that all the events with the event ID you specified in the rule definition have triggered **Rule One**.

5. Go back to **Rule configuration** to change the priority of the rules.

## 3.2 How to get systems information not present in log data

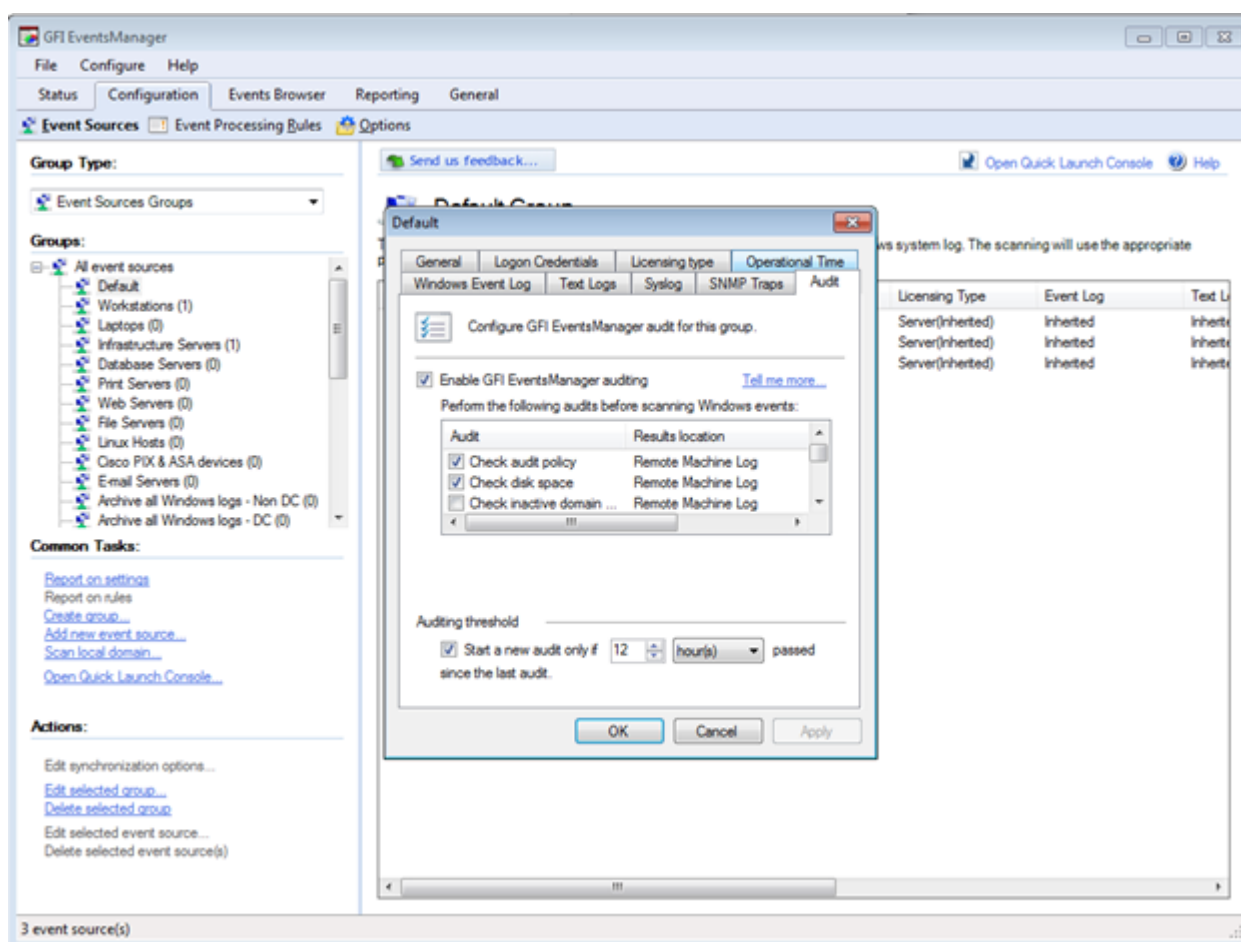
Although most of the information you receive about the systems you monitor comes from logs, GFI EventsManager has also its own audit system based on checks that can detect various situations occurring on Windows machines. For example, this audit can detect the presence of inactive accounts, disks becoming full, inactive domain machines, Microsoft firewall not enabled and more.

When such situations occur, the checks generate custom events that can be processed similar to any other regular event. To test these checks:

1. Open the **Properties** of the local machine and enable the checks from the **Audit** tab.

### NOTE

The checks are executed when the next event scan begins. We also recommend you set the **Auditing threshold** to 12 hours as shown below.



Screenshot 9: Setting the auditing threshold

## 3.3 How to detect possible hacker activities

For Windows machines running a Microsoft Vista or newer operating system, GFI EventsManager has special features that enable you to analyze the network activity occurring on those machines based on **Filtering Platform Connection**

graph from the dashboard enables you to quickly analyze the network activity on various computers based on protocol, port, addresses, user name and application names.

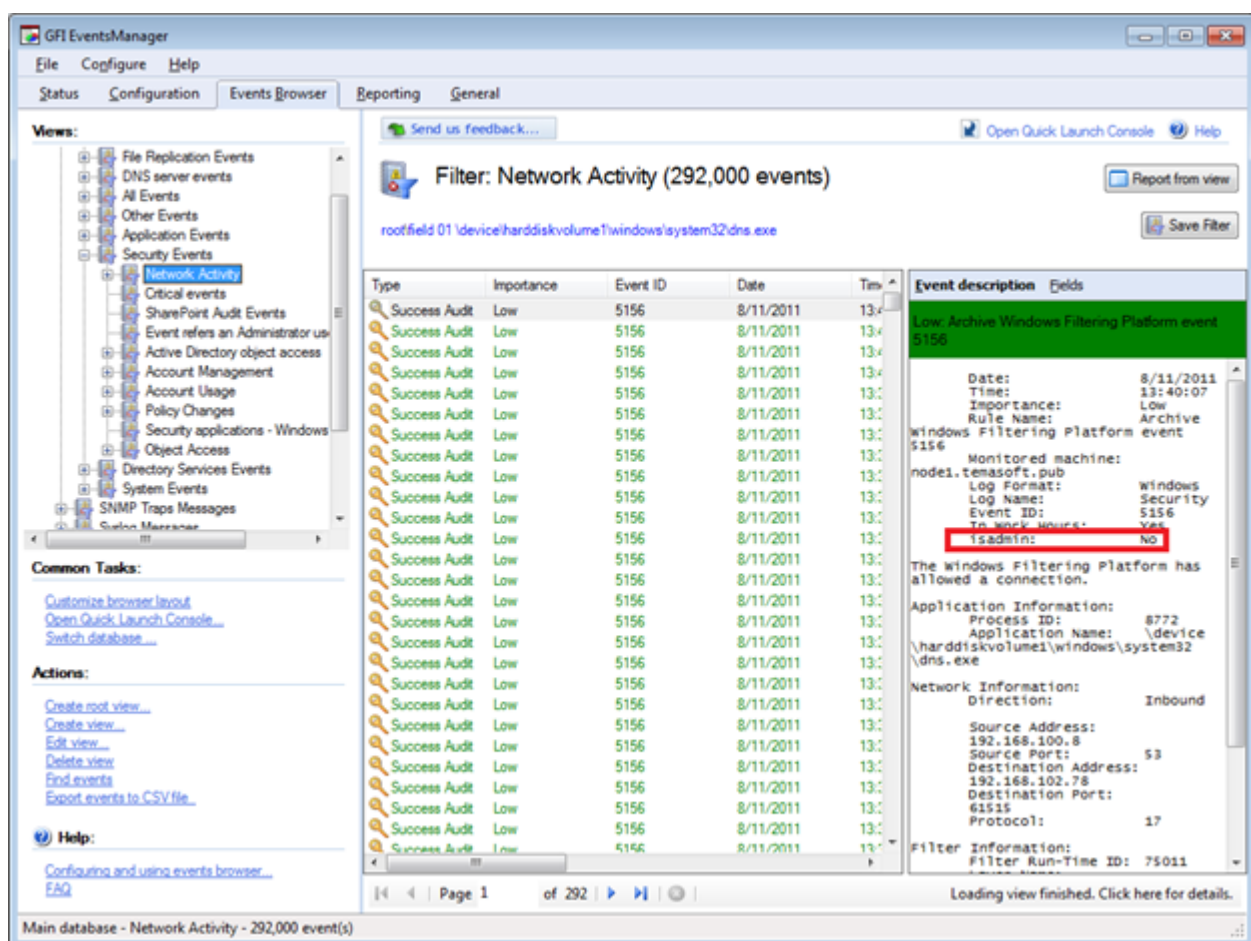
One of the immediate applications of this analysis capability is to detect possible hacker activity. GFI EventsManager has predefined rules that can detect :

- » Suspicious Email activity on the machine.
- » DNS queries originating from system applications.
- » Connections opened by different applications.

At this stage, we recommend you use the **Top Activity Network Events** graph and note the network activity occurring on the two machines you monitor.

### 3.4 How to detect events that refer to administrators

GFI EventsManager enables you to detect Windows events that refer to administrators.



*Screenshot 10: Detect events generated by users with administrative privilege*

## NOTE

For each Windows event there is a field that describes if the event refers to an administrator. You can define filters, rules or custom reports based on this field.

#### NOTE

For practice/evaluation purposes, we suggest you go to the **Browser** tab > **Windows Events** and create a view that will show only the Security events that refer to administrators.

### 3.5 How to anonymize personal data from events

If you need to comply with laws that require personal data from logs that should only be revealed to authorized persons, you can use the **Anonymization** feature in GFI EventsManager since it encrypts the personal data found in Windows Security logs, SQL Server and Oracle audit logs.

If you are interested in this feature we recommend:

- » Enabling anonymization from **Configuration > Options > Console Security > Audit Options > Anonymization**
- » Collecting a few Windows events and see how the anonymized columns look in the Browser.
- » Decrypting the anonymized data by turning off the anonymization.

### 3.6 How to create custom reports

GFI EventsManager includes a reporting engine with many predefined reports you can customize, run or schedule as you like. The reporting engine also enables you to define new reports with flexible layouts. You can also generate reports on the fly, directly from a view in the **Event Browser**.

To create custom reports:

1. From **Reporting** tab > **Reports**, right-click a root folder/folder/root report and select **Create Report**.

**Create Report**

General | Layout | Chart | Schedule | Options | Other

Create new Report to organize in a simpler way the collected events.

Name:  
New General

Description:  
New report description.

Select sort column :  
 ☒ Ascending

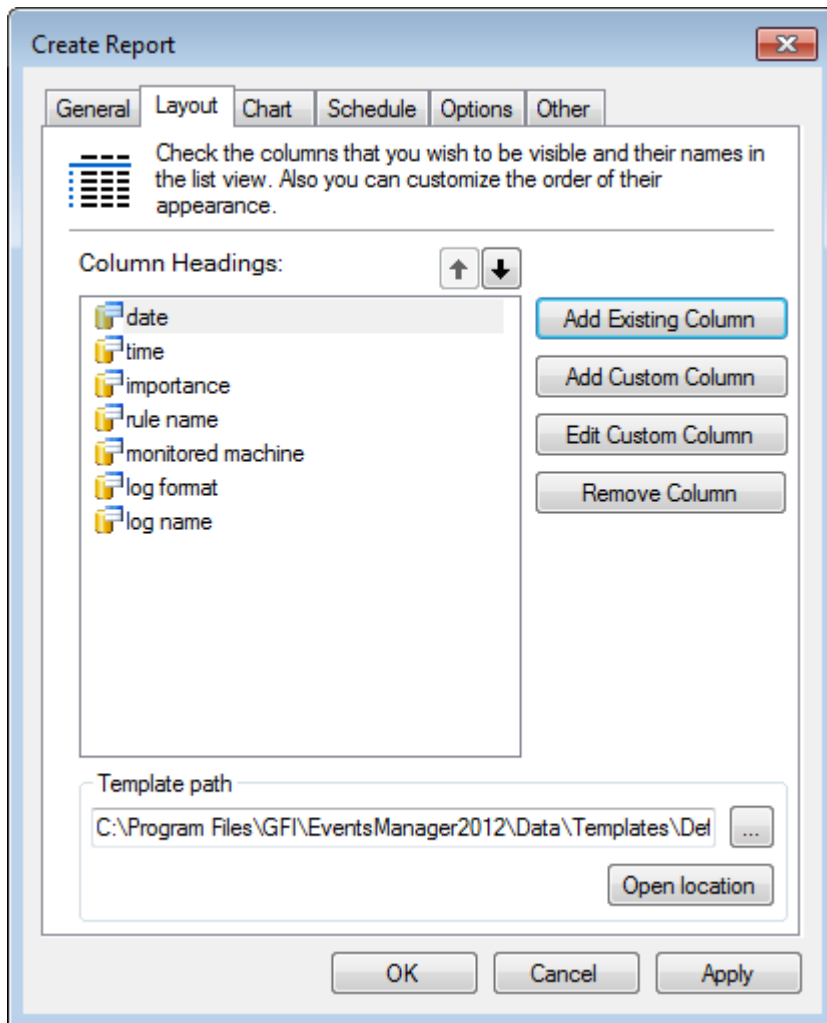
AND ☐ Not

Screenshot 11: Creating a root report

- From the **General** tab, specify a name and description (optional) for the new root report.
- Click **Add** to select a field on which to base the query condition. For the selected field, specify the **Field Operator** and **Field Value**. Click **OK**

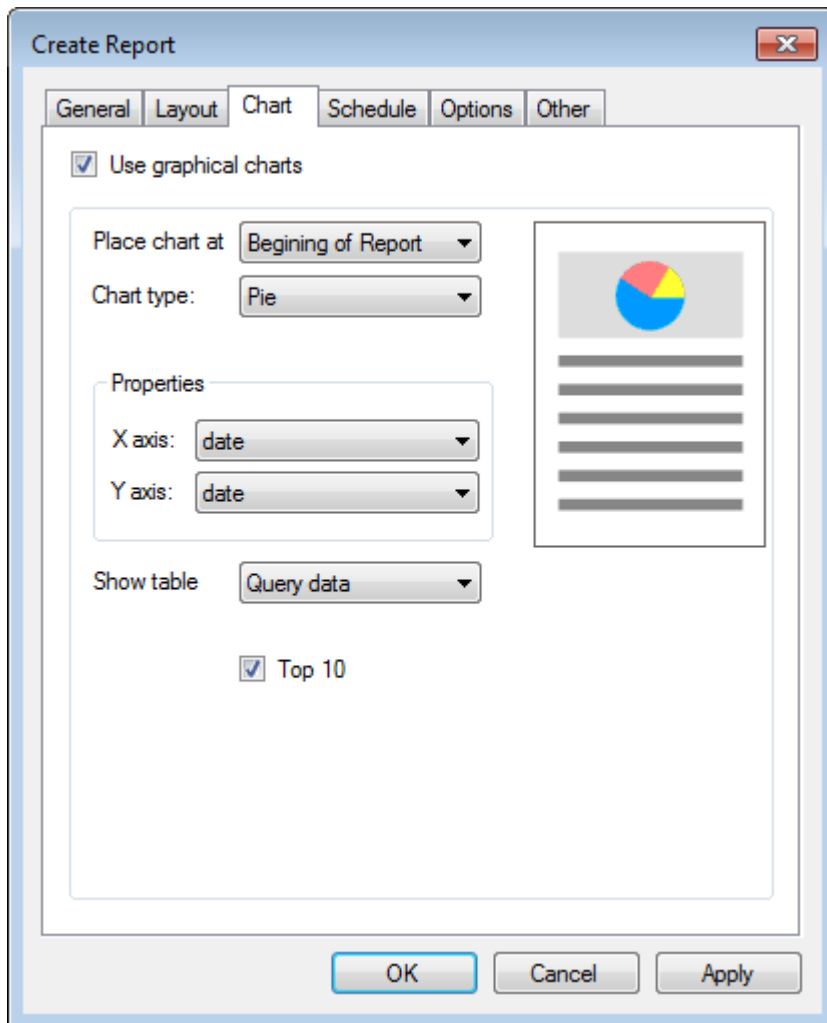
#### Note

Repeat this step until all the required fields are selected.



Screenshot 12: Configuring new root report layout options

4. Click **Layout** tab and add the column headings that you want to be visible in the report. If you have a saved report template, click **Open location** to browse and load your template.



Screenshot 13: Inserting a chart in a new root report

5. (Optional) Click **Chart** tab and select **Use graphical charts** to include graphs in your report.
6. From the **Place chart at** drop-down menu, specify the location of the chart. Select from:
  - » Beginning of Report
  - » End of Report.
7. From **Properties > X axis** and **Y axis**, configure the X and Y Axis properties. I.e. select the data represented in the chart.
8. Select **Top 10** to view the Top 10 records only.

**Create Report**

General Layout Chart **Schedule** Options Other

☐ Inherit from Parent

☒ Use schedule

Generation Time 11:00:11

Recurrence pattern Monthly

☒ Day 1 of every 1 month(s)

☐ The First Day of every 1 month(s)

☒ Send report by email to:

EventsManagerAdministrators

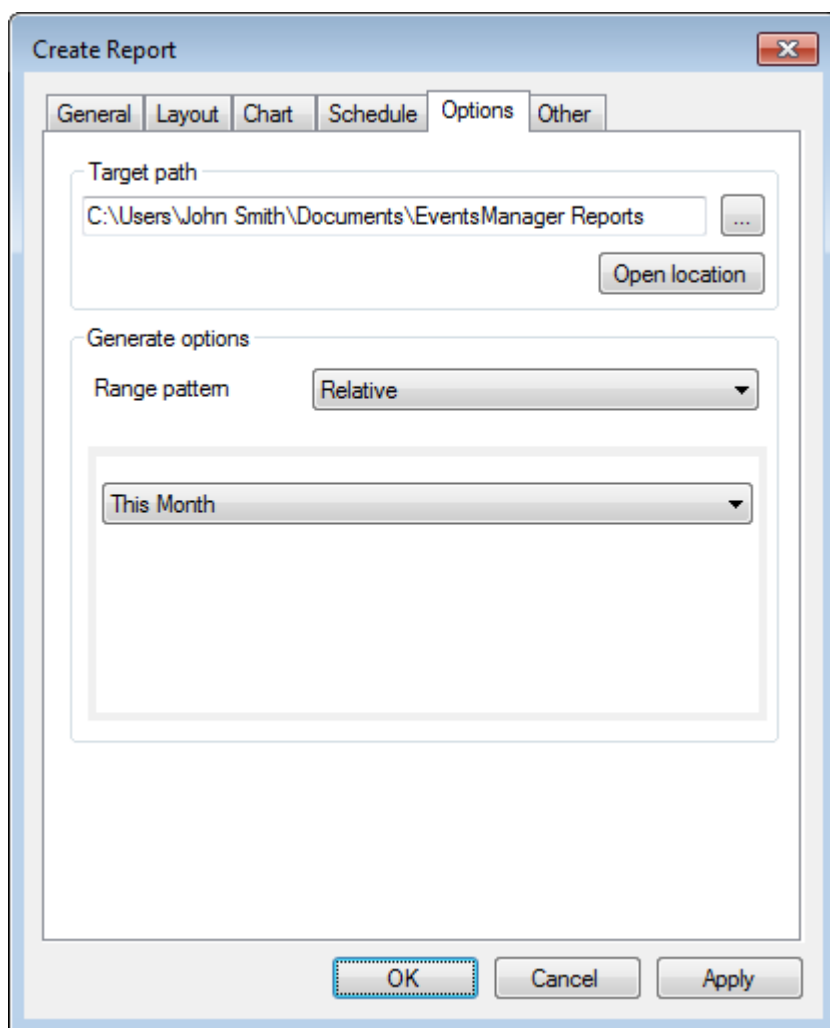
Configure

OK Cancel Apply

Screenshot 14: Configuring the schedule for when the report is generated

9. (Optional) Click **Schedule** tab and configure schedule settings.

10. Select **Send report by email to** and click **Configure** to select the recipients of this report.



Screenshot 15: Create new report Options

11. Click **Options** tab and specify the path to where the report generates to in the **Target path** area.
12. From the **Range pattern** drop-down menu, select the options described in the table below:

Pattern	Description
<b>All Time</b>	Select <b>All Time</b> to generate the report based on information from all the related logs.
<b>Relative</b>	Generate the report based on events from: <ul style="list-style-type: none"> <li>» Today</li> <li>» Yesterday</li> <li>» Last 7 Days</li> <li>» This Month</li> <li>» Last Month.</li> </ul>
<b>Day</b>	Specify a single day that you want to base your report on.
<b>Month</b>	Specify a month and year that you want to base your report on.
<b>Date Range</b>	Specify a <b>From</b> and <b>To</b> date to base report information on events collected in the specified time period.

**Create Report**

General | Layout | Chart | Schedule | Options | **Other**

☒ Split report if contains more than  records.

Max number of records per page

☒ Limit records to

OK Cancel Apply

Screenshot 16: Record limit settings

13. Click **Other** tab to configure report record limits. Available options are described in the table below:

Option	Description
<b>Split report if it contains more than {X} records</b>	Select the checkbox to enable record limit per report. GFI EventsManager automatically creates a new report for every number of records you specify. Example: if you key in 50, 000 and the report contains 150, 000 records, GFI EventsManager generates three reports.
<b>Max number of records per page</b>	Specify the number of records that are displayed in a single page.
<b>Limit records to</b>	Specify the maximum number of records that are included in the report. Records that exceed the limit are ignored.