GFI LanGuard™

Network security scanner and patch management

SmartGuide

This SmartGuide is an important tool to enhance your success with the GFI LanGuard® product.

GFI®

Welcome to GFI LanGuard: GFI LanGuard is an all-in-one solution for patch management, vulnerability scanning and network auditing.

Introduction

This SmartGuide is designed to give a high level overview of what GFI LanGuard is, what it does, how to effectively use the power of GFI LanGuard. This is an important tool to help plan a successful deployment.
This SmartGuide includes the following:

- **GFI LanGuard product overview**
- **Why customers purchase GFI LanGuard**
- **Five (5) major topics to consider before deploying GFI LanGuard**
- **How to keep your computers secure and up-to-date**
- **Examples of GFI LanGuard reports.**

With this guide and a little planning ahead of time, you will be able to deploy an efficient and easy-to-maintain environment. Please take the time to review this document before installing the product.

For additional detailed documentation you can reference GFI's knowledgebase called SkyNet (**kb.gfi.com**) and the **GFI LanGuard documentation**.

If, after reading the SmartGuide, you have questions about any of the issues raised in this document, please **contact our support organization** or **create a support ticket**.

GFI LanGuard product overview

GFI LanGuard is a comprehensive network management solution. It acts as a virtual security consultant helping in the following areas: **patch management, vulnerability checking, network and software auditing, asset inventory, risk analysis and compliance**. Simply stated, GFI LanGuard:

- **Scans, detects, assesses and helps rectify security vulnerabilities** on the network
- **Scans for missing non-security patches, security patches, service packs and more**
- **Has powerful reporting** to identify issues and lock down the network against hackers
- **Provides a complete network security overview with minimal administrative effort**.

GFI LanGuard **scans, analyzes and helps remediate** your network.

- Either agent-based or agent-less, GFI LanGuard **scans** the network for security related issues and gathers security relevant information. It gathers information about security vulnerabilities, missing patches, missing service packs, open ports, open shares, users and groups, installed applications and hardware inventory. GFI LanGuard integrates with over 2,500 security applications such as antivirus, anti-spyware or firewalls and reports on their status.
- With the results of the scans you can then **analyze** the status of your network. GFI LanGuard provides a powerful dashboard to browse and investigate the scan results. Security sensors are triggered when issues are detected. A vulnerability level is assigned to each scanned computer based on the items found during the audit. GFI LanGuard also provides reports and results comparisons.
- After scanning and analyzing, GFI LanGuard assists to **remediate** the security issues, automating the process where possible.
- After creating a baseline scan, you can identify any differences or changes to the security and computer configurations of all the computers in the network. You can decide to take such actions as to deploy missing Microsoft® and non-Microsoft updates, rollback updates, deploy custom software and scripts, uninstall unauthorized applications, open remote desktop connections to scanned computers, etc. All of these actions will help to ensure your network is up-to-date and the latest security patches are applied.

Why customers purchase GFI LanGuard

Based on our experience, below are the top four reasons GFI customers purchase GFI LanGuard:

1. To **minimize the risk of security breaches** by:
    a. scanning the network for security and vulnerability issues
    b. automatically detecting and uninstalling any unauthorized applications
    c. auditing software (which PCs have what software) and hardware devices on the network
    d. receiving alerts and reports regarding the security environment of the network
2. To **automate patch management** – detect and deploy missing patches for Microsoft and Mac OS® X operating systems and Microsoft, Mac and other third party applications
3. To conduct **network auditing and network health monitoring**
4. To aid with **compliance for security regulations** that require regular vulnerability assessment and patch management (e.g., PCI DSS, HIPAA, GCSx CoCo, SOX, GLB/GLBA, etc.).

Before deploying GFI LanGuard

There are five major aspects of GFI LanGuard to consider before deployment. It is important that you understand each of them so, if after reading the sections below you have any questions or want to discuss any of them, please **contact us.**

1. **Licensing GFI LanGuard**
2. **System installation requirements**
3. **Scanning profiles – what you need to know**
4. **Choosing the right database**
5. **Scanning and performance tips**

1. Licensing GFI LanGuard

GFI LanGuard is licensed based on the number of active ("Active") IPs* you are scanning.
For example:

- » If you have an IP range of 192.160.1.1 through 192.160.1.254.
- » And you have 20 Active IPs in that range that you want to scan, you only have to license the 20 Active IPs.
- » However, it is important to note that if there are more than 20 Active IPs in that range, AND you only license 20 IPs in GFI LanGuard, you will only be scanning the first 20 Active IPs (hence any Active IP beyond the 20 will not be scanned).

* An "Active" IP is defined as an IP address that is reachable and available through a connection request sent in the form of NETBIOS queries, SNMP queries and/or ICMP pings.

Note: Network discovery is not bound by license limitations. This means you can discover and have shown in GFI LanGuard an unlimited number of active devices from your network, but you will only be able to scan up to the number allowed by your license.

2. GFI LanGuard system installation requirements

GFI LanGuard has hardware and software requirements that must be met prior to installing GFI LanGuard. The most important of these requirements are listed below and the full set can be found **here**.

System requirements: Hardware

Hardware requirements depend on network size. Refer to table below for the **suggested minimum specifications** according to your network size.

	1 to 100 computers	100 to 500 computers	500 to 3,000* computers	Agent
Processor	2 GHz Dual Core	2.8 GHz Dual Core	3 GHz Quad Core	1 GHz+
Physical Storage	5 GB	10 GB	20 GB	350 MB
Memory	2GB	4 GB	8 GB	25 MB
Network Bandwidth	1544 Kbps	1544 Kbps	1544 Kbps	1544 Kbps

***Note:** If you are looking to manage 2000+ seats of GFI LanGuard, we recommend that you contact us for pricing as well as suggestions regarding the proper management and deployment of this solution.

System requirements: Software

Supported operating systems (x86 or x64)	Supported databases	Other required components
Microsoft Windows Server 2008 Standard/Enterprise Microsoft Windows Server 2003 Standard/Enterprise Microsoft Windows 7 Professional/Enterprise/Ultimate Microsoft Windows Vista Business/Enterprise/Ultimate Microsoft Windows XP Professional (SP2 or higher) Microsoft Small Business Server 2008 Standard Microsoft Small Business Server 2003 (SP1)	Microsoft Access Microsoft SQL Server® 2000 or later MSDE/SQL Server Express Edition	**Other server components:** The following components are required to be installed on the server where GFI LanGuard is installed (they are installed automatically by GFI LanGuard if they are missing): Microsoft .NET Framework 3.5 **Target computer components:** The following components are required to be installed on target computers for GFI LanGuard to be able to scan them: Secure Shell (SSH) - Required for UNIX based scan targets. Commonly included as part of all major Unix/Linux distributions. Windows Management Instrumentation (WMI) - Required to scan Windows-based scan targets. Included in all Windows 2000 or newer operating systems. File and Printer Sharing and Remote Registry need to be enabled

System requirements: Mac OS target computers for patch management

Supported operating systems (x86 or x64)	Other required components
Mac OS X 10.5 (Leopard) Mac OS X 10.6 (Snow Leopard) Mac OS X 10.7 (Lion) Mac OS X 10.8 (Mountain Lion)	Secure Shell (SSH) must be enabled on the target Mac OS machines.

GFI LanGuard agent:

Supported operating system (x86 or x64)	Agent footprint
Microsoft Windows Server 2008 Standard/Enterprise Microsoft Windows Server 2003 Standard/Enterprise Microsoft Windows 7 Professional/Enterprise/Ultimate/ Home Premium Microsoft Windows Vista Business/Enterprise/Ultimate/Home Microsoft Windows XP Professional (SP2 or higher) Microsoft Small Business Server 2008 Standard Microsoft Small Business Server 2003 (SP1) Microsoft Windows 2000 Professional/Server/Advanced	Scanning agent minimum required resources: Agent RAM usage: 25 MB Disk space required: 350 MB

GFI LanGuard relay agent:

GFI LanGuard relay agents act as cache stores for GFI LanGuard program updates and patches, allowing for reduced network bandwidth consumption between the GFI LanGuard server and client computers.
A computer is eligible as relay agent when it has:

- Good uptime (an offline relay agent incapacitates its clients)
- A fast network connection to its clients
- Enough disk space for caching.

System requirements: Hardware

	1 to 100 clients	100 to 500 clients	500 to 1,000 clients
Processor	2 GHz Dual Core	2 GHz Dual Core	2.8 GHz Dual Core
Physical storage	5 GB	10 GB	10 GB
Memory	2 GB	2 GB	4 GB
Network bandwidth	100 Mbps	100 Mbps	1 Gbps

3. Scanning profiles – What you need to know

Out of the box, GFI LanGuard comes with an extensive list of scanning profiles*. A list is available **here**
At the highest level, the three out-of-box categories of profiles are:

a. Complete/combination scans
b. Vulnerability assessment scans
c. Network and software audit scans.

*Scanning profile: A scanning profile is a set of criteria used to define the scan. GFI LanGuard has multiple pre-defined profiles that can be customized and you can also create/customize your own scanning profiles.

4. Database recommendations

Each time a scan is run, the results are stored in a database. There are three types of databases you can use. The choice of database is dependent on: the size of the scanned network, the frequency of the scans and the types of scans (e.g., complete, partial, etc.) you perform:

a. Microsoft Access® (GFI LanGuard includes the Microsoft Access database but does not require having Access installed)
b. MSDE/Microsoft SQL Express Edition
c. Microsoft SQL Server 2000 or later
    i. If you are looking at Microsoft SQL Server to use as your preferred database but are unsure of the licensing requirements, check out the Microsoft SQL licensing information pages SQL 2008, SQL 2005, SQL Express 2008.
    ii. **You may want to consult with Microsoft or your Microsoft partner for advice**.
    iii. The default Microsoft Access scan results database which ships with GFI LanGuard is good for evaluation purposes, but is not recommended for more than five computers. It is less reliable and its size is limited to a maximum of 2GB.

* **NOTE: GFI does not license or represent Microsoft or any of its products. We also do not know all the ins and outs of your internal systems, applications and data. The content in this SmartGuide is here to provide some suggestions on issues to consider when choosing database and hardware requirements on implementing GFI LanGuard. They are strictly provided as a guideline.**

5. Scanning and performance tips

Agent-less scans:

» No installs on client machines
» All processing is done by the central server, no resources from client machines are required
» Work on rough devices and systems where agents are not supported.

Agent-based scans:

» Have better performance due to distributed load across clients
» Work better in low bandwidth environments because the communication between server and clients is much less intensive than in the case of agent-less scans
» Better support of laptops because agents will continue to do their job and when they are online they will just synchronize with the sever
» Improved results accuracy because local scans have access to more information than remote scans.

Relay agents:

» Important in multiple-site or very large installations
» Performance improvements
    • Patches and product definition files reach the remote machines faster
» Bandwidth-saving
    • Recommended to have at least one relay agent for each remote location in geographically distributed networks
    • Each file is copied across the WAN only once per location and computers will get them locally from the relay agent near them.

If performance is an issue and agent-less scans are desired, here are some tips that might help:

- If you are concerned with your network bandwidth consumption, e.g., a slower network, you may want to consider reviewing the Complete/Combination Scans (Full Scan (Slow Networks)) profile in the product manual. Scanning Profiles of the GFI LanGuard product document is found **here**.
- If you choose to do a complete scan of the network: The larger and more complex your network the longer the scan can take. The default setting with GFI LanGuard is that you can scan three (3) simultaneous IPs. To decrease the time it takes to scan your network you can change the default setting to up to 10 (ten) IPs at one time. HOWEVER, understand that with the time gain, you will utilize more network resources. Please see **Recommendations for scanning large networks with GFI LanGuard** for more details.
- A full scan can be time consuming. So before performing one we recommend you identify a representative sample of your network and run a test scan to ensure your environment is correctly configured. For example, a small test scan would quickly show errors that you would want to rectify before scanning all Active IPs on your network, e.g., cannot connect to WMI or remote registry.
- It is recommended that you do not scan more than 2,000 IPs in a single scan. This is not a limitation of GFI LanGuard, however is recommended to keep your scanning time low.
- Make sure you use a scanning profile which performs only the operations you need (e.g., don't use the "Full Scan" profile just to check for open shares, port scanning is a very time consuming process, so consider doing these as a separate scan.
- When scanning IP ranges, you may want to check and exclude from scanning certain devices like printers, IP phones, etc.

Security software might interfere with GFI LanGuard and prevent it from functioning properly:

- When scanning your network, there can be issues with your security (e.g., antivirus) software. Such problems can be avoided by following a few configuration guidelines.
  Please refer to **the SkyNet article.**
- By default some firewall applications (like the Windows XP Service Pack 2 inbuilt firewall) disable various ports and services. This can make the target computers totally un-discoverable, or negatively affect the scanning accuracy.
- Make the following changes on the target computer's firewall. When you do this you only need to specify the IP address of the computer where GFI LanGuard is installed:
  - Enable File and Printer Sharing
  - Enable port 135 for message sending
  - Enable Windows Management Instrumentation (WMI) traffic.

How scanning agents work:

- GFI LanGuard installs the scanning agents automatically on the selected computers
- Scanning agents only install on Windows systems (*see System installation requirements table in this document*)
- By default scanning agents perform a full scan of their host machine once per day, but the frequency, the scan time and scanning profile can be configured
- Scanning agents consume CPU power only when the host computer is audited. This is normally a few minutes per day and the priority of the process is below normal so that it will not interfere with the work done on that machine
- GFI LanGuard scanning agents can be uninstalled from the main console. By default, the agents will auto-uninstall themselves if they have no contact with their server for 60 days. The number of days can be configured
- GFI LanGuard scanning agents communicate their status to GFI LanGuard server using the TCP port 1070. The port number can be configured
- GFI LanGuard can be configured to automatically perform network discovery on domains or organizational units and install agents automatically on the newly discovered machines

» GFI LanGuard automatically handles situations where scanning agents were removed by mistake or they need to be upgraded.

If you have further questions regarding scanning or performance issues please contact us **here**; for additional technical articles please click **here**.

How relay agents work:

» Any scanning agent can be assigned as a relay agent (e.g., one relay agent per remote site).

» The relay agent downloads the service packs, patches and product updates from the GFI LanGuard server. In doing so, the patches and product updates only cross the network once to the remote locations.

» All other machines at that remote site can be configured to download patches and product updates from the local relay agent.

***Note:** More information on configuring relay agents can be located **here**.

Keeping your computers secure and up to date

GFI LanGuard is installed, the database is configured, and a few scans have been run and they may have uncovered some security issues. The purpose of this section is to provide guidelines on how we recommend handling some of the more common security issues.

The three main topics that we will discuss are:

1. **Keeping GFI LanGuard up to date**
2. **Detecting and remediating missing security updates**
3. **Detecting and remediating other network vulnerabilities**

1. Keeping GFI LanGuard up to date

» Make sure the machine that GFI LanGuard is installed on has Internet access.* GFI LanGuard performs daily checks for updated information on vulnerabilities and patches. Security vulnerabilities are discovered every day, we suggest that you scan your network on a regular basis.

» If a proxy server is used, it can be set in the GFI LanGuard user interface > main menu > Configure > Proxy Settings.

***Note**: If Internet access is not available on the machine where GFI LanGuard is installed, the product can be configured to get the updates from an alternative location. More details are available **here**.

2. Detecting and remediating missing security updates

Many security vulnerabilities can be resolved by ensuring all security patches and service packs are up-to-date on each machine. So the first thing that you need to do is scan your network for missing patches (Please refer to "Missing Patches" scanning profile of the GFI LanGuard manual **here**). After you have scanned your network for missing patches/service packs, using GFI LanGuard you can then simply deploy these missing patches/service packs to the target machines.

» **It is recommended that you install service packs first**

» After the service packs are deployed, we recommend a rescan of the network (which will give you an updated view of the patch status of your network)

» After the rescan, if no service packs are available, then deploy any missing patches

» If Internet bandwidth or disk space is an issue:

- GFI LanGuard is able to use the repository of a WSUS server in the network. This makes use of the patches and service packs already downloaded by WSUS saving you space and bandwidth. More details **here**.

- If a WSUS server is not available, you can also schedule downloads of patches/service packs by GFI LanGuard during low peak hours.

» GFI LanGuard can also auto-remediate patches/service packs if pre-approved by the administrator.

3. Detecting and remediating other network vulnerabilities

Once your computers are up-to-date (patched), we suggest you run a scan to check for other vulnerabilities or potential security issues.

» From the results of the scan it is possible to get detailed information about particular vulnerabilities.

» GFI LanGuard comes with tools to help address vulnerabilities by remotely uninstalling (unauthorized) software, or enabling antivirus/anti-spyware/firewall, or triggering definitions update for antivirus/anti-spyware, or deploying custom software and scripts, or opening remote desktop connections to computers, etc.

» GFI LanGuard can scan routers, switches, firewalls and printers for the firmware version that you are running and notify you if vulnerabilities exist in that version. If your version has vulnerability, we recommend that you update the firmware on that device.

Examples of GFI LanGuard reports

GFI LanGuard reports are designed to satisfy the requirements of both management and technical staff by delivering a graphical view of the security status of your network. Examples of GFI LanGuard reports are located **here**.

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

Email: ussales@gfi.com

33 North Garden Avenue, Suite 1200, Clearwater, FL 33755, USA

Telephone: +888 688-8457 (US/Canada)

Fax: +1 727 562-5199

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: 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

Email: sales@gfiap.com