

Deploying GFI LANguard S.E.L.M.

Design overview & deployment strategies

This white paper gives an overview of how GFI LANguard S.E.L.M. works and discusses installation and deployment issues, enabling you to choose the best way to deploy the product on your network.

Introduction

This white paper gives an overview of how GFI LANguard S.E.L.M. works and discusses installation and deployment issues, enabling you to choose the best way to deploy the product on your network.

Introduction.....	2
GFI LANguard S.E.L.M. design.....	2
Deployment considerations	3
Deployment examples.....	5
GFI LANguard S.E.L.M. connector.....	8
Deployment FAQ/issues.....	8
About GFI LANguard Security Event Log Monitor (S.E.L.M.)	9
About GFI	9

GFI LANguard S.E.L.M. design

The main design concept behind GFI LANguard S.E.L.M. is to make event log monitoring possible without installing an agent or client on each machine to be monitored. This way, the administrator can avoid a lot of extra configuration and maintenance.

GFI LANguard S.E.L.M. has operational components (services not visible to the user) and user interface components. By default, both are installed but it is possible to install only the operational components (except if you use Microsoft Access as a backend). Here is a list of the components that are installed:

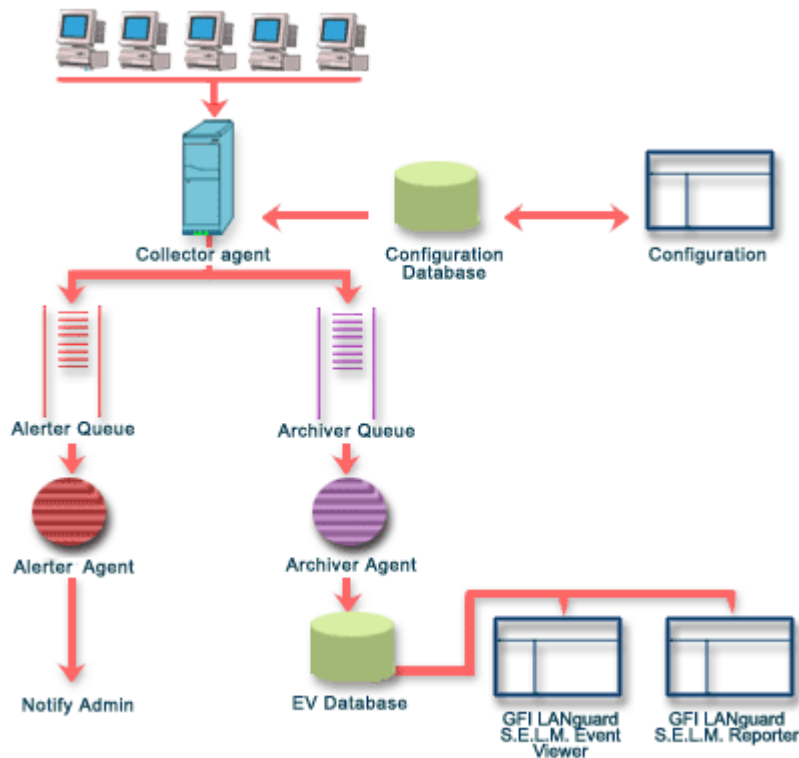
Operational components (not visible/accessible by the user)

1. GFI LANguard S.E.L.M. collector agent service
2. GFI LANguard S.E.L.M. alerter agent service
3. GFI LANguard S.E.L.M. archiver agent service.

User interface components (visible/accessible by the user)

1. GFI LANguard S.E.L.M. Configuration MMC snap-in
2. GFI LANguard S.E.L.M. Event Viewer MMC snap-in
3. GFI LANguard S.E.L.M. Reporter MMC snap-in
4. GFI LANguard S.E.L.M. support tools.

The image below shows how GFI LANguard S.E.L.M. components work together.



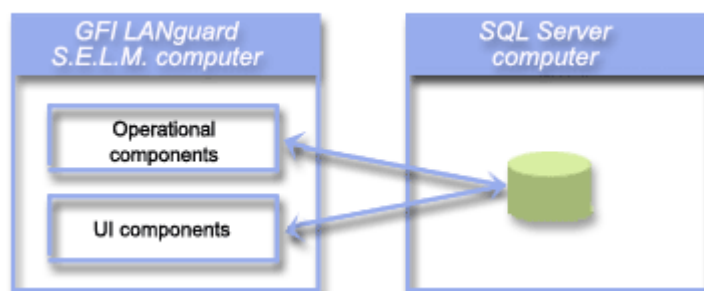
Overview of how GFI LANguard S.E.L.M. works

Deployment considerations

Choice of database backend

During installation, you can select the type of database backend GFI LANguard S.E.L.M. must use. The database backend can either be an

1. MS Access Database
2. SQL database using MS SQL Server, or
3. SQL database using MSDE (Lightweight, free version of MS SQL).



When GFI LANguard S.E.L.M. uses MS SQL Server as a database backend, that SQL Server need not be located on the same machine as GFI LANguard S.E.L.M. Also, if using SQL or MSDE, you can have multiple GFI LANguard S.E.L.M.s writing to the same SQL backend. The advantage of this is that, in large networks, you can deploy multiple collectors/analyzers but still have one consolidated database of events.

For small sites where low information volume is to be collected, GFI LANguard S.E.L.M. can be configured to use the MS Access database as a backend.

When the information size grows, then GFI LANguard S.E.L.M. should be configured to use an MS SQL Server as a backend. MS SQL Server allows for better scalability, management of the database as well as increased performance.

Single/multiple domain environment

If you have multiple domains, then we recommend – both for bandwidth and security reasons – that you have at least one GFI LANguard S.E.L.M. installation for each domain. Each installation would write to its own database backend. If you want to connect these databases to one single database, use the GFI LANguard S.E.L.M. connector.

Ports and protocols used by GFI LANguard S.E.L.M.

GFI LANguard S.E.L.M. uses RPC over SMB to retrieve events, and therefore requires ports 445 and 139 to communicate with the target machine. (If GFI LANguard S.E.L.M. is using its WAN Connector - which uses DTS in order to retrieve the data - or a SQL Server database, then it also requires the SQL port, which by default is 1433.) This traffic is secured by default using Windows 2000/XP Kerberos or Windows NT LM2. Therefore, the traffic and the event data cannot be tampered with. Traffic from the queried machine travels back to the original machine on the initial source port.”

Computer identification considerations

GFI LANguard S.E.L.M. identifies computers via computer name or IP. If NETBIOS-compatible computer names are used, you have to ensure that your DNS service is properly configured for name resolutions. Unreliable name resolution will downgrade system performance dramatically. Note that if you disable NETBIOS over TCP/IP, you can still use GFI LANguard S.E.L.M.,

however you must specify computer name by IP.

Bandwidth considerations for GFI LANguard S.E.L.M.

Retrieving a single event from a machine costs approximately 300 bytes of data. A machine configured with the recommended GFI LANguard S.E.L.M. auditing policies will generate approximately 10 events per day. So a machine, that is not being intruded, being monitored by GFI LANguard S.E.L.M will generate 3kb of traffic per day on the network. On a modern network, this is peanuts.

NOTE: Although much text is displayed in the event log records, only the parameters required to compose that message are transferred between the host computer and the target computer. Language-independent strings are not transferred and that greatly reduces the information being passed over the communication line between the two machines.

Deployment examples

1 - For smaller single domain networks

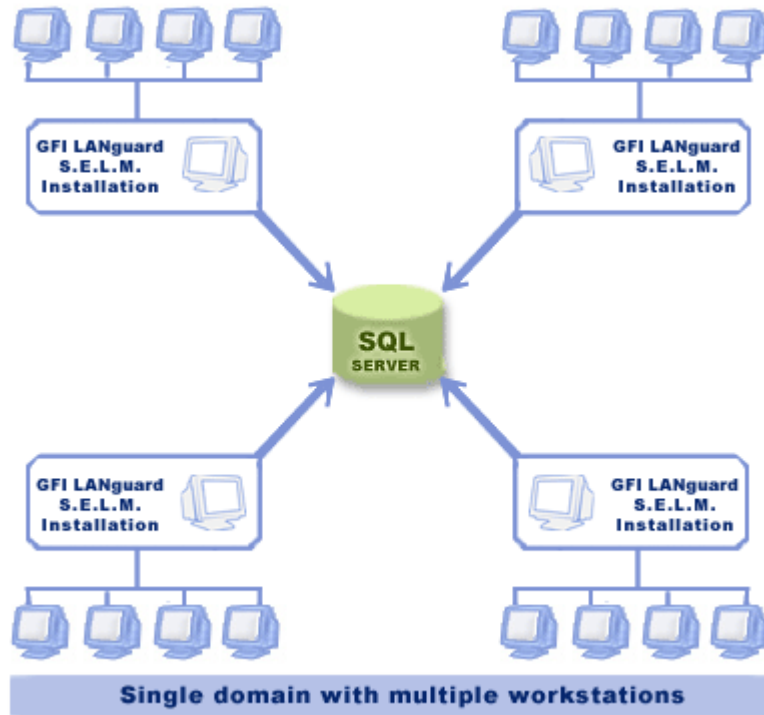
For networks of up to 300 machines, for example 10 servers and 290 workstations, a single GFI LANguard S.E.L.M. installation with Access or SQL backend is sufficient.

As a general rule, if you want to monitor a server in real time, then one GFI LANguard S.E.L.M. installation per 15 servers is recommended. You can monitor workstations every hour, in which case one installation of GFI LANguard S.E.L.M. can handle up to 200 workstations as long as the importance level of a server is set as higher than the importance level of a workstation.

2 - For larger, single domain networks

If you have a larger network, for example 50 servers and 1,000 workstations, it is best to deploy multiple GFI LANguard S.E.L.M. installations. In order to keep data centralized, we recommend using a single SQL server as a backend and having each GFI LANguard S.E.L.M. installation write to the same SQL server backend.

For 50 servers and 1,000 workstations, for example, you can use 5 GFI LANguard S.E.L.M. installations, each monitoring 10 servers and 200 workstations, writing to the same SQL database.



Deployment in larger networks

3 - A large multi-site, multi-domain WAN network

If you have a multi-site (geographical site) and therefore probably a multi-domain network, we recommend that you install a GFI LANguard S.E.L.M. installation in each site. Optionally, this installation can act as a satellite server to the main parent GFI LANguard S.E.L.M. installation using the GFI LANguard S.E.L.M. connector.

By way of example, suppose you have a network of 4,370 machines, spread over 4 sites, each site being a separate domain, as follows:

- St Paul - 250 computers to be monitored
- Kansas City - 100 computers to be monitored
- Chicago - 4000 computers to be monitored
- Columbus - 20 computers to be monitored

You would need at least 4 installations, one for each domain. However, the Chicago domain has many computers. We recommend a maximum of 300 computers to be monitored, meaning that in Chicago you would need 14 GFI LANguard S.E.L.M. installations. Each installation would monitor a separate set of computers. Therefore:

- St Paul - 1 Installation
- Kansas City - 1 Installation

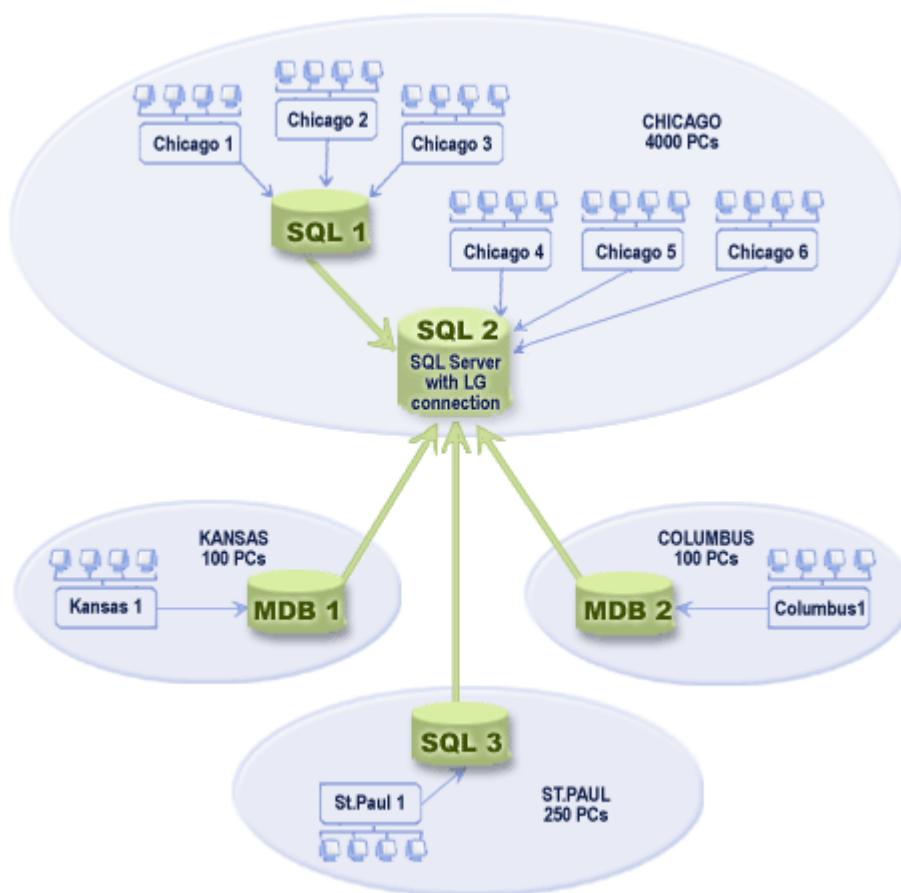
- Chicago - 14 installations
- Columbus - 1 installation

Assuming that Chicago has a fast network, all the installations write to the same database. If the network is not that fast, you could consider having 2 SQL database backends.

In the smaller sites, like Columbus and Kansas City, one can easily use MS Access as a database backend and save on the license cost of SQL server.

NOTE: GFI LANguard S.E.L.M. has minimal impact on the performance of the machine it is installed on. Also, it uses a minimal amount of bandwidth.

The resulting set-ups would look as indicated below, 14 installations in the Chicago site (although only six are shown), and one for St. Paul, Kansas and Columbus.



Deployment over a large multi domain wan network

Because GFI LANguard S.E.L.M. allows you to install only the 'operational components', you can install it pretty much invisibly on some segments of the network - not only to reduce

administration, but possibly also for security reasons. A GFI LANguard S.E.L.M. installation without configuration or reporting tools would make it more difficult to tamper with the configuration or the data being collected.

GFI LANguard S.E.L.M. connector

The GFI LANguard S.E.L.M. connector was designed specifically for multiple domain/geographical sites. The connector 'connects' the various database backends to a single data source, allowing you to consolidate all/part of the collected security data into a single database on which you can run reports.

With the GFI LANguard S.E.L.M. connector, you can specify that other GFI LANguard S.E.L.M. installations become a satellite server for the main parent server. The GFI LANguard S.E.L.M. connector will retrieve all relevant data from the database of the satellite servers and consolidate them into one database. It can do this based on filters, so that you can filter the data you want to centralize and reduce bandwidth and storage consumption.

Deployment FAQ/issues

What if I want to use a mixture of MS Access and SQL database backends? Can I still consolidate the data into a central database?

Yes you can. The GFI LANguard S.E.L.M. connector can collect events from the satellite servers and merge them into a central GFI LANguard S.E.L.M. database. You can configure the connector to filter the event information you specify.

On which operating systems can GFI LANguard S.E.L.M. be installed?

GFI LANguard S.E.L.M. can be installed on any of the following operating systems:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2003 Server
- Windows XP Professional.

Does GFI LANguard S.E.L.M. need a dedicated machine?

GFI LANguard S.E.L.M. does not necessarily require a dedicated computer. It can quite happily retrieve data in the background from up to 250 computers. The resource usage of GFI LANguard S.E.L.M. is very low. Instead of dedicating a machine, it is better to separate the load over multiple GFI LANguard S.E.L.M. installations if you have large network.

About GFI LANguard Security Event Log Monitor (S.E.L.M.)

GFI LANguard Security Event Log Monitor (S.E.L.M.) performs event log based intrusion detection and network-wide event log management. GFI LANguard S.E.L.M. archives and analyzes the event logs of all network machines and alerts you in real time to security issues, attacks and other critical events. GFI LANguard S.E.L.M.'s intelligent analysis means you do not need to be an 'Event Guru' to be able to: Monitor users attempting to access secured shares and confidential files; Monitor critical servers and create alerts for specific events and conditions occurring on your network; Back up and clear event logs automatically on remote machines; Detect attacks using local user accounts; and much more!

For more info on GFI LANguard S.E.L.M. and to download your free trial, please visit <http://www.gfi.com/lanselm/>.

About GFI

GFI is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong, Adelaide, Hamburg and Cyprus which support more than 160,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at <http://www.gfi.com>.

© 2006 GFI Software Ltd. All rights reserved. The information contained in this document represents the current view of GFI on the issues discussed as of the date of publication. Because GFI must respond to changing market conditions, it should not be interpreted to be a commitment on the part of GFI, and GFI cannot guarantee the accuracy of any information presented after the date of publication. This White Paper is for informational purposes only. GFI MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT. GFI, GFI EndPointSecurity, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor and their product logos are either registered trademarks or trademarks of GFI Software Ltd. in the United States and/or other countries. All product or company names mentioned herein may be the trademarks of their respective owners.

