**GFI LANguard Network Security Scanner 7** 

## Manual

By GFI Software Ltd.



Email: info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI SOFTWARE Ltd.

LANguard is copyright of GFI SOFTWARE Ltd. 2000-2006 GFI SOFTWARE Ltd. All rights reserved.

Version 7.0 – Last updated May 17, 2006

## Contents

		1
Introductior	n to GFI LANguard Network Security Scanner	1
Importance	of internal network security	1
Key feature	۶۶	2
GFI LANgu	ard N.S.S. components	4
License sch	1eme	6
Installing GFI L	ANguard Network Security Scanner	7
System req	juirements	7
Fire	ewall considerations	<u>7</u>
Installation	procedure	
Entering yo	Jur license key after installation	11
Getting started	: Performing an audit	13
Introduction	٦	13
Ab	out scanning profiles (list of vulnerability checks/tests)	13
Log	gon credentials to access the target computer(s)	14
Imp	portant considerations	14
Performing	a security scan using default settings	
Performing	a scan using different (default) scanning profiles	
Performing	a scan using alternative target logon credentials	
Starting see	curity scans directly from the toolbar	19
Getting started	: Analyzing the security scan results	21
Introduction	۱	21
Analyzing t	he scan results	21
Vul	nerabilities	23
Pot	tential vulnerabilities	27
Op	en shares	
Pa	ssword policy settings	29
Re	distry settings	
0-		29
Se	curity audit policy settings	
Sec Op	en ports	29 30 32
See Op Use	en ports ers and groups	
See Op Use Log	en ports ers and groups	
Sei Op Usi Log Ru Ru	en ports en ports ers and groups gged on users nning services	
Sei Op Usi Loc Ru Re Ins	en ports en ports gged on users nning services mote running processes talled applications	
Sei Op Usi Log Ru Re Ins	en ports en ports ers and groups gged on users nning services mote running processes talled applications twork devices	
Sei Op Usi Log Ru Re Ins Ne US	ers and groups gged on users nning services mote running processes talled applications by devices	
Sei Op Usi Log Ru Re Ins Ne US Re	en ports en ports gged on users nning services. mote running processes talled applications. twork devices. B devices. porting unauthorized devices as high security	
Sea Op Usa Log Ru Re Ins Ne US Re vul	globy bedange curity audit policy settings en ports ers and groups	
Sea Op Usa Log Ru Re Ins Ne US Re vul Svs	curity audit policy settings en ports ers and groups	
Sei Op Usi Log Ru Re Ins Ne US Re vul Sys NE	curity audit policy settings en ports ers and groups gged on users nning services mote running processes talled applications twork devices B devices porting unauthorized devices as high security nerabilities stem hot fixes patching status TBIOS names	
Sei Op Usi Log Ru Re Ins Ne US Re Vul Sys NE	curity audit policy settings en ports ers and groups gged on users nning services mote running processes talled applications twork devices B devices porting unauthorized devices as high security nerabilities stem hot fixes patching status TBIOS names anned target computer details	
Sei Op Usi Ru Ru Re Ins Ne US Re Vul Sys NE Sca Act	curity audit policy settings en ports ers and groups gged on users nning services mote running processes talled applications twork devices B devices porting unauthorized devices as high security nerabilities stem hot fixes patching status TBIOS names anned target computer details ive sessions	
Se Op Us Ru Ru Re Ins Ne US Re vu Sys NE Sca Act Re	curity audit policy settings en ports ers and groups	

Saving	g and loading scan results	43	
	Introduction	43	
	Saving scan results to an external (XML) file	43	
	Loading saved scan results	44	
	Loading saved scans from database backend	44	
	Loading saved scan results from an external (XML) file	45	
Filteri	ng scan results	47	
	Introduction	47	
	Running a filter on a scan		
	Creating a custom scan filter		
Config	guring GFI LANguard N.S.S.	55	
	Introduction	55	
	Scanning Profiles	55	
	Scheduled scans	56	
	Creating a scheduled scan	57	
	Configuring result notification options	59	
	Computer Profiles	60	
	About SSH Private Key file authentication	60	
	Creating a new computer profile	61	
	Changing the properties of a computer profile	61	
	Using computer profiles in a scan	62	
	Parameter files	62	
	Database Maintenance Options	64	
	Introduction		
	Configuring your database backend	64	
	Storing scan results in an Microsoft Access database	05	
	Datckend		
	Database maintenance - manage saved scan results		
	Database maintenance - auvanceu options	00	
Scann	ing Profiles	71	
	Introduction	71	
	Scanning profiles in action	73	
	Scanning your local computer with the 'Default Scanning Profile'	73	
	Scanning your local computer with the 'Applications	70	
	Creating a new scanning profile	73	
	Customizing a scanning profile		
	Configuring TCP/UDP ports scanning options	76	
	Enabling/disabling TCP Port scanning	76	
	Enabling/disabling UDP Port scanning		
	Customizing the list of TCP/UDP ports to be scanned		
	Adding a new TCP/UDP port to the list		
	How to edit or remove a port	78	
	Configuring OS data retrieval options	78	
	Customizing OS Data Retrieval parameters	78	
	Configuring vulnerabilities scanning options	79	
	Enabling/disabling vulnerability scanning	79	
	Customizing the list of vulnerabilities to be scanned	80	
	Customizing the properties of vulnerability checks	80	
	Vulnerability checks - advanced options	82	
	Configuring patch scanning options	83	
	Enabling/disabling missing patch detection checks	83	
	Customizing the list of software patches to be scanned	84	
	Using the search bulletin information facility	84	

Comparing scan results interactively	
Configuring what information will be reported	
Generating a Results Comparison Report	

**Results comparison** 

Configuring the security scanning options	85
Configuring the attached devices scanning options	
Enabling/disabling checks for installed network devices	
Compiling a list of unauthorized network devices	
Compiling a list of safe network devices	89
Configuring advanced network device scanning options	90
Enabling/disabling checks for attached USB devices	91
Compiling a list of unauthorized USB devices	91
Compiling a list of safe USB devices	92
Configuring the applications scanning options	92
Enabling/disabling checks for installed applications	93
Compiling a list of unauthorized applications	94
Compiling a list of safe applications	95
Enabling/disabling checks for security applications	95
Customizing the list of security application for scanning	96
Configuring security applications - advanced options	96

#### GFI LANguard N.S.S. program updates

#### 99

105

#### Patch management: Deploying Microsoft Updates

Introduction	
About the patch deployment agent	
About recalled patches	105
Multilingual patch management	107
Selecting the target computers where patches will be deployed	107
Deploying missing updates on one computer	108
Deploying missing updates on a range of computers	108
Deploying missing updates on all computers	108
Selecting which patches to deploy	109
Download the patch and service pack files	110
Stopping active downloads	111
(Optional) Configure alternative patch file deployment parameters	112
Deploy the updates	113
Starting the patch deployment process	

#### Patch management: Deploying custom software

115

Introduction	115
Selecting targets for custom software/patch deployment	115
Enumerating the software to be deployed	116
Start the deployment process	117
Scheduling patch deployment	117
Deployment options	118
Before deployment options	118
After deployment options	119
Advanced deployment options	120

#### 121

	.20
Viewing scheduled operations	
Viewing the progress of scheduled scans	
Viewing the progress of scheduled deployments	126
Tools	127
Introduction	
DNS lookup	127
Trace Route	128
Whois Client	129
SNMP Walk	130
SNMP Auditing tool	131
Microsoft SQL Server Audit tool	131
Enumerate computers tool	132
Starting a security scan	133
Deploying custom patches	133
Enabling auditing policies	133
Enumerate users tool	134
Using GFI LANguard N.S.S. from the command line	135
Using 'Insscmd.exe' - the command line scanning tool	
Example: How to launch target computer scanning from the	
command line tool	136
Using 'deploycmd.exe' - the command line patch deployment tool	136
Example: How to launch a patch deployment process from the command line tool	138
Adding vulnerability checks via custom conditions or scripts	139
Introduction	139
GFI LANguard N.S.S. VBscript language	139
GFI LANguard N.S.S. SSH Module	140
Keywords:	140
Adding a vulnerability check that uses a custom VB (.vbs) script	
Step 1 : Create the script	
Step 2: Add the new vulnerability check:	
Adding a vulnerability check that uses a custom shell script	
Step 1 : Create the script	
Step 2: Add the new vulnerability check:	
Adding a CGL vulnerability check	
Adding a Conversion of the con	147
Adding other vulnerability checks	
Adding other vulnerability checks	153
Adding other vulnerability checks	153
Adding other vulnerability checks <b>Miscellaneous</b> Enabling NetBIOS on a network computer Installing the Client for Microsoft Networks component on Windows 2000 or higher	<b>153</b> 153
Adding other vulnerability checks	<b>153</b> 153 154
Adding other vulnerability checks	<b>153</b> 153 154
Adding other vulnerability checks	<b>153</b> 153 154 155
Adding other vulnerability checks	<b>153</b> 153 154 155 159
Adding other vulnerability checks <b>Miscellaneous</b> Enabling NetBIOS on a network computer Installing the Client for Microsoft Networks component on Windows 2000 or higher Configuring Password Policy Settings in an Active Directory-Based Domain Viewing the Password Policy Settings of an Active Directory-Based Domain	<b>153</b> 153 154 155 159 <b>161</b>
Adding other vulnerability checks Miscellaneous Enabling NetBIOS on a network computer Installing the Client for Microsoft Networks component on Windows 2000 or higher Configuring Password Policy Settings in an Active Directory-Based Domain Viewing the Password Policy Settings of an Active Directory-Based Domain Troubleshooting	153 153 154 155 159 161
Adding other vulnerability checks <b>Miscellaneous</b> Enabling NetBIOS on a network computer Installing the Client for Microsoft Networks component on Windows 2000 or higher Configuring Password Policy Settings in an Active Directory-Based Domain Viewing the Password Policy Settings of an Active Directory-Based Domain	<b>153</b> 153 154 155 159 <b>161</b> 161
Adding other vulnerability checks	<b>153</b> 153 154 155 159 <b>161</b> 161 161
Adding other vulnerability checks	<b>153</b> 153 154 155 159 <b>161</b> 161 161 161
Adding other vulnerability checks Miscellaneous Enabling NetBIOS on a network computer Installing the Client for Microsoft Networks component on Windows 2000 or higher Configuring Password Policy Settings in an Active Directory-Based Domain	<b>153</b> 153 154 155 159 <b>161</b> 161 161 161 162 162

Web Forum	
Build notifications	

#### Index

### Introduction

#### Introduction to GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (GFI LANguard N.S.S.) is a security auditing tool, which proactively reports, and supports fixing of network vulnerabilities in a timely fashion.

During a security audit, GFI LANguard N.S.S. scans your entire network, IP by IP, and alerts you about weaknesses discovered on your network(s). Using a combination of operating system functions together with the features offered by GFI LANguard N.S.S., you can proactively deal with the security issues detected. For example, security issues can be proactively detected by shutting down unnecessary ports, closing shares as well as installing service packs and hot-fixes before malicious persons can exploit them.

By default, GFI LANguard N.S.S. allows you to perform security audits on both Windows and Linux-based target computers. During an audit, the scanning engine collects various hardware and software information from the scanned targets. This includes the service pack level of each target computer, potentially vulnerable devices such as wireless access points and USB devices, installed applications, as well as open shares and open ports. The scanner also enumerates specific OS configuration settings such as Windows registry settings and password policy configuration details aiding in the identification of common security issues related to an improperly configured operating system (such as an OS running on default settings).

GFI LANguard N.S.S. is also equipped with algorithms that check for the presence of particular security software (i.e. anti-virus and antispyware applications) as well as ensure that they are running with the latest definition files released by their parent company. Where applicable, the scanning engine will also check that important security features such as real time scanning are enabled on anti-virus and antispyware applications allowing you to ensure that the security solutions deployed on your network are running effectively.

Out of the box, GFI LANguard N.S.S. also supports patch management for non-English operating systems. This means that you can automatically download missing Microsoft updates in a variety of languages and deploy them network-wide. You can also use the patch deployment engine to remotely install custom software as well as third party (non-Microsoft) patches network-wide (for instance anti-virus definition updates).

#### Importance of internal network security

Internal network security is very often underestimated by its administrators. In fact, in certain environments such security does not even exist, allowing one user to easily access another user's computer using well-known exploits, trust relationships and default settings. Most of these attacks require little or no skill, putting the integrity of a network at stake.

Due to the amount of flexibility needed for normal operation, internal networks cannot afford maximum security. On the other hand, with no security at all, internal users can be a major threat to many corporate internal networks.

According to the CERT Co-ordination Centre at Carnegie Mellon University in the US:

"An 'insider intrusion' is any compromise of a network, system or database that is committed by someone who has (or used to have) legitimate access to the network, system or data. Such 'insiders' can include current and former employees, part-time employees, business partners, consultants and contractors." - Computer Weekly.

A user within the company already has access to many internal resources without needing to bypass firewalls or other security mechanisms. In fact, these security measures are generally used to prevent non-trusted external sources, such as Internet users, from accessing the internal network. However, most threats come from internal users. An internal user, equipped with hacking skills, can successfully penetrate and achieve administrative network rights while ensuring that their abuse is hard to identify or even detect. The Computer Crime and Security Survey compiled in 2003 by the Computer Security Institute and the FBI discovered that approximately 65% of respondents reported at least one security incident involving an insider.

Poor network security may also allow malicious users that break into a network system to access the rest of the internal network more easily. This would enable a sophisticated attacker to read and possibly leak confidential emails and documents, delete data and damage computers - leading to loss of important information and more. Spiteful intruders may also use your network and network resources to turn around and attack (or spy!) other sites (i.e. attack relaying). In this way, all evidence of the attack will lead back to you and your company, without exposing the hacker's own identity.

Most vulnerabilities can be easily patched and attacks against known exploits can be easily stopped by administrators if they get to know about them in time. GFI LANguard N.S.S. assists administrators in the identification of these vulnerabilities!

#### **Key features**

- Finds rogue services and open TCP and UDP ports.
- Detects known CGI, DNS, FTP, Mail, RPC and other vulnerabilities.
- Detects rogue or backdoor users.
- Detects open shares and enumerates who has access to these shares including their respective permissions.
- Enumerates groups, including group members during target computer scanning.

- Enumerates USB devices attached to target computers (for example, Apple iPod, and other portable storage devices).
- Enumerates network devices and identifies if these devices are Wired, Wireless or Virtual.
- Enumerates services and their respective state.
- Enumerates remote running processes.
- Enumerates installed applications.
- Checks that the signature files of supported installed security applications (anti-virus and anti-spyware) are updated. Where applicable the security scanner will also examine the running configuration settings of particular security software (for example, BitDefender anti-virus) to verify that key features such as real-time scanning are enabled.
- Scheduling of network security scans and email reporting on completion.
- Security scanning and OS data collection for Windows operating systems.
- Security scanning and OS data collection for Linux operating systems through SSH.
- Logon to remote Linux targets through conventional logon credentials strings as well as through Public Key authentication (i.e. using SSH Public/Private Key files).
- Self-updating Automatically downloads definition files for the latest vulnerability checks, missing patches information on program startup.
- Patch management support for Windows 2000/XP/2003 operating systems, Microsoft Office XP or later, Microsoft Exchange 2000 and Microsoft SQL Server 2000 or later.
- Patch management support for multilingual operating systems.
- Allows you to save security scan results in Microsoft Access or Microsoft SQL Server database backend and XML files.
- Reports to administrator on completion of a scheduled scan with detailed full scan results and/or detected changes identified between successive scans.
- Live host detection and Operating system identification.
- SNMP Auditing.
- Microsoft SQL Auditing.
- Script debugger that you can use to create and debug custom vulnerability checks. Checks are created using a VBscript compatible scripting language.
- Supports multithreading (i.e. allows scanning of multiple computers at the same time).
- Includes command line tools that allow you to scan and deploy software updates/patches and third party applications without bringing up the GFI LANguard N.S.S. user interface. These command line tools can be used directly from the command line prompt, through third party applications as well as through custom scripts and batch files.

#### **GFI LANguard N.S.S. components**

GFI LANguard N.S.S. is built on an architecture that allows for high reliability and scalability catering for both medium to larger sized networks.

GFI LANguard N.S.S. consists of five main components which are:

- GFI LANguard N.S.S configuration/user interface
- GFI LANguard N.S.S. Attendant service
- GFI LANguard N.S.S. Status Monitor.
- GFI LANguard N.S.S. Patch Agent service
- GFI LANguard N.S.S. Script Debugger.

#### GFI LANguard N.S.S. configuration/user interface



Screenshot 1 - GFI LANguard N.S.S. configuration interface

Launch GFI LANguard N.S.S. from **Start Programs GFI LANguard Network Security Scanner 7.0 LANguard Network Security Scanner**.

Use this application to:

- Launch network security scans and patch deployment sessions.
- View saved and real time security scan results.
- Configure scan options, scan profiles and report filters.
- Use specialized network security administration tools.

#### **GFI LANguard N.S.S. attendant service**

This is the background service which runs the scheduled operations. These include scheduled network security scans and scheduled patch deployment operations.

#### GFI LANguard N.S.S. patch agent service

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

GFI LANguard N.S.S. Script Debugger



Screenshot 2 - GFI LANguard N.S.S. Script Debugger

This module allows you to write and debug custom scripts using a VBScript-compatible language. Use this module to create scripts for custom vulnerability checks. These checks can then be included in GFI LANguard N.S.S. to custom-scan network targets.

Launch the GFI LANguard N.S.S. Script Debugger from Start > Programs > GFI LANguard Network Security Scanner 7.0 > LNSS Script Debugger.

🎒 GFI Languard NSS Status	5 Monitor		
Active scheduled scans Sch	neduled deployments		
Target	Profile	Start time	Status
2 172.16.130.122	Default	11/18/2004 3:53:53 PM	completed
•		<u>R</u> emove finished scans	<u>S</u> top selected scans
			ОК

#### **GFI LANguard N.S.S. Status Monitor**

Screenshot 3 - GFI LANguard N.S.S. Monitor

Use this module to monitor the status of scheduled scans and scheduled software-update deployment sessions. In addition, from this module you can also stop scheduled operations which have not yet been executed.

Launch the GFI LANguard N.S.S. Status Monitor from **Start** > **Programs** > **GFI LANguard Network Security Scanner 7.0** > **LNSS Status Monitor**.

#### License scheme

The GFI LANguard N.S.S. licensing scheme works on the number of computers and devices that you wish to scan. For example, the 100 IP license allows you to scan up to 100 computers or devices from a single workstation/server on your network.

For more information on GFI LANguard N.S.S. licensing visit: <u>http://www.gfi.com/pricing/pricelist.aspx?product=LANSS</u>.

## Installing GFI LANguard Network Security Scanner

#### System requirements

Install GFI LANguard Network Security Scanner on a computer which meets the following requirements:

- Windows 2000 (SP4) / XP (SP2) / 2003 operating system.
- Internet Explorer 5.1 or higher.
- Client for Microsoft Networks component (included by default in Windows 95 or higher).
   NOTE: For more information on how to install the Client for Microsoft Networks component refer to the 'Installing the Client for Microsoft Networks component on Windows 2000 or higher' section in the 'Miscellaneous' chapter.
- Secure Shell (SSH) (included by default in every Linux OS distribution pack).

#### Firewall considerations

Firewalls installed on either the host or target computer(s) will interfere with the operations of GFI LANguard N.S.S.

You must either:

• Disable the firewall software on the host/target computer(s)

Or

 Use the Windows Internet Connection Firewall domain policies to configure the necessary ports and services required by GFI LANguard N.S.S. to operate correctly. For more information on how to configure Active Directory policies to support scanning of/from computers running the Windows Internet connection Firewall (XP SP2 or 2003 SP1) visit: http://kbase.gfi.com/showarticle.asp?id=KBID002177.

#### Installation procedure

1. Launch the GFI LANguard Network Security Scanner installation wizard by double-clicking on **languardnss7.exe**. As soon as the welcome dialog is displayed, click **Next** to start the installation.

2. In the license dialog, read the licensing agreement carefully. Select the 'Accept the Licensing agreement' option and click on **Next** to continue.

3. Specify the full username, the company name and the license key. If you are evaluating the product, leave the license key as default (i.e. 'Evaluation'). Click on **Next** to continue.

🙀 GFI LANguard Network Security Scanner 7.0 Setup		
User Account Information Please enter requested data		
The GFI LANguard N.S.S. a scheduled updates of config under a domain administrato Set up the GFI LANguard N.	ttendant service handles scheduled security scans and juration files. It is recommended to run the attendant service r account. S.S. attendant service to run under	
Account:	Domain\account	
Password:	*******	
Confirm Password:	*******	
NOTE: Specify the user nam	ne in the format 'DOMAIN\administrator'.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Screenshot 4 - Specify domain administrator credentials or use local system account

4. Specify the service account under which GFI LANguard N.S.S will be running. Click on **Next** to continue.

**IMPORTANT:** GFI LANguard N.S.S. **must run with administrative credentials**. It is recommended to provide Domain Administrator or Enterprise Administrator account details. This is required because GFI LANguard N.S.S. will most likely need administrative rights to access the targets computers on your network. However, it is not mandatory to provide a Domain/Enterprise Administrator account details for every target computer, since separate credentials can be provided from the configuration interface after the installation (**Configuration → Computer Profiles node**).

🚰 GFI LANguard Network Security Scanner 7.0 Setup
Installation Type Choose the installation type that best suits your needs.
Choose a database in which GFI LANguard Network Security Scanner will store the scan information. The scan information can be stored in:
Microsoft Access [MS Access does NUT need to be installed].
Microsoft <u>SQL</u> Server 7 or higher/MSDE.
Note: For larger networks it is recommended that you use Microsoft SQL server (7 or higher) or MSDE. MSDE is provided for free on the Microsoft Office 2000/XP/2003 CD. For more information please see the manual.
< <u>B</u> ack <u>N</u> ext > Cancel

Screenshot 5 - Choose database backend

5. Specify which database backend will be used to store the scan results/information. You can choose between Microsoft Access, Microsoft SQL Server 7/2000 or MSDE. Click on **Next** to continue.

**NOTE 1:** Microsoft Access database backend usage is recommended for small networks. For medium and larger networks, usage of Microsoft SQL Server 7/2000 as a database backend is recommended.

**NOTE 2:** MSDE can handle up to 2 GB of data while Microsoft SQL server is capable of handling larger volumes of data efficiently and without limitations.

🙀 GFI LANguard Network Security Scanner 7.0 Setup								
so	<b>QL Server Selection</b> Please enter the reque	sted information.			<b>?</b> ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
	Please specify an SQL server and account which will be used to create and take ownership of the databases. Please note that the account should have the proper permissions to create databases.							
	SQL server details:							
	<u>S</u> erver:	EMMANUELG-DEV2		AUTORESPONDER	-			
	🔲 Use Windows auth	entication		FSERVER ISA2K4	<b>•</b>			
	Login using the followir	ig credentials (SQL Accour	nt):					
	<u>U</u> ser:	sa						
	Password:	******						
			< <u>B</u> ack	<u>N</u> ext >	Cancel			

Screenshot 6 - Specify SQL Server details

6. If Microsoft SQL Server is selected as a database backend, specify the logon credentials that will be used when logging on to the database. You can use SQL Server user accounts details or Windows NT authentication details to access the database. Click on **Next** to continue.

**NOTE:** When using Windows NT authentication, ensure that the GFI LANguard N.S.S. services are running under user accounts which have the necessary administrative access rights and privileges to log on to and manage the SQL Server databases.

👹 GFI LANguard Ne	etwork Security Scann	er 7.0 Setup		_ 🗆 🗙				
Mail Settings Enter administrator	email and SMTP mail serv	er settings		S. C				
Please enter the details of the SMTP server and email address which are to be used by GFI LANguard Network Security Scanner 7.0 for email notifications on schedule scan reports.								
<u>F</u> rom	LNSS@127.0.0.1							
<u>I</u> o:	administrator@localho	ost						
S <u>M</u> TP server:	127.0.0.1		<u>P</u> ort: 25	ō				
<ul> <li>SMTP server d</li> <li>SMTP server re</li> </ul>	oes n <u>o</u> t require authentica equires <u>a</u> uthentication.	tion.						
SMTP User:								
SMTP Password:			<u>∨</u> erify m	ail settings				
		< <u>B</u> ack	<u>N</u> ext >	Cancel				

Screenshot 7 - Specify alerting email address and mail server details

7. Specify the SMTP/mail server details (Hostname/IP and Port) as well as the email address where generic administrative notifications will be sent. Click on **Next** to continue.

8. Specify the installation path for GFI LANguard N.S.S. and click **Next**. The installation will need approximately 40 MB of free disk space.

9. Click **Finish** to finalize the installation.

#### Entering your license key after installation

If you have purchased GFI LANguard N.S.S., enter your License key in the **General ► Licensing** node (no re-installation/re-configuration required)

**NOTE 1:** By default, GFI LANguard N.S.S. has an unrestricted fully functional evaluation period of 10 days. If the data you provided in the download form is correct, you will receive by email a license key which enables you to evaluate GFI LANguard N.S.S. for 30 days.

**NOTE 2:** GFI LANguard N.S.S. licensing is based on the:

- Number of computers/IPs that will be running GFI LANguard Network Security Scanner.
- Number of computers/IPs that you wish to scan.

For example, if you wish to install GFI LANguard N.S.S. on one server, and you will be scanning a network of 20 target computers, then you have to purchase a 25 IP license.

**NOTE 3:** Entering the License Key should not be confused with the process of registering your company details on our website. This is important since it allows us to give you support and notify you of important product news. You may register and obtain your GFI customer account from: <u>http://www.gfi.com/pages/regfrm.htm</u>

**NOTE 4:** To find out how to buy GFI LANguard N.S.S., follow the **General ▶ How to purchase** node.

## **Getting started: Performing an audit**

#### Introduction

An audit of network resources enables the administrator to identify and assess possible risks within a network. Doing this manually involves a tiresome series of repetitive and time consuming tasks that must be accurately performed on each and every network computer. GFI LANguard N.S.S. automates the security auditing process and remotely scans computers for known vulnerabilities, common misconfiguration and other potential security issues in a relatively short time. The information collected during the scanning process is then used to assist the tracking and mitigation of security issues that have been identified. Typical information enumerated during the security scanning process includes:

- The service packs level of the computer
- Missing security patches
- Wireless access points
- USB devices
- Open shares
- Open ports
- Services/applications active on the target computer(s)
- Key registry entries
- Weak passwords
- Users and groups.

To perform a security audit the scanning engine requires you to specify three primary parameters:

1. Target computer(s) to scan for security issues.

2. Scanning Profile to use (specifies vulnerability checks/tests to be done against the specified targets).

3. Authentication details to be used to log on to the target computer(s).

#### About scanning profiles (list of vulnerability checks/tests)

Before starting a scan you must specify which vulnerability checks/tests to be run against the specified target(s).

This is required because GFI LANguard N.S.S. contains a multitude of vulnerability checks that can be run on your network infrastructure. Although much of these vulnerability checks can be run against all network computers, there are some 'specialized' checks which are role specific and thus their results depend both on the services that are running on that particular target computer(s) as well as the desired

type of security scan you need to perform. For example, CGI vulnerability checks need to be run only when scanning Web servers.

In GFI LANguard N.S.S. the vulnerability checks that will be run against a target in a security scan are specified in templates called 'Scanning Profiles'. These scanning profiles hold the 'scanning instructions/parameters' that the scanning engine will follow during a security audit i.e. the vulnerability checks that must be executed against the targets as well as the information that is to be retrieved from these targets. For more information on scanning profiles, refer to the 'Scanning Profiles' chapter in this manual.

For a well balanced security scan use the 'Default Scanning Profile' option.

#### Logon credentials to access the target computer(s)

During a security scan, for some types of information retrieval/vulnerability tests, GFI LANguard N.S.S. needs to remotely log on to each target computer. By default GFI LANguard N.S.S. uses the security context of the user under which it is running. You can also specify alternative logon credentials to run a scan under a different security context from the currently logged on user.

While the above would fit most network scanning needs you may meet situations when you log on to some target computers with a particular administrative account and onto some other target computers with a totally different administrative account.

To cater for this situation GFI LANguard N.S.S. allows you to configure computer profiles for different targets which are located in your network. Use computer profiles to specify the logon credentials to use when logging in to a target computer even when a security scan is being run under a different security context. For example, you can use computer profiles to make sure that the computer FILESERVER is always scanned with the account COMPANY\fileserveradmin and that the computer WEBSERVER is always scanned with the account COMPANY\webserveradmin.

For more information on computer profiles refer to the 'Computer Profiles' section in the 'Configuring GFI LANguard N.S.S.' chapter in this manual.

#### Important considerations

1. Please note that if your company runs any type of Intrusion Detection Software (IDS) during scanning, **GFI LANguard N.S.S. will set off a multitude of IDS warnings and intrusion alerts in these applications.** If you are not responsible for the IDS system, make sure to inform the person in charge about any planned security scans.

2. Along with the IDS software warnings, be aware that a lot of the scans will show up in log files across the board. UNIX logs, web servers, etc. will all show the intrusion attempts made by the computer running GFI LANguard Network Security Scanner. If you are not the sole administrator at your site make sure that the other administrators are aware of the scans you are about to run.

#### Performing a security scan using default settings

Out of the box, GFI LANguard N.S.S. includes default configuration settings which allow you to run an immediate (basic) scan soon after the installation is complete.

For a default scan you must only specify which target computer(s) you wish to audit. By default, GFI LANguard N.S.S. will:

- Authenticate to the targets using the currently logged on user account credentials (i.e. the credentials under which GFI LANguard N.S.S. is running).
- Use a generic list of default vulnerability checks which are preconfigured in the 'Default' scanning profile. This is one of the default scanning profiles which ships with GFI LANguard N.S.S.

To perform you first scan, please do as follows:

#### 1. Click on **File ▶ New**.

🐠 G	FI LANguard N.S.S.	. 7.0				
<u>F</u> ile	<u>T</u> ools <u>C</u> onfigure	<u>H</u> elp				_
	<u>N</u> ew		•	<u>S</u> can single computer	Ctrl+N	Password:
	Save Scan Results	Ctrl+S		Scan range of computers	Ctrl+R	
	Exit			Scan list of computers	Ctrl+L	0 ▼ Profile: Derault ▼ <u>Scan</u>
	-		_	Scan <u>d</u> omain	Ctrl+D	pan Results
				S <u>c</u> heduled Scan		

Screenshot 8 - Selecting the type of security scan

2. Select the type of scan that you wish to perform by selecting one of the following options:

- Scan single computer... Select this option to scan a single computer.
- Scan range of Computers... Select this option to scan a specific range of computers.
- Scan list of Computers... Select this option to scan a custom list of computers.
- Scan a Domain... Select this option to scan an entire Windows domain.

**NOTE**: At this point in time, you may ignore the **Scheduled Scan** option. This option is used to configure vulnerability scans which will be automatically executed on a specific day/time. Scheduled scans are described in more detail in the 'Configuring GFI LANguard N.S.S.' chapter in this manual.

New scan	New scan
Scan Lype: Single computer	Scan Type: Range of computers
This Computer     Another Computer     Computer name/IP-Address)	Scan (rom IP address: 130.16.100.1 130.16.100.255
Scan Profile: Default	Scan Profile: Default
New scan	New scan X
Scan Ivpe: List of computers	Scan <u>T</u> ype: Domain
List of computers: TMJason Add EMMANUELC-64BIT KEITHTEST-1 Select Import Export Scan Profile: Default	Select domain(s) to scan:
OK Cancel	OK Cancel

Screenshot 9 - New Scan options dialogs.

3. Specify the requested target details (i.e. host name, IP, range of IPs or domain name).

4. Click on the **OK** button to start your default scan.

#### About the scanning process

GFI LANguard Network Security Scanner will start the scanning process by first identifying the targets which are available for scanning (i.e. target computers which are switched on and reachable over the network). This is done by automatically sending requests to the specified target computers using NETBIOS queries, ICMP ping and SNMP queries.

If a target computer does not respond to these queries, GFI LANguard N.S.S. will assume that the device is currently turned off or that it does not exist on the specified IP address. By default, GFI LANguard N.S.S. will NOT scan target computers which fail to reply to scanning requests.

After that the connection to a target computer is established, the scanning engine will execute the specified or default set of vulnerability checks. During a default scan the scanning engine will automatically execute a preconfigured and generic list of vulnerability checks which will test multiple areas of your network for specific weaknesses. Further on you will learn how to run checks that are more specific by selecting, customizing or creating different scanning profiles.

#### Performing a scan using different (default) scanning profiles

Apart from the default scanning profile, GFI LANguard N.S.S. ships with an extensive list of different scanning profiles each of which is preconfigured to perform specific or more specialized vulnerability checks. The scope of having different scanning profiles is to minimize the configuration changes required prior to every scan by using already configured vulnerability scanning templates.

In this vulnerability scan, you will specify two primary parameters:

- Targets that you wish to scan.
- The scanning profile (i.e. the vulnerability checks/tests) that will be run against your targets.

By default, GFI LANguard N.S.S. will again authenticate to the targets using the currently logged on user account credentials (i.e. the credentials under which GFI LANguard N.S.S. is running).

To run a network security audit using a different scanning profile:

1. Click on **File ▶ New**.

2. Select the type of scan that you wish to perform (for example, Scan single computer).

3. Specify the requested target details (i.e. host name, IP, range of IPs or domain name).

New scan		×			
Scan <u>T</u> ype:	Scan <u>Type</u> : Single computer				
• This Comp	puter				
O <u>A</u> nother C	Computer				
	(Computer name/IP Address)				
Scan <u>P</u> rofile:	Missing Patches	•			
	CGI Scanning				
	Full TCP & UDP Port Scan				
	- Only Web	Ľ			
	Only SNMP Disa Massa All				
	Share Finder				
	Trojan Ports	•			

Screenshot 10 - New Scan dialog: Selecting a different scanning profile

4. From the 'Scan Profile' drop down at the bottom of the dialog, select the scanning profile that will be used for this network security scan.

For example, select *'Missing Patches'* to perform a network scan that checks and enumerates missing Microsoft software patches as well as the targets which are missing these patches.

5. Click on the **OK** button to start your scan.

#### Performing a scan using alternative target logon credentials

When performing a security scan GFI LANguard N.S.S. must authenticate to the target computer(s). This is required so that the scanning engine is allowed permissions to run the configured vulnerability checks against the target and to retrieve the system information required.

GFI LANguard N.S.S. authenticates to targets by 'physically' logging on to the computer(s) using the logon credentials of an account with administrative rights. This does not necessarily need to be a Domain Administrator or Enterprise Administrator account; however this user account must have administrative privileges on the target computer(s).

Different systems often require different authentication methods. For example Linux systems often request a private key file instead of the conventional password string. GFI LANguard N.S.S. supports both methods.

For more information about authentication methods refer to the 'Computer Profiles' section in the 'Configuring GFI LANguard N.S.S.' chapter in this manual.

To run a network security audit using specific logon credentials:



Screenshot 11 - GFI LANguard N.S.S. new scan toolbar: Authentication methods drop down list

1. From the credentials drop down list in the GFI LANguard N.S.S. scan toolbar, specify the authentication method to be used in this security audit by selecting one of the following options:

- 'Currently Logged-On User' Select this option to authenticate to target computers using Windows NT account credentials (i.e. using the account under which GFI LANguard N.S.S. is running).
- *'Null Session'* Select this option to try and connect to target computers without authentication. In this way, you can identify what information can be accessed by non-authenticated (internal/external) users.
- *'Alternative credentials'* Select this option to authenticate to target computers using specific credentials. Specify these credentials in the 'Username' and 'Password' fields provided next to this drop down list.
- *'SSH Private Key'* Select this option to authenticate to Linux based target computers using a username and a private key file instead of a password string (i.e. through Public Key authentication).

**NOTE:** For more information about Public Key authentication, refer to the 'About SSH Private Key file authentication' section in the 'Configuring GFI LANguard N.S.S.' chapter in this manual.

2. Click on **File ▶ New.** 

3. Select the type of scan that you wish to perform (for example, Scan single computer).

4. Specify the requested target details (i.e. host name, IP, range of IPs or domain name).

5. From the 'Scan Profile' drop down at the bottom of the dialog, select the scanning profile that will be used for this network security scan.

6. Click on the **OK** button to start your scan.

#### Starting security scans directly from the toolbar

To run a network security audit directly from the toolbar:

👩 GFI LANguard N.S.S. 7.0				_ 🗆 🗙
<u>File T</u> ools <u>C</u> onfigure <u>H</u> elp				
🚺 🜔 New Scan 🔛 🎽 Using:	Currently Logged-On User 🔻	User Name:	Password:	
	Currently Logged-On User Alternative Credentials a NULL Session SSH Private Key			

Screenshot 12 - GFI LANguard N.S.S. new scan toolbar

1. From the credentials drop down list in the GFI LANguard N.S.S. toolbar, select the authentication method to be used and if required specify the respective credentials in the adjacent fields.

GFI LANguard N.S.S. 7.0				_ 🗆 ×
File Lools Lonngure Help	ly Logged-On User ▼ User Name: [		Password:	
Tools Explorer	Scan Target: 130.168.1.25-130.16 Scanned Computers	8.1.100 <b>v</b> P <u>r</u> ofile: Scan Results	Default Default CGI Scanning Full TCP & UDP Port Scan Missing Patches Only Web Only SNMP Ping them All Share Finder	Scan

Screenshot 13 - GFI LANguard N.S.S. target details toolbar

2. In 'Scan Target' drop down below, specify the targets that will be scanned (for example, TMJason, 130.12.1.20-130.12.1.30, etc.).

3. From the 'Profile' drop down select the scanning profile that will be used for this network security scan.

4. Click on the **Scan** button to start your network vulnerability scan.

# Getting started: Analyzing the security scan results

#### Introduction

After a security scan completes, GFI LANguard N.S.S. generates and displays the scan results in a dedicated window inside the configuration interface.

Scan results are organized by type into different categories. The amount of result categories and the type of information collected during a security scan is entirely dependent on the type of checks that have been run against the targets as well as on the parameters that have been configured in the scanning profile that was used in the audit. Hence, you will certainly obtain different scan result categories for every different scanning profile that you use to audit your network. For more information on scanning profiles refer to the 'Scanning Profiles' section further on in this manual.

You can also run filters on your scan results and display only specific scan result details. This is achieved by applying 'Scan Filters' to this information. For more information on scan filters refer to the 'Filtering scan results' chapter in this manual.

#### Analyzing the scan results



Screenshot 14 - GFI LANguard N.S.S. configuration interface: Analyzing the scan results

Use the information presented in the 'Scanned computers' section (middle pane) to navigate the results of the scanned computers. Security scan results are organized in a number of category subnodes. These can be easily used to investigate and identify security issues in the scanned targets.

Scan results are organized in the following categories:

- A Vulnerabilities
- A Potential vulnerabilities
- 🗟 Shares
- Applications
- B Network devices
- 🗟 USB devices
- <a>
   Password policy
- Security audit policy
- 🐵 Registry
- Kong Open TCP ports
- 🗹 System patching status
- B NETBIOS names
- 🕅 Computer
- 🖪 Groups
- 🖇 Users
- 🖪 Logged on users
- Design Sessions
- Services
- 📓 Processes
- 🐺 Remote time of day (TOD)
- Electric Local drives.

To view the scan results data retrieved during a security scan, click on the category of interest. The information is shown in the 'Scan Results' (right) pane.

#### Vulnerabilities



Screenshot 15 - The Vulnerabilities node

Click on the **A** Vulnerabilities sub-node to view the security vulnerabilities identified on the target computer. Detected vulnerabilities are grouped by type and severity into five main categories:

- Solution of the service packs of the service p
- Ø Missing patches
- Ø High security vulnerabilities
- Ø Medium security vulnerabilities
- Solution Security vulnerabilities.

#### Vulnerabilities Missing service packs

A Service Pack (SP) is a software program that corrects a set of known bugs or adds new features to operating systems and applications.

GFI LANguard N.S.S. checks for missing Microsoft software updates by comparing the version of the service packs currently installed on the scanned target(s) with the ones made currently available by the manufacturer.



Screenshot 16 - Missing Service Packs results tree

**NOTE:** GFI LANguard N.S.S. is capable of checking for missing software updates and service packs on various Microsoft products. For a complete list of supported products go to <a href="http://kbase.gfi.com/showarticle.asp?id=KBID002573">http://kbase.gfi.com/showarticle.asp?id=KBID002573</a>.

Details shown in the results tree of this category include the:

- Ø 'Product name' and 'Service Pack Number'.
- URL:' The URL link to a Knowledge Base article or other support documentation related to the detected missing service pack.
- **W** '*Release date:*' The date when the reported service pack was released.

To access more detailed information on a missing service pack, rightclick on the particular service pack and select **More details** ....

Bulletin Info						×
Bulletin						
Bulletin ID:	Not Available	QNumber:	840663	Date:	2005-05-13	
Ttile:	Visio 2003 Service Pa	ck 1				
Description:	Visio 2003 Service P contains significant : the fixes included w combines them into	ack 1 provides th security enhancer ith SP1 have beer one update.	e latest updates ments as well as s n previously relea	to Microsoft Office Vis tability and performa sed as separate upda	io 2003. Service Pack 1 (SP1) nce improvements. Some of ites. This service pack	
Applies To:	Office 2003					
URL:	http://support.micros	oft.com/oas/defa	ault.aspx?LN=en-	us&gprid=65278x=9	<u>8v=8</u>	
File						
File Name:	Visio2003-KB840663-	FullFile-ENU.CAB				
File Size:	22,476 KB					
File URL:	http://www.downloa	d.windowsupdate	com/msdownloa	d/update/v3-1999051	8/cabpool/visio2003-kb84066	<u>53-</u>
					⊡ose	

Screenshot 17 - Missing Service pack: Bulletin info dialog

This will bring up the 'Bulletin Info' dialog of the respective service pack. The information shown in this bulletin includes:

- The QNumber. This is a unique ID number which is assigned by Microsoft to each software update for identification purposes.
- The release date of the bulletin/service pack.
- A long description of the service pack and its contents.
- The list of OS/Application(s) to which the service pack applies.
- The URL link to more information about the respective service pack.
- The name of the service pack file and the relative file size.
- The URL from where you can manually download this service pack.

#### Vulnerabilities > Missing patches

A patch is an update which is released by a software company to address a technical/security issue. It is very common for attackers to exploit these known vulnerabilities in order to gain access to a network. Failure to patch target systems make you vulnerable to an attack resulting in either loss of business time and/or data. GFI LANguard N.S.S. scans target computers to ensure that all relevant security updates released by Microsoft are installed.



Screenshot 18 - Missing patches detected during target scanning

Missing patches discovered during target scanning are listed and grouped under the 'Missing Patches' category.

Details shown in results tree of this category include the:

- 😵 😵 Sé 'Patch ID' and 'Product name'.
- *Bugtraq ID/URL:* The ID and URL of the respective Microsoft Knowledge Base article.
- Severity:' The effect that the patch has on the security level of a network device.
- *If the Posted:* The release date of the missing patch.

To access more detailed information, right-click on a particular patch and select **More details...**.This will bring up the 'Bulletin Info' dialog containing addition details on the respective software patch.

**NOTE:** GFI LANguard N.S.S. is capable of checking for missing software updates and service packs on various Microsoft products. For a complete list of supported products go to <a href="http://kbase.gfi.com/showarticle.asp?id=KBID002573">http://kbase.gfi.com/showarticle.asp?id=KBID002573</a>.



Vulnerabilities > High, medium, low security vulnerabilities

Screenshot 19 - High, medium, low security vulnerabilities

The 'High', 'Medium' and 'Low security vulnerabilities' sub-nodes contain information on weaknesses discovered while probing a target device. These vulnerabilities are organized into 8 groups:

- 🚞 CGI abuses.
- ETP vulnerabilities.
- DNS vulnerabilities.
- Dail vulnerabilities.
- Contraction
   RPC vulnerabilities.
- Service vulnerabilities.
- Cartery vulnerabilities.
- Disc/Linux/UNIX vulnerabilities.

The content of each group is described below:

#### • 🗀 CGI abuses

This group contains details of the security vulnerabilities (such as misconfiguration issues) discovered on scanned web servers. Supported web servers include Apache, Netscape, and Microsoft I.I.S. The information listed in this section includes:

- Image: Willing of the state of
- o 'Description:' A short description of the respective vulnerability.
- Bugtraq ID/URL:' The ID of the relevant Microsoft Knowledge Base article(s) and the URL to more detailed information on the vulnerability.

## ETP, DNS, Mail, RPC and Misc/Linux/UNIX vulnerabilities

These groups include details of the security weaknesses discovered during the scanning of particular network targets such as FTP servers, DNS servers, and SMTP/POP3/IMAP mail servers. The information shown in these sections includes links to Microsoft Knowledge Base articles or other support documentation related to the service pack.

#### Cartery Service vulnerabilities

This group includes details of security vulnerabilities associated to services which are running on the scanned network device(s). Other details enumerated in this section include unused accounts which are still active and accessible on the scanned target computers.

#### Cartery vulnerabilities

This group includes details of the vulnerabilities discovered in the registry settings of a scanned network device. The details shown in this category include links to support documentation as well as a short description of the respective vulnerability.

#### Potential vulnerabilities



Screenshot 20 - Potential vulnerabilities node

Click on the A Potential vulnerabilities sub-node to view scan result items which were classified as possible network weaknesses. These scan result items, although not classified as vulnerabilities, require your meticulous attention since they can be exploited by malicious users during an attack.

For example, during a security scan GFI LANguard N.S.S. will enumerate all of the modems which are installed and configured on the target computer. If these modems are not used or connected to a telephone line, they are of no threat to your network (i.e. no vulnerability). On the other hand, if the modems are used and connected they can be used by your network users to gain unauthorized and unmonitored access to the Internet.

This would further allow them to both bypass your firewall and any other Internet security settings implemented (for example, virus scanning, site rating and content blocking) as well as generate high telephone bills for the company. In addition to the above, hackers might detect such connections and exploit them to gain uncontrolled access to your network system through this unmonitored route. As a result, GFI LANguard N.S.S. considers installed modems as potential threats and enumerates them in a dedicated category (i.e. the 'Potential Vulnerability' sub-node) for your attention and analysis.

#### Open shares

Click on the Shares sub-node to view all shares on a target computer.



Screenshot 21 - Shares node

In the wild, there are various worms and viruses (for example, Klez, Bugbear, Elkern and Lovgate) which spread out using open shares detected on the computers of a network.

GFI LANguard N.S.S. enumerates the properties of all shares discovered on your network. Use this data to ensure that:

1. No user is sharing whole drives with other users.

2. Anonymous/unauthenticated access to shares is not allowed and that appropriate access permissions are set up.

3. Startup folders or similar system files are not shared as these could allow less privileged users to execute code on target computers.

4. No user has unnecessary or unused shares.

For every open share detected the following information is retrieved from the target computer:

- Share name
- Directory which is being shared on the target computer
- Share permissions and access rights
- NTFS permissions and access rights.

**NOTE:** Every Windows computer has administrative shares (C\$, D\$, E\$ etc.) which GFI LANguard N.S.S. will by default enumerate during target computer scanning. As these can become irrelevant to your security audit you can configure GFI LANguard N.S.S. not to report such administrative shares. For more information on how to achieve this refer to the 'Customizing OS Data Retrieval parameters' section in the 'Scanning Profiles' chapter in this manual.

# **Password policy settings**



Screenshot 22 - Password policy node

Click on the **Password Policy** sub-node to view the password policy settings of the scanned target computer(s).

Windows 2000/XP/2003 security policies provide a set of rules that can be configured for all user accounts to protect against brute force password guessing attacks. Such policies include account lockout control policies as well as password strength enforcement policies. These are essential to the enforcement of a secure network as they make it very difficult for an attacker to locate a weak link in your user base. Typical vulnerabilities in an IT infrastructure include weak passwords which are made up of few characters for example, blank or default passwords or password which are identical to the respective username.

Use the password policy settings which GFI LANguard N.S.S. retrieves from scanned target computers to identify configuration vulnerabilities on your network.

### **Registry settings**

Click on the **B Registry** sub-node to view important registry key values configured on your target computer.



Screenshot 23 - Registry node

By examining the values in the **Run** node, you can check which programs are configured to be automatically launched at startup.

This information allows you to identify Trojans, authorized or unauthorized applications as well as valid applications which can provide remote access into your network. Any type of software which is run without your express instruction from the start menu should be noted and checked for validity.

Failure to do so may provide an entry opportunity into your system.

### Security audit policy settings

Click on the Security Audit Policy sub-node to view the security audit policy settings configured on a scanned target computer.

An important part of any security plan is the ability to monitor and audit events happening on your network. These event logs are frequently referenced in order to identify security holes or breeches. Identifying attempts and preventing them from becoming successful breeches 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.

Whilst scanning, GFI LANguard N.S.S. extracts the currently configured security audit policy settings from the target computer(s). Use this information to identify whether auditing policies are properly set up on your network computers.

GFI recommends that you set up the audit policy settings of your network computers as follows:

Auditing Policy	Success	Failure
Account logon events	Yes	Yes
Account management	Yes	Yes
Directory service access	Yes	Yes
Logon events	Yes	Yes

Object access	Yes	Yes
Policy change	Yes	Yes
Privilege use	No	No
Process tracking	No	No
System events	Yes	Yes

You can also remotely configure the audit policy settings of target computers directly from the GFI LANguard N.S.S configuration interface. This is done as follows:

1. From the 'Scanned Computers' (middle) pane, right-click on the respective target computer and select **Enable auditing on ▶ This computer**. This will launch the 'Audit Policy Administration Wizard'. Click on **Next** to proceed with the configuration.

**NOTE 1:** To remotely configure auditing policies on a particular selection of target computers, right-click on any target computer (which is listed in the middle pane) and select **Enable auditing on > Selected computers**.

**NOTE 2:** To remotely configure auditing policies on all target computers listed in the 'Scanned Computers' (middle) pane, right-click on any target computer and select **Enable auditing on**  All **computers**.

GFI LANguard N.S.S. Administration Wizard		
Switch on security auditing policies Automatic turning on of security auditing polic	icies	<u>G</u>
Specify which auditing policies are to be turn policies have been selected by default:	ned on. The recommended auditing	
Auditing Policy	Success Failur	e
Audit account logon events Audit account management Audit directory service access Audit logon events Audit object access Audit policy change Audit privilege use Audit process tracking Audit system events		
Click on Next to turn on the selected auditing	g policies.	
	< <u>B</u> ack <u>N</u> ext >	Cancel

Screenshot 24 - The Audit Policy Administration wizard

2. Select/unselect the check boxes of the auditing policies that you wish to set up on the selected target computer(s). For example, to log successful events, select the 'Successful' check box of the relevant auditing policy. Click on **Next** to initiate the audit policy configuration process on the remote target computer(s).

GFI LAN	Iguard N.S.S. Admini:	stration Wizard			
Арр	<b>blication of security</b> The results of the applic	auditing policie cation of the secu	s results ity auditing policie:	s to all computers.	S A
	<u>R</u> esults:				
	Computer	Result			
	EMMANUELC	Success			
	,				
			< Back	Next >	Cancel
				<u>How</u>	

Screenshot 25 - Results dialog in audit policy wizard

3. A dialog will now show the audit policy configuration results. Click on **Next** to proceed to the last stage of the configuration process.

4. Click on Finish to close the 'Audit Policy Administration Wizard'.

# **Open ports**

Click on the **Solution** Open Ports sub-node to view a list of ports which are detected as being open for listening on a scanned target computer.



Screenshot 26 - Open TCP ports node

Open ports represent active services and applications which can be exploited by malicious users to gain access to a computer. It is very important to only leave the ports which you know are necessary for the central/core functions of your network services. All other ports should be closed.

By default GFI LANguard N.S.S. is configured to use the 'Default Scanning Profile'. Via the use of this scanning profile, not all of the 65535 TCP and UDP ports are checked as this may take a long time to complete per target computer. When using the 'Default Scanning Profile', GFI LANguard N.S.S. performs checks on the ports most commonly exploited by hackers, Trojans, viruses, spyware and malware. Use the 'Full TCP & UDP Port Scan' scanning profile to run a full open port check on all targets.

For more information on how to run security audits using different scanning profiles refer to the 'Scanning profiles in action' section in the 'Scanning Profiles' chapter in this manual.

For more information on how to customize a scanning profile refer to the 'Creating a new scanning profile' section in the 'Scanning Profiles' chapter in this manual.

### Service fingerprinting

Further to detecting if the port is open or not, GFI LANguard N.S.S. uses service fingerprint technology to analyze the service(s) which are running behind the detected open port(s). Through service fingerprinting you can ensure that no hijack operation has taken place on that port. For example, you can verify that behind port 21 of a particular target computer there is an FTP server running and not an HTTP server.

### Dangerous port reporting



Screenshot 27 - Scan Results: Dangerous ports are marked in RED

When a commonly exploited port is found open, GFI LANguard N.S.S., will mark it in red. Care is to be taken as even if a port shows up in red, it does not mean that it is 100% a backdoor program. Nowadays with the array of software being released it is becoming more common that a valid program uses the same ports as some known Trojans.

### **Users and groups**

Click on the **S Users** sub-node to view all local user accounts on target computer(s). Click on the **S Groups** sub-node to view all local groups on the scanned target computer(s).

Use this information to identify rogue or unused users and groups that can allow access to unauthorized visitors! These include the 'Guest' account and other unused or obsolete user accounts and groups. Some backdoor programs re-enable the 'Guest' account and grant it administrative rights. Use the details enumerated in the **Users** subnode of the scan results to inspect the access privileges assigned to each user account.

**NOTE:** Users should not use local accounts to log on to a network computer. For better security, users should log on to network computers using a 'Domain' or an 'Active Directory' account.

### Logged on users

Click on the **S** Logged on Users sub-node to access the list of users that are logged on to the scanned target computer locally (via an interactive logon) or remotely (via a remote network connection).



Screenshot 28 - Logged on users node

For every logged on user that is detected, the following information is retrieved (depending on applicability).

- 🗳 Logged on username.
- If *time and Date of the Logon'* The time and date when the user logged on the target computer.
- If *'Time elapsed since their logon'* How long the user has been logged on this computer.
- If 'Number of programs running' The number of programs that the interactively logged on user was running at the time of the scan.

- Idle time' How long the remote user's connection has been idle (i.e. completely inactive).
- Client type' The platform/operating system that the remote user used to connect to the target computer.
- If 'Transport' The name of the service that was used to initiate the remote connection between the remote computer and the target computer (for example, NetBios.Smb, Terminal Service, Remote Desktop).

### **Running services**

Click on the **Services** sub-node to access the list of services that were running on the target computer(s) during the security scan. Use this information to identify unknown/unrequired running services on your network computer(s).

**NOTE:** Each running service can be a potential security weak spot in your network system. For this reason, we recommend that you close/disable all unnecessary applications and services that are running your network. This exercise automatically hardens your network by reducing the entry points through which an attacker can penetrate into your system.

#### Remote running processes

Click on the **B Remote Processes** sub-node to access the list of processes that were running on the target computer during a scan.

GFI LANguard N.S.S. 7.0 Eile Iools Configure Help	Using: Currently	Logged-(	On User 💌 ∐ser Na	me:		Password:			⊐ ×
Scan Target: localhost	Scan Target, localhost Y Profile: Default Y Stop								
Scanned Computers	Scan Results								
🖁 🖳 130.16.130.68 [JONA	Process	PID	Path	User	PPID	Domain	Command line	Handle count	
🖁 🛛 🗛 Vulnerabilities (15)	👪 agentsvr.exe	1512	C:\WINDOWS\	jonan	672	GFIMALTA	C:\WINDOWS\	149	
🆳 🦳 🚹 Potential Vulnerabiliti	👪 alg.exe	228		LOCAL SERVICE	512	NT AUTHORITY		108	E
— 🔂 Shares (7)	🕴 ASFAgent.exe	1056	C:\Program Files	SYSTEM	512	NT AUTHORITY	"C:\Program File	122	
— 🔯 Applications (56)	👪 aspnet_wp.exe	5912	\\?\C:\WIND0	ASPNET	1220	JASON	aspnet_wp.exe	125	8
- B Network devices (9)	🕴 ComExec.exe	1704	C:\WINDOWS\	SYSTEM	512	NT AUTHORITY	C:\WINDOWS\	502	•
USB devices (5)	🔀 CIDAEMON.EXE	1320	C:\WINDOWS\	SYSTEM	1068	NT AUTHORITY	"cidaemon.exe"	171	4
Password policy	🔀 CIDAEMON.EXE	3568	C:\WINDOWS\	SYSTEM	1068	NT AUTHORITY	"cidaemon.exe"	139	<b>—</b>
Bogistry	CIDAEMON.EXE	492	C:\WINDOWS\	SYSTEM	1068	NT AUTHORITY	"cidaemon.exe"	111	1
Open TCR Ports (7)	👪 cisvc.exe	1068	C:\WINDOWS\	SYSTEM	512	NT AUTHORITY	C:\WINDOWS\	457	1
Sustem patching statu	🚦 csrss.exe	444		SYSTEM	388	NT AUTHORITY		1210	F
- 191 NETBIOS names (5)	🚦 ctfmon.exe	2408	C:\WINDOWS\	jonan	2304	GFIMALTA	"C:\WINDOWS	64	
- B9 Computer	🔀 dllhost.exe	2796	C:\WINDOWS\	jonan	672	GFIMALTA	C:\WINDOWS\	211	F
- 🚾 Groups (11)	👪 dllhost.exe	4992	C:\WINDOWS\	SYSTEM	512	NT AUTHORITY	C:\WINDOWS\	224	I.
— 🌉 Users (10)	👪 dllhost.exe	5048		IWAM_JONAN	672	JASON		284	1
— 🧟 Logged On Users (6)	🔀 EXCEL.EXE	4776	C:\Program Files	jonan	2304	GFIMALTA	"C:\Program File	245	4
- 🔁 Sessions (1)	👪 explorer.exe	2304	C:\WINDOWS\	jonan	2176	GFIMALTA	C:\WINDOWS\	1506	1
- 🎇 Services (99)	👪 hh.exe	2140	C:\WINDOWS\	jonan	3508	GFIMALTA	"C:\WINDOWS	263	4
- 🔛 Processes (65)	🕴 hh.exe	4852	C:\WINDOWS\	jonan	2304	GFIMALTA	"C:\WINDOWS	284	E
	👪 hk.cmd.exe	2360	C:\WINDOWS\	jonan	2304	GFIMALTA	"C:\WINDOWS	75	1
	👪 lap.exe	1196	C:\Program Files	SYSTEM	512	NT AUTHORITY	"C:\Program File	78	4
	👪 inetinfo.exe	1220	C:\WINDOWS\	SYSTEM	512	NT AUTHORITY	C:\WINDOWS\	668	4
	1						<u> </u>		١Ē
		9		• • • • • • • • • • • • • • • • • • • •		2			_
					Over	all progress: 0/1			

Screenshot 29 - List of running processes enumerated during a target scan

During security scanning, GFI LANguard N.S.S. harvests various information on the processes which are running on scanned target computers. Details enumerated during security scanning include:

- Process name
- Process ID
- Path
- User

- PPID
- Domain
- Command Line
- Handle Count
- Thread Count
- Priority.

## **Installed applications**



Screenshot 30 - List of installed applications enumerated during target computer scanning

Click on the **D** Applications sub-node to access the complete list of applications that are installed on a scanned target computer. Discovered applications are organized into three groups:

- Anti-virus applications
- Anti-spyware applications
- General applications.

The anti-virus **applications** and anti-spyware **applications** groups contain the list of security applications installed on a scanned target computer. Details enumerated in these groups include:

- 🖏 Application name.
- *C* 'Real time protection:' Denotes if real time protection is enabled or disabled in an anti-virus application.
- If 'Up to date:' Denotes if the anti-virus/anti-spyware signature files of a security application are up to date. This is achieved by checking (where applicable) the signature file status flag of an application.
- If *Last update:'* Shows the date and time of the last antivirus/anti-spyware signatures update.
- If *'Version:'* Shows the version number of the security application.
- *If 'Publisher:'* Shows the manufacturer details.

The **General applications** group contains the list of general purpose applications installed on a scanned target computer. These include all software programs which are not classified as anti-virus or antispyware products such as Adobe Acrobat Reader and GFI LANguard Network Security Scanner.

Details enumerated in the General Applications group include:

- Solution Application name.
- If *'Version:'* Shows the version number of the application.
- *If 'Publisher:' Shows t*he manufacturer details.

#### Network devices

Click on the **Network Devices** sub-node to access the list of network devices/components (for example, wired and wireless network cards) which are installed on a scanned target computer. Use this information to analyze and identify unauthorized devices connected to your network.

Unmonitored network devices, especially wireless ones, are becoming a main source of information leakage in organizations. Special care must be given to ensure that only authorized wireless devices are connected to your network infrastructure!.



Screenshot 31 - Network devices enumerated during a security scanning session

GFI LANguard N.S.S. identifies all devices on your network including physical and wireless ones. The information enumerated in the **Network Devices** sub-node is organized in four main groups:

- Physical devices (Wired)
- In Wireless devices
- IVITUAL devices
- Boftware enumerated devices.

Each group includes various details about the device detected including:

- MAC Address
- Assigned IP Address(es)
- 🗹 Hostname
- 🗹 Domain
- **I** DHCP details
- 🗹 WEP (were available)
- SSID (were available)
- 🗹 Gateway
- 🧹 Status.

### **USB** devices



Screenshot 32 - List of USB devices detected on a scanned target computer

Click on the diverse Sub-node to access the list of USB devices connected to the target computer(s). Use the information collected in this sub-node to identify unauthorized USB devices currently plugged into the scanned target computer(s). These unauthorized devices may include portable storage devices such as the Apple iPod, or Creative Zen as well as USB wireless devices and Bluetooth dongles.

# Reporting unauthorized devices as high security vulnerabilities



Screenshot 33 - Dangerous USB device listed as a High Security Vulnerability

GFI LANguard N.S.S. can be configured to distinguish between authorized and unauthorized USB devices. For more information, refer to the 'Compiling a list of unauthorized network devices' section in the 'Scanning Profiles' chapter in this manual.

# System hot fixes patching status



Screenshot 34 - The list of missing and installed patches enumerated during target computer scanning

Click on the System patching status node for an overview of the patching status of a target computer.

### **NETBIOS** names

Click on the **I NETBIOS names** sub-node to access the list of NetBIOS names enumerated during target computer scanning.

Each computer on a network has a unique NetBIOS name. The NetBIOS name is 16-byte address that allows NetBIOS resources to be identified on the network. NETBIOS names are successfully mapped to an IP address using NetBIOS name resolution.

During the target probing process, GFI LANguard N.S.S. queries the identity and availability of a target network computer using NetBIOS. If available, the target computer will respond to the request by sending the respective NetBIOS name.



### Scanned target computer details

Screenshot 35 – Computer's node

Click on the **Description** Click on the **Descrip** 

- IP 'MAC:' Shows the MAC address of the network card which the target computer is using to connect to the network.
- If 'Time To Live (TTL):' Shows the maximum number of network hops allowed before a data packet expires/is discarded. Based on this value, you can identify the distance (i.e. the number of router hops) between the computer running GFI LANguard N.S.S. and the target computer that was just scanned. Typical TTL values include 32, 64, 128, and 255.
- Solution of a Server.
- *C* 'Domain:' Denotes the domain/workgroup details. When scanning targets which are part of a domain, this field shows the list of trusted domain(s). If the scanned target computer is not part of a domain, this field will show the name of the respective Workgroup.
- If 'LAN Manager:' Shows the type of operating system and LAN Manager in use (for example, Windows 2000 LAN Manager).

• *If 'Language:'* - Shows the language setting configured on the scanned target computer (for example, English).

### Active sessions

💮 GFI LANguard N.S.S. 7.0	
<u>F</u> ile <u>I</u> ools <u>C</u> onfigure <u>H</u> elp	
🛛 💽 New Scan 🚽 🎽 Using: Currently Logged-On User 👻 User I	Name: Bassword:
Tools Explorer  Q Scan Target: 127.0.0.1	▼ Profile: Default ▼ Scan
GFI LANguard Network S	
Security Scanner (De Scanned Computers	Scan Results
B ★ Tools Configuration General B ★ Configuration B ★ Configuration B ★ Configuration B ★ Configuration B ★ Configuration C ↓ C ↓ C ↓ C ↓ C ↓ C ↓ C ↓ C ↓ C ↓ C ↓	<ul> <li>□ - → JONAS</li> <li>○ Computer. JONAS</li> <li>○ Username:</li> <li>○ Open files: 0</li> <li>○ Connection time: 7 seconds</li> <li>○ User flags: 0</li> <li>○ Client type: Windows 2002 Service Pack 2 2500</li> <li>○ Transport: \Device\NwlnkNb</li> </ul>

Screenshot 36 - Session's node

Click on the **B** Sessions sub-node to access the list of hosts that were remotely connected to the target computer during scanning. The details shown in this sub-node include:

- Computer:' The IP Address of the host which was remotely connected to the scanned target computer.
- Sername:' The logged on username.
- *If 'Open files:'* The number of files accessed during the session.
- Connection time.' The duration of the connection session i.e. the time (in seconds) that the user(s) has been remotely connected to the scanned target computer.
- Idle Time:' The total time (in seconds) during which the connection was inactive.
- Client type' The platform/operating system that the remotely logged on computer (i.e. client computer) is running.
- If '*Transport*' The name of the service that was used to initiate the remote connection between the client computer and the target computer (for example, NetBios.Smb).

**NOTE:** The information enumerated in this sub-node also includes the remote connection details of the scanning session just performed by GFI LANguard N.S.S. i.e. the IP of the computer that is running GFI LANguard N.S.S., the logon credentials, etc.

### Remote time of day

Click on the **B Remote TOD (time of the day)** sub-node to view the network time that was read from the target computer during the scan.

This time is generally set on network computers by the respective domain controller.

### Local drives

Click on the **Local Drives** sub-node to view the list of physical drives that are accessible on the scanned target computer. The information enumerated in this sub-node includes the drive letter, the total disk space and the available disk space.

# Saving and loading scan results

# Introduction

By default, GFI LANguard N.S.S. automatically saves scan results to an Microsoft Access or Microsoft SQL Server database backend. However, through further configuration you can also save scan results to an external XML file.

Saved scan results can be re-loaded from both XML files and database backend into the GFI LANguard N.S.S. user interface for further processing. For example, you can re-load scan results for comparison or to deploy already discovered missing patches on particular targets without re-scanning the network system.

## Saving scan results to an external (XML) file

Once GFI LANguard N.S.S. completes a security scan, the results are automatically saved to the database backend. To save these results to an external XML file:

### 1. Go to File > Save scan results...

2. Specify the name of the XML file where the results will be stored (for example, ScanResult\_11052006.xml).

3. Click on **Save**.

# Loading saved scan results



Loading saved scans from database backend

Screenshot 37 - Reloaded scan results

GFI LANguard N.S.S. can store scan results in an Microsoft Access or Microsoft SQL Server database backend. In the same database file, by default, GFI LANguard N.S.S. will save the scan results of the last 10 scans performed on the same target with the same scanning profile.

**NOTE:** You can change the number of saved scan results from the **Database Maintenance** node through the **Manage Saved Scan Results** tab. For more information refer to the 'Manage saved scan results' section in the 'Database Maintenance Options' chapter.

To load saved scan results from the database backend:

1. Right click on the **Security Scanner (default)** node and select **Load saved scan results from... ▶ Database**. This will bring up the saved scan results dialog.

Database source			×
General			
			(
Select the scan	result to use for th	e required operation.	
larget	Profile	∨ Date	Completed
Iocalhost	Default	30/09/2005 14:48:45	Yes
📓 localhost	Default	30/09/2005 14:42:06	Yes
🧉 localhost	Default	29/09/2005 16:31:02	Yes
📓 localhost	Default	27/09/2005 13:28:12	Yes
📓 localhost	Default	27/09/2005 13:24:04	Yes
192.168.100.1-192	Default	07/09/2005 14:35:51	Yes
🖾 localhost	Default	06/09/2005 11:37:20	Yes
		OK	Cancel

Screenshot 38 - Saved Scan Results dialog

- 2. Select the scan results that you wish to load.
- 3. Click on **OK**.

### Loading saved scan results from an external (XML) file

To load saved scan results from an external XML file:

1. Right click on the **Security Scanner (default)** node and select **Load saved scan results from... ▶ XML...** This will bring up the saved XML scan results dialog.

- 2. Select the scan results file that you wish to load.
- 3. Click on **OK**.

# **Filtering scan results**

# Introduction

Following a security scan, you can filter the scan results and only display the information that you wish to analyze. For example, you can filter the information collected during a scan and only display details related to computers with high security vulnerabilities.



Screenshot 39 - Scan filter nodes

To filter scan results, you must apply a 'Scan Filter' over the data collected in the security scan. Scan filters are queries which extract and display specific scan result details. GFI LANguard N.S.S. ships with a number of default filters. These include:

- Full report: Shows all security related data collected during a scan.
- Vulnerabilities [High Security]: Shows critical issues which require immediate attention such as missing service packs, missing patches, high security vulnerabilities and open ports.
- Vulnerabilities [Medium Security]: Shows issues which may need to be addressed by the administrator such as average threats and medium vulnerability patches.
- Vulnerabilities [AII]: Shows all High and Medium vulnerabilities discovered during a security scan such as missing patches, and missing service packs.

- Missing patches and service packs: Shows all missing service packs and patch files discovered on the scanned target computer(s).
- Important devices USB: Shows all the USB devices attached to the scanned target computer(s).
- Important devices Wireless: Shows all the wireless network cards, (both PCI and USB) attached to the scanned target computer(s).
- **Open ports:** Shows all open TCP and UDP ports discovered on the scanned target computer(s).
- **Open shares:** Shows all open shares and the respective access rights.
- **Auditing policies:** Shows the auditing policy settings of the scanned target computer(s).
- **Password policies:** Shows the active password policy settings configured on the scanned target computer(s).
- **B** Groups and users: Shows the users and groups detected on the scanned target computer(s).
- **Computer properties:** Shows the properties of each target computer.
- Installed applications: Shows all the installed applications (including security software) discovered during target computer scanning.
- IN Non-updated security Software: Shows only the installed security applications (i.e. anti-virus/anti-spyware software) that have missing updates and outdated signature definition files.

**NOTE:** You can also create new scan filters or customize the above default scan filters.

# Running a filter on a scan

To run a scan result filter on security scan results:

1. Launch and complete a security scan of your network or load the scan results of past scans from your database or XML file.



Screenshot 40 - Scan filters: Full report

#### 2. Expand the Security Scanner > Scan filter nodes.

3. Select the scan filter that you want to trigger (e.g. Vulnerabilities all).

### Creating a custom scan filter

To create a custom scan filter:

1. Right click on the **Security Scanner** ▶ **Scan filter** node and select **New** ▶ **Filter...** . This will bring up the new scan filter properties dialog.

Advanced Properties	×
General Report Items Scan Filter Properties	
Filter name: Vulnerabilities (High security) Filter conditions:	
Queries         ✓       High vulnerabilities exists         ✓       OR Missing patches exists         ✓       OR Missing service packs exists	A <u>d</u> d Edit <u>Rem</u> ove All
Filter Property condition when added C And C Or	
OK Cancel	Apply

Screenshot 41 - The new Scan filter properties dialog: General tab-page

2. In the **General** tab which opens by default, specify the name of the new scan filter.

Add Filter Properties		×
Select the filter property on	which you want to make	a restriction:
Filter Condition		
📴 Operating system		
📴 Hostname		
📴 User logged in		
💑 Domain		
💑 Trusted domain		
📴 Computer usage		
🔒 Service Pack		
🌇 Time to live		
💵 MAC address		
💵 MAC vendor		
🕒 SNMP		
📴 Security auditing		
🔊 Share		
🔊 Shares		
🚾 Group		
🕵 User		-
	<u>N</u> ext >	Cancel

Screenshot 42 - Filter properties dialog

3. Click on Add and select the required filter property from the provided list (for example, Operating System). The filter property

defines what type of information will be extracted from the scan results (i.e. the area of interest of the scan filter).

4. Click on **Next** to continue.

Add Filter Properties	×
Filter Condition Properties	
Filter Property Information	
Filter condition to add	
Property: Operating system	
Conditions: is equal to	
Value: Windows XP	
Summary: Determine if operating system is equal to [Windows XP]	
< <u>B</u> ack Add Cancel	

Screenshot 43 - Filter condition properties dialog

5. Select the required filter condition from the 'Conditions' drop down and specify the filter value. The filter value is the reference string that this scan filter will use in accordance with the specified condition to extract information from scan results.

6. Click on **Add** to continue.

**NOTE:** You can create multiple filter conditions for every scan filter. This allows you to create powerful filters which isolate more accurately the scan results information that you may want to analyze.

Advanced Properties	×
General Report Items	
Select the items that will be contained in	HTML report.
🗊 Show header table	
B NETBIOS names	
Computers	
SNMP	
🔊 Shares	
Applications	
🔣 Groups	
🔁 Sessions	
💑 Trusted domains	
🥵 Users	
Logged on users	
🖃 🖧 Network devices	
B Physical	
III Virtual	
" Wireless	
ОК	Cancel Apply

Screenshot 44 - The new Scan-Filter properties dialog: Report Items tab-page

7. Click on the Report Items tab.

8. Select the information categories/sub-nodes which will be displayed in the configuration interface at the end of the filtering process.

9. Click on **OK** to create the filter.

The new filter will be added as a new permanent sub-node under the **Security Scanner > Scan filters** node.

**NOTE:** To delete or customize a scan filter, right-click on the target filter and selecting **Delete...** or **Properties** respectively.

# Example 1 – Create a filter which displays all computers that have a particular patch missing

In this example, we will create a filter which lists all Windows based computers that have the MS03-026 patch (i.e. the blaster virus patch) missing.

1. Right click on the **Security Scanner ▶ Scan filter** node and select **New ▶ Filter...** . This will bring up the new scan filter properties dialog.

2. In the filter name field type in 'Missing Blaster Patch'.

- 3. Click on the Add button.
- 4. Select the 'Operating System' option and then click on Next.

Add Filter Properties	×
Filter Condition Properties	
Filter Property Information	
Filter condition to add	
Property: Operating system	
Conditions: is equal to	
Value: Windows	
Summary: Determine if operating system is equal to [Windows]	
< <u>B</u> ack Add Cancel	

Screenshot 45 - Filter conditions dialog

5. From the conditions drop down select '*Includes*' and in the value field type in '*Windows*'.

6. Click on the **Add** button to add the condition to the filter.

Advanced Properties		×
General Report Items		
Scan Filter Properties		
<u>F</u> ilter name:		
Missing Blaster Patch		
Filter conditions:		
Queries           Operating system is equal to 'Windows'		<u>E</u> dit <u>R</u> emove Remove All
Filter Property condition when added @ And	O Dr	
	OK	Cancel

Screenshot 46 - The new Scan Filter properties dialog: General tab-page

7. From the new scan filter properties dialog, click on **Add** to create another filter condition in which we will specify the required patch name (i.e. MS03-026).

8. From the list of filter properties, select 'Patch' and then click on **Next**.

9. From the conditions drop down select *'is not installed'* and in the value field type in *'MS03-026'*.

10. Click on the **Add** button to include this condition in the scan filter.

11. Click on **OK** to finalize the configuration and create the filter. The new filter is added as a new permanent sub-node. (**Security Scanner ▶ Scan filter ▶ Missing Blaster Patch**).

# Example 2 – Create a filter that lists all Sun stations with a web server

To create a filter which lists all Sun workstations that are running a web server on port 80, perform the following steps:

1. Right click on the **Security Scanner ▶ Scan filter** node and select **New ▶ Filter...** This will bring up the new scan filter properties dialog.

2. In the filter name field type in 'Sun WS web servers on port 80'.

3. Click on the **Add** button.

4. From the list of filter properties select 'Operating System' and then click on **Next**.

5. From the conditions drop down select '*Includes*' and in the value field type in 'Sun OS'.

6. Click on the **Add** button.

7. From the properties dialog, click on the **Add** button to add another filter condition.

8. Select '*TCP Port*' and click on **Next**. This will bring up again the filter conditions dialog.

9. From the conditions drop down select *'is open'* and in the value field type in *'80'*.

10. Click on the Add button to include this condition in the scan filter.

11. Click on OK to finalize the configuration and create the filter. The new filter will be added as a new permanent node. (Security Scanner
▶ Scan filter ▶ Sun WS web servers on port 80).

# Configuring GFI LANguard N.S.S.

# Introduction

All the GFI LANguard N.S.S. configuration options are accessible via a set of sub-nodes included under the **Configuration** node. These are the:

- Scanning profiles node
- **Scheduled scans** node
- Secondary Second Second Second
- Section Alerting options node
- 👒 Parameter files node

Use the above mentioned nodes to:

- Customize the default security scanning profiles
- Add new scanning profiles with different scanning options
- Configure scheduled security scans
- Configure the GFI LANguard N.S.S. email alerting options
- Configure the database backend to use.

# **Scanning Profiles**

Scanning Profiles are preconfigured templates which define the way that vulnerability scanning is carried out (for example, which vulnerability checks will be executed during a target computer scan). These profiles provide the vulnerability test instructions and parameters which the scanning engine requires to perform a security audit against selected targets.

GFI LANguard N.S.S. supports multiple scanning profiles. In fact it ships with a number of default scanning profiles which you can use to perform general or specialized target vulnerability scans. Further more, you can customize these default scanning profiles by adding or removing vulnerability checks as well as customize the respective operational parameters. You can also create new custom scanning profiles which suite your network infrastructure and target scanning needs.

For more information on how to create, configure and customize scanning profiles refer to the 'Scanning Profiles' chapter in this manual.

## **Scheduled scans**

Use the **Configuration** > **Scheduled Scans** sub-node to configure scans which are to be automatically executed periodically or on a specific day/time. This allows you to automatically execute particular scans at night or early in the morning on regular bases. The 'Scheduled Scan' configuration options are organized in 2 tabs; the **Result Saving** tab and the **Results Notification** tab. To access these tabs Right click on **Configuration** > **Scheduled Scans** and select **Properties**. This will bring up the Scheduled Scans configuration dialog.

Scheduled Scans Properties	×	
Result saving Results Notification		
Specify where to save scan results to XML or HTML reports.		
For result comparison operations, GFI LANguard N.S.S. saves all scan results to the database backend.		
You can configure GFI LANguard N.S.S. to output the scheduled scan results also to XML or HTML report files in a directory on the hard drive.		
Save as XML files WARNING: Saving scheduled scan results to XML can take several minutes for large scans and can cause performance degradation.		
Save scheduled scan results to XML file	L	
C:\Program Files\GFI\LANguard Network Security Scann		
Save as HTML reports           Generate and save scan result html reports to:           C:\Program Files\GFI\LANguard Network Security Scann		
OK Cancel <u>Apply</u>		

Screenshot 47 - The Scheduled Scans configuration dialog

By default, all scheduled scan results are stored in the database backend. Use the **Result Saving** tab to configure the scheduled scans properties and store scheduled scan results to a specific XML file or HTML file (one file per scheduled scan).

GFI LANguard N.S.S. can also be configured to automatically send scheduled scan reports to a specific email address/recipient (for example, Administrator) at the end of a scheduled scan. Use the **Results notifications** tab to specify which reports to email and the destination email address. GFI LANguard N.S.S. can automatically email 2 types of report; the 'Full Scan' report and the 'Results Comparison' report.

# Creating a scheduled scan

🔗 GFI LANguard N.S.S. 7.0						
Eile <u>T</u> ools <u>⊂</u> onfigure <u>H</u> el	þ					
🚺 🚺 New Scan 📝 🕴 Using	g: Currently Logged-O	n User 🔻 User Nam	e:	Password:		<b>I</b>
Tools Explorer 🌐 🎗	🍅   🗙 💣   🇞	1				
GFI LANguard Network Sec	🔺 Scan Target	Last Scanned	Next Scan	Interval	Profile	Descrip
Security Scanner (Defa	3 TMJason	<never scanned=""></never>	21/10/2005 12:00:00	1 Hours(s)	Default	Test M
tiene tools	ISAServer	<never scanned=""></never>	21/10/2005 12:00:00	1 Hours(s)	Default	ISASer
Configuration     E - 5 Configuration	<u> </u>					
Scheduled Scans	P2					
- Computer Profiles						
Alerting Options						
Parameter Files						
Database Maintena						
⊕-∰ General						
•	•					•

Screenshot 48 - List of configured Scheduled Scans

To create a scheduled scan:

1. Right click on the **Configuration → Scheduled Scans** sub-node and select **New → Scheduled scan...** This will bring up the 'New Scheduled Scan' configuration dialog.

Т	1Jason Properties 💦 💦	(		
	General Logon Credentials			
	Configure the scheduled scan.			
	Scan target: TMJason			
	Scanning profile: Default			
	Description: Test Machine scheduled scan			
	Perform a scan:			
	O One time only			
	● Every: 1 Hours ▼			
	Next scan: 21/10/2005 💌 12:00:00			
	,			
	OK Cancel Apply			

Screenshot 49 - New Scheduled Scan dialog

2. In the **General** tab which opens by default, specify the target computers (hostname, IP and IP range).

3 Select the scanning profile that will be used for this scheduled scan and specify a description of the scheduled scan.

4. If this scheduled scan is to be run periodically, specify the frequency at which the scan will be launched.

5. Specify the date and time at which the scheduled scan will start.

6. If alternative logon credentials are required, click on the **Logon Credentials** tab.

7. From the provided drop down list, select one of the following options:

- 'Alternative Credentials' Select this option to authenticate to target computers a specific username and password string.
- 'SSH Private Key' Select this option to authenticate to Linux based target computers using Private Key authentication. Specify the username and the 'Private Key' file in the provided fields.

**NOTE:** Alternatively, you can configure scheduled scans to get the authentication details directly from Computer Profiles. To enable this feature select the *'Use data from computer profiles'* option. For more information on computer profiles, refer to the 'Computer Profiles' section further on in this chapter.

8. Click on **OK** to save your settings.

### Configuring the scan results saving options

Scheduled Scans Properties	×	
Result saving Results Notification	_	
Specify where to save scan results to XML or HTML reports.		
For result comparison operations, GFI LANguard N.S.S. saves all scan results to the database backend.		
You can configure GFI LANguard N.S.S. to output the scheduled scan results also to XML or HTML report files in a directory on the hard drive.		
Save as XML files		
WARNING: Saving scheduled scan results to XML can take several minutes for large scans and can cause performance degradation.		
Save scheduled scan results to XML file		
C:\Program Files\GFI\LANguard Network Security Scann		
Save as HTML reports		
Generate and save scan result html reports to:		
C:\Program Files)(GET)  ANguard Network Security Scape		
OK Cancel Apply		

Screenshot 50 - Scheduled Scans properties dialog

By default, scheduled scan results are stored in the Microsoft Access or Microsoft SQL Database backend. However, you can also output the scan results to an XML or HTML report file. These files can then be used further on for report comparison operations. To store the scan results in an XML/HTML file:

1. Right click on the **Configuration ►** Scheduled Scans sub-node and select **Properties**. This will bring up the scheduled scans properties dialog.

2. To save the scan results to an XML file, select the 'Save scheduled scan results to XML file' option and specify the name and path of the XML file.

3. To save scan results to an HTML file, select the 'Generate and save scan result HTML reports to:' option and specify the name and path of the HTML file.

4. Click on **OK** to save the settings.

### Configuring result notification options

Scheduled Scans Properties		
Result saving Results Notification		
Specify whether to send scheduled scan reports by email to the administrator		
Once a scheduled security scan is completed send the following emails to the administrator:		
Eull scan results in HTML format. NOTE: Full scan results will generate a large size email for large networks.		
Result comparison with previous security scheduled scan with same scan target and scanning profile. NOTE: If there are no differences, the email will not be sent.		
NOTE: Administrator email and mail server settings are configured from Configuration\Alerting Options		
OK Cancel Apply		

Screenshot 51 - Scheduled Scan properties: Results Notification tab

GFI LANguard N.S.S. can be configured to send scheduled scan reports to a particular recipient via email. Reports that can be sent via email include the 'Full Scan Results' report and the 'Results comparison report'. The 'Full Scan Results' report contains the results of the scheduled scan that has just been completed. The 'Result Comparison' report includes the changes/differences identified between the results of the latest scan and the results of the preceding scan.

**NOTE:** The 'Results Comparison' report will not be emailed to the administrator if no differences exist between the compared scan results or if you are running your very first scheduled scan.

To specify which reports will be sent via email after a scheduled scan:

1. Right click on the **Configuration ▶ Scheduled Scans** sub-node and select **Properties**. This will bring up the scheduled scans properties dialog.

2. Click on the **Results Notifications** tab.

3. Select the report(s) that will be emailed upon completion of the scheduled scan.

4. Click on **OK** to save your settings.

**NOTE:** Use the **Configuration** Alerting Options node to make changes in the mail server settings or administrator email address.

# **Computer Profiles**

Use the **Configuration** > **Computer Profiles** sub-node to specify and store the logon credentials of your network computers.

When working in both large and smaller-sized networks, you always find that for some computers, you have to log in with one set of credentials and for some other computers you have to log in with a different set of credentials. Particular systems such as Linux based systems often make use of special authentication methods such as Public key authentication. Such authentication methods generally require special/custom logon credentials such as private key files instead of the conventional password strings.

Through computer profiles, you can specify a different set of logon credentials for each target computer. The scanning engine can then refer to the logon credentials stored in these computer profiles when authenticating to target computers. This in turn obsoletes the need to specify a default set of logon credentials prior to starting a network scan as well as makes it possible to scan in the same (single) session target computers which require different logon credentials and authentication methods.

For example, you can run vulnerability checks on Windows targets which require username/password credential strings and Linux based targets which require username/SSH private key files, in a single scanning session.

### About SSH Private Key file authentication

GFI LANguard N.S.S. connects to Linux based target computers through SSH connections. In Public Key cryptography, 2 keys (in the form of text files) are used to verify the authenticity of an SSH connection request. These keys are identified as the 'SSH Private Key' and 'SSH Public Key'.

The SSH Private Key is the half of the key pair that the scanning engine will use to authenticate to a remote Linux based target. This means that the SSH Private Key is used instead of the conventional password string and hence must be stored on the computer which is running GFI LANguard N.S.S.

The SSH Public Key is the part which the remote target computer will use to challenge the authentication of GFI LANguard N.S.S. and is stored on the remote target computer(s).

The SSH Key pair (i.e. Public and Private Keys) are manually generated using a third party tool such as SSH-KeyGen (generally included by default in the Linux SSH package).

## Creating a new computer profile

test-Profile1 Properties		X
General Logon Credent	ials	
Specify creder	itials to use to log on to target computer(s).	_
Logon to target comput O s <u>e</u> curity context of being made.	er(s) using the account under which the security scan is	
Iternative credent	ials:	
<u>U</u> ser Name:	JasonM	
Password:	*****	
C certificate authenti	fication (Linux/Unix logons):	
Uger Name:		
Certificate file:	ļ	
NOTE: To scan Windows computers use the scan security context (currently logged on user/service user) or alternative logon credentials.		
To scan non-Windows of specify alternative cred	omputers such as Linux machines you need to entials or a certificate authentification file.	
	OK Cancel <u>A</u> pply	

Screenshot 52 - Computer Profile properties dialog

To create a new computer profile:

1. Right click on the **Configuration ▶ Computer Profiles** sub-node and select **New ▶ Computer(s) Profile...** This will bring up the Computer Profile properties dialog.

2. In the **General** tab which opens by default, specify the target computer name.

3. Click on the Logon Credentials tab.

4. Select the required authentication method and specify the respective logon credentials.

5. Click on **OK** to save your settings.

### Changing the properties of a computer profile

🕼 GFI LANguard N.S.S. 7.0			
Eile Iools Configure Help			
🛛 🜔 New Scan 🔹 Using: Currently Logged-On User 💌 🗉	ser Name: Passwor	d:	<b>E</b> 😴
Tools Explorer 🛛 🕲 🗙 😭			
GFI LANguard Network Securi Computer(s)	Logon method	Username	Password / Path
E Security Scanner (Default TMJason	Alternative credentials	JasonM	<supplied></supplied>
Configuration     Scanning Profiles     Scheduled Scans     Gomputer Profiles     Alerting Options     Parameter Files     Database Maintenanc     El-     General	Security certificates	JasonM	C:\GFI_LNSS.cer
			•

Screenshot 53 - List of existing computer profiles

To change the properties of an existing computer profile:

1. Click on the **Configuration** > **Computer Profiles** sub-node.

2. Right click on the computer profile that you wish to configure and select **Properties**.

3. Make the required changes and click on **OK** to save your settings.

### Using computer profiles in a scan

💇 GFI LANguard N.S.S. 7.0				
<u> E</u> ile <u>T</u> ools <u>C</u> onfigure <u>H</u> elp				
🚺 🕐 New Scan Using: Currenti	ly Logged-On User 👻 User Name: Th	ne "Use data from com	puter profile	es" button
Tools Explorer #	1 🛎   🗙 💼			
GFI LANguard Network Security	△ Computer(s)	Logon method	Username	Password / Path
🗄 👩 Security Scanner (Default)				
🕀 🎯 Tools				
😟 🤔 Configuration				
😟 🎲 General				
	•			•

Screenshot 54 - The 'Use data from computer profiles' button

To use the credentials specified in the **Computer Profiles** node in a scan, click on the 🔄 ('Use data from computer profiles' button) included in the GFI LANguard N.S.S. tool bar.

# **Parameter files**

🕃 GFI LANguard N.S.S. 7.0				
Eile <u>T</u> ools <u>C</u> onfigure <u>H</u> elp				
🚺 New Scan 🛛 Using: Currently Logged-On User 💌 User Name: Password: 🛛 📓 🕏				
Tools Explorer 4 File	Name	Description		
GFI LANguard Network Security	enterprise_numbers.txt	List of OID (Object Identifier) to enterprise (vendor/university) relation codes.		
😟 🚮 Security Scanner (Default)	ethercodes.txt	Mapping list for mac address to vendor identification.		
🗉 🥳 Tools 🖉 🗒	ftp.txt	List of ftp server banners used to identify OS by installed ftp service.		
🖻 🤔 Configuration 🖉 i	identd.txt	List of Ident server banners used to identify OS by installed Ident service.		
🕀 🏹 Scanning Profiles 📳 🖉	object_ids.txt	Mapping list for SNMP object identifiers to vendor / product identification.		
Scheduled Scans	passwords.txt	List of common weak passwords.		
Computer Profiles	rpc.txt	Mapping list for RPC protocol service numbers to service name identification.		
Alerting Options	smtp.txt	List of SMTP banners used to identify OS by installed SMTP service.		
Parameter Files 2	snmp-pass.txt	List of community strings used to assert SNMP implementation weaknesses.		
Database Maintenance C	telnet.txt	List of telnet server banners used to identify OS by installed telnet service.		
E General	www.txt	List of web server banners used to identify OS by installed web service.		
	$\sum$			
		2		
# 1	last updated: 00	ctober 13, 2003		
#				
# C	5 fingerprinting	g (WWW service - port 80)		
# <sup>#</sup>	ased on banner i	cesponses		
		<u> </u>		

Screenshot 55 - List of Parameter Files

Use the **Configuration** > **Parameter Files** sub-node to access and edit the various text based parameter files that GFI LANguard N.S.S. uses for target computer scanning.

**NOTE:** Only advanced users should modify these files. If these files are modified in an incorrect way, they will affect the functionality and reliability of the GFI LANguard N.S.S. target discovery process.

The following is a list of the parameter files that can be accessed and modified through the **Parameter Files** node:

- Enterprise\_numbers.txt This file contains a list of the OIDs (Object Identifiers) and the associated enterprise (vendor/university) relation codes. During target scanning, GFI LANguard N.S.S. will first query the 'object ids.txt' file for information on the discovered network device. If this information is not available, GFI LANguard N.S.S. will then reference the *Enterprise numbers.txt'* file and will attempt to identify the product manufacturer through the vendor specific information (retrieved from the target device). The vendor information is based on SMI Network Management Private Enterprise Codes, which can be found on: http://www.iana.org/assignments/enterprise-numbers.
- Ethercodes.txt This file contains a list of Mac addresses together with their associated vendor(s).
- **Ftp.txt** This file contains a list of FTP server banners through which GFI LANguard N.S.S. can identify the OS of a target computer i.e. GFI LANguard N.S.S. can identify the type of OS running on a target computer, by analyzing the installed FTP server.
- Identd.txt This file contains 'identd' protocol banners through which GFI LANguard N.S.S. can identify the OS running on a target computer. i.e. GFI LANguard N.S.S. can identify an OS through the banner information.
- **Object\_ids.txt** This file contains the SNMP object\_ids as well as the associated vendor(s) and product(s). When a device responds to an SNMP query, GFI LANguard N.S.S. will compare the Object ID information (sent by the target computer) to the OID information stored in this file.
- **Passwords.txt** This file has a list of passwords which are used to check target computers for weak passwords (i.e. to perform dictionary attacks).
- Rpc.txt This file contains the list of RPC protocol service numbers together with the associated service name identification. When RPC services are found running on a UNIX/Linux based target computer, GFI LANguard compares the RPC information received to the information listed in this file. In this way it can identify and verify the associated service name identification.
- Smtp.txt This file contains a list of SMTP banners together with the associated Operating Systems. As with 'FTP' and 'identd' files, these banners are used by GFI LANguard N.S.S. to identify the OS that is running on the target computer.
- Snmp-pass.txt This file contains a list of popular community strings. GFI LANguard N.S.S. uses these community strings to assert and identify SNMP weaknesses on a target computer. During target probing, the scanning engine will check if any of the community strings listed in this file are being used by the SNMP target server. Should it be the case, these community strings will be reported by the SNMP scanning tool in the scan results.
- **Telnet.txt** This file contains a list of different telnet server banners. GFI LANguard N.S.S. will use these telnet banners to identify which OS is running on a target computer.

 Www.txt – This file contains a list of different web server banners. GFI LANguard N.S.S. will use these web server banners to identify which OS is running on a target computer.

## **Database Maintenance Options**

### Introduction

Use the **Configuration Database Maintenance Options** node to select and configure the GFI LANguard N.S.S. database backend. The database backend is used to store the results of network security scans.

From the **Database Maintenance Options** node, you can also configure the database backend maintenance features. For example, you can configure GFI LANguard N.S.S. to automatically delete scan results which are older than a particular age.

If you are using a Microsoft Access database backend, you can also schedule database compaction. Compaction allows you to repair any corrupted data and to delete database records marked for deletion in your database backend.

### Configuring your database backend

To configure the database maintenance options, right-click on the **Configuration → Database Maintenance Options** node and select **Properties**. This will bring up the database maintenance properties dialog.



Screenshot 56 - The database maintenance properties dialog
The options included in this dialog are accessible through three tabs. These are the:

- Change Database tab
- Manage Saved Scan Results tab
- Advanced tab.

#### Selecting your database backend

Use the **Change Database** tab to specify which database backend will be used to store the saved scan results. Supported database backends include *Microsoft Access* and *Microsoft SQL Server 2000 or higher*.

## Storing scan results in an Microsoft Access database backend

To store scan results in an Microsoft Access database:

1. Right click on the **Configuration > Database Maintenance Options** node and select **Properties**.

2. Select the 'Microsoft Access' option

3 Specify the full path (including the file name) of your Microsoft Access database backend.

**NOTE 1:** If the specified database file does not exist it will be created for you.

**NOTE 2:** If the specified database file already exists and belongs to a previous version of GFI LANguard N.S.S. the following message is displayed.

Warning	X
	A database corresponding to a previous version of GFI LANguard N.S.S. was found. Do you want to upgrade the database? NOTE: Choosing No will delete and recreate the database.
	Yes No Cancel

Screenshot 57 - Database backend upgrade dialog

Click on **Yes** to upgrade the existing scan results database to GFI LANguard N.S.S. 7.0.

Click on No to overwrite the existing database.

4. Click on the **OK** button to save your settings.

## Storing scan results in an Microsoft SQL Server database backend

Properties				
Change Database Manage Saved Scan Results Advanced				
Current GFI LANguard N.S.S. database backend settings				
File path: C:\Program Files\GFI\LANguard Network Se				
New GFI LANguard N.S.S. database backend settings				
Indicate below the new type of database backend to use:				
○ MS Access				
Please specify the name or IP of the machine containing the SQL Server / MSDE database to use:				
Server: TMJason_SQLserver				
Use NT authority credentials				
Use the below SQL/MSDE credentials to log into the database backend:				
User name: JasonM				
Password:				
OK Cancel Apply				

Screenshot 58 - Microsoft SQL Server database backend options

To store scan results in an Microsoft SQL Server database:

1. Right click on the **Configuration Database Maintenance Options** node and select **Properties**.

2. Select the 'Microsoft SQL Server' option.

3. Select the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

4. Specify the SQL Server credentials or select the 'Use NT authority credentials' option to authenticate to the SQL server using windows account details.

5. Click on **OK** to save your settings.

**NOTE 1:** If the specified server and credentials are correct, GFI LANguard N.S.S. will automatically log on to your SQL Server and create the necessary database tables. If the database tables already exist it will re-use them.

**NOTE 2:** When using NT authority credentials, make sure that GFI LANguard N.S.S. services are running under an account which has both access and administrative privileges on the SQL Server databases.

operties			
Change Database Manage Saved Scan Results Advanced			
Saved scan results in database backend			
Target	Profile	∇ Date ▲	
🧧 localhost	Default	21/10/2005 14:1	
📓 localhost	Default	21/10/2005 09:5	
Iocalhost	Default	30/09/2005 14:4:	
📓 localhost	Default	30/09/2005 14:4:	
📓 localhost	Default	29/09/2005 16:3	
🔲 localhost	Default	27/09/2005 13:2	
📓 localhost	Default	27/09/2005 13:2 🖵	
1001001001100	at 19 2 6		
	Delete scan(s)	Mark scan(s) as <u>r</u> ead only	
Saved scan results retaining options Retain:			
Scans which are	less than 30 da	ys 💌 old	
C only last 10 scans per scan target per profile NOTE: Scan results marked as read only will not be removed by the database results cleanup operations.			

#### Database maintenance - manage saved scan results

Screenshot 59 - Database maintenance properties: Managed saved scan results tab

Use the **Manage Saved Scan Results** tab to maintain your database backend and delete saved scan results which 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 N.S.S. automatically deletes saved scan results which 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.

To manually delete saved scan results, select the particular result(s) and click on the **Delete Scan(s)** button.

To let GFI LANguard N.S.S. manage database maintenance for you, select one of the following options:

- 'Scans which are less than' Select this option to automatically delete scan results which are older than a specific number of days/weeks or months.
- 'Only last' Select this option to retain only a specific number of recent scan results.

#### Database maintenance - advanced options

Properties 🛛 🗙				
Change Database Manage Saved Scan Results 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 backend you need to manualy set maintenance plans according to your company policies.				
Compact Now				
Schedule repair/compact database operation				
○ <u>0</u> ne time only				
● Every: 1 weeks ▼				
Next operation 28/10/2005 💌 14:35:23 🗧				
OK Cancel Apply				

Screenshot 60 - Database Maintenance properties: Advanced tab

Use the **Advanced** tab to compact and repair an Microsoft Access based database backend.

One of the most important things you can do to improve your database's performance is to regularly repair and compact it. During compaction the database files are reorganized and records that have been marked for deletion are removed. In this way you can regain precious storage space.

During the compaction process, GFI LANguard N.S.S. also repairs corrupted database backend files. Corruption may occur for various reasons. In most cases, a Microsoft Access database gets corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, hung up processes, forced reboots, etc.).

Through the Advanced tab, you can:

- Manually repair and compact a Microsoft Access database backend by clicking on the **Compact Now** button.
- Automate and schedule compaction of the Microsoft Access database backend. In this way, the GFI LANguard attendant service will automatically handle the compaction process for you.

Through the options provided in the **Advanced** tab, you can specify the frequency at which the scheduled database compaction will take place.

To compact your Microsoft Access database backend once, select the 'One time only' option.

To compact your database backend on regular basis (i.e. periodically), select the *'Every'* option and specify:

1. The frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

2. The date and time when the first/next compaction session will take place.

## **Scanning Profiles**

#### Introduction

Scanning profiles are configurable templates which determine the vulnerability tests that will be run against the target computers as well as the data that will be retrieved from scanned targets during a security audit.

GFI LANguard N.S.S. ships with a default list of scanning profiles which you can use to perform different scans on your network and retrieve various information without having to make configuration changes. The number of tests performed by each scanning profile varies according to the network vulnerability area which must be checked for weaknesses.

For example, you can have scanning profiles that run a number of vulnerability checks which cover various/extensive areas of your network (for example, the 'Default' scanning profile) as well as 'specialized' scanning profiles which run vulnerability checks and report only weaknesses related to a specific area of your network (for example, such as the Trojan Ports scanning profile which scans only for open ports which are commonly exploited by hackers and Trojan applications).

The list of default scanning profiles is accessible by expanding the **Configuration ▶ Scanning profiles** node. Out of the box, GFI LANguard N.S.S. includes an extensive list of different scanning profiles, some of which are listed below:

- Default: Use this scanning profile to retrieve various pieces of information as well as perform a balanced varied set of security vulnerability tests on your target computer(s). The information retrieved from the target(s) includes: Commonly exploited open ports, installed applications, installed security applications and status of signature files, OS data, users and groups, network devices, missing patch and service packs, USB devices, shares, time of day, sessions, audit policies and running services.
- **CGI scanning**: Use this scanning profile to retrieve OS information and perform security tests which are directly relevant to Web Servers.
- Full TCP and UDP port scan: Use this scanning profile to perform a full TCP and UDP open port scan on the target(s). All ports from 0-65535 are checked and queried during the scanning process.
- **Missing patches**: Use this scanning profile to check the target(s) for missing security updates and service packs.
- **Ping them all**: Use this scanning profile to check which target(s) in the specified range are turned on.

- Share finder: Use this scanning profile to check which shares are open on the target(s) as well as retrieve any properties related to these shares.
- **Removable media protection**: Use this scanning profile to check which removable media devices are connected to the target computer(s).
- **Applications**: Use this scanning profile to check which applications are installed on the target computer(s).
- Other options are also available.

The selection of a scanning profile for a security scan is generally dictated by the:

1. Type of tests to be performed and the data retrieval operations you want to run against your target(s).

2. Time you have to generate these reports.

**WARNING:** The more vulnerability checks you want to run, the more time will be consumed to complete the security audit scan.



Screenshot 61 - The Scanning Profiles node

The default set of scanning profiles is fully customizable. You can also create new custom scanning profiles which suite your network layout as well as your scanning needs. For example, you may want to create a scanning profile that is set to be used when scanning the computers in your DMZ as opposed to your internal network.

Through the use of 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. This is possible by creating different preconfigured scanning profiles which suite specifically the security scanning needs of your IT infrastructure and which can be individually utilized in different network scanning sessions. Use scanning profiles to your advantage as they allow you to perform specialized tests and queries (for example, enumerate only the installed applications) on your networks saving you time when less more specialized information is needed while at the same time allowing you to perform tests which take lots of time under different conditions (for example, full TCP/UDP port scans).

## Scanning profiles in action

## Scanning your local computer with the 'Default Scanning Profile'

- 1. Go on File > New > Scan single computer...
- 2. Select the 'This computer' option.

New scan
Scan <u>Type</u> : Single computer
This Computer
O Another Computer
(Computer name/IP Address)
Scan Profile: Default
OK Cancel

Screenshot 62 - New Scan dialog

- 3. Set the value of the 'Scan Profile' combo box to 'Default'.
- 4. Click on **OK** to start the scan.

**TIP:** Take note of the time it takes to complete the scan as well as the information range it returns.

## Scanning your local computer with the 'Applications Scanning Profile'

- 1. Go on File > New > Scan single computer...
- 2. Select the 'This computer' option.

New scan		×	
Scan <u>T</u> ype:	Single computer	-	
· · · · · · · · · · · · · · · · · · ·			
This Comp	outer		
O <u>A</u> nother Co	omputer		
	(Computer name/IP Address)		
	-	_	
Scan <u>P</u> rofile:	Default		
	Only SNMP		
	Share Finder		
	Trojan Ports		
	Removable Media Protection		
	Applications	_	
	USB Devices		

Screenshot 63 - New Scan Dialog: Selecting the 'Applications' vulnerability scanning profile

- 3. Set the value of the 'Scan Profile' combo box to 'Applications '.
- 4. Click on **OK** to start the scan.

As you can see the time it takes to complete a vulnerability scan using the 'Applications' scanning profile is considerably less than that of the 'Default' scanning profile previously performed. This is because the 'Applications' scanning profile only performs specific vulnerability checks which analyze and report the applications that are installed on the scanned target computers. Hence no other unrelated vulnerability checks are run against the target(s) and no extra data is retrieved from the target computer(s).

On the other hand, the 'Default' scanning profile is more generic and performs vulnerability checks on almost all vulnerable areas of your network. Hence it takes more time to complete the scan as well as more information is retrieved from the scanned targets and reported in the scan results.

### Creating a new scanning profile

To create a new scanning profile:

1. Right click on the **Configuration ▶ Scanning profiles** node and select **New ▶ Scan Profile...** 

2. Specify the name of the new profile in the dialog on display.



Screenshot 64 - The Scanning Profile configuration page

#### 3. Click on the **OK** button.

In the right pane of the configuration interface, you will now be presented with a tabbed interface through which you can configure the operational parameters for this new scanning profile. The tabs displayed at the top of the scanning profile configuration page are listed below:

- **TCP ports** tab Use the options in this tab to enable TCP port scanning and to specify which TCP ports are to be checked.
- **UDP ports** tab Use the options in this tab to enable UDP port scanning and to specify which UDP ports are to be checked.
- **OS data** tab Use the options in this tab to specify which operating system data is to be retrieved from the target(s).
- **Vulnerabilities** tab Use the options in this tab to enable vulnerability scanning and to specify which vulnerability checks will be run on the target(s).
- Patches tab Use the options in this tab to enable scanning for missing patches and to specify which missing security updates will be checked on the target(s).
- **Scanner properties** tab Use the options in this tab to configure the scanning engine's operational and target discovery parameters (for example, timeout values, query methods etc.).
- **Devices** Use the options in this tab to enable scanning for attached devices and to specify which installed network and USB devices are authorized/unauthorized.
- **Applications** Use the options in this tab to enable installed application scanning and specify which installed applications are authorized/unauthorized.

## Customizing a scanning profile

To customize a scanning profile:

- 1. Expand the **Configuration > Scanning Profiles** node.
- 2. Select the scanning profile to be edited.

3. From the right pane, use the tabs at the top of the page to access the required configuration page(s) and make the necessary parameter changes. The changes will become effective in the next new scan.

## **Configuring TCP/UDP ports scanning options**

GF1LANguard N.S.S. 7.0   Elle Iools   Configure Help   New Scan Image: Scale Sc	sion User Name: Password:	- 🗆 ×
Tools Explorer     Image: Security Scanner (Default)     Image: Tools     Image: Only Security Scanner (Default)	CCP Ports   UDP Ports   OS Data   Vulnerabilities   Patches   Scanner O pecify what information is to be retrieved by the scanner when using this Enable TCP Port Scanning O Ports Description	ptions   Devices   Applications : profile
Scanning Profiles Default (active) GGI Scanning GGI Scanning GGI Scanning GGI Scanning Git Scanning Ghy Web Ghy Web Ghy Web Ghy Web Ghy SNMP Ghy Share Finder Ghy Share	■ 1-65535   Full Port List     ✓   13   Daytime ⇒ Time of the Day     ✓   17   Qotd ⇒> Quote of the Day     ✓   17   Explored and the point of the Day     ✓   17   Diation of the Day     ✓   17   Explored and the Day     ✓   17   Diation of the Day     ✓   17   FTP ⇒ File Transfer Protocol     ✓   22   SSH => Remote Login Protocol     ✓   23   Telnet => Remote Login Protocol     ✓   25   SMTP => Simple Mail transfer Protocol     ✓   42   NameServer => With Next Name Server     ✓   53   Domain => Domain Name Server     ✓   79   Finger     ✓   80   HTTP => World Wide Web, HTTP     ✓   93   inuxconf     ✓   110   Pop2 => Post Office Protocol 3     ✓   111   SurRPC => SUN Remote Procedure Call     ✓   113   identd => Authentication Service     ✓   118   SolServ => SOL Services	[very time consur
	Advanced Add	Edit <u>R</u> emove

Screenshot 65 - Scanning Profiles properties: TCP Ports tab options

#### Enabling/disabling TCP Port scanning

To enable TCP Port Scanning in a particular scanning profile,

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **TCP Ports** tab.

3. Select the check box next to the 'Enable TCP Port Scanning' option.

**NOTE:** TCP Port scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no open TCP port tests will be performed in the security audits carried out by this scanning profile.

#### Enabling/disabling UDP Port scanning

To enable UDP Port Scanning in a particular scanning profile,

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile that you wish to customize.

2. Click on the **UDP Ports** tab.

3. Select the check box next to the 'Enable UDP Port Scanning' option.

**NOTE:** UDP Port scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no open UDP port tests will be performed in the security audits carried out by this scanning profile.

#### Customizing the list of TCP/UDP ports to be scanned

To specify which TCP/UDP ports will be enumerated and processed by a scanning profile during a security audit:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **TCP Ports** or **UDP Ports** tab accordingly.

3. Select the check box of the TCP/UDP ports that will be checked by this scanning profile.

#### Adding a new TCP/UDP port to the list

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **TCP Ports** or **UDP Ports** tabs accordingly.

3. Click on the Add button. This will bring up the Add Port dialog.

Properties - Port 80 🛛 🗙				
Port Details				
Enter the number of the port and the port description.				
Port number/range:				
<b>SI</b>				
Port description:				
HTTP => World Wide Web, HTTP				
☐ Is a <u>t</u> rojan port				
OK Cancel Apply				

Screenshot 66 - Add Port dialog

4. Specify the port number or port range (for example, '80-200') and a suitable port description.

**NOTE:** Always include specified port ranges within single (') quotes (for example, '80-200').

5. If the application associated with this port is a Trojan program, select the 'Is a Trojan port' option.

#### How to edit or remove a port

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **TCP Ports** or **UDP Ports** tab accordingly.

3. Select the port that you wish to edit or remove.

4. Click on the Edit or Remove buttons accordingly.

**NOTE:** When a port is removed, it will be deleted from ALL of the scan profiles. If you want to stop GFI LANguard N.S.S. from checking for its presence only, unselect the check box next to it.

### **Configuring OS data retrieval options**



Screenshot 67 - Scanning Profiles properties: OS Data tab options

Use the **OS Data** tab to specify which OS information will be collected from a target computer during security scanning. GFI LANguard N.S.S. can retrieve operating system data from both Windows and Linux based target computers.

#### **Customizing OS Data Retrieval parameters**

To specify which OS Data will be enumerated and processed by a scanning profile during a security audit:

1. Expand the **Configuration > Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **OS Data** tab.

3. Expand the 'Windows OS Data' group and 'Linux OS Data' group accordingly.

4. Specify which Windows/Linux OS information is to be retrieved by the security scanner from the target operating systems.

For example, if you want to exclude administrative shares from scan results, expand set the *'Enumerate shares'* option and set the 'Display admin shares' option to *'No'*.

## Configuring vulnerabilities scanning options



Screenshot 68 - Scanning Profiles properties: Vulnerabilities tab options

Use the **Vulnerabilities** tab to specify which vulnerabilities will be investigated during target computer scanning. By default, GFI LANguard N.S.S. ships with a pre-defined list of vulnerability checks. You can customize and select which checks are to be performed during a security audit on a scan profile by scan profile basis. You can also add your own custom vulnerability checks to suit your network's security scanning requirements.

#### Enabling/disabling vulnerability scanning

To enable vulnerability scanning in a particular scanning profile,

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile that you wish to customize.

2. From the right pane, click on the Vulnerabilities tab.

3. Select the check box next to the 'Enable Vulnerability Scanning' option.

**NOTE:** Vulnerability scanning is configurable 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. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the Vulnerabilities tab.

$\Delta$	Name	Impact (Desc 🔺
	😫 All Servers: (e)shop Online-Shop System 👘	Allows attack
	🚺 All Servers: A1Stats (a1disp)	Remote file re
$\checkmark$	📳 All Servers: a1 stats CGI script show files	Possible to vi
$\checkmark$	🚺 All Servers: Abe Timmerman zml.cgi File D	Remote file re
$\checkmark$	🛃 All Servers: ad.cgi	Ad.cgi has a l
$\checkmark$	😫 All Servers: Adcycle	Possible Wea
$\checkmark$	👭 All Servers: Adcycle - build.cgi	Build.cgi if it h
$\checkmark$	😫 All Servers: Aglimpse	It is possible t
$\checkmark$	😫 All Servers: AHG's 'search.cgi' Search En	Remote users
$\checkmark$	😫 All Servers: Alex Heiphetz Group EZShop	Possible direc
$\checkmark$	😫 All Servers: AnyForm2	It is possible t
$\checkmark$	😫 All Servers: Arts Store.cgi	Remote file re
$\checkmark$	😫 All Servers: Auktion.cgi	Remote comr
$\checkmark$	😫 All Servers: BBS Forum vulnerability	Possible Rem
$\checkmark$	👭 All Servers: Brian Stanback bsguest.cgi	Possible to ru
$\checkmark$	🛃 All Servers: Brian Stanback bslist.cgi	Possible to ru 🚽
1		

Screenshot 69 - Select the vulnerability checks to be run by this scanning profile

3. Select the check box next to the vulnerability tests that you wish to run through this scanning profile.

#### Customizing the properties of vulnerability checks

All the checks listed in the **Vulnerabilities** tab have specific properties which determine when the check is triggered and what details will be enumerated during a scan.

E	dit CGI Abuse		×
	General Description		
	⊻ulnerability Name:	All Servers: (e)shop Online-Shop System	
	Short Description:	Allows attackers to execute commands (web ser	
	Security <u>L</u> evel:	<b></b>	
	<u>B</u> ugtraqID/URL:	ê 🖉	
	Time consumption:	Quick to execute	
	Trigger condition		
	HTTP Method:	GET method	
	To check for the <u>U</u> RL:	eshop.pl?seite=;cat%20/etc/passwd	
	Under the <u>D</u> irectories:	cgi-bin	
	<u>R</u> eturn string:	Contains the text	
		ROOT:	
		OK Cancel Apply	

Screenshot 70 - Vulnerability properties dialog: General tab

Vulnerability check properties include:

- Vulnerability name and short description.
- Security Level associated with the vulnerability.
- BugtraqID/URL to relevant information.
- Time consumed by the respective vulnerability check during scanning.
- Vulnerability check trigger conditions (for example, HTTP method, the Return string).

To change the properties of a vulnerability check:

- 1. Right click on the vulnerability to customize and select **Properties**.
- 2. Make the required changes to the check properties.
- 3. Click on **OK** to save your settings.

Vulnerability	checks	- advanced	options
---------------	--------	------------	---------

Advanced Vulnerabilities Properties					
[General]					
Specify advanced vulnerability scanning options					
Vulnerability Scan Options					
Internal checks					
Weak passwords					
FTP anonymous access allowed					
Administrator account exists					
Users that never logged on					
New vulnerabilities are enabled by default	Yes				
CGI Probing Settings					
Send CGI request through proxy	No				
Proxy IP					
Proxy port					
OK Canc	el <u>A</u> pply				

Screenshot 71 - Advanced vulnerability scanning dialogs

Use the **Advanced** button included in the **Vulnerabilities** tab to bring up the advanced vulnerabilities scanning options. From these options you can:

1. Configure extended vulnerability scanning features which check your target computers for weak passwords, anonymous FTP access, and unused user accounts.

2. Configure how GFI LANguard N.S.S. is to handle newly created vulnerability checks which you create. Specify whether to automatically include or exclude newly added vulnerability checks in the other scanning profiles.

3. Configure GFI LANguard N.S.S. to send CGI requests through a specific proxy server. This is mandatory when CGI requests will be sent from a computer which is behind a firewall to a target web server which is 'outside' the firewall (for example, Web servers which are on a DMZ). The firewall will generally block all the CGI requests which are directly sent by GFI LANguard N.S.S. to a target computer which 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 be used to convey the CGI request to the target.

## Configuring patch scanning options

GFI LANguard N.S.S. 7.0   Elle <u>I</u> ools <u>C</u> onfigure <u>H</u> elp				
New Scan 👹 🍟 Using: a NULL S	Session 👻 🛛	ser Name:	Passi	vord:
Tools Explorer	TCP Ports UDP Ports	: OS Data Vul	nerabilities Patches Scann	er Options Devices Applications
GFI LANguard Network Security Scan Generative Scanner (Default) Generative Scanner (Default) Generation Generation Generation	Specify what informatic Detect installed and Patch management da Pulation to be shealed	n is to be retrieve d missing service tabase - <u>Confiqu</u>	ed by the scanner when using packs / patches re supported languages	) this profile
Default (active)	Builetin names	ONumber	□ □ Date posted	Tala
CGI Scanning	Bulletin names	000101	2005.07.01	Windows Server 2002 Service P
		896426	2005-06-27	Security Update for Windows Se
- S Missing Patches	Not Available	891861	2005-06-27	Update Bollup 1 for Windows 20
Only Web		893066	2005-06-14	Security Lodate for Windows 20
Only SNMP	Not Available	890830	2005-06-13	Windows Malicious Software Be
Ping them All		890830	2005-06-13	Windows Malicious Software Be
Share Finder	MS05-019	893066	2005-06-13	Security Update for Windows XP
Slow Networks	MS05-025	883939	2005-06-13	Cumulative Security Update for I
Removable Media Protection	☑ 00 MS05-030	897715	2005-06-13	Cumulative Security Update for
Test-Profile	MS05-027	896422	2005-06-13	Security Update for Windows XP
Scheduled Scans	☑ ØMS05-027	896422	2005-06-13	Security Update for Windows Se
Computer Profiles	☑ 00 MS05-026	896358	2005-06-13	Security Update for Windows XP
Alerting Options	☑ 00 MS05-026	896358	2005-06-13	Security Update for Windows Se
- 🍣 Parameter Files	☑ 00 MS05-032	890046	2005-06-13	Security Update for Windows XP
Database Maintenance Options	☑ ፩ MS05-032	890046	2005-06-13	Security Update for Windows Se 🗨
teneral			File: gfipatche:	en.xml; Version: 1; Last updated on: Never 408 patches
	Find bulletin:		Find	
<b>τ</b>	You could search by er	ntering a bulletin r	name (e.g. MS02-017) or ente	ering a QNumber (e.g. Q311967)

### Customizing the missing patch scanning profile options

Screenshot 72 - Scanning Profiles properties: Patches tab options

Use the **Patches** tab to specify which security updates are to be checked for when scanning a target computer. The patches to be checked are selected from the complete list of available software updates which is included in this tab. This list is automatically updated whenever GFI releases a new missing patch definition file update for GFI LANguard N.S.S.

From this tab you can also view the Bulletin information of each software update in the list. To access this information, right-click on the respective patch and select **Properties**.

#### Enabling/disabling missing patch detection checks

To enable missing patch detection checks in a particular scanning profile,

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Patches** tab.

3. Select the check box next to the 'Detect installed and missing service packs/patches' option.

**NOTE:** Missing patch detection checks are configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no missing patch detection checks will be performed in the security audits carried out by this scanning profile.

#### Customizing the list of software patches to be scanned

To specify which missing software patches will be enumerated and processed by a scanning profile during a security audit:

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile that you wish to customize.

Bulletin names	QNumber	∇ Date posted	Title 🔺
🗖 🙆 MS05-049	900725	2005-10-13	Security Update for Windows XP x64,
🗖 😫 MS05-049	900725	2005-10-13	Security Update for Windows XP (KB.
🗖 🖸 🖾 MS05-044	905495	2005-10-13	Security Update for Windows XP (KB.
🗹 🥸 MS05-049	900725	2005-10-13	Security Update for Windows Server.
🗹 🥸 MS05-044	905495	2005-10-13	Security Update for Windows Server.
🗹 🥸 MS05-044	905495	2005-10-13	Security Update for Windows Server.
🗹 🔇 MS05-049	900725	2005-10-13	Security Update for Windows Server.
🗹 🔇 MS05-044	905495	2005-10-13	Security Update for Internet Explore.
🗹 🔇 MS05-049	900725	2005-10-13	Security Update for Windows Server.
🗹 🔇 MS05-047	905749	2005-10-13	Security Update for Windows XP (KB.
🗹 🔇 MS05-047	905749	2005-10-13	Security Update for Windows 2000 (.
🗹 🔇 MS05-049	900725	2005-10-13	Security Update for Windows 2000 (. 🥃
ন 🔦			

2. From the right pane, click on the Patches tab.

Screenshot 73 - Selecting the missing patches to be enumerated

3. Select/unselect the check box next to the missing patch checks that you wish to run through this scanning profile.

Bulletin Info							×
Bulletin							
Bulletin ID:	MS05-019	QNumber:	893066	Da	te: 2	2005-06-14	
Ttile:	Security Update fo	r Windows 2000 (KE	893066)				
Description:	A security issue f Windows-based s update from Micr	as been identified tl system and gain con osoft. After you inst	hat could allow trol over it. Yo all this item, yo	an attacker to remo u can help protect y ou may have to rest	itely co our con art you	ompromise your nputer by installing this ır computer.	
Applies To:	Windows 2000 fa	mily					
URL:	http://support.mic	rosoft.com					
File							
File Name:	Windows2000-KB8	93066-v2-x86-ENU.	EXE				
File Size:	739 KB						
File URL:	http://www.down	oad.windowsupdate	com/msdownl	oad/update/v3-1999	90518/	cabpool/windows2000-kb893	2

#### Using the search bulletin information facility

Screenshot 74 - Extended bulletin information

To search for a particular bulletin:

1. Specify the bulletin name (for example, MS02-017) or QNumber (for example, Q311987) in the search tool entry box included at the bottom of the right pane.

2. Click on Find to start searching for your entry.

## Configuring the security scanning options

New Scanning ger un Osingt a Note S	0221		
I GELLANguard Network Security Scap	7	CP Ports   UDP Ports   OS Data   Vulnerabilities   Patches Sca	nner Options Devices Applica
Security Scanner (Default)	St	ecify network discovery and other parameters on how the scann bug information.	er is to discover machines and c
Configuration		Network Discovery Methods	
🖻 🐺 Scanning Profiles		Netbios queries	Yes
Default (active)		SNMP queries	Yes
- GI Scanning		Ping sweep	Yes
Full TCP & UDP Port Scan		Custom TCP discovery (e.g. 21, 25, 80)	
Missing Patches		Network Discovery Options	
Only Web		Scanning delay (default 100 ms)	100
Ping them All		Network discovery query responses timeout (default 500 ms)	500
- Share Finder		Number of retries (default 1)	1
		Include non-responsive computers	No
- Slow Networks		Netbios Query Options	
Removable Media Protection		Scope ID	
Test-Profile		SNMP Query Options	
Computer Profiles		Load SNMP enterprise numbers	Yes
Alerting Options		Community strings (e.q. public, private)	public
Parameter Files		Global Port Query Options	
Database Maintenance Options		TCP port scan query timeout (default 1500 ms)	1500
🖅 🇀 😰 General		UDP port scan query timeout (default 600 ms)	600
	Ξ	WMI Options	
		WMI timeout (default 20000 ms)	20000
	-	SSH Options	
	⊨		

Screenshot 75 - Scanning Profiles properties: Scanner Options tab

Use the **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.

Configurable options include timeouts, types of queries to run during target discovery, SNMP scopes for queries and more.

**NOTE:** Configure these parameters with extreme care! An incorrect configuration can effect the security scanning performance of GFI LANguard N.S.S.

## Configuring the attached devices scanning options

Screenshot 76 - The Devices configuration page: Network Devices tab options

Use the **Devices** tab to enable the scanning and reporting of network and USB devices installed on your target computers.



Screenshot 77 - Dangerous network devices are listed as High Security Vulnerabilities

Together with device enumeration, you can further configure GFI LANguard N.S.S. to generate high security vulnerability alerts whenever particular USB and network hardware is detected. This is achieved by compiling a list of unauthorized/blacklisted network and USB devices which you wish to be alerted of.

You can also configure GFI LANguard N.S.S. to exclude particular devices from the scan results which are considered as 'safe' such as USB keyboards. This is achieved by compiling a list of safe/white-listed devices which you would like the scanning engine to ignore during a security audit.

Create a high security vulnerability for USB devices whose name contains:				
Bluetooth				
Mass storage				
pen				
drive				
Creative				
<u>P</u> en				

Screenshot 78 - List of unauthorized/blacklisted network devices

Network and USB device scanning is configurable on a scan profile by scan profile basis. Therefore you can customize your device audits by creating multiple scanning profiles with different unauthorized or safe devices lists.

For example, you can create a generic device-scanning profile which checks and enumerates all USB and network devices found connected to your targets. In this case, you do not need to specify any device in the unauthorized and ignore lists of your scanning profile. Similarly you can create a separate scanning profile which enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers.



Screenshot 79 - List of unauthorized/blacklisted network devices

However, in this case 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 2 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 unauthorized/safe devices lists.

Use the **USB Devices** sub-tab to configure the attached USB devices scanning options and unauthorized/safe devices lists.

#### Scanning for attached network devices



Screenshot 80 - Device configuration page: Network Devices tab options

#### Enabling/disabling checks for installed network devices

To enable scans for attached network devices in a particular scanning profile:

1. Expand the **Configuration > Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Devices** tab.

3. Select the check box next to the 'Enable Scanning for installed Network Devices on the target computer(s)' option.

**NOTE:** Network device scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no checks for installed network devices will be performed in the security audits carried out by this scanning profile.



Screenshot 81 - Devices configuration page: Unauthorized devices and Ignore devices lists

#### Compiling a list of unauthorized network devices

To compile a list of dangerous network devices:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

- 2. From the right pane, click on the **Devices** tab.
- 3. Click on the Network Devices sub-tab.

Create a high security vulnerability for network devices whose name contains:	
Wireless Wifi Infra Ired	A

Screenshot 82 - List of unauthorized/blacklisted network devices

4. In the list under 'Create a high security vulnerability for network devices whose name contains:' specify the names of the network devices that you wish to classify as high security vulnerabilities.

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.

#### Compiling a list of safe network devices

To compile a list of safe network devices:

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile that you wish to customize.

- 2. From the right pane, click on the **Devices** tab.
- 3. Click on the Network Devices sub-tab.

4. In the list under 'Ignore devices (Do not list/save to db) whose name contains:' specify the names of the safe network devices that you wish to exclude from the scan results.

**NOTE:** Include only one network device name per line.

#### Configuring advanced network device scanning options

Adva	nced Network Devices Properties	×
Ger	neral	
	Specify advanced network devices options.	
[	- Enumerate Network Devices	
	Enumerate wired network devices	Yes
	Enumerate wireless network devices	Yes
	Enumerate software enumerated network devices	Yes
	Enumerate virtual network devices	Yes
	OK Cancel	Apply

Screenshot 83 - Advanced network devices configuration dialog

From the **Devices** tab, you can also specify the type of network devices that will be 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:

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile that you wish to customize.

- 2. From the right pane, click on the **Devices** tab.
- 3. Click on the **Network Devices** sub-tab.
- 4. Click on the **Advanced** button at the bottom of the page.
- 5. Set the required options to 'Yes'.
- 6. Click on the **OK** button.

### Scanning for USB devices



Screenshot 84 - Dangerous USB devices are listed as High Security Vulnerabilities

#### Enabling/disabling checks for attached USB devices

To enable scans for attached USB devices in a particular scanning profile:

1. Expand the **Configuration > Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Devices** tab.

3. Select the check box next to the 'Enable scanning for USB Devices installed on the target computer(s)' option.

**NOTE:** USB device scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no checks for attached USB devices will be performed in the security audits carried out by this scanning profile.

#### Compiling a list of unauthorized USB devices

To compile a list of unauthorized/dangerous USB devices:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Devices** tab.

3. Click on the **USB Devices** sub-tab.

4. In the list under 'Create a high security vulnerability for USB devices whose name contains:' specify the names of the USB devices that you wish to classify as high security vulnerabilities.

Create a high security vulnerability for USB devices whose name contains:	
Bluetooth	<b></b>
Mass storage	
pen	
drive	
Creative	
<u>P</u> en	
<u> </u>	

Screenshot 85 - List of unauthorized/blacklisted USB devices

For example, if you enter the word "iPod" you will be notified through a high security vulnerability alert when a device whose name contains the word " iPod" is detected.

#### Compiling a list of safe USB devices

To compile a list of safe USB devices:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

- 2. From the right pane, click on the **Devices** tab.
- 3. Click on the **USB Devices** sub-tab.

4. In the list under 'Ignore (Do not list/save to db) devices whose name contains:' specify the names of the safe USB devices (for example, USB mouse) that you wish to exclude from the scan results.

NOTE: Include only one USB device name per line.

## Configuring the applications scanning options

Use the **Applications** tab to specify which installed applications will be investigated by this scanning profile during a target computer scan.



Screenshot 86 - The applications configuration page

Through this tab, you can also configure GFI LANguard N.S.S. to detect and report 'unauthorized' or 'hot' software installed on scanned targets and to generate high security vulnerability alerts whenever such software is discovered.



Screenshot 87 - List of supported anti-virus and anti-spyware applications

By default, GFI LANguard N.S.S. also supports integration with particular security applications. These include various anti-virus and anti-spyware software. During security scanning, GFI LANguard N.S.S. will check if the supported virus scanner(s) or anti-spyware software is correctly configured 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 applications configuration page. These are the **Installed Applications** sub-tab and the **Security Applications** sub-tab.

#### Enabling/disabling checks for installed applications

To enable scans for installed applications in a particular scanning profile:

1. Expand the **Configuration > Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Applications** tab.

3. Select the check box next to the '*Enable Scanning for installed applications on target computers*' option.

**NOTE:** Installed applications scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no checks for installed applications will be performed in the security audits carried out by this scanning profile.

## Scanning for installed applications



Screenshot 88 - The Applications tab: Installed Applications tab options

### Compiling a list of unauthorized applications

To compile a list of dangerous applications:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

- 2. From the right pane, click on the **Applications** tab.
- 3. Click on the **Installed Applications** sub-tab.

4. Select the 'All applications except the ones whose name contains:' option.



Screenshot 89 - List of unauthorized applications

5. In the list underneath the previously selected option, specify the names of the installed applications which you want to classify as high security vulnerabilities.

For example, if you enter the word "Kazaa" you will be notified through a high security vulnerability alert when an application whose name contains the word "Kazaa" is detected.

#### Compiling a list of safe applications

To compile a list of safe applications:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

- 2. From the right pane, click on the **Applications** tab.
- 3. Click on the Installed Applications sub-tab.

4. In the list under 'Ignore (Do not list/save to db) applications whose name contains:' specify the names of the applications (for example, Excel) that you wish to exclude from the scan results.

NOTE: Include only one application name per line.

#### Scanning for security applications



Screenshot 90 - The Applications configuration page: Security Applications tab options

GFI LANguard N.S.S. ships with a default list of anti-virus and antispyware applications which can be checked during security scanning.

#### Enabling/disabling checks for security applications

To enable checks for installed security applications in a particular scanning profile:

1. Expand the **Configuration > Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Applications** tab.

3. Select the check box next to the 'Detect and process installed antivirus/anti-spyware software on target computers' option.

**NOTE:** Installed security applications scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is

not selected, no checks for installed security applications will be performed in the security audits carried out by this scanning profile.

#### Customizing the list of security application for scanning

To specify which security applications will be scanned during an audit:

1. Expand the **Configuration** > **Scanning Profiles** node and select the scanning profile that you wish to customize.

2. From the right pane, click on the **Applications** tab.

3. Click on the Security Applications tab.



Screenshot 91 - Selecting the security applications to be investigated

4. Select the check boxes of the security applications that you wish investigate when performing security audits with this scanning profile.

#### Configuring security applications - advanced options

Adva	inc	ed Applications Properties	×
Ger	ner	a	
		Specify advanced applications options	
Γ	-	Generate high security vulnerabilities when	
		A security product is out of date	Yes
		Real time protection for an antivirus is disabled	Yes
		Real time protection for an antispyware is disabled	No
		No supported antivirus is installed	No
		No supported antispyware is installed	No
	-	Timeout	
		HTTP/FTP timeout when checking updates on remote sites	60
		OK Cancel	Apply

Screenshot 92 - Advanced configuration options dialog

Use the **Advanced** button included in the **Security Applications** configuration page to configure extended security product checks which generate high security vulnerability alerts when:

- The anti-virus or anti-spyware product definitions files are out of date.
- The 'Realtime Protection' feature of a particular anti-virus or antispyware application is found disabled.
- None of the selected anti-virus or anti-spyware software is currently installed on the scanned target computer.

# **GFI LANguard N.S.S. program updates**

#### Introduction

GFI LANguard N.S.S. uses a number of parameter files which serve different purposes in the process of security scanning your network. These databases are updated periodically by GFI offering the latest Microsoft patch management updates, vulnerability checks and device identification data. Periodically GFI also provides new GFI LANguard N.S.S. builds that contain new features as well as engine fixes and enhancements which improve the performance of your network security scanning tools.

Use the 'Program Updates' tool to download the latest reference files and program builds. By default, GFI LANguard N.S.S. is configured to automatically check for program updates at every startup. Program updates can also be started manually by bringing up the 'Program Update Wizard' from **Help > Check for updates**.

## Checking the version of current installed updates



Screenshot 93 - Details on the currently installed updates

Click on the **General** > **Program Updates** node to view the update status of your GFI LANguard N.S.S.

The program update details are organized into categories and are shown in the right pane of your configuration interface. Each category includes the date of the last update performed, the date of the most recent download as well as the version of the current installed database updates.

# Downloading software updates from Microsoft in different languages

Dpdate LANguard Network Security Scanner	_ 🗆 ×
Choose which packages to update Disabled items represents packages already updated that you can also update by checking "Update ALL files" or packages without update.	
Packages: Microsoft Software Updates - German Version Microsoft Software Updates - French Version Microsoft Software Updates - Italian Version Microsoft Software Updates - Spanish Version	
Checked packages details: Size: 2209000 bytes Inss_7_patchmngmt_de.cab - Version 4 - Thursday, November 10th, 2005 Added New Patches Inss_7_patchmngmt_fr.cab - Version 4 - Thursday, November 10th, 2005 Added New Patches Update <u>A</u> LL files (including the ones already updated)	
< <u>B</u> ack <u>N</u> ext >	Cancel

Screenshot 94 - Selecting the Microsoft update files

Out of the box, GFI LANguard N.S.S. supports multilingual patch management. Through multilingual patch management you can download and deploy missing Microsoft product updates, discovered during a security scan, in a variety of different languages.

The security scanning engine identifies missing Microsoft patches and service packs by referencing 'Microsoft Software Update files'. These files contain the latest (complete) list of product updates currently provided by Microsoft and are available in all languages supported by Microsoft products.

Use the GFI LANguard N.S.S. 'Program Update' tool, to download the latest 'Microsoft Software Update files' in all languages currently in use on your network. This would allow the security scanning engine to discover and report both English as well as non-English missing patches and service packs. Based on this information, you can then use the patch deployment engine to download and install the missing update files in their respective languages network wide.

Supported languages include: English, German, French, Italian, Spanish, Arabic, Danish, Czech, Finnish, Hebrew, Hungarian, Japanese, Korean, Dutch, Norwegian, Polish, Portuguese, Portugese\_Brazilian, Russian, Swedish, Chinese, Chinese\_Taiwan, Greek, and Turkish.

Information on how to download multilingual 'Microsoft Update Files' is provided further on in this chapter.
### Starting program updates manually

To manually start a GFI LANguard N.S.S. program update:

1. Right click on the **General** ▶ **Program Updates** node and select **Check for Updates...**. This will bring up the 'Check for updates wizard'.

💭 Update LANguard Network Security Scanner	_ 🗆 ×
<b>Choose which action to do in the next step</b> 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.	<b>e</b>
Update application files from the following location     Location     GFI web site     Alternative location:     http://www.gfi.com/Insupdate	j
Download all update files from GFI web site to this path:      Browse      From the second s	]
< Back	ancel

Screenshot 95 - The Check for Updates wizard: Stage 1

2. Specify the location from where the required update files will be downloaded.

3. To change the default update-download path, select the *'Download all update files.....to this path'* option.

4. Click on **Next** to proceed with the update.

😳 Update LANguard Network Security Scanner	
Choose which packages to update Disabled items represents packages already updated that you can also update by checking "Update ALL files" or packages without update.	
Packages:	•
<ul> <li>Microsoft Software Opdates - Preficit Version</li> <li>Microsoft Software Updates - Italian Version</li> <li>Microsoft Software Updates - Spanish Version</li> <li>Microsoft Software Updates - Arabic Version</li> </ul>	<b>_</b>
Checked packages details:	
Size: 2209000 bytes	<b>_</b>
Inss_7_patchmngmt_de.cab - Version 4 - Thursday, November 10th, 2005 Added New Patches	
Inss_7_patchmngmt_fr.cab - Version 4 - Thursday, November 10th, 2005 Added New Patches	•
Update ALL files (including the ones already updated)	
< <u>B</u> ack <u>N</u> ext >	Cancel

Screenshot 96 - The Check for updates Wizard: Stage 2

5. Select the updates that you wish to download. Available updates include:

- **GFI LANguard N.S.S. Vulnerabilities Update:** Select this option to download new vulnerability checks and fixes.
- GFI LANguard N.S.S. Dictionaries Update: Select this option to download dictionary file updates (for example, weak community strings dictionary file updates, weak passwords dictionary files updates, etc.)..).
- **Microsoft Software Updates:** Select the 'Microsoft Software Update' files of all languages currently in use on your network. For more information refer to the 'Downloading Microsoft updates in different languages' section at the beginning of this chapter.

**NOTE:** Select the 'Update ALL files (including the ones already updated)' option at the bottom of the dialog to update all files.

6. Click on **Next** to continue.

7. Click on Start to begin the update process.

### Checking the availability of software updates at program startup

By default, GFI LANguard N.S.S. checks for the availability of supported updates at every program startup. To disable automated software update checks at startup:

1. Right click on the **General** ▶ **Program Updates** node and select **Properties**. This will bring up the Program Updates **P**roperties dialog.

-Build Updates-

Check for newer builds at startup

Screenshot 97 - The 'Check for newer builds at startup' option

2. Unselect the 'Check for newer builds at startup' option at the bottom of the dialog.

# Configuring which updates to check on program startup

To configure which updates are checked at program startup:

Program Updates Properties	×
General	
Specify which updates to check for at startup.	
Product database/engine updates:	
<ul> <li>✓ Vulnerabilities Database</li> <li>✓ GFI LANguard N.S.S. Dictionaries Update</li> <li>✓ Microsoft Software Updates - English Version</li> <li>Microsoft Software Updates - German Version</li> <li>Microsoft Software Updates - Italian Version</li> <li>Microsoft Software Updates - Italian Version</li> <li>Microsoft Software Updates - Spanish Version</li> <li>Microsoft Software Updates - Arabic Version</li> <li>Microsoft Software Updates - Danish Version</li> <li>Microsoft Software Updates - Czech English Version</li> <li>Microsoft Software Updates - Finnish Version</li> </ul>	
Ownload updates from the <u>G</u> FI Web site.	
http://www.gfi.com/Insupdate	
Build Updates	
OK Cancel Apply	

Screenshot 98 - Program Updates Properties dialog

1. Right click on the **General** > **Program Updates** node and select **Properties**.

2. Select the database and engine updates that you wish to download.

3. Specify the location from where you wish to download the selected program updates.

4. Click on **OK** to save these settings.

# Patch management: Deploying Microsoft Updates

### Introduction

Use the patch management tool to automatically keep your Microsoft products up to date with the latest patches and service packs. Supported Microsoft products include Windows 2000, XP and 2003 Operating systems, Microsoft Office XP or later, Microsoft Exchange 2000 or later and Microsoft SQL Server 2000 or later. A complete list of Microsoft products supported by GFI LANguard N.S.S. is available on <a href="http://kbase.gfi.com/showarticle.asp?id=KBID002573">http://kbase.gfi.com/showarticle.asp?id=KBID002573</a>.

To successfully deploy patches and service packs on your network system, you must:

Step 1: Scan your network system.

Step 2: Select the computers on which patches and service packs will be deployed.

Step 3: Select the patches and service packs that will be deployed.

Step 4: Download the required patches and service pack files.

Step 5: Deploy the downloaded patches and service packs to your targets.

To successfully deploy patches on the selected target computers, you must make sure that:

- GFI LANguard N.S.S. is running under an account which has administrative rights on the target computer to which the updates will be deployed.
- NetBIOS service is enabled on the remote computer.

For more information on how to enable NetBIOS refer to the 'Enabling NetBIOS on a target computer' section in the 'Miscellaneous' chapter.

### About the patch deployment agent

GFI LANguard N.S.S. makes use of a patch deployment agent to deploy patches, service packs and custom software on remote targets. The patch deployment agent is a service which is silently (and automatically) installed on the remote target computer during patch deployment. Its purpose is to successfully run and monitor the installation of updates at a (configurable) scheduled time, making GFI LANguard N.S.S. more efficient and reliable than counterparts running agent-less patch deployment.

### About recalled patches

It is not uncommon that Microsoft recalls patches and service packs. Cases in point are the MS03-045 patch for Windows and MS03-047

patch for Exchange that were released on the 15<sup>th</sup> October 2006. Patches are generally recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates.

When this happens, GFI LANguard N.S.S. will still report recalled patches as missing, even though these cannot be installed. If you do not want to be informed about these missing patches you must disable checking for that particular patch. This is done as follows:

1. Expand the **Configuration** > **Scanning Profiles** sub-node and select the profile that you wish to configure.

2. From the right pane, click on the **Patches** node and unselect the respective bulletin from the provided list.

You can also add recalled patches to an ignore list. The patch ignore list allows you to exclude particular patches such as recalled patches from security scanning audits. To add a missing patch to the ignore list:

- 1. Perform a security scan on your network.
- 2. From the scan results, access the list of missing patches.
- 3. Select the patch that you want to add to the ignore list.



3. Right click and select **Patches** > Add to ignore list for > This computer.



Screenshot 99 - Patches included in the ignore list of a particular target

To view the patches in the ignore list of a particular target computer , click on the **San Results** > **System patches status** node.

### Multilingual patch management

The GFI LANguard N.S.S. patch management engine automatically downloads and installs the missing Microsoft security software updates and service packs which match the language being used by the target computer.

For more information on multilingual patch management refer to the 'Downloading Microsoft updates in different languages' section at the beginning of this chapter.

### Selecting the target computers where patches will be deployed

Once a network security scan has completed, you can start the deployment of missing patches and service packs on your target computers.

Missing patches and service packs can be deployed on a single target computer, on a selection of target computers as well as on all target computers that have missing patches and service packs.



Screenshot 100 - Deploying missing service packs and patches

### Deploying missing updates on one computer

From the 'Scanned Computers' (middle) pane, right-click on the computer that you wish to update and select **Deploy Microsoft** updates ▶ [Service packs on or Patches on] ▶ This computer.

### Deploying missing updates on a range of computers

1. From the 'Scanned Computers' (middle) pane, select the check box of the computers that you wish to update.

2. Right click on any of the selected computers and select **Deploy** Microsoft updates ▶ [Service packs on or Patches on] ▶ Selected computers.

### Deploying missing updates on all computers

From the 'Scanned Computers' (middle) pane, right-click on any of the listed target computers and select **Deploy Microsoft updates** ► [Service packs on or Patches on] ► All computers.

# Selecting which patches to deploy



Screenshot 101 - Patch Deployment options page

After you have specified which target computers will be updated, GFI LANguard N.S.S. will automatically bring up the Patch Deployment options. These options are displayed in the right pane of the configuration interface together with the list of target computers selected and the English/non-English updates that will be downloaded and deployed on the enumerated targets.

**NOTE:** To manually open the patch deployment options click on **Tools > Deploy Microsoft patches**.

### Sorting results

The Patch Deployment options page allows you to organize and view the list of service packs and patches to be deployed in two ways:

- 'Sort by computers' This view shows the list of missing patches grouped per target computer.
- 'Sort by patches' This view shows the list of all missing patches sorted by 'Update file name'.

Switch between these views by clicking on the **Sort by computers** and **Sort by patches** tabs accordingly.

### Selecting the patches to be deployed

Sort by computers	Sort by patches	Deployi	ment Status	
Update file name			State	Bull
🔲 🌄 Windows-KB	3890830-V1.10-EN	VU.exe	Not downloaded	Not
🛛 🗖 🏹 WindowsXP	-KB896424-x86-E	NU.exe	Not downloaded	MSI
🔲 🌉 WindowsXP	-KB900725-x86-E	NU.exe	Not downloaded	MS
🛛 🗹 🔀 WindowsXP	-KB905749-x86-E	NU.exe	Not downloaded	MSI
🛛 🗹 🔀 Windows×P	-KB904706-x86-E	NU.exe	Not downloaded	MSI
🛛 🗹 🏹 WindowsXP	-KB905414-x86-E	NU.exe	Not downloaded	MSI
<ul> <li>■</li> </ul>				

Screenshot 102 - Selecting patches to be downloaded and deployed

By default, GFI LANguard N.S.S. will download and deploy all the missing English and non-English patches and service packs discovered during a network security scan. To exclude particular patches from a download and deployment session, unselect the check box next to the respective patch.

### Download the patch and service pack files

After selecting the required patches and service packs you can start to download these update files.

Once triggered, GFI LANguard N.S.S. will automatically handle downloading of missing patches and service in their respective languages (English and non-English).



Screenshot 103 - A list of patches to be downloaded

### Starting patch and service pack downloads

To start the download of a specific patch or service pack, right-click on the respective patch file and select **Download File**.

To start the download of all the selected patches or service packs, right-click on any patch file and select **Download all checked files**.

The icons next to each update file show the current download status. These icons indicate the following states:

- Bownloaded
- Currently being downloaded
- Waiting for user to navigate to the web page to click on the link to download the file
- Not downloaded.

### Downloads which require user intervention

GFI LANguard N.S.S. 7.0				
∃le <u>T</u> ools <u>⊂</u> onfigure <u>H</u> elp				
🜔 New Scan 🕴 Using: Alternative C	redentials 🛛 👻 User Name: 172.16	.130.144\administr Password: *	****	
Tools Explorer 4	Specify updates to apply and select S	Start to start the deployment of upd	lates	<u>Options</u>
GFI LANguard N.S.S.		1.		
Security Scanner (Default)	Sort by computers Sort by patches	Status		
- Call Ficers	C Scanned compu Language	<ul> <li>Update file name</li> </ul>	State	Bule≜ g
Vulnerabilities [High sec	MICHALRESV English	Addinsec.exe	startin	g download MS0 S
- Vulnerabilities [Medium		M M fpwec	Not d	ownloaded MS0
- 📝 Vulnerabilities [All]		isahf68.exe	Not di	ownloaded MS0
<ul> <li>Missing Patches and Se</li> </ul>	lat fai	M CALletcoPkg exe	Nord	hwnloaded MSH
- Martin Devices - US				
Important Devices - Wi	MICROSOT			<u>Go</u>
Open Ports	Download Conter			
Auditing Policies	Download Center			
- Password Policies	Download Center Home	Office 2000 Und	late: Service Pack 3	(SP3)
Groups and Users	Download Categories	Office 2000 opu		
Computer Properties	Games	The Office 2000 Service	Pack 3 (SP3) provides the late	st product updates to Office
	DirectX	2000 and offers you the highest levels of performance and security available for Office		
🗄 🏇 Tools	Internet	2000. It can be installed	by enterprise, small business,	or individual users.
Deploy Microsoft Updates	Windows (Security &			
Deploy Custom Software	Updates)	Quick Info		
CONS LOOKUP	Windows Media			Office 2000 Update:
	Drivers	File Name:	O2kSp3.exe	English
	Office and Home	Download Size:	13271 KB	
	Applications	Data Dublishadi	10/01/0000	Download
Shimp Audit	Mobile Devices	Date Published:	10/21/2002	
	Macintosh & Other	Version:	3	
- Configuration	14			
Scanning Profiles	G. Daelau immediatelu			Beset Start
	<ul> <li>Deploy inmediately</li> </ul>			Jiden
- 🍓 Scheduled Scans 🖉				
Scheduled Scans	C Deploy on Nov 18, 2004	at 4:46 PM		

Screenshot 104 -Downloading a patch from a web page

Certain patch files require that you manually download them from a specific target site. These files are denoted by the  $\ll$  icon which is shown next to these particular files.

For such downloads, GFI LANguard N.S.S. will automatically open the parent web page in the bottom area of the deployment tool. Click on the download link shown in this web page to start the download process.

### Stopping active downloads

To stop an active patch-download, right-click on the particular patch and select **Cancel Download**.

## (Optional) Configure alternative patch file deployment parameters

Patch properties		×
General		
Patch file name:	Visio2003-KB840663-FullFile-ENU.CAB	
Bulletin:	Visio 2003 Service Pack 1	
Affected product:	Office	
Source <u>U</u> RL:		
http://www.downle	oad.windowsupdate.com/msdownload/update/v3-:	
Download directory	:	
C:\Program Files\G	FI\LANguard Network Security Scanner 7.0\Repos	
Deploy patch with t	he following command line parameters:	
/quiet /norestart D	ISABLESRCPROMPT=1 LOCALCACHESRCRES=0 N	
	OK Cancel	ply

Screenshot 105 - Patch file properties dialog

You can optionally configure alternative patch deployment parameters on a patch by patch basis. Parameters that can be configured include the download URL and the destination path of the downloaded patch file. To change the deployment and download settings of a missing patch:

1. Right click on the particular patch file and select **Properties**. This will bring up the patch file properties dialog.

2. Make the required changes and click on **OK** to save these settings.

# Deploy the updates



Screenshot 106 - Patch deployment options

### Starting the patch deployment process

After the required patch files have been downloaded, you can proceed with the deployment of these files on the respective targets. To start the deployment process, click on the **Start** button at the bottom-right of the patch deployment page.

### Monitoring the patch deployment process



Screenshot 107 - Monitoring the deployment process

To view the patch deployment activity in progress, click on the **Deployment Status** tab located next to the **Sort by patches** tab at the top of the right pane.

# Patch management: Deploying custom software

### Introduction

Use the 'Custom Software Deployment' tool to install custom software and deploy third party software patches or updates network wide.

For example, you can use this tool to deploy virus signature updates on your network computers.

The deploy custom software tool is accessible from **Tools** > **Deploy Custom software**. The process of deploying custom software is very similar to the process of deploying Microsoft updates on a computer. To deploy custom software on a target computer you must:

Step 1. Select the computer on which the software/update file will be installed.

Step 2. Specify the software which will be deployed.

Step 3. Start the deployment process.

### Selecting targets for custom software/patch deployment



Screenshot 108 - Selecting the target computers

1. Click on the **Tools > Deploy Custom software** node.

2. From the 'Computer(s) to deploy software' area (in the middle of the configuration dialog), click on **Add** to include a single computer, or click on **Select** to specify a range of computers on which custom software will be deployed.

**NOTE:** The list of computers can also be imported from a text file by clicking on the **Import** button.

# Enumerating the software to be deployed

😅 GFI LANguard N.S.S. 7.0			
<u>File T</u> ools <u>C</u> onfigure <u>H</u> elp			
🚺 New Scan Using: Current	ly Logged-On User 💌 User Name:	Passwor	rd: 🗾 📓
Tools Explorer	Configure which computers and which sof	tware files are to be deployed	<u>Options</u>
🕀 👰 Security Scanner (Default	Software to deploy Deployment Status	Options	, D
E 🍅 Tools	Software:	Genera	al Advanced
Deploy Microsoft Upda	Software Location Parameters	Add	
C DNS Lookus	C\cmdasuser exe	Befor	re deployment:
Traserente		Edit 🔽 V	Varn user before deployment (send a message)
Whois			Wait for user's approval
Epumerate Computers		Hemove	
Senumerate Users		L 5	top services before deployment
Snmp Audit		1	Services
Snmp Walk		/ <u>u_</u>	
😽 SQL Server Audit			software to deploy to target computer(s) via:
🖻 🤔 Configuration			dministrative shares
🖅 🍒 Scanning Profiles	Computer(s) to deploy software on:		
Scheduled Scans	Na. Notes	Add. C C	Sustom share:
Computer Profiles	T. WABNING : Filters will not		
Alerting Options	3	Remove After	deployment:
Parameter Files			o not reboot (shut down the computer(s)
Database Maintenanc		Seject	
		Import	epoot the target computer(s)
Version Information			Let the user decide when to reboot
		0 s	hut down the target computer(s)
			And the second sec
Support Center		IV D	velete cogied files from remote
	1	U	omparents) and appoyntent
GFI LANguard N.S.S.	C. D. J. J. L. D. D. L.	Con	nputer filters
- 🥭 GFI LANguard S.E.L.M	Deploy immediately Heset	<u>start</u>	
GFI Network Server M	C Deploy on 21/10/2005 🔽 at	13:33:35	

Screenshot 109 - Selecting the software to deploy

1. From the 'Software' area (in the middle of the configuration interface), click on **Add.** 

Edit patch	
Specify the location of the file to deploy on the target r	machines:
Deploy the file at location:	
C:\cmdasuser.exe	<b>2</b>
With the following parameters:	
C Windows operating system patch	
C Internet explorer patch	
⊂ <u>⊂</u> ustom	
OK Ca	ncel

Screenshot 110 - Specifying the software to deploy

2. Specify the source file location.

3. To specify command line parameters to pass on during the deployment of the file, select one of the following options:

- 'Windows operating system patch' Select this option if you are going to deploy Windows OS patches.
- 'Internet explorer patch' Select this option if you are going to deploy Internet Explorer patches.
- *'Custom'* Select this option if you want to include custom parameters. Specify the required parameters in the entry box provided at the bottom of the dialog.

### Start the deployment process

New Scan       Using: Currently Logged-On User       User Name:       Bessword:       Image: Currently Logged-On User       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software files are to be deployed       Image: Configure which computers and which software are are computer are computers and which softwar	GFI LANguard N.S.S. 7.0 File Tools Configure Help		
cols Explorer       1         Configure which computers and which software files are to be deployed       Dptions         Configure which computers and which software files are to be deployed       Dptions         Configure which computers and which software files are to be deployed       Dptions         Configure which computers       Add         Computer (s) to deploy of the sector deployment (send a message)       Wait for user's approval         Configuration       Scheduled Scans         Conputer (s) to deploy software on:       Name         Name       Notes         TMJASON       WARNING : Filters will no         Parameter Files       Support Center         Support Center       Support Center         Support Center       Support Center         Support Center       Computer (s) to velocit/shut down the computer (s)         Computer (s) after deployment       Computer (s) after deployment	New Scan Using: Current	ly Logged-On User 👻 User Name:	Password:
GFI LANguard Network Securi       Software to deploy       Deployment Status       Options       Image: Software So	Tools Explorer 🏾 📮	Configure which computers and which software files are to b	e deployed
Software to deploy       Deployment Status       Options       Image: Software to deploy         Software       Software       General       Add         Software to deploy       Deployment Status       General       Advanced         Software to deploy       Deploy furcesoft Upd;       Edit       Image: Software to deploy       Before deployment (send a message)         Software to deploy       Edit       Image: Software to deploy to target computer;       Image: Software to deploy to target computer;         Software to deploy cost       Software to deploy to target computer;       Image: Software to deploy t	🍯 GFI LANguard Network Securi 🔺		
Software       General       Advanced         Before deployment (send a message)       Before deployment (send a message)         Wain user before deployment (send a message)       Wain user before deployment (send a message)         Wain user before deployment (send a message)       Wain user before deployment (send a message)         Wain user before deployment (send a message)       Wain user before deployment (send a message)         Wain user before deployment (send a message)       Wain user before deployment (send a message)         Software Location       Bemove         Software to deploy to target computer(s) via:       Computer Profiles         Computer Profiles       Computer(s) to deploy software on:         Name       Notes         Parameter Files       Database Maintenand         Parameter Files       Database Maintenand         Porgram Updates       Import         Program Updates       Import         Porgram Updates       Import         Poleio optic files from remote computer(s)       Shut down the target computer(s)         Computaries after deployment       Select         Program Updates       Import         Poleio optic files after deployment       Statt         Support Center       Statt         Statt deployment       Statt	🗄 👰 Security Scanner (Default	Software to deploy Deployment Status	Options 4
★ Deploy Microsoft Updi         ★ Deploy Custom Software         ★ Deploy Custom Software         ★ Dis Lookup         ★ Traceroute         ★ Whois         ★ Traceroute         ★ Whois         ★ Enumerate Computers         ★ Enumerate Users         ★ Software Location	🖃 🎯 Tools	Software:	General Advanced
• Deploy Custom Softw           • Deploy Custom Softw             • Whols           • Deploy Custom Softw             • Whols           • Educed Custom Softw             • Stopservices before deployment (send a message)           • Wait for user's approval             • Sonp Audit           • Conjuter(s) to deploy software on:           • Copy software to deploy to target computer(s) via:             • Conjuter(s) to deploy software on:           • Name           • Notes             • Maintenance           • Notes           • Add             • Parameter Files           • Mathason ware consol (shu down the comp	- K Deploy Microsoft Upda	Software Location Parameters Add	
Works Lookup         Whois         Whois         Whois         Enumerate Computers         Simp Audit         Somp Walk         Computer(s) to deploy software on:         Name       Notes         Matering Options         Parameter Files         Database Maintenance         Somp Parameter Files         Database Maintenance         Somp Parameter Files         Support Center	Seploy Custom Softw.		Before deployment:
Waik for user's approval         Waik for user's approval         Stop services before deployment         Somp Walk         Computer[s] to deploy software on:         Computer[s] to deploy software on:         Name       Notes         Add         Parameter Files         Datases Maintenance         Sepect         Import         Program Updates         Support Center         Knowledge Base     <	DNS Lookup	Edit	Warn user before deployment (send a message)
Winds       Bemove         Winds       Winds         Winds       Stop services before deployment         Stop services before deployment       Stop services before deployment         Stop services before deployment       Stop services before deployment         Stop services before deploy to target computer(s) via:       Computer (s) to target computer(s) via:         Scaning Profiles       Computer (s) to deploy software on:       Computer (s) to deploy software on:         Parameter Files       Database Maintenanc       Alering Options         Program Updates       TMJASON       WARNING : Filters will no         Program Updates       Import       Remove         How to purchase       Support Center       Shut down the target computer(s)         Support Center       Support Center       Shut down the target computer(s)         Below on 21/10/2005       at 13:33:35       Deploy on 21/10/2005	* Traceroute		
Stop services before deployment         Stop services before deployment         Stop services before deployment         Stop services before deployment         Stop services	Whois	<u>R</u> emove	j wait for user's approval
Elulier de Gers Somp Audit Computer Profiles Scheduled Scans Computer Profiles Addem Parameter Files Database Maintenance Parameter Files Database Maintenance Parameter Files Database Maintenance Select Program Updates Wather Audit Program Updates Werson Information Uncessing How to purchase Support Center Knowledge Base GFI LANguard S.E.L.* Deploy immediately Reset Start Deploy on 21/10/2005 At 13:33:35 Somp Audit Computer(s) at a 13:33:35	K Fourmerate Computers		Stop services before deployment
<ul> <li>Simp Walk</li> <li>Solution Walk</li> <li>Computer (s) to deploy software on:</li> <li>Computer (s) to deploy to target computer(s)</li> <li>Computer (s) to deploy to target computer(s)</li> <li>Computer (s) to deploy to target computer(s)</li> <li>Computer (s) the user decide when to reboot</li> <li>Support Center</li> <li>Support Center</li> <li>Support Center</li> <li>GFI LANguard S.E.L.*</li> <li>Complaining all to deploy immediately Reset</li> <li>GFI LANguard S.E.L.*</li> <li>Comploy on 21/10/2005 at at 13:33:35 #</li> </ul>	K Some Audit		Services
<ul> <li>Simple Valak</li> <li>Somputer(s) to deploy software on:</li> <li>Computer(s) to deploy software on:</li> <li>Computer Profiles</li> <li>Scheduled Scans</li> <li>Computer Profiles</li> <li>Alerting Options</li> <li>Mame</li> <li>Notes</li> <li>Add</li> <li>Computer Profiles</li> <li>Alerting Options</li> <li>Parameter Files</li> <li>Database Maintenanc</li> <li>General</li> <li>Program Updates</li> <li>Wersion Information</li> <li>Knowledge Base</li> <li>GFI LANguard N.S.S.</li> <li>GFI LANguard S.E.L.M</li> <li>Deploy immediately</li> <li>Reset</li> <li>Start</li> <li>Computer(s) at 13:33:35</li> </ul>	Ké Somo Walk		
Second and a data     Computer (s) to deploy to target computer (s) to apply of target computer (s) to apply software on:     Computer (s) to deploy and the target computer (s)     Comp	Sol Server Audit		Construction to deploy to townsh computer/a) visu
<ul> <li>Administrative shares</li> <li>Administrative shares</li> <li>Computer Profiles</li> <li>Administrative shares</li> <li>Computer Profiles</li> <li>Administrative shares</li> <li>Computer Profiles</li> <li>Administrative shares</li> <li>Custom share:</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Add</li> <li>Custom share:</li> <li>C</li></ul>			Copy software to deploy to target computer(s) via:
Scheduled Scans Computer Profiles Computer Profiles Database Maintenanc Parameter Files Database Maintenanc Program Updates Wersion Information Ucensing How to purchase Support Center Support Center Support Center Computer (s) Computer	Econingeration	Computer(a) to deploy asthuran and	<ul> <li>Administrative shares</li> </ul>
Name       Notes       Add         Alerting Options       Alerting Options         Database Maintenanc       Decomposition         Database Maintenanc       Select         Program Updates       Import         Wersion Information       Import         How to purchase       Support Center         Knowledge Base       GFI LANguard N.S.S.         GFI LANguard S.E.L.M       C Deploy immediately         Reset       Start         Deploy on 21/10/2005       at 13:33:35	Scheduled Scans	Computer(s) to deploy software on:	C Custom share:
Alerting Options Parameter Files Database Maintenanc Database Maintenanc Database Maintenanc Program Updates Wersion Information How to purchase Support Center Knowledge Base GFI LANguard S.E.L.M GFI LANguard S.E.L.M Deploy immediately Reset Start Deploy immediately Reset Star	Computer Profiles	Name Notes Add	,
Parameter Files       After deployment:         Operation       After deployment:         Operation       Select         Operation       Import         Operation       Import         Operation       Import         Operation       Select         Operation       Import         Operation       Select         Operatin       Select	Alerting Options	STMJASON WARNING : Filters will no	
Database Maintenanc     General     General     General     General     General     General     Import     Import     Import     General	- Sarameter Files	THEMOVE	After deployment:
General     Program Updates     Program	👋 Database Maintenanc	Select	Do not reboot/shut down the computer(s)
Program Updates     Wersion Information     Wersion     Wersion Informatio     Wersion Informatio	🗄 🍅 General		C Reboot the target computer(s)
Wersion Information     Licensing     How to purchase     Support Center     Knowledge Base     GFI LANguard S.E.L.+     GFI LANguard S.E.L.+     GFI LANguard S.E.L.+     C Deploy immediately Reset Start     Computer(s)     Deploy immediately Reset Start	- 🏠 Program Updates	Import	Let the user decide when to reboot
Licensing     How to purchase     Support Center     Knowledge Base     GFI LANguard N.S.S.     GFI LANguard S.E.L.#     GFI LANguard S.E.L.#     C Deploy immediately     Reset     Start     C Deploy immediately     Reset     Start     C Deploy immediately     Reset     Start	- 😥 Version Information		
How to purchase     Support Center     Knowledge Base     GFI LANguard N.S.S.     GFI LANguard S.E.L.#     GFI LANguard S.E.L.#     C Deploy immediately     Reset     Start     C Deploy on 21/10/2005     at 13.33.35	Licensing		C Shut down the target computer(s)
Support Center     Knowledge Base     GFI LANguard S.E.L.*     GFI LANguard S.E.L.*     GFI LANguard S.E.L.*     C Deploy immediately Reset     Start     C Deploy on 21/10/2005     At 13.33.35	- 🥭 How to purchase		Delete copied files from remote
Knowledge Base     GFI LANguard N.S.S.     GFI LANguard S.E.L.     C Deploy immediately Reset Start     GFI Network Server M     Deploy on 21/10/2005 ▼ at 13:33:35 →	Support Center		computer(s) after deployment
GFI LANguard N.S.S.     GFI LANguard S.E.I.Ir     GFI LANguard S.E.I.Ir     GFI Network Server IV     Deploy on 21/10/2005    at 13:33:35	Knowledge Base		
GFI Lewydard S.E.L.F GFI Network Server Y C Deploy on 21/10/2005 V at 13:33:35	GFI LANguard N.S.S.	Deploy immediately     Reset     Start	Comercian Cilbars
C Deploy on 21/10/2005 Y at 13:33:35	GFI LANguard S.E.L.M		
		C Deploy on 21/10/2005 🔽 at 13:33:35 🚎	×

Screenshot 111 - Software deployment details

Once you have specified which software will be deployed and on which target computer(s), begin the software deployment by clicking on the **Start** button.

### Scheduling patch deployment

To schedule custom software deployment:

- 1. Select the 'Deploy on' option.
- 2. Specify the preferred date and time in the provided fields.

3. Click on the **Start** button to activate the scheduled deployment process.

### **Deployment options**

### **General deployment options**

of GFI LANguard N.S.S. 7.0		
🚺 New Scan Using: Current	y Logged-On User 💌 User Name:	Password:
Tools Explorer 4	Configure which computers and which software files	are to be deployed
🗄 👧 Security Scanner (Default	Software to deploy Deployment Status	Options III
🖻 🥸 Tools	Software	General Advanced
	Software Location Parameters Add	
Copioy Custom Softw-	C\cmdasuset exe	Before deployment:
Traceroute	<u>E</u> dit.	🔽 Warn user before deployment (send a message)
Whois		Wait for user's approval
Enumerate Computer:	<u>H</u> emo	Dive
😪 Enumerate Users		1 Stop services before deployment
Snmp Audit		Services,
Snmp Walk		
🛠 SQL Server Audit		Copy software to deploy to target computer(s) via:
Configuration		<ul> <li>Administrative shares</li> </ul>
Scanning Profiles	Computer(s) to deploy software on:	C. Custom share:
Computer Profiles	Name Notes Add.	
Alerting Options	3 TMJASON WARNING : Filters will no	
Parameter Files	Hemo	After deployment:
🔏 Database Maintenanc	Selec	t   • Do not reboot/shut down the computer(s)
🖻 🍅 General		C Reboot the target computer(s)
	Impor	t
Version Information		
		Shut down the target computer(s)
How to purchase		Delete cogied files from remote
Knowledge Base		computer(s) after deployment
GFI LANguard N.S.S.		Computer filters
GFI LANguard S.E.L.M	Deploy immediately Reset <u>Star</u>	tt
GFI Network Server M	O Deploy on 21/10/2005 at 13:33:35	

Screenshot 112 - General deployment options

The general deployment options allow you to configure before and after patch deployment actions.

### Before deployment options

Configure the 'Before deployment' options in the **General** tab as follows:

 'Warn users before deployment' – Select this option if you want to send a message to the target computer before deploying an update.

GFI LANg	uard Patch Agent 🛛 🔀
1	Warning !!! Microsoft Hotfixes are going to be installed by LANguard Network Security Scanner ! This installation was initiated by JASON\jason. The system may reboot after installation ! Save your work and click on OK to continue.
	OK

Screenshot 113 - Deployment Warning: Informs users that a deployment process is about to start

In this way, target computer users will be allowed to save and close running programs before patches are deployed on their computer(s).

 'Wait for user's approval' – Select this option to request the approval of a target computer user before starting the deployment of a file. This allows the target computer user to put on hold the deployment process in case some other important process (for example, a system backup) is already under way. In this way other processes can be left to finish prior to the deployment, just in case the target computer requires a reboot after the installation of the file. To start the patch deployment, the target computer user must click on the **OK** button included in the message dialog.

• 'Stop services before deployment' – Select this option to stop specific services before starting the deployment. Specify the services that you wish to stop by clicking on the **Services...** button.

### After deployment options

Configure the 'After deployment' options in the General tab as follows:

- 'Do not reboot' Select this option if you do NOT want to (remotely) reboot the target computer after the deployment process.
- *'Reboot the target computers'* Select this option to automatically reboot target computers after that the software or patches have been installed.
- 'Let the user decide when to reboot' Select this option to let target computer users interactively decide when to reboot the computers where software/patches have been deployed.

When this option is enabled, the dialog shown below is automatically displayed on the target computers' desktop.

GFI LANguard N.S.S.		
Microsoft Hotfixes were installed by LANguard Network Security Scanner! Windows needs to be restarted to complete the installation.		
C Restart now		
C Remind me in 1 in minutes		
Restart on		
🔿 Don't bother me again		
ок		

Screenshot 114 - Post deployment options dialog: Allows users to decide when to reboot the target computer

From this dialog users can select one of the following reboot options:

- o 'Restart Now' Select this option for immediate restart.
- *'Remind me in [X] Minutes'* Select this option to generate a reboot reminder at specific time intervals (in minutes).
- *'Restart on [date] at [time]'* Select this option to automatically reboot the target computer on a specific day and/or at a specific time.
- 'Don't bother me again' Select this option to abort remote rebooting.

- 'Shutdown the target computer(s)' Select this option to shutdown target computers after software/patch deployment.
- 'Delete copied files on the remote computers after deployment' Select this option to delete the source/installation file from the target computer after that it successfully installed.
- Computer filters Click on the **Computer filters** button to configure particular target filtering conditions. These settings will allow the deployment of patches only if specific operating systems are installed and running on the target computer(s).

### Advanced deployment options

🚰 GFI LANguard N.S.S. 7.0		
<u>File T</u> ools <u>C</u> onfigure <u>H</u> elp		
New Scan Using: Current	ly Logged-On User 👻 User Name:	Password:
New Scan       Using: Current         Tools Explorer       U         G FT LANguard Network Securi       Security Scanner (Default         Security Scanner (Default       Tools         Beploy Custom Softw       Poploy Microsoft Updi         Whois       Fit Taceroute         Security Scanner (Default       Security Scanner (Default)         Whois       Security Scanner (Default)         Security Taceroute       Security Scanner (Default)         Security Scanner (Default)       Security Scanner (Default)         Security Scanner (Default)       Security Scanner (Default)         Scanning Profiles       Scanning Profiles         Scanning Profiles       Detabase Maintenanc         Debabase Maintenanc       Debabase Maintenanc         Support Center       Knowledge Base         Siger LANguard N.S.S.       Sept LANguard S.S.L.M.         Sept LANguard S.S.L.M.       Server M	y Logged-On User Liser Name: Configure which computers and which software files are to b Software to deploy Deployment Status Software: Software Location Parameters Add Edit Remove Computer(s) to deploy software on: Name Notes Computer(s) to deploy software on: Name Notes TMJASON WARNING : Filters will ne Remove Select Import Copeloy immediately Reset Start Copeloy on 21/10/2005 at 13:33.35	Password:       Image: Content of the playment of the playment threads:       Image: Content of the playment threads:       Image: Content of the playment of the playment operation is complete.         Very Deployment threads:       Image: Content of the playment operation is complete.       Image: Content of the playment operation is complete.         Deployment threads:       Image: Content of the playment operation is complete.       Image: Content of the playment operation is complete.         Deployment threads:       Image: Content of the playment operation is complete.         Image: Content of the playment operation is complete.       Image: Content operation of the playment operation is complete.         Image: Content operation of the playment operation of the playment operation of the playment operation is complete.       Image: Content operation oper

Screenshot 115 - Advanced deployment options

Use the **Advanced** tab to access the advanced deployment options from where you can configure the following deployment parameters:

- Configure the number of patch deployment threads that will be used.
- Configure the deployment timeout.
- Configure the deployment agent service to run under alternative credentials.

# **Results comparison**

### Introduction

Through regular audits and scan results comparison you can analyze the changes that occur between successive network security audits. This helps you to immediately identify new vulnerabilities in a timely manner as well as assist you in the investigation and mitigation of unfixed/pending security issues that keep popping up repeatedly in every network security scan.

GFI LANguard N.S.S. ships with a results comparison tool. Use this tool to automatically generate reports which show the difference between two consecutive/non-consecutive scans. Comparison reports can be triggered interactively or automatically.

Generate comparison reports interactively from the **Security Scanner Result comparison** node. Comparison reports can be interactively generated by selecting the scan results (consecutive and non-consecutive scans) to be compared.

Configure the options in the **Configuration** > **Scheduled Scans** node > **Results notifications** tab to automatically generate comparison after every scheduled scan. Reports generated after scheduled scan allow you to compare the last scan results with the results of the previous (scheduled) scan. For more information refer to the 'Scheduled Scans' section in the 'Configuring GFI LANguard N.S.S.' chapter.

Use the information harvested through result comparisons to proactively secure your network from dangerous user activity and protect computers from emerging threats by fixing all possible vulnerabilities before these are exploited.

## Comparing scan results interactively

GFI LANguard N.S.S. allows you to store scan results in database or XML files. By default, GFI LANguard N.S.S. stores all the scan results into the Microsoft Access/Microsoft SQL Server database backend. When scheduled scans are performed GFI LANguard N.S.S. will also store the results of the respective scan into an XML file for reporting purposes.

GFI LANguard N.S.S. ships with a results comparison tool which allows you to compare saved scan results and generate a list of network changes discovered.

### Configuring what information will be reported

The result comparison tool can report various information discovered during the comparison of 2 saved scan results. Configure the information that will be included in the report as follows:



1. Click on Security Scanner > Result comparison node.

Screenshot 116 - Results comparison configuration options

2. From the right pane, click on the **Options** button.

3. Select the check box of the information item that you want to include in the report. Available items include:

- **New items:** Select this option to include all security issues that were enumerated in the latest scan results and which were not recorded in the previous/older scan results.
- **Removed items:** Select this option to include all result items (for example, installed applications) and components/devices (for example, Network cards, USB devices, Wireless devices, etc.).) that were recorded in the previous/older scan but which have not been recorded in the latest scan.
- **Changed items:** Select this option to include all result items that have changed, such as a service which were enabled or disabled in between scans.
- Show vulnerability changes: Select this option to include all new and fixed vulnerabilities identified between the compared scan results.
- Show only hot-fix changes: Select this option to include all missing and installed patches identified between the compared scan results.

<u>Eile T</u> ools <u>C</u> onfigure <u>H</u> elp		
🜔 New Scan 🔝 🐥 Using:	Currently Logged-On User 💌 User Name:	Password:
Tools Explorer         Image: Construction of the security of the securety of the security of the securety of the securety of	Scan result 1:         Iocalhost - Default - 21/10/2005 09:51:56           Scan result 2:         Iocalhost - Default - 06/09/2005 11:37:20	Or         Compare         Orations           >-         -         -         -
General		Options     General     General     Display the following items:     Vew items.     Changed items.     Changed items.     Options:     Show vulnerability changes.     Show only hotfix changes.
L		×

### **Generating a Results Comparison Report**

Screenshot 117 - Comparing scan results

To generate a scan results comparison report:

1. Click on the Security Scanner > Result comparison node.

2. Click on the search file buttons to select the scan result files that you wish to compare. You can compare results stored in XML files or database files but you cannot directly compare XML file results to database file results.

3. Click on **Compare** to start the results comparison process.

# The Results Comparison Report



Screenshot 118 - Results Comparison Report

The Results Comparison Report shows the target configuration and network layout changes that have been identified between the two scan results.

# **GFI LANguard N.S.S. Status Monitor**

### Viewing scheduled operations

Use the GFI LANguard N.S.S. Status Monitor to view the state of active scheduled scans and scheduled update deployments.

GFI LANguard N.S	.S. Monitor
« 🛃 🕒 👰	18:00

Screenshot 119 - GFI LANguard N.S.S. Status Monitor icon shown in the Windows system tray

The Status Monitor is automatically opened in the Windows system tray whenever the GFI LANguard N.S.S. configuration interface is started. To bring up the Status Monitor click on the 🖾 icon located in your Windows system tray.

NOTE: Bring up the Status Monitor without opening the GFI LANguard N.S.S. configuration interface from Start ▶ Program files ▶ GFI LANguard Network Security Scanner 7.0 ▶ LNSS Status Monitor.

GFI Languard NSS Status Monitor			
Active scheduled scans   Scheduled de		Charl Vines 5	Chahan
172.16.130.122	Default	11/18/2004 3:53:53 PM	completed
1		1	
		<u>Remove finished scans</u>	top selected scans
			OK

### Viewing the progress of scheduled scans

Screenshot 120 - Status Monitor: Active scheduled scans tab.

To view scheduled scans in progress:

1. Bring up the GFI LANguard N.S.S. Status Monitor.

2. Click on the Scheduled Scans tab.

**NOTE 1:** Cancel any scheduled scan that is in progress by clicking on the **Stop Selected Scan(s)** button.

**NOTE 2:** From the **Scheduled Scans** tab you can only view and cancel scheduled scans that are in progress.

**NOTE 3:** View or cancel scheduled scans that have not yet started from the GFI LANguard N.S.S. configuration interface (**Configuration >** Scheduled Scans).

🚰 GFI Languard NSS Status Monitor	
Active scheduled scans Scheduled deployments	
□       Custom Deployment 1 (Scheduled)         □       □	
	Cancel selected deployment
	OK

Viewing the progress of scheduled deployments

Screenshot 121 - Status Monitor: Scheduled deployments

To view scheduled deployments in progress:

1. Bring up the GFI LANguard N.S.S. Status Monitor.

2. Click on the Scheduled deployments tab.

**NOTE:** Cancel any scheduled deployment that is in progress by clicking on the **Cancel Selected deployments** button.

# Tools

### Introduction

GFI LANguard N.S.S. ships with a default set of network tools which help you troubleshoot common network problems and assist you in the administration of your network.

Use the **S** Tools node in the GFI LANguard N.S.S. configuration interface to access the following list of default network tools:

- Skinger Stresser
   Skin
- % Whois Client
- Strace Route
- SNMP Walk
- SNMP Audit
- SQL Server Audit
- Strate Computers
- Strate Users.

### **DNS** lookup

Use the **Tools > DNS Lookup** tool to resolve domain names into the corresponding IP address and to retrieve particular information from the target domain (for example, MX record, etc.).



Screenshot 122 - The DNS Lookup tool

To resolve a domain/host name:

#### 1.Click on the **Tools > DNS lookup** node.

- 2. Specify the hostname to resolve.
- 3. Specify the information that you wish to retrieve:
- *'Basic Information'* Select this option to retrieve the host name and the relative IP address.
- 'Host Information' Select this option to retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.

**NOTE:** Most DNS entries do not contain this information for security reasons.

- 'Aliases' Select this option to retrieve information on the 'A Records' configured on the target domain.
- 'MX Records' Select this option to enumerate all the mail servers and the order (i.e. priority) in which they receive and process emails for the target domain.
- *'NS Records'* Select this option to specify the "name-servers" that are authoritive for a particular domain or sub domain

4. Specify (if required) the alternative DNS server that will be queried by the DNS Lookup tool or leave as default to use the default DNS server.

5. Click on the **Retrieve** button to start the process.

### **Trace Route**



Screenshot 123 - Trace route tool

Use the **Tools** > **Traceroute** tool to identify the path that GFI LANguard N.S.S. followed to reach a target computer. To use this tool:

- 1. In the 'Trace' dropdown, specify the name/IP or domain to reach.
- 2. 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:

- V Indicates a successful hop taken within normal parameters.
- A Indicates a successful hop, but time required was quite long.
- A Indicates a successful hop, but the time required was too long.
- X Indicates that the hop was timed out (> 1000ms).

### Whois Client

📴 GFI LANguard N.S.S. 7.0			_ 🗆 ×
Eile <u>T</u> ools <u>⊂</u> onfigure <u>H</u> elp			
🜔 New Scan Using: Current	tly Logged-On User 👻 User Name:	Password:	
Tools Explorer 1 GFI LANguard Network Security	Query (domain/IP/name): www.gfi.com	<u>R</u> etrieve	<u>Options</u>
Security Scanner (Default)     Scan Filters     Result comparison     Tools	Starting WhoIS operation for:www.gfi.com	Options General	
September 2015 Peerloy Microsoft Updat	Maria Caman Vanime 1.2	Whois server to query:     C Choose one for <u>me</u> Lise the following server	
Physic Coston Dottware     Physic Coston Dottware     Physic Coston Dottware     Whois     Physic Computers     Song Audit     Song Audit     Song Audit     Song Valk     Song Val	Whole Server Version 1.3 Domain names in the .com and .net domains can now be registe with many different competing registrars. Go to http://www.intern for detailed information. Domain Name: GFI.COM Registrar: CORE INTERNET COUNCIL OF REGISTRARS Whois Server: whois corenic.net Referral URL: http://www.corenic.net Name Server: SERVER1.GFI.COM Name Server: SERVER1.GFI.COM Status: ACTIVE Updated Date: 03-aug-2004 Creation Date: 03-aug-1995 Expiration Date: 02-aug-2006	whois1.ausregistry.net.au whois.ripe.net whois.arin.net whois.arin.net whois.nic.gov whois1.ausregistry.net.au	Add Remove
General	>>> Last update of whois database: Wed, 17 Nov 2004 19:00:0 NOTICE: The expiration date displayed in this record is the date registrar's sponsorship of the domain name registration in the regi currently set to expire. This date does not necessarily reflect the date of the domain name registrant's agreement with the sponsor registrar. Users may consult the sponsoring registrar's Whois dat view the registrar's reported date of expiration for this registration. TERMS OF USE: You are not authorized to access or query our database through the use of electronic processes that are high-v automated event as reasonable necessary to register.		
		J	

Screenshot 124 - Whois tool

Use the **Tools** > Whois Client tool to look up information on a particular domain or IP address.

Select the Whois Server that will look for your information from the options area on the right of the configuration interface, or leave as default to let the tool automatically select a domain server for you.

To look for information on a particular domain or IP address, specify the domain/IP or hostname in the 'Query' drop down and click on the **Retrieve** button.

### **SNMP** Walk

GFI LANguard N.S.S. 7.0		
<u> </u>		
🚺 🕥 New Scan 🛛 Using: Curre	ently Logged-On User 👻 User Name:	Password:
Tools Explorer	IP address: 127.0.0.1 💌 Object ID: 1.3.6.1.2	2.1.1 <u>B</u> etrieve <u>Options</u>
Security Scanner (Defaul	Description: iso.org.dod.internet.mgmt.mib-2.system	Options I
Result comparison Tools Deploy Microsoft Upc -% Deploy Custom Softv -% DiNS Lookup -% Traceroute -% Whois -% Enumerate Computer -% Snmp Audit -% Snmp Audit -% Song Walk -% Sol Server Audit -% General	iso iso idod internet	General         Community string to query:         C       Use default community string(public)         Image: Community string       Add         Image: Private router disco       Remove         Image: Private router disco       Remove

Screenshot 125 - SNMP Walk

Use the **Tools** SNMP Walk tool to probe your network nodes and retrieve SNMP information (for example, OID's). To start an SNMP scan on a target:

### 1. Click on the **Tools > SNMP Walk** node.

2. Specify the IP address of the computer that you wish to scan for SNMP information.

3. Click on the **Retrieve** button to start the process.

**NOTE 1:** SNMP activity is often blocked at the router/firewall so that Internet users cannot SNMP scan your network.

**NOTE 2:** It is possible to provide alternative community strings.

**NOTE 3:** The information enumerated through SNMP can be used by malicious users to attack your system. Unless this service is required it is highly recommended that SNMP is turned off.

### **SNMP** Auditing tool

OF LET LANGUARD N.S.S. 7.0				= <u></u> U
<u>File Lools Lonfigure Help</u>				
New Scan Using: Curre	ently Logged-On User 👻 📃s	er Name:		Password:
Tools Explorer 🌐 📮	IP of computer running SNN	IP 127.0.0.1		Betrieve
GFI LANguard Network Secu	n or compare ranning cr			
😑 👰 Security Scanner (Defaul	Ip Address	Computer Name	public priv	Options 🎵
E Scan Filters	🖳 127.0.0.1	localhost		General
Tools				]
🖉 🖉 Deploy Microsoft Upd				Query SNMP Service for the weak/common community strings specified in the following
😽 Deploy Custom Softv				dictionary file:
😽 DNS Lookup				C/\Program Eiler\GEI\LANguard Network Ser
* Traceroute				
Section Sectio				Refresh information
😽 Enumerate Users				
Snmp Audit				Je Resolve computer names.
Snmp Walk				
THE Configuration				
⊕ General				
-				
			F	
w×Ú	1	00		Overall progress: 100%

Screenshot 126 - SNMP Audit tool

Use the **Tools > SNMP Audit** tool to perform SNMP audits on network targets and identify weak community strings.

This tool identifies and reports 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 that you want to from the tool options at the right of the configuration interface.

To perform an SNMP Audit:

- 1. Click on the **Tools** > **SNMP Audit** node.
- 2. Specify the IP address of the computer that you wish to audit.
- 3. Click on the **Retrieve** button to start the process.

### **Microsoft SQL Server Audit tool**

Use the **Tools** → **Microsoft SQL Server Audit** tool to perform a security audit on a particular Microsoft SQL server installation. This tool allows 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. During the audit process, this tool will perform dictionary attacks on the SQL server accounts using the credentials specified in the *'passwords.txt'* dictionary file. However, you can also direct the 'SQL Server Audit' tool to use other dictionary files. You can also customize your dictionary file by adding new passwords to the default list.

To perform an SQL Server Audit:

1. Click on the **Tools** > **SQL Server Audit** node.

2. Specify the IP address of the SQL server that you wish to audit.

**NOTE:** By default, this tool will check the vulnerability of the administrator/sa account. If you want to perform dictionary attacks on all the other SQL user accounts, select the *'Audit all SQL user accounts'* option and specify the SQL Server logon credentials. These credentials are required to authenticate to the SQL server when retrieving the respective list of user accounts.

3. Click on the **Retrieve** button to start the process.

### Enumerate computers tool

GFI LANguard N.S.S. 7.0           Elle         Tools         Configure         Help           Image: Scan         Using:         Current	tly Logged-On User	• User Name:		ļ	Password:	- 🗆 ×
Tools Explorer   GFI LANguard Network Security	Enumerate compute	rs in domain: 🙀 GFIM,	ALTA	-	Retrieve Optio	ns
Security Scanner (Default)	Name	Operating System	🛆 Туре		Options	џ
🕀 😼 Scan Filters	🔜 PABXBOX	Windows server 2003	Server		Ceneral Information Source	
Result comparison	🔜 ISA2K4	Windows server 2003	Server		deneral Information Source	
	🔜 ISASERVER	Windows server 2003	Server		C Enumerate all computers.	
Deploy Microsoft Updat     Microsoft Updat	🚚 SMSSERVER	Windows server 2003	Server		<ul> <li>Only these:</li> </ul>	
Depioy Custom Sortwar     Secondary	S EMMANUELC	Windows server 2003	Server			
* Traceroute	🔜 EMMANUELG	Windows server 2003	Server		<ul> <li>Operating System</li> </ul>	_
Whois	🔜 FAXSRV	Windows server 2003	Server		Windows 95 / 98 / ME	
Fnumerate Computers	🔜 FILESERVER	Windows server 2003	Server		Windows NT	
Se Enumerate Users	🔜 MAILARCH	Windows server 2003	Server		Windows 2000	
Snmp Audit	🔜 TERMINAL	Windows server 2003	Server		Windows 2003	<ul><li>✓</li></ul>
Snmp Walk	NICKATESTSRV	Windows server 2003	Server		Windows XP	✓
😽 SQL Server Audit	🔜 MAILGATE	Windows server 2003	Server		Novell	
🖻 🤔 Configuration	🔜 VISGFIT	Windows server 2003	Server		Linux	
🕀 🍒 Scanning Profiles	🔜 WILLIAM	Windows server 2003	Server		<ul> <li>Services</li> </ul>	
Scheduled Scans	📲 DENNISM	Windows XP	Workstation		Microsoft SOL Servers	
Computer Profiles	🔜 EDWARD	Windows XP	Workstation		Primary Domain Controllers	Ē.
Alerting Options	🔜 EMMANUELG	Windows XP	Workstation		Backup Domain Controllers (BDC)	
Parameter Files	🔜 IVAN	Windows XP	Workstation		Apple file protocol servers	H
Database Maintenance	🔜 JASON	Windows XP	Workstation		Servers charing print queue	
H- 1 General	🚚 JENS	Windows XP	Workstation		Servers sharing print queue	
	🚚 JENSTEST	Windows XP	Workstation	•	Servers sharing dai in service	
	•				L Types	_
	Charles and a size of the	(******)		_	Workstations	
Getting the computers of GFIMALTA Ready. Found 68 computers.					Servers	
					Windows for workgroups	
I						
Found 68 computers		Domain: GFIMALTA				

Screenshot 127 - Enumerate Computers tool

Use the **Tools Enumerate Computers** tool to identify 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 OS installed on the discovered computers, and any additional details that might be collected through NetBIOS.

Computers can be enumerated using one of the following methods:

- From the Active Directory This method is much faster and will also include computers that are currently switched off.
- Using the Windows Explorer interface This method enumerates computers through a real-time network scan and therefore it is slower and will not include computers that are switched off.

Use the **Information Source** tab provided in the 'Enumerate Computers' tool to configure your preferred method of computer discovery.

**NOTE:** For an Active Directory scan, you will need to run the tool (i.e. GFI LANguard N.S.S.) under an account which has access rights to the Active Directory.

### Starting a security scan

The 'Enumerate Computers' tool scans your entire network and identifies domains and workgroups as well as their respective computers. After enumerating the computers in a domain or workgroup, you can use this tool to launch a security scan on the listed computers. 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 allows 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 which will guide you through the configuration process. For more information on how to remotely configure auditing policies on particular targets refer to the 'Security Audit Policy settings' section in the 'Getting started: Performing an audit' chapter.

### Enumerate users tool

<b>©¦ GFI LANguard N.S.S. 7.0</b> Eile <u>T</u> ools <u>C</u> onfigure <u>H</u> elp				
💽 New Scan 🛛 Using: Security Certificat	es 🔹 User I	Name:	Certificate File:	2 🛃
Tools Explorer   GFI LANguard Network Security Scan	<u>E</u> numerate users in	domain: 🛃 GFIMALTA	✓ <u>R</u> etrieve	<u>O</u> ptions
🔄 👧 Security Scanner (Default)	User Name	FullName	Options	ą.
E-Scan Filters	🚨 Administrator	Administrator	General	
Full Report	🚨 newarch	newarch		
Vulnerabilities [High secur	🗞 Guest		Enumerate all users	
Wulnerabilities [All]	🚨 smsadmin	SMS Administrator	C Enumerate the following:	
Missing Patches and Serv	🗞 krbtgt		Users	
Mining Interview - USB	Iuser_fileserver	luser_fileserver	Contacts	
📝 Important Devices - Wire	Ω robert	Robert Abela		
📝 Open Ports	🚨 nickg	Nick Galea	Highlight:	
- 💕 Open Shares	🚨 nvcadmin	Norman Virus Control Admin	Disabled accounts	
- 📝 Auditing Policies 🛛 👘	🚨 nicka	Nicholas Aquilina	Locked accounts	
Password Policies	🚨 selm	S.E.L.M	····	
Groups and Users	🚨 sandro	Sandro Gauci		
Computer Properties	A IWAM_MAIL	Internet Guest Account		
Result comparison	IUSR_MAILS	Internet Guest Account		
E- 100 Tools	IUSR_BACKUP	Internet Guest Account		
* Deploy Microsoft Updates	A IWAM_BACK	Launch IIS Process Account		
Se DNS Lookup	IUSR_SQLSE	Internet Guest Account		
Se Traceroute	🚨 sus	SUS updater		
Whois	<u>n</u>	aacable		
Sector Computers	<u>u</u>	Alin Irimias		
🔆 🛠 Enumerate Users	<u>a</u>	Anne Katrin Schulz		
	<u>8</u>	Bogdan Coroian	-	
atte Como Walle	<u>ا ا</u>			
		····· • ······		

Screenshot 128 - The Enumerate Users tool dialog

Use the **Tools Enumerate Users** tool to scan the Active Directory and retrieve the list of all users and contacts included in this database.

To enumerate users and contacts contained in the Active Directory of a domain, select the domain name from the provided list of domains on your network and click on the **Retrieve** button. You can filter the information to be extracted and display only the users or contacts details. In addition, you can optionally configure this tool to highlight disabled or locked accounts. This is achieved through the configuration options included at the right side of the enumerate users tool.

From this tool you can also enable or disable any user account that has been enumerated. This is achieved by right-clicking on the account and selecting **Enable/Disable account** accordingly.

# Using GFI LANguard N.S.S. from the command line

By default, GFI LANguard N.S.S. ships with two command line tools; *'Insscmd.exe'* and *'deploycmd.exe'*. These command line tools allow you to launch network vulnerability scans and patch deployment sessions without bringing up the GFI LANguard N.S.S. configuration interface.

The parameters of these command line tools are configured through a set of command line switches. A complete list of supported switches together with a description of the respective function is provided below.

### Using 'Insscmd.exe' - the command line scanning tool

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:

Insscmd [Target] [/profile=profileName] [/report=reportPath] [/output=pathToXmlFile] [/user=usrname /password=password] [/UseComputerProfiles] [/email=emailAddress] [/DontShowStatus] [/?]

### Switches:

- 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 N.S.S. will be used.

**NOTE**: In the configuration interface, 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 **Configuration ▶ Scanning Profiles** node.

- **/Output** (Optional) Specify the full path (including filename) of the XML file where the scan results will be saved.
- /Report (Optional) Specify the full path (including filename) of the HTML file where the scan results HTML report will be output/saved.
- /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 Computer Profiles (Configuration ▶ Computer Profiles node).

- /Email (Optional) Specify the email address on which the resulting report(s) will be sent at the end of this scan. Reports will be emailed to destination through the mail server currently configured in the Configuration → Alerting Options node (of the configuration interface).
- **/DontShowStatus** (Optional) Include this switch if you want to perform silent scanning. In this way, the scan progress details will not be shown.
- **/?** (Optional) Use this switch to show the command line tool's usage instructions.

**NOTE:** Always enclose full paths, and profile names within double quotes (i.e. '[path or profile name]') for example, "Default", "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. Supported variables include:

- **%INSTALLDIR%** During scanning, this variable will be replaced with the path to the GFI LANguard N.S.S. 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: How to launch target computer scanning from the command line tool.

For this example, we will be assuming that a scan with the following parameters is required:

1. 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 an HTML report and save it in 'c:\result.html'.

4. Send the HTML report via email to 'Inss@127.0.0.1'

The command line tool instruction for this particular security scan is:

Insscmd.exe 130.16.130.1 /Profile="Default" /Output="c:\out.xml" /Report="c:\result.html" /email="Inss@127.0.0.1"

### Using 'deploycmd.exe' - the command line patch deployment tool

The 'deploycmd.exe' command line patch deployment tool allows you to deploy Microsoft 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] [/username=UserName /password=Password] [/UseComputerProfiles] [/warnuser] [/useraproval] [/stopservices] [/customshare=CustomShareName] [/reboot] [/rebootuserdecides] [/shutdown] [/deletefiles] [/timeout=Timeout(sec)] [/?]

#### Switches:

- **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 Computer Profiles (Configuration ► Computer Profiles node).
- /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 which 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 installation 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 configuration interface. For more information on how to specify services to be stopped, refer to the 'Deployment options' section in the 'Patch Management: Deploying custom software' chapter.

- **/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).
- **/shutdown** (Optional Parameter) Include this switch if you want to shutdown 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 successfully 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.

• *I*? - (Optional) Use this switch to show the command line tool's usage instructions.

## Example: How to launch a patch deployment process from the command line tool.

For this example, we will be assuming that a patch deployment session with the following parameters is required:

- 1. Deploy a file called 'patchA001002.XXX'
- 2. On target computer 'TMjason'.

3. Reboot the target computer after successful deployment of the file.

The command line tool instruction for this particular patch deployment session is:

deploycmd TMjason /file="patchA001002.XXX" /reboot

# Adding vulnerability checks via custom conditions or scripts

#### Introduction

GFI LANguard N.S.S. allows you to enhance the already provided network scanning capabilities by adding new custom vulnerability checks.

Custom vulnerability checks can be created using scripts or by configuring a set of custom vulnerabilities. Scripts can be created using any VB script compatible scripting language. By default, GFI LANguard N.S.S. ships with a script editor which you can use to create your custom scripts.

New checks must be included in the list of checks supported by GFI LANguard N.S.S. Use the **Vulnerabilities** tab to add new checks to the default list of vulnerability checks on a scan profile by scan profile basis.

**NOTE:** Only expert users should create new vulnerability checks. Scripting errors and wrong configurations in a vulnerability check can result in false positives or provide no vulnerability information at all.

#### **GFI LANguard N.S.S. VBscript language**

GFI LANguard N.S.S. supports and runs scripts written in VBscript compatible languages. Use VBscript compatible languages to create custom scripts which can be run against your network targets.

Security auditing scripts can be developed using the script editor which ships with GFI LANguard Network Security Scanner. This builtin script editor includes syntax highlighting capabilities as well as debugging features which support you during script development. Open the script editor from Start > Programs > GFI LANguard Network Security Scanner 7.0 > LNSS Script Debugger.

NOTE: For more information on how to develop scripts using the builtin script editor, refer to the 'Scripting documentation' help file included in Start ▶ Programs ▶ GFI LANguard Network Security Scanner 7.0 ▶ LNSS Scripting documentation.

**IMPORTANT NOTE:** GFI does not support requests related to problems in custom scripts. You can post any queries that you may have about GFI LANguard N.S.S. scripting on the GFI LANguard forums at <u>http://forums.gfi.com/</u>. Through this forum you will be able to share scripts, problems and ideas with other GFI LANguard N.S.S. users.

.....

#### GFI LANguard N.S.S. SSH Module

GFI LANguard N.S.S. 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 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.

#### 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 Network Security Scanner. Standard keywords identified by the SSH module include:

- TRUE:
- FALSE:
- AddListItem
- SetDescription
- !!SCRIPT\_FINISHED!!

Each of these keywords triggers an associated and specific process in the SSH Module. The function of each keyword is described below:

- **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 which adds results to the vulnerability check report (i.e. scan results). These results are shown in the GFI LANguard N.S.S. configuration interface 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 string]]]]* Includes the value that will be added to the scan results node.

**NOTE:** 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.

**IMPORTANT NOTE:** 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 VB (.vbs) script

Use the script editor which ships with GFI LANguard N.S.S. to create custom scripts that can be run against your network targets to identify specific vulnerabilities. To create new vulnerability checks that use custom vbscripts you must do as follows:

- Step 1 : Create the script
- Step 2: Add the new vulnerability check:

The following are examples of how this is done.

#### Step 1 : Create the script

1. Launch the Script Debugger from Start ▶ Programs ▶ GFI LANguard Network Security Scanner 7.0 ▶ LNSS Script Debugger.

#### 2. Go on **File ▶ New...**

3. Create a script. For this example use the following dummy script code.

Function Main

echo "Script has run successfully"

Main = true

End Function

4. Save the script in 'C:\Program Files\GFI\LANguard Network Security Scanner 7.0\Data\Scripts\myscript.vbs'.

#### Step 2: Add the new vulnerability check:

1. Open the GFI LANguard N.S.S. configuration interface.

2. Expand the **Configuration → Scanning Profiles** node and select the scanning profile where the new vulnerability check will be added.

3. Click on the Vulnerabilities tab.

4. From the middle pane, select the category in which the new vulnerability check will be included (for example, DNS Vulnerabilities).

Add Vulnerability		×	
General Description			
		T	
⊻ulnerability Name:	TMJasonTest		
Short Description:	test check		
Security <u>L</u> evel:	Medium Security		
BugtragID/LIBL:			
This vulnerability check v all met:	This vulnerability check will be triggered when the following conditions are		
Check type	Details		
VB Script	returns TRUE (1) "tomcat.vbs"		
	1		
Add Rem	Edit		
	OK Cancel Apply		

Screenshot 129 - The new vulnerability check dialog

5. Click on the **Add** button. This will bring up the new vulnerability check dialog.

6. Specify the basic details such as the vulnerability name, short description, security level,

and BugtraqID/URL (if applicable). Optionally, you can also specify how long the check takes to execute.

7. Click on the **Add...** button. This will bring up the check triggering conditions dialog.

A	dd triggering cond	ition	×
	Define check		
	Check type:	VB Script	-
	Condition:	returns TRUE (1)	-
	VB Script file:	myscript.vbs	🖻 🧭
		Add	Cancel

Screenshot 130 - The check triggering conditions dialog

8. From the '*Check type:*' drop down select 'VBScript' and specify the triggering condition in the 'Condition' field.

9 Click on the  $\cong$  (open) button and select the custom VBscript file that will be executed by this check. For this example select '*myscript.vbs*'.

10. Click on **Add** to include the vulnerability check to the list.

11. Select the relative vulnerability check box so that it is include it in the next network vulnerability scan.

#### Testing the vulnerability check/script used in our example

Scan your local host computer using the scanning profile where the new check was added.

```
    ⊢ ☐ Miscellaneous Alerts (1)
    ⊢ I Script run test
    └─ I Description: Script has run successfully
```

In the scan results, a vulnerability warning will be shown in the **Vulnerabilities ▶ Miscellaneous Alerts** node of the scan results.

#### Adding a vulnerability check that uses a custom shell script

In GFI LANguard N.S.S. you can add vulnerability checks which use custom shell scripts to check Linux and UNIX based targets. These checks are remotely executed over SSH by the SSH module. Script can be written using any scripting language that outputs text results to the console.

In the following example we will create a vulnerability check (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

echo "FALSE:"

fi

echo "!!SCRIPT\_FINISHED!!"

3. Save the file in 'C:\Program Files\GFI\LANguard Network Security Scanner 7.0\Data\Scripts\myscript.sh"



Step 2: Add the new vulnerability check:

Screenshot 131 - Adding a new vulnerability check

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile where you wish to add the new vulnerability check.

2. Click on the Vulnerabilities tab.

3. From the middle pane, select the category in which the new vulnerability check will be included (for example, DNS Vulnerabilities).

4. Click on the **Add** button. This will bring up the new vulnerability check dialog.

7. Specify the basic details such as the vulnerability name, short description, security level, and BugtraqID/URL (if applicable). Optionally, you can also specify how long the check takes to execute.

8. Click on the **Add...** button. This will bring up the check triggering conditions dialog.

A	dd triggering condi	tion	×
	Define check		
	Check type:	SSH Script	•
	Condition:	returns TRUE (1)	•
	SSH Script file:	osdata.ssh 🗃 😂	è
		Add Car	ncel

Screenshot 132 - The check triggering conditions dialog

9. From the 'Check type:' drop down select 'SSH Script' and specify the triggering condition in the 'Condition' field.

10 Click on the  $\not\cong$  (open) button and select the custom SSH script file that will be executed by this check. For this example use '*myscript.sh*'.

11. Click on Add to include the vulnerability check to the list.

12. From the list of checks, select the relative vulnerability check box so that it is include it in the next network vulnerability scan.

#### Testing the vulnerability check/script used in our example

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. The **A** Vulnerabilities node will the vulnerability warning shown below.

Erile test.file exists

🖳 🗹 Description: The test file "test.file" exists in the current scanned user home directory

#### Adding a CGI vulnerability check

When creating new CGI vulnerability checks, you do not need to create a VB or SSH script. In fact, the scanning functionality of CGI checks is configurable through the options included in the check properties dialog.

G GF1 LANguard N.S.S. 7.0         Ele       Iools       Configure       Help         Image: One we Scanser       Image: One Scanser       Using: C         Tools       Explorer       Image: One Scanser       Image: One Scanser         Image: One Scanser       Image: One Scanser       Image: One Scanser       Image: One Scanser         Image: One Scanser       Image: One Scanser       Image: One Scanser       Image: One Scanser         Image: One Scanser       Image: One Scanser       Image: One Scanser       Image: One Scanser	urrently Logged-On User ■ User Nam TCP Ports   UDP Ports   OS Data Vuln Specify what information is to be retrieved IV Epable Vulnerabilities Scanning	2 Password: Patches   Scanner Options   Devices   A d by the scanner when using this profile	pplications
Construction     C	Advanced	Image: State Stat	Allows attackers to execute commands Remote file retrieving Possible to view atbitary files Remote file retrieving Ad.cgi has a known exploit which allows Possible Vaek authentification Build.cgi if it has execute permission and It is possible to force the web server to s Remote users can execute atbitary corr Possible directory listing, probably view It is possible to force the web server to s Remote command execution Possible to increact the server to s Remote command execution Possible to run atbitary commands (wet Possible to run atbitary co
	Advanced	Add	4 <u>H</u> emove

Screenshot 133 - Creating a CGI vulnerability check

To create a new CGI vulnerability check:

1. Go to the **Configuration > Scanning Profiles > CGI Scanning** node.

- 2. From the right pane, click on the Vulnerabilities tab.
- 3. From the middle pane, select the CGI Abuses node.

4. Click on the **Add** button. This will bring up the new CGI vulnerability check dialog.

E	dit CGI Abuse	×
	General Description	
	······	1
	⊻ulnerability Name:	All Servers: (e)shop Online-Shop System
	Short Description:	Allows attackers to execute commands (web ser
	Security <u>L</u> evel:	
	<u>B</u> ugtraqID/URL:	<u>ک</u>
	Time consumption:	Quick to execute
	Trigger condition	
	HTTP Method:	GET method
	To check for the <u>U</u> RL:	eshop.pl?seite=;cat%20/etc/passwd
	Under the <u>D</u> irectories:	cgi-bin
	<u>R</u> eturn string:	Contains the text
		ROOT:
		OK Cancel Apply

Screenshot 134 - The new CGI vulnerabilities check dialog

5. Specify the basic details of this vulnerability check such as the name, short description, security level, and BugtraqID/URL (if applicable). Optionally, you can also specify how long the check takes to execute.

6. In the 'Trigger condition' area of the dialog, specify the following parameters:

- 'HTTP method' Specify the type of http request that the CGI vulnerability check will use when querying information. CGI vulnerability checks supports 2 HTTP methods which are the 'GET method' and the 'HEAD method'.
- 'To check for the URL:' Specify the name of the CGI script that will be executed during target computer scanning.
- 'Under the Directories:' Specify the directories where the CGI script is located.
- 'Return String' Specify the expected result string. GFI LANguard N.S.S. defines if this check is successful by comparing the specified return string to the text in the check results. This text comparison is carried out using specific conditions which are set by selecting one of the following options:

- 'Contains any text' Select this option if you want the check to be successful when any part of the specified string is present in the check results.
- 'Contains the text' Select this option if you want the check to be successful ONLY when the specified string is entirely present in the check results.
- 'Contains the text' Select this option if you want the check to be successful ONLY when the specified string is NOT present in the check results.

7. Click on **OK** to save the configuration settings.

**NOTE:** To automatically include new checks in the next target computer scan, click on the **Advanced** button and set the *'New vulnerabilities are enabled by default'* option to 'Yes'.

#### Adding other vulnerability checks

GFI LANguard N.S.S. allows you to create particular vulnerability checks which do not use VB or SSH scripts. These checks are based on the same concepts of CGI vulnerability checks, but with different configuration parameters and options.



Screenshot 135 - Creating a CGI vulnerability check

To create these type of checks:

1. Expand the **Configuration** Scanning Profiles node and select the scanning profile where you wish to add the new vulnerability check.

2. From the right pane, click on the **Vulnerabilities** tab.

3. From the middle pane, select the category where you wish to create the new vulnerability check.

4. Click on the **Add** button. This will bring up the new vulnerability check dialog.

Edit Yulnerability					×
General Description					
⊻ulnerability Name:	Importe	ed_IMAP4 serv	ver (wu-imapd bu	ufferoverflo	
Short Description:	Wu-ima	apd is vulnerat	ole to a buffer ov	verflow cond	
Security <u>L</u> evel:				•	
BugtragID/URL:	http://	www.securityf	ocus.com/bid/4	713/ 🔗	
Time consumption:	Quick I	to evecute		 	
	gaicit				
This vulnerability check v all met:	will be tr	iggered when	the following co	onditions are	
Check type		Details			
🗹 Operating System		is "Unix"			
VB Script		returns T	RUE (1) ''imap_	buffer_ov	
		Add tri	iggering conditio	on	
		<u>E</u> dit tri	ggering conditio	m	
		Remov	ve triggering cor	ndition	
Add Rem	ove	E dit			
		ОК	Cancel	Apply	

Screenshot 136 - The new vulnerability check dialog

5. Specify the basic details such as the vulnerability name, short description, security level, and BugtraqID/URL (if applicable). Optionally, you can also specify how long the check takes to execute.

6. Click on the **Add...** button. This will bring up the check triggering conditions dialog.

Ed	Edit triggering condition 🛛 🗙				
	Define check Check type: Condition: Operating System:	Operating System  Operating System  Reg Key  Reg Path  Reg Value  Service Pack  Hotfix  IIS  IIS Version			
		Change Cancel			

Screenshot 137 - The check triggering conditions dialog

7. From the 'Check type:' drop down select the required check type and specify a corresponding trigger condition in the 'Condition' field. A

Supported Check Type	Supported Trigger Conditions		
Operating System	• Is		
	Is Not		
Begistry Key*	• Exists		
• Registry Rey	Not Exists		
Begistry Path *	Exists		
	Not Exists		
	Is Equal With		
Registry Value	Is Not Equal With		
	Is Less Than		
	Is Greater Than		
	• Is		
Service Pack	Is Not		
	Is Lower Than		
	Is Higher Than		
Hot fix	Is Installed		
	Is Not Installed		
• 115	Is Installed		
	Is Not Installed		
	• Is		
IIS Version	Is Not		
	Is Lower Than		
	Is Higher Than		
RPC Service	Is Installed		
	Is Not Installed		
NT Service	Is Installed		
	Is Not Installed		
NT Service running	Is running		
	Is not running		
	Automatic		
NT Service startup type	• Manual		
	Disabled		
Port (TCP)	Is Open		
	Is Closed		
UDP Port	Is Open		
	Is Closed		
FTP banner **	• Is		
	Is Not		
HTTP banner **	• Is		
	Is Not		
SMTP banner **	• Is		
	Is Not		
POP3 banner **	• Is		
	Is Not		

list of the supported check types and their respective trigger conditions is included below:

DNS banne	• **	ls
	•	Is Not
	• **	ls
	•	Is Not
- Tolpot bopp	•	ls
	•	Is Not
- Corint	•	Returns True (1)
• Schpt	•	Returns False (0)
	•	Returns True (TRUE:)
• 33H 30hpt	•	Returns False (FALSE:)

\* Works only under HKEY\_LOCAL\_COMPUTER

\*\* You can build expressions that check for Version 1.0 through 1.4, and Version 2.0 through 2.2, but not Version 1.5 through 1.9. See the examples below.

8. Click on **Add** to include the selected condition in the vulnerability check.

9. Click on the **OK** button to save the settings and exit from the configuration dialog.

#### **Additional Information:**

E	dit Yulnerability			×
	General Description			
	⊻ulnerability Name:	Importe	ed_RLOGIN service enabled	
	Short Description:	This se	ervice is vulnerable to TCP spoo	ofing attack
	Security Level:			•
	BugtraqID/URL:	tp://w	ww.cert.org/tech_tips/usc20_fr	ull.htm 🔗
	Time consumption:	, Time c	onsumina	
		1	, , , , , , , , , , , , , , , , , , ,	
	This vulnerability check all met:	will be t	riggered when the following cor	nditions are
	Check type Details			
	Operating System		is "Unix"	
	CP Port		is OPEN "513"	
	VB Script		returns TRUE (1) "rlogin.v	/bs"
	Add Rer	nove	Edit	
			OK Cancel	Apply
_				

Screenshot 138 - A vulnerability check with multiple trigger conditions

1. Each vulnerability check can include multiple trigger conditions. In this way, you can rest assured that a vulnerability check is triggered

only when required (i.e. if all the specified trigger criteria/conditions are met).

### **Miscellaneous**

#### **Enabling NetBIOS on a network computer**

1. Log on to the target computer with administrative rights

2. Navigate to the Windows Control Panel (**Start > Control Panel**) and double-click on 'Network Connections' icon.



Local Areas Connection' icon

3. Right click on 'Local Areas Connection' icon of the NIC card that you wish to configure and select **Properties**.

- 4. Click on 'Internet Protocol (TCP/IP)' and select Properties.
- 5. Click on the **Advanced** button.
- 6. Click on the **WINS** tab.

Advanced TCP/IP Settings		? ×
IP Settings DNS WINS Options		
WINS addresses, in order of use:		
		t Ţ
Add	Remo <u>v</u> e	
If LMHOSTS lookup is enabled, it applies to all TCP/IP is enabled.	connections fo	r which
✓ Enable LMHOSTS lookup	Import LMI	HOSTS
NetBIOS setting Default Use NetBIOS setting from the DHCP set used or the DHCP server does not prov enable NetBIOS over TCP/IP.	rver. If static IF ide NetBIOS se	'address is etting,
C Enable NetBIOS over TCP/IP		
Disable NetBIOS over TCP/IP		
[	ОК	Cancel

Screenshot 139 - Local Areas Connection properties: WINS tab

7. Select the 'Default' option from the 'NetBIOS Setting' area.

**NOTE:** If static IP is being used or the DHCP server does not provide NetBIOS setting, select the *'Enable NetBIOS over TCP/IP'* option instead.

8 Click on **OK** and exit the 'Local Area Properties' dialog(s).

# Installing the Client for Microsoft Networks component on Windows 2000 or higher

The Client for Microsoft Networks is an essential networking software component for the Microsoft Windows family of operating systems. A Windows computer must run the Client for Microsoft Networks to remotely access files, printers and other shared network resources. These step-by-step instructions explain how to verify that the client is present and, if not, how to install it.

1. Navigate to the Windows Control Panel (**Start ▶ Settings ▶ Control Panel**).

2. Right click on the "Local Area Connection" item and select **Properties**. This will bring up the 'Local Area Connection Properties' dialog.

**NOTE:** If the computer runs any older version of Windows, like Windows 95 or Windows 98, locate and right click on Network Neighborhood, then choose **Properties**. Alternatively, navigate to Control Panel and open the *'Network'* item.

🚣 Local Area Connection Propertie	25		?	×
General Authentication Advanced				
Connect using:				
Intel(R) PRO/1000 MT Network Con <u>C</u> onfigure				
This connection uses the following ite	ems:			
<ul> <li>✓ Elient for Microsoft Networks</li> <li>✓ Elie and Printer Sharing for Microsoft Networks</li> <li>✓ QoS Packet Scheduler</li> <li>✓ Thternet Protocol (TCP/IP)</li> </ul>				
I <u>n</u> stall <u>U</u> ninstall P <u>r</u> operties				
Description Allows your computer to access resources on a Microsoft network.				
<ul> <li>Show icon in notification area when connected</li> <li>Notify me when this connection has limited or no connectivity</li> </ul>				
	OK	Can	cel	

Screenshot 140 - Local Area Connection Properties dialog

3. From the **General** tab which opens by default, select the checkbox next to *'Client for Microsoft Networks'* and click on **Install...** to begin the installation process.

**NOTE 1:** If *'Client for Microsoft Windows'* checkbox is already selected, then the component is already installed.

**NOTE 2:** If the network is currently active, you may not see any checkboxes in the window. In this case, click the **Properties** button one more time to reach the full **General** tab.

**NOTE 3:** If the computer runs any older version of Windows, view the **Configuration** tab and verify if *'Client for Microsoft Windows'* is

present in the displayed list. If not, install the component by clicking on the **Add...** button.

4. From the new dialog on display, select '*Client*' and click on **Add...** to continue.

5. From the list of manufacturers at the right of the active window choose '*Microsoft*'. Then, choose "Client for Microsoft Windows" from the list of Network Clients on the right side of the window. Click on the **OK** button to continue.

6. To finalize the installation, click on the **OK** button and reboot the computer. After the computer has restarted, Client for Microsoft Windows will be automatically installed.

# Configuring Password Policy Settings in an Active Directory-Based Domain

**NOTE:** You must be logged on as a member of the Domain Admins group.

To implement password policies on network computers belonging to an Active Directory domain:

1. Navigate to the Control Panel (**Start** > **Settings** > **Control Panel**) and open the 'Administrative Tools'.



Screenshot 141 - Active Directory Users and Computers configuration dialog

2. Open the 'Active Directory Users and Computers'. Right click on the root container of the domain and select **Properties**.

christest.com Properties		? ×
General Managed By Group Policy		
Current Group Policy Object Links fo	r christest	
Group Policy Object Links	No Override	Disabled
S Default Domain Policy		
S Domain Policy		
Group Policy Objects higher in the list have the h This list obtained from: christophertest.christest.c	ighest priority. om	
<u>N</u> ew A <u>d</u> d <u>E</u> dit		Up
<u>Options</u> Dele <u>t</u> e <u>P</u> roperties		Do <u>w</u> n
Block Policy inheritance		
Close	Cancel	Apply

Screenshot 142 - Configuring a new Group Policy Object (GPO)

3. In the properties dialog, click on the **Group Policy** tab. Then click on **New** to create a new Group Policy Object (GPO) in the root container.

4. Specify the name of the new group policy (for example, "Domain Policy") and then click on **Close**.

**NOTE:** Microsoft recommends that you create a new Group Policy Object rather than editing the default policy (called 'Default Domain Policy'). This makes it much easier to recover from serious problems with security settings. If the new security settings create problems, you can temporarily disable the new Group Policy Object until you isolate the settings that caused the problems.

5. Right click on the root container of your domain and select **Properties**. This will bring up again the Domain Properties dialog.

6. Click on the **Group Policy** tab, and select the new Group Policy Object Link that you have just created (for example, *'Domain Policy'*).

7. Click on **Up** to move the new GPO to the top of the list, and then click on **Edit** to open the Group Policy Object Editor.



Screenshot 143 - The Group Policy Object Editor

8. Expand the **Computer Configuration** node and navigate to **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy** folder.

Enforce password history Properties	? ×
Security Policy Setting	
Enforce password history	
Define this policy setting	
Keep password history for:          24          passwords remembered	
OK Cancel	Apply

Screenshot 144 - Configure the GPO password history

9. From the right pane, double-click on the 'Enforce password history' policy. Then select the 'Define this policy setting' option, and set the 'Keep password history' value to '24'.

10. Click on the **OK** button to close the dialog.

Maximum password age Properties	? ×
Security Policy Setting	
Maximum password age	
Define this policy setting	
Password will expire in:	
42 🕂 days	
OK Cancel A	pply

Screenshot 145 - Configuring GPO password expiry

11. From the right pane, this time double-click on the 'Maximum password age' policy. Then select the 'Define this policy setting' option and set the 'Password will expire' value to 42 days.

12. Click on **OK** to close the properties dialog.

Minimum password age Properties	? ×
Security Policy Setting	
Minimum password age	
Define this policy setting	
Password can be changed after:	
OK Cancel App	ply

Screenshot 146 - Configuring the minimum password age

13. From the right pane, double-click on the *'Minimum password age'* policy. Then select the *'Define this policy setting'* option and set the *'Password can be changed after:'* value to '2'.

14. Click on the **OK** button to close the dialog.

Minimum password length Properties	? ×
Security Policy Setting	
Minimum password length	
Define this policy setting	
Password must be at least:	
OK Cancel A	pply

Screenshot 147 - Configuring the minimum number of characters in a password

15. From the right pane, double-click on the *'Minimum password length'* policy. Then select the *'Define this policy setting'* option and set the value of the *'Password must be at least:'* entry field to '8'.

16. Click on the **OK** button to close the dialog.



Screenshot 148 - Enforcing password complexity

17. From the right pane, double-click on the 'Password must meet complexity requirements' policy. Then enable the 'Define this policy setting in the template' option, and select 'Enabled'.

18. Click on the **OK** button to close the dialog.

19. At this stage the password policy settings of the new GPO have been configured. Close all dialogs and exit the 'Active Directory Users and Computers' configuration dialog.

# Viewing the Password Policy Settings of an Active Directory-Based Domain

**NOTE:** You must be logged on as a member of the Domain Admins group.

Use the following procedure to verify that the appropriate password policy settings are applied and effective in the Domain Policy GPO. Verifying the settings and their operation ensures that the correct password policies will be applied to all users in the domain. To verify password policy settings for an Active Directory domain

1. Navigate to the Control Panel (**Start** > **Settings** > **Control Panel**) and open the 'Administrative Tools'.

2. Open the 'Active Directory Users and Computers'. Right click on the root container of the domain and select **Properties.** 

3. Click on the **Group Policy** tab. Then select the GPO to be checked (for example, '*Domain Policy GPO*') and click on **Edit** to open the Group Policy Object Editor.

4. Expand the **Computer Configuration** node and navigate to **Windows Settings ► Security Settings ► Account Policies ► Password Policy** folder.



Screenshot 149 - Verifying the GPO settings

The password policy configuration settings are displayed in the right pane of the GPO editor. Assuming that you have configured the password policy of your GPO as shown in the above screenshot, you should verify that users cannot specify passwords that are shorter than eight characters. These password policy settings should also prevent users from create non-complex passwords, and should not allow users to change passwords which are not older than two days.

### Troubleshooting

#### Introduction

The troubleshooting chapter explains how you should go about resolving issues you have. The main sources of information available to users are:

- The manual most issues can be solved by reading the manual.
- The GFI Knowledge Base accessible from the GFI website.
- The GFI support site.
- Contacting the GFI support department by email at support@gfi.com
- Contacting the GFI support department using our live support service at <u>http://support.gfi.com/livesupport.asp</u>
- Contacting our support department by telephone.

#### **Knowledge Base**

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most upto-date listing of support questions and patches.

The Knowledge Base can be found on http://KBase.gfi.com

#### Request support via email

If, after using the Knowledge Base and this manual, you have any problems that you cannot solve, you can contact the GFI support department. The best way to do this is via email, since you can include vital information as an attachment that will enable us to solve the issues you have more quickly.

The **Troubleshooter**, included in the program group, automatically generates a series of files needed for GFI to give you technical support. The files would include the configuration settings, debugging log files and so on. To generate these files, start the troubleshooter wizard and follow the instructions in the application.

In addition to collecting all the information, you will be asked a number of questions. Please take your time to answer these questions accurately. Without the proper information, it will not be possible to diagnose your problem.

Then go to the troubleshooter\support folder, located under the main program directory, compress the files in ZIP format, and send the generated ZIP file to <u>support@gfi.com</u>.

Ensure that you have registered your product on our website first, at <u>http://customers.gfi.com</u>.

We will answer your query within 24 hours or less, depending on your time zone.

#### Request support via web chat

You may also request support via 'LiveSupport (web chat)'. You can contact the GFI support department using our LiveSupport service at <a href="http://support.gfi.com/livesupport.asp">http://support.gfi.com/livesupport.asp</a>

Ensure that you have registered your product on our website first, at <a href="http://customers.gfi.com">http://customers.gfi.com</a>

.....

#### **Request support via phone**

You can also contact GFI by phone for technical support. Please check our support website for the correct numbers to call, depending on where you are located, and for our opening times.

Support website:

http://support.gfi.com

Ensure that you have registered your product on our website first, at <a href="http://customers.gfi.com">http://customers.gfi.com</a>

#### Web Forum

User to user support is available via the web forum. The forum can be found at:

http://forums.gfi.com/

#### **Build notifications**

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, go to:

http://support.gfi.com

### Index

#### Α

Alerting Options 55, 60, 136 alerts 11 Applications 36, 75, 92, 94, 95, 96, 97 Attendant service 4

#### С

command line tools 3, 135 Computer Profiles 8, 18, 55, 60, 61, 62, 136, 137 custom scripts 5, 139, 143

#### D

database backend 3, 9, 10, 43, 44, 55, 56, 64, 65, 66, 68, 69 Database Maintenance Options 55, 64, 65, 66 DNS Lookup 127, 128

#### Ε

Enumerate Computers 127, 132, 133 Enumerate Users 127, 134

#### G

groups 34

#### I

installation 7, 8, 11, 105, 131, 136, 137

#### L

License 6 licensing 6, 7, 11 Logged on Users 34

#### Μ

Microsoft SQL Server Audit 127, 131 Multilingual patch management 107

#### Ν

NetBIOS 39, 40, 153

network devices 3, 37, 86, 90 network tools 127

#### Ο

Open Ports 32, 48 Operating System 3 OS data 75, 78

#### Ρ

Parameter files 55, 62 Password Policy 29 patch deployment 4, 105, 109, 112, 113, 118, 119, 120, 136, 137 Patch management 3, 105, 115 **Physical devices** 37 program updates 99, 101, 103

#### R

recalled patches 106 **Registry** 26, 27, 29, 149 Remote Processes 35 results comparison 121, 123

#### S

scan results 3, 4, 9, 21, 43, 44, 45, 47, 51, 56, 58, 59, 63, 65, 66, 67, 80, 122, 123, 135, 136, 140, 143 Scanning Profiles 14, 21, 29, 33, 39, 55, 71, 72, 75, 76, 77, 78, 79, 80, 83, 84, 85, 88, 89, 90, 91, 92, 93, 94, 95, 96, 106, 135, 141, 144, 145, 147 Scheduled Scans 55, 56, 57, 58, 59, 125, 126 Script Debugger 4, 5, 139, 141 script editor 139, 141 Security Audit Policy' 30 services 3, 10, 27, 32, 35, 63, 66, 105, 119, 137 Shares 28, 48 SNMP Audit 127, 131 SNMP Walk 127, 130 SSH 7, 140, 141, 143, 145, 147, 150 SSH Private Key 18, 58, 60, 140 Status Monitor 4, 6, 125, 126 System patching status 39 System requirements 7

#### Т

TCP Ports 76 Trace Route 127, 128

#### USB devices 1, 3, 13, 38, 39, 48, 71, 75, 86, 87, 91, 92, 122 Users 2, 32–39, 32–39, 139 users and groups 34, 48

#### ۷

Virtual devices 37 Vulnerabilities 23, 24, 26, 27, 47, 75, 79, 80, 82, 91, 141, 143, 144, 145, 146, 147

#### W

Whois 127, 129 Wireless devices 37

#### U