# How to perform network-wide security event log monitoring

Using GFI EventsManager™ for intrusion detection
and essential auditing of security event logs

This white paper explains the need to monitor
security event logs network-wide and how you can
achieve this using GFI EventsManager.
It is written by Randy Franklin Smith, author of
the in-depth series on the Windows security log in
Windows 2000 & .NET Magazine.

**GFI®**

# Contents

## Introduction

Microsoft Windows machines have basic audit facilities but they fall short of fulfilling real-life business needs (i.e., monitoring Windows computers in real-time, periodically analyzing security activity, and maintaining a long-term audit trail). Therefore, the need exists for a log-based intrusion detection and analysis tool such as GFI EventsManager. This paper explains how GFI EventsManager's innovative architecture can fill the gaps in Windows' security log functionality – without hurting performance and while remaining cost-effective. It discusses the use of GFI EventsManager to implement best practice and fulfill due diligence requirements imposed by auditors and regulatory agencies; and provides strategies for making maximum use of GFI EventsManager's capabilities.

About the writer: This white paper is written by Randy Franklin Smith, Windows event log monitor guru and writer of an in-depth series on the Windows security log for Windows 2000 & .NET Magazine (now Windows IT Pro Magazine).

## How GFI EventsManager works

### Architectural overview

GFI EventsManager performs intrusion detection and network security reporting by monitoring the security event logs of all Windows 2000/NT/XP/2003 servers and workstations in the organization. It alerts you in real-time about possible intrusions and attacks.

To ensure proper integration with the overall Windows environment, GFI EventsManager uses standard Windows technology such as Microsoft Message Queuing (MSMQ), Microsoft Management Console (MMC), Microsoft Windows Installer, and Open Database Connectivity (ODBC).
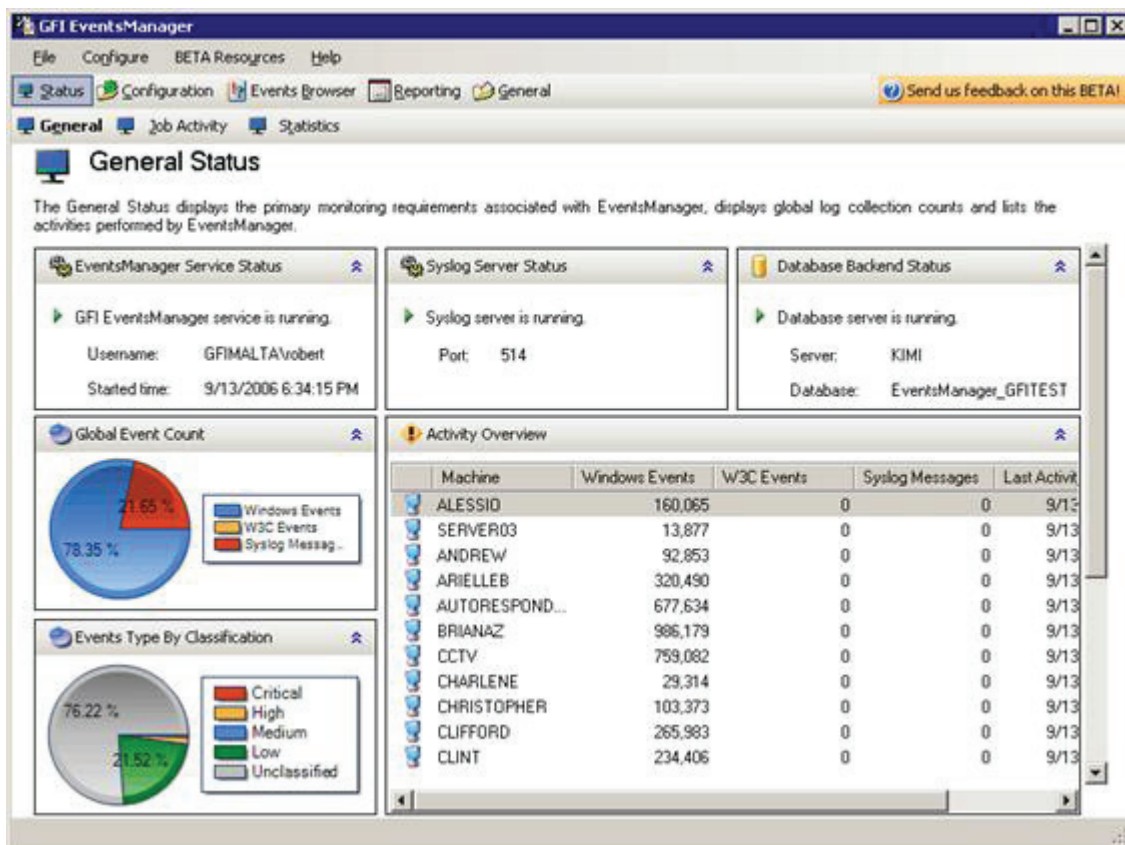
Implementing network-wide monitoring with GFI EventsManager requires little effort because you don't need to install software on each computer you want to monitor. The administrator installs GFI EventsManager on only one host computer, and then simply registers all the other systems to be monitored. The product's Collector Agent then uses native Win32 APIs to collect security events from the monitored computers. The Collector Agent stores these events in a Microsoft Access database or on a Microsoft SQL Server. This ODBC architecture lets administrators use standard reporting tools, such as Crystal Decisions' Crystal Reports, to create custom reports.

Next, GFI EventsManager's Alerter Agent compares the collected events to a Categorization Rules table, and then classifies the events as low security, medium security, high security, or critical. The Alerter Agent sends SMTP notification of critical events to an administrator-configured email address (e.g., a pager) to inform administrators immediately of possible intrusion attempts. For each monitored computer, the administrator can specify event-collection frequency, identify normal operating times, and specify a computer security level of low, medium, or high. The security-level setting lets the Alerter Agent interpret as 'more severe' any suspicious events on systems that host more sensitive information or processes, thus reducing the amount of false positives reported to the administrator.

Administrators can use GFI EventsManager's enhanced event viewer or the GFI EventsManager Reporter to perform regular analysis of all security events. To ensure a proper balance between resource consumption and timely alerts, administrators can specify a different collection frequency for each computer. The Archiver Agent periodically moves older activity from the active database to an archive for long-term storage. GFI EventsManager uses MSMQ technology to maintain high-performance communication between its internal agents.

### Real-time monitoring and categorization of security events

The heart of GFI EventsManager's intelligent alert capability is the Event Processing Rules node of the GFI EventsManager MMC Configuration snap-in.

*GFI EventsManager management console*

GFI EventsManager's default security categorization rules are designed to help the product recognize and notify the administrator of important events but avoid disturbing the administrator with false alarms. The rules let GFI EventsManager look for telltale indicators, such as events that occur at unusual hours or on high-security computers. Lower-priority events do not trigger an immediate alert but are always available for daily or weekly analysis by the administrator. GFI EventsManager categorizes each event as low security, medium security, high security, or critical. To do so, the product analyzes the event ID (e.g., the event IDs that correlate to failed logon, account lockout, file access) and the characteristics – including OS, domain role, security level, and normal operating hours - of the computer on which the event occurred, and then applies the categorization rules to this information. Administrators can tailor GFI EventsManager's processing rules according to their network's specific characteristics.

## Categorization based on where event is collected from

GFI EventsManager deals with the arcane differences in the way Windows NT and Windows 2000/XP/2003 log events by adapting to the particular OS release it is running on. The product also recognizes the difference between workstations, member servers, and domain controllers, and interprets an event differently according to the computer's domain role.

Take network logons as an example of why the product must distinguish between OSs and domain roles. When someone connects to a computer from over the network (e.g., by accessing a shared folder), Windows NT logs event ID 528 with logon type 2, whereas Windows 2000 logs event ID 540. Because GFI EventsManager considers the OS, it can correctly identify the event ID, according to whether the event occurs on a Windows NT or Windows 2000/XP/2003 system. Network logons to domain controllers or servers are common and shouldn't be regarded as suspicious during normal working hours. However, users do not typically need to access resources on other users' workstations.

Network logons to workstations should be considered suspicious because attackers that gain remote access to a workstation can impersonate the user of that workstation and employ that user's credentials to access other servers on the network. Consequently, GFI EventsManager classifies network logons to workstations as being of higher severity than network logons to domain controllers or servers.

Network-wide monitoring of workstations as well as servers

Because Windows security activity is scattered among all computers in the domain, broad deployments of GFI EventsManager reap the most value. By deploying GFI EventsManager to monitor all workstations, member servers and domain controllers in a network, the product can form a comprehensive security picture. In a broad deployment scenario, GFI EventsManager's default categorization rules recognize specific scenarios, including:

» Failed logons

» Account lockouts

» After-hours account creation and group-membership changes

» After-hours logons to high-security systems

» Entry to user workstations through network logons

» Audit-policy changes

» Cleared security logs

» Successful or failed file access (including access to specific filenames).

An event can be interpreted in a variety of ways, based on circumstances. Therefore, when GFI EventsManager categorizes an event, the product includes a description that specifically explains the categorization decision. The description also explains what the event might indicate and recommends further steps the administrator can take to confirm and respond to the situation.

By default, GFI EventsManager reports critical events through SMTP email, but administrators can choose for notification to occur at a lower event-security level. To stay on top of lower-severity events for which no notifications are sent, administrators can follow the recommendations in the section below on due diligence analysis.

## Due diligence analysis

To satisfy the demands of general-controls reviews by public auditors and regulatory agencies (Sarbanes-Oxley Act), corporations should complement real-time monitoring with a regular review of lower-severity events. To help administrators follow this recommendation without devoting themselves full-time to the task, GFI EventsManager includes several pre-built reports. Administrators can follow up on events of every severity simply by reviewing the Yesterday's High Security Events, Last Week's Medium Security Events, and Last Month's Low Security Events reports on a daily, weekly, or monthly basis. Additional reports let administrators review the current day's activity or review medium and low-security events on a more frequent basis.

## Strategies to reap maximum value

GFI EventsManager provides flexible security log management functionality, but when deploying the product, it is important to consider individual business needs and to take steps to minimize false positive alerts. When planning a GFI EventsManager deployment, the administrator should consider the relative security level of his or her computers, the potential performance load in relation to the necessary timeliness of alerts, and specific risk scenarios for his or her environment.

## Select the proper security levels for computers

GFI EventsManager relies on the administrator to select the proper security level for each monitored computer. When registering a workstation, the administrator should consider the user assigned to the workstation. The workstations of users who have access to important resources, such as administrators and users who conduct financial transactions, should be configured as high security. Other workstations that might be classified as high security are those that are located in the computer room and those that host a critical process, such as the corporation's physical-access system. The workstations of users who have little access to critical information or processes should be configured as low security. The medium security classification can be used for the workstations of typical users who fall between these two extremes.

Given domain controllers' important security role, administrators should classify these computers as medium security or high security. Typically, computers in the demilitarized zone (DMZ) – e.g., email gateways and web servers – should be classified as high security, as should servers that host human resources, financial or research and development data. Application and database servers usually host important information or processes and should typically be classified as medium security or high security. Low and medium-security levels should be used for file servers that host general departmental information. Companies that have an existing information security classification system can use that system to identify user workstations and servers that are involved with confidential data.

## Balance resource consumption with timely alerts

The frequency with which GFI EventsManager collects events from each monitored computer has an impact on the CPU utilization of those computers and on the network's overall bandwidth. The higher a computer's security level, the more frequently the computer will be queried, but the computer's role also affects collection frequency. A high-security workstation, for example, is usually less important than a high-security server. The table below shows recommended collection frequencies according to a system's domain role and security level. Given the number of workstations in most corporate environments, querying workstations less often will result in the greatest network-bandwidth savings.

| Role | Security Level | Collection Frequency |
| --- | --- | --- |
| Domain Controller | High | 1 minute |
| | Medium | 5 minutes |
| | Low | 15 minutes |
| Member Server | High | 1 minute |
| | Medium | 5 minutes |
| | Low | 1 hour |
| Workstation | High | 5 minutes |
| | Medium | 6 hours |
| | Low | 1 day |

*Recommended collection frequencies*

## Ensure security log maintenance and integrity

Technically, a well-automated attack on a poorly configured system could let an intruder gain Administrator authority on the computer and clear the log before GFI EventsManager's next collection. However, Windows faithfully records a specific event whenever the log is cleared - even when auditing has been disabled – and by default GFI EventsManager classifies that event as a critical event on every system.

Therefore, make it a policy never to clear a security log manually on computers monitored by GFI EventsManager. (This policy is best practice in any case because it ensures that events are never lost and preserves accountability among administrators.)  By default, GFI EventsManager automatically clears the security log each time the program collects events, so manually clearing the log is never necessary.

Windows requires a configured maximum log size for each computer. When the log reaches this preset limit, the OS stops logging activity. Thus, if the log fills up between GFI EventsManager's collections, important activity could be lost. Administrators should configure each system's maximum security-log size according to GFI EventsManager's collection frequency for that computer and the amount of activity on the computer. For systems with a high GFI EventsManager collection frequency, even an unreasonably small log will not have an opportunity to fill up. However, given today's available disk sizes, there is little point in setting a small

log size. Administrators can remove any uncertainty simply by using a standard Windows event log size of between 5MB and 10MB. In an Active Directory (AD) environment, administrators can easily use a Group Policy Object (GPO), linked to the domain root, to configure Windows 2000 computers with a standard log size. Administrators must manually configure Windows NT computers as well as Windows 2000 computers that are not managed by AD.

Windows can be configured to crash when the security log fills up. For extremely critical high-security computers or to meet legal auditing requirements (e.g., on systems that control wire transfers), this setting might be necessary. However, to minimize the possibility of such a crash, administrators should set short GFI EventsManager collection intervals and a log size large enough to guarantee that the computer can't process enough activity to fill the log during this interval.

## Use file-access auditing for internal security

Windows file auditing lets administrators enable auditing on selected files for specific types of access. Windows file auditing is most useful for monitoring how users are accessing documents such as Microsoft Excel and Microsoft Word files. However, this type of auditing can also be used to monitor, for example, changes to folders that contain executables or unauthorized attempts to access database files. Administrators can audit failed or successful attempts to open a given file or folder for read, write, delete and other types of access. (To monitor changes to an object, enable auditing for successful writes. To monitor users who try to read files they aren't authorized to read, enable auditing for failed reads.)

Note that Windows logs potential, not definite changes: Object audit events are trapped at the time an application opens the object for the requested types of access. For example, a user might open a Word document for read and write access but simply close the document without making any changes. In that case, Windows will log an open event (event ID 560) and a close event (event ID 562) to show that the user opened the object for write access.

As you would expect, GFI EventsManager includes categorization rules for all object events. But GFI EventsManager also provides the capability to promote object-access events that are connected with important (as specified by the administrator) files or directories. This ability lets an administrator enable auditing for as many files and folders as he or she wishes, whilst at the same time configure GFI EventsManager to pay special attention to crucial files and folders. The administrator simply configures auditing for all desired objects, then configures GFI EventsManager to promote to critical status all events that are connected with specified file or folder names.

Windows does a good job of recording successful and failed access to objects, but object auditing is the most laborious type of auditing to analyze because of the volume of information that it typically produces. To detect important file-level activity without spending hours perusing security logs, administrators should combine GFI EventsManager with a well thought out object auditing configuration. When configuring object auditing, an administrator must consider three vectors:

» Which objects to audit

» Which subjects (i.e., users or groups) to track for each object

» Which types of access to audit for each subject.

When deciding which objects to audit, administrators should remember that GFI EventsManager can be configured to pay special attention to a subset of those objects. Therefore, the primary consideration is conservation of system resources. The more objects audited, the more CPU time, network bandwidth, and disk space consumed.

When deciding which users or groups to track for a given object, the best choice is usually the 'Everyone' group. Limiting the subjects might expose a company to claims of unfairness or targeting if the security log is ever used as part of a personnel action. Using groups other than 'Everyone' as subjects is risky because important access events can be missed if someone is accidentally granted object access.

Deciding which types of access to audit deserves extra consideration. First, this vector is an important throttle

for controlling how much "noise" is logged. Generally, any type of successful read access should be ignored; otherwise the log will quickly become saturated with innocuous events. Successful write attempts are useful when you need to know who might have changed an object or need to detect suspicious changes to objects (e.g., HTML, image or Active Server Pages – ASP files on a web server) that should be updated only under controlled circumstances. Auditing failed read or write attempts can identify unauthorized users who tried to open an object but were successfully prevented by the object's access control list (ACL).

The one situation in which limiting auditing to a specific group (rather than the 'Everyone' group) is useful is when the administrator wants to be alerted when an object's ACL fails to prevent an inappropriate user from accessing an object in a certain way. For example, a financial services company might have both an investment banking and a brokerage practice. To prevent insider trading, the brokers should never be able to access the investment bankers' Access database. To implement a failsafe, the administrator can configure Windows to audit successful read attempts by the Brokers group on the investment-banking database. That way, even if the database's ACL is accidentally weakened or a broker is accidentally added to the Investment Bankers group, Windows will detect the broker when he or she accesses the database. If the administrator has configured GFI EventsManager to promote events connected with the filename of the investment banking database, the administrator will be notified as soon as the access occurs.

This example demonstrates the importance of properly limiting the users, groups and types of access that you configure Windows to audit. You can configure GFI EventsManager to monitor only specific objects, but the types of access (e.g., failed read, successful read, failed write or successful write) that the product tracks are dependent on the types of access you configure in Windows. Therefore, you should try to configure only the necessary types of Windows auditing, depending on which types of access you want GFI EventsManager to consider critical. For example, suppose you want to monitor a file payroll.xls for failed reads. If you turn on Windows auditing for all types of access, then configure GFI EventsManager to monitor for payroll.xls events; GFI EventsManager will alert you not only when someone accesses the file for a failed read, but every time anyone accesses the payroll.xls in any way. To prevent this overload of alerts, you need to enable Windows auditing for failed reads only.

## Detect web server intrusion and defacement

For web servers, real-time security log monitoring is extremely important and effective because identifying suspicious activity on web servers is easier than on internal-network servers. File access auditing is especially valuable in detecting defacement. A web server configured according to best practice will have clearly defined folders for HTML, ASP and image files. These files are fairly static compared to databases or other files that are modified in response to people browsing the website. By configuring Windows to audit any successful changes to these directories and configuring GFI EventsManager to promote access events connected with filenames in these directories, the administrator will be notified immediately of any changes to the website. To prevent false positives resulting from legitimate updates to a website, it will be necessary to temporarily disable auditing of successful object access events. Doing so will prevent Windows from recording the updates. If the administrator simply wants to prevent alerts from being sent, an alternative is to remove the relevant folder name from GFI EventsManager's special watchlist. The changes will still be logged by Windows and classified in GFI EventsManager's database according to the product's categorization rules, but the events will not be promoted to critical and thus no alert will be sent.

## Hold administrators accountable

One of the problems inherent in the Windows Security log is a lack of administrator accountability. Although Windows records administrator activity (e.g., account maintenance and privilege use), the Security log is always vulnerable to an administrator who decides to clear the log, disable auditing or shut down the system and tamper directly with the log file by booting a DOS 3.5" disk.

A secure installation of GFI EventsManager can address those problems and enforce accountability. GFI EventsManager's default configuration provides pre-built administrator activity reports and recognizes log clearing and audit policy changes as critical events. Because GFI EventsManager frequently collects events from high-security computers to a physically separate database, securing the product installation means

physically securing the computer that hosts the GFI EventsManager database. The computer should also be hardened against network attack, according to the recommendations in documents such as the National Security Agency's Security Recommendation Guides for Windows (available for free at www.nsa.gov).

## Create a long-term audit trail

To support accountability, legal investigations and trends analysis, save security logs to write-once media, such as burnable CD-ROMs. GFI EventsManager's automatic archiving functionality produces an audit database than can be saved in this manner.

## Conclusion

Windows includes complete functionality for capturing security events but provides little or nothing in the way of analysis, archiving and real-time monitoring capabilities. Cryptic event descriptions compound the problem, as does the fact that each computer maintains a separate security log. Yet in today's networked business environment, it is essential to track security activity and to respond immediately to intrusion attempts. GFI EventsManager builds on Windows' auditing foundation to provide an easy-to-deploy way to meet those needs, whilst a well-deployed GFI EventsManager installation also provides for a reduction of false positives in the alert process, administrator accountability and secure archive logs.

For more info on GFI EventsManager and to download your free trial, please visit http://www.gfi.com/eventsmanager.

## About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small and medium-sized enterprises (SME) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMEs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

**USA, CANADA AND CENTRAL AND SOUTH AMERICA**

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

**UK AND REPUBLIC OF IRELAND**

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

**EUROPE, MIDDLE EAST AND AFRICA**

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

**AUSTRALIA AND NEW ZEALAND**

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

**GFI**®