



GFI EventsManager

Network-wide event log management

Event logs are a valuable tool to monitor network security and performance that are often underutilized due to their complexity and volume. As organizations grow in size, they require a more structured approach towards event log management and retention. A recent survey carried out by SANS Institute found that 44% of system administrators do not keep logs more than a month.

Proper log management helps you to meet several objectives including:

- Information system and network security
- System health monitoring
- Legal and regulatory compliance
- Forensic investigations

GFI EventsManager collects data from all devices that use Windows event logs, W3C, and Syslog and applies the best rules and filtering in the industry to identify key data. This allows you to track when staff swipe their fob, pick up the phone to call home, turn on their PC, what they do on their PC and which files they access during their work day. GFI EventsManager also provides you with real-time alerting when critical events arise and suggests remedial action.

■ Network-wide analysis of event logs made easy

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 includes an intelligent event processor which processes logs and presents information in a centralized, easy and user-friendly fashion.

■ "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.

■ 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.

■ 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.

■ Extended event log support

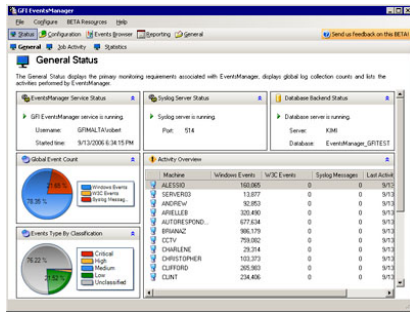
GFI EventsManager processes various event log types including Windows event logs, Syslog events, and W3C event logs. This allows you to collect more data from the different hardware and software systems that are most commonly available on a typical corporate network.

Benefits

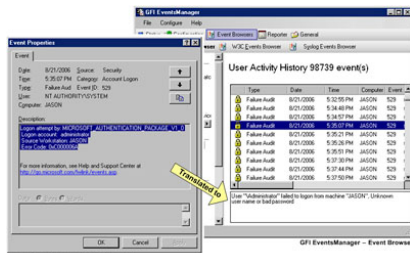
Why use GFI EventsManager?

- Centralizes Syslog, W3C and Windows events generated by firewalls, servers, routers, switches, phone systems, PCs and more
- Wizard assisted configuration simplifies end-user operation and maintenance
- Unrivalled event scanning performance scalable to over 6 million events per hour
- Preconfigured event processing rules for effective out-of-the-box event classification and management
- Automated 24/7 event activity monitoring and alerting
- Powerful reporting for effective network activity monitoring and immediate ROI.

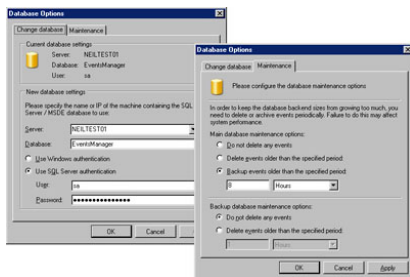
GFI EventsManager



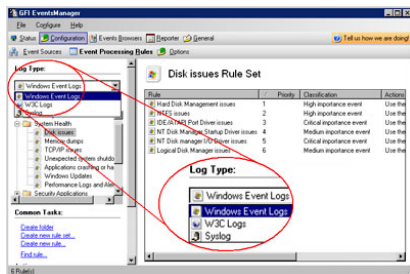
GFI EventsManager management console



Makes cryptic logs easier to understand

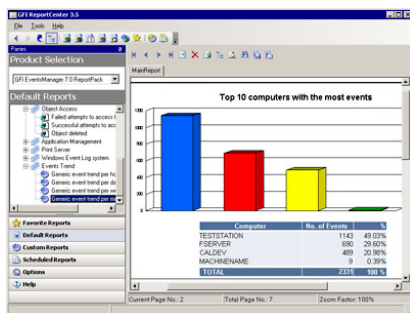


Centralized event logging



Support for multiple log types (Windows event logs, W3C, Syslog)

GFI EventsManager ReportPack



Report showing Top 10 event-generating machines

■ 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 enables you to identify security trends. Use its standard reports – which you can customize – or create custom reports from scratch. The standard reports include:

- 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

■ A Swiss knife to meet different corporate requirements

GFI EventsManager helps your organization to address the following 4 areas:

- 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.

■ Other features:

- Remove “noise” or untrivial 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) 2.6 or later
- Access to MSDE / SQL Server 2000 or later

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

GFI Software
Unit 2, St. John's Mews
St. John's Rd. Hampton Wick
Kingston-upon-Thames
Surrey KT1 4AN, 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 Software GmbH
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49(0) 40 3068 1000
Fax +49(0) 700 3068 1010
sales@gfisoftware.de

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 05 Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

