

GFI Product Manual

GFI *EventsManager*[™]

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or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors.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-02.00.01

Last updated: September 26, 2012

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	System requirements	8
3.4	Upgrading from a previous version	11
3.5	Database and Files backend	13
3.6	Alerting	15
3.7	Multiple domain, multiple site environments	16
3.8	Bandwidth considerations.....	17
3.9	Licensing.....	17
4	Performance and Sizing	19
4.1	Introduction	19
4.2	Benchmark test results	19
4.3	Bandwidth utilization	20
4.4	Steps required for determining the deployment solution	20
4.5	Recommendations.....	22
5	Deploying GFI EventsManager on a Single Domain LAN	23
5.1	Introduction	23
5.2	Scenario 1: Small single domain network with default Audit Policy enabled	24
5.3	Scenario 2: Large single domain network.....	25
5.4	Deployment Phases	25
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	31
7.1	Introduction	31
7.2	Deployment Scenario Description	32
7.3	Deployment Phases	33

8	Deploying GFI EventsManager on Demilitarized Zone	34
8.1	Introduction	34
8.2	Automate management of Web and Mail server events	34
8.3	Automate management of DNS server events	35
8.4	Automate management of network appliance events	35
8.5	Where to deploy GFI EventsManager	35
8.6	Deployment scenario description	39
8.7	Deployment Phases	40
9	GFI EventsManager Reporting	41
9.1	Introduction	41
9.2	Available reports	41
10	Appendix 1: Instance Calculator	43
11	Appendix 2: Checklist	45
	Index	49

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, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.



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 Considerations Describes important issues that should be taken into consideration when preparing the plan for a GFI EventsManager deployment project.
Chapter 4	Performance and Sizing 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 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	DESCRIPTION
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 Text Log 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	GFI EventsManager Reporting Gives an overview of the GFI EventsManager Reporting feature and describes the available reports.
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: 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

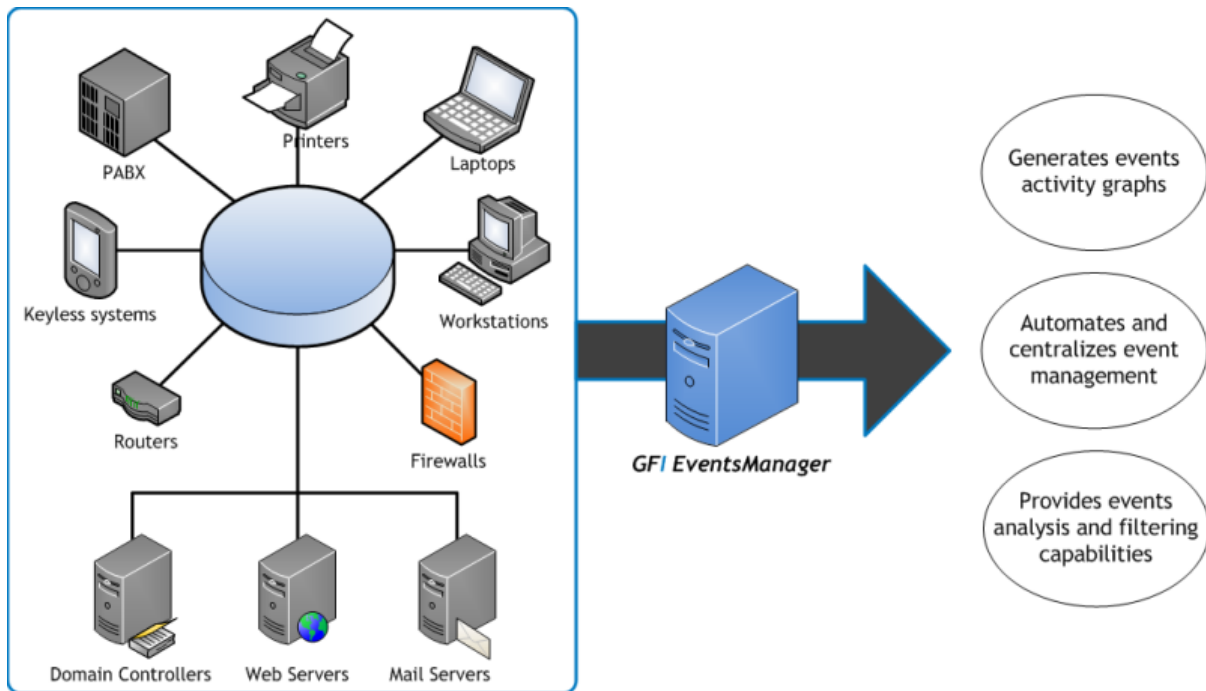


Figure 1 - GFI EventsManager integrates into any existing IT infrastructure

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 Text Logs, 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.
- › Store collected events in a centralized 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?

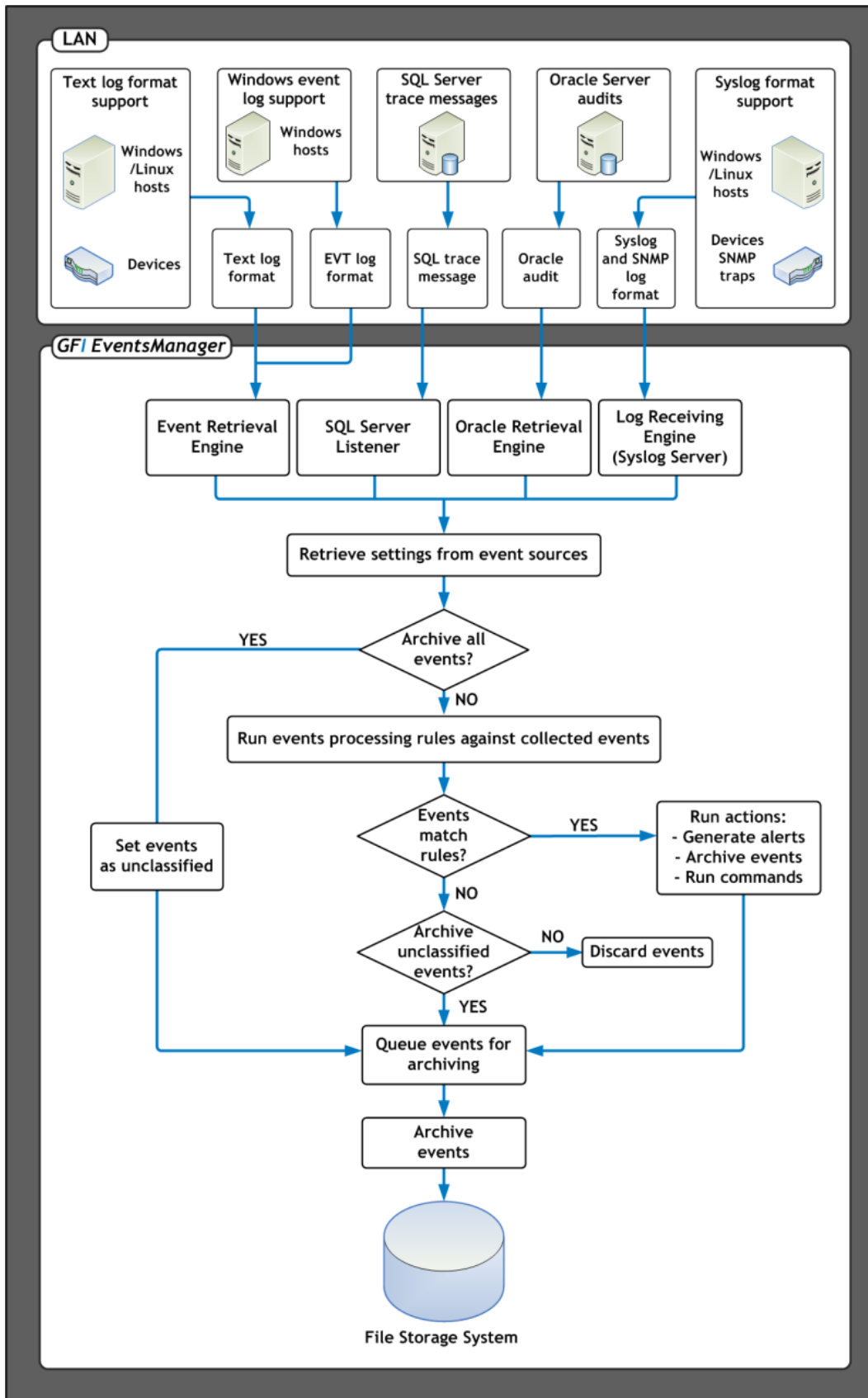


Figure 2 - The GFI EventsManager operational stages

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

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

2.2.1 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**.

Table 1 - GFI EventsManager engines

ENGINE	DESCRIPTION
The Event Retrieval Engine	<p>The Event Retrieval Engine is used to collect Windows Event Logs and Text from networked event sources. During the Event Collection process this engine will:</p> <ol style="list-style-type: none">1. Log-on to the event source(s)2. Collect events from the source(s)3. Send collected events to the GFI EventsManager Server4. Log-off from the event source(s). <p>The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console</p>
The SQL Server Listener	<p>The listener receives trace messages from the scanned Microsoft SQL Server in real time. On receipt, EventsManager processes the message immediately.</p>
The Oracle Retrieval Engine	<p>The Oracle Retrieval Engine connects periodically to Oracle servers and collects audits from a specific auditing table. Similar to the Microsoft Windows Event Retrieval Engine, GFI EventsManager processes events generated by the Oracle server.</p>
Log Receiving Engine	<p>The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/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.</p> <p>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 however customizable via the GFI EventsManager management console.</p>

2.2.2 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 and network alerts on key events
- » Trigger remediation actions such as the execution of executable files or scripts on key events
- » Optionally archive collected events in the database backend.

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.

3 Deployment Considerations

3.1 Introduction

This chapter contains important factors to consider when designing a plan for GFI EventsManager deployment. It is made up of the following sections:

- » Deployment objectives
- » System requirements
- » Upgrading from a previous version
- » Database and Files backend
- » Alerting
- » Multiple domain, multiple site environments
- » Bandwidth considerations
- » Licensing

3.2 Deployment Objectives

Spend some time to consider which devices to monitor and for what purpose. Follow the steps below to develop a plan to successfully install GFI EventsManager:

STEP	DESCRIPTION
Step 1	Clearly identify the objectives to achieve through GFI EventsManager. Your objectives can be focused on one or more of the following areas: <ul style="list-style-type: none">» Legal Compliance» System Health Monitoring» Security Monitoring» Forensic Analysis.
Step 2	After establishing your main objectives, identify: <ul style="list-style-type: none">» The logs to collect events from» Configuration settings of the logs at source:<ul style="list-style-type: none">• Windows audit settings• Syslog logging options• SNMP traps logging options• Text 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 configure GFI EventsManager, may lead to:

- » Irrelevant events collection
- » Higher database growth rate
- » Unnecessary resource utilization in collecting unimportant events
- » Additional administrator time required to filter unimportant events.

3.3 System requirements

3.3.1 Hardware requirements

Table 2 - Hardware requirements

HARDWARE COMPONENT	SPECIFICATION
Processor	2.5 GHz dual core or higher.
RAM	3 GB.

3.3.2 Storage requirements

The following specifications are based on the average size of event logs, i.e.

Table 3 - Storage requirements

STORAGE SPACE	NUMBER OF EVENTS
Events stored per 1 Gb of storage space	2,006,994
Events stored in 500 Gb of storage space	1,003,497,032



The above specifications are based on an average size of event logs, being 535bytes per event.

3.3.3 Software requirements

Operating System (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

- » Microsoft .NET framework 4.0
- » Microsoft Data Access Components (MDAC) 2.8 or later
- » A mail server (when email alerting is required).



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>

3.3.4 Event source settings

The below table describes the configuration required for event sources:

Table 4 - System requirements: Event source settings

LOG TYPE	DESCRIPTION
Windows event log processing	Enable remote registry.

LOG TYPE	DESCRIPTION
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, refer to Miscellaneous .

3.3.5 Ports and permissions

The table below specifies the Ports required by GFI EventsManager:

Table 5 - System requirements: Ports and protocols

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.

The table below specifies the Firewall Permissions required by GFI EventsManager:

Table 6 - System requirements: Firewall permissions

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
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

FIREWALL PERMISSIONS AND AUDIT POLICIES	MICROSOFT WINDOWS SERVER 2008	MICROSOFT WINDOWS SERVER 2003	MICROSOFT WINDOWS XP	MICROSOFT WINDOWS VISTA	MICROSOFT WINDOWS 7
Audit policy: Audit system events	Enable	Enable	Enable	Enable	Enable



3.3.6 Monitoring event logs from Microsoft Windows Vista or later

GFI EventsManager cannot be installed on Microsoft Windows XP to monitor events of Microsoft Windows Vista or later. Microsoft Windows Vista and Microsoft Windows 7 introduced extensive structural changes in event logging and event log management. The most important of these changes include:

- » 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 old 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
- » Microsoft Windows 7
- » Microsoft Windows Server 2008.

	Windows XP events can be collected when GFI EventsManager is installed on Microsoft Windows Vista or later machines.
	When GFI EventsManager is using a non-domain account to collect events from Microsoft Vista machines or later, target machines must have User Account Control (UAC) disabled. For more information on how to disable UAC, refer to Disable UAC to scan target machines section in this manual.

3.3.7 Other considerations

CONSIDERATION	DESCRIPTION
Firewalls and Antivirus software	<p>If firewall(s) are enabled and anti-virus software installed on the computer where GFI EventsManager is running, make sure that:</p> <ul style="list-style-type: none"> » 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. <p>For more information on the ports and permissions that must be enabled, refer to Ports and permissions.</p>
Computer identification	<p>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.</p>

3.4 Upgrading from a previous version

Upgrading from versions older than GFI EventsManager 2011 is not fully supported. Some settings may be lost due to the underlying technology changes.

3.4.1 Methods of upgrading

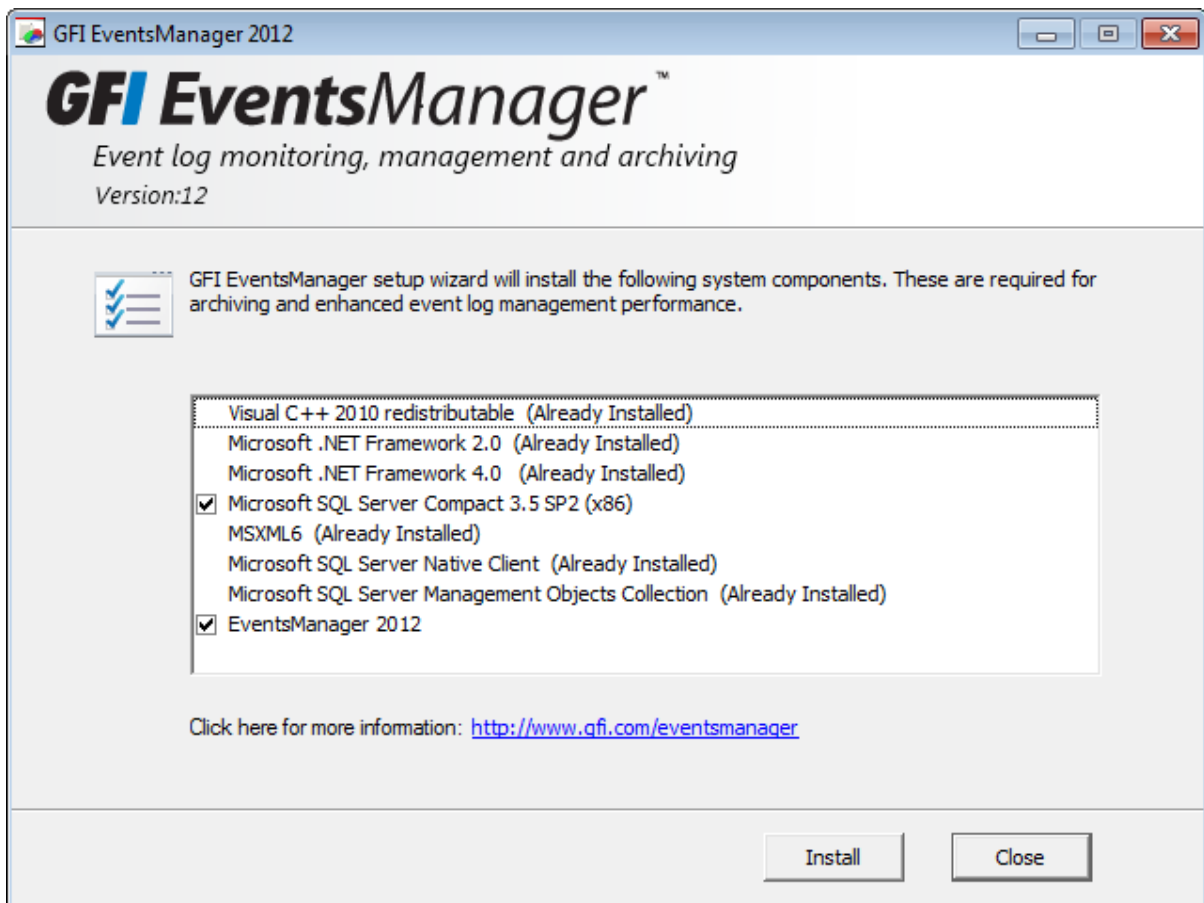
Table 7 - Upgrade methods

METHOD	DESCRIPTION
Automatic	Launch the new setup and complete the wizard to upgrade and retain data. For more information, refer to Upgrading GFI EventsManager .
Manual	Export events from an older version of GFI EventsManager and import it in the new one using Database Operations. For more information, refer to Database Operations .

3.4.2 Upgrading GFI EventsManager

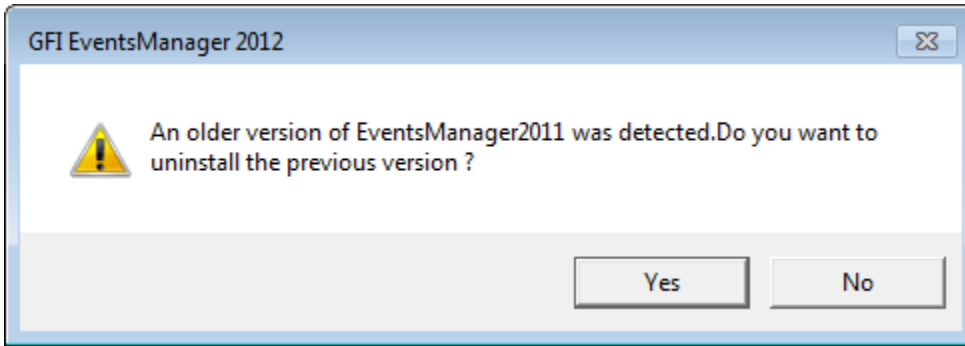
To upgrade to a new version:

1. Launch **EventsManager.exe**.



Screenshot 1 - Upgrade prerequisite check

2. Click **Install** to install the required missing components and the new version of GFI EventsManager.

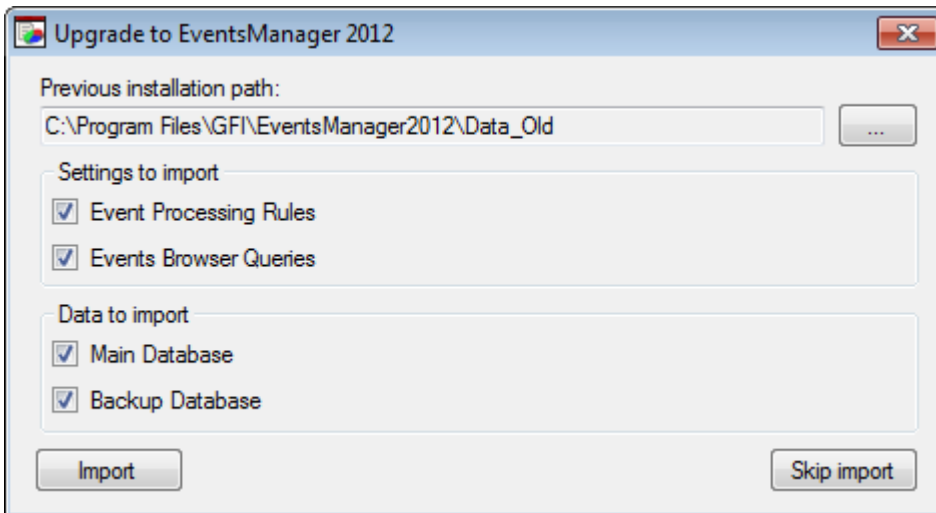


Screenshot 2 - Uninstall previous version

3. Before installing the new version, select one of the options described below. Wait for GFI EventsManager to install:

Table 8 - Upgrade options

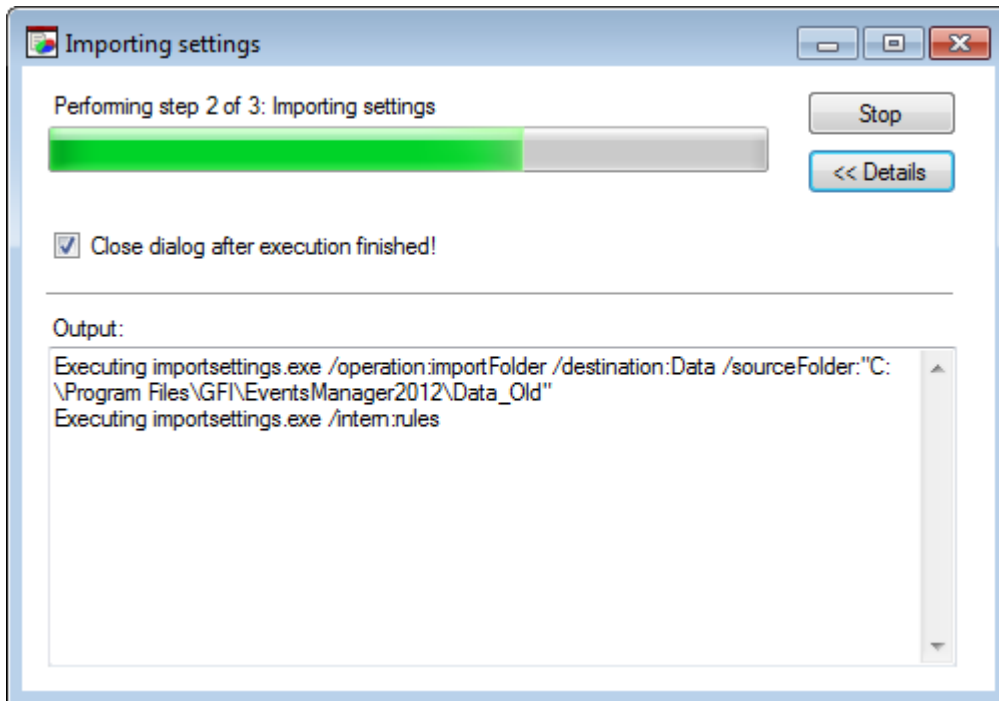
OPTION	DESCRIPTION
Yes	Replaces the old version with the new one.
No	Keeps the old version and the installation stops.



Screenshot 3 - Upgrade import dialog

4. Once installed, the upgrade dialog is automatically launched. Select the settings to import and the location from where to import events.

5. Click **Import** to start importing data.



Screenshot 4 - Import progress

6. Wait for the import job to finish. GFI EventsManager Management Console opens automatically on completion.

3.5 Database and Files backend

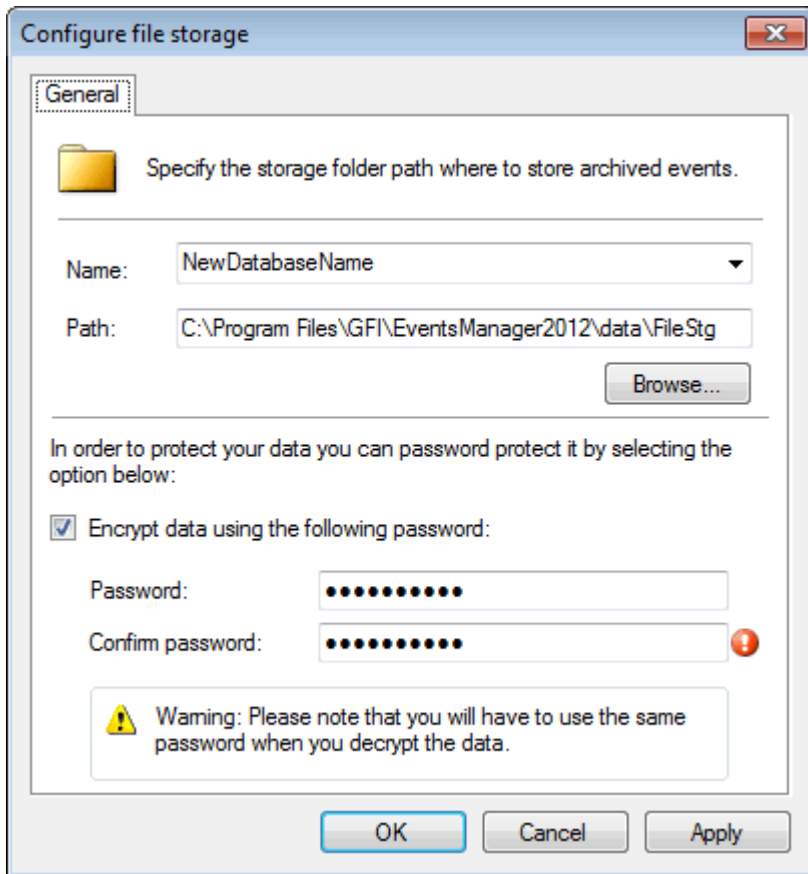
GFI EventsManager uses a built in file storage system which allows great scalability with its fast read/write capabilities even when processing high volumes of events. You may have as many databases as required. The Events Browser enables you to easily switch from on database to another, allowing you to view past events from older databases.

As an example, you can create a new database for every month or year depending on the volume of event logs that you estimate to process.

You can also encrypt new databases before starting to use them. The live database can only be encrypted though esmllibm.exe.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.



Screenshot 5 - Configuring the file storage system

3.5.1 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. This also has a negative impact on reporting performance, causing reports to take longer to generate.

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

Table 9 - Available database operations

DATABASE OPERATION	DESCRIPTION
Import from file	The Import from file job enables you to import data as part of the data centralization process. Only files created from an Export to file job are supported for import.
Export to file	The Export to file job enables you to export data into a file to import into another instance of GFI EventsManager or to archive in an external storage media for safekeeping.
Import from SQL Server database	The Import from SQL Server database job enables you to import events collected from older versions of GFI EventsManager.
Import from legacy files	The Import from legacy files job enables you to import configuration files exported from older versions of GFI EventsManager.
Import from legacy file storage	The Import from legacy file storage job enables you to import data archived by a previous version of GFI EventsManager. Archive files were exported in a special file format utilized by GFI EventsManager.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

3.6 Alerting

Alerting is an important aspect of events management, enabling 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 notifications to function, the following must be configured:

ALERTING METHOD	REQUIRED SETTINGS
Email	For email alerting to function, you should ensure that: <ul style="list-style-type: none"> » SMTP server details are configured » The SMTP server is always available » Internet access is always available.
Network messages	For alerts to be sent using network messages ensure that Messenger service in Windows is started. This service is not related to the Windows Messenger application.
SMS	For SMS alerting to function ensure that: <ul style="list-style-type: none"> » 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 information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

3.7 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.

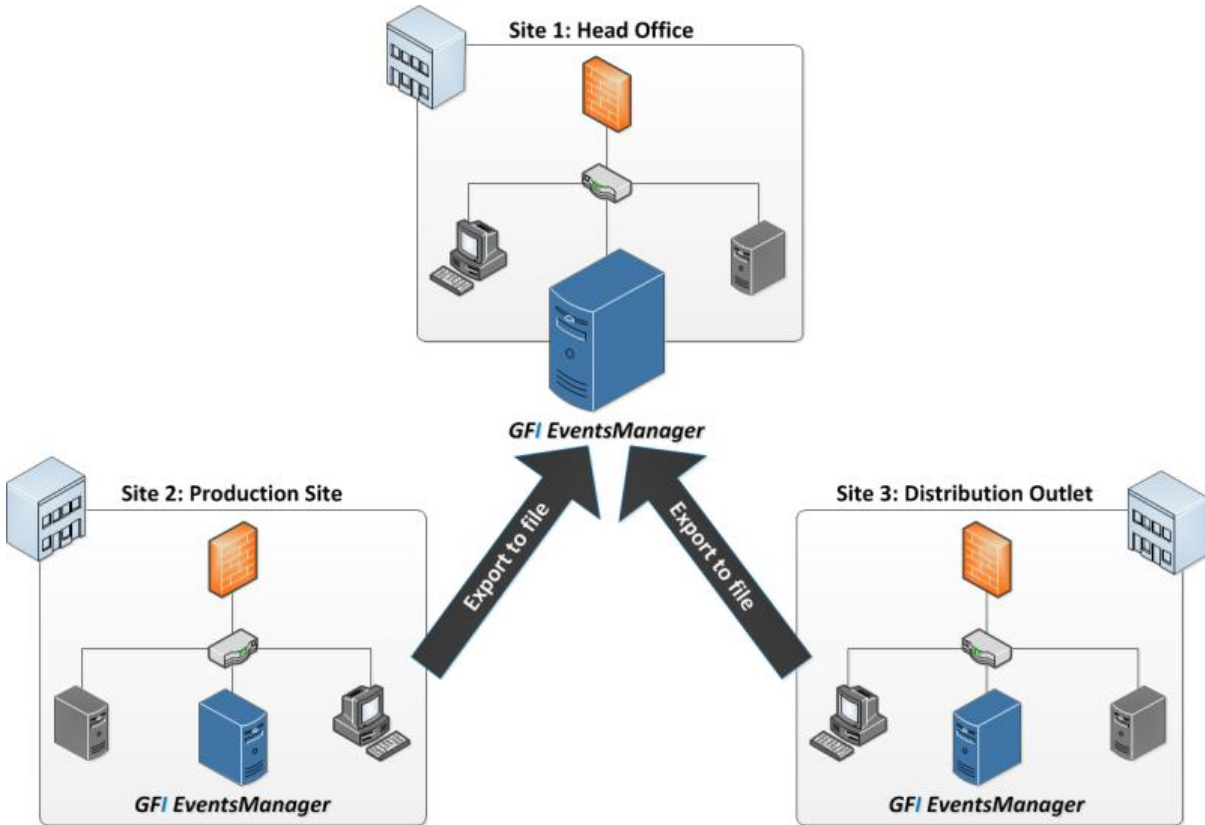


Figure 3 - Processing events from multiple domains and multiple site

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](#).

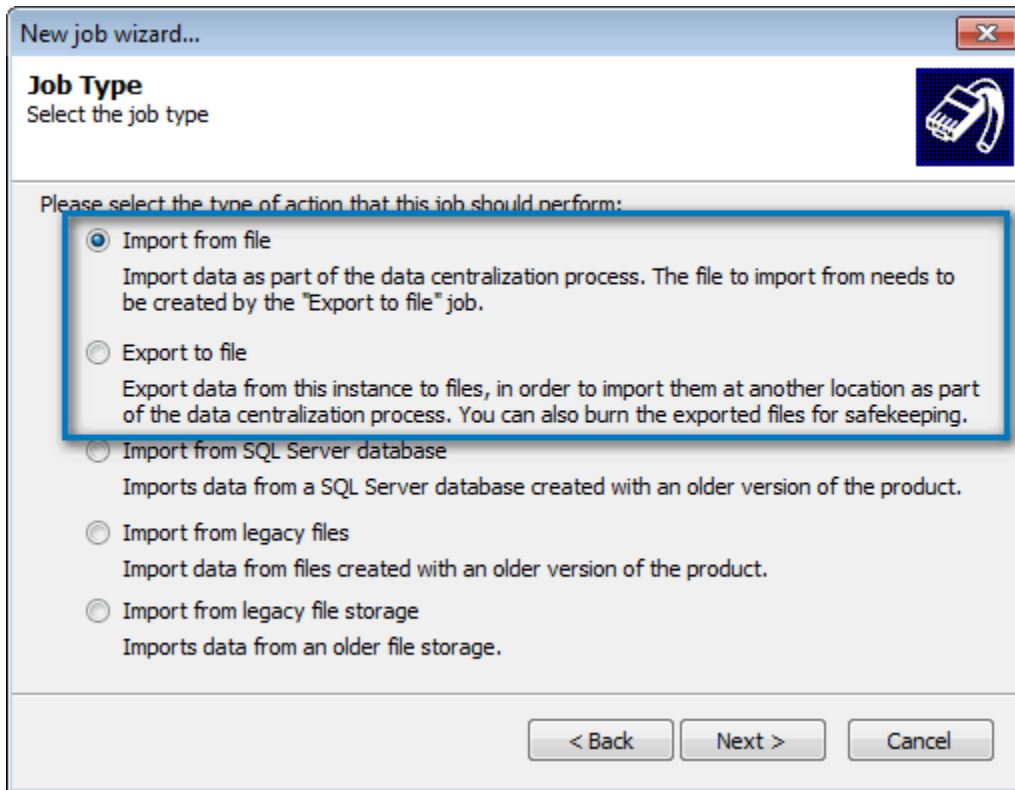


When installing GFI EventsManager, specify administrative credentials to collect events from all event sources across domains.

For multiple sites on a WAN, the recommended setup is to have at least one GFI EventsManager installation on each site. Using Database Operations, configure each GFI EventsManager installation to import and export events to a central location.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.



Screenshot 6 -Export to file and Import from file database operations

3.8 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 information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

3.9 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, through the information from the following sections:

- » [Benchmark test results](#)
- » [Bandwidth utilization](#)
- » [Steps required for determining the deployment solution](#)
- » [Recommendations](#)

4.2 Benchmark test results

The test results shown 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
- » Text 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, GFI EventsManager was installed on a separate machine.

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

Table 10 - Benchmark test one

BENCHMARK TEST 1	
Processor	2x Intel Xeon 3.0 GHz
RAM	4GB
Operating System	Windows 2003 Server Enterprise
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 11 - Benchmark test two

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

BENCHMARK TEST 2	
GFI EventsManager configuration settings	Process using default rules
Events per hour processed	Between 5.5 and 6 million

Table 12 - Benchmark test three

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

Table 13 - Benchmark test four

BENCHMARK TEST 4	
Processor	Intel Pentium 4 2.8 GHz
RAM	2GB
Operating System	Windows XP SP2
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 14 - 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 15 - 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 is 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

STEP	DESCRIPTION
Step 1	<p>The first steps to be taken are the following:</p> <ul style="list-style-type: none"> » Calculate the total number of events that will be collected every hour » Determine whether events are archived or processed.

STEP	DESCRIPTION
Step 2	<p>The benchmark results provided can then be used to establish:</p> <ul style="list-style-type: none"> » Number of GFI EventsManager instances required » Required hardware resources.

4.4.1 Further information to help in the evaluation

The below table contains information useful for evaluating GFI EventsManager:

- » 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 considering 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).

4.4.2 Issues to consider

The issues to consider when deploying GFI EventsManager are:

- » 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
- » Scanning large Text logs requires higher RAM specifications
- » Incoming Syslog messages at a rate of 2,000 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.



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 other applications.

Table 16 - 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 17 - RAM requirements for maximum performance

RAM	
Minimum	2GB
When collecting up to 3 million events per hour	3GB
When collecting more than 3 million events per hour	Increase RAM for better performance

Table 18 - 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.



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. For more information, refer to the following sections:

- » [Scenario 1: Small single domain network with default Audit Policy enabled](#)
- » [Scenario 2: Large single domain network.](#)

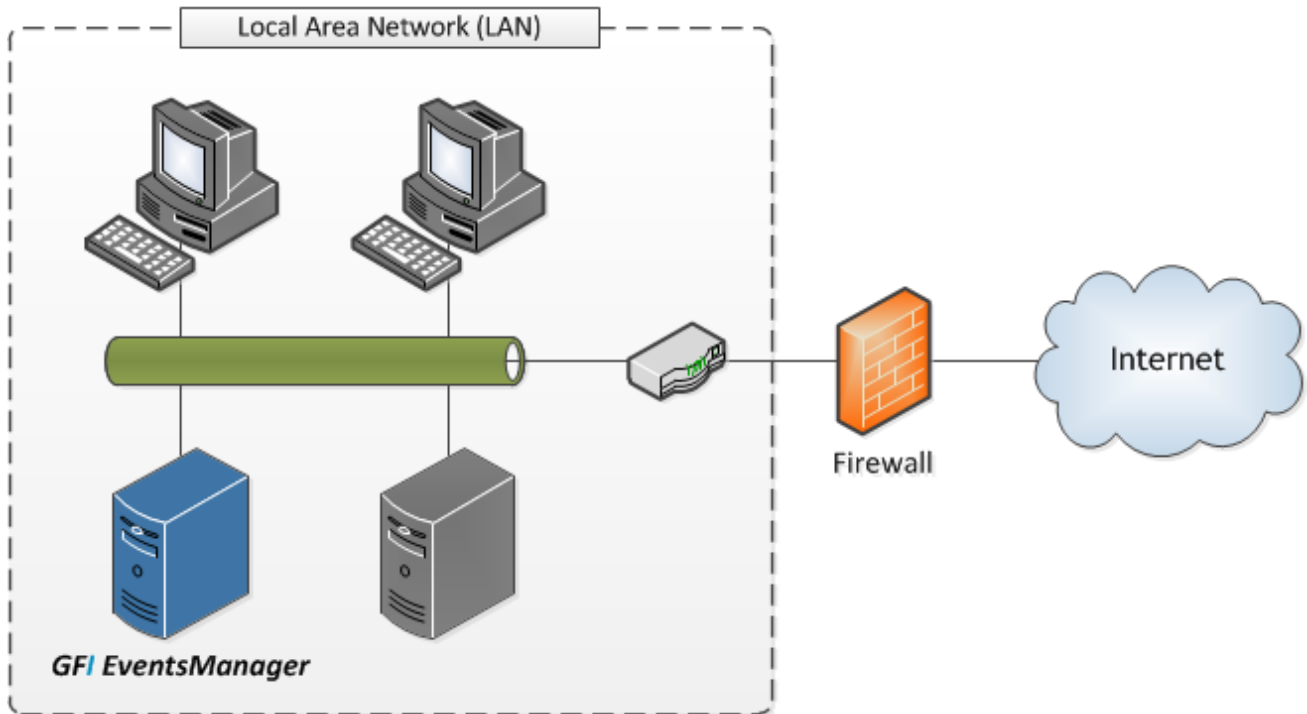


Figure 4 - GFI EventsManager on a single domain LAN

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

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

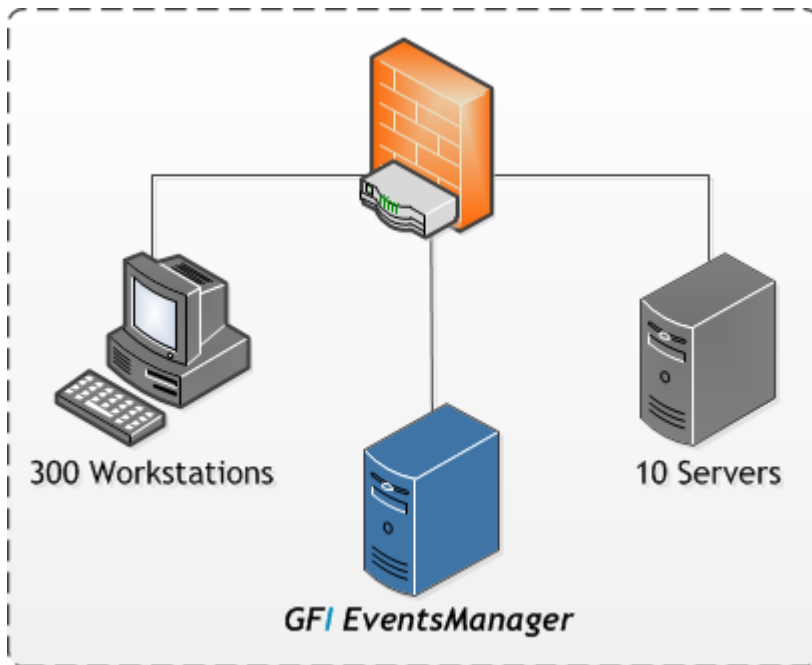


Figure 5 - Small single domain network

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

To manage these events use one of the following options:

- » Make use of default actions to export events from the main database into a secondary storage database to avoid performance issues on the primary 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

5.3 Scenario 2: Large single domain network

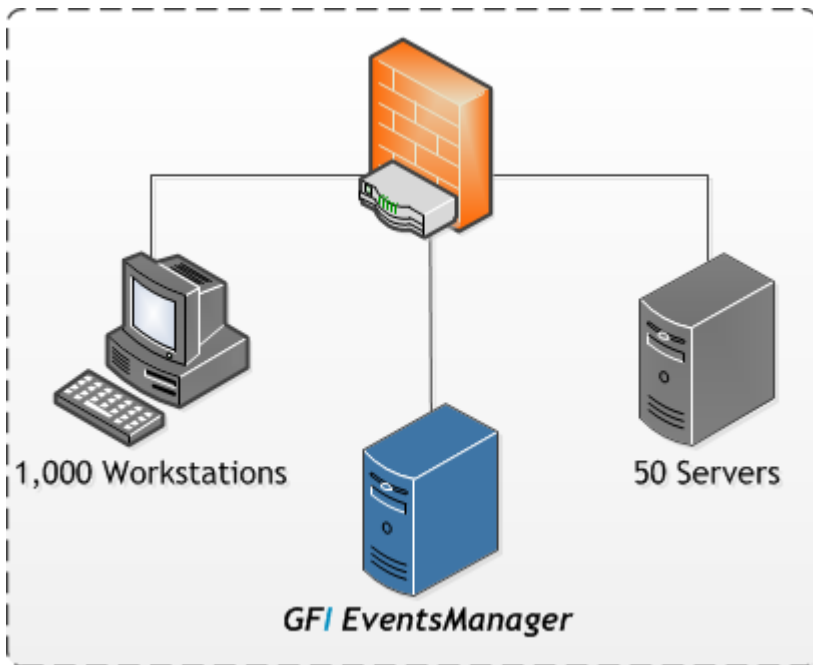


Figure 6 - Large single domain network

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

To manage these events use one of the following options:

- » Make use of default actions to export events from the main database into a secondary storage database to avoid performance issues on the primary 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

5.4 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. Ensure that the server has all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
2. Install GFI EventsManager.
3. Configure and add Event Sources. Event sources can be added:

Manually from **Configuration** tab ► **Event Sources** in GFI EventsManager console.

Using the Automatic network discovery wizard

Using the GFI EventsManager synchronization feature.

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

5. (Optional) Configure rule-sets from **Configuration** tab ► **Event Processing Rules**.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

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. For more information, refer to the following sections:

- » [Deployment scenario description](#)
- » [Deployment phases.](#)

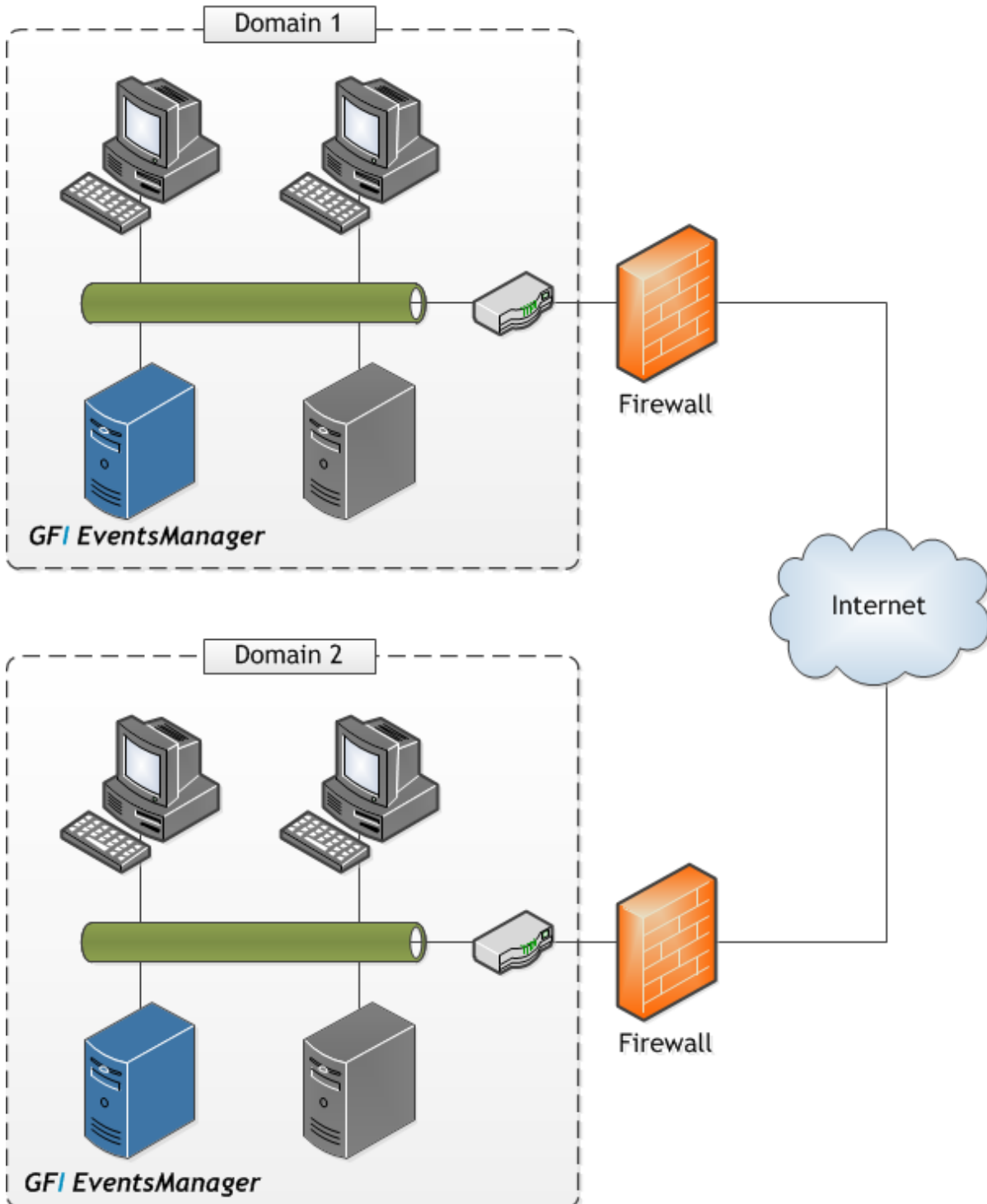


Figure 7 - GFI EventsManager on multiple domain over WAN

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

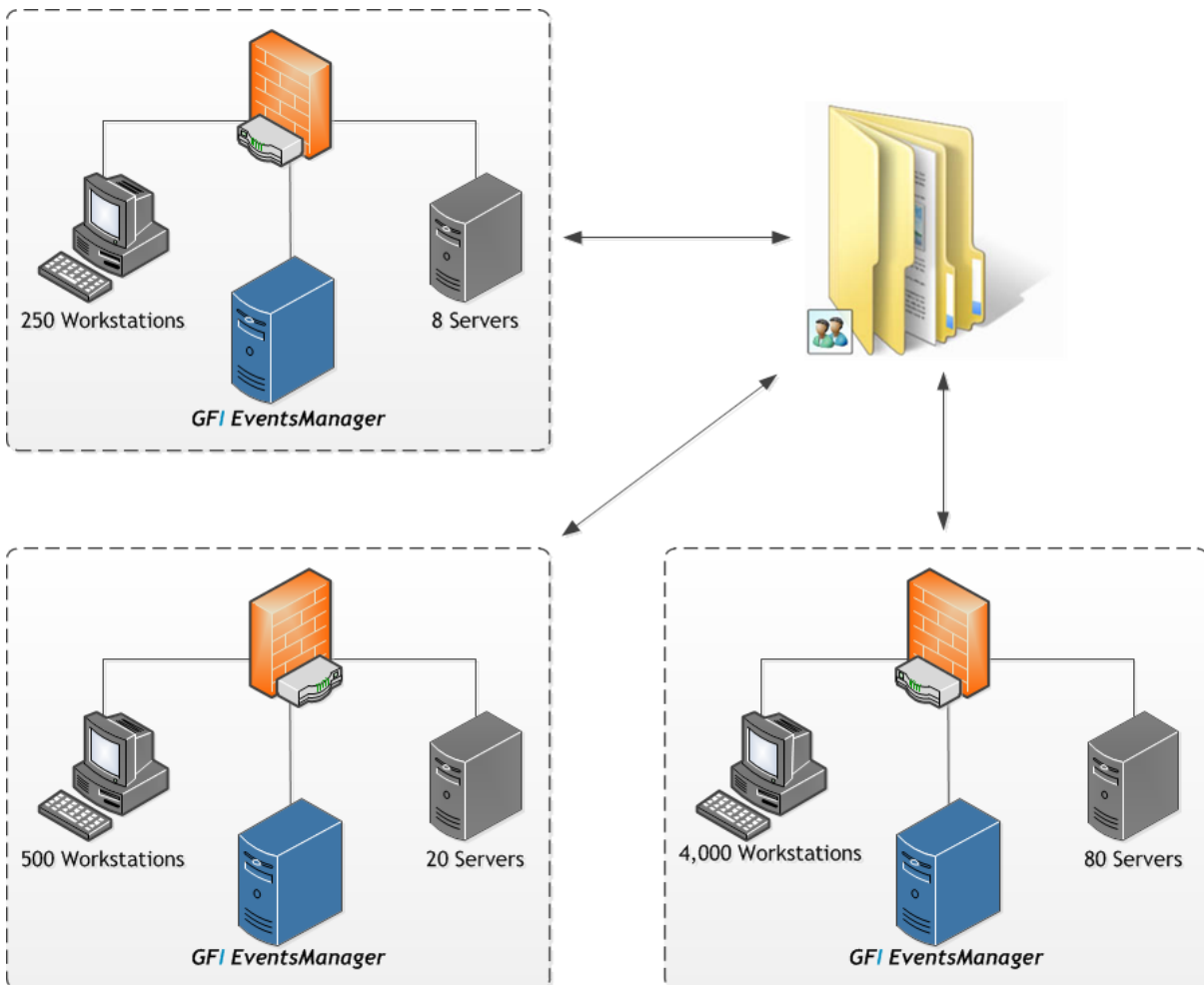


Figure 8 - Multiple sites with multiple domains

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

6.2.1 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 19 - 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

EVENT SOURCE	NUMBER OF DEVICES	EVENTS PER DEVICE PER HOUR	TOTAL EVENTS PER HOUR
The total number of events			705,500
Approximate database storage growth per month in GB			75
Total number of GFI EventsManager installations			1

Table 20 - 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 21 - 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 EVENTS MANAGER 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 EVENTS MANAGER INSTANCE 2			
Event Source	Number of devices	Events per device per hour	Total Events per hour
Workstations	2500	2,000	5,000,000

6.3 Deployment Phases

For information about how to deploy GFI EventsManager in the above scenario, refer to the following sections:

- » [Deployment Phases for Sites 1 and 2](#)
- » [Deployment Phases for Site 3.](#)

6.3.1 Deployment Phases for Sites 1 and 2

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

1. Ensure that the server has all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
2. Ensure that the GFI EventsManager machine has the right permissions to access and write events in the shared folder.
3. Install GFI EventsManager.
4. Configure and add Event Sources. Event sources can be added:

Manually from **Configuration** tab ► **Event Sources** in GFI EventsManager console.

Using the Automatic network discovery wizard

Using the synchronization feature in GFI EventsManager.

5. Create **Database Operations** to export and import events to and from the shared folder.
6. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
7. (Optional) Configure rule-sets from **Configuration** tab ► **Event Processing Rules**.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

6.3.2 Deployment Phases for Site 3

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

1. Ensure that the servers have all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
2. Ensure that the GFI EventsManager machines have the right permissions to access and write events in the shared folder.
3. Install GFI EventsManager on both machines.
4. Configure and add Event Sources. Event sources can be added:

Manually from **Configuration** tab ► **Event Sources** in GFI EventsManager console.

Using the Automatic network discovery wizard

Using the synchronization feature in GFI EventsManager.

5. Create **Database Operations** to export and import events to and from the shared folder.
6. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
7. (Optional) Configure rule-sets from **Configuration** tab ► **Event Processing Rules**.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

7 Deploying GFI EventsManager in a Mixed Environment

7.1 Introduction

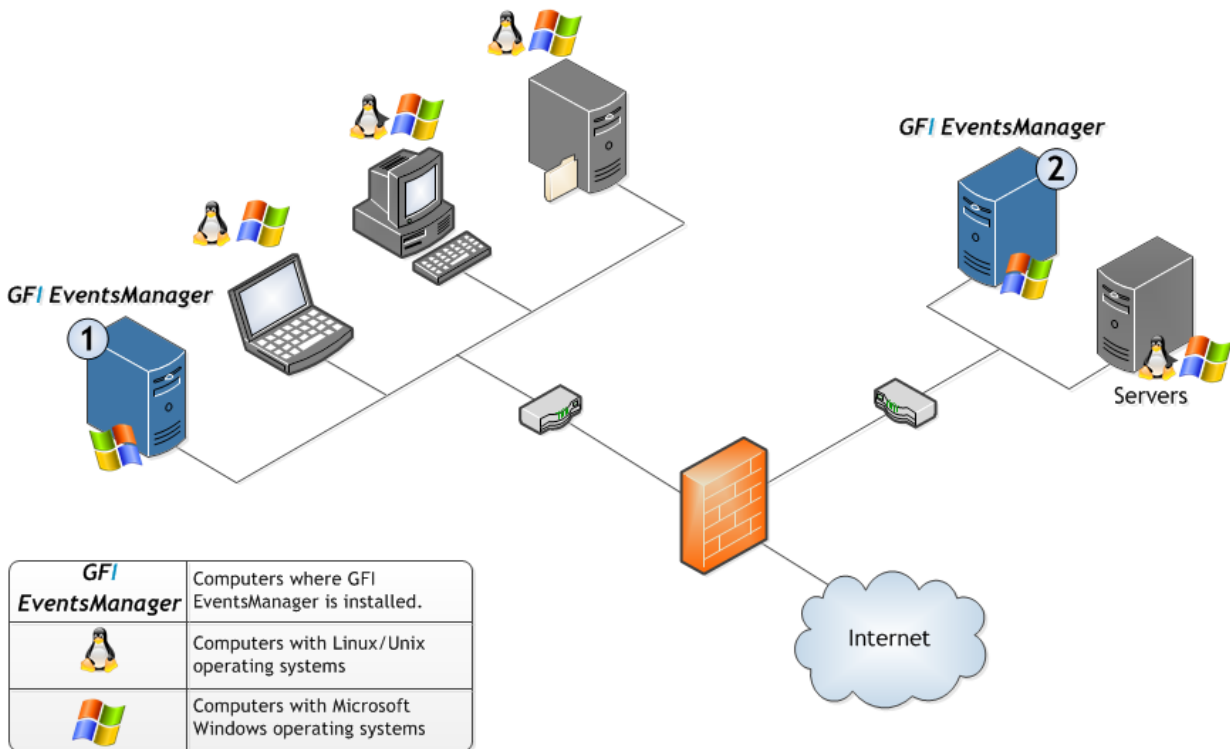


Figure 9 - GFI EventsManager in a mixed environment

This chapter describes a scenario for deploying GFI EventsManager on a LAN where computer systems and network devices generate Windows, Syslog and Text log events. For more information, refer to the following sections:

- » [Deployment scenario description](#)
- » [Deployment phases.](#)

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).

Text logs mainly used by web servers to log web related events including web logs. Text logs 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, Text Logs, SNMP Traps and Syslog messages through one solution.

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

7.2 Deployment Scenario Description

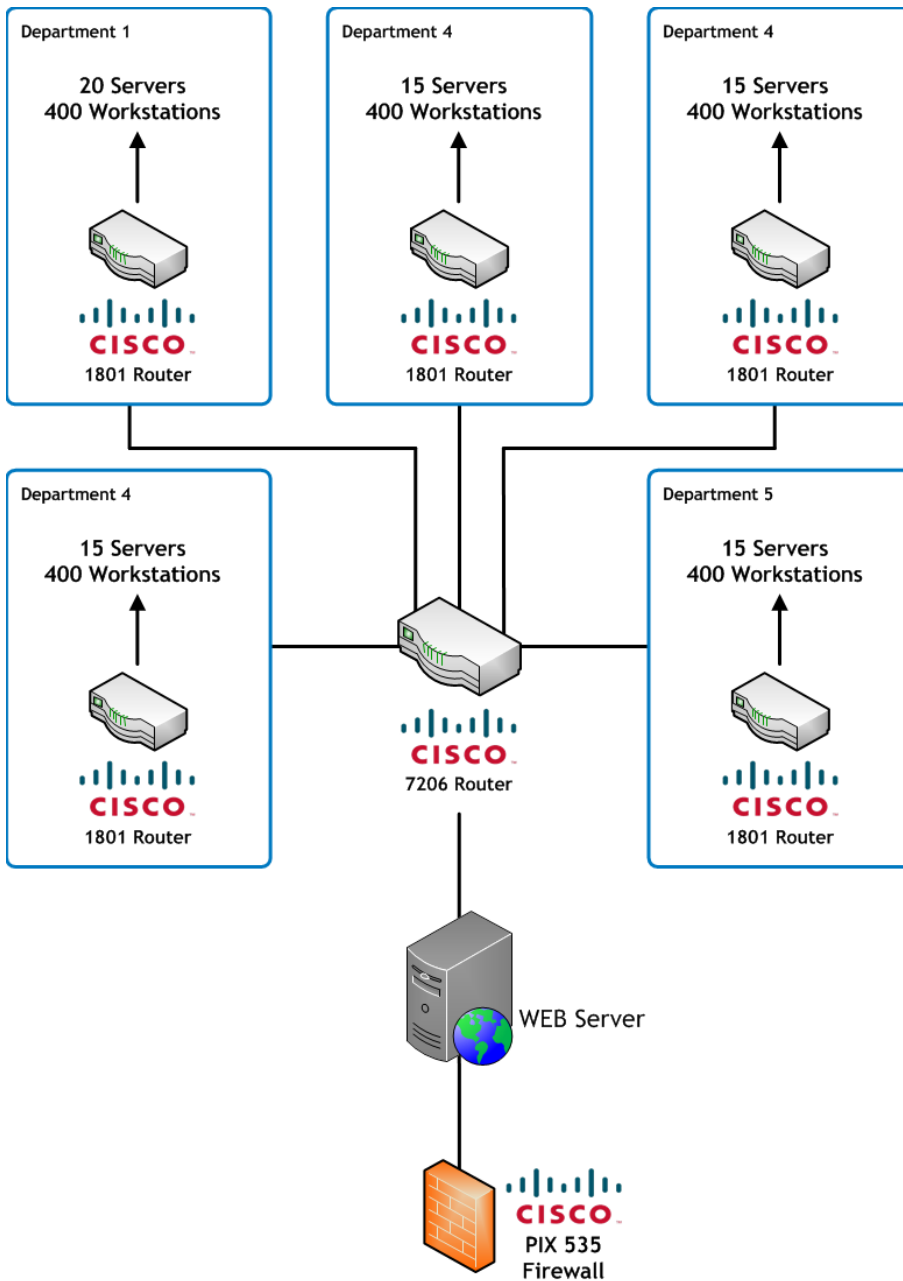


Figure 10 - Scenario for a mixed environment

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

DEPARTMENT	RESOURCES
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.

Equipment used in scenario:

EQUIPMENT	DESCRIPTION
Operating Systems	<ul style="list-style-type: none"> » Microsoft Windows servers are installed with Microsoft Windows 2003 Server Enterprise » Microsoft Windows Workstations are installed with Microsoft Windows XP SP2.

EQUIPMENT	DESCRIPTION
Cisco routers	<ul style="list-style-type: none"> » Event logging configured at severity level 5 » Routers have been configured to send Syslog messages to GFI EventsManager
Cisco firewalls	<ul style="list-style-type: none"> » Event logging configured at severity level 5 » Firewall has been configured to send syslog messages to GFI EventsManager
Web server	<ul style="list-style-type: none"> » 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.

7.2.1 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

7.2.2 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. Ensure that the servers have all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
2. Install GFI EventsManager on both machines.
3. Configure and add Event Sources. Event sources can be added:
 - » Manually from **Configuration** tab ► **Event Sources** in GFI EventsManager console.
 - » Using the Automatic network discovery wizard
 - » Using the synchronization feature in GFI EventsManager.
4. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
5. (Optional) Configure rule-sets from **Configuration** tab ► **Event Processing Rules**.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

8 Deploying GFI EventsManager on Demilitarized Zone

8.1 Introduction

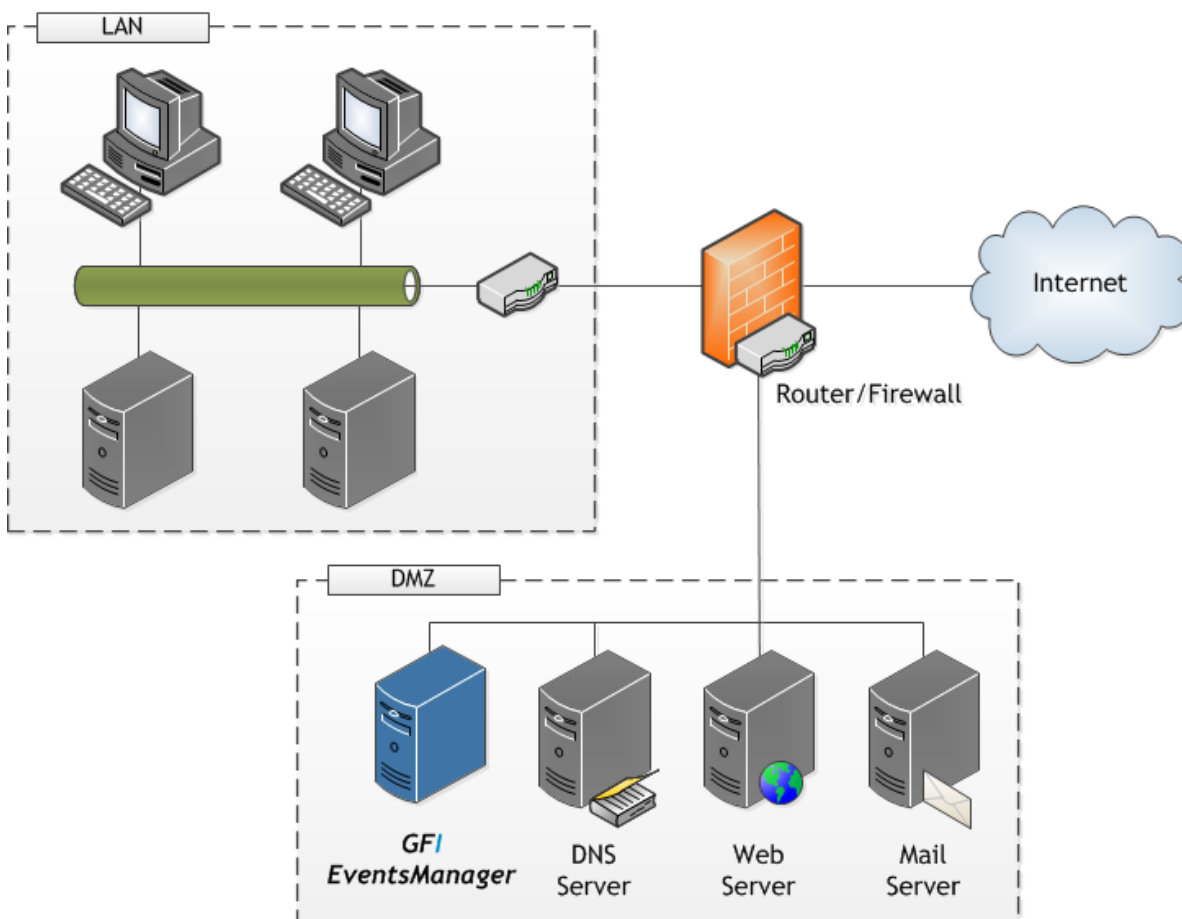


Figure 11 - The DMZ sits between the internal LAN and the Internet

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, Text logs and Syslog messages.

For more information, refer to the following sections:

- › [Automate management of Web and Mail server events](#)
- › [Automate management of DNS server events](#)
- › [Automate management of network appliance events](#)
- › [Where to deploy GFI EventsManager](#)
- › [Deployment scenario description](#)
- › [Deployment phases](#)

8.2 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).

8.3 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.

8.4 Automate management of network appliance events

Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (example: 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.

8.5 Where to deploy GFI EventsManager

This section describes four possible scenarios that can be used to monitor and process events from a DMZ using GFI EventsManager. For more information, refer to the following sections:

- » [Scenario 1](#)
- » [Scenario 2](#)
- » [Scenario 3](#)

8.5.1 Scenario 1

Processing events generated on the DMZ from the LAN is possible. This scenario requires GFI EventsManager to be installed and configured on the LAN.

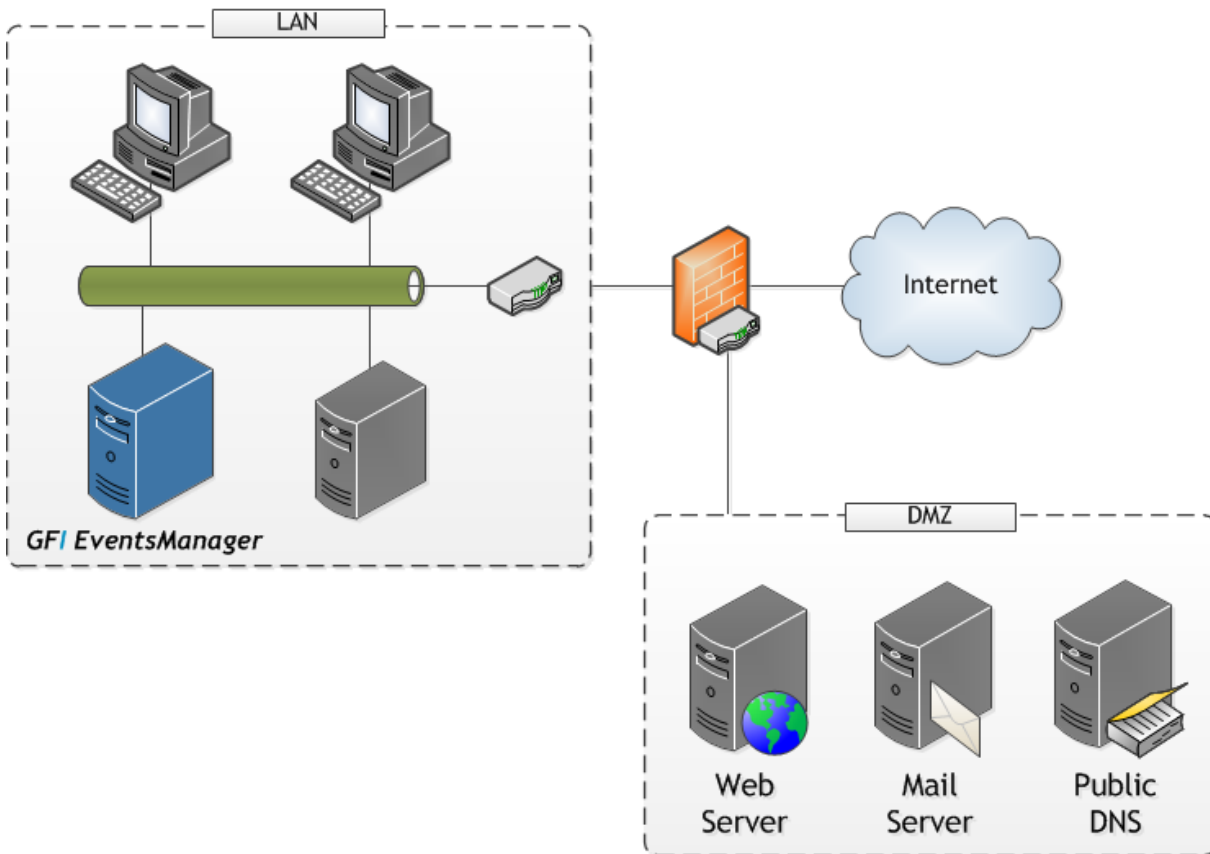


Figure 12 - Scenario1- Deploying GFI EventsManager on the LAN

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, refer to [Ports and permissions](#).

8.5.2 Scenario 2

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

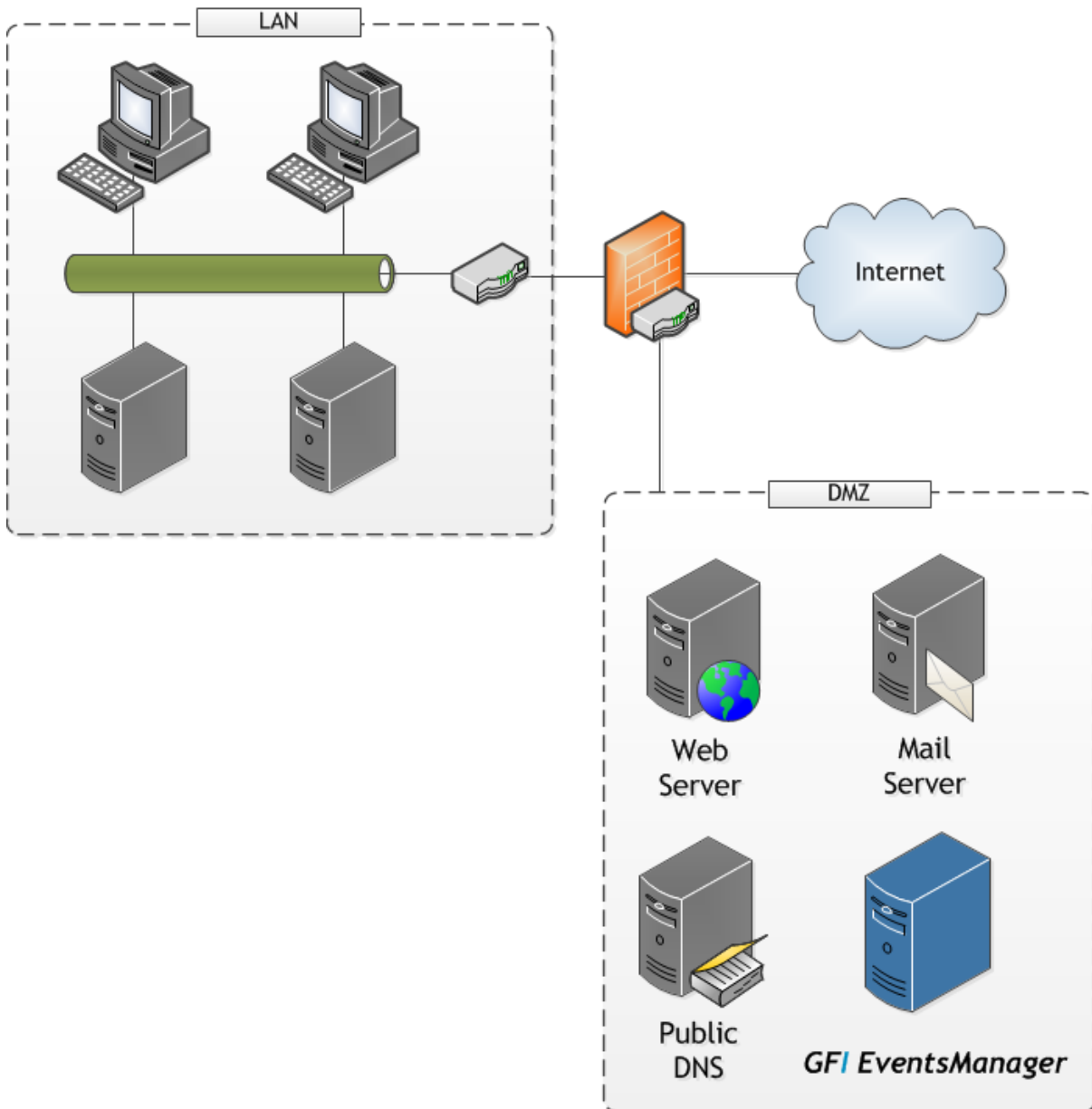


Figure 13 - Scenario 2 and 3- Deploying GFI EventsManager on the DMZ



In Scenario 2, data stored in the DMZ may be at a high risk of compromise.

8.5.3 Scenario 3

GFI EventsManager can be deployed within the DMZ and configured to collect and process all events generated on the corporate LAN and DMZ.

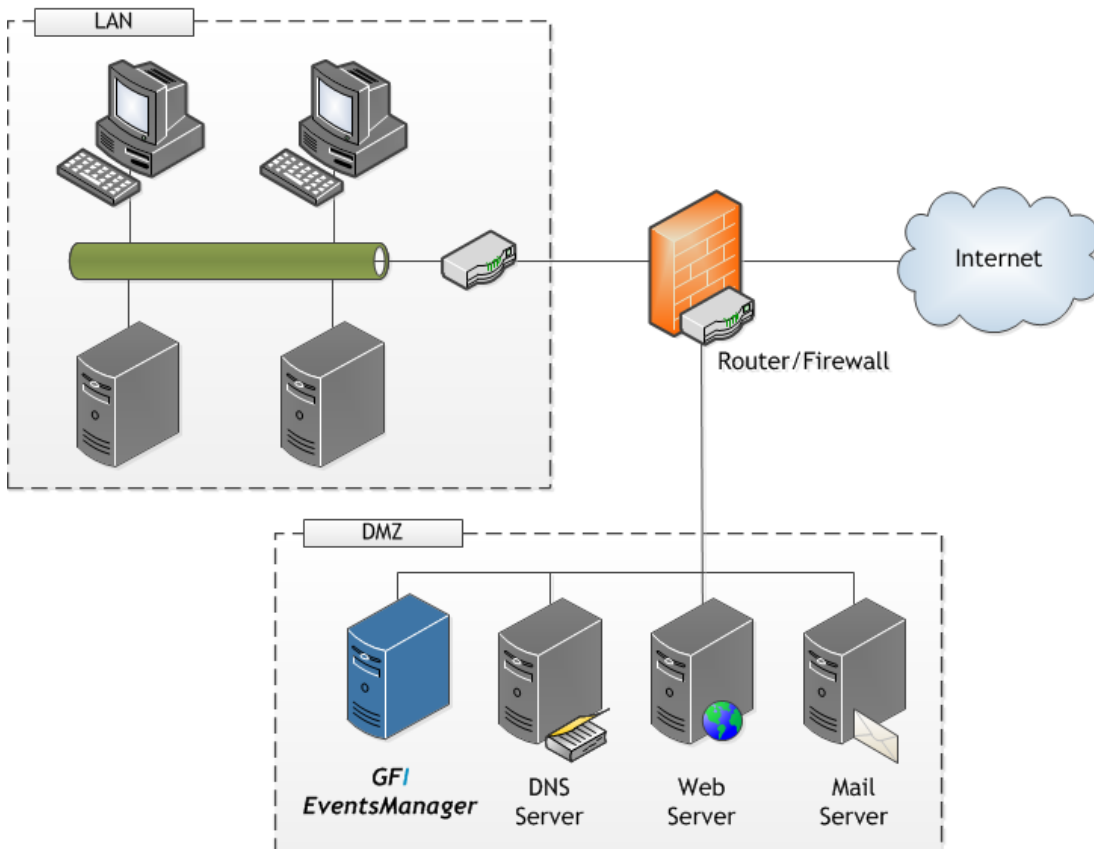


Figure 14 - Scenario 4 - Deploying GFI EventsManager on the DMZ and collect all events

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

8.6 Deployment scenario description

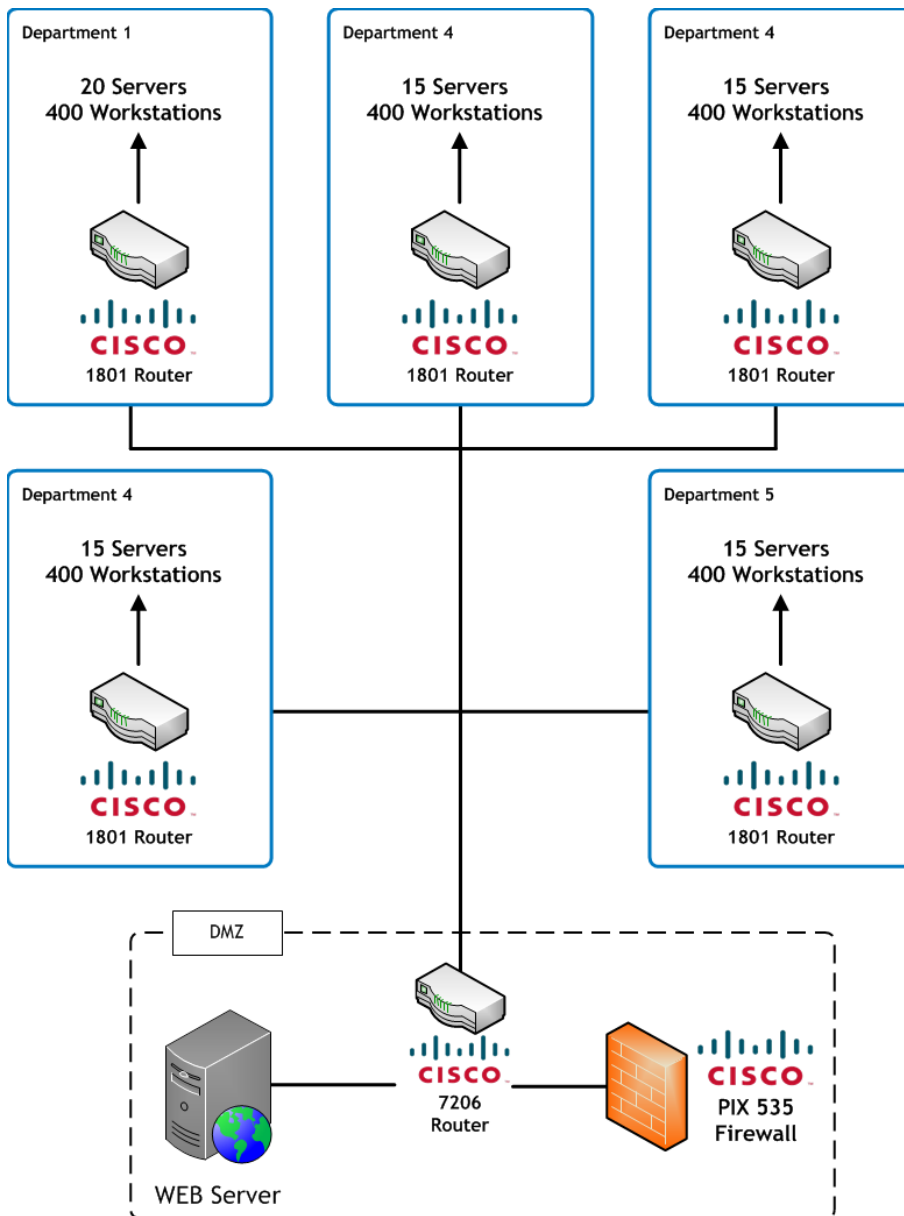


Figure 15 - Monitoring events on a DMZ

8.6.1 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

Hardware used in scenario

HARDWARE	DESCRIPTION
Cisco routers	<ul style="list-style-type: none"> » Event logging notification severity is set to 5 » Routers configured to send syslog messages to GFI EventsManager
Cisco firewall	<ul style="list-style-type: none"> » Event logging notification severity is set to 5 » Firewall has been configured to send syslog messages to GFI EventsManager
Web server	<ul style="list-style-type: none"> » 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 in the following order:

- » 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.

8.7 Deployment Phases

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

1. Ensure that the servers have all the system requirements and that all firewall permissions are configured before installing GFI EventsManager.
2. Install GFI EventsManager on both machines.
3. Configure and add Event Sources. Event sources can be added:
 - » Manually from **Configuration** tab ► **Event Sources** in GFI EventsManager console.
 - » Using the Automatic network discovery wizard
 - » Using the synchronization feature in GFI EventsManager.
4. (Optional) Configure the **Administrator Account** and the **Alerting Options** if necessary.
5. (Optional) Configure rule-sets from **Configuration** tab ► **Event Processing Rules**.

9 GFI EventsManager Reporting

9.1 Introduction

GFI EventsManager includes a fully-fledged reporting system that enables you to generate graphical IT-level, technical and management reports, based on collected and processed events.

GFI EventsManager 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.

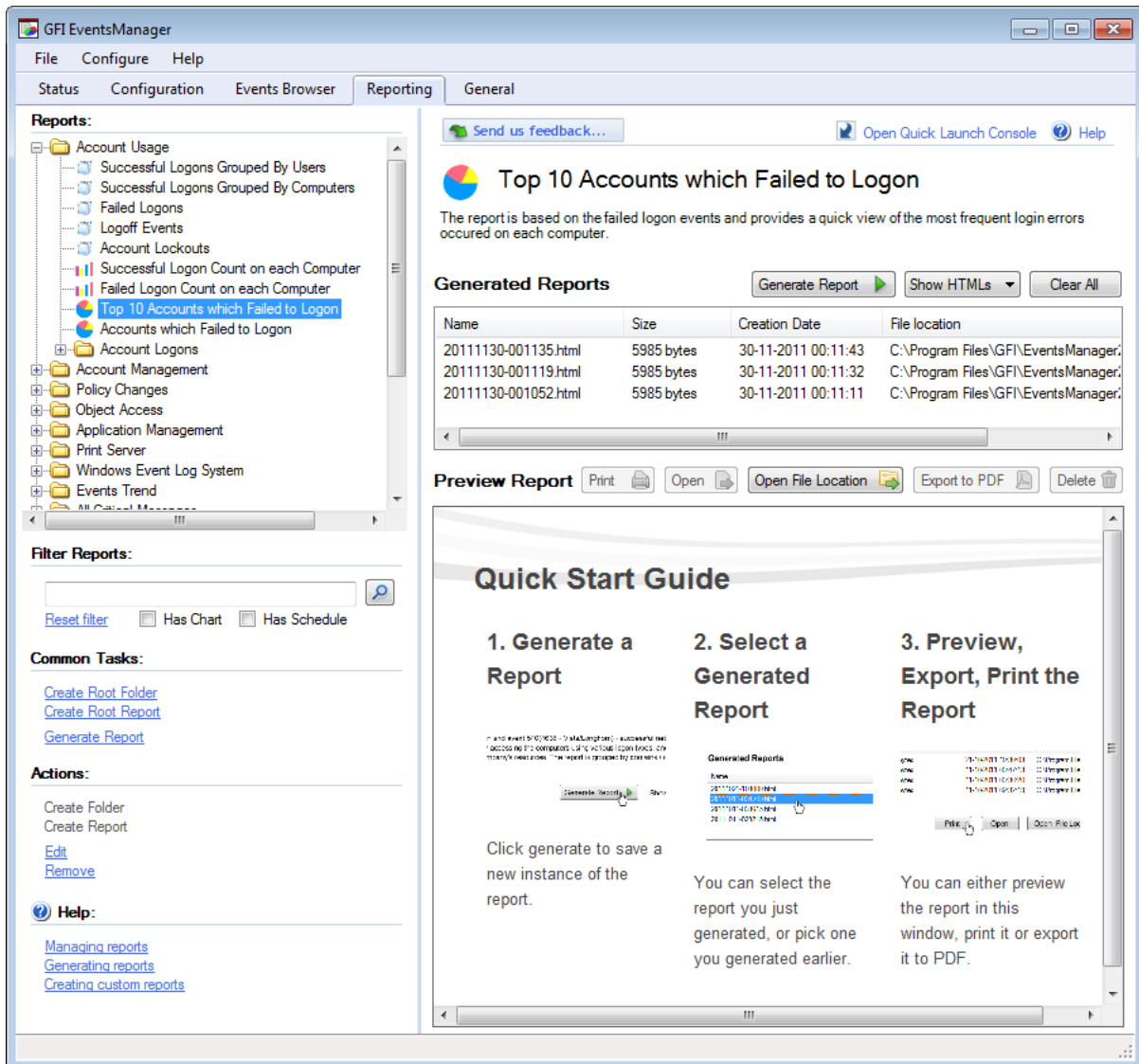


Figure 16 - Reporting tab

9.2 Available reports

GFI EventsManager's extensive report list contains reports for various requirements designed to facilitate reporting as much as possible. The following report categories are included in GFI EventsManager by default. Each category contains a number of reports that can be used out of the box or customized to fit your requirements:

Table 22 - Available reports

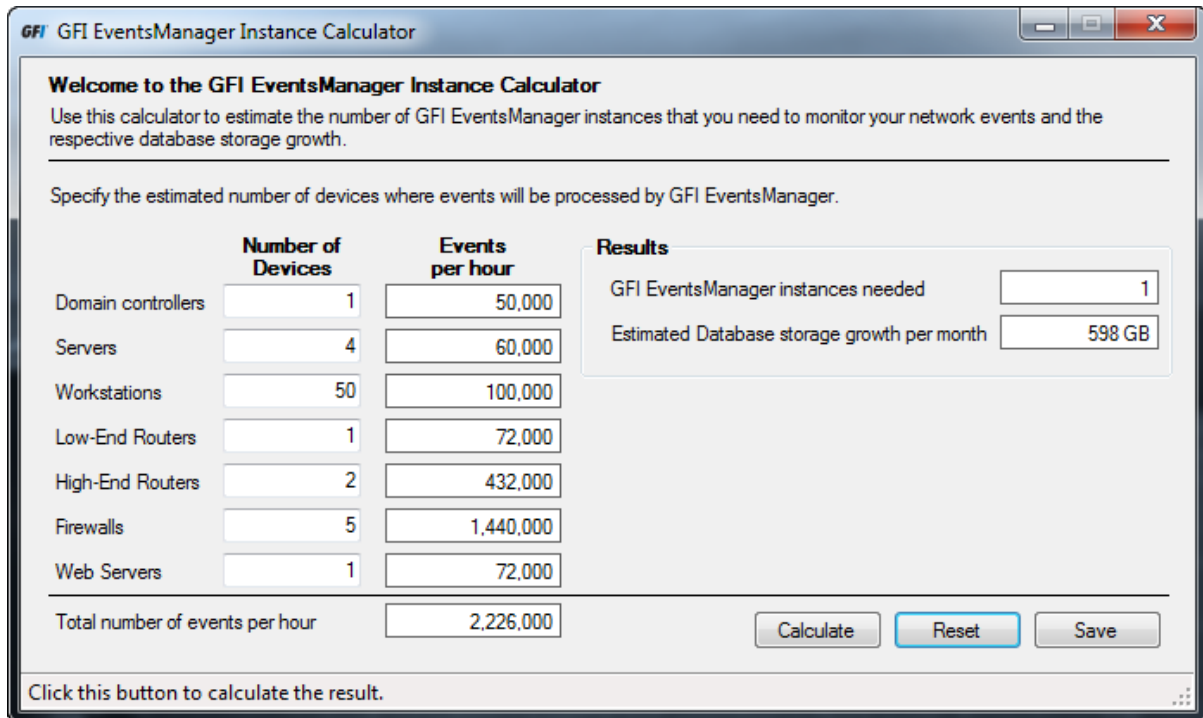
REPORT CATEGORY	DESCRIPTION
Account Usage	Use the reports in this category to identify user logon issues. The event details shown in these reports include successful/failed user logons and locked user accounts.
Account Management	Use the reports in this category to generate a graphical overview of important events that took place across your entire network. The event details shown in these reports include changes in user and computer accounts as well as changes in security group policies.
Policy Changes	Use the reports in this category to identify policy changes effected on your network.
Object Access	Use the reports in this category to identify object access issues. The event details shown in these reports include successful/failed object access and objects that have been deleted.
Application Management	Use the reports in this category to identify faulty applications and application installation and removal issues. The event details shown in these reports include applications that have been installed or removed as well as applications, which are crashing and hanging.
Print Server	Use the reports in this category to display details related to printing events. Details provided in these reports include documents that have been printed, the users that triggered the printing event and the date/time when the printing operation took place.
Windows Event Log System	Use the reports in this category to identify audit failures and important Windows event log issues. Details provided in these reports include the starting and stopping of event log services, clear log operations as well as errors generated during event logging.
Events Trend	Use the reports in this category to display statistical information related to event generation. Charts provided enumerate the 10 computers and users with most events. Other reports provide event counts on a network-wide basis as well as on a computer-by-computer basis. Reports in this category can be generated for each main time - by hour, day, week or month.
All Critical	Use the reports in this category to display information related to critical Windows events, Syslog, W3C, Custom Events, SNMP Traps and SQL Server Audit events. The charts provided enumerate the 10 most critical events.
Miscellaneous, Customizable	Use the reports in this category to generate reports that offer broad customization. These can be used to generate reports based on any Windows event log, using filtering conditions and grouping modes that are not covered by the other default reports.
PCI DSS Compliance / GCSx Code of Connection Requirements / SOX Compliance / HIPAA Compliance / GLBA Compliance	Use the reports in these categories to generate legal compliance regulations reports.
General and Security Requirements	Use the reports in this category to generate various reports required by several GCSx Code of Connection memos.
LOGbinder SP reports	Use the reports in this category to generate reports related to Microsoft SharePoint audit events.



For information, refer to the user manual, available on the GFI website at <http://www.gfi.com/products/gfi-eventsmanager/manual>.

10 Appendix 1: Instance Calculator

The instance calculator 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	50,000
Servers	4	60,000
Workstations	50	100,000
Low-End Routers	1	72,000
High-End Routers	2	432,000
Firewalls	5	1,440,000
Web Servers	1	72,000
Total number of events per hour		2,226,000

Results
GFI EventsManager instances needed: 1
Estimated Database storage growth per month: 598 GB

Calculate Reset Save

Click this button to calculate the result.

Screenshot 7 - GFI EventsManager Instance calculator

Download the GFI EventsManager Instance Calculator from:

http://www.gfi.com/app/eventsmanager/GFI_EventsManager_Calculator.rar

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: Checklist

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	<input type="checkbox"/>
System Health Monitoring	<input type="checkbox"/>	Forensic Analysis	<input type="checkbox"/>
Notes:			
Identify logs to collect events from:			
Windows	<input type="checkbox"/>	Syslog	<input type="checkbox"/>
		W3C	<input type="checkbox"/>
Notes:			
Identify configuration settings required of the logs at "source"			<input type="checkbox"/>
Notes:			
Identify events to be configured as noise			<input type="checkbox"/>
Notes:			
Determine whether events will be archived or processed using default rule sets			<input type="checkbox"/>
Notes:			
Determine whether additional rule set configuration is required			<input type="checkbox"/>
Notes:			
Determine number of GFI EventsManager instances required			
Determine number of geographically remote sites			<input type="checkbox"/>
Notes:			
Determine which devices to monitor			<input type="checkbox"/>
Notes:			
Calculate instances required			<input type="checkbox"/>
Notes:			
Determine quantity and type of licenses required			<input type="checkbox"/>
Notes:			

Determine deployment machine(s) to use	
Verify if machine(s) meet recommended specifications	<input type="checkbox"/>
Notes:	
Verify load on the machines	<input type="checkbox"/>
Notes:	
Verify system settings for event sources	
Windows Event Logs:	
Remote registry service is enabled and running	<input type="checkbox"/>
Windows audit service is enabled and running	<input type="checkbox"/>
Notes:	
W3C (CLF) Logs:	
W3C log source folders are accessible via Windows Administrative Shares	<input type="checkbox"/>
Notes:	
Syslog:	
Sources are configured to send their Syslog messages through UDP port	<input type="checkbox"/>
Firewall(s) are configured to allow Syslog messages through UDP ports	<input type="checkbox"/>
Notes:	
Determine administrative credentials required for Windows and W3C event sources	<input type="checkbox"/>
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	<input type="checkbox"/>
Notes:	
Determine firewall and anti-virus configuration requirements	
Verify that traffic is not blocked on the ports in use by GFI EventsManager	<input type="checkbox"/>
Notes:	
Verify esmui.exe and esmproc.exe are allow access through firewall(s)	<input type="checkbox"/>
Notes:	
Verify that GFI EventsManager folders are excluded from real-time scanning	<input type="checkbox"/>
Notes:	
Verify that alerting traffic is not blocked by firewall(s)	<input type="checkbox"/>
Notes:	

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

Index

A

Account Usage Reports 42
alerting 15, 26, 30, 40
anti-virus 10

B

bandwidth 7, 17, 20, 22
benchmark 1, 19, 20, 21, 29

C

Cisco router 31, 40
Configuration settings 19, 20

D

database backend 3, 14, 19, 21
Database Backend 3, 5, 9, 14, 19, 21
database maintenance 14
Database Operations 17, 27, 30

E

Email 3, 15
Event color-coding 3
Event finder tool 3
Event processing rules 3, 5
Event query 3
Event query builder 3
event source 16, 25, 28, 29, 30, 33, 40

F

firewall 10, 25, 30, 32, 33, 39, 40

I

IIS 31

K

Knowledge Base 2

L

LAN 2, 22, 23, 31, 34, 35, 36, 39

N

Network alerts 5

P

port 35

R

remote site 1, 28
ReportPack 3, 41

S

SMS 15
SNMP traps 3, 5, 9
specifications 19
SQL Server 3
Storage 24, 29, 40
Storage Folder 5
syslog 2, 19, 31, 33, 35, 40
Syslog 2, 19, 31, 33, 35, 40
SYSLOG 2, 19, 31, 33, 35, 40
Syslog message 21, 33, 34, 40
Syslog messages 5, 9, 21, 33, 34, 40

W

W3C 2, 19, 31, 34, 35
W3C log 19, 31
W3C logs 19, 31
WAN 16, 22, 27
web server 31, 32, 33, 40
Windows 7 8, 9, 10
Windows Event Logs 5
Windows Vista 8, 9, 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.