Installation Guide

GFI EventsManager™

Find out how to deploy GFI EventsManager in different environments.

GFI®

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or 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 warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

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

Document Version: 13.1.0

Last updated (month/day/year): 03/21/2017

Contents

1 Introduction

The enormous volume of system event logs generated daily is of growing importance to organizations that must record information for forensic and compliance purposes. It is essential to perform real-time network-wide event log monitoring, analysis and reporting to address any incidents or security concerns and combat threats to business continuity.

GFI EventsManager assists with this monumental task by automatically and centrally monitoring and managing event logs - supporting a wide range of event types generated both by applications and devices from top vendors as well as for custom ones.

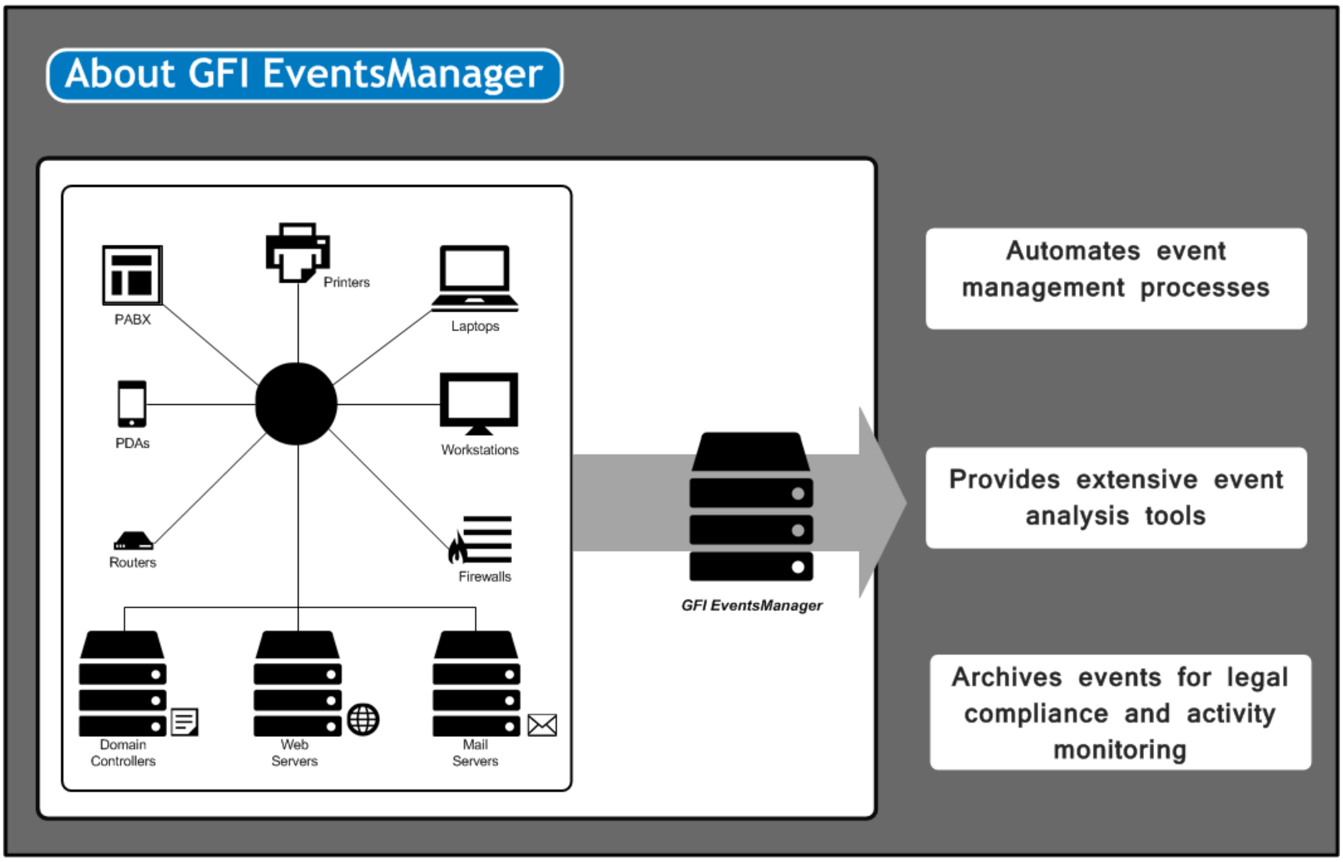
These sections provide you with information about how events management is achieved, using GFI EventsManager.

Topics in this section:

1.1 About GFI EventsManager

The enormous volume of system event logs generated daily is of growing importance to organizations that must record information for forensic and compliance purposes. It is essential to perform real-time network-wide event log monitoring, analysis and reporting to address any incidents or security concerns and combat threats to business continuity.

GFI EventsManager assists with this monumental task by automatically and centrally monitoring and managing event logs - supporting a wide range of event types generated both by applications and devices from top vendors as well as for custom ones.


About GFI EventsManager
PABX
Printers
Laptops
PDAs
Workstations
Routers
Firewalls
Domain Controllers
Web Servers
Mail Servers
GFI EventsManager
Automates event management processes
Provides extensive event analysis tools
Archives events for legal compliance and activity monitoring

Screenshot 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 are able to:

- Automatically monitor computers and network devices through GFI EventsManager's wide range of event log support; such as Text Logs, Windows® Event Logs, Syslogs, SNMP Traps Messages, Active Monitoring Events and even custom event logs
- Monitor computers and services running on your network through active monitoring features such as continuous checking of HTTP/HTTPS/FTP site availability, server roles queries, firewall queries and more
- Optimize security and performance while tracking operational issues by auditing your critical systems/devices; such as routers, firewall, sensors, servers and database engines
- Create and maintain an automated network security system which detects intrusion attacks
- Achieve compliance with various regulations and acts including SOX, PCI DSS, Code of Connection, HIPAA, data protection laws and others
- Proactively detect events which will lead to disaster such as hardware failure. When such events are processed, GFI EventsManager provides an early warning to give you control and take corrective action
- Minimize the risk and business loss due to systems downtime and misconfiguration
- Easily browse events from any number of databases through the extensive Events Browser; which helps you carry out forensic investigations with minimal human input
- Automatically processes and archives event logs, collecting and highlighting the information you need to know about the most important events occurring in your network so you are never caught off guard

- Generate technical IT level and management level reports from the extensive list of reports and also create new ones from existing reports or collected events

- Protect your business by tracking the security events in your network. Find who is responsible for security breaches and network threats

> For a full list of features, refer to: http://www.gfi.com/eventsmanager#features

1.2 How GFI EventsManager works

The operational functionality of GFI EventsManager is divided in the following stages:

- Stage 1: Event Collection

- Stage 2: Event Processing

1.2.1 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**.

Engine	Description
The Event Retrieval Engine	Used to collect Windows® Event Logs and Text Logs from networked event sources. During the Event Collection process this engine will: 1. Log-on to the event source(s) 2. Collect events from the source(s) 3. Send collected events to GFI EventsManager Server 4. Log-off from the 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 SQL Server® Listener	The listener receives trace messages from the scanned Microsoft® SQL Server® in real time. On receipt, GFI EventsManager processes the message immediately.
The Oracle Retrieval Engine	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.
Log Receiving Engine	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. 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.

1.2.2 Stage 2: Event Processing

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

- Analyze 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.

GFI EventsManager can be configured to archive events without running events processing rules. In such cases, even though no rules will be applied against collected logs, archiving will still be handled by the Event Processing stage. For more information, refer to **Events Processing Rules** from the **Administrator Guide**.

> **Important**
> Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to the following article: http://go.gfi.com/?pageid=esm_process_rights

1.3 Conventions used in this guide

The table below describes the common terms and conventions used in this Guide:

Term	Description
Note	Additional information and references essential for the operation of GFI EventsManager.
Important	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and filenames.
`Code`	Indicates text values to key in, such as commands and addresses.

2 Installing GFI EventsManager

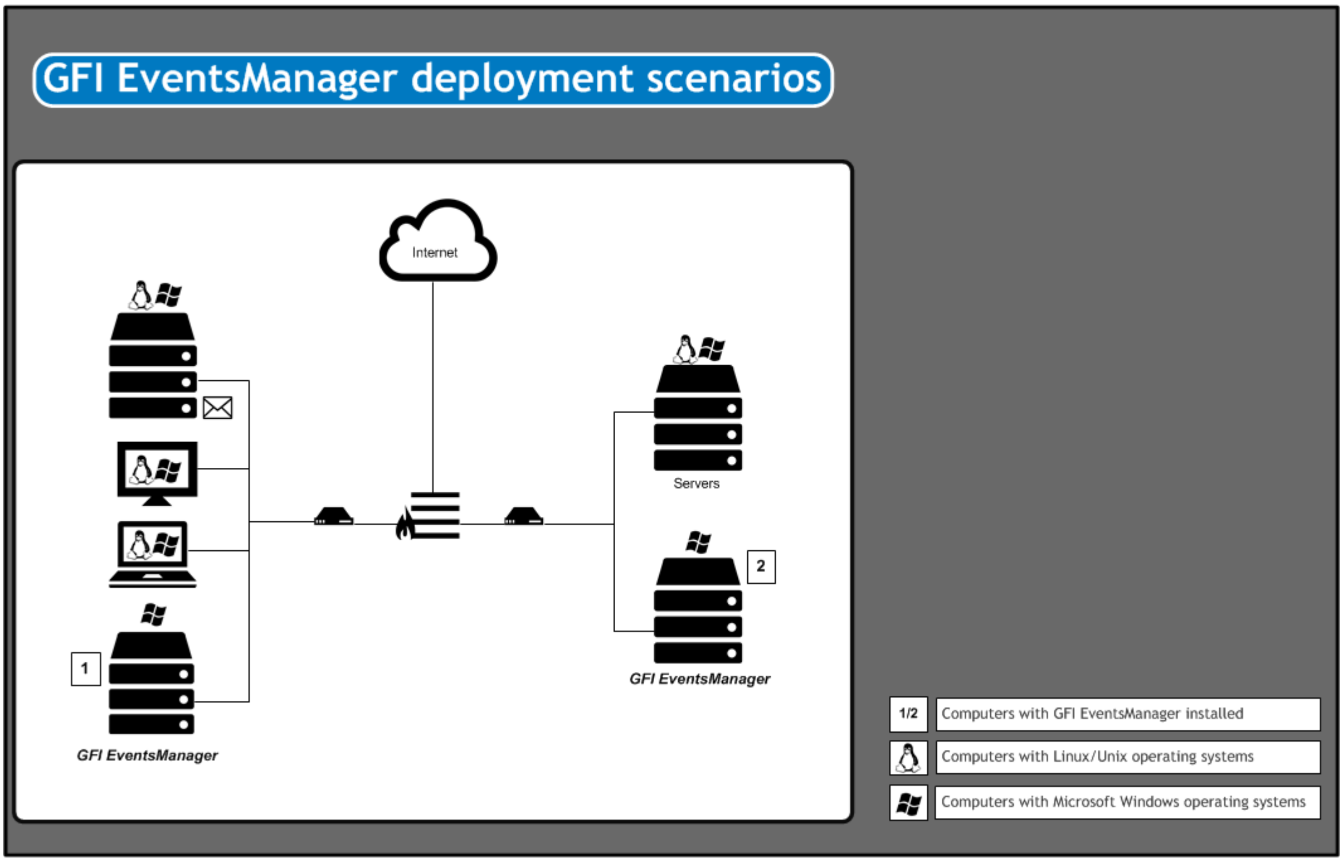
This section describes the possible deployment scenarios supported by GFI EventsManager. It is essential to review system requirements and computer settings prior to installing the product to ensure full communication between GFI EventsManager and the network devices/computers that must be monitored.

2.1 Deployment scenarios

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network. If you want to collect event logs from Microsoft® Windows® Vista or later operating systems, GFI EventsManager must be installed on a machine running Microsoft® Windows® Vista, 7, Server 2008 or Server 2012.

Use GFI EventsManager to manage event logs generated by:

- The same computer where it is installed
- All the servers, workstations and network devices that are reachable from the computer on which it is installed on.


GFI EventsManager deployment scenarios
Internet
Servers
2
GFI EventsManager
1
GFI EventsManager
1/2
Computers with GFI EventsManager installed
Computers with Linux/Unix operating systems
Computers with Microsoft Windows operating systems

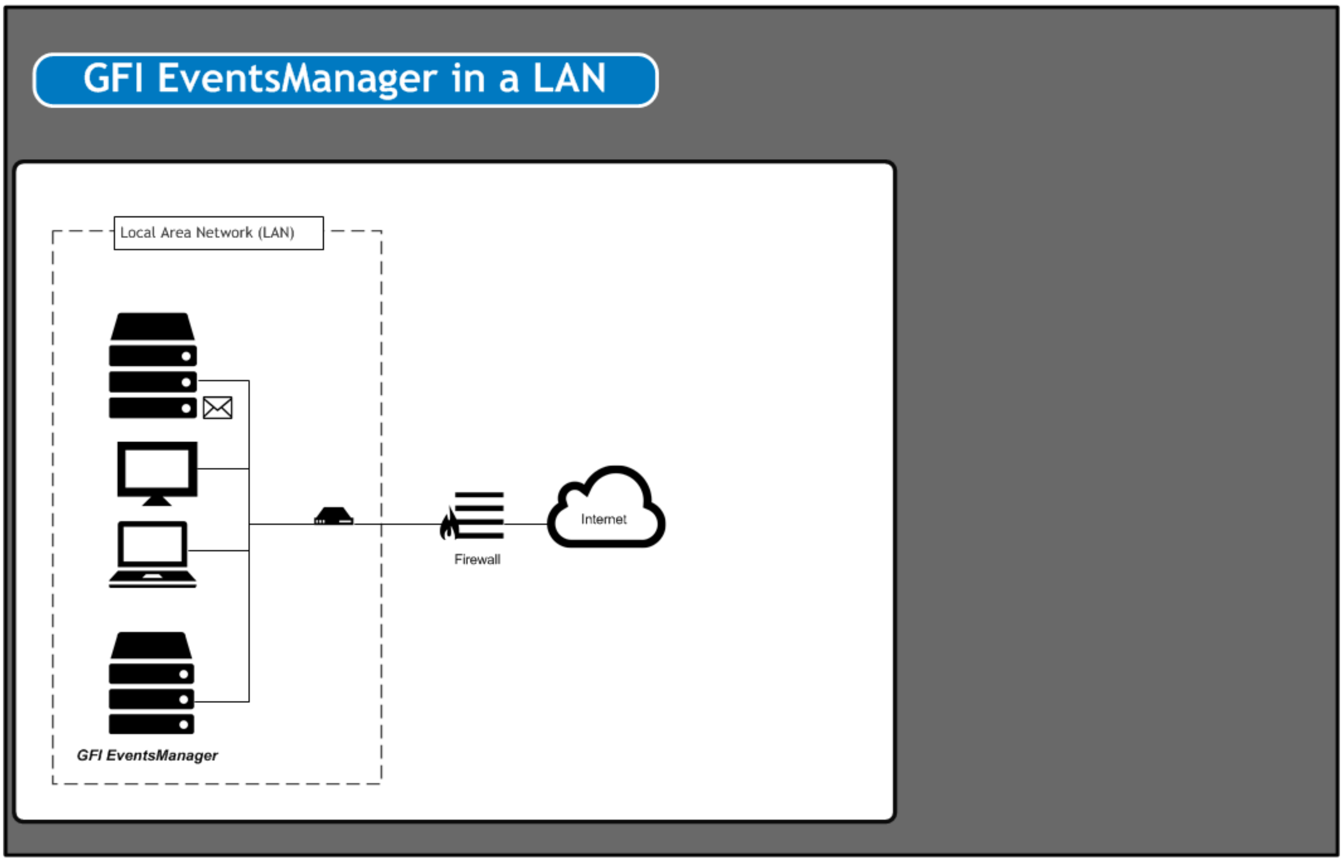
Screenshot 2: GFI EventsManager deployment scenario

This section contains information about deploying GFI EventsManager in a:

- Local Area Network (LAN) - Monitor activity of the main production network, servers and workstations
- Demilitarized Zone (DMZ) - Monitor events generated by public service servers, such as mail servers, web servers and DNS servers
- Wide Area Network (WAN) - Monitor events generated by computers and network devices spread across different geographical locations.

2.1.1 GFI EventsManager within in a Local Area Network (LAN)

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.



Screenshot 3: Deployment of GFI EventsManager in LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows® events, Text Logs, Syslog messages, SNMP Trap and SQL Server® audit messages generated by any hardware or software that is connected to the LAN, including:

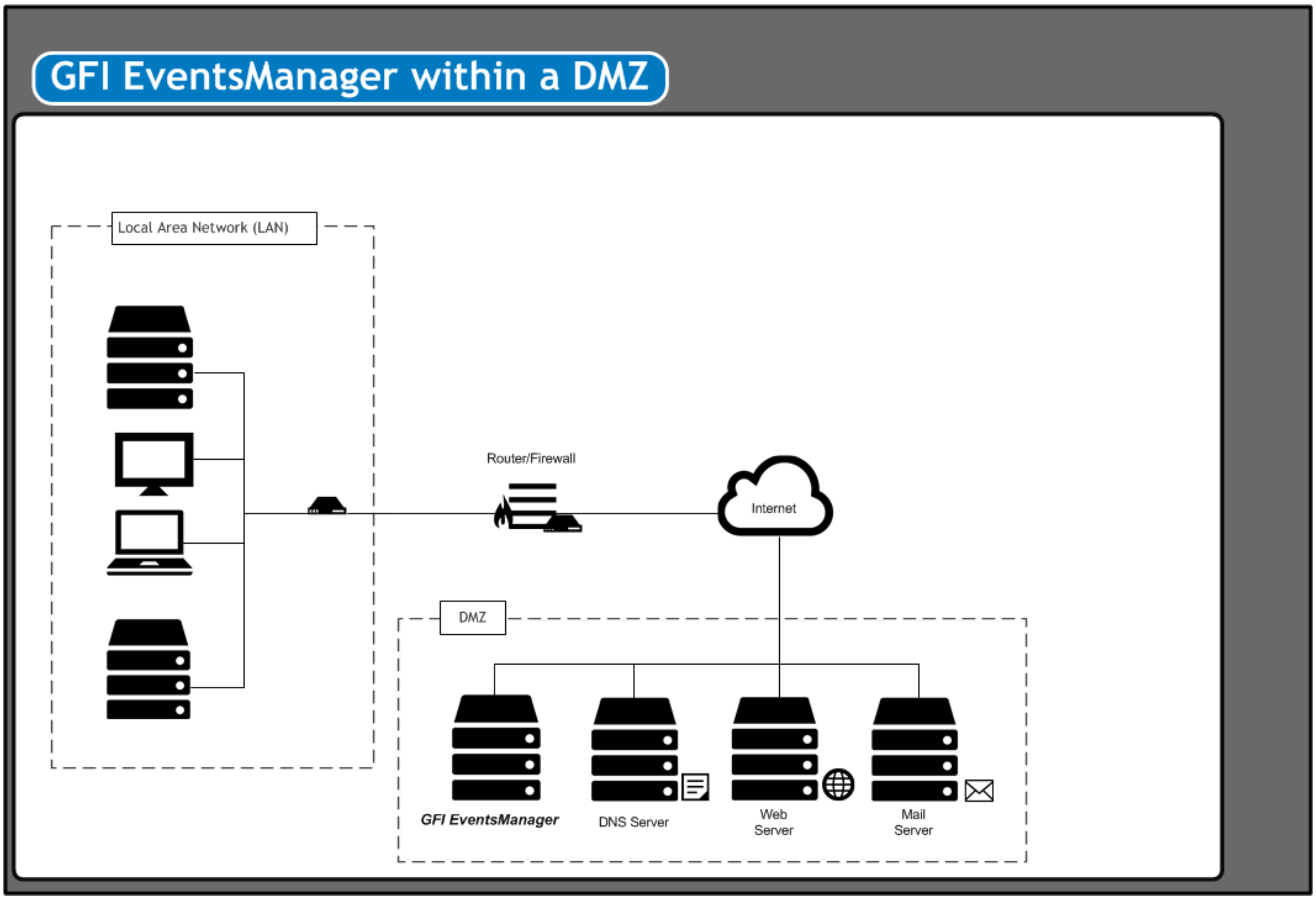
Device	Example
Workstations and laptops	End-user computers and systems.
Servers	Web servers, Mail servers, DNS servers and more.
Network devices	Routers, switches and any other device that generates performance logs.
Software	Including GFI EndPointSecurity, GFI LanGuard and other applications that generate logs.
Specialized Services	Microsoft® Internet Information Server – IIS.
PABXs, Keyless Access Systems, Intrusion detections systems and more	GFI EventsManager enables you to monitor any device that is attached to the network.

2.1.2 GFI EventsManager within a Demilitarized Zone (DMZ)

GFI EventsManager is able to monitor events generated by machines in a DMZ, from being installed within the LAN or by being installed directly in the DMZ. Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

- The communication ports used by GFI EventsManager are not blocked by the firewall. For more information on the communication ports used by GFI EventsManager refer to: http://go.gfi.com/?pageid=esm_ports.
- GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

> **Important**
> GFI recommends to install GFI EventsManager directly in the DMZ as opposed to enabling firewall ports and permissions to allow communication between LAN and DMZ computers, servers and network devices.



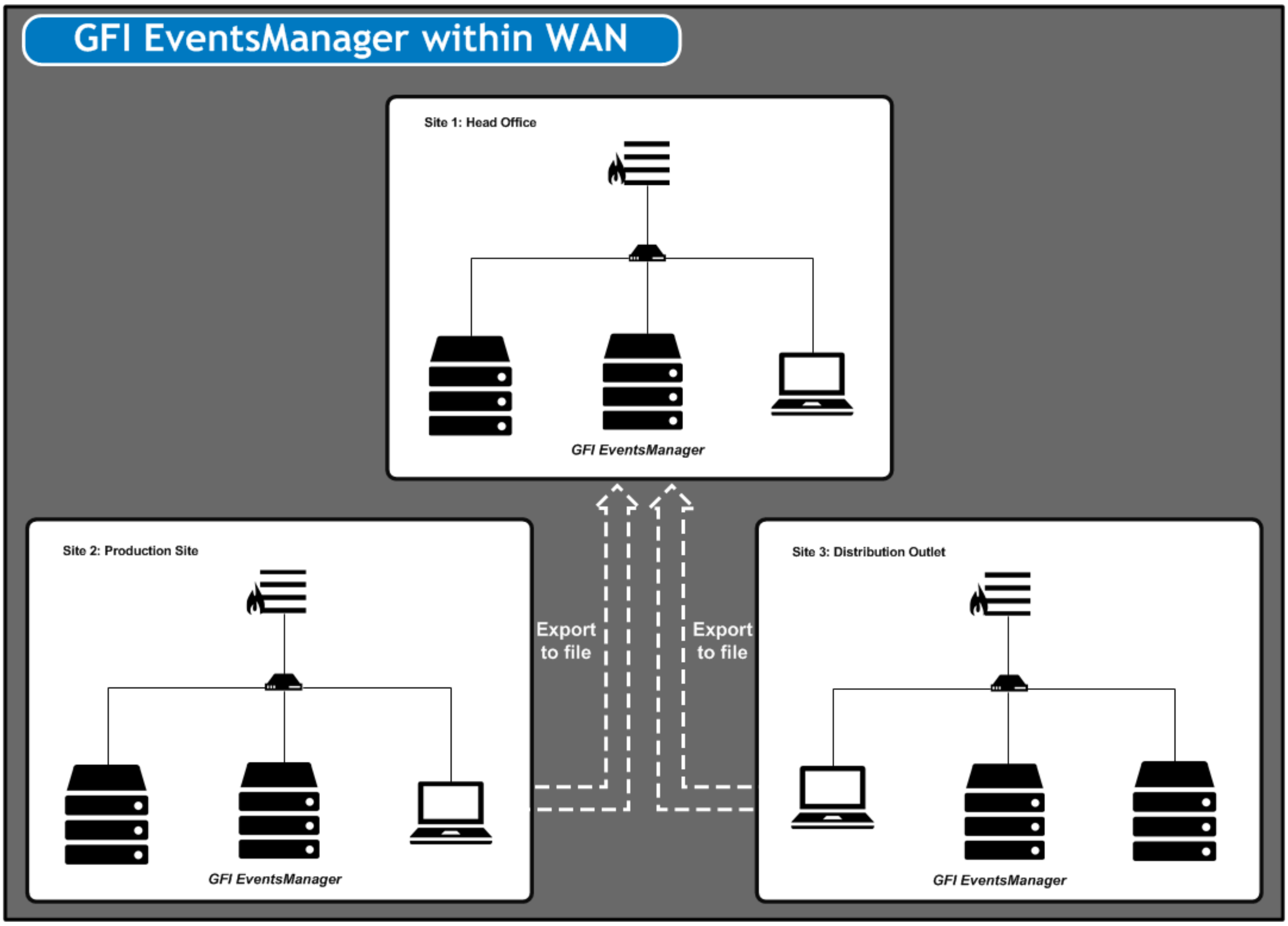
Screenshot 4: The DMZ sits between the internal LAN and the Internet

A DMZ is the neutral network which sits between the “internal” corporate network and the “outside world” (Internet). The deployment of GFI EventsManager in a DMZ helps you automate the management of events generated by DMZ hardware and software systems; such as:

DMZ Automation	Description
Automate management of Web and Mail server events	DMZ networks are normally used for the running of hardware and software systems that have Internet specific roles such as HTTP servers, FTP servers, and Mail servers. Hence, you can deploy GFI EventsManager to automatically manage the events generated by: » 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 including the Syslog auditing services messages generated by Sun Solaris v. 9 or later » Automate management of DNS server events » If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically collect and process DNS server events including those stored in your Windows® DNS Server logs.
Automate management of DNS server events	If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically 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 (example: Cisco IOS series routers) not only help protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can augment the operational performance of your systems. By deploying GFI EventsManager on your DMZ, you can collect the events generated by such network appliances. For example, you can configure GFI EventsManager to act as a Syslog Server and collect in real-time the Syslog messages generated by Cisco IOS routers.

2.1.3 GFI EventsManager within a Wide Area Network (WAN)

GFI EventsManager can be installed in environments that have multiple sites in different geographical locations.



Screenshot 5: Export data from remote sites to the main instance of GFI EventsManager

This is achieved by installing an instance of GFI EventsManager at each location. Periodically (based on a schedule), you can export events from the remote sites and import them into the central database for complete consolidation of event logs.

Events for the remote site can then be viewed through the Events Browser. Reports with information relevant to remote sites can also be generated using data from the central database. Use the Switch Database option to view or report on information stored on remote databases.

> **Note**
>
> For more information refer to Database Maintenance from the **Administrator Guide**.

2.2 System requirements

To install GFI EventsManager, the host computer must meet the system requirements specified below. If you plan to manage a large number of event sources in a high traffic network, consider using a computer with greater system specs. Refer to the following sections for information about:

- Hardware requirements
- Supported operating systems and other software
- Firewall ports, protocols and permissions
- Event source settings

2.2.1 Software requirements

Software	Description
Supported operating systems (32-bit and 64-bit)	GFI EventsManager can be installed on a computer running any of the following operating systems: » Windows® Server 2016 - Essentials, Standard or Datacenter » Windows® Server 2012 R2- Essentials, Standard or Datacenter » Windows® Server 2012 - Essentials, Standard or Datacenter » Windows® Server 2008 R2 – Standard or Enterprise » Windows® Server 2008 - Standard or Enterprise » Windows® SBS 2011 - Standard or Premium » Windows® SBS 2008 - Standard or Premium » Windows®10 - Pro or Enterprise » Windows®8 - Pro or Enterprise » Windows® 7 - Enterprise, Professional or Ultimate » Windows® Vista SP1 - Enterprise, Business or Ultimate **NOTE** GFI EventsManager cannot be installed on Server Core Installations.
Other software components	The following required components can be installed automatically when installing GFI EventsManager. For more information, refer to Installing GFI EventsManager (page 22). » Visual C++ 2010 redistributable » Microsoft® .NET Framework 2.0 » Microsoft® .NET Framework 4.0 » Microsoft® SQL Server® Compact 3.5 SP2 » MSXML6 » Microsoft® SQL Server® Native Client » Microsoft® SQL Server® Management Objects Collection.
DLib Database Server	DLib Database Server is the component where GFI EventsManager stores processed logs. The database server can be installed on the same computer that is running GFI EventsManager as well as on a separate remote computer or network drive.
Optional recommended software	Install the following recommended software components to ensure full functionality of GFI EventsManager: » Microsoft® Data Access Components (MDAC) 2.8 or later downloadable from http://go.gfi.com/?pageid=esm_mdac » A mail server (when email alerting is required).

> **NOTE**
> When GFI EventsManager is using a non-domain account to collect events from Windows® Vista machines or later, target machines must have User Account Control (UAC) disabled.

2.2.2 Hardware requirements

The following table contains hardware requirements for GFI EventsManager:

Hardware Component	Specification
Processor	2.5 GHz dual core or higher.
RAM	3 GB.
Hard disk	10 GB free space.

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

2.2.3 Storage requirements

The storage requirements below are based on the average size of an event log, being 535 bytes per event. The following specifications indicate the required hard disk size, that caters for your infrastructure's requests:

Hard Disk 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

2.2.4 Firewall ports and protocols

The following table contains ports and protocols that must be allowed by the firewall of the GFI EventsManager host:

Port	Protocols	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.

2.2.5 Firewall permissions

The following list contains permissions that must be allowed by the firewall of the GFI EventsManager host:

- Remote Event Log Management
- File and Printer Sharing
- Network Discovery

2.2.6 Antivirus exceptions

If an antivirus application 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 **esmproc.exe** are allowed access through the firewall(s).
- GFI EventsManager folders are excluded from real-time antivirus scanning.

2.2.7 Event source settings

The following table contains settings that must be configured on your event sources. Event sources are computers that you want to monitor by GFI EventsManager:

Log Type	Description
Windows® event log processing	Enable remote registry.
Text 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 Enabling event source permissions manually and Enabling event source permissions automatically from the **Administrator Guide**.

2.2.8 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.

2.3 Importing and Exporting settings

The provided import and export tool, enables you to seamlessly move configurations from one instance of GFI EventsManager to another. This can also be done as part of a disaster recovery plan, to avoid having to reconfigure GFI EventsManager in case of a disaster. The following settings can be imported/exported using GFI EventsManager:

- Event Sources
- Event Processing Rules
- Events Browser Filters
- Options (including Default Classification Actions, Alerting Options, Database operations and more).

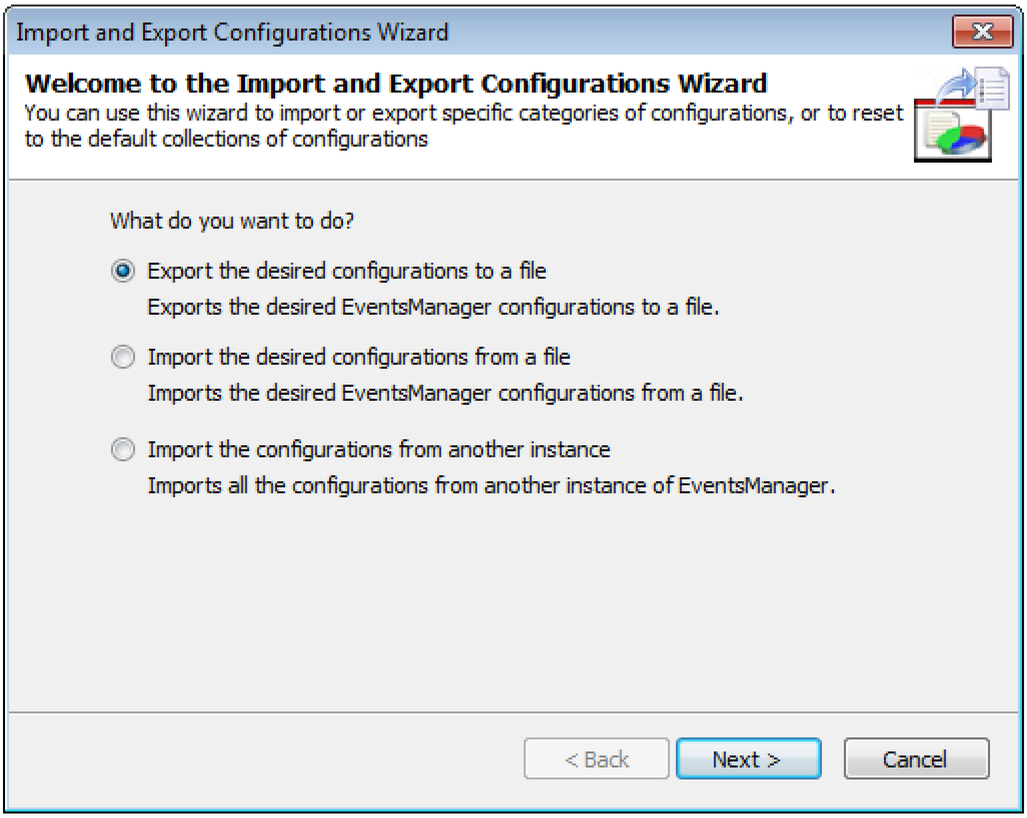
This section contains information about:

- Exporting configurations to a file
- Importing configurations from a file
- Importing configurations from another instance

2.3.1 Exporting configurations to a file

To export you GFI EventsManager configurations:

1. Click **File > Import and Export Configurations...**.



Import and Export Configurations Wizard

Welcome to the Import and Export Configurations Wizard

You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations

What do you want to do?

● Export the desired configurations to a file

Exports the desired EventsManager configurations to a file.

○ Import the desired configurations from a file

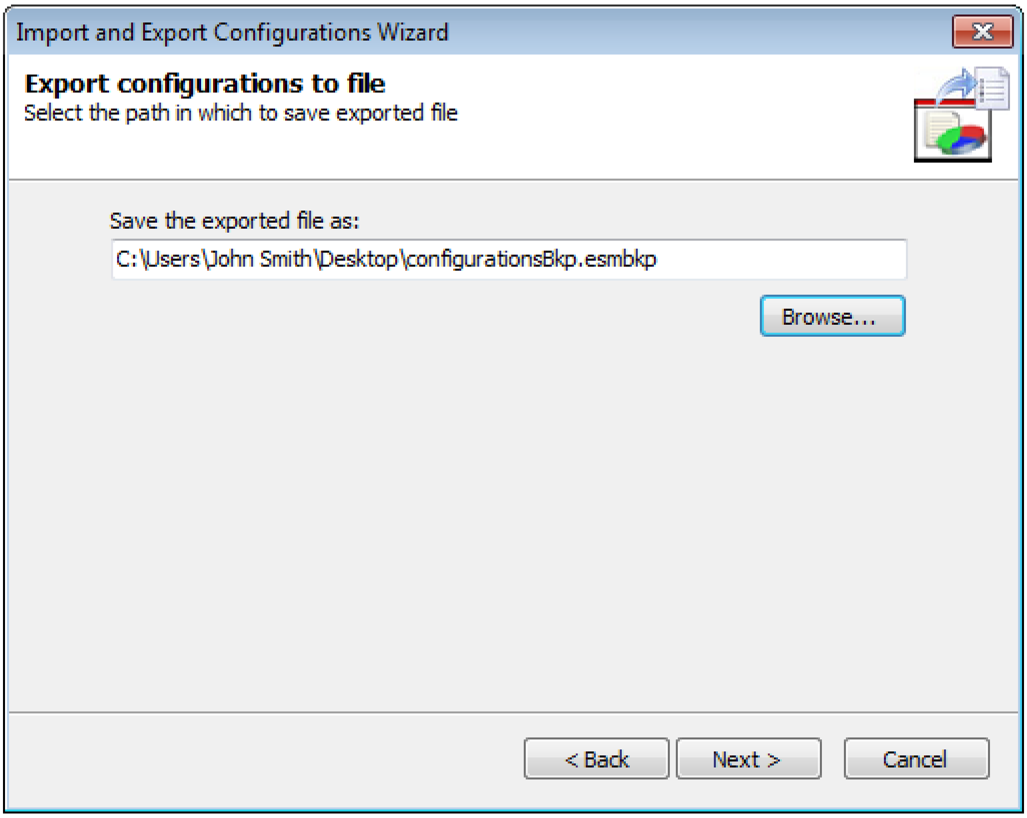
Imports the desired EventsManager configurations from a file.

○ Import the configurations from another instance

Imports all the configurations from another instance of EventsManager.

Screenshot 6: Export configurations to a file

2. Select **Export the desired configurations to a file** and click **Next**.



Import and Export Configurations Wizard

Export configurations to file

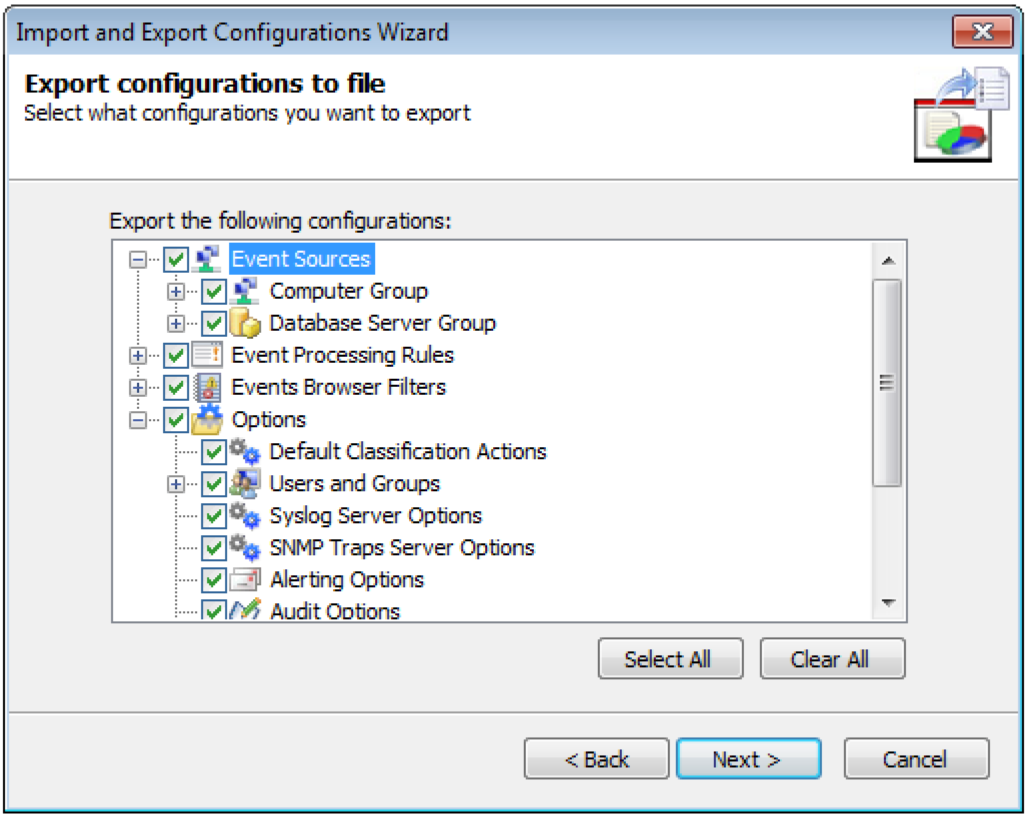
Select the path in which to save exported file

Save the exported file as:

C:\Users\John Smith\Desktop\configurationsBkp.esmbkp

Screenshot 7: Specify export destination

3. Specify the location where the exported file will be saved or click **Browse...** to look for the location. Click **Next**.



Import and Export Configurations Wizard

Export configurations to file

Select what configurations you want to export

Export the following configurations:

- ☑ Event Sources
  - ☑ Computer Group
  - ☑ Database Server Group
- ☑ Event Processing Rules
- ☑ Events Browser Filters
- ☑ Options
  - ☑ Default Classification Actions
  - ☑ Users and Groups
  - ☑ Syslog Server Options
  - ☑ SNMP Traps Server Options
  - ☑ Alerting Options
  - ☑ Audit Options

Screenshot 8: Select export configurations

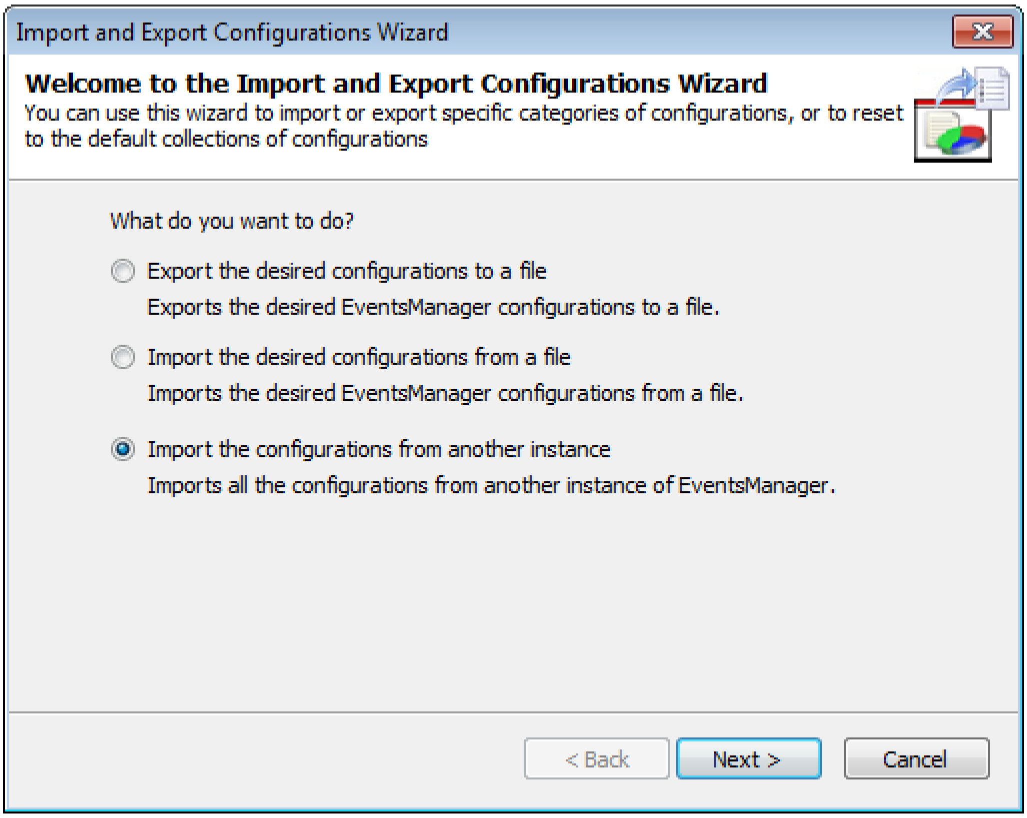
4. Select the configurations you want to export and click **Next**.

5. Wait for GFI EventsManager to export the configuration and click **OK**

2.3.2 Importing configurations from another instance

To import configurations from another instance of GFI EventsManager:

1. Click **File > Import and Export Configurations...**



Welcome to the Import and Export Configurations Wizard

You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations

What do you want to do?

○ Export the desired configurations to a file

Exports the desired EventsManager configurations to a file.

○ Import the desired configurations from a file

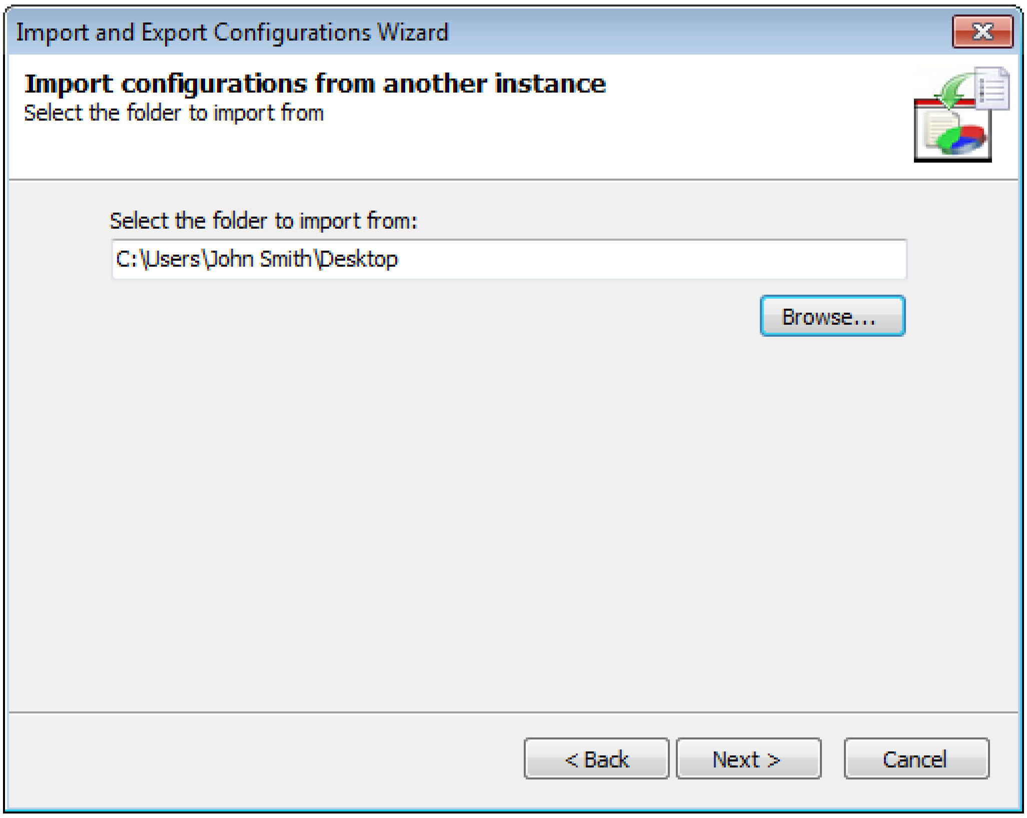
Imports the desired EventsManager configurations from a file.

● Import the configurations from another instance

Imports all the configurations from another instance of EventsManager.

Screenshot 9: Import configurations from another instance of GFI EventsManager

2. Select **Import the configurations from another instance** and click **Next**.


Import and Export Configurations Wizard

Import configurations from another instance

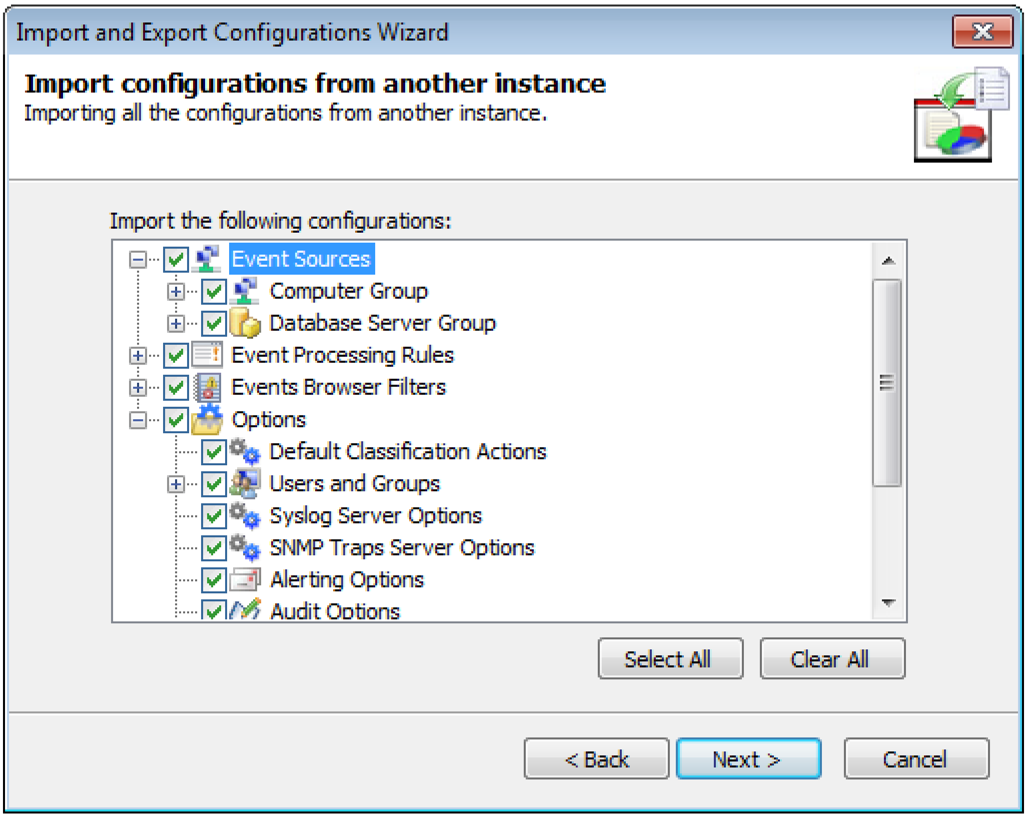
Select the folder to import from

Select the folder to import from:

C:\Users\John Smith\Desktop

Screenshot 10: Specify instance location

3. Specify the installation folder path of the instance you want to import configurations from. Alternatively, click **Browse...** to look for it. Click **Next**.


Import and Export Configurations Wizard

Import configurations from another instance

Importing all the configurations from another instance.

Import the following configurations:

- ☑ Event Sources
  - ☑ Computer Group
  - ☑ Database Server Group
- ☑ Event Processing Rules
- ☑ Events Browser Filters
- ☑ Options
  - ☑ Default Classification Actions
  - ☑ Users and Groups
  - ☑ Syslog Server Options
  - ☑ SNMP Traps Server Options
  - ☑ Alerting Options
  - ☑ Audit Options

Screenshot 11: Select configurations to import from another instance of GFI EventsManager

4. Select the configurations you want to import and click **Next**.

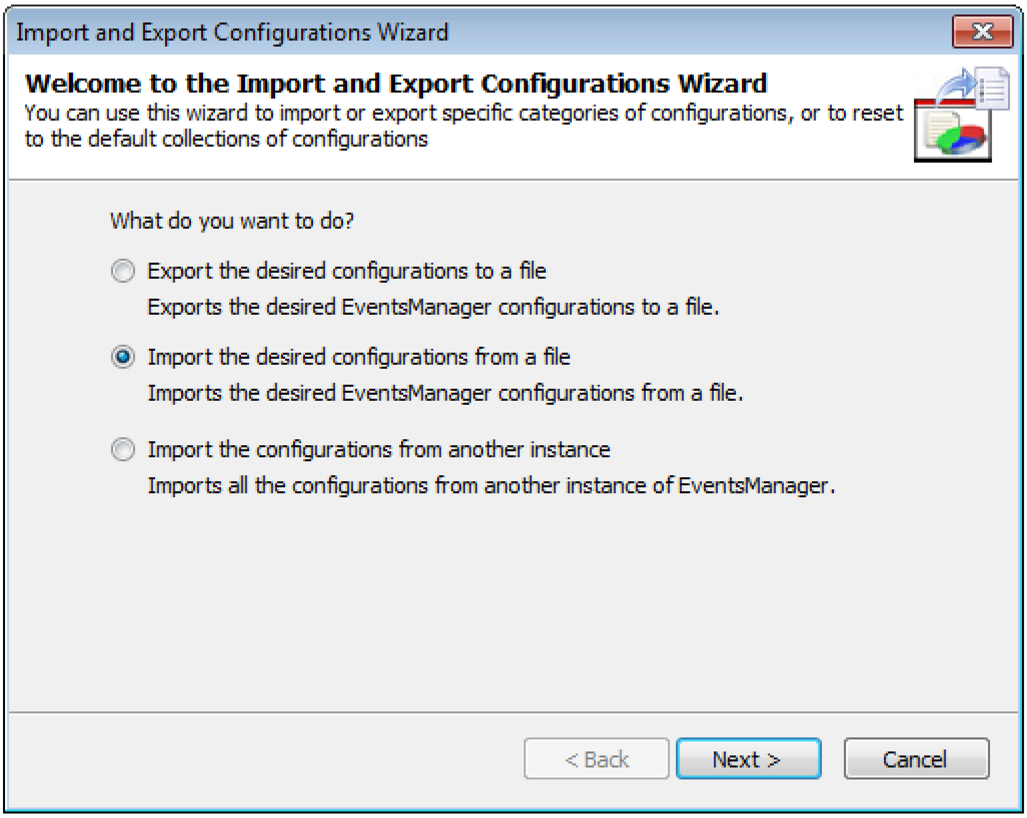
5. Wait for the configurations to import and click **OK**

> **Note**
>
> If GFI EventsManager detects other configurations, it will ask you if you want to override or merge both configurations.

2.3.3 Importing configurations from a file

To import configurations from a file:

1. Click **File > Import and Export Configurations...**.



Import and Export Configurations Wizard

Welcome to the Import and Export Configurations Wizard

You can use this wizard to import or export specific categories of configurations, or to reset to the default collections of configurations

What do you want to do?

○ Export the desired configurations to a file

Exports the desired EventsManager configurations to a file.

● Import the desired configurations from a file

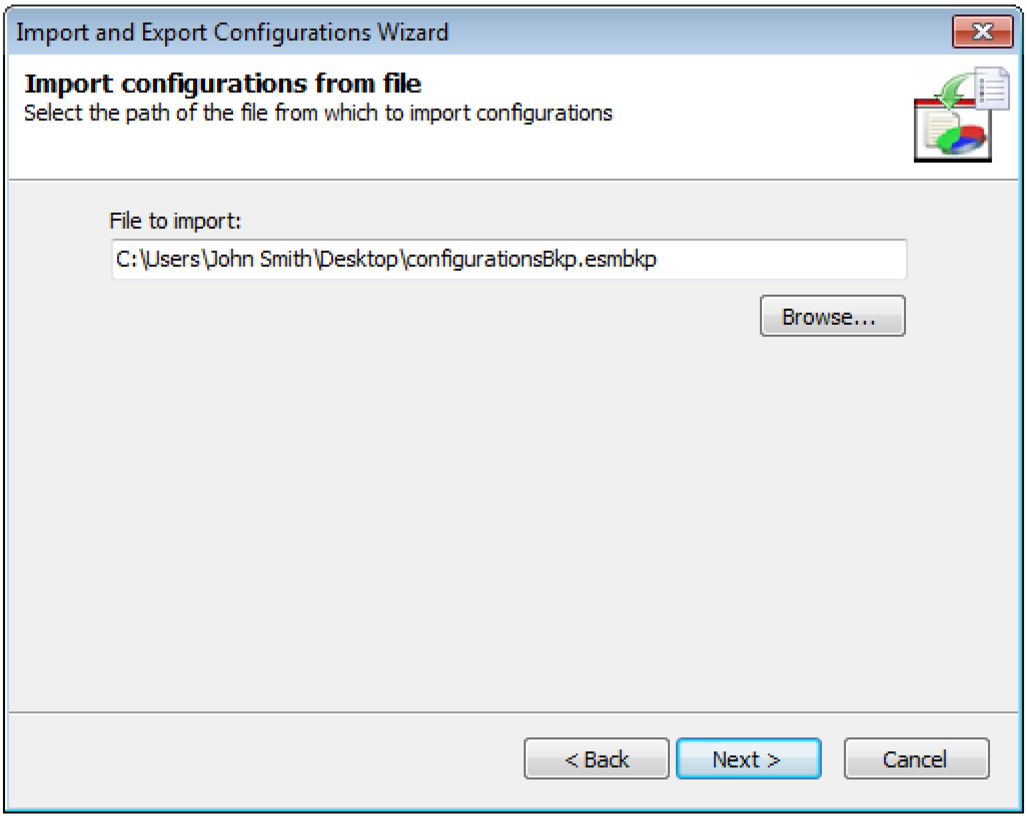
Imports the desired EventsManager configurations from a file.

○ Import the configurations from another instance

Imports all the configurations from another instance of EventsManager.

Screenshot 12: Import configurations from a file

2. Select **Import the desired configurations from a file** and click **Next**.



Import and Export Configurations Wizard

Import configurations from file

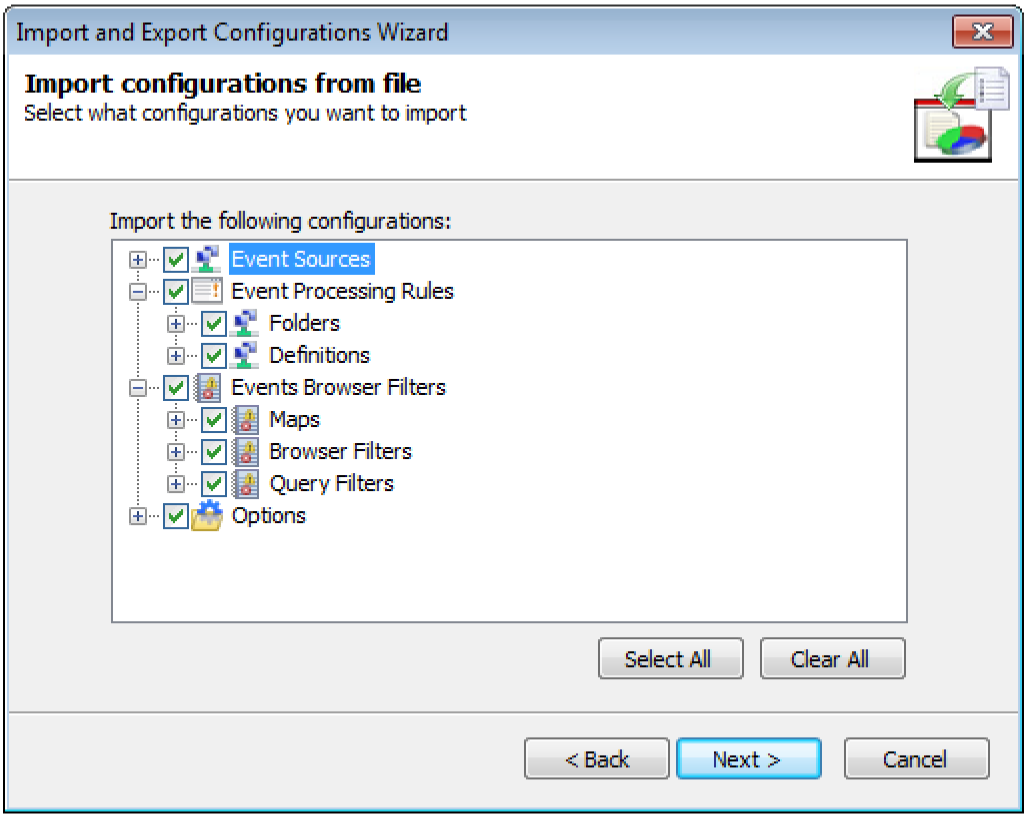
Select the path of the file from which to import configurations

File to import:

C:\Users\John Smith\Desktop\configurationsBkp.esmbkp

Screenshot 13: Specify configuration file location

3. Specify the path where the import file is stored or click **Browse...** to look for it. Click **Next**.



Import and Export Configurations Wizard

Import configurations from file

Select what configurations you want to import

Import the following configurations:

- ☑ Event Sources
- ☑ Event Processing Rules
  - ☑ Folders
  - ☑ Definitions
- ☑ Events Browser Filters
  - ☑ Maps
  - ☑ Browser Filters
  - ☑ Query Filters
- ☑ Options

Screenshot 14: Select configurations to import

4. Select the configurations you want to import and click **Next**.

5. Wait for GFI EventsManager to import the configurations and click **OK**

Note

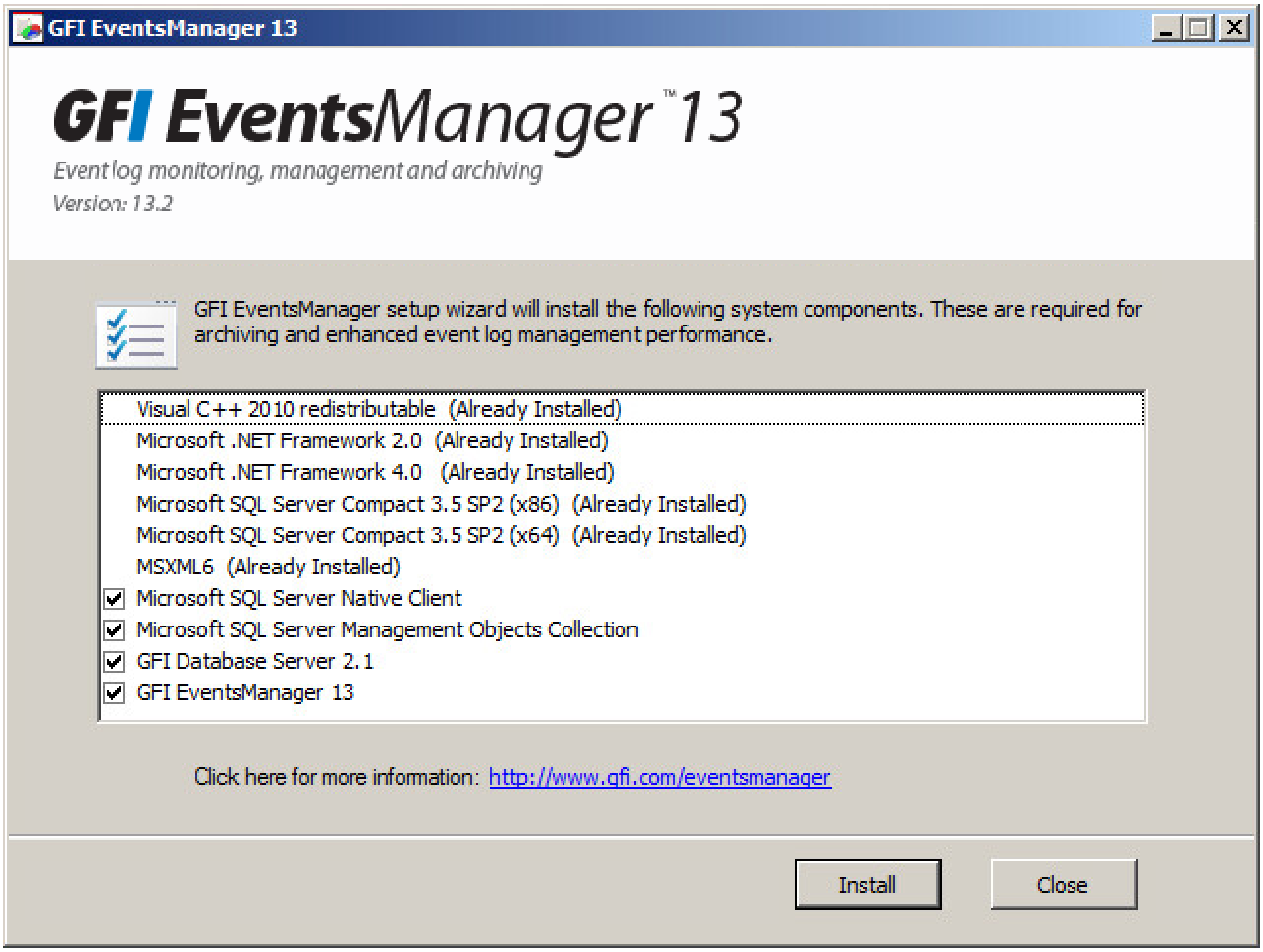
If GFI EventsManager detects other configurations, it will ask you if you want to override or merge both configurations.

2.4 Installing GFI EventsManager

To install GFI EventsManager:

1. Right-click the GFI EventsManager installer and choose **Properties**. From the **General** tab, click **Unblock** and then **Apply**. This step is required to prevent the operating system from blocking certain actions by the installer.

2. Launch the installer.



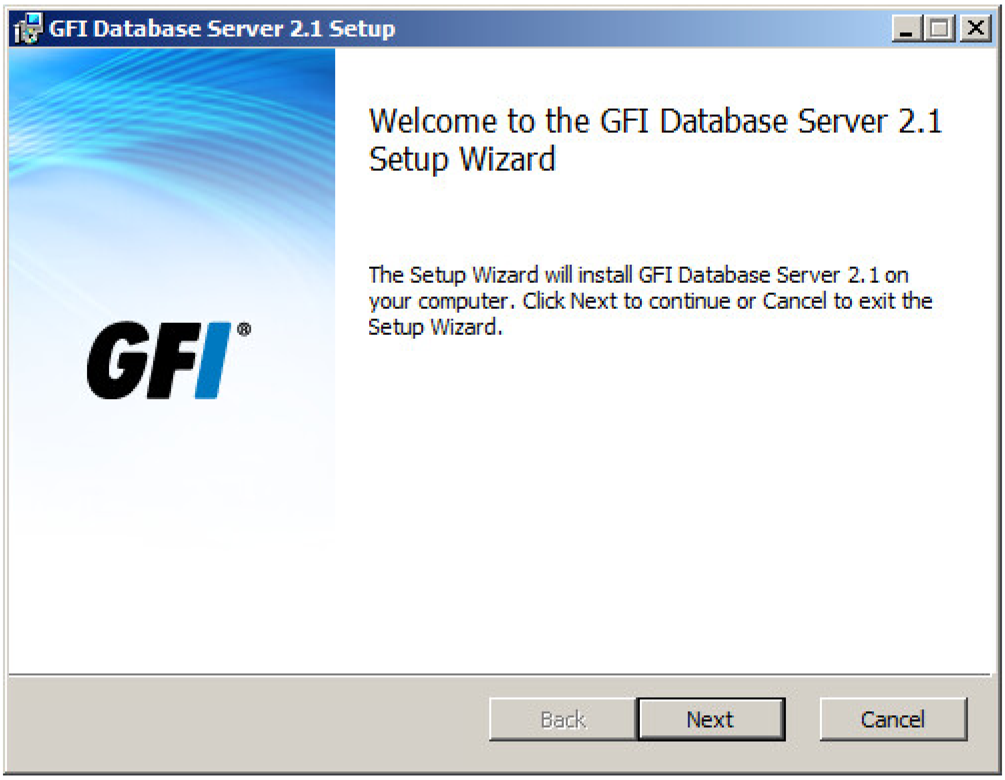
GFI EventsManager setup wizard will install the following system components. These are required for archiving and enhanced event log management performance.

Visual C++ 2010 redistributable (Already Installed)
Microsoft .NET Framework 2.0 (Already Installed)
Microsoft .NET Framework 4.0 (Already Installed)
Microsoft SQL Server Compact 3.5 SP2 (x86) (Already Installed)
Microsoft SQL Server Compact 3.5 SP2 (x64) (Already Installed)
MSXML6 (Already Installed)
☑ Microsoft SQL Server Native Client
☑ Microsoft SQL Server Management Objects Collection
☑ GFI Database Server 2.1
☑ GFI EventsManager 13

Click here for more information: http://www.gfi.com/eventsmanager

Screenshot 15: Prerequisite check

3. The installer displays a list of system components that must be installed prior to installing the product. Click **Install** to start the installation of missing system components (if necessary).



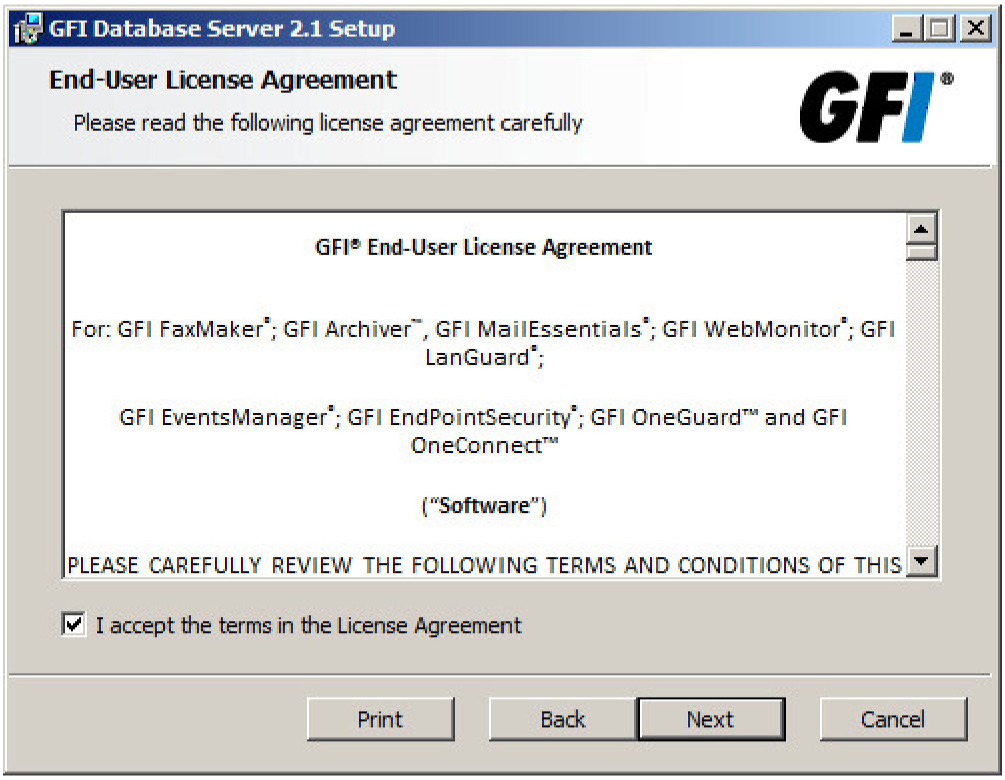
GFI Database Server 2.1 Setup

Welcome to the GFI Database Server 2.1 Setup Wizard

The Setup Wizard will install GFI Database Server 2.1 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Screenshot 16: DLib Database Server

4. The DLib Database Server install wizards opens automatically after system components are installed. Click **Next** at the wizard welcome screen.



GFI Database Server 2.1 Setup

End-User License Agreement

Please read the following license agreement carefully

GFI® End-User License Agreement

For: GFI FaxMaker®; GFI Archiver™, GFI MailEssentials®; GFI WebMonitor®; GFI LanGuard®;

GFI EventsManager®; GFI EndPointSecurity®; GFI OneGuard™ and GFI OneConnect™

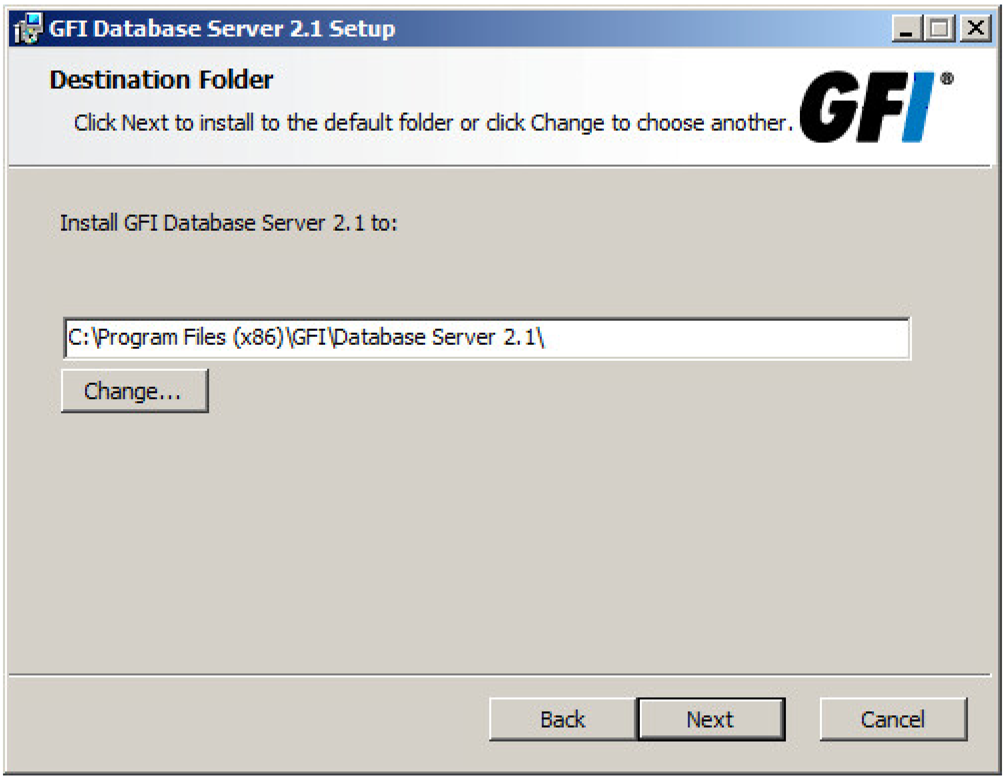
("Software")

PLEASE CAREFULLY REVIEW THE FOLLOWING TERMS AND CONDITIONS OF THIS

☑ I accept the terms in the License Agreement

Screenshot 17: DLib Database Server EULA

5. Read the license agreement. Select **I accept the terms in the License Agreement** and click **Next**.



GFI Database Server 2.1 Setup

Destination Folder

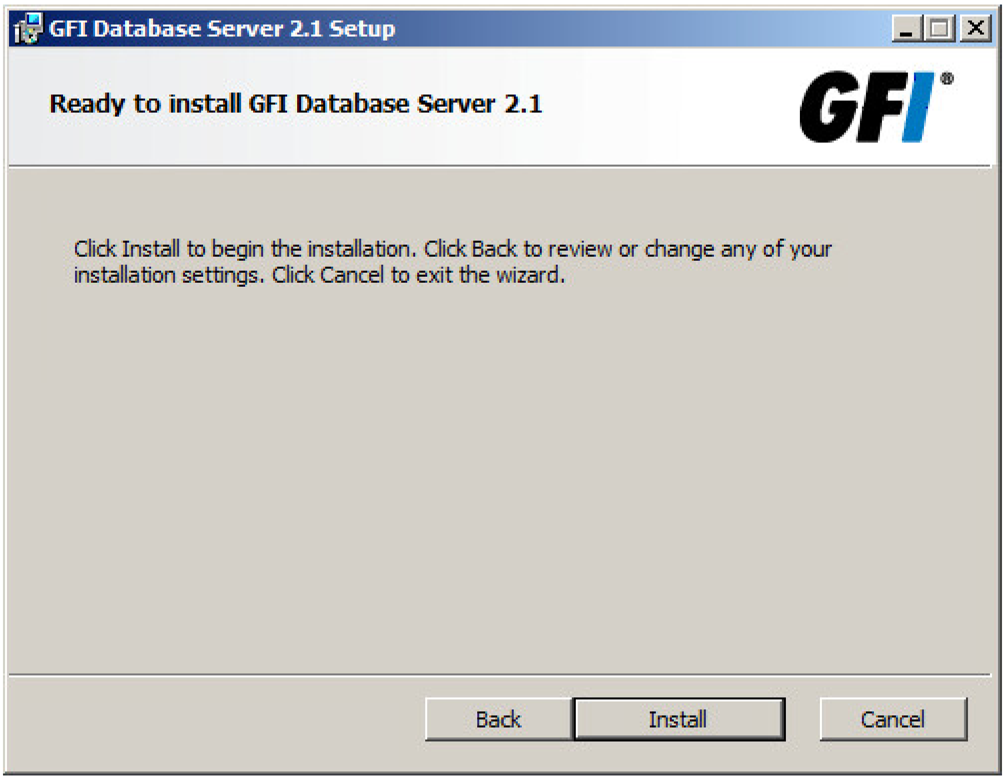
Click Next to install to the default folder or click Change to choose another.

Install GFI Database Server 2.1 to:

C:\Program Files (x86)\GFI\Database Server 2.1\

Screenshot 18: DLib install folder

6. Click **Next** to install the database server in the default folder or click **Change...** to select an alternate folder where it is installed.



GFI Database Server 2.1 Setup

Ready to install GFI Database Server 2.1

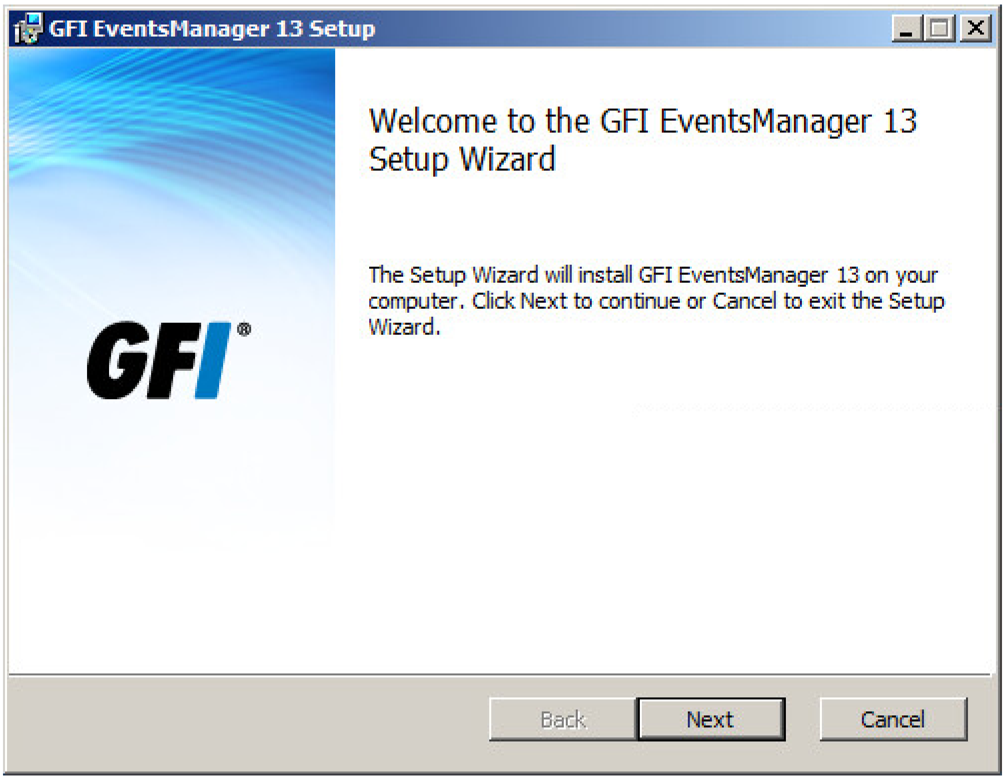
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Screenshot 19: Start installing DLib Database Server

7. Click **Install** to start installing DLib Database Server. Click **Finish** when prompted.

Note

After the database server is installed, the installer automatically opens the install wizard of GFI EventsManager Management Console.

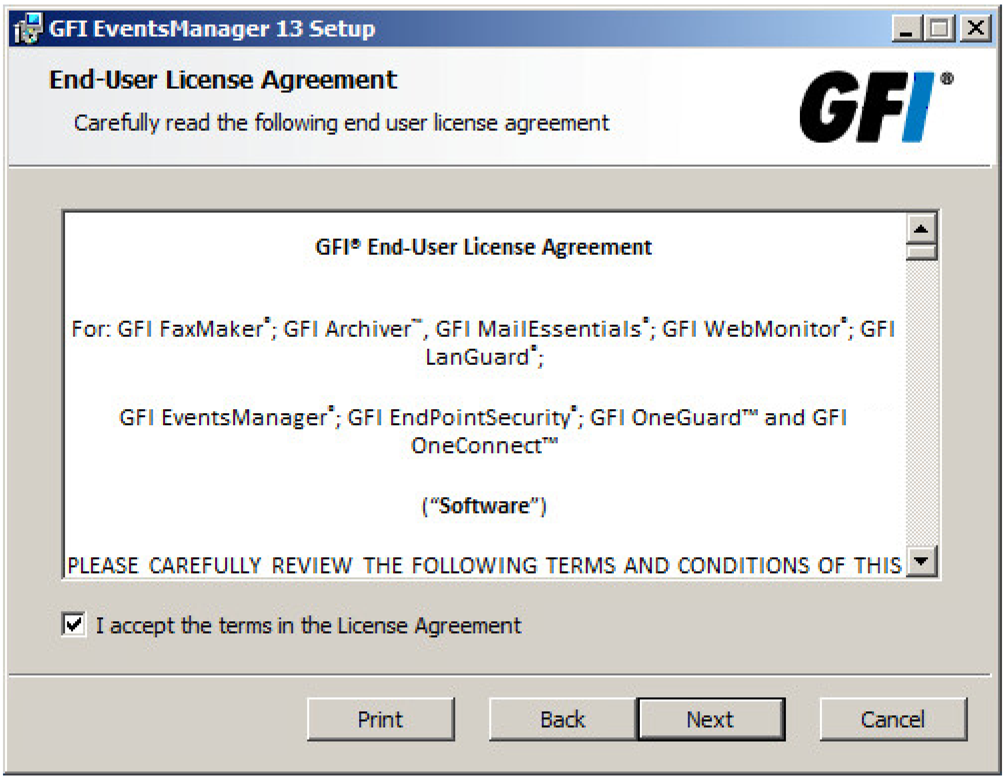


Welcome to the GFI EventsManager 13 Setup Wizard

The Setup Wizard will install GFI EventsManager 13 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Screenshot 20: GFI EventsManager setup wizard welcome screen

8. Click **Next** at the wizard welcome screen.



End-User License Agreement

Carefully read the following end user license agreement

GFI® End-User License Agreement

For: GFI FaxMaker®; GFI Archiver™, GFI MailEssentials®; GFI WebMonitor®; GFI LanGuard®;

GFI EventsManager®; GFI EndPointSecurity®; GFI OneGuard™ and GFI OneConnect™

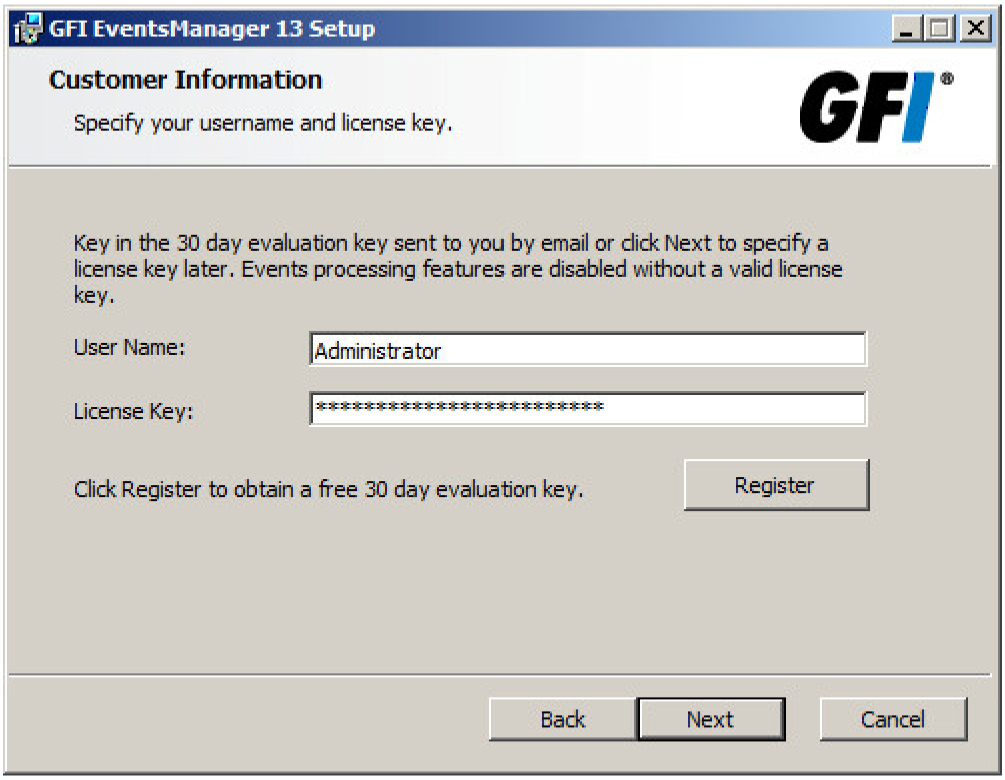
("Software")

PLEASE CAREFULLY REVIEW THE FOLLOWING TERMS AND CONDITIONS OF THIS

☑ I accept the terms in the License Agreement

Screenshot 21: GFI EventsManager EULA

9. Carefully read the license agreement. Select **I accept the terms in the License Agreement** and click **Next**.



GFI EventsManager 13 Setup

Customer Information

Specify your username and license key.

Key in the 30 day evaluation key sent to you by email or click Next to specify a license key later. Events processing features are disabled without a valid license key.

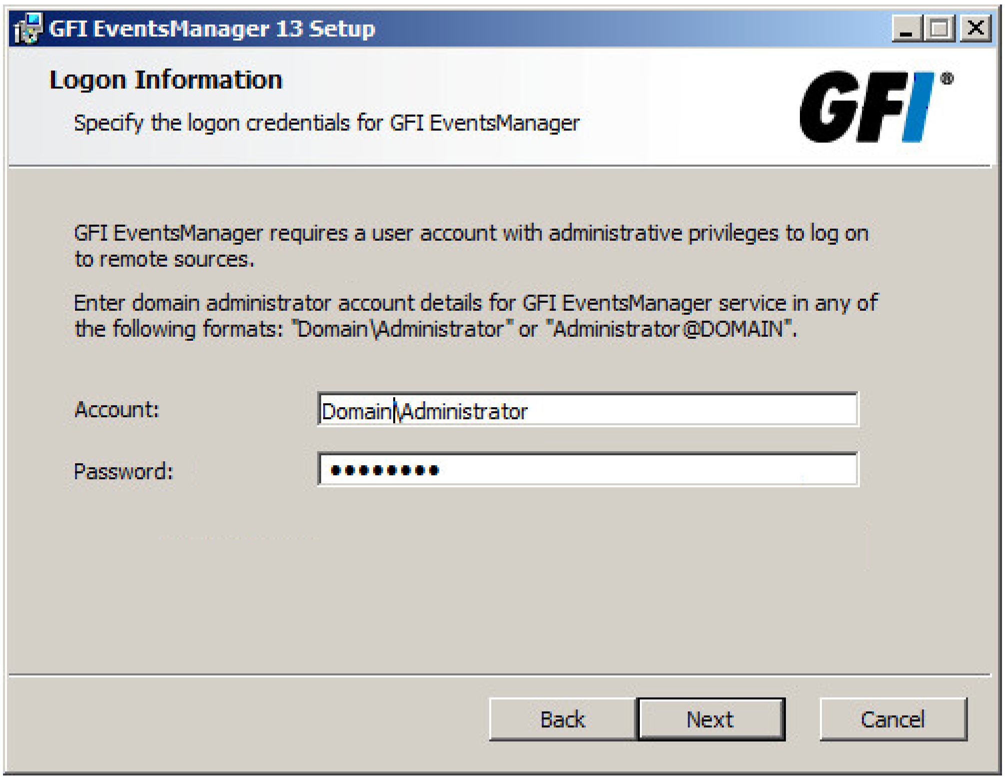
User Name: Administrator

License Key: **************************

Click Register to obtain a free 30 day evaluation key.

Screenshot 22: GFI EventsManager registration details

10. Key in your user name and license key in the **User Name** and **License Key** fields. To register for a free 30 day evaluation license key, click **Register**. Click **Next**.



GFI EventsManager 13 Setup

Logon Information

Specify the logon credentials for GFI EventsManager

GFI EventsManager requires a user account with administrative privileges to log on to remote sources.

Enter domain administrator account details for GFI EventsManager service in any of the following formats: "Domain\Administrator" or "Administrator@DOMAIN".

Account: Domain\Administrator

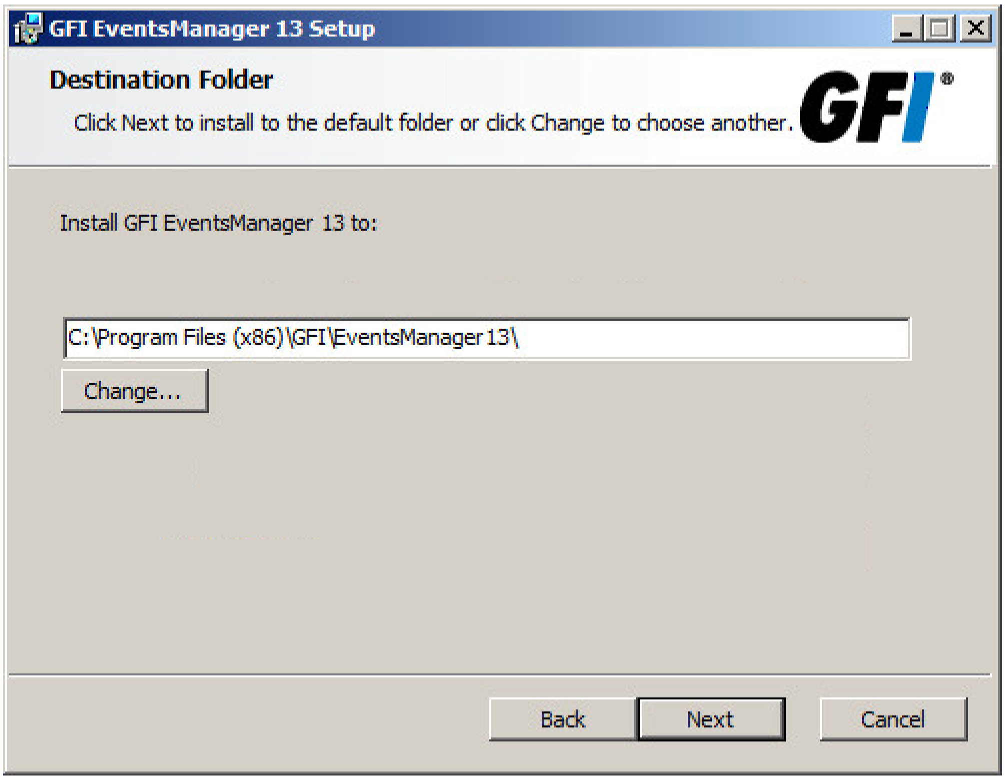
Password: ••••••••

Screenshot 23: Remote logon credentials for event log monitoring

11. Key in the logon credentials that GFI EventsManager uses to log onto remote computers.

NOTE

It is recommended to use a domain administrator or an account with administrative rights over all the remote computers managed by GFI EventsManager.



GFI EventsManager 13 Setup

Destination Folder

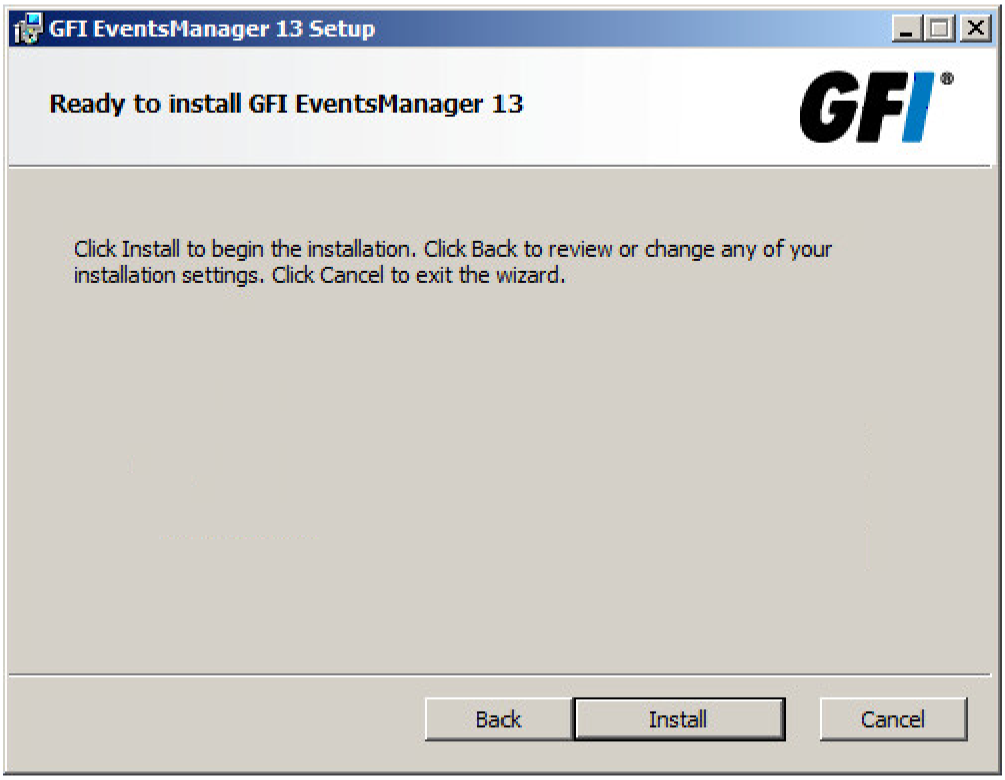
Click Next to install to the default folder or click Change to choose another.

Install GFI EventsManager 13 to:

C:\Program Files (x86)\GFI\EventsManager 13\

Screenshot 24: GFI EventsManager install folder

12. Click **Next** to install the Management Console in the default folder or click **Change...** to select an alternate folder where it is installed.

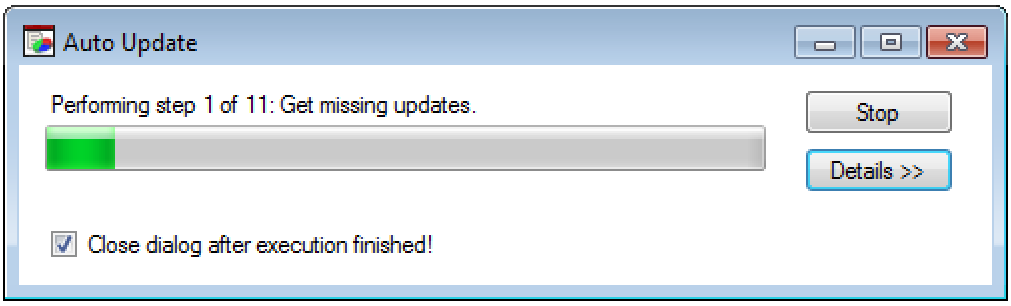

GFI EventsManager 13 Setup
Ready to install GFI EventsManager 13
GFI
Back
Install
Cancel

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Screenshot 25: GFI EventsManager installation completed

13. Click **Install** to start the installation.

14. When the installation is complete, click **Finish**.

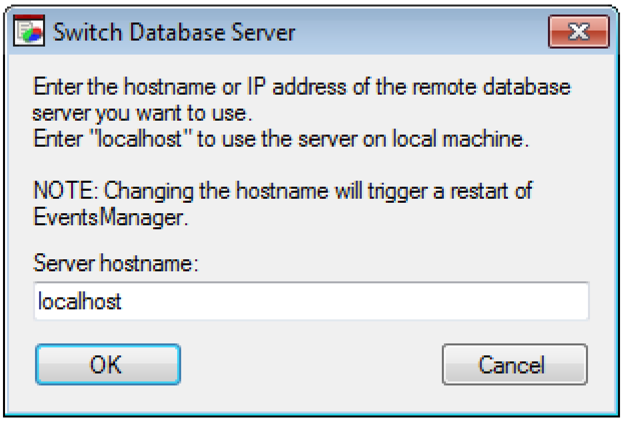


Performing step 1 of 11: Get missing updates.

☑ Close dialog after execution finished!

Screenshot 26: Auto updates check

15. If GFI EventsManager detects an Internet connection, it automatically attempts to download product updates from GFI updates servers. Click **Details** to expand the information section of the Auto Update dialog and view the updates that are being downloaded.



Switch Database Server

Enter the hostname or IP address of the remote database server you want to use.
Enter "localhost" to use the server on local machine.

NOTE: Changing the hostname will trigger a restart of EventsManager.

Server hostname: localhost

Screenshot 27: Set the database backend

> **NOTE**
> After product updates are applied, the **Switch Database Server** dialog opens. This dialog is used to link the management console to a database server. You can switch database servers from the Management Console. For more information about switching databases go to http://go.gfi.com/?pageid=esm_adminguide#cshid=1049

16. Specify the computer that has D-Lib Database Server installed on it. If the database you want to use is on:

    - A remote computer - key in the **computer name** or **IP address**
    - The localhost - key in **localhost** (default).

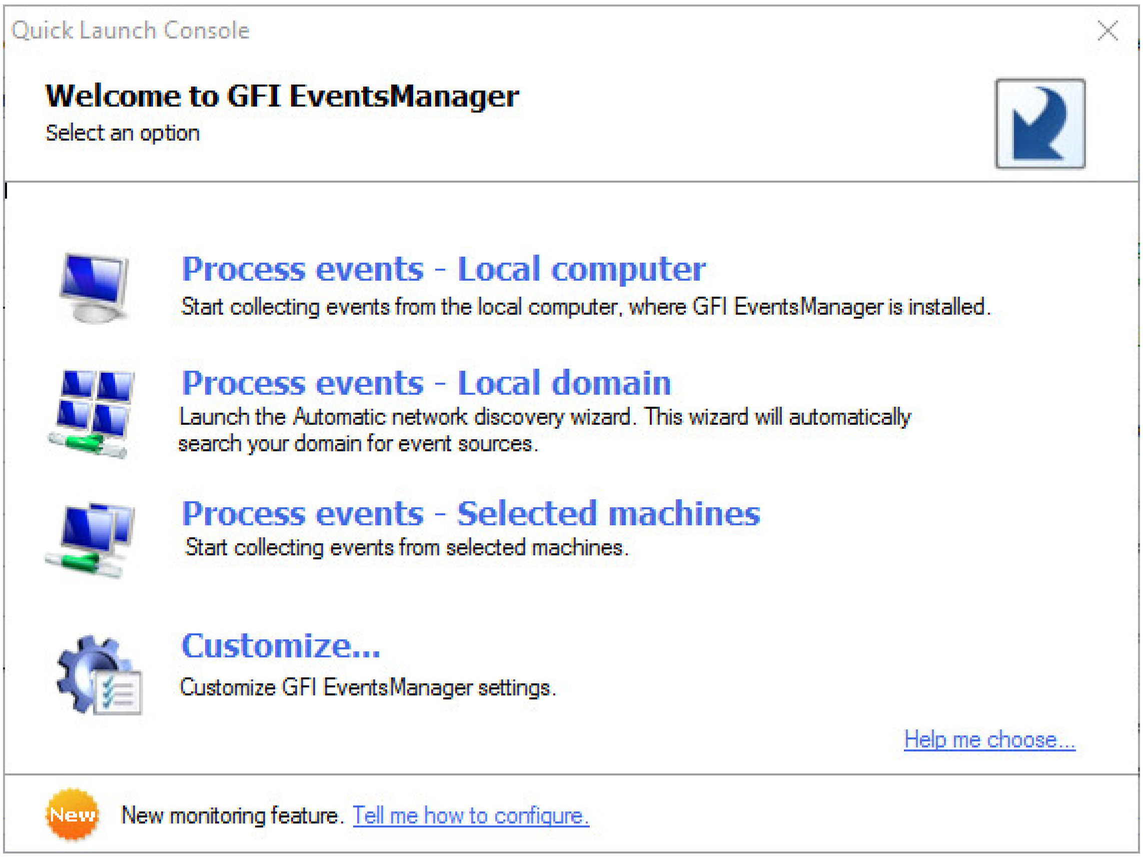
Click **OK**

> **NOTE**
> Once the installation is complete, the Management Console opens automatically. To launch it manually, click **Start > All Programs > GFI EventsManager > Management Console**.

> **NOTE**
> Test the installation to ensure that all the components were successfully installed. For more information refer to Testing the installation.

3 Testing the installation

After all the required components are installed, the Management Console opens automatically. By default, it is configured to launch the **Quick Launch Console** on start up.



Quick Launch Console

Welcome to GFI EventsManager

Select an option

Process events - Local computer

Start collecting events from the local computer, where GFI EventsManager is installed.

Process events - Local domain

Launch the Automatic network discovery wizard. This wizard will automatically search your domain for event sources.

Process events - Selected machines

Start collecting events from selected machines.

Customize...

Customize GFI EventsManager settings.

Help me choose...

New monitoring feature. Tell me how to configure.

Screenshot 28: Running GFI EventsManager for the first time

Select an option from the Quick Launch Console to process events or customize default settings:

Option	Description
Process events - Local computer	Start processing logs generated by the GFI EventsManager host. **Note** For more information refer to Process events - Local computer.
Process events - Local domain	Start processing logs generated by computers and network devices within the same domain as the GFI EventsManager host. **Note** For more information refer to Process events - Local domain.
Process events - Selected machines	Start processing logs generated by specific computer(s). **Note** For more information refer to Process events - Selected machines.

Option	Description
Customize...	Customize default settings, such as: » Event sources and log types » Events processing rules » Database operations » Alert recipients » Alerting options » Active monitoring For more information go to http://go.gfi.com/?pageid=esm_adminguide.

3.1 How to process events for the Local computer

This option enables you to automatically add the localhost as an event source and start processing logs generated by it.

To process events from the local computer:

1. Open the GFI EventsManager Quick Launch Console. In the welcome page, click **Process events - Local computer**.

2. After the localhost logs start processing, you can:

Icon	Description
	Browse events Access the built-in events and forensic tools that will help you locate, analyze and filter key events.
	Generate reports Access reporting features including instant/scheduled report generations and automated report distribution.
	View dashboard Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager.
	Customize Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, system checks, key events notifications, and more.

> **Note**
>
> To confirm that logs are successfully processed, go to **Status** tab **> Job Activity** and check that there are activity logs under the **Operational History** section.

3.2 How to process events for the Local domain

This option enables you add one or more computers that are on the same domain or workgroup as GFI EventsManager. The Automatic Network Discovery wizard enables you to select the type of event sources you want to add and then lists the sources that are detected.

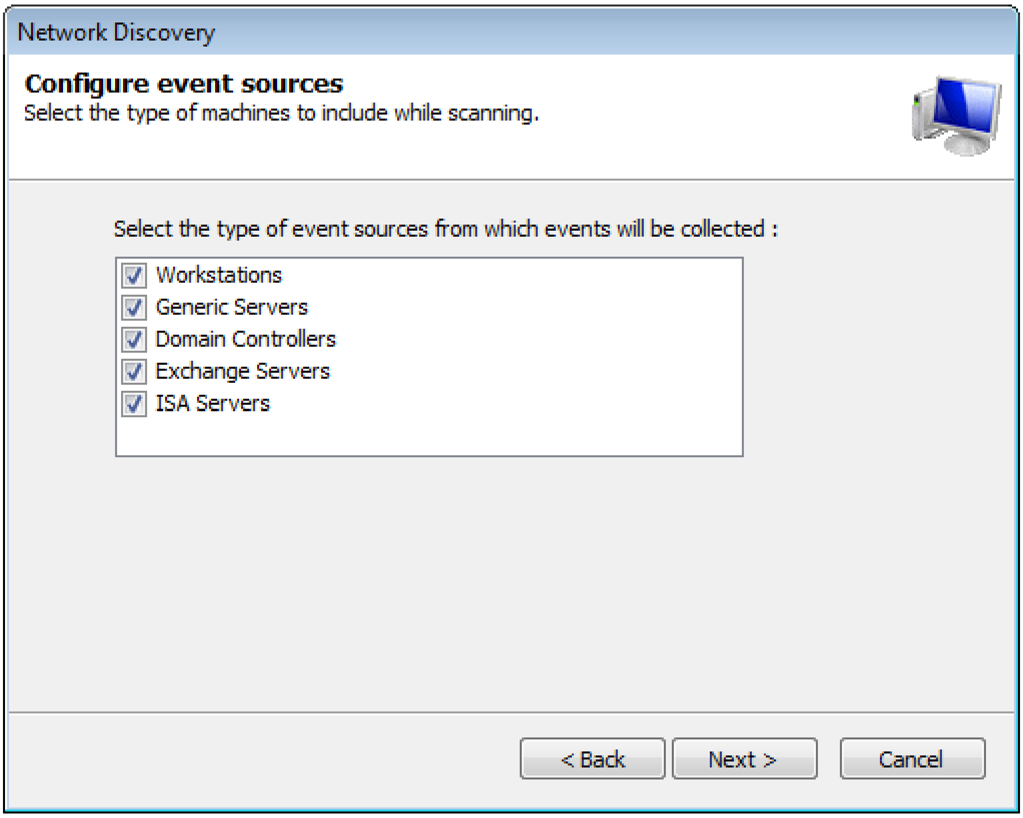
To process event from computers on the same domain/workgroup:

1. Open the GFI EventsManager Quick Launch Console. In the welcome page, click **Process events - Local domain**. This opens the **Automatic Network Discovery** wizard.

Note

The wizard can also be launched from **Configuration** tab > **Event Sources**. From the left pane, right-click **All event sources** and select **Scan local domain**.

2. Click **Next** at the wizard welcome screen.



Network Discovery

Configure event sources

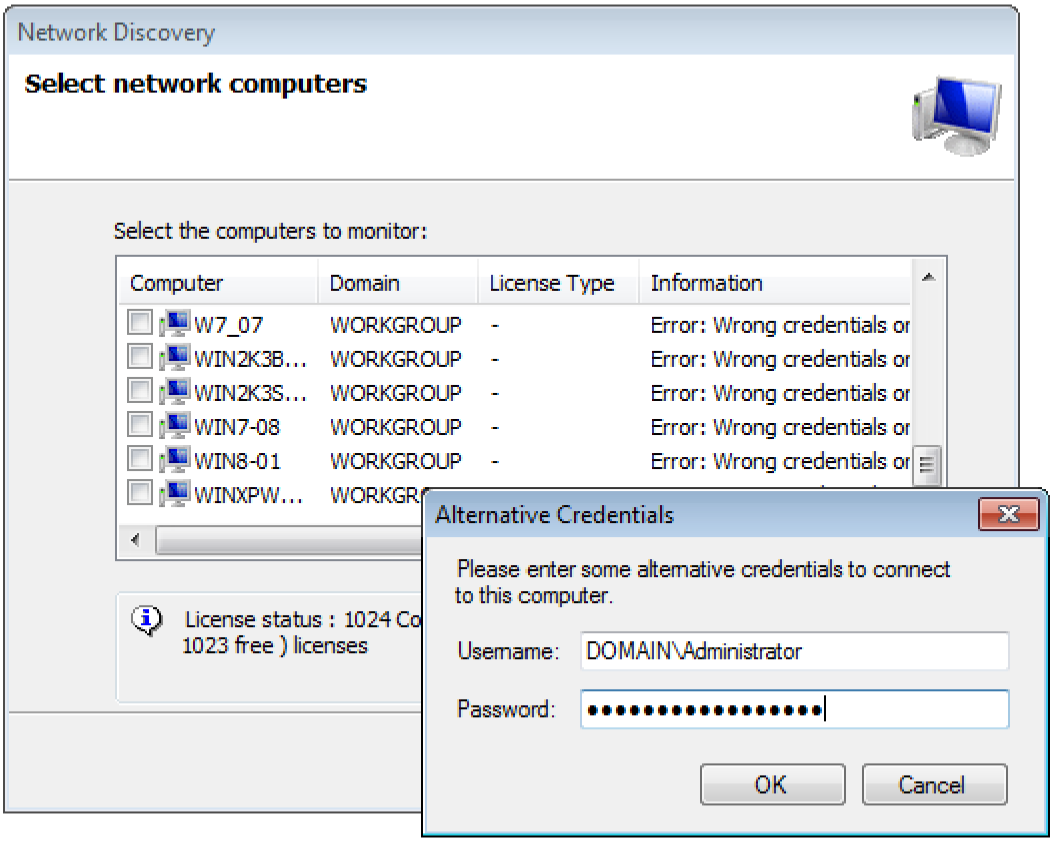
Select the type of machines to include while scanning.

Select the type of event sources from which events will be collected :

- ☑ Workstations
- ☑ Generic Servers
- ☑ Domain Controllers
- ☑ Exchange Servers
- ☑ ISA Servers

Screenshot 29: Select event source types to detect on your network

3. Select the type of event sources that the wizard will attempt to detect on your network. Click **Next**.



Network Discovery

Select network computers

Select the computers to monitor:

Computer	Domain	License Type	Information
□ W7_07	WORKGROUP	-	Error: Wrong credentials or
□ WIN2K3B...	WORKGROUP	-	Error: Wrong credentials or
□ WIN2K3S...	WORKGROUP	-	Error: Wrong credentials or
□ WIN7-08	WORKGROUP	-	Error: Wrong credentials or
□ WIN8-01	WORKGROUP	-	Error: Wrong credentials or
□ WINXPW...	WORKGR		

License status : 1024 Co
1023 free) licenses

Alternative Credentials

Please enter some altemative credentials to connect to this computer.

Usemame: DOMAIN\Administrator

Password: ●●●●●●●●●●●●●●●●●

Screenshot 30: Search network progress

> **Note**
>
> If GFI EventsManager detects computers that cannot be logged onto using the supplied credentials, it enables you to specify alternate logon credentials for each computer you select.

4. Select a computer from the list and key in the username and password. Click **OK** to close the **Altemative Credentials** dialog. Repeat this step until all the required sources are added.

5. Click **Next** and **Finish**.

> **Note**
>
> To automatically add new computers that are joined to the same domain/workgroup as GFI EventsManager, you must configure Synchronization Options.

3.3 How to process events for Selected machines

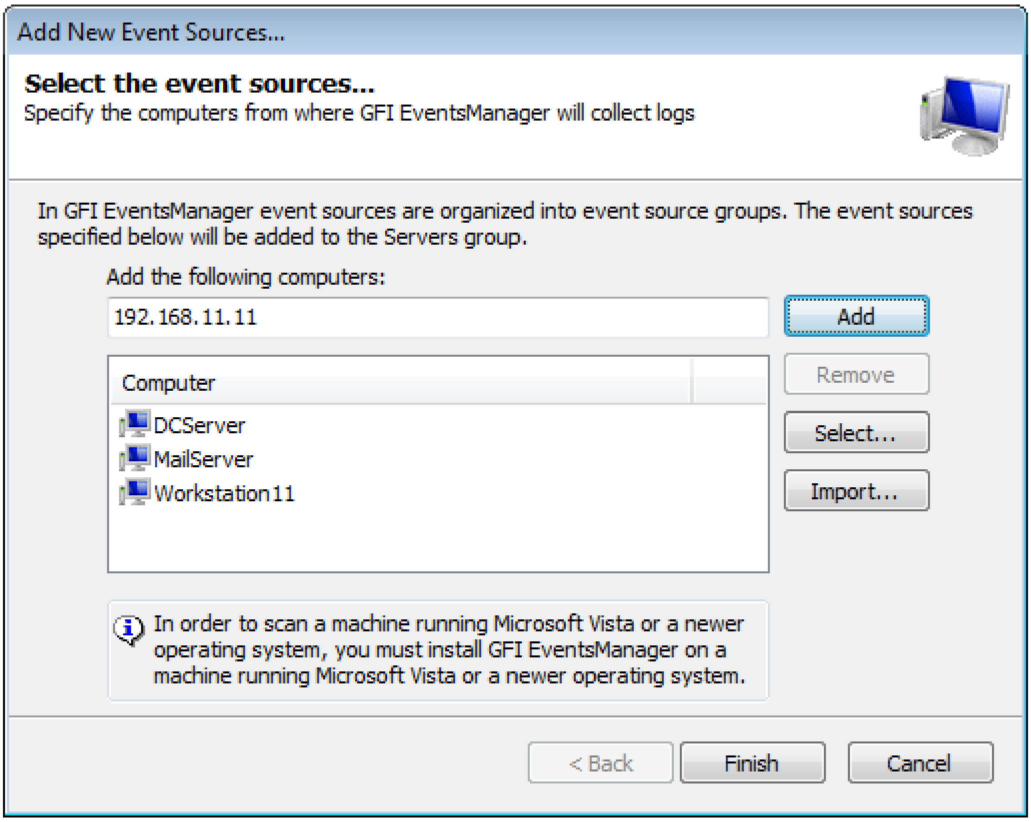
This option enables you to add specific computers manually, by:

- Keying in computer names and IPs
- Selecting computers from reachable domains and workgroups
- Importing computers from a text file containing a single computer name per line.

To process events of selected machines:

1. Open the GFI EventsManager Quick Launch Console. In the welcome page, click **Process events - Selected machines**.

2. This opens the **Add New Event Source** dialog.



Add New Event Sources...

Select the event sources...

Specify the computers from where GFI EventsManager will collect logs

In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the Servers group.

Add the following computers: 192.168.11.11

Computer
DCServer
MailServer
Workstation11

In order to scan a machine running Microsoft Vista or a newer operating system, you must install GFI EventsManager on a machine running Microsoft Vista or a newer operating system.

Screenshot 31: Add new event source wizard

3. The following table describes the available options:

Option	Description
Add	Key in the computer name or IP address in the **Add the following computers** field. Click **Add** to add the specified computer to the **Computer** list. Repeat this step until you add all the event sources to the selected group. **Note** Since Syslog and SNMP traps use IP addresses to determine the source of an event, it is recommended to use the source IP address instead of the computer name when adding Syslog and SNMP Traps sources.
Remove	Select one or more computers from the **Computer** list and click **Remove** to delete them from the list.

Option	Description
Select...	Click **Select...** to launch the **Select Computers...** dialog: 1. From the **Domain** drop-down menu, select the domain you want to scan for available sources and click **Search**. 2. From the search results list, select the computers you want to add. 3. Click **OK** to close the **Select Computers...** dialog and return to the **Add New Event Sources...** dialog.
Import...	Click **Import...** to import computers from a text file. Ensure that the text file contains only one computer name or IP address per line.

4. Click **Finish** to finalize your settings. GFI EventsManager immediately attempts to scan the added event sources, using the default logon credentials.

> **Note**
>
> If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add events sources. To launch **Network Discovery Wizard**, right-click **All event sources** from the event sources tree and select **Scan local domain**.

> **Note**
>
> To confirm that logs are successfully processed, go to **Status** tab **> Job Activity** and check that there are activity logs under the **Operational History** section.

4 Troubleshooting

Use the information in the following sections to resolve issues encountered in GFI EventsManager:

- Documentation
- GFI Knowledge Base
- Request technical support
- Web forum

4.1 Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

4.2 GFI Knowledge Base

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI Knowledge Base always has the most up-to-date listing of technical support questions and patches. In case the information in this guide does not solve your problems, next refer to GFI Knowledge Base by visiting: http://kb.gfi.com/.

4.3 Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

> **Note**
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

User to user technical support is available via the GFI web forum. Access the web forum by visiting: http://forums.gfi.com

5 Glossary

A

Actions

The activity that will be carried out as a result of events matching specific conditions. For example you can trigger actions whenever an event is classified as critical. Actions supported by GFI EventsManager include Email alerts, event archiving and execution of scripts.

Alerts

Notifications which inform recipients that a particular event has occurred. GFI EventsManager can generate Email alerts, SMS alerts and Network alerts.

Archive

A collection of events stored in the SQL Server based database backed of GFI EventsManager.

Audit account management

Generates events when account management operations are done such as create/delete a user account or group, enable/disable a user account and set/change a user password. For more information, refer to http://technet.microsoft.com/en-us/library/cc737542(WS.10).aspx

Audit process tracking

Generates events which track actions such as programs which are launched, closed, as well as other indirect object access information which contain important security information. For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(WS.10).aspx

Audit system events

Generates events when important system events happen such as user restarts or shuts down the target computer or when an event occurs that affects the security log. For more information, refer to http://-technet.microsoft.com/en-us/library/cc782518(WS.10).aspx

C

COM+ Network Access

Enable this firewall permission to allow client machines to access applications or services that resides on the server. This allows GFI EventsManager to access resource from all servers. For more information about this permission, refer to http://technet.microsoft.com/en-us/library/cc731967.aspx

E

Email alerts

Email notifications which inform recipients that a particular event has occurred. To enable email alerts, you must have access to an active mail server.

Event classification

The categorization of events as Critical, High Medium, Low or Noise.

Event logs

A collection of entries which describe events that occurred on the network or on a computer system. GFI EventsManager supports different types of event logs including: Windows Event Log, W3C Logs, Syslog, SNMP Traps and SQL Server audit events.

Event processing rules

A set of instructions which are applied against an event log.

F

File and Printer sharing

Enable this firewall permission to allow GFI EventsManager to access events definitions on target machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc779133 (WS.10).aspx

I

Internet Protocol Security

A framework of open standards used to encrypt and authenticate network packets during a communication session between computers. Using cryptography services, IPsec ensures data integrity, authentication and confidentiality.

IPsec

Internet Protocol Security is a framework for a set of protocols for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the Application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

M

Management Information Base

A MIB is the equivalent of a data dictionary or codebook. It associates object identifiers (OIDs) with a readable label and various other parameters related to an active network object such as a router. Its main function is to assemble and interpret SNMP messages transmitted from SNMP-enabled network devices. The information stored in MIBs is organized hierarchically and is normally accessible using a protocol such as SNMP.

N

Network alerts

Network messages (known as Netsend messages) which inform recipients that a particular event has occurred. These messages are sent through an instant messenger system/protocol and are shown as a popup in the system tray of the recipient's desktop. To setup network alerts, you must specify the name or IP of the computers where the Netsend messages will be sent.

Network discovery

Enable this firewall permission to allow GFI EventsManager to gather information about connected machines on the network that can be scanned. For more information, refer to http://-technet.microsoft.com/en-us/library/cc181373.aspx

Noise

Repeated log entries which report the same event.

O

Object auditing

Enable this auditing feature to audit events of users accessing objects (example, files, folder and printer). For more information, refer to http://technet.microsoft.com/en-us/library/cc976403.aspx

R

Remote Event Log Management

Required to allow GFI EventsManager to access and collect events from remote machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc766438.aspx

Rule-set folder

The folder which contains one or more rule-sets.

Rule-sets

A collection of event processing rules.

S

SMS alerts

SMS notifications which inform recipients that a particular event has occurred. In GFI EventsManager, SMS alerts can be sent through various sources including mobile phones with modem capabilities and email-to-SMS web-based gateways.

SNMP Object Identifier (OID)

An SNMP object identifier is an address made up of a sequence of 'dotted' numbers (Example: 1.3.6.1.4.1.2682.1). These numbers uniquely identify and locate a specific device (Example: hub) within the entire network. SNMP OIDs are a key component in the assembly of SNMP messages. In fact, an SNMP server cannot interpret or assemble messages which don't have an OID. Individual vendors often create their own MIBs that only include the OIDs associated specifically with their device.

SNMP Traps

Notifications/alerts generated and transmitted by active network components (Example: hubs, routers and bridges) to SNMP server(s) whenever important events such as faults or security violations occur. Data contained in SNMP Traps may contain configuration, status as well as statistical information such as number of device failures to date.

Syslog messages

Notifications/alerts most commonly generated and transmitted to a Syslog server by UNIX and Linux-based systems whenever important events occur. Syslog messages can be generated by workstations, servers as well as active network devices and appliances such as Cisco routers and Cisco PIX firewalls to record failures and security violations amongst other activities.

U

Unclassified events

Events that did not satisfy any of the event processing conditions configured in the event processing rules.

W

W3C logs

W3C is a common log format developed by the World Wide Web Consortium. W3C logs are text-based flat files used mainly by web servers including Microsoft Internet Information Server (IIS) to record web related events such as web logs.

Windows Event Logs

A collection of entries which describe events that occurred on a computer system running Windows OS.

6 Index