# **GFI Lan**Guard<sup>™</sup>

**GFI**<sup>®</sup>

# ADMINISTRATOR GUIDE

Find out how to configure GFI LanGuard in different environments and how to set up advanced features.



The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or 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 warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

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

GFI and GFI LanGuard are trademarks or registered trademarks of GFI Software or its affiliates in the US and other countries. Any other trademarks contained herein are the property of their respective owners.

GFI LanGuard is copyright of GFI Software. - 1999-2018 GFI Software. All rights reserved.

Document Version: 12.3

Last updated (month/day/year): 01/30/2018

# Contents

1 Introduction	6
1.1 How GFI LanGuard works	6
1.1.1 Basic scanning and auditing of network devices	6
1.1.2 GFI LanGuard Agents	7
1.1.3 Relay Agents	8
1.2 The GFI LanGuard Central Management Server	
1.3 GFI LanGuard Components	10
1.4 Supported features per operating system, application and device	
1.5 About this guide	14
1.5.1 Terms and conventions used in this manual	14
2 Installing GFI LanGuard	
2.1 Deployment scenarios	
2.2 System Requirements	
2.2.1 GFI LanGuard system requirements	
2.2.2 GFI LanGuard Agent and Relay Agent system requirements	23
2.2.3 Central Management Server system requirements	
2.3 Importing and exporting GFI LanGuard settings	
2.4 Installing GFI LanGuard	
2.4.1 Important notes	
2.4.2 Installation procedure	
2.4.3 Obtaining a GFI LanGuard subscription	
2.5 Upgrading GFI LanGuard	
2.5.1 Upgrading from GFI LanGuard 12.1 or later	
2.5.2 Upgrading from GFI LanGuard 12	
2.5.3 Upgrading from GFI LanGuard 2015 or earlier	
2.6 Testing the installation	
3 GFI LanGuard Central Management Server	
3.1 Installing GFI LanGuard Central Management Server	
3.1.1 Central Management Server system requirements	
3.1.2 Installing Central Management Server	
3.1.3 Uninstalling Central Management Server	44
3.2 Joining GFI LanGuard to Central Management Server	45
3.3 Configuring GFI LanGuard Central Management Server	
3.3.1 Configuring GFI LanGuard Central Management Server database settings	
3.3.2 Specifying data retention settings	49
3.3.3 Configuring Central Management Server user privileges	
3.3.4 Managing GFI LanGuard sites in Central Management Server	51
	52
3.3.5 Configuring HTTPS Certificate in Central Management Server	
3.3.5 Configuring HTTPS Certificate in Central Management Server	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.3.7 Configuring Central Management Server Updates</li> </ul>	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.3.7 Configuring Central Management Server Updates</li> <li>3.4 Using the GFI LanGuard Central Management Server Console</li> </ul>	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.3.7 Configuring Central Management Server Updates</li> <li>3.4 Using the GFI LanGuard Central Management Server Console</li> <li>3.4.1 Central Management Server Home Page</li> </ul>	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.3.7 Configuring Central Management Server Updates</li> <li>3.4 Using the GFI LanGuard Central Management Server Console</li> <li>3.4.1 Central Management Server Home Page</li> <li>3.4.2 Central Management Server Dashboards</li> <li>2.4.2 Central Management Server Consultation</li> </ul>	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.7 Configuring Central Management Server Updates</li> <li>3.4 Using the GFI LanGuard Central Management Server Console</li> <li>3.4.1 Central Management Server Home Page</li> <li>3.4.2 Central Management Server Dashboards</li> <li>3.4.3 Central Management Server Computer Tree</li> </ul>	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.3.7 Configuring Central Management Server Updates</li> <li>3.4 Using the GFI LanGuard Central Management Server Console</li> <li>3.4.1 Central Management Server Home Page</li> <li>3.4.2 Central Management Server Dashboards</li> <li>3.4.3 Central Management Server Computer Tree</li> <li>3.4.4 Using GFI LanGuard Central Management Server Reports</li> </ul>	
<ul> <li>3.3.5 Configuring HTTPS Certificate in Central Management Server</li> <li>3.3.6 Email settings in Central Management Server</li> <li>3.7 Configuring Central Management Server Updates</li> <li>3.4 Using the GFI LanGuard Central Management Server Console</li> <li>3.4.1 Central Management Server Home Page</li> <li>3.4.2 Central Management Server Dashboards</li> <li>3.4.3 Central Management Server Computer Tree</li> <li>3.4.4 Using GFI LanGuard Central Management Server Reports</li> </ul>	

4.1.1 Deploying Agents	73
4.1.2 Deploy Agents manually	75
4.1.3 Agent properties	
4.1.4 Agents settings	
4.1.5 Configuring Relay Agents	
4.1.6 Managing Agent groups	
4.1.7 Updating Agents	
4.2 Scanning Your Network	94
4.2.1 About Scanning Profiles	
4.2.2 Available Scanning Profiles	
4.2.3 Manual scans	
4.2.4 Enabling security audit policies	
4.2.5 Scheduled scans	
4.2.6 Agent scheduled scans	
4.2.7 Starting an Agent scan manually	
4.2.8 Discovering Mobile Devices	
4.3 Dashboard	
4.3.1 Achieving results from the dashboard	
4.3.2 Using the Dashboard	
4.3.3 Using the Computer Tree	
4.3.4 Using Attributes	
4.3.5 Dashboard actions	
4.3.6 Exporting issue list	
4.3.7 Dashboard views	
4.4 Interpreting Results	
4.4.1 Interpreting scan results	
4.4.2 Loading results from the database	160
4.4.3 Saving and loading XML results	161
4.5 Remediate Vulnerabilities	
4.5.1 Automatic Remediation	162
4.5.2 Manual Remediation	185
4.5.3 Sending Mobile Device Notifications	197
46 Activity Monitoring	200
461 Monitoring Security Scans	200
462 Monitoring Software Updates Download	200
463 Monitoring Remediation Operations	204
464 Monitoring Product Undates	206
47 Reporting	208
471 Available reports	208
472 Generating reports	214
473 Scheduling Reports	216
474 Customizina default reports	210
4.7.5 Full text searching	
48 Data collected from a network audit	
4.8.1 System Patching Status	
4.8.7 System rateming status	
1.9.2 Prote	
4.0.5 FUILS	
4.0.4 Softwale	
4.0 Common Vulnerabilities and Evocures (CV/E)	20 רכר
ד. כטוווווטון עמוופומטוותבא מווט באַטטעובא (כעב)	
5 Settings	
5.1 Configuring Alerting Options	

8 Index	
7 Glossary	
6.6 Kequesting technical support	
6.5 Web Forum	
6.4 GFI Knowledge Base	
6.3 Using the Agent Diagnostics Tool	
6.2 Using the Troubleshooter Wizard	
6.1 Resolving common issues	
6 Troubleshooting and support	
5.9 Uninstalling GFI LanGuard	
5.8 Configuring NetBIOS	
5.7.3 SSH Module	
5.7.2 Creating custom scripts using Python Scripting	
5.7.1 Creating custom scripts using VBscript	
5.7 Script Debugger	
5.6.9 Command Line Tools	
5.6.8 SQL Server® Audit	
5.6.7 SNMP Walk	
5.6.6 SNMP Auditing	
5.6.5 Enumerate Users	
5.6.4 Enumerate Computers	274 275
5.6.2 Macional 5.6.2	272 274
5.6.2 Traceroute	270 270
5.6.1 DNSLookun	270 270
5.6. Itilities	200 z م70
5.5.4 Configuring Network & Software Adult Options	201 مده
5.5.5 Configuring Network & Software Audit options	
5.5.2 Configuring Vulnerabilities	
5.5.1 Create a new Scanning Profile	
5.5 Scanning Profile Editor	
5.4.1 Methods to avoid database limitation issues	
5.4 Limiting Database Size	
5.3 Configuring Program Updates	
5.2 Configuring Database Maintenance Options	
E 2 Configuring Database Maintanance Options	226

# **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<sup>®</sup> 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<sup>®</sup> Windows, Linux and MAC operating systems as well as third party products

» Automatic uninstallation of unauthorized software.

# 1.1 How GFI LanGuard works

Use GFI LanGuard to scan, analyze and remediate the health of your network devices. Install GFI LanGuard on a server within your network to:

#### SCAN

Scan network devices to detect vulnerabilities, missing patches, open ports, running services and more.

#### ANALYZE

View the network security status and analyze network security trends in the graphical dashboard and by generating reports.

#### REMEDIATE

Install missing updates, uninstall unauthorized applications, execute scripts, open remote desktop connections and run other tasks to maintain the health of your network and devices connected to it.

On installation, GFI LanGuard identifies reachable machines within your network. It collects information sets from the network machines as part of its Network Discovery operations and performs a deep scan to enumerate all the information related to target computers.

GFI LanGuard can be deployed in a number of ways, depending on the number and type of computers and devices you want to monitor, network bandwidth usage during normal operation times and the network topology.

Use the information below to help you understand the different deployment options. For more information, refer to <u>Deployment scenarios</u> (page 15).

#### 1.1.1 Basic scanning and auditing of network devices

Install GFI LanGuard on a server that meets the system requirements to run scans and audits of computers and devices. No additional software installations are required. 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. For more information, refer to Manual scans (page 96).



Screenshot 1: GFI LanGuard scanning devices over the network.

Note that scans run in this mode use the resources of the machine where GFI LanGuard is installed and utilize more network bandwidth since all auditing is done remotely. When you have a large network of scan targets, this mode can drastically decrease GFI LanGuard's performance and can affect network speed. Refer to the sections below if you have a large network.

#### 1.1.2 GFI LanGuard Agents

GFI LanGuard can be configured to automatically deploy agents on computers. Agents minimize network bandwidth utilization because audits are done using the scan target's resources and only a result XML file is transferred over the network. Devices that have a GFI LanGuard agent installed will be scanned even if the device is not connected to the company network and are more accurate that agent-less scans because agents can access more information on the local host. For more information refer to Managing Agents,

Typically, networks contain a mixture of agent-based devices and other devices scanned over the network.



Screenshot 2: Devices that have an agent installed and devices scanned by GFI LanGuard over the network.

Agents send scan data to GFI LanGuard through TCP port 1072. This port is opened by default when installing GFI LanGuard. Agents do not consume resources on the scan target unless the agent is performing a scan or a remediation operation.

Note that agents can only be deployed on computers running a Microsoft Windows operating system and they require approximately 25 MB of memory and 350 MB of hard disk space.

#### 1.1.3 Relay Agents

Relay agents reduce the load from the server where GFI LanGuard is installed to increase server performance and to apply bandwidth load balancing techniques. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers. The main advantages of using relay agents are:

» Reduced bandwidth consumption in local or geographically distributed networks. If a Relay Agent is configured on each site, a patch is only downloaded once and distributed to client computers

- » Reduced hardware load from the GFI LanGuard server component and distributed amongst relay agents
- » Using multiple Relay Agents increases the number of devices that can be protected simultaneously.



Screenshot 3: Devices relaying data through a GFI LanGuard Relay Agent.

Note that you can have cascading relay agents where a relay agent relays data through another relay agent. It is recommended to keep the number of computers and agents directly connected to the GFI LanGuard server or to one Relay Agent below 100.

Only devices that have the GFI LanGuard Agent installed can be promoted to Relay Agents. Promoting an agent to a Relay Agent is done from within GFI LanGuard. For more information, refer to <u>Configuring Relay Agents</u> (page 83).

### 1.2 The GFI LanGuard Central Management Server

GFI LanGuard Central Management Server is aimed at very large networks that want to monitor the operation of multiple GFI LanGuard instances in one central console. It offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances. For more information refer to GFI LanGuard Central Management Server.



Screenshot 4: Multiple GFI LanGuard instances monitored by the GFI LanGuard Central Management Server

The GFI LanGuard Central Management Server is used for reporting only. Scans and remediation take place within each individual GFI LanGuard instance. Information is centralized to the GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard, depending on network size and amount of data being transferred.

# 1.3 GFI LanGuard Components

This section provides you with information about GFI LanGuard components. The installation files enable you to install both GFI LanGuard from where you can perform patch management and remediation tasks from the dashboard and also GFI LanGuard Central Management Server - a web console that unifies multiple GFI LanGuard installations into one centralized console. All the other components are deployed through GFI LanGuard once installation is complete. Available components are described in the table below:

Component	Description
GFI LanGuard Central Man- agement Server	Also known as Central Management Server, this component provides integration between several GFI LanGuard instances, even in remote locations. GFI LanGuard Central Management Server enables reporting but does not allow scans or remediation tasks. For more information, refer to <u>GFI LanGuard Central Management Server</u> (page 40).
GFI LanGuard	Enables you to manage agents, perform scans, analyze results, remediate vulnerability issues and generate reports. For more information, refer to <u>Introduction</u> (page 6).
GFI LanGuard Agents	Enable data processing and auditing on target machines; once an audit is finished, result is sent to GFI LanGuard. For more information, refer to <u>Deploying Agents</u> (page 73).
GFI LanGuard Update Sys- tem	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. For more information, refer to <u>Configuring Program</u> <u>Updates</u> (page 240).
GFI LanGuard Attendant Service	The background service that manages all scheduled operations, including scheduled network security scans, patch deployment and remediation operations. For more information, refer to <u>Scanning Your Network</u> (page 94).
GFI LanGuard Scanning Pro- files Editor	This editor enables you to create new and modify existing scanning profiles. For more information, refer to <u>Scan</u> - ning Profile Editor (page 247).
GFI LanGuard Command Line Tools	Enables you to launch network vulnerability scans and patch deployment sessions as well as importing and export- ing profiles and vulnerabilities without loading up GFI LanGuard. For more information, refer to <u>Command Line</u> <u>Tools</u> (page 281).

# 1.4 Supported features per operating system, application and device

GFI LanGuard provides a detailed analysis of the state of your network and a complete picture of installed applications, hardware on your network, mobile devices that connect to the Exchange servers, the state of security applications (antivirus, anti-spam, firewalls, etc.), open ports and any existing shares and services running on your machines.

GFI LanGuard features, such as Device Identification and Port Scanning (DI/PS), Vulnerability Assessment (VA), Patch Management (PM), Software Audit (SA) and Hardware Audit (HA) are supported by a wide range of devices, operating systems and applications listed in the table below:

Windows <sup>®</sup> Server Operating System	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability Assessment	<u>PM Patch Man-</u> agement	<u>SA Soft-</u> ware <u>Audit</u>	HA Hard- ware Audit
Server 2016	1	1	1	1	1

Windows <sup>®</sup> Server Operating System	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability <u>Assessment</u>	PM Patch Man- agement	<u>SA Soft-</u> ware Audit	<u>HA Hard</u> - ware Audit
Server 2012 (including R2)	4	1	4	1	1
Server 2008 (including R2) Stand- ard/Enterprise	4	4	4	1	1
Server 2003 Standard/Enterprise	4	1	4	1	1
Small Business Server 2011	4	<	<	1	<
Small Business Server 2008 Standard	4	4	1	1	1
Small Business Server 2003 (SP1)	1	1	1	1	1

Windows <sup>®</sup> Client Operating System	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability Assessment	<u>PM Patch Man-</u> agement	<u>SA Soft-</u> ware <u>Audit</u>	<u>HA Hard</u> - ware Audit
Windows 10 Professional/Enterprise	<	1	1	1	1
Windows 8/8.1 Pro- fessional/Enterprise	4	4	4	4	4
Windows 7 Pro- fessional/Enterprise/Ultimate	4	4	4	4	1
Windows Vista Busi- ness/Enterprise/Ultimate	4	4	4	4	4
Windows XP Professional (SP2 or higher)	1	1	1	1	1

Windows <sup>®</sup> Third Party Applications	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability <u>Assessment</u>	<u>PM Patch Man-</u> agement	<u>SA Soft</u> - ware <u>Audit</u>	<u>HA Hard</u> - ware Audit
Microsoft Office	×	1	1	×	ж
Microsoft Exchange	×	1	1	×	×
Microsoft SQL Server	×	1	1	×	8
Microsoft Visual Studio	×	1	1	×	×
Other Microsoft applications	×	1	1	×	34
Java Runtime Environment	×	1	1	×	×
Adobe Flash Player	×	1	1	×	8
Adobe Reader	×	1	1	×	×
Adobe AIR	×	1	1	×	×
Adobe Shockwave Player	×	1	1	×	×

Windows <sup>®</sup> Third Party Applications	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability Assessment	PM Patch Man- agement	<u>SA Soft-</u> ware <u>Audit</u>	<u>HA Hard</u> - ware Audit
Mozilla Firefox	×	1	<	×	×
Apple Safari	×	4	4	×	×
Apple QuickTime	×	1	1	×	×
Apple iTunes	×	1	1	×	8
Opera Browser	×	1	1	×	24

Linux Distributions	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability Assessment	PM Patch Man- agement	<u>SA Soft-</u> ware <u>Audit</u>	<u>HA Hard</u> - ware Audit
Mac OS X (versions supported by OS vendor)	4	4	4	₹.	1
Red Hat Enterprise Linux (versions supported by OS vendor)	4	4	4	Ľ	4
CentOS (versions supported by OS vendor)	4	4	4	1	<
Ubuntu (versions supported by OS vendor)	ح ا	4	1	4	4
Debian (versions supported by OS vendor)	4	4	1	<	<
SUSE Linux Enterprise (versions sup- ported by OS vendor)	4	4	1	1	4
openSUSE (versions supported by OS vendor)	1	4	1	<	<
Other distributions	1	1	×	1	1

Virtual Machines (with supported guest operating systems)	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability Assessment	PM Patch Man- agement	<u>SA Soft</u> - ware <u>Audit</u>	<u>HA Hard</u> - ware Audit
VMware	1	1	1	1	1
Microsoft <sup>®</sup> Hyper-V	1	1	1	1	1
Oracle Virtual Box	1	1	<	1	1
Citrix Xen	1	1	1	1	1
Parallels	1	1	1	1	1

Network Devices	DI/PS Device Iden- tification and Port Scanning	VA Vulnerability Assessment	PM Patch Man- agement	<u>SA Soft</u> - ware Audit	<u>HA Hard</u> - ware Audit
Cisco	1	1	×	×	×
HP	1	1	24	×	×
Linksys	1	1	24	×	×
D-Link	1	1	*	×	×
Netgear	1	×	*	×	×
SonicWall	1	×	*	×	×
Alcatel Lucent	1	×	24	×	×
3Com	1	×	*	×	×
Nortel	1	×	*	×	×
Juniper Networks	1	×	×	×	×
IBM	1	×	*	×	×
Dell	1	×	×	×	×
НЗС	1	×	*	×	×
Nortel Networks	4	×	×	×	×

Mobile Devices	DI/PS Device Iden- tification and Port Scanning	<u>VA Vul</u> - nerability Assessment	PM Patch Man- agement	<u>SA Soft</u> - ware Audit	<u>HA Hard</u> - ware Audit
Google Android	1	1	×	×	×
Apple iOS	1	1	8	×	×
Windows phone	4	1	×	×	×

Acronyms used in table above:

- » **DI/PS**: Device Identification and Port Scanning
- » VA: Vulnerability Assessment
- » PM: Patch Management
- » SA: Software Audit
- » HA: Hardware Audit

For a detailed list of every supported model of each application see http://go.gfi.com/?pageid=LAN\_ WindowsThirdPartyApplications

For a detailed list of every supported model of each device see http://go.gfi.com/?pageid=LAN\_SupportedDevices

# 1.5 About this guide

The aim of this Administrator Guide is to help System Administrators install, configure and run GFI LanGuard with minimum effort.

### 1.5.1 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 Deployment scenarios	15
2.2 System Requirements	19
2.2.1 GFI LanGuard system requirements	20
2.2.2 GFI LanGuard Agent and Relay Agent system requirements	23
2.2.3 Central Management Server system requirements	25
2.3 Importing and exporting GFI LanGuard settings	27
2.4 Installing GFI LanGuard	
2.4.1 Important notes	30
2.4.2 Installation procedure	31
2.4.3 Obtaining a GFI LanGuard subscription	34
2.5 Upgrading GFI LanGuard	35
2.5.1 Upgrading from GFI LanGuard 12.1 or later	35
2.5.2 Upgrading from GFI LanGuard 12	36
2.5.3 Upgrading from GFI LanGuard 2015 or earlier	37
2.6 Testing the installation	38

### 2.1 Deployment scenarios

GFI LanGuard deployments depend on the number of computers and devices you want to monitor and traffic load on your network during normal operation time. Refer to the following deployment scenarios to determine whether you want to:

» Deploy a GFI LanGuard instance - Install a GFI LanGuard instance to scan, detect and remediate network vulnerabilities.

» Deploy GFI LanGuard Central Management Server - connect multiple GFI LanGuard instances in one centralized UI for reporting purposes.

» Deploy GFI LanGuard in Agent-less mode - in this mode, GFI LanGuard creates a remote session with scan targets and audits them over the network.

» Deploy GFI LanGuard Agents - deploy Agents on newly discovered computers to minimize network bandwidth utilization.

» Deploy GFI LanGuard Relay Agents - Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and forward them to client computers to reduce the load from the GFI LanGuard server. » Deploy GFI LanGuard in mixed mode - in this mode GFI LanGuard is configured to work in Agent and Agent-less mode on the network.

#### Deploy a GFI LanGuard instance

Any GFI LanGuard deployment starts with installing the product in your environment. After a GFI LanGuard instance is successfully installed, it will:

» Determine reachable machines on your network and collect information from 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.

» Once targets are identified, GFI LanGuard performs a 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.

Deploy the GFI LanGuard Central Management Server to connect multiple GFI LanGuard instances

With GFI LanGuard Central Management Server, multiple GFI LanGuard instances can be brought together through a common console, even when installed in separate locations. The GFI LanGuard Central Management Server console offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances. It also offers centralized reporting and visibility by capturing data from the various deployments of GFI LanGuard. For more information, refer to GFI LanGuard Central Management Server (page 40).



GFI LanGuard Central Management Server is used only for reporting. Scans and remediation take place only in GFI LanGuard and then information is centralized to GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard. Synchronization usually takes a few minutes. Delay depends on network size and amount of data being transferred.

#### Deploy GFI LanGuard in Agent-less mode

Agent-less auditing is started from GFI LanGuard. 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. For more information, refer to <u>Manual scans</u> (page 96).



#### 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.

#### Deploy GFI LanGuard Agents

GFI LanGuard can be configured to automatically deploy agents on newly discovered 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 1072. 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. For more information, refer to <u>Managing Agents</u> (page 73).

#### NOTE

GFI LanGuard Agents can be deployed only on machines running Microsoft Windows operating systems that meet a minimum set of system requirements. For more information, refer to <u>GFI LanGuard system requirements</u> (page 20).

#### Deploy GFI LanGuard Relay Agents

Relay agents are used to reduce the load from the GFI LanGuard server. Computers configured as relay agents download patches and definitions directly from the GFI LanGuard server and 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. For more information, refer to <u>Configuring Relay Agents</u> (page 83).



#### Deploy GFI LanGuard in mixed mode

In mixed mode, GFI LanGuard is configured to work in Agent mode on some computers and in Agent-less mode on other computers or devices.

The following screenshot shows how GFI LanGuard can be deployed in mixed mode on a Local Area Network (LAN):



# 2.2 System Requirements

The following topics provide information about the system requirements for all GFI LanGuard components.

2.2.1 GFI LanGuard system requirements	20
2.2.2 GFI LanGuard Agent and Relay Agent system requirements	23
2.2.3 Central Management Server system requirements	25

#### 2.2.1 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 <sup>®</sup> Server 2016
Windows <sup>®</sup> Server 2012 (including R2)
Windows <sup>®</sup> Server 2008 (including R2) Standard/Enterprise
Windows <sup>®</sup> 10 Professional/Enterprise
Windows <sup>®</sup> 8/8.1 Professional/Enterprise

Operating System
Windows <sup>®</sup> 7 Professional/Enterprise/Ultimate
Windows <sup>®</sup> Vista Business/Enterprise/Ultimate
Windows <sup>®</sup> 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 <sup>°</sup> 2008 or later	This database server has a 10GB limit and is therefore recommended for networks containing up to 500 com- puters. If a database server is not available, the GFI LanGuard installer can automatically download and run the Microsoft SQL Express installer.
SQL Server <sup>®</sup> 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 Shar- ing	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 inform- ation 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: <ul> <li>Auditing computers</li> <li>Agent management</li> <li>Patch deployment.</li> </ul>

#### 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\

#### 2.2.2 GFI LanGuard Agent and Relay Agent system requirements

Computers running GFI LanGuard Agent and GFI LanGuard Relay Agent 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
- » Antivirus & Backup exclusions

#### Hardware requirements

#### **GFI** LanGuard Agent

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

Component	Requirement
Processor	1 GHz
Physical Storage	800MB are required for the installation & an additional 2GB are required during a scan to extract update archives.
RAM	25 MB dedicated to GFI LanGuard
Network band- width	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 (an offline Relay Agent incapacitates its clients)
- » 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:

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

#### 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 (32-bit/64-bit)

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

Windows <sup>®</sup> Operating System	GFI LanGuard Agent	GFI LanGuard Relay Agent
Windows Server 2016	4	4
Windows Server 2012 (including R2)	4	4
Windows Server 2008 R2 Standard/Enterprise (latest SP)	4	4
Windows Server 2008 Standard/Enterprise (latest SP)	4	4
Windows Server 2003 Standard/Enterprise	4	8
Windows 10 Professional/Enterprise	4	4
Windows 8/8.1 Professional/Enterprise	4	4
Windows 7 Professional/Enterprise/Ultimate (latest SP)	4	4
Windows Vista Business/Enterprise/Ultimate	4	4
Windows XP Professional (latest SP)	4	8
Small Business Server 2011	4	4
Small Business Server 2008 Standard	4	8
Small Business Server 2003 (latest SP)	4	*

#### 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

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

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.

#### 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\

#### 2.2.3 Central Management Server system requirements

Computers running GFI LanGuard Central Management Server must meet the system requirements described below.

#### Hardware requirements

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

Component	Requirement
Processor	2.8 GHz quad-core
Physical Storage	10 GB HDD free space
RAM	8 GB RAM

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

The following table lists operating systems and versions where the GFI LanGuard Central Management Server can be installed. Ensure that these operating systems are running the latest Service Pack as provided by Microsoft.

Operating System
Windows <sup>®</sup> Server 2016
Windows <sup>®</sup> Server 2012 (including R2)
Windows <sup>®</sup> Server 2008 (including R2) Standard/Enterprise
Windows® 10 Professional/Enterprise
Windows® 8/8.1 Professional/Enterprise
Windows® 7 Professional/Enterprise/Ultimate
Windows <sup>®</sup> Vista Business/Enterprise/Ultimate
Windows <sup>®</sup> Small Business Server 2011

#### Supported databases

GFI LanGuard Central Management Server uses a database to store information retrieved from multiple GFI LanGuard installations. The database backend can be any of the following:

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

#### Firewall Ports and Protocols

GFI LanGuard instances communicate with the GFI LanGuard Central Management Server via port **1077**. Configure your firewall to allow **inbound** connections on TCP port **1077**, on computers running GFI LanGuard and the GFI LanGuard Central Management Server.

If port 1077 is already in use by another application, the GFI LanGuard Central Management Server automatically searches for an available port in the range of **1077-1277**.

#### 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\

### 2.3 Importing and exporting GFI LanGuard settings

The Import and Export Configurations Wizard is a GFI LanGuard feature that enables you to import and export settings, including:

- » Scanning Profiles
- » Vulnerability Assessment
- » Ports (TCP/UDP)
- » Results Filtering Reports
- » Auto-Remediate Settings (Auto-Uninstall and Patch settings)
- » Options (Database Backend, Alerting, Schedule scan and Internal Settings).

This feature is useful when you want to retain configuration settings from an older version of GFI LanGuard and reuse them in a new version. The following sections contain information about:

- » Exporting configurations to a file
- » Importing configurations from a file
- » Importing configurations from another instance of GFI LanGuard

Exporting configurations to a file

To export the configurations:

- 1. Launch GFI LanGuard.
- 2. From the top navigation click File > Import and Export Configurations.
- 3. Select Export the desired configuration to a file and click Next.
- 4. Specify the path were to save the exported configuration, and click Next.

Import and Export Configurations Wizard	83
Welcome to the Import and Export Configurations Wizard Use this wizard to import or export GFI LanGuard configurations.	<b>Ø</b>
What do you want to do?	
<ul> <li>Export the desired configurations to a file Export GFI LanGuard configuration to a file (.cfg)</li> <li>Import the desired configurations from a file Import GFI LanGuard configurations from a file (.cfg)</li> <li>Import the configurations from another instance Import GFI LanGuard configurations from another installation</li> </ul>	
< Back Next >	Cancel

Screenshot 5: Export configurations to file

5. Wait for the configuration tree to load and select the configurations to export. Click **Next** to start export.

- 6. A notify dialog will confirm that exporting is completed.
- 7. Click **OK** to finish.

Importing configurations from a file

To import saved configurations:

1. Launch GFI LanGuard.

2. From the top navigation click **File > Import and Export Configurations**.

3. Select Import the desired configuration from a file and click Next.

4. Specify the path from where to load configuration, and click Next.

5. Wait for the configuration tree to load and select the configurations to import. Click **Next** to start import.

Import and Export Configurations Wizard	83
Welcome to the Import and Export Configurations Wizard Use this wizard to import or export GFI LanGuard configurations.	ø
What do you want to do?	
<ul> <li>Export the desired configurations to a file Export GFI LanGuard configuration to a file (.cfg)</li> <li>Import the desired configurations from a file Import GFI LanGuard configurations from a file (.cfg)</li> <li>Import the configurations from another instance Import GFI LanGuard configurations from another installation</li> </ul>	
< Back Next >	Cancel

Screenshot 6: Import configurations from a file

6. Confirm the override dialog box by clicking **Yes** or **No** as required.

- 7. A notify dialog will confirm that exporting is completed.
- 8. Click **OK** to finish.

Importing configurations from another instance of GFI LanGuard

1. Launch GFI LanGuard.

2. From the top navigation click **File > 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 on the machine from where you want to import the configurations. The default location is:

Operating Systems	Path
Windows <sup>®</sup> XP Professional (SP2 or higher)	<local disk="">\Documents and Settings\All Users\Application Data\GFI\LanGuard <version></version></local>
Windows <sup>®</sup> Server 2003 Standard/Enterprise	<local disk="">\Documents and Settings\All Users\Application Data\GFI\LanGuard <version></version></local>
Windows <sup>®</sup> Vista Business/Enterprise/Ultimate and later	<local disk="">\Program Files\GFI\LanGuard <version></version></local>
Windows <sup>®</sup> Server 2008 (including R2) Stand- ard/Enterprise and later	<local disk="">\Program Files\GFI\LanGuard <version></version></local>

Import and Export Configurations Wizard	8
Welcome to the Import and Export Configurations Wizard Use this wizard to import or export GFI LanGuard configurations.	ø
What do you want to do?	
<ul> <li>Export the desired configurations to a file</li> <li>Export GFI LanGuard configuration to a file (.cfg)</li> <li>Treact the desired configurations form a file</li> </ul>	
Import the desired configurations from a file Import GFI LanGuard configurations from a file (.cfg)	
Import the configurations from another instance Import GFI LanGuard configurations from another installation	
< Back Next >	Cancel

Screenshot 7: Import setting

5. Select which settings you want to import and click **Next**.

6. While importing, GFI LanGuard will ask you whether you want to override or keep your settings. Select one of the following options:

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

7. Click **OK** when the import is ready.

# 2.4 Installing GFI LanGuard

#### 2.4.1 Important notes

Before running the installation wizard:

» 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. For more information, refer to <u>Upgrading GFI LanGuard</u> (page 35).

» You must have a GFI Account or a license key to install GFI LanGuard. For more information, refer to <u>Obtaining a</u> <u>GFI LanGuard subscription</u> (page 34).

» Ensure that the machine where GFI LanGuard is going to be installed meets the system requirements. For more information, refer to GFI LanGuard system requirements (page 20).

» 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 <u>Firewall Ports and Protocols</u> (page 22).

- » Disable third-party antivirus during the installation process.
- » Save any pending work and close all open applications on the machine.

#### 2.4.2 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.

GFI LanGuard			
<b>GF</b> Network	<b>LanGuard</b> <sup>™</sup> security scanner and patch management	ent	
Select the components to be installed. Missing prerequisites will be downloaded and installed.			
		👆 Downloaded	🛐 Installed
0	Microsoft .NET Framework 4.5.1	$\checkmark$	$\checkmark$
	GFI LanGuard	$\checkmark$	×
$\overline{\mathbf{v}}$	GFI LanGuard Central Management Server	$\checkmark$	X
		Nex	t Cancel

Screenshot 8: 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. For more information, refer to <u>Obtaining a GFI LanGuard subscription</u> (page 34).

Database Configuration	×
Please configure a Microsof SQL server name:	t SQL Server.
SQL database name:	LNSSScanResults12
Use Windows Authentic	ation
SQL Login:	SA
Password:	•••••
	OK Cancel

Screenshot 9: 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.	
SQL database name	Displays the database name. GFI LanGuard keeps the default name of the database. During an upgrade, you may decide to specify a different database name so that you can use a clean database while maintaining the old database from a previous version.	
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.

🖶 GFI LanGuard Setup 📃 🔲 🗙			
End-User License Agreement			
Please read the following license agreement carefully	<u> </u>		
GFI® End-User License Agree	ement		
For: GFI FaxMaker <sup>*</sup> ; GFI Archiver <sup>**</sup> , GFI MailEssential LanGuard <sup>*</sup> ;	s <sup>*</sup> ; GFI WebMonitor <sup>*</sup> ; GFI		
GFI Network Server Monitor*; GFI EventsManager* a	nd GFI EndPointSecurity®		
("Software")			
PLEASE CAREFULLY REVIEW THE FOLLOWING TERMS AN			
<ul> <li>I accept the terms in the License Agreement</li> <li>I do not accept the terms in the License Agreement</li> </ul>			
< Back	Next > Cancel		

Screenshot 10: 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**.

🚏 GFI LanGuard Setup 📃 🖂 🗙				
Attendant service credentials				
Specify the cred operations	entials needed to run scheduled GFI LanGuard			
Administrator use	account (in format 'DOMAIN\administrator'):			
Na <u>m</u> e:	Domain\John Smith			
Password:	•••••			
NOTE: Specify the administrator account under which the scheduled operations such as scans, product update and auto-remediation will operate.				
To Successfully run these operations, the specified account must have administrator privileges over target computers.				
	< Back Cancel Cancel			

Screenshot 11: Attendant service credentials

10. Key in the administrator credentials and password. The credentials are used for the service account under which scheduled operations run. Click **Next**.

#### NOTE

It is highly recommended to provide a valid username and password and not to skip this option. Scan and remediation processes will fail if the credentials do not have permission on the remote machines.

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

12. Click **Finish** to finalize the 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.

#### NOTES

Test your installation after the product is installed. For more information, refer to <u>Testing the installation</u> (page 38).

#### 2.4.3 Obtaining a GFI LanGuard subscription

During the GFI LanGuard installation, you are requested to key in your GFI account credentials or a license key.

Choose the procedure that best describes your scenario for information on how to obtain a subscription:

#### Evaluating GFI LanGuard for 30 days

For a free GFI LanGuard trial for 30 days:

1. Fill in the registration form at https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-lan-guard/download

2. Check your mail box and open the email from sales@gfi.com.

- 3. Click the link provided to confirm your account details and to create a password for your GFI Account.
- 4. After confirming your account details, the installer is automatically downloaded.
- 5. During the installation process, provide your GFI account credentials.

#### I have a GFI Account and want to install GFI LanGuard for the first time

During installation, key in the username and password associated with your account and verify that the account is valid.

Your license status can also be verified from the GFI Accounts Portal. Login to https://accounts.gfi.com and click **My** products. Select GFI LanGuard to check the status of your license.

#### Upgrading to a newer build or Service Release of the same version

When upgrading GFI LanGuard to a build of the same version, such as when installing a Service Release, you have two options to enter a license:

Enter your GFI account credentials or select a license key from the Available keys list.

If you don't have access to your previous license key, but you have a GFI account, you can retrieve the license key from the GFI Accounts portal. Login to https://accounts.gfi.com and click **My products**. Select GFI LanGuard to get your license key.

#### Upgrading to a newer version of GFI LanGuard

When upgrading your current installation to a newer major version, there are two scenarios:

- » If using GFI Accounts, enter your credentials.
- » If using a license key, upgrade your key:

Log in to the GFI Customer Area on https://customers.gfi.com/.

• If you have a valid GFI LanGuard maintenance agreement, click the blue key icon on the right and select **Upgrade License Key** to upgrade your license key. Then, key in your upgraded license key.

• If you do not have a valid GFI LanGuard maintenance agreement, click on the blue key icon on the right and select **Renewal**. Then, renew your maintenance agreement. On completion a new license key is available.

## 2.5 Upgrading GFI LanGuard

Choose your current GFI LanGuard version for notes and instructions on how to upgrade to the latest version while retaining all settings:

- » GFI LanGuard 12.1
- » GFI LanGuard 12
- » GFI LanGuard 2015 and earlier

To determine your current version number open the GFI LanGuard console click 💷 and navigate to Help > About.

#### 2.5.1 Upgrading from GFI LanGuard 12.1 or later

This topic describes how to upgrade a GFI LanGuard version 12.1 or later installation to the latest version while retaining all settings.

#### Important notes before upgrading

» GFI LanGuard 12.2 supports TLS 1.1. 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 local policy. For more information, refer to <u>GFI</u> LanGuard and TLS 1.1 or higher (page 21).

» Ensure your server meets the system requirements.

» Backup your current GFI LanGuard database and the GFI LanGuard Data directory which is typically available from: C:\ProgramData\GFI\LanGuard <version>\

» Export the GFI LanGuard settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to <u>Importing and exporting GFI LanGuard settings</u> (page 27).

- » Log on to your current GFI LanGuard server as an Administrator or use an account with administrative privileges.
- » Save any pending work and close all open applications on the machine before starting the upgrade.

» Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

#### Upgrade procedure

1. Download the latest build of GFI LanGuard on the server where GFI LanGuard is currently installed. Go to http://go.g-fi.com/?pageid=lan\_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded 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 installer.

4. In the components screen, select **GFI LanGuard** to install a local server instance. You may optionally select **GFI LanGuard Central Management Server** to install a central server instance. Install only one instance of the Central Management Server within your organization.

5. Follow the wizard steps to install the new version.

6. On update completion, test your installation by running a scan to ensure GFI LanGuard installed successfully.

#### 2.5.2 Upgrading from GFI LanGuard 12

This topic describes how to upgrade a GFI LanGuard version 12 installation to the latest version while retaining all settings.

#### Important notes before upgrading

» GFI LanGuard 12.1 introduces the Central Management Server for GFI LanGuard instances installed in another language. GFI LanGuard Central Management Server brings together the management of multiple GFI LanGuard instances through a common console, enabling you to manage many more devices. You can install this component on the local server while running the upgrade process. Install only one instance of the Central Management Server within your organization. Note that this component can be installed on any machine within the organization and has different system requirements than the product.

» GFI LanGuard 12.2 supports TLS 1.1. 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 local policy. For more information refer to Support for TLS 1.1

» Ensure your server meets the system requirements.

» Backup your current GFI LanGuard database and the GFI LanGuard Data directory which is typically available from: C:\ProgramData\GFI\LanGuard <version>\

» Export the GFI LanGuard settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to Importing and exporting GFI LanGuard settings (page 27).

» Log on to your current GFI LanGuard server as an Administrator or use an account with administrative privileges.

» Save any pending work and close all open applications on the machine before starting the upgrade.

» Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

#### Upgrade procedure

1. Download the latest build of GFI LanGuard on the server where GFI LanGuard is currently installed. Go to http://go.g-fi.com/?pageid=lan\_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded 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 installer.

4. In the components screen, select **GFI LanGuard** to install a local server instance. You may optionally select **GFI LanGuard Central Management Server** to install a central server instance. Install only one instance of the Central Management Server within your organization.

5. Follow the wizard steps to install the new version.

6. On update completion, test your installation by running a scan to ensure GFI LanGuard installed successfully.
## 2.5.3 Upgrading from GFI LanGuard 2015 or earlier

This topic describes how to upgrade a GFI LanGuard version 2015 or earlier installation to the latest version while retaining all settings.

The upgrade can be performed for the following versions:

- » GFI LanGuard 2015
- » GFI LanGuard 2014
- » GFI LanGuard 2012

### Important notes before upgrading

» Log in to the GFI Customer Area to get a new license key. Click the blue key icon on the right and select **Upgrade** License Key, or click Renewal to extend your maintenance agreement.

» GFI LanGuard 12 introduces the Central Management Server. GFI LanGuard Central Management Server brings together the management of multiple GFI LanGuard instances through a common console, enabling you to manage many more devices. You can install this component on the local server while running the upgrade process. Install only one instance of the Central Management Server within your organization. Note that this component can be installed on any machine within the organization and has different system requirements than the product.

» Installation on Windows Server 2003, Windows Small Business Server 2003 or Windows XP are no longer supported. Install the latest version of GFI LanGuard on a supported OS and then import the settings from your current installation to the new instance. For more information, refer to <u>Importing and exporting GFI LanGuard settings</u> (page 27).

» GFI LanGuard 12 does not support Microsoft SQL Server 2005 or earlier versions. If using an unsupported version it is recommended to install a supported version and move your current GFI LanGuard database to the new SQL server. Configure your current GFI LanGuard instance to use the new database and proceed to upgrade GFI LanGuard.

» GFI LanGuard 12 does not support Microsoft Access database. If using a Microsoft Access database, on running the upgrade, GFI LanGuard can be configured to use an existing SQL Server or SQL Express. Alternatively the wizard can install Microsoft SQL 2012 Express for free on the local server.

» Ensure your server meets the system requirements.

» Backup your current GFI LanGuard database and the GFI LanGuard Data directory which is typically available from: C:\ProgramData\GFI\LanGuard <version>\

- » Export the GFI LanGuard settings before upgrade. This backup may be useful in case the upgrade fails. For more information, refer to <u>Importing and exporting GFI LanGuard settings</u> (page 27).
- » Log on to your current GFI LanGuard server as an Administrator or use an account with administrative privileges.
- » Save any pending work and close all open applications on the machine before starting the upgrade.

» Disable anti-virus software on the server machine during the upgrade installation. Re-enable it once upgrade is complete.

#### Upgrade procedure

1. Download the latest build of GFI LanGuard on the server where GFI LanGuard is currently installed. Go to http://go.g-fi.com/?pageid=lan\_trial, click **Login** and key in your GFI Account credentials.

2. Right-click the newly downloaded 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 installer.

4. In the components screen, select **GFI LanGuard** to install a local server instance. You may optionally select **GFI LanGuard Central Management Server** to install a central server instance. Install only one instance of the Central Management Server within your organization.

5. After specifying your account's license key, the wizard prompts you to choose an existing Microsoft SQL Server or SQL Express. Alternatively click the option to install Microsoft SQL Express (free) on the local server. Follow the Microsoft SQL Express 2012 wizard.

6. Follow the wizard steps to install the new version side-by-side to your old version.

7. On launching GFI LanGuard the first time, you will be asked to import the configuration from the old instance. Choose the settings to import and click **Next**.

8. On import completion, test your installation by running a scan to ensure GFI LanGuard installed successfully. When the operation of the new version is confirmed, you may proceed to uninstall the old version from Windows Programs and Features.

## 2.6 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 12: Launch a scan

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

Launch a New Scan					
Sc <u>a</u> n Target: localhost	¥	P <u>r</u> ofile: Full Scan	~	0	
<u>C</u> redentials:		<u>U</u> sername:	Password:	Key file:	
Currently logged on user	~				 Scan
Scan Options					

Screenshot 13: 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 14: 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. For more information, refer to Interpreting scan results (page 151).

# **3 GFI LanGuard Central Management Server**

With GFI LanGuard Central Management Server, multiple GFI LanGuard instances installed in separate locations can be brought together through a common console. The GFI LanGuard Central Management Server console offers administrators a view of the security and vulnerability status for all computers, networks or domains managed by the different GFI LanGuard instances. It also offers centralized reporting and visibility by capturing data from the various deployments of GFI LanGuard.



GFI LanGuard Central Management Server is used only for reporting. Scans and remediation take place only in GFI LanGuard and then information is centralized to GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard. Synchronization usually takes a few minutes. Delay depends on network size and amount of data being transferred.

#### 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.

## 3.1 Installing GFI LanGuard Central Management Server

GFI LanGuard Central Management Server uses the same installation file of GFI LanGuard. Before starting the installation ensure that the system requirements are met. For more information, refer to <u>Central Management Server system</u> requirements (page 41).

3.1.1 Central Management Server system requirements	41
3.1.2 Installing Central Management Server	42
3.1.3 Uninstalling Central Management Server	44

## 3.1.1 Central Management Server system requirements

Computers running GFI LanGuard Central Management Server must meet the system requirements described below.

#### Hardware requirements

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

Component	Requirement
Processor	2.8 GHz quad-core
Physical Storage	10 GB HDD free space
RAM	8 GB RAM

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

The following table lists operating systems and versions where the GFI LanGuard Central Management Server can be installed. Ensure that these operating systems are running the latest Service Pack as provided by Microsoft.

Operating System
Windows <sup>®</sup> Server 2016
Windows <sup>®</sup> Server 2012 (including R2)
Windows <sup>®</sup> Server 2008 (including R2) Standard/Enterprise
Windows <sup>®</sup> 10 Professional/Enterprise
Windows <sup>®</sup> 8/8.1 Professional/Enterprise
Windows <sup>®</sup> 7 Professional/Enterprise/Ultimate
Windows <sup>®</sup> Vista Business/Enterprise/Ultimate
Windows <sup>®</sup> Small Business Server 2011

#### Supported databases

GFI LanGuard Central Management Server uses a database to store information retrieved from multiple GFI LanGuard installations. The database backend can be any of the following:

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

#### Firewall Ports and Protocols

GFI LanGuard instances communicate with the GFI LanGuard Central Management Server via port 1077. Configure your

firewall to allow **inbound** connections on TCP port **1077**, on computers running GFI LanGuard and the GFI LanGuard Central Management Server.

If port 1077 is already in use by another application, the GFI LanGuard Central Management Server automatically searches for an available port in the range of **1077-1277**.

### 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\

## 3.1.2 Installing Central Management Server

To install GFI LanGuard Central Management Server:

1. Logon using administrator credentials on the machine where to install GFI LanGuard Central Management Server.

#### NOTE

If you are installing both GFI LanGuard and GFI LanGuard Central Management Server on the same machine, the installation wizard will first guide you to install GFI LanGuard. For more information, refer to <u>Installing GFI</u> <u>LanGuard</u> (page 30).

2. Launch the setup and select the installation language.

#### 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.

GFI LanGuar	d		
<b>GF</b> Network	LanGuard <sup>™</sup> security scanner and patch management	ent	
<b>*</b>	Select the components to be installed. Missing (	prerequisites will be download	ed and installed.
		👆 Downloaded	🛐 Installed
0	Microsoft .NET Framework 4.5.1	$\checkmark$	$\checkmark$
	GFI LanGuard	$\checkmark$	×
	GFI LanGuard Central Management Server	$\checkmark$	×
		Ne>	ct Cancel

Screenshot 15: Select components to be installed

3. Ensure GFI LanGuard Central Management Server is selected in the components list and click **Next**.

Database Configuration	×
Please configure a Microsoft : SQL server name:	5QL Server.
SQL database name:	LNSSScanResults12
Use Windows Authenticat	ion
SQL Login:	SA
Password:	•••••
	OK Cancel

Screenshot 16: Configure the database server

4. 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 Central Management Server database is hosted.

OPTION	DESCRIPTION
Use Windows Authentication	Select this option if you want the GFI LanGuard Central Management Server to use the Microsoft Windows cre- dentials of the currently logged in user when connecting to the Microsoft SQL database.
Username / Password	If GFI LanGuard Central Management Server 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.

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

🙀 GFI LanGuard Centra	Management Server Setup	
Service logon information The following logon information is used by GFI LanGuard Central Management Service		
Administrator user acco	unt (in format 'DOMAIN\administrator'):	
<u>U</u> ser Name:	WIN-O0U9HBG95G2\Administrator	
Password:	•••••••	
NOTE: The account must have the "Logon As Service" right. If it doesn't, it will be switched ON automatically for the specified account.		
	Back Next Cancel	

Screenshot 17: Key in credentials for the Windows service

6. In the Service logon information screen, key in the administrator credentials and password for the Windows service under which scheduled operations run. Click **Next** to continue setup.

7. Click **Install** to install GFI LanGuard Central Management Server in the default location or **Browse** to change path.

8. Click **Finish** to finalize installation.

## 3.1.3 Uninstalling Central Management Server

To uninstall GFI LanGuard Central Management Server

#### 1. Click Start > Control Panel > Programs > Programs and Features.

- 2. Select GFI LanGuard Central Management Server from the list, and click Uninstall.
- 3. When Are you sure you want to uninstall GFI LanGuard Central Management Server? appears, click Yes.
- 4. On completion, click **Finish**.

## 3.2 Joining GFI LanGuard to Central Management Server

The GFI LanGuard Central Management Server provides centralized reporting for multiple GFI LanGuard instances. However, each and every GFI LanGuard instance needs to be manually configured to point to a GFI LanGuard Central Management Server to avail yourself of this feature.

#### 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.

GFI LanGuard Central Management Server is used only for reporting. Scans and remediation take place only in GFI LanGuard and then information is centralized to GFI LanGuard Central Management Server soon after it becomes available in GFI LanGuard. Synchronization usually takes a few minutes. Delay depends on network size and amount of data being transferred.

#### NOTE

GFI LanGuard Central Management Server requires a Microsoft SQL or SQL Express database. If this is not configured, click the provided link or navigate to **Database Maintenance Options > Database backend settings** to set up an SQL Database. For more information, refer to <u>Configuring Database Maintenance Options</u> (page 236).

To configure Central Management Server options:

#### 1. Click **Configuration** tab > **Central Management Server**.



Screenshot 18: The GFI LanGuard Central Management Server page

2. Click **Configure** GFI LanGuard Central Management Server.

Central Management Server	×
General Site Details	
Central Management Server properties.	
Enable central management	
Server information	
Server address: WIN-00U9HBG95G2	
Port: 1077 🛨	
Use GFI LanGuard service credentials to authenticate	
Username:	
Password:	
OK Ca	incel

Screenshot 19: Central Management Server dialog - General tab

3. From the **General** tab, configure the following options:

Option	Description
Enable central management	Click to enable GFI LanGuard Central Management Server. Also enables you to provide the server IP address and port on which this instance of GFI LanGuard will communicate with GFI LanGuard Central Management Server.
Use GFI LanGuard service cre- dentials to authenticate	Enables you to use the GFI LanGuard service credentials provided during setup to authenticate with GFI LanGuard Central Management Server. This is enabled by default. If disabled, you will need to provide a user- name and a password to be used with GFI LanGuard Central Management Server.

4. Click **Site Details** to continue setup

Central Manage	ement Server	×
General Site	Details	
Site details =		
Specify in GFI LanG	formation about this GFI LanGuard instance that will be shown in uard Central Management Console	
Name:	WIN-00U9HBG95G2	
Descriptio	n:	
Location:	.0	
Latitude:	0.00 😴	
Longitude	0.00 🛫	
	OK Cancel	

Screenshot 20: Central Management Server dialog - Site Details tab

5. In the **Site Details** tab, provide the site details that will be shown in GFI LanGuard Central Management Server. These include the name of this GFI LanGuard instance, a description, the location name and the latitude and longitude values.

## 3.3 Configuring GFI LanGuard Central Management Server

The following topics help you configure GFI LanGuard Central Management Server:

3.3.1 Configuring GFI LanGuard Central Management Server database settings	48
3.3.2 Specifying data retention settings	49
3.3.3 Configuring Central Management Server user privileges	49
3.3.4 Managing GFI LanGuard sites in Central Management Server	51
3.3.5 Configuring HTTPS Certificate in Central Management Server	52
3.3.6 Email settings in Central Management Server	
3.3.7 Configuring Central Management Server Updates	57

## 3.3.1 Configuring GFI LanGuard Central Management Server database settings

GFI LanGuard Central Management Server supports Microsoft SQL Server and SQL Server Express databases (2005 and later editions) that can be configured to store collected monitoring data. This data is used by GFI LanGuard Central Management Server to populate the dashboards and for reporting purposes.

The currently configured database can be viewed from **Settings > Database**. Here you can also specify data retention settings.

To change the current database configuration or create a new database:

1. In GFI LanGuard Central Management Server, go to **Settings > Database**.

<b>GFI Lan</b> Guard		â	<b>(</b>	ы	٠	٠	?	
SETTINGS								
Database	Database Settings	l Server dat	abase an	d autom	atic datah	ase clear	0110	
Users		L Server aut		aatonii			nup.	
Sites	SQL Server							
HTTPS Certificate	WIN-O0U9HBG95G2\S	SQLEXPRES	SS					
Email	Windows Authenticati	on SQL	Server A	uthentica	ation			
	Database Name							_
Updates	LGCMCScanResults1	3						
	Retention Policy							
	Never delete history	Keep hist	tory for a	specifie	d period			
	Months							
	36							

Screenshot 21: Configuring Database settings for GFI LanGuard Central Management Server

#### 2. Under the **Database Server** area, modify the following options:

OPTION	DESCRIPTION
SQL Server	The name of the SQL Server instance. Key in the name of the server where the database is installed.
Windows Authentic- ation	Select this option to use Windows credentials when connecting to your SQL Server.

OPTION	DESCRIPTION
SQL Server Authentic- ation	If your SQL Server has been installed in SQL Server Authentication Mode, select this option and provide <b>Username</b> and <b>Password</b> .
Database Name	If you want to create a new database, use this field to type the name of the database you want to create in SQL Server.
	<b>IMPORTANT</b> Ensure that the database name entered is unique, otherwise you will overwrite the existing database.

## 3.3.2 Specifying data retention settings

Retention policy settings define whether to keep all historical data stored in the configured database or whether to delete this data after a specified amount of time. By default, GFI LanGuard Central Management Server is set to keep historical data for a period of 36 months.

To change data retention settings:

1. In GFI LanGuard Central Management Server, go to **Settings > Database**.

2. Under the **Retention Policy** area, modify the following options:

Select from the following options:

OPTION	DESCRIPTION	
Never delete history	Select to keep all data gathered by GFI LanGuard Central Management Server indefinitely.	
	NOTE If selecting this option ensure adequate disk space on the server.	
Keep history for a spe- cified period	Select this option to delete collected data after a defined amount of time. Use the Months field to spe- cify an amount in months. Default is 36.	

## 3.3.3 Configuring Central Management Server user privileges

Use this area to configure user access rights to the GFI LanGuard Central Management Server Console. Configured users will be able to access the console from any location using an internet browser. GFI LanGuard Central Management Server uses Active Directory to authenticate users.

GFI LanGuard Central Management Server offers the following roles:

OPTION	DESCRIPTION
IT Manager	This role is made up of both the Site Admin and the Auditor roles and allows users full access to the GFI LanGuard Cen- tral Management Server.
Site Admin	Users with Site Admin rights are able to configure and manage the console.
Auditor	The auditor role permits users to access the reporting tools of GFI LanGuard Central Management Server Console and the Dashboards.

To add a new user:

1. In the top navigation bar, click the settings icon.

- 2. Select **Users**.
- 3. Click **Add User** icon.

<b>GFI Lan</b> Guard	🔒 Home	Oashboard	L Reports	<b>2</b>	¢ 0	L WIN-00U9HBG95G2\Administrato
SETTINGS						
Database	User Setti	ngs				
Users	Configure per	r-user privileges.				
Sites	Users					Q Search
	Add new a	uthorization rule:				
HTTPS Certificate	User	User Group Bo	b Smith			
Email	IT Mai	nager				
	<ul> <li>Can re</li> </ul>	egister new sites				
Updates	Default r Apply th	role for new sites Sites is role for all sites Site	e Admin 🔻			
	Set role i	for each citer	Site Admin	Auditor	None	
	Malta	a	o Site Admin			
						Save Cancel
	Na	me	Туре		Role	
	🗷 🗙 WIN	I-O0U9HBG95G2\Adminis	tr User		IT Man	ager
	🗷 🗙 WIN	I-O0U9HBG95G2\LANGUA	AR User		Site Ac	min
	🗷 🗙 Jon	Snow	User		Site Ac	Imin
	🗷 🗙 Jane	2 Doe	User		IT Man	ager

Screenshot 22: Configuring user access rights to the GFI LanGuard Central Management Server Console

## 4. Select from the following options:

OPTION	DESCRIPTION
Search	Click the Search icon to expand a search field where you can key in a user or group name to search for.
User / User Group	Key in the name of an existing Active Directory User or Group of users. A list of existing users or groups is automatically displayed as you type. Select the desired name from the list.
IT Manager	Check the checkbox to assign the role of IT Manager to the user. This role gives users both Site Admin and Auditor rights.
Can register new sites	Select this option if you want the user to be able to register new sites with GFI LanGuard Cen- tral Management Server.
Default role for new sites	Set the default role for this user for new sites that are added to GFI LanGuard Central Man- agement Server.
Apply this role for all sites	Select the role for the new user to apply to existing sites.
Set role for each site	Use the provided buttons if you want to manually set different roles for different sites. Use the drop down list to select one of the following options: <b>None</b> , <b>Auditor</b> , <b>Site Admin</b> .

### 5. Click **Save**.

## 3.3.4 Managing GFI LanGuard sites in Central Management Server

The Sites window lists all the GFI LanGuard instances that have been connected to the GFI LanGuard Central Management Server. The following details are listed:

OPTION	DESCRIPTION
Name	The name of the machine where the GFI LanGuard instance is installed.
Location	The location where the GFI LanGuard machine is located.
Last sync	The date when the GFI LanGuard instance last synced with the GFI LanGuard Central Management Server.
License usage	An amount showing the percentage used.
License expiry	The date when the current GFI LanGuard Central Management Server expires.
Status	Shows the current license status, for example whether it has been registered or expired.

#### IMPORTANT

New sites cannot be added through the GFI LanGuard Central Management Server console. The configuration needs to be carried out in GFI LanGuard as the GFI LanGuard Central Management Server cannot automatically detect GFI LanGuard instances. For more information refer to: http://go.gfi.com/?pageid=LGCMSSites

#### Editing site details

You can edit details of sites that have been connected to GFI LanGuard Central Management Server. To do this:

1. In the list of sites, click the edit icon next to the site to edit.

2. Select the **Identity and Sync Information** tab to edit the following details:

OPTION	DESCRIPTION
Name	The name of the site where a GFI LanGuard instance is located. You can replace this by a friendly name. This name will appear as alt text when hovering over markers in the home page.
Location	The name of the country where a GFI LanGuard instance is located.
Latitude / Longitude	Use the down and up arrows to manually set the latitude and longitude of the GFI LanGuard instance location.
Description	A description of the site, for example, Main Office.
Last Sync	This field contains the date and time of the last synchronization between the GFI LanGuard instance and GFI LanGuard Central Management Server which cannot be edited.

#### 3. Select the Authorized users tab to edit the following details:

OPTION	DESCRIPTION
Site admins	Site admins are granted access to the configuration area of GFI LanGuard Central Man- agement Server. Click the Add icon to add new users or groups.
Auditors	Auditors have access to reports and dashboard areas of the GFI LanGuard Central Man- agement Server Console. Click the Add icon to add new users or groups.

### NOTE

Users or groups configured in the Users area will be automatically added to these lists. For more information, refer to <u>Configuring Central Management Server user privileges</u> (page 49).

4. Select the License information tab to view additional information related to license usage and license expiry date.

5. Click Save.

## 3.3.5 Configuring HTTPS Certificate in Central Management Server

GFI LanGuard Central Management Server Console is accessed securely through HTTPS. This requires digital certificates for server authentication and communication encryption purposes. By default, GFI LanGuard Central Management Server Console uses a certificate issued during installation by a special-purpose Certificate Authority (CA) called **GFI LanGuard Central Management Console CA**. The web clients of GFI LanGuard Central Management Server Console are subsequently presented a certificate chain consisting of:

- » A self-signed CA certificate issued by GFI LanGuard Central Management Console CA
- » A certificate issued to the computer where the product is installed, having as subject the name of the computer

For any web browser or a GFI LanGuard instance to seamlessly connect to GFI LanGuard Central Management Server Console, the **GFI LanGuard Central Management Console CA** certificate needs to be trusted. Trust the CA certificate by adding it to the list of Trusted Certificate Authorities on client computers.

The **GFI LanGuard Central Management Console CA** creates a single certificate during installation. This certificate is then permanently disabled and the CA cannot issue more certificates. This makes it safe to add this CA to the list of Trusted Certificate Authorities on client computers.

Alternatively, if you already have a trusted certificate, you can use it instead of the default certificate generated by GFI LanGuard.

The following topics provide more information on how to implement Trusted Root Certificates:

## Adding the CA Certificate as Trusted Certificate Authority

This topic describes how to download the CA certificate from within GFI LanGuard Central Management Server and how to install it as a Trusted Certificate Authority.

For Microsoft Internet Explorer, Google Chrome and Opera on Microsoft Windows

1. Open GFI LanGuard Central Management Server Console in your browser.

- 2. When you receive the certificate error in the browser, select **Continue to this website (not recommended)**.
- 3. Key in the authentication credentials.
- 4. From the top navigation menu click the **Settings** icon.

5. Select **HTTPS Certificate** and click **Download certificate**. The following file will be downloaded to your computer: root.cer.

6. Locate the file and double-click to open.

Certificate	x						
General Details Certification Path							
Certificate Information							
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.							
Issued to: GFI LanGuard Central Management Server CA							
Issued by: GFI LanGuard Central Management Server CA							
Valid from 30/ 08/ 2015 to 30/ 08/ 2025							
Install Certificate Issuer Statement Learn more about <u>certificates</u>							
ОК							

Screenshot 23: Installing the CA Certificate

## 7. Click Install Certificate....

8. In the Certificate Import Wizard, click **Next**.

rtificate Import Wizard	<u> </u>
Certificate Store Certificate stores are system areas w	here certificates are kept.
Windows can automatically select a ce the certificate.	ertificate store, or you can specify a location for
O Automatically select the certific	ate store based on the type of certificate
Place all certificates in the follow	wing store
Certificate store:	
	Browse
	Select the certificate store you want to use.
Learn more about <u>certificate stores</u>	Personal Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Active Directory User Object
	Show physical stores
	OK Cancel

Screenshot 24: Select location for imported certificate

9. Select Place all certificates in the following store, then click Browse... and select Trusted Root Certification Authorities. Click OK

10. Click **Next**.

11. Click Finish.

12. Click **OK** The CA Certificate is now trusted.

For Mozilla Firefox on any operating system

1. Open GFI LanGuard Central Management Server Console in your browser.

2. When you receive the certificate error in the browser, select I Understand the Risks then click Add Exception....

3. In the **Add Security Exception** window, click **Confirm Security Exception**. This allows you to continue to the application.

4. Key in the authentication credentials.

5. From the top navigation menu click the **Settings** icon.

6. Select **HTTPS Certificate** and click **Download certificate**. The following file will be downloaded to your computer: root.pem.

7. In Mozilla Firefox, go to Settings > Options > Advanced > Certificates > View Certificates > Authorities tab and click Import....

8. Select the previously downloaded file root.pem.

neral	Data	Choices	Network	Update	Certificates	
Certifica	ate Manager					X
You	r Certificates	People Serve	ers Authorities (	Others		
Y	ou have certi	ficates on file	that identify these	certificate author	ities:	
C	ertificate Na	me		Security Device		<b>E</b>
4	(c) 2005 TÜR	RKTRUST Bilgi İ	İletişim ve Bilişim			<u>^</u>
	TÜRKTRU	ST Elektronik S	ertifika Hizmet S	Builtin Object T	oken	
4	A-Trust Ges.	f. Sicherheitss	ysteme im elektr			
	A-Trust-n	Qual-03		Builtin Object T	oken	
4	AC Came	Downloading (	Certificate			
	Chamb	Variabaria		Carlina I	atherity (CA)	
	Global (	You have be	en asked to trust a	new Certificate A	Authority (CA).	
14	AC Came	Do you want	t to trust "GFI Land	Guard Central Mar	nagement Server CA" f	or the following purpose
	View	Z Trust thi	s CA to identify w	ebsites.	5	51 1
	<u>v</u> iew	Trust thi	s CA to identify en	nailusers		
		Trust th	- CA to identify en	Annual and a second	_	
		i rust thi	s CA to identify so	ntware developer	5.	
	_	Before trusti	ng this CA for any	purpose, vou sho	ould examine its certific	ate and its policy and
		procedures (	if available).			
		View	Examine CA ce	ertificate		

Screenshot 25: Importing a trusted CA Certificate in Firefox

9. Select Trust this CA to identify websites and click OK to complete the import.

For Safari, Google Chrome and Opera on Apple OS X

1. Open GFI LanGuard Central Management Server Console in your browser.

2. When you receive the certificate error in the browser, select **Continue**. This allows you to continue to the application.

3. Key in the authentication credentials.

4. From the top navigation menu click the **Settings** icon.

5. Select **HTTPS Certificate** and click **Download certificate**. The following file will be downloaded to your computer: root.p12.

6. Open the downloaded file root.p12 with Keychain Access.

	Do you y LanGuar This certi your deci Settings.	want your computer to trust certificates signed by "GFI rd Central Management Console CA" from now on? ficate will be marked as trusted for the current user only. To change ision later, open the certificate in Keychain Access and edit its Trust		
GFI LanG	uard Cent	ral Management Console CA		
Certificate Certi	GFI Lar Root cert Expires: O This ro	nGuard Central Management Console CA tificate authority duminică, 20 aprilie 2025, 15:29:49 Ora de vară a Europei de Est pot certificate is not trusted		
Subje	Country			
Orga	anization	GFI LanGuard Central Management Console (steli1) (20152921032948)		
Organizatio	onal Unit	GFI LanGuard Central Management Console		
Comm	on Name	GFI LanGuard Central Management Console CA		
Issu	er Name Country	US		
Orga	anization	GFI LanGuard Central Management Console (steli1)		
	Hide	Certificate Don't Trust Always Trust		

Screenshot 26: Configuring a CA Certificate in Safari, Google Chrome and Opera on Apple OS X

8. Select Always Trust.

#### Using an existing SSL certificate in Central Management Server

GFI LanGuard Central Management Server can be configured to use existing SSL certificates. This allows you to leverage your existing trust infrastructure. Follow the steps below after installing GFI LanGuard Central Management Server:

1. Open Internet Information Services Manager (IIS Manager).

- 2. From the **Connections tree**, select your server.
- 3. In the right pane, open Server Certificates.
- 4. From the **Actions** menu, click **Import...**.
- 5. In the Import Certificate dialog, click ... to browse and locate the PFX file which contains your existing SSL certificate.
- 6. If the certificate is password protected, key in the password and click **OK**
- 7. In the Connections tree, expand Sites and select GFI LanGuard Central Management Server Website.
- 8. From the **Actions** menu, click **Bindings...**

9. In the **Site Bindings** dialog, select **https** from the list and click **Edit...**.

#### NOTE

Ensure your existing SSL certificate is trusted on all machines where GFI LanGuard is installed since GFI LanGuard requires the certification chain to be trusted by the operating system.

## 3.3.6 Email settings in Central Management Server

The Email settings page lets you configure alerting options. These are required when GFI LanGuard Central Management Server needs to send important administrative notifications. To configure sender and recipient details:

#### 1. Click Settings > Email.

2. In the SMTP Server Details area, key in the parameters described below:

Option	Description
From email address	The sender email address. GFI LanGuard Central Management Server will use this email account to send the required emails.
SMTP Server	Key in the IP address of the server through which emails are routed.
Port	Define the port number through which emails are routed. Default value is 25
Authentication	Enable if SMTP server requires a username and password to authenticate when sending administrative noti- fications. Enter a username and password in the appropriate fields.
Use SSL	Select this option if you have an SSL (Secure Sockets Layer Protocol) encrypted connection to send the required emails.
Send noti- fications by email	Enable to send important administrative notifications via email.

#### 3. In the Email Recipients area, key in the following:

Email Address	Emails sent by GFI LanGuard Central Management Server are received by the email addresses configured in this area. Key in the email address in the appropriate field and press the add icon. Add as many email addresses as required.
Verify Email Settings	Click Verify Email Settings to verify that email settings are configured correctly.

4. Click Save.

## 3.3.7 Configuring Central Management Server Updates

The Product Updates area displays information about version and build number of the currently installed GFI LanGuard Central Management Server instance as well as the history of installed updates. Product updates enable you to keep your GFI LanGuard Central Management Server installation up to date with the latest updates. When enabled, GFI LanGuard Central Management Server checks for new updates at specified intervals, downloads the updates, and installs them.

#### NOTE

During product updates the GFI LanGuard Central Management Server services need to be stopped and restarted. This action causes disruption with remote GFI LanGuard instances. Operations can resume once the services are restarted.

To configure system updates:

#### 1. Go to Settings > Updates.

#### 2. Configure the following:

OPTION	DESCRIPTION
Install updates automatically	When enabled, GFI LanGuard Central Management Server automatically checks for new updates, downloads newly found packages and installs them. Click <b>Customize</b> to specify a schedule for the updates.
Update Now	Click to make GFI LanGuard Central Management Server check for updates.
Download from alternative ver- sion	Enable this option if you want GFI LanGuard Central Management Server to check in a particular location when looking for new product updates. Specify the URL location where to look for in the available field.
Proxy Server	<ul> <li>Enable if GFI LanGuard Central Management Server needs to connect to a specific Proxy Server to download updates. Provide the following details:</li> <li>Proxy Address - specify the IP address of the server from where GFI LanGuard Central Management Server will download the new updates.</li> <li>Port - Specify the port number used by GFI LanGuard Central Management Server to connect to the Proxy Server. Default is 8080.</li> <li>Authentication - if authentication is required, enable this option and provide the credentials of the target server.</li> </ul>

#### 3. Click Save.

## 3.4 Using the GFI LanGuard Central Management Server Console

The GFI LanGuard Central Management Server Console can be accessed by authorised users through any supported internet browser by using the following address:

https://<server name/IP address>:1077/Home/Home.

Different user access rights can be granted from the settings area. For more information, refer to <u>Configuring Central</u> Management Server user privileges (page 49).

The following topics provide information on how to use GFI LanGuard Central Management Server Console:

3.4.1 Central Management Server Home Page	58
3.4.2 Central Management Server Dashboards	60
3.4.3 Central Management Server Computer Tree	62
3.4.4 Using GFI LanGuard Central Management Server Reports	66

## 3.4.1 Central Management Server Home Page

The home page of the GFI LanGuard Central Management Server console offers two graphical overviews of relevant information collected from deployed GFI LanGuard instances at remote locations. To display the home page click **Home** in the top navigation.



Screenshot 27: The GFI LanGuard Central Management Server Home page

Toggle between the following views:

OPTION	DESCRIPTION
Sites Overview	A map displays GFI LanGuard instances that have been connected to the GFI LanGuard Central Management Server. High, Medium and Low markers define the vulnerability status of the sites at a glance, while an additional filter can be toggled to display the following: Vulnerability Status     Auditing Status     Patch Management Status     License Usage

OPTION	DESCRIPTION
Top Sites	The Top Sites view offers an in-depth look at the status of top sites. The interactive info-graphic offers the following 4 nodes: <b>Vulnerability Status</b> - View the number of vulnerabilities found on a site, grouped by severity. This area enables you to determine a site's vulnerability rating with high, medium and low percentages. You can also filter data by:
	<ul> <li>number of high vulnerability nodes</li> <li>percentage of high vulnerability nodes</li> <li>number of nodes</li> </ul>
	» Patch Management Status - View sites that are missing updates. Filter by:
	<ul> <li>number of nodes having missing updates</li> <li>percentage of nodes having missing updates</li> <li>number of nodes</li> </ul>
	» Auditing Status - identify how many audits have been performed in top sites grouped by time. Filter data by the following:
	<ul> <li>number of nodes not scanned last week</li> <li>percentage of nodes not scanned last week</li> <li>number of nodes not scanned last 24 hours</li> <li>percentage of nodes not scanned last 24 hours</li> <li>number of nodes</li> </ul>
	» License Usage - Explore top sites by their license status. Available filters are:
	<ul> <li>license usage</li> <li>license limit</li> <li>number of nodes</li> <li>expiry date</li> </ul>
NOTE	
NOIL	

The sites displayed by the GFI LanGuard Central Management Server represent GFI LanGuard instances that have been set up within each GFI LanGuard deployment. The GFI LanGuard Central Management Server is unable to detect any sites automatically. To view or edit details of connected sites refer to: Managing Sites.

The bottom part of the home page contains three widgets with additional information, listed in the following table:

Option	Description
Notifications	A list of events describing actions carried out or problems that have been identified by GFI LanGuard Central Management Server, for example when a service is not running.
Security Sensors	Displaying information related to security issues such as missing updates or malware protection issues. Click any item in the list to drill down further details.
Missing Updates / Operating Sys- tems / Software	Toggle between <b>Missing Updates</b> , <b>Operating Systems</b> and <b>Software</b> view to obtain quick information about what operating systems are running within your network or which important patches need to be deployed. Click Show all to be redirected to the dashboards.

## 3.4.2 Central Management Server Dashboards

The dashboards in GFI LanGuard Central Management Server Console provide information related to issues, missing patches or updates, vulnerabilities and other important information that provide insight into the security status of your entire network. Click **Dashboard** in the top navigation to access the overview page.

<b>GFI Lan</b> Guard			🔒 Home	Dashboard     La Reports	2 O L WIN-OOU9HBG95G2\Administrator
Q Search V ALL DEVICES & T	Computers	Aufnerabilities	Hardware System		
Entire Network     Entire Network     WORKGROUP     Other Computers     Mobile Devices	Entire Network - 1 Computer	WIN-OOU9HBG95G2	Software Hodates	Service Parks and Lindate Rollings	Vulgerabilities
	Low	MAC Address: 00-15-SD-03-EB-08 Manufacturer: Microsoft Corporation Model: Virual Machine Operating System: Windows Serve 2008 82:x64 OS Install Date: G-03/2015 6:20:27 PM	Missing software updates detected Malware Protection Issues Malware protection is missing or is out of date on Audit Status All computers were successfully scanned recently	Missing service packs or update rollups detected Firewall issues No firewall related issues detected in your network Credentials Setup Logion was successful on all computers	Unauthorized Applications Ro unauthorized Applications Ro unauthorized explorations detected Agent Health Issues Ro agent health walls was performent
	Top 5 issues to address	High	Vulnerability Tr	end Over Time	
	Systems (R82001983) Microsoft, HST Framework 4.5.2 for Windows Server 2008 R2 x84-based Systems (R82001983) Microsoft, HST Framework 4.5.2 for Windows Server 2008 R2 x64-based	Medum Low N/A 8/12/2015 8/	13/2015 8/19/2015	8/19/2015	8/19/2015 8/19/2015
	Agent Status		Scan A	ctivity	
	() Agent Not Installed	S 2.5 0 8/12/2015 Scan Activity Remediation Activity	8/13/2015 8/1	4/2015 8/18/	2015 8/19/2015

Screenshot 28: The overview dashboard

The **Overview** page is a dashboard that provides instant access to important information obtained from various GFI LanGuard installations. Information such as the vulnerability level of computers, domains or entire networks, missing updates alerts, vulnerability trends, top issues that need to be addressed and other data is displayed in one location for ease of access. Several additional dashboards that focus on specific features can be accessed by clicking the appropriate tabs in the upper part of the Console. These dashboards are described in the following table:

OPTION	DESCRIPTION
Computers	Select this dashboard to view information related to computers audited by GFI LanGuard. The Computers dash- board provides the discovered machine names, IP address, Domain name, installed Operating System and other relevant data.
History	The History view shows the changes done to target computers between audits. The report includes changes related to vulnerability level, user accounts, groups, ports, shares and registry entries. Audit results can be filtered by date, grouped by computer, information category or date and exported in several formats.
Vulnerabilities	A list of missing updates and types of vulnerabilities affecting your network. Select items from the list to display additional details.
Patches	Displays a list of missing or installed patches and service packs found during a network audit. When a patch or service pack is selected from the list, the <b>Details</b> section provides more information on the selected item.
Ports	Displays details on open TCP or UDP ports found during a network audit. When a port is selected from the <b>Port</b> List, the <b>Details</b> section provides more information on the selected port.
Software	A list of installed applications found during a network audit. When an application is selected from the <b>Application</b> List, the <b>Details</b> section provides more information on the selected application.
Hardware	Displays more information on the hardware found during a network audit. Select hardware from the list to display more details.
System Information	The <b>System Information</b> tab displays information associated with the operating system of a scan targets, such as users and groups, ongoing processes and services currently running.

## NOTE

When a computer or domain is selected, the results related to the selected computer/domain are automatically updated in the dashboard.

## 3.4.3 Central Management Server Computer Tree

GFI LanGuard Central Management Server Console includes filtering and grouping options that enable you to quickly find a site, computer or domain and immediately display results. These options can be managed from the **Computer Tree** within the Dashboard and Reports areas.

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.

Saved filters can also be used to generate targeted reports. For more information, refer to <u>Using GFI LanGuard Central</u> <u>Management Server Reports</u> (page 66).

The following are functions supported by the computer tree:

- » Simple filtering
- » Advanced filtering
- » Grouping
- » Saved Filters

#### Simple filtering

To filter for a specific computer or group:

1. From the left pane, click the **Filter** icon.



Screenshot 29: Using a simple filter

2. Next to each filter item, configure the filtering criteria.

3. Click Apply.

## Advanced filtering

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

- 1. From the left pane, click the **Filter** icon.
- 2. Next to **Advanced filters** click **Define**.

92.168.3.64	Advanced Filter Define an advanced filter by selecting the criteria and the logical operators.	
And Domain Determine And Compu Determine And Vulnera Determine high, med	In Equal to <domain name=""> ** e if network domain is equal to [Value]. uter name Equal to <computer name=""> ** e if computer name is equal to [Value]. rability level Equal to High ** e if vulnerability level is equal with [Value] Note: Possible values are: tium, low. OK Canc el</computer></domain>	

Screenshot 30: Using advanced filtering

- 3. From the **Advanced Filtering** dialog, click the **Add** icon.
- 4. Select filtering conditions and key in the condition value. You can add as many as required.
- 5. Click **OK**

## Grouping

To group machines by specific attributes:

1. From the left panel, click **Grouping** icon.



Screenshot 31: Group machines by specific attributes

2. Click on one of the following tabs and select a specific attribute:

Tabs	Attributes
Computers	<ul> <li>Site</li> <li>Domain and Organizational Unit</li> <li>Operating System</li> <li>Network Role</li> <li>Relays Distribution</li> <li>Attributes</li> </ul>
Mobile Devices	<ul> <li>» Site</li> <li>» User Account</li> <li>» Operating System</li> <li>» Device Model</li> <li>» Attributes</li> </ul>

#### NOTE

If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to <u>Using</u> <u>Attributes in Central Management Server</u> (page 66).

#### 3. Click Apply.

#### Saved Filters

Saved Filters enable you to customize views and save them to quickly find frequently accessed information. Saved filters are also used in report scheduling. For more information, refer to <u>Scheduling a report in GFI LanGuard Central</u> <u>Management Server</u> (page 71).

To use a saved filter, click the **Filters** icon and select a saved filter from the drop down list.

To save a new filter:

1. From the **Computers tree**, click the **Filters** icon.

2. Click inside the Filter field and key in a name for the filter.

3. Configure the filtering options. Use the available drop down lists next to each filter option or click **Advanced Filters** for more options.

4. Click the **Save** icon.

## Using Attributes in Central Management Server

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.

Attributes are configured in separate GFI LanGuard sites. When the remote sites synchronize with GFI LanGuard Central Management Server, they appear in the attributes list. For more information, refer to Using Attributes (page 130).

## 3.4.4 Using GFI LanGuard Central Management Server Reports

This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard Central Management Server. New reports can be added by customizing existing reports and saving them with a new name. For more information, refer to <u>Customizing GFI LanGuard Central Management Server Reports</u> (page 72).

There are two main types of reports:

» General reports - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity

» Legal compliance reports - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

For information on how to generate or schedule a report, refer to the following sections:

- » Generating reports
- » Scheduling reports

#### General reports

To view **General** reports:

1. Click **Reports** tab.

2. Click View, and from the list of reports, click General Reports, then select any of the following reports:

Report Title	Description
Network Security Overview	<ul> <li>An executive summary report showing:</li> <li>Network vulnerability level</li> <li>Most vulnerable computers</li> <li>Agent status</li> <li>Audit status</li> <li>Vulnerability trends over time</li> <li>Information on operating systems</li> <li>Servers and workstations.</li> </ul>

Report Title	Description
Computer Secur- ity Overview	An executive summary report showing: Computer vulnerability level Agent status Audit status Vulnerability trends over time Computer summary and details.
Vulnerability Status	Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by: <ul> <li>Computer name</li> <li>Vulnerability severity</li> <li>Timestamp</li> <li>Category.</li> </ul>
Patching Status	<ul> <li>Shows statistical information related to missing and installed updates detected on your scan targets. Updates can be grouped by name, severity, timestamp, vendor and category. Use this report to get:</li> <li>Missing vs. Installed updates comparison</li> <li>Charts and tables displaying missing updates distribution for each item from the first and second grouping criteria</li> <li>Charts and tables displaying installed updates distribution for each item from the first and second group-ing criteria</li> <li>Patching details for missing and installed patches.</li> </ul>
Full Audit	A technical report showing information retrieved during an audit. Amongst others, the report contains information on:  Vulnerabilities  Open ports Hardware and software.
Software Audit	<ul> <li>Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on:</li> <li>Antivirus</li> <li>Antispyware</li> <li>Applications inventory.</li> </ul>
Scan History	An overview of the network security audits performed over time. Amongst others, the report includes information on: Most scanned computers Least scanned computers Auditing status History listing.
Remediation His- tory	<ul> <li>Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on:</li> <li>Remediation actions per day</li> <li>Remediation distribution by category</li> <li>Remediation list grouped by computers.</li> </ul>
Network Security History	<ul> <li>Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to:</li> <li>The vulnerability level</li> <li>User accounts</li> <li>Groups</li> <li>Ports</li> <li>Shares</li> <li>Registry entries.</li> </ul>

Report Title	Description
Baseline Com- parison	Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on:
Mobile Devices Audit	<ul> <li>Shows information related to detected mobile devices found during an audit. Amongst others, the report includes information on:</li> <li>&gt; Vulnerability distribution by severity</li> <li>&gt; Vulnerability distribution by computer</li> <li>&gt; Vulnerability listing by computer.</li> </ul>
Sites Overview	Shows a high level overview of managed GFI LanGuard sites, displaying for each site
Sites Summary	List of GFI LanGuard sites. For each site the report shows:  Number of nodes  License usage Vulnerability level  Patching and auditing status User rights assignments.
USB Devices	Lists all USB devices found in an audit, grouped by computer.
Missing Microsoft <sup>®</sup> Secur- ity Updates	<ul> <li>Shows statistical information related to missing Microsoft<sup>®</sup> security updates, detected on your scan targets.</li> <li>Select items to include in your report:</li> <li>General missing updates distribution chart</li> <li>Distribution table</li> <li>Vulnerability list.</li> </ul>
Missing Non- Microsoft <sup>®</sup> Secur- ity Updates	<ul> <li>Shows statistical information related to missing non-Microsoft<sup>*</sup> security updates, detected on your scan targets.</li> <li>Select items to include in your report:</li> <li>General missing updates distribution chart</li> <li>Distribution table</li> <li>Vulnerability list.</li> </ul>
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.
Computer Sum- mary	<ul> <li>A summary of scan target information, including:</li> <li>&gt; Operating system information</li> <li>&gt; Agent status</li> <li>&gt; Vulnerabilities severity.</li> </ul>
Hardware Audit	Illustrates information related to the hardware found during an audit.
Computer Details	<ul> <li>Provides a detailed list of computer properties, including:</li> <li>MAC Address</li> <li>Time to Live</li> <li>Network Role</li> <li>Domain</li> <li>Lan Manager</li> <li>Is relay agent</li> <li>Uses relay agent</li> <li>Attributes</li> <li>Operating system</li> <li>IP address.</li> </ul>
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.

Report Title	Description	
Open Ports	Lists all the open ports found during an audit. The results are grouped by port type (TCP and UDP).	
Services	Lists all services found during an audit. Results are grouped by computer name.	
Groups and Users	Lists all Groups and Users found during an audit. The result is grouped by computer name.	
Mobile Device Policies	Lists all mobile device policies found during an audit. The result is grouped by computer name.	
Unauthorized Applications	Lists all unauthorized applications installed scan targets, including: >> Top Computers with Unauthorized Applications >> Top Unauthorized Applications >> Applications Inventory >> Computers without Antivirus Installed	
Antivirus Applic- ations	Shows information related to the antivirus installed on scan targets.	
New Devices	Lists all new devices found during last week audits.	

## Legal Compliance reports

## To view **Legal Compliance** reports:

### 1. Click **Reports** tab.

2. Click **View** and from the list of reports, expand any of the following compliance reports suites:

Report Suite Title	Description
PCI DSS Compliance Reports	<ul> <li>The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. GFI LanGuard Central Management Server provides you with a number of reports that cater for PCI DSS compliance, including:</li> <li>PCI DSS Requirement 1.4 - Installed Firewall Applications</li> <li>PCI DSS Requirement 2.2.3 - Disk Encryption Applications</li> <li>PCI DSS Requirement 5.2 - Antivirus Applications</li> <li>PCI DSS Requirement 6.1 - Remediation History by Date</li> <li>PCI DSS Requirement 1.2.12 - Open Trojan Ports by Host.</li> </ul>
HIPAA Compliance Reports	<ul> <li>The Health Insurance Portability and Accountability Act (HIPAA) is a requirement of all healthcare providers that regulates the exchange of private patient data. This helps prevent unlawful disclosure or release of medical information. To help you follow HIPAA regulations, GFI LanGuard Central Management Server provides you with a suite of HIPAA compliance reports, including:</li> <li>» HIPAA 164.308(a)(1)(ii)(A) - Missing Security Updates by Host</li> <li>» HIPAA 164.308(a)(1)(ii)(A) - Vulnerability Distribution by Host</li> <li>» HIPAA 164.308(a)(4)(ii)(A) - Open Ports</li> <li>» HIPAA 164.308(a)(5)(ii)(D) - Audit Policy</li> <li>» HIPAA 164.308(a)(8) - Baseline Changes Comparison.</li> </ul>
SOX Compliance Reports	The Sarbanes-Oxley Act (SOX) is regulation created in response to high-profile financial scandals as well as to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. GFI LanGuard Central Management Server provides a list of SOX compliance reports, including: SOX 302.a - Network Vulnerability Summary SOX 302.a - Remediation History by Host SOX 302.a - Security Scans History SOX 404 - Vulnerability Listing by Category SOX 404 - Missing Security Updates by Host.

Report Suite Title	Description
GLBA Compliance Reports	<ul> <li>The Gramm–Leach–Bliley Act (GLBA) is an act that allows consolidation between Banks and Insurance companies. Part of the act focuses on IT network compliance for such companies. GFI LanGuard Central Management Server offers a list of GLBA Compliance reports, including:</li> <li>GLBA 501.b - Baseline Changes Comparison</li> <li>GLBA 501.b - Network Patching Status</li> <li>GLBA 501.b - Open Trojan Ports by Host</li> <li>GLBA 501.b - Vulnerable Hosts Based on Open Ports</li> <li>GLBA 501.b - Vulnerable Hosts by Vulnerability Level.</li> </ul>
PSN CoCo Com- pliance Reports	<ul> <li>The Public Service Network - Code of Connection (PSN CoCo) is simply a list of conditions that should be met before connecting an accredited network to another accredited network. GFI LanGuard Central Management Server helps you monitor the status of such connections through the list of PSN CoCo Compliance reports, which include:</li> <li>PSNCoCo RIS. 1 - Baseline Changes Comparison</li> <li>PSNCoCo MAL. 1 - Disk Encryption Applications</li> <li>PSNCoCo MAL. 1 - Installed Firewall Applications</li> <li>PSNCoCo PAT. 1 - Installed Security Updates by Host</li> <li>PSNCoCo PAT. 1 - Installed Security Updates by Severity.</li> </ul>
CIPA	The Children's Internet Protection Act (CIPA) addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. GFI LanGuard Central Management Server provides a list of CIA Compliance reports including: » Req. 47 USC § 254(l)(1)(A)(iv) - Network Vulnerability Summary » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Distribution by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Category » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Severity » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerability Listing by Severity » Req. 47 USC § 254(l)(1)(A)(iv) - Network Patching Status » Req. 47 USC § 254(l)(1)(A)(iv) - Network Patching Status » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level » Req. 47 USC § 254(l)(1)(A)(iv) - Vulnerable Hosts Based on Open Ports » Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Remediation History by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(l)(1)(A)(iv) - Baseline Changes Comparison
FERPA Compliance Reports	<ul> <li>The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. GFI LanGuard Central Management Server provides a list of FERPA Compliance reports, including:</li> <li>FERPA 20 USC 1232g (b) - Network Patching Status</li> <li>FERPA 20 USC 1232g (b) - Network Security Log by Host</li> <li>FERPA 20 USC 1232g (b) - Remediation History by Date</li> <li>FERPA 20 USC 1232g (b) - Vulnerability Distribution by Host</li> <li>FERPA 20 USC 1232g (b) - Vulnerability Based on Open Ports.</li> </ul>
ISO/IEC 27001 & 27002 Compliance Reports	The Information technology – Security techniques – Information security management systems (ISO/IEC) standard formally specifies a management system that is intended to bring information security under explicit management control. GFI LanGuard Central Management Server offers an extensive list of ISO/IEC Compliance reports, including: > ISO/IEC 27001 A. 10.4 - Antivirus Applications > ISO/IEC 27001 A. 10.7.2 - Disk Encryption Applications > ISO/IEC 27001 A. 10.6.2 - Open Shares > ISO/IEC 27001 A. 10.6.2 - Services > ISO/IEC 27001 A. 10.6.2 - System Information.

Report Suite Title	Description
FISMA Compliance Reports	The Federal Information Security Management Act (FISMA) assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. GFI LanGuard Central Management Server helps you be compliant to FISMA standards through the provided reports, which include: FISMA NIST SP 800-53 AC-2 - Groups and Users FISMA NIST SP 800-53 PM-5 - Computer Details FISMA NIST SP 800-53 PM-5 - Computer Summary FISMA NIST SP 800-53 SI-5 - Missing Security Updates by Host FISMA NIST SP 800-53 SI-7 - Antivirus Applications.
CAG Compliance Reports	The Consensus Audit Guidelines (CAG) is a publication of best practice guidelines for computer security. The project was initiated as a response to extreme data losses experienced by organizations in the US defense industrial base. GFI LanGuard Central Management Server offers a list of CAG Compliance reports, including:
NERC CIP Compliance Reports	The North American Electric Reliability Corporation (NERC) develops standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. GFI LanGuard Central Management Server provides a list of NERC CIP Compliance reports, including: NERC CIP-005 R2 - Installed Firewall Applications NERC CIP-005 R2 - Open Ports NERC CIP-007 R2 - Open Shares NERC CIP-007 R2 - Services NERC CIP-007 R2 - System Information.

## Generating a report in GFI LanGuard Central Management Server

To use one of the reports:

- 1. From the top navigation, click **Reports**.
- 2. Select a report category from the View menu.
- 3. Hover over one of the report names and click **Generate** to run the report.

## Scheduling a report in GFI LanGuard Central Management Server

Reports can be run on a schedule. To schedule a report:

- 1. From the top navigation, click **Reports**.
- 2. Use the  $\ensuremath{\text{Mew}}$  filter on the left to select the category of reports you need.
- 3. Hover over a report and click **Schedule**.
- 4. In the **General** tab, define the following:

OPTION	DESCRIPTION
Enable Schedule	Click to enable a schedule for the selected report.
One time only on	Select this option and specify date and time if you want the report to run only once.

OPTION	DESCRIPTION
Recurrence pattern	Select this option if you want the report to be generated a number of times. Specify
	Daily, Weekly, Monthly intervals and the time of day at which to generate the report.

For each of the selected options, define additional recurrence details.

#### 5. In the **Customize** tab, define the following:

OPTION	DESCRIPTION
Choose a filter that applies to the target	Filters enable you to generate more targeted reports. For example, you can gen- erate reports for high vulnerability issues only. Select one of the saved filters from the drop down list that apply to the currently selected report. If you have not saved any filters, this option will be grayed out. For information on how to create new filters refer to: Using the Computer Tree.
Export to file	Select this option to export the generated report. This can be saved to file or sent by email as an attachment. Use the <b>Report Format</b> drop down field to specify the format of the exported report. Available formats are *.pdf, *.rtf, *.xls, *.xlsx, *.html, *.mht and *.png
Send by email	Select this option if you want the generated report to be automatically sent as an attachment by email. GFI LanGuard Central Management Server uses configured email settings when sending reports. To view currently configured settings click <b>Email Setup</b> . For more information, refer to <u>Email settings in Central Management</u> <u>Server</u> (page 57).
Override general alerting options and send email to:	Select this option if you want GFI LanGuard Central Management Server to ignore currently configured email settings and send the generated report to a specific email addresses. Enter the email address in the available field. Separate multiple email addresses with a semi-colon.

6. Click Save.

## Customizing GFI LanGuard Central Management Server Reports

Existing reports can be modified and saved as new reports. For a full list of default reports, refer to: Available reports.

To customize a report:

- 1. From the top navigation, click **Reports**.
- 2. Hover over one of the report names and click **Customize**.
- 3. Modify the following options:

OPTION	DESCRIPTION
Report name	Every report name must be unique. Click on the report name to change.
Report Items	Each report is preconfigured with a list of specific items to include in the report. For example, the Software Audit report includes Antivirus Status, Applications Inventory and Computers without Antivirus amongst others. Select the items to be included in the report from the available list. The cri- teria change according to the selected report.
Filters	Filtering helps create more targeted reports. Filters are different for each report. Click the <b>Filters</b> tab and configure the criteria to use.
Grouping & Sorting	Configure the items and report criteria by which the report will be grouped and sorted.

4. Click **Generate** to run the report or **Save as Custom** to store the customized report as a new report.
# 4 Using GFI LanGuard

GFI LanGuard helps you strengthen your network's security and integrity with positive patch management, vulnerability management and legal compliance results, while ensuring that your network is protected using the most up-to-date vulnerability detection methods and techniques.

4.1 Managing Agents	73
4.2 Scanning Your Network	
4.3 Dashboard	
4.4 Interpreting Results	
4.5 Remediate Vulnerabilities	
4.6 Activity Monitoring	
4.7 Reporting	
4.8 Data collected from a network audit	
4.9 Common Vulnerabilities and Exposures (CVE)	

# 4.1 Managing Agents

GFI LanGuard can be configured to deploy agents automatically on newly discovered machines or manually, on selected computers. Agents enable faster audits and drastically reduce network bandwidth utilization. When using Agents, audits are performed using the scan target's resource power. Once an audit is finished, the results are transferred to GFI LanGuard in an XML file.

# NOTE

GFI LanGuard Agents can be deployed only on machines running Microsoft Windows operating systems that meet a minimum set of system requirements. For more information, refer to <u>GFI LanGuard system requirements</u> (page 20).

Topics in this section:

4.1.1 Deploying Agents	73
4.1.2 Deploy Agents manually	75
4.1.3 Agent properties	77
4.1.4 Agents settings	
4.1.5 Configuring Relay Agents	
4.1.6 Managing Agent groups	
4.1.7 Updating Agents	92

# 4.1.1 Deploying Agents

To deploy GFI LanGuard Agents on network computers:

1. Launch GFI LanGuard.

2. From the Home menu, select Manage Agents. Alternatively, click Configuration tab > Agents Management.



Screenshot 32: Manage agents

3. From **Common Tasks**, click **Deploy Agents** to select the target scan computers and click **Next**. Select one of the options described below:

Option	Description
Local Domain	Deploy agents on all reachable computers within the same workgroup / domain where GFI LanGuard is installed. No fur- ther configuration is required in <b>Define target</b> step.
Custom	Deploy agents on specific computers or group of computers. Add new rules to search or specify target scan computers.

4. If **Custom** option is selected, click **Add new rule** and select the **Rule type** described below:

Rule type	Description
Computer name is	Manually enter a computer name or import the names from a saved text (.txt) file. Click <b>Select</b> and manually select computers from the list, or click <b>Import</b> and specify the text file location.
Domain name is	Select domains from the list of reachable domains.
Organization unit is	<ul> <li>Select computers from one or more reachable organization units. Use the following options:</li> <li><b>Retrieve</b> – Specify the user name and password to retrieve the list</li> <li><b>Refresh</b> – Refresh the list of domains and Organization Units</li> <li><b>Add</b> – Manually add an Organization Unit.</li> </ul>

Repeat step 4 for each rule. Once completed, click **OK** 

### 5. From **Deploy Agents** dialog, click **Next**.

- 6. (Optional) Select Authenticate using checkbox to specify alternate credentials.
- 7. (Optional) Click **Advanced Settings**, and configure the settings in the following tabs:

Tab	Description
General	Configure the schedule for when GFI LanGuard automatically scans for new machines in the network perimeter where agents are enabled.
Audit Sched- ule	Configure how often the agent audits the host computer (where the agent is installed). Select the recurrence pat- tern, the time the audit will start and the scan profile to use.
Auto remediation	Configure GFI LanGuard to automatically download and install missing patches and service packs. Uninstall unauthorized applications on the scanned computers. For more information, refer to <u>Automatic Remediation</u> (page 162).

8. Click **Next** and **Finish** to complete agent deployment.

# 4.1.2 Deploy Agents manually

To deploy agents manually:

1. Launch GFI LanGuard and select **Dashboard**.

# 2. From Common Tasks, select Add more computers.

Add more computers	
Step 1 of 4: Define import type Select the source of computers.	s.
Import type	Description
Add computers from the network	Add computers from network
Add computers from a text file	The list may include domains, workgroups,
Add computers manually	organizational units and computers.
	< Back Next > Cancel

Screenshot 33: Add more computers - Select import type

3. From the Add more computers wizard, select one of the following options:

Option	Description
Add computers from the network	Select domains, organizational units and computers from the list. Use the <b>Add domain</b> to add a new domain to the list of computers.
Add computers from a text file	Import computer list from text file. Click <b>Browse</b> and locate the text file containing the list of computers.
Add computers manually	Manually create a list of computers. Use the <b>Add</b> and <b>Remove</b> buttons to add and remove computers from the list. Use the <b>Import</b> and <b>Export</b> buttons to import and export the list from\to a text file.

Click Next.

Assign custom attributes	o the selected computers	2
<ul> <li>Skip attributes assign</li> <li>Assign custom attributes</li> </ul>	ent tes:	
Attribute	Value	Add
Location	FirstFloor	
Department	R&D	Euit.
Note: Custom attribute share the same	es enable advanced grouping and filtering of computer attributes, allowing for easy identification by custom gr	s. Computers added at this stage will ouping and filtering.

Screenshot 34: Add more computers - Assign attributes to new computers

4. Custom attributes can be assigned to specific computers to ease grouping and filtering. From the **Assign attributes** wizard, configure the following:

Option	Description
Skip attributes assignment	No attributes are added to the computers list.
Assign custom attributes	Assign attributes to the list of computers. Click the <b>Add</b> button and specify the new attribute name and value.
	<b>NOTE</b> When importing a list of computers from a text file, GFI LanGuard automatically assigns the file name as an attribute (File) to the imported list.

#### 5. Click **Finish**.

# NOTE

If the selected computers have different login credentials from the GFI LanGuard machine, GFI LanGuard launches a dialog that enables you to specify valid credentials.

6. Once the computers are added to the list, click **Close**.

7. From the computer tree, right-click the newly added computers and select the computer where to deploy the agent and from the **Agent Status** click **Deploy Agent**.

8. Configure the Agent properties. For more information, refer to Agent properties (page 77).

# 4.1.3 Agent properties

To modify agent properties:

- 1. Click **Configuration** tab > Agents Management.
- 2. From the right pane, right-click an agent and select Properties.

#### NOTE

The **Properties** dialog can also be accessed from the computer tree within the **Dashboard**. Right-click a computer or a group and select **Properties**.

SERV08-06 Properties	
General Agent Status	Attributes Relays
View com	puter details and configure credentials
Computer details	
Name:	SERV08-06
Туре:	N/A
Credentials Status: Creden	tials defined. using: Alternative credentials
Usemame:	SERV08-06\admin
Password:	••••••
	OK Cancel

Screenshot 35: Agent Properties - General tab

3.(Optional) From **General** tab, specify the name, type and authentication method for the selected agent.

SERV08-06 Properties
General Agent Status Attributes Relays
Agent deployment status
Agent status: Installed
Deploy agent Uninstall agent
Agent activity settings
Audit host computers every day at 12:00.
Change scan schedule
Scanning profile:
Full Scan 👻
Auto remediation settings
Auto remediation is: OFF
Change settings
OK Cancel

Screenshot 36: Agent Properties - Agent Status tab

4. From Agent Status tab, enable/disable agent deployment by clicking Deploy agent or Disallow agent installation.

5. Click **Change scan schedule...** to configure the selected agent's scan schedule.

6. From **Scanning profile** drop-down menu, select the active scan profile.

7. From **Auto remediation settings**, click **Change settings...** to enable/disable agent auto-remediation. For more information, refer to <u>Configuring auto-remediation options</u> (page 173).

V08-06 Properties		
eneral Agent Status	Attributes Relays	
Custom attri and filtering	butes can be applied to cor based on these attributes.	nputers allowing custom grouping
Attribute	Value	Inherited
Location	FirstFloor	No
Department	R&D	No
	Add	Edit Remove
Note: Attributes o operating s container,	Add can be assigned to compute system groups, or any other an attribute is automatically	Edit Remove ers or containers (domains, container). When assigned to a inherited by all members.

Screenshot 37: Agent Properties - Attributes tab

8. Click **Attributes** tab to manage the attributes assigned to the selected computer. Use the **Add**, **Edit** and **Remove** buttons to manage attributes.

SERV08-06 Properties	×
General Agent Status Attributes Relays	
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.	
Set as relay agent	_
Status: This computer is not a relay agent.	
Set as relay Remove relay	
Advanced settings.	
Assign a relay agent     Onnect directly to GFI LanGuard server.     Use relay agent: There are no applicable relays to be used.     There are no applicable relays to be used.	
OK Cano	el

Screenshot 38: Agent Properties - Relays tab

9. Click **Relays** tab to configure agent relays. Relays enable computers other than the one hosting GFI LanGuard to act as GFI LanGuard server. This helps you load-balance traffic directed to that machine and optimize network scanning performance.

10. Configure the options described below:

Option	Description
Set as relay	Set the selected computer as a relay agent. The selected computer will send product updates and patches to other agents to reduce the load from the GFI LanGuard machine. Click <b>Set as relay</b> and follow the configuration wizard.
Remove relay	Remove the relay agent role from the selected computer. Click <b>Remove relay</b> and follow the configuration wiz- ard.
Connect directly to GFI LanGuard server	The selected computer will download product updates and patches from the GFI LanGuard server.
Use relay agent	The selected computer will use a relay agent to download product updates and patches. Select the relay agent to use from the drop down list.

11. (Optional) Click **Advanced Settings** and configure the following options:

Option	Description
Caching directory	All patches and updates are stored in this location before installation on the client computer.
Port where to serve	The port used by the relay agent to serve requests.
Address where to server	The address used by client computers to connect to the relay agent (By default the DNS host name is used).

12. Click **OK** twice.

# 4.1.4 Agents settings

To configure additional agents' settings:

- 1. From **Configuration** tab, select **Agents Management**.
- 2. Click Agents Settings.



Screenshot 39: Agent Settings - General tab

3. Configure the options described below:

Option	Description
Auto	Set the number of days after which GFI LanGuard Agents automatically uninstall themselves if the host computer is unre-
uninstall	sponsive for the set period of days.

Option	Description
Agents report using	Configure the port and IP address used by agents to communicate and report status to GFI LanGuard. When GFI LanGuard machine has multiple IP addresses and Default setting is selected, GFI LanGuard automatically selects the IP address to use.

Agents Settings			<b>—</b> ×
General Update	Timeframe Adv	anced	
Specify	he timeframe in v	which agents are allowed	d to download updates.
Timeframe			
O	0h 03h 06	h 09h 12h 15h	18h 21h 24h
Sunday			
Monday Tuesday			
Wednesday Thursday	<u> </u>		
Friday Saturday			
			OK Cancel

Screenshot 40: Agent Settings - Update Timeframe tab

- 4. Specify the timeframe in which agents are allowed to download updates.
- 5. Click **OK** to save and close dialog.

Agents Settings	×
General Update Timeframe Advanced	
Advanced options for the management of GFI LanGuard agents.	
Data transfer	5
When administrative shares are disabled on remote computers:	
Create temporary custom share	
OK Cancel	

Screenshot 41: Agent Settings - Advanced tab

6. (Optional) Click **Advanced** tab and select **Create temporary custom share**. When this option is enabled and administrative shares are disabled on agent machines, GFI LanGuard creates a temporary shared folder for transferring information.

7. Click **OK** to save and close dialog.

#### WARNING

Communication on TCP port **1072** must be enabled in Windows firewall for GFI LanGuard Agents to send data to GFI LanGuard.

# **4.1.5 Configuring Relay Agents**

In larger networks you may experience increased network bandwidth use due to the amount of data transferred from the GFI LanGuard server to managed computers. The data consists of definition updates delivered to Agent computers and of patches being deployed to target computers.

To help avoid performance issues and to apply load balancing techniques, GFI LanGuard enables you to configure Agents as a relay of the server. Agents that are configured as Relay Agents act as caching points. These download patches and definitions directly from GFI LanGuard server or from an upstream Relay Agent and forward them to client computers (which can be Agent-based and Agent-less computers). The main advantages of using Relay Agents are: » Reduced bandwidth consumption in local or geographically distributed networks. If a Relay Agent is configured on each site, a patch is only downloaded once and distributed to client computers

- » Reduced hardware load from the GFI LanGuard server component and distributed amongst relay agents
- » Using multiple Relay Agents increases the number of devices that can be protected simultaneously.

Follow the below recommendations to take full advantage of Relay Agents:

1. Keep the number of computers/agents directly connected to the GFI LanGuard server or to one Relay Agent below 100.

2. In geographically distributed networks, designate at least one Relay Agent for each remote site. This ensures that each file is only transmitted once from the GFI LanGuard server site to the remote site.

3. Fine-tune network use by configuring cascading Relay Agents

Refer to the following sections for information about:

- » Configuring an Agent as a Relay
- » Configuring Relay Agent advanced options
- » Connecting computers to a Relay Agent

Configuring an Agent as a Relay

To configure an Agent to act as a Relay Agent:

#### NOTE

The machine where GFI LanGuard is installed cannot be configured as a Relay Agent. The **Relays** tab from the Agent's **Properties** dialog is missing for the GFI LanGuard host.

1. Open GFI LanGuard.

#### 2. Click **Configuration** tab > **Agents Management**.

3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

#### NOTE

Alternatively, right-click on an computer/group from the computer tree and select Properties.

SERV08-06 Properties		×	
General Agent Status Att	iributes Relays		
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.			
Set as relay agent Status: This compu	ter is not a relav agent.		
Set as relay	Remove relay		
	Advanced settings.		
Assign a relay agent	o GFI LanGuard server.		
Use relay agent:	SERV08-04 👻		
	OK	zel	

Screenshot 42: Agent Properties dialog

4. From the **Relays** tab, click **Set as relay...** 

Set computer as relay		? 🔀
Step 1 of 3: Welcom Setup remote com	ne Iputer as a relay agent.	X
You are preparing	to setup "SERV08-06" as a relay agent.	
When usir     bandwidth     server and	ng agent relays in your network you can lighten the weight on your Lar n consumption by allowing specific computers to connect to a relay rath d taking advantage of the caching the relay is responsible for.	Guard server and the her than directly to the
A relay co - Should h - Is expect - Must be	mputer: have enough disk space to ensure proper caching. ted to handle increased load and have longer uptimes. allowed by the firewall to open port 1070.	
	< Back	Next > Cancel

Screenshot 43: Set computer as relay wizard

5. Carefully ready the warning about resource requirements for the computer running a Relay Agent. Click **Next**.

Set computer	as relay	? 💌
Step 2 of 3 Choose	: Cache location the caching location on the remote computer.	X
Choose	the location where the relay agent will do the caching:	
%Agen	tData%\RelayCache\	
Note:	A relay agent requires at least 5 GB of free space to work correctly.	
	Use %AgentData% as placeholder for agent data folder.	
Last kno	own disk drives information:	
C: 1	Total space 29.90 GB (Free 22.04 GB)	
	< Back Next	Cancel

Screenshot 44: Choose caching directory for the new Relay Agent

6. Choose the caching location for the Relay Agent. The caching directory is used by the relay to store audit and remediation information when auditing remote computers. By default, the **RelayCache** folder is created in C:\ProgramData\GFI\LanGuard 12\RelayCache.Click **Next**.

#### NOTE

Use the **%AgentData%** placeholder to quickly refer to the Agent's data folder.

Set computer as relay
Step 3 of 3: Finish Next steps.
After pressing Finish, computer "SERV08-06" will be setup as a relay agent as soon as the computer is detected on-line.
You can monitor this process in "Dashboard" > "Overview" > "Agent status".
Next steps: • After the relay agent setup is complete you can start configure other computers in your network to use this relay when performing remediation and auto-update operations.
< Back Finish Cancel

Screenshot 45: Settings summary step

## 7. Click **Finish**.

#### NOTE

After you click **Finish**, the selected Agent is configured as a Relay Agent. You can monitor this process from **Dashboard > Overview > Agent status**.

Configuring Relay Agent advanced options

To configure Relay Agent advanced options:

- 1. Open GFI LanGuard.
- 2. Click **Configuration** tab > **Agents Management**.

3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

# NOTE

Alternatively, right-click on an computer/group from the computer tree and select Properties.

SERV08-04 Properties	×
General Agent Status Attributes Relays	
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.	
Set as relay agent	-
Status: This computer is an active relay agent.	
Set as relay Remove relay	
Advanced settings	.
Assign a relay agent     Onnect directly to GFI LanGuard server.	
Use relay agent: There are no applicable relays to be used.	
OK Canc	el

Screenshot 46: Relay Agent properties - Advanced settings

4. Click **Relays** tab > **Advanced settings...** 

Relay Agent	Advanced Settings	×
General		
K	Change advanced settings for the relay agent, like remote caching directory, port and address.	
Caching d	irectory:	
%AgentDa	ata % \RelayCache \	
Address:	SERV08-04 Default	
TCP port:	1070	
	OK Cano	el

Screenshot 47: Relay Agent advances settings dialog

5. From the **Relay Agent Advanced Settings** dialog, configure the options described below:

Option	Description
Caching directory	Location where the relay agent caches information when auditing remote computers.
Address	Displays the computer name that is running the relay agent. Click <b>Default</b> to restore the field to its original value.
TCP port	Communication port used by the relay agent to communicate with GFI LanGuard server. Port 1072 is assigned by default and is automatically changed if GFI LanGuard detects that port 1072 is being used by another application.

# 6. Click **OK**

Connecting computers to a Relay

To connect a computer to a Relay:

1. Open GFI LanGuard.

#### 2. Click **Configuration** tab > Agents Management.

3. Right-click on the Agent you want to configure and select **Properties**. This opens the Agent's **Properties** dialog.

# NOTE

Alternatively, right-click on an computer/group from the computer tree and select Properties.

4. Click **Relays** tab.

5. From the **Assign a relay agent** area, select **Use relay agent** and choose the relay from the drop-down menu.

6. Click **OK** 

# 4.1.6 Managing Agent groups

The computer tree enables you to configure agent properties of groups of computers. To configure computer group properties:

1. From the computer tree, right-click a group of computers and click **Properties**.

2.(Optional) From **General** tab, specify name, type and authentication method for the selected group.

3. Select **Agent Status** tab, and configure the following options:

Option	Description
Enable automatic agents deployment	Automatically deploy agents on newly discovered computers.
Remove all agents	Remove all installed agents from this group.
Change scan schedule	Configure the schedule, when GFI LanGuard searches for new computers.
Scanning profile	Configure the audit schedule; when target computers are scanned.
Auto remediation set- tings	Configure the auto remediation actions to perform on all computers in this group. For more information, refer to <u>Configuring Agent auto-remediation</u> (page 183).

#### 4. Select **Network Discovery** and configure the following options:

Option	Description
Check automatically for new machines in this group	GFI LanGuard will search for new machines automatically.

Option	Description
Change schedule	Change the schedule when GFI LanGuard searches for new computers.
Run now	Run network discovery.
Scan OU recursively	Recursively, loop through all organization units and enroll computers.

5. Select **Attributes** tab to manage the attributes assigned to the computer selected. Use the **Add**, **Edit** and **Remove** buttons to manage attributes.

EMP Properties		X	
General Agent Status Attr	ributes Relays		
Custom attributes and filtering based	can be applied to compute d on these attributes.	rs allowing custom grouping	
Attribute	Value	Inherited	
	New attribute		×
	Add an attribute or de	ute for 'TEMP'. You can create a n fine a value for an existing one.	ew
Note: Attributes can b	Name: Location		•
operating syster container, an at	Value: Marketing	3	•
	C	KCancel	
		OK Cancel	

Screenshot 48: Agent Attributes

6. Click **Relays** tab to configure agent relays. Relays enable computers other than the one hosting GFI LanGuard to act as GFI LanGuard server. This helps you load-balance traffic directed to that machine and optimize network scanning performance.

WINXPWEBWORKS Properties	x
General Agent Status Attributes Relays	
Using agent relays in your network allows you to increase overall GFI LanGuard performance by distributing the load across the network.	
Set as relay agent	
Status: This computer is not a relay agent.	
Set as relay Remove relay	
Advanced settings	
Assign a relay agent     Onnect directly to GFI LanGuard server.	
Use relay agent: There are no applicable relays to be used.	
OK Cance	:

Screenshot 49: Agent Relays

7. Configure the options described below:

Option	Description
Connect directly to GFI LanGuard server	The selected computer will download product updates and patches from the GFI LanGuard server.
Use relay agent	The selected computer will use a relay agent to download product updates and patches. Select the relay agent to use from the drop down list.

#### Note

Some options are disabled because they are applicable only for single computers.

# 8. Click **OK**

# 4.1.7 Updating Agents

GFI LanGuard Agents manage updates for three primary components:

» **Product updates** - updates to the agent itself. Ensures that agents are running with the latest updates as released by GFI

» Threat definition updates - vulnerability definitions that enable agents to detect the latest threats as soon as they are detected and fixed by software vendors

» Security updates - missing third-party and system, patches and service packs detected on a target computer

GFI LanGuard merges **Product** and **Threat Definition** updates and are handled as a single entity; separately from **Security** updates.

# Threat definition updates

GFI LanGuard definition updates are important to run at regular intervals to ensure that any updates, as released by vendors, are detected and reported back by GFI to your solution. The **UpdateAgent** Method exposes an out parameter in which the results XML are built. It is synchronous and the update process will not return a value, until it ends.

GFI recommends triggering a GFI LanGuard Agent update session, immediately after the installation. This ensures that agents:

- » Acquire the latest patch definition files from GFI. This ensures that scans always detect the latest missing patches
- » Acquire the latest vulnerability definitions as soon as they become available from GFI
- » Acquires product updates to fix bugs which surfaced after GFI LanGuard SDK was released.

With the increasing number of sophisticated cyber threats occurrences, GFI recommends you to check for updates once every 24 hours on every end-point or designated concentrator.

A lesson learned by GFI is to trigger agents to check for updates at random time intervals. Configuring agents to check for and download updates simultaneously, causes undesired network bandwidth problems if a significant number of downloads occur at the same time. Randomizing the update times is enough to smoothen out the update operation, effectively making the process unnoticeable.

#### IMPORTANT

» GFI LanGuard Agents connect to **\*.software.gfi.com/lnsupdate/** to retrieve threat definition updates. Ensure that this URL is not blocked by your firewall and/or web gateway.

» GFI LanGuard definition updates do not include patches and service packs as release by Microsoft and other vendors over time. These patch updates are treated separately to all of the above.

# Security updates

Security updates refer to the missing patches and service packs detected on target computers by patch management scans. These updates fix bugs or performance issues of the operating system and third-party software installed on a computer. Patch updates are downloaded directly from the vendors servers. Microsoft updates are downloaded from Microsoft and third parties such as Adobe and Firefox are downloaded from third party servers respectively. GFI does not tamper or provide customized installations of patch and service pack updates. We distribute patches as provided and signed off by the vendor.

# Supported software vendors

The following table provides you with links to supported Microsoft and Third-Party application patches:

Supported Patches	Link
Supported Microsoft applications	https://www.gfi.com/lannetscan/msappfullreport.htm
Supported Microsoft applications (Detailed)	https://www.gfi.com/lannetscan/msfullreport.htm

Supported Patches	Link
Supported MAC OS X applications	https://www.gfi.com/lannetscan/macfullreport.htm
Supported Third-Part applications (Detailed)	https://www.gfi.com/lannetscan/3pfullreport.htm
Supported security applications	https://www.gfi.com/lannetscan/securityappfullreport.htm
Supported OVAL and CVE checks	https://www.gfi.com/lannetscan/ovalfullreport.htm

#### IMPORTANT

Ensure that end point firewall settings, web-gateways and caching proxy server allow traffic from the below URLs:

- » gfi-downloader-137146314.us-east-1.elb.amazonaws.com
- » \*software.gfi.com/lnsupdate/
- » \*.download.microsoft.com
- » \*.windowsupdate.com
- » \*.update.microsoft.com

# 4.2 Scanning Your Network

This topic provides you with information about the different scanning profiles that ship with GFI LanGuard, as well as how to trigger immediate or scheduled manual scans. Select the most suitable scanning profile and scanning mode (such as using Agent-less versus Agent-based scans), depending on the availability and location of your scan targets.

Topics in this section:

4.2.1 About Scanning Profiles	94
4.2.2 Available Scanning Profiles	95
4.2.3 Manual scans	96
4.2.4 Enabling security audit policies	
4.2.5 Scheduled scans	
4.2.6 Agent scheduled scans	
4.2.7 Starting an Agent scan manually	
4.2.8 Discovering Mobile Devices	

# 4.2.1 About Scanning Profiles

GFI LanGuard enables you to scan your IT infrastructure for particular vulnerabilities using pre–configured sets of checks known as scanning profiles. Scanning profiles enable you to scan your network targets and enumerate only specific information. For example, you may want to use a scanning profile that is set to be used when scanning the computers in your DMZ as opposed to your internal network.

In practice, scanning profiles enable you to focus your vulnerability scanning efforts on to a specific area of your IT infrastructure, such as identifying only missing security updates. The benefit is that you have less scan results data to analyze; tightening up the scope of your investigation and help you quickly locate the information that you require, more easily.

Through multiple scanning profiles, you can perform various network security audits without having to go through a reconfiguration process for every type of security scan required.

# 4.2.2 Available Scanning Profiles

GFI LanGuard ships with the default scanning profiles described in the sections below. To create your own custom scanning profiles, refer to Creating a new Scanning Profile. Use the information provided in the following sections to understand what each scanning profile detects on your scan targets:

- » Complete/Combination Scans profiles
- » Vulnerability Assessment profiles
- » Network and Software Audit profiles

# Complete/Combination Scans

Complete/Co	mbination Scans profiles
Full Vul- nerability Assessment	Use this scanning profile to enumerate particular network vulnerabilities such as open TCP/UDP ports commonly exploited by Trojans as well as missing patches and service packs. The list of vulnerabilities enumerated by this pro- file can be customized through the Vulnerabilities tab. Installed USB devices and applications are not enumerated by this profile. This profile. This profile will scan for all vulnerabilities. This includes vulnerabilities which have an associated Microsoft <sup>®</sup> patch to them and which are considered missing patches.
Full Scan (Active)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN environments.
Full Scan (Slow Net- works)	Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB devices connected and more The vul- nerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with WAN environments.

#### Vulnerability Assessment

Vulnerability Asse	essment profiles
Top SANS 20 Vulnerabilities	Use this scanning profile to enumerate all vulnerabilities reported in the SANS top 20 list.
High Security Vulnerabilities	Use this scanning profile to enumerate open TCP/UDP ports and high security vulnerabilities. The list of TCP/UDP ports and high security vulnerabilities that will be enumerated by this profile can be customized through the TCP/UDP Ports tabs and the Vulnerabilities tab respectively.
Last Year's Vul- nerabilities	Use this scanning profile to enumerate network vulnerabilities that emerged during the last 12 months.
Only Web	Use this scanning profile to identify web-server specific vulnerabilities. This includes scanning and enumerating open TCP ports that are most commonly used by web-servers such as port 80. Only TCP ports commonly used by web-servers are scanned by this profile. Network auditing operations as well as enumeration of vulnerabilities and missing patches are not performed using this profile.
Missing Patches	Use this scanning profile to enumerate missing patches. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.
Critical Patches	Use this scanning profile to enumerate only missing patches that are tagged as critical. The list of critical patches that will be enumerated by this profile can be customized through the Patches tab.
Last Month's Patches	Use this scanning profile to enumerate only missing patches that were released last month. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.

Vulnerability Asse	ssment profiles
Only Service Packs	Use this scanning profile to enumerate missing service packs. The list of service packs that will be enumerated by this profile can be customized through the Patches tab.
Non- Microsoft <sup>®</sup> Patches	Use this scanning profile to enumerate missing Third-Party patches, such as Adobe products.
Security Patches	Use this scanning profile to enumerate missing $Microsoft^{\circ}$ and non- $Microsoft^{\circ}$ Security Patches on your scan targets.

# Network & Software Audit

Network & Sof	tware Audit profiles
Trojan Ports	Use this scanning profile to enumerate open TCP/UDP ports that are commonly exploited by known Trojans. The list of TCP/UDP ports to be scanned can be customized through the TCP Ports and UDP Ports tabs respectively. Only the TCP/UDP ports commonly exploited by known Trojans are scanned by this profile. Network auditing operations as well as enumeration of other open TCP/UDP ports and missing patches are not performed by this profile.
Port Scan- ner	Use this scanning profile to enumerate open TCP/UDP ports including those most commonly exploited by Trojans. The list of ports that will be enumerated by this profile can be customized through the TCP/UDP ports tab.
Software Audit	Use this scanning profile to enumerate all software applications installed on scan targets. This includes security soft- ware such as antivirus and antispyware.
Full TCP & UDP Scan	Use this scanning profile to audit your network and enumerate all open TCP and UDP ports.
Only SNMP	Use this scanning profile to perform network discovery and retrieve information regarding hardware devices (routers, switches, printers, etc.) that have SNMP enabled. This enables you to monitor network–attached devices for conditions that require administrative attention.
Ping Them All	Use this scanning profile to audit your network and enumerate all computers that are currently connected and run- ning.
Share Finder	Use this scanning profile to audit your network and enumerate all open shares either hidden or visible. No vul- nerability checks are performed by this profile.
Uptimes	Use this scanning profile to audit your network and identify how long each computer has been running since the last reboot.
Disks Space Usage	Use this scanning profile to audit your network and retrieve system information on available storage space.
System Information	Use this scanning profile to retrieve system information such as operating system details, wireless/virtual/physical net- work devices connected, USB devices connected, installed applications and more.
Hardware Audit	Use this scanning profile to audit your network and enumerate all hardware devices currently connected to your net- work computers.
Network Discovery	Use this scanning profile to enumerate any IP enabled device connected to your network.

# 4.2.3 Manual scans

Manual scan is the process of performing audits on target computers without using agents. To perform a manual scan on a specific computer:

1. Launch GFI LanGuard.

2. From the **Home** tab click **Launch a Scan**. Alternatively, click the **Scan** tab.

Launch a New Scan					
Sc <u>a</u> n Target:		P <u>r</u> ofile:			
localhost	¥	Full Scan	×		
<u>C</u> redentials:		<u>U</u> sername:	Password:	Key file:	
Currently logged on user	~				Scan
Scan Options					

Screenshot 50: Manual scan settings

3. From the **Scan Target** drop-down menu, select the target computer or group of computers to scan using the following options:

Option	Description
Localhost	Audit the local host where GFI LanGuard is installed.
Domain: primary domain	Audit the entire domain / workgroup of the computer / server where GFI LanGuard is installed.

#### NOTE

Optionally, from the computer tree, right-click a computer/computer group and select **Scan > Custom Scan**.

4. Click the browse button (...) to define custom rules for adding scan targets.

Custom target properties	×
Computers Group	
Define a custom group of computers.	
Group name:	
customgroup_2011_11_28_20_33_13	
Add any computer that satisfies one of the following rules:	
Add new rule Clear rule list	
Computer name is: W711 Remove	
Computer name is: <u>W712</u> Remove	
Computer name is: W713 Remove	
Computer name is: <u>W714</u> Remove	
Except for the computers that satisfy the following rules:	
Add new rule Clear rule list	
Computer name is: <u>192.168.11.11</u> Remove	
Computer name is: <u>192.168.11.21</u> Remove	
OK Cano	:el

Screenshot 51: Custom target properties

5. From the **Custom target properties** dialog, click **Add new rule** links to create a custom rule for computers you want to scan or exclude from scanning.

Add new rule	<b>—</b>
General	
Define rules for custom target.	
Rule type: Computer name is	•
Computer name	
Computer or range is	
SQLSERVER	Add
Serv08-09 A	Remove
W7-14	Select
	Import
	Export
· · · · · · · · · · · · · · · · · · ·	
C	K Cancel

Screenshot 52: Add new rule...

# 6. From the **Add new rule** dialog, select the **Rule type** described below to add computers:

Rule type	Description
Computer name is	Search and add computers by name. Key–in a valid computer name and click <b>Add</b> for each computer. Click <b>OK</b> to apply changes.
Computers file list is	Search and add computers from a text file. Click the browse button and locate the text file. Click <b>OK</b> to apply changes.
	<b>NOTE</b> When submitting a list of target computers from file, ensure that the file contains only one target computer name per line.
Domain name is	Search and add computers that are members of a domain. Select the domains from the list and click ${f OK}$
IP address is	Search and add computers by IP address. Select <b>This computer</b> to add the local host or <b>Scan another computer</b> to add a remote computer. Key–in the IP address if required and click <b>OK</b>

Rule type	Description
IP address range is	Search and add computers within an IP range. Select <b>Scan an IP address range</b> and key in the IP range or select CIDR subnet and key–in the range using CIDR notation.
	<b>NOTE</b> The Classless Inter–Domain Routing (CIDR) provides an alternative way of specifying an IP address range. The notation is as follows: <base address=""/> / <ip network="" prefix="">. Example: 192.168.0.0/16</ip>
Organization unit is	Search and add computers within an organizational unit. Click <b>Select</b> and from the list select the Organizational units. Click <b>OK</b>

7. Once the rules are added, click **OK** to close the **Add new rule dialog**. Click **OK** to close the **Custom target properties** dialog and return to the scan settings.

8. From the **Profile** drop–down menu, select the scan profile that you want GFI LanGuard to action during the scan. For more information, refer to Available Scanning Profiles (page 95).

9. From the **Credentials** drop-down menu, select the log-on method used by GFI LanGuard to log onto the scan targets. The table below describes the available options:

Option	Description
Currently logged on user	Use the current logged on user credentials when logging on scan targets.
Alternative credentials	Use custom credentials. Key–in the user name and password to use.
A null session	Log onto scan targets using a null session. The user will log onto the target machine as an anonymous user.
A private key file	Log onto UNIX/LINUX/MAC machines using SSH. Three elements are required for the login: >> Username >> SUDO password >> path to the file that stores the private key

# NOTE

The credentials provided need to have administrator privileges in order for GFI LanGuard to log–on to the target computers and carry out the network audit.

10. (Optional) Click **Scan Options** and configure the options described below:

Option	Description
Use per computer cre- dentials when available	Login to the target machines using the credentials specified in the Dashboard
Remember credentials	Use the configured credentials as default when performing an audit.
Wake up offline computers	GFI LanGuard attempts to power on offline computers using Wake-on-LAN. For more information, refer to <u>Configuring Wake-on-LAN on scan targets</u> (page 178).
Shut down computers after scan	Shut down when a scan is complete.

11. Click **Scan** to start auditing the selected targets.

# 4.2.4 Enabling security audit policies

An important part of any security plan is the ability to monitor and audit events on your network. These event logs are frequently referenced to identify security holes or breaches. Identifying attempts and preventing them from becoming successful breaches of your system security is critical. In Windows, you can use **Group Policies** to set up an audit policy that can track user activities or system events in specific logs.

To keep track of your system auditing policy, GFI LanGuard collects the security audit policy settings from target computers and includes them in the scan result. To access more information on the result click on **Security Audit Policy** sub–node.

Apart from gaining knowledge on the current audit policy settings, you can also use GFI LanGuard to access and modify the audit policy settings of your target computers. To achieve this:

1. After scanning a remote computer, from the **Scan Results Overview** panel, right–click on the respective target computer and select **Enable auditing on** > **This computer/Selected computers/All computers**.

teri on security additing policies			
Automatic turning on of security auditing poli	icies		
Specify which auditing policies are to be tun have been selected by default:	ned on. The recommend	led auditing p	oolicies
Auditing Policy	Success	Failure	
Audit account logon events		✓	*
Audit account management	$\checkmark$		
Audit directory service access	$\checkmark$		Ξ
Audit logon events	$\checkmark$		
Audit object access	✓		
Audit policy change	$\checkmark$	$\checkmark$	
Audit privilege use			-
Select Next to turn on the selected auditing	policies		
	ponoiou.		

Screenshot 53: The audit policy administration wizard

2. Select/unselect auditing policies accordingly, and click **Next** to deploy the audit policy configuration settings, on the target computer(s).

3. At this stage, a dialog will show whether the deployment of audit policy settings was successful or not. To proceed to the next stage click **Next**. Click **Back** to re-deploy settings on failed computers.

4. Click **Finish** to finalize configuration. Restart a scan to update results.

# 4.2.5 Scheduled scans

A scheduled scan is a network audit that is scheduled to run automatically on a specific date/time and at a specific frequency. Scheduled scans can be set to execute once or periodically. Scheduled scan status is monitored using the **Activity Monitor** tab **> Security Scans**.

GFI recommends scheduled scans:

- » When GFI LanGuard Agents are not deployed on the target computers
- » To automatically perform periodical/regular network vulnerability scans using same scanning profiles and parameters
- » To automatically trigger scans after office hours and generate alerts and auto-distribution of scan results via email
- » To automatically trigger auto-remediation options, (Example: Auto-download and deploy missing updates).

The following sections contain information to guide you in configuring and executing scheduled scans:

- » Creating a scheduled scan
- » Editing scheduled scan settings
- » Configuring scheduled scan properties

#### Creating a scheduled scan

- 1. Launch GFI LanGuard.
- 2. Click Configuration tab >Scheduled Scans.
- 3. From Common Tasks, select New scheduled scan.

New scheduled scan	<b>—</b> ———————————————————————————————————
Step 1 of 9: Define target type Select the type of targets to be scanned and describe this scan.	
Scan type	Description
Scan a single computer	Scan a single computer.
Scan a range of computers	Choose the local computer or specify the
Scan a list of computers	computer.
Scan computers in text file	
Scan domains or organizational units	
Scan job description:	
Itell me more	< Back Next > Cancel

#### Screenshot 54: New Scheduled Scan dialog

#### 4. Select one of the options described below and click Next.

Option	Description
Scan a single computer	Scan local host or one specific computer.

Option	Description
Scan a range of computers	Scan a number of computers defined through an IP range.
Scan a list of computers	Create manually a list of targets, import targets from a file or select targets from the network list.
Scan computers in text file	Scan targets enumerated in a specific text file.
Scan a domains or organizational units	Scan all targets connected to a specified domain/organizational unit.

5. Depending on the option selected in the previous step, specify the respective target computer(s) details and click **Next**.

New scheduled scan Step 3 of 9: Set the triggering time Set the triggering time for this scheduled scan job.	
Triggering time	Description
<ul> <li>One time only, on: 14/05/2012 v at: 15:08:06 v</li> <li>Recurrence pattern: daily at: 15:08:06 v</li> <li>Every 1 days</li> </ul>	Set the triggering time for this scheduled scan job
© Every weekday	
<u>Tell me more</u>	< Back Next > Cancel

Screenshot 55: Scheduled scan frequency

6. Specify date/time/frequency of the new scheduled scan and click **Next**.

New scheduled scan	
Select parameters to use for scan job.	10
Scan profile	Description
Scan job operation:	Scan your network for all supported
Complete/Combination scans	vulnerabilities including open TCP/UDP ports, missing patches and service packs, USB
Select scan profile:	devices and more. This scanning profile is also used to retrieve system information.
<ul> <li>Full Vulnerability Assessment</li> <li>Full Scan</li> <li>Full Scan (Slow Networks)</li> </ul>	NOTE: The vulnerability check timeouts in this profile are preconfigured to suit the network traffic and transmission delays usually associated with LAN environments.
NOTE: Scan profiles contain pre-set parameters used by the scanner for the job type selected.	
<u>Tell me more</u>	< Back Next > Cancel

Screenshot 56: Select scanning profile

7. From the **Scan job operation** drop-down menu, select the scanning profile to be used during the scan and click **Next**. For more information, refer to <u>Available Scanning Profiles</u> (page 95).

specify credentials to use to log i	on to remote targets.	
Credentials		Description
GFI LanGuard 12 Attendant S	ervice account	Perform the scan using the account under which GET LanG and 12 Attendant Service
<ul> <li>Alternative credentials</li> </ul>		runs.
User name:		
Password:		
SSH Private Key		
User name:		
SUDO Password:		
Key file:		
Use per computer credentials	when available	

Screenshot 57: Remote logon credentials

8. (Optional) Specify **Remote logon credentials** and click **Next**. Remote logon credentials can be either one of the following:

Option	Description
GFI LanGuard 12 Attendant Ser- vice account	Performs the scan using the credentials specified while installing GFI LanGuard.
Alternative credentials	Specify alternate credentials to connect to the scan computers.
	<b>NOTE</b> Ensure the supplied credentials have administrative privileges.

Option	Description
SSH Private Key	Key in a username with respective SUDO password and select the key file used to logon to UNIX/LINUX/MAC based systems.
Use per computer credentials when available	Use predefined credentials for the scan being configured.

w scheduled scan	
Step 6 of 9: Power saving options Choose different power saving options for this scan job	
Power saving options	Description
Wait for offline machines to connect to the network.	LanGuard can attempt to wake-up computer detected as off-line using the Wake-on-LAN
Wake up offline computers	algorithm.
Shut down computers after the job has finished	
If nonexistent systems are specified in the scan target the scan will not finish until the user manually stops it from Activity Monitor -> Security Scans.	
(i) Tell me more	< Back Next > Cancel

Screenshot 58: Scheduled scan reporting options

9. From the **Power saving** options, configure the following options:

Option	Description
Wait for offline machines to connect to network	If this option is selected, GFI LanGuard attempts to wait for offline machines to connect to the net- work.
Attempt to wake up off- line computers	GFI LanGuard attempts to power on offline machines using Wake-on-LAN. For more information, refer to <u>Configuring Wake-on-LAN on scan targets</u> (page 178).
Shut down computers after the job has finished	After a computer has been scanned or an auto-remediation job has been done, GFI LanGuard attempts to shut down the computer if the time is in the specified timeframe.
	<b>NOTE</b> If shut down options are defined in Auto-remediation options, the power saving options are ignored.

New scheduled scan	
Step 7 of 9: Specify auto-remediation options.         Please configure automatic remediation options.         Auto remediation         Ø Download and deploy missing updates         Ø Download and deploy missing service packs and update rollups         Ø Uninstall unauthorized applications         Configure auto-remediation options         View applications which this scan will uninstall         Image: The provide the provided proved proved provided provided provided provided provid	<b>Description</b> Automatically uninstall unauthorized applications. When this option is enabled, GFI LanGuard will automatically uninstall unauthorized applications detected, which are validated for auto-uninstall.
<ul> <li>auto-deployment.</li> <li>It is recommended to have System Restore on for the system drive on the target computers.</li> </ul>	
<u>Tell me more</u>	< Back Next > Cancel

Screenshot 59: Scheduled scan auto-remediation options

10. From the auto-remediation dialog, select the required options and click **Next**. The table below describes the list of available options:

Option	Description
Download and deploy missing updates	Automatically download and deploy missing patches on target machines.
Download and deploy missing service packs and update rollups	Automatically download and deploy missing service packs on target machines.
Uninstall unauthorized applications	If this option is selected all applications validated as unauthorized, will be uninstalled from the scanned computer (unauthorized applications are defined in Application Inventory). For more information, refer to <u>Configuring unauthorized applications auto-uninstall</u> (page 169).
Configure auto- remediation	Automatic-Remediation enables you to automatically download and deploy missing patches as well as uninstall unauthorized applications during scheduled operations, automatically. For more information, refer to <u>Automatic Remediation</u> (page 162).
View applications which this scan will uninstall	Click the link to launch the applications which will be uninstalled dialog. This will list all the applications that will be uninstalled when the scheduled scan is finished.

New scheduled scan	<b>—</b>
Step 8 of 9: Configure reporting options Choose which reporting options you would like to enable for this schedu	uled scan.
Reporting options	Description
✓ Email the scan report	Include in the report the full scan results.
Save the scan report to disk:	
C:\ProgramData\GFI\LanGuard 12\Reports	
Choose scan report content:	
Comparison data and auto remediation details	
✓ Other report: Scan Based - Full Audit ∨	
Configure alerting options	
Alerting options are not configured!	
Scans for large networks will generate a large report!	
<u>Tell me more</u>	< Back Next > Cancel

# 11. (Optional) Configure **Reporting options** as described below:

Option	Description
Email the scan report	Send a report by email at the end of each scheduled scan.
Save the scan report to disk	Save a report to disk at the end of each scheduled scan
Comparison data and auto remediation details	Include details of auto remediation actions performed and result comparison with previous security scans.
	<b>NOTE</b> Comparison is done between scans with same scan target(s) and scanning profile.
Full scan results data	Include full scan result details.
Configure alerting options	(Optional) Click Configure alerting options to specify sender/recipient details. For more information, refer to <u>Configuring Alerting Options</u> (page 235).
Override general alerting options, and send email to	(Optional) Send a report by email to specific email address. GFI LanGuard alerting options are overridden.

Screenshot 60: Scheduled scan reporting options

Please review the setting	gs for this scheduled scan job.
Scheduled scan sum	mary
Target	localhost
Triggering time	Occurs every day at 15:08:06.
Scanning profile	Full Scan
Credentials	GFI LanGuard 12 Attendant Service account
Auto-remediation	Automatically download and deploy missing patches and service packs, and uninstall unauthorized applications
Power Saving Options	Wait for offline computers and attempt to wake up offline computers.
Warning	Alerting options are not configured (email reports will not be sent).

Screenshot 61: Scheduled scan reporting options

12. Review the scan settings summary and click Finish.

NOTE
By default, all new scheduled scans are disabled. To enable, select <b>Configuration</b> tab <b>&gt;Scheduled Scans</b> and click
on the 🧠 button.
NOTE

Confirm that the new scheduled scans are successfully set by clicking on **Activity Monitor** tab > **Security Scans**.

## Editing scheduled scan settings

Scan schedules can be reviewed, edited, or deleted from **Configuration** tab > **Scheduled Scans** node. All scans are listed in the review page together with the relevant information. Use the scheduled scan toolbar to perform the actions described below:

lcon	Description
*5	Add new scan Display the New scheduled scan wizard and create a new scheduled scan.
5	<b>Delete</b> Use this button to delete the selected scheduled scan.

Icon	Description
1	<b>Properties</b> Review and edit the properties of the selected scan.
4	<b>Enable/Disable</b> Toggle the status of the selected scan between enabled and disabled. This enables you to activate/suspend a scanning schedule without deleting the scheduled scan.
Ø	<b>Scan now</b> Trigger the selected scheduled scan. This button overrides the scheduled scan date/time settings and executes an immediate scan.

Configuring scheduled scan properties

The scheduled scan properties page enables you to configure all the parameters of the scheduled scans.

To use the scheduled scan properties tab:

# 1. Go to **Configuration** tab > **Scheduled Scans**.

2. Select the scheduled scan and click the Scheduled Scan Properties.

192.168.11.11-192.168.11.21 Properties					
General Logon Credential	s Power Saving	Auto Reme	diation	Reporting	
Configure the sc	heduled scan.				_
<u>S</u> can target:	192.168.11.11-1	92.168.11.2	1		
Scanning profile:	Scanning profile:				•
Description:					
Scan schedule:					
One time only, on:	28/11/2011	🔲 🔻 a <u>t</u> :	20:37:1	L7 🔺	
Recurrence pattern:	daily	▼ a <u>t</u> :	20:37:0	)2 🌲	
Every 1 Every weekday	days				
		)K	Cance		ly



Tab	Description
General	Make changes to scan target setting, type of scanning profile and scan frequency.
Tab	Description
------------------------	--
Logon Cre- dentials	Specify logon credentials used when scanning the specified target.
Power Sav- ing	Configure power saving options. This dialog enables you to configure the scan to wait for offline machines to connect to the network, attempt to wake up offline machines and shut down machines when the scan is completed.
Auto- remediation	Configure the remediation options applicable to the scan being configured. This includes downloading and installing missing patches and service packs and unauthorized software un–installation.
Reporting	Configure reporting options used for the selected scheduled scan.

3. Click **OK** 

# 4.2.6 Agent scheduled scans

GFI LanGuard enables you to configure scheduled scans on computers running agents. Scheduling can be configured from the Agent properties dialog as follows:

1. Launch GFI LanGuard.

- 2. From the Home screen, select View Dashboard.
- 3. From the computer tree, right-click the computer/computer group you want to configure and select Properties.
- 4. Click Agent Status tab > Change scan schedule....

Agent activity recurrence	x
General	
Configure the agent activity recurrence for WIN7_03.	
Enable schedule Run task every day at 12:00.	
Recurrence pattem: daily at: 12:00:00	
<ul> <li>Every 1 days</li> <li>Every weekday</li> </ul>	
OK Cancel	

Screenshot 63: Agent Activity Recurrence

5. Select **Enable Schedule** and configure the recurrence pattern.

## 6. Click **OK**

## NOTE

Additional properties can be configured from the **Properties** dialog. For more information, refer to <u>Agent</u> properties (page 77).

# 4.2.7 Starting an Agent scan manually

To start an on demand scan on an agent computer:

- 1. Launch GFI LanGuard.
- 2. Click **View Dashboard** and select the computer(s) you want to start scanning.
- 3. From the **Agent Status** section, click **Scan Now**.

#### Note

Scan Now is only visible when the Agent Status is Agent Installed.

# 4.2.8 Discovering Mobile Devices

GFI LanGuard enables you to discover and manage mobile devices (such as phones or tablets) that connect to your mobile device management source.

This section contains information about:

- » Configuring a mobile device information source
- » Adding mobile device management sources
  - Microsoft Exchange Server
  - Microsoft Office 365
  - Google Apps for Business
  - Apple Profile Manager
- » Managing retention policies
- » Unmanaged devices

Configuring a mobile device information source

To manually configure mobile devices:

- 1. Click on **Configuration** tab > **Mobile Devices**.
- 2. From the right pane, select one of the options.

🥑 GFI LanGuard								
Dashboard	Scan	Remediate	Activity Monitor	Reports	Configuration	Utilities	• 🕑	Discuss this version
Configurations: 		Mobile Manage mo	Devices	nd other mobil	le devices.			
Mobile Devices Mobile Devices Software Categories Auto-Uninstall Validation Software Updates Auto-Deployment Software Updates Auto-Deployment Auto-Deployment Comparison Device Auto-Download	GFI LanGuard can detect mobile devices which connect to various services for email access. <u>Tell me more</u> Image: Add Mobile Device Management Source         Provide details and credentials for connecting to a mobile device information source.         Image: Retention Policy							
Control Action C	Drag a d	column header i	here to group by that	column	pe	centry.		
Common Tasks: Add Management Source Manage Retention Policy	Co	unt = 0						
	🔞 Use	e <u>Activity Moni</u>	tor to view mobile dev	ice scan activ	ity.		Delet	e selected configurations

Screenshot 64: Mobile Devices

Adding mobile device management sources

To add a mobile device management source:

# 1. Click Add mobile device management source.

2. Select the type of Mobile Device Management Source.

Add Mobile Device Manager	nent Source	<b>—</b>
Step 1 of 2: Configure a mobile de	vice management source.	
Source Details		
Туре:	Microsoft Exchange Server	•
Server Name:	Microsoft Exchange Server Microsoft Office 365	
Credentials	Google Apps for Business Apple Profile Manager	
Please provide credential group and has the 'Log o	s for a user which is member of the 'Exchange Organization Administrators' d n as a service' right.	omain
User name:		
Password:		
Use per computer cre	dentials when available	
	< Back Next >	Cancel

Screenshot 65: Configuring a mobile device management source: Selecting type of source

Source: Microsoft Exchange Server

1. Specify the credentials for Microsoft Exchange and click **Next**.

Add Mobile Device Manage	ement Source
Step 1 of 2: Configure a mobile d	device management source.
Source Details	
Туре:	Microsoft Exchange Server
Server name:	SRV01
Credentials	
Please provide credenti domain group.	ials for a user which is member of the 'Exchange Organization Administrators'
Authenticate using:	GFI LanGuard 11 Attendant Service account
User name:	
Password:	
Use per computer of	credentials when available
	< Back Next > Cancel

Screenshot 66: Configuring a mobile device management source: Source details

2. Configure when to refresh mobile device information and select (Optional) Exclude mobile devices and click Next.

Add Mobile Device Management Source	
<b>Step 2 of 2:</b> Configure when to refresh the mobile device information using server 'SRV01'.	
✓ Enable schedule <i>Run the audit every day at 15:08.</i> Recurrence pattem: Daily recurrence pattem	
<ul> <li>Every</li> <li>Every weekday</li> </ul>	
Exclude mobile devices	
< Back Finish	Cancel

Screenshot 67: Configuring a mobile device management source: Scheduling an audit

3. Select or unselect the accounts to manage and click **Finish**.

Add Mobil	e Dev	vice Management Source				×
Step 3 o Un	of 3: nselec	t a user account in order for GF	I LanGuard to sto	p managing mot	ile devices.	
	ß	Account	Name		Job Title	
<b>=</b>	Dep	partment: Development				
± 💌	Dep	partment: Finance				
± 💌	Dep	partment: Infrastructure				
± 📃	Dep	partment: Management				
± 🖌	Dep	partment: N\A				
± 💌	Dep	partment: Public Relations				
± 💌	Dep	partment: Sales				
		Count = 12				
Autor	matica	ally manage new accounts				
				< Back	Finish	Cancel

Screenshot 68: Configuring a mobile device management source: Managing devices

# Source: Microsoft Office 365

1. Specify the credentials for Microsoft Office 365 and click Next.

#### NOTE

» The specified account needs to be a global administrator.

» Working with **Microsoft Office 365** requires .NET Framework 4.5. GFI LanGuard provides the facility to to install .NET 4.5 automatically whilst configuring a new mobile device management source with **Microsoft Office 365**.

Add Mobile Device Ma	nagement Source
Step 1 of 2: Configure a mot	pile device management source.
Source Details	
Туре:	Microsoft Office 365
Server name:	Microsoft Office 365
Credentials Please provide vou	r Office 365 credentials.
5 1 11	
Email address:	jonnsmith@mail.onmicrosoft.com
Password:	••••••
	< Back Next > Cancel

Screenshot 69: Configuring a mobile device management source: Source details

2. Configure when to refresh mobile device information and select (Optional) Exclude mobile devices and click Next.

Add Mobile Device Management Source	
<b>Step 2 of 2:</b> Configure when to refresh the mobile device information using server 'SRV01'.	
✓ Enable schedule <i>Run the audit every day at 15:08.</i> Recurrence pattem: Daily recurrence pattem	
<ul> <li>Every</li> <li>Every weekday</li> </ul>	
Exclude mobile devices	
< Back Finish	Cancel

Screenshot 70: Configuring a mobile device management source: Scheduling an audit

3. Select or unselect the accounts to manage and click **Finish**.

Add Mobil	e Dev	vice Management Source				×
Step 3 o Un	of 3: nselec	t a user account in order for GF.	[LanGuard to sto	op managing mob	ile devices.	
	ß	Account	Name		Job Title	
± 🔳	Dep	artment: Development				
± 💌	Dep	artment: Finance				
÷ 💌	Dep	artment: Infrastructure				
÷ 📄	Dep	artment: Management				
± 💌	Dep	artment: N\A				
± 🖌	Dep	artment: Public Relations				
÷ 💌	Dep	artment: Sales				
		Count = 12				
Autor	matica	ally manage new accounts				
				< Back	Finish	Cancel

Screenshot 71: Configuring a mobile device management source: Managing devices

#### Source: Google Apps for Business

#### NOTES

» If you use Google Apps for Business , GFI LanGuard can retrieve the list of mobile devices that connect to your Google Apps domain.

» By default, your Google Apps domain is not configured to allow querying by other software such as GFI LanGuard. Below are the required step-by-step changes required for your Google Apps domain configuration to enable mobile device scanning with GFI LanGuard

To configure your Google Apps domain to enable mobile device scanning with GFI LanGuard:

1. Enable API access in your Google Apps Admin console. Log in to your admin account and select **Security**. If **Security** is not listed, select **More controls > Security** from the options shown in the gray box. Select **API reference**, and then select the checkbox to Enable API access. Click **Save** to save your changes.

2. Set up a new project in the Google APIs Console and activate the Admin SDK API for this project.

3. In the **Credentials** section of your project, enable **OAuth** authentication by selecting **Create New Client ID**. Choose the **Service Account** option and save the service account's Client ID, email address and the generated private key file.

4. Grant read-only access to user data to your Service Account:

a. Open your Google Apps domain control panel, at https://www.google.com/a/cpanel/example.com

b. Click **Security** icon. This can be found under **More controls** 

#### c. Select Advanced tools > Manage third party OAuth Client access

- d. In the Client name field enter the service account's **Client ID**
- e. In the **One or More API Scopes** field, copy and paste the following list of scopes
  - https://www.googleapis.com/auth/admin.directory.device.mobile.readonly
  - https://www.googleapis.com/auth/admin.directory.group.readonly
  - https://www.googleapis.com/auth/admin.directory.user.readonly

#### f. Click Authorize.

5. Optionally enable **Application auditing** so that GFI LanGuard can report the applications installed on mobile devices:

- » Log in to your admin account and select Device Management/Device management settings.
- » In the Advanced settings section. mark the Enable application auditing option.
- » Click **Save** to save your changes.

#### NOTE

For more information on how to set up Google Apps for API access see:

- » http://go.gfi.com/?pageid=LAN\_GoogleAppsPrerequisites
- » http://go.gfi.com/?pageid=LAN\_GoogleAppsGeneratingOAuth

6. Specify the credentials for Google Apps for Business and click Next.

Add Mobile Device Manage	ment Source
Step 1 of 2: Configure a mobile de	evice management source.
Source Details	
Туре:	Google Apps for Business
Service Account Name:	Google Apps for Business
Credentials	
Please provide your Goo	gle Apps for Bussiness domain name and the path to your certificate file.
Email address:	johnsmith@example.com
Google certificate file:	C: \Users \admin \Desktop \5d5g5g5dfg5df6fdf6588879as-privatekey.p12
	< Back Next > Cancel

Screenshot 72: Configuring a mobile device management source: Source details

7. Configure when to refresh mobile device information and select (Optional) Exclude mobile devices and click Next.

Add Mobile Device Management Source	×
Step 2 of 2: Configure when to refresh the mobile device information using server 'SRV01'.	
✓ Enable schedule Run the audit every day at 15:08.          Recurrence pattem:       daily       at: 15:08:52       ⇒	
Daily recurrence pattern	
<ul> <li>Every days</li> <li>Every weekday</li> </ul>	
Exclude mobile devices	
< Back Finish	Cancel

Screenshot 73: Configuring a mobile device management source: Scheduling an audit

8. Select or unselect the accounts to manage and click **Finish**.

Add Mobil	dd Mobile Device Management Source				
Step 3 O	Step 3 of 3: Unselect a user account in order for GFI LanGuard to stop managing mobile devices.				
	🗅 Account	Name	Job Title		
± 📄	Department: Development				
± 💌	Department: Finance				
± 💌	Department: Infrastructure				
± 📃	Department: Management				
± 💌	Department: N\A				
± 💌	Department: Public Relations				
± 💌	Department: Sales				
	Count = 12				
Autor	matically manage new accounts				
		< Back	Finish Cancel		

Screenshot 74: Configuring a mobile device management source: Managing devices

# NOTE

GFI LanGuard can query Apple Profile Manager for the list of managed mobile devices such as mobile phones or tablets running iOS. You need to provide root credentials to the OS X Server hosting Profile Manager.

1. Specify the credentials for Apple Profile Manager and click Next.

Add Mobile Device Mar	nagement Source			
Step 1 of 2: Configure a mobile device management source.				
Source Details				
Type:	Apple Profile Manager			
Server Name:	MACSERVER			
Please provide cred User name: Password: SSH port:	entials for a user which has root privileges.			
✓ Use per comput	er credentials when available			
	< Back Next > Cancel			

Screenshot 75: Configuring a mobile device management source: Source details

2. Configure when to refresh mobile device information and select (Optional) Exclude mobile devices and click Next.

Add Mobile Device Management Source	<b>—</b> ×
Step 2 of 2: Configure when to refresh the mobile device information using server 'SRV01'.	
Enable schedule Run the audit every day at 15:08.	
Recurrence pattem: daily  at: 15:08:52	
Daily recurrence pattern	
<ul> <li>● Every 1</li></ul>	
Exclude mobile devices	
< Back Finish	Cancel

Screenshot 76: Configuring a mobile device management source: Scheduling an audit

3. Select or unselect the accounts to manage and click Finish.

Add Mobil	dd Mobile Device Management Source					
Step 3 o Un	Step 3 of 3: Unselect a user account in order for GFI LanGuard to stop managing mobile devices.					
	D .					
	Li Account	Name	Job Title			
🖽 📄	Department: Development					
± 🖌	Department: Finance					
÷ 🖌	Department: Infrastructure					
± 🔤	Department: Management					
± 🖌	Department: N\A					
± 🖌	Department: Public Relations					
± 💌	Department: Sales					
	Count = 12					
Autor	natically manage new accounts					
		< Back	Finish Cance	1		

Screenshot 77: Configuring a mobile device management source: Managing devices

## NOTE

Use Managing retention policies to clean up mobile devices that have not recently connected.

To manage retention policies:

- 1. Click on **Configuration** tab > **Mobile Devices**.
- 2. From the right pane, select Manage retention policy.
- 3. Specify the time frame to keep non-active devices.

Mobile Device Retention	×
General	
Configure how to remove mobile devices which did not connect recently.	
Keep mobile devices which have connected during the last	
OK Cance	

Screenshot 78: Managing retention policies

Unmanaged devices

GFI LanGuard does not perform full audits of mobile devices unless a mobile device management source has been configured and user accounts are approved.

To view unmanaged mobile devices:

## 1. Click **Dashboard** tab and from the computer tree select > **Unmanaged mobile devices**.

(Optional)To change settings for unmanaged devices:

- 2. From the right pane, select a server containing unmanaged mobile devices and click **Configure**.
- 3. Select a user account to start managing the devices connected to the particular account.

🌒 GFI LanGuard								
Dashboard	Scan R	Remediate	Activity Monitor	Reports	Configuration	Utilities	🕐 - D	)iscuss this version
Filter Group Search		Unma Select the	naged Mobile	e Devic	<b>ES</b> Guard to manage.			
▲ Settire Network     Image: Cool Index of the Index of	GFI Lan	Guard can de	tect mobile devices w	hich connect	to Microsoft Exchar	ige Server for	email access. Clear	<u>Tell me more</u>
📕 Unmanaged mobile devices	Manager	ment Server			Status			Configure
	~ <b>⊑</b> ⊠ e	x2013lnss			Managed			Configure
	8	🖁 adrianoced	chi@noc.com		3 unmanaged devic	es		
		占 alenacerkv	a@noc.com		1 unmanaged devic	es		
	8	占 alexplin@r	noc.com		1 unmanaged devic	es		
	1	占 benjaminjo	hnes@noc.com		1 unmanaged devic	es		
	1 8	semmanuelt	tino@noc.com		1 unmanaged devic	es		
		fionabrowr	n@noc.com		1 unmanaged devic	es		
	8	] jasonuhr@	noc.com		1 unmanaged devices 1 unmanaged devices			
		sjohnparker	@noc.com					
	8	] josephmah	ler@noc.com		2 unmanaged devic	es		
	8	simonemar	n@noc.com		2 unmanaged devic	es		
		simonrave	@noc.com		4 unmanaged devic	es		
		s wolfgangra	at@noc.com		3 unmanaged devic	es		
				Count = 1				
								i

Screenshot 79: Unmanaged mobile devices

# 4.3 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 section:

4.3.1 Achieving results from the dashboard	123
4.3.2 Using the Dashboard	
4.3.3 Using the Computer Tree	
4.3.4 Using Attributes	130
4.3.5 Dashboard actions	132
4.3.6 Exporting issue list	133
4.3.7 Dashboard views	133

# 4.3.1 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.

# 4.3.2 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 80: View Dashboard

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

# 4.3.3 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

» Sync-up with Active Directory

## 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**.

Filter	Group	Search		
🗸 Filters ar	re: ON			
Vulnerability le	vel: All	$\bigtriangledown$		
Operating System: All				
Last scan time:	All	$\bigtriangledown$		
Agent status: A	$\bigtriangledown$			
Network role: All				
Advanced filtering				
Clear filters OFF filters				

Screenshot 81: Simple filtering

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 82: 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**

#### Grouping

To group machines by specific attributes:

1. From the left panel, click **Group**.

Filter	Group	Search			
Computers	Mobile Devices				
Group comput	ters by:				
Oomain	and Organization	al Unit (Default)			
Operat	Operating System				
Network Role					
Relays Distribution					
<ul> <li>Attributes: Location</li> </ul>					
C Apply grouping					

#### Screenshot 83: Grouping

2. Click on one of the following tabs and select a specific attribute:

Tabs	Attributes
Computers	<ul> <li>Domain and Organizational Unit</li> <li>Operating System</li> <li>Network Role</li> <li>Relays Distribution</li> <li>Attributes</li> </ul>
Mobile Devices	<ul> <li>&gt;&gt; User Account</li> <li>&gt;&gt; Operating System</li> <li>&gt;&gt; Device Model</li> <li>&gt;&gt; Attributes</li> </ul>

## NOTE

If **Attributes** is selected, select the attribute from the drop down list. For more information, refer to <u>Using</u> <u>Attributes</u> (page 130).

3. If Attributes is selected, select the attribute from the drop-down list.

#### 4. Click Apply grouping.

## 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**.

Filter	Group	Search		
Machine Name				
Group results by information category				
Group re	Group results by computer			
Search history				
Advanced search				

Screenshot 84: Search specific computers and groups

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

Option	Description
Group results by inform- ation category	Search results are grouped by category. The result contains the latest computer information. Amongst others results are grouped by: 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.          NOTE         For more information, refer to Full text searching (page 223).

## Sync-up with Active Directory

This feature enables you to perform the following tasks:

- » Add computers that are in Active directory but not yet in GFI LanGuard
- » Move computers to the correct Organizational Unit (OU) in the GFI LanGuard computer tree
- » Remove computers that have been deleted from Active Directory but are still present in GFI LanGuard
- 1. Right-click the computer tree to synchronize and select Synchronize with Active Directory.
- 2. If displayed, key in the domain credentials require to retrieve the domain's Organizational Units and click **OK**
- 3. Click **Next** to start the synchronization process.

4. In the list of discovered computers, review the displayed list of changes that this process will do. This list shows where specific computers will be repositioned to which Active Directory Organizational Units. Click **Next**.

- 5. Review the list of computers that will be added to GFI LanGuard from Active Directory. Click **Next**.
- 6. Review the list of computers that are no longer present, or have been deleted from Active Directory. Click Sync.

7. On process completion, click **Finish**.

# 4.3.4 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

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 85: 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.

## 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**.

Attribute	Value	Add.
Location	1st Floor	Edit
	Add an attribute for '{0}'. You can ca attribute or define a value for an exis Name: Department Value: Support	reate a new isting one.
Note: Custom attri share the same	OK Cancel	ied at this stage will

Screenshot 86: 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.

## Configuring attributes

To configure attributes:

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

New attribute					
Add attri	d an attribute for 'TEMP'. You can create a new ibute or define a value for an existing one.				
Name:	Location	•			
Value:	2nd Floor	•			
	OK Cancel				

Screenshot 87: 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.

## 4.3.5 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.

Actions:	
۲	Remediate
<b>Ø</b>	Acknowledge
0	Ignore
	Change Severity
	Rules Manager

Screenshot 88: Actions section in the Dashboard

3. Select one of the following actions:

Action	Description
Remediate	Launch the Remediation Center to deploy and manage missing patches.
	<b>NOTE</b> For more information, refer to <u>Manual Remediation</u> (page 185).
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.

Action	Description
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, and include reasons why to ignore such vulnerabilities. Configure for which machine this rule applies and the time span that the issue is ignored.
Change Sever- ity	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 Man- ager	Launch the Rules Manager dialog. This enables you to search and remove configured rules and view the reasons to ignore missing patches and vulnerabilities.

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

# 4.3.7 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

## Overview



Screenshot 89: 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:

Section	Description
Network security level	This rating indicates the vulnerability level of a computer/network, depending on the num- ber and type of vulnerabilities and/or missing patches found. A high vulnerability level is a res- ult of vulnerabilities and/or missing patches which average severity is categorized as high.
Computer vulnerability dis- tribution	This chart is available only when selecting a domain or a workgroup, and displays the dis- tribution 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 vul- nerable computers discovered during the scan. The icon color on the left indicates the vul- nerability level.

Section	Description
Agent Status	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:
	» 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	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 selec- ted 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.
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.

Section	Description
Security Sensors	<ul> <li>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:</li> <li>Missing Software Updates</li> <li>Missing service packs</li> <li>Vulnerabilities</li> <li>Firewall Issues</li> <li>Unauthorized Applications</li> <li>Audit Status</li> <li>Credentials setup</li> <li>Malware Protection Issues</li> <li>Agent Health Issues.</li> </ul>

# Computers view

🔮 GFI LanGuard												
Dashboard Scan Remediate					Activity Monitor Reports Configuratio» (9) Tiscuss this version							
Dashboard      Section      Construction      Construction	Com	Scan       Remediate       Activity Monitor       Reports       Configuratio® (Inclusion)         Overview       Computers       Image: State of the state							Software	>		
	VL	Computer 192.168.2.8 SERV08-06 WIN7_06 SERV03-01 SERV08-04	Name	Do - WORKGF WORKGF	main ROUP ROUP ROUP		OS N/A Windows 7 Windows 2003 Windows 2008	SP - Gold 2 , Gold	Last D 02/07/2 03/07/2 03/07/2	iscovery - 012 15:12 012 14:43 012 14:47	Last Audit - 02/07/2012 1 03/07/2012 1 03/07/2012 1	△ - - 5:12 - 4:43 - 4:47 -
Common Tasks:       ×         Manage agents       Add more computers         Add more computers       Scan and refresh information now         Custom scan       Set credentials         Deploy agent       Deploy agent	<[[		Count=5	]								.:

Screenshot 90: 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:

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 com- puter and if yes, displays the type of credentials being used by the agent.
Vulnerabilities	<ul> <li>View the number of vulnerabilities found on a computer grouped by severity. Severity of a vulnerability can be:</li> <li>High</li> <li>Medium</li> <li>Low</li> <li>Potential.</li> </ul>
Patching status	View the number of: Missing Security/non-Security Updates Missing Service Packs and Update Rollups Installed Security/non-Security Updates Installed Service Packs and Updates Rollups.
Open ports	View the number of: >> Open TCP ports >> Open UDP ports >> Backdoors.

Option	Description
Software	<ul> <li>View the number of:</li> <li>Antiphishing engines</li> <li>Antispyware engines</li> <li>Antivirus engines</li> <li>Backup applications</li> <li>Data loss prevention applications</li> <li>Device access and desk encryption applications</li> <li>Firewalls</li> <li>Installed applications</li> <li>Installed applications</li> <li>Peer to peer applications</li> <li>Unauthorized applications</li> <li>Virtual machines</li> <li>VPN clients</li> <li>Web browsers.</li> </ul>
Hardware	View information on: Number of disk drives Free disk space Memory size Number of processors Other hardware.
System information	View information on: The number of shared folders Number of groups View information on: Number of groups Logged users Audit policy status.
Attributes	Adds an <b>Attributes</b> 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.

## 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 91: History view in the Dashboard

## 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 92: Vulnerabilities view in the Dashboard

#### NOTE

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

## Configuring actions

From the actions section select one of the actions described below to manage and remediate vulnerabilities and missing patches found in your network.

Action	Description
Remediate	Launch the Remediation Center to deploy and manage missing patches.
	NOTE
	For more information, refer to Manual Remediation (page 185).

Action	Description
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, and include reasons why to ignore such vulnerabilities. Configure for which machine this rule applies and the time span that the issue is ignored.
Change Sever- ity	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 Man- ager	Launch the Rules Manager dialog. This enables you to search and remove configured rules and view the reasons to ignore missing patches and vulnerabilities.

# 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.

🥑 GFI LanGuard							
Dashboard	Scan Remediate Activity Monitor	Reports Configuration Utili 🏵 🌒 🕆 Discuss this version					
Filter Group Search	Image: Computers         Image: Computers <th computers<<="" image:="" th=""><th>Vulnerabilities Patches Ports Software *</th></th>	<th>Vulnerabilities Patches Ports Software *</th>	Vulnerabilities Patches Ports Software *				
🔺 💐 Entire Network 🛛 🖷	Entire Network - 2 compute	ers					
Localhost : W711	Patch Types	Patch List					
Local Domain : WORKGROUP	Missing County Hadatas (1)						
	Missing Security Opdates (1)     Missing Non-Security Updates (24)	Drag a column header here to group by that column					
📕 😰 alenacerkva@noc.com	🕐 Missing Service Packs and Update Rollups	D         Patch name         Date posted         Applies to         No. of computers					
▶ 🕎 alexplin@noc.com 🗧	Vinstalled Security Updates (93)	FOXITR54209 2012-09-07 Foxit Reader 1					
🕨 🙀 emmanueltino@noc.com 🛛 🕒	Installed Service Packs and Update Rollup	WS06-061: MS 2012-04-04 SQL Server 1					
🕨 😰 fionabrown@noc.com	· · ·	MS08-069: Se 2011-07-12 Windows 1					
▶ 🕎 jasonuhr@noc.com		MS11-015: Se 2011-03-08 Windows 1					
johnparker@noc.com		MS11-019: Se 2011-04-12 Windows 1					
josephmahler@noc.com		MS11-024: Se 2011-04-12 Windows 1					
Simonemann@noc.com	4 III +	Count=93					
wolfgangrat@noc.com	Details Installed on						
Unmanaged mobile devices	Installed Security Update: N	IS11-015: Security Update for Windows 7 (KB2479943)					
	Bulletin ID: MS	511-015					
	QNumber: 24	79943 March 2011					
	Severity: Cr	itical					
	Applies to: Wi	ndows					
	Uninstallable by LanGuard: Yes Description: A security issue has been identified that could allow an						
	un co	authenticated remote attacker to compromise your system and gain					
	up	date from Microsoft. After you install this update, you may have to start your system.					
	URL: htt	tp://go.microsoft.com/fwlink/?LinkId=207841					
	References: Se	curityFocus:46682, OVAL:12506, CVE-2011-0042, OVAL:12281, /E-2011-0032, SecurityFocus:46680					
	<u></u>						

Screenshot 93: Patches view in Dashboard

## NOTE

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

# 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.



Screenshot 94: Ports view in Dashboard

## NOTE

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

# 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.

🧳 GFI LanGuard	_		
🔲 🔽 👌 ( 🔶   🔶 🛛 Dashboard	Scan Remediate Activity	Monitor Reports Configuration	> (2) Tiscuss this version
Filter Group Search	« Jistory Vulnerabilities I	Patches Ports Softwar	e Hardware System Information
🔺 💐 Entire Network 🛛 🖷	Entire Network - 6 con	nputers	
Nocalhost : WIN7_06			
🕨 🕎 Local Domain : WORKGROUP 🛛 🖣	Application Category	Applications List	
TEMASOFT      Mobile Devices	All Applications (27)     Antispyware (1)	Drag a column header here to group l	by that column
	Antiphishing (2)	Application name Version	Publisher No. of computers
	VPN Client (1)	🧃 Adobe Flash Play 11.1.10	Adobe S 1
	Web Browser (2)	FastStone Captur 7.1	FastSton 1
	Disk Encryption (1)	GFI LanGuard 2012 11.0.20	GFI Soft 1
	Patch Management (3)	GFI WebMonitor 7.0.11357	GFI Soft 1
	- ONE Fileing (1)	IIS 7.5 Express 7.5.1070     Merrore A NET Fr. 4.0.20210	Microsoft 1
		Microsoft .NET Fr 4.0.30319	Microsoft 2
		Count=27	
			¥
	Details Installed on Not installed o	n	
Common Tasks: ¥	Application: Adobe Flas	h Player 11 ActiveX	Actions:
	Version: 11.1.102.55		=
Manage agents Add more computers	Publisher: Adobe Systems	Incorporated	Add to Category
Scan and refresh information now Custom scan			Software Categories
<u>Set credentials</u> Deploy agent			Ŧ
			.:

Screenshot 95: Software view in Dashboard

From the actions section select one of the actions described below to manage and categorize software applications.

Option	Description
Add to category	Add applications to a particular category
Software Cat- egories	Configure rules for particular software categories and applications. For more information refer to Configure software categories

### 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.
### Configuring software categories

GFI LanGuard comes with a software categories feature that enables you to add and sort software according to different categories. GFI LanGuard also supports editing on software details.

- » Adding New Software Categories
- » Adding New Software to a Category
- » Importing Software to a Category
- » Customizing Software

To configure Software categories:

1. Click on the **Configuration** tab > **Software Categories** to set categories for specific applications or to create a new software categories.

GFI LanGuard							
📃 💷 🚯   🗲   🔿 🔹 Dashboard	Scan Remediate A	ctivity Monitor	Reports	Configuration	Utilities	🕖 🔹 Discuss this	s version
Configurations: Agents Management Scanning Profiles Scheduled Scans Mobile Devices Software Categories Applications Inventory Auto-Uninstall Validation	Software Manage softwa GFI LanGuard is able to so Use this tool to manually s	Categories re classification intr can for software ins et categories for sp	o categories. talled in the r vecific applic	network and automa ations or to create a	tically classify it i new custom softw	nto predefined or custon vare category. <u>Tell me n</u>	n categories. 10re
Patch Auto-Deployment		-	Find	Clear	Ade	d 🔻 Edit	Remove
Patch Auto-Download     Aerting Options     Database Maintenance Options	Name				Publisher		
	🍕 Antiphishing						
	Mantispyware						
I 🔒 Licensing	V Backup				Software	Software Company	
Common Taske	v 🖉 Data Loss Preve	ntion			bortmare	company	
	Software Comp	any C			Software	Company	
Go to: Software inventory	🗸 🌲 Device Access C	ontrol					
Actions:	🐌 Software B				Software	Company	
New software category	🛑 Software Comp	any C			Software	Company	
Add software to category	Disk Encryption						
Import	V 🔐 Firewall						
Edit	Software Comp	any C			Software	Company	
Remove	Health Agent						
	Can Instant Messeng	jer t					
	Pater Hallagen	any C			Software	Company	
	Peer-To-Peer	anyc			Sortware	Company	
	Count = 6						•
	A new scan is requir	ed to reflect in <u>Das</u>	hboard and	Reports any change	s made here.		

Screenshot 96: Software Categories

### Adding New Software Categories

To add new software categories:

1. Click **Configuration** tab > **Software Categories** and from the right panel click on the **Add**drop-down list and select**New software category**.

New software category		×
Name		
Security		
(	ОК	Cancel

Screenshot 97: Software category name

2.

Key in the name for the new software category.

### Adding New Software to a Category

To add new software to a category:

1. Click **Configuration** tab > **Software Categories** and from the right panel click on the **Add**drop-down list and select**Add software to category**.

Indilic		
Equals	Software X	
Publisher (optional)		
Equals	(enter a value)	
Category		r +
Category           (Select All)           Antivirus		•
Category (Select All) Antivirus Antiphishing		+
Category (Select All) Antivirus Antiphishing Antispyware		• 
Category (Select All) Antivirus Antiphishing Antispyware Backup		• •

Screenshot 98: Adding a software to a category

2.

Enter the name and publisher of the new software and select the category for the new software.

### Importing Software to a Category

To import software to a category:

1. Click **Configuration** tab > **Software Categories** and from the right panel click on the **Add**drop-down list and select**Import**.

Import		2	٢.
10	Import softwares from text file that contains one software name per line.		
	Text file:		
	C:\Program Files\7-Zip\History.txt	se	
	Software name	*	
	9.15 beta 2010-06-20	0	
	- New localization: Tatar.		
	9.14 beta 2010-06-04		
	9.13 beta 2010-04-15		
	Count = 785	Ŧ	
	Category		
	▼ + ···	-	1
	Select All)	*	1
	Antivirus		
	Antiphishing	ļU	
			зđ
	DataLossPrevention		
	DeviceAccessControl	Ŧ	
	OK Cancel	//	

Screenshot 99: Importing a software to a category

2. Select the text file containing the software name and select the category you want the software to be included in.

# Customizing Software

To customize software in a category:

1. Click **Configuration** tab > **Software Categories** and from the right panel click **Edit**.

Software details	×
Name	
Equals 🔹	Software Company C
Publisher (optional)	
Equals 🔹	Software Company
Category	
Data Loss Prevention; Device Ad	ccess Control; Firewall; Patch Management 🔻 🔸
	OK Cancel

Screenshot 100: Editing software details

2.

Change the necessary details and click **OK** to save the changes.

### Hardware View

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



Screenshot 101: Hardware view in Dashboard

#### NOTE

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

### System Information View

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



Screenshot 102: System Information view in Dashboard

#### NOTE

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

# 4.4 Interpreting Results

On completion of a network security scan, it is important to identify the areas that require immediate attention. Use the information provided in this topic to determine the correct analysis and interpretation approach to get the most out of your scan results and apply the appropriate fixes.

Topics in this section:

4.4.1 Interpreting scan results	. 151
4.4.2 Loading results from the database	160
4.4.3 Saving and loading XML results	. 161

### 4.4.1 Interpreting scan results

The **Scan Results Overview** and **Scan Results Details** sections in the **Scan** tab, are designed to facilitate the result analysis process as much as possible. Use the information in the following sections to learn how scan results are interpreted and to know which areas require your immediate attention:

- » Viewing scan results
- » Vulnerability level rating
- » Vulnerability Assessment
- » Network & Software Audit

#### Viewing scan results

Use this section to interpret results generated by manual scans and results stored in the database backend. For more information, refer to <u>Manual scans</u> (page 96).

To view scan results:

1. Launch GFI LanGuard and click the **Scan** tab.

2. Launch a new scan or load the result from the database/file. For more information, refer to Loading results from the database (page 160).

3. Once completed, the results are displayed in the Scan Result Overview and the Scan Results Details sections.

V GFI LanGuard	
Dashboard Scan Remed	diate Activity Monitor Reports C >> (9) > Discuss this version
Launch a New Scan	
Scan Target: Profile:	
localhost 🗸 🛄 Full Sca	an 🔻 🔞
<u>C</u> redentials: <u>U</u> sernan	ne: <u>P</u> assword:
Currently logged on user 👻	<u>S</u> can
Scan Options	
Scan Results Overview	Scan Results Details
🖃 🧳 Scan target: localhost 🧧	A
🚊 🖓 🕼 192.168.2.12 [WIN7_06] (Windows 7 Gold)	Scan completed!
🖃 🐴 Vulnerability Assessment	Summary of scan results generated during this network audit.
High Security Vulnerabilities (2)	
Medium Security Vulnerabilities (1)	
Low Security Vulnerabilities (5)	
Potential Vulnerabilities (1)     Missing Service Packs and Undate Pollups (3)	Vulnerability level:
Missing Security Updates (1)	The average vulnerability level for this scanning session is: High
Network & Software Audit	
👜 🐚 System Patching Status	
🖨 🍓 Ports	Results statistics:
🐝 Open TCP Ports (6)	14311 audit operations
🐝 Open UDP Ports (8)	Audit operations processed: processed
🕀 🦂 Hardware	Missing software updates: 16 (16 Critical/High)
🖽 📆 Software	Other vulnerabilities: 8 (2 Critical/High)
🖽 🐨 📆 System Information	Potential vulnerabilities: 1
4	Open porte: 20 (0 unauthorized)
Scanner Activity Window	*

Screenshot 103: Results overview

From **Scan Results Overview**, expand a computer node to access results retrieved during the scan. Security scan results are organized in two sub–nodes tagged as:

- » Vulnerability Assessment
- » Network & Software Audit

While a scan is in progress, each computer node has an icon that categorizes the response time. The table below describes the different icons used by GFI LanGuard to categorize the response time. The first icon indicates that the scan is queued, while the second icon indicates that the scan is in progress.

Category	Information	Description
2 🕰	Fast response	Less than 25ms
2. 9	Medium response	Between 25ms and 100ms
2	Slow response	More than 100ms

### Vulnerability Level Rating

The GFI LanGuard vulnerability level is a rating assigned to each scanned computer. The rating can be viewed from:

» Scan Results Details – This section in the Scan tab provides you with a vulnerability level meter assigned the computers/groups that have been scanned

» **Dashboard** – The Dashboard section provides you with information for specific computers or selected groups of computers, from the computer tree. Select the computer/group and view the vulnerability meter from the right pane. Select Entire Network to view the vulnerability level for all your scan targets.



Screenshot 104: Vulnerability level meter

### How is the vulnerability level calculated?

The vulnerability level is calculated using a weighting system. After a scan, GFI LanGuard groups the discovered vulnerabilities in categories sorted by severity rating:

- » High
- » Medium
- » Low

For each rating, a weighted score is given. This is based on the total number of vulnerabilities per category.

#### NOTE

When the vulnerability level cannot be assessed or vulnerability scanning was not performed, GFI LanGuard gives a rating of **N/A**.

#### Weight scores

Category	Number of Detected Vulnerabilities	Scores
High Vulnerabilities	1-2 3-5 > 5	8 9 10
Medium Vulnerabilities	1-2 3-5 > 5	5 6 7
Low Vulnerabilities	1-2 3-5 > 5	2 3 4

#### Score classification

After categorizing detected vulnerabilities and generating a score for each category, the overall vulnerability level is generated. The vulnerability level is the severity rating with the highest score.

Vulnerability level scores:

- » A score of >= 8, results in **High** vulnerability rating
- » A score of <= 7 and >= 5, results in **Medium** vulnerability rating
- » A score of <= 4 and >=1, results in a Low vulnerability rating

### Example

During a scan of Computer A, the following vulnerabilities were discovered:

- » 3 high vulnerabilities
- » 8 medium vulnerabilities
- » 5 low vulnerabilities

The score for each category was calculated with the following results:

- » 3 high vulnerabilities = 9
- » 8 medium vulnerabilities = 7
- » 5 low vulnerabilities = 3

The vulnerability level for Computer A is therefore **HIGH**.



Screenshot 105: Dashboard Vulnerability Meter

The vulnerability level is indicated using color-coded graphical bar:

- » Red bar = high vulnerability level
- » Green bar = low vulnerability level.

### Vulnerability Assessment



Screenshot 106: The Vulnerability Assessment node

Click on any **Vulnerability Assessment** node to view the security vulnerabilities identified on the target computer grouped by type and severity.

### High Security Vulnerabilities

Click on the **High Security Vulnerabilities** or **Low Security Vulnerabilities** sub–nodes for a list of weaknesses discovered while auditing a target device. Groups are described in the following table:

Group	Description
Mail, FTP, RPC, DNS and Miscellaneous	Shows vulnerabilities discovered on FTP servers, DNS servers, and SMTP/POP3/IMAP mail servers. Links to Microsoft <sup>®</sup> Knowledge Base articles or other support documentation are provided.
Web	Lists discovered vulnerabilities on web servers (such as wrong configuration issues). Supported web servers include Apache, Internet Information Services (IIS®) and Netscape.
Services	Lists vulnerabilities discovered in active services as well as the list of unused accounts that are still active and accessible on scanned targets.
Registry	Registry settings of a scanned network device are listed. Links to support documentation and short vul- nerability descriptions are provided.
Software	Enumerates software installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.
Rootkit	Enumerates discovered vulnerabilities because of having a rootkit installed on the scanned network device(s). Links to supporting documentation and short vulnerability descriptions are provided.

#### Potential vulnerabilities

Select **Potential vulnerabilities** sub-node to view scan result items classified as possible network weaknesses. Although not classified as vulnerabilities, these scan result entries still require particular attention since malicious users can exploit them during malicious activity.

For example, during vulnerability scanning GFI LanGuard enumerates all modems installed and configured on target computers. If unused, modems are no threat to your network. If connected to a telephone line these modems can, however, be used to gain unauthorized and unmonitored access to the Internet. Users can potentially bypass corporate perimeter security including firewalls, antivirus, website rating and web content blocking. This exposes the corporate IT infrastructure to a wide range of threats including hacker attacks. GFI LanGuard considers installed modems as possible threats and enumerates them in the **Potential Vulnerabilities** sub–node.

#### Missing Service Packs

Click **Missing Service Packs and Update Rollups** or **Missing Security Updates** sub-nodes to check any missing software updates or patches. For a full list of missing service packs and missing patches that can be identified by GFI LanGuard, refer to http://go.gfi.com/?pageid=ms\_app\_fullreport

#### Bulletin information.

To access bulletin information, right-click on the respective service pack and select More details>Bulletin Info.

Bulletin Info							<b>×</b>
Bulletin							
Bulletin ID:	Not Available	QNumber:	890830	Date:	2011-02-08	Severity:	Undefined
Title:	Windows Malicious Software Removal Tool x64 - February 2011 (KB890830)						
Description:	After the down malicious softw an infection is f version of the t can download a	load, this tool are (including jound, the too tool will be off a copy from th	runs one time ti Blaster, Sasser, I will display a st ered every moni e Microsoft Dow	o check your and Mydoor atus report t h. If you wa nload Cente	computer for infe n) and helps remo the next time that ant to manually run r, or you can run	ection by specif ve any infectio you start you n the tool on y an online versi	ic, prevalent on that is found. If r computer. A new our computer, you on from
Applies To:	Windows Serve Windows Serve Windows XP x6 Windows Vista	er 2003 er 2003, Datao 4 Edition	enter Edition				
URL:	http://go.micros	oft.com/fwlink	(/?LinkId=39987				
							Close

Screenshot 107: Bulletin info dialog

### Network & Software Audit

Scan Results Overview					
🖃 🏈 Scan target: localhost					
🖮 🗹 🗑 192.168.2.12 [WIN7_06] (Windows 7 Gold)					
🕀 📷 Vulnerability Assessment					
🖮 🚎 Network & Software Audit					
🖨 👋 System Patching Status					
🍿 Missing Service Packs and Update Rollups (3)					
🖤 🅡 Missing Security Updates (1)					
🕡 Missing Non-Security Updates (12)					
🖤 🥩 Installed Service Packs and Update Rollups (9)					
🥩 Installed Security Updates (77)					
Installed Non-Security Updates (25)					
🕀 📲 Ports					
🕀 🍂 Hardware					
🕀 🧃 Software					
🗄 🖏 System Information					

Screenshot 108: The network and software audit node

Click **Network & Software Audit** to view security vulnerabilities identified on scanned targets. In this section, vulnerabilities are grouped by type and severity.

#### System Patching Status

Click **System Patching Status** to view all missing and installed patches on a target machine. Available links are:

- » Missing Service Packs and Update Rollups
- » Missing Security Updates

- » Missing Non-Security Updates
- » Installed Service Packs and Update Rollups
- » Installed Security Updates
- » Installed Non-Security Updates.

Scan Results Details						
System Patching Status Select one of the following system patching status categories bellow						
Missing Service Packs and Update Rollups (3) Allows you to analyze the missing service packs information						
<b>Missing Security Updates (1)</b> Allows you to analyze the missing security updates information						
<b>Missing Non-Security Updates (12)</b> Allows you to analyze the non-security updates information						
Installed Service Packs and Update Rollups (9) Allows you to analyze the installed service packs information						
Allows you to analyze the installed security update information						
Allows you to analyze the installed non-security updateinformation						

Screenshot 109: System patches status

#### **Open Ports**

Click **Ports** to view all open TCP and UDP ports detected during a scan. If a commonly exploited port is discovered to be open, GFI LanGuard marks it in red.

#### NOTE

Some software products may use the same ports as known Trojans. For additional security, GFI LanGuard identifies these ports as a threat.

Apart from detecting open ports, GFI LanGuard uses service fingerprint technology to analyze the services that are running behind the detected open ports. With service fingerprint, GFI LanGuard can detect if malicious software is using the detected open port.



Screenshot 110: All UDP and TCP ports, found during a scan

#### Hardware audit

Click **Hardware** to view all details discovered by the hardware audit. The hardware audit, amongst others, displays information such as MAC addresses, IP addresses, device type; device vendor etc. The table below describes the hardware information groups:

Information	Description
Network Devices	Includes information of all physical, virtual and software–enumerated devices.
Local Drives	Includes information on local drives such as available disk space and file system type.
Processors	Includes information regarding the processor of a target machine, such as vendor name and processor speed.
Motherboard	Includes information regarding the motherboard of a target machine, such as product name, manufacturer, version and serial number.
Memory details	Includes information regarding the memory allocation of a target machine, such as free physical/virtual memory available.
Storage details	Includes information regarding the storage of a target machine, such as floppy disk drive, CD/ROM and hard drives.
Display adapters	Includes information regarding the display and video devices of a target machine, such as the device manufacturer.
Other devices	Includes information of devices that do not fall under the mentioned categories above, such as keyboard, ports, mouse and human interface devices.

#### Software audit

Click **Software** to view all details involved in the software audit. The software audit amongst others displays information such as:

- » Application name
- » Publisher
- » Version.

The table below describes the hardware information groups:

lcon	Description
General Applications	Enumerates installed software on scan targets.

lcon	Description
Antivirus Applications	Lists installed antivirus engines on scan targets.
Instant Messenger Applications	Lists all detected instances of Instant messenger applications on scan targets.
Patch Management Applic- ations	Lists all the installed patch management applications, detected on your scan targets during a scan.
Web Browser Applications	Contains scanned targets that have Internet browsers installed.
Firewall Applications	Enumerates information on installed Firewall applications on scan targets.
Antiphishing Applications	Lists information of installed antiphishing engines on scan targets.
VPN Client Applications	Includes information on installed Virtual Private Network clients on scan targets.
Peer-To-Peer Applications	Shows installed Peer–To–Peer applications on scan targets.

# System Information

Click **System Information** to view all details related to the operating system installed on a target machine. Table below describes the system information groups:

Category	Information	Identify
Shares	<ul> <li>Share name</li> <li>Share remark (extra details on the share).</li> <li>Folder which is being shared on the target computer</li> <li>Share permissions and access rights</li> <li>NTFS permissions and access rights.</li> </ul>	<ul> <li>&gt;&gt; Users sharing entire hard-drives, shares that have weak or incorrectly configured access permissions.</li> <li>&gt;&gt; Start-up folders, and similar system files, that are accessible by unauthorized users, or through user accounts, that do not have administrator privileges, but are allowed to execute code on target computers.</li> <li>&gt;&gt; Unnecessary or unused shares.</li> </ul>
Password Policy	<ul> <li>» Minimum password</li> <li>length</li> <li>» Maximum password</li> <li>length</li> <li>» Minimum password</li> <li>expiry date</li> <li>» Force logoff</li> <li>» Password history.</li> </ul>	<ul> <li>Incorrectly configured lockout control</li> <li>Password strength enforcement policies.</li> </ul>
Security Audit Policy	<ul> <li>» Audit account logon events</li> <li>» Audit account man- agement</li> <li>» Audit directory service access</li> <li>» Audit logon events</li> <li>» And more</li> </ul>	<ul> <li>Security holes or breaches.</li> <li>NOTE         To view Security Audit Policy, enable auditing on target computers. For more information, refer to Enabling security audit policies (page 100).     </li> </ul>
Registry	<ul> <li>Registered owner</li> <li>Registered organization</li> <li>Product name</li> <li>Current build number.</li> </ul>	Hardware and software settings such as which drivers and applications will be automatically launched at system startup.

Category	Information	Identify
NETBIOS Names	<ul> <li>» Workstation service</li> <li>» Domain name</li> <li>» Domain controllers</li> <li>» File server service.</li> </ul>	<ul><li>» Rogue computers</li><li>» Wrong configurations.</li></ul>
Groups	<ul> <li>Account operators</li> <li>Administrators</li> <li>Backup operations</li> <li>Guest.</li> </ul>	<ul> <li>&gt;&gt; Wrong configurations</li> <li>&gt;&gt; Security flaws due to rogue or obsolete user groups.</li> </ul>
Users	<ul><li>» Full name</li><li>» Privilege</li><li>» Flags</li><li>» Login.</li></ul>	» Rogue, obsolete or default user accounts.
Logged On Users	» List of logged on users.	<ul> <li>Authorized and unauthorized users currently logged on computers.</li> </ul>
Sessions	<ul> <li>Lists hosts remotely con- nected to the target com- puter during scanning.</li> </ul>	» Authorized and unauthorized remote connections.
Services	» List of active services.	» Rogue or malicious processes; redundant services.
Processes	» List of active processes.	» Rogue or malicious processes.
Remote TOD (time of day)	» Time of remote work- station, server or laptop.	<ul> <li>Time inconsistencies and regional settings</li> <li>Wrong configurations.</li> </ul>

## 4.4.2 Loading results from the database

By default, saved scan results are stored in a database. GFI LanGuard stores the results data of the last 10 scans performed per scanning profile. You can configure the number of scan results that are stored in a database file. For more information, refer to <u>Configuring Database Maintenance Options</u> (page 236).

To load saved scan results from the database backend or from XML files:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button > File > Load Scan Results from > Database...

arget	Profile	⊽ Date	Completed	Notes
file:C:\Users\John	Full Scan	28/11/2011 20:37:	Yes	
192.168.11.11-192	Full Scan	28/11/2011 20:37:	No	
localhost	Full Scan	28/11/2011 20:37:	No	
localhost	Full Scan	28/11/2011 20:26:	Yes	
localhost	Full Scan	01/06/2011 20:33:	Yes	
domain:primary do	Full Scan	25/05/2011 23:39:	Yes	
localhost	Full Scan	25/05/2011 23:34:	Yes	
localhost	Full Scan	25/05/2011 23:33:	Yes	
localhost	Full Scan	25/05/2011 21:51:	Yes	
file:customgroup_2	Full Scan	25/05/2011 21:51:	Yes	
domain:primary do	Full Scan	25/05/2011 21:34:	Yes	
Iocalhost	Full Scan	25/05/2011 21:34:	No	

Screenshot 111: Reloaded scan results

3. Select the saved scan result and click **OK** 

4. Analyze loaded results. For more information on how to interpret results. refer to the following sections:

- » Vulnerability Assessment
- » Network and Software Audit.

## 4.4.3 Saving and loading XML results

Scan results are an invaluable source of information for systems administrators. GFI LanGuard results are stored in a SQL Server<sup>®</sup> or a Access<sup>™</sup> database. In addition, scan results can also be exported to XML.

To save scan results to XML file:

1. Launch GFI LanGuard.

2. Perform a manual scan. For more information, refer to Manual scans (page 96).

3. Once the scan is completed, click GFI LanGuard button > File > Save Scan Results.

4. Locate the destination where you want to save the XML and click **Save**.

To load saved scan results from an XML file:

1. Click the GFI LanGuard button > File > Load Scan Results from > XML File...

- 2. Locate the scan results to load and click  $\mathbf{OK}$
- 3. Analyze loaded results.

#### NOTE

For more information on how to interpret results, refer to the following sections:

- » Vulnerability Assessment
- » Network and Software Audit

# 4.5 Remediate Vulnerabilities

GFI LanGuard enables you to manually or automatically fix vulnerabilities on network computers. Use the information in this topic to learn how to configure and manage remediation operations to maintain a high level of security amongst your scan targets.

Topics in this section:

4.5.1 Automatic Remediation	162
4.5.2 Manual Remediation	185
4.5.3 Sending Mobile Device Notifications	197

### 4.5.1 Automatic Remediation

Automatic-Remediation enables you to automatically download and deploy missing patches as well as uninstall unauthorized applications during scheduled operations, automatically.

#### IMPORTANT

Auto-remediation and un-installation of un-authorized applications only work with scanning profiles that detect missing patches and/or installed applications.

Automatic Remediation tasks:

- » Review Auto-Remediation Considerations
- » Configure Missing Updates Auto-Deployment
- » Configure Unauthorized Applications Auto-Uninstall
- » Configure Auto-Remediation options
- » Configure Wake-on-LAN on client machines
- » Configure End-User reboot and shut down options
- » Define Auto-Remediation Messages
- » Configure Agents Auto-remediation
- » Configuring Software Categories

#### Auto-remediation notes

Before enabling and configuring auto-remediation options, review the following notes about:

#### Installing software

Always test patches in a test environment before deployment.

By default, Microsoft<sup>®</sup> updates are not enabled for automatic deployment. Manually approve each patch (as it is tested) or set all Microsoft<sup>®</sup> updates as approved.

#### Uninstalling software

To uninstall software, a 3-stage process is required in order to identify whether the selected application supports silent uninstall:

Stage	Description
Stage 1	Select the application to auto-uninstall.
Stage 2	Ensure that application supports silent uninstall. Test this by trying to remotely uninstall the application. This is the val- idation process.
Stage 3	Setup a scheduled audit that will remove the unauthorized application. This is done automatically (using agents) or manu- ally (agent–less approach).

Auto-remediation and un-installation of un-authorized applications only work with scanning profiles that detect missing patches and/or installed applications.

### Configuring missing updates auto-deployment

GFI LanGuard ships with a patch auto-deployment feature that enables you to deploy missing patches and service packs in all languages supported by Microsoft<sup>®</sup> products. GFI LanGuard also supports patching of third party (Non-Microsoft<sup>®</sup>) patches. For a complete list of supported third party applications refer to http://go.gfi.com/?pageid=3p\_fullreport. Refer to the following section for information about:

- » Enabling Patch Auto-Deployment
- » Configuring Patch Auto-Deployment advanced options
- » Configuring Patch Auto-download settings

#### Enabling Patch Auto-Deployment

To configure patch auto-deployment:

#### 1. Click on **Configuration** tab > **Software Updates** > **Patch Auto–Deployment**.

2. In the right pane, select the method for approval.

#### Manual approval

Use the **Manual approval** tab to approve patches one by one. This is achieved by using the list of unapproved patches grouped by vendor or severity that you want to be approved.

🔮 GFI LanGuard							
💷 🔽 😚   🔶   🌧 🛛 Dashb	ooard Scan Remediate	Activity Monito	or Reports	Configuration	Utilities	• 🕐	Discuss this version
Configurations:	Patch Auto-I The Patches Auto-De	Deploymer ployment option e	nables you to sele	ct which patches a	are approved for	automat	ic patch deployment.
Abolice Devices     Software Categories     Applications Inventory     Auto-Uninstall Validation	Manual Approval     Approve only the patches t	Automatic App	roval	cause issues.			
Software updates     Soft	Group by: Vendor				▼ Find		Clear Options
	⊕ 😵 Adobe Systems, Inc ⊕ 😼 Apache Software Fo	Drag	a column header h	nere to group by th	nat column		
🖃 🏂 General	🕀 😡 Apple	B	Approval	Bulletin ID	Date	posted	
····· T Version Information	🗄 😼 Apple Computer, Inc	. 0	Click to configure	iAdProducer	-4.0.1.0 2013-	06-19	iAd Producer (4.0.1.)
: 🐞 Licensing	🗄 😼 Box, Inc.	0	Click to configure	WNMP564	2013-	06-19	Winamp 5.64
	Lecho Corporation	ē	Click to configure	JavaForOSX	(-1.0 2013-	06-18	Java for OS X 2013-(
Common Tasks:	Foxit Corporation	ĨÕ	Click to configure	JavaForMac	OSX10 2013-	06-18	Java for Mac OS X 10
Options		ě	Click to configure	TSVN180244	401 2013-	06-18	TortoiseSVN 1.8.0 64
	Igor Paviov	ration 0	Click to configure	TSVN180244	401 2013-	06-18	TortoiseSVN 1.8.0
Actions:	H-M Microsoft		Click to configure	PdfXCV2521	2013-	06-18	PDF-XChange Viewer
	Hozilla	ě	Click to configure	PdfXCV2521	10 2013-	06-18	PDF-XChange Viewer
Approve selected patches	E IN Nullsoft, Inc.	ě	Click to configure	PdfXCV2521	10 2013-	06-18	PDE-XChange Viewer
Clear approval configuration	🗉 😼 Opera Software	- ă	Click to configure	JAVA7025	2013-	06-18	Java Runtime Enviror
Show Bulletin Info	🕀 📢 Oracle	ă	Click to configure	1AVA7025	2013-	06-18	lava Runtime Enviror
	🗄 😼 pdfforge.org	ă	Click to configure	GC 27 0 1	453 116 2013-	06-18	Google Chrome 27.0
	🕀 😼 RARLAB	ă	Click to configure	E7Client371	2013	06-18	FileZilla Client 3 7 1
	RealNetworks		Create 40004		2015	00 10	Thezand cherre 5.7.1
	Riverbed Technolog	JY	Count: 12234		1		
	🗉 🗤 Skype Limited			III			
	Approved patches are depl	oyed automatically	after agent or sche	eduled scans with e	enabled patch au	to-depla;	yment.

Screenshot 112: Patch auto-deployment: Manual approval

### NOTE

Key-in a search criteria and click **Find** to search for a specific application.

#### Automatic approval

The **Automatic approval** tab enables you to specify which group of patches are automatically approved according to a category for a particular vendor.

🌒 GFI LanGuard							[	- • <del>x</del>
📃 📰 👌   🗲   🔿 🛛 Dashl	board Scan Remediate	Activity Monitor	Reports	Configuration	Utilities	; 🕐 -	Discuss this	version
Configurations: Agents Management Conning Profiles Scheduled Scans Mobile Devices Coffware Categories Configurations	Patch Auto The Patches Auto-	Deployment Deployment option enab	les you to select	which patches a	re approve	d for automati	ic patch deployn	nent.
Grand Auto-Uninstall Validation	Enable automatic approval for	the following updates			Security U	lpdates		Critical
Patch Auto-Download	Pro	duct	Critic Seve	enity	ortant erity	Moderate Severity	Low Severity	Updates
	Adobe Systems, Inc.	adation			1			
General	Apple	Idation						
🔓 Licensing	Apple Computer, Inc.				1			
Common Tasks:	Decho Corporation				1			
Options	Foxit Corporation     Google Inc.		<b>V</b>					
1.0	Igor Pavlov							
Actions:	H. Malwarebytes Corpora	tion						
Disapprove selected patches	🕀 🔲 Mozilla							
Show Bulletin Info	Opera Software				1			
	Oracle     Oracle				1			
	⊕ RARLAB							
	RealNetworks							
	Disable automatic approva	III al for major version upgrad	les		J			
								.:

Screenshot 113: Patch auto-deployment: Automatic approval

## Configuring Patch Auto-Deployment advanced options

To configure auto-remediation:

1. Click **Configuration** tab > **Software Updates** > **Patch Auto–Deployment** and from **Common Tasks**, click **Advanced options**.

0	otions			<b>—</b> ×
	General			
	Patch auto-dep	oloyment options		
	Send an email whe	n new patches or serv	ice packs are available	e
	Show:			
	<ul> <li>Patches for pro</li> </ul>	oducts that were detec	ted in the network	
			Grand	
		UK	Cancel	Apply

Screenshot 114: Patch Auto–Deployment Advanced Options

2. Configure the following options:

Option	Description
Send an email when new patches or service packs are available.	Send an email when new patches are identified.
Show all patches:	Displays all the identified patches .
Show patches for products that were detected in the network:	Displays only the patches identified on the selected network.

3. Select the appropriate check boxes and click **OK** to save changes.

#### Configuring Patch Auto-download settings

GFI LanGuard ships with a patch auto-download feature that enables the automatic download of missing patches and service packs in all languages supported by Microsoft<sup>®</sup> products. In addition, you can also schedule patch auto-download by specifying the time-frame within which the download of patches is performed.

To configure patch auto-download:

#### 1. Click **Configuration** tab > **Software Updates > Patch Auto–Download**.

2. From the right pane, click the link.

Patch Auto-download Properties	3
General Patch Repository Timeframe	
Configure patches auto-download options.	
Enable patch auto-download	
Select patches to download:	
All patches NOTE: Download all patches for deployment. If you want to download patches only for a specific vendor, product line or language use the configure option.	
Configure	
Only needed patches NOTE: Download only required patches as determined by previous scans	
Number of download threads: 5	
OK Cancel Apply	

Screenshot 115: Configuring Patch Auto-download Properties

3. In the **General** tab, select between **All patches** or **Only needed patches**.

4. In the **All patches** tab click **Configure** to restrict auto-download of patches for configured languages.

	▼ Find Clear
oduct name	Languages
Adobe Systems, Inc.	
Apache Software Foundation	
Apple	
AudacityTeam.org	
Box, Inc.	
CanneverbeLtd.	
CoreFTP	
🗹 Decho Corporation	
🗹 Don Ho	
dotPDN LLC	
Foxit Corporation	
Google Inc.	
🗹 Igor Pavlov	
M ImgBurn	
🗹 IrfanSkiljan	
Malwarebytes Corporation	

Screenshot 116: Configuring Patch Auto-download - All Patches Properties

### NOTE

Selecting **All patches > Configure**, enables administrators to manually select the Microsoft<sup>®</sup> patches to download, regardless of whether these are required for deployment. The **Only needed patches** option downloads only patches required for deployment.

Patch Auto-download Properties	×
General Patch Repository Timeframe	
Set repository path for software updates and service packs.	
Download directory:	
C:\Program Files\GFI\LanGuard 11\Repository	
☑ Use files downloaded by WSUS when available	
Specify the path of the <u>W</u> SUSContent folder:	
Remove patches that have not been used for 1 year -	
OK Cancel Apply	

Screenshot 117: Patch Repository settings

4. To change the location where the downloaded patches are stored click the **Patch Repository** tab and specify the required details.

5. Select Use files downloaded by WSUS when available, if you are using an existing setup of WSUS.

6. Select **Remove patches that have not been used for** and select the time duration if you want to remove files that have not been used for remediation in the specified time interval.

7. To change the time frame during which patch downloads are performed, click **Timeframe** tab and specify the required details.

#### 8. Click Apply and OK

#### Configuring unauthorized applications auto-uninstall

Application auto–uninstall entails that applications marked as unauthorized for specific scanning profiles are first validated for a successful uninstall on a test machine. Subsequently a scheduled scan based on the scanning profile for which the application is marked as unauthorized, is configured to auto–uninstall applications.

GFI LanGuard applications inventory provides a list of all applications detected during past scans. The list is used to specify unauthorized applications. You can also manually add applications to the list. You can do this by specifying the entire name as well as a partial name, specify generic names or part of an application name. GFI LanGuard automatically scans the list of applications and detects partial names. Refer to the following sections for information about:

- » Setting an application as unauthorized
- » Adding new applications to the unauthorized list
- » Validating unauthorized applications for auto-uninstall
- » Managing applicable scheduled scans

#### Setting an application as unauthorized

#### 1. Click on **Configuration** tab > **Applications inventory** sub-node.

2. From the list of applications detected on the right, double click the application to set as unauthorized.

Configure application wizard
Step 1 of 2: Mark application as unauthorized Select the profiles under which the application will be unauthorized
Configure application: Microsoft SQL Server Management Studio Express (Version: 9.00.2047.00, Publisher: Microsoft Corporation)
Unauthorized applications are classified in scan results as 'High Security Vulnerability'
To mark this application as unauthorized select the scanning profiles which will classify this software as 'High Security Vulnerability'
Scanning profiles:
Full Scan
Full Scan (Slow Networks)
Software Audit
System Information
Tell me more     < Back     Next >     Cancel

Screenshot 118: Unauthorized application

3. Select the scanning profile for which this application will be set as unauthorized and click Next.

4.GFI LanGuard can associate partial names with entries already in the list. As a result, the system will prompt you to confirm whether to apply the same changes also to applications partially have the same name.

5. Click **Finish** to finalize settings.

Adding new applications to the unauthorized list

#### 1. Click **Configuration** tab > **Applications inventory** sub-node.

#### 2. From Common Tasks, click Add a new application.

3. In the welcome screen, click **Next**.

Add unauthorized application wiza	rd	
Step 1 of 4: Specify application Specify a generic application n	n details name and optional details such as publisher and version	0
Specify a complete or partial a	application name by which this application can be identified:	
Application name	Application NAme	
Note: Partial application	names are accepted.	
Optionally you can provide the	e following details:	
Version Number	1.0	
Publisher	Publisher Name	
Itell me more	< Back Next >	Cancel

Screenshot 119: Applications inventory wizard

- 4. Specify application name. Optionally provide the version number and publisher name. Click Next.
- 5. Select the scanning profiles that will detect unauthorized applications (Example: Full Scan) and click Next.
- 6. Specify whether changes made will effect applications, which have partial/full name match. Click **Next** to continue.

7. Review the information and click **Finish**.

#### Validating unauthorized applications for auto-uninstall

Application auto–uninstall validation enables you to validate the uninstallation procedure for the applications which are to be automatically uninstalled by GFI LanGuard. This is a requirement prior to the actual uninstallation process and no applications are un–installed during scans unless verified.

#### 1. Click **Configuration** tab > **Applications Inventory** > **Auto–Uninstall Validation**

🌒 GFI LanGuard							
📃 🔹 🚯 🛛 🗲 🗠 🔶 🕞 Dashbo	ard	Scan	Remediate	Activity Monitor	Repor	ts Configuratic»	🕖 🔹 Discuss this version
Configurations:	C			n Auto-Uninst	all Va		a automatically uninetalled by GEI
Scheduled Scans     Mobile Devices     Software Categories	1	Valida	anGuard.	applications for a	utomatic	uninstall	
Applications Inventory <u>Auto-Uninstall Validation</u> Software Updates	Ū	Drag a	o column header h	ere to group by that c	olumn	1	
Patch Auto-Deployment		ß	Validation status		Δ	Version	Application name
		2	Validation pending	) (will not be uninstalle	d)	11.1.102.55	Adobe Flash Player 11 ActiveX
		1	Validation pending	) (will not be uninstalle	d)	7.1	FastStone Capture 7.1
General			Validation pending	y (will not be uninstaller	1)	14.0.4763.1000	Microsoft Office Standard 2010
Manage applicable scheduled scans			Count-3				
Go to: Scheduled scans			count-5				
Actions: Validate selected application	2	Review	r agents and so formation	"" Validatio cheduled scans tha Manage	n fails on s t will aut applicable	ome of your applications o-uninstall validated agents Ma	<u>? Let us know</u> Validate  unauthorized applications  nage applicable scheduled scans
		To mark	applications det	ected during past sca	ns as unau	uthorized click on Appli	cations Inventory node.

Screenshot 120: Application auto-uninstall validation

2. From the right pane, select an application to validate and click Validate.

3. In the Application auto-uninstall validation wizard, click Next.

4. Select the computer where to test the application auto-uninstall and click Next.

5. Provide the authentication details for the validation operation and click **Next**.

6. Review the Auto–uninstall validation wizard information and click Start.

#### Managing applicable scheduled scans

The **Manage applicable scheduled scans** button enables you to review or edit scheduled scans, which will perform the validated applications auto install. To manage a scheduled scan:

1. From the Auto–Uninstall validation pane, click Manage applicable scheduled scans.

2. From, Manage applicable schedule scans dialog, click one of the options described below:

Option	Description
Edit selected scan	Modify the selected schedule scan. For more information, refer to <u>Editing scheduled scan settings</u> (page 107).
Create a new sched- uled scan	Add a new scheduled scan using the new scheduled scan wizard. For more information, refer to <u>Creating</u> <u>a scheduled scan</u> (page 101).
View all scheduled scans	Manage scheduled scans. For more information, refer to Editing scheduled scan settings (page 107).

### Configuring auto-remediation options

To edit the general deployment options:

- 1. Launch GFI LanGuard.
- 2. From the computer tree, right-click a computer/computer group and select Properties.

SERV08-06 Properties	×
General Agent Status Attributes Relays	
Agent deployment status Agent status: Installed	
Deploy agent Uninstall agent	
Agent activity settings Audit host computers every day at 12:00.	
Change scan schedule	
Scanning profile:	
Full Scan 👻	
Auto remediation settings	51
Auto remediation is: OFF	
Change settings	
OK Cano	el

Screenshot 121: Computer properties

3. Select the Agent Status tab and from Auto remediation settings, click Change settings...

Auto remediation settings	×
General	
Auto-Remediation enables GFI LanGuard to automatically download and install missing updates, service packs and update rollups, and uninstall unauthorized applications on the scanned computers.	
After receiving scan results from the agent:	
Download and deploy missing updates	
Download and deploy missing service packs and update rollups	
Uninstall unauthorized applications	
Configure auto-remediation options	
It is recommended to have System Restore on for the system drive on the target computers.	
Remediation actions are conducted from the GFI LanGuard console computer where the updates are downloaded and distributed to remediation targets.	
There are updates that are not approved for auto-deployment.	
OK Cance	

Screenshot 122: General auto-remediation settings

4. Select the action to take after receiving scan results from the agent. Click **Configure auto-remediation options...** 

Remediation options	x
Before Deployment After Deployment Advanced	
Warn user before deployment (show a message)	
Messages	
Stop services before deployment	
Services	
Copy software to deploy to target computers via:	
Administrative shares	
Custom share:	
OK Cance	el

Screenshot 123: Before deployment options

# 5. Configure **Before Deployment** options described below:

Option	Description
Wake up offline com- puters	Start computers if they are turned off. For more information, refer to <u>Configuring Wake-on-LAN on scan</u> targets (page 178).
Warn user before deploy- ment (show message)	Displays a message on the target machine to warn the user before deploying software.
Wait for user's approval	Wait for user's approval before deploying software.
Messages	Click <b>Messages</b> to select the end-user's computer language and define the warning message. For more information, refer to <u>Configuring auto-remediation messages</u> (page 180).
Administrative shares	Make a copy of the software on the default network shares.
Custom shares	Make a copy of the software in a custom share. Key-in the folder name in the text box.
Remember settings	Saves your configured settings and uses them during the next remediation job.

Remediation options
Before Deployment After Deployment Advanced
Reboot/shut down options:
O not reboot/shut down the computers
Reboot the target computers (only if required)
Reboot the target computers
Shut down the target computers
Reboot/shut down schedule:
Immediately after deployment
At the next occurrence of 14:37:36 in Sunday, Mon V
When between 14:37:36 → and 14:37:36 →
on Sunday, Mon 🔻
Let the user decide     Preview
Show notification before shut down for 5 immutes with message:
Delete copied files from remote computers after deployment
Run a patch verification scan after deployment
OK

Screenshot 124: After deployment options

# 6. Click After Deployment tab. Configure After Deployment options described below:

Option	Description
Do not reboot/shut- down the com- puter	Leave scan target(s) turned on after remediating vulnerabilities, even if patches require a reboot to be installed completely.
Reboot the target computers only if required	GFI LanGuard reboots a target machine only if at least one patch requires a reboot. If no patches require a reboot, a reboot is not executed.
Reboot the target computers	Always reboots computers after remediating vulnerabilities.
Shut down the tar- get computers	Target machine will shut down after deploying software.
Immediately after deployment	Reboots/shuts down computers immediately after remediating vulnerabilities.

Option	Description
At the next occur- rence of	Specify the time when the computers reboot/shut down.
When between	This option enables you to specify time and day values. If the remediation job is completed between the spe- cified times (start time and end time), the computer(s) will reboot/shut down immediately. Otherwise, the reboot/shut down operation is postponed until the next entrance into the specified time interval.
Let the user decide	Click <b>Preview</b> to view a screenshot of the dialog in the user manual. This dialog opens on the end-user's com- puter after remediating vulnerabilities. For more information, refer to <u>Configuring end-user reboot and shut</u> <u>down options</u> (page 179).
Show notification before shut down for	Shows a custom message on the end user's computer for a specified number of minutes before reboot/shut down.
Delete copied files from remote com- puters after deploy- ment	Deletes the downloaded patches / service packs after they are deployed.
Run a patch veri- fication scan after deployment	Verifies deployed patches, scanning target when the deployment process is complete.
	<ul> <li>NOTE</li> <li>&gt;&gt; If the user chooses to reboot computer after the deployment, the Patch Verification Scan will occur after the machine was restarted.</li> <li>&gt;&gt; If the user chooses to shut down the computer after deployment, the computer will be restarted and the Patch Verification Scan will shut down the computer.</li> </ul>
Remember set- tings	Saves your configured settings and uses them during the next remediation job.

Remediation options
Before Deployment After Deployment Advanced
Number of deployment threads: 5 (max 10) WARNING: Deploying with more than 5 threads may render the UI unresponsive until the deployment operation is complete.
Deployment timeout (seconds): 600
Deploy patches under the following administrative account (domain/user or user@FQDN format):
Account name: DOMAIN\administrator
Password:
Note: Only select this option if you want to run the installation packages on the target computers under an account other than the Local System account. If you need to select this option, make sure that the specified account has the Log on as service privilege on the target computers.
OK Cancel

Screenshot 125: Advanced deployment options

7. (Optional) Select **Advanced** tab. Configure the options described below:

Option	Description
Number of deployment threads	Specify the maximum number of processing threads allowed to start when deploying software updates. The number of threads determines the number of concurrent deployment operations an agent can handle.
Deployment timeout (seconds)	Specify the time (in seconds) an agent attempts to deploy an update. If the specified time is exceeded, the agent stops the unresponsive deployment and starts a new deployment thread. This feature enables you to stop the process thread so that if an update is taking longer than normal deployment time, the remediation operation continues without jeopardizing the rest.
Deploy patches under the fol- lowing admin- istrative account	Select this option to use a custom administrative account to log and deploy patches on target machines. The account selected must have Log–on as service privilege on the target computers. For more information on how to configure an account with log–on as service privilege, refer to http://go.gfi.com/?pageid=LAN_LogonService.

# 8. Click **OK** to apply changes.

# Configuring Wake-on-LAN on scan targets

Wake-on-LAN enables GFI LanGuard to wake machines from the following states:

- » Powered off
- » Sleep
- » Hibernated

#### IMPORTANT

If you have routers between the client machine and the GFI LanGuard machine, the router and the GFI LanGuard machine must be configured to allow Wake-on-LAN broadcast packets on UDP port 9.

The motherboard and the network interface card of the computer running GFI LanGuard, must support Wake-on-LAN. To configure Wake-on-LAN on a Windows<sup>®</sup> operating system:

- 1. Click Start, right click Computer and select Manage.
- 2. From the left panel, expand System Tools and click Device Manager.
- 3. Right click the Network Interface Card and select Properties.
- 4. From the **Power Management** tab, select the following options:
  - Allow this device to wake up the computer
  - Only allow a magic packet to wake the computer

#### Note

Magic Packet is the wake up signal that is sent by GFI LanGuard to the scan target network card.

#### 5. Click OK

Once the **Network Interface Card** is configured, run a **FULL** scan on the client machine. This enables GFI LanGuard to gather the required information from the client machine. For more information, refer to Manual scans (page 96).

### Configuring end-user reboot and shut down options

When configuring **After Deployment** settings, in **Auto-remediation options**, you can configure GFI LanGuard to notify and let the user decide when to reboot or shut down the computer after completing an administrative task. The below dialog opens on the user's computer and enables him/her to select one of the following options:

GFI LanGuard					
Administrative tasks have been performed by GFI LanGuard! Your computer needs to be restarted for the tasks to complete.					
Restart now					
Remind me in	1 minutes				
Restart on	8/10/2011 🗐 🔻 1:58:39 PM 🛓				
🔘 Don't bother me again					
	ОК				

Screenshot 126: Reboot/shut down options

The table below describes the available options:

Option	Description
Restart now	Reboots/shuts down the computer immediately after completing an administrative task.
Remind me in	Specify a time interval (in minutes), when to remind the end-user.
Restart on	Specify the date and time when the machine reboots/shuts down.
Don't bother me again	The user is not prompted again.

### Configuring auto-remediation messages

GFI LanGuard enables you to automatically display warning messages before and after remediation operations. These messages are displayed on the end-users' computer and in some cases, allows them to select after deployment options, or notify them about the operations to be carried out. You can customize predefined messages and set the language according to the scan target's computer language.

To configure warning messages:

1. Launch GFI LanGuard.

#### 2. Click **Remediate tab > Remediation Center**.

#### 3. From Remediation Center, select a remediation action, such as Deploy Software Updates.

🜒 GFI LanGuard						- • •	
🔲 🔽 👌 🧲 🛛 🔿 🛛 Dashboard	Scan Rem	ediate Activi	ty Monitor	Reports Conf	igur.» 🕐 🔹 Discuss	this version	
Entire Network - 5 computers							
Filter Group Search	Nemediat	on Center	👂 Remediat	ion Jobs			
Entire Network     Deploy Software Updates     Use this option to deploy missing software updates detected on your network.							
List of missing updates for current selection (Entire Network - 5 computers)							
Image: split align: split a					Find	Clear	
emmanueltino@gfi.com	D	Bulletin	Severity	Mate posted ♥	Title	Vendor	
▶ 💇 fionabrown@gfi.com 🛛 🧕	🗏 🗹 Sec	urity Update (2	.06)				
🕨 💇 jasonuhr@gfi.com 🛛 🤟	÷ 💌 😫	MS12-042	Important	2012-06-12	Security Update for	Microsoft	
) 🔮 johnparker@gfi.com 📒	+ 💌 🤡	MS12-041	Important	2012-06-12	Security Update for	Microsoft	
🕨 🔮 josephmahler@gfi.com 🗧	+ 💌 🤡	MS12-041	Important	2012-06-12	Security Update for	Microsoft	
🕨 🛒 simonemann@gfi.com 🧧	+ 💌 🤡	MS12-041	Important	2012-06-12	Security Update for	Microsoft	
	+ 💌 🥸	MS12-042	Important	2012-06-12	Security Update for	Microsoft	
	🕀 💌 🤡	MS12-037	Moderate	2012-06-12	Cumulative Security	Microsoft	
Common Tasks: ¥	🕀 💌 🤡	MS12-037	Critical	2012-06-12	Cumulative Security	Microsoft	
Manage agents	- F 💌 😣	MS12-037	Moderate	2012-06-12	Cumulative Security	Microsoft	
Add more computers		Count=301				~	
Scan and refresh information now	<((					>	
Custom scan			Tota	al selected: 220 softwa	are updates	emediate	
Set credentials Deploy agent			1010				

Screenshot 127: Remediation Center - Deploy Software Updates

#### 4. Click Remediate.
Deploy software updates	<b>×</b>
Review current deployment options	
<ul> <li>Deploy immediately</li> <li>Deploy on 04/07/2012 at 10:17:31</li> </ul>	
Credentials: - currently logged on user - use per computer credentials when available	<u>Customize</u>
Before deployment options: - warn user before deployment (show a message) - copy software to deploy to target computers via administrative share	<u>Customize</u>
After deployment options: - do not reboot/shut down the computers - delete copied files from remote computers after deployment - run patch verification scan	<u>Customize</u>
Advanced options	OK Cancel

Screenshot 128: Deployment options dialog

5. Click Advanced options.

Remediation options
Before Deployment After Deployment Advanced
Wake up offline computers
<ul> <li>Warn user before deployment (show a message)</li> <li>Wait for user's approval</li> </ul>
Messages
Stop services before deployment
Services
Copy software to deploy to target computers via:
Administrative shares
Custom share:
Remember settings OK Cancel

Screenshot 129: Before Deployment Message options

6. From the **Remediation options** dialog, click **Before Deployment tab > Messages...** 

Warning messages	×
General	
Customize the messages shown to the user during deployments according to target computer's language.	
Language: English 💌	
Messages	h I I
When not waiting for user approval:	
Waming!!! GFI LanGuard is performing administrative tasks initiated by \$computername\\$username! Your computer may need to restart for the tasks to complete!	
When waiting for user approval:	
Warning!!! GFI LanGuard is performing administrative tasks initiated by \$computermame\\$username! Your computer may need to restart for the tasks to complete. Please save your work and select OK to continue.	
· · · · · · · · · · · · · · · · · · ·	
Apply OK Cancel	

Screenshot 130: Customizing warning messages

7. Customize any of the following options:

Option	Description
Language	Select the message language.
When not waiting for user	Use or customize the pre-defined message that launches on the end user's computer when GFI
approval	LanGuard is not waiting for approval.
When waiting for user	Use or customize the pre-defined message that launches on the end user's computer when GFI
approval	LanGuard is waiting for approval.

### 8. Click Apply and OK

### Configuring Agent auto-remediation

In an agent-based environment, automatic remediation options can be set for every deployed agent. This enables you to configure every agent with specific auto-remediation options to suit your requirements.

To configure agent auto-remediation actions:

1. Launch GFI LanGuard.

### 2. Click **Configuration** tab > **Agents Management**.

3. From the right pane, right-click an agent and select **Properties**.

4. Select the Agent Status tab and in the Auto remediation settings section click Change Settings.

5. Select **Download and deploy missing updates** to enable automatic remediation for missing patches.

6. Select **Download and deploy missing service packs and update rollups** to enable automatic remediation for missing service packs.

7. Select **Uninstall unauthorized applications** to enable automatic remediation for unauthorized applications.

8. (Optional) Click **Configure auto-remediation options...** to further customize remediation options. For more information, refer to <u>Configuring auto-remediation options</u> (page 173).

9. Click **OK** 

## 4.5.2 Manual Remediation

Apart from automatically downloading patches and service packs, GFI LanGuard can also deploy these updates network–wide as well as recall any patches that were deployed.

Both patch deployment and patch rollback operations are managed by an agent service that manages all file transfers between GFI LanGuard and remote targets. This service is installed automatically on the remote target computer during the patch deployment process.

Manual Remediation tasks:

- » Review Manual Remediation important notes
- » Learn more about the Remediation Center
- » Deploy Software Updates
- » Uninstall Software Updates
- » Deploy custom software
- » Uninstall Applications
- » Be protected against Malware
- » Connect remotely to a machine using GFI LanGuard.
- »

Sending Mobile Device Notifications

### Manual remediation notes

1. While an infrequent occurrence, patches may be recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates such as conflict issues with present software or hardware. Examples of updates recalled by the manufacturer include patches MS03–045 and MS03–047 for Exchange that were released by Microsoft<sup>®</sup> on October 15, 2006.

2. Ensure that the NetBIOS service is enabled on the remote target computer. For more information, refer to Configuring NetBIOS (page 299).

3. A complete list of Microsoft products for which GFI LanGuard can download and deploy patches is available at http://go.gfi.com/?pageid=ms\_app\_fullreport

4. Non-Microsoft software update patches supported by GFI LanGuard is available at http://go.gfi.com/?pageid=3p\_fullreport

5. The complete patch management process, from detection to remediation, is supported for most of the non-Microsoft products. There is, however a small set of products that GFI LanGuard cannot update and which GFI LanGuard functionality is limited to detecting missing updates. Examples of these products are

- » Apache Webserver
- » MySQL
- » VMware Player and Workstation

6. GFI LanGuard can be set to automatically download missing patches and service packs discovered during a network security scan. For more information, refer to <u>Configuring missing updates auto-deployment</u> (page 163).

### Using the Remediation Center

The **Remediation Center** enables you to fix security issues found during a network scan by deploying or uninstalling applications from target machines. To access the **Remediation Center**, select **Remediate** tab **> Remediation Center**.



Screenshot 131: Remediation center

From the left panel, expand and locate a computer or a domain to perform remediation actions. The available remediation actions are described below:

Action	Description
Deploy Software Updates	Deploy missing patches discovered when auditing target computers. For more information, refer to <u>Deploying Software Updates</u> (page 187).
Uninstall Software Updates	Uninstall service packs from target computers. For more information, refer to <u>Uninstalling Software</u> <u>Updates</u> (page 189).
Deploy Custom Software	Deploy custom applications and scripts on target computers. For more information, refer to <u>Deploy</u> - ing Custom Software (page 191).
Uninstall Applications	Uninstall applications from target computers. For more information, refer to <u>Uninstalling Custom</u> <u>Applications</u> (page 192).
Malware Protection	Perform Malware protection actions on target computers. For more information, refer to <u>Malware Pro-</u> <u>tection</u> (page 194).
Remote Support via Remote Desktop Con- nection	Connect to a target machine and perform administrative tasks using remote desktop connection. For more information, refer to <u>Using Remote Desktop Support</u> (page 196).

## Deploying Software Updates

Use the **Deploy Software Updates** feature to manually deploy:

- » Missing Service Packs and Update Rollups
- » Missing Security Updates
- » Missing Non-Security Updates.

This feature enables you to specifically select the items you want to deploy and provides you with a detailed description for each.

#### NOTE

To view additional information about an update, right-click on an update and select More details > Bulletin info...

To manually deploy software updates:

- 1. Launch GFI LanGuard.
- 2. Click Remediate tab and expand Deploy Software Updates.

🌒 GFI LanGuard											×
💷 🐨 🚷   ←   →	Dashboard	Scan	Remediate	Activity M	onitor Rep	ports Config	guration Utilit	ies	Ø Discuss	this version	
	0	ا 📎	WORKGR	OUP - 5 cor	nputers						
Filter Group S	Search		Remediation	Center	Remediation	lobs					
											_
Search Entire Network	- 0		Deploy	Software	Updates						
			Use this o	ption to deploy m	issing updates	detected on sele	ected computers.			<ul> <li></li> </ul>	
Group by category											
Group by computer		L	ist of missin	g updates for	r current sel	lection (WOR	KGROUP - 5 co	mputers)			
Search history											
Advanced search							<ul> <li>Find</li> </ul>	Clear			
🖌 💐 Entire Network	<b>i</b> ^	ſ		Bulletin	Severity	Date posted ⊽	Title	Vendor	Size	Applies to	
Nocalhost : W711	8		🗉 📃 Secu	rity Update (25	2)						
🖌 🙀 Local Domain : WORKGROU	р 🖣		🕀 📃 🔮 I	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 Ki	3 Windows	
🕼 W7_07			🕀 📄 🥑 I	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 KE	8 Windows	
🕼 W710			🕀 📄 🥑 I	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 Ki	3 Windows	
🕼 W711	8		🕀 📄 🥑 I	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 KE	3 Windows	
🕼 W712			🕀 📄 🍪 I	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KE	8 Windows	
W802			🕀 📃 🔮 I	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KE	3 Windows	
DOMAIN	li .		🕀 📄 🤣 I	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KE	3 Windows	
Common Tasks:	¥		🕀 📄 🤣 I	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KE	8 Windows	
			🕀 📄 🥥 I	MS13-002	Critical	2013-01-08	Security Updat	Microsoft	582.00 KE	3 Windows	
Manage agents Add more computers			Co	unt=0							
Scan and refresh information now			<[[							)>)	
Custom scan										) di-t-	
Set credentials							No updates	s are currently selec	ted.	remediate	
Deploy agent											

Screenshot 132: Deploying software updates

3. From the computer tree, select the computer/group where to deploy software updates.

4. From the **List of missing updates**, select the updates to deploy.

#### NOTE

Use the search bar to look for specific missing updates or use the filtering options for each column heading to view the required data only.

#### 5. Click Remediate.

Deploy software updates	<b>x</b>
Review current deployment options	
Opploy immediately	
⑦ Deploy on 14/05/2012 ■ at 18:08:30 ➡	
Credentials:	<u>Customize</u>
- currently logged on user	
- use per computer credentials when available	
Before deployment options:	Customize
- warn user before deployment (show a message)	COStornizo
- copy software to deploy to target computers via administrative share	
After deployment options:	Customize
- do not reboot/shut down the computers	
- delete copied files from remote computers after deployment	
Advanced options OK	Cancel

Screenshot 133: Deploy software updates options

6. The **Deploy software updates** dialog, enables you to edit deployment options before starting the deployment operation. Review the options described below:

Option	Description
Deploy imme- diately	Selected by default. Leave selected to deploy missing updates immediately.
Deploy on	Specify a date and time when to deploy missing updates .
Credentials	Provides you with the credentials settings for updates. Click ${f Customize}$ to change settings .
Before deploy- ment options	Provides you with the actions taken before deploying software updates. Click <b>Customize</b> to edit the before deploy- ment message, and the type of share created to transfer updates and scan details files.
After deploy- ment options	Provides you with the actions taken after deploying missing software updates. Click <b>Customize</b> to configure whether the computer(s) reboot, shutdown or display a message to the end-user.
Advanced options	Click <b>Advanced options</b> to configure the: <ul> <li>Number of deployment threads. Maximum = 10</li> <li>Deployment timeout</li> <li>Alternate credentials.</li> </ul> Select <b>Remember settings</b> to reuse the same configuration when running the next deployment job. For more information, refer to <u>Configuring auto-remediation options</u> (page 173).

7. Click **OK** to start deploying updates. You are automatically taken to the **Remediation Jobs** tab where you can monitor the progress of the deployment operation.

## Uninstalling Software Updates

The Uninstall Software Updates feature enables you to manually remove:

- » Installed Service Packs and Update Rollups
- » Installed Security Updates
- » Installed Non-Security Updates.

To manually uninstall software updates:

1. Launch GFI LanGuard.

#### 2. Click Remediate tab and expand Uninstall Software Updates.

🌒 GFI LanGuard									
🔲 🐨 👌 🗧 🚽 🔿 🖉 Dashboa	ard Scan	Remed	liate Activity	Monitor F	Reports Con	figuration Utilit	ies 🔮	) • Discuss	this version
Filter Group Search		WORK(	GROUP - 5 c	omputers	on Jobs				
Search Entire Network		Unir Use th	nstall Softward	are Updat tall software up	es dates currently d	eployed on network.			۲
Group by computer	1	List of ins	talled updates	s for current	selection (W	ORKGROUP - 5 c	omputers )		
Search history			-		-				<u>^</u>
Advanced search						Find	Clear		
🔺 💐 Entire Network	• •		ර Bulletin	Severity	Date posted	⊽ Title	Vendor	Size	Applies to
Nocalhost : W711		🗉 🗹 Se	curity Update (	(252)					
🛛 😰 Local Domain : WORKGROUP 🛛 🖣		🕀 💌 🌾	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 KB	Windows
🕼 W7_07		+ 💌 🌾	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 KB	Windows
🕼 W710		🕀 💌 🌾	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 KB	Windows
🕼 W711		🕀 💌 🌾	MS13-006	Important	2013-01-08	Security Updat	Microsoft	150.69 KB	Windows
🕼 W712		🕀 💌 🌾	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KB	Windows
W802		🕀 💌 🌾	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KB	Windows
Þ 😰 DOMAIN 🗧	h 🗸 👘	± 🗹 🌾	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KB	Windows
Common Taska:	×	+ 💌 🌾	MS13-001	Critical	2013-01-08	Security Updat	Microsoft	246.60 KB	Windows
Common Tasks:	-	+ 💌 🌾	MS13-002	Critical	2013-01-08	Security Updat	Microsoft	582.00 KB	Windows
Manage agents			Count=384						~
Add more computers		<[[			Ш				)>
Scan and retresh information now Custom scan Set credentials Deploy agent						Total selected	l: 252 software update	s 💽 R	emediate

*Screenshot 134: Uninstalling software updates* 

- 3. From the computer tree, select the computer/group where to uninstall software updates.
- 4. From the **List of installed updates**, select the updates you want to uninstall.

#### NOTE

Use the search bar to look for specific installed updates or use the filtering options for each column heading to view the required data only.

#### 5. Click Remediate.

Uninstall software updates	<b>x</b>
Review current deployment options	
O Uninstall immediately	
O Uninstall on 14/05/2012 → at 18:09:45 →	
Credentials:	Customize
- currently logged on user	
- use per computer credentials when available	
Before deployment options:	Customize
- warn user before deployment (show a message)	
- copy software to deploy to target computers via administrative share	
After deployment options:	Customize
- do not reboot/shut down the computers	
- delete copied files from remote computers after deployment	
Advanced options OK	Cancel

Screenshot 135: Uninstall software updates options

6. The **Uninstall software updates** dialog, enables you to edit uninstall options before starting the uninstall operation. Review the options described below:

Option	Description
Uninstall imme- diately	Selected by default. Leave selected if you want to uninstall updates immediately.
uninstall on	Specify a date and time for when updates are uninstalled.
Credentials	Provides you with the credentials settings that are used to uninstall updates. Click <b>Customize</b> to change settings and use alternate credentials.
Before deploy- ment options	Provides you with the actions taken before uninstalling software updates. Click <b>Customize</b> to edit the before deployment message, and shares mode used to transfer updates.
After deploy- ment options	Provides you with the actions taken after uninstalling software updates. Click <b>Customize</b> to configure whether the computer(s) reboot, shutdown or display a message to the end-user.
Advanced options	Click <b>Advanced options</b> to configure the: Number of deployment threads. Maximum = 10 Deployment timeout Alternate credentials. Select <b>Remember settings</b> to reuse them when running the payt deployment operation. For more information.
	refer to Configuring auto-remediation options (page 173).

7. Click **OK** to start uninstalling the selected updates. You are automatically taken to the **Remediation Jobs** tab where you can monitor the progress of the uninstall operation.

## Deploying Custom Software

Apart from security updates and patches, GFI LanGuard also enables you to remotely deploy third party or custom software network–wide. Software that can be remotely deployed includes:

- » Security applications such as antivirus/antispyware solutions and software firewalls
- » Third party software updates and patches such as antivirus/antispyware signature file updates
- » Custom code such as scripts and batch-files
- » Desktop applications such as Microsoft<sup>®</sup> Office 2007 and more.

To specify which software to deploy:

#### 1. Click on **Remediate** tab > **Remediation Center**.

2. From the computer tree, select the computers where the new software will be deployed and click **Deploy Custom Software**.



Screenshot 136: List of software to be deployed

3. Use the options described in below to add the applications to deploy:

Option	Description
Add	Click this button to launch the Add custom software dialog. This dialog enables you to add an application to the list and if required configure parameters.

Option	Description
Edit	Select an application and click this button to launch the Add custom software dialog. This dialog enables you to modify the existing installation parameters.
Remove	Select an application from the list and click this button to remove the application.
Import	Click this button to import the applications parameters from an XML file.
Export	Click this button to export the applications parameters to XML file.

#### 4. Click **Deploy** and configure the options described below:

Option	Description
Deploy immediately	Deploy the selected applications immediately.
Deploy on	Deploy the selected applications on a specific date and time. Configure when to deploy the applications.
Credentials	Select the authentication method to use or specify a username and password. Select <b>Use per computer credentials when available</b> , to use the credentials specified in the computer properties. For more information, refer to <u>Agent</u> <u>properties</u> (page 77).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to <u>Con-figuring auto-remediation options</u> (page 173).
After deploy- ment options	Configure the actions to perform after deploying the selected applications. For more information, refer to <u>Con-figuring auto-remediation options</u> (page 173).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to <u>Configuring auto-remediation options</u> (page 173).

### 5. Click **OK**

6. To view the deployment progress, click **Remediation Jobs** from the right panel.

## Uninstalling Custom Applications

Using this feature, you can control the installed applications, on which computers, and uninstall any unauthorized applications present on network computers.

To uninstall applications:

1. Select **Remediate** tab > **Remediation Center** and click **Uninstall Applications**.

Image: Scan Remediate Activity Monitor Reports Configuratic % (*) * Discuss this version         Image: Scan Remediate Activity Monitor Reports Configuratic % (*) * Discuss this version         Image: Scan Remediate Activity Monitor Reports Configuratic % (*) * Discuss this version         Image: Scan Remediation Center Remediation Jobs         Image: Scan Remediation Center Remediation Jobs         Image: Scan Remediation Center Remediation Scale         Image: Scan Remediation Center Remediation Jobs         Image: Scan Remediation Center Remediation Scale         Image: Scan Remediation Center Remediation Jobs         Image: Scan Remediation Remediation Jobs         Image: Scan Remediation Remediation Jobs         Image: Scan Remediation Remediation Jobs         Image: Remediation Remediation Jobs         Image: Remediation Remediation Jobs         Image: Remediation Remediation Jobs         Image: Remediation Remediation Jobs         Image: Remediation Remediation Jobs         Image: Remediation Remediation Remediation Jobs	🌒 GFI LanGuard		×			
Filter Search   Filter   Group Search   Centre Network   Search Centre Network   Centre Network   Local bonain: WORKGROUP   Total selected: 25 applications   Common Tasks:   Stan and Infersh Information now   Addome search   Standard Infersh Information now Cation search Standard Infersh Information now<	Dashboard 🚷 🕹	Scan Remediate Activity Monitor Reports Configuratic» 🕖 🔭 Discuss this version				
<ul> <li>Sentre Network</li> <li>Localhost: WIN7_06</li> <li>Local Domain: WORKGROUP</li> <li>THASOFT</li> <li>Mobie Devices</li> <li>Mobie Devices</li> <li>Itis of installed applications for current selection (Entire Network - 6 computers)</li> <li>List of installed application name  Version Publisher</li> <li>Uninstall Junauthorized applications for current selection (Entire Network - 6 computers)</li> <li>Itis of installed application name  Version Publisher</li> <li>Itis of Installed Install</li> <li>Itis of Installed Install</li> <li>Itis of Installed Instal</li></ul>	Filter Group Search	Computers  Remediation Center  Remediation Jobs				
Common Tasks:       V         Manage agents       Add more computers         Scan and refresh information now Quetom scan       Microsoft SQL Server         Below agent       Microsoft SQL Server         Manage agents       Microsoft SQL Server         Add more computers       Scan and refresh information now Quetom scan         Set credentials       Deploy agent	Pentire Network     Entire Network     Localhost : WIN7_06     Solution     Local Domain : WORKGROUP     TEMASOFT     Mobile Devices	Uninstall Applications Uninstall unauthorized applications detected on network.  List of installed applications for current selection (Entire Network - 6 computers)				
Common Tasks:       >         Manage agents       Add more computers         Add more computers       Scan and refresh information now         Custom scan       Count=25         Set credentials       Total selected: 25 applications         Deploy agent       Uninstall		Image: Construct of the second se				
	Common Tasks:       >         Manage agents       Add more computers         Add more computers       Scan and refresh information now         Custom scan       Set credentials         Deploy agent       Deploy agent	Image: Second				

Screenshot 137: Uninstall applications

2. Expand the application to display the list of computers and select the computers where the application will be uninstalled.

### NOTE

The list of applications displayed relies on the unauthorized applications set up for the scanning profile in use. For more information, refer to <u>Configuring unauthorized applications auto-uninstall</u> (page 169).

3. Repeat step 2 for all applications that will be uninstalled and click **Uninstall**.

#### NOTE

Key in a criteria and click **Find** to search a vulnerability. Click **Clear** to clear previous search results.

#### 4. Configure the options described below:

Option	Description
Uninstall immediately	Uninstall the selected applications immediately.
Uninstall on	Uninstall the selected applications on a specific date and time. Configure when to uninstall the applications.

Option	Description
Credentials	Select the authentication method to use or specify a username and password. Select <b>Use per computer credentials when available</b> , to use the credentials specified in the computer properties. For more information, refer to <u>Agent</u> <u>properties</u> (page 77).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to <u>Con-</u> <u>figuring auto-remediation options</u> (page 173).
After deploy- ment options	Configure the actions to perform after deploying the selected applications. For more information, refer to <u>Con-</u> <u>figuring auto-remediation options</u> (page 173).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to <u>Configuring auto-remediation options</u> (page 173).

### 5. Click **OK**

6. To view the un-installation progress, click **Remediation Jobs** from the right panel.

## Malware Protection

Use the **Malware Protection** section to remediate vulnerabilities related to malware protection identified on target computers. Amongst others, this section enables you to scan target machines for spyware, viruses and enable local firewall.

### NOTE

To scan a machine for viruses and spyware, the target machine must have antivirus and antispyware installed.

🌒 GFI LanGuard						
Dashboard 🎲 🕹	d Scan	Remediat	e Activity Mor	itor Reports	Configuratic 🏾 🕐 🔻	Discuss this version
💡 🌆 📿	🧼 E	ntire Netw	ork - 6 comp	uters		
Filter Group Search	- 🍋 R	emediation C	enter 🏼 🏷 Rer	nediation Jobs		
Entire Network      Eccalhost : WIN7_06      Eccal Domain : WORKGROUP      ECCAL DOMAIN : WORKGROUP      ETEMASOFT	Lis	Malware Use this option	Protection In to fix problems id	entified with malwa	are protection software in Entire Network - 6 cc	you network
Mobile Devices	[				▼ Find	Clear
		🛛 🗋 Rem	ediation name			
		🗹 👸 Upda	te software product	:		
			Computer name	Operating system	Application name	•
			VIN7_06	Windows 7	Windows Defend	er
			VIN7_03	Windows 7	Windows Defend	er
			count=2			
Common Tasks: ¥						
Manage agents						
Add more computers		Cour	t=1			
Scan and refresh information now Custom scan Set credentials Deploy agent					Total selected: 1 action	Remediate
						.:

Screenshot 138: Malware protection

To remediate malware protection vulnerabilities:

#### 1. Select **Remediate** tab > **Remediation Center** and click **Malware Protection**.

2. Locate and expand the malware vulnerability and select the computers to remediate.

### NOTE

Key in a criteria and click **Find** to search a vulnerability. Click **Clear** to clear previous search results.

3. Click Remediate and configure the options described below:

Option	Description
Deploy immediately	Deploy the selected applications immediately.
Deploy on	Deploy the selected applications on a specific date and time. Configure when to deploy the applications.
Credentials	Select the authentication method to use or specify a username and password. Select <b>Use per computer credentials</b> when available, to use the credentials specified in the computer properties. For more information, refer to <u>Agent</u> properties (page 77).
Before deployment options	Configure the actions to perform before deploying the selected applications. For more information, refer to <u>Con-</u> <u>figuring auto-remediation options</u> (page 173).

Option	Description
After deploy- ment options	Configure the actions to perform after deploying the selected applications. For more information, refer to <u>Con-figuring auto-remediation options</u> (page 173).
Advanced options	Configure other options related to reboot/shut down and delete copied files from remote computers. For more information, refer to <u>Configuring auto-remediation options</u> (page 173).

#### 4. Click **OK**

5. To view the action progress, click **Remediation Jobs** from the right panel.

### Using Remote Desktop Support

Through Remote Support, you can control remote computers using Terminal Services and Remote Desktop Protocol. Remote Support enables you to install missing patches, service packs and custom software through a remote connection.

GEL an Guard	
Dashboard	Scan Remediate Activity Monitor Reports Configuratic» (9) Discuss this version
Filter Group Search	Image: Second state       Image: Second state         Image: Second state       Image: Second state
	Remote Support via Remote Desktop Connection         Use this option to remotely connect to specific targets for maintenance purposes.         Computer list       WIN7_01 Image: Computer list
Mobile Devices	⊃ Welcome
Common Tasks:       Image agents         Add more computers         Scan and refresh information now         Custom scan         Set credentials         Deploy agent	Stindows <sup>.</sup> 7 Professional

Screenshot 139: Remote desktop connection

To connect remotely to a target machine:

- 1. Click **Remediate** tab and from the left panel select a computer or domain/workgroup.
- 2. Expand Remote Support via Remote Desktop Connection from the right panel.
- 3. Depending on your selection, the list contains the available computers that allow remote desktop connection.
- 4. Double-click a machine from the list to connect.

### NOTE

To disconnect a machine, select **Remediation Center > Remote Support via...**, right-click a machine from the list and select **Disconnect**.

### NOTE

To disable remote connection, right click a machine and select **Disable Remote Connection**.

### 4.5.3 Sending Mobile Device Notifications

GFI LanGuard enables you to send an email notification regarding software updates for the mobile device to an email account associated with the device. The notification can either be a custom email message or a default one.

To configure mobile device alerts:

1. Click on **Dashboard** tab and from the computer tree select > **Mobile Devices**.

2. Right click on a selected account and select Send email notification.

Send Mail Notification		<b>—</b> ×-
Step 1 of 4: Select mail notification type.		
Notification type:		
	< Back Next >	Cancel

Screenshot 140: Sending mail notifications: Notification type

3. Select Missing operating system updates for a default email or Custom mail for a custom email.

Se	Send Mail Notification					
	Ste	p 2 c Sel no	of 4: lect n tifica	nobile devices for which to send missing operating system updat tion.	tes mail	
		×	ß	Mobile Device	New Operating System	
	Ð	~	Оре	erating System: i05 6.1		
	Θ	<b>×</b>	Оре	erating System: iOS 6.0		
		1	8	simonemann@noc.com (Apple iPhone 4)	iOS 6.1.2	
		*	8	simonemann@noc.com (Apple iPhone 4)	iOS 6.1.2	
	Ð	•	Оре	erating System: iOS 5.0.1		
			Оре	erating System: Android 4.0.3		
		~	8	alexplin@noc.com (HTC One X)	Android 4.1.1	
		<b>~</b>	8	alexplin@noc.com (HTC One X)	Android 4.1.1	
	Ð	<b>~</b>	Оре	erating System:		
				Count = 20		
				< Back	Next > Cancel	

Screenshot 141: Sending mail notifications: Selecting a device

4. Select the devices for which to send a notification email for missing operating system updates and click **Next**.

5. Specify a subject and an email body if **Custom mail** is selected and click **Next** to send.

Send Mail Notification	×
Step 3 of 4: Mail notification template.	
Subject: GFI LanGuard : Mobile device missing updates notification	
Hello, Your mobile device %MobileDeviceModel% is running operating system %CurrentOperatingSystem%. It is recommended to upgrade to the latest available operating system version: %NewOperatingSystem%.	Î
Note: Use %MobileDeviceModel% as place holder for mobile device model. Use %CurrentOperatingSystem% as place holder for current operating system. Use %NewOperatingSystem% as place holder for new operating system.	
< Back Next >	Cancel

Screenshot 142: Sending mail notifications: Default notification template

Send Mail Notification		×
<b>Step 3 of 4</b> : Mail notification template.		
Subject:		
Hello.		â
< <insert here="" text="" your="">&gt;</insert>		
Best regards.		•
	< Back Next >	Cancel

Screenshot 143: Sending mail notifications: Custom notification template

# 4.6 Activity Monitoring

Monitoring enables you to learn more about how GFI LanGuard is performing in your infrastructure. The **Activity Monitor** tab in GFI LanGuard enables you to monitor active security scans, remediation jobs and download operations of missing updates and security definitions.

Topics in this section:

4.6.1 Monitoring Security Scans	
4.6.2 Monitoring Software Updates Download	202
4.6.3 Monitoring Remediation Operations	204
4.6.4 Monitoring Product Updates	206

## 4.6.1 Monitoring Security Scans

The Security Scans section enables monitoring of all the security scans that are currently in progress.

To monitor active security scans:

- 1. Launch GFI LanGuard.
- 2. Click Activity Monitor tab and from the left panel click Security Scans.

🥑 GFI LanGuard						
💷 🔹 🔶 🔶 Da	ashboard Sc	an Remediate	Activity Monitor	Reports Configi 🏽 🥑 🔻	Discuss this versi	on
Activity Monitor:		Security Sc Provides visibility t	ans	and status of all scans.		
Troduct Opdates Activity	Drag a c	olumn header here to g	group by that column			
	Вт	arget	Profile	Start time		Ren
Common Tasks:	📀 w	IN7_03	Full Scan	22/05/2012 12:02:58	completed	N/A
Filter security scans Go to: Scheduled scans Refresh	<ul> <li>♥</li> <li>♥</li> <li>♥</li> <li>♥</li> <li>♥</li> <li>♥</li> <li>SE</li> <li>♥</li> <li></li> /ul>	IN7_01 IN7_06 RV08-06 e:TGList 20120522102	Full Scan Full Scan Full Scan 71 Full Scan	22/05/2012 12:00:15 22/05/2012 12:00:09 22/05/2012 10:30:22 22/05/2012 10:27:19	completed completed completed completed	N/A N/A N/A N/A
Actions: Stop selected scans View remediation details View scan results details		calhost calhost ount=7	Full Scan Full Scan	22/05/2012 10:05:59 21/05/2012 14:10:44	completed completed	N/A N/A
	<(		III			>

Screenshot 144: Monitoring security scans

### NOTE

To stop a scan right-click the security scan and select **Stop selected scans**.

#### NOTE

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

### Filter Security Scans

The **Security Scan** section enables you to configure what type of scans to monitor. To configure what type of scans are displayed:

- 1. Launch GFI LanGuard.
- 2. Click Activity Monitor tab and from Common Tasks, click Filter security scans.

Filter secu	rity scans
General	
	Specify which scans should activity monitor display in security scans list.
Sca	ns history
	All scans
	Only last 100  ⇒ scans
	Only scans performed in the last 7 days
Sca	ns type
	✓ Interactive scans
	Scheduled scans
	Agent scans
	OK Cancel Apply

Screenshot 145: Filter security scan dialog

#### 3. Configure the options described below:

Option	Description
All scans	Displays all scans.
Only last X scans	Displays only the last X scans.

Option	Description
Only scans performed in the last X days	Displays only the scans performed in the last X days.
Interactive scans	Displays only manual scans. For more information, refer to Manual scans (page 96).
Scheduled scans	Displays only scheduled scans. For more information, refer to <u>Scheduled scans</u> (page 100).
Agent scans	Displays only scans performed on agent computers. For more information, refer to <u>Starting an</u> <u>Agent scan manually</u> (page 111).

4. Click **OK** 

## 4.6.2 Monitoring Software Updates Download

The **Software Updates Download** screen enables you to monitor, pause, cancel or change priority to all the scheduled patch downloads.

🧭 GFI LanGuard							
Dashbo	ard Sca	n Remediate	Activity Monitor	Reports	Config: 🗙 🕜 🔻	Discuss this version	L
Activity Monitor: Security Scans Software Updates Download Remediation Operations	<b>A</b>	Software U Monitor and manage	Ipdates ge the software update	es which are cu	rrently being down	nloaded.	
Product Updates Activity	Drag a co	lumn header here to	group by that column			203	
	D File			Bulletin ID	Progress		Title
Common Taska:	LO2     LO     L	Q5_y_IdA9O7AMIRc	1pYnfbbA=_ie9-wi	MS12-023	100% (11	124kb of 11124kb )	Cumulat
	👿 zd)	Zh_CPID8ii +isAO9K0	YJ61pA=_SQLServ	Not Available	100% (311	983kb of 311983kb )	Microso
Go to: Patch auto-download options	🕢 eV	Wwq50oztI5cosEk6	EGz9U2ik=_window	Not Available	100% (4	004kb of 4004kb )	Window
Edit proxy settings	🕢 w1	rxcnmn+5tmsT5gfV	V5WXeoovo=_wind	Not Available	100% (550	717kb of 550717kb )	Window
	7+	nUjYLf1BnQz0CqTA0	)ZEhBKUOg=_excel	MS12-030	100% (20	897kb of 20897kb )	Security
Actions:	💽 XfN	zRAvu0ldv540080v	GuQ2z_Iw=_graph	MS12-030	100% (1	739kb of 1739kb )	Security
Pause all downloads	🔮 AG	Gi_oXM2p2y2vQCJ	NSOGFpmqM=_inst	APSB12-09	100% (4	030kb of 4030kb )	Adobe F
Cancel selected downloads	💟 1ni	XVNOYeYD3ThrhJcL	W1Lb4VWs=_msco	MS12-027	100% (	472kb of 472kb )	Security
Change download phoney	₩ KM	/Ekb5ww4yXhJw9jPv	v90NPFFcs=_vcredi	MS11-025	100% (8	779kb of 8779kb )	Security
		r 1A4EU8XdbcBL2aQ	+IAyVWLM=_msptl	MS11-089	100% (	412kb of 412kb )	Security
	Co	int=11					)>

Screenshot 146: Security updates download

The icon in the first column indicates the download status. The table below describes the different states:



lcon	Description
٠	<b>Downloading</b> Update is being downloaded.
0	Failed An error occurred while downloading the update. Refer to Error column for more details regarding the error encountered.
θ	<b>Pending</b> Update is queued for download.
Θ	Cancelled User cancelled update download.

### Right-click an entry and select one of the options described below:

Option	Description
Configure Patch Auto-Download	Enables or disables auto–patch download and used to configure where the patches are stored. For more information, refer to Patch auto-download settings.
Edit proxy settings	Configure the proxy settings used by GFI LanGuard to connect to the Internet. For more information, refer to <u>Configuring Program Updates</u> (page 240).
Change download priority	Change the download priority. Select between, High, normal or low priority.
Cancel selected downloads	Stop and remove the selected download.
Pause all downloads	Temporarily pause all downloads.

### Troubleshooting failed Software Updates

This section provides you with information about three software update errors, which are likely to cause software updates to fail from downloading and/or installing.

The table below provides you with the actual error message that you will receive if one of the errors has to occur and a possible cause and solution, for each:

Error Message	Cause	Solution
The file URL points to a different file than expected. Try re-scan-	The Third-Party vendor replaces old patches with updated patches, using the same URL. GFI has no control over	Download the latest Product Updates manually and re-scan your targets. For more information, refer to <u>Configuring Program</u> <u>Updates</u> (page 240).
ning with the latest program updates	now Third-Party vendors replace updates and URLs.	<b>NOTE</b> There is a 12 to 24 hour delay between Third-Parties releasing new updates and GFI LanGuard adding support for them. During this time, you will continue to receive the error message, even though you download and scan your targets using the latest product updates.

Error Message	Cause	Solution
The repository folder is not accessible. See Configuration - Patch Auto-download	The repository folder is the location where updates are downloaded to. GFI LanGuard enables you to specify alternate repositories than the default location. This error is generally caused after specifying an invalid or inaccessible repository path (example, the given path refers to a location on a shutdown computer).	<ol> <li>Manually check that you can access the folder path, using the same logon credentials.</li> <li>Ensure that the specified path is a valid:         <ul> <li>Local path - example: C:\Share or C:\Folder</li> <li>UNC path - example: \\NetworkShare\Folder</li> </ul> </li> <li>Ensure that the path is keyed in correctly.</li> <li>NOTE         <ul> <li>For more information, refer to Configuring Patch Auto-download settings, from Configure Missing Updates Auto-Deployment.</li> </ul> </li> </ol>
Internet connection not available	The computer where GFI LanGuard is installed, does not have Internet access. There are many possible causes to this problem.	Establish an Internet connection and attempt to download the failed updates.

## 4.6.3 Monitoring Remediation Operations

Remediation operations can be monitored from the following places:

- » Remediation Jobs sub-tab
- » Remediation Operations view

### Remediation Jobs sub-tab

The **Remediation Jobs** section enables you to monitor the remediation actions currently in progress.

To view remediation jobs in progress:

1. Launch GFI LanGuard.

2. Click **Remediate** tab > **Remediation Jobs** sub-tab.

🔮 GFI LanGuard	
Dashboard	Scan Remediate Activity Monitor Reports Configuration >> (2) > Discuss this version
💎 占 Q	Entire Network - 6 computers
Filter Group Search	Nemediation Center
🔺 🐙 Entire Network 🛛 🚔	Remediation jobs for selected computers:
Localhost : WIN7_06	Drag a column header here to group by that column
Local Domain : WORKGROUP	□         Status         Remediation Type         Scheduled on         ♥         Started On         Ended On
Mobile Devices	Complete Updates Deployme 22/05/2012 13:54:28 22/05/2012 13: 22/05/2012 14:05:
	Complete Updates Deployme 22/05/2012 13:54:16 22/05/2012 13: 22/05/2012 14:11:
	Complete Updates Deployme 22/05/2012 12:50:01 22/05/2012 12: 22/05/2012 13:05:
	Count=4
	Remediation iob details:
Common Tasks: ×	E S Downloads
Manage agents	WIN7_03 (Timed out: The Patch Agent did not respond in the permitted time interval.
Add more computers	Iona to complete.
Custom scan	No agents with auto-remediation enabled.
Set credentials Deploy agent	One scheduled scan with auto-remediation enabled.

Screenshot 147: Monitoring jobs from the Remediation jobs sub-tab

3. From the computer tree, select **Entire Network** to view all the running, as well as completed operations. Select specific computers/groups to view remediation jobs history and/or remediation progress for the selected item(s).

### NOTE

Right-click a remediation job and select **Cancel selected deployment** to stop the operation.

#### NOTE

Right-click a remediation job and select **Go to associated schedule scan** to view the pre-configured scan which triggered the remediation.

#### NOTE

The **Remediation job details** section provides you with granular progress details indicating the total number of files that have to be downloaded, download progress for each file and the current operation being executed as part of the remediation job.

### Remediation Operations view

The remediation operations screen enables you to monitor as well as cancel all the scheduled remediation features within GFI LanGuard.

To view remediation job activity:

1. Launch GFI LanGuard.

#### 2. Click Activity Monitor > Remediation Operations.

🧳 GFI LanGuard						
🔲 🔽 🚷   🗲   🔿 🛛 Dashboard	d (	Scan Remediate	Activity Monitor	Reports Config	» 🕐 🔹 Discus	s this version
Activity Monitor: Security Scans Software Updates Download Remediation Operations Product Updates Activity	4	Remediation	n Operations remediation operatio	ns		
Thouse opulies nearly	Drag	a column header here to g	roup by that column			
	ß	Status	Remediation Type	Scheduled on ∇	Started On	Ended On
Actions:	8	Running	Updates Deplo	22/05/2012 13:5	22/05/2012	
Go to associated scheduled scan Cancel selected deployment		Running Running	Updates Deplo Updates Deplo	22/05/2012 13:5 22/05/2012 13:5	22/05/2012 22/05/2012	
Collapse Expand All Collapse All		Complete with errors	opuates Depio	22/03/2012 12.5	22/03/2012	22/03/2012 13
	Rem 	Count=4	enabled. emediation enabled.			

Screenshot 148: Monitoring jobs from the Remediation Operations view

3. Use the view to monitor the status and history of all the running and complete remediation jobs.

#### NOTE

Right-click a remediation job and select **Cancel selected deployment** to stop the operation.

#### NOTE

Right-click a remediation job and select **Go to associated schedule scan** to view the pre-configured scan which triggered the remediation.

#### NOTE

The **Remediation job details** section provides you with granular progress details indicating the total number of files that have to be downloaded, download progress for each file and the current operation being executed as part of the remediation job.

### 4.6.4 Monitoring Product Updates

The **Product Updates Activity** screen enables you to view a history of the product updates, performed by GFI LanGuard and the real time update activity of the GFI LanGuard agents. For more information, refer to <u>Configuring Program</u>. <u>Updates</u> (page 240).

To monitor GFI LanGuard updates:

- 1. Click the Activity Monitoring tab and select Program Updates Activity
- 2. From the right pane select **GFI LanGuard Updates**.

🌒 GFI LanGuard	
Dashb	ioard Scan Remediate Activity Monitor Reports Config.» 🕖 🕆 Discuss this version
Activity Monitor: Security Scans Software Updates Download Remediation Operations	Program Updates Activity Monitor GFI LanGuard program updates activity
	GFI LanGuard Updates     GFI LanGuard Agent Updates       Scheduled update session 10/03/2014 10:20:14 (Done)       Scheduled update session 09/03/2014 10:21:11 (Done)
Common Tasks: Go to: Scheduled updates options Go to: Check for updates Edit proxy settings Actions: Expand Collapse Expand all Collapse all	<ul> <li>Scheduled update session 03/03/2014 10:21:11 (Done)</li> <li>Scheduled update session 07/03/2014 10:21:03 (Done)</li> <li>Scheduled update session 06/03/2014 10:21:03 (Done)</li> <li>Scheduled update session 05/03/2014 10:20:31 (Done)</li> <li>Scheduled update session 04/03/2014 10:20:31 (Done)</li> <li>Scheduled update session 03/03/2014 10:20:31 (Done)</li> <li>Scheduled update session 02/03/2014 10:20:31 (Done)</li> <li>Scheduled update session 03/03/2014 10:20:30 (Done)</li> <li>Scheduled update session 02/03/2014 10:20:50 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 28/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 26/02/2014 10:20:39 (Done)</li> <li>Scheduled update session 26/02/2014 10:20:39 (Done)</li> <li>Scheduled update session 26/02/2014 10:20:39 (Done)</li> <li>Scheduled update session 26/02/2014 10:20:39 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:39 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:39 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Scheduled update session 22/02/2014 10:20:30 (Done)</li> <li>Manual update session 19/02/2014 15:00:50 (Done)</li> <li>Manual update session 19/02/2014 14:49:09 (Failed)</li> </ul>

Screenshot 149: Product updates activity - GFI LanGuard Updates

To monitor GFI LanGuard Agent updates:

- 1. Click on the Activity Monitoring tab and select Program Updates Activity
- 2. From the right pane select GFI LanGuard Agent Updates.

🦪 GFI LanGuard							
Dashb	oard	Scan Ren	nediate Activ	vity Monitor Repor	ts Configt 🏾 🕐 🗸	Discuss this ver	sion
Activity Monitor: Security Scans Software Updates Download Remediation Operations	Program Updates Activity Monitor GFI LanGuard program updates activity						
Program Updates Activity	Ô	GFI LanGuard	Updates	GFI LanGuard A	gent Updates		
	ß	Status	Computer name	Start time 🔹	End time	Duration	Size
Common Tasks:	± 🔇	Succeeded	W7_07	08/03/2014 12:00:02	08/03/2014 12:04:45	4 minutes, 43 s	2.52 MB
Go to: Scheduled updates options	± 🔇	Succeeded	W710	08/03/2014 12:00:01	08/03/2014 12:03:44	3 minutes, 43 s	2.52 MB
Go to: Check for updates Edit proxy settings	± 📀	Succeeded	W710	06/03/2014 12:00:09	06/03/2014 12:03:43	3 minutes, 34 s	2.04 MB
	± 🔇	Succeeded	W7_07	06/03/2014 12:00:03	06/03/2014 12:04:28	4 minutes, 25 s	2.04 MB
Actions:	± 🔇	Succeeded	W7_07	04/03/2014 12:00:09	04/03/2014 12:31:14	31 minutes, 5 s	90.64 MB
Evpand	± 🔇	Succeeded	W710	04/03/2014 12:00:06	04/03/2014 12:25:43	25 minutes, 37	90.64 MB
Collapse	± 🔇	Succeeded	W710	24/02/2014 10:52:49	24/02/2014 11:12:30	19 minutes, 41	103.26 MB
Expand all Collapse all	± 🔇	Succeeded	W7_07	24/02/2014 10:51:34	24/02/2014 11:12:23	20 minutes, 49	103.26 MB
	•	Note: Setting <u>ti</u> bandwidth usa	Count: 8 <u>meframes</u> when a ge.	gents are allowed to get	t updates or using <u>relay</u>	<u>s</u> can improve netw	ork

Screenshot 150: Product updates activity - GFI LanGuard Agent Updates

# 4.7 Reporting

GFI LanGuard includes a reporting module which enables you to generate text and graphical reports based on information obtained from network security scans. This topic provides you with an overview of the available reports as well as how to create your own reports for a tailored solution. Through the Reports tab, you are able to generate technical activity reports for IT staff and also executive reports that normally contain less technical details and focus more on overall statistics.

Topics in this section:

4.7.1 Available reports	208
4.7.2 Generating reports	214
4.7.3 Scheduling Reports	
4.7.4 Customizing default reports	
4.7.5 Full text searching	

## 4.7.1 Available reports

This section provides you with information about the reports that are available by default in the **Reports** tab of GFI LanGuard.

There are two main types of reports:

» General reports - provide detailed technical reports as well as executive summary reports about LAN security and patch management activity

» Legal compliance reports - provide system and network audit information that enable you to be compliant with standards, laws and regulations related to corporate network usage and management conventions.

### General reports

To view **General** reports:

#### 1. Click **Reports** tab.

2. Click **View**, and from the list of reports, click **General Reports**, then select any of the following reports:

Report Title	Description
Network Security Overview	<ul> <li>An executive summary report showing:</li> <li>Network vulnerability level</li> <li>Most vulnerable computers</li> <li>Agent status</li> <li>Audit status</li> <li>Vulnerability trends over time</li> <li>Information on operating systems</li> <li>Servers and workstations.</li> </ul>
Computer Secur- ity Overview	An executive summary report showing: Computer vulnerability level Agent status Audit status Vulnerability trends over time Computer summary and details.
Vulnerability Status	<ul> <li>Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by:</li> <li>Computer name</li> <li>Vulnerability severity</li> <li>Timestamp</li> <li>Category.</li> </ul>
Patching Status	<ul> <li>Shows statistical information related to missing and installed updates detected on your scan targets. Updates can be grouped by name, severity, timestamp, vendor and category. Use this report to get:</li> <li>Missing vs. Installed updates comparison</li> <li>Charts and tables displaying missing updates distribution for each item from the first and second grouping criteria</li> <li>Charts and tables displaying installed updates distribution for each item from the first and second grouping criteria</li> <li>Patching details for missing and installed patches.</li> </ul>
Full Audit	A technical report showing information retrieved during an audit. Amongst others, the report contains information on: >> Vulnerabilities >> Open ports >> Hardware and software.
Software Audit	<ul> <li>Shows all unauthorized applications installed on target machines found during an audit. Amongst others, the report includes information on:</li> <li>Antivirus</li> <li>Antispyware</li> <li>Applications inventory.</li> </ul>

Report Title	Description
Scan History	An overview of the network security audits performed over time. Amongst others, the report includes information on: Most scanned computers Least scanned computers Auditing status History listing.
Remediation His- tory	<ul> <li>Shows information related to remediation actions performed on target computers. Amongst others, the report includes information on:</li> <li>Remediation actions per day</li> <li>Remediation distribution by category</li> <li>Remediation list grouped by computers.</li> </ul>
Network Security History	<ul> <li>Shows the changes done on scan targets between audits. Amongst others, the report includes changes related to:</li> <li>The vulnerability level</li> <li>User accounts</li> <li>Groups</li> <li>Ports</li> <li>Shares</li> <li>Registry entries.</li> </ul>
Baseline Com- parison	Enables you to compare the results of all scan targets to a base computer. From the drop down list select the base computers and click Generate. The results are grouped by computer name and amongst others includes information on:
Mobile Devices Audit	<ul> <li>Shows information related to detected mobile devices found during an audit. Amongst others, the report includes information on:</li> <li>&gt;&gt; Vulnerability distribution by severity</li> <li>&gt;&gt; Vulnerability distribution by computer</li> <li>&gt;&gt; Vulnerability listing by computer.</li> </ul>
USB Devices	Lists all USB devices found in an audit, grouped by computer.
Missing Microsoft <sup>®</sup> Secur- ity Updates	<ul> <li>Shows statistical information related to missing Microsoft<sup>®</sup> security updates, detected on your scan targets.</li> <li>Select items to include in your report:</li> <li>General missing updates distribution chart</li> <li>Distribution table</li> <li>Vulnerability list.</li> </ul>
Missing Non- Microsoft <sup>®</sup> Secur- ity Updates	<ul> <li>Shows statistical information related to missing non-Microsoft<sup>®</sup> security updates, detected on your scan targets.</li> <li>Select items to include in your report:</li> <li>General missing updates distribution chart</li> <li>Distribution table</li> <li>Vulnerability list.</li> </ul>
Missing Security Updates	Lists statistical information related to missing security updates, found on scanned computers.
Computer Sum- mary	<ul> <li>A summary of scan target information, including:</li> <li>&gt;&gt; Operating system information</li> <li>&gt;&gt; Agent status</li> <li>&gt;&gt; Vulnerabilities severity.</li> </ul>

Report Title	Description
Hardware Audit	Illustrates information related to the hardware found during an audit.
Computer Details	Provides a detailed list of computer properties, including: MAC Address Time to Live Network Role Domain Lan Manager Is relay agent Uses relay agent Attributes Operating system IP address.
Open Shares	Lists all the shared folders found during an audit. The results are grouped by computer name.
Open Ports	Lists all the open ports found during an audit. The results are grouped by port type (TCP and UDP).
Services	Lists all services found during an audit. Results are grouped by computer name.
Groups and Users	Lists all Groups and Users found during an audit. The result is grouped by computer name.
Mobile Device Policies	Lists all mobile device policies found during an audit. The result is grouped by computer name.
Unauthorized Applications	Lists all unauthorized applications installed scan targets, including: >> Top Computers with Unauthorized Applications >> Top Unauthorized Applications >> Applications Inventory >> Computers without Antivirus Installed
Antivirus Applic- ations	Shows information related to the antivirus installed on scan targets.
New Devices	Lists all new devices found during last week audits.

## Legal Compliance reports

## To view Legal Compliance reports:

### 1. Click **Reports** tab.

2. From the list of reports, expand any of the following compliance reports suites:

Report Suite Title	Description
PCI DSS Compliance Reports	<ul> <li>The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. GFI LanGuard provides you with a number of reports that cater for PCI DSS compliance, including:</li> <li>PCI DSS Requirement 1.4 - Installed Firewall Applications</li> <li>PCI DSS Requirement 2.2.3 - Disk Encryption Applications</li> <li>PCI DSS Requirement 5.2 - Antivirus Applications</li> <li>PCI DSS Requirement 6.1 - Remediation History by Date</li> <li>PCI DSS Requirement 12.12 - Open Trojan Ports by Host.</li> </ul>

Report Suite Title	Description
HIPAA Compliance Reports	The Health Insurance Portability and Accountability Act (HIPAA) is a requirement of all healthcare providers that regulates the exchange of private patient data. This helps prevent unlawful disclosure or release of medical information. To help you follow HIPAA regulations, GFI LanGuard provides you with a suite of HIPAA compliance reports, including: HIPAA 164.308(a)(1)(ii)(A) - Missing Security Updates by Host HIPAA 164.308(a)(1)(ii)(A) - Vulnerability Distribution by Host HIPAA 164.308(a)(4)(ii)(A) - Open Ports HIPAA 164.308(a)(5)(ii)(D) - Audit Policy HIPAA 164.308(a)(8) - Baseline Changes Comparison.
SOX Compliance Reports	<ul> <li>The Sarbanes-Oxley Act (SOX) is regulation created in response to high-profile financial scandals as well as to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. GFI LanGuard provides a list of SOX compliance reports, including:</li> <li>» SOX 302.a - Network Vulnerability Summary</li> <li>» SOX 302.a - Remediation History by Host</li> <li>» SOX 302.a - Security Scans History</li> <li>» SOX 404 - Vulnerability Listing by Category</li> <li>» SOX 404 - Missing Security Updates by Host.</li> </ul>
GLBA Compliance Reports	<ul> <li>The Gramm-Leach-Bliley Act (GLBA) is an act that allows consolidation between Banks and Insurance companies. Part of the act focuses on IT network compliance for such companies. GFI LanGuard offers a list of GLBA Compliance reports, including:</li> <li>GLBA 501.b - Baseline Changes Comparison</li> <li>GLBA 501.b - Network Patching Status</li> <li>GLBA 501.b - Open Trojan Ports by Host</li> <li>GLBA 501.b - Vulnerable Hosts Based on Open Ports</li> <li>GLBA 501.b - Vulnerable Hosts by Vulnerability Level.</li> </ul>
PSN CoCo Com- pliance Reports	<ul> <li>The Public Service Network - Code of Connection (PSN CoCo) is simply a list of conditions that should be met before connecting an accredited network to another accredited network. GFI LanGuard helps you monitor the status of such connections through the list of PSN CoCo Compliance reports, which include:</li> <li>PSNCoCo RIS. 1 - Baseline Changes Comparison</li> <li>PSNCoCo MAL. 1 - Disk Encryption Applications</li> <li>PSNCoCo MAL. 1 - Installed Firewall Applications</li> <li>PSNCoCo PAT. 1 - Installed Security Updates by Host</li> <li>PSNCoCo PAT. 1 - Installed Security Updates by Severity.</li> </ul>
CIPA	The Children's Internet Protection Act (CIPA) addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. GFI LanGuard Central Management Server provides a list of CIA Compliance reports including: » Req. 47 USC § 254(1)(1)(A)(iv) - Network Vulnerability Summary » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerability Distribution by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerability Listing by Category » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerability Listing by Gategory » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerability Listing by Severity » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerability Listing by Severity » Req. 47 USC § 254(1)(1)(A)(iv) - Open Trojan Ports by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Network Patching Status » Req. 47 USC § 254(1)(1)(A)(iv) - Network Patching Status » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerable Hosts by Vulnerability Level » Req. 47 USC § 254(1)(1)(A)(iv) - Vulnerable Hosts Based on Open Ports » Req. 47 USC § 254(1)(1)(A)(iv) - Remediation History by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Remediation History by Date » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Host » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(1)(1)(A)(iv) - Network Security Log by Date » Req. 47 USC § 254(1)(1)(A)(i

Report Suite Title	Description
FERPA Compliance Reports	<ul> <li>The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. GFI LanGuard provides a list of FERPA Compliance reports, including:</li> <li>FERPA 20 USC 1232g (b) - Network Patching Status</li> <li>FERPA 20 USC 1232g (b) - Network Security Log by Host</li> <li>FERPA 20 USC 1232g (b) - Remediation History by Date</li> <li>FERPA 20 USC 1232g (b) - Vulnerability Distribution by Host</li> <li>FERPA 20 USC 1232g (b) - Vulnerability Based on Open Ports.</li> </ul>
ISO/IEC 27001 & 27002 Compliance Reports	The Information technology – Security techniques – Information security management systems (ISO/IEC) standard formally specifies a management system that is intended to bring information security under explicit management control. GFI LanGuard offers an extensive list of ISO/IEC Compliance reports, including: > ISO/IEC 27001 A. 10.4 - Antivirus Applications > ISO/IEC 27001 A. 10.7.2 - Disk Encryption Applications > ISO/IEC 27001 A. 10.6.2 - Open Shares > ISO/IEC 27001 A. 10.6.2 - Services > ISO/IEC 27001 A. 10.6.2 - System Information.
FISMA Compliance Reports	The Federal Information Security Management Act (FISMA) assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. GFI LanGuard helps you be compliant to FISMA standards through the provided reports, which include: FISMA NIST SP 800-53 AC-2 - Groups and Users FISMA NIST SP 800-53 PM-5 - Computer Details FISMA NIST SP 800-53 PM-5 - Computer Summary FISMA NIST SP 800-53 SI-5 - Missing Security Updates by Host FISMA NIST SP 800-53 SI-7 - Antivirus Applications.
CAG Compliance Reports	The Consensus Audit Guidelines (CAG) is a publication of best practice guidelines for computer security. The project was initiated as a response to extreme data losses experienced by organizations in the US defense industrial base. GFI LanGuard offers a list of CAG Compliance reports, including:
NERC CIP Com- pliance Reports	The North American Electric Reliability Corporation (NERC) develops standards for power system operation, monitoring and enforcing compliance with those standards, assessing resource adequacy, and providing educational and training resources as part of an accreditation program to ensure power system operators remain qualified and proficient. GFI LanGuard provides a list of NERC CIP Compliance reports, including: NERC CIP-005 R2 - Installed Firewall Applications NERC CIP-005 R2 - Open Ports NERC CIP-007 R2 - Open Shares NERC CIP-007 R2 - Services NERC CIP-007 R2 - System Information.

## 4.7.2 Generating reports

GFI LanGuard ships with an extensive list of default reports. These can be used as they are, or modified to provide information precisely to your requirements.

#### NOTE

For more information, refer to Customizing default reports (page 219).

To generate a report:

1. Click **Reports** tab.

2. From the computer tree, select the computer/group you want to report on.

#### NOTE

Select Entire Network to report on all the computers listed under the computer tree.

- 3. From the reports list, select the report you want to generate.
- 4. (Optional) From the right pane, click **Customize report** if changes to report items are required.
- 5. Click Generate report.



Screenshot 151: Report sample - Part 1



Screenshot 152: Report sample - Part 2



Screenshot 153: Report sample - Part 3

## 4.7.3 Scheduling Reports

To automate reporting tasks, GFI LanGuard enables you to generate and optionally send reports, based on a schedule. You can configure schedules for existing or custom reports.

This section contains information about:

- » Creating new scheduled reports
- » Configuring scheduled reports options
- » Managing scheduled reports

### Creating new scheduled reports

To create a new scheduled report:

1. Click **Reports** tab.

### 2. From Actions, select New scheduled report.

1	Report Template	
	Schedule Report Template:	Network Security Overview
	Schedule Report Name:	Schedule for report 'Network Security Overview'
	Schedule Report Description:	An executive summary report showing network vulnerability level, most vulnerable computers, agent status and audit status, vulnerability trends over time, information on operating systems, servers and

Screenshot 154: Select scheduled report template

3. From the **Report Template** section, configure the following options:

Option	Description
Schedule Report Tem- plate	Select an existing report from the drop-down menu. This enables you to create a new report based on the settings of an existing one.
Schedule Report Name	Key in a unique name for the new report.
Schedule Report Description	Optionally, key in some information about the report such as report items or schedule settings.



Screenshot 155: Add or remove target domains and/or computers

4. From the **Target Domains & Computers** section, configure the following options:
| Option | Description  |
|--------|--|
| ÷      | From the computer tree, select a domain or workgroup and click <b>Add Domain</b> . The selected domains/workgroups are added to the report.                            |
| ÷      | Click <b>Add IP</b> to open the <b>Add IP address range</b> dialog. From the <b>Add IP address range</b> dialog, key in an IP range or Sub-<br>net and click <b>OK</b> |
| ×      | Select the Domain/Workgroup/IP range you want to remove and click <b>Remove Domain/IP</b> .  |

3	Filter	
	Chose a filter that applies to the targ	et
	MyFilter	•
	None CustomFilter	
	MyFilter	
	NewFilter	

5. From the **Filter** drop-down menu, select a filter that you want to apply to the new scheduled report. This enables you to generate reports based on data pertaining to scan targets included in the filter.

### NOTE

Only custom filters can be applied to scheduled reports. For more information, refer to <u>Using the Dashboard</u> (page 125).

4 Sched	luling Settings					
<b>▼</b> Enab <i>Run the</i>	ole schedule <i>Report every day at</i>	17:31.				
One	e time only, on:	08/11/2012		at:	17:22:26	*
Rec	currence pattern:	daily	-	at:	17:31:44	*
Daily re	ecurrence pattern					
⊚ E <sup>.</sup> ⊚ E	very 1	days				

6. From **Scheduling Settings**, configure the following options:

Option	Description
Enable Schedule	Select to turn on report scheduling and generate the report according to schedule settings.
One time only, on	Specify a date and time when the report is generated. This option generates the report once, on the specified date.
Recurrence pat- tern	Select recurrence frequency and specify the time the scheduled report is generated.

5	Alerting & Saving Settings	
	<ul> <li>Export to file</li> <li>Click on the 'Export Settings' button to customize the report storage options and specify the file format and destination folder where this report will be stored.</li> <li>Export Settings</li> <li>Send by email</li> <li>Click on the 'Alerting Options' button to customize and configure the general alerting options.</li> </ul>	
	Alerting Options         Override general alerting options, and send email to:         Add Schedule	

#### 7. From Alerting & Saving Settings, configure the following options:

Option	Description
Export to file	Select to save the report in a folder.
Export Settings	Click <b>Export Settings</b> and from the <b>Scheduled Reports Storage Options</b> dialog, specify the folder where the report is saved and the format the report is saved in.
Send by email	Select to send report by email. The report is sent to recipients configured in Alerting Options.
Alerting Options	Click <b>Alerting Options</b> and configure alerts recipients and mail server settings. For more inform- ation, refer to <u>Configuring Alerting Options</u> (page 235).
Override general alerting options, and send email to	Select to use email recipients other than the ones configured in Alerting Options.

#### 8. Click Add Schedule to save the report.

#### NOTE

## Configuring scheduled reports options

To configure additional scheduled reports settings:

#### 1. From the Scheduled Reports section, click Scheduled Reports Options.

2. Click **Alerting Options** to configure email settings to use to send reports. For more information, refer to <u>Configuring Alerting Options</u> (page 235).

3. Click **Storage Options** to specify the format and the location where generated reports are saved.

#### NOTE

```
By default, all generated reports are stored as PDF in: <GFI LanGuard install directory>\Reports.
```

## Managing scheduled reports

To manage scheduled reports:

- 1. Click **Reports** tab.
- 2. From Scheduled Reports, click Scheduled Reports List.

GFI LanGuard Scheduled Reports Manage GFI LanGuard Scheduled Reports				
Scheduled Reports List				
Schedule Name	Report Name			
Schedule for report 'Network Security Overview'	Network Security Overview			
Schedule for report 'Vulnerability Status'	Vulnerability Status			
Count=2				
<(()	)>			

Screenshot 156: Edit scheduled reports options

3. Double-click a report from the right pane to edit schedule report settings.

Scheduled Reports Activity Logs				
Date	Туре	Report Name		
08/11/2012 17:23: 08/11/2012 17:23:	Information Error	Schedule for report "Vulnerability Status" Schedule for report "Vulnerability Status"		

Screenshot 157: Monitor scheduled reports activity

4. Monitor schedule reports activity from the **Scheduled Reports Activity Logs** section at the bottom of the right pane.

## 4.7.4 Customizing default reports

GFI LanGuard enables you to create new reports based on the settings of an existing report. This saves you time and enables you to fine-tune existing reports, so that the data-set used to build the report precisely matches your requirements.

This section contains information about:

- » Creating custom reports
- » Customizing report logos
- » Customizing Email Report Format

#### Creating custom reports

To create a custom report:

- 1. Click **Reports** tab.
- 2. From the **Reports** list, select an existing report on which settings of the new reports are based on.

NOTE

Not all reports are editable.

Vulnerability Status				
Shows statistical information related to the vulnerabilities detected on target computers. Vulnerabilities can be grouped by computer name, vulnerability severity, timestamp and category.				
Gen Use this report	erate Report <u>Customize report</u>			
Chart group	t displaying general vulnerabilities distribution based on selected second ping criteria			
2 Table criter	e displaying general vulnerabilities distribution based on selected grouping ia			
3 Chart	t displaying vulnerabilities distribution for each item from first grouping criteria			
4 Vulne	erabilities details for each item from first grouping criteria			

Screenshot 158: Edit report settings from the report sample preview

3. From the right pane, click **Customize report** to show advanced report options.

Report Items Filters Grouping & Sorting	Discard Changes
Select the items to include in the report:	
General Distribution Chart	
V Distribution Table	
Distribution Chart	
✓ Vulnerability List Detail View	
Save as new report	

Screenshot 159: Configuring report items

4. Click **Report Items** tab and select the related items that you want to include in the report.

Report Items Filters Grouping &	Sorting	Discard Changes
Configure the filtering criteria to use:		
Vulnerability Name/Update Name	Vulnerability Name	
Product Name	"Microsoft Windows Firewall"	× -
Severity	"Medium"	<b>X</b> -
Timestamp	Last 3 Months	•
Vulnerability Category	"Malware" or "Firewall Vulnerabilities"	<b>X</b> -
Save as new report		

Screenshot 160: Configuring report filtering options

5. Click **Filters** tab and configure the available filters that relate to the report.

Report Items Filters Grouping & Sortin	Discard Changes			
Configure the first category grouping and ordering	to apply			
Group by:	Direction:			
Computer 👻	Ascending 👻			
Configure the second category grouping and orde	ering to apply			
Group by:	Direction:			
Vulnerability Severity	Descending -			
Configure the additional ordering to apply				
Order by:	Direction:			
Vulnerability Timestamp				
Save as new report				

Screenshot 161: Configure report grouping and sorting options

6. Click **Grouping & Sorting** tab and configure:

- » First category grouping report information is grouped by the selected field
- » Second category grouping grouped information is sub-grouped by the selected field
- » Additional ordering order report information according to the selected field.
- 7. Click Save as new report...

8. From the Add report dialog, key in a name and an optional description for the new custom report. Click OK

#### Customizing report logos

GFI LanGuard enables you to use your company/custom logo in the built–in reports included in the product. Logos can be placed in the header or footer sections of the report.

#### Customizing Report Header Logo

1. Create / select your image.

2. Resize image to: Width = 125, Height = 25.

#### 3. Rename the image to **headerlogo.png**.

4. Add custom graphics to the **logo** folder which can be found in ProgramData\GFI\LanGuard12\Graphics\Logo.

#### Customizing Report Footer Logo

1. Create / select your image.

2. Resize image to: Width = **109**, Height = **41**.

3. Rename the image to **footerlogo.png**.

4. Add custom graphics to the **logo** folder which can be found in ProgramData\GFI\LanGuard12\Graphics\Logo.

### Customizing Email Report Format

For each scheduled email report type, there is a predefined HTML format file that includes placeholders delimited with '%' symbol (for example: %TITLE%, %NAME%). You can edit the HTML format, edit HTML style, move and delete placeholders to further customize the e mail body of generated reports. The default template location is: <GFI LanGuard install directory> \ LanGuard 12 \ Templates \ template\_ mailbody.xml.

Take into consideration that GFI LanGuard can only manage known placeholders (listed below) with their predefined role. Placeholders are usable in all scheduled report types. The table below describes the customizable placeholders:

Placeholder	Description	
%TITLE%	Email title for the generated report.	
%NAME%	Scheduled report name.	
%DESCRIPTION%:	Scheduled report description.	
%TARGET%	Targets (computers, domains) represented in the scheduled report.	
%LAST_RUN%	Last run date and time of the scheduled report.	
%NEXT_RUN%	Next run date and time of the scheduled report.	
	<b>NOTE</b> This placeholder is used only for daily digest reports.	
%PROFILE%	Scanning profile used whilst running the scheduled scan.	
	<b>NOTE</b> This placeholder is used only for post–scheduled scan reports.	
%DURATION%	Scheduled scan duration.	
	<b>NOTE</b> This placeholder is used only for post–schedules scan reports.	
%ITEMS_COUNT%	Collected items count.	
	<b>Note</b> This placeholder is used only for post–scheduled scan reports.	

Placeholder	Description
%AUTOREMED_ MISSINGPATCHES%	Used in the report if Auto-remediate Missing Patches option is enabled for the scheduled scan.
	<b>NOTE</b> This placeholder is used only for post–scheduled scan reports.
%AUTOREMED_MISSINGSPS%	Used in the report if Auto-remediate Missing Service Packs option is enabled for the scheduled scan.
	<b>Note</b> This placeholder is used only for post–scheduled scan reports.
%AUTOREMED_UNINSTAPPS%	Used in the report if Auto–remediate Uninstall Applications option is enabled for the scheduled scan.
	NOTE This placeholder is used only in post–scheduled scan reports.

## 4.7.5 Full text searching

The full text search feature returns results in a structured and configurable manner. Any returned results offer clickable links for further details.

To use the full text search feature:

1. Click **Reports** tab > **Search** sub-tab.

#### NOTE

Search can also be accessed from **Computer tree> Search**.

2. Enter you search item and click **Search**.

🌒 GFI LanGuard		×
Dashboard	Scan Remediate Activity Monitor Reports Configr» 🕖 * Discuss this version	
Filter Group Search	WORKGROUP - 4 computers          Settings       Search	
Localhost : WIN7_06	Win7_06 Search Advanced search	
Local Domain : WORKGROUP	26 results found	
Mobile Devices	<ul> <li>Computer Information</li> <li>WIN7_06 (192.168.2.12)</li> <li>WIN7_06 NetBIOS name: WIN7_06, Description: Workstation Service.</li> <li>WIN7_06 NetBIOS name: WIN7_06, Description: File Server Service.</li> <li>WIN7_06 Computer name: WIN7_06, IP: 192.168.2.12, Domain: WORKGROUP, Operating s Professional 6.1, Network role: Workstation, Service pack: , Time to live (TTL): , Re 00-15-5D-03-1D-C0, MAC vendor. Microsoft Corporation, Is Windows OS: yes, Lan Default system Runlevel: 0, Vulnerability level: High, Virtual machine: Microsoft Hyp</li> </ul>	a lig oc
Common Tasks: ×	55041-006-2359943-86223, Is machine virtual: yes.	
Manage agents Add more computers Scan and refresh information now	Hardware Devices	<b>.</b>
Custom scan	Page 1 of 2   4 4 🕨 🕅 10	0%
Set credentials Deploy agent		

Screenshot 162: Customize the report parameters

3. (Optional) Click **Advanced search** to configure filters to narrow your search results to something more specific.

4. Analyze the search results from the results section at the bottom.

The result contains links that enable you to navigate between computers, software products and vulnerabilities. For example, you can click a missing service pack link to open the missing patches for a specific computer.

Seattings Search	_
Search	
TEMP Search Advanced search	
20 results found	
🔣 🚯 🖃 🔍 100% 🔻 🍕 🖺 🗋 🕶 Full Screen	
Bo	•
Se Computer Information	
TEMP (192.168.3.17)	
TEMP NetBIOS name: TEMP Description: File Server Service	J
TEMP	
NetBIOS name: TEMP, Description: Workstation Service.	
Computer name: TEMP, IP: 192.168.3.17, Domain: WORKGROUP, Operating system: ) Professional 6.1, Network role: Workstation, Service pack: , Time to live (TTL): , Real tir 00-15-5D-03-EC-8B, MAC vendor. Microsoft Corporation, Is Windows OS: yes, Langua Default system Runlevel: 0, Vulnerability level: High, Virtual machine: Microsoft Hyper-V 00371-177-0000061-85337, Is machine virtual: yes.	
Kardware Devices	
TEMP (192.168.3.17) Microsoft Virtual Machine Bus Network Adapter#3 Network interface card name: Microsoft Virtual Machine Bus Network Adapter #3, Card 1 Virtual Machine Bus Network Adapter #3, IP address(es): 192.168.3.17, fe80::f500:a81: 00:15:5D:03:EC:8B, DHCP is set, DHCP server: 10.44.100.1, Domain: gfimalta.com, Hc 10.44.100.7, Gateway(s): 192.168.3.254, Netmask address: 255.255.255.0, 64, Vendor.	
Logged on Users	
TEMP (192.168.3.17)	v
Page 1 of 2 4 5 5 100%	,

Screenshot 163: Navigate using report links

## 4.8 Data collected from a network audit

When auditing networks, GFI LanGuard enumerates and processes information about system patching status, hardware, software, ports and system information of each scanned machine.

For more information, refer to Interpreting scan results (page 151).

This information is collected from scan targets using the ports and protocols described in the following sections.

Topics in this section:

4.8.1 System Patching Status	
4.8.2 Hardware	

4.8.3 Ports	
4.8.4 Software	
4.8.5 System Information	230

## 4.8.1 System Patching Status

GFI LanGuard shows a list of patches missing or deployed on scanned machines, including security and non-security patches of Microsoft operating systems, Mac OS X, major Linux distributions and third-party applications. Various patch management actions can then be taken based on the collected information.

For more information, refer to Missing Service Packs (page 155).

The table below displays a summary of the information gathered by the system patching status:

Data	Description	Ports	Protocol
Missing Service Packs and Update Rollups	Discovers missing Microsoft <sup>®</sup> and non-Microsoft <sup>®</sup> service packs.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM</li> <li>135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and</li> <li>printer sharing</li> <li>Remote</li> <li>registry</li> <li>Windows</li> <li>update agent</li> </ul>
Missing Security Updates	Discovers missing Microsoft <sup>®</sup> and non-Microsoft <sup>®</sup> security patches.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM</li> <li>135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and</li> <li>printer sharing</li> <li>Remote</li> <li>registry</li> <li>Windows</li> <li>update agent</li> </ul>
Missing Non-Security Updates	Discovers missing Microsoft <sup>®</sup> and non-Microsoft <sup>®</sup> patches unrelated to security.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM</li> <li>135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and</li> <li>printer sharing</li> <li>Remote</li> <li>registry</li> <li>Windows</li> <li>update agent</li> </ul>
Installed Service Packs and Update Rollups	Lists installed Microsoft <sup>®</sup> and non-Microsoft <sup>®</sup> service packs.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM</li> <li>135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and</li> <li>printer sharing</li> <li>Remote</li> <li>registry</li> <li>Windows</li> <li>update agent</li> </ul>
Installed Security Updates	Lists installed Microsoft <sup>®</sup> and non-Microsoft <sup>®</sup> security patches.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM</li> <li>135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and</li> <li>printer sharing</li> <li>Remote</li> <li>registry</li> <li>Windows</li> <li>update agent</li> </ul>

Installed Non-Security Lists installed Microsoft <sup>®</sup> and non-Microsoft <sup>®</sup> natches upre-	
Updates lated to security. Updates lated to security. DC 135 DC dynam	<ul> <li>Y 139 &gt;&gt; SMB</li> <li>Y 445 &gt;&gt; File and</li> <li>Y 445 &gt;&gt; File and</li> <li>Y Printer sharing</li> <li>&gt;&gt; Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li>Y Remote</li> <li< td=""></li<></ul>

## 4.8.2 Hardware

GFI LanGuard displays a hardware audit of each scanned device. In a glance you can see the hardware specification and a list of devices attached during scan.

For more information, refer to <u>Hardware audit</u> (page 158).

The table below displays a summary of the information gathered by the hardware audit.

Data	Description	Ports	Protocol
Network devices	Lists physical and virtual network adapters.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM 135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>
Local drives	Lists drives discovered on scanned target(s). Local drives include: Hard disks CD/DVD drives Floppy drives	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM 135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>
Processors	Lists processors discovered during a scan.	<ul> <li>» TCP 139</li> <li>» TCP 445</li> <li>» DCOM 135</li> <li>» DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>
Motherboards	Lists motherboards discovered during a scan.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM 135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>
Memory details	<ul> <li>Returns memory information of scanned target(s), including:</li> <li>&gt; Total physical memory</li> <li>&gt; Free physical memory</li> <li>&gt; Total virtual memory</li> <li>&gt; Free virtual memory</li> </ul>	<ul> <li>» TCP 139</li> <li>» TCP 445</li> <li>» DCOM 135</li> <li>» DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>
Storage details	Lists every storage device discovered during a scan. Storage devices include: Hard disks Virtual hard disks Removable disks Floppy drives CD/DVD drives	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM 135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>

Data	Description	Ports	Protocol
Display adapters	Lists video cards discovered during a scan.	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM 135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> <li>WMI</li> </ul>
USB Devices	Lists all the detected USB devices that are attached to the net- work/scan targets.	<ul> <li>» TCP 139</li> <li>» TCP 445</li> <li>» DCOM 135</li> <li>» DCOM</li> <li>dynamic</li> </ul>	<ul> <li>» SMB</li> <li>» File and printer sharing</li> <li>» Remote registry</li> <li>» WMI</li> </ul>
Other devices	Lists generic devices discovered during a scan, including: >> System devices/drivers >> Human Interface Devices (HID) >> Mouse and keyboard >> Communication ports (Serial and Parallel) >> Floppy disk controllers >> Hard disk controllers	<ul> <li>TCP 139</li> <li>TCP 445</li> <li>DCOM 135</li> <li>DCOM</li> <li>dynamic</li> </ul>	<ul> <li>» SMB</li> <li>» File and printer sharing</li> <li>» Remote registry</li> <li>» WMI</li> </ul>

## 4.8.3 Ports

GFI LanGuard displays a list of open ports found on the system after a scan.

Apart from detecting open ports, GFI LanGuard uses service fingerprint technology to analyze the services that are running behind the detected open ports. With service fingerprint, GFI LanGuard can detect if malicious software is using the detected open port.

For more information, refer to Open Ports (page 157).

The table below displays a summary of the information gathered by ports node.

Data	Description	Ports	Protocol
Open TCP ports	Checks for open TCP ports	All enabled ports in the scan profile	Windows sockets
Open UDP ports	Checks for open UDP ports	All enabled ports in the scan profile	Windows sockets

## 4.8.4 Software

The software audit displays the applications, divided by categories, that are installed on scanned computers. For each application, the audit displays details such as application name, publisher and version.

For more information, refer to Software audit (page 158).

The table below displays a summary of the information gathered by the software audit:

Data	Description	Ports	Protocol
General applications	Enumerates every application installed on the scan target(s).	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Antiphishing applications	Lists antiphishing applications.	TCP 139 TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>

Data	Description	Ports	Protocol
Antispyware applications	Lists antispyware applications.	<ul><li>&gt; TCP</li><li>139</li><li>&gt; TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Antivirus applications	Lists antivirus applications.	<ul> <li>TCP</li> <li>139</li> <li>TCP</li> <li>445</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Backup applications	Lists backup applications.	<ul> <li>TCP</li> <li>139</li> <li>TCP</li> <li>445</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Data Loss Prevention	Lists Data Loss Prevention applications.	<ul> <li>TCP</li> <li>139</li> <li>TCP</li> <li>445</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Device Access Control	Lists Device Access Control applications.	<ul><li>&gt; TCP</li><li>139</li><li>&gt; TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Disk Encryption	Lists Disk Encryption applications.	<ul> <li>» ТСР</li> <li>139</li> <li>» ТСР</li> <li>445</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Firewall applications	Lists firewall applications.	<ul> <li>» ТСР</li> <li>139</li> <li>» ТСР</li> <li>445</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Health Agent	Lists system health monitoring applications.	<ul> <li>» ТСР</li> <li>139</li> <li>» ТСР</li> <li>445</li> </ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Instant Messenger	Lists Instant Messenger applications.	<ul><li>&gt; TCP</li><li>139</li><li>&gt; TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Patch management applications	Lists patch management applications.	<ul><li>&gt; TCP</li><li>139</li><li>&gt; TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Peer To Peer	Lists Peer to Peer (P2P) applications.	<ul><li>TCP</li><li>139</li><li>TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
URL Filtering	Lists web filtering applications.	<ul><li>&gt; TCP</li><li>139</li><li>&gt; TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>

Data	Description	Ports	Protocol
Virtual Machine Software	Lists virtualization software detected on your net- work.	» ТСР 139 » ТСР 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Virtual Private Network (VPN) Client applications	Lists VPN client applications.	» ТСР 139 » ТСР 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Web Browser applications	Lists web browsers.	<ul><li>&gt;&gt; TCP</li><li>139</li><li>&gt;&gt; TCP</li><li>445</li></ul>	<ul> <li>» SMB</li> <li>» File and printer sharing</li> <li>» Remote registry</li> </ul>

### NOTE

For a full list of supported security applications including vendors and products, refer to http://go.gfi.com/?pageid=security\_app\_fullreport

## 4.8.5 System Information

GFI LanGuard displays various system details of scanned machines, such as information about the operating system, password and security policies and applications automatically launched at system startup.

For more information, refer to System Information (page 159).

The information gathered by the System Information node includes:

Data	Description	Ports	Protocol
Shares	<ul> <li>Lists all shares discovered during a scan. Information includes:</li> <li>Share name</li> <li>Share remark</li> <li>Share path</li> <li>Share permissions</li> </ul>	<ul><li>» TCP</li><li>139</li><li>» TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Password policy	Lists the password policy configuration.	<ul><li>» TCP</li><li>139</li><li>» TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Security audit policy	Security audit policy configuration.	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>

Data	Description	Ports	Protocol
Registry	Lists selected information from the system registry. Amongst others, enumerated information includes: Registry owner Current build number Current type Current version Vendor identifier Software type	» ТСР 139 » ТСР 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
NetBIOS names	<ul> <li>Lists NetBIOS names of the scanned target(s). This node includes:</li> <li>Workstation service</li> <li>Domain name</li> <li>File server services</li> <li>Browser service elections</li> </ul>	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Computer	Lists computer identifiers including: MAC address Time to live Network role OS Serial number Language Machine type (physical or virtual)	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Groups	Lists local or domain/workgroup groups.	» ТСР 139 » ТСР 445	<ul> <li>SMB</li> <li>File and printer shar- ing</li> <li>Remote</li> <li>registry</li> </ul>
Users	Lists local or domain/workgroup users.	» ТСР 139 » ТСР 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Logged on users	Lists locally and remotely logged on users.	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Sessions	Lists the active sessions at the time of the scan.	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Services	Lists every service discovered during a scan.	» TCP 139 » TCP 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>

Data	Description	Ports	Protocol
Processes	Lists every active process discovered during a scan.	» ТСР 139 » ТСР 445	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>
Remote TOD (time of day)	Lists the current time and uptime of the scanned target(s).	<ul><li>» TCP</li><li>139</li><li>» TCP</li><li>445</li></ul>	<ul> <li>SMB</li> <li>File and printer sharing</li> <li>Remote registry</li> </ul>

## 4.9 Common Vulnerabilities and Exposures (CVE)

GFI LanGuard is CVE certified. This topic describes how CVE certification is used in GFI LanGuard.

CVE (Common Vulnerabilities and Exposures) is a list of standardized names for vulnerabilities and other information security exposures. Its aim is to standardize the names for all publicly known vulnerabilities and security exposures.

CVE is a dictionary which aim is to facilitate data distribution across separate vulnerability databases and security tools. CVE makes searching for information in other databases easier and should not be considered as a vulnerability database by itself.

CVE is a maintained through a community–wide collaborative effort known as the CVE Editorial Board. The Editorial Board includes representatives from numerous security–related organizations such as security tool vendors, academic institutions, and governments as well as other prominent security experts. The MITRE Corporation maintains CVE and moderates editorial board discussions.

## About CVE Compatibility

"CVE-compatible" means that a tool, Web site, database, or service uses CVE names in a way that allows it to cross-link with other repositories that use CVE names. CVE-compatible products and services must meet the four requirements:

Compatibility	Description
CVE Searchable	A user must be able to search for vulnerabilities and related information using the CVE name.
CVE Output	Information provided must include the related CVE name(s).
Mapping	The repository owner must provide a mapping relative to a specific version of CVE, and must make a good faith effort to ensure accuracy of that mapping.
Documentation	The organization's standard documentation must include a description of CVE, CVE compatibility, and the details of how its customers can use the CVE–related functionality of its product or service.

#### Note

For an in-depth understanding of CVE compatibility refer to the complete list of CVE requirements available at http://go.gfi.com/?pageid=LAN\_CVE\_Requirements

#### About CVE and CAN

CVE names (also called "CVE numbers," "CVE–IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. CVE names have "entry" or "candidate" status. Entry status indicates that the CVE

name has been accepted to the CVE List while candidate status (also called "candidates," "candidate numbers," or "CANs") indicates that the name is under review for inclusion in the list.

Each CVE name includes the following:

- » CVE identifier number (i.e. "CVE-1999-0067").
- » Indication of "entry" or "candidate" status.
- » Brief description of the security vulnerability or exposure.
- » Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

#### NOTE

For an in-depth understanding of CVE names and CANs, refer to: http://go.gfi.com/?pageid=cvecert

## Searching for CVE Entries

CVE entries can be searched from the Scanning profiles node within the Configuration tab.

Find <u>b</u> ulletin:	Find	Find next
Search by bulletin name (e.g. MS02-017) or QNumber (e.g. Q311967).		
Caraganah at 1.6 4. Caparah in a fax OVE information		

Screenshot 164: Searching for CVE information

To search for a particular CVE bulletin:

1. Specify the bulletin name (for example, CVE–2005–2126) in the search tool entry box included at the bottom of the right pane.

2. Click on **Find** to start searching for your entry.

#### Obtaining CVE Names

CVE entry names can be obtained through the GFI LanGuard user interface from within the Scanning profiles node within the Configuration tab. By default, the CVE ID is displayed for all the vulnerabilities that have a CVE ID.

#### Importing and Exporting CVE Data

CVE data can be exported through the impex command line tool. For more information, refer to <u>Using impex.exe</u> (page 284).

# **5** Settings

GFI LanGuard enables you to run vulnerability scans straight out of the box – using the default settings configured prior to shipping. If required you can also customize these settings to suit any particular vulnerability management requirements that your organization might need. You can customize and configure various aspects of GFI LanGuard including scan schedules, vulnerability checks, scan filters and scan profiles.

Topics in this section:

5.1 Configuring Alerting Options	
5.2 Configuring Database Maintenance Options	236
5.3 Configuring Program Updates	
5.4 Limiting Database Size	
5.4.1 Methods to avoid database limitation issues	
5.5 Scanning Profile Editor	
5.5.1 Create a new Scanning Profile	
5.5.2 Configuring Vulnerabilities	
5.5.3 Configuring Patches	258
5.5.4 Configuring Network & Software Audit options	
5.5.5 Configuring security scanning options	
5.6 Utilities	
5.6.1 DNS Lookup	
5.6.2 Traceroute	
5.6.3 Whois	
5.6.4 Enumerate Computers	
5.6.5 Enumerate Users	
5.6.6 SNMP Auditing	
5.6.7 SNMP Walk	
5.6.8 SQL Server® Audit	
5.6.9 Command Line Tools	
5.7 Script Debugger	
5.7.1 Creating custom scripts using VBscript	
5.7.2 Creating custom scripts using Python Scripting	
5.7.3 SSH Module	
5.8 Configuring NetBIOS	
5.9 Uninstalling GFI LanGuard	

## 5.1 Configuring Alerting Options

To configure alerting options:

## 1. Click **Configuration** tab > **Alerting options**.

2. Click the link in the right pane.

Alerting Options	Properties	×
General Notific	ations	
Specify SMTP server and email address details for email notifications after each scheduled scan.		
<u>T</u> o:	administrator@mydomain.com	
<u>C</u> C:	manager@mydomain.com	
Erom:	languard@mydomain.com	
Server:	localhost	
Port:	465	
Use SSL/TLS encrypted connection		
SMTP Serve	er requires login	_
User name:	languard	
Password:	••••••	
	Verify Settings	
	OK Cancel <u>App</u>	ly

Screenshot 165: Configuring Alerting Options

3. Key–in the parameters described below:

Option	Description
То	The recipient email address. Emails sent by GFI LanGuard are received by this email address.
сс	Key-in another email address in this field if you need to send a copy to another email address.
From	The sender email address. GFI LanGuard will use this email account to send the required emails.
Server	Defines the server through which emails are routed. This can be either an FQDN (Fully Qualified Domain Name) or an IP Address.
Port	Defines the IP port through which emails are routed. Default value is 25
Use SSL/TLS encryp- ted connection	Select this option if you have an SSL (Secure Sockets Layer Protocol) or TLS (Transport Layer Security Pro- tocol) encrypted connection to send the required emails.

Option	Description
SMTP Server requires login	Select this option if the SMTP server requires a username and password to authenticate.

4. Click on the Verify Settings button to verify email settings.

5. Select Notifications and configure the following options:

Option	Description
Enable daily digest	Receive daily report with all changes made on the entire network. Configure the time when the daily digest email is received.
Report format	Specify the report format received by email.
Send an email on new product news	Receive an email containing new product news.

6. Click **OK** 

## 5.2 Configuring Database Maintenance Options

GFI LanGuard ships with a set of database maintenance options through which you can maintain your scan results database backend in good shape.

For example, you can improve product performance and prevent your scan results database backend from getting excessively large by automatically deleting scan results that are older than a specific number of months.

If you are using an Access<sup>™</sup> database backend, you can also schedule database compaction. Compaction enables you to repair any corrupted data and to delete database records marked for deletion in your database backend; ensuring the integrity of your scan results database. The following sections provide you with information about:

- » Using SQL Server<sup>®</sup> as a database backend
- » Managing saved scan results
- » List scanned computers
- » Configure advanced database maintenance options
- » Configure database retention options

Using SQL Server<sup>®</sup> as a database backend

#### IMPORTANT

It is highly recommended to use SQL Server® once product evaluation is exceeded.

To store scan results in an SQL Server<sup>®</sup> database:

1. Click Configuration tab > Database Maintenance Options > Database backend settings.

Prop	oerties						×		
С	hange D	atabase	Scanne	d Computers	Saved Scan Results	Retention	A 🔹 🕨		
	Current (	GFI LanG	uard data	abase backen	d settings				
	Database type: Server name:			Microsoft S	Microsoft SQL Server				
				.\SQLEXP	RESS				
	Database name:		LNSSScar	Results12					
		User na	me:	Current Win	idows user				
	New GF	l LanGua	rd databa	se backend :	settings				
	Mici		UL Serv				- 11		
	Exis	ting <u>S</u> ervi	er: [.	\SQLEXPRE	55		<u> </u>		
	Database <u>N</u> ame: L		_NSSScanResults12						
	Use Windows Auth		entication						
	SQL <u>L</u> ogin:								
	Pas	swor <u>d</u> :	[						
	Micr	osoft Acc	ess (onlu	recommender	during evaluation)				
	Path	n of new (	tatabase.	file:	s danng evaluation)				
	E atir of new database in			LanGuard 12	no.				
	U: Merogramulata / u FINLianuluard 12/scanresults.mdb Browse								
					OK Cance	A L	pply		

Screenshot 166: SQL Server<sup>®</sup> database backend options

2. Select the **MS SQL Server** option and choose the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

3. Specify the SQL Server credentials or select the **Use Windows Authentication** option to authenticate to the SQL server using windows account details.

4. Click **OK** to finalize your settings.

#### NOTE

If the specified server and credentials are correct, GFI LanGuard automatically logs on to your SQL Server and create the necessary database tables. If the database tables already exist, it re–uses them.

#### NOTE

When using Windows Authentication credentials, make sure that GFI LanGuard services are running under an account that has both access and administrative privileges on the SQL Server databases.

5. Click **Yes** to stop all current scans.

6. If the current Access<sup>™</sup> database contains data, click **OK** to transfer all scan data to the SQL Server<sup>®</sup> database.

Managing saved scan results

Use the Saved Scan Results tab to maintain your database backend and delete saved scan results that are no longer

required. Deletion of non-required saved scan results can be achieved manually as well as automatically through scheduled database maintenance.

During scheduled database maintenance, GFI LanGuard automatically deletes saved scan results that are older than a specific number of days/weeks or months. You can also configure automated database maintenance to retain only a specific number of recent scan results for every scan target and scan profile.

Properties				×					
Change Database Scanned Comput	ers Saved Scar	n Results	Retention A	4 >					
Your current GFI LanGuard license enables you to scan an unlimited number of different target IP addresses/computers.									
/ Computer	Last scanned	Scans	Is Licensed	*					
BERNARD01 (192.168.3.13)	08/11/2011	1	Yes						
BERNARDSQL (192.168.3.80)	25/05/2011	2	Yes	-					
BERNARDSQLSRV (192.168	08/11/2011	2	Yes	-					
ELIFTEST-2003 (192.168.3.16)	08/11/2011	1	Yes						
💻 DC (192.168.3.23)	08/11/2011	1	Yes						
📃 DC1 (192.168.3.10)	08/11/2011	1	Yes						
📃 EUGENIA-TEST (192.168.3.5)	08/11/2011	2	Yes						
📃 FAXSRV (192.168.3.109)	08/11/2011	1	Yes						
📃 GFI-PATCHTST2 (192.168.3	08/11/2011	1	Yes						
📃 GFI-RESDUAL (192.168.3.124)	25/05/2011	4	Yes						
GFI-RESEARCH (192.168.3.12)	25/05/2011	4	Yes						
📃 GFI-RESMON (192.168.3.128)	25/05/2011	4	Yes						
GFI-RES-SP1 (192.168.3.34)	25/05/2011	5	Yes	*					
	D	elete selec	cted computer(s	)					
	ОК	Cance	el Apj	oly					

Screenshot 167: Database maintenance properties: Managed saved scan results tab

To manage saved scan results:

1. Click on the **Configuration** tab > **Database Maintenance Options** > **Manage saved scan results**.

2. To delete saved scan results, select the particular result(s) and click **Delete Scan(s)**.

3. To let GFI LanGuard manage database maintenance for you, select **Scans generated during the last** to delete scan results, which are older than a specific number of days/weeks, or months or **Scans per scan target per profile in number of** to retain only a specific number of recent scan results.

#### List scanned computers

GFI LanGuard maintains a global list of scanned computers for licensing purposes. Any computers in excess of what is specified in the licensing information are not scanned.

GFI LanGuard enables systems administrators to delete scanned computers in order to release licenses that were previously utilized.

To delete computers previously scanned:

#### 1. Click Configuration tab > Database Maintenance Options > Manage list of scanned computers.

2. Select the computers to delete and click **Delete selected computer(s)**.

#### IMPORTANT

Deleting computers from the database is a one-way operation that will also delete all computer related data from the database. Once deleted, this data is no longer available.

Configure advanced database maintenance options

GFI LanGuard enables you to repair and compact the Access<sup>™</sup> database backend automatically to improve performance.

During compaction, the database files are reorganized and records that have been marked for deletion are removed. In this way, you can regain used storage space. During this process, GFI LanGuard also repairs corrupted database backend files. Corruption may occur for various reasons. In most cases, a Access<sup>™</sup> database is corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, unresponsive operations forced reboots, and so on).

Properties 💌								
Scanned Computers Saved Scan Results Retention Advanced								
Please configure the database compaction options.								
The below option is only available when using Microsoft Access as a database backend. When using SQL Server / MSDE as a database a backend you need to manually set maintenance plans according to your company policies.								
Compact Now								
Database compact and repair frequency								
🔘 One time only								
<u>N</u> ext operation 15/11/2011 ■▼ 21:15:56 등								
OK Cancel Apply								

Screenshot 168: Database Maintenance properties: Advanced tab

To compact and repair a Access<sup>™</sup> database backend:

#### 1. Click Configuration tab > Database Maintenance Options > Database maintenance plan.

2. To manually launch a repair and compact process on an Access<sup>™</sup> database backend, click **Compact Now**.

3. To automate the repair and compact process on an Access<sup>™</sup> database backend select:

- » **One time only** to schedule a onetime Access<sup>™</sup> database repair and compact
- » **Every** to execute a repair and compact process on a regular schedule.

Specify the date, time and frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

#### Configure database retention options

Database retention options enable you to keep your database clean and consistent, by configuring GFI LanGuard to automatically delete unwanted scan results and scan history information while retaining important ones.

To configure retention settings:

#### 1. Click **Configuration** tab > **Database Maintenance Options** > **Database backend settings** > **Retention** tab.

#### 2. Configure the options described below:

Option	Description
Keep scans generated during the last	Keep scan results generated during the specified number of days/weeks/months.
Keep scans per scan target per profile number of	Specify the number of scan results to keep, for every scan target by every scan pro- file.
Never delete history	Select this option if you want to keep all scan history.
Keep history for the last	Keep scan history for the specified number of days/weeks/months.

#### 3. Click **OK**

## 5.3 Configuring Program Updates

This tool enables GFI LanGuard to detect the latest vulnerabilities and maintain its scanning performance. Configure GFI LanGuard to auto–download updates released by GFI to improve functionalities in GFI LanGuard. These updates also include checking GFI web site for newer builds. Updates can be enabled/disabled by selecting the checkbox in the **Auto–download** column.

GFI LanGuard can download all Unicode languages. This includes (but is not limited to) English, German, French, Italian, Spanish, Arabic, Danish, Czech, Finnish, Hebrew, Hungarian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Portuguese/Brazilian, Russian, Swedish, Chinese, Chinese (Taiwan), Greek, and Turkish.

The following sections provide you with information about:

- » Configuring proxy settings
- » Configuring auto-update options
- » Installing program updates manually

#### Configuring proxy settings

To manually configure proxy server settings for Internet updates:

#### 1. Click on **Configuration** tab > **Program Updates**.

#### 2. From Common Tasks select Edit proxy settings.

GFI LanGuard Proxy Settings
General
Use this option to manually provide your proxy server settings.
✓ Override automatic proxy detection
C Connect directly to the Internet
© Connect via a proxy server
Server: 192.168.11.11:8080
Proxy server requires <u>a</u> uthentication:
User name: administrator
Pass <u>w</u> ord: *********
Note: Patch file download, scheduled updates and some operations performed during the scanning process need to open Internet connections.
OK Cancel Apply

Screenshot 169: Configuring proxy server settings

3. Select **Override automatic proxy detection;** configure the options described below:

Option	Description
Connect directly to the Inter- net	A direct Internet connection is available.
Connect via a proxy server	Internet access is through a proxy server. Update the Server name and port number using this format <server>:<port></port></server>
Proxy server requires authen- tication	(Optional) Enter username and password if required by the proxy server.

### 4. Click **OK**

Configuring auto-update options

GFI LanGuard can check for the availability of software updates at every program startup. To disable/enable this feature

#### 1. Click on **Configuration** tab > **Program Updates**. From **Common Tasks** select **Edit program updates options**.

Program Updates Options	x
General	
Configure your default program updates options such as updates schedule or provide an alternative download location.	_
Enable scheduled updates	
<u>R</u> ecurrence pattern: daily ➡ a <u>t</u> : 14:50:00	
Every 1 days	
Every weekday	
<ul> <li>Download updates from the GFI Web site.</li> <li>Download updates from an alternative location:</li> </ul>	
OK Cancel Apply	

Screenshot 170: Configure updates at application startup

2. Select/unselect **Check for updates at application startup** to enable/disable auto update checks at application startup.

3. Select/unselect enable scheduled updates to configure the frequency of update checks.

4. Specify whether GFI LanGuard download updates from GFI website or from an alternative location.

5. Click **OK** 

Installing program updates manually

To start GFI LanGuard program updates manually:

- 1. Click on **Configuration** tab > **Program Updates**.
- 2. From Common Tasks click Check for updates.

😅 Update GFI LanGuard	×
Choose which action to do in the next step You can choose to update the application files or to download all the update files to a specific path used further as an alternative update location.	9
Obvious application files from the following location    Output: Output: Output: Output: Download all update files from GFI web site to this path:   Browse	
< Back Next > Car	ncel

Screenshot 171: Check for Updates wizard

3. Specify the location from where the required update files will be downloaded.

4. (Optional) Change the default download path, select **Download all update files...** to this path to provide an alternate download path to store all GFI LanGuard updates.

5. Click **Next** to proceed with the update.

6. Select the updates and click **Next**.

7. Click **Start** to start the update process.

#### NOTE

If having problems when downloading updates, check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to <u>Gateway permissions</u> (page 22).

## 5.4 Limiting Database Size

GFI LanGuard enables you to work with either Microsoft SQL Server or Microsoft SQL Server Express as database backend.

#### NOTE

Microsoft SQL Server Express edition is free but places limits on database size. We recommend using Microsoft SQL Server Express for GFI LanGuard deployments managing up to 2,000 computers or devices. For larger deployments, use Microsoft SQL Server Standard Edition which is not free but has an upper limit of 524 Petabytes.

## NOTE

If your database reaches the limit of your SQL Server Express version, you will begin to experience errors due to the inability of the database tables to accept new data.

The following is a list with some brief information about some SQL Server Express edition versions and their size limits:

- » 2008 Express 4 GB
- » 2008 R2 Express 10 GB
- » 2012/2014/2016 Express 10 GB

## 5.4.1 Methods to avoid database limitation issues

### Upgrade database

» If you are currently using an Access database we highly recommend upgrading to a Microsoft SQL Server or Microsoft SQL Server Express database.

» When you migrate your database from Access to SQL Server or SQL Server Express, GFI LanGuard automatically copies your data to the new database so no data is lost.

#### Delete old scans manually or automatically

To delete manually:

- 1. Click **Configuration** tab > **Database Maintenance Options**.
- 2. Select Manage Scan Results and delete old and unneeded scans.



Screenshot 172: Deleting Old Scans Manually

To delete automatically:

1. Click Configuration tab > Database Maintenance Options.

2. Select Manage Retention Policy and set the retention policy that fits your needs.

Image: Configurations:       Dashboard       Scan       Remediate       Activity Monitor       Reports       Configuration       > (a) > (b)	🏈 GFI LanGuard						
Configurations: Agents Management Scanning Profiles Scheduled Scans Mobile Devices Software Categories Database backend settings	🔲 🔽 🚷 🛛 🥧 🖉 Dashboard	Scan Remediate	Activity Monitor	Reports	Configuration	» 🕐 -	Discuss this version
<ul> <li>Atto-Uninstal Validation</li> <li>Atto-Uninstal Validation</li> <li>Software Updates</li> <li>Software Updates</li> <li>Current database backend set</li> <li>Current database backend set</li> <li>Patch Auto-Download</li> <li>Poterbase Maintenance Options</li> <li>Manage Ist of scanned com</li> <li>Manage Ist of scanned com</li> <li>Manage Ist of scanned computers.</li> <li>Man</li></ul>	Configurations: Agents Management Scanning Profiles Scheduled Scans Mobile Devices Mobile Devices Software Categories Applications Inventory Patch Auto-Deployment Patch Auto-Deployment Patch Auto-Deployment Patch Auto-Download Alerting Options Database Maintenance Options General Common Tasks: Database backend settings Manage Ist of scanned computers Manage retention policy Database maintenance plan	Databo The data security s Database Configure d Current dat Current dat Current dat Current bac Manage lis Manage the Manage sc automatic d Manage re Configure a Manage the	ase Maintenan base maintenance op scan results database backend settings atabase backend set abase backend: MS , kend path: C:\F at of scanned comp list of previously sca an results in results from the d atabase cleanup. tention policy utomatic database c maintenance plan automatic compact/	Ce Optic tions enable Change Da Change Da Scan res Ke Scan hist Scan hist Nu Scan hist Ke	e you to perform atabase Scanned Configure automatic ults eep scans generate 30 day eep scans per scan 10 tory ever delete history eep history for the la 36 mor	maintena Computers database c d during the s target per p sst sst	Ance operations on the Saved Scan Results Retention A. leanup options. e last orofile in number of OK Cancel Apply

Screenshot 173: Deleting Old Scans Automatically

#### Backup

To back up a Microsoft SQL Server Database use the instructions at:

#### http://go.gfi.com/?pageid=LAN\_SQLDatabaseBackupMSDN

To clean-up your database:

#### 1. Go to Configuration > Database Maintenance Options > Database backend settings...

2. Disconnect GFI LanGuard from the database you've backed up and you want to delete, by connecting to another temporary database (eventually Access database).

3. Delete the database from the SQL Server using SQL Server Management Studio.

4. Go to GFI LanGuard under **Configuration > Database Maintenance Options > Database backend settings...** and reconnect to the SQL Server.

Properties						×			
Change [	Database	Scanned	d Computers	Saved Scan Results	Retention	A, • •			
Current GFI LanGuard datab		base backen	ase backend settings						
	Database type:			Microsoft SQL Server					
Server name:			.\SQLEXP	RESS					
	Database name:			nResults12					
	User na	me:	Current Win	ndows user					
New GF	Fl LanGua crosoft Sl	ird databa: DL Servi	se backend : er/SQL_Sei	settings rver Express					
Fxi	stina Serv	er I							
Database <u>N</u> ame: L									
~	Use Wind	lows Authe	entication						
SQ	SQL <u>L</u> ogin:								
Pas	sswor <u>d</u> :								
Mice Pat	rosoft Acc th of new ( \Program[	ess (only r database f Data\GFI\	ecommendeo file: LanGuard 12	d during evaluation) Ascanresults.mdb	Browse.				
				OK Cance	el A	pply			

Screenshot 174: Microsoft SQL Server/SQL Server Express Database

## 5.5 Scanning Profile Editor

The scanning profiles that ship with GFI LanGuard are already pre–configured to run a number of vulnerability checks on selected target. You can however disable vulnerability scanning as well as customize the list of vulnerability checks executed during a scan. Scans can be modified through the **Scanning Profile Editor**.

Topics in this section:

5.5.1 Create a new Scanning Profile	247
5.5.2 Configuring Vulnerabilities	248
5.5.3 Configuring Patches	258
5.5.4 Configuring Network & Software Audit options	261
5.5.5 Configuring security scanning options	268

## 5.5.1 Create a new Scanning Profile

The **Scanning Profiles Editor** enables you to create new scanning profiles. To create a new custom scanning profile: 1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. In Scanning Profiles Editor from Common Tasks, click New scanning profile.

GFI LanGuard Scanning Profiles Editor							
Scanning Profiles			۰ (2)	Discuss	this version		
Profile categories:	🍋 Vulnerability Assessment (	ptions	💫 🝋 Network & Software Audit Opt	ons 🔌	Scanner Options		
Complete/Combination Scans Vulnerability Assessment Network & Software Audit	Vulnerabilities     Patches       Choose scan profile conditions.     Enable vulnerability scanning		I				
Profiles:	Group by: Type 🔻	Name	<b>A</b>				
Full Vulnerability Assessment Full Scan (Active) Full Scan (Slow Networks)	Vulnerability Assessment         Scan (Active)         Scan (Active)         Scan (Slow Networks)         Image:						
New scanning profile Set Active Rename Delete	Software		All Servers: Abe Timmerman zmi.cgi Fi All Servers: Adcycle - build.cgi All Servers: Aglimpse All Servers: AHG's 'search.cqi' Search	: Disclosure	it Validation Flaw		
Help: <u>Scanning Profiles</u> <u>LanGuard Scripting</u>	Advanced	Advanced     Add     Edit     Remove					
	Adding, editing or removing vulnerabilities are selected	erabilities f	from the above list applies the change	to all the p	profiles where the		
	<u>r</u>						

Screenshot 175: The Scanning Profile Editor

4. Specify the name of the new profile and optionally select **Copy all settings from an existing profile** to clone settings from an existing profile.

5. Click **OK** to save settings. The new scanning profile is added under **Profiles** in the left pane.

## 5.5.2 Configuring Vulnerabilities

The **Vulnerability Assessment Options** tab enables you to configure which Microsoft<sup>®</sup>/non-Microsoft<sup>®</sup> and Security/non-Security updates are checked when scanning targets with the selected profile.

The following sections provide you with information about:

- » Enabling vulnerability scanning
- » Customizing the list of vulnerabilities to be scanned
- » Customizing vulnerability checks properties
- » Setting up vulnerability check conditions

Enabling vulnerability scanning

To enable vulnerability scanning:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

Scanning Profiles		
Profile categories: Complete/Combination Scans Vulnerability Assessment Network & Software Audit	🍋 Vulnerability Assessment Options	Network & Software Audit Options
	🍓 Vulnerabilities 🛛 🔯 Patches	
	Choose scan profile conditions.	
	Enable vulnerability scanning	

Screenshot 176: Enabling vulnerability scanning for the selected scanning profile

3. From the **Vulnerability Assessment Options** tab, click **Vulnerabilities** sub-tab.

- 4. Select the scanning profile to customize from the left pane under Profiles.
- 5. In the right pane, select Enable Vulnerability Scanning.

#### NOTE

Vulnerability scanning is configured on a scan profile by scan profile basis. If in a particular profile this option is not selected, no vulnerability tests will be performed in the security audits carried out by this scanning profile.

Customizing the list of vulnerabilities to be scanned

To specify which vulnerabilities will be enumerated and processed by a scanning profile during a security audit:

1. From **Vulnerability Assessment Options** tab, select the scanning profile to customize from the left pane under **Profiles**.

🍋 Vulnerability Assessment (	Options Network & Software Audit Options	Scanner Option	s	
🍓 Vulnerabilities 🛛 👩 Patches				
Choose scan profile conditions.				
Enable vulnerability scanning				
	N			
Group by: Type		CVEID	Security Focus ID	
	Abyss web server Bufferoverflow	OVE 2002 0575	8062	
	AFS-Kerberos Support in OpenSSH Pos      Alerter service enabled	CVE-2002-0575	4560	
Mail	All Servers: (e)shop Online-Shop System	CVE-2001-1014	3340	
Miscellaneous	All Servers: A1Stats (a1disp)	CVE-2001-0561	2705	
Registry	All Servers: Abe Timmerman zml.cgi File	CVE-2001-1209	3759	
Rootkit	All Servers: Adcycle - build.cgi	CVE-2000-1161	1969	
- 🔽 🧖 RPC	All Servers: Aglimpse		2026	
Services	All Servers: AHG's 'search.cgi' Search E	CVE-2002-2113	3985	
🔽 🧖 Software	All Servers: Alex Heiphetz Group EZSho	CVE-2000-1092	2109	
web	🔽 🚺 All Servers: Arts Store.cgi	CVE-2001-0305	2385	
🗄 🔽 闷 Potential Vulnerabilities	🗹 🕕 All Servers: Auktion.cgi	CVE-2001-0212	2367	
	🗹 🕕 All Servers: Brian Stanback bsguest.cgi	CVE-2001-0099	2159	
	🗹 🕕 All Servers: Brian Stanback bslist.cgi	CVE-2001-0100	2160	
	🗹 🕕 All Servers: Commerce.cgi	CVE-2001-0210	2361	
	🗹 🕕 All Servers: COWS CGI Online Worldwe		3915	
	🗹 🕕 All Servers: DCShop vulnerability	CVE-2001-0821	2889	
	All Commences Discretes Manager Frances			
	Food on the sect this as			
	5990 Vulnerabilities			
Advanced	Add	Edit	Remove	
Find vulnerability: by Name	Find	Find next	]	
• Adding, editing or removing vulnerabilities from the above list applies the changes to all the profiles where the edited vulnerabilities are selected.				

Screenshot 177: Select the vulnerability checks to be run by this scanning profile

2. In the right pane, select the vulnerability checks to execute through this scanning profile.

Customizing vulnerability checks properties

All the checks listed in the **Vulnerabilities** tab have specific properties that determine when the check is triggered and what details will be enumerated during a scan.

Edit vulnerability		×
General Conditions	Description References	
<u>N</u> ame:	Alerter service enabled	
<u>Type</u> :	Services	
OS <u>F</u> amily:	windows -	
OS <u>V</u> ersion:	Windows 7 Pro	
Product:		
Timestamp:	01/12/1997	
S <u>e</u> verity:	🚺 Medium 👻	
	OK Cancel Apply	

Screenshot 178: Vulnerability properties dialog: General tab

To change the properties of a vulnerability check:

1. Right-click on the vulnerability to customize, select Properties.

2. Customize the selected vulnerability check from the tabs described below:

Tab	Description
General	Use this tab to customize the general details of a vulnerability check including vulnerability check name, vulnerability type, OS family, OS version, Product, Timestamp and Severity.
Conditions	Use this tab to configure the operational parameters of this vulnerability check. These parameters will define whether a vulnerability check is successful or not.
Description	Use this tab to customize the vulnerability check description.
References	Use this tab to customize references and links that lead to relevant information in the OVAL, CVE, MS Security, Secur- ity Focus and SANS TOP 20 reports.

3. Click on **OK** to save your settings.

Setting up vulnerability check conditions

The **Conditions** tab enables you to add or customize conditions, which define whether the computer or network being scanned is vulnerable, or not. It is therefore of paramount importance that any custom checks defined in this section are set–up by qualified personnel that are aware of the ramifications of their actions.

Edit vulnerability
General Conditions Description References
This vulnerability will be triggered when the below conditions are met.
AND • Not +()+ -()-
Windows NT Service Test AND
• Object:
Service name: Alerter
Operator: equals
Value: running
Unix Inetd Test
• Object: 2\
Attribute: Protocol
Operator: evists
Description:
Performs several checks related to a specified NT service.
-
Add Edit Delete Clear 🛧 🔸
OK Cancel Apply

Screenshot 179: Vulnerability conditions setup tab

To add a vulnerability check condition:

1. From **Vulnerability Assessment Options** tab > **Vulnerabilities** sub-tab, right-click a vulnerability from the list of vulnerabilities and select **Properties**.

## 2. From the **Edit vulnerability** dialog, click **Conditions** tab **>Add**.
ep 1 of 3: Select the type of check	
speary what do you want to check normale list below	
<u>C</u> heck type:	
▷ · 🛅 Windows Checks	
Unix Checks	
Solaris Checks	
Linux Checks	=
Independent Checks	-
Independent Family Test	
Independent File MD5 Test	
Independent FTP Banner Test	
Independent HTTP Banner Test	
Independent OS Version Test	-
Check description:	
Executes a VB script and returns a boolean value.	*
	T

Screenshot 180: Check properties wizard - Select check type

3. Select the type of check to be configured and click  $\ensuremath{\textbf{Next}}.$ 

Object properties:	
Properties	Values
📝 Script file	anon_ftp_upload.vbs 💽 🔀
How many of the mate	ning objects must satisfy the condition for the check to return TRUE:
How many of the mate at least one Description:	ning objects must satisfy the condition for the check to return TRUE:

Screenshot 181: Check properties wizard - Define the object to examine

4. Define the object to examine and click **Next**.

Check properties	×
Step 3 of 3: Set the condition Select the attribute and the desired value(s)	
Attribute: Result Operator: equals	
Value:	
Description: The result of the script execution. It can be 1 for TRUE, or 0 for FALSE.	*
< Back Finish Car	ncel

Screenshot 182: Check properties wizard - Set required conditions

5. Specify required conditions and click **Finish** to finalize your settings.

Edit vulnerability
General Conditions Description References
This vulnerability will be triggered when the below conditions are met.
AND Not +()+ ()- AND endent HTTP Banner Test AND XOR ws Metabase Test OR Linux RPM Info Test
Description: Checks the RPM header information for a given RPM package.
OK Cancel Apply

Screenshot 183: Check properties wizard - Defining conditional operators

6. If more than one condition is set up, define conditional operators and click **OK** to finalize your configuration settings.

Vulnerabilities 🧑 Patches			
Choose scan profile conditions.			
📝 Enable vulnerability scanning			
Group by: Type 🔻	Name 🔺	CVE ID	Security Focus ID
🖃 🔽 🍓 Vulnerabilities	🗹 🚺 Abyss Web server Bufferoverflow		8062 🔺
🔽 🍓 DNS	🗹 則 AFS-Kerberos Support in OpenSSH Poses a Securi	CVE-2002-0575	4560
🔽 🍓 FTP	Alerter service enabled		
🔽 🍓 Hardware	🔽 🕕 All Servers: (e)shop Online-Shop System	CVE-2001-1014	3340
🔽 🍓 Mail	🔽 🕕 All Servers: A1Stats (a1disp)	CVE-2001-0561	2705
🔽 🍓 Miscellaneous	🗹 🕕 All Servers: Abe Timmerman zml.cgi File Disclosure	CVE-2001-1209	3759
🔽 🍓 Registry	🗹 則 All Servers: Adcycle - build.cgi	CVE-2000-1161	1969
🔽 🝓 Rootkit	🗹 🕕 All Servers: Aglimpse		2026
🔽 🚰 RPC	🗹 🕕 All Servers: AHG's 'search.cgi' Search Engine Inpu	CVE-2002-2113	3985
🔽 🍓 Services	🔽 🕕 All Servers: Alex Heiphetz Group EZShopper Direc	CVE-2000-1092	2109
🔽 🍓 Software	🗹 🕕 All Servers: Arts Store.cgi	CVE-2001-0305	2385
🔤 🔽 🖓 Web	🗹 🕕 All Servers: Auktion.cgi	CVE-2001-0212	2367
🖃 🔽 🍓 Potential Vulnerabilities		015 0004 0000	h l
🔤 🔽 🦓 Information	7500 uulaaashikkaa		-
	7599 Vulherabilities		
Advanced	Add	Edit	Remove
Find <u>v</u> ulnerability: by Name	Find     Find	d next	

Screenshot 184: Advanced vulnerability options

7. (Optional) Click **Advanced** in the **Vulnerabilities** tab to launch the advanced vulnerabilities scanning options.

Advanced Vulnerabilities Properties					
0	Gener	al			
	Ę	Specify advanced vulnerabilities options.			
	-	Vulnerability Scan Options			
		<ul> <li>Internal checks</li> </ul>			
		Weak passwords	$\checkmark$		
		FTP anonymous access allowed	$\checkmark$		
		Administrator account exists			
		Users that never logged on			
		New vulnerabilities are enabled by default	Yes		
		Show vulnerabilities with errors during evaluatio	No		
	-	CGI Probing Settings			
		<ul> <li>Send CGI request through proxy</li> </ul>	No		
		Proxy IP address			
		Proxy port			
		ОК	Cancel Apply		

Screenshot 185: Advanced vulnerability scanning dialogs

The options in Advanced Vulnerabilities Options are used to:

» Configure extended vulnerability scanning features that check your target computers for weak passwords, anonymous FTP access, and unused user accounts.

» Configure how GFI LanGuard handles newly created vulnerability checks.

» Configure GFI LanGuard to send CGI requests through a specific proxy server. This is mandatory when CGI requests will be sent from a computer that is behind a firewall to a target web server that is 'outside' the firewall. For example, Web servers on a DMZ.

The firewall will generally block all the CGI requests that are directly sent by GFI LanGuard to a target computer that is in front of the firewall. To avoid this, set the **Send CGI requests through proxy** option to 'Yes' and specify the name/IP address of your proxy server and the communication port which will be used to convey the CGI request to the target.

## 5.5.3 Configuring Patches

The **Patches** tab specifies the security updates checked during vulnerability scanning. The patches checked are selected from the complete list of supported software updates, included in this tab. This list is automatically updated whenever GFI releases a new GFI LanGuard missing patch definition file.

The following sections contain information about:

- » Enabling/disabling missing patch detection checks
- » Customizing the list of software patches to scan

#### » Searching for Bulletin Information

Enabling/disabling missing patch detection checks

🔋 GFI LanGuard Scanning Profiles Edit	or							• ×
Scanning Profiles					•	Discu	ss this version	
Profile categories:	🍓 Vulnerability Assessment	Options	Network & S	oftware Audit Op	otions	💐 Sc	anner Options	
Complete/Combination Scans Vulnerability Assessment	🍓 Vulnerabilities 🛛 👩 Patches		1					
🥵 Network & Software Audit	Choose scan profile conditions.							
	Detect installed and missing software	are update	es and service packs					
Profiles:	Software updates to check for:							
	Group by: Severity 🔻	Bulletin II	)	Severity	QNum	ber	Date posted	r Title
😽 Full Scan (Active)	🖃 🔽 🔯 All Patches	🗹 🤯 G	C_19_0_1084_46	Critical	GC_1	9_0_1	2012-05-15	
🍇 Full Scan (Slow Networks)	🔽 🔯 Critical	🗹 🤯 н	Π1222	Important	HT12	22	2012-05-15	
	🔽 🔯 Important	🗹 🧿 o	PERA1164	Critical	OPER	A1164	2012-05-10	
	🔤 🔽 🧑 Moderate	🗹 🤯 S	FR517	Important	SFR5	17	2012-05-09	:
	🔽 💽 Low	🗹 🤨 A	PSB12-13	Critical	APSB	12-13	2012-05-08	
	🔤 🔽 💀 Undefined	🗹 🔯 A	PSB12-13	Critical	APSB	12-13	2012-05-08	
		🗹 😳 M	IS12-021	Important	26454	<del>1</del> 10	2012-05-08	:
		🗹 😳 M	IS12-029	Critical	25968	380	2012-05-08	:
		🗹 🤨 M	IS12-029	Critical	25969	917	2012-05-08	: .
Common Tasks:		🗹 😳 M	IS12-029	Important	25983	332	2012-05-08	: .
		🗹 😳 M	IS12-030	Important	25533	371	2012-05-08	: :
New scanning profile		🗹 😳 M	IS12-030	Important	25533	371	2012-05-08	: .
Set Active		🔽 🙆 M	IS12-030	Important	25968	342	2012-05-08	
Delete	•	•						•
<u></u>	Advanced	File: la	anss 11 patchmnom	t.mdb: Version:	140: Las	t updated	d on: 21/05/2012	2 14:13:15
(2) Help:							1516	2 patches
<b></b>								
Scanning Profiles	Find update:		Find	Fine	dnext			
Languard Schpling	Search by bulletin ID (e.g. MS12-001	) or QNumb	ber (e.g. Q2644615)					
	N							

Screenshot 186: Scanning Profiles properties: Patches tab options

To enable missing patch detection checks in a particular scanning profile:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. From the Vulnerability Assessment Options tab, click Patches sub-tab.

4. Select the scanning profile that you wish to customize from the left pane under Profiles.

5. In the right pane, select **Detect installed and missing service packs/patches** option.

#### NOTE

Missing patch scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable missing patch scanning in all profiles where missing patch scanning is required.

Customizing the list of software patches to scan

To specify which missing security updates will be enumerated and processed by a scanning profile:

1. From the Vulnerability Assessment Options tab, click Patches sub-tab

2. Select the scanning profile to customize from the left pane under **Profiles**.

Bulletin names	Severity	QNumber	Date posted 🔍	Title
🗹 🔯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla 🔺
🗹 🔯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🔯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🤯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla
🗹 🔯 SeaMonkey 2.5	Critical	SeaMonkey	2011-11-22	Mozilla 🔻
٠ III				•

Screenshot 187: Select the missing patches to enumerate

3. In the right pane, select/unselect which missing patches are enumerated by this scanning profile.

Searching for Bulletin Information

Find <u>b</u> ulletin:		Find	Find next		
Search by bulletin name (e.g. MS02-017) or QNumber (e.g. Q311967).					

Screenshot 188: Searching for bulletin information

To search for a particular bulletin:

1. From **Vulnerability Assessment Options > Vulnerabilities > Find bulletin**, specify the bulletin name (example: MS02–017) or QNumber (example: Q311987), in the search tool entry box included at the bottom of the right pane.

2. Click **Find** to search for your entry.

B	ulletin Info				×
	Bulletin				
	Bulletin ID:	MS09-014	QNumber:	963027	
	Date:	2009-04-14	Severity:	Critical	
	Title:	Cumulative Security Update for Inter	net Explorer 5.	01 Service Pack 4 (KB963027)	
	Description:	Security issues have been identified Microsoft Internet Explorer and gain update from Microsoft. After you ins	that could allo control over it stall this item, y	w an attacker to compromise a system that is running . You can help protect your system by installing this you may have to restart your computer.	
	Applies To:	Windows 2000			
	URL:	http://go.microsoft.com/fwlink/?LinkI	d=146659		
				Clos	e

Screenshot 189: Extended bulletin information

## 5.5.4 Configuring Network & Software Audit options

The scanning profiles that ship with GFI LanGuard are already pre–configured to run a number of network and software audit checks on selected target. You can however disable scanning as well as customize the list of network and software audits executed during a scan.

This section contains information about:

- » Configuring TCP/UDP port scanning options
- » Configuring System Information options
- » Configuring Device scanning options
- » Configuring Applications scanning options

## Configuring TCP/UDP port scanning options

8 GFI LanGuard Scanning Profiles Edit	or				_	
Scanning Profiles				<b>(</b> ) *	Discuss this version	xn
Profile categories:	Culnerabili 🍋	ty Assessment Options	💫 Network & Software	Audit Options	💐 Scanner Option	IS
Complete/Combination Scans Vulnerability Assessment	TCP Ports U	OP Ports System Inform	ation Devices Applicatio	ins		
🥵 Network & Software Audit	Choose scan profile conditions.  Image: Choose scan profile conditions in the scale of the scale					
Profiles:	Ports 🔺	Description				
Section 2017 Full Vulnerability Assessment	1	TCP Port Service Mult	tiplexer			*
Note: Full Scan (Active)	2 🕤 🕐 2	Compressnet Manage	ement Utility, If this service is	not installed bewar	e could be trojan: Dea	th 🔲
Networks) 😽 😽	3	Compressnet Compre	ession Process			
	5	Remote Job Entry, If	this service is not installed be	ware could be troja	an: yoyo	
	7	Echo				
	11	Active Users, If this s	service is not installed beware	could be trojan: Sk	tun	
	13	DAYTIME - (RFC 867)	)			
	17	Quote of the Day				
	18	Message Send Protoc	ol, If this service is not install	ed beware could be	e trojan: Skun	
	19	Character Generator				
Common Tasks:	20	FTP - data, If this ser	vice is not installed beware co	ould be trojan: Ama	inda	
New scanning profile	21	FIP - control (comma	nd)			
Set Active		Secure Shell (SSH)				
Rename		Figure to the second se	ncrypted text communications			
Delete	25	Any private printer of	rotocol (SMTP)			
	S 35	Any private printer se	erver protocoi			-
🕐 Help:						•
Scanning Profiles	Advanced Add					
Landuard Scripting	! If you add,	edit or remove a port, the	changes will be applied to all	the profiles.		
						.:

#### Screenshot 190: Scanning Profiles properties: TCP Ports tab options

Option	Description
Enabling/disabling TCP Port scanning	To enable TCP Port Scanning in a particular scanning profile: 1. From the <b>Network &amp; Security Audit Options</b> tab, click <b>TCP Ports</b> sub-tab. 2. Select the scanning profile that you wish to customize from the left pane under <b>Profiles.</b> 3. Select <b>Enable TCP Port Scanning</b> option.
Configuring the list of TCP ports to be scanned	To configure which TCP ports will be processed by a scanning profile: 1. From <b>Network &amp; Security Audit Options</b> tab, click <b>TCP Ports</b> sub-tab. 2. Select scanning profile to customize from the left pane under <b>Profiles</b> . 3. Select TCP ports to analyze with this scanning profile.
Customizing the list TCP ports	<ol> <li>From the Network &amp; Security Audit Options tab, click TCP Ports sub-tab.</li> <li>Select the scanning profile that you wish to customize from the left pane under Profiles.</li> <li>Customize the list of TCP Ports through Add, Edit or Remove.</li> </ol>

## NOTE

The list of supported TCP/UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles

## Configuring System Information options

🔋 GFI LanGuard Scanning Profiles Edit	or	
Scanning Profiles		🕖 👻 Discuss this version
Profile categories:	🍋 Vulnerability Assessment Options 🛛 🗟 Network &	Software Audit Options
Complete/Combination Scans     Vulnerability Assessment     Network & Software Audit	TCP Ports         UDP Ports         System Information         Devices           Choose scan profile conditions.	Applications
Profiles:	Windows System Information     Retrieve basic OS information by SMB     Request server information     Identify PDC (Primary Domain Controller)	Yes Yes No
	Identify BDC (Backup Domain Controller) Enumerate trusted domains Enumerate shares Display admin shares	No No Yes
	Display hidden shares Enumerate local users Enumerate groups	Yes No
Common Tasks: New scanning profile	Enumerate users logged on locally Enumerate users logged on remotely Enumerate disk drives	Yes Yes No
Rename Delete	Request remote time of day Request information from remote registry Enumerate services	Yes Yes No
Help: <u>Scanning Profiles</u> <u>LanGuard Scripting</u>	Enumerate sessions	No Vo
		.:

Screenshot 191: Scanning Profiles properties: System Information tab options

To specify what **System Information** is enumerated by a particular scanning profile:

#### 1. From the Network & Security Audit Options tab, click System Information sub-tab.

2. Select the scanning profile that you wish to customize from the left pane under Profiles.

3. From the right pane, expand the **Windows System Information** group or Linux System Information group accordingly.

4. Select which Windows/Linux OS information is retrieved by the security scanner from scanned targets.

For example, to enumerate administrative shares in scan results, expand the **Enumerate shares** option and set the **Display admin shares** option to '**Yes**'.

#### Configuring Device scanning options

Use the Devices tab to enumerate network devices. Together with device enumeration, you can further configure GFI LanGuard to generate high security vulnerability alerts whenever a USB or Network device is detected.

This is achieved by compiling a list of unauthorized/blacklisted Network and USB devices that you want to be alerted.

🔏 GFI LanGuard Scanning Profiles Edito		x
Scanning Profiles	Ø Discuss this version	
Profile categories:	🍋 Vulnerability Assessment Options 🛛 💫 Network & Software Audit Options	
<ul> <li>Complete/Combination Scans</li> <li>Vulnerability Assessment</li> <li>Network &amp; Software Audit</li> </ul>	TCP Ports UDP Ports System Information Devices Applications Choose scan profile conditions.	
	Enable scanning for hardware devices on target computer(s)	
Profiles: Full Vulnerability Assessment Full Scan (Active) Full Scan (Slow Networks)	Network Devices USB Devices Configure which USB devices you want to mark as dangerous and which you want to have ignored in your scan results. Devices which will be marked as dangerous will have a high security vulnerability notification in the scan results. Devices which are on the ignore list will not be listed or saved to the database.	
	Create a high security vulnerability for USB devices which name contains: iPod iPad iPad iPhone	*
Common Tasks:	Ignore (Do pot list/save to db) devices which name contains:	Ŧ
<u>New scanning profile</u> <u>Set Active</u> <u>Rename</u> <u>Delete</u>		*
Help: <u>Scanning Profiles</u> <u>LanGuard Scripting</u>		Ŧ
		.::

Screenshot 192: The network devices configuration page

GFI LanGuard can also exclude from the scanning process specific USB devices that you consider safe. Such devices can be a USB mouse or keyboard. This is achieved through a safe/white list of USB devices to ignored during scanning.

Similarly you can create a separate scanning profile that enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers. In this case however, you must specify 'Bluetooth' and 'Wireless' or 'WiFi' in the unauthorized network and USB lists of your scanning profile.

All the device scanning configuration options are accessible through the two sub-tabs contained in the devices configuration page. These are the **Network Devices** tab and the **USB Devices** tab.

Use the **Network Devices** sub-tab to configure the attached network devices scanning options and blacklisted (unauthorized)/white-listed (safe) devices lists.

Use the **USB Devices** sub-tab to configure the attached USB devices scanning options and unauthorized/safe devices lists.

Option	Description
Enabling/disabling checks for all installed network devices	To enable network device (including USB device) scanning in a particular scanning profile: 1. From the <b>Network &amp; Security Audit Options</b> tab, click <b>Devices</b> sub–tab. 2. Click <b>Network Devices</b> tab. 3. Select the scanning profile to customize from the left pane under <b>Profiles</b> . 4. From the right pane, select <b>Enable scanning for hardware devices</b> on target computer(s).
	<b>NOTE</b> Network device scanning is configurable on a scan profile by scan profile basis. Make sure to enable network device scanning in all profiles where this is required.

Option	Description
Compiling a net- work device black- list/white–list	To compile a network device blacklist/white–list for a scanning profile: 1. From the Network & Security Audit Options tab, click Devices sub–tab. 2. Click Network Devices tab. 3. Select the scanning profile to customize from the left pane under Profiles. 4. In the right pane: to create a network device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under Create a high security vulnerability for network devices which name contains. For example, if you enter the word 'wireless' you will be notified through a high security vulnerability alert when a device whose name contains the word 'wireless' is detected. To create a network device white–list, specify which devices you want to ignore during network vulnerability scanning in the space provided under Ignore (Do not list/save to db) devices which name contains. NOTE Only include one network device name per line.
Configuring advanced network device scanning options	<ul> <li>From the Network Devices tab, you can also specify the type of network devices checked by this scanning profile and reported in the scan results. These include 'wired network devices', 'wireless network devices', 'software enumerated network devices' and 'virtual network devices'. To specify which network devices to enumerate in the scan results:</li> <li>1. From the Network &amp; Security Audit Options tab, click Devices sub-tab.</li> <li>2. Click on the Network Devices tab (opens by default).</li> <li>3. Select the scanning profile that you wish to customize from the left pane under Profiles.</li> <li>4. Click Advanced at the bottom of the page.</li> <li>5. Set the required options to Yes. Click OK to finalize your settings.</li> </ul>
Scanning for USB devices	To compile a list of unauthorized/unsafe USB devices: 1. From the Network & Security Audit Options tab, click the Devices sub-tab. 2. Click USB Devices tab. 3. Select the scanning profile that you wish to customize from the left pane under Profiles. 4. In the right pane. specify which devices you want to classify as high security vulnerabilities in the space provided under Create high security vulnerability for USB devices which name contains. For example, if you enter the word 'iPod', you will be notified through a high security vulnerability alert when a USB device whose name contains the word 'iPod' is detected. To create a USB device white–list, specify which USB devices you want to ignore during network vulnerability scanning in the space provided under Ignore (Do not list/save to db) devices which name contains. NOTE Only include one USB device name per line.

Configuring Applications scanning options

The **Applications** tab enables you to specify which applications will trigger an alert during a scan.

💈 GFI LanGuard Scanning Profiles Edito	or			
Scanning Profiles			<b>@</b> *	Discuss this version
Profile categories:	Vulnerability Assessment Optio	ns 🛛 🗟 Network & Softwa	are Audit Options	Kanner Options
<ul> <li>Vulnerability Assessment</li> <li>Network &amp; Software Audit</li> </ul>	TCP Ports UDP Ports System I Choose scan profile conditions.	nformation Devices Applic	ations	
Enable scanning for installed applications on target computer(s)				
Profiles:	Unauthorized Applications A	dvanced Options		
<b>Full Vulnerability Assessment</b> Full Scan (Active)	Specify which installed applications a	re authorized/un-authorized an	d which you do not nee	ed to be notified about.
Networks)	NOTE: When an application is not au	thorized a high security vulnera	ability warning will be ge	enerated.
Specify which applications are authorized to be installed: <ul> <li>Only the applications in the list below</li> <li>All applications except the ones in the list below</li> </ul>				
	Application 1			
	Application 2	V1.0	Publisher A	
Common Tasks:	Application 3	V2.0	Publisher B	
<u>New scanning profile</u> <u>Set Active</u> <u>Rename</u> <u>Delete</u>	Ignore (Do not list/save to db) appli	ations in the list below:	Add	Edit Remove
	Application name	Version	Publisher	
Welp:				
Scanning Profiles				
LanGuard Scripting			Add	Edit Remove
				.:

Screenshot 193: The applications configuration page

Through this tab, you can also configure GFI LanGuard to detect and report unauthorized software installed on scanned targets and to generate high security vulnerability alerts whenever such software is detected.

Option	Description
Scanning installed applications	By default,GFI LanGuard also supports integration with particular security applications. These include various antivirus and antispyware software. During security scanning, GFI LanGuard checks the correct configuration of virus scanner(s) or antispyware software and that the respective definition files are up to date. Application scanning is configurable on a scan profile by scan profile basis and all the configuration options are accessible through the two sub-tabs contained in the <b>Applications</b> tab. These are the <b>Unauthorized</b> <b>Applications</b> sub-tab and the <b>Advanced Options</b> sub-tab.
Enabling/disabling checks for installed applications	To enable installed applications scanning in a particular scanning profile: 1. From the <b>Network &amp; Security Audit Options</b> tab, click on the <b>Applications</b> sub–tab. 2. Click on the <b>Unauthorized Applications</b> sub–tab. 3. Select the scanning profile that you wish to customize from the left pane under <b>Profiles</b> . 4. Select the <b>Enable scanning for installed applications on target computer(s)</b> checkbox.
	<b>NOTE</b> Installed applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable installed applications scanning in all profiles where this is required.

Option	Description
Compiling installed applic- ations black- list/white–list	To compile installed applications blacklist/white–list: 1. From the Network & Security Audit Options tab, click Applications sub-tab. 2. Select Unauthorized Applications sub-tab. 3. Select the scanning profile to customize from the left pane under Profiles. 4. From the right pane, select Enable scanning for installed applications on target computer(s) checkbox. 5. Specify the applications that are authorized for installation. Select from: • Only the applications in the list below - Specify names of applications that are authorized for installation. These applications will be ignored during a security scan • All applications except the ones in the list below - Specify the names of the applications that are unau- thorized for installation. Applications not in this list will be ignored during a security scan. 6. In the Ignore (Do not list/save to db) applications from the list below options key in applications by clicking Add. Any application listed is white–listed. NOTE Include only one application name per line.
Advanced applic- ation scanning options	<ul> <li>GFI LanGuard ships with a default list of antivirus and antispyware applications that can be checked during security scanning.</li> <li>The Advanced Options tab enables you to configure when GFI LanGuard will generate high security vulnerability alerts if it detects certain configurations of a security application.</li> <li>Alerts are generated when:</li> <li>No antivirus, antispyware or firewall is detected</li> <li>A fake antivirus or antispyware is detected</li> <li>Antivirus or antispyware definitions are not up to date</li> <li>Antivirus or antispyware product is expired</li> <li>Antivirus or antispyware product is expired</li> <li>Antivirus or antispyware product detects malware on the scanned computer(s)</li> <li>Firewall is disabled</li> <li>HTTP/FTP timeout when checking for product updates on remote sites. This option generates an alert if the number of seconds defined for timeout is exceeded.</li> </ul>
Enabling/disabling checks for security applications	<ul> <li>To enable checks for installed security applications in a particular scanning profile:         <ol> <li>From the Network &amp; Security Audit Options tab, click on the Applications sub-tab.</li> <li>Click on the Advanced Options tab.</li> <li>Select the scanning profile that you wish to customize from the left pane under Profiles.</li> <li>Select Enable scanning for installed applications on target computer(s) checkbox.</li> </ol> </li> <li>Agent-less scans) Select Enable full security applications audit for agent-less scans checkbox.</li> <li>MOTE         <ol> <li>Agent-less scans temporarily runs a small service on the remote computers in order to retrieve the relevant information.</li> <li>Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.</li> <li>The number of supported security applications is constantly updated. Click the link available in order to get the latest version of the list. Configuring security applications sub-tab.</li> <li>Click Advanced Options tab.</li> <li>Select the scanning profile that you wish to customize from the left pane under Profiles.</li> <li>Select Enable scanning for installed security applications sub-tab.</li> <li>Click Advanced Options tab.</li> <li>Select the scanning profile that you wish to customize from the left pane under Profiles.</li> <li>Select Enable scanning for installed applications on target computer(s) checkbox.</li> <li>Griek Thable scanning for installed applications on target computer(s) checkbox.</li> <li>Griek the scanning profile that you wish to customize from the left pane under Profiles.</li> <li>Select these scanning for installed applications on target computer(s) checkbox.</li> <li>Griek thes</li></ol></li></ul>
	Security applications scanning are configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.

## 5.5.5 Configuring security scanning options

Use **Scanner Options** tab to configure the operational parameters of the security–scanning engine. These parameters are configurable on a scan profile by scan profile basis and define how the scanning engine will perform target discovery and OS Data querying.

🔋 GFI LanGuard Scanning Profiles Edit	or	
Scanning Profiles		🕖 🔭 Discuss this version
Profile categories:	Vulnerability Assessment Options 🛛 💫 Network & Software	Audit Options 🔍 Scanner Options
Complete/Combination Scans     Vulnerability Assessment     Network & Software Audit	Specify network discovery and other parameters on how the scanner	is to discover machines and output debug information.
	<ul> <li>Network Discovery Methods</li> </ul>	
	NetBIOS queries	Yes
Profiles:	SNMP queries	Yes
No. 10 Tell Vulnerability Assessment	Ping sweep	Yes
National (Active)	Custom TCP discovery (e.g. 21, 25, 80)	
🔩 Full Scan (Slow Networks)	Network Discovery Options	
	Scanning delay (default 100 ms)	100
	Network discovery query responses timeout (default 500 ms)	500
	Number of retries (default 1)	1
	Include non-responsive computers	No
	Perform a TCP port probing in order to detect mobile devices	No
	Network Scanner Options	
	Scanning threads count	3
Common Tasks:	NetBIOS Query Options	
New energies and the	Scope ID	
New scanning profile	SNMP Query Options	
Set Active Rename	Load SNMP enterprise numbers	Yes
Delete	Community strings (e.g. public, private)	public, private
<u></u>	Global Port Query Options	
Help:	TCP port scan query timeout (default 1500 ms)	1500
🥑 пар.	UDP port scan query timeout (default 600 ms)	600
Scanning Profiles		<b>(</b> *
LanGuard Scripting		
	<u>p</u>	

Screenshot 194: Scanning Profiles properties: Scanner Options tab

Configurable options include timeouts, types of queries to run during target discovery, number of scanning threads count, SNMP scopes for queries and more.

## IMPORTANT

Configure these parameters with extreme care! An incorrect configuration can affect the security scanning performance of GFI LanGuard.

To configure scanner options:

1. From **Scanning Profile Editor > Profile categories**, select the category that contains the scanning profile you want to edit (example: **Complete/Combination Scans**).

2. From the **Profiles** section, select the scanning profile you want to edit (example: Full Vulnerability Assessment).

- 3. From the right pane, click Scanner Options.
- 4. Configure the following parameters that determine the scanning behavior of GFI LanGuard:

Parameter	Description
Network Discovery Methods	
NetBIOS queries	Enable/disable the use of NetBios queries to discover network devices.
SNMP queries	Enable/disable the use of SNMP queries to discover network devices.
Ping sweep	Enable/disable the use of Ping sweeps to discover network devices.
Custom TCP discovery	Discover online machines by querying for the specified open TCP ports.
Network Discovery Options	
Scanning delay	Key in the time interval (in milliseconds) between one scan and another.
Network discovery query responses timeout	Amount of time in milliseconds the security scanner will wait before timing out when performing a machine discovery query (NetBIOS/SNMP/Ping).
Number of retries	Number of times security scanner will retry to connect to a non-responsive machine before skipping it.
Include non-responsive computers	Run scans on all the PCs regardless of whether they are detected as being online or not.
Perform a TCP port prob- ing in order to detect mobile devices	Perform a TCP port probing in order to detect mobile devices using known ports.
Network Scanner Options	
Scanning threads count	Key in the number of scan threads that can run simultaneously.
NetBIOS Query Options	
Scope ID	Used for NetBIOS environments requiring a specific scope ID in order to allow querying.
SNMP Query Options	
Load SNMP enterprise num- bers	Specifies whether security scanner should use the OID (Object Identifier database) containing ID to Vendor map to identify the various types of devices.
Community strings	Specifies whether security scanner should use the specified community string for SNMP server detec- tion and information retrieval.
Global Port Query Options	
TCP port scan query timeout	Amount of time in milliseconds security scanner will wait during a TCP port scan before timing out and moving on to scan the next port.
UDP port scan query timeout	Amount of time in milliseconds security scanner will wait during a UDP port scan before timing out and moving on to scan the next port.
WMI Options	
WMI timeout	Amount of time in milliseconds security scanner will wait for a reply from the remote WMI server before timing out and moving on to the next scan item.
SSH Options	
SSH timeout	Amount of time in milliseconds security scanner will wait for a SSH script to return before timing out and moving on to the next scan item.
Alternative SSH port	Alternative SSH ports to use when the default port 22 is unreachable.
Scanner activity window	

Parameter	Description
Type of scanner activity out- put	Activity progress modes: simple (basic progress - start / stop of operations), or verbose (more detailed information on process flow).
Display received packets	Output TCP packets in raw format as they were received by security scanner.
Display sent packets	Output TCP packets in raw format as they were sent by security scanner.
OS Information Retrieval Options	
Create custom share if administrative privileges are disabled	If administrative shares are disabled the scanner will temporarily create a custom hidden share of the form <random guid="">\$. The share is used to retrieve data that helps identifying vulnerabilities and missing patches.</random>
Start remote registry	If the remote registry service is stopped on the scanned machine, enable this option to temporarily open it during the security scanning.

# 5.6 Utilities

GFI LanGuard provides you with a set of network utilities that enable you to monitor network activity, gather network information and audit network devices.

Topics in this section:

5.6.1 DNS Lookup	270
5.0.1 DNS LOOKup	
5.6.2 Traceroute	
5.6.3 Whois	
5.6.4 Enumerate Computers	
5.6.5 Enumerate Users	
5.6.6 SNMP Auditing	
5.6.7 SNMP Walk	278
5.6.8 SQL Server® Audit	
5.6.9 Command Line Tools	

## 5.6.1 DNS Lookup

DNS lookup resolves domain names into the corresponding IP address and retrieves particular information from the target domain (for example, MX record, etc.).

To resolve a domain/host name:

1. Launch GFI LanGuard.

- 2. Click Utilities tab and select DNS Lookup in the left pane under Tools.
- 3. Specify the hostname to resolve in Hostname/IP to resolve.

🧳 GFI LanGuard	
🔲 🔹 🔶 🔶 Dashb	oard Scan Remediate Activity Monitor Reports Configuration Utilities 🕑 🔭 Discuss this version
Tools:	Hostname/IP to resolve: gfi.com   Retrieve Options
Whois	Starting DNS Lookup Request for gfi.com: 14:39:19
SNMP Audit	Performing DNS Lookup operation through DNS Server 192.168.2.1 <u>Resolving host afi.com</u> Please wait
🐳 SQL Server Audit	Basic information results: A: 215.134.217.18 (gfi.com) NS: ns1.gfi.com NS: ns2.gfi.com
Credentials:	A: 216.134.217.110 (ns1.gfi.com)
Authenticate using: Currently logged on user	MX Priority: 10, MX Server: gfi.com.primx.na0108.smtproutes.com         MX Priority: 90, MX Server: gfi.com.bak-mx.na0108.smtpbak.com         NS: ns2.gfi.com         NS: ns1.gfi.com         A: 216.134.217.110 (ns1.afi.com)
Password:	
✓       Remember credentials         ✓       Use per computer credentials	Completed DNS Lookup Request for gfi.com: 14:39:20
Common Tasks.	
Edit DNS lookup options	

Screenshot 195: DNS Lookup tool

4. Under **Common Tasks** in the left pane, click on **Edit DNS Lookup options** or click **Options** on the right pane and specify the information described below:

Option	Description
Basic Information	Retrieve the host name and the relative IP address.
Host Information	Retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.
Aliases	Retrieve information on the 'A Records' configured on the target domain.
MX Records	Enumerate all the mail servers and the order (i.e. priority) in which they receive and process emails for the target domain.
NS Records	Specify the 'name–servers' that are authoritative for a particular domain or sub domain.

## NOTE

Some DNS entries do not contain certain information for security reasons.

DNS Lookup Options	×
General	
Specify DNS Lookup information to be retrieved and the DNS server to be used	2
Retrieve the following information:	
✓ Basic information ✓ Host information ✓ Aliases	
MX Records VS Records	
DNS Server(s) to query: <ul> <li>Use default DNS server</li> <li>Use alternative DNS server(s)</li> </ul> Add Remove	
OK Cancel Apply	

Screenshot 196: DNS Lookup tool options

5. (Optional) Specify the alternative DNS server that will be queried by the DNS Lookup tool or leave as default to use the default DNS server.

6. Click **Retrieve** to start the process.

## 5.6.2 Traceroute

Traceroute identifies the path that GFI LanGuard followed to reach a target computer.

🜒 GFI LanGuard							
Dashb	oard	Scan	Remediate Activity Monitor Reports	Configur	ation Util	ities 🕐 🔹	Discuss this version
Tools:	Trace	(domain/lf	P address/name): gfi.com		route	Dptions	
	Нор	Itera	IP Address (Hostname)	Time (ms)	Best time	Average	Worst tim
剩 Whois	$\sqrt{1}$	1	192, 168, 2, 1	0	0	0.00	0
Enumerate Computers	V2	1	10.36.188.1	6	6	6.00	6
Enumerate Users	<b>√</b> 3	1	212.56.130.1 (vl03-north01.csr01.melita.com)	6	6	6.00	6
SNMP Audit	<b>V</b> 4	1	212.56.129.100 (g200-south02.csr01.melita.c	8	8	8.00	8 =
SNMP Wak	√ 5	1	151.5.142.1	16	16	16.00	16
SQL Server Audit	<b>√</b> 6	1	151.6.125.194 (PAVB-B01-Ge2-0.70.wind.it)	14	14	14.00	14
	17	1	151.6.4.161	40	40	40.00	40
	<b>√</b> 8	1	151.6.1.129	42	42	42.00	42
Condentiale	<b>√</b> 9	1	212.245.228.30	72	72	72.00	72
	🗸 10	1	212.73.241.153	42	42	42.00	42
Authenticate using:	✓ 11	1	4.69.142.189 (ae-0-11.bar1.Milan1.Level3.net)	43	43	43.00	43
Currently logged on user 🔹	√ 12	1	4.69.142.186 (ae-7-7.ebr2.Paris1.Level3.net)	61	61	61.00	61
Usemame:	🗸 13	1	4.69.143.126 (ae-23-23.ebr2.Paris1.Level3.n	57	57	57.00	57
	🗸 14	1	4.69.137.50 (ae-41-41.ebr2.Washington1.Le	138	138	138.00	138 🔻
Password:			(		)		
Remember condentials		1,200 -					
		1,000					
Use per computer credentials	t t	800					
	8	600					
Common Tasks:	l 🏻	400	· · · · · · · · · · · · · · · · · · ·				
Edit traceroute options		200	0 6 6 8 16 14 40	42 7	2 42 4	3 - 61 - 9	138 145 154 <b>[</b>
		-	1 2 3 4 5 6 7	8 9	10 1	1 12 1	13 14 15 16
	•						4
Ready							.:

Screenshot 197: Traceroute tool

To use the Traceroute tool:

1. Launch GFI LanGuard.

2. Click Utilities tab and select Traceroute in the left pane under Tools.

3. In the **Trace (domain/IP/name)**, specify the name/IP or domain to reach.

4. (Optional) Under **Common Tasks** in the left pane, click on **Edit Traceroute options** or click **Options** on the right pane to change the default options.

5. Click on the **Traceroute** button to start the tracing process.

Traceroute will break down, the path taken to a target computer into 'hops'. A hop indicates a stage and represents a computer that was traversed during the process.

The information enumerated by this tool includes the IP of traversed computers, the number of times that a computer was traversed and the time taken to reach the respective computer. An icon is also included next to each hop. This icon indicates the state of that particular hop. The icons used in this tool include:

lcon	Description
$\checkmark$	Indicates a successful hop taken within normal parameters.
<u>.</u>	Indicates a successful hop, but time required was quite long.
<b>A</b>	Indicates a successful hop, but the time required was too long.
x	Indicates that the hop was timed out (> 1000ms).

## 5.6.3 Whois

Whois looks up information on a particular domain or IP address.



Screenshot 198: Whois tool

1. Launch GFI LanGuard.

2. Click Utilities tab and select Whois in the left pane under Tools.

3. In **Query (domain/IP/name)** menu, specify the name/IP or domain to reach.

4. (Optional) From **Common Tasks** in the left pane, click **Edit Whois options** or **Options** on the right pane to change the default options.

5. Click **Retrieve** to start the process.

## 5.6.4 Enumerate Computers

🥑 GFI LanGuard				
Dashb	oard Scan	Remediate Activity Monitor	Reports Configuration Utilities 🖉 🕆 Discuss this version.	
Tools:	Enumerate com	outers in domain:	P   Retrieve Options	
Traceroute	Name	Operating System	Туре	
whois	MTMMG9	Windows 7	Workstation	*
Enumerate Computers	MTMMG9	Windows 7	Workstation	
SNMP Audt	ERV08-06	Windows Server 2008 R2	Server	
SNMP Walk	E TC-DELL	Windows XP	Workstation	
SQL Server Audit	WIN7_03	Windows 7	Workstation	
	WIN7_06	Windows 7	Workstation	
Credentials: Authenticate using: Currently logged on user  Usemame: Password: Remember credentials Use per computer credentials	4			- v
Common Tasks:	Start gathering	j information	v	
Edit enumerate computers options	Getting the compu Ready. Found 6	uters of WORKGROUP computers.		
Found 6 computers		Domain: WORKGROUP		.::

Screenshot 199: Enumerate Computers tool

The enumerate computers utility identifies domains and workgroups on a network. During execution, this tool will also scan each domain/workgroup discovered so to enumerate their respective computers.

- » The information enumerated by this tool includes:
- » The domain or workgroup name
- » The list of domain/workgroup computers
- » The operating system installed on the discovered computers
- » Any additional details that might be collected through NetBIOS.

Computers are enumerated using one of the following methods:

Option	Description
From Active Dir- ectory®	This method is much faster and will include computers that are currently switched off.
From Windows Explorer	This method enumerates computers through a real–time network scan and therefore it is slower and will not include computers that are switched off.

To enumerate computers:

- 1. Launch GFI LanGuard.
- 2. Click Utilities tab and select Enumerate Computers in the left pane under Tools.
- 3. In the **Enumerate computers in domain**, select the desired domain.
- 4. From **Common Tasks** in the left pane, click **Edit Enumerate Computers options** or **Options** on the right pane.

5. Select whether to enumerate computers from Active Directory<sup>®</sup> or Windows Explorer.

6. Click **Retrieve** to start the process.

## NOTE

For an Active Directory<sup>®</sup> scan, you will need to run the tool under an account that has access rights to Active Directory<sup>®</sup>.

## Starting a Security Scan

To start a security scan directly from the 'Enumerate Computers' tool, right–click on any of the enumerated computers and select Scan.

You can also launch a security scan and at the same time continue using the Enumerate Computers tool. This is achieved by right-clicking on any of the enumerated computers and selecting Scan in background.

## Deploying Custom Patches

You can use the Enumerate Computers tool to deploy custom patches and third party software on the enumerated computers. To launch a deployment process directly from this tool:

1. Select the computers that require deployment.

2. Right-click on any of the selected computers and select **Deploy Custom Patches**.

## Enabling Auditing Policies

The Enumerate Computers tool also enables you to configure auditing policies on particular computers. This is done as follows:

1. Select the computers on which you want to enable auditing policies.

2. Right–click on any of the selected computers and select **Enable Auditing Policies**. This will launch the **Auditing Policies configuration Wizard** that will guide you through the configuration process.

## 5.6.5 Enumerate Users

🌒 GFI LanGuard				• <b>X</b>			
📃 🖛 🧄 🔶 🕞 Dashb	oard Scan Reme	diate Activity Monitor Report	s Configuration Utilities 🕖 🔭 Discuss this version	L			
Tools:	Enumerate users in dom	ain: Usability 🔻	<u>R</u> etrieve Options				
Traceroute	User name	Full name	Description	Pass			
Whois	Administrator	Administrator	Built-in account for administering the computer/domain				
Enumerate Computers	🔊 Guest		Built-in account for guest access to the computer/domain	Yes			
Enumerate Users	🔊 krbtgt		Key Distribution Center Service Account				
SNMP Audit	🔔 hr.manager	HR Manager					
SQL Server Audit	🔔 it.manager	IT Manager					
	🔔 sales 1	Sales 1					
	🔔 sales2	Sales 2					
	🔔 sales.manager	Sales Manager					
Credentials:	🔔 dave.williams	Dave Williams	CEO				
Authenticate using:	🔔 hr 1	HR 1					
Currently logged on user 🔹	🔔 hr2	HR 2					
Usemame:	🚨 marketing.manager	Marketing Manager					
	🚨 marketing1	Marketing 1					
Password:	🚨 marketing2	Marketing 2					
	🔔 it1	Π1					
✓ Remember credentials	🔔 it2	IT 2					
✓ Use per computer credentials	accountsmanger	Accounts Manager					
	•	III					
Common Tasks:	Start gathering users	(	···· <b>v</b> ········				
Edit enumerate users options	Attempting to connect to the Usability domain Error: Could not connect to the Usability domain with the supplied credentials. Check the user name and password Retrieving first 0 users details Found 0 users Ready. Found users NOTE : Possible reasons for this:						
Found 0 users							

Screenshot 200: The Enumerate Users tool dialog

To scan the Active Directory<sup>®</sup> and retrieve the list of all users and contacts included in this database:

#### 1. Launch GFI LanGuard.

- 2. Click Utilities tab and select Enumerate Users in the left pane under Tools.
- 3. In the **Enumerate users in domain** menu, select the desired domain.

4. From **Common Tasks** in the left pane, click **Edit Enumerate Users options** or **Options** on the right pane to filter the information to extract and display only the users or contacts details. In addition, you can optionally configure this tool to highlight disabled or locked accounts.

5. Click **Retrieve** to start the process.

#### NOTE

This tool can enable or disable enumerated user accounts. Right–click on the account and select **Enable/Disable account** accordingly.

## 5.6.6 SNMP Auditing

GFI LanGuard uses the Simple Network Management Protocol (SNMP) to obtain information, like hardware specifications and operating system version, from network devices, such as servers, computers, printers, hubs, switches, and routers. Through SNMP, GFI LanGuard can monitor network performance, audit network usage and detect network faults.

## IMPORTANT

GFI LanGuard supports SNMPv1 and SNMPv2c. SNMPv3 and SNMP over TLS / DTLS are NOT supported.

💞 GFI LanGuard ■■ 🔹 🍖 I 🔶 I → Dashbi	oard Scan Re	mediate Act	ivity Moni	itor R	eports	Configu	ration	Utilities	(2) - Di	iscuss th	is version	• <b>×</b>
Tools:	IP address or range	of IP addresses for	computer(:	s) running 9	6N <u>M</u> P: [	127.0.0.1		•	<u>R</u> etrie	ve	Options	
<ul> <li>DIVS LOOKUP</li> <li>Traceroute</li> <li>Whois</li> <li>Enumerate Computers</li> <li>Enumerate Users</li> <li>SNMP Audit</li> <li>SNMP Walk</li> <li>SQL Server Audit</li> </ul>	IP Address	Computer	public	private	all pri	router	cisco	admin	ргоху	write	access	root
Credentials:												
Authenticate using: Currently logged on user  Usemame: Password:												
<ul> <li>Remember credentials</li> <li>Use per computer credentials</li> </ul>												
Common Tasks: Edit SNMP audit options												
	•											4
												.:

Screenshot 201: SNMP Audit tool

This tool identifies weak SNMP community strings by performing a dictionary attack using the values stored in its default dictionary file (snmp-pass.txt).

You can add new community strings to the default dictionary file by using a text editor (for example, notepad.exe).

You can also direct the SNMP Audit tool to use other dictionary files. To achieve this, specify the path to the dictionary file from the Options dialog.

To perform SNMP audits on network targets and identify weak community strings:

1. Launch GFI LanGuard.

2. Click Utilities tab and select SNMP Audit in the left pane under Tools.

3. In the **IP of computer running SNMP**, specify the IP to reach.

4. From **Common Tasks** in the left pane, click **Edit SNMP Audit options**, or use the **Options** button available in the topright section of the screen, to edit the default options.

5. Click **Retrieve** to start the process.

## 5.6.7 SNMP Walk

GFI LanGuard uses the Simple Network Management Protocol (SNMP) to obtain information, like hardware specifications and operating system version, from network devices, such as servers, computers, printers, hubs, switches, and routers. Through SNMP, GFI LanGuard can monitor network performance, audit network usage and detect network faults.

## IMPORTANT

GFI LanGuard supports SNMPv1 and SNMPv2c. SNMPv3 and SNMP over TLS / DTLS are NOT supported.

🥑 GFI LanGuard				
Dashb	oard Scan	Remediate Activity Monitor Report	s Configuration Utilities 🕐 🔹	Discuss this version
Tools:	IP addr <u>e</u> ss:	127.0.0.1	<u>R</u> etrieve Options	]
<ul> <li>DNS Lookup</li> <li>Traceroute</li> <li>Whois</li> </ul>	Description:	iso.org.dod.internet.mgmt.mib-2.system		
Enumerate Computers     Enumerate Users     SNMP Audit     SNMP Walk     SQL Server Audit			Name	Value
Credentials:		▷ snmpDot3MauMgt ▷ etherMIB		
Authenticate using: Currently logged on user Usemame: Password:		dot55rMIB     egp    entityMIB		
<ul> <li>Remember credentials</li> <li>Use per computer credentials</li> </ul>		▷ - □ icmp ▷ - □ ipMIB ▷ - □ interfaces ▷ - □ ifMIB		
Common Tasks: Edit SNMP walk options				
Found 0 items				.:

Screenshot 202: SNMP Walk tool

To probe your network nodes and retrieve SNMP information (for example, OID's):

1. Launch GFI LanGuard.

#### 2. Click Utilities tab and select SNMP Walk in the left pane under Tools.

3. In the IP address menu, specify the IP address of the computer that you wish to scan for SNMP information.

4. From **Common Tasks** in the left pane, click **Edit SNMP Audit options**. Alternatively use the **Options** button available in the top-right section of the screen, to edit the default options, such as providing alternative community strings.

5. Click **Retrieve** to start the process.

#### IMPORTANT

SNMP activity is normally blocked at the router / firewall so that internet users cannot SNMP scan your network. Malicious users can use information collected through SNMP scanning to hack your network or systems. Unless this service is required, it is highly recommended to disable it.

## 5.6.8 SQL Server<sup>®</sup> Audit

This tool enables you to test the password vulnerability of the 'sa' account (i.e. root administrator), and any other SQL user accounts configured on the SQL Server<sup>®</sup>. During the audit process, this tool will perform dictionary attacks on the SQL Server<sup>®</sup> accounts using the credentials specified in the 'passwords.txt' dictionary file. However, you can also direct the SQL Server<sup>®</sup> Audit tool to use other dictionary files. You can also customize your dictionary file by adding new passwords to the default list.

To perform a security audit on a particular SQL Server<sup>®</sup> installation:

- 1. Launch GFI LanGuard.
- 2. Click Utilities tab and select SQL Server Audit in the left pane under Tools.



Screenshot 203: SQL Server<sup>®</sup> Audit

3. In the Audit MS SQL Server menu, specify the IP address of the SQL Server® that you wish to audit.

4. From **Common Tasks** in the left pane, click **Edit SQL Server**<sup>®</sup> **Audit options** or **Options** button on the right pane to edit the default options such as performing dictionary attacks on all the other SQL user accounts.

5. Click **Audit** to start the process.

## 5.6.9 Command Line Tools

The command line tools enable 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.

Use the information in this section to learn how to run patch management functions using the following CMD tools:

- » Lnsscmd.exe
- » Deploycmd.exe
- » Impex.exe

Using Insscmd.exe

The 'Insscmd.exe' command line target–scanning tool allows you to run vulnerability checks against network targets directly from the command line, or through third party applications, batch files and scripts. The 'Insscmd.exe' command line tool supports the following switches:

```
lnsscmd <Target> [/profile=profileName] [/report=reportPath]
[/reportname=reportName] [/output=pathToXmlFile] [/user=username
/password=password] [/Email [/EmailAddress=EmailAddress]] [/DontShowStatus]
[/UseComputerProfiles] [/Wake] [/Shutdown [/ShutdownIntervalStart=<hh:mm:ss>]
[/ShutdownIntervalEnd=<hh:mm:ss>]] [/?]
```

#### Insscmd command switches

Switch	Description
Target	Specify the IP / range of IPs or host name(s) to be scanned.
/Profile	(Optional) Specify the scanning profile that will be used during a security scan. If this parameter is not specified, the scanning profile that is currently active in the GFI LanGuard will be used.
	<b>NOTE</b> In GFI LanGuard, the default (i.e. currently active) scanning profile is denoted by the word (Active) next to its name. To view which profile is active expand the <b>Configuration</b> tab > <b>Scanning Profiles</b> node.
/Output	(Optional) Specify the full path (including filename) of the XML file where the scan results will be saved.
/Report	(Optional) Directory or full file name for the output scan report.
/ReportName	(Optional) Name of the report to generate. If not specified, the report is saved with a default name.
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during security scanning. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the dashboard.
/Email	(Optional) Send the resulting report by e-mail. The e-mail address and mail server specified in <b>Con-</b> figuration > Alerting Options are used.
/EmailAddress	(Optional) Dependent on <b>/Email</b> . Overrides the general alerting options and uses the specified email address.
/DontShowStatus	(Optional) Include this switch if you want to perform silent scanning. In this way, the scan progress details will not be shown.
/UseComputerProfiles	(Optional) Use per computer credentials when available.
/Wake	(Optional) Wake up offline computers.
/Shutdown	(Optional) Shuts down computers after scan.

Switch	Description
/ShutdownIntervalStart	(Optional) Dependent on <b>/Shutdown</b> . The start time of the interval when shutdown is allowed. Use hh:m-m:ss format.
/ShutdownIntervalEnd	(Optional) Dependent on <b>/Shutdown</b> . The end time of the interval when shutdown is allowed. Use hh:m-m:ss format.
/?	(Optional) Use this switch to show the command line tool usage instructions.

## NOTE

Always enclose full paths and profile names within double quotes. For example, "[path or path name]" or "C:\temp\test.xml".

The command line target-scanning tool allows you to pass parameters through specific variables. These variables will be automatically replaced with their respective value during execution. The table below describes the supported variables:

#### Supported variables

Variable	Description
%INSTALLDIR%	During scanning, this variable will be replaced with the path to the GFI LanGuard installation directory.
%TARGET%	During scanning this variable will be replaced with the name of the target computer.
%SCANDATE%	During scanning this variable will be replaced with the date of scan.
%SCANTIME%	During scanning this variable will be replaced with the time of scan.

### Example

1. To perform a security scan on a target computer having IP address '130.16.130.1'.

2. Output the scan results to `c:\out.xml' (i.e. XML file).

3. Generate a PDF report and save it in 'c:\result.odf'.

4. Send the PDF report via email to 'lanss@domain.com'

The command should be as follows:

lnsscmd.exe 130.16.130.1 /Profile="Default" /Output="c:\out.xml"
/Report="c:\result.pdf" /Email /emailAddress="lanss@domain.com"

#### Using deploycmd.exe

The 'deploycmd.exe' command line patch deployment tool allows you to deploy Microsoft<sup>®</sup> patches and third party software on remote targets directly from the command line, or through third party applications, batch files or scripts. The 'deploycmd.exe' command line tool supports the following switches:

```
deploycmd <target> </file=FileName> [/switches=Switches] [/username=UserName
/password=Password] [/warnuser] [/userapproval] [/stopservices]
[/customshare=CustomShareName] [/reboot] [/rebootuserdecides] [/wake] [/shutdown]
[/deletefiles] [/timeout=Timeout(sec)] [/usecomputerprofiles]
[/RebootCountdown=Time(sec)] [/RebootCountdownMessage="Custom message"]
[/RebootAtFirstOccurenceOf=Time(formatted as "hh:mm:ss")]
[/ShutDownAtFirstOccurenceOf=Time(formatted as "hh:mm:ss")] [/RebootInInterval]
[/ShutDownInInterval] [/RebootIntervalStart=Time(formatted as "hh:mm:ss")]
[/RebootIntervalEnd=Time(formatted as "hh:mm:ss")] [/?]
```

## deploycmd command switches

Switch	Description
Target	Specify the name(s), IP or range of IPs of the target computer(s) on which the patch(es) will be deployed.
/File	Specify the file that you wish to deploy on the specified target(s).
/User and /Password	(Optional) Specify the alternative credentials that the scanning engine will use to authenticate to a target computer during patch deployment. Alternatively you can use the /UseComputerProfiles switch to use the authentication credentials already configured in the Dashboard.
/warnuser	(Optional) Include this switch if you want to inform the target computer user that a file/patch installation is in progress. Users will be informed through a message dialog that will be shown on screen immediately before the deployment session is started.
/useraproval	(Optional) Include this switch to request the user's approval before starting the file/patch install- ation process. This allows users to postpone the file/patch installation process for later (for example, until an already running process is completed on the target computer).
/stopservice	(Optional) Include this switch if you want to stop specific services on the target computer before installing the file/patch.
	NOTE You cannot specify the services that will be stopped directly from the command line tool. Services can only be added or removed through the GFI LanGuard UI.
/customshare	(Optional) Specify the target share where you wish to transfer the file before it is installed.
/reboot	(Optional Parameter) Include this switch if you want to reboot the target computer after file/patch deployment.
/rebootuserdecides	(Optional Parameter) Include this switch to allow the current target computer user to decide when to reboot his computer (after patch installation).
/wake	Wakes up offline computers.
/shutdown	(Optional Parameter) Include this switch if you want to shut down the target computer after the file/patch is installed.
/deletefiles	(Optional Parameter) Include this switch if you want to delete the source file after it has been suc- cessfully installed.
/timeout	(Optional Parameter) Specify the deployment operation timeout. This value defines the time that a deployment process will be allowed to run before the file/patch installation is interrupted.
/usecomputerprofiles	(Optional) Use data from computer profiles.
/RebootCountdown	(Optional) Display a reboot countdown window for a number of seconds to the remote user before rebooting.
/RebootCountdownMessage	(Optional) Used in conjunction with <b>/RebootCountdown</b> . Displays a custom message to the remote user before rebooting the computer.
/RebootAtFirstOccurenceOf	(Optional) Reboot a computer at the first occurrence of a specified time. The time is expected in the 24 hour format "hh:mm:s s". Example, 18:30:00.
/ShutDownAtFirstOccurenceOf	(Optional) Shutdown a computer at the first occurrence of a specified time. The time is expected in the 24 hour format "hh:mm:s s". Example, 18:30:00.
/RebootInInterval	(Optional) Reboot the computer after deployment if deployment completes in the specified time interval. Otherwise wait to specify the interval manually. Requires parameters /Re-bootIntervalStart and /RebootIntervalEnd.

Switch	Description
/ShutdownIntervalStart	(Optional) Dependent on <b>/Shutdown</b> . The start time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutdownIntervalEnd	(Optional) Dependent on <b>/Shutdown</b> . The end time of the interval when shutdown is allowed. Use hh:mm:ss format.
/ShutDownInInterval	(Optional) Shutdown the computer after deployment if deployment completes in the specified time interval. Otherwise wait to specify the interval manually.
/?	(Optional) Use this switch to show the command line tool's usage instructions.

#### Example

1. Deploy a file called 'patchA001002.XXX'.

2. On target computer 'TMJohnDoe'.

3. Reboot the target computer after successful deployment of the file.

The command should be as follows::

deploycmd TMJohnDoe /file="patchA001002.XXX" /reboot

Using impex.exe

The Impex tool is a command line tool that can be used to Import and Export profiles and vulnerabilities from GFI LanGuard Network Security Scanner. The parameters supported by this tool are the following:

impex [[/H] | [/?]] | [/XML:xmlfile [/DB:dbfile] [[/EX] [/MERGE]] | [/IM [/ONLYNEWER]] [/PROFILES | /VULNS | /PORTS | /PROFILE:name | /VULNCAT:cat [/VULN:name] | /PORTTYPE:type [/PORT:number]] [/SKIP | /OVERWRITE | /RENAME:value]]

Switch	Description
/H /? Run impex without parameters	Displays help information.
/XML: <xmlfile></xmlfile>	This parameter specifies the name of the imported or exported XML file. <xmlfile> needs to be replaced with the name of the file the profile is being exported to.           NOTE           This parameter is mandatory to import or export alerts.</xmlfile>
/DB: <dbfile></dbfile>	Where <dbfile> is the database file to be used during the import/export operation. If this is not specified the default "operationsprofiles.mdb" file will be used.</dbfile>
/EX	Exports data from database to XML file (Default option)
/MERGE	If this is specified when the target XML for export already exists, the file will be opened and data will be merged; otherwise the XML file is first deleted.
/IM	Imports data from XML file to database
/ONLYNEWER	When specified only vulnerabilities newer than the newest vulnerability in the database will be imported.
/PROFILES	Exports/Imports all scanning profiles.
/VULNS	Exports/Imports all vulnerabilities.

#### impex command switches

Switch	Description
/PORTS	Exports/Imports all ports
/PROFILE: <name></name>	Exports/Imports the specified scanning profile.
/VULNCAT: <category></category>	Exports/Imports all vulnerabilities of the specified category.
/VULN: <name></name>	Exports/Imports the specified vulnerability (/VULNCAT must be specified).
/PORTTYPE: <type></type>	Exports/Imports all ports of the specified type.
/PORT: <number></number>	Exports/Imports the specified port (/PORTTYPE must be specified).
/SKIP	If an item already exists in the target XML/database, that item will be skipped
/OVERWRITE	If an item already exists in the target XML/database, that item will be overwritten.
/RENAME: <value></value>	If an item already exists in the target XML/database, that item will be renamed to <value>. If /PROFILE or /VULN was specified, port information merged with that item is a port or renamed by prefixing its name with <value> in any other case.</value></value>

#### Example 1

To import specific entries from an XML file:

impex /xml:regcheck.xml /vuln:"Blaster Worm" /vulncat:"Registry Vulnerabilities"

#### Example 2

To import a whole XML file:

impex /xml:regcheck.xml /im

## NOTE

The Impex executable can be located in the GFI LanGuard installation folder.

#### NOTE

If the specified <xmlfile>, <dbfile>, <name>, <category> or <value> contain any space character, the whole value must be placed between double quotes. Example:

» <xmlfile> containing space = "Vulnerability Checks Definitions.xml"

>> <xmlfile> without space = VulnerabilityChecksDefinitions.xml

#### NOTE

It is recommended that if the vulnerabilities are imported into another installed instance of GFI LanGuard; that installation will have the same build number as the one the database has been exported from.

#### IMPORTANT

It is highly recommended not to use the **Impex** tool if GFI LanGuard application (LanGuard.exe) or LanGuard scanning profiles (scanprofiles.exe) are running.

# 5.7 Script Debugger

Scripts that identify custom vulnerabilities can be created using any VBScript compatible scripting language. By default, GFI LanGuard ships with a script editor that you can use to create your custom scripts.

New checks must be included in the list of checks supported by GFI LanGuard. Use the Vulnerability Assessment tab to add new checks to the default list of vulnerability checks on a scan profile by scan profile basis. GFI LanGuard also supports Python scripting.

Topics in this section:

5.7.1 Creating custom scripts using VBscript	286
5.7.2 Creating custom scripts using Python Scripting	. 290
5.7.3 SSH Module	294

## 5.7.1 Creating custom scripts using VBscript

GFI LanGuard supports and runs scripts written in VBscript compatible languages. Use VBscript compatible languages to create custom scripts that can be run against your network targets.

Security auditing scripts can be developed using the script editor that ships with GFI LanGuard. This built–in script editor includes syntax highlighting capabilities as well as debugging features that support you during script development. Open the script editor from **Start > Programs > GFI LanGuard > LanGuard Script Debugger**.

## NOTE

For more information on how to develop scripts using the built–in script editor, refer to the **Scripting documentation** help file included in **Start > Programs > GFI LanGuard > LanGuard Scripting documentation**.

## NOTE

GFI does not support requests related to problems in custom scripts. You can post any queries that you may have about GFI LanGuard forums at http://forums.gfi.com/. Through this forum, you are able to share scripts, problems and ideas with other GFI LanGuard users.

## Adding a vulnerability check that uses a custom VBScript (.vbs)

To create new vulnerability checks that use custom VBScripts, follow the steps described in this section:

- » Step 1: Create the script
- » Step 2: Add new vulnerability checks
- » Step 3: Test the vulnerability check/script

### Step 1: Create the script

1. Launch the Script Debugger from Start > Programs > GFI LanGuard > LanGuard Script Debugger.

#### 2. Go on **File > New**.

3. Create a script. For this example, use the following sample script code.

```
Function Main
```

```
echo "Script has run successfully"
```

```
Main = true
```

End Function

4. Save the script in <LanGuard installation folder path> \Data\Scripts\myscript.vbs. Step 2: Add new vulnerability checks

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. In the new window, add a new vulnerability by clicking **Add** under the list of vulnerability checks.

Add vulneral	oility		
General C	onditions Descript	tion References	
<u>N</u> ame:	Add vulnerability	y EX	
<u>T</u> ype:	General Cond	itions Description References	
OS <u>F</u> amily:	Description:	Add vulnerability	<b>-X</b>
OS <u>V</u> ersion	This check	General Conditions Description References	
Product:			
Timestamp		CVE-2000-1161	
S <u>e</u> verity:		MS Security BID:	
		Security Focus BID:	
		1969	J
		Top 20 SANS report: <u>Y</u> ear:	
		C <u>h</u> apter:	
		OK	2

Screenshot 204: Add vulnerability dialog

4. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

5. Click the **Conditions** tab and click on the **Add** button. This will bring up the check properties wizard.

Specify what do you want to check from the list below	N
Check type:	 
Independent POP3 Banner Test	
Independent Port Open Test	
Independent Python Script Test	
Independent SMIP Banner Test	
Independent SNMP Test	
Independent TCP Rapper Test	
Independent TELNET Banner Test	=
Independent Text File Content Test	
Independent VB Script Test	
	-
Check description:	
Executes a VB script and returns a boolean value.	
•	
	-

Screenshot 205: Adding vulnerability checks - Select type of check

6. Select **Independent checks > VBScript** node and click **Next**.
| Object properties:                                 |   |
|--|---|
| Properties   | Values  |
| 🧭 Script file                                      | 404_path_disclosure.vbs   |
| How many of the mat                                | tching objects must satisfy the condition for the check to return TRUE: |
| How many of the material at least one Description: | tching objects must satisfy the condition for the check to return TRUE: |

Screenshot 206: Adding vulnerability checks - Select VB Script file

7. Click **Choose file** and select the custom VBscript file that will be executed by this check. Click **Next**.

Check properties	<b>—</b>
Step 3 of 3: Set the condition Select the attribute and the desired value(s)	<b>%</b>
Attribute:	
Operator: equals	
Value:	
Description:	
The result of the script execution. It can be 1 for TRUE, or 0 for PALSE.	Ť
< Back Finish	Cancel

Screenshot 207: Adding vulnerability checks - Define conditions

8. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

9. Click **OK** to save new vulnerability check.

Step 3: Test the vulnerability check/script

Scan your local host computer using the scanning profile where the new check was added.

In Scan tab > Results, a vulnerability warning will be shown in the Vulnerability Assessment node of the scan results.

#### 5.7.2 Creating custom scripts using Python Scripting

GFI LanGuard also supports a new type of vulnerability checks – Python Script Test. This type of check is available under the Independent Checks type.

#### IMPORTANT

For information about Python Scripting, refer to the GFI LanGuard scripting documentation from **Start > Programs > GFI LanGuard Scripting Documentation**.

To add a new python script check:

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. In the new window, add a new vulnerability by clicking **Add** under the list of vulnerability checks.

Add vulneral	bility		
General C	conditions Descr	iption References	
<u>N</u> ame:	Add vulnerabi	lity	
<u>Type</u> :	General Cor	nditions Description References	
OS <u>F</u> amily:	Description:	Add vulnerability	x
OS <u>V</u> ersion	This check	General Conditions Description References	_
		OVAL ID:	
Product:			
Timestamp		CVE ID:	
S <u>e</u> verity:		MS Security BID:	
		Security Focus BID:	
		1969	
		Top 20 SANS report:	
		C <u>h</u> apter:	
		OK Cancel	

Screenshot 208: Add vulnerability dialog

4. Go through the **General**, **Description** and **References** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

5. Click the **Conditions** tab and click on the **Add** button. This will bring up the check properties wizard.

Specify what do you want to check from the list below	~
	_
Check type:	
🛛 📝 Independent Python Script Test	
Independent TCP Banner Test	=
Independent TELNET Banner Test	
Independent Text File Content Test	
Independent vB Script Test	-
Check description:	
Executes a Python script and returns a boolean value.	
	*

Screenshot 209: Adding vulnerability checks - Select type of check

6. Select Independent checks > Independent Python Script Test node and click Next.

Object properties:	
Properties	Values
🧭 Script file	conficker.py
How many of the matc	hing objects must satisfy the condition for the check to return TRUE:
How many of the matc at least one Description:	hing objects must satisfy the condition for the check to return TRUE:

Screenshot 210: Adding vulnerability checks - Select Python Script file

7. Click **Choose file** and select the custom Python Script file that will be executed by this check. Click **Next**.

Check properties	<b>—</b>
Step 3 of 3: Set the condition Select the attribute and the desired value(s)	42
Attribute: Result	
Operator: equals	
<u>V</u> alue: 1	
Description:	
The result of the script execution. It can be 1 for TRUE, or 0 for FALSE.	*
< Back Finish	Cancel

Screenshot 211: Adding vulnerability checks - Defining conditions

8. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

9. Click **OK** to save new vulnerability check.

#### 5.7.3 SSH Module

GFI LanGuard includes an SSH module which handles the execution of vulnerability scripts on Linux/UNIX based systems.

The SSH module determines the result of vulnerability checks through the UI (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 operating system.

#### Keywords

The SSH module can run security scanning scripts through its terminal window. When a security scan is launched on Linux/UNIX based target computers, vulnerability checking scripts are copied through an SSH connection to the respective target computer and run locally.

The SSH connection is established using the logon credentials (i.e. username and password/SSH Private Key file) specified prior to the start of a security scan.

The SSH module can determine the status of a vulnerability check through specific keywords present in the text output of the executed script. These keywords are processed by the module and interpreted as instruction for the GFI LanGuard. Standard keywords identified by the SSH module include the following:

Keyword	Description
TRUE: / FALSE	These strings indicate the result of the executed vulnerability check/script. When the SSH module detects a TRUE: it means that the check was successful; FALSE: indicates that the vulnerability check has failed.
AddListItem	This string triggers an internal function that adds results to the vulnerability check report (i.e. scan results). These results are shown in GFI LanGuard after completion of a scan. This string is formatted as follows: AddListItem([[[parent node]]]], [[[[actual string]]]])
[[[[parent node]]]]	Includes the name of the scan results node to which the result will be added.
[[[actual	Includes the value that will be added to the scan results node.
5011119]]]]	<b>NOTE</b> Each vulnerability check is bound to an associated scan result node. This means that 'AddListItem' results are by default included under an associated/default vulnerability node. In this way, if the parent node parameter is left empty, the function will add the specified string to the default node.
SetDescription	This string triggers an internal function that will overwrite the default description of a vulnerability check with a new description. This string is formatted as follows: SetDescription([New description])
!!SCRIPT_ FINISHED!!	This string marks the end of every script execution. The SSH module will keep looking for this string until it is found or until a timeout occurs. If a timeout occurs before the '#SCRIPT_FINISHED!!' string is generated, the SSH module will classify the respective vulnerability check as failed.
	It is imperative that every custom script outputs the '!!SCRIPT_FINISHED!!' string at the very end of its checking process.

#### Adding a vulnerability check that uses a custom shell script

In the following example a vulnerability check is created (for Linux based targets) which uses a script written in Bash. The vulnerability check in this example will test for the presence of a dummy file called 'test.file'

#### Step 1: Create the script

1. Launch your favorite text file editor.

2. Create a new script using the following code:

```
#!/bin/bash
if [ -e test.file ]
then
    echo "TRUE:"
else
    echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
3.Save the file in <GFI LanGuard installation folder path>
..\Data\Scripts\myscript.sh
```

#### Step 2: Add the new vulnerability check

1. Launch GFI LanGuard.

2. Click the GFI LanGuard button and select **Configuration > Scanning Profile Editor**. Alternatively, press **CTRL + P** to launch the **Scanning Profiles Editor**.

3. From the middle pane, select the category in which the new vulnerability check will be included (for example, High Security Vulnerabilities...).

Add vulnerat	oility		
General C	onditions Descri	ption References	
<u>N</u> ame:	Add vulnerabil	ity 💌	
<u>Type</u> :	General Cor	nditions Description References	
OS <u>F</u> amily:	Description:	Add vulnerability	×
OS <u>V</u> ersion	This check	General Conditions Description References	
		OVAL ID:	
Product:			C>
Timestamp		<u>C</u> VE ID: CVE-2000-1161	è
Severity:		MS Security BID:	
			R R R R R R R R R R R R R R R R R R R
		Security Focus BID:	
		1969	C
		Top 20 SANS report: <u>Y</u> ear:	
		C <u>h</u> apter:	
		ОК	Cancel

4. In the new window, add a new vulnerability by clicking **Add** in the middle pane.

Screenshot 212: Add vulnerability dialog

5. Go through the **General**, **Description** and **Reference** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Choose the **Conditions** tab and click **Add** button. This will bring up the check properties wizard.

ep 1 of 3: Select the type of	check			
specify what do you want to t	neck from the list below			<b>V</b>
Check type:				
▷ · 🛅 Windows Checks				
🖉 🗁 Unix Checks				
📝 Unix File Test				
Unix Process Tes	t			
Unix RPC Service	Test			
Unix SSH Script I	est			
Selaria Chadra				
built Linux Checks				
Independent Checks				
Check description:				
Executes a SSH script on the	target computer and re	turns a boolean value or	a string.	*
				*

Screenshot 213: Adding vulnerability checks - Select type of check

7. Select **Unix checks > SSH Script Test** node and click on Next button to continue setup.

Object properties:	
Properties	Values
🧭 Script file	sans06macskype.sh
How many of the matc	hing objects must satisfy the condition for the check to return TRUE:
How many of the match at least one Description:	hing objects must satisfy the condition for the check to return TRUE:

Screenshot 214: Adding vulnerability checks - Select SSH file

8. Click **Choose file** and select the custom SSH Script file that will execute during this check. Click **Next** to proceed.

Check properties	×
Step 3 of 3: Set the condition Select the attribute and the desired value(s)	<b>%</b>
Attribute: Result (boolean)  Operator: equals	
Value:	
Description: The result of the script execution. It can be 1 for TRUE, or 0 for FALSE.	*
< Back Finish	Cancel

Screenshot 215: Adding vulnerability checks - Define conditions

9. Select the relative condition setup in the wizard to finalize script selection. Click Finish to exit wizard.

10. Click **OK** to save new vulnerability check.

#### Step 3: Test the vulnerability check/script used in the example

Scan your local host computer using the scanning profile where the new check was added.

1. Log on to a Linux target computer and create a file called 'test.file'. This check will generate a vulnerability alert if a file called 'test.file' is found.

2. Launch a scan on the Linux target where you created the file.

3. Check you scan results.

### 5.8 Configuring NetBIOS

To check if your scan targets are using NetBIOS:

1. Navigate to Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings.

#### Note

In Windows<sup>®</sup> XP, click **Control Panel > Network Connections**.

2. Right-click on Local Area Connection and select Properties.

#### 3. Click Internet Protocol (TCP/IP) and select Properties.

#### 4. Click **Advanced > WINS**.

- 5. From the NetBIOS setting area, ensure that Default or Enable NetBIOS over TCP/IP are selected.
- 6. Click **OK** and exit the **Local Area Properties** dialog(s).

#### NOTE

If static IP is being used or the DHCP server does not provide NetBIOS setting, select the Enable NetBIOS over TCP/IP option.

# 5.9 Uninstalling GFI LanGuard

To uninstall GFI LanGuard:

- 1. Click Start > Control Panel > Add or Remove Programs.
- 2. Select GFI LanGuard from the list, and click **Remove**.
- 3. In the uninstall wizard, click Next.
- 4. Select the configuration data files to remove during un-installation and click Next.
- 5. On completion, click **Finish**.

# 6 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:

6.1 Resolving common issues	
6.2 Using the Troubleshooter Wizard	
6.3 Using the Agent Diagnostics Tool	
6.4 GFI Knowledge Base	
6.5 Web Forum	
6.6 Requesting technical support	305

# 6.1 Resolving common issues

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

Issue Encountered	Solution/Description
The database structure is incorrect. Do you want to delete and recreate the database?	<ul> <li>Description</li> <li>This warning is usually encountered when trying to configure the database backend. It occurs when the database structure is corrupted.</li> <li>Or</li> <li>The database returns a timeout because the connection cannot be established.</li> <li>Solution</li> <li>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.</li> </ul>
In <b>Configuration &gt; Database Main- tenance Options &gt; Database backend</b> <b>settings</b> Microsoft Access database option is unavailable.	GFI LanGuard 12 and later versions do not support Microsoft Access databases. We recommend using Microsoft SQL Server Express which is available as a free download.

Issue Encountered	Solution/Description
Incomplete results and errors when scanning remote machines	Description         Errors similar to the following may be encountered:         >> Failed to open test key to remote registry         >> The scan will not continue         >> Access Denied         >> Could not connect to remote SMB server.
	<ul> <li>These errors may be encountered because:</li> <li>The remote machine has an account similar to the one used by GFI LanGuard to log in as an administrator.</li> <li>The user account used by GFI LanGuard does not have administrative privileges.</li> </ul>
	<ul> <li>Solution</li> <li>To solve this issue do one of the following:</li> <li>Log on the GFI LanGuard machine and configure GFI LanGuard to use an alternate domain administrator account.</li> <li>Delete the local user account on the remote machine.</li> <li>Launch GFI LanGuard executable with 'Run As' using a Domain Administrator account.</li> </ul>
	<b>NOTE</b> For more information, refer to http://go.gfi.com/?pageid=LAN_ProbScanningRM
GFI LanGuard program updates not working	<ul> <li>Description Updates will not work if GFI LanGuard machine does not have a direct connection to the Internet. Solution To solve this issue do one of the following: <ul> <li>Configure GFI LanGuard machine to have direct Internet access.</li> <li>Install another instance of GFI LanGuard on a machine with Internet access and configure GFI LanGuard to check for updates from the new installation. <li>Check your firewall settings to ensure that exceptions for the URLs used for updates are in place. For more information, refer to Gateway permissions (page 22). </li> <li>NOTE For more information refer to http://go.gfi.com/?pageid=LAN_CheckAltUpdates</li></li></ul></li></ul>
Firewall installed on GFI LanGuard is blocking connection with target com- puters	<ul> <li>Description</li> <li>Scanning might slow down or be blocked if a firewall is installed on GFI LanGuard machine.</li> <li>Solution</li> <li>Configure the firewall to allow the following components in outbound connections:</li> <li> <ul> <li>&lt;\Program Files\GFI\LanGuard&gt;\*.exe</li> <li>&lt;\Program Files\GFI\LanGuard Agent&gt;\*.exe</li> </ul> </li> </ul>
	<b>NOTE</b> For more information, refer to http://go.gfi.com/?pageid=LAN_SetBestPerformance
GFI LanGuard is failing to retrieve workgroup computers when using Enumerate Computers	<b>Description</b> 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.
	<b>NOTE</b> To solve this issue, refer to http://go.gfi.com/?pageid=LAN_CannotEnumerate

Issue Encountered	Solution/Description
GFI LanGuard found open ports that another port scanner found closed	Description         GFI LanGuard uses a different approach than other port scanners to detect open ports.         Solution         To view the status of a port and determine if the port is closed or opened:         1. Click Start > Programs > Accessories > Command Prompt.         2. Key in netstat -an, and press Enter.         3. The generated list displays all computer active connections.

# 6.2 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 > GFI LanGuard Troubleshooter**.

2. Click **Next** in the introduction page.

Troubleshooter Wizard - Gathering Information	<b>x</b>
Information Details Please select the information to gather.	•
The troubleshooter should:	
<ul> <li>Automatically detect and fix known issues (Recommended)</li> </ul>	
Gather only application information and logs. Note: Use this option when the problem is already located and only support files are needed.	
< Back Next > Canc	el

Screenshot 216: Troubleshooter wizard – Information details

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

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.

Troubleshooter Wizard - Gathering Information
Known Issues The troubleshooter will check your installation for common issues.
Details: Could not connect to the GFI LanGuard update server. Possible reasons: you are not connected to the Internet; your proxy set Checks if the Attendant Service user has administrator privileges. Checks if the LNSSCommunicator COM object can be instantiated. Checks if the CRMI COM object can be instantiated. Checks if the Attendant Service is installed on this computer. Checks if the Attendant Service is running on this computer. Checks if the Attendant Service is available. The scanning profiles database is available.
The Windows patches database is available.
Finished all checks.
< Back Next > Cancel

Screenshot 217: 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.

# 6.3 Using the Agent Diagnostics Tool

The GFI LanGuard Agent Diagnostics tool is designed to assist you in case of technical issues related to GFI LanGuard. Through this tool, you can verify agent connectivity, view error messages and obtain a a summary with all the relevant state information about the agent.

To use the Agent Diagnostics Tool:

1. Select the agent from the computer tree from the **Dashboard**.

2. Right click agent and select Agent Diagnostics.

3. The Agent Diagnostics Tool retrieves all the information required to solve common issues. Click **Export** to export and view the diagnostics report.

# 6.4 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.

### 6.5 Web Forum

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

# 6.6 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.

# 7 Glossary

#### Α

#### Access™

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

#### Active Directory<sup>™</sup> (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.

#### В

#### 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<sup>®</sup> 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.

#### С

#### 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<sup>®</sup> 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.

#### Ε

#### 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.

#### Μ

#### 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<sup>®</sup> Access<sup>™</sup> 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<sup>®</sup> to improve an application or an operating system.

#### Microsoft® WSUS

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

#### Ν

#### 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.

#### 0

#### 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.

#### Ρ

#### 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<sup>®</sup> 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

Simple Network Management Protocol is a protocol for network management. It is used to collect information from network devices, such as servers, printers, hubs, switches, and routers.

#### **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<sup>®</sup> relational database management system. Microsoft<sup>®</sup> included extra functionality to the SQL Server<sup>®</sup> (transaction control, exception handling and security) so that Microsoft SQL Server<sup>®</sup> can support large organizations.

#### SSD

Solid State Drives are storage devices for computers. These drives use flash memory technology to provide superior performance and durability to traditional Hard Disk Drives.

#### 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.

#### Т

### 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  ${\sf GFI}$  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.

#### XML

Х

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

# 8 Index

#### A

270, 279 Advanced 1, 55, 62, 75, 80, 83, 89, 118, 125, 165, 178, 181, 188, 190, 192, 194, 196, 220, 224, 239, 257, 265, 300 Agent 15, 23, 66, 77, 90, 94, 109, 111, 135, 137, 144, 173, 183, 185, 202, 207, 209, 226, 229, 267, 302, 304 Agent-based 83, 94 Agent-less 15, 22, 25, 83, 94, 144 Alerting Options 57, 72, 218, 235, 281 Antiphishing 138, 159, 228 Antispyware 67, 138, 209, 229 Applications scanning options 261 Attendant service 10, 33, 103 Attributes 65-66, 68, 76, 79, 91, 128, 130, 138, 211 Audit 10, 61, 66, 72, 75, 87, 90, 95, 97, 100, 114, 124, 135, 138-139, 142-144, 149, 151, 161-163, 209, 225, 227-228, 230, 261, 270, 279-280 Audit schedule 75 Auto-deployment 162-163, 204 auto-download 101, 163, 204 Auto-remediation 104, 162, 179-180 Auto-Update 240 В Backup 20, 23, 27, 35-37, 42, 138, 160, 229, 246 Baseline Comparison 68, 210 Bulletin Info 155, 187 С CGI 258 Check 21, 34, 50, 90, 93, 95, 155, 166, 204, 242, 253, 286, 299, 301 Client 8, 11, 15, 81, 83, 117, 159, 162, 179, 230 Command Line Tools 10, 281 Common Vulnerabilities and Exposures 232 Complete/Combination scans 95, 268 Compliance 69, 73, 211 Components 10, 19-20, 24, 31, 36, 38, 43, 92, 302

Activity 66, 100, 109, 135, 155, 200, 205-206, 208-209, 219,

Computer 34, 39, 52, 62, 67, 72, 74, 77, 81, 90, 93, 98, 111, 122, 125, 134, 139, 154, 172-173, 179-180, 185-187, 189, 191, 197, 204-205, 209, 214, 223, 231, 251, 271-272, 290, 304 Computer Security Overview 67, 209 Computer Summary 68, 210 Computer Tree 62, 72, 77, 84, 90, 97, 109, 122, 125, 130, 153, 173, 187, 189, 191, 197, 205, 214, 217, 223, 304 Conditions 64, 70, 96, 212, 251, 288, 291, 296

Custom 14, 74, 76, 83, 95, 97, 175, 185-186, 191-192, 196-197, 216, 247, 269, 276, 286, 290, 294

Custom target properties 97

CVE 6, 94, 232, 251

#### D

Daily Digest 222, 236 Dashboard 6, 10, 51, 62, 75, 77, 88, 99, 109, 111, 122-123, 125, 130, 132-134, 139-140, 142-144, 149-150, 153, 197, 283, 304 database retention options 240 Deploy custom software 185 Deploy Software Updates 180, 185-187 deploycmd.exe 282 Device scanning options 261 DHCP 300 Display adapters 158, 228 DNS 81, 155, 270 DNS Lookup 270 Drivers 159, 228 F. Enumerate Computers 275, 302

Enumerate Users 277 Export 27, 35-37, 72, 76, 192, 218, 284, 304

#### F

File and printer sharing 226-228, 230 Find 1, 62, 125, 164, 193, 195, 233, 260 Firewall applications 159, 229 Floppy disk controllers 228 Footer 222 Full Audit 67, 209 G

General applications 228 Groups 50-51, 61, 67, 90, 129, 131, 138, 155, 205, 210, 231

#### н

Hardware 6, 8, 10, 20, 23, 26, 41, 61, 67, 84, 96, 129, 133, 138, 149, 158, 185, 209, 225, 227, 264, 271, 277-278

Hardware Audit 10, 68, 96, 211

Header 221

Human Interface Devices (HID) 228

#### L

IIS 56, 155

impex.exe 284

Import 53, 56, 74, 76, 102, 192, 284

Install 14, 42, 52, 115, 196, 218, 222

Installed Non-Security Updates 157, 189, 227

Installed Security Updates 70, 157, 189, 212, 226

Installed Service Packs and Update Rollups 68, 157, 189, 210, 226

Installing 8, 15-16, 30, 34, 40, 42, 53, 56, 103, 163, 203, 240, 283

#### L

Level 61, 70, 123, 132, 134, 141, 152, 162, 212, 287, 291, 296 List scanned computers 236 Insscmd.exe 281 Loading Results 160 Local drives 158, 227 Logged on users 160, 231 Μ

Malware 136, 185-186, 194 Management Console 52 Memory details 158, 227 Messages 162, 175, 182, 304 Microsoft Access 37, 301 Missing Non-Security Updates 157, 187, 226 Missing Security Updates 68, 155, 187, 210, 226 Missing Service Packs and Update Rollups 137, 155, 187, 226 Monitor 6, 15, 70, 88, 96, 100, 188, 190, 212, 219, 270, 277-278 Motherboards 227

Mouse and keyboard 228

#### Ν

NetBIOS 22, 25, 185, 231, 269, 275, 299 Network & Software Audit 96, 151, 261 Network devices 6, 13, 96, 158, 227, 264, 269-270, 277-278 Network Security History 67, 210 Network Security Overview 66, 209 Notifications 14, 57, 60, 185, 197, 236

#### 0

Open Ports 69, 157, 211 Open Shares 68, 211 Open TCP ports 137, 228 Open UDP ports 137, 228 OVAL 6, 94, 233, 251, 287, 291, 296 Ρ

Password 32, 34, 44, 46, 49, 56-57, 74, 99, 104, 159, 192, 194-195, 230, 236, 241, 280-281, 294

Patch management 229

Patching Status 67, 156, 209, 226

PCI DSS 69, 211

Ports 6, 10, 22, 24, 26-27, 41, 61, 67, 95, 133, 135, 137, 143, 157, 210, 225-228, 230, 262, 269, 303

Processors 138, 158, 227

Product Updates 57, 80, 92-93, 203, 206, 267

Profiles 10, 27, 94-95, 101, 144, 162-163, 169, 233-234, 247, 249, 259, 261, 268, 281, 287, 290, 296

Protocols 16, 22, 24, 26, 41, 225

Proxy 58, 94, 203, 241, 258

Python 286, 290

#### R

Real-time 133

References 251, 287, 291

Registry 16, 21, 61, 67, 155, 210, 226-228, 231, 270, 285, 302

Relay Agents 8, 15, 22, 24, 27, 42, 83, 135

Remediation Center 132, 140, 180, 185-186, 191-192, 195, 197

Remediation History 67, 210

Remediation Jobs 188, 190, 192, 194, 196, 200, 204 Remediation Operations 10, 18, 21, 162, 180, 204 Remote Desktop Connection 186, 196 Remote registry 226-228, 230

#### S

Saved scan results 237

Scan History 67, 210

Scanning Profile Editor 247-249, 259, 268, 287, 290, 296

Scanning Profiles 10, 27, 94-95, 144, 162-163, 169, 247, 249, 259, 262, 268, 281, 287, 290, 296

Scheduled Scans 101, 109, 135, 170, 202

Script 286

Script Debugger 286

Security audit policy 100, 230

Security Scanning Options 268

Security Scans 10, 69, 100, 124, 200, 208, 212

Security Updates 22, 68, 93-94, 137, 155, 187, 189, 191, 202, 210, 226, 248, 258

Server 9-10, 15, 20, 24-25, 29, 31, 36-37, 40-42, 44-45, 47-49, 51-52, 56-58, 60, 62, 66, 71-72, 80, 83, 91, 94-95, 97, 111, 161, 218, 231, 235-236, 241, 243, 258, 269, 280-281, 300-301

Sessions 10, 160, 231, 281

Shares 10, 61, 67, 83, 96, 159, 175, 190, 210, 230, 263, 270

SMB 16, 22, 25, 226-228, 230, 302

SMTP 57, 155, 236

SNMP 22, 25, 96, 268, 277-278

SNMP Auditing 277

SNMP Walk 278

Software 2, 6, 10, 20, 23, 27, 35-37, 42, 60-61, 66-67, 72, 93, 95, 109, 117, 130, 133, 136, 138, 144-145, 151, 161-163, 175, 180, 185-187, 189, 191, 196-197, 202-203, 209, 224-225, 228, 231, 241, 258, 261, 276, 282

Software Audit 10, 67, 72, 95, 151, 161-162, 209, 261

SQL 11, 21, 26, 32, 37, 41, 43, 45, 48, 161, 236, 243, 280, 301

SQL Server Audit 280

SSH 21, 25, 99, 104, 269, 294

Storage details 158, 227

System Information 61, 70, 96, 133, 150, 159, 213, 225, 230, 261

System Patching Status 156, 225-226

#### Т

TCP/UDP port scanning options 261

Traceroute 272

#### U

Unauthorized 6, 69, 75, 105, 136, 138, 155, 162-163, 170, 184, 211, 266

Unauthorized Applications 69, 136, 162, 211, 266

Uninstall 6, 27, 38, 75, 81, 105, 162, 171, 184-186, 223

Uninstall Applications 185-186, 192, 223

Uninstall Software Updates 185-186, 189

Upgrade 15, 30, 35-37, 244

Upgrading 34-37, 244

USB 68, 95, 210, 228, 263

Users 29, 49, 52, 58, 61, 69, 129, 138, 155, 180, 211, 231, 277, 279, 283, 286

Utilities 270, 273-275, 277-280

#### V

VBscript 286

VPN client applications 230

- Vulnerabilities 6, 10, 15, 34, 60-61, 66-67, 94-95, 130, 132-133, 136-137, 140, 153, 162, 176, 185, 194, 209, 224, 232, 240, 248, 260, 265, 270, 285-286, 296
- Vulnerability Assessment 6, 10, 27, 95, 151, 161-162, 248, 259, 268, 286, 290

Vulnerability Level Rating 152

Vulnerability Status 59, 67, 209

#### W

Wake-on-LAN 99, 104, 162, 178 Whois 274 WINS 300 WMI 16, 227, 269