

GFI Product Manual

GFI LanGuard™

Installation and Setup Guide



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI LanGuard is copyright of GFI SOFTWARE Ltd. - 1999-2012 GFI Software Ltd. All rights reserved.

Document Version: 11.1

Last updated (month/day/year): 04/04/2013

Contents

1 Introduction	7
1.1 About this guide	7
1.1.1 Terms and conventions used in this manual	7
1.2 How GFI LanGuard works	8
1.3 How GFI LanGuard Agents work	8
1.4 How GFI LanGuard Relay Agents work	9
1.5 GFI LanGuard Components	9
2 Installing GFI LanGuard	10
2.1 Deployment scenarios	10
2.1.1 Deploying GFI LanGuard in mixed mode	10
2.1.2 Deploying GFI LanGuard using Relay Agents	11
2.1.3 Deploying GFI LanGuard in Agent-less mode	12
2.2 System requirements	14
2.2.1 Hardware requirements	14
2.2.2 Software requirements	15
2.2.3 Firewall Ports and Protocols	16
2.2.4 Gateway permissions	17
2.2.5 Supported antivirus/anti-spyware applications	18
2.3 Upgrading from previous versions	18
2.4 New installation	20
2.5 Post install actions	23
3 Testing the installation	25
4 The GFI LanGuard Dashboard	27
4.1 Achieving results from the dashboard	27
4.2 Using the Dashboard	27
4.3 Using the Computer Tree	28
4.3.1 Simple filtering	28
4.3.2 Advanced filtering	29
4.3.3 Grouping	30
4.3.4 Searching	30
4.4 Using Attributes	31
4.4.1 Assigning attributes to a computer	31
4.4.2 Assigning attributes to a group	32
4.4.3 Configuring attributes	33
4.5 Dashboard actions	34
4.6 Exporting issue list	34
4.7 Dashboard views	35
4.7.1 Overview	35
4.7.2 Computers view	38
4.7.3 History view	40
4.7.4 Vulnerabilities View	41
4.7.5 Patches View	42
4.7.6 Ports View	43

4.7.7 Software View	44
4.7.8 Hardware View	45
4.7.9 System Information View	46
5 Troubleshooting and support	47
5.1 Resolving common issues	47
5.2 Using the Troubleshooter Wizard	49
5.3 GFI SkyNet	51
5.4 Web Forum	51
5.5 Requesting technical support	51
6 Glossary	53
7 Index	61

List of Figures

Screenshot 1: Pre-requisite check dialog	19
Screenshot 2: Import and Export settings from a previous instance	20
Screenshot 3: End-user license agreement	21
Screenshot 4: Specify user details and license key	21
Screenshot 5: Attendant service credentials	22
Screenshot 6: Import and Export configurations	23
Screenshot 7: Launch a scan	25
Screenshot 8: Launch a scan properties	25
Screenshot 9: Scan results summary	26
Screenshot 10: View Dashboard	28
Screenshot 11: Simple filtering	29
Screenshot 12: Add Filter Properties	29
Screenshot 13: Search specific computers and groups	30
Screenshot 14: Assigning attributes: Single computer	32
Screenshot 15: Assigning attributes: Multiple computers	33
Screenshot 16: New attribute dialog	33
Screenshot 17: Actions section in the Dashboard	34
Screenshot 18: Dashboard Overview	35
Screenshot 19: Analyze results by computer	38
Screenshot 20: History view in the Dashboard	40
Screenshot 21: Vulnerabilities view in the Dashboard	41
Screenshot 22: Patches view in Dashboard	42
Screenshot 23: Ports view in Dashboard	43
Screenshot 24: Software view in Dashboard	44
Screenshot 25: Hardware view in Dashboard	45
Screenshot 26: System Information view in Dashboard	46
Screenshot 27: Troubleshooter wizard - Information details	50
Screenshot 28: Troubleshooter wizard - Gathering information about known issues	51

List of Tables

Table 1: Terms and conventions used in this manual	7
Table 2: GFI LanGuard Components	9
Table 3: Hardware requirements - GFI LanGuard Server	14
Table 4: Hardware requirements - GFI LanGuard Agent	14
Table 5: Hardware requirements - GFI LanGuard Relay Agent	15
Table 6: Supported Operating Systems	15
Table 7: Supported database backends	16
Table 8: Software requirements - Additional components	16
Table 9: Ports and Protocols	17
Table 10: Import override options	24
Table 11: Search options	31
Table 12: Dashboard actions	34
Table 13: Software information from an audit	36
Table 14: View by computers information	38
Table 15: GFI LanGuard common Issues	47
Table 16: Information gathering options	50

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® and MAC computers. 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 and MAC operating systems as well as third party products
- » Automatic un-installation of unauthorized software.

Topics in this chapter:

1.1 About this guide	7
1.2 How GFI LanGuard works	8
1.3 How GFI LanGuard Agents work	8
1.4 How GFI LanGuard Relay Agents work	9
1.5 GFI LanGuard Components	9

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

Table 1: Terms and conventions used in this manual

Term	Description
	Additional information and references essential for the operation of GFI LanGuard.
	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.
<i>Italics text</i>	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.

1.2 How GFI LanGuard works

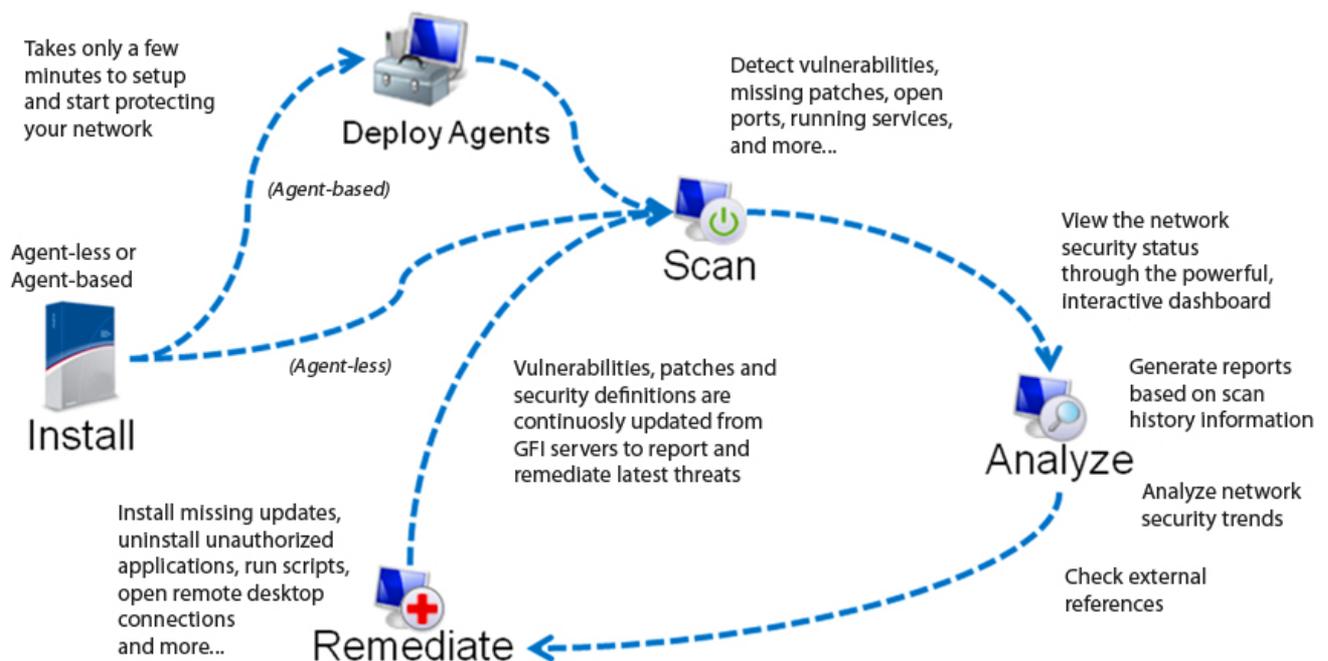


Figure 1: How GFI LanGuard works

Upon installation, GFI LanGuard operates in two stages:

- » First it determines the machines that are reachable. It also tries to collect information sets from the target machines as part of its Network Discovery operations, using a subset of SMB, NETBIOS, and ICMP protocols. Supported targets include the localhost, IP, computer name, computers list, IP range, whole domain/workgroup and/or organizational unit.
- » Second, once the targets are identified, GFI LanGuard performs a deep scan to enumerate all the information related to the target computer. GFI LanGuard uses a variety of techniques to gain access to this information ranging from file and folder property checks, registry checks, WMI commands, SMB commands as well as port scan checks (TCP/UDP) and more.

1.3 How GFI LanGuard Agents work

GFI LanGuard can be configured to automatically discover and deploy agents on new computers. Agents minimize network bandwidth utilization. This is because in Agent-less mode, the GFI LanGuard server component performs audits over the network; while in Agent mode, audits are done using the scan target's resources and only a result XML file is transferred over the network.

Agents send scan data to GFI LanGuard through TCP port 1070. This port is opened by default when installing GFI LanGuard. Agents do not consume resources of the scan target's machine unless it is performing a scan or remediation operations. If an Agent becomes unresponsive for 60 days, it is automatically uninstalled from the target machine.



Note

By default, Agents auto-uninstall after 60 days. To customize the timeframe, go to **Configuration** tab > **Agents Management** and from the right pane, click **Agents Settings**. Specify the number of days in the **General** tab of the **Agents Settings** dialog.



Note

Agents can only be installed on computers running a Microsoft Windows operating system and they require approximately 25 MB of memory and 350 MB of hard disc space.

1.4 How GFI LanGuard Relay Agents work

GFI LanGuard enables you to configure any machine with a GFI LanGuard Agent installed on it, to act as a GFI LanGuard server. These Agents are called **Relay Agents**. Relay Agents reduce the load from the GFI LanGuard server component. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers just as if it were the server component.

1.5 GFI LanGuard Components

This section provides you with information about components that are installed by default, when you install GFI LanGuard. Once you install the product, you can manage patch management and remediation tasks from the Management Console. The Management Console is also referred to as the Server component of GFI LanGuard, as described in the table below:

Table 2: GFI LanGuard Components

Component	Description
GFI LanGuard Server	Also known as the Management Console. Enables you to manage agents, perform scans, analyze results, remediate vulnerability issues and generate reports.
GFI LanGuard Agents	Enable data processing and auditing on target machines; once an audit is finished, result is sent to GFI LanGuard.
GFI LanGuard Update System	Enables you to configure GFI LanGuard to auto-download updates released by GFI to improve functionality. These updates also include checking GFI web site for newer builds.
GFI LanGuard Attendant Service	The background service that manages all scheduled operations, including scheduled network security scans, patch deployment and remediation operations.
GFI LanGuard Scanning Profiles Editor	This editor enables you to create new and modify existing scanning profiles.
GFI LanGuard Command Line Tools	Enables you to launch network vulnerability scans and patch deployment sessions as well as importing and exporting profiles and vulnerabilities without loading up the GFI LanGuard management console.

2 Installing GFI LanGuard

This chapter guides you in selecting the most appropriate deployment solution that caters to your requirements as well as provides you with information about how to successfully deploy a fully functional instance of GFI LanGuard.

Topics in this chapter:

2.1 Deployment scenarios	10
2.2 System requirements	14
2.3 Upgrading from previous versions	18
2.4 New installation	20
2.5 Post install actions	23

2.1 Deployment scenarios

GFI LanGuard can be installed on any machine which meets the minimum system requirements. Use the information in this section to determine whether you want to monitor a pool of Agent-less, Agent-based or a mix of both, depending on the:

- » Number of computers and devices you want to monitor
- » Traffic load on your network during normal operation time.

The following sections provide you with information about different deployment scenarios supported by GFI LanGuard:

- » [Deploying GFI LanGuard in mixed mode](#)
- » [Deploying GFI LanGuard using Relay Agents](#)
- » [Deploying GFI LanGuard in Agent-less mode](#)

2.1.1 Deploying GFI LanGuard in mixed mode

GFI LanGuard can be configured to deploy agents automatically on newly discovered machines or on manually selected computers. Agents enable data processing and auditing to be done on target machines; once an audit is finished, the result is transferred to GFI LanGuard through an XML file.

Agent-based scans:

- » Have better performance because the load is distributed across client machines.
- » Can work on low bandwidth environments because the communication between the server and agents is reduced.
- » Are suitable for laptops. Computers will be scanned even if the computer is not connected to the company network.
- » Are more accurate than manual scans, agents can access more information on the local host.

The following screenshot shows how GFI LanGuard can be deployed using agents on a Local Area Network (LAN):

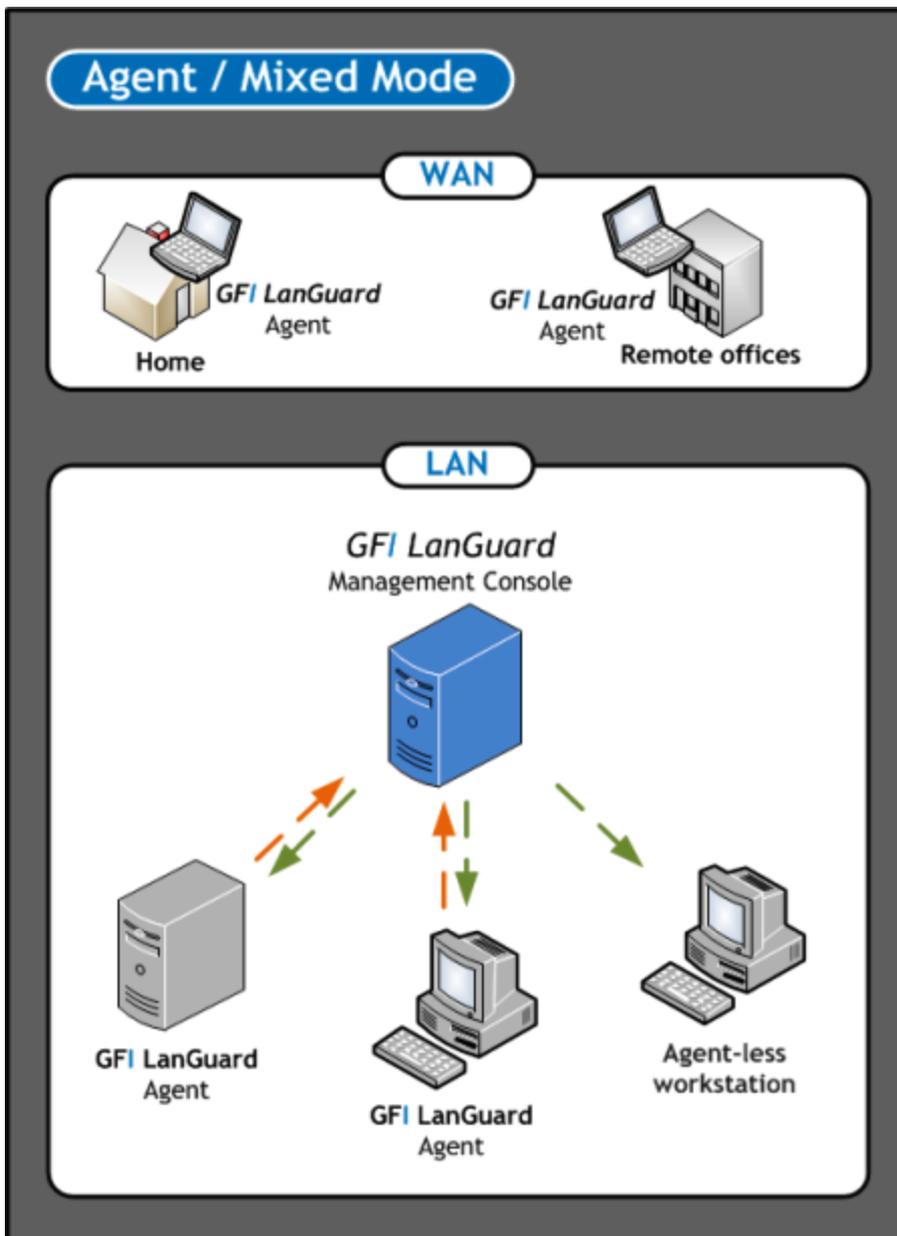


Figure 2: Agent/Mixed Mode

2.1.2 Deploying GFI LanGuard using Relay Agents

Relay agents are used to reduce the load from the GFI LanGuard server. Computers configured as relay agents will download patches and definitions directly from the GFI LanGuard server and will forward them to client computers. The main advantages of using relay agents are:

- » Save Network Bandwidth in local or geographically distributed networks. If a relay agent is configured on each site, a patch is only downloaded once and distributed to clients
- » Load is removed from the GFI LanGuard server component and distributed amongst relay agents
- » Since computers are managed from multiple relay agents, it increases the number of devices that can be protected simultaneously.

In a network, computers can be grouped and each group can be assigned to a relay agent as shown below.

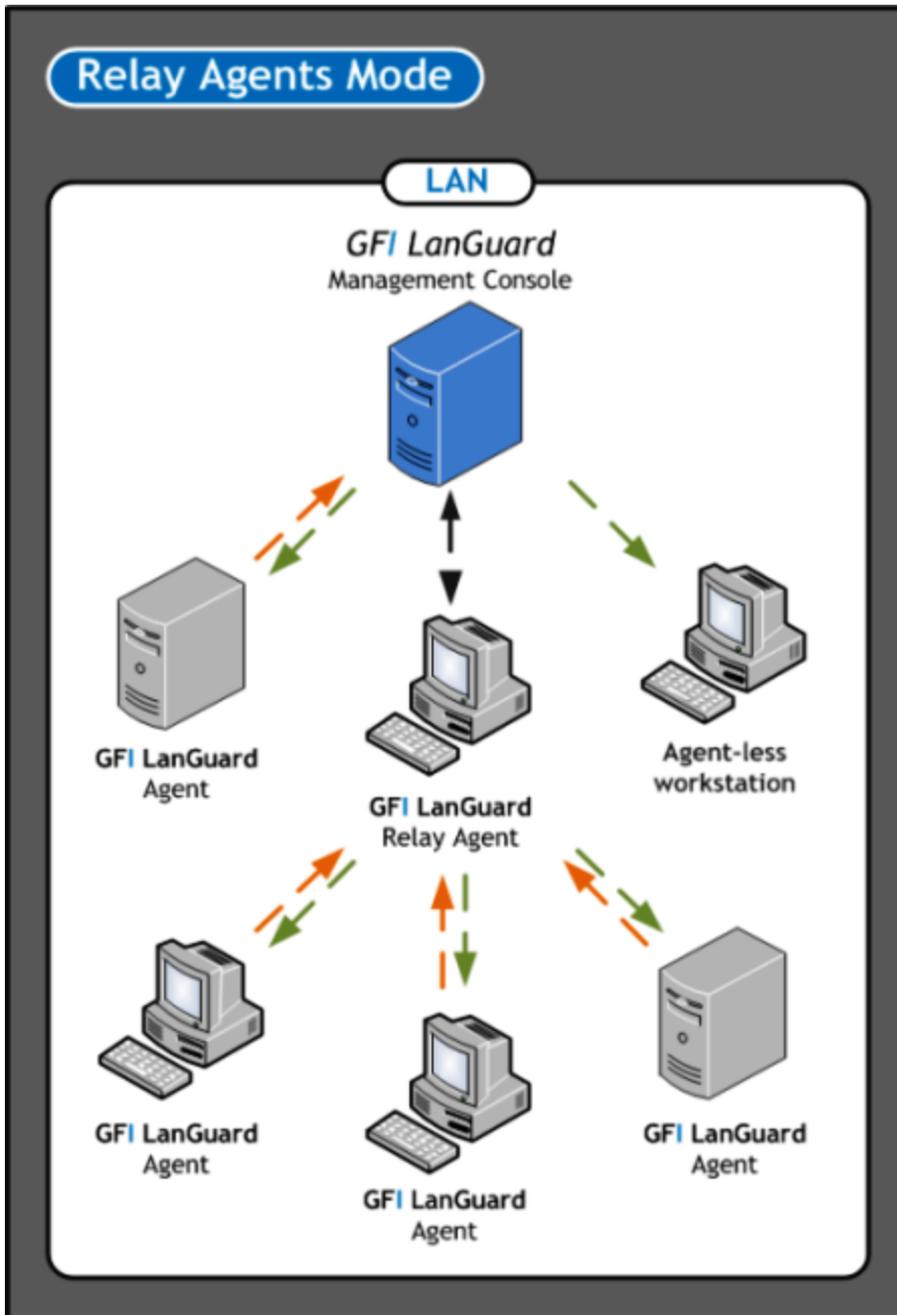


Figure 3: Relay Agent Mode



Note

For more information refer to **Configuring Relay Agents** from the **Administrator Guide**.

2.1.3 Deploying GFI LanGuard in Agent-less mode

Agent-less auditing is started from the GFI LanGuard management console. GFI LanGuard creates a remote session with the specified scan targets and audits them over the network. On completion, the results are imported into the results database and the remote session ends.

You can audit single computers, a range of specific computers and an entire domain/workgroup.



Note

Scans in Agent-less mode use the resources of the machine where GFI LanGuard is installed and utilize more network bandwidth since auditing is done remotely. When you have a large network of scan targets, this mode can drastically decrease GFI LanGuard's performance and affects network speed. In larger networks, deploy Agents/Relay Agents to balance the load appropriately.

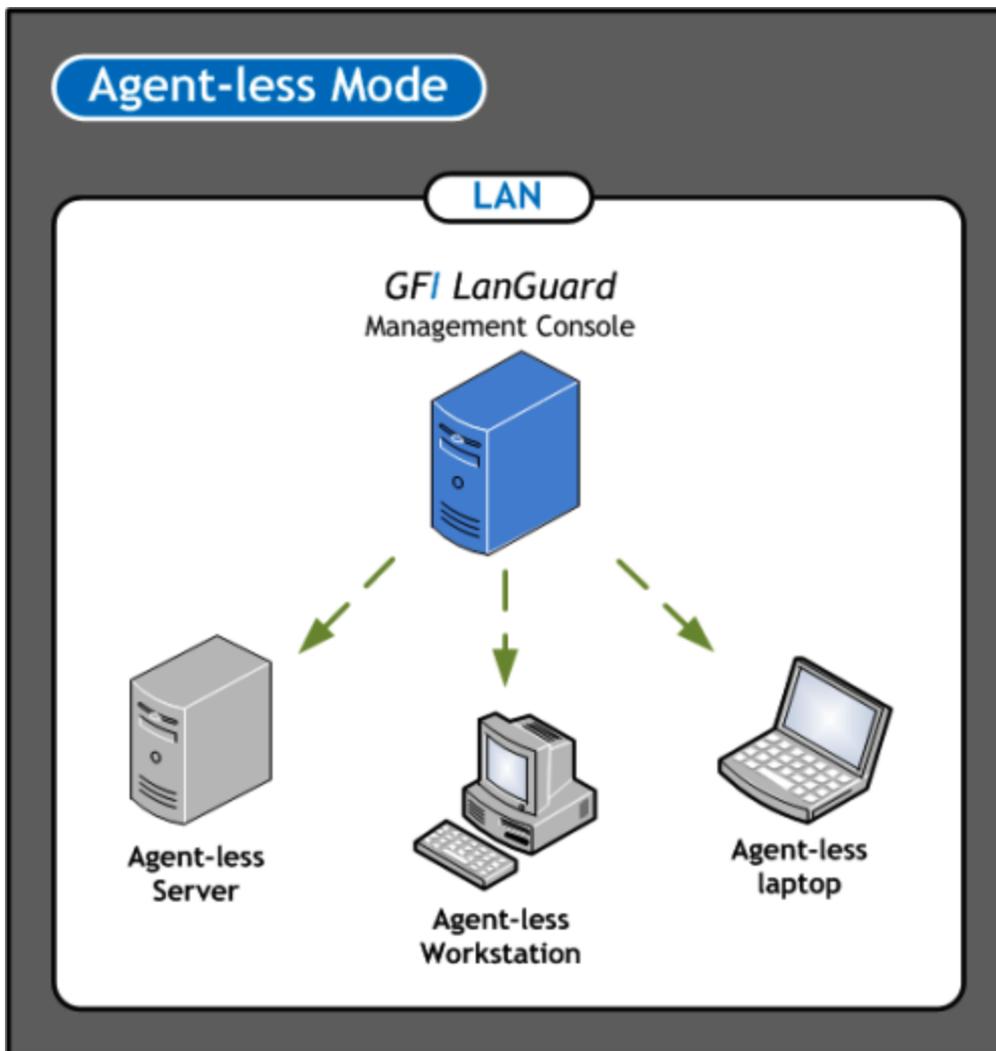


Figure 4: Agent-Less Mode

2.2 System requirements

Computers running GFI LanGuard Server/Agent/Relay Agent must meet the system requirements described below for performance reasons .



Note

If you are looking for a patch management solution for 2,000 or more computers, we recommend that you contact us for pricing, as well as suggestions regarding the proper deployment and management procedure for such a solution.

Refer to the following sections for information about:

- » [Hardware requirements](#)
- » [Software requirements](#)
- » [Firewall ports and protocols](#)
- » [Gateway permissions](#)
- » [Supported antivirus/anti-spyware applications](#)

2.2.1 Hardware requirements

Ensure that the below hardware requirements are met, on computers running any of the following components:

- » [GFI LanGuard Server](#)
- » [GFI LanGuard Agent](#)
- » [GFI LanGuard Relay Agent](#)

GFI LanGuard Server

Computers hosting GFI LanGuard Server must meet the following hardware requirements:

Table 3: Hardware requirements - GFI LanGuard Server

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

GFI LanGuard Agent

Computers running a GFI LanGuard Agent must meet the following hardware requirements:

Table 4: Hardware requirements - GFI LanGuard Agent

Component	Requirement
Processor	1 GHz
Physical Storage	350 MB
RAM	25 MB
Network bandwidth	1544 kbps

GFI LanGuard Relay Agent

A computer is eligible to be configured as a Relay Agent when:

- » The computer is online and has good uptime
- » Has fast network access to computers connected to it
- » Has the required disk space to allow caching.

Computers configured as Relay Agents must meet the following hardware requirements:

Table 5: Hardware requirements - GFI LanGuard Relay Agent

Component	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
RAM	2 GB	2 GB	4 GB
Network bandwidth	100 Mbps	100 Mbps	1 Gbps

2.2.2 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](#)
- » [Target computer components](#)
- » [Other software components](#)

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

The following table lists operating systems that GFI LanGuard Server/Agent/Relay Agent can be installed on:

Table 6: Supported Operating Systems

Operating System	GFI LanGuard	GFI LanGuard Agent	GFI LanGuard Relay Agent
Windows® Server 2012	✓	✓	✓
Windows® Server 2008 (including R2) Standard/Enterprise	✓	✓	✓
Windows® Server 2003 Standard/Enterprise	✓	✓	✓
Windows® 8	✓	✓	✓
Windows® 7 Professional/Enterprise/Ultimate	✓	✓	✓
Windows® Vista Business/Enterprise/Ultimate	✓	✓	✓
Windows® XP Professional (SP2 or higher)	✓	✓	✓
Windows® Small Business Server 2008 Standard	✓	✓	✓
Windows® Small Business Server 2003 (SP1)	✓	✓	✓
Windows® 2000 Professional/Server/Advanced	✗	✓	✓
» SP4			
» Internet Explorer 6 SP1 or higher			
» Windows Installer 3.1 or higher			

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:

Table 7: Supported database backends

Database	Recommended Use
Microsoft® Access	Recommended only during evaluation and for up to 5 computers.
MSDE/SQL Server Express® edition	Recommended for networks containing up to 500 computers.
SQL Server® 2000 or later	Recommended for larger networks containing 500 computers or more.

Target computer components

The following table provides you with information about components that are required to be installed/enabled on computers to be scanned remotely by GFI LanGuard:

Table 8: Software requirements - Additional components

Component	Description
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	Required to enumerate and collect information about scan targets.
Remote Registry	Required for GFI LanGuard to run a temporary service for scanning a remote target.

Additional GFI LanGuard Server components

The following additional component is required on the computer where the GFI LanGuard Server component is installed:

- » Microsoft .NET® Framework 3.5.

2.2.3 Firewall Ports and Protocols

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

- » [GFI LanGuard Server 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 **1070**, 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 1070 is already in use by another application, it automatically searches for an available port in the range of **1070-1170**.

To manually configure the communication port:

1. Launch GFI LanGuard.
2. Click **Configuration** tab > **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

GFI LanGuard communicates with managed computers (Agents and Agent-less), using the ports and protocols below. The firewall on managed computers needs to be configured to allow **Inbound** requests on ports:

Table 9: Ports and Protocols

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	Computer discovery.
445	SMB	Used while: <ul style="list-style-type: none"> » Auditing computers » Agent management » Patch deployment.

2.2.4 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:

- » *software.gfi.com/lnsupdate/
- » *.download.microsoft.com
- » *.windowsupdate.com
- » *.update.microsoft.com
- » All update servers of Third-Party Vendors supported by GFI LanGuard.



Note

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

2.2.5 Supported antivirus/anti-spyware applications

GFI LanGuard detects outdated definition files for a number of Anti-virus and Anti-spyware software. For a full list of supported Anti-virus and Anti-spyware software, refer to:

http://go.gfi.com/?pageid=security_app_fullreport

2.3 Upgrading from previous versions

GFI LanGuard retains all settings and result information from any previous version of GFI LanGuard. This enables you to:

- » Install GFI LanGuard without uninstalling the previous version.
- » Import settings to GFI LanGuard from other instances.
- » Deploy agents on the same machines where you have a previous version of GFI LanGuard installed.



Note

Software upgrades from versions older than GFI LanGuard 9 cannot be performed.

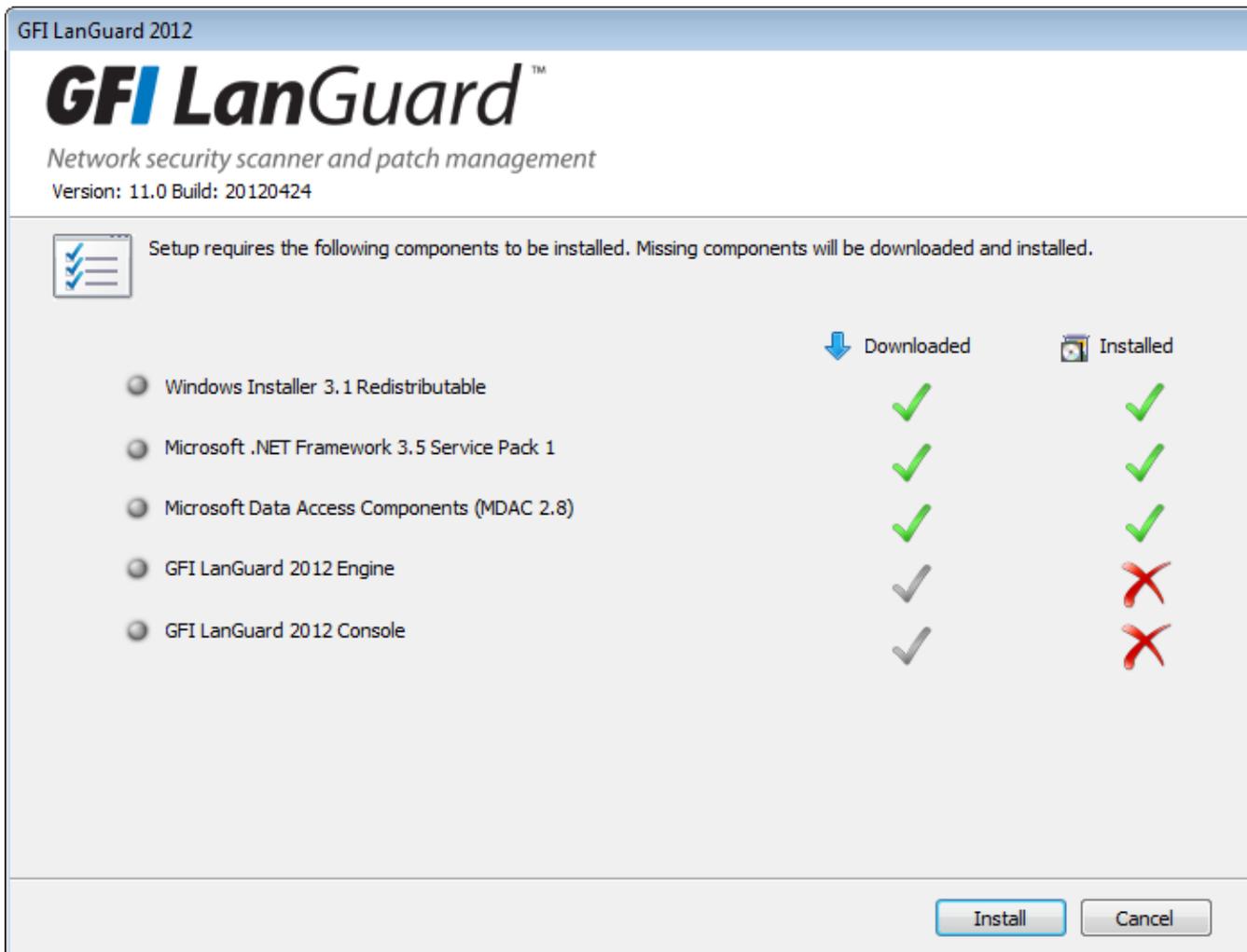


Note

License keys of earlier versions of GFI LanGuard are not compatible and must be upgraded to run GFI LanGuard.

To upgrade to a newer version:

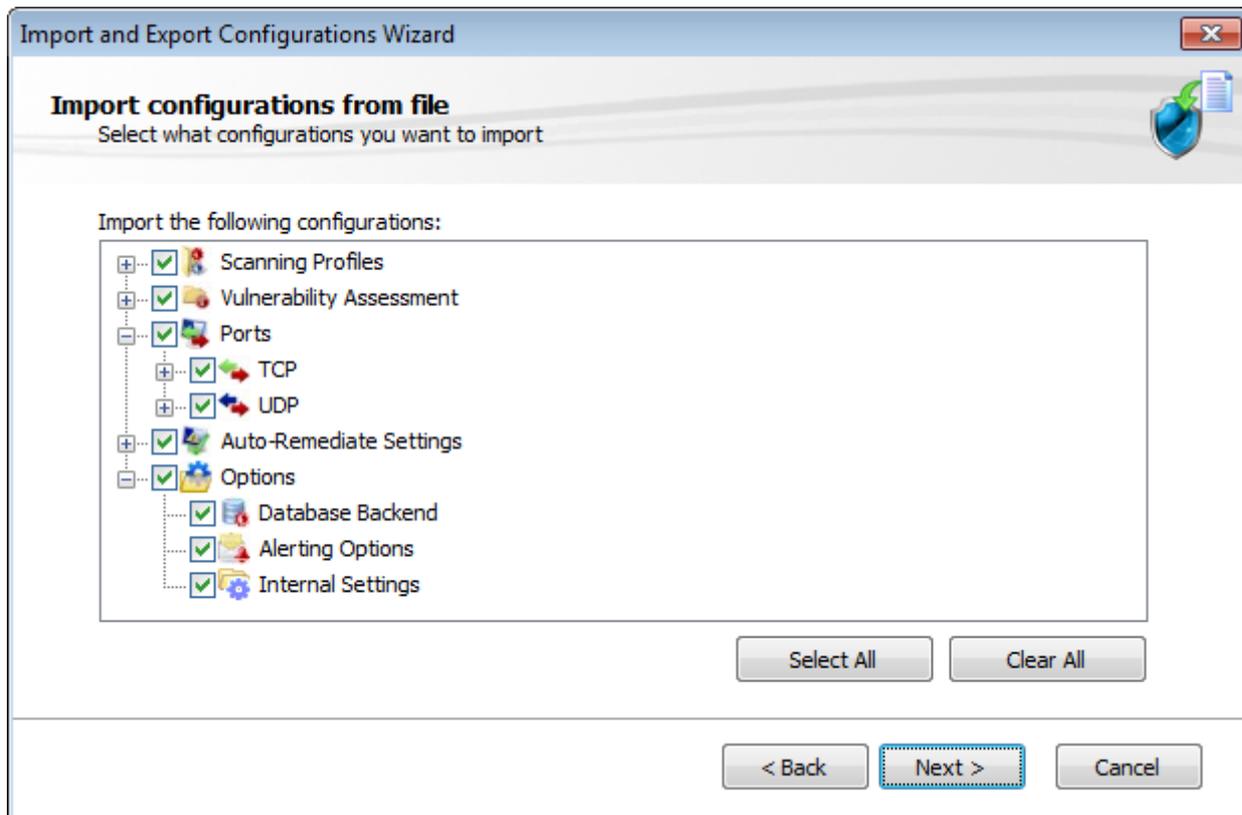
1. Logon using administrator credentials on the machine where you wish to install GFI LanGuard.
2. Launch GFI LanGuard installation.



Screenshot 1: Pre-requisite check dialog

3. The pre-requisite check dialog shows an overview of the status of the components required by GFI LanGuard to operate. Click **Install** to start the installation.

4. Follow the onscreen instructions to complete the upgrade.



Screenshot 2: Import and Export settings from a previous instance

5. Once GFI LanGuard is installed, it detects the previous installation and automatically launches the **Import and Export Configuration Wizard**. This enables you to export various configurations from the previous version and import them into the new one.
6. Select the configurations to import and click **Next** to finalize the import process.

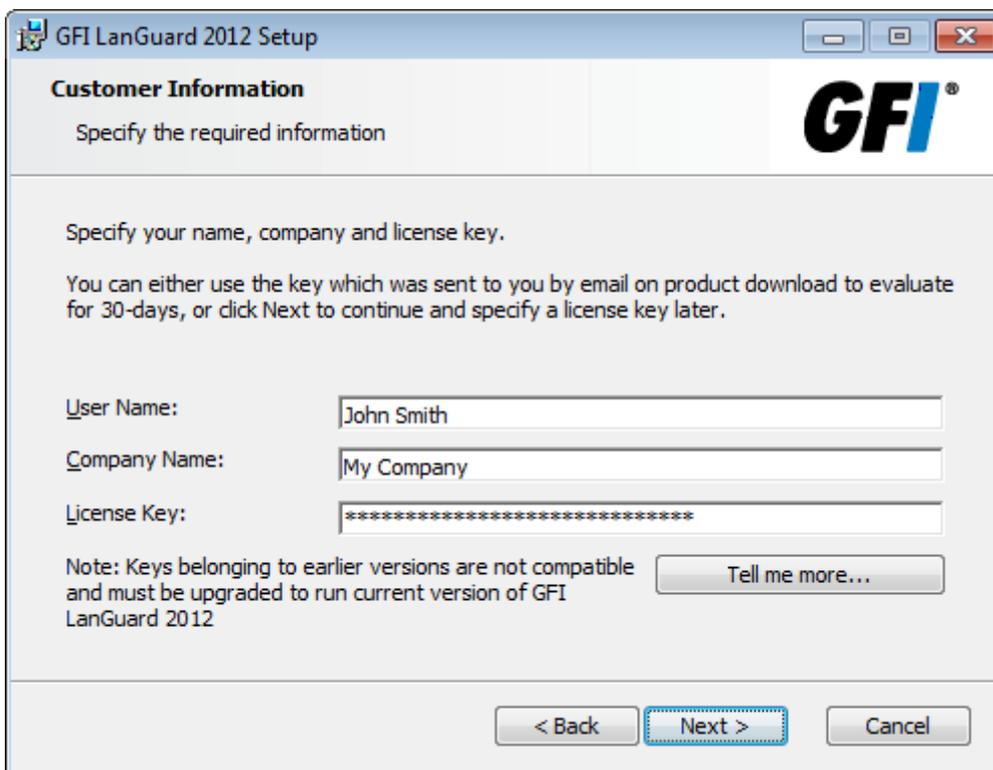
2.4 New installation

1. Logon using administrator credentials on the machine where to install GFI LanGuard.
2. Launch GFI LanGuard setup.
3. Click **Install** in the pre-requisite check window to download and install any missing required components.
4. In the GFI LanGuard welcome screen, click **Next**.



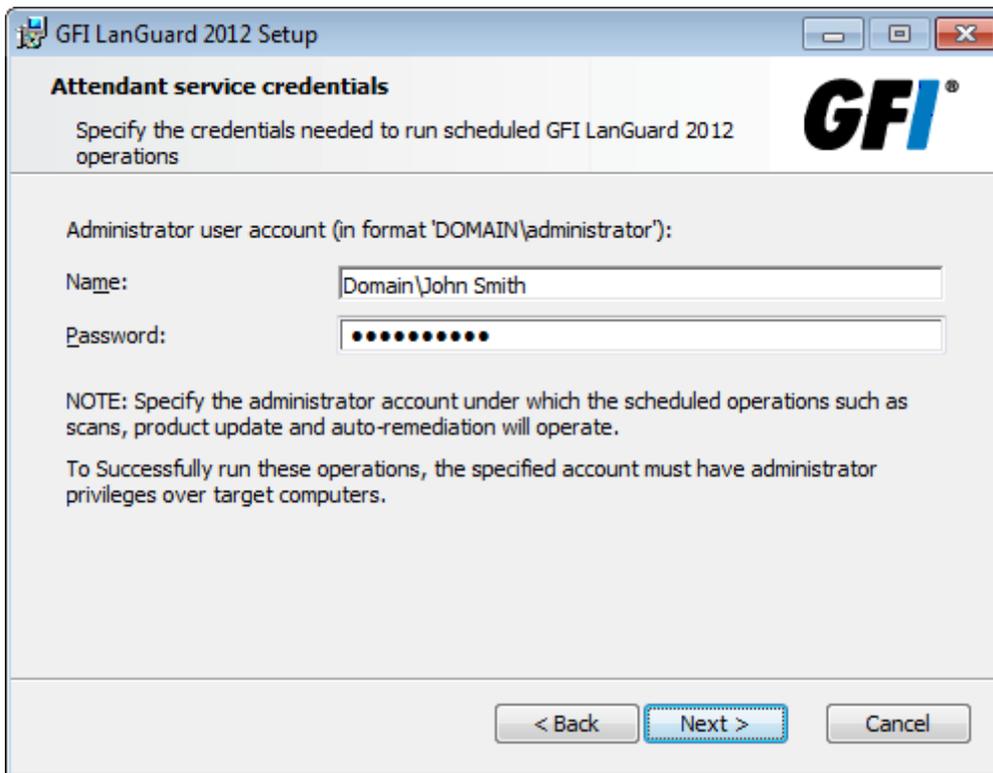
Screenshot 3: End-user license agreement

5. Read the licensing agreement carefully. To proceed with the installation, select **I accept the terms in the License Agreement** and click **Next**.



Screenshot 4: Specify user details and license key

6. Specify user details and enter license key. Click **Next**.



Screenshot 5: Attendant service credentials

7. Key in the administrator credentials and password. This is by the service under which scheduled operations operate. Click **Next** to continue setup.
8. Click **Install** to install GFI LanGuard in the default location or **Browse** to change path.
9. 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.



Note

An Internet connection is required to download missing components.



Note

If the credentials are invalid, a message stating that this option can be skipped is displayed. It is highly recommended to provide a valid username and password and not to skip this option.



Note

Use Microsoft Access database only if evaluating GFI LanGuard and using up to 5 computers. For more information refer to [Configuring Database Maintenance Options](#).



Note

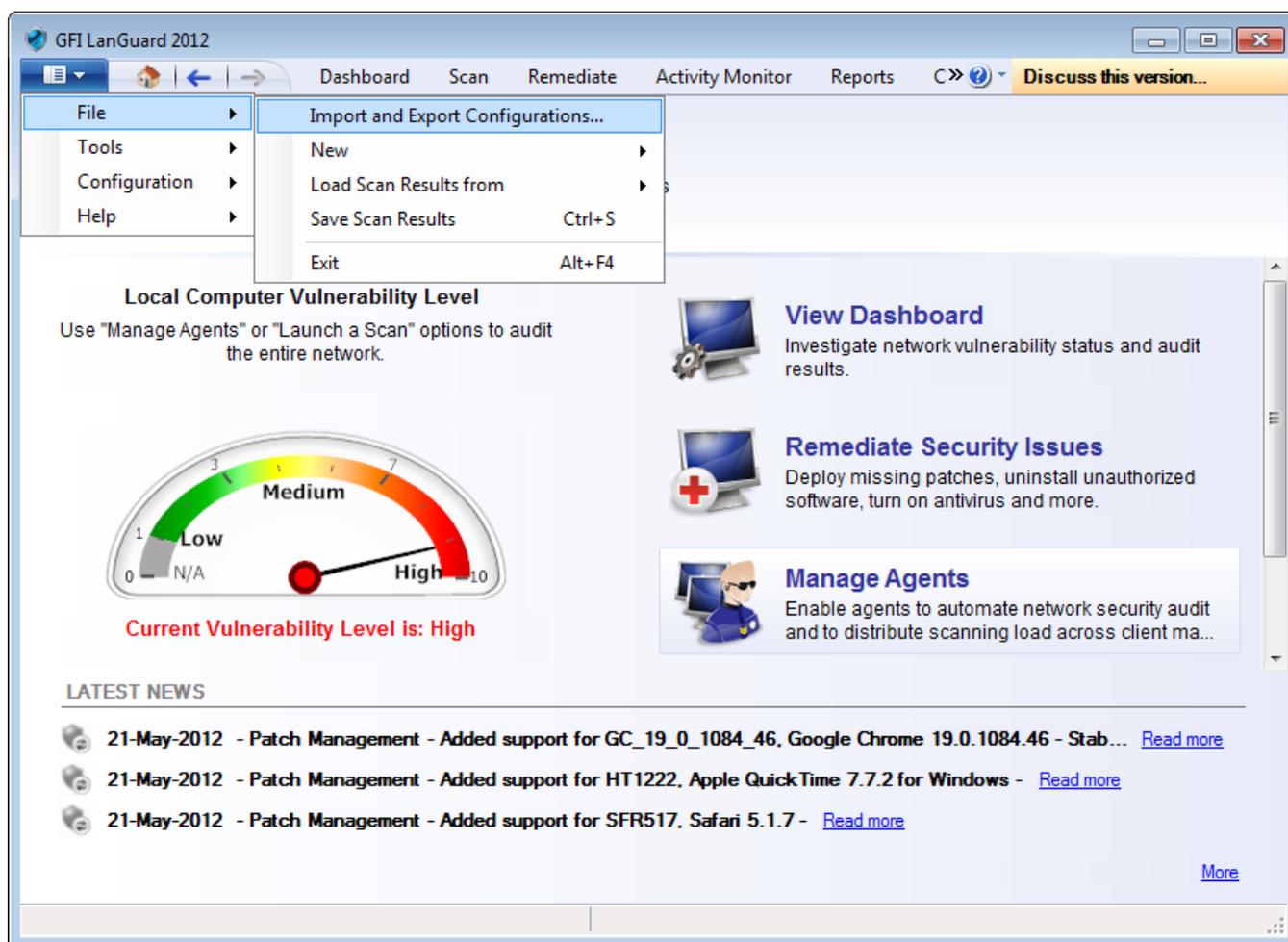
Test your installation after the product is installed. For more information, refer to [Testing the installation](#) (page 25).

2.5 Post install actions

GFI LanGuard can be installed on a machine with an older version of GFI LanGuard without uninstalling it. This enables you to retain configuration settings and reuse them in the new version.

To import the settings from the earlier version:

1. Launch the GFI LanGuard management console from **Start > Programs > GFI LanGuard 2012 > GFI LanGuard 2012**.
2. Click the **GFI LanGuard** button > **File > Import and Export Configurations...** to launch the **Import and Export Configurations** wizard.



Screenshot 6: Import and Export configurations

3. Select **Import the configuration from another instance** and click **Next**.
4. Click **Browse** to select the GFI LanGuard installation folder. The default location is:
 - » **64-bit machines (x64)** - <Local Disk>\Program Files (x86)\GFI\ LanGuard <Version>
 - » **32-bit machines (x86)** - <Local Disk>\Program Files\GFI\ LanGuard <Version>

5. Click **Next**.
6. Select the settings to import and click **Next**.
7. While importing, GFI LanGuard asks to override or keep existing settings. Select:

Table 10: Import override options

Option	Description
Yes	Override current setting with imported setting.
No	Keep current setting and ignore imported setting.
Auto Rename	Rename imported settings and keep the current settings.

8. Click **OK** when complete.

3 Testing the installation

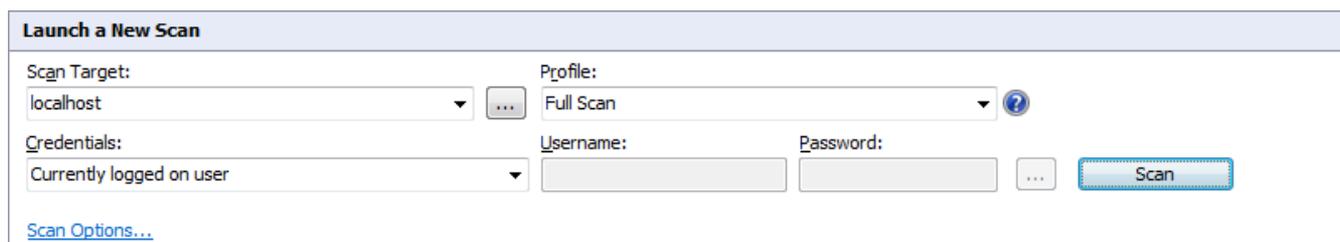
Once GFI LanGuard is installed, test your installation by running a local scan to ensure it installed successfully.

1. Launch GFI LanGuard.



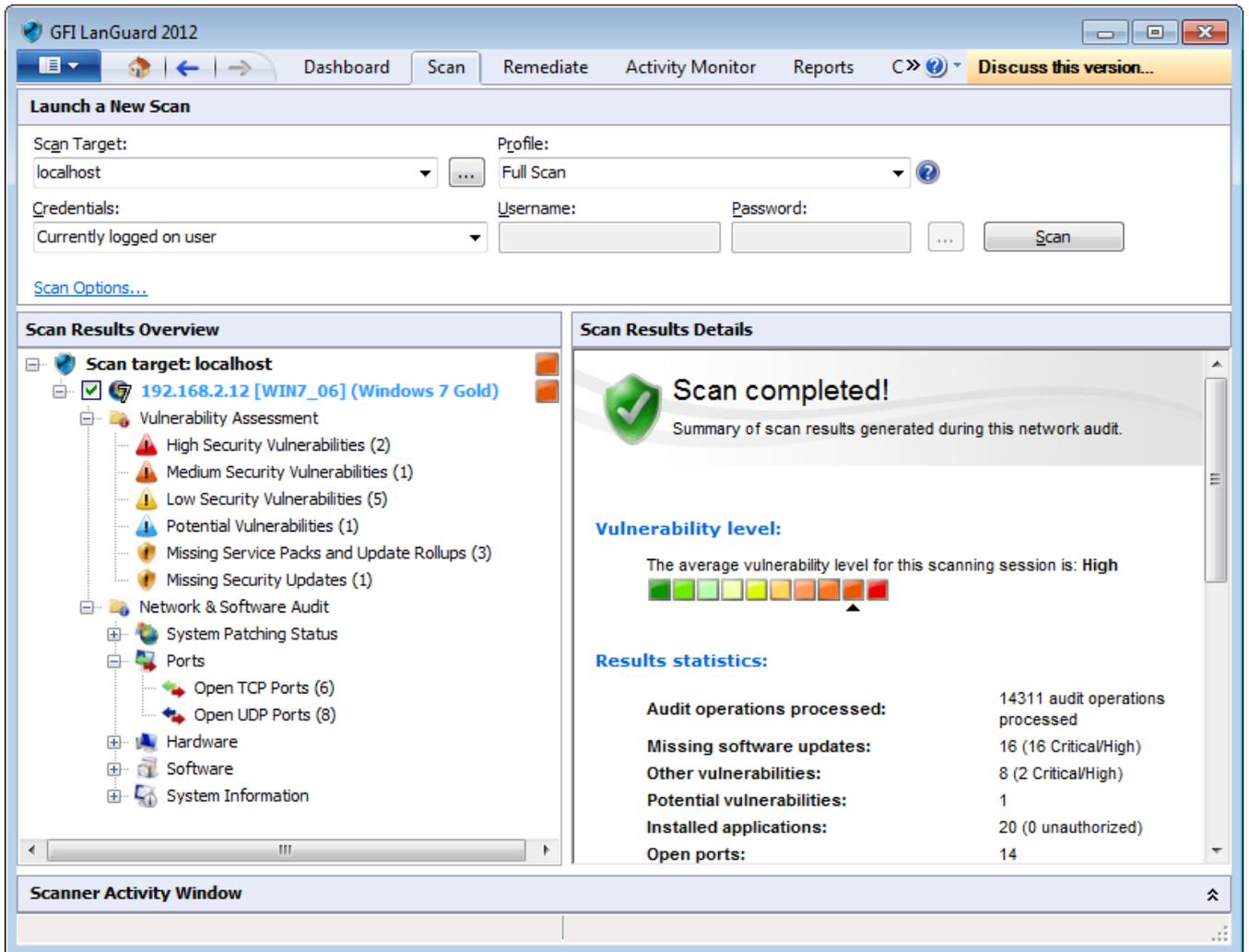
Screenshot 7: Launch a scan

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



Screenshot 8: 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 9: 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.

4 The GFI LanGuard Dashboard

The **Dashboard** section provides you with extensive security information based on data acquired during audits. Amongst others, the Dashboard enables you to determine the current network vulnerability level, the top-most vulnerable computers, and the number of computers in the database.

Topics in this chapter:

4.1 Achieving results from the dashboard	27
4.2 Using the Dashboard	27
4.3 Using the Computer Tree	28
4.4 Using Attributes	31
4.5 Dashboard actions	34
4.6 Exporting issue list	34
4.7 Dashboard views	35

4.1 Achieving results from the dashboard

The dashboard is an important feature of GFI LanGuard. As the central point of the application, it enables you to perform all the common tasks supported by GFI LanGuard, including:

- » Monitoring all computers managed by GFI LanGuard
- » Managing scan targets. Add, edit or remove computers, domains and workgroups
- » Deploying agents on scan targets and configure agent settings
- » Configuring computer credentials
- » Configuring auto-remediation options
- » Configuring recurrent network discovery on the managed domains/workgroups/OUs
- » Trigger security scans/refresh scan information
- » Analyze computers security state and audit details
- » Jump to relevant locations by clicking on security sensors and charts.

4.2 Using the Dashboard

This section provides the required information on how to use the GFI LanGuard Dashboard. To display the **Dashboard**:

1. Launch GFI LanGuard and click **Dashboard** tab.



Screenshot 10: View Dashboard

2. From the computers list, select a computer or computer group. The dashboard information updates according to your selection.

4.3 Using the Computer Tree

GFI LanGuard includes filtering and grouping options that enable you to quickly find a computer or domain and immediately display results.

When a computer or group is selected from the computer tree, results in the dashboard are automatically updated. Press **CRTL** and select multiple computers to display results for specific computers.

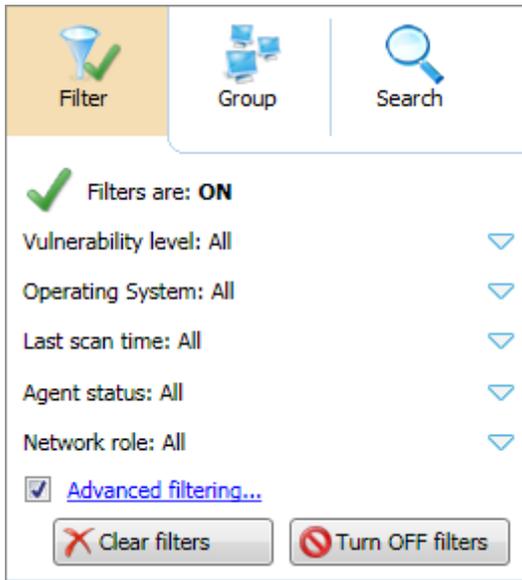
The following are functions supported by the computer tree:

- » [Simple filtering](#)
- » [Advanced filtering](#)
- » [Grouping](#)
- » [Searching](#)

4.3.1 Simple filtering

To filter for a specific computer or group:

1. From the left pane, click **Filter**.
2. Configure the criteria and click **Turn ON filters**.

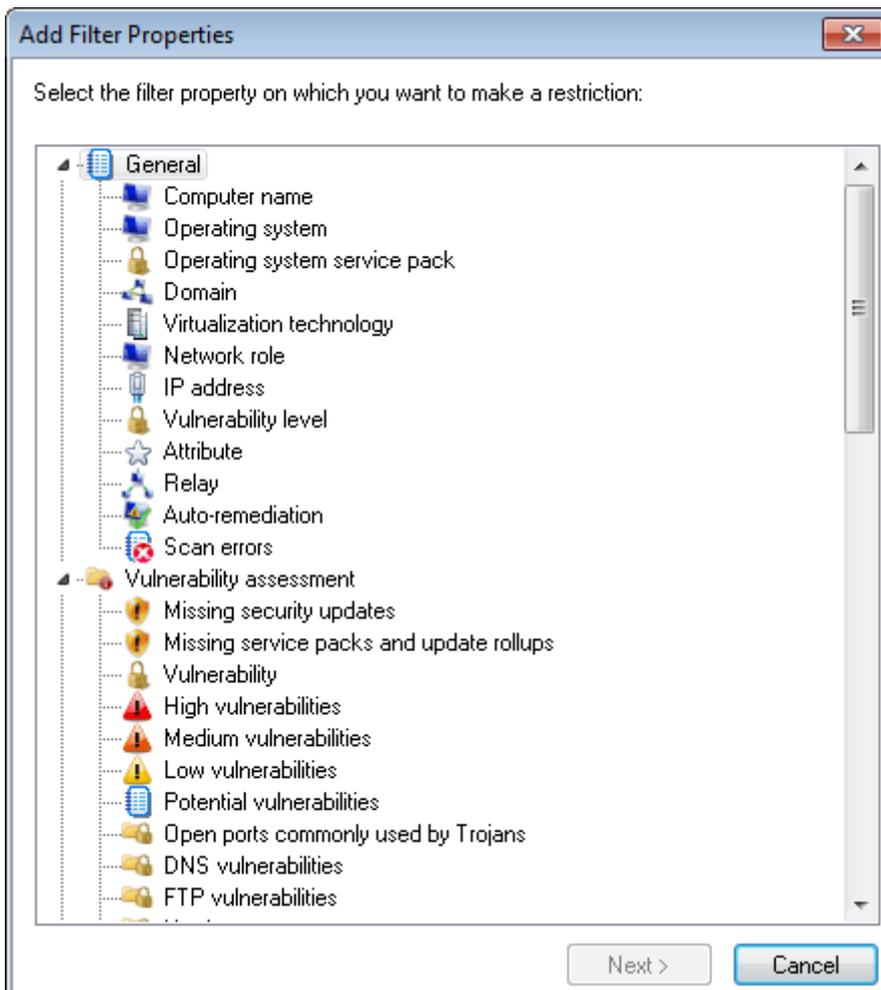


Screenshot 11: Simple filtering

4.3.2 Advanced filtering

To filter for a specific computer or group using advanced filtering:

1. From the left pane, click **Filter** and **Advanced filtering...**
2. From the **Advanced Filtering** dialog, click **Add**.



Screenshot 12: Add Filter Properties

3. Select the filter property to restrict and click **Next**.
4. Select the condition and key in the condition value. Click **Add**.
5. Repeat steps 2 to 4 for each condition. Click **OK**.

4.3.3 Grouping

To group machines by specific attributes:

1. From the left panel, click **Group**.
2. Select one of the following attributes:
 - » Domain and Organizational Unit
 - » Operating System
 - » Network Role
 - » Relays Distribution
 - » Attributes.



Note

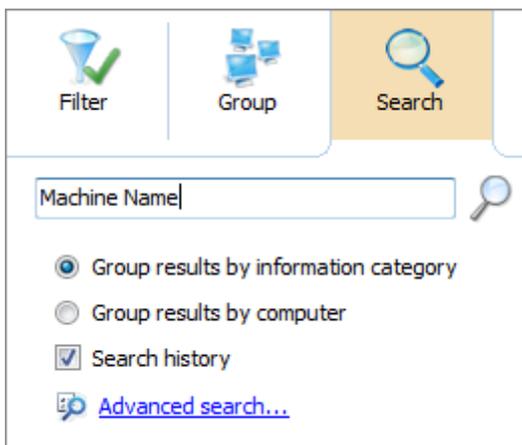
If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to [Using Attributes](#) (page 31).

3. If **Attributes** is selected, select the attribute from the drop-down list.
4. Click **Apply grouping**.

4.3.4 Searching

The Search tab within the **Computers tree** enables you to search and display results for a specific computer or group. To display results for a specific computer:

1. From the **Computers tree**, select **Search**.



Screenshot 13: Search specific computers and groups

2. Key in the search criteria and use the following options:

Table 11: Search options

Option	Description
Group results by information category	Search results are grouped by category. The result contains the latest computer information. Amongst others results are grouped by: <ul style="list-style-type: none"> » Computer Information » Hardware devices » Logged on Users » Processes » Virtual technology
Group results by computer	Search results are grouped by computer name. The result contains the latest computer information.
Search History	Search results include the information from previous scans.
Advanced search	Configure advanced search options. <p> Note For more information, refer to the Full Text Searching section of the Administrator Guide.</p>

4.4 Using Attributes

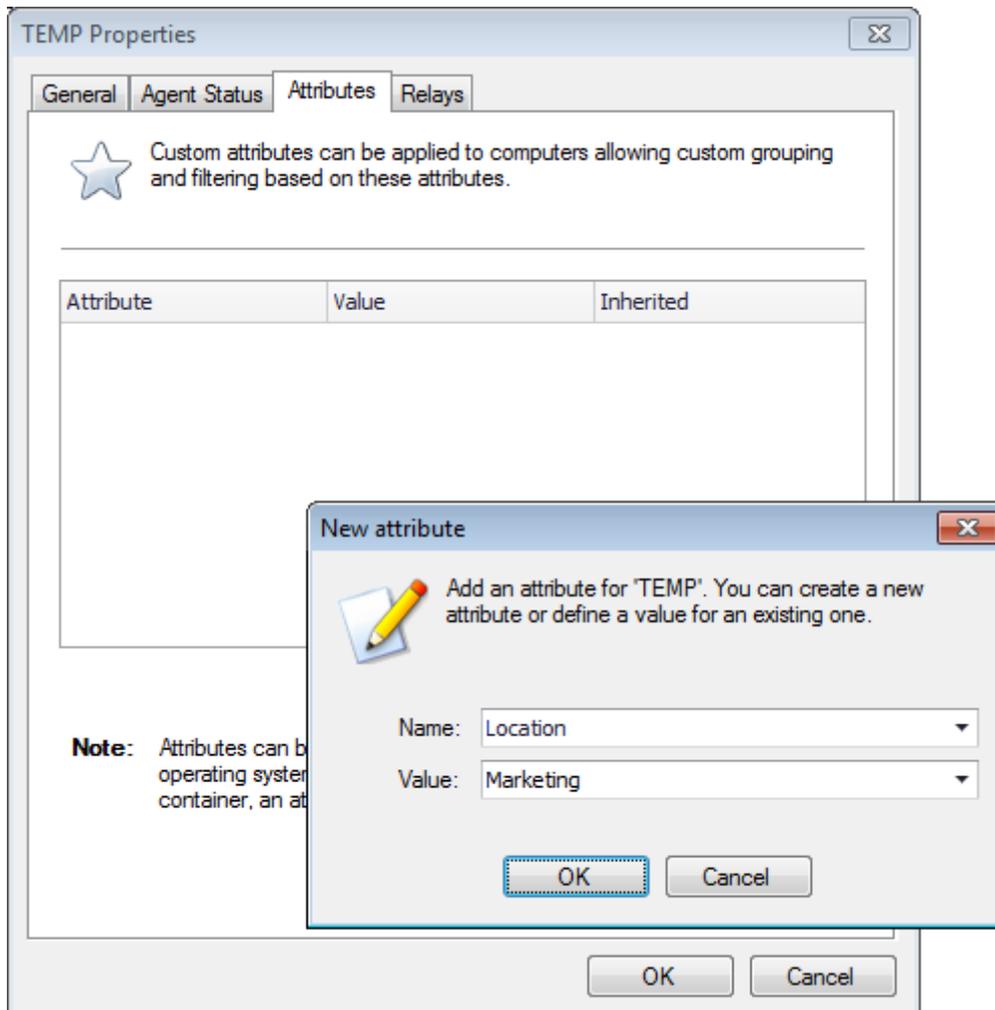
Attributes enable you to group and configure single or multiple computers at one go. Attributes also enable you to remediate vulnerabilities or deploy software on specific computers based on the assigned attribute. The following sections contain information about:

- » [Assigning attributes to a computer](#)
- » [Assigning attributes to a group](#)
- » [Configuring attributes](#)

4.4.1 Assigning attributes to a computer

To assign attributes to a single computer:

1. Click **Dashboard** tab.
2. From the computer tree, right-click a computer and select **Assign attributes**.



Screenshot 14: Assigning attributes: Single computer

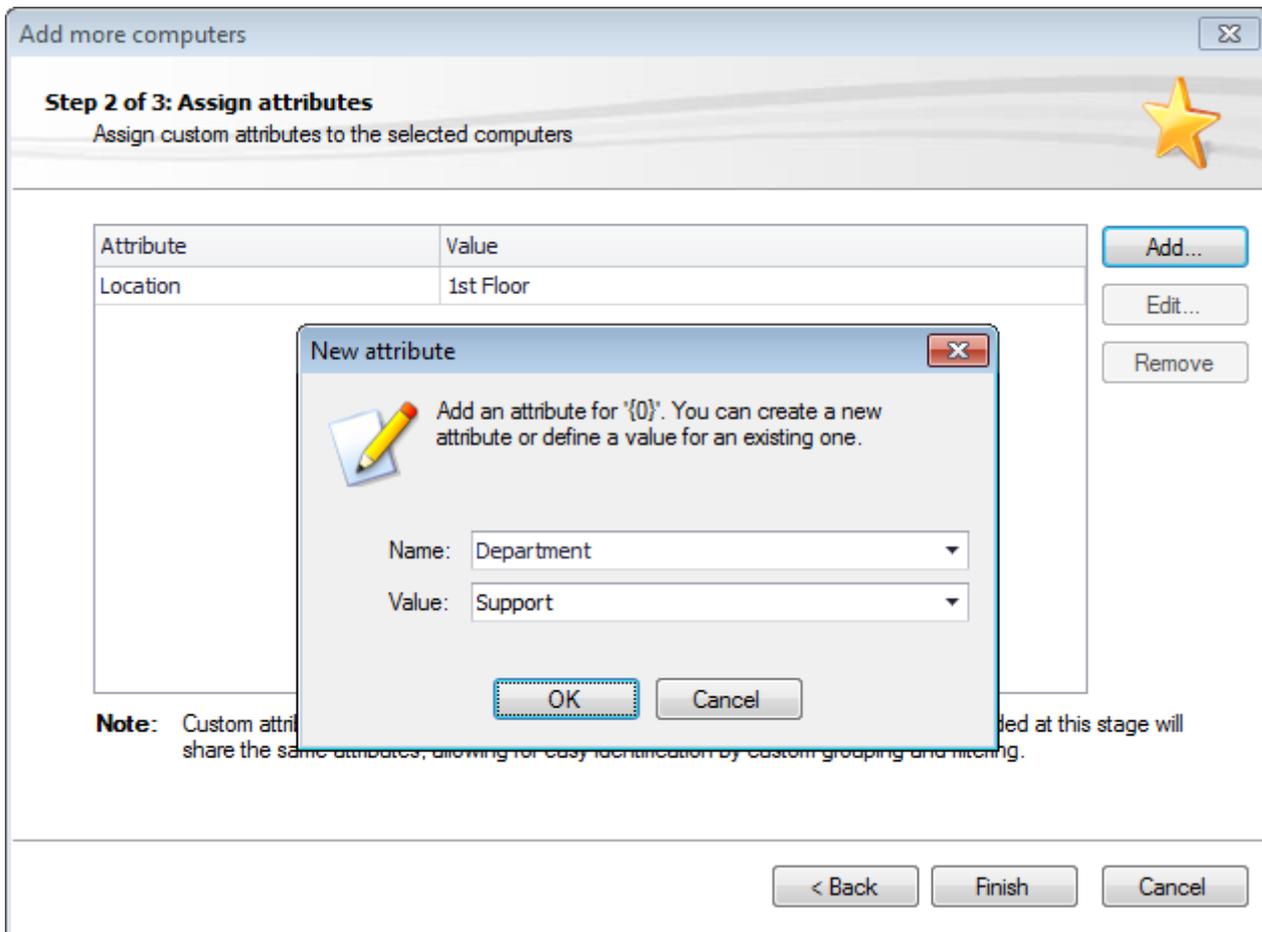
3. From the **Properties** dialog > **Attributes** tab, click **Add**.
4. Configure new attributes settings and click **OK**.
5. Click **OK** to save your settings.

4.4.2 Assigning attributes to a group

GFI LanGuard enables you to assign attributes to specific groups, domains, organizational units and networks. Once attributes are assigned, each member of the selected group inherits the attributes settings.

To assign attributes to a group:

1. Click **Dashboard** tab.
2. From the computers list, right-click network and select **Assign attributes**.
3. From the **Add more computers** wizard, select network and click **Next**.



Screenshot 15: Assigning attributes: Multiple computers

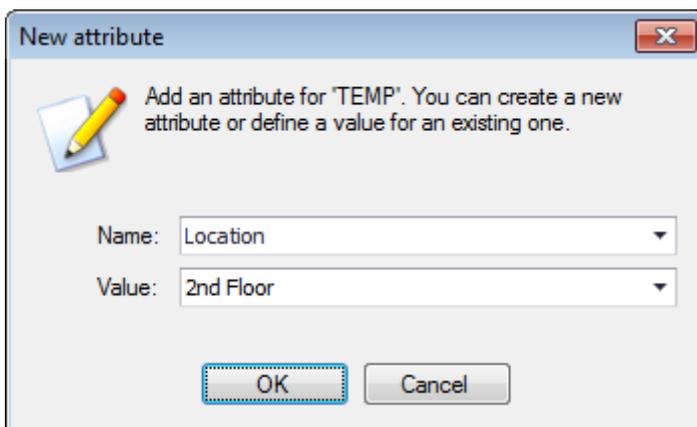
4. Click **Add** and configure the respective attributes. Use the **Edit** and **Remove** buttons to edit or remove the selected attributes.

5. Click **Finish** to save your settings.

4.4.3 Configuring attributes

To configure attributes:

1. From the **Properties** dialog, click **Attributes** tab.
2. Click **Add** to launch the **New attribute** dialog.



Screenshot 16: New attribute dialog

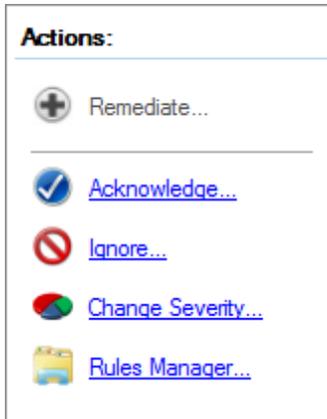
3. From the **Name** drop-down menu, select an attribute or key-in a name to create a new one.

4. Specify a value for the attribute in the **Value** field. Click **OK**.
5. Repeat steps 2 to 4 until you add all the required attributes.
6. Click **OK** to save your settings.

4.5 Dashboard actions

The **Actions** section enables you to manage and remediate vulnerabilities and missing patches found in your network. To access the **Actions** section:

1. Select **Dashboard** tab.
2. Click **Vulnerabilities** or **Patches** tab.



Screenshot 17: Actions section in the Dashboard

3. Select one of the following actions:

Table 12: Dashboard actions

Action	Description
Remediate	Launch the Remediation Center to deploy and manage missing patches.  Note For more information, refer to the Manual Remediation section of the Administrator Guide.
Acknowledge	Launch the Rule-Acknowledge Patch dialog. This enables you to acknowledge issues so that they will not affect the Vulnerability level of your network. Configure for which machine this rule applies
Ignore	Launch the Rule-Ignore Patch dialog. This enables you to ignore missing patches or vulnerabilities so that they will not be reported as issues in the future. Configure for which machine this rule applies and the time span that the issue is ignored.
Change Severity	Launch the Rule-Change Severity dialog. This enables you to change the severity level of vulnerability. Configure for which machines this rule applies and the severity level.
Rules Manager	Launch the Rules Manager dialog. This enables you to search and remove configured rules.

4.6 Exporting issue list

GFI LanGuard enables you to export issue lists to Portable Document Format (PDF), Microsoft Office Excel (XLS) or Hyper Text Markup Language (HTML). When a list supports exporting, these icons



are displayed in the top-right corner of the list. Select the respective icon and configure the export settings.

4.7 Dashboard views

The GFI LanGuard dashboard is made up of multiple views. These different views enable real-time monitoring of your scan targets and allow you to perform instant remedial and reporting operations. The following sections contain information about:

- » [Dashboard overview](#)
- » [Computers view](#)
- » [History view](#)
- » [Vulnerabilities view](#)
- » [Patches view](#)
- » [Ports view](#)
- » [Software view](#)
- » [Hardware view](#)
- » [System Information view](#)

4.7.1 Overview



Screenshot 18: Dashboard Overview

The **Dashboard Overview** is a graphical representation of the security level/vulnerability level of a single computer, domain or entire network.

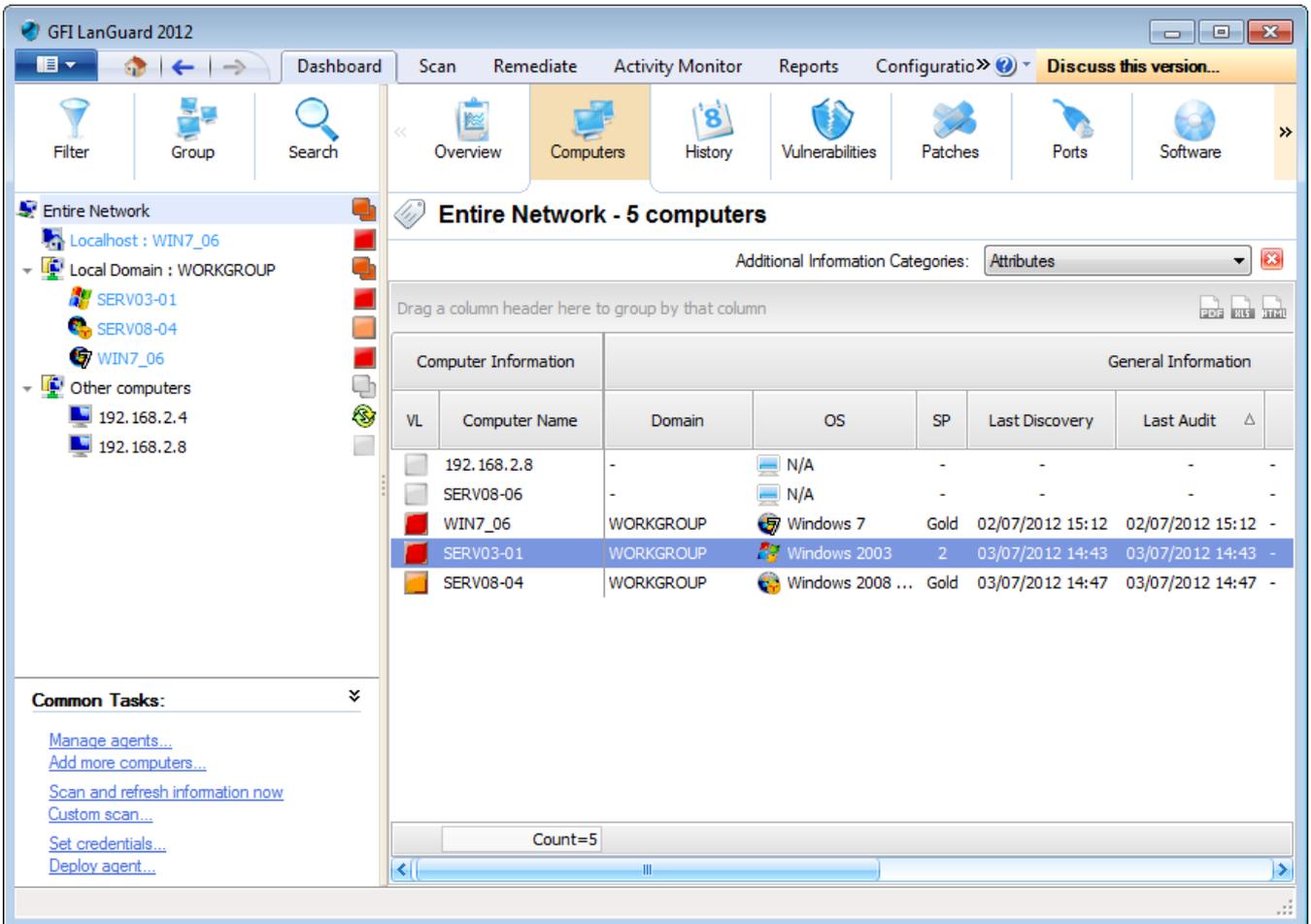
When a computer or domain is selected, the results related to the selected computer/domain are automatically updated in the dashboard. Below is a description of each section found in the dashboard:

Table 13: Software information from an audit

Section	Description
Network security level	This rating indicates the vulnerability level of a computer/network, depending on the number and type of vulnerabilities and/or missing patches found. A high vulnerability level is a result of vulnerabilities and/or missing patches which average severity is categorized as high.
Computer vulnerability distribution	This chart is available only when selecting a domain or a workgroup, and displays the distribution of vulnerabilities on your network. This chart enables you to determine how many computers have high, medium and low vulnerability rating.
Most vulnerable computers	This list is available only when selecting a domain or a workgroup, and shows the most vulnerable computers discovered during the scan. The icon color on the left indicates the vulnerability level.
Agent Status	<p>When selecting a domain or workgroup, a chart showing the overall agent status of all computers within the domain/workgroup is displayed. This enables you to determine the number of agents installed or pending installation on the selected domain/workgroup. When selecting a single computer, this section displays an icon representing the agent status. The icons are described below:</p> <ul style="list-style-type: none"> »  Not installed - Agent is not installed on the target machine. »  Pending installation - Installation is pending. A status can be pending when the machine is offline or the agent is being installed. »  Pending uninstall - Uninstallation is pending. A status can be pending when the machine is offline or the agent is being uninstalled. »  Installed - Agent is installed on the target machine. »  Relay Agent Installed - The selected computers are relay agents.
Audit status	This chart is available only when selecting a domain or workgroup and enables you to identify how many audits have been performed on your network grouped by time.
Vulnerability trends over time	When a domain or workgroup is selected, this section displays a line graph showing the change of vulnerability level over time grouped by computer count. When a single computer is selected, this section displays a graph showing the change of vulnerability level over time for the selected computer.
Computers by network role	This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by network role. Amongst other roles, this graph identifies the number of servers and workstations per selected domain.
Computers by operating system	This chart is available only when selecting a domain or a workgroup and displays the number of audited computers, grouped by the installed operating system.
Computer details	This section is available when selecting a single computer and enables you to view the selected computer details.
Scan activity	This line graph is available only when selecting a single computer and enables you to view the number of scans/audits performed on the selected computer. In addition enables you to verify if scheduled scans are being performed.

Section	Description
Remediation Activity	This line graph is available only when selecting a single computer and enables you to view the number of remediation activities performed on the selected computer. In addition, this graph enables you to verify that auto-remediation is performed.
Top 5 Issues to Address	This section is available only when selecting a single computer, and displays the top five issues to address for the selected computer.
Results statistics	This section is available only when selecting a single computer and displays an overview of the audit result. Amongst others, the result enables you to identify the number of missing patches, number of installed applications, open ports and running services.
Security Sensors	This section enables you to identify issues at a glance. Click a sensor to navigate and display issues and vulnerabilities for a specific computer or group. Sensors enable you to identify: <ul style="list-style-type: none"> » Missing Software Updates » Missing service packs » Vulnerabilities » Firewall Issues » Unauthorized Applications » Audit Status » Credentials setup » Malware Protection Issues » Agent Health Issues.

4.7.2 Computers view



Screenshot 19: Analyze results by computer

Select this view to group audit results by computer. From the drop-down list, select one of the options described below:

Table 14: View by computers information

Option	Description
Agent Details	Select this option to view the agent status. This option enables you to identify if an agent is installed on a computer and if yes, displays the type of credentials being used by the agent.
Vulnerabilities	View the number of vulnerabilities found on a computer grouped by severity. Severity of a vulnerability can be: <ul style="list-style-type: none"> » High » Medium » Low » Potential.
Patching status	View the number of: <ul style="list-style-type: none"> » Missing Security/non-Security Updates » Missing Service Packs and Update Rollups » Installed Security/non-Security Updates » Installed Service Packs and Updates Rollups.

Option	Description
Open ports	View the number of: <ul style="list-style-type: none"> » Open TCP ports » Open UDP ports » Backdoors.
Software	View the number of: <ul style="list-style-type: none"> » Antiphishing engines » Antispyware engines » Antivirus engines » Backup applications » Data loss prevention applications » Device access and desk encryption applications » Firewalls » Installed applications » Instant messengers » Peer to peer applications » Unauthorized applications » Virtual machines » VPN clients » Web browsers.
Hardware	View information on: <ul style="list-style-type: none"> » Number of disk drives » Free disk space » Memory size » Number of processors » Other hardware.
System information	View information on: <ul style="list-style-type: none"> » The number of shared folders » Number of groups » Number of users » Logged users » Audit policy status.
Attributes	Adds an Attributes column and groups your scan targets by the assigned attribute.



Note

To launch the **Overview** tab and display more details on a specific computer, double click a computer from the list.

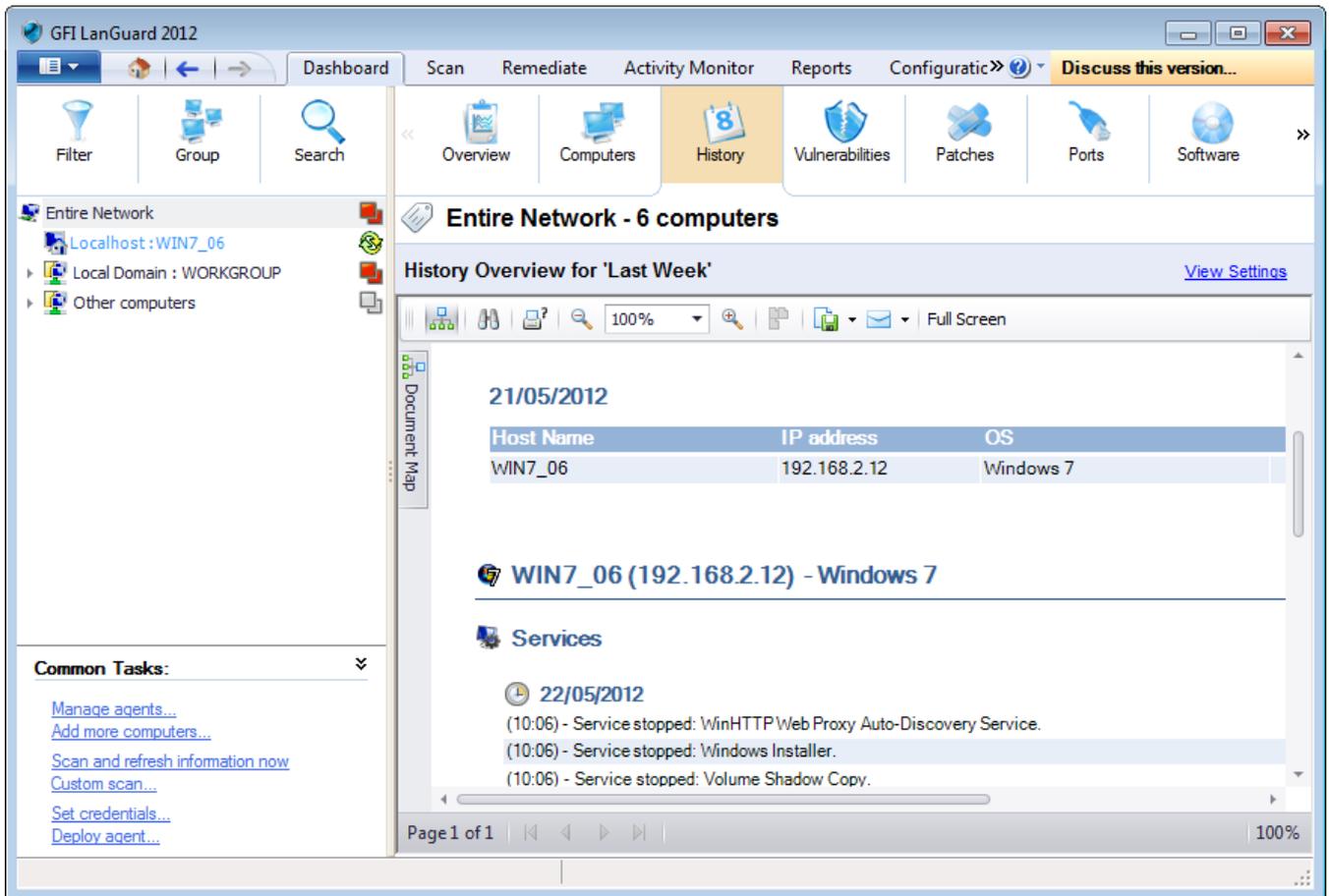


Note

Drag and drop a column header in the designated area to group data by criteria.

4.7.3 History view

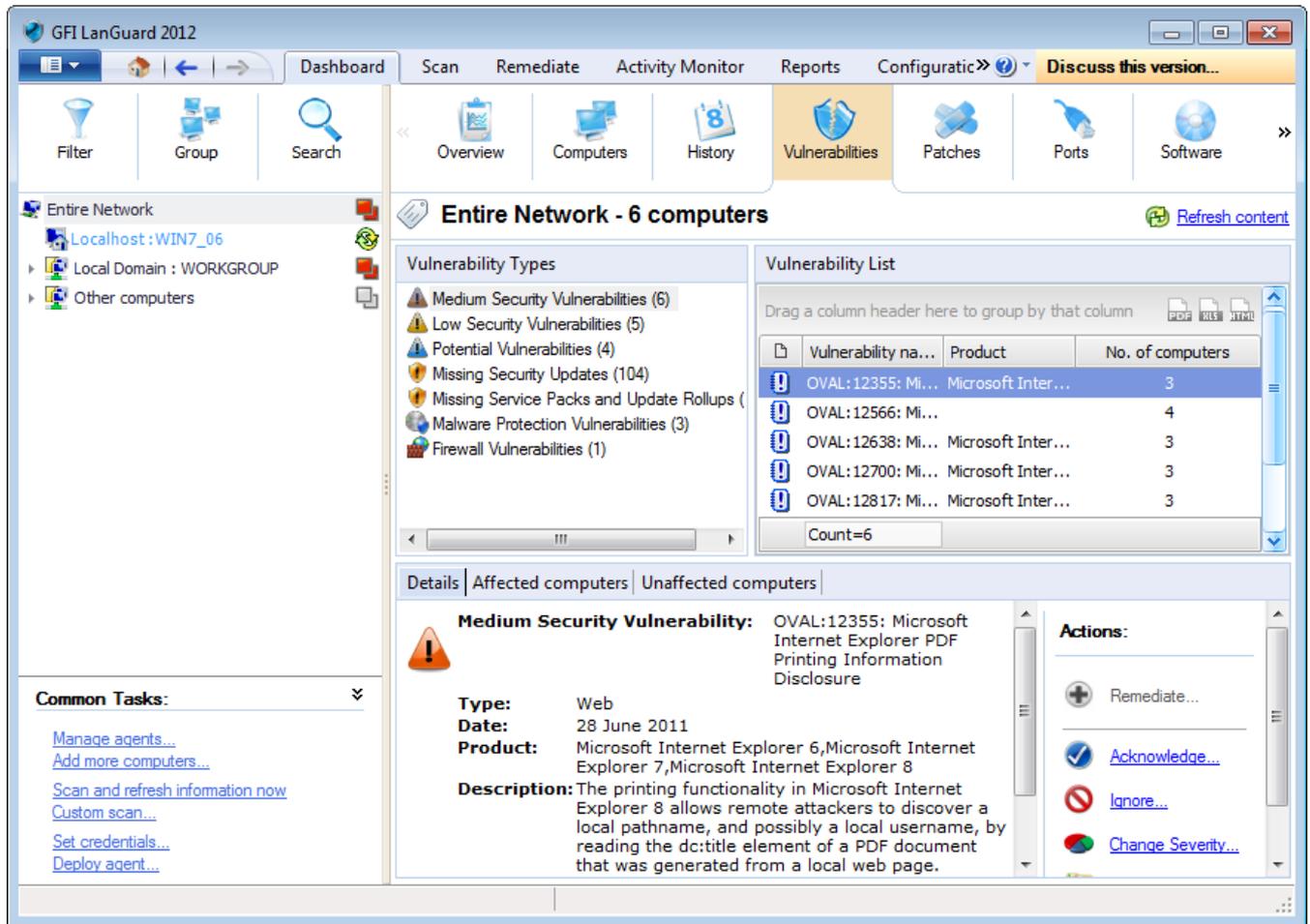
Select this view to group audit results by date for a specific computer. To configure the history starting date or history period click the link provided.



Screenshot 20: History view in the Dashboard

4.7.4 Vulnerabilities View

Display more details on the vulnerabilities found on a network and the number of affected computers. When a vulnerability is selected from the **Vulnerability List**, the **Details** section provides more information on the selected vulnerability. From the **Details**, section click **Affected computers** or **Unaffected computers** to display a list of affected and unaffected computers.



Screenshot 21: Vulnerabilities view in the Dashboard



Note

Drag and drop a column header in the designated area to group data by criteria.

4.7.5 Patches View

Display more details on the missing/installed patches and service packs found during a network audit. When a patch/service pack is selected from the list, the **Details** section provides more information on the selected patch/service pack. From the **Details** section, click **Missing on** to display a list of computers having the selected patch missing.

The screenshot shows the GFI LanGuard 2012 interface. The top navigation bar includes 'Dashboard', 'Scan', 'Remediate', 'Activity Monitor', 'Reports', 'Configuratic...', and 'Discuss this version...'. The main navigation area has icons for 'Filter', 'Group', 'Search', 'Overview', 'Computers', 'History', 'Vulnerabilities', 'Patches', 'Ports', and 'Software'. The 'Patches' view is active, showing 'Entire Network - 6 computers'. The 'Patch Types' section lists: Missing Security Updates (104), Missing Non-Security Updates (85), Missing Service Packs and Update Rollups (1), Installed Security Updates (94), Installed Non-Security Updates (26), and Installed Service Packs and Update Rollups (1). The 'Patch List' table has columns: Patch n..., Date ..., Sev..., Applies to, and No. of computers. The first row is selected: AP SB12-09, 2012-05-04, Critical, Adobe Flash Player 11.2.202.235 exe, 1. The 'Details' section for this patch shows: **Missing Security Update:** AP SB12-09: Adobe Flash Player 11.2.202.235 exe. **Bulletin ID:** AP SB12-09. **QNumber:** AP SB12-09. **Date:** 04 May 2012. **Severity:** Critical. **Applies to:** Adobe Flash Player 11. **Description:** These players contain fixes for critical vulnerabilities identified in Security Bulletin AP SB12-09. All users are encouraged to update to the new players v11.2.202.235. **URL:** <http://www.adobe.com/support/security/bulletins/apsb12-09.html>. The 'Actions' panel includes: Remediate..., Acknowledge..., Ignore..., Change Severity..., and Rules Manager...

Screenshot 22: Patches view in Dashboard



Note

Drag and drop a column header in the designated area to group data by criteria.

4.7.6 Ports View

Display more details on the open ports found during a network audit. When a port is selected from the **Port List**, the **Details** section provides more information on the selected port. From the **Details** section, click **View computers having this port open** to display a list of computers having the selected port open.

The screenshot shows the GFI LanGuard 2012 interface. The top navigation bar includes 'Dashboard', 'Scan', 'Remediate', 'Activity Monitor', 'Reports', 'Configuratic...', and 'Discuss this version...'. The main navigation area has icons for Filter, Group, Search, History, Vulnerabilities, Patches, Ports (selected), Software, Hardware, and System Information. The left pane shows the 'Entire Network' tree with 'Localhost: WIN7_06', 'Local Domain: WORKGROUP', and 'Other computers'. The main content area is titled 'Entire Network - 6 computers' and shows 'Port Types' (Open TCP Ports (11), Open UDP Ports (8)) and a 'Port List' table. The 'Port List' table has columns for Port, Process, and No. of computers. The selected row is 'TCP 135' with 2 computers. Below the table is a 'Details' section for 'Open TCP Port: TCP 135' with fields for Type (TCP), Port number (135), and Description (DCE endpoint resolution). A link 'View computers having this port open' is also present.

Port	Process	No. of computers
TCP 135		2
TCP 135	svchost.exe	2
TCP 139		4
TCP 445		2
TCP 445	System	2

Screenshot 23: Ports view in Dashboard

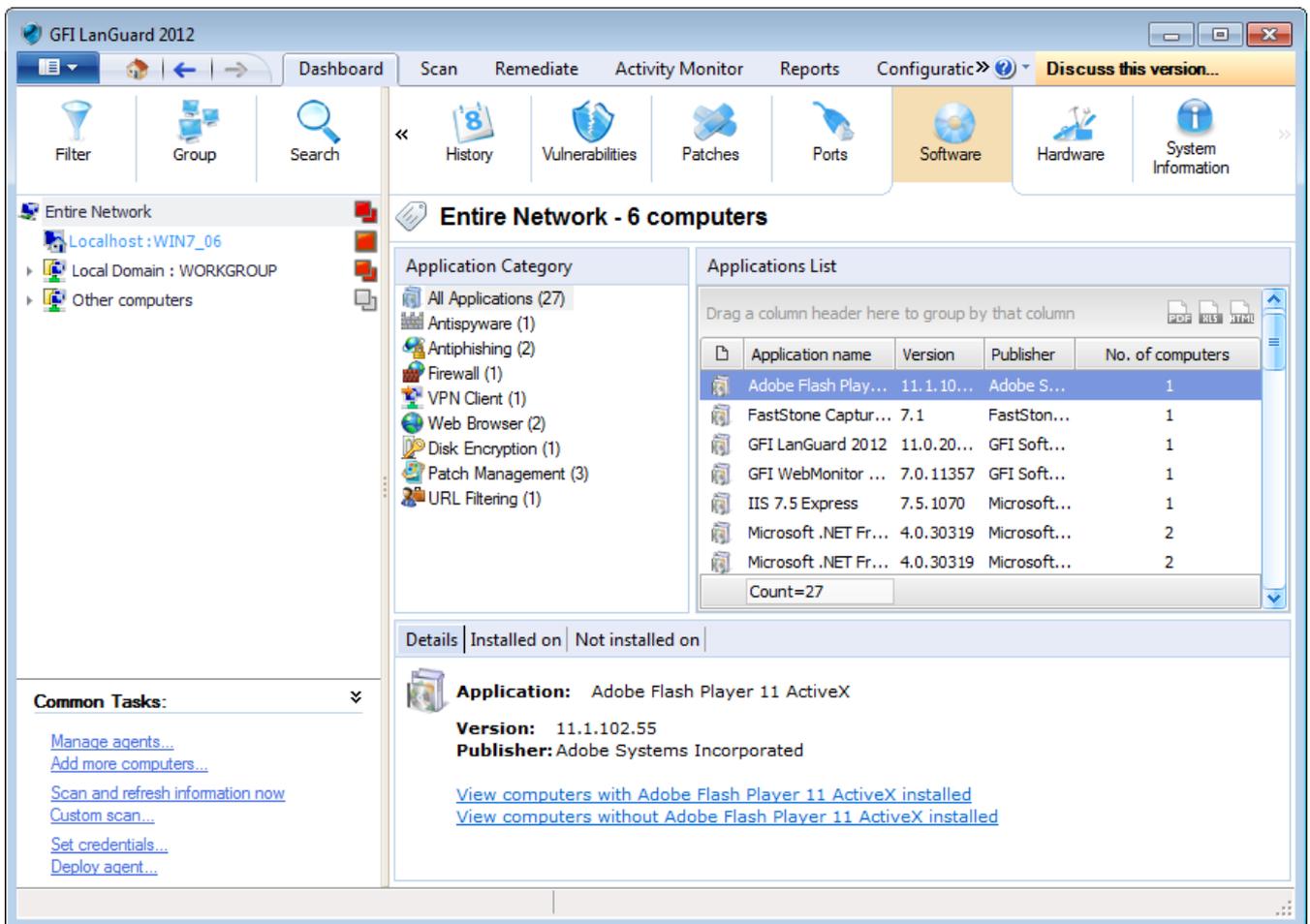


Note

Drag and drop a column header in the designated area to group data by criteria.

4.7.7 Software View

Display more details on the installed applications found during a network audit. When an application is selected from the **Application List**, the **Details** section provides more information on the selected application.



The screenshot shows the GFI LanGuard 2012 interface. The top navigation bar includes 'Dashboard', 'Scan', 'Remediate', 'Activity Monitor', 'Reports', 'Configuratic>>', and 'Discuss this version...'. Below this is a secondary navigation bar with icons for 'Filter', 'Group', 'Search', 'History', 'Vulnerabilities', 'Patches', 'Ports', 'Software' (highlighted), 'Hardware', and 'System Information'. The main content area is titled 'Entire Network - 6 computers'. On the left, there is a tree view showing 'Entire Network' with sub-items: 'Localhost : WIN7_06', 'Local Domain : WORKGROUP', and 'Other computers'. Below the tree is a 'Common Tasks' section with links: 'Manage agents...', 'Add more computers...', 'Scan and refresh information now', 'Custom scan...', 'Set credentials...', and 'Deploy agent...'. The main area is divided into two panes: 'Application Category' and 'Applications List'. The 'Application Category' pane shows a list of categories: 'All Applications (27)', 'Antispyware (1)', 'Antiphishing (2)', 'Firewall (1)', 'VPN Client (1)', 'Web Browser (2)', 'Disk Encryption (1)', 'Patch Management (3)', and 'URL Filtering (1)'. The 'Applications List' pane has a table with columns: 'Application name', 'Version', 'Publisher', and 'No. of computers'. The table contains the following data:

Application name	Version	Publisher	No. of computers
Adobe Flash Play...	11.1.10...	Adobe S...	1
FastStone Captur...	7.1	FastSton...	1
GFI LanGuard 2012	11.0.20...	GFI Soft...	1
GFI WebMonitor ...	7.0.11357	GFI Soft...	1
IIS 7.5 Express	7.5.1070	Microsoft...	1
Microsoft .NET Fr...	4.0.30319	Microsoft...	2
Microsoft .NET Fr...	4.0.30319	Microsoft...	2

Below the table is a 'Count=27' summary. At the bottom of the main area, there is a 'Details' section with tabs for 'Installed on' and 'Not installed on'. The 'Details' section shows information for 'Adobe Flash Player 11 ActiveX':
Application: Adobe Flash Player 11 ActiveX
Version: 11.1.102.55
Publisher: Adobe Systems Incorporated
There are also two links: '[View computers with Adobe Flash Player 11 ActiveX installed](#)' and '[View computers without Adobe Flash Player 11 ActiveX installed](#)'.

Screenshot 24: Software view in Dashboard



Note

Drag and drop a column header in the designated area to group data by criteria.

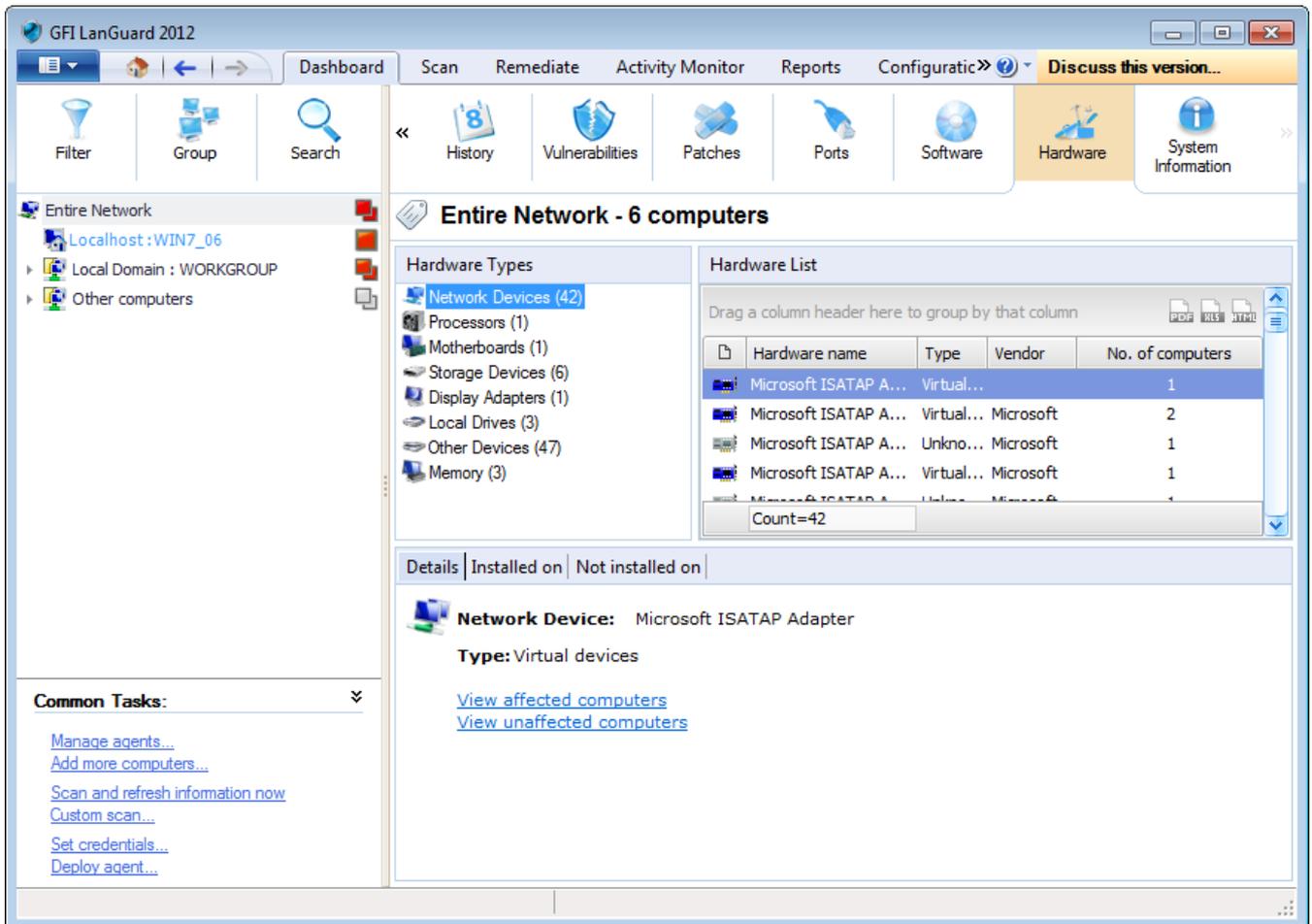


Note

Agent-less scans require to temporarily run a service on the remote machine. **Select Enable full security applications audit...** to enable this service on all agent-less scanning profiles.

4.7.8 Hardware View

Display more information on the hardware found during a network audit. Select hardware from the list to display more details.



The screenshot shows the GFI LanGuard 2012 interface. The top navigation bar includes 'Dashboard', 'Scan', 'Remediate', 'Activity Monitor', 'Reports', 'Configuratic>>', and 'Discuss this version...'. The main dashboard has tabs for 'History', 'Vulnerabilities', 'Patches', 'Ports', 'Software', 'Hardware', and 'System Information'. The 'Hardware' tab is active, showing 'Entire Network - 6 computers'. On the left, a tree view shows 'Entire Network' with sub-items: 'Localhost : WIN7_06', 'Local Domain : WORKGROUP', and 'Other computers'. Below this is a 'Common Tasks' section with links like 'Manage agents...', 'Add more computers...', 'Scan and refresh information now', 'Custom scan...', 'Set credentials...', and 'Deploy agent...'. The main area is split into 'Hardware Types' and 'Hardware List'. 'Hardware Types' lists: Network Devices (42), Processors (1), Motherboards (1), Storage Devices (6), Display Adapters (1), Local Drives (3), Other Devices (47), and Memory (3). 'Hardware List' has a table with columns: Hardware name, Type, Vendor, and No. of computers. The table contains several rows of Microsoft ISATAP Adapter data. Below the table is a 'Details' section for a selected 'Network Device: Microsoft ISATAP Adapter', with 'Type: Virtual devices' and links to 'View affected computers' and 'View unaffected computers'.

Screenshot 25: Hardware view in Dashboard

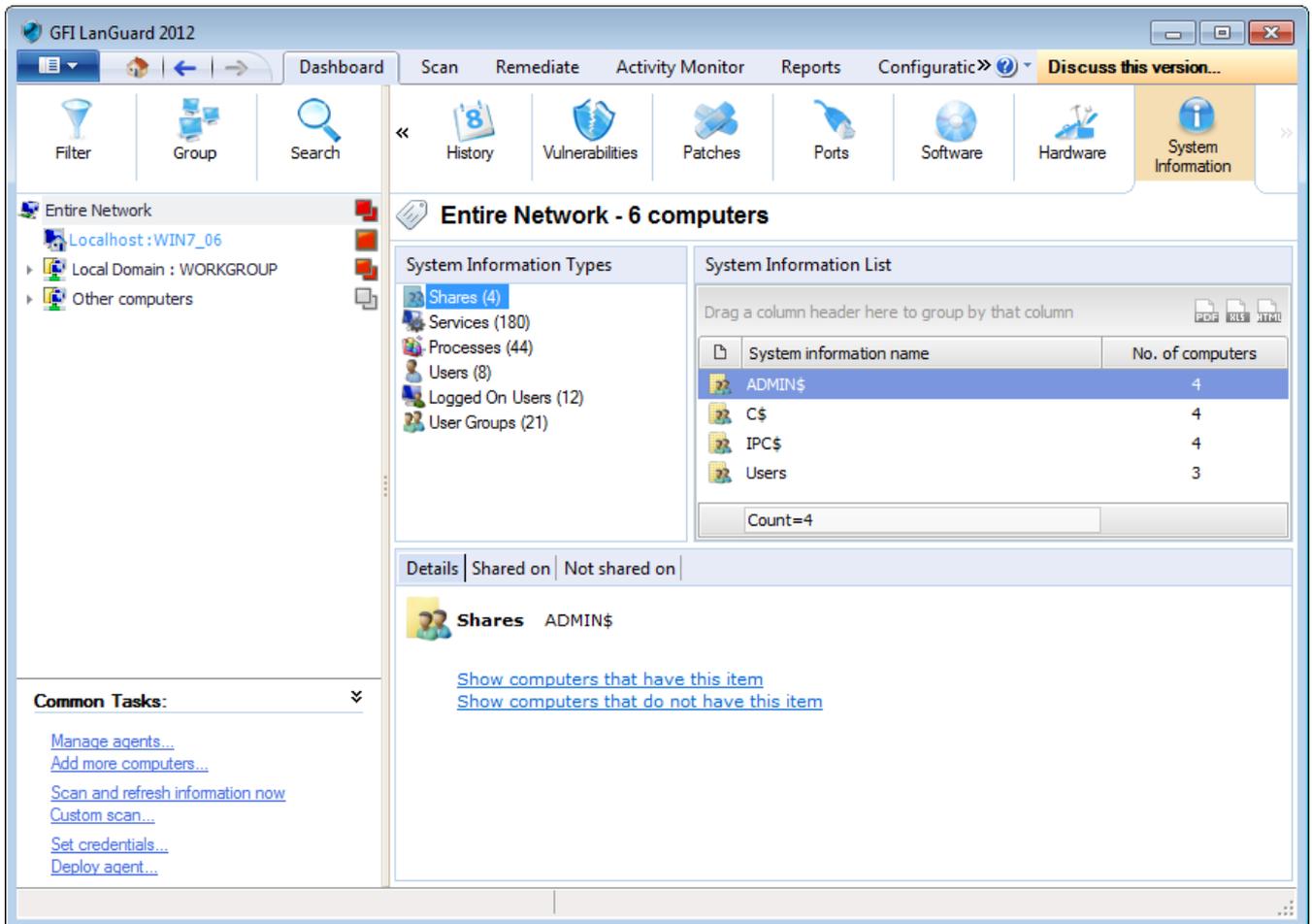


Note

Drag and drop a column header in the designated area to group data by criteria.

4.7.9 System Information View

The System Information tab, displays information associated with the operating system of a scan target(s).



Screenshot 26: System Information view in Dashboard



Note

Drag and drop a column header in the designated area to group data by criteria.

5 Troubleshooting and support

This chapter explains how to resolve issues encountered while using GFI LanGuard. These issues can be resolved using the contents of this **Installation and Setup 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 chapter:

5.1 Resolving common issues	47
5.2 Using the Troubleshooter Wizard	49
5.3 GFI SkyNet	51
5.4 Web Forum	51
5.5 Requesting technical support	51

5.1 Resolving common issues

The table below provides you with solutions to the most common problems you may encounter when using GFI LanGuard:

Table 15: GFI LanGuard common Issues

Issue Encountered	Solution/Description
Failed to connect to database error is encountered when trying to configure the database backend.	<p>Description</p> <p>This issue may occur when the following two conditions are met:</p> <ol style="list-style-type: none">1. GFI LanGuard is installed on Windows 2000 SP4 with MDAC 2.5 SP 32. The database backend is SQL Server® having the database instance name different from the SQL Server® machine name. <p>Solution</p> <p>Install Microsoft® Data Access Components (MDAC 2.6 or later) on GFI LanGuard machine and try again.</p> <p>MDAC can be downloaded from: http://go.gfi.com/?pageid=download_mdac</p>
The database structure is incorrect. Do you want to delete and recreate the database? Warning is encountered when trying to configure the database backend.	<p>Description</p> <p>This issue occurs when the database structure is corrupted.</p> <p>Or</p> <p>The database returns a timeout because the connection cannot be established.</p> <p>Solution</p> <p>When this message is encountered: Check that all SQL credentials are correct and there are no connectivity problems between the GFI LanGuard machine and the SQL server. It is important to note that when OK is clicked all saved scans are lost.</p>

Issue Encountered	Solution/Description
<p>When trying to access the Change database tab while configuring an SQL database, a Failed to connect to database error is encountered</p>	<p>Description</p> <p>This issue may occur when the following two conditions are met:</p> <ul style="list-style-type: none"> » GFI LanGuard is installed on Windows 2000 SP4 with MDAC 2.5 SP 3. » The database backend is SQL Server® having the database instance name different from the SQL Server® machine name. <p>Solution</p> <p>Install Microsoft® Data Access Components (MDAC 2.6 or later) on the GFI LanGuard machine and try again.</p> <p>Note</p> <p>MDAC can be downloaded from: http://go.gfi.com/?pageid=download_mdac</p>
<p>Incomplete results and errors when scanning remote machines</p>	<p>Description</p> <p>Errors similar to the following may be encountered:</p> <ul style="list-style-type: none"> » Failed to open test key to remote registry » The scan will not continue » Access Denied » Could not connect to remote SMB server. <p>These errors may be encountered because:</p> <ul style="list-style-type: none"> » The remote machine has an account similar to the one used by GFI LanGuard to log in as an administrator. » The user account used by GFI LanGuard does not have administrative privileges. <p>Solution</p> <p>To solve this issue do one of the following:</p> <ul style="list-style-type: none"> » Log on the GFI LanGuard machine and configure GFI LanGuard to use an alternate domain administrator account. » Delete the local user account on the remote machine. » Launch GFI LanGuard executable with 'Run As' using a Domain Administrator account. <p>Note</p> <p>For more information, refer to http://go.gfi.com/?pageid=LAN_ProbScanningRM</p>
<p>GFI LanGuard program updates not working</p>	<p>Description</p> <p>Updates will not work if GFI LanGuard machine does not have a direct connection to the Internet.</p> <p>Solution</p> <p>To solve this issue do one of the following:</p> <ul style="list-style-type: none"> » Configure GFI LanGuard machine to have direct Internet access. » Install another instance of GFI LanGuard on a machine with Internet access and configure GFI LanGuard to check for updates from the new installation. <p>Note</p> <p>For more information refer to http://go.gfi.com/?pageid=LAN_CheckAltUpdates</p>

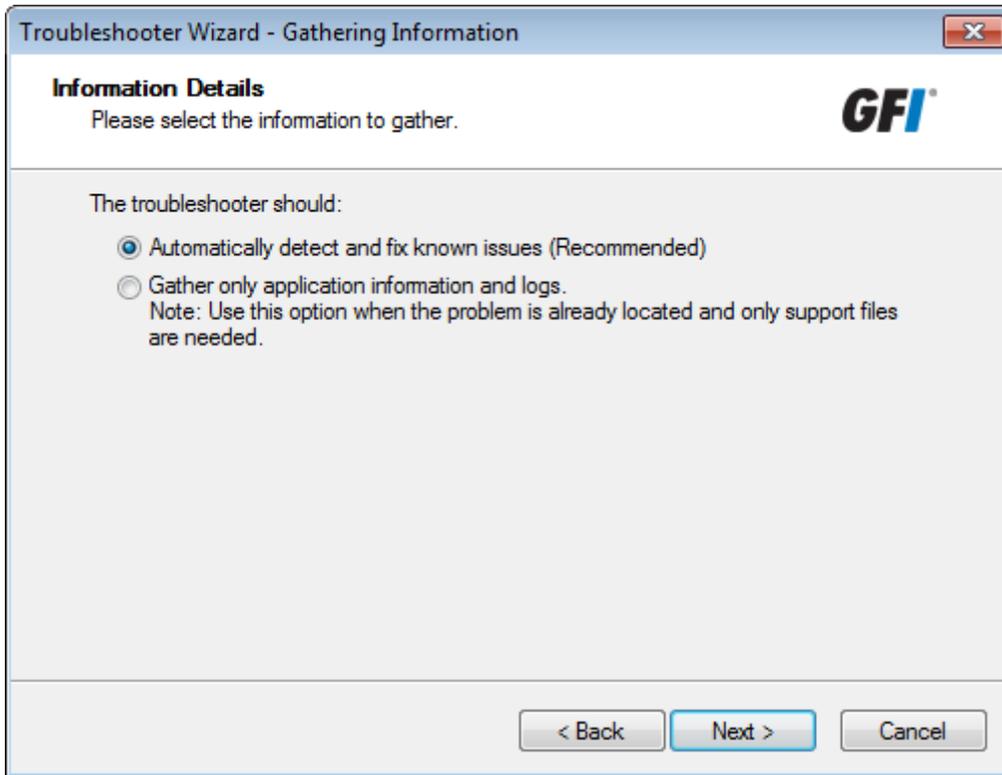
Issue Encountered	Solution/Description
<p>Firewall installed on GFI LanGuard is blocking connection with target computers</p>	<p>Description Scanning might slow down or be blocked if a firewall is installed on GFI LanGuard machine.</p> <p>Solution Configure the firewall to allow the following components in outbound connections:</p> <ul style="list-style-type: none"> » <..\Program Files\GFI\LanGuard>*.exe » <..\Program Files\GFI\LanGuard Agent>*.exe <p>Note For more information, refer to http://go.gfi.com/?pageid=LAN_SetBestPerformance</p>
<p>GFI LanGuard is failing to retrieve workgroup computers when using Enumerate Computers</p>	<p>Description GFI LanGuard uses the Windows mechanism to retrieve the machines within a workgroup. In this mechanism a Master Browser computer will create and store a list of all computers. In some cases, the Master Browser role can fail resulting in GFI LanGuard not retrieving computers information.</p> <p>Note To solve this issue, refer to http://go.gfi.com/?pageid=LAN_CannotEnumerate</p>
<p>GFI LanGuard found open ports that another port scanner found closed</p>	<p>Description GFI LanGuard uses a different approach than other port scanners to detect open ports.</p> <p>Solution To view the status of a port and determine if the port is closed or opened:</p> <ol style="list-style-type: none"> 1. Click Start > Programs > Accessories > Command Prompt. 2. Key in <code>netstat -an</code>, and press Enter. 3. The generated list displays all computer active connections.

5.2 Using the Troubleshooter Wizard

The GFI LanGuard troubleshooter wizard is a tool designed to assist you when encountering technical issues related to GFI LanGuard. Through this wizard, you are able to automatically detect and fix common issues as well as gather information and logs to send to our technical support team.

To use the Troubleshooter Wizard:

1. Launch the troubleshooting wizard from the **Start > Programs > GFI LanGuard 2012 > GFI LanGuard 2012 Troubleshooter**.
2. Click **Next** in the introduction page.



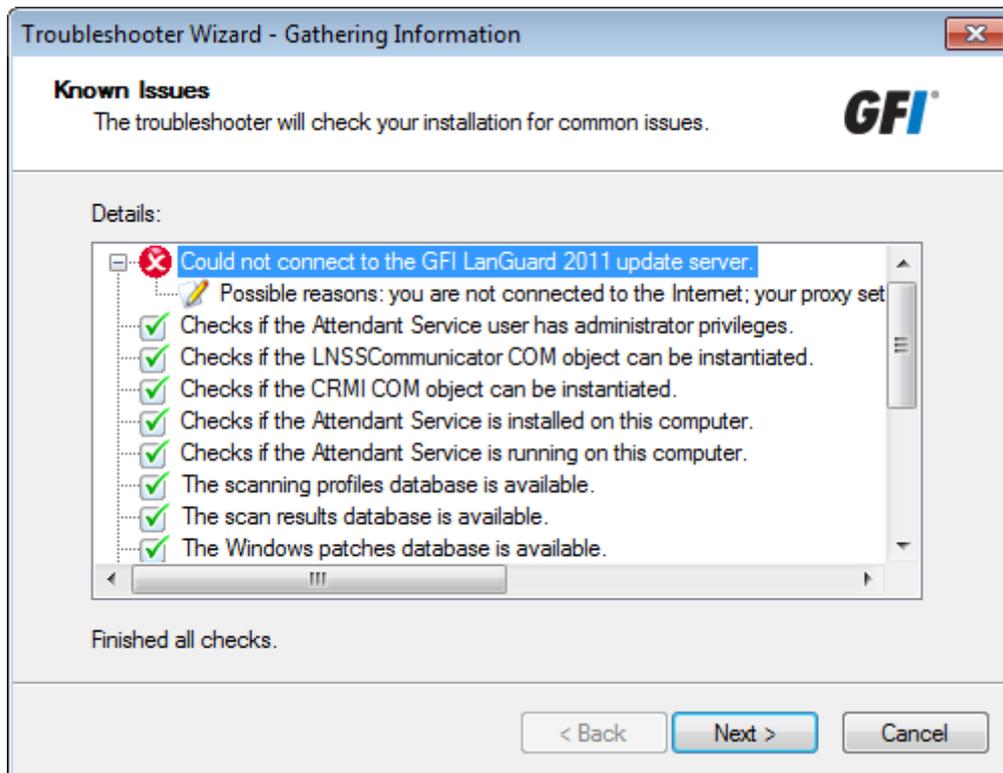
Screenshot 27: Troubleshooter wizard - Information details

3. In the Information details page select one of the following options described below:

Table 16: Information gathering options

Option	Description
Automatically detect and fix known issues	(Recommended) Configure GFI LanGuard to automatically detect and fix issues.
Gather only application information and logs	Gather logs to send to GFI support.

4. Click **Next** to continue.



Screenshot 28: Troubleshooter wizard - Gathering information about known issues

5. The troubleshooter wizard will retrieve all the information required to solve common issues. Click **Next** to continue.

6. The troubleshooter will fix any known issues that it encounters. Select **Yes** if your problem was fixed or **No** if your problem is not solved to search the GFI Knowledge base for information.

5.3 GFI SkyNet

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI SkyNet always has the most up-to-date listing of technical support questions and patches. In case that the information in this guide does not solve your problems, next refer to GFI SkyNet by visiting <http://kb.gfi.com/>.

5.4 Web Forum

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

5.5 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: <http://www.gfi.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.

6 Glossary

A

Access™

A Microsoft® desktop relational database management system included in the Microsoft® Office package. Access™ is normally used for small databases.

Active Directory™ (AD)

A technology that provides a variety of network services, including LDAP-like directory services.

Anti-spyware

A software countermeasure that detects spyware installed on a computer without the user's knowledge.

Antivirus

A software countermeasure that detects malware installed on a computer without the user's knowledge.

Apache web server

An open source HTTP server project developed and maintained by the Apache software foundation.

Applications auto-uninstall

An action that enables the auto-uninstall of applications that support silent uninstall from GFI LanGuard.

Auto-download

A GFI LanGuard technology that automatically downloads missing patches and service packs in all 38 languages.

Auto-patch management

A GFI LanGuard technology that automatically downloads missing Microsoft® updates and deploys them over the network.

Auto-remediation

A GFI LanGuard technology that automatically downloads and deploy missing patches. If an application is blacklisted in GFI LanGuard, auto-remediation will uninstall the application from the target computer during scheduled operations.

B

Backdoor program

An alternative method used to access a computer or computer data over a network.

Batch-files

A text files containing a collection of instructions to be carried out by an operating system or an application.

Blacklist

A list of USBs or Network devices names that are considered as dangerous. When a USB\Network device name contains a blacklisted entry while scanning a network, GFI LanGuard will report the device as a security threat (High security vulnerability).

Bluetooth

An open wireless communication and interfacing protocol that enables exchange of data between devices.

Bulletin Information

Contains a collection of information about a patch or a Microsoft® update. Used in GFI LanGuard to provide more information on an installed patch or update. Information includes; Bulletin id, title, description, URL and file size.

C

Common Gateway Interface (CGI)

A communication script used by web servers to transfer data to a client internet browser.

Common Vulnerabilities and Exposures (CVE)

A list of standardized names for vulnerabilities and other information security exposures. The aim of CVE is to standardize the names for all publicly known vulnerabilities and security exposures.

D

Dashboard

A graphical representation that indicates the status of various operations that might be currently active, or that are scheduled.

Demilitarized Zone (DMZ)

A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.

deploycmd.exe

A GFI LanGuard command line tool, used to deploy Microsoft® patches and third party software on target computers.

DMZ

A section of a network that is not part of the internal network and is not directly part of the Internet. Its purpose typically is to act as a gateway between internal networks and the internet.

DNS

A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

DNS Lookup tool

A utility that converts domain names into the corresponding IP address and retrieves particular information from the target domain

Domain Name System

A database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

E

Enumerate computers tool

A utility that identifies domains and workgroups on a network.

Enumerate users tools

A tools which enables you to retrieve users and user information from your domain/workgroup.

Extensible Markup Language (XML)

An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.

F

File Transfer Protocol

A protocol used to transfer files between network computers.

FTP

A protocol used to transfer files between network computers.

G

GFI EndPointSecurity

A security solution developed by GFI that helps organizations to maintain data integrity by preventing unauthorized access and transfers from removable devices.

GPO

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

Group Policy Object (GPO)

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

I

ICMP pings

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error

messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

impex.exe

A Command line tool, used to Import and Export profiles and vulnerabilities from GFI LanGuard.

Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is used by the operating systems of networked computers to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached. ICMP can also be used to relay query messages.

Internet Information Services (IIS)

A set of Internet-based services created by Microsoft® Corporation for internet servers.

L

Linux

An open source operating system that is part of the Unix operating system family.

Insscmd.exe

A GFI LanGuard command line tool that allows running vulnerability checks against network targets.

Local Host

In networking, the local host is the computer you are currently using. One can reference to the local host by using the reserved IP address 127.0.0.1. In this manual the Local host is the machine where GFI LanGuard is installed.

M

Mail server

The server that manages and stores client emails.

Malware

Composed from malicious and software, malware is a general term used for all software developed to harm and damage a computer system. Viruses, worms and Trojans are all type of malware.

Microsoft® Access™ database

A Microsoft® desktop relational database management system included in the Microsoft® Office package. Microsoft® Access™ is normally used for small databases.

Microsoft® IIS

A set of Internet-based services created by Microsoft® Corporation for internet servers.

Microsoft® Windows service packs

A collection of updates and fixes provided by Microsoft® to improve an application or an operating system.

Microsoft® WSUS

An acronym for Microsoft® Windows Server Update Services. This service enables administrators to manage the distribution of Microsoft® updates to network computers.

N

NETBIOS

An acronym for Network Basic Input/output. This system provides services to allow applications on different computers within a network to communicate with each other.

Netscape

A web browser originally developed by Netscape Communications Corporation.

O

Open Vulnerability and Assessment Language (OVAL)

A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.

OVAL

A standard that promotes open and publicly available security content, and standardizes the transfer of this information across the entire spectrum of security tools and services.

P

Patch agent

A background service that handles the deployment of patches, service packs and software updates on target computers.

Python scripting

A high-level computer programming scripting language.

R

Remote Desktop Protocol

A protocol developed by Microsoft® to enable clients to connect with the user interface of a remote computer.

S

SANS

An acronym for System Administration, Networking and Security research organization. An institute that shares solutions regarding system and security alerts.

Scan profiles

A collection of vulnerability checks that determine what vulnerabilities are identified and which information will be retrieved from scanned targets.

Script Debugger

A GFI LanGuard module that allows you to write and debug custom scripts using a VBScript-compatible language.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol is a technology used to monitor network devices such as, routers, hubs and switches.

SNMP

Acronym for Simple Network Management Protocol, a technology used to monitor network devices such as, routers, hubs and switches.

SNMP Auditing tool

A tool that reports weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary.

SNMP Walk tool

A tool used to probe your network nodes and retrieve SNMP information.

Spyware

A form of malware intended to collect information from a computer without notifying the user.

SQL Server Audit tool

A tool used to test the password vulnerability of the -sa- account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server.

SQL Server®

A Microsoft® relational database management system. Microsoft® included extra functionality to the SQL Server® (transaction control, exception handling and security) so that Microsoft® SQL server can support large organizations.

SSH Module

A module used to determine the result of vulnerability checks through the console (text) data produced by an executed script. This means that you can create custom Linux/UNIX vulnerability checks using any scripting method that is supported by the target-s Linux/UNIX OS and which outputs results to the console in text.

T

TCP ports

Acronym for Transmitting Control Protocol. This protocol is developed to allow applications to transmit and receive data over the internet using the well-known computer ports.

Terminal Services

A service that allows connecting to a target computer and managing its installed applications and stored data.

Traceroute tool

A tool used to identify the path that GFI LanGuard followed to reach a target computer.

Trojans

A form of malware that contains a hidden application that will harm a computer.

U

UDP ports

An acronym for User Datagram Protocol, these used to transfer UDP data between devices. In this protocol received packets are not acknowledged.

Uniform Resource Locator (URL)

The Uniform Resource Locator is the address of a web page on the world wide web.

Universal Serial Bus (USB)

A Serial bus standard widely used to connect devices to a host computer.

URL

The Uniform Resource Locator is the address of a web page on the world wide web.

V

VBScript

A Visual Basic Scripting language is a high-level programming language developed by Microsoft®.

Virus

A form of malware that infects a computer. The aim of a virus is to harm a computer by corrupting files and applications. A virus is a self-replicating program and can copy itself all over the computer system.

W

Web server

A server that provides web pages to client browsers using the HTTP protocol.

White-list

A list of USBs or Network devices names that are not considered as dangerous. When a USB/Network device name contains a white-listed entry while scanning a network, GFI LanGuard will ignore the device and consider it as a safe source.

Whois tool

A tool that enables you to look up information on a particular domain or IP address.

Wi-Fi/Wireless LAN

A technology used commonly in local area networks. Network nodes use data transmitted over radio waves instead of cables to communicate with each other.

X**XML**

An open text standard used to define data formats. GFI LanGuard uses this standard to import or export scanned saved results and configuration.

7 Index

A

Activity 36
Advanced 15, 28
Agent 14, 36, 38, 44, 49
Agent-based 10
Agent-less 8, 10, 16, 44
Antiphishing 39
Antispyware 39
Attendant service 9, 22
Attributes 30-31, 39
Audit 27, 36, 38, 40, 42-45

B

Backup 39

C

Check 19-20, 47
Client 9-10
Command Line Tools 9
Components 9, 14, 19, 22, 47
Computer 8, 22, 25, 28, 36
Computer Tree 28, 31
Conditions 47
Custom 7

D

Dashboard 27, 31, 34-35, 40-46

E

Enumerate Computers 49
Export 20, 23

F

Find 28
Full Text Searching 31

G

Groups 30, 32, 39

H

Hardware 7, 14, 31, 35, 39, 45

I

Import 18, 23

Install 18, 23

Installing 8, 10

L

Level 27, 34-35

M

Malware 37
Management Console 9, 12, 23
Microsoft Access 22
Missing Service Packs and Update Rollups 38
Monitor 10

N

NetBIOS 17
Notifications 7

O

Open TCP ports 39
Open UDP ports 39
OVAL 7

P

Password 22
Ports 14, 35, 37, 39, 43, 49
Processors 39
Protocols 16

R

Real-time 35
Registry 8, 16, 48
Relay Agents 9-10, 15, 36
Remediation Center 34
Remediation Operations 8, 16

S

Scanning Profiles 9
Scheduled Scans 36
Security Scans 9, 27
Security Updates 17, 38
Server 8-10, 14, 47
Sessions 9
SMB 8, 17, 48

SNMP 17

Software 14, 18, 35, 37, 39, 44

SQL 16, 47

SSH 16

System Information 35, 46

U

Unauthorized 7, 39

Unauthorized Applications 37

Uninstall 9, 36

Upgrading 18

Users 31, 39

V

Vulnerabilities 31, 34-36, 38, 41

Vulnerability Assessment 7

W

WMI 16

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

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

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

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

Telephone: +356 2205 2000

Fax: +356 2138 2419

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

sales@gfiap.com

