



**Information Systems
& Network Security**



**Legal & Regulatory
Compliance**



**Forensic
Investigations**



**System Health
Monitoring**

Event monitoring, management and archiving made easy

The huge volume of system events generated daily is a valuable source of information for organizations to meet legal and compliance obligations and address IT security risks. Growing threats to business continuity calls for an approach that includes real-time monitoring of the network and also the ability to report and analyze this data to meet stringent and more demanding legal or compliance obligations. Without the proper tools however, this is an overwhelming task. With thousands of customers and competitive pricing, GFI EventsManager™ eases the burden on administrators and simplifies the complexity of events management, archiving and reporting.

GFI EventsManager is an events monitoring, management and archiving solution that helps organizations meet legal and regulatory compliance such as SOX, PCI DSS, and HIPAA. This award-winning software supports a wide range of event types such as W3C, Windows events, Syslog and, in the latest version, SNMP traps generated by devices such as firewalls, routers and custom devices.

Award-winning solution
Competitive pricing
Thousands of customers

BENEFITS



- Increases network uptime and identifies problems through real-time alerts and dashboard
- Fast and cost-effective monitoring and management of the entire network
- Meets legal and regulatory compliance (SOX, PCI DSS, HIPAA)
- Centralizes Syslog, W3C, Windows events, SQL Server audits and SNMP Traps generated by firewalls, servers, routers, switches, phone systems, PCs and more
- Unrivaled event scanning performance scalable to over 6 million events per hour
- Built-in processing rules which provide for effective out-of-the-box event classification and management of devices from Cisco, 3Com, IBM, HP and many others



GFI EventsManager™
Automated network-wide event log management

GFI EventsManager also helps you to:

- Gather information from all supported devices and log types at a high level of granularity and depth
- Obtain a detailed view of what is happening across various environments thanks to the variety of log types which are supported
- Track and report on SQL server activity such as alteration of DB tables and attempts to access data without necessary privileges
- Provide reliable data sources for forensic investigations.

GFI EventsManager for network security

GFI EventsManager acts as a host-based intrusion detection system by analyzing security events in real time. This way you can detect intruders and security breaches without having to install a network-based intrusion detection system.

GFI EventsManager for system health monitoring

Using GFI EventsManager, you can proactively monitor your mission-critical servers. You can also monitor events generated by Microsoft ISA Server, Exchange Server, SQL Server and IIS, and prevent network disasters from occurring. For example, you can monitor email queues, SMTP gateways, MAPI availability, bad hard disk blocks, disk space and more.

GFI EventsManager for regulatory compliance

GFI EventsManager is an aid to meet the log retention and log reviewing requirements of regulatory bodies and acts including: Basel II, PCI Data Security Standard, Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, HIPAA, FISMA, USA Patriot Act, Turnbull Guidance 1999, UK Data Protection Act, EU DPD.

GFI EventsManager for forensic investigation

Event logs are a reference point when something goes wrong and provide a history of events that is often required when you need to carry out forensic investigations. GFI EventsManager guarantees a timely in-house forensic investigation of event logs – freeing you of expensive outsourced consultancy and audit costs.

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

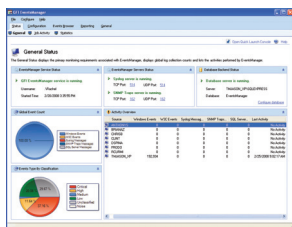
generated by network resources. Administrators can gather information from Windows machines and third-party devices at a greater level of granularity and also process information at extended tags level and base the decision on what to do with that information on the spot, without further information management.

Analysis of event logs including SNMP Traps, Windows event logs, SQL Server audit logs, W3C logs and Syslog

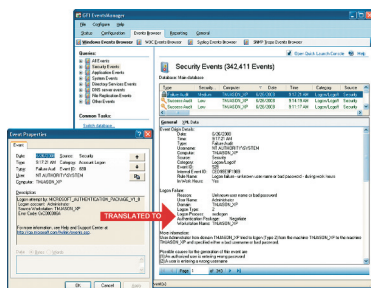
As a network administrator, you have experienced the cryptic and voluminous logs that make log analysis a daunting process. GFI EventsManager is a log processing solution that provides network-wide control and management of Windows event logs, W3C logs, SQL Server audit logs and Syslog events generated by your network sources. GFI EventsManager supports Simple Network Management Protocol, 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.

Other features:

- Centralized event logging
- Real-time 24 x 7 x 365-day monitoring and alerting
- High-performance scanning engine
- Collects events data distributed over a WAN into one central database/ and/or auto-archives all event logs to files
- Rule-based event log management
- Powerful dashboard
- Advanced event filtering features including one-click rule and filter creation
- Event log scanning profiles
- View reports on key security information happening on your network
- Helps to comply with PCI DSS and other regulations
- Supports for new devices
- SQL Server Auditing
- 'Translates' cryptic Windows events
- Multi-functionality to meet different corporate requirements
- Removes 'noise' or trivial events that make up a large ratio of all security events
- Reports scheduling and automated distribution via email
- Supports for virtual environments



GFI EventsManager management console



Makes cryptic logs easier to understand

System requirements

- Windows 2000/2003/XP/Vista/2008/7
- .NET framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 or later
- Access to MSDE / SQL Server 2000 or later.

For more information and to download your free evaluation version please visit <http://www.gfi.com/eventsmanager/>



GFI EventsManager[™]
Automated network-wide event log management

Contact us

Malta
Tel +356 2205 2000
Fax +356 2138 2419
sales@gfi.com

UK
Tel + 44 (0)870 770 5370
Fax + 44 (0)870 770 5377
sales@gfi.co.uk

USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
ussales@gfi.com

Asia Pacific - South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

For more GFI offices please visit <http://www.gfi.com/company/contact.htm>