GFI LanGuard™

Installation and Setup Guide

GFI®

Contents

1 Introduction

GFI LanGuard is a patch management and network auditing solution that enables you to easily manage and maintain end-point protection across devices within your LAN. It acts as a virtual security consultant that offers Patch Management, Vulnerability Assessment and Network Auditing support for Windows® Linux and MAC computers as well as mobile devices. GFI LanGuard achieves LAN protection through:

» Identification of system and network weaknesses via a comprehensive vulnerability checks database. This includes tests based on OVAL, CVE and SANS Top 20 vulnerability assessment guidelines

» Auditing of all hardware and software assets on your network, enabling you to create a detailed inventory of assets. This goes as far as enumerating installed applications as well as devices connected on your network

» Automatic download and remote installation of service packs and patches for Microsoft® Windows, Linux and MAC operating systems as well as third party products

» Automatic uninstallation of unauthorized software.

1.1 About this guide

The aim of this Installation and Setup Guide is to help System Administrators install and test GFI LanGuard with minimum effort.

1.1.1 Terms and conventions used in this manual

Term	Description
Note	Additional information and references essential for the operation of GFI LanGuard.
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 file names.
Code	Indicates text values to key in, such as commands and addresses.

2 Installing GFI LanGuard

The following topics provide information on how to successfully deploy a fully functional instance of GFI LanGuard and how to upgrade existing installations.

Topics in this section:

2.1 GFI LanGuard system requirements

Computers running GFI LanGuard must meet the system requirements described below for performance reasons.

Refer to the following sections for information about:

» Hardware requirements

» Software requirements

» Firewall ports and protocols

» Gateway permissions

» Antivirus & Backup exclusions

Hardware requirements

Computers hosting GFI LanGuard must meet the following hardware requirements:

Component	1 to 100 Computers	100 to 500 Computers	500 to 3,000 Computers
Processor	2 GHz Dual Core	2.8 GHz Dual Core	3 GHz Quad Core
Physical Storage	5 GB	10 GB	20 GB
RAM	2 GB	4 GB	8 GB
Network bandwidth	1544 kbps	1544 kbps	1544 kbps

Software requirements

GFI LanGuard components can be installed on any computer that meets the software requirements listed in this section. For more information, refer to:

» Supported operating systems

» Supported databases

» GFI LanGuard and TLS 1.1 or higher

» Target computer components

Supported operating systems (32-bit/64-bit)

The following table lists operating systems and versions where GFI LanGuard can be installed. Ensure that you are running the Full (with GUI) version of these operating systems, and running the latest Service Pack as provided by Microsoft.

Operating System
Windows® Server 2016
Windows® Server 2012 (including R2)
Windows® Server 2008 (including R2) Standard/Enterprise
Windows® 10 Professional/Enterprise
Windows® 8/8.1 Professional/Enterprise

Operating System
Windows® 7 Professional/Enterprise/Ultimate
Windows® Vista Business/Enterprise/Ultimate
Windows® Small Business Server 2011

Supported databases

GFI LanGuard uses a database to store information from network security audits and remediation operations. The database backend can be any of the following:

Database server	Recommended Use
SQL Server Express® 2008 or later	This database server has a 10GB limit and is therefore recommended for networks containing up to 500 computers. If a database server is not available, the GFI LanGuard installer can automatically download and run the Microsoft SQL Express installer.
SQL Server® 2008 or later	Recommended for larger networks containing 500 computers or more.

For improved performance, it is highly recommended to use an SSD drive for the database server. Compared to traditional Hard Disk Drives, SSDs deliver superior performance with lower access time and lower latency.

GFI LanGuard and TLS 1.1 or higher

If you plan to deploy GFI LanGuard in an environment where TLS 1.1 and above is running, you need to enable FIPS-Compliant algorithms on the computer where the GFI LanGuard is installed.

To enable FIPS-Compliant algorithms:

1. Go to **Start > Run** and type `gpedit.msc`

2. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies**.

3. Double-click **Security Options**.

4. In the details pane, double-click **System cryptography: Use FIPS-compliant algorithms for encryption, hashing, and signing**.

5. Check **Enabled** and click **OK**

6. Reboot the computer or open a command prompt and type `gpupdate /force`.

Target computer components

The following table provides you with information about components that are required to be installed or enabled on computers to be scanned remotely (agent-less) by GFI LanGuard:

Component	Description
Secure Shell (SSH)	Required for UNIX/Linux/Mac OS based scan targets. SSH server must be installed and enabled.
File and Printer Sharing	Required for machines running Microsoft operating systems to enumerate and collect information about scan targets.
Remote Registry	Ensure that this service is running on machines using Microsoft operating systems. This is required to collect information about scan targets, such as Operating System details, user and computer data.

Firewall Ports and Protocols

This section provides you with information about the required firewall ports and protocols settings for:

» GFI LanGuard and Relay Agents

» GFI LanGuard Agent and Agent-less computers

GFI LanGuard and Relay Agents

Configure your firewall to allow **inbound** connections on TCP port **1072**, on computers running:

» GFI LanGuard

» Relay Agents

This port is automatically used when GFI LanGuard is installed, and handles all inbound communication between the server component and the monitored computers. If GFI LanGuard detects that port 1072 is already in use by another application, it automatically searches for an available port in the range of **1072-1170**.

To manually configure the communication port:

1. Launch GFI LanGuard.

2. Go to **Configuration > Manage Agents**.

3. From the right pane, click **Agents Settings**.

4. From the **Agents Settings** dialog, specify the communication port in the **TCP port** text box.

5. Click **OK**

GFI LanGuard Agent and Agent-less computers

Communications between GFI LanGuard and managed computers (Agents and Agent-less), are done using the ports and protocols below. The firewall on managed computers needs to be configured to allow **inbound** requests on the following ports:

TCP Ports	Protocol	Description
22	SSH	Auditing Linux systems.
135	DCOM	Dynamically assigned port.
137	NetBIOS	Computer discovery and resource sharing.
138	NetBIOS	Computer discovery and resource sharing.
139	NetBIOS	Computer discovery and resource sharing.
161	SNMP	Used for computer discovery. GFI LanGuard supports SNMPv1 and SNMPv2c. SNMPv3 and SNMP over TLS / DTLS are not supported.
445	SMB	Used while: » Auditing computers » Agent management » Patch deployment.

Gateway permissions

To download definition and security updates, GFI LanGuard connects to GFI, Microsoft, and Third-Party update servers via HTTP. Ensure that the firewall settings of the machine where GFI LanGuard is installed allows connections to:

» gfi-downloader-137146314.us-east-1.elb.amazonaws.com

» *software.gfi.com/lnsupdate/

» *.download.microsoft.com

» *.windowsupdate.com

» *.update.microsoft.com

» All update servers of Third-Party Vendors supported by GFI LanGuard.

For more information, refer to:

» Supported Third-Party applications: http://go.gfi.com/?pageid=LAN_PatchMng

» Supported application bulletins: http://go.gfi.com/?pageid=3p_fullreport

» Supported Microsoft applications: http://go.gfi.com/?pageid=ms_app_fullreport

» Supported Microsoft bulletin: http://go.gfi.com/?pageid=ms_fullreport

Antivirus & Backup exclusions

Antivirus & backup software can cause GFI LanGuard to malfunction if it is denied access to some of its files.

Add exclusions that prevent antivirus & backup software from scanning or backing up the following folder on the GFI LanGuard server, Agents, Relay Agents and the GFI LanGuard Central Management Server: <system drive>\ProgramData\GFI\

2.2 Installing GFI LanGuard

2.2.1 Important notes

» If you are currently using a previous version of GFI LanGuard, you can upgrade your current installation while at the same time retaining all your existing configuration settings. Upgrade is not reversible; you cannot downgrade to the previous version that you had installed.

» You must have a GFI Account or a license key to install GFI LanGuard.

» Before running the installation wizard:

  ● Ensure that the machine where GFI LanGuard is going to be installed meets the specified system requirements. For more information, refer to GFI LanGuard system requirements (page 6).

  ● Configure your firewall to allow GFI LanGuard to connect to GFI servers and to the remote machines to be monitored. For more information, refer to Firewall Ports and Protocols (page 8).

  ● Disable third-party antivirus during the installation process.

  ● Save any pending work and close all open applications on the machine.

2.2.2 Installation procedure

1. Log in using administrator credentials on the machine where you want to install GFI LanGuard.

2. Right-click the GFI LanGuard 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.

3. Launch the GFI LanGuard installer.

4. Select the language for your installation and click **OK**.

NOTES

» The GFI LanGuard Central Management Server and all GFI LanGuard instances joined to it need to be installed in the same language.

» The graphical user interface of the GFI LanGuard Central Management Server is available only in English, including in instances when GFI LanGuard is installed in another language.
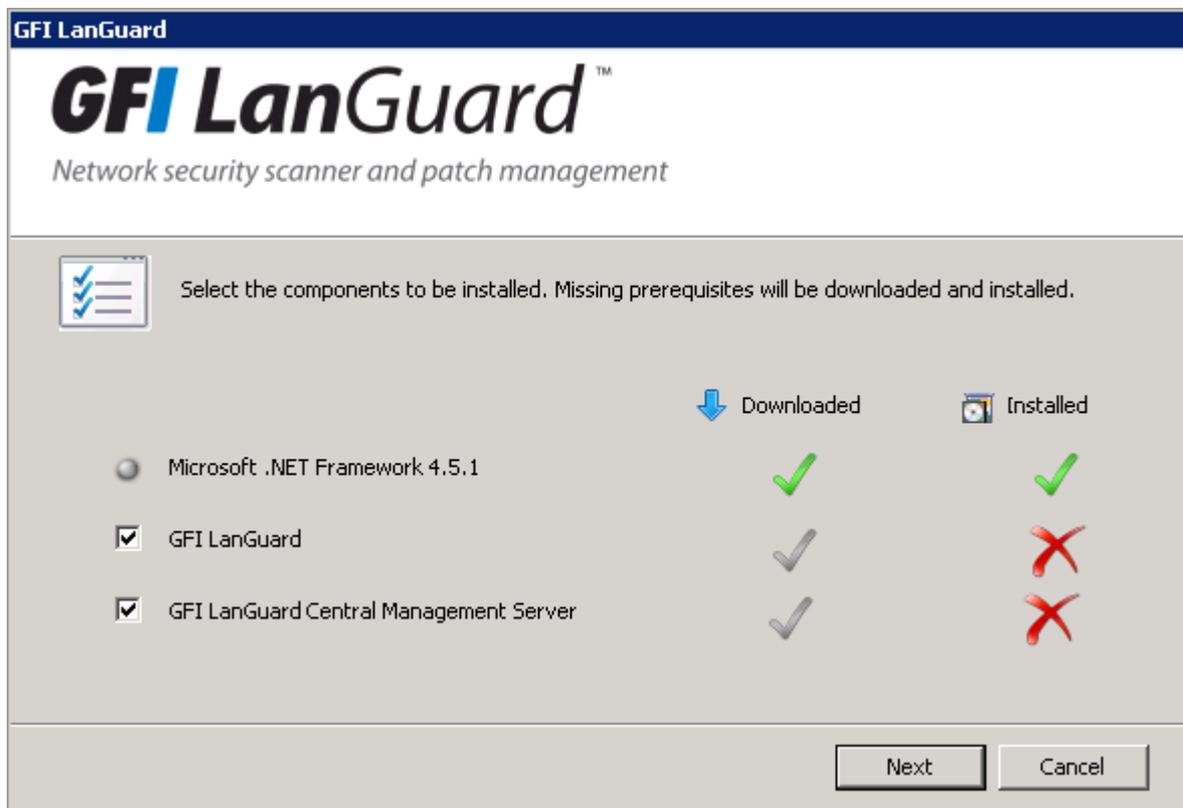
Screenshot 1: Select components to be installed

5. From the list of components, select **GFI LanGuard** and click **Next**. The installation wizard will automatically download and install any missing components.

NOTE

An Internet connection is required to download missing components.

6. In the **Username** and **Password** fields, enter your GFI Accounts area credentials or the account used when signing up to download GFI LanGuard. Click **Sync** to retrieve the license keys registered to your account. Choose a key from the **Available keys** drop-down. If you do not have a GFI account or if you do not have a license key, click **Sign up here** and fill in the registration form. You may also manually specify a license key in the **Enter license key** field. Click **OK** when a valid license is specified.
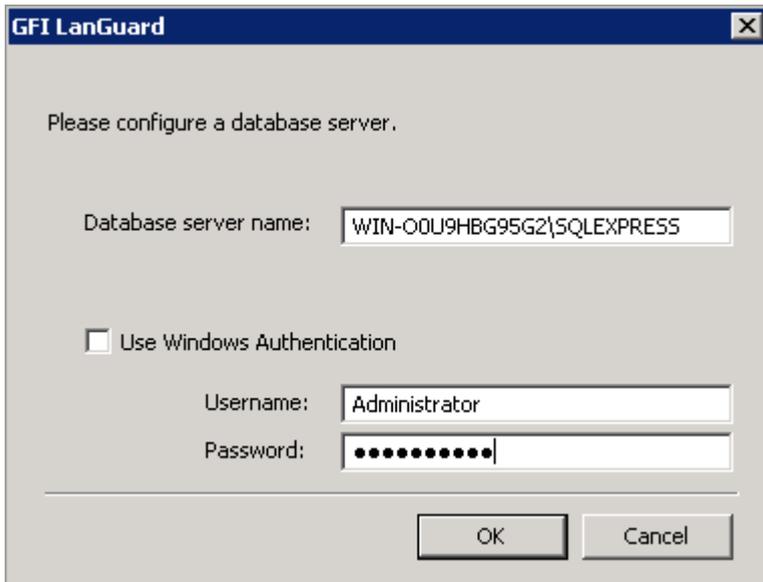
Screenshot 2: Configure the database server

7. In the database server configuration window provide the following details:

OPTION	DESCRIPTION
Database server name	The name of the Microsoft SQL server where the GFI LanGuard database is hosted.
Use Windows Authentication	Select this option if you want the GFI LanGuard to use the Microsoft Windows credentials of the currently logged in user when connecting to the Microsoft SQL database.
Username / Password	If GFI LanGuard is not using Windows Authentication when connecting to the Microsoft SQL database, provide the username and password to be able to connect to the database.

8. In the GFI LanGuard welcome screen, click **Next**.

Screenshot 3: End-user license agreement

9. Read the licensing agreement carefully. To proceed with the installation, select **I accept the terms in the License Agreement** and click **Next**.
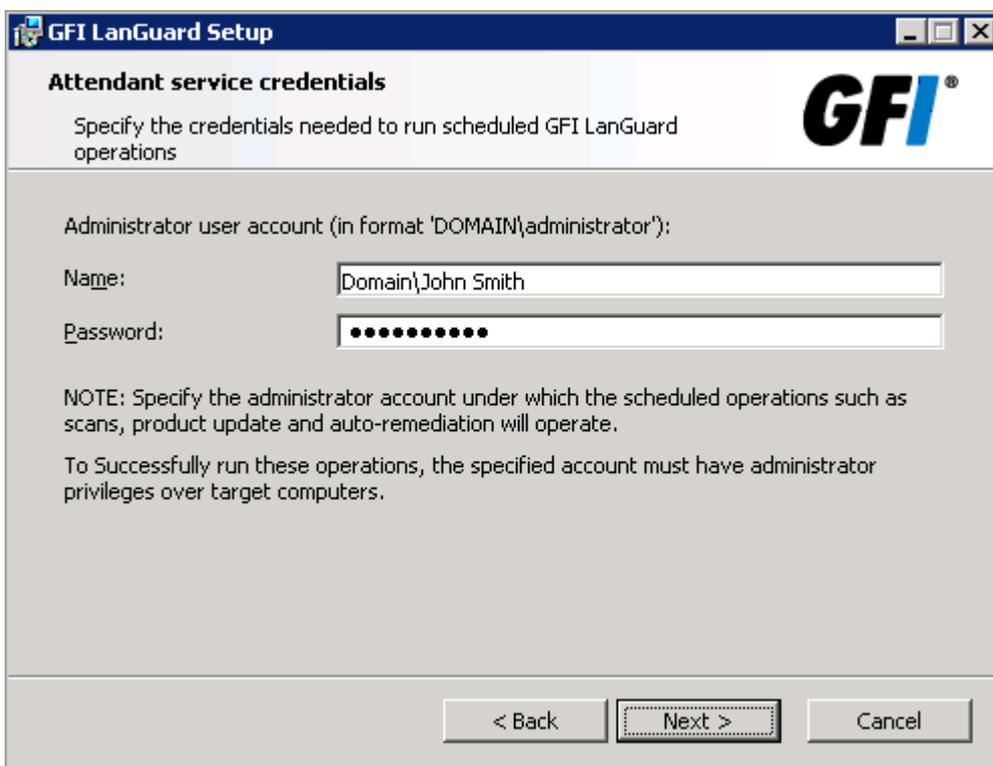
Screenshot 4: Attendant service credentials

10. Key in the administrator credentials and password. This is the service under which scheduled operations run. Click **Next** to continue setup.

11. Click **Install** to install GFI LanGuard in the default location or **Browse** to change path.

12. Click **Finish** to finalize installation.

When launched for the first time, GFI LanGuard automatically enables auditing on the local computer and scans the local computer for vulnerabilities. On completion, the GFI LanGuard **Home** page displays the vulnerability result.

2.3 Testing the installation

Once GFI LanGuard is installed, test your installation by running a local scan to ensure it installed successfully.

1. Launch GFI LanGuard.

Screenshot 5: Launch a scan

2. From GFI LanGuard home page, click **Launch a Scan**.

Screenshot 6: Launch a scan properties

3. From **Scan Target** drop–down menu, select **localhost**.

4. From **Profile** drop–down menu, select **Full Scan**.

5. Click **Scan** to start the scan on the local computer.

6. The scan progress is displayed in the **Scan** tab.
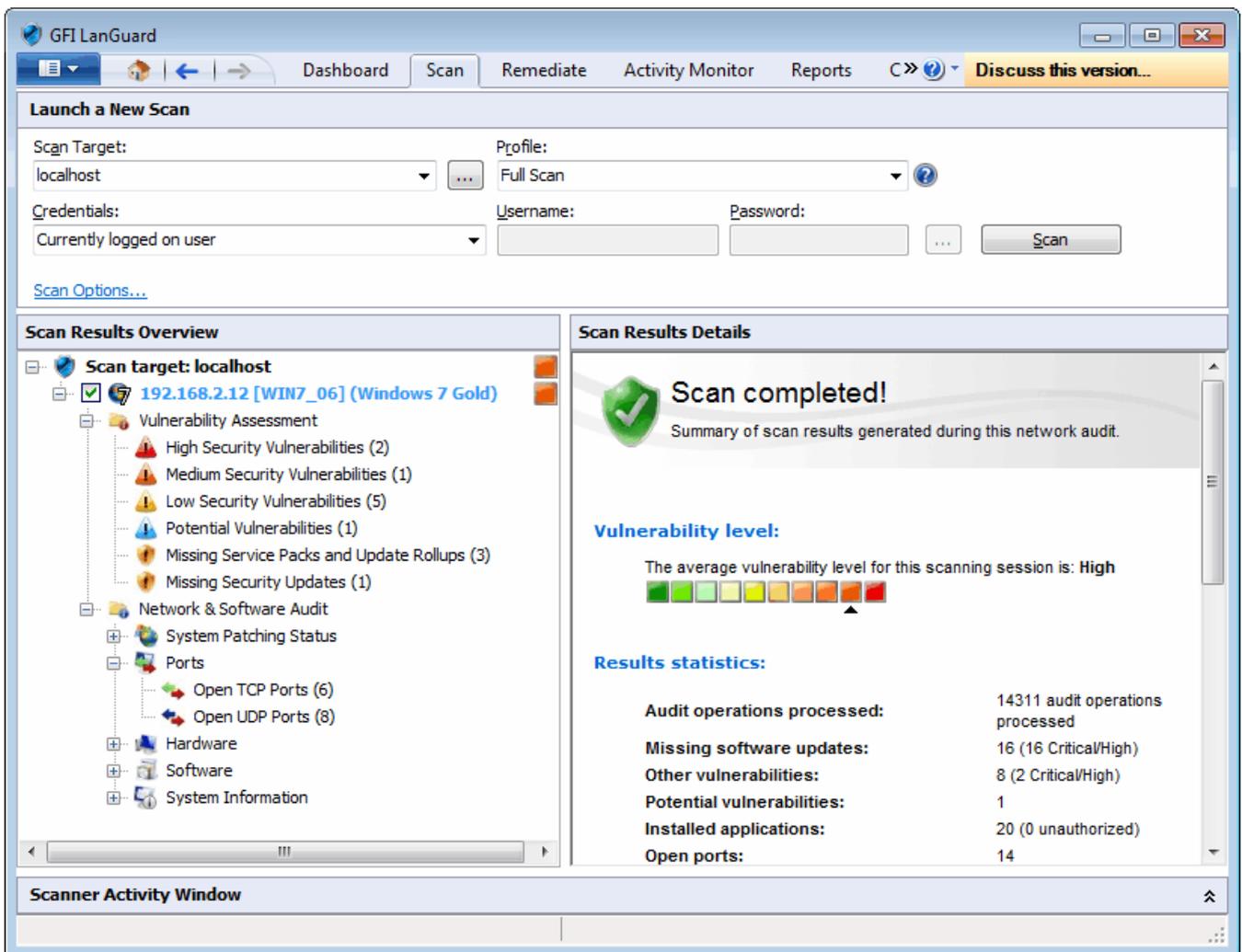
Screenshot 7: Scan results summary

7. On completion, the **Progress** section will display an overview of the scan result.

8. Use the **Scan Results Details** and **Scan Results Overview** to analyze the scan result.

3 Troubleshooting and support

This topic explains how to resolve issues encountered while using GFI LanGuard. These issues can be resolved using the contents of this guide. If any issues remain unresolved after reviewing the manual, check if your problem is listed below.

Refer to the following sections for information about resolving common issues and contacting our support team.

Topics in this section:

3.1 GFI Knowledge Base

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

3.2 Web Forum

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

3.3 Requesting 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: https://www.g-fi.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.

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.