



GFI Product Manual

GFI *EventsManager*[™]

Event log monitoring, management and archiving

Deployment Guide



<http://www.gfi.com>
info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI EventsManager is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: ESM-DG-01.00.00

Last updated: September 12, 2011

Contents

1	Introduction	1
1.1	Document Scope	1
1.2	Document Limitations	1
1.3	Intended Audience	1
1.4	How this guide is structured	1
1.5	Knowledge Base	2
2	Introducing GFI EventsManager	3
2.1	About GFI EventsManager	3
2.2	How does GFI EventsManager work?	4
3	Deployment Considerations	7
3.1	Introduction	7
3.2	Deployment Objectives	7
3.3	Upgrading from previous versions	7
3.4	Minimum System Requirements	8
3.5	Firewalls and Anti-virus software	10
3.6	Computer identification considerations	11
3.7	Database and Files backend	11
3.8	Database Maintenance	12
3.9	Database availability	13
3.10	Alerting	13
3.11	Multiple domain, multiple site environments	14
3.12	Bandwidth considerations	15
3.13	Licensing	15
4	Performance and Sizing	17
4.1	Introduction	17
4.2	Benchmark test results	17
4.3	Bandwidth utilization	18
4.4	Steps required for determining the deployment solution	19
4.5	Recommendations	20
5	Deploying GFI EventsManager on a Single Domain LAN	23
5.1	Introduction	23
5.2	Deployment Phases	26
6	Deploying GFI EventsManager on a Multiple Domain WAN	27
6.1	Introduction	27
6.2	Deployment Scenario Description	28
6.3	Deployment Phases	29
7	Deploying GFI EventsManager in a Mixed Environment	33
7.1	Introduction	33
7.2	Deployment Scenario Description	34
7.3	Deployment Phases	35

8	Deploying GFI EventsManager on Demilitarized Zone	37
8.1	Introduction	37
8.2	Where to deploy GFI EventsManager	38
8.3	Deployment scenario description	41
8.4	Deployment Phases	42
9	Deploying GFI EventsManager ReportPack	45
9.1	Introduction	45
9.2	About the GFI EventsManager ReportPack	46
9.3	GFI EventsManager ReportPack management console	46
9.4	Deployment Phases	47
9.5	Deployment scenario	48
10	Appendix 1: Instance Calculator	51
10.1	Introduction	51
11	Appendix 2: SQL Server Best Practices	53
11.1	Introduction	53
12	Appendix 3: Checklist	55
12.1	Introduction	55
	Index	59

1 Introduction

1.1 Document Scope

This Deployment Guide aims to provide IT Management with the necessary information to successfully deploy GFI EventsManager on a corporate network. It is an important aid that should be used during the planning stage of any deployment project.

This document is the result of benchmark tests carried out at GFI Laboratories. This will help in determining the resources required for the GFI EventsManager deployment.

A number of scenarios are also described as case studies. These reflect real-world IT environment scenarios of various sizes and complexities and are an additional aid in the planning stage of a GFI EventsManager deployment.

1.2 Document Limitations

This document does not provide system and network administrators with detailed instructions on how to install and configure GFI EventsManager.

It is also beyond the scope of this document to provide network setup and maintenance specific instructions. This includes, but is not limited to, administration and maintenance of TCP/IP networks and Active Directory installation and administration.

For information on how to install and configure GFI EventsManager, refer to the user manual, available on the GFI website at <http://www.gfi.com/eventsmanager>.

For information on network setup and administration refer to the respective supplier documentation.

1.3 Intended Audience

The material in this guide is aimed at IT managers and the technical staff responsible for the setting up of a GFI EventsManager deployment plan.

1.4 How this guide is structured

CHAPTER	DESCRIPTION
Chapter 1	Introduction Introduces the Deployment Guide and explains its structure.
Chapter 2	Introducing GFI EventsManager Provides an overview of GFI EventsManager and how it works.
Chapter 3	Deployment Describes important issues that should be taken into consideration when preparing the plan for a GFI EventsManager deployment project.
Chapter 4	Performance and Presents benchmark results for a number of tests carried out to assess GFI EventsManager performance. Use these benchmarks to determine the performance and sizing metrics required.
Chapter 5	Deploying GFI EventsManager on a Single Domain LAN Describes two typical case scenarios involving small and large LANs. The steps taken to determine the GFI EventsManager deployment path are also listed.

CHAPTER	DESCRIPTION
Chapter 6	Deploying GFI EventsManager on a Multiple Domain WAN Describes a typical case scenario for a WAN with multiple domains and geographically remote sites. The steps taken to determine the GFI EventsManager deployment path are also listed.
Chapter 7	Deploying GFI EventsManager in a Mixed Environment Describes the scenario for deploying GFI EventsManager on a LAN where computer systems and network devices generate Windows, Syslog and W3C events.
Chapter 8	Deploying GFI EventsManager on Demilitarized Zone Describes the scenario for deploying GFI EventsManager to monitor events generated by hardware and software systems on a Demilitarized zone.
Chapter 9	Deploying GFI EventsManager ReportPack Gives an overview of the GFI EventsManager ReportPack and describes the steps required to deploy it.
Chapter 10	Appendix 1: Instance Calculator Provides a link to the GFI EventsManager Calculator. This Microsoft Excel spreadsheet helps you to get an estimate of the number of GFI EventsManager instances required on your network.
Chapter 11	Appendix 2: SQL Server Best Practices Describes some SQL Server best practices and links to SQL Server resources available on the Microsoft website.
Chapter 12	Appendix 3: Checklist Provides additional help during the planning stage of the GFI EventsManager deployment project. The checklist lists the important points discussed in the deployment guide.

1.5 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. The Knowledge Base always has the most up-to-date listing of support questions and patches.

The Knowledge Base can be found on <http://kbase.gfi.com/>.

2 Introducing GFI EventsManager

2.1 About GFI EventsManager

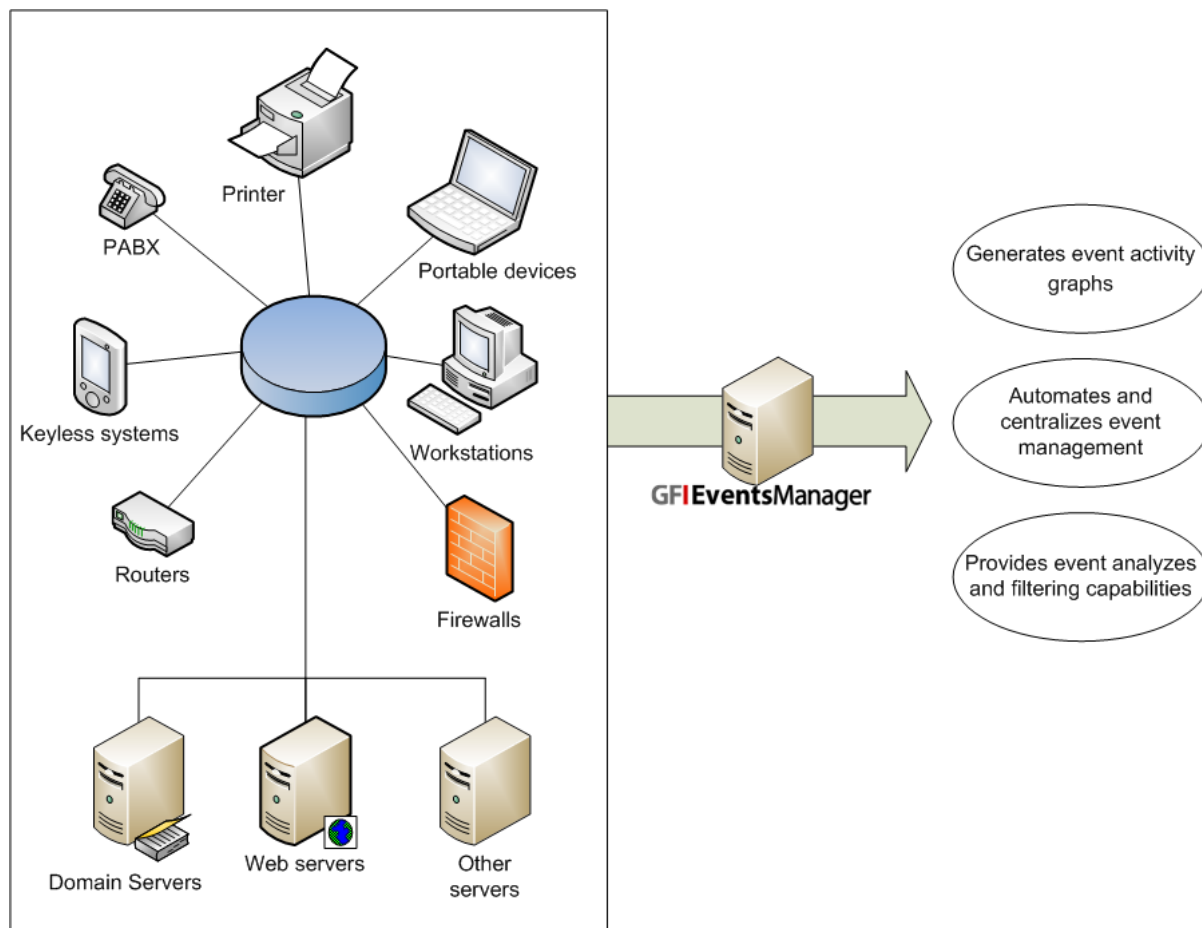


Figure 1 - GFI EventsManager integrates into any existing IT infrastructure

GFI EventsManager is a results oriented event log management solution which integrates into any existing IT infrastructure, automating and simplifying the tasks involved in network-wide events management.

Through the features supported by GFI EventsManager you can:

- » Automatically collect W3C, Syslog, SNMP Traps, SQL Server audit messages, Oracle Server audit events and Windows events from network devices and Windows/Linux/Unix based systems and manage them through one console.
- » Archive collected events in a centralized SQL Server based database backend for future analysis and forensic studies.
- » Automatically transfer events from the database to external files.
- » Filter unwanted events and classify key events through the use of powerful default or custom-built event processing rules.
- » Automate alerting and remedial actions such as the execution of scripts and files on key events.
- » Monitor your network activity and the status of your GFI EventsManager scanning engine through a built-in graphical dashboard.
- » Analyze events through a built-in events browser as well as export these events to CSV and HTML files for further processing and report customization.

- » Simplify event forensics through specialized tools which include a built-in event query builder, an event finder tool and an event color-coding tool.
- » Increase event processing power through a high-performance event scanning engine.
- » Generate, schedule as well as email event activity and trend reports through GFI EventsManager ReportPack - the powerful reporting companion tool which ships by default with GFI EventsManager.
- » Monitor the operational health status of your SQL Servers and Oracle servers in real-time by processing the activity logs or messages generated by day-to-day database server operations.

2.2 How does GFI EventsManager work?

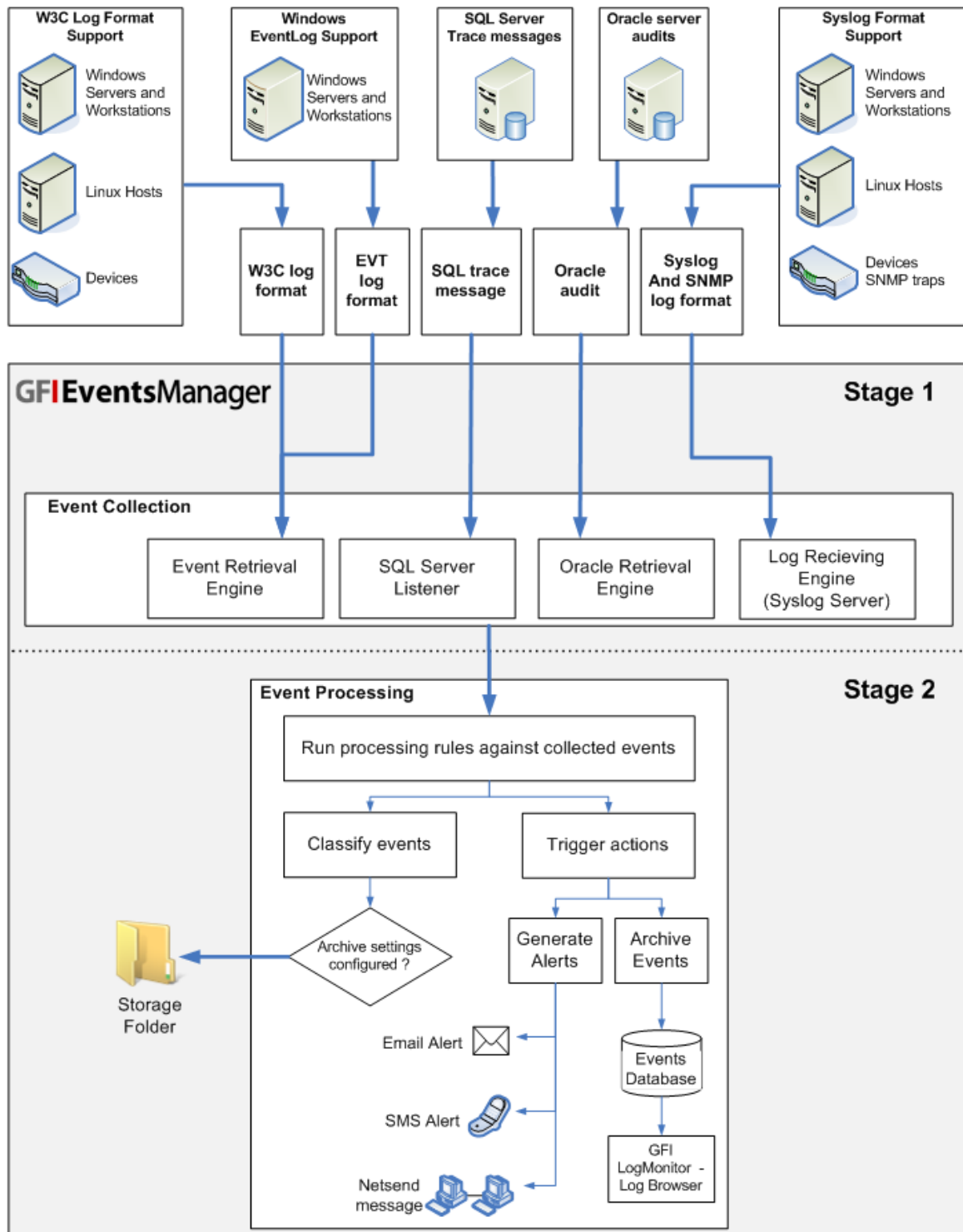


Figure 2 - The GFI EventsManager operational stages

The operational functionality of GFI EventsManager is divided into 2 stages:

- » **Stage 1:** Event Collection
- » **Stage 2:** Event Processing

A description of every stage is provided below.

Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of two event collection engines: The Event Retrieval Engine and the Event Receiving Engine.

The Event Retrieval Engine is used to collect Windows Event Logs and W3C logs from networked event sources. During the Event Collection process this engine will:

1. Logs on the event source(s)
2. Collects events from source(s)
3. Sends collected events to the GFI EventsManager Server
4. Logs off from event source(s).

The **Event Retrieval Engine** collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console.

The **Oracle Retrieval Engine** works in a similar way as the Event Retrieval Engine. It regularly connects to Oracle servers, collects the audit events and disconnects from the servers.

The **Event Receiving Engine** acts as Syslog and SNMP Traps server. It can process messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured.

By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are customizable via the GFI EventsManager management console.

The **SQL Server Listener** connects to SQL Servers and listens to trace events generated by the servers in real-time.

Stage 2: Event Processing

During this stage, GFI EventsManager will run a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

- » Analyze the collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- » Filter events that match specific conditions
- » Trigger email, SMS, SNMP traps and network alerts on key events
- » Trigger remediation actions such as file execution, scripts and batch commands on key events

Optionally archive collected events in the database backend or in storage files on disk. After processing the rules, GFI EventsManager can be configured to store the collected events in a storage folder. The administrator can configure the path of the storage folder

and configure which events are stored. This function will minimize database growth, and allows the administrator to store only important events in the database.



Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to:
<http://kbase.gfi.com/showarticle.asp?id=KBID001122>.

3 Deployment Considerations

3.1 Introduction

This chapter contains important issues to consider when preparing the plan for a GFI EventsManager deployment project

3.2 Deployment Objectives

Clearly identify from the outset the objectives to achieve through GFI EventsManager.

Your objectives can be centered around one or more of the following areas:

- » Legal Compliance
- » System Health Monitoring
- » Security Monitoring
- » Forensic Analysis

Then identify:

- » The logs to collect events from
- » Configuration settings of the logs at **source**:
 - Windows audit settings
 - Syslog logging options
 - SNMP traps logging options
 - W3C logging options
 - Oracle audit settings
- » Events to be classified as noise
- » Any additional rule-set configuration.

When configuring settings of the logs at **source**; ensure that only relevant, usable event data is being collected.

The default rule-sets applied by GFI EventsManager upon installation are adequate to most needs, though you might decide to carry out some customization based on your objectives.

Failure to adequately define objectives and to configure GFI EventsManager accordingly, may lead to:

- » irrelevant events being collected
- » higher database growth rate
- » unnecessary resource utilization in collecting unimportant events
- » additional administrator time required to filter out the unimportant events.

3.3 Upgrading from previous versions

Upgrading from versions 2010 and retaining configuration settings is fully supported.

Upgrading from version 8.x onwards is possible, but any configuration settings are lost. In this case it is recommended that configuration settings must be exported before upgrading and after upgrade they are imported into the new version.

Upgrading from versions older than version 8 is not supported due to the underlying operational and processing technology subsystems that are different from the current version of GFI EventsManager. You can still however run an older (pre-version 7) version of GFI EventsManager on the same machine where a newer version of GFI EventsManager is installed, since there are no conflicts between the older and the newer versions.

3.4 Minimum System Requirements

3.4.1 Hardware requirements

- » Processor: 2.5 GHz dual core or higher
- » RAM: 2GB
- » Hard disk: 10 GB of available space



Hard disk size depends on your environment, the size specified in the requirements is the minimum required to install and archive events.



If Microsoft SQL Server is installed on the same machine as GFI EventsManager, consider using 1GB to 2GB more RAM than required.

3.4.2 Software requirements

Supported Operating Systems (x86 or x64)

- » Windows Server 2008 - Standard or Enterprise
- » Windows Server 2008 R2 - Standard or Enterprise
- » Windows Server 2003 SP2 - Standard or Enterprise
- » Windows 7 - Enterprise, Professional or Ultimate
- » Windows Vista SP1 - Enterprise, Business or Ultimate
- » Windows XP Professional SP3
- » Windows SBS 2008
- » Windows SBS 2003

Other components

- » .NET framework 4.0
- » Microsoft Data Access Components (MDAC) 2.8 or later
- » (Optional) A mail server (If email alerting is configured)
- » Microsoft SQL Server 2005 or later (including Microsoft SQL Express edition) for events archiving.



Microsoft SQL server must have TCP port 1433 open to store events collected by GFI EventsManager. For more information, refer to <http://support.microsoft.com/kb/287932>



Microsoft Data Access Components (MDAC) 2.8 can be downloaded from <http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en>

Event sources

The table below describes the configuration required for event sources

SCAN FOR:	CONFIGURATION
Windows event log processing	Enable remote registry.
W3C log processing	The source folders must be accessible via Windows shares
Syslog and SNMP Traps processing	Configure sources/senders to send messages to the computer/IP where GFI EventsManager is installed.
Scanning machines with Windows Vista or later	Install GFI EventsManager on a computer running Windows Vista or later.
System auditing	Enable auditing on event sources. For information on how to enable auditing, refer to Miscellaneous section in this manual.

3.4.3 Ports and permissions

Ports used by GFI EventsManager

The table below describes the ports used by GFI EventsManager to collect and process events.

PORT	PROTOCOL	DESCRIPTION
135	UDP and TCP	Target machines use this port to publish information regarding available dynamic ports. GFI EventsManager uses this information to be able to communicate with the target machines.
139 and 445	UDP and TCP	Used by GFI EventsManager to retrieve the event log descriptions from target machines.
162	UDP and TCP	Used by GFI EventsManager to receive SNMP traps. Ensure that this port is open on the machine where GFI EventsManager is installed
514	UDP and TCP	Used by GFI EventsManager to receive SYSLOG messages.
1433	UDP and TCP	Used by GFI EventsManager to communicate with the SQL Server database backend. Ensure that this port is enabled on Microsoft SQL Server and on the machine where GFI EventsManager is installed.
1521	UDP and TCP	Used to collect Oracle Server audit logs. Port 1521 is the default port for this connection. If the port is changed manually in the Oracle Listener's configuration, adjust firewall settings accordingly.
49153	UDP and TCP	Used by GFI EventsManager to collect events from event sources with Microsoft Windows Vista or Microsoft Windows 7.

Firewall permissions

When using Microsoft Windows firewall, enable the firewall permissions and policies listed in the table below.

FIREWALL PERMISSIONS AND AUDIT POLICIES	MICROSOFT WINDOWS SERVER 2008	MICROSOFT WINDOWS SERVER 2003	MICROSOFT WINDOWS XP	MICROSOFT WINDOWS VISTA	MICROSOFT WINDOWS 7
Remote Event Log Management	Enable	Not applicable	Not applicable	Enable	Enable
File and Printer sharing	Enable	Enable	Enable	Enable	Enable
Network discovery	Enable	Not applicable	Not applicable	Enable	Enable

FIREWALL PERMISSIONS AND AUDIT POLICIES	MICROSOFT WINDOWS SERVER 2008	MICROSOFT WINDOWS SERVER 2003	MICROSOFT WINDOWS XP	MICROSOFT WINDOWS VISTA	MICROSOFT WINDOWS 7
Audit policy: Object access	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Process tracking	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Audit account management	Enable	Enable	Enable	Enable	Enable
Audit policy: Audit system events	Enable	Enable	Enable	Enable	Enable

For more information how to set permissions refer to the following sections:



- » To apply settings manually on each event source, refer to [Enabling permissions on events sources manually](#)
- » To apply settings automatically on event sources using Microsoft Active Directory GPO, refer to [Setting permissions on events sources automatically via GPO](#).

Microsoft Windows Vista and Microsoft Windows 7

Microsoft Windows Vista and Microsoft Windows 7 introduced extensive structural changes in event logging and event log management. The most important of these changes included:

- » A new XML-based format for event logs. This provides a more structured approach to reporting on all system occurrences.
- » Event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- » A new file format (evtx) that replaces the previous evt file format.

Due to these changes, to collect and process event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a system running Microsoft Windows Vista or later. (For example, GFI EventsManager cannot be installed on Microsoft Windows XP to monitor events on Microsoft Windows 7 machines).

	Windows XP events can be collected when GFI EventsManager is installed on Microsoft Windows Vista or later machines.
	<p>Disable User Account Control (UAC) when GFI EventsManager is using a non-domain account to collect events from Microsoft Vista machines or later.</p> <p>For more information on how to disable UAC, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003637</p>

3.5 Firewalls and Anti-virus software

If firewall(s) are enabled and anti-virus software installed on the computer where GFI EventsManager is running, make sure that:

- » Traffic is not blocked on the ports in use by GFI EventsManager
- » **esmui.exe** and **esmpoc.exe** are allowed access through the firewall(s)
- » GFI EventsManager folders are excluded from real-time anti-virus scanning.

For more information on the ports and permissions that must be enabled, refer to [Ports and permissions that must be enabled](#) section in this guide.

3.6 Computer identification considerations

GFI EventsManager identifies computers via computer name or IP. If NETBIOS-compatible computer names are used, ensure that your DNS service is properly configured for name resolution. Unreliable name resolution downgrades overall system performance. If you disable NETBIOS over TCP/IP, you can still use GFI EventsManager, however you must specify computer name by IP.

3.7 Database and Files backend

3.7.1 Database backend

GFI EventsManager makes use of two or more databases:

- » **Main database** - The collected events are stored. Events collected within the main database can be automatically moved to the backup database through a configurable maintenance schedule.
- » **Backup databases** - Events within the main database may be moved on a schedule to optimize performance and archiving.

Databases supported by GFI EventsManager include:

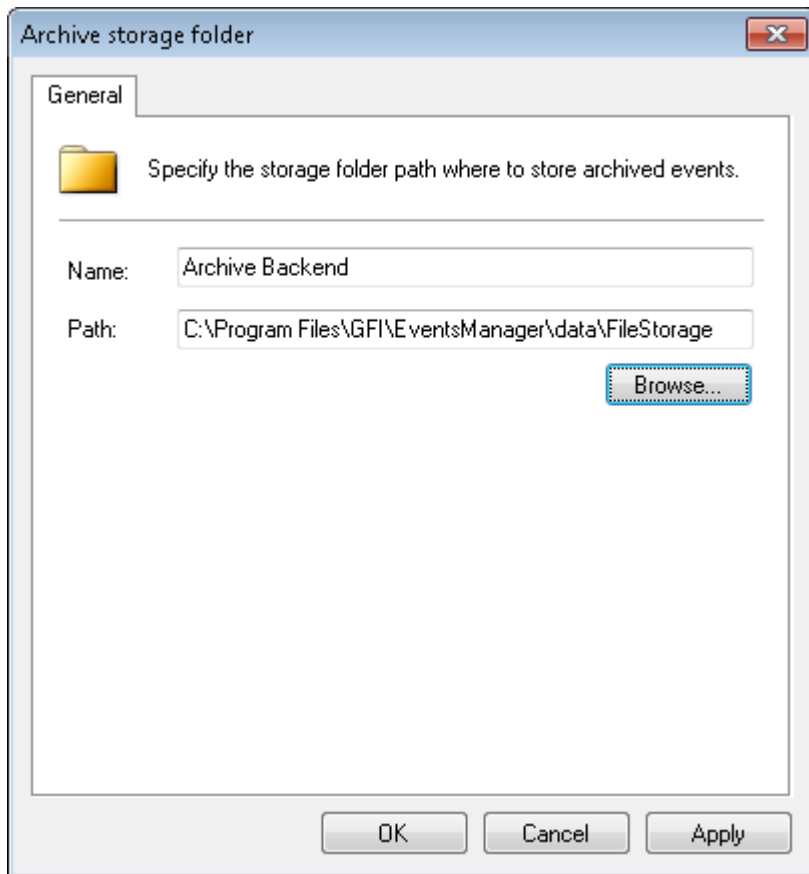
- » Microsoft SQL Server 2005 (Including Express edition)
- » Microsoft SQL Server 2008 (Including Express edition)



Microsoft SQL Server 2005 Express and Microsoft SQL Server 2008 Express editions have a maximum database size of 4GB and 10 GB respectively.

3.7.2 Files and storage folder

GFI EventsManager can be configured to archive all collected events in a storage folder after applying processing rules. This can be done in parallel with saving the events into the main SQL Server database as well. This feature allows the system to store all the events retrieved from event sources, on the local host (where GFI EventsManager is installed).



Screenshot 1 - Configure the Archive storage folder

3.8 Database Maintenance

Periodical database maintenance is essential in preventing excessive data growth in the database backend. A large database drastically affects the performance of GFI EventsManager; events browsing is slower and queries take longer to execute. There is also a negative impact on GFI EventsManager ReportPack performance, with reports taking longer to be generated.

Through GFI EventsManager a number of database operations (maintenance jobs), can be carried out on the database backend. These include:

- » Move to database - Moves events from the main database to the backup database or to another existing database.
- » Export to file - Exports events from the main database to a compressed binary file which can also be encrypted and backed to CD/DVD or tape for safekeeping.
- » Import from file - Imports events from GFI EventsManager export files or from storage files into the main database backend.
- » Delete data - Removes events from the main or backup database back-ends.
- » Filters that determine which events are affected by the database operation can be applied for each operation.

For more information on how to configure database operations, refer to the GFI EventsManager 2011 Manual available from <http://www.gfi.com/products/gfi-eventsmanager/manual>.

3.9 Database availability

If the database is temporarily unavailable, all scanning activity is interrupted. Scan requests are queued and executed when the database is available.

Reasons for a database becoming unavailable may include:

- » detaching/attaching of the database
- » taking the database offline
- » restoring the database
- » network problems

Use GFI Network Server Monitor to monitor the resources and connection to the SQL Server and be notified when this connection is in danger of downtime. For more information on GFI Network Server Monitor, refer to <http://www.gfi.com/nsm>.

3.10 Alerting

Alerting is an important aspect of events management, enabling in real time notifications on important events. One or more people can be alerted in various ways including: email, network messages, and SMS notifications sent through an email-to-SMS gateway or service.

For email alerting to function you should ensure that:

- » SMTP server details are configured
- » The SMTP server is always available
- » Internet access is always available.

For alerts to be sent using network messages ensure that:

- » The Messenger service in Windows is started. This service is not related to the Windows Messenger application.

For SMS alerting to function ensure that:

- » Service provider details are configured
- » For email to SMS, the SMTP server is always available and that internet access is also always available.

For each of the alerting methods mentioned, firewall(s) may need to be configured not to block alerting traffic.

For more information on how to configure Alerting options refer to the GFI EventsManager 2010 Manual available from <http://www.gfi.com/products/gfi-eventsmanager/manual>.

3.11 Multiple domain, multiple site environments

Most companies adopt an environment that consists of multiple domains. This section describes how GFI EventsManager can be used in such environments.

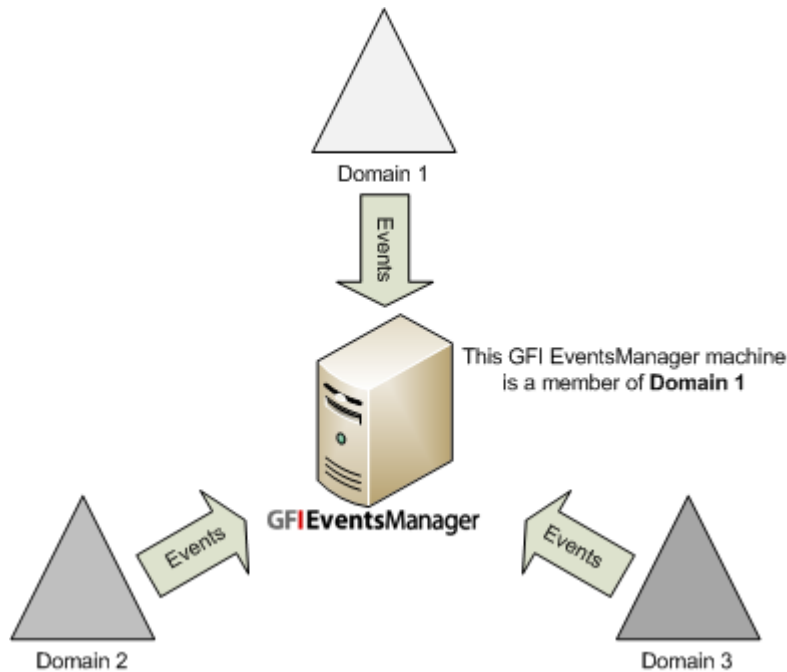
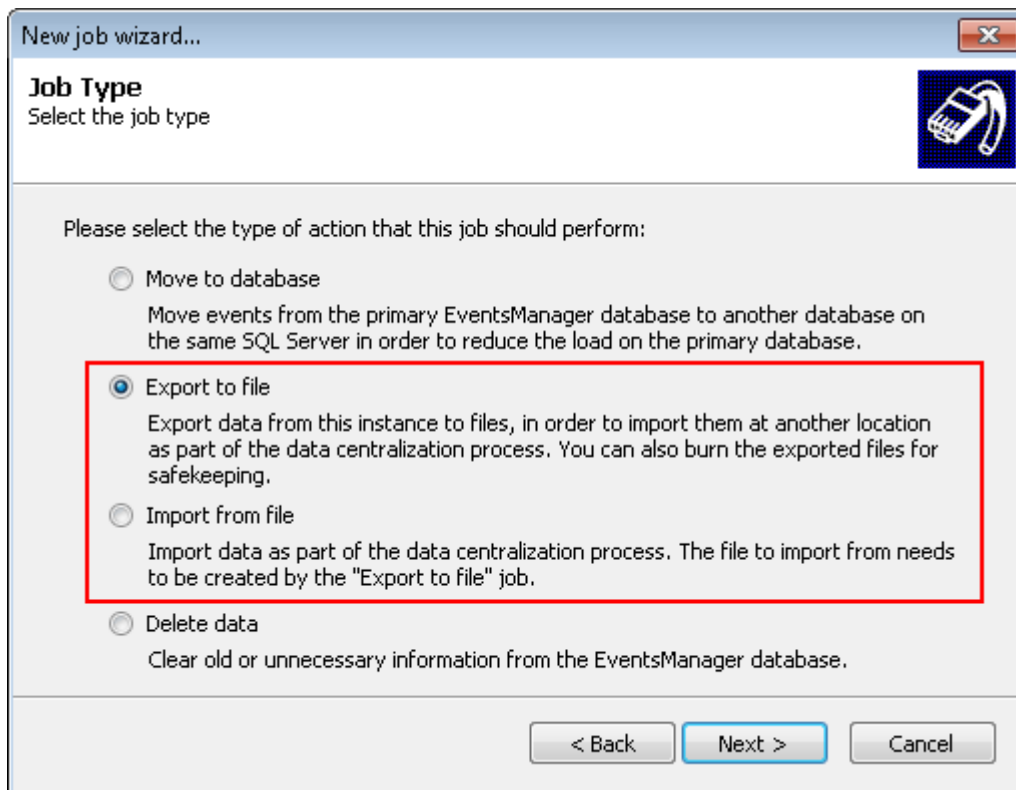


Figure 3 - Processing events from multiple domains and multiple site

GFI EventsManager installation can scan event sources across multiple domains. The limitation is on the number of events collected per hour, which should not exceed the 6 million mark for every GFI EventsManager instance. For more information refer to the [Performance and sizing](#) and [Deploying GFI EventsManager on a Multiple domain WAN](#) chapters. GFI EventsManager should also be configured with adequate administrative credentials to be able to collect events from all sources across domains.

For multiple sites on a WAN, the recommended setup is to have at least one GFI EventsManager installation on each site. Using the Database Operations configure each GFI EventsManager installation to import and export events to a central location. For more information on how to configure Database Operations, refer to the GFI EventsManager 2011 Manual available [here](#).



Screenshot 2 -Export to file and Import from file database operations

3.12 Bandwidth considerations

The impact of collecting and processing events from a computer on the Local Area Network is very low.



Processing of events from a remote computer on a geographically remote site of a Wide Area Network is not recommended.

When collecting events from geographically remote sites, it is recommended to have at least one GFI EventsManager installation per site. Using the Database Operations, configure each GFI EventsManager installation to import and export events to a central location. For more information on how to configure Database Operations, refer to the GFI EventsManager 2011 Manual available from <http://www.gfi.com/products/gfi-eventsmanager/manual>.

3.13 Licensing

For licensing information, refer to <http://www.gfi.com/products/gfi-eventsmanager/pricing>.

4 Performance and Sizing

4.1 Introduction

The information in this chapter is based on tests aimed at assessing the total number of events GFI EventsManager is capable of processing in a one hour period. Tests were repeated a number of times with varying load conditions on the machines used in the tests.

Use this information plan for performance and sizing metrics for your GFI EventsManager environment.

4.2 Benchmark test results

The test results shown in the table below were obtained under these conditions:

- » For each test, events were collected from 10 computers with identical specifications
- » All available logs on the Windows 2003 Server Enterprise machines were scanned
- » All available logs on the Windows XP SP2 machines were scanned
- » Syslog sources were configured to send messages to GFI EventsManager
- » W3C logs were scanned
- » A number of one hour tests were carried out, with varying load on the machines in each test. Results show the minimum/maximum number of events processed during these tests
- » GFI EventsManager was configured either to archive the events collected or to process them using the default rule sets
- » When using the default rule sets, not all events processed were stored in the database backend. This applies, for example, to events classified as noise.
- » GFI EventsManager was installed on one of the test machines
- » For tests 3 and 4, SQL Server and GFI EventsManager were installed on separate machines.

The main hardware and software specifications for each test are listed in the following tables.

Table 1 - Benchmark test one

BENCHMARK TEST 1	
Processor	2x Intel Xeon 3.0 GHz
RAM	4GB
Operating System	Windows 2003 Server Enterprise
Database Backend	Local instance of SQL Server 2000
GFI EventsManager configuration settings	Archive all
Events per hour archived	Between 4 and 4.4 million
Events per hour processed	0 (all events are archived without processing)

Table 2 - Benchmark test two

BENCHMARK TEST 2	
Processor	2x Intel Xeon 3.0 GHz
RAM	4GB
Operating System	Windows 2003 Server Enterprise

BENCHMARK TEST 2	
Database Backend	Local instance of SQL Server 2000
GFI EventsManager configuration settings	Process using default rules
Events per hour processed	Between 5.5 and 6 million

Table 3 - Benchmark test three

BENCHMARK TEST 3	
Processor	Intel Pentium 4 2.8 GHz
RAM	2GB
Operating System	Windows XP SP2
Database Backend	Remote instance of SQL Server 2005
GFI EventsManager configuration settings	Archive all
Events per hour archived	Between 3.3 and 3.7 million

Table 4 - Benchmark test four

BENCHMARK TEST 4	
Processor	Intel Pentium 4 2.8 GHz
RAM	2GB
Operating System	Windows XP SP2
Database Backend	Remote instance of SQL Server 2005
GFI EventsManager configuration settings	Process using default rules
Events per hour processed	Between 4.3 and 4.7 million

4.3 Bandwidth utilization

The table below shows network bandwidth utilization during the tests. Figures quoted were achieved in test environments and may not be representative of your IT environment.

Table 5 - Bandwidth utilization

BANDWIDTH UTILIZATION	
Client machines peak utilization	10 to 15 percent
Client machines average utilization	3 to 5 percent
Server peak utilization	50 percent
Server average utilization:	16 percent

Table 6 - Bandwidth utilization test notes

TEST NOTES	
Note 1	Tests were carried out on a 100Mb LAN.
Note 2	Client machines refers to the machines being monitored by GFI EventsManager.
Note 3	Server machine refers to the machine where GFI EventsManager and SQL Server are installed.
Note 4	Peak utilization was recorded over very short time intervals.
Note 5	Peak utilization on client machines - certain machines reached a peak of 10 percent, whilst others reached a peak of 15 percent.
Note 6	Average utilization on client machines - certain machines averaged 3 percent utilization, whilst others averaged 5 percent utilization.
Note 7	There were a significant number of time intervals where bandwidth utilization was 1 percent and below.

4.4 Steps required for determining the deployment solution

The first steps to be taken are the following:

- » calculate the total number of events that will be collected every hour
- » determine whether events are archived or processed.

The benchmark results provided can then be used to establish:

- » the number of GFI EventsManager instances required
- » hardware resources required.

Further information to help in the evaluation

- » According to the **Microsoft Security Monitoring and Attack Detection Planning Guide**, the average growth of security events per hour on a domain controller, with object access auditing disabled is around 3000 events. In total, a domain controller can generate up to 10,000 to 15,000 windows events from all windows logs per hour. The **Microsoft Security Monitoring and Attack Detection Planning Guide** can be downloaded from <http://www.microsoft.com/downloads/en/details.aspx?FamilyId=95A85136-F08F-4B20-942F-DC9CE56BCD1A&displaylang=en>
- » GFI's research indicates that a Windows 2003 domain controller with 3000+ very active domain users generates around 100,000 windows events per hour
- » A typical Windows XP/Vista/ Windows 7 workstation generates around 1000 security audits per hour and around 1500 - 2000 windows events (from all logs) per hour.
- » Microsoft indicates that a Windows 2008 domain controller with the default Audit Policy enabled generates on average 60,000 events/hour with a peak of 500,000 events/hour. GFI recommends to consider an average of 100,000 events/hour.
- » Tests performed by GFI show that even a Windows 7 workstation can generate between 30,000 - 100,000 events per hour if auditing is enabled for network and global object related events.
- » When auditing SQL Server or Oracle servers, the number of events can vary from a few to hundreds of thousand per hour. It is recommended to carefully plan for what kind of information you need to audit (for example, determine which databases or users are really important to monitor).

Issues to consider

- » The database backend can become a bottleneck when archiving all events into the database backend. Processing takes more time and there will be an increase in database size. This requires regular maintenance and attention.
- » Using default-processing rules, only the important events are usually archived into the database. Processing will be faster with minimum storage utilization. If every event log is required to be stored, GFI recommends you to use file storage instead of database storage so that only important information is stored in the SQL Server database.
- » Scanning large W3C logs requires higher RAM specifications.
- » Incoming SYSLOG messages at a rate of 2000 per hour will not affect benchmarks.
- » For Windows Vista and Windows 7 operating systems, the number of events generated can be very high. This applies if certain audit categories are enabled including: Object Access event categories like Filtering Platform Connection events and Global Objects Events. It is therefore not recommended to store all events into the SQL Server database. Use the alternative file storage if archiving all events is required.



Using a single GFI EventsManager installation to process events over WAN is not recommended. For more information on a recommended setup, refer to [Multiple domain, multiple site environments](#) section in this guide.

4.5 Recommendations

Use the recommended specifications shown below to determine the hardware requirements to install GFI EventsManager and obtain maximum performance. These recommendations were determined following the benchmark tests.



The RAM specified in tables below must be dedicated to GFI EventsManager. Remember to take in consideration the amount of RAM required by the SQL Server database backend and other applications.

Table 7 - Processor required for maximum performance

PROCESSOR	
Collecting up to 3 million events per hour	Intel Pentium 4 2.8 GHz
Collecting more than 3 million events per hour	2x Intel Xeon 3.0 GHz (Dual-Processor setup)

Table 8 - RAM requirements for maximum performance

RAM	
Minimum	512MB
When collecting up to 3 million events per hour	1GB
When collecting more than 3 million events per hour	Increase RAM for better performance.

Table 9 - Bandwidth requirements for maximum performance

BANDWIDTH	
LAN	The impact when processing windows events remotely is very low.
WAN	Install an instance of GFI EventsManager at each site and import/export events on a centralized location.

Table 10 - SQL Server considerations

SQL SERVER	
Edition	SQL Server 2005 Workgroup Edition or above
Bandwidth	Bandwidth savings of 16% can be achieved if SQL Server and GFI EventsManager are installed on the same machine. If a remote SQL Server instance is required, a gigabit network connection is recommended. For more information on bandwidth utilization, refer to Bandwidth utilization section in this guide.
Storage	Database storage is dependent on: <ul style="list-style-type: none"> » Deployment environment » Types of logs monitored and processed » Processing rules

SQL SERVER

RAM	Minimum 2 GB allocated for SQL Server
Disk space allowance for data file	On average 1-2 Kb per event



Figures quoted in the above scenarios are only indicative and may not be representative of your IT environment.

5 Deploying GFI EventsManager on a Single Domain LAN

5.1 Introduction

GFI EventsManager can be deployed on Windows based networks as well as on mixed environments where Linux and UNIX systems are being used as well.

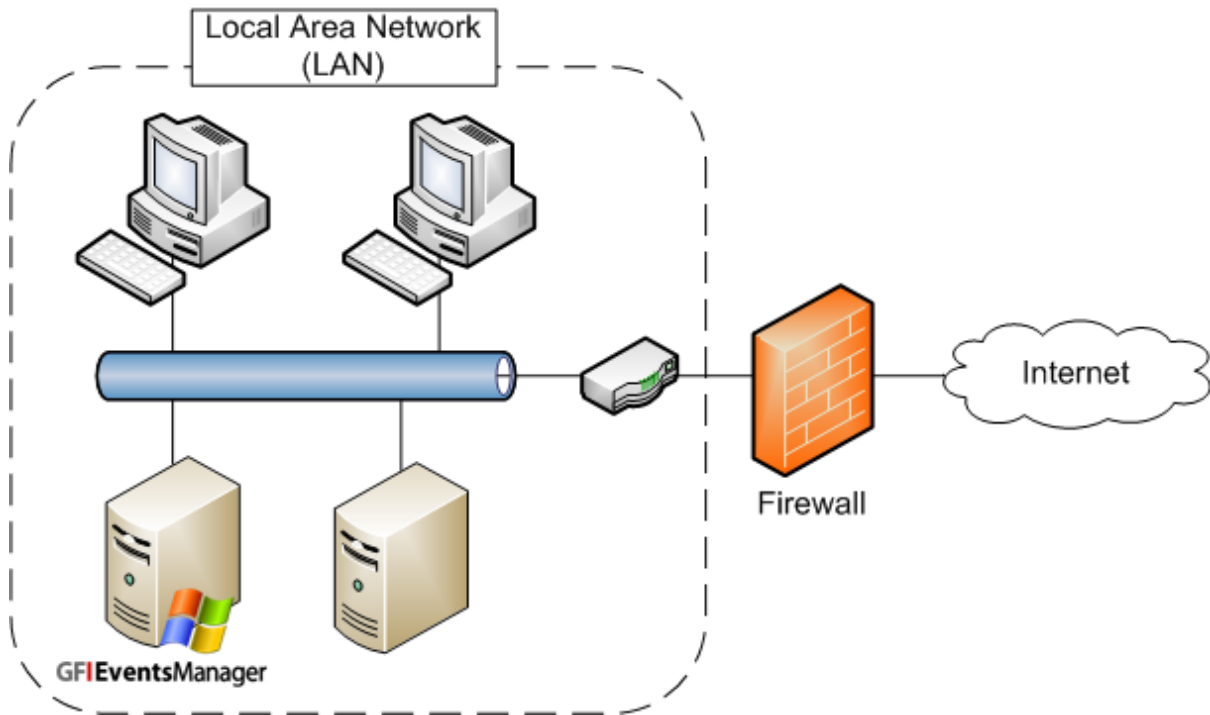


Figure 4 - GFI EventsManager on a single domain LAN

Before deploying GFI EventsManager on your Local Area Network (LAN), review the [Deployment considerations](#) section in this guide.

Scenario 1: Small single domain network with default Audit Policy enabled

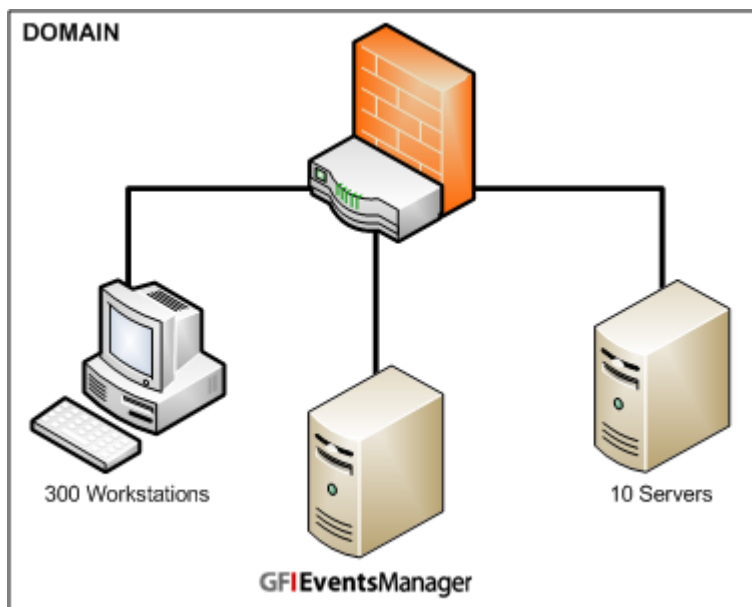


Figure 5 - Small single domain network

Network with default Audit Policy enabled on all machines:

- » 1 Microsoft Windows 2003/2008 servers Domain Controller
- » 9 Microsoft Windows 2003/2008 servers
- » 300 Windows XP SP2/Vista/Win7 workstations
- » GFI EventsManager configured to process events using default rule-sets.

Calculating the number of events per hour and the database growth per month:

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Domain controllers	1	100,000	100,000
Servers	9	15,000	135,000
Workstations	300	2,000	600,000
The total number of events			835,000
Approximate database storage growth per month in GB			89
Total number of GFI EventsManager installations			1

If Filtering Platform Connection audit or Object Audit on global objects are turned on, we recommend to not archive the corresponding events into the SQL Server backend database. To manage these events use one of the following options:

- » Make use of the file storage to archive all the events while keeping only the important events (the ones that trigger rules and are classified as important) into the SQL Server database
- » If you want to keep all the events into the database, use the database operations to backup the events often (on a weekly basis) and remove the old events from the main database

Scenario 2: Large single domain network

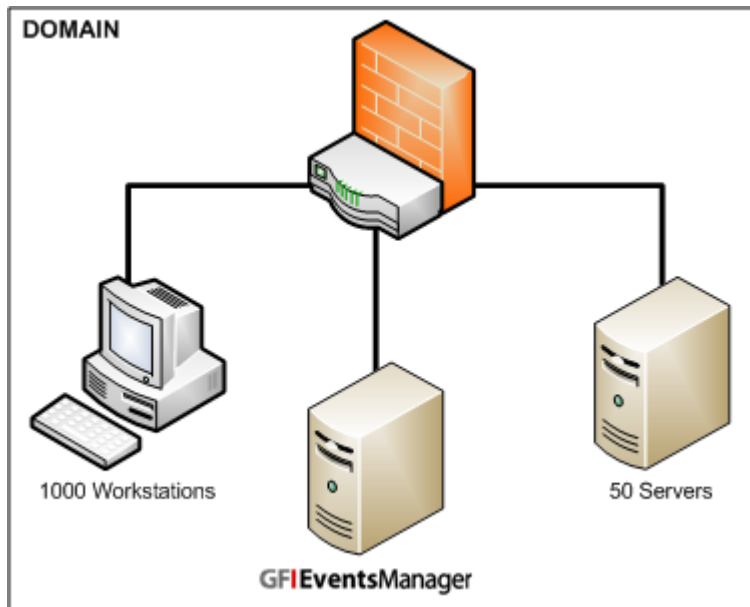


Figure 6 - Large single domain network

Network consists of:

- » 1 Microsoft Windows 2003/2008 servers Domain Controller
- » 49 Microsoft Windows 2003/2008 servers
- » 1000 Windows XP SP2/Vista/Win 7 workstations
- » GFI EventsManager configured to process events using the default rule-sets.

Using the figures described in [Performance and sizing](#) chapter of this guide you can calculate the number of events per hour and the database growth per month:

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Domain controllers	1	300,000	300,000
Servers	49	100,000	4,900,000
Win 7 Workstations	1000	30,000	30,000,000
The total number of events			2,835,000
Approximate database storage growth per month in GB			301
Total number of GFI EventsManager installations			1

If Filtering Platform Connection audit or Object Audit on global objects are turned on, we recommend to not archive the corresponding events into the SQL Server backend database. To manage these events use one of the following options:

- » Make use of the file storage to archive all the events while keeping only the important events (the ones that trigger rules and are classified as important) into the SQL Server database
- » If you want to keep all the events into the database, use the database operations to backup the events often (on a weekly basis) and remove the old events from the main database

5.2 Deployment Phases

Deployment phases for small or large single domain networks are identical. The following steps are required to deploy and configure GFI EventsManager:

1. Install and configure the SQL Server backend. This can be remotely installed or on the GFI EventsManager machine. Create a user account with the required privileges to enable GFI EventsManager to archive events.



To enable GFI EventsManager to archive events, the account must have read and write access privilege on the database.

2. Ensure that the server has all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.

3. Install GFI EventsManager.

4. Configure the SQL database backend from GFI EventsManager.

5. Configure and add Event Sources. Event sources can be added:

- » manually from **Configuration ► Event Sources** in GFI EventsManager console.
- » using the **Automatic network discovery wizard**
- » using the GFI EventsManager synchronization feature.

6. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.

7. (Optional) Configure rule-sets

For more information on how to perform all the actions mentioned above, refer to the user manual, available on the GFI website at <http://www.gfi.com/eventsmanager>.

6 Deploying GFI EventsManager on a Multiple Domain WAN

6.1 Introduction

GFI EventsManager can be deployed on Windows based networks as well as on mixed environments where Linux and UNIX systems are being used as well.

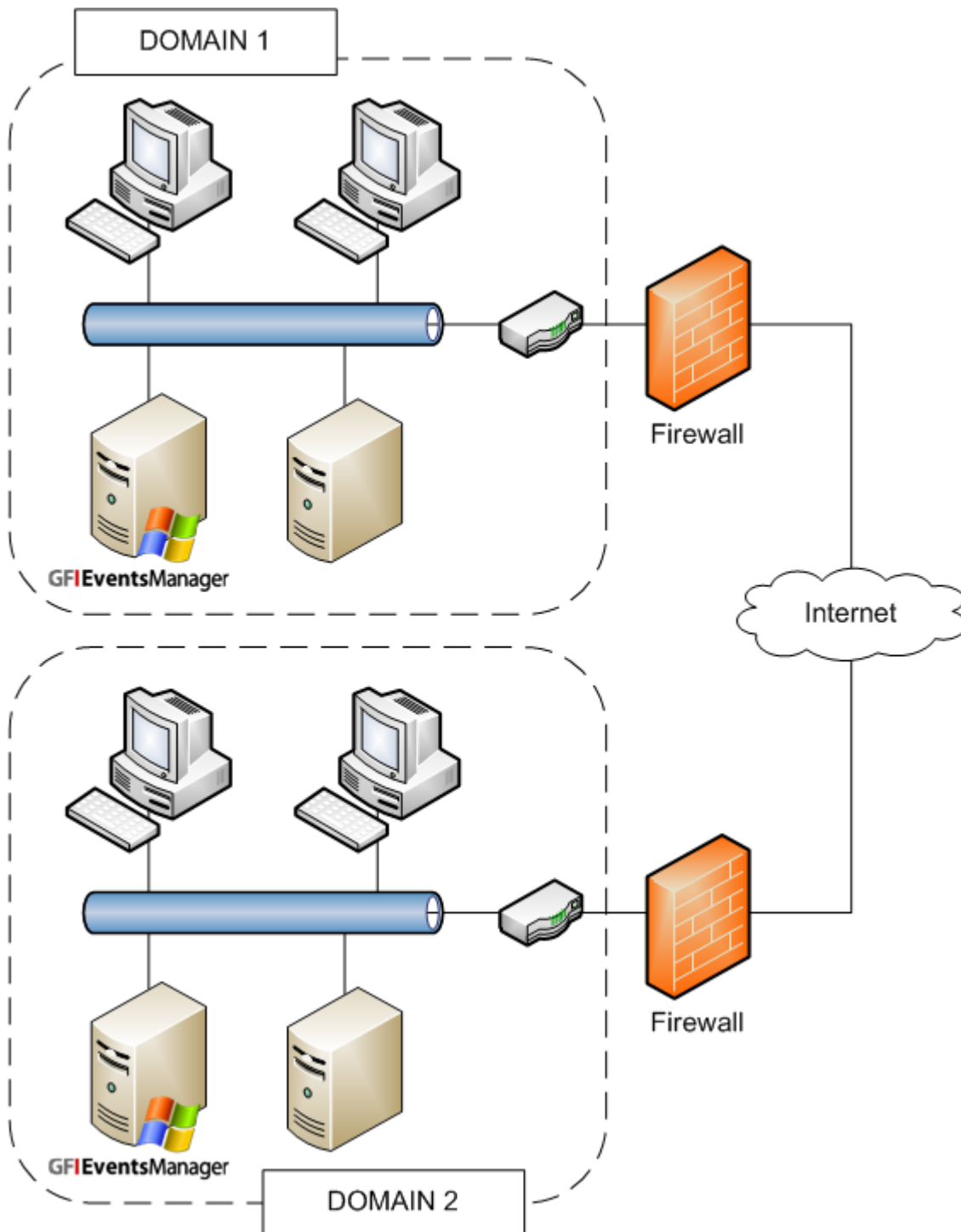


Figure 7 - GFI EventsManager on multiple domain over WAN

Using the export and import jobs within the database operations, GFI EventsManager enables you to collect events from multiple domains over the internet.

Before deploying GFI EventsManager, review the [Deployment considerations](#) section in this guide.

6.2 Deployment Scenario Description

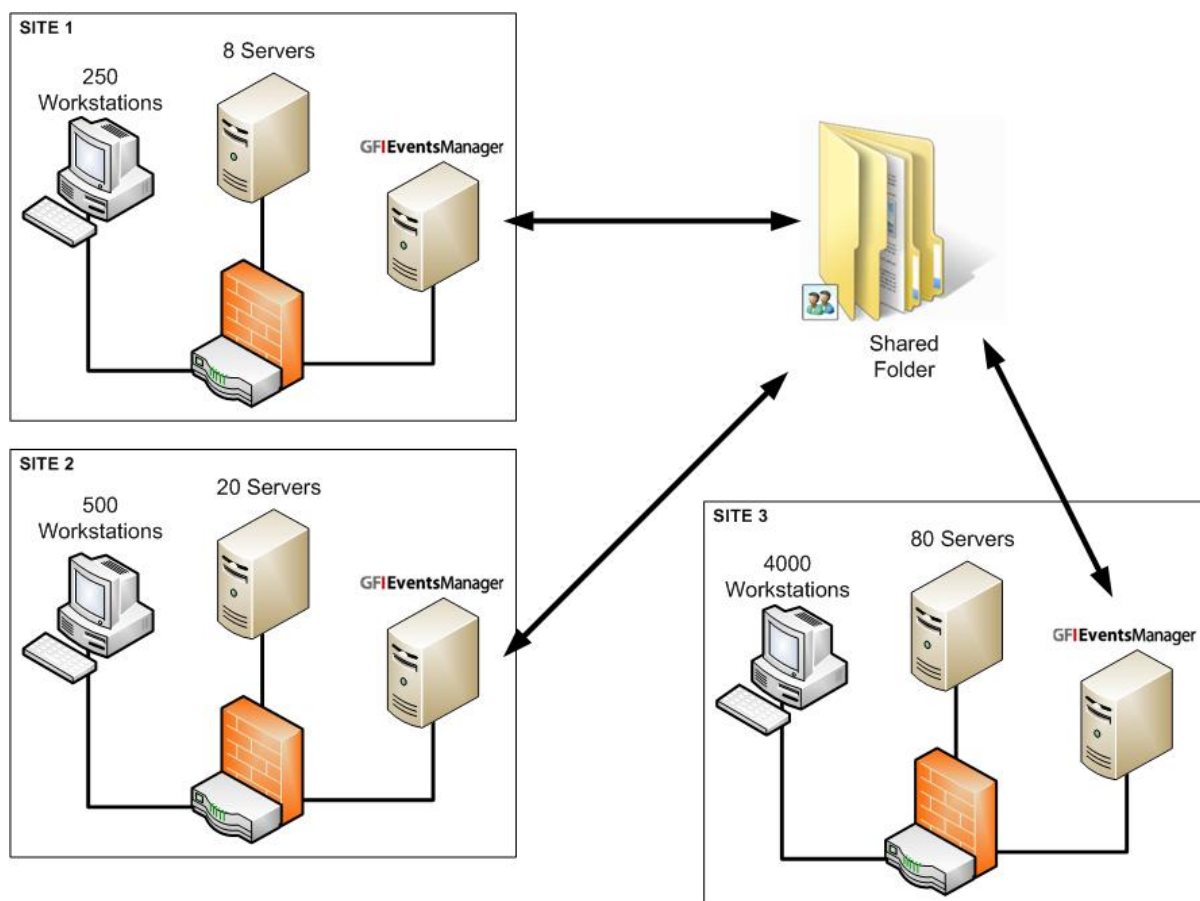


Figure 8 - Multiple sites with multiple domains

The scenario consists of three remote sites, each on a separate domain. GFI EventsManager is configured to process events using the default rule-sets. Each GFI EventsManager is configured to export and import events from a shared folder located in Site 3.

SITE	DOMAIN CONTROLLER (MICROSOFT WINDOWS SERVER 2003/2008)	SERVERS (MICROSOFT WINDOWS SERVER 2003/2008)	WORKSTATIONS (MICROSOFT WINDOWS XP/VISTA/WIN 7)
Site 1	1	7	250
Site 2	1	19	500
Site 3 (Head office)	1	79	4000

Calculation of number of events per hour

Using the figures described in chapter [Performance and sizing](#) of this guide you can calculate the number of events per hour and the database growth per month:

Table 11 - Calculation for Site 1

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Domain controllers	1	100,000	100,000
Servers	7	15,000	105,000
Workstations	250	2,000	500,000
The total number of events			705,500
Approximate database storage growth per month in GB			75
Total number of GFI EventsManager installations			1

Table 12 - Calculation for Site 2

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Domain controllers	1	100,000	100,000
Servers	19	15,000	285,000
Workstations	500	2,000	1,000,000
The total number of events			1,385,000
Approximate database storage growth per month in GB			147
Total number of GFI EventsManager installations			1

Table 13 - Calculation for Site 3

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Domain controllers	1	100,000	100,000
Servers	79	15,000	1,185,000
Workstations	4000	2,000	8,000,000
The total number of events			9,285,000
Approximate database storage growth per month in GB			985
Total number of GFI EventsManager installations			2



The recommended number of GFI EventsManager instances for Site 3 is based on results from Benchmark test 2. Refer to [Benchmark test results](#) for more information.

At Site 3, the load should be balanced between the 2 GFI EventsManager instances. The 2 instances can be configured as follows:

GFI EVENTSMANAGER INSTANCE 1

Event Source	Number of devices	Events per device per hour	Total Events per hour
Domain controllers	1	100,000	100,000
Servers	79	15,000	1,185,000
Workstations	1500	2,000	3,000,000
The total number of events			4,285,000

GFI EVENTSMANAGER INSTANCE 2

Event Source	Number of devices	Events per device per hour	Total Events per hour
Workstations	2500	2,000	5,000,000
The total number of events			

6.3 Deployment Phases

Deployment Phases for Sites 1 and 2

The following steps are required to deploy and configure GFI EventsManager on Sites 1 and 2:

1. Install and configure the SQL Server backend. This can be installed remotely or on the GFI EventsManager machine. Create a user account with the required privileges to enable GFI EventsManager to archive events.



To enable GFI EventsManager to archive events, the account must have read and write access privilege on the database.



It is recommended to have an SQL Server installation for every GFI EventsManager installation.

2. Ensure that the server has all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
3. Ensure that the GFI EventsManager machine has the right permissions to access and write events in the shared folder.
4. Install GFI EventsManager.
5. Configure the SQL database backend from GFI EventsManager.
6. Configure and add Event Sources. Event sources can be added:
 - » manually from **Configuration ► Event Sources** in GFI EventsManager console.
 - » using the **Automatic network discovery wizard**
 - » using the synchronization feature in GFI EventsManager.
7. Create Database Operations to export and import events to and from the shared folder.
8. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
9. (Optional) Configure rule-sets

For more information on how to perform all the actions mentioned above, refer to the user manual, available on the GFI website at <http://www.gfi.com/eventsmanager>.

Deployment Phases for Site 3

The following steps are required to deploy and configure GFI EventsManager on Sites 3:

1. Install and configure the SQL Server backend. This can be installed remotely or on the GFI EventsManager machine. Create a user account with the required privileges to enable GFI EventsManager to archive events.



To enable GFI EventsManager to archive events, the account must have read and write access privilege on the database.



It is recommended to have an SQL Server installation for every GFI EventsManager installation.

2. Ensure that the servers have all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
3. Ensure that the GFI EventsManager machines have the right permissions to access and write events in the shared folder.
4. Install GFI EventsManager on both machines.
5. Configure the SQL database backend from GFI EventsManager.

6. Configure and add Event Sources. Event sources can be added:
 - » manually from **Configuration ► Event Sources** in GFI EventsManager console.
 - » using the **Automatic network discovery wizard**
 - » using the synchronization feature in GFI EventsManager.
7. Create Database Operations to export and import events to and from the shared folder.
8. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
9. (Optional) Configure rule-sets
10. (Optional) Configure a separate SQL Server instance to be the main database backend, in which all events from the shared folder will be archived. The main database backend will be used to consolidate reporting.

For more information on how to perform all the actions mentioned above, refer to the user manual, available on the GFI website at <http://www.gfi.com/eventsmanager>.

7 Deploying GFI EventsManager in a Mixed Environment

7.1 Introduction

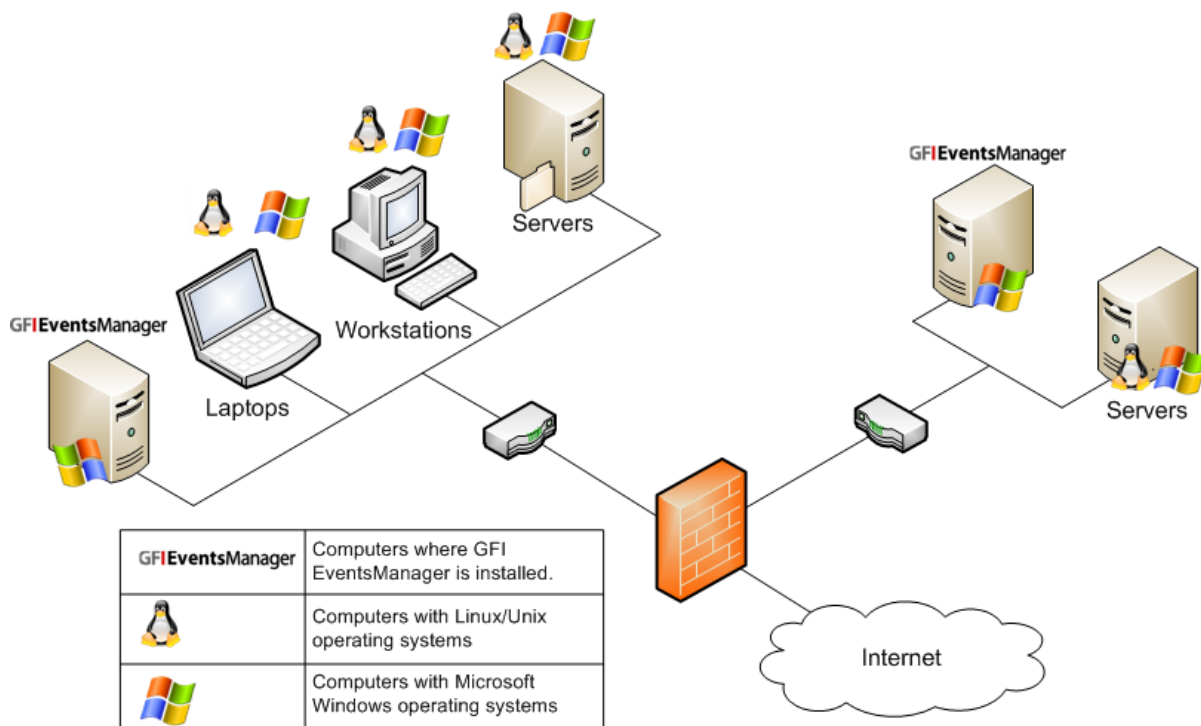


Figure 9 - GFI EventsManager in a mixed environment

This chapter describes a scenario for deploying GFI EventsManager on a LAN where computer systems and network devices generate Windows, Syslog and W3C events.

The Syslog standard is most commonly used for the logging events generated by UNIX and Linux computer systems as well by network devices and appliances (for example, Cisco routers and the Cisco PIX firewalls).

W3C logs mainly used by web servers to log web related events including web logs. W3C events are generated by all the popular web servers, including Microsoft Internet Information Servers (IIS) and Apache.

GFI EventsManager centralizes event management and allows you to collect and process Windows, W3C and Syslog messages through one solution.

Before deploying GFI EventsManager, review the [Deployment considerations](#) section in this guide.

7.2 Deployment Scenario Description

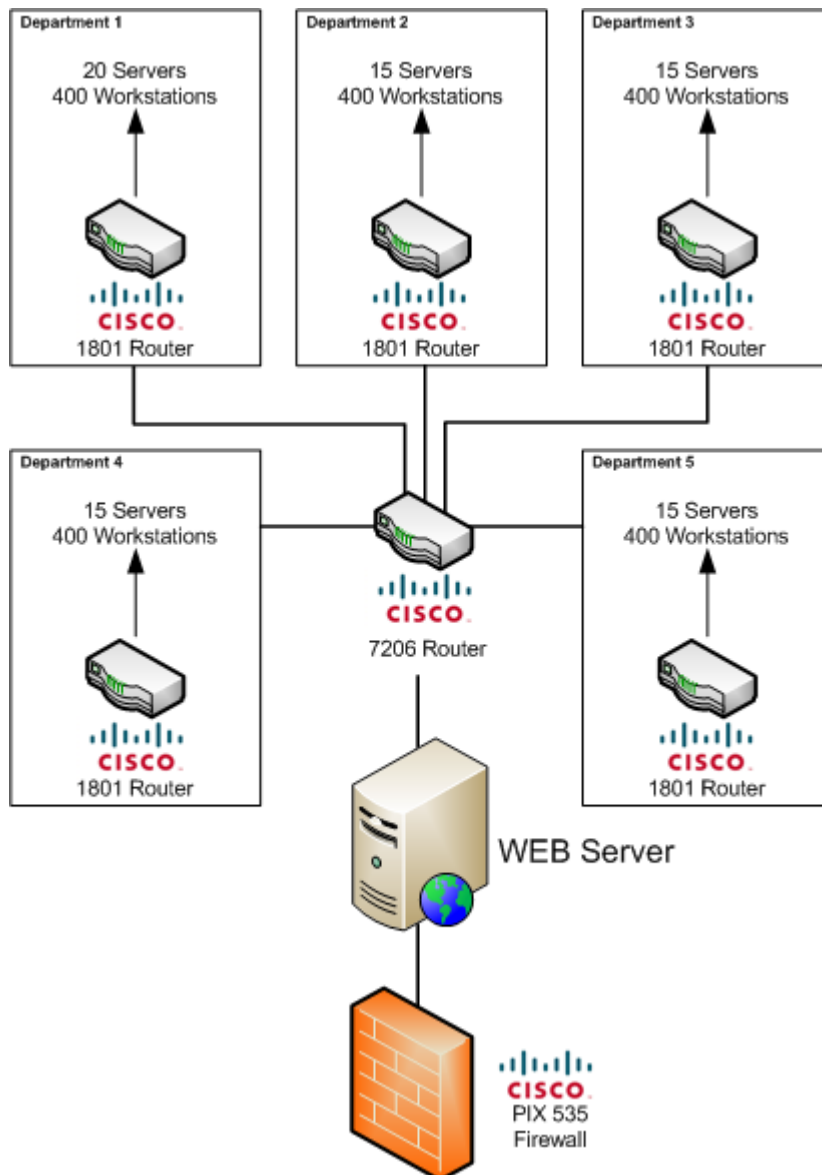


Figure 10 - Scenario for a mixed environment

Within the scenario, there are five departments, each with their own resources linked to the corporate LAN:

Department 1 - 20 servers, 400 workstations, web server, firewall and 2 routers to be monitored

Department 2 - 15 servers, 400 workstations and 1 router to be monitored

Department 3 - 15 servers, 400 workstations and 1 router to be monitored

Department 4 - 15 servers, 400 workstations and 1 router to be monitored

Department 5 - 15 servers, 400 workstations and 1 router to be monitored.

Operating system on the computers:

- » Microsoft Windows servers are installed with Microsoft Windows 2003 Server Enterprise
- » Microsoft Windows Workstations are installed with Microsoft Windows XP SP2.

Cisco routers:

- » Event logging configured at severity level 5
- » Routers have been configured to send Syslog messages to GFI EventsManager

Cisco firewall:

- » Event logging configured at severity level 5
- » Firewall has been configured to send syslog messages to GFI EventsManager

Web server:

- » Microsoft Internet Information Services on Microsoft Windows 2003 Server Enterprise
- » The number of events generated by the web server is proportional to the number of times it is accessed. Thus a heavily accessed web site will generate much more events than a lightly accessed web site.

Calculating the number of events generated

Using the figures described in the [Performance and sizing](#) chapter of this guide, calculate the number of events per hour and the database growth per month:

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Web Servers	1	72,000	72,000
Servers	80	15,000	1,200,000
Workstations	2,000	2,000	4,000,000
Cisco 7206 Router	1	216,000	216,000
Cisco 1801 Router	5	72,000	360,000
Cisco PIX 535 Firewall	1	288,000	288,000
The total number of events			6,136,000
Approximate database storage growth per month in GB			651
Total number of GFI EventsManager installations			2

GFI EventsManager instances required

The two GFI EventsManager instances can be configured as follows:

- 1 GFI EventsManager instance can be configured to monitor the workstations
- 1 GFI EventsManager instance can be configured to monitor the servers, network devices and web server

7.3 Deployment Phases

The following steps are required to deploy and configure GFI EventsManager:

1. Install and configure the SQL Server backend. This can be installed remotely or on the GFI EventsManager machine. Create a user account with the required privileges to enable GFI EventsManager to archive events.



To enable GFI EventsManager to archive events, the account must have read and write access privilege on the database.



It is recommended to have an SQL Server installation for every GFI EventsManager installation.

2. Ensure that the servers have all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
3. Install GFI EventsManager on both machines.
4. Configure the SQL database backend from each GFI EventsManager instance. Both installations of GFI EventsManager can be configured to use the same SQL server.
5. Configure and add Event Sources. Event sources can be added:
 - » manually from **Configuration ► Event Sources** in GFI EventsManager console.
 - » using the **Automatic network discovery wizard**
 - » using the synchronization feature in GFI EventsManager.
6. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
7. (Optional) Configure rule-sets
8. (Optional) Configure a separate SQL Server instance to be the main database backend, in which all events from the shared folder will be archived. The main database backend will be used to consolidate reporting.

For more information on how to perform all the actions mentioned above, refer to the user manual, available on the GFI website at <http://www.gfi.com/eventsmanager>.

8 Deploying GFI EventsManager on Demilitarized Zone

8.1 Introduction

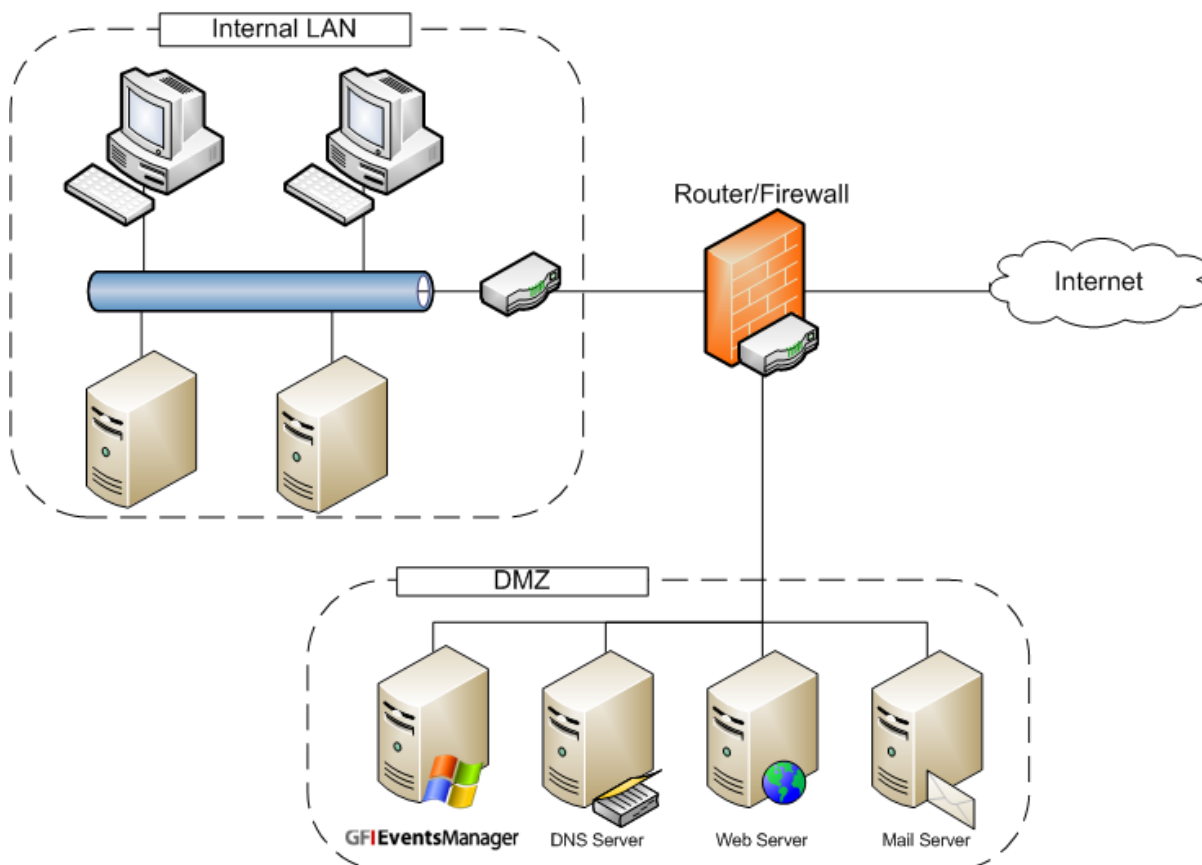


Figure 11 - The DMZ sits between the internal LAN and the Internet

GFI EventsManager can be deployed to monitor a Demilitarized Zone. The DMZ is a sub-network that resides between the internal network and the Internet enabling an organization to expose internal services to external users.

The deployment of GFI EventsManager on a Demilitarized zone helps you automate the management of events generated by DMZ hardware and software systems.

When deployed on a DMZ, GFI EventsManager centralizes event management and enables you to collect and process Windows, W3C and Syslog messages.

Automate management of Web and Mail server events

DMZ networks are normally used to run hardware and software systems that have internet specific roles such as HTTP servers, FTP servers, and Mail servers.

GFI EventsManager can be deployed to automatically process events generated by:

- » Linux/Unix based web-servers including the W3C web-logs generated by Apache web-servers on LAMP web platforms.
- » Windows based web-servers including the W3C web-logs generated by Microsoft Internet Information Servers (IIS).
- » Linux/Unix and Windows based mail-servers
- » Syslog “auditing services” messages on Sun Solaris ver. 9 (or later).

Automate management of DNS server events

An organization can have a public DNS in the demilitarized zone to provide DNS resolution to external users.

GFI EventsManager can collect and process DNS server events including those stored in your Windows' DNS Server logs.

Automate management of network appliance events

Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (e.g. Cisco IOS series routers, CISCO PIX firewalls) not only enable you to protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can increase the operational performance of your systems.

GFI EventsManager can collect and process events generated by such network appliances. GFI EventsManager can be configured to act as a Syslog and SNMP traps Listener and collect in real-time the Syslog and SNMP traps messages generated by the Cisco appliances and other devices.

GFI EventsManager has built-in support (through MIB files and dedicated processing rules) for a wide range of devices and equipment capable of sending SNMP Traps messages. You can also extend the support by adding your own MIB information to the existing database.

8.2 Where to deploy GFI EventsManager

8.2.1 Introduction

This section describes four possible scenarios that can be used to monitor and process events from a DMZ using GFI EventsManager.

8.2.2 Scenario 1

Processing events generated on the DMZ from the LAN is possible. This scenario requires that GFI EventsManager and the SQL database backend is installed and configured on the LAN.

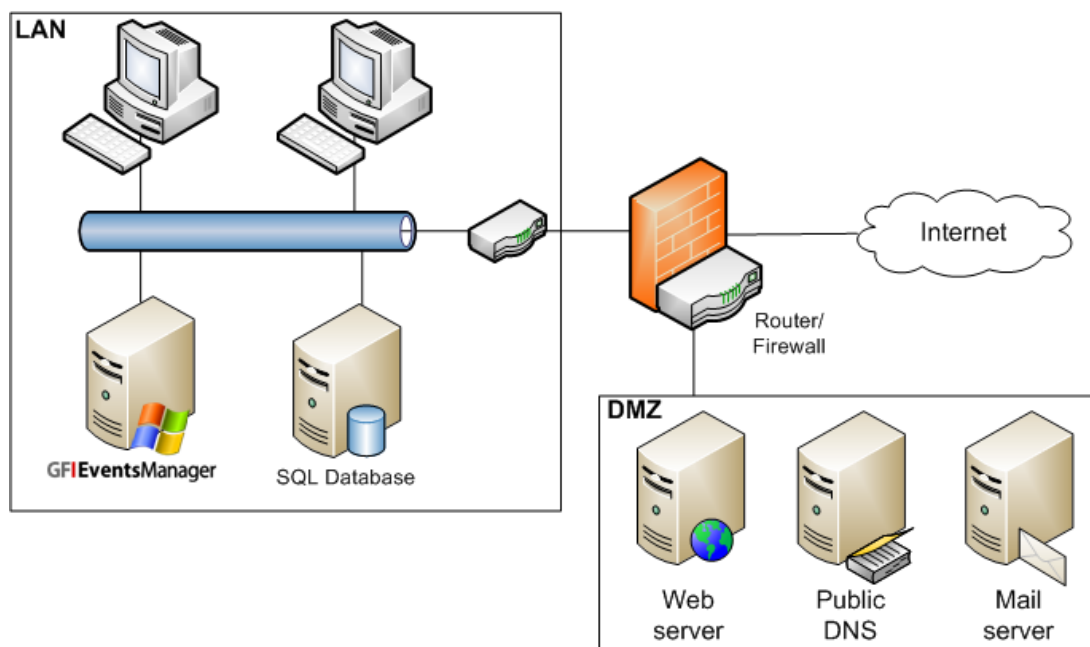


Figure 12 - Scenario1- Deploying GFI EventsManager on the LAN

In this scenario, ensure that the firewall between the LAN and the DMZ is configured to allow GFI EventsManager to collect events from the DMZ. For more information on the ports and permissions that must be enabled, refer to [Ports and permissions that must be enabled](#) section in this guide.

8.2.3 Scenarios 2 and 3

In Scenario 2, GFI EventsManager and the SQL Database backend can be deployed within the DMZ and configured to collect and process events related to the DMZ.

In Scenario 3, GFI EventsManager can be deployed within the DMZ and configured to collect and process events related to the DMZ. The SQL database backend is installed and configured on the corporate LAN.

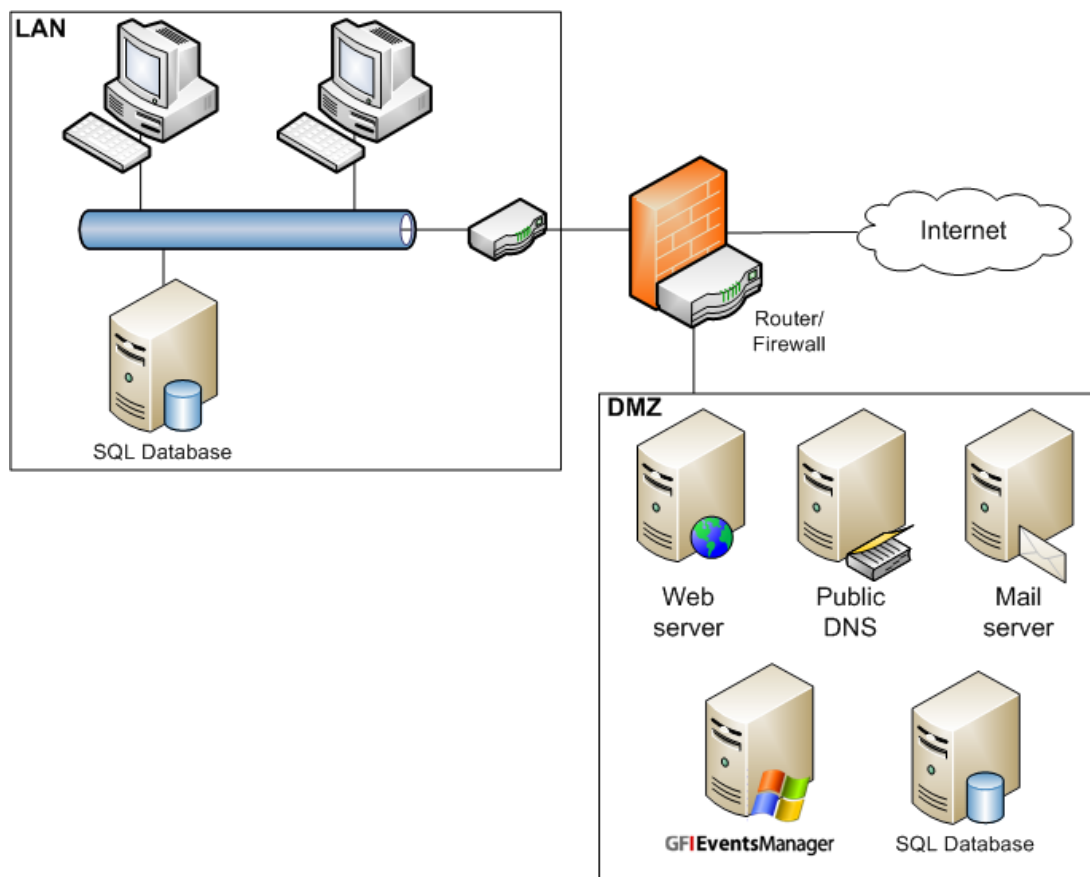


Figure 13 - Scenario 2 and 3- Deploying GFI EventsManager on the DMZ

The only difference between these two scenarios is the installation of the database backend. In Scenario 2 the database backend is installed on the DMZ, while the database backend in Scenario 3 is installed in the corporate LAN.

Both scenarios offer a feasible solution. The number of computers, devices and subsequent number of events on the DMZ might however not justify having a GFI EventsManager solely monitoring DMZ related events.



In Scenario 2, data in the database on the DMZ may also be at a higher risk of compromise.

8.2.4 Scenario 4

GFI EventsManager can be deployed within the DMZ and configured to collect and process all events generated on the corporate LAN and DMZ. The SQL database backend is installed and configured on the DMZ.

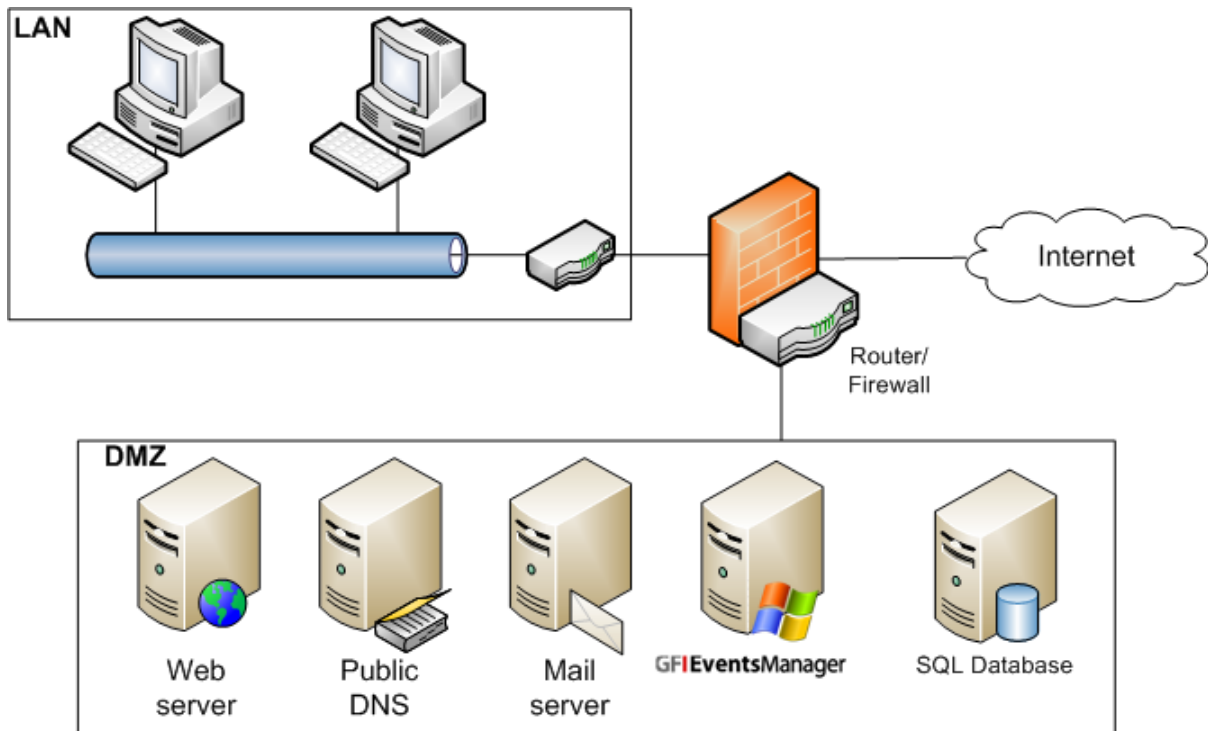


Figure 14 - Scenario 4 - Deploying GFI EventsManager on the DMZ and collect all events

This scenario is not recommended. All audit data will be exposed on the DMZ. Sensitive data may be compromised.

8.3 Deployment scenario description

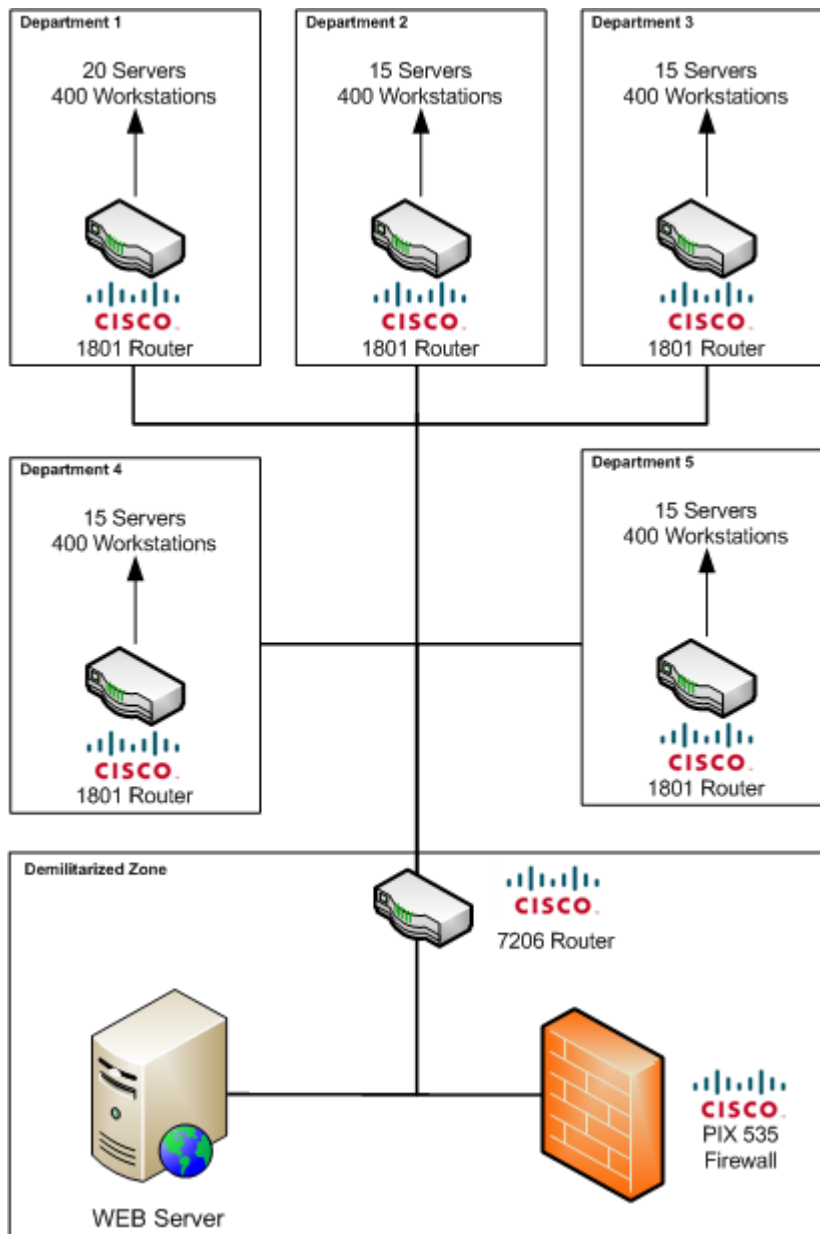


Figure 15 - Monitoring events on a DMZ

8.3.1 Calculating the number of events generated

The scenario consists of the following devices:

CORPORATE LAN	
Microsoft Windows 2003/2008 Servers	80
Microsoft Windows XP SP2/Vista/win7 Workstations	2000
Cisco 1801 routers	5
DMZ	
Cisco 7206 router	1
Cisco PIX 535 firewall	1
Web server	1

Cisco routers:

- » Event logging notification severity is set to 5
- » Routers configured to send syslog messages to GFI EventsManager

Cisco firewall:

- » Event logging notification severity is set to 5
- » Firewall has been configured to send syslog messages to GFI EventsManager

Web server:

Microsoft Internet Information Services on Microsoft Windows 2003 Server Enterprise

- » The number of events generated by the web server is proportional to the number of times it is accessed. Thus a heavily accessed web site will generate much more events than a lightly accessed web site.
- » Using the figures described in the [Performance and sizing](#) chapter of this guide, calculate the number of events per hour and the database growth per month:

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
Web Servers	1	72,000	72,000
Servers	80	15,000	1,200,000
Workstations	2000	2,000	4,000,000
Cisco 7206 Router	1	216,000	216,000
Cisco 1801 Router	5	72,000	360,000
Cisco PIX 535 Firewall	1	288,000	288,000
The total number of events			6,136,000
Approximate database storage growth per month in GB			651
Total number of GFI EventsManager installations			2

Both GFI EventsManager instances can be configured:

- » A GFI EventsManager instance can be configured to process events from all workstations.
- » A GFI EventsManager instance can be configured to process events from all servers, network devices and the web server

8.4 Deployment Phases

The following steps are required to deploy and configure GFI EventsManager:

1. Install and configure the SQL Server backend. Create a user account with the required privileges to enable GFI EventsManager to archive events.



To enable GFI EventsManager to archive events, the account must have read and write access privilege on the database.



It is recommended to have an SQL Server installation for every GFI EventsManager installation.

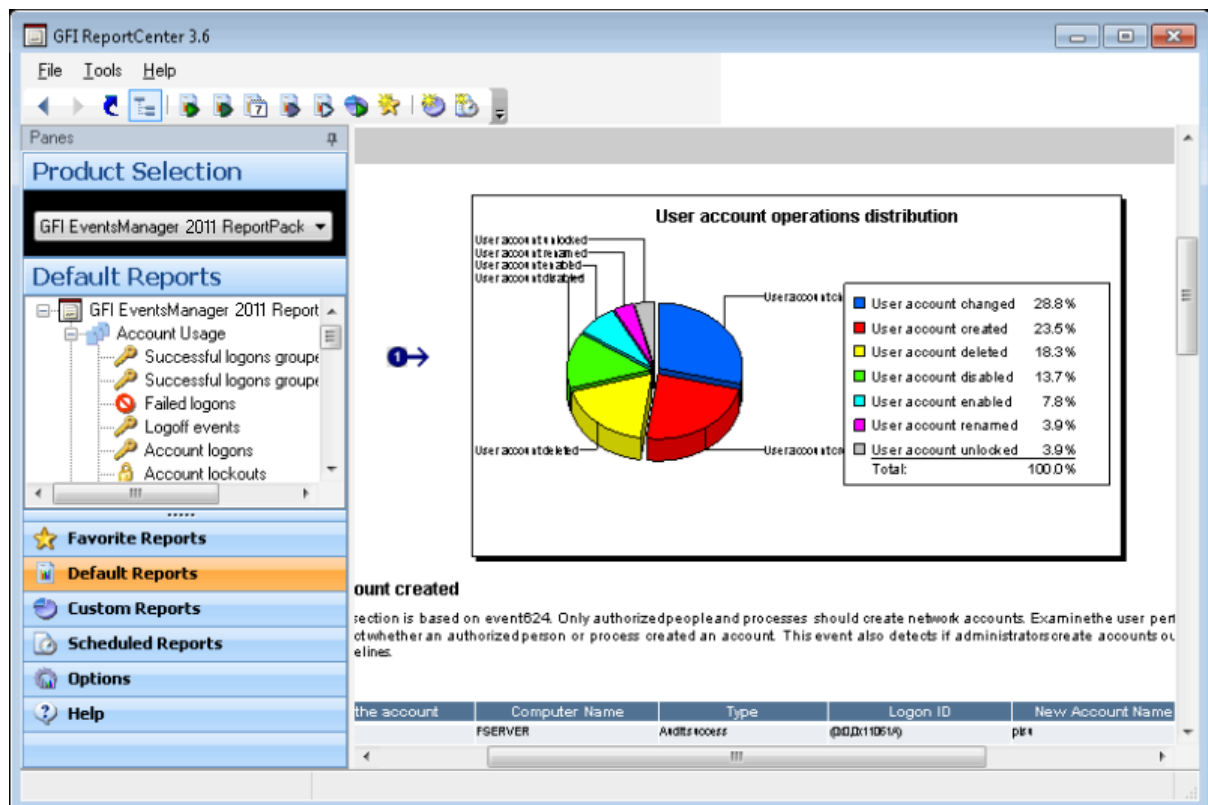
2. Ensure that the servers have all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.

3. Install GFI EventsManager on both machines.
4. Configure the SQL database backend from each GFI EventsManager instance. Both installations of GFI EventsManager can be configured to use the same SQL server.
5. Configure and add Event Sources. Event sources can be added:
 - » Manually from **Configuration ► Event Sources** in GFI EventsManager console.
 - » Using the **Automatic network discovery wizard**
 - » Using the synchronization feature in GFI EventsManager.
6. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
7. (Optional) Configure rule-sets
8. (Optional) Configure a separate SQL Server instance to be the main database backend, in which all events from the shared folder will be archived. The main database backend will be used to consolidate reporting.

For more information on how to perform all the actions mentioned above, refer to the user manual, available on the GFI website at <http://www.gfi.com/eventsmanager>.

9 Deploying GFI EventsManager ReportPack

9.1 Introduction



GFI EventsManager ReportPack

The GFI EventsManager ReportPack is a fully fledged reporting companion to GFI EventsManager. It enables you to generate graphical IT-level, technical and management reports based on the events collected and processed by GFI EventsManager.

GFI EventsManager ReportPack provides you with easy-to-view trend reports for management as well as daily drill-down reports for technical staff. This caters for information required to fully understand the events activity on your corporate network and to provide the necessary data to meet various compliance regulations.

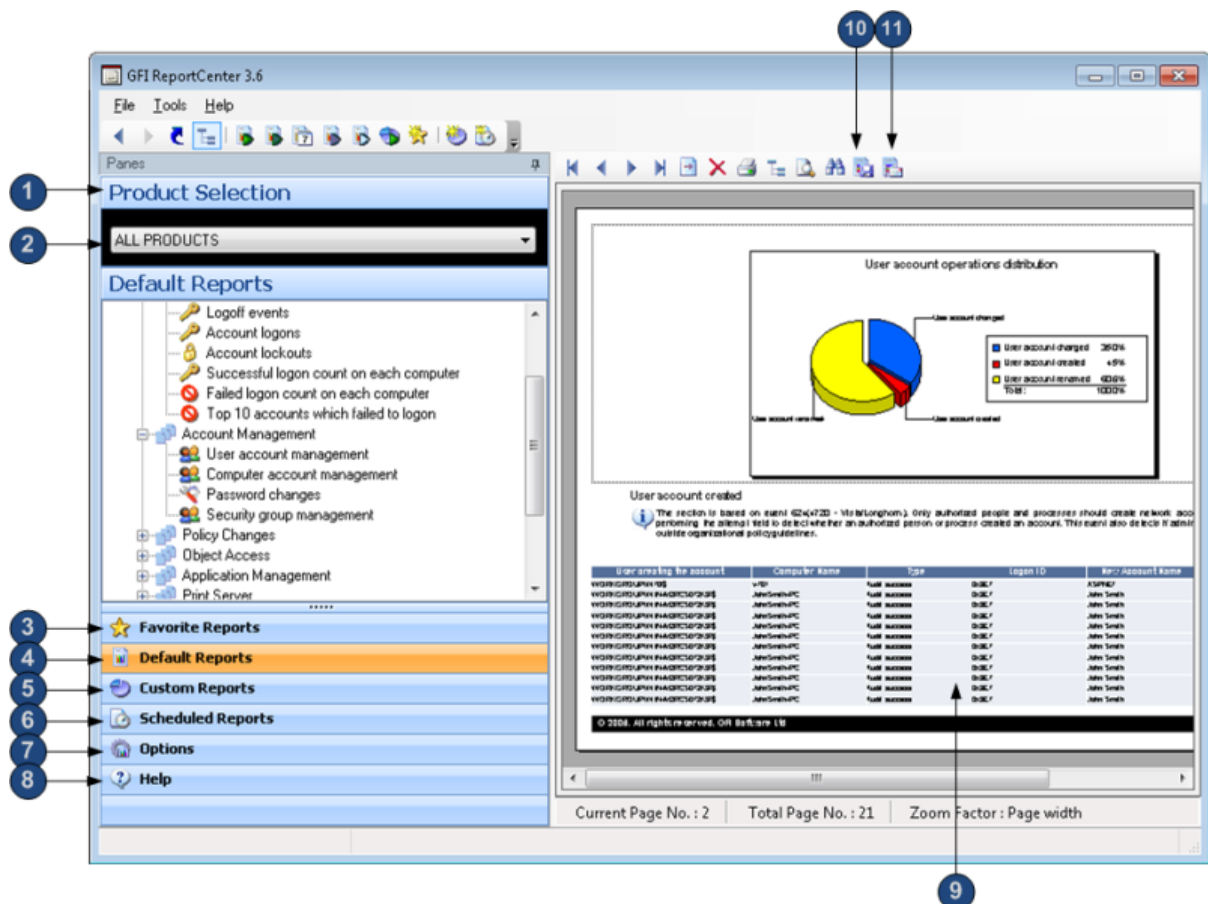
For more information on GFI EventsManager ReportPack, refer to <http://www.gfi.com/eventsmanager/esmreportpack.htm>

9.2 About the GFI EventsManager ReportPack

The GFI EventsManager ReportPack provides the following graphical and text based reports:

- » Account Usage
- » Account Management
- » Policy Changes
- » Object Access
- » Application Management
- » Print Server
- » Windows Event Log system
- » Events Trend
- » PCI DSS Compliance Reports
- » General and Security Requirements
- » SOX Compliance
- » HIPAA Compliance
- » GLBA Compliance
- » All critical messages
- » Miscellaneous, customizable reports.

9.3 GFI EventsManager ReportPack management console



Screenshot 3 - The GFI ReportCenter management console

The following table describes the components within the management console:

1	Navigation Pane - Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
2	Product Selection drop-down list - To generate reports for a specific product, select the product from the drop down list.
3	Favorite Reports - Use this navigation button to access your favorite/most used reports.
4	Default Reports - Use this navigation button to access the default list of reports that can be generated for the selected product.
5	Custom Reports - Use this navigation button to access the list of customized reports that can be generated for the selected product.
6	Scheduled Reports - Use this navigation button to access the list of scheduled reports for automatic generation and distribution.
7	Options - Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.
8	Help - Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
9	Report Pane - Use this multi-functional pane to: <ul style="list-style-type: none">» View and analyze generated reports» Maintain the scheduled reports list» Explore samples and descriptions of default reports.
10	Export - Use this button to export generated reports to various formats including HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC), and Rich Text Format (RTF).
11	Send email - Use this button to instantly distribute the last generated report via email.

9.4 Deployment Phases

To deploy GFI EventsManager ReportPack:

1. Install and configure GFI EventsManager
2. Install GFI ReportCenter Framework. Download GFI ReportCenter from <http://www.gfi.com/reportcenter>
3. Install GFI EventsManager ReportPack. During the installation the following settings need to be configured:
 - » Database backend
 - » Email settings for scheduled reports

For more information on how to install and configure the GFI ReportPack refer to GFI EventsManager ReportPack Manual downloadable from <http://www.gfi.com/products/gfi-eventsmanager/manual>

9.5 Deployment scenario

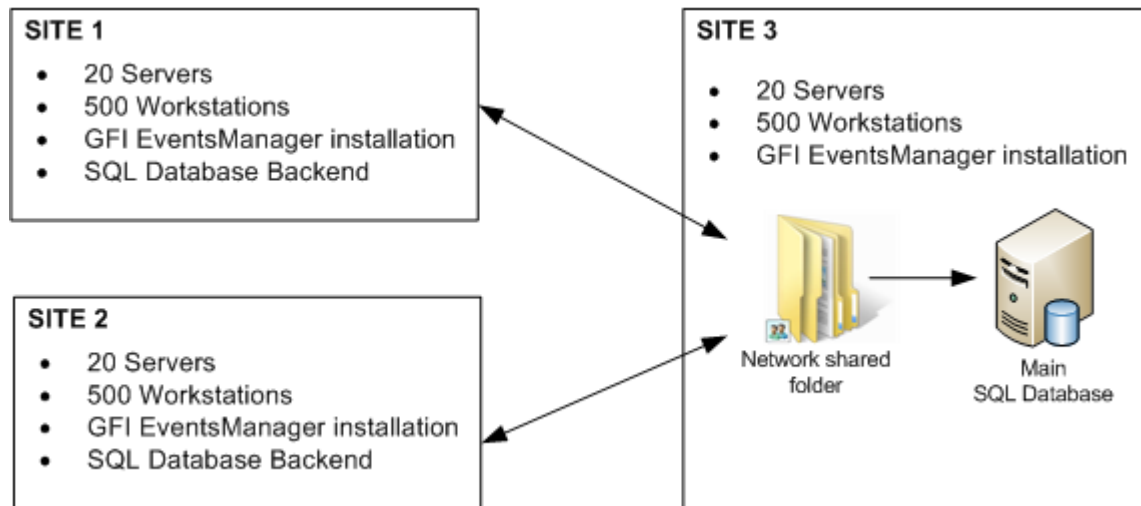


Figure 16 - Multiple sites with centralized reporting

Site 1 and Site 2

Each site contains a GFI EventsManager installation that process events generated within the site and an SQL Database backend that stores the data collected by the GFI EventsManager installation. A GFI EventsManager database operation is configured to export all data collected within the site from the database backend to a network-shared folder located in Site 3.

Site 3 (Head office)

This site contains:

- » A GFI EventsManager installation - this will process events generated by all sites
- » A main SQL Database backend that stores all events generated by all sites.
- » A GFI EventsManager database operation is configured to import all data from the network-shared folder to the Main SQL Database located in Site 3.

GFI EventsManager ReportPack installation

GFI EventsManager ReportPack is installed on all sites and can be configured as follows:

1. Configure the GFI ReportPack on all sites to connect to the local SQL Server backend. All reports generated at each site will contain information relevant to that site. The reports generated from the main database at Site 3 will contain correlated data from all sites.
2. Configure the GFI ReportPack on all sites to connect to the main database backend at Site 3. All reports generated at each site will contain information from all sites.

Issues to consider

Bandwidth and performance in the above scenarios are an issue, as data for the reports generated is transferred over the network.

Network unavailability between remote sites on the WAN is also an issue. If a site is unreachable, data is not retrieved.

Recommendation

The scenario to adopt depends on three factors:

- » Bandwidth/Performance considerations
- » Network availability
- » Company policy and requirements.

Reports via email

To send reports via email ensure that:

- » The SMTP server details are configured
- » The SMTP server is always available
- » Internet access is always available.

10 Appendix 1: Instance Calculator

10.1 Introduction

The instance calculator to enables you to estimate the number of GFI EventsManager instances required on your network.

Welcome to the GFI EventsManager Instance Calculator
Use this calculator to estimate the number of GFI EventsManager instances that you need to monitor your network events and the respective database storage growth.

Specify the estimated number of devices where events will be processed by GFI EventsManager.

	Number of Devices	Events per hour
Domain controllers	1	100,000
Servers	2	30,000
Workstations	100	200,000
Low-End Routers	1	72,000
High-End Routers	1	216,000
Firewalls	1	288,000
Web Servers	1	72,000
Total number of events per hour		978,000

Results
GFI EventsManager instances needed: 1
Estimated Database storage growth per month: 104 GB

Calculate **Reset** Save

Key in the number of Web Servers to include.

Screenshot 4 - GFI EventsManager Instance calculator

Download the GFI EventsManager Instance Calculator from:

<http://www.gfi.com/eventsmanager/esm7calculator.xls>

Launch calculator and key-in the number devices in your network. Click **Calculate** to get an estimate of the number of events generated per hour and the total number of GFI EventsManager instances required.



Calculator should only be used to estimate the GFI EventsManager instances required and database growth. Events per hour used and database growth may not be representative of your IT environment.

11 Appendix 2: SQL Server Best Practices

11.1 Introduction

The SQL Server Best Practices resources provided below are available from the Microsoft website.

Database Engine Tuning Advisor (DTA)

The DTA enables the administrator to create optimal set of indexes, views and partitions on the database backend without expertise knowledge. For more information refer to <http://msdn.microsoft.com/en-us/library/ms173494.aspx>

Monitoring and Tuning for Performance

This content is part of the product documentation for SQL Server 2008, available on the MSDN Library. For information, refer to <http://msdn.microsoft.com/en-us/library/ms189081.aspx>

SQL Server best practices analyzer

Microsoft SQL Server Best Practices Analyzer is a database management tool that enables you to verify the implementation of common best practices on your SQL servers. For more information refer to

<http://www.microsoft.com/downloads/en/details.aspx?familyid=b352eb1f-d3ca-44ee-893e-9e07339c1f22&displaylang=en>

Maximum Capacity Specifications for SQL Server 2008 R2

This content is part of the product documentation for SQL Server 2008 R2, available on the MSDN Library. For information, refer to <http://msdn.microsoft.com/en-us/library/ms143432.aspx>

Additional resources

For more resources refer to the SQL Server Books Online from <http://msdn.microsoft.com/en-us/library/ms130214.aspx>

12 Appendix 3: Checklist

12.1 Introduction

Use this checklist as an aid during the planning stage of the GFI EventsManager deployment project. The checklist highlights the important phases of a deployment project. Refer to the topics within the deployment guide for further information on each checklist item.

Identify deployment objectives		
Use GFI EventsManager for:		
Legal Compliance	<input type="checkbox"/>	Security Monitoring
System Health Monitoring	<input type="checkbox"/>	Forensic Analysis
Notes:		
Identify logs to collect events from:		
Windows	<input type="checkbox"/>	Syslog
	<input type="checkbox"/>	W3C
Notes:		
Identify configuration settings required of the logs at "source"		
Notes:		
Identify events to be configured as noise		
Notes:		
Determine whether events will be archived or processed using default rule sets		
Notes:		
Determine whether additional rule set configuration is required		
Notes:		

Determine number of GFI EventsManager instances required		
Determine number of geographically remote sites		
Notes:		
Determine which devices to monitor		
Notes:		
Calculate instances required		
Notes:		
Determine quantity and type of licenses required		
Notes:		

Determine SQL Server backend to use		
Determine whether new SQL Server installation is required		
Notes:		
Determine edition to use		
Notes:		

Verify is SQL Server machine(s) meet recommended specifications Notes:	
Determine whether SQL Server instance will be local or remote Notes:	
Determine database maintenance strategy Notes:	
Verify SQL Server authentication details Notes:	
Verify if GFI EventsManager WAN Connector is required Notes:	
Determine deployment machine(s) to use	
Verify if machine(s) meet recommended specifications Notes:	
Verify load on the machines Notes:	
Verify system settings for event sources	
Windows Event Logs: Remote registry service is enabled and running Windows audit service is enabled and running Notes:	
W3C (CLF) Logs: W3C log source folders are accessible via Windows Administrative Shares Notes:	
Syslog: Sources are configured to send their Syslog messages through UDP port Firewall(s) are configured to allow Syslog messages through UDP ports Notes:	
Determine administrative credentials required for Windows and W3C event sources Notes:	
Determine non-trusted domains configuration requirements	
If non-trusted domains will be monitored, determine the alternate administrative credentials required by GFI EventsManager to collect data from these domains Notes:	
Determine firewall and anti-virus configuration requirements	
Verify that traffic is not blocked on the ports in use by GFI EventsManager Notes:	

Verify esmui.exe and esmproc.exe are allow access through firewall(s) Notes:	<input type="checkbox"/>
Verify that GFI EventsManager folders are excluded from real-time scanning Notes:	<input type="checkbox"/>
Verify that alerting traffic is not blocked by firewall(s) Notes:	<input type="checkbox"/>

Determine alerting requirements	
Email alerting: Identify SMTP server details Verify that the SMTP server will always be available Verify that internet access will always be available Notes:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Network messages: Verify that the messenger service in Windows is enabled and running Notes:	<input type="checkbox"/>
SMS alerting: Identify service provider details Notes:	<input type="checkbox"/>
Email-to-SMS messages: Identify service provider details Identify SMTP server details Verify that the SMTP server will always be available Verify that internet access will always be available Notes:	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

A

alerting 13, 26, 31, 43

anti-virus 10

B

bandwidth 15, 18, 20, 48

benchmark 1, 17, 18, 19, 29

C

Cisco firewall 35

Cisco router 33, 42

Configuration settings 7, 17, 18, 47

D

database backend 3, 5, 11, 12, 17, 18, 19, 26, 30, 31, 36, 38, 39, 40, 43, 47, 48

Database Backend 3, 5, 9, 11, 12, 17, 18, 19, 26, 30, 31, 36, 38, 39, 40, 43, 47, 48

database maintenance 12

Database Operations 12, 14, 15, 27, 31

Default reports 47

disk space 21

E

Email 4, 5, 13, 47, 49

Event color-coding 4

Event finder tool 4

Event processing rules 3, 5

Event query 4

Event query builder 4

event source 5, 14, 25, 26, 28, 29, 30, 31, 36, 43

F

Favorite reports 47

firewall 10, 26, 30, 34, 35, 36, 41, 42

I

IIS 33

GFI EventsManager

K

Knowledge Base 2

L

LAN 2, 20, 23, 33, 37, 38, 39, 41

N

Navigation button 47

Network alerts 5

P

port 5, 38

Product Selection drop down list 47

R

remote site 2, 28

ReportPack 4, 45, 46, 47, 48

S

Scheduled reports 47

SMS 13

SNMP traps 3, 9

specifications 17, 19, 53

SQL Server 2, 3, 4, 11, 17, 18, 20, 26, 30, 35, 36, 42, 43, 48, 53

Storage 5, 11, 12, 20, 24, 28, 29, 42

Storage Folder 5, 11, 12

syslog 2, 5, 17, 33, 35, 37, 38, 42

Syslog 2, 5, 17, 33, 35, 37, 38, 42

SYSLOG 2, 5, 17, 33, 35, 37, 38, 42

Syslog message 5, 19, 35, 37, 42

Syslog messages 5, 9, 19, 35, 37, 42

W

W3C 2, 7, 17, 33, 37

W3C log 7, 17, 33

W3C logs 17, 33

WAN 14, 20, 27

web server 33, 34, 35, 42

Windows 7 10

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

ENGLAND AND 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.com

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



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided “as is” with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.