

Installation

Introduction

Where can I install GFI EventsManager on my network?

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network.

Use GFI EventsManager to manage the events generated:

- On the same computer where it is installed
- On all the computers that are reachable from the computer on which it is installed.

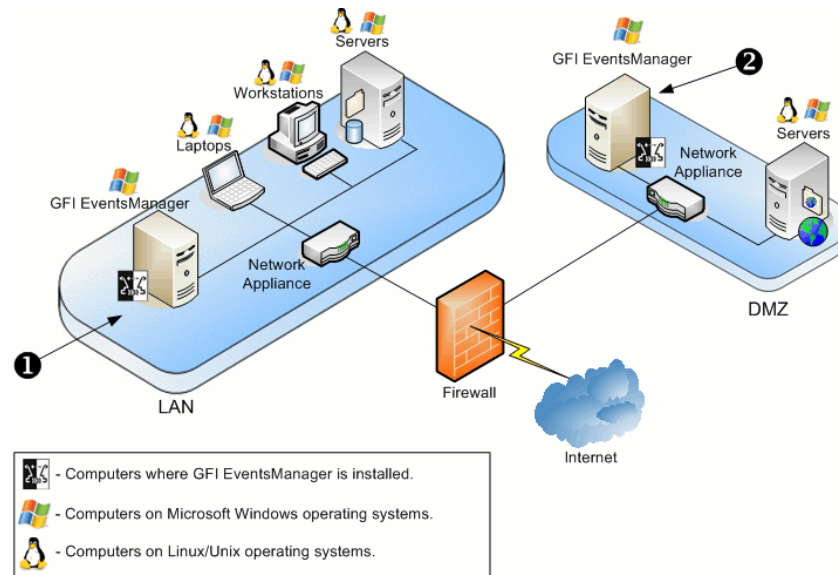


Figure 3 – GFI EventsManager deployment scenario

GFI EventsManager can be deployed:

- 1 Within your network to monitor the activity of internal servers and workstations/end points.
- 2 On the DMZ to monitor and manage the events generated on your servers.

Deployment of GFI EventsManager on a local area network

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

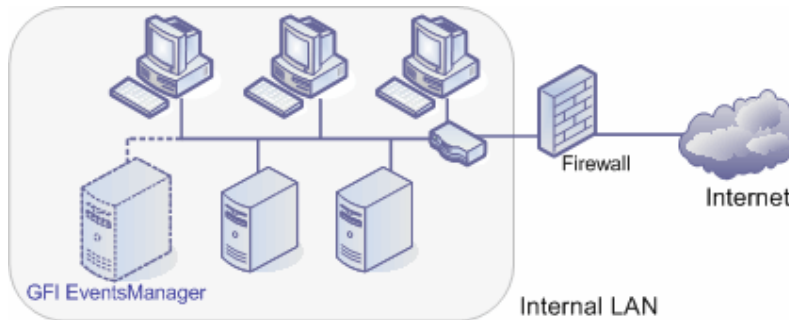


Figure 4 - Deployment of GFI EventsManager on LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows events, W3C event logs, Syslog messages, SNMP Trap and SQL Server audit messages generated by any hardware or software that is connected to the LAN, including:

- Workstations and Servers (e.g. Apache web-servers)
- Network appliances (e.g. Cisco PIX firewalls)
- Third party software (e.g. GFI EndPointSecurity)
- Specialized Services (e.g. Microsoft Internet Information Server - IIS)
- PABXs, Keyless Access Systems, Intrusion detections systems, etc.

When installed on a LAN, GFI EventsManager can also be used to collect events from hardware and software systems deployed on a Demilitarized Zone (DMZ). Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

1. 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: <http://kbase.gfi.com/showarticle.asp?id=KBID002770>.
2. That GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

Deployment of GFI EventsManager on a demilitarized zone

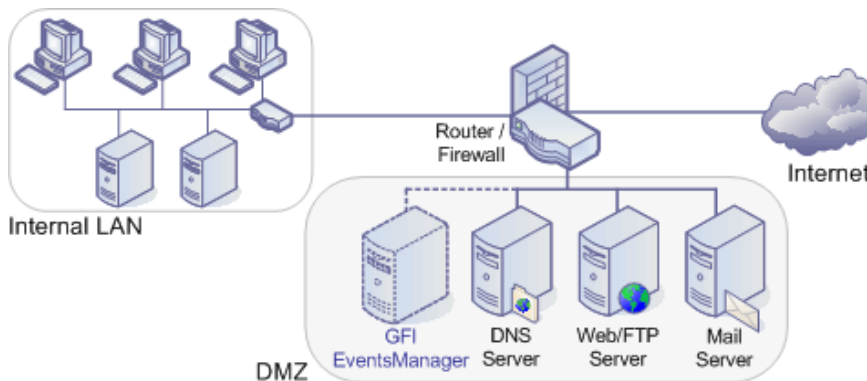


Figure 5 - The DMZ sits between the internal LAN and the Internet

GFI EventsManager can also be deployed on a Demilitarized Zone (DMZ). This is the neutral network which sits between the “internal”

corporate network and the “outside world” (i.e. the internet). The deployment of GFI EventsManager on a DMZ helps you automate the management of events generated by DMZ hardware and software systems.

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:

- 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 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 network appliance events

Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (e.g. Cisco IOS series routers) 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.

Managing Microsoft Windows Vista & Windows Server 2008 events

Microsoft Windows Vista and Windows Server 2008 introduced extensive structural changes in event logging and event log management mechanisms. 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.
- The introduction of event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- A new file format (evtx) that replaces the old evt file format.

NOTE 1: To collect and process Microsoft Windows Vista events, GFI EventsManager must be installed on a system running Microsoft Windows Vista.

NOTE 2: To collect and process Microsoft Windows Server 2008 events, GFI EventsManager must be installed on a system running Microsoft Windows Server 2008.

Hardware requirements

- Processor: 2.5 GHz or higher processor clock speed
- RAM: 1024 MB
- Hard disk: 2 GB of available space
- Others: Keyboard and mouse or compatible pointing device.

Software requirements

Software requirements - Installation machine(s)

- Microsoft Windows 2008, 2003 (SP2), 2000 (SP4), XP (SP2), VISTA
- .NET framework 2.0
- Microsoft Data Access Components (MDAC) 2.8+ or later
- Microsoft SQL Server (including access to Microsoft SQL Server Native Client, SQL Server Management Objects with SQL Profiler components)

Software requirements - Scanned machine(s)

- For Microsoft Windows event log scanning:
 - Remote registry service must be enabled.
 - Windows audit service must be enabled.
 - VISTA machines must be within the same domain as the scan server as well as have UAC disabled. For details on how to turn off UAC refer to <http://technet2.microsoft.com/WindowsVista/en/library/0d75f774-8514-4c9e-ac08-4c21f5c6c2d91033.mspx?mfr=true>.
- W3C log scanning:
 - The source folders must be accessible via Windows shares.
- Syslog and SNMP Traps:
 - Sources/senders must be configured to send messages to the computer/IP address where GFI EventsManager is installed.

Upgrading from a previous version

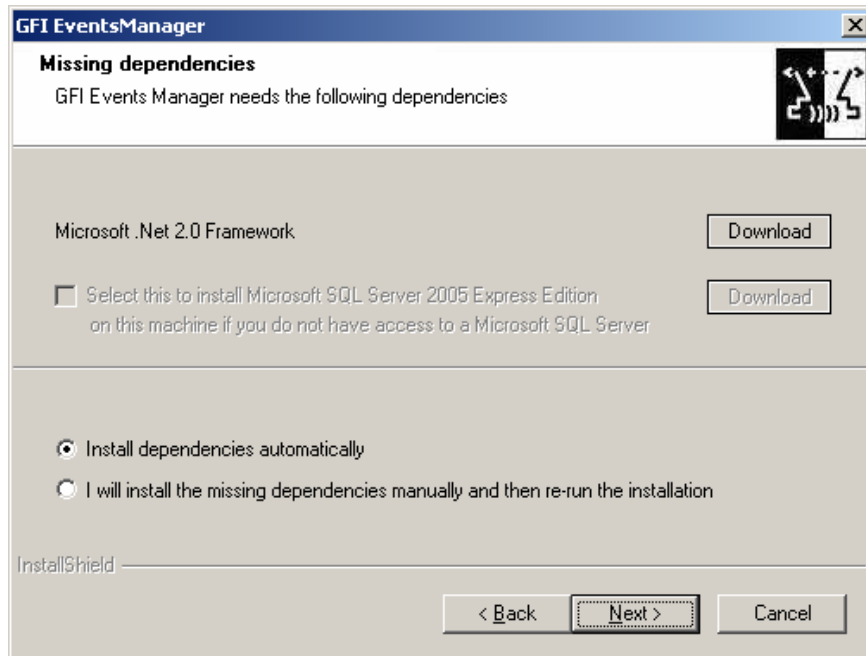
Upgrading from version 7.0 or version 7.1 of GFI EventsManager to GFI EventsManager version 8 is fully supported. To upgrade to GFI EventsManager 8, follow the installation procedures provided in the installation procedure section within this chapter of the user manual

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

Installation procedure

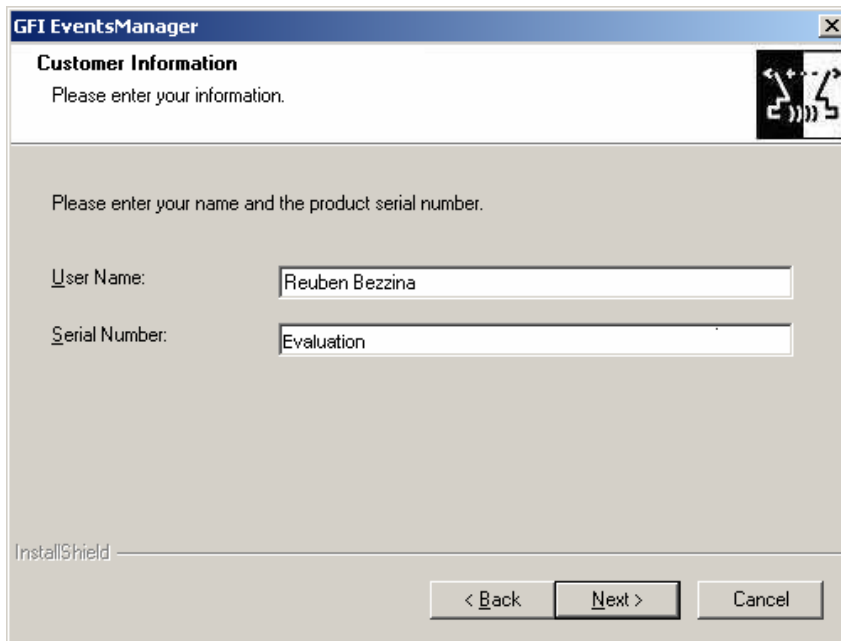
GFI EventsManager includes an installation wizard which will assist you through the installation process. To start the installation:

1. Close all running applications and log-on the target computer using an account which has local administrative privileges.
2. Double-click on **eventsmanager8.exe**.



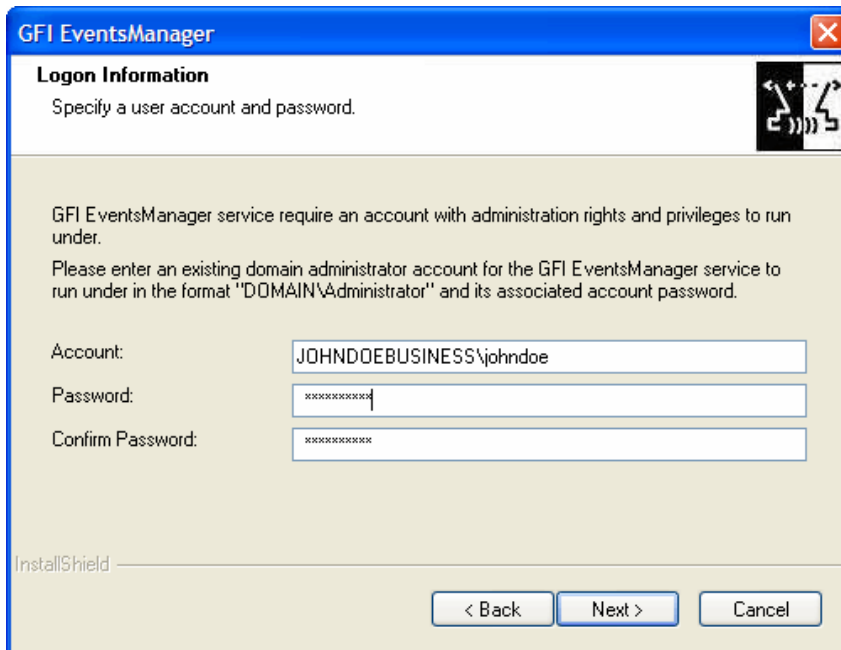
Screenshot 2 – Missing dependencies dialog

3. If GFI EventsManager detects that the basic dependencies are not present, a dialog will outline the missing dependency or dependencies and you will be allowed to install the missing dependencies manually or automatically.
4. As soon as the welcome dialog is displayed, click **Next** to start the installation.
5. Read the licensing agreement carefully. To continue installing the product, select the 'I accept the Licensing agreement' option and click **Next**.



Screenshot 3 - Customer and License detail screen

6. Specify your name and license key. If you are evaluating the product, leave the license key as default (i.e. **'Evaluation'**) and click **Next**.



Screenshot 4 - Logon information screen

7. GFI EventsManager must run under an account which has domain administrative privileges. Enter the user name and password of domain administrator account and click **Next** to continue.

8. Specify an alternative installation path or click on **Install** to leave as default and proceed with the installation.

9. Click **Finish** to finalize the installation.