

INTRODUCTION

Welcome to GFI LANguard: Your all-in-one solution for Patch Management, Vulnerability Scanning and Network Auditing. GFI LANguard (or "LANguard") scans your network and ports to detect, assess and correct security vulnerabilities with minimal administrative effort.

This Guide is designed to give you a high level overview of what LANguard is, what it does, how you can make quick and effective use of the power of LANguard, and help you plan for a successful deployment.

This Guide provides:

1. An **overview** of what LANguard can do for your business
2. **Six (6) important topics** to consider before you deploy LANguard
3. **How to Keep Your Computers Secure and Up to Date** to get the best out of LANguard

For more detailed documentation you can continue with:

1. GFI LANguard Frequently Asked Questions (FAQ) – <http://kbase.gfi.com/showarticle.asp?id=KBID001966>
2. GFI's Knowledge Base – <http://kbase.gfi.com>
3. GFI LANguard documentation – <http://www.gfi.com/lannetscan/manual>

If after reading the SmartGuide you have questions, we are here to help, please contact us [here](#).

GFI LANguard Overview

Let's start with a review of what GFI LANguard does. Simply stated, through the performances of the three (3) cornerstones of vulnerability management: **Patch Management, Vulnerability Checking** and **Network Auditing**, LANguard **Scans, Analyzes and helps Remediate** your network.

Either manually or on a scheduled basis, LANguard **Scans** your network for security related issues and gathers security relevant information. Such as gathering information about security vulnerabilities, missing patches, open ports, open shares, user and groups, installed applications, and hardware inventory etc.

With the results of the scans you can then **Analyze** the status of your network. GFI LANguard provides tools to browse and investigate the scan results; we assign a vulnerability level to each scanned computer based on the items found during the audit and provide reports and results comparisons. Samples of these reports and scans are included as **Exhibit A here**.

With the Scan and the analysis, GFI LANguard assists you to **Remediate** the security issues, automating the process where possible.

After creating a baseline scan, you can determine any differences or changes to the security and computer configurations of all the computers in the network. You can then decide to take such actions as deploy missing Microsoft security patches and service packs, rollback Microsoft updates, deploy custom software and scripts, uninstall unauthorized applications, open remote desktop connections to scanned computers, etc. All of these actions will ensure your systems are up to date and have the latest security patches applied.

Our experience is that our customers generally license GFI LANguard to achieve the following:

PATCH MANAGEMENT

- Detect and Deploy Missing Patches

VULNERABILITY SCANNING

- Scanning of Windows OS or applications
- Identify and close down open shares, ports, etc.

NETWORK AUDITING

- Network Health Monitoring
- Network Auditing
- Identify which PCs have what software installed
- Change Management – when things change
- Identify devices on the network

SIX IMPORTANT TOPICS TO CONSIDER BEFORE DEPLOYING GFI LANGUARD

There are six (6) issues to consider before deploying GFI LANguard. It is important that you understand each of them so, if after reading the section below you has any questions or want to discuss any of them, please [contact us](#).

1. [Licensing](#)
2. [System Installation Requirements](#)
3. [Scanning Profiles – What you Need to Know](#)
4. [Choosing the Right Database](#)
5. [Scanning and Performance Tips](#)
6. [GFI LANguard Filtering and/or Reporting](#)

1. LICENSING

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

1. If you have an IP range of 192.160.1.1 through 192.160.1.254.
2. And you have 20 Active IPs in that range that you want to scan, you only have to license the 20 Active IPs.
3. 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.

2. SYSTEM INSTALLATION REQUIREMENTS

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 10 scan targets	10 to 500 scan targets	500 to 1500 scan targets
Processor	1 GB	2 GHz	2 x 3 GHz Quad Core
Physical Storage	1 GB	2 GB	10 GB
Memory	1 GB	2 GB	4 GB
Network bandwidth usage	256 KBps	256 KBps to 550 KBps	256 KBps to 550 KBps

System Requirements: Software

Supported operating systems (x86 or x64)

- Microsoft Windows Server 2008 Standard/Enterprise
- Microsoft Windows Server 2003 Standard/Enterprise
- Microsoft Windows 2000 Professional/Server/Advanced Server (SP4 or higher)
- Microsoft Windows 7 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 Small Business Server 2000 (SP2)

Supported databases

- 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:

- Microsoft .NET Framework 2.0

Target computer components

The following components are required to be installed on target computers for GFI LANguard to be able to scan them:

- Windows Management Instrumentation (WMI) – Required to scan Windows-based scan targets. Included in all Windows 2000 or newer operating systems (this is typical for Windows environments).
- Secure Shell (SSH) – Required for UNIX based scan targets. Commonly included as part of all major Unix/Linux distributions.
- SAMBA (SMB) server – Required for UNIX-based scanning targets. Commonly included as part of all major Unix/Linux distributions.

3. SCANNING PROFILES – WHAT YOU NEED TO KNOW

Out of the box, LANguard comes with an extensive list of scanning profiles*. A list of available scanning profiles is available at: <http://support.gfi.com/manuals/en/lanscan9/lanscan9manual.1.43.html>

At the highest level, the three (3) out of box profiles are:

1. Complete/Combination Scans
2. Vulnerability Assessment Scans
3. Network and Software Audit Scans

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

4. CHOOSING THE RIGHT DATABASE


Each time a scan is run, the results are stored in a database. There are three (3) Microsoft 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:

- Microsoft Access (LANguard includes the Microsoft Access Database but does not require having Access installed)
- Microsoft SQL Express
- Microsoft SQL Server

If you are looking at Microsoft SQL Server to use as your preferred database but are unsure of the licensing requirements, below are some links to Microsoft SQL licensing information pages.

[SQL 2008](#), [SQL 2005](#), [SQL Express 2008](#)

 **As always you may want to consult your Microsoft partner for advice.**

 The default Microsoft Access scan results database which ships with GFI LANguard is not enough for large networks. Switching to a Microsoft SQL Server database must be strongly considered for networks larger than 250 active IPs when the IP is a computer. (As a computer scan will return more information than say, a printer).

* **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 are 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

Here are some suggestions for ensuring more successful scans.

- 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 Section 7. Scanning Profiles of the LANguard product document 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 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 a 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.
- When scanning your network, there can be issues with your security (e.g., anti-virus) software. Such problems can be avoided by following a few configuration guidelines. Please refer to <http://kbase.gfi.com/showarticle.asp?id=KBID002344>
- 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 computers firewall. When you do this you only need to specify the IP address of the computer where LANguard is installed

- Enable File and Printer Sharing
- Enable port 135 for message sending
- Enable Windows Management Instrumentation (WMI) traffic

- 💡 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.

If you have further questions regarding scanning or performance issues please contact us [here](#); for additional technical articles please click [here](#).

6. GFI LANGUARD FILTERING AND/OR REPORTING

GFI LANguard is a powerful tool that allows you to Scan, Analyze and Remediate your network. The information that is provided by LANguard allows you to do effective Patch Management, Vulnerability Scanning and Network Auditing. Having the data is only half the results you get with LANguard. There are two (2) different methods to summarizing the results of your scans: Results Filtering and the GFI LANguard ReportPack.

- **Results Filtering:** Though the LANguard interface you can create your own filter (e.g., on the fly, quick, simple report). Scan results typically present a lot of information and Results Filtering is utilized when you only want specific information to achieve a particular goal, e.g., identifying only which patches are missing in your system. Results Filtering can be done from a recent scan or one loaded from the database.

To create a new results filter follow the steps described [here](#).

- **GFI LANguard ReportPack:** Included with the product (as a separate download found [here](#)) is an easy to use reporting facility, the [GFI LANguard ReportPack](#). The reports available in the ReportPack are designed to satisfy the needs of the organization: both from the high level graphical views for management (e.g., Trend reports) to the detailed reports and scans (such as daily drill down reports) needed to satisfy the needs of technical staff. As we know for management, a picture can be worth a thousand words.

Types of reports created through LANguard ReportPack include:

- **Executive reports:** overview and trend analysis information through graphical reports. Sample Executive reports: [Network Vulnerability Summary](#) and [Network Vulnerability Trend](#).
- **Statistical reports:** information related to vulnerability and operating system distribution throughout the network. Sample Statistical reports: [OS Service Pack Distribution](#), [Vulnerability Distribution by Host](#) and [Vulnerability Distribution by OS](#).
- **Technical reports:** technical information on vulnerabilities, missing patches and trojans. Sample Technical reports: [Installed Patches Grouped by Host](#), [Missing Patches Grouped by OS](#), [Open Trojan Ports by Host](#) and [Vulnerability Listing by Host](#).
- **Top 20 reports:** the top 20 most vulnerable hosts based on open ports, missing patches or trojans. Sample Top 20 reports: [Open Trojan Ports](#), [Vulnerable Hosts based on Missing Patches](#) and [Vulnerable Hosts based on Open Ports](#).

IMPORTANT: To install the GFI ReportPack, use the following procedure

1. Install GFI LANguard
2. The default database will be Microsoft Access, (which is pre-configured). If you choose to use Microsoft SQL as your database you will need to have SQL installed and then change your database settings to use Microsoft SQL
3. Finally, install the ReportPack. (PLEASE NOTE: When you install the ReportPack, there is a component called "GFI ReportCenter" that installs first, and then the GFI LANguard ReportPack will install. The GFI ReportCenter is a common security component that all GFI ReportPacks use.)

Full documentation on GFI LANguard ReportPack can be found [here](#).

Keeping Your Computers Secure and Up to Date

So you have installed LANguard, configured the database and installed the ReportPack. You then performed a few scans and may have found security issues. The purpose of this section is to provide guidelines on how we recommend approaching some of the more common security issues. The three (3) main topics that we will discuss are: keeping LANguard Up to Date, Detecting and Remediating Microsoft Patches/Service Packs and Detecting and Remediating Other Network Vulnerabilities.






1. Keeping LANguard Up To Date

- Make sure the machine that LANguard is installed on has Internet access.* LANguard performs daily checks for updated information on vulnerabilities and patches. Security vulnerabilities are discovered every day, we suggest that you scan you 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.

***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 Microsoft Patches/Service Packs

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 Section 7 "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 LANguard during low peak hours.
-  **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.
- LANguard comes with tools to help address vulnerabilities by remotely uninstalling (unauthorized) software, or deploy custom software and scripts, or open remote desktop connections to computers, etc.