



GFI EventsManager

Event monitoring, management and archiving

The huge volume of system events that is generated daily is a valuable source of information for network administrators to help them monitor configuration changes, administrative actions, identify system errors and suspected security breaches. This is, however, an overwhelming task without the proper tools. The larger the network, the greater is your need for a solution that allows you to monitor, manage and archive thousands of events that are generated by devices across heterogeneous networks.

GFI EventsManager 8, an award-winning events monitoring, management and archiving solution, supports a wide range of event types such as W3C, Windows events, Syslogs and, in the latest version, SNMP traps generated by devices such as firewalls, routers and sensors. Providing support for devices from the top 20 manufacturers in the world as well as custom devices, GFI EventsManager allows you to monitor an extended range of hardware products, report on the health and operational status of each one and collect data for analysis. You can also track employee activity on the network such as changes made to their PCs, files accessed during the day, meet legal and regulatory compliance such as SOX, PCI DSS, HIPAA and much more.

- Information system and network security: Detect intruders and security breaches
- System health monitoring: Proactively monitor your servers
- Legal and regulatory compliance: An aid to meet regulatory compliance
- Forensic investigations: A reference point when something goes wrong.

Benefits

Why use GFI EventsManager?

- Centralizes Syslog, W3C, Windows events and SNMP Traps generated by firewalls, servers, routers, switches, phone systems, PCs and more
- Increase network uptime and identify problems through real-time alerting
- Fast and cost-effective monitoring and management of the entire network
- SQL Server Auditing for SQL Server 2000, 2005, 2008 and also MSDE & SQL Express
- Unrivalled event scanning performance scalable to over 6 million events per hour
- Certified for Windows Server 2008; Supports Windows Vista

■ Centralized event logging

Event logs are constantly and automatically generated by a user or by an automatic/background process and logs are often stored in disparate locations. GFI EventsManager stores all captured event logs into one SQL database that may also reside remotely. You may also configure scheduled backups of your event logs.

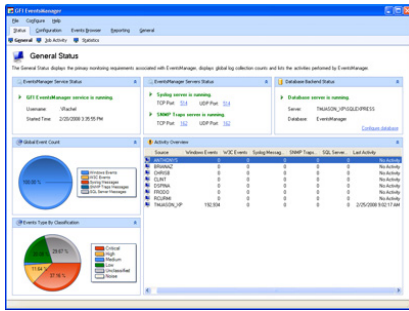
■ Analysis of event logs including SNMP Traps, Windows Event logs, W3C logs and Syslog

As a network administrator, you have experienced the cryptic and voluminous logs that make log analysis a daunting process. GFI EventsManager is a log processing solution that provides network-wide control and management of Windows event logs, W3C logs, and Syslog events generated by your network sources. GFI EventsManager now supports Simple Network Management Protocol version 3 which is the language spoken by low level devices such as routers, sensors, firewalls, etc. Through SNMP users can now monitor a whole range of hardware devices on their infrastructure with the ability to report on the health and operational status of each device.

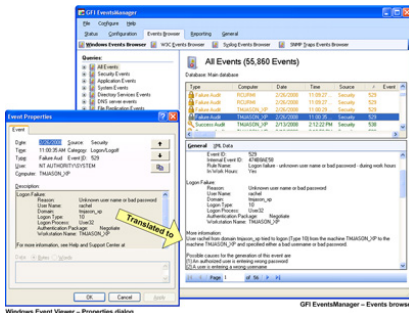
■ Certified for Windows Server 2008; Supports Vista

GFI EventsManager has achieved 'Certified for Windows Server 2008' status and can be installed on, and collect events from Windows Vista and Windows 2008. Although these new platforms use a different log format, GFI EventsManager presents events from various operating systems in the same manner, thus allowing the user to get used to a common structure, irrespective of the platform being monitored. GFI EventsManager also supports Windows 2000, Windows XP and Windows 2003.

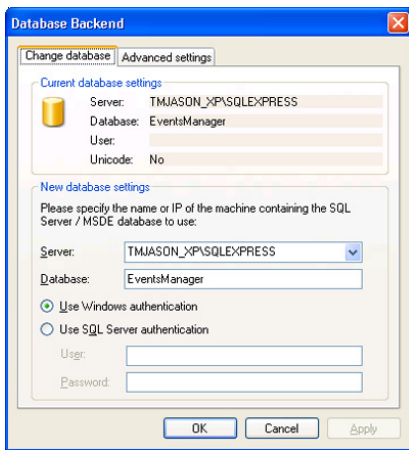
GFI EventsManager



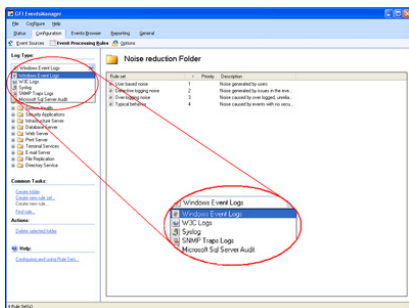
GFI EventsManager management console



Makes cryptic logs easier to understand

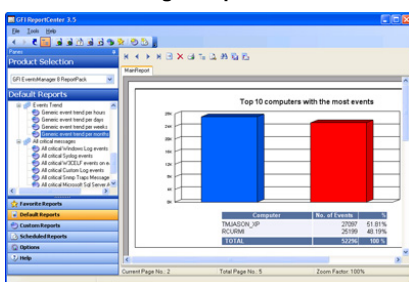


Centralized event logging



Support for multiple log types (Windows event logs, W3C, Syslog, SNMP Traps, Microsoft SQL Server audit)

GFI EventsManager ReportPack



Report showing Top 10 event-generating machines

■ Deeper granular control of events

GFI EventsManager helps you monitor a wider range of systems and devices through the centralized logging and analysis of various log types including Windows events, Syslog, W3C and now SNMP traps that are generated by network resources. Administrators can gather information from Windows machines and third-party devices at a greater level of granularity and also process information at extended tags level and base the decision on what to do with that information on the spot, without further information management.

■ Support for new Devices

Managing SNMP Trap for myriad devices requires the ability to understand the 'language' each manufacturers uses to define events. The definitions and device information are contained in Management Information Base (MIB) definition files which are provided by the manufacturers. GFI EventsManager ships with MIB definitions for the following vendors: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis and others. GFI EventsManager is also capable of importing the MIB files of new devices as soon as these become available.

■ SQL Server Auditing

GFI EventsManager now supports SQL server auditing for all commercial and free versions of SQL Server including 2000, 2005, 2008, MSDE and SQL Express. Auditing allows the user to track and report on SQL server activity such as: Running of SQL statements, altering DB tables, attempts to access data without necessary privileges, etc. This can ensure data in SQL servers is authentic and thus reliable.

■ "Translates" cryptic windows events

Cryptic logs make log analysis a lengthy process. GFI EventsManager "translates" the often cryptic event descriptions to clear, concise explanations and suggestions for action.

■ High performance scanning engine

GFI EventsManager incorporates a totally re-designed event scanning engine that is fine-tuned for maximum scanning performance. Tests demonstrate that it is able to scan and collect up to 6 million events/hr. Furthermore, its plug-in based methodology allows additional features and modules to be integrated without interfering with existing code.

■ Real-time alerts

GFI EventsManager can send you alerts when key events or intrusions are detected. You can trigger actions such as scripts or send an alert to one or more people by email, network messages, and SMS notifications sent through an email-to-SMS gateway or service.

■ Collect events data distributed over a WAN into one central database

You can collect events data from GFI EventsManager installations on multiple sites and locations across your network into a central database using the Database Operations functionality. This enables you to easily monitor thousands of workstations and servers across the network without impacting on bandwidth and storage use. It integrates and centralizes events collected and processed and allows you to backup/restore events on demand. Through database operations you can manage the size of the database – without the need for manual intervention – not only through centralization but by also being able to export events and back them up as needed.

■ Rule-based event log management

GFI EventsManager ships with a pre-configured set of log processing rules that allow you to filter and classify events that satisfy particular conditions. You can run these default rules without performing any configuration or you can choose to customize these rules or create tailored ones that suite your network infrastructure.

■ Advanced event filtering features

GFI EventsManager's powerful filtering sieves through the recorded event logs and allows you to browse the required events without deleting any records from your database backend. You may also selectively highlight specific events using a color or the integrated event finder tool.

■ Event log scanning profiles

Scanning profiles allow you to configure the set of event log monitoring rules that will be applied to a specific computer or to a group of computers and provide a centralized way of tuning event log processing rules. You can also setup a set of rules that only apply to workstations in a particular department. You may also create separate complementary profiles that provide additional and more specialized event log rules on a computer by computer basis.

■ View reports on key security information happening on your network

GFI EventsManager reporter, which ships with the product, allows you to create or customize reports, including standard reports, such as:

- Account usage reports
- Account management reports
- Policy changes reports
- Object access reports
- Application management reports
- Print server reports
- Windows event log system reports
- Events trend reports

■ Helps to comply with PCI DSS and other regulations

As from September 2007 all businesses handling cardholder data – irrespective of size – have to be fully compliant with strict security standards drawn up by the world's major credit card companies. Data logging is key to meeting PCI DSS requirements since logs provide audit trails of all activities in a credit card holder data environment and hence, a comprehensive log management system, such as GFI EventsManager, would provide you with the functionality you need to help you become PCI DSS compliant.

■ Other features:

- Remove "noise" or trivial events that make up a large ratio of all security events
- Real-time 24 x 7 x 365 day monitoring and alerting
- Graphically monitor the status of GFI EventsManager and your network through the built-in status monitor
- Report scheduling and automated distribution via email.

■ You're in good company...

Many leading companies have chosen GFI EventsManager. Here are just a few: Primerica, Pepsico France, Royal & Sunalliance USA Inc., ATP, Ceridian Canada and many more.

System requirements

- .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 or later
- Access to MSDE / SQL Server 2000 or later

Awards



Download your evaluation version from <http://www.gfi.com/eventsmanager/>

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com