



**Information systems and network security**

**Legal and regulatory compliance**

**Forensic investigations**

**System health monitoring**

***Event monitoring, management and archiving made easy***

The huge volume of system events generated each day is a valuable source of information for system administrators. Effective infrastructure management helps ensure a reliable network, secure systems and high availability, while enabling organizations to meet their legal and compliance obligations. Real-time network and system monitoring is needed to achieve business continuity and security, but with potentially hundreds of thousands of system events being generated daily, managing them is a challenge.

GFI EventsManager™ eases the burden on administrators by collecting, managing and identifying infrastructure problems as they happen. It makes a monumental task manageable and allows a faster, more targeted response to any issue as it arises. Proactive management leads to increased uptime and real-time security monitoring. GFI EventsManager supports a wide range of event types such as W3C, Windows events, SQL Server audit events, Oracle audit events, Syslog and SNMP traps generated by various machines, servers and devices.

**Award-winning solution**  
**Competitive pricing**  
**Thousands of customers**

**BENEFITS**



- » Protect your business by detecting and analyzing security incidents through event logs
- » Benefit from network uptime and identify problems through real-time alerts and dashboard
- » Fast and cost-effective monitoring and management of the entire network
- » Invaluable companion to help achieve regulatory compliance with SOX, PCI DSS, HIPAA and many more
- » Centralized Syslog, W3C, Windows events, SQL Server and Oracle audits and SNMP traps generated by firewalls, servers, routers, switches, phone systems, PCs and more
- » Built-in processing rules enabling out-of-the-box alerting, classification and management of events generated by various systems and devices from CISCO, 3Com, HP and others.



**GFI EventsManager™**  
*Event log monitoring, management and archiving*

### 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 Oracle and SQL server activities such as alteration of DB tables, attempts to access data without necessary privileges, etc.
- » Provide reliable data sources for forensic investigations.

### GFI EventsManager for network security

GFI EventsManager is able to analyze security events in real time. This way you can detect security incidents and analyze them in detail to find out who is responsible for them.

### GFI EventsManager for system health monitoring

Using GFI EventsManager, you can proactively monitor your mission-critical network devices and servers. You can monitor firewalls, sensors, routers and the events generated by Microsoft ISA Server, SharePoint, 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, providing a history of events that is often required when you need to carry out forensic investigations. GFI EventsManager provides 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 SNMP traps

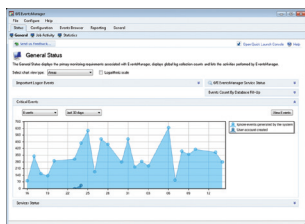
that are generated by network resources. Administrators can gather information from Windows machines and third-party devices at a greater level of granularity and also process information at extended tags level and base the decision on what to do with that information on the spot, without further information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

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

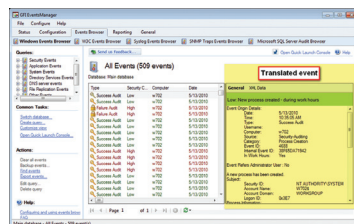
As a network administrator, you have experienced the cryptic and voluminous logs that make log analysis a daunting process. GFI EventsManager is a log processing solution that provides network-wide control and management of Windows event logs, W3C logs, SQL Server and Oracle audit logs and Syslog events 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 24x7 x 365-day monitoring and alerting
- » High-performance scanning engine
- » Collection of events data distributed over a WAN into one central database/and/or auto-archiving of all event logs to files
- » Rule-based event log management
- » Auto update mechanism
- » Powerful dashboard
- » Advanced event filtering features including one-click rule and filter creation
- » Event log scanning profiles
- » Reports on key security information happening on your network
- » Tracking of user activity on SharePoint
- » Assistance in complying with PCI DSS and other regulations
- » Support for new devices
- » SQL Server auditing
- » Support for Oracle server auditing for Oracle 9i, 10g, 11g
- » 'Translation' of cryptic Windows events
- » Multi-functionality to meet different corporate requirements
- » Removal of 'noise' or trivial events that make up a large ratio of all security events
- » Reports scheduling and automated distribution via email
- » Events can be exported into customizable HTML files
- » Support for virtual environments.



GFI EventsManager management console



Makes cryptic logs easier to understand

### System requirements

- » Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7
- » .NET framework 2.0
- » Microsoft Data Access Components (MDAC) 2.8 or later
- » Access to SQL Server 2005 (any edition) or newer.

Download your free trial from <http://www.gfi.com/eventsmanager>

**Microsoft**  
GOLD CERTIFIED  
Partner

### 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.html>

**GFI EventsManager**<sup>™</sup>

Event log monitoring, management and archiving