GFI LANguard Network Security Scanner 8

Manual

By GFI Software

http://www.gfi.com
Email: info@gfi.com

Version 8.0 – Last updated April 11, 2007

Contents

9. Scanning Profiles 83

10. GFI LANguard N.S.S. updates 115

11. Patch management: Deploying Microsoft Updates 121

1. Introduction

Introduction to GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (N.S.S.) is a security scanning, network auditing and patch deployment tool which enables you to scan and protect your network by:

- Identifying system and network weaknesses using a state of the art vulnerability check database based on OVAL and SANS Top 20 vulnerability database.
- Auditing of all hardware and software aspects of system installations on your network allowing you to create a detailed inventory of assets present on your IT infrastructure. This goes as far as enumerating installed applications as well as USB devices connected on your network. Further to this, GFI LANguard N.S.S. also checks whether your anti-virus and anti-spyware protection is enabled by analyzing the configuration settings of such software.
- Enabling you to automatically download and remotely install service packs and patches for Microsoft operating systems and third party products.

How is this manual structured

This manual is logically structured to assist you to in getting GFI LANguard N.S.S. up and running in the shortest time possible:

- **Chapters 1** and **2** provide you with an introduction to GFI LANguard N.S.S. and overview of how to install GFI LANguard N.S.S. on your system.
- **Chapter 3** shows you how to navigate the management console.
- **Chapters 4** and **5** provide you with "Getting started" information related to performing audits and analyzing security scan results.
- **Chapter 6** shows you how to save and load scan results of scans previously performed.
- **Chapter 7** demonstrates how to filter results using the results filter tab to display on screen reports.

NOTE: At this stage, you will have gained enough knowledge to run GFI LANguard N.S.S. on default settings.

- **Chapter 8** deals with how you can customize GFI LANguard N.S.S. to suit your particular network needs.
- **Chapter 9** is exclusively dedicated to scanning profiles and their customization. You will also learn how to create new scanning profiles to scan for specific issues.

- **Chapter 10** deals with GFI LANguard N.S.S. program updates, the configuration of such updates and how to turn them on and off.
- **Chapters 11** and **12** enable you to discover how to deploy Microsoft updates, service packs and third party software. You will also discover how to roll back (uninstall) Microsoft updates.
- **Chapter 13** will enable you to learn how to use GFI LANguard N.S.S. to generate a results comparison report between scans held in different periods of time.
- **Chapter 14** demonstrates the functionality of GFI LANguard N.S.S.' status monitor and the features that are included within. It assists you in interpreting the various tabs that are included in the status monitor.
- **Chapter 15** shows you how to use the various tools that are implemented within GFI LANguard N.S.S. Amongst others these include DNS Lookup, Traceroute and enumeration of users and computers.
- **Chapters 16** and **17** deals with advanced features related to the use of GFI LANguard N.S.S. via command-line and how to add custom vulnerabilities using scripts.
- **Chapter 18** engages any miscellaneous issues that could not be included in other sections of the manual.
- **Chapter 19** is a troubleshooting guide that assists you in resolving any issues you might encounter during the use of this product.

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.
- Scans for all known vulnerabilities reported in the OVAL, CVE and SANS Top 20 databases.
- Enumerates:
    - Groups (group members during target computer scanning).
    - USB devices attached to target computers.
    - Network devices (wired, wireless, or virtual).
    - Services and their respective state.
    - Remote running processes.
    - 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/Vista operating systems, Microsoft Office XP or later, Microsoft Exchange 2000/2003 and Microsoft SQL Server 2000 or later.
- Patch management support for multilingual operating systems that are Unicode compliant.
- Patch rollback support.
- 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, operating system identification, SNMP Auditing and 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.
- Improved multithreading capabilities that allows more that three computers to be scanned at a 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

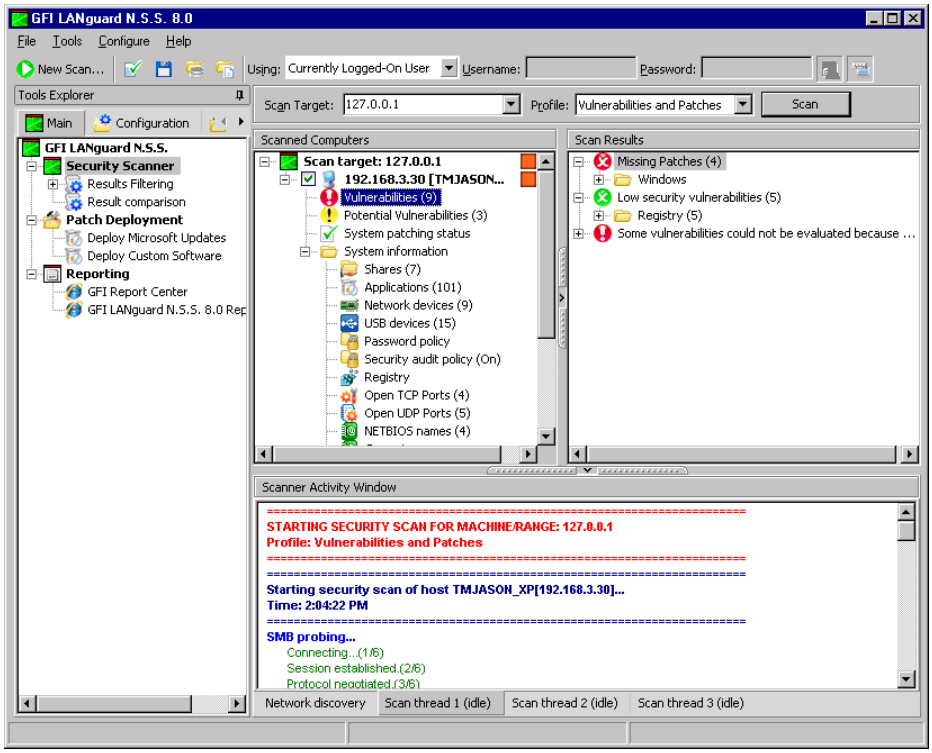
GFI LANguard N.S.S. is built on an architecture that allows for high reliability and scalability that caters for both medium to larger sized networks.

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

- GFI LANguard N.S.S. management console
- 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. management console



Screenshot 1 - GFI LANguard N.S.S. management console

Launch the GFI LANguard N.S.S. management console from **Start ▸ Programs ▸ GFI LANguard Network Security Scanner 8.0 ▸ LANguard Network Security Scanner**.

Use this console 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.

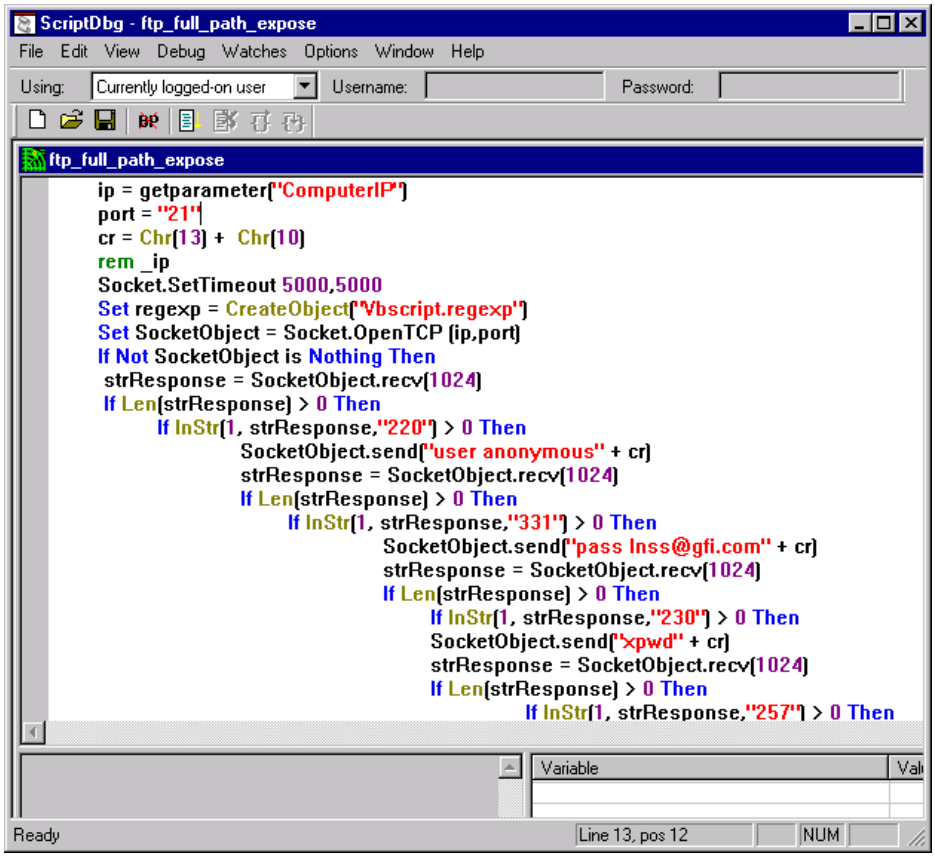
GFI LANguard N.S.S. attendant service

This background service runs all scheduled operations of GFI LANguard N.S.S. including scheduled network security scans and patch deployment operations.

GFI LANguard N.S.S. patch agent service

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

GFI LANguard N.S.S. script debugger

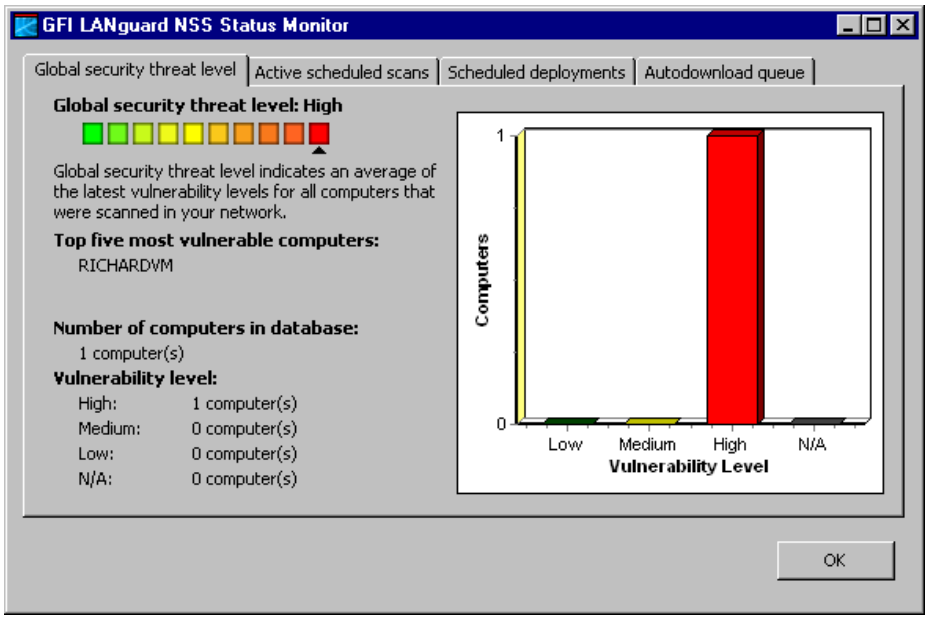


Screenshot 2 - GFI LANguard N.S.S. script debugger

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 through which you can custom-scan network targets for specific vulnerabilities.

Launch the GFI LANguard N.S.S. script debugger from **Start ▸ Programs ▸ GFI LANguard Network Security Scanner 8.0 ▸ GFI LANguard N.S.S. Script Debugger**.

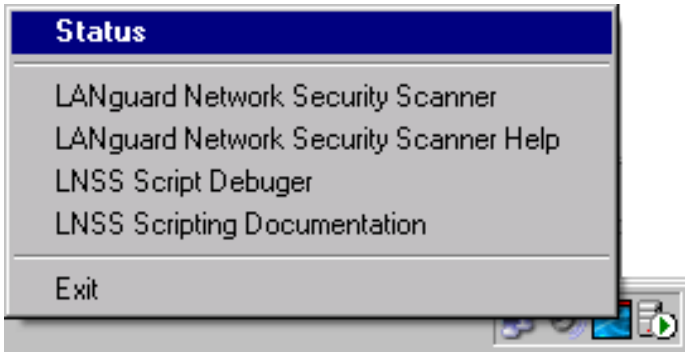
GFI LANguard N.S.S. status monitor



Screenshot 3 - GFI LANguard N.S.S. status monitor

Use the GFI LANguard N.S.S. status monitor to:

- Examine the security threat level of your entire network
- Monitor the status of scheduled scans, software-updates and patch deployment sessions
- Stop scheduled operations that have not yet been executed
- Supervise the status of your patch autodownload queue.



Screenshot 4 - Launching the GFI LANguard N.S.S. status monitor

The GFI LANguard N.S.S. status monitor is automatically launched in the system tray on computer start-up. To access the status monitor, right-click on the GFI LANguard N.S.S. icon and select **Status**.

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: http://www.gfi.com/pricing/pricelist.aspx?product=lanss.

2. Installing GFI LANguard Network Security Scanner

System requirements

Install GFI LANguard N.S.S on a computer that meets the following requirements:

- Windows 2000 (SP4), XP (SP2), 2003, VISTA 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

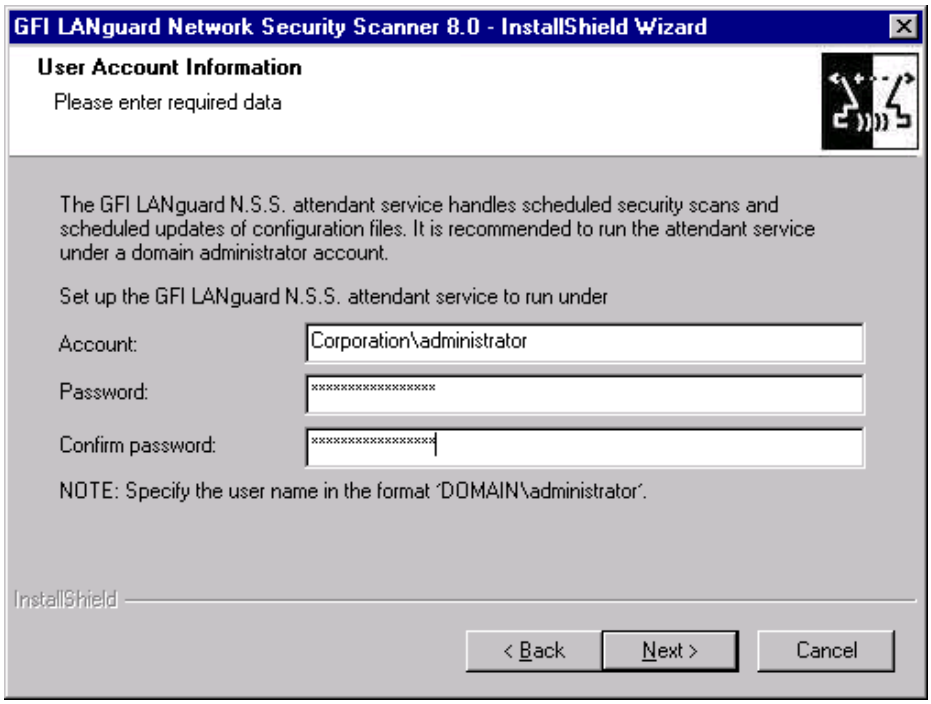
To install GFI LANguard N.S.S. 8:

1. Double-click on **lanuardnss8.exe** and click **Next**.

2. Read the licensing agreement carefully. To proceed with the installation, select the '*Accept the Licensing agreement'* option and click **Next**.

3. Specify licensing details and click **Next** to continue.

NOTE: Default key allows 10 days evaluation.



Screenshot 5 - Specify domain administrator credentials or use local system account

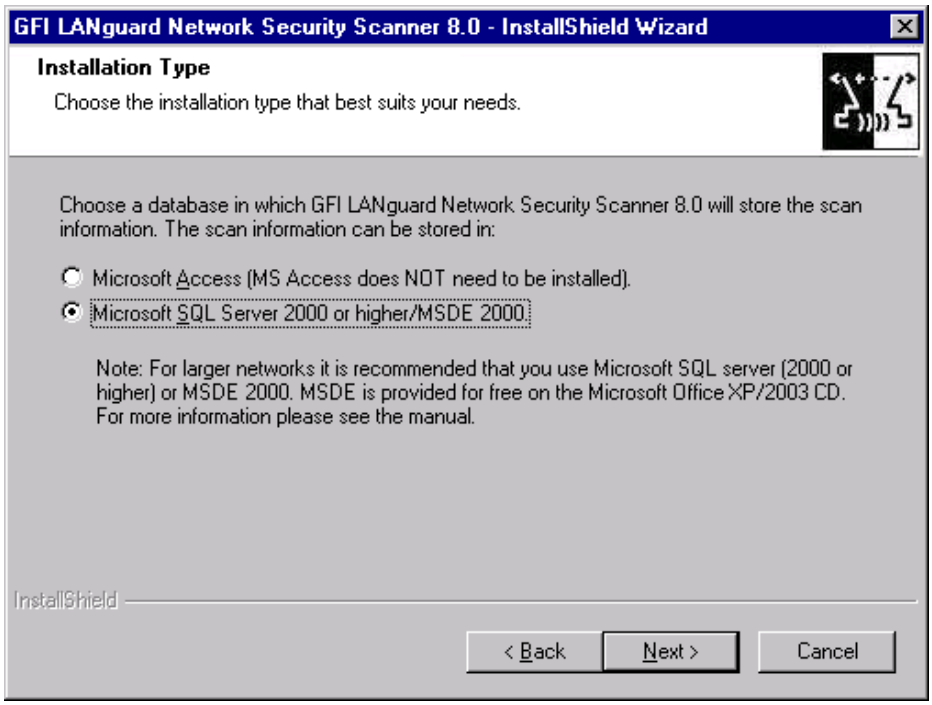
4. If GFI LANguard N.S.S. is already running on your system you will be asked to upgrade to a newer version or build.

NOTE: For more information refer to '*Upgrading earlier versions of GFI LANguard N.S.S.'* section within this chapter.

5. Specify the service account under which GFI LANguard N.S.S. will be running and click **Next**.

NOTE 1: GFI LANguard N.S.S. requires administrative privileges to scan network computers.

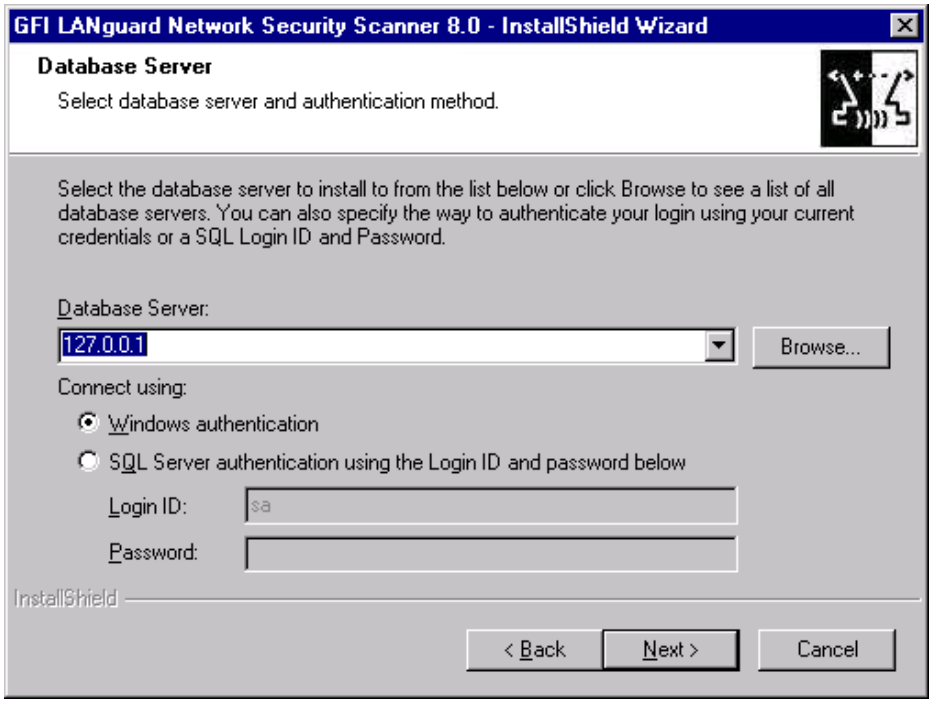
NOTE 2: For more information on how to specify different administrator credentials on a computer-by-computer basis refer to the *'Computer Profiles'* section in this manual.



Screenshot 6 - Choose database backend

6. Select database backend to use when storing network audit results and click **Next**.

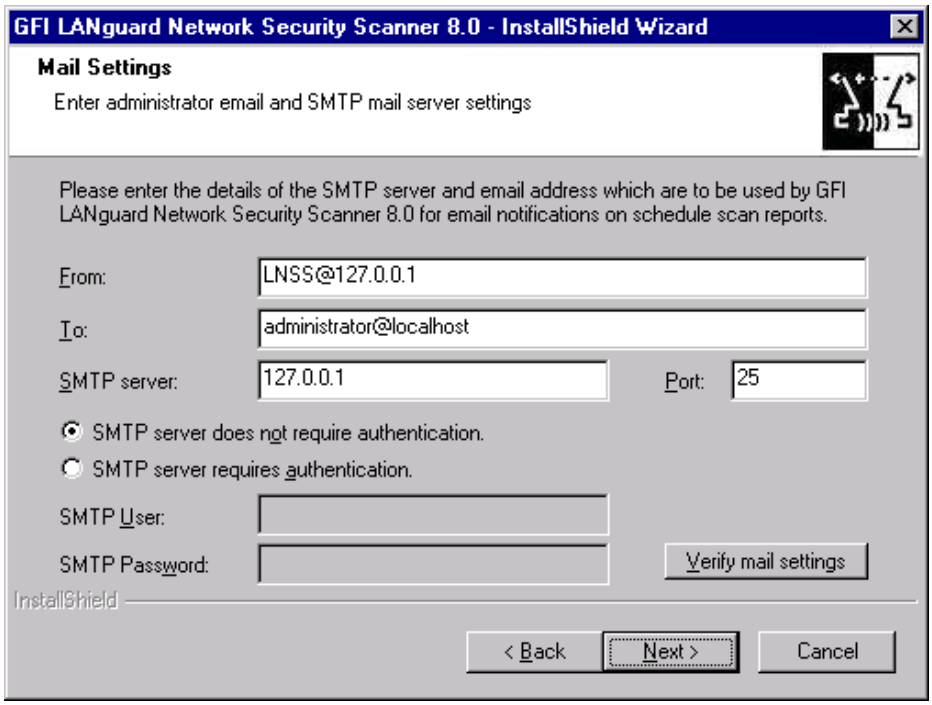
NOTE: We recommend the use of Microsoft SQL Server Express or higher.



Screenshot 7 - Specify SQL Server details

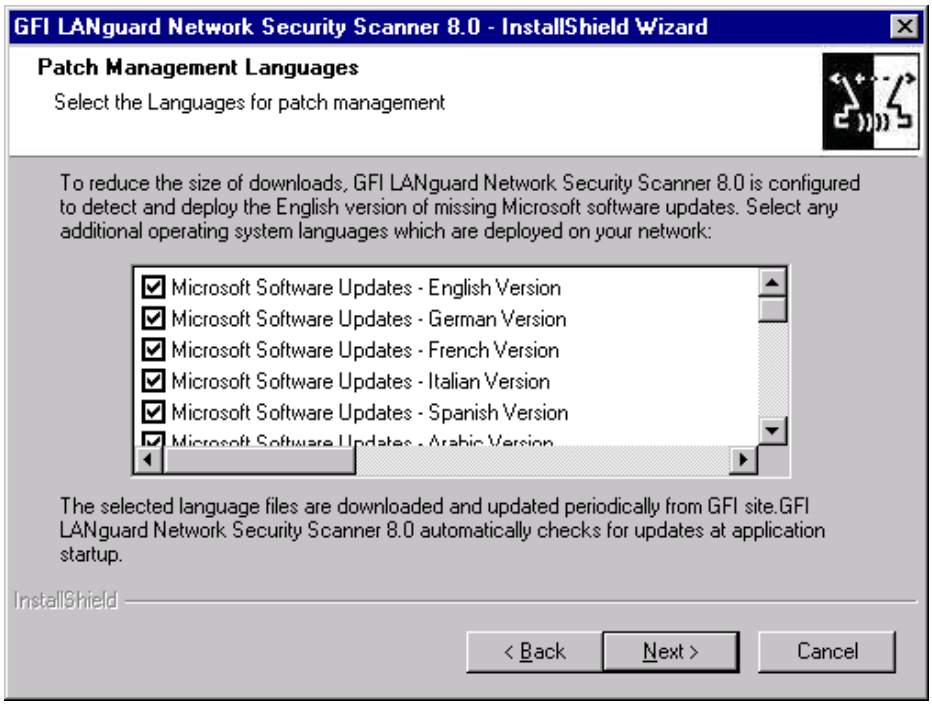
7. If Microsoft SQL Server is selected, specify SQL server details and authentication method. Click on **Next** to continue.

NOTE: GFI LANguard N.S.S. services require administrative privileges over the SQL Server database backend.



Screenshot 8 - Specify alerting email address and mail server details

8. Specify the SMTP mail server details and email address where administrator notifications will be sent. Click on **Next** to continue.



Screenshot 9 - Specify patch languages

9. Select the patch management languages that will be supported by GFI LANguard N.S.S. and click **Next**.

10. Specify the installation path for GFI LANguard N.S.S. and click **Next**.

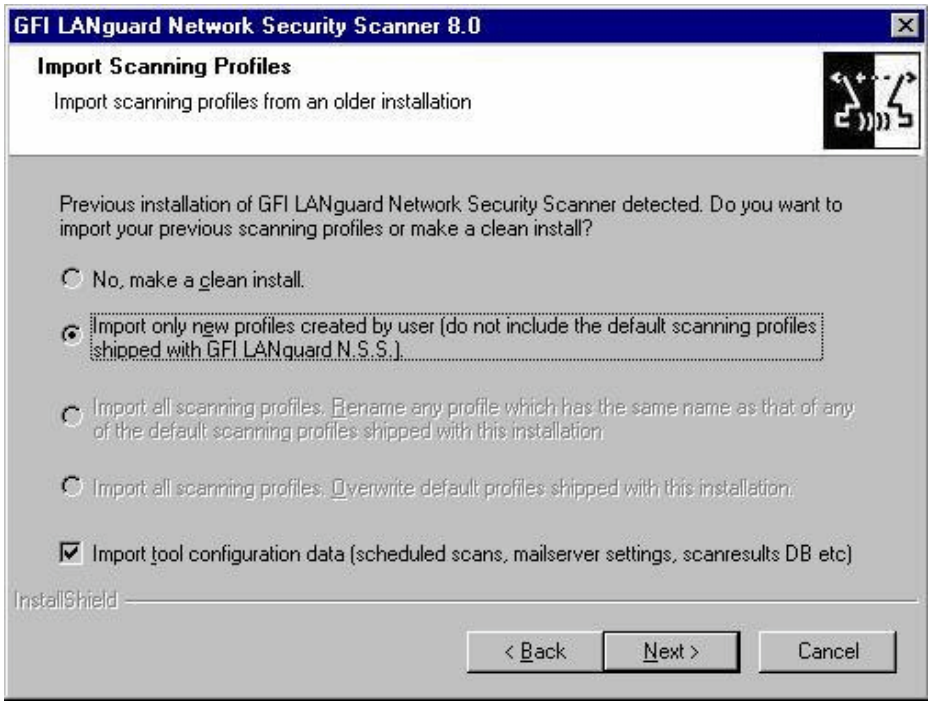
11. Click **Finish** to finalize the installation.

Upgrading earlier versions of GFI LANguard N.S.S.

You can upgrade earlier versions (5, 6, and 7) of GFI LANguard N.S.S. and retain the current custom scan profiles, scheduled scan details, mailserver settings and the scan results database.

To achieve this:

1. Launch GFI LANguard N.S.S. installation.



Screenshot 10 - Choose import options

2. When prompted select the required import options.

3. Continue installation by following the instructions listed in the installation procedure section above.

NOTE: Evaluation versions and older builds of GFI LANguard N.S.S. 8 can be upgraded to the latest build using the same method.

Entering your license key after installation

After installing GFI LANguard N.S.S. you can enter your license key without re-installing or re-configuring the product. To achieve this:

1. Launch GFI LANguard N.S.S. management console.

2. Click on **Configuration** (upper-left of the management console).

3. Select **General ▸ Licensing**.

NOTE 1: By default, GFI LANguard N.S.S. has an unrestricted fully functional evaluation period of 10 days. However, if the data you provided in the download/registration form is correct, you will receive by email an extended license key. This key will extend your default evaluation period by 20 days, allowing you to evaluate the product for a total of 30 days.

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

- Number of computers on which GFI LANguard N.S.S. will be running.

- Number of computers that will be scanned by GFI LANguard N.S.S.

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: To find out how to buy GFI LANguard N.S.S., click on **Configuration** button and choose **General ▸ How to purchase** node.

Registering as a GFI customer

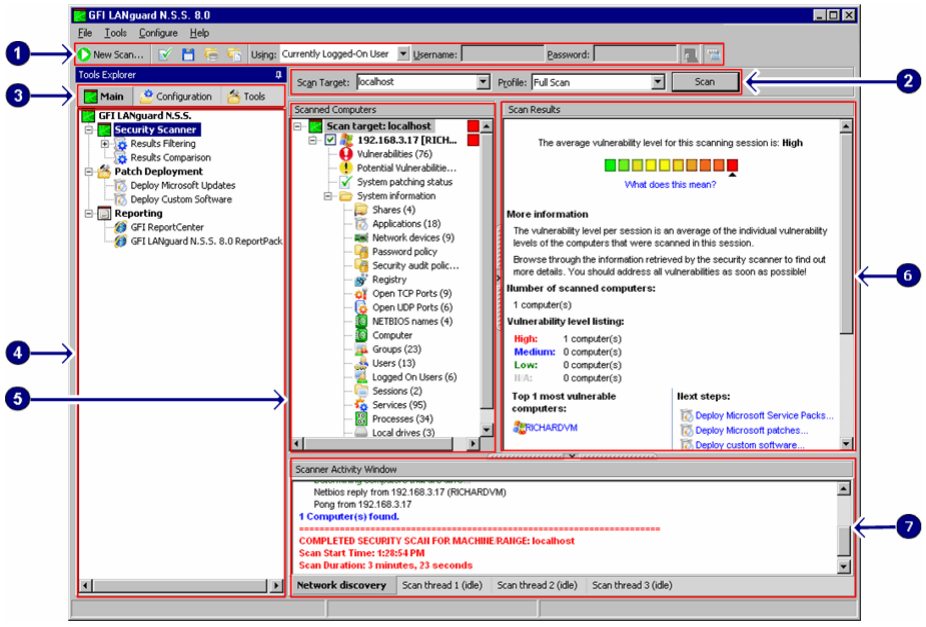
It is important that you register your company and obtain a GFI customer account. This would allow us to give you support and notify you of important product news. To register and obtain your GFI customer account visit: http://www.gfi.com/pages/regfrm.htm.

3. Navigating the management console

Introduction

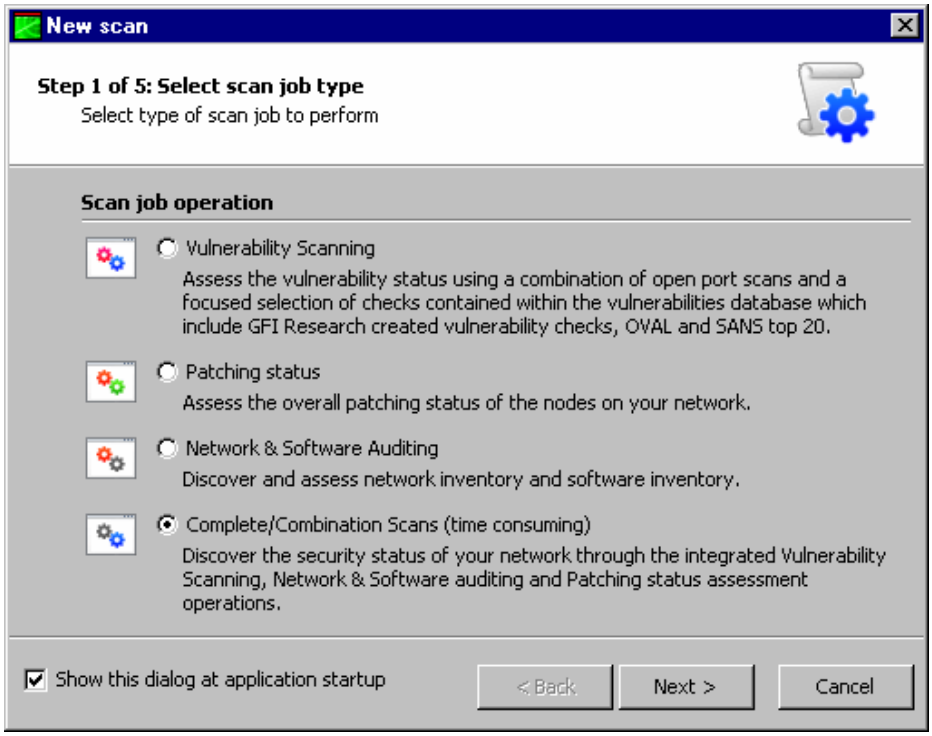
The GFI LANguard N.S.S. management console offers a standardized, common management interface through which you can configure the product as well as run network vulnerability scans, perform patch management tasks and collect system information from a single point of administration.

Navigating the GFI LANguard N.S.S. management console



Screenshot 11 – GFI LANguard N.S.S. 8.0 user interface

1	**Scan toolbar –** Enables you to perform scan related operations such as launch new vulnerability scans and configure alternate scan credentials.
2	**Quick Scan toolbar –** Allows you to quickly launch a vulnerability scan on a particular IP using a specific profile.
3	**Tool Buttons –** Includes 3 buttons **Main**, **Configuration** and **Tools** through which you can switch the options that are accessible through the left pane.
4	**Left Pane –** Allows access to the options available through the **Main, Configuration** and **Tools** buttons. These include scan result filters scheduled scan customization and network administration tools.
5	**Middle Pane –** Shows the vulnerability scan results – broken down into specific categories such as vulnerabilities, potential vulnerabilities, and system information.
6	**Right Pane –** Shows more detailed information on the scan results as well as a graphical representation of the threat level on a computer-by-computer basis as well as on scan-by-scan basis.
7	**Scanner Activity Window –** Displays the activity of scans that are in progress.



Screenshot 12 - New scan wizard

NOTE: On launching GFI LANguard N.S.S. for the first time you are presented with the security scan wizard. This assists you in performing your first network scans using GFI LANguard N.S.S. For more information on how to start a new scan please refer to the "*Performing a security scan using default settings*" section in the "*Getting started: Performing an audit chapter*" of this manual.

4. Getting started: Performing an audit

Introduction

Security scans enable systems administrators to identify and assess possible risks within a network. Through GFI LANguard N.S.S. this is performed automatically, without all the unnecessary repetitive and time-consuming tasks related to performing them manually.

In this chapter you will discover how to perform security scans using default and custom settings, how to start scans directly from the toolbar and how to configure scan ranges.

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).

For a thorough security scan use the *'Full Scan'* option.

About authentication credentials

When performing a security scan GFI LANguard N.S.S. must authenticate to the target computer(s) in order to execute the vulnerability checks and retrieve system information.

To achieve this, GFI LANguard N.S.S. must 'physically' log on to the target computer(s) with administrative rights i.e. using a local administrator account, domain administrator, enterprise administrator account or any other account that has administrative privileges over the target computer(s). Different systems often require different authentication methods. For example, to scan Linux systems you are often required to provide a private key file instead of the conventional password string.

NOTE 1: For more information about authentication methods refer to the 'Computer Profiles' section in the 'Configuring GFI LANguard N.S.S.' chapter.

NOTE 2: 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.

About the scanning process

The target computer scanning process has three distinct stages.

Stage 1: Determine availability of target computer:

During this stage, GFI LANguard N.S.S. will determine whether a target computer is available for vulnerability scanning. This is

achieved through connection requests that are sent in the form of NETBIOS queries, SNMP queries and/or ICMP pings.

NOTE: By default, GFI LANguard N.S.S. will NOT scan the devices that fail to respond to the connection requests sent via NETBIOS queries/SNMP queries/ICMP pings.

Stage 2: Establish connection with target device:

In the second stage of its target scanning process, GFI LANguard N.S.S. will establish a direct connection with the target computer by remotely logon on to it. This is achieved using the scan credentials configured in step 5 of the new scan wizard.

Stage 3: Execute vulnerability checks:

During this final stage, GFI LANguard N.S.S. will execute the vulnerability checks configured within the selected scanning profile. This will result in the identification and reporting of specific weaknesses present on your target computer.

NOTE 1: GFI LANguard N.S.S. ships with a default list of scanning profiles that are preconfigured with vulnerability checks. Nevertheless you can also customize both the scanning profiles and the vulnerability checks contained within. For more information on how to achieve this refer to the "Scanning Profiles' chapter.

NOTE 2: Please note that if any type of Intrusion Detection Software (IDS) is running during scans, 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.

NOTE 3: Along with the IDS software warnings, kindly note that a lot of the scans will show up in log files across diverse systems. UNIX logs, web servers, etc. will all show the intrusion attempts made by the computer running GFI LANguard N.S.S. 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

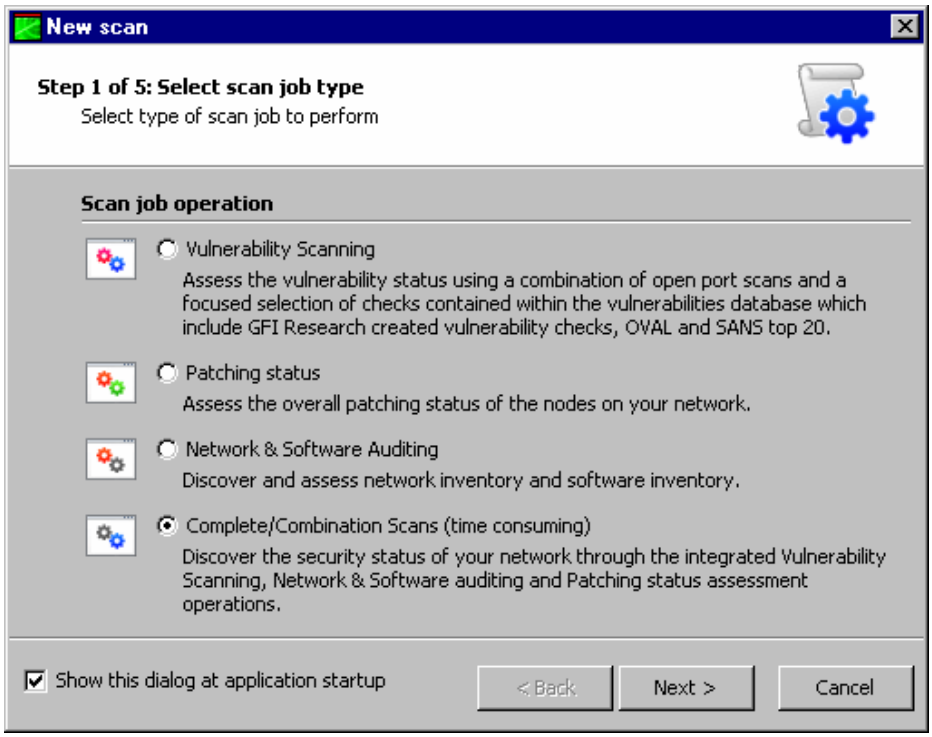
Out of the box, GFI LANguard N.S.S. includes default configuration settings that allow you to run immediate scans soon after the installation is complete.

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

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

To perform your first scan, do as follows:

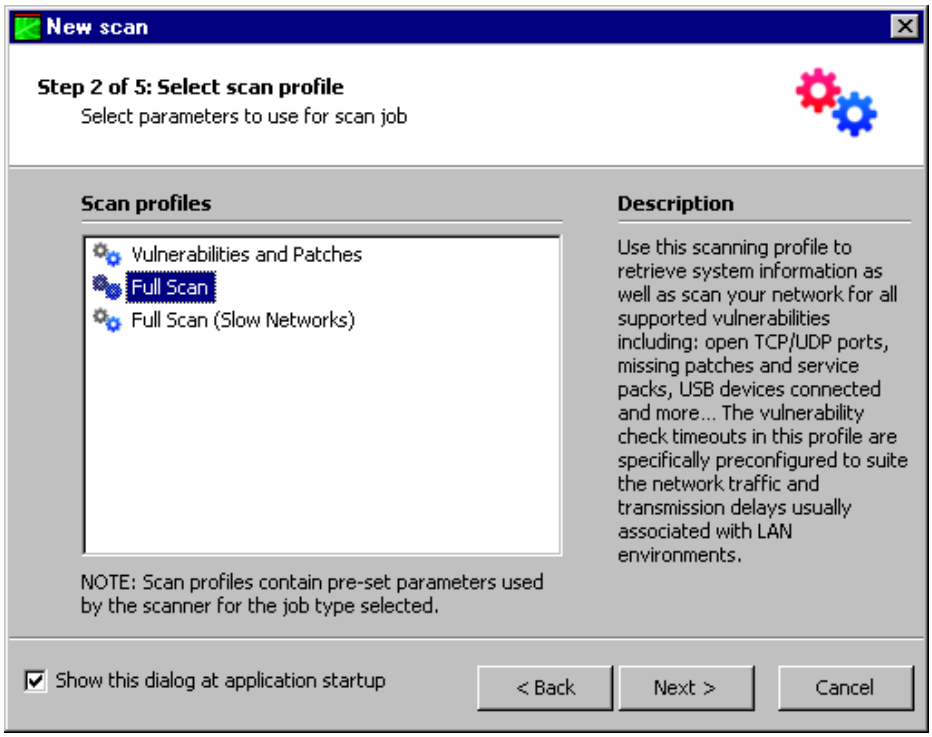
1. Click on **New Scan…** button



Screenshot 13 - Selecting the type of security scan

2. Select one of the following scanning operations and click **Next**:

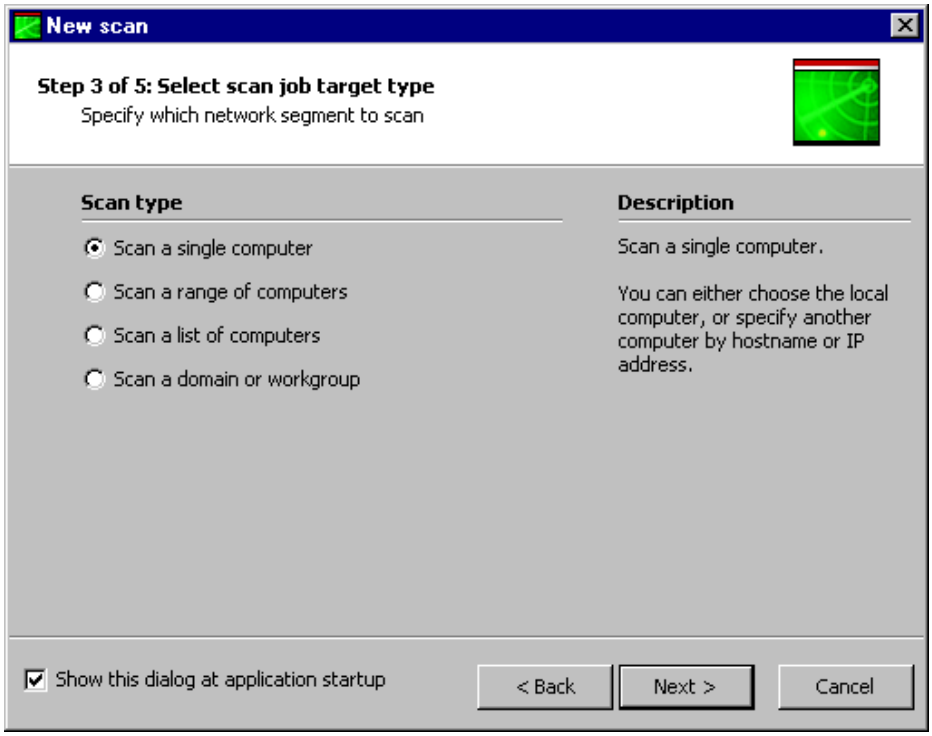
- *'Vulnerability Scanning'* – Use this scanning operation to enumerate all the vulnerabilities present on target computers including missing patches.
- *'Patching status'* – Use this scanning operation to enumerate only missing patches on target computers.
- *'Network and Software Auditing'* – Use this scanning operation to enumerate system information without including vulnerabilities and missing patches.
- *'Complete/Combination scan'* – Use this scanning operation to retrieve system information and enumerate all vulnerabilities including missing patches.



Screenshot 14 - Choose the scanning profile

3. Select the required scanning profile and click **Next**.

NOTE: For a detailed description of what each individual scanning profile does please refer to the "*Scanning profile description*" section in the Scanning Profiles chapter in this document.

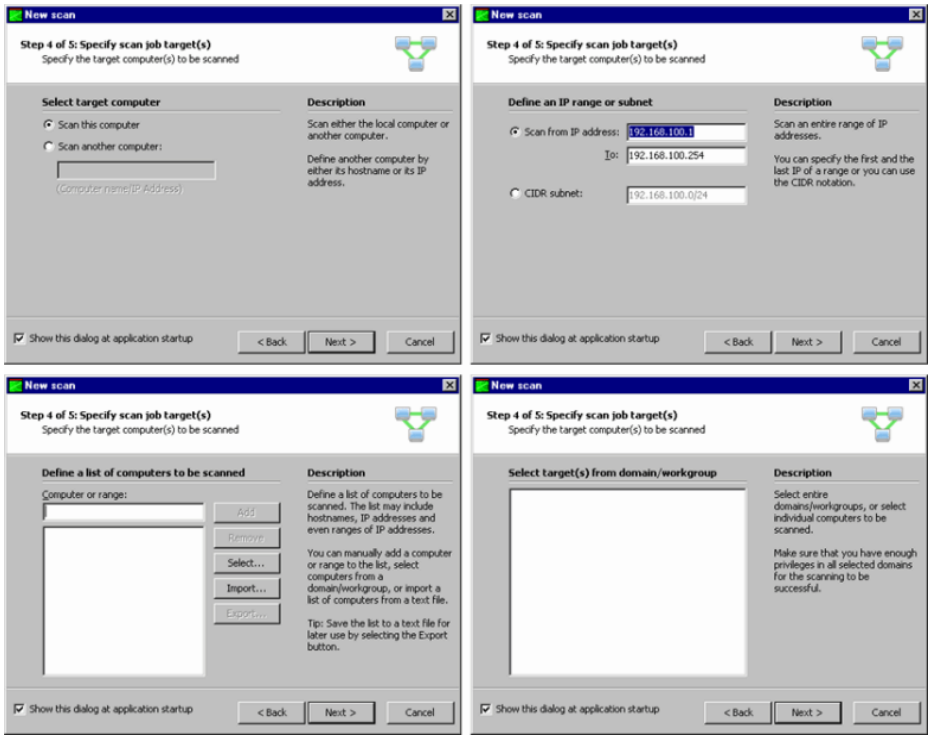


Screenshot 15 - Selecting scan range

4. Select one of the following scan target types and click **Next**:

- *'Scan single computer…'* – Select this option to scan a single computer.

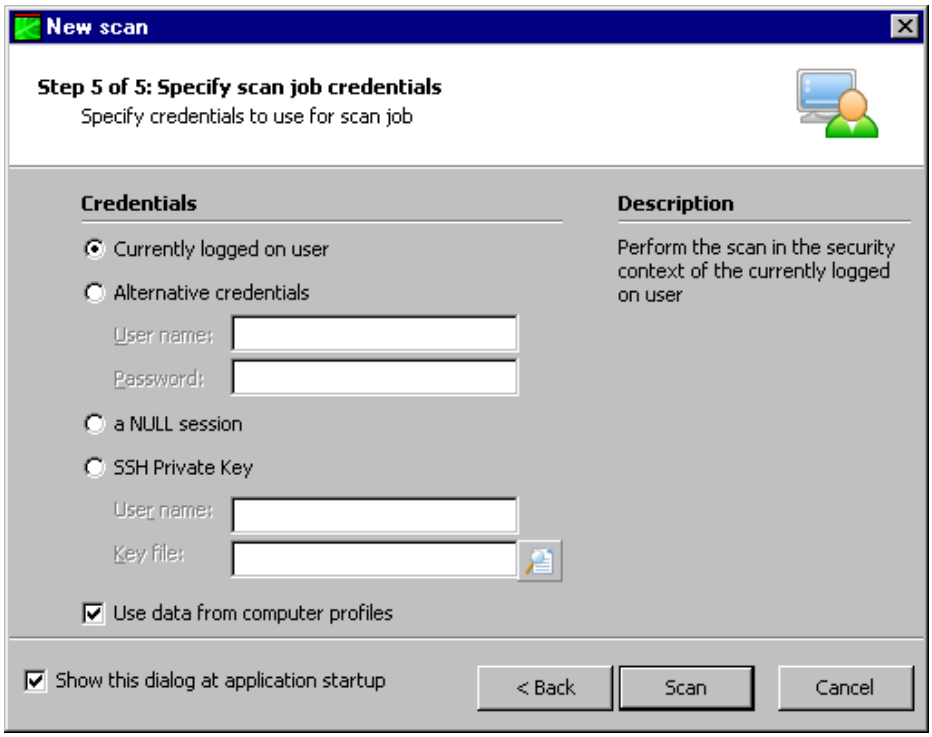
- *'Scan range of Computers…'* – Select this option to scan a specific range of computers.
- *'Scan list of Computers…'* – Select this option to scan a custom list of computers.
- *'Scan a Domain…'* – Select this option to scan an entire Windows domain.



Screenshot 16 - New Scan range options dialogs.

5. Specify scan target details (i.e. host name, IP, range of IPs or domain name) and click **Next**.

NOTE: When configuring IP ranges, GFI LANguard N.S.S. 8.0 also allows you to specify which IPs must be excluded from this range. For more information on this feature please refer to **Configuring scan ranges** section in this document.



Screenshot 17 - Specify the scan credentials

6. Specify the authentication details to be used during this scan. Click on the **Scan** button to initiate the scanning process.

Configuring scan ranges

GFI LANguard N.S.S. 8.0 provides enables you to configure ranges and exclusions to scan rages for IP addresses to scan. These are set up in the 'computer or range' field within the new scan wizard.

Scan ranges

Ranges are configured through the use of the '/' character. Though this character users can, for example, key in:

- 192.168.0.1/165

This will scan all the available addresses from 192.168.0.1 to 192.168.0.165.

Scan range exclusions

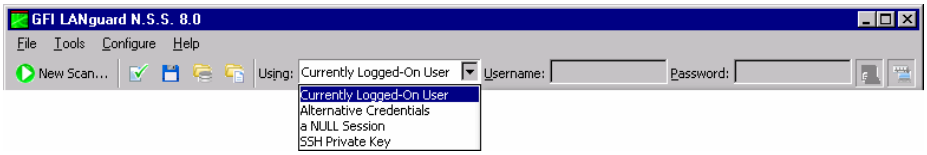
Scan range exclusions are configured through the use of the '+' and '-' characters. Ex:

- +192.168.0.1/165
- -192.168.0.13

In the example above all the available computers which IP address is in the 192.168.0.1 to 192.168.0.165 range will be scanned, except for 192.168.0.13. which will be excluded.

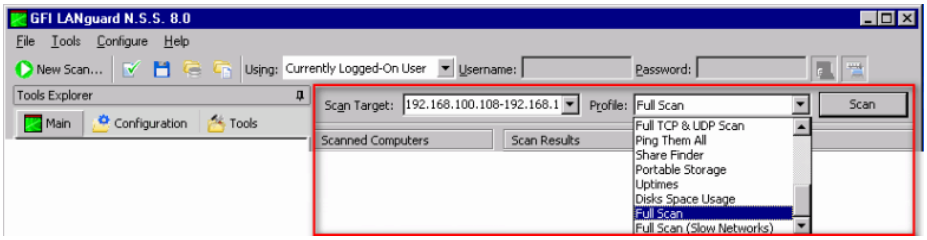
Quick-start scans using currently logged on user credentials

You can trigger network vulnerability scans directly from the toolbar without having to perform major configurations as well as without bringing up the new scan wizard. To achieve this:



Screenshot 18 - GFI LANguard N.S.S. new scan toolbar

1. From credentials drop-down list provided in the toolbar select the **Currently logged on user** option.



Screenshot 19 - GFI LANguard N.S.S. target details toolbar

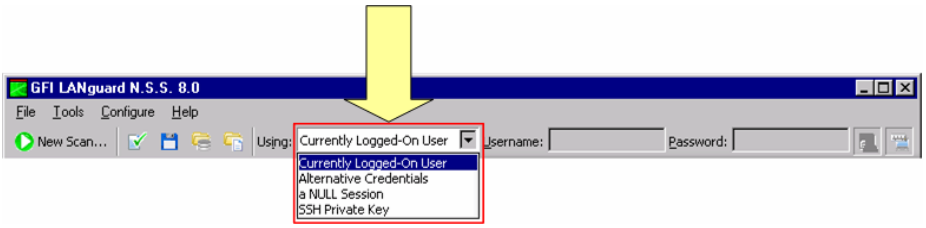
2. In 'Scan Target' drop down, specify the targets to be scanned using these credentials (for example, TMJason, 130.12.1.20-130.12.1.30, etc.).

3. From the 'Profile' drop down select the scanning profile to be used for this network vulnerability scan.

4. Click on **Scan** to initiate the scanning process.

Quick-start scans using alternative logon credentials

To run a network security audit using alternative logon credentials:



Screenshot 20 - GFI LANguard N.S.S. new scan toolbar: Authentication methods drop down list

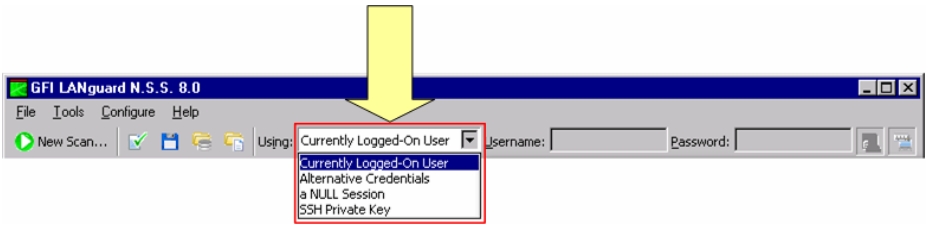
1. From credentials drop-down list provided in the toolbar select the **Alternative credentials** option.

2. In the adjacent fields specify the username and password to be used during this scan.

3. Configure the rest of the options as described in the 'Quick-start scans using currently logged on user credentials' section above.

Quick start scans using SSH Private Key

To run a network security audit using SSH Private key credentials do as follows:



Screenshot 21 - GFI LANguard N.S.S. new scan toolbar: Authentication methods drop down list

1. From credentials drop-down list provided in the toolbar select the **SSH Private key** option.

2. In the adjacent fields specify the username and private key file to be used during this scan.

3. Configure the rest of the options as described in the 'Quick-start scans using alternative credentials' section above.

Quick-start scans using a null session

One of the most serious threats in a network system is the misconfiguration of passwords. Default passwords or even worse blank password (technically referred to as 'null' passwords) are a big vulnerability because they could easily allow malicious users to gain access to your system without any considerable effort. GFI LANguard N.S.S. allows you to specifically verify whether your target computers have null passwords through a 'null session'. During null sessions, the scanning engine will attempt to logon to a target computer with blank credentials. The benefit of such an exercise is that is such a scan is successful, it means your target is accessible without the need of logon credentials. To run a null session:

1. From credentials drop-down list provided in the toolbar select the **Null Session** option.

2. In 'Scan Target' drop down, specify the targets to be scanned during this null session.

3. From the 'Profile' drop down select the scanning profile to be used during this network vulnerability scan.

4. Click on **Scan** to initiate the scanning process.

5. Getting started: Analyzing the security scan results

Introduction

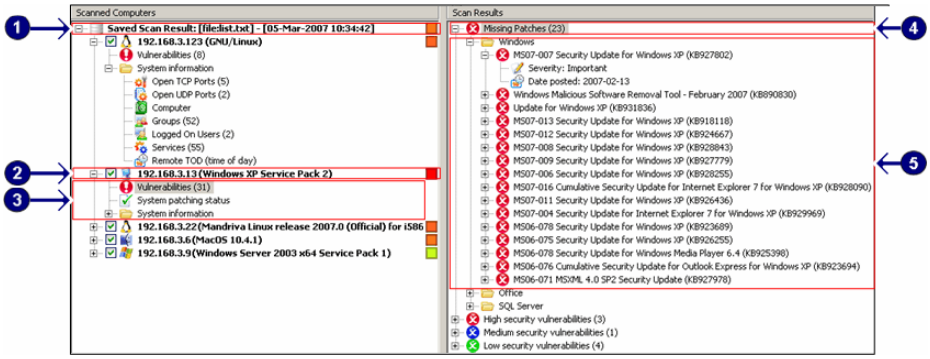
The most important thing following a network security scan is identifying which areas and systems require your immediate attention. This is achieved by analyzing and correctly interpreting the information collected and generated during a network security scan.

This chapter is entirely focused on this aspect and will guide you through the steps required to:

1. Access the vulnerability scan results
2. Analyze and interpret the scan data/results
3. Identify what to do after that a network scan is completed.

Scan results

GFI LANguard N.S.S. 8.0 displays scan results in the scan results window. You can navigate the scan results by clicking on the nodes displayed in the scanned computers pane (middle pane). This causes the scan results to change dynamically from one computer to the next and from one detailed information display to the next.



Screenshot 22 - Scan Results

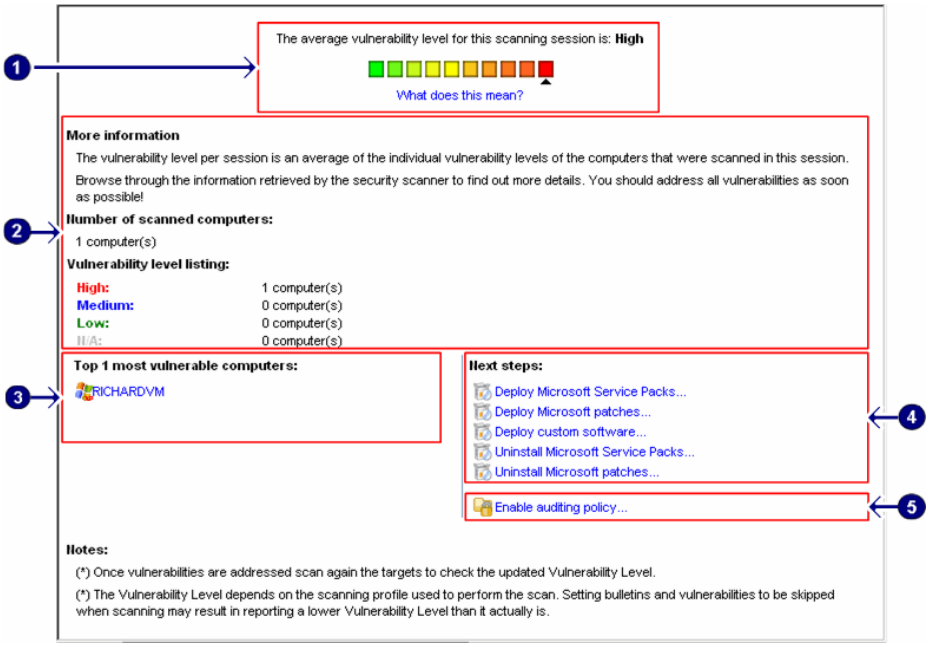
The information included in the results pane includes:

1	**Scan target node:** Displays information related to scan targets in terms of scan range and if scan result was retrieved from database.
2	**Scan computer node:** Displays information related to scanned computer. This includes if scan was successful and O/S details.
3	**Scan details node:** Displays information related to the scan performed on target computer. This includes number of vulnerabilities found, system patching status, etc.
4	**Scan results node:** Displays the results of the scans carried out for specific computers.
5	**Scan results details:** Displays the details of the scan results. This includes vulnerability or missing patch name, level of patch/vulnerability, detailed vulnerability/missing patch details, connected device information, etc.

Analyzing the summary scan results for the scanned network

Clicking on the scan target node displays a graphical representation of the total network vulnerability level. This is an automated (combined) interpretation of the scan results obtained following the successful scanning of one or more network computers.

In addition, to the network vulnerability level, GFI LANguard N.S.S. 8 also provides guidelines on how to resolve the weaknesses discovered during vulnerability scanning.



Screenshot 23 - Results Pane

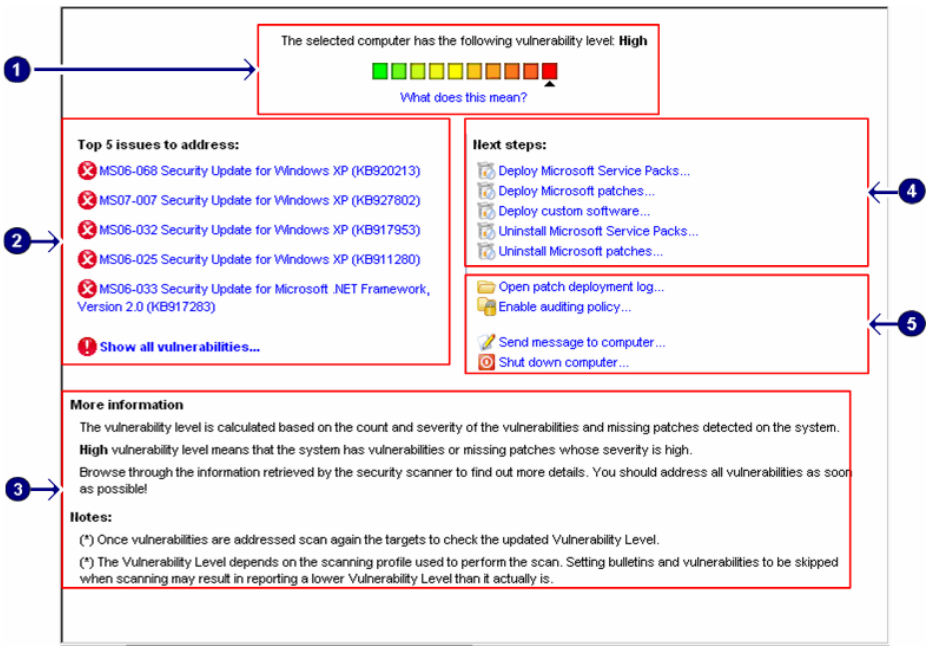
The information included in the results pane includes:

1	A graphical measurement based on a weighted sum of the vulnerabilities detected in the last scan.
2	Scan details as well as a description of the current network vulnerability level.
3	The top 5 most vulnerable computers.
4	Links to tasks that assist you in fixing vulnerabilities discovered during scans.
5	Links through which you can enable/configure auditing policies.

Analyzing the target computer scan summary

Clicking on the target-computer node will display a graphical representation of its vulnerability level. This is an automated interpretation of the scan results obtained following the successful scanning of that particular target computer.

In addition, to the vulnerability level, GFI LANguard N.S.S. 8 also provides guidelines on how to resolve the weaknesses discovered during vulnerability scanning.



Screenshot 24 – Results Pane

The information included in the results pane includes:

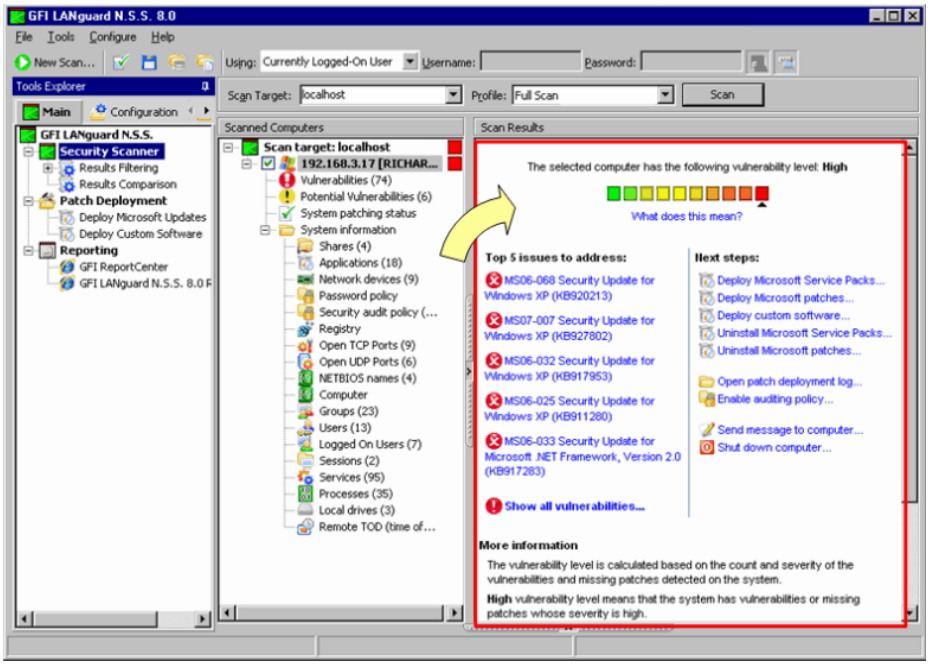
1	A graphical measurement based on a weighted sum of the vulnerabilities detected in the last scan.
2	The top 5 issues to address in order to fix the vulnerabilities discovered during the scan for that specific computer. Click on any of the listed issues to access the respective bulletin information.
3	More information related to the results pane information displayed.
4	Links to tasks with which you can fix weaknesses and vulnerabilities discovered.
5	Additional options through which you can view and enable policies as well as send administration messages and shutdown computers.

What to do after a scan

The scan results summary of GFI LANguard N.S.S. includes a list of common tasks/recommended actions which can assist you in resolving network weaknesses commonly discovered during vulnerability scans. Suggested actions include:

- **Deploy service packs/patches** – Use these options to resolve issues that require the download and deployment of missing Microsoft patches and service packs. Clicking on any of these options will take you to the patch/service pack management options from where you can download and automatically deploy patches and service packs network-wide. For more information on how to use these options refer to the 'Patch management: Deploying Microsoft updates' chapter
- **Deployment custom software** – Use this option to deploy scripts, files or third party applications network-wide. For more information on how to achieve this refer to the 'Patch management: Deploying custom software' chapter.
- **Uninstall service packs or patches** – Use these options to resolve issues that require uninstall of service packs or patches previously deployed on network computers.
- **Enable Auditing Policy** – Use this option to resolve vulnerabilities related to the wrong configuration of Microsoft auditing policies. Clicking on this option will launch the GFI LANguard N.S.S. Auditing Policies Administrative Support Wizard through which you can configure auditing policies on your target computers.

Analyzing the detailed scan results



Screenshot 25 - 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 sub-

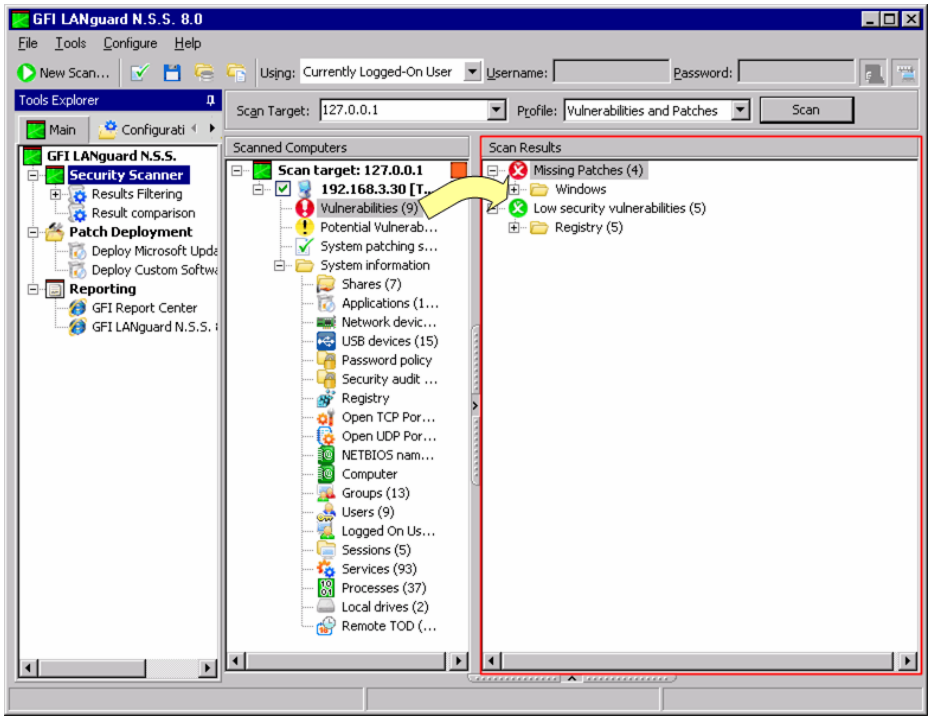
nodes. These can be easily used to investigate and identify security issues in the scanned targets.

Scan results are organized in the following categories:

- Vulnerabilities
- Potential vulnerabilities
- System Patching Status
- Shares
- Applications
- Network devices
- USB devices
- Password policy
- Security audit policy
- Registry
- Open TCP ports
- Open UDP ports
- System patching status
- NETBIOS names
- Computer
- Groups
- Users
- Logged on users
- Sessions
- Services
- Processes
- Local drives.
- Remote time of day (TOD)

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.

Detailed scan results: Analyzing Vulnerabilities



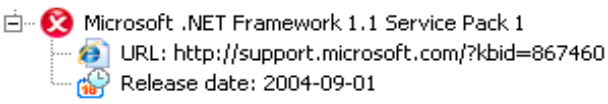
Screenshot 26 - The Vulnerabilities node

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

- Missing service packs
- Missing patches
- High security vulnerabilities
- Medium security vulnerabilities
- Low 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 Microsoft Corporation.



Screenshot 27 - Missing Service Packs results tree

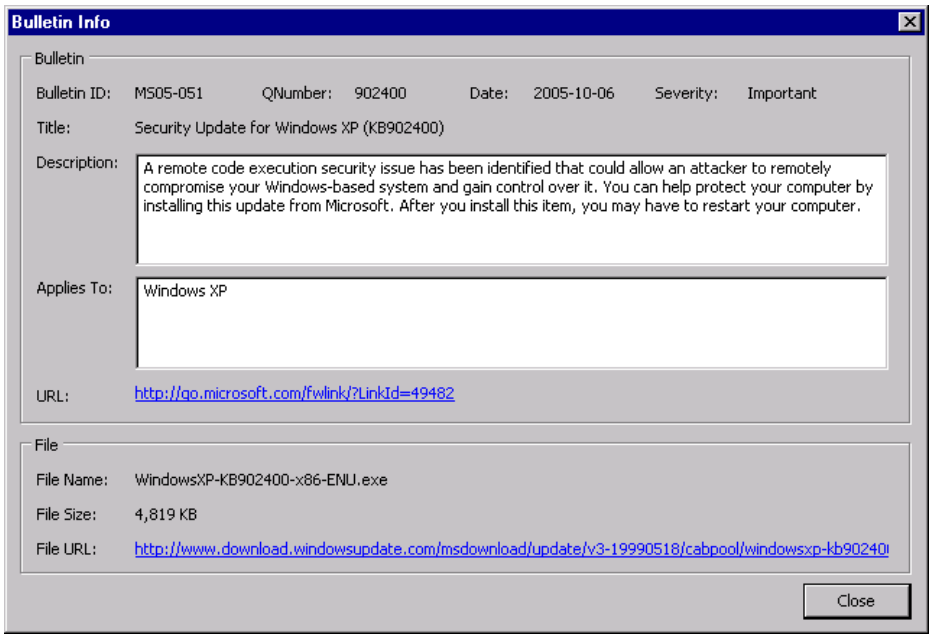
NOTE: GFI LANguard N.S.S. can identify missing patches and service packs on various Microsoft products. For a complete list of supported products visit: http://kbase.gfi.com/showarticle.asp?id=KBID001820.

Details listed under the results tree of the 'Missing Service Packs' category include the:

- *'Product name'* and *'Service Pack Number'.*
- *'URL:'* - The URL link to support articles related to the missing service pack.
- *'Release date:'* - The date when the reported service pack was released.

Bulletin information

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



Screenshot 28 - Missing Service pack: Bulletin info dialog

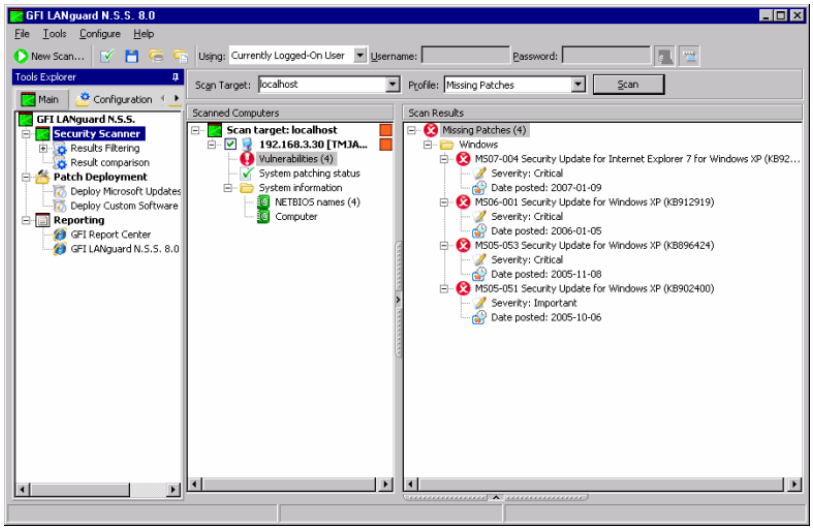
This will bring up the 'Bulletin Info' dialog of the respective service pack. The information shown in this bulletin includes:

- The QNumber. This is a unique ID number that 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 that 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 install missing patches on network computers makes 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.



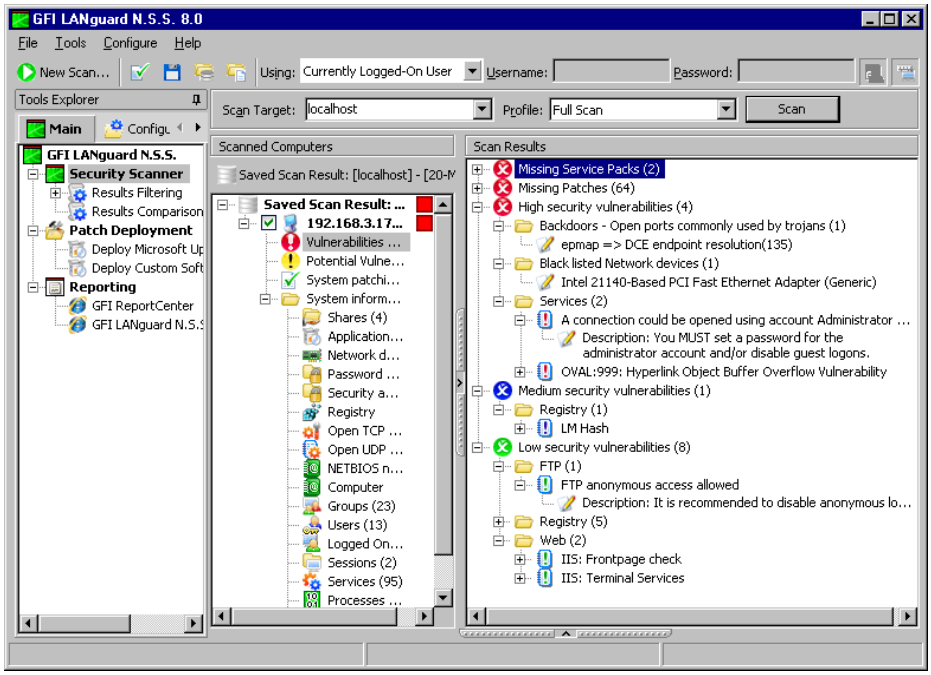
Screenshot 29 - Missing patches detected during target scanning

Missing patches discovered during target scanning are listed and grouped under the 'Missing Patches' category. Details shown in results tree of this category include:

- *'Patch ID'* and *'Product name'*.
- *'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.
- *'Date Posted:'* - The release date of the missing patch.

To access bulletin information right-click on the respective patch and select **More details ▸ Bulletin Info**.

Vulnerabilities ▸ High, medium, low security vulnerabilities



Screenshot 30 - 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 10 groups:

- Mail
- FTP
- Web
- Registry
- Services
- RPC
- DNS
- Software
- Rootkit
- Miscellaneous

The content of each group is described below:

Mail, FTP, RPC, DNS and Miscellaneous – These groups contains the vulnerabilities discovered on 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.

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

o *'Vulnerability check name'* (for example, Imported_IIS: FrontPage Check)

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

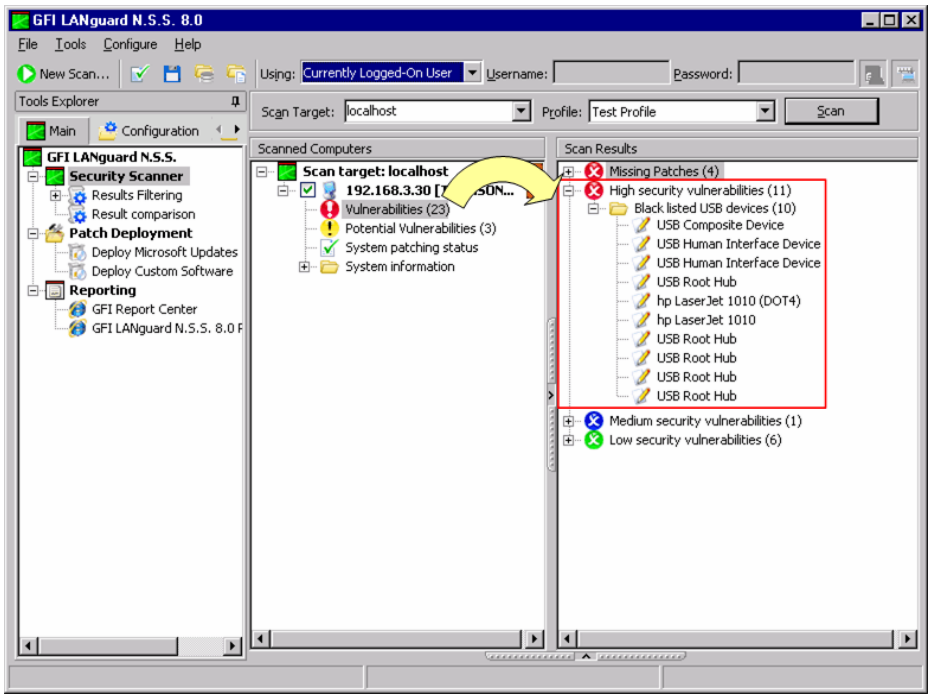
Services – This group contains vulnerabilities discovered in active services as well as the list of unused accounts that are still active and accessible on scanned targets.

Registry – This group contains 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.

Software – This group contains vulnerabilities found in software installed on the scanned network device(s). The details shown in this category include links to supporting documentation as well as a short description of the vulnerability.

Rootkit – This group includes details of vulnerabilities discovered as a result of having a rootkit installed on the scanned network device(s). The details shown in this category include links to supporting documentation as well as a short description of the vulnerability.

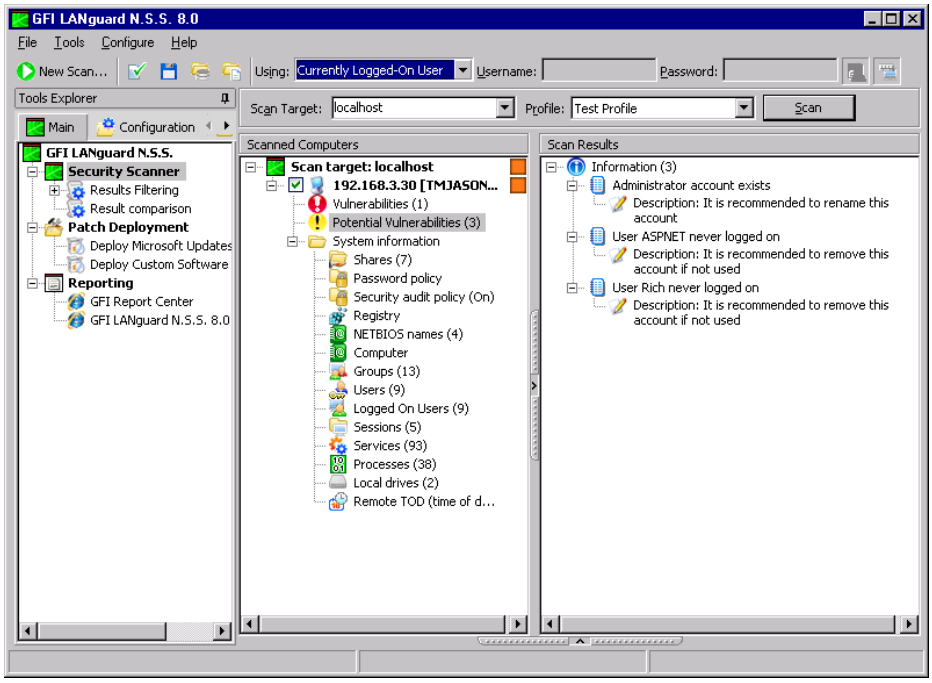
Reporting unauthorized devices as high security vulnerabilities



Screenshot 31 - 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.

Detailed scan results: Analyzing potential vulnerabilities



Screenshot 32 - Potential vulnerabilities node

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

For example, during vulnerability scanning GFI LANguard N.S.S. will enumerate all of the modems that are installed and configured on the target computer. If unused these modems are of no threat to your network, however if connected to a telephone line these modems can be used to gain unauthorized and unmonitored access to the Internet. In practice this means that users can bypass corporate perimeter security including firewalls, anti-virus, website rating and web content blocking exposing the corporate IT infrastructure to a multitude of threats including hacker attacks.

As a result, GFI LANguard N.S.S. considers installed modems as possible threats and enumerates them in the 'Potential Vulnerability' sub-node for your attention and analysis.

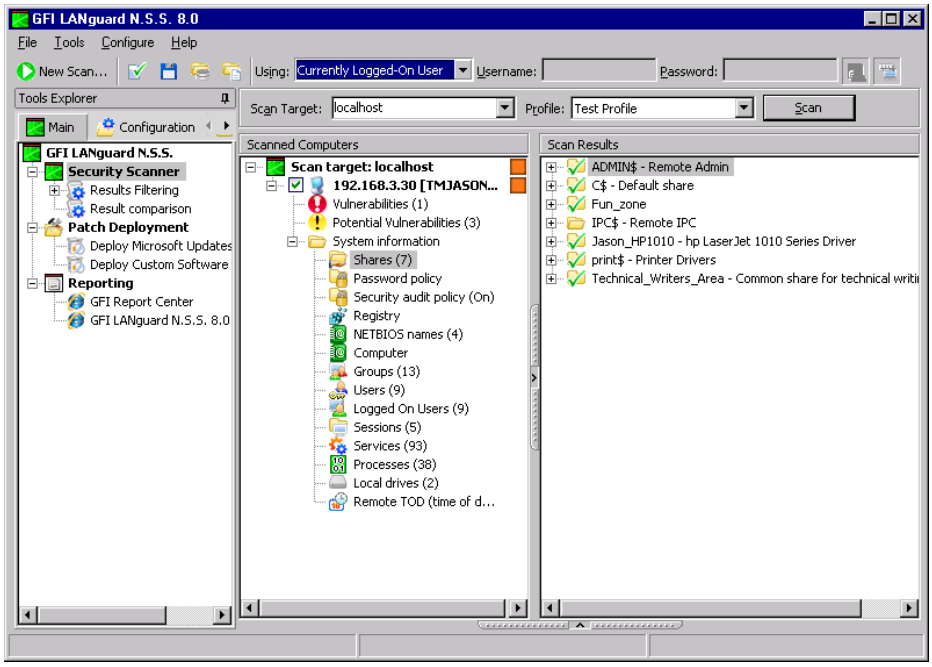
Detailed scan results: Analyzing shares

In the wild, there is malicious software (e.g. worms and viruses such as Klez, Bugbear, Elkern and Lovgate) that can spread out and infect entire systems through open shares that are available on network computers.

Handling open shares

GFI LANguard N.S.S. 8 is able to identify open shares present on network computers and enumerate them in the scan results for your

attention and analysis. To access the list of open shares discovered on a target computer, click on the **Shares** sub-node.



Screenshot 33 - Shares node

Through the details provided in the **Shares** sub-node you can identify:

1. Users sharing entire hard-drives.

2. Shares that have weak or incorrectly configured access permissions e.g. shares that can be accessed without the need for authentication.

3. Startup folders and similar system files that are accessible by unauthorized users or through user accounts that don't have administrator privileges but are yet allowed to execute code on target computers.

4. Unnecessary or unused shares.

For every open share detected GFI LANguard N.S.S. collects and enumerates the following information in the scan results:

- Share name
- Share remark (extra details on the share)
- Folder which is being shared on the target computer
- Share permissions and access rights
- NTFS permissions and access rights.

Handling administrative shares

Every Windows computer has administrative shares (C$, D$, E$ etc.) which GFI LANguard N.S.S. will by default enumerate during target computer scanning.

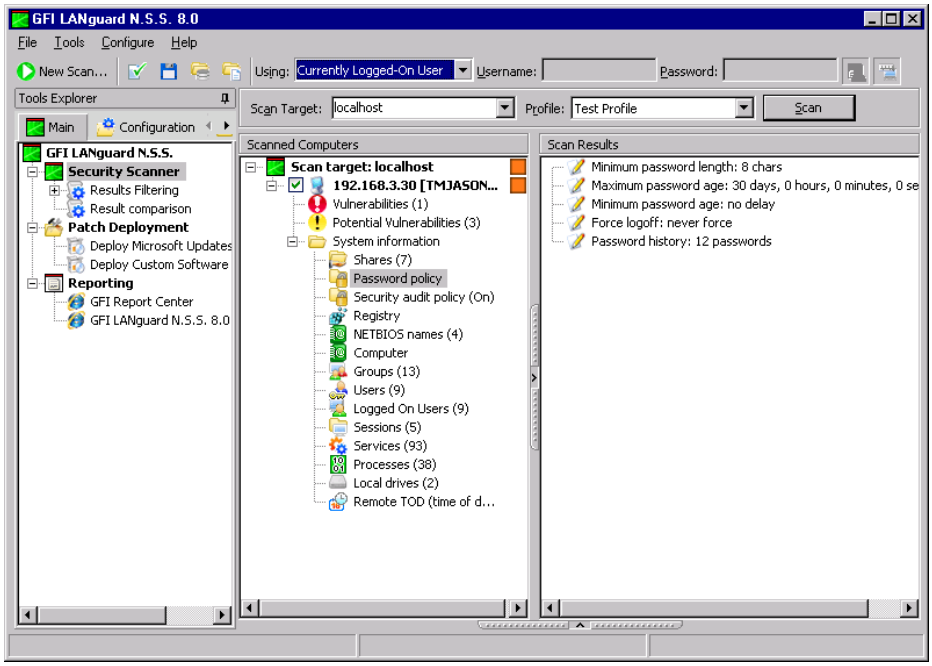
As these can become irrelevant to your security audit you can configure GFI LANguard N.S.S. not to report such administrative shares. For more information on how to achieve this refer to the

'Customizing OS Data Retrieval parameters' section in the *'Scanning Profiles'* chapter.

Detailed scan results: Analyzing password policy

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. These include account lockout control and password strength enforcement policies which if correctly configured make it very difficult for an attacker to crack user/logon credentials.

Typical vulnerabilities in an IT infrastructure are the result of incorrectly configured lockout control and password strength enforcement policies. These include default passwords and weak passwords that are made up of few characters or which are identical to the respective username.



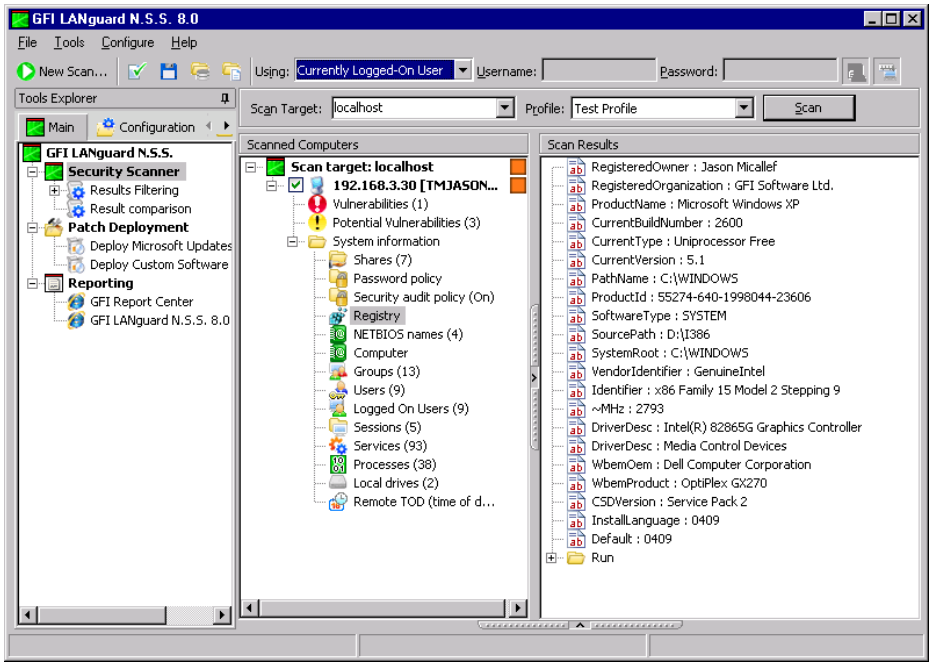
Screenshot 34 - Password policy node

GFI LANguard N.S.S. helps you identify misconfiguration in your password policies by collecting the password policy settings currently configured on target computers and including them as part of the scan results. This way you avoid the need of having to physically check these out on the respective machines. To access the password policy settings collected during a scan click on the **Password Policy** sub-node.

Detailed scan results: Analyzing registry settings

The registry is one of the most delicate parts of Windows-based operating systems since it coordinates the various hardware and software blocks of a system. It is quite obvious that in order to keep up with its task, the registry must store key information. These include hardware and software settings such as which drivers and applications will be automatically launched at system startup.

The registry's prominent role within a Windows-based system makes a primary target for all hackers and malicious users. Just by gaining access to the registry settings, a crafty hacker could enable malicious software such as Trojans to automatically run at every program start-up. This way he would be able to gain backdoor access to a system unnoticed.



Screenshot 35 - Registry node

GFI LANguard N.S.S. helps you identify foul play in your registry by collecting the registry settings from all scanned computers and making them available for you to analyze from a centralized location. To access the registry settings collected during a scan, click on the **Registry** sub-node.

For example, by examining the values in the **Run** folder which is included by default in the scan results, you can identify which programs are set to automatically run at system startup. This way you can identify any type of software that is automatically run without your express instruction.

Detailed scan results: Analyzing security audit policy settings

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 breaches. Identifying attempts and preventing them from becoming successful breaches of your system security is critical. In Windows, you can use 'Group Policies' to set up an audit policy that can track user activities or system events in specific logs.

In order to help you keep track of your system's auditing policy GFI LANguard N.S.S. collects the security audit policy settings from scanned target computers and includes in the scan results. This information is accessed by click on the **Security Audit Policy** sub-node.

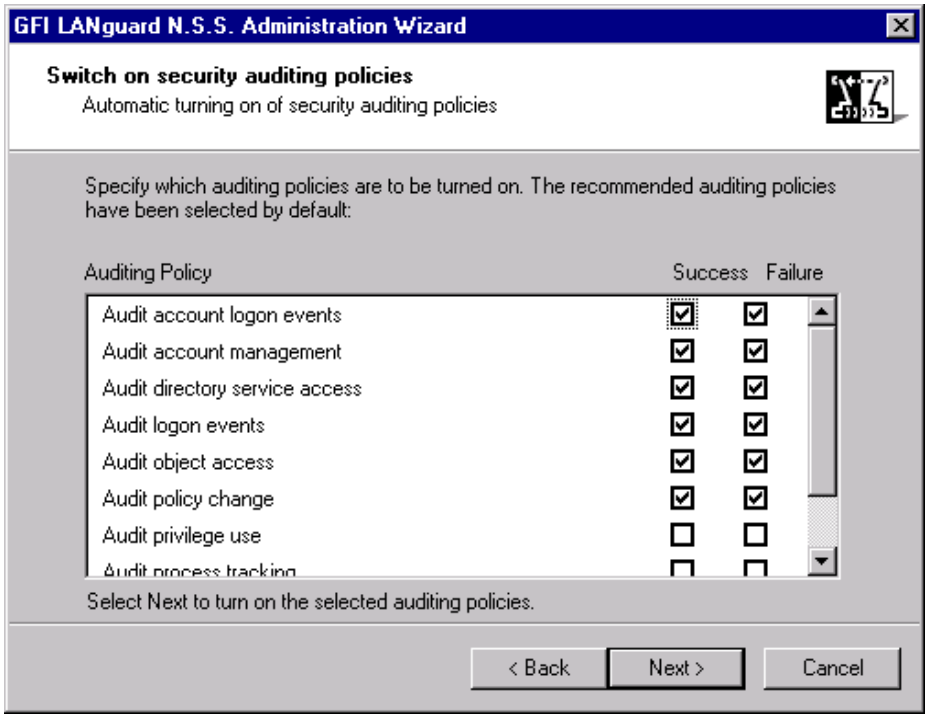
NOTE: GFI recommends that you set up the audit policy settings of your network computers as follows:

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

Apart from gaining knowledge on the current audit policy settings, you can also use GFI LANguard N.S.S. 8 to access and modify the audit policy settings of your target computers. To achieve this:

1. From the 'Scanned Computers' (middle) pane, right-click on the respective target computer and select:

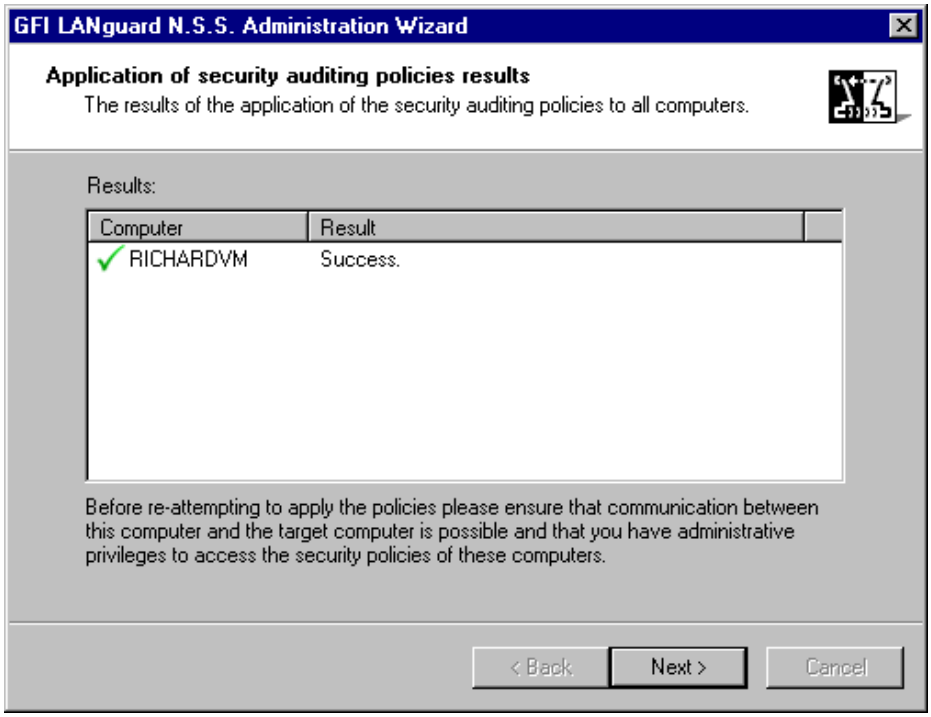
- **Enable auditing on ▸ This computer** to configure the audit policy settings of that particular computer.
- **Enable auditing on ▸ Selected computers** to configure the audit policy settings of multiple computers.
- **Enable auditing on ▸ All computers** to configure the audit policy settings of all scanned computers.



Screenshot 36 - 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(s). For example, to log successful events, select the *'Successful'* check box of the relevant

auditing policy. Click on **Next** to deploy the audit policy configuration settings on the target computer(s).



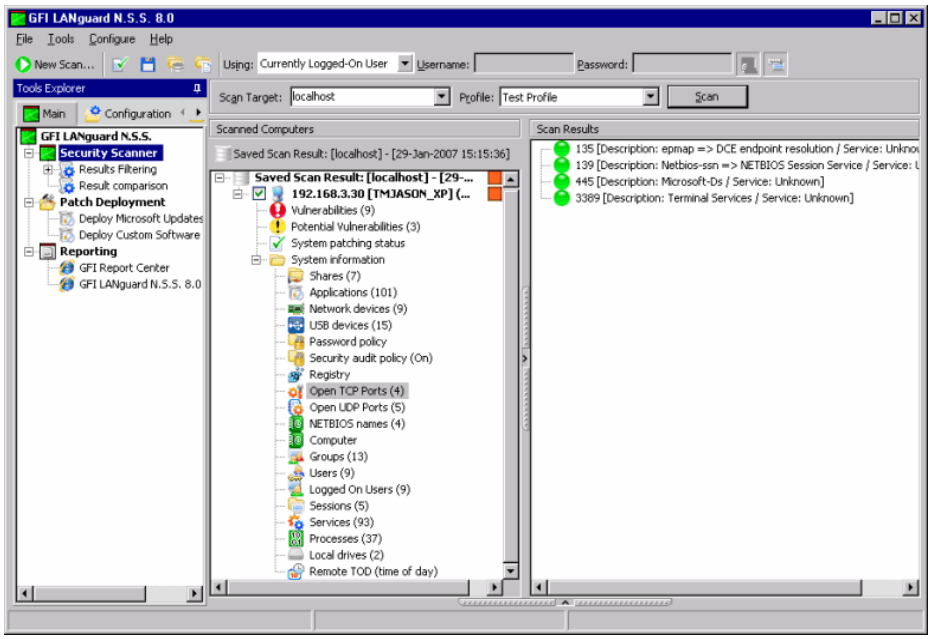
Screenshot 37 - Results dialog in audit policy wizard

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

4. Click **Finish** to finalize your settings and close the 'Audit Policy Administration Wizard'.

Detailed scan results: Analyzing open TCP ports

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



Screenshot 38 - Open TCP ports node

During vulnerability scanning GFI LANguard N.S.S. 8 will enumerate all TCP ports found open on a target computer. The list of ports is then accessible through the scan results by clicking on the **Open TCP Ports** sub-node.

Important considerations

By default GFI LANguard N.S.S. is configured to use the *'Full Scan'.* 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.

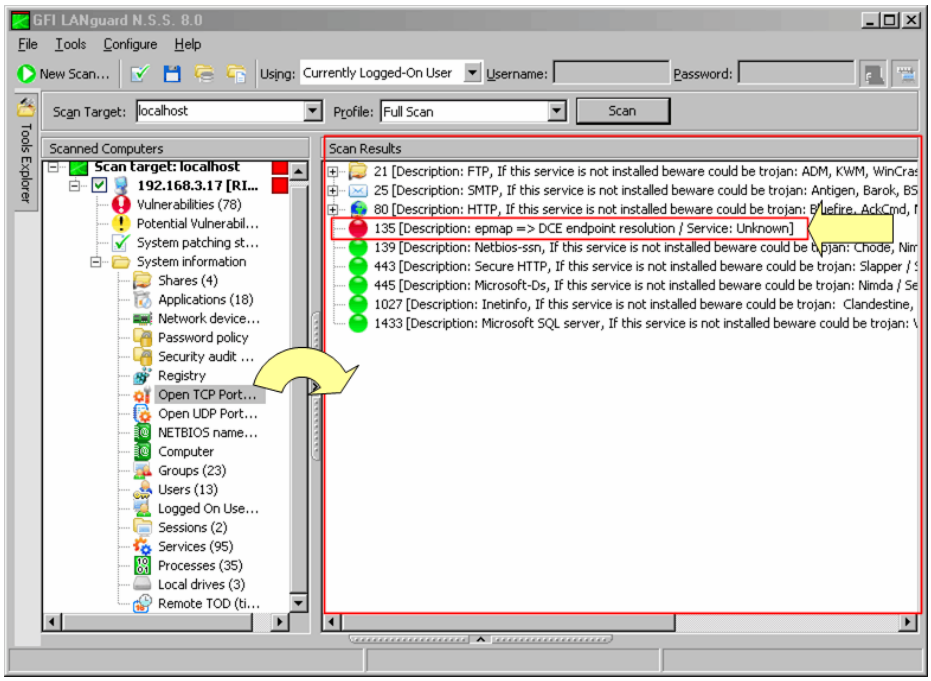
For more information on how to run security audits using different scanning profiles refer to the 'Scanning profiles in action' section in the 'Scanning Profiles' chapter in this manual.

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) that 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 39 - 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.

Detailed scan results: Analyzing users and groups

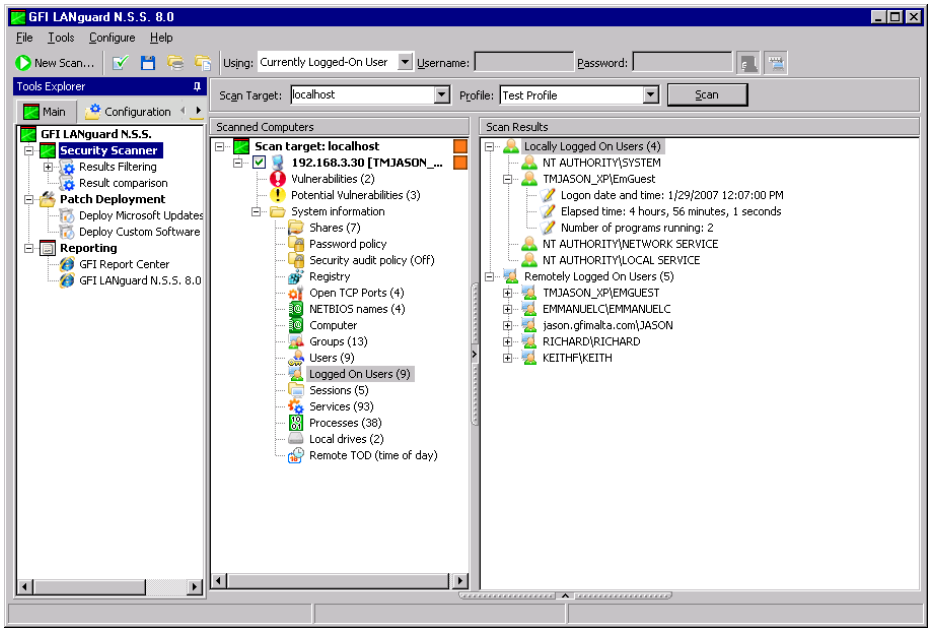
Rogue, obsolete or default user accounts can be exploited by malicious or unauthorized users to gain access to restricted areas of your IT infrastructure. The 'Guest' account for example is just one example of commonly exploited accounts – reason being that more often than not, this account is left configured within a system and even worse without changing the default password settings. Malicious users have developed applications which can automatically re-enable the 'Guest' account and grant it administrative rights; Empowering users to gain access to sensitive areas of the corporate IT infrastructure.

GFI LANguard N.S.S. collects information on all user accounts and user groups currently enabled on scanned targets. This information is organized in the scan results under 2 separated nodes. To access the list of user accounts identified during on a target computer, click on the **Users** sub-node. Use the information enumerated in this sub-node to inspect the access privileges assigned to each user account. To gain access to the list of user-groups configured on a target computer, click on the **Groups** sub-node.

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.

Detailed scan results: Analyzing logged on users

Click on the **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 40 - Logged on users node

The logged on user details enumerated by GFI LANguard N.S.S. includes:

- Logged on username.
- *'Logon date and time'* – The time and date when the user logged on the target computer.
- *'Elapsed time'* – How long the user has been logged on this computer.
- *'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).
- *'Open Files'* – How many files are opened the remote user's connection.
- *'Client type'* – The platform/operating system that the remote user used to connect to the target computer.
- *'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).

Detailed scan results: Analyzing services

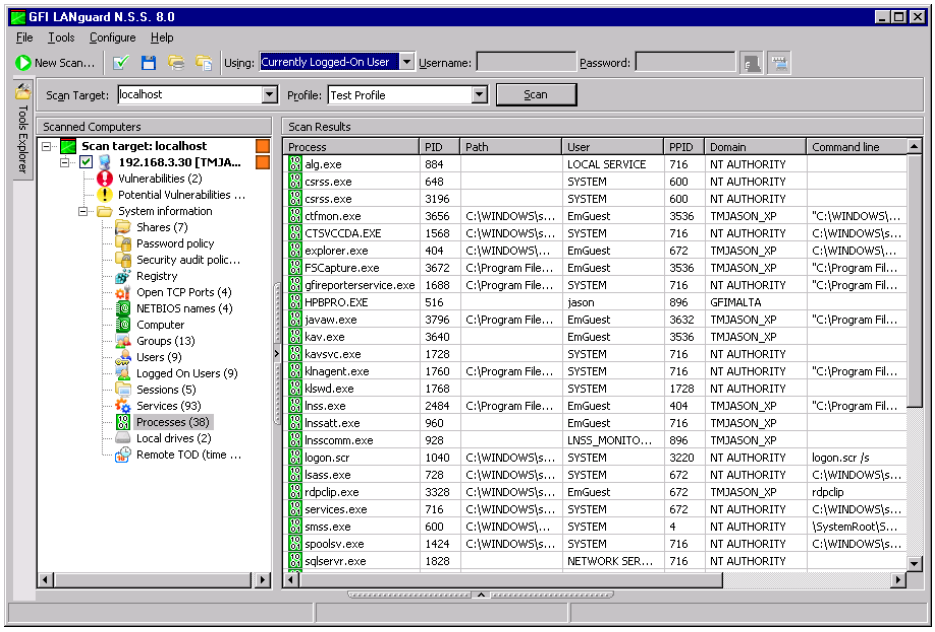
Active services can be a potential security weak spot in your network system. Any of these services can be a Trojan, a viruses or another type of malware which can seriously affect your system in a

dangerous way. Further more, unnecessary applications and services that are left running on a system consume valuable system resources.

During the scanning process, GFI LANguard N.S.S. enumerates all services running on a target computer for you to analyze. This way you can identify which services must be stopped. Further to the freeing up of resources, this exercise automatically hardens your network by reducing the entry points through which an attacker can penetrate into your system. To access the list of services enumerated during a scan, click on the **Services** sub-node.

Detailed scan results: Analyzing Processes

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

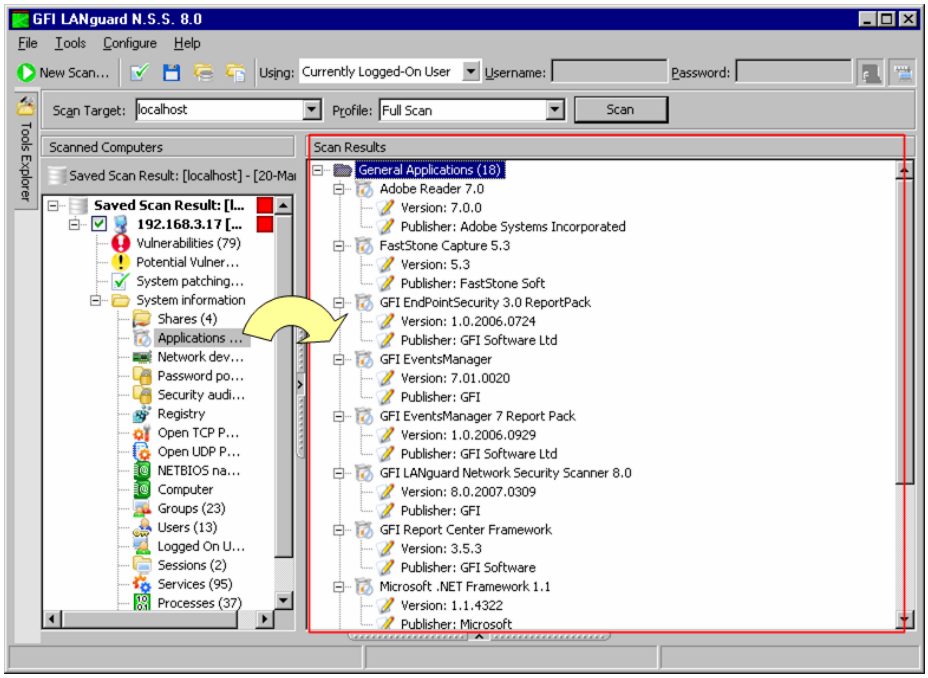


Screenshot 41 - List of running processes enumerated during a target scan

During security scanning, GFI LANguard N.S.S. harvests various information on active processes including:

- Process name
- Process ID (PID)
- Path
- User
- PPID
- Domain
- Command Line
- Handle Count
- Thread Count
- Priority.

Detailed scan results: Analyzing installed applications



Screenshot 42 - List of installed applications enumerated during target computer scanning

Click on the **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.

Anti-virus and Anti-spyware applications groups

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.*
- *'Real time protection:'* – Denotes if real time protection is enabled or disabled in an anti-virus application.
- *'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.
- *'Last update:'* – Shows the date and time of the last anti-virus/anti-spyware signatures update.
- *'Version:'* – Shows the version number of the security application.
- *'Publisher:'* – Shows the manufacturer details.

General applications group

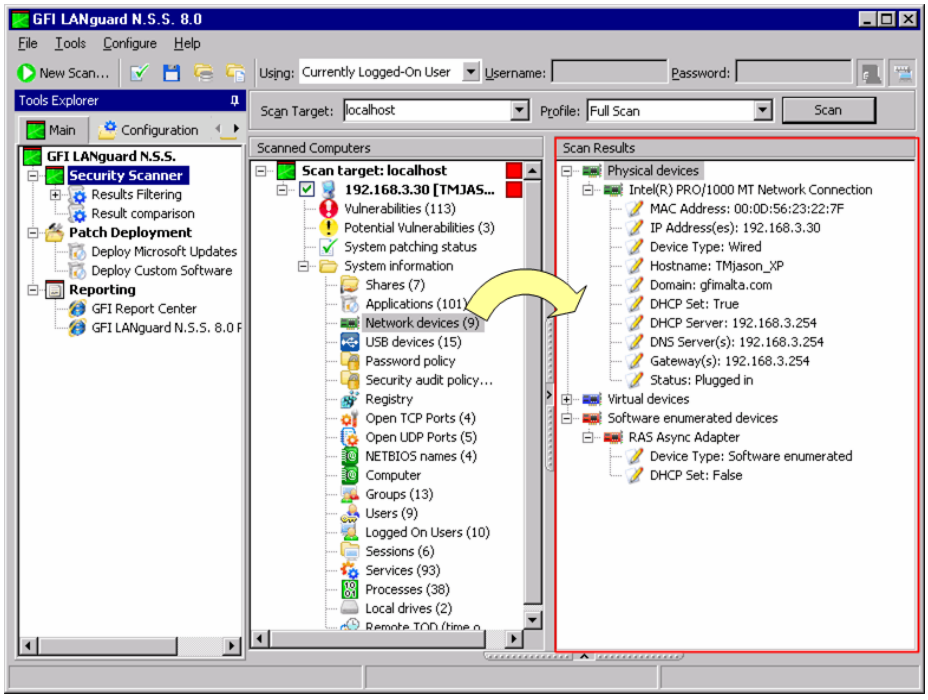
The **General applications** group contains the list of general purpose applications installed on a scanned target computer. These include all software programs, which are not classified as anti-virus or anti-spyware products such as Adobe Acrobat Reader and GFI LANguard N.S.S.

Details enumerated in the **General Applications** group include:

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

Detailed scan results: Analyzing network devices

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 43 - Network devices enumerated during a security scanning session

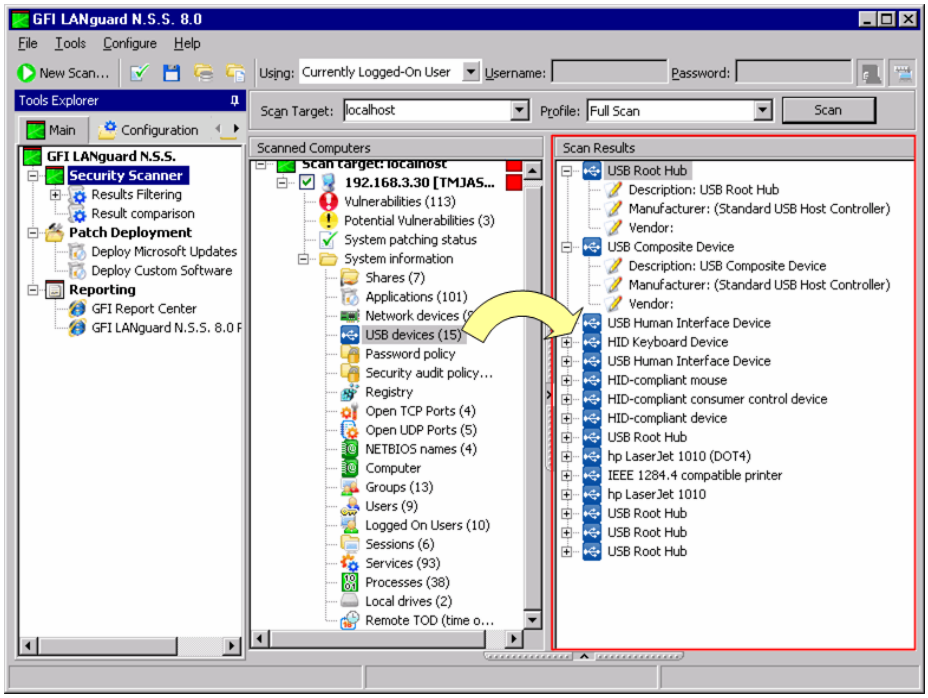
As parts of the vulnerability scanning process, GFI LANguard N.S.S. enumerates all hardware and software network devices including physical and wireless ones. To access this information click on the **Network Devices** sub-node. The information collected in this sub-node is grouped as follows:

- Physical devices (Wired)
- Wireless devices
- Virtual devices
- Software enumerated devices.

Each group includes various details about the device detected including:

- *MAC Address*
- *IP Address(es)*
- *Device Type*
- *Hostname*
- *Domain*
- *DHCP details*
- *WEP (were available)*
- *SSID (were available)*
- *Gateway*
- *Status.*

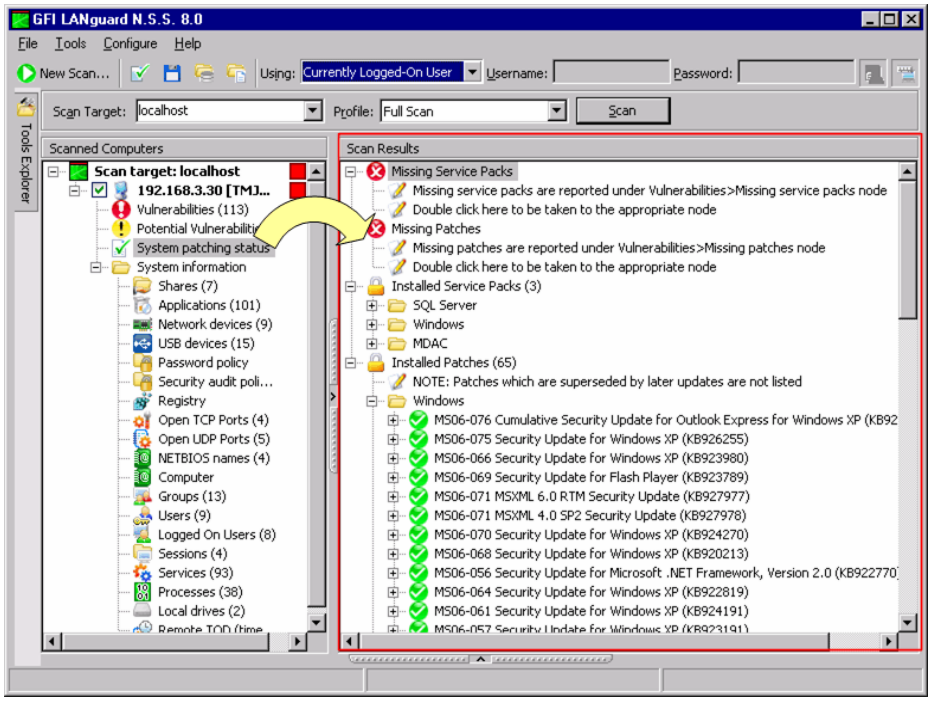
Detailed scan results: Analyzing USB devices



Screenshot 44 - List of USB devices detected on a scanned target computer

Click on the **USB Devices** 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 that are currently plugged into the scanned target computer(s) and which malicious insiders can use to steal valuable information or upload malicious files that can cripple your entire network. These include portable storage devices such as the Apple iPod, or Creative Zen as well as USB wireless devices and Bluetooth dongles.

Detailed scan results: Analyzing system hot fixes patching status



Screenshot 45 - The list of missing and installed patches enumerated during target computer scanning

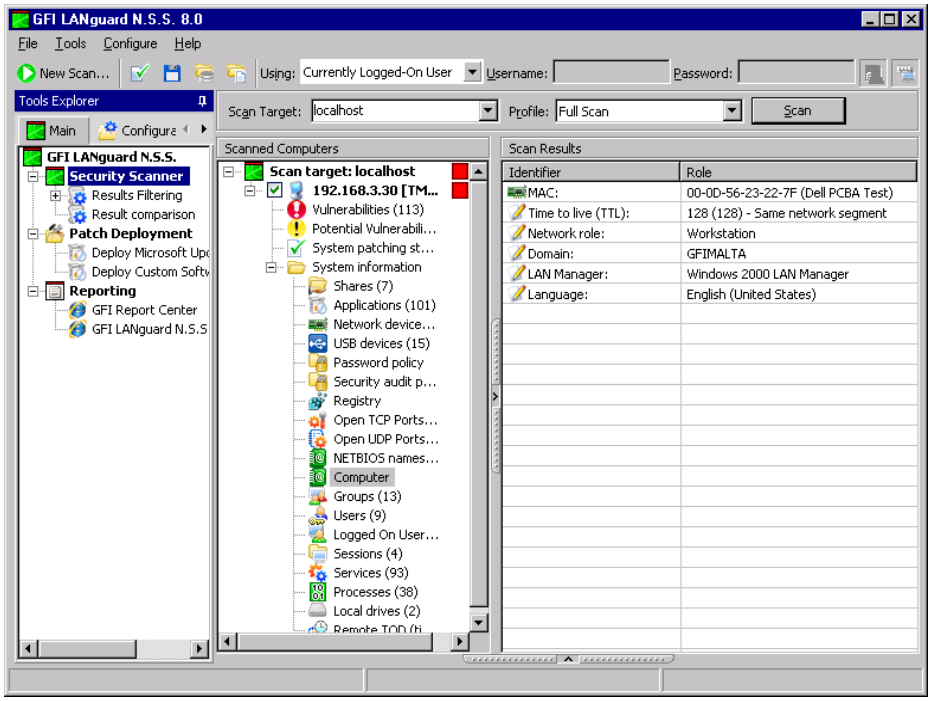
Click on the **System patching status** node for an overview of the patching status of a target computer.

Detailed scan results: Analyzing NETBIOS names

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 vulnerability scanning 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. To access NETBIOS details collected during a scan, click on the **NETBIOS names** sub-node.

Detailed scan results: Analyzing scanned target computer details

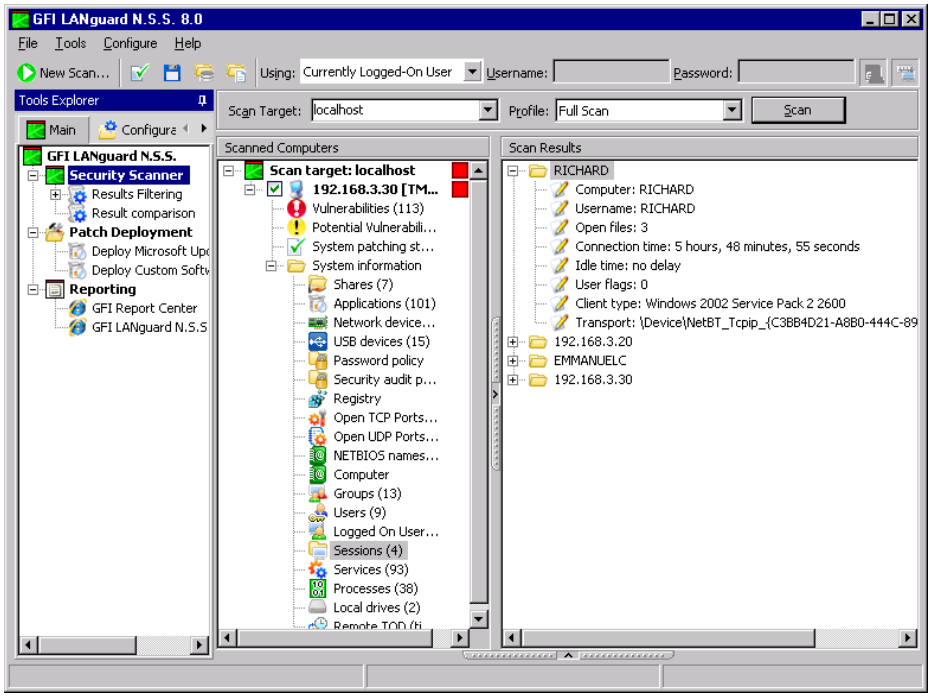


Screenshot 46 – Computer's node

Click on the **Computer** sub-node to access particular details about the scanned target computer including:

- '*MAC:*' – Shows the MAC address of the network card that the target computer is using to connect to the network.
- *'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.
- '*Network Role:*' – Denotes whether the scanned target computer is a workstation or a server.
- '*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.
- '*LAN Manager:*' – Shows the type of operating system and LAN Manager in use (for example, Windows 2000 LAN Manager).
- '*Language:*' – Shows the language setting configured on the scanned target computer (for example, English).

Detailed scan results: Analyzing sessions



Screenshot 47 – Session's node

Click on the **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.
- '*Username:'* – The logged on username.
- '*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.
- '*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.

Detailed scan results: Analyzing remote time of day

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

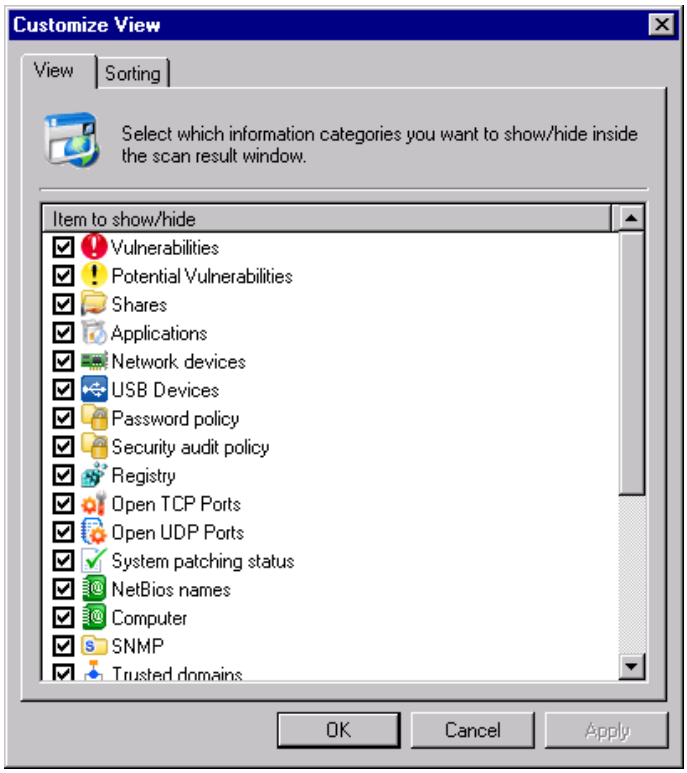
This time is generally set on network computers by the respective domain controller.

Detailed scan results: Analyzing 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.

Displaying and sorting scan categories

GFI LANguard N.S.S. 8.0 provides you with the ability to hone down and sort available scan categories and scanned computers. This allows you to focus on specific data that might require your attention in more detail without getting lost in other data that might not be relevant at that point in time.



Screenshot 48- Customize view

To customize and sort the list of scan results:

1. Click on the **Customize view** button.

2. From the **View** tab select which scan categories you want to show or hide. Click **Apply** to save setting.

3. Click on the **Sorting** tab and set your sorting preferences by selecting the required sorting options. Click **OK** to finalize your settings.

6. Saving and loading scan results

Introduction

Scan results are an invaluable source of information for systems administrators. GFI LANguard N.S.S. 8.0's results are stored in a MS-SQL Server or a MS-Access database and is exportable to a an XML format.

In this chapter you will discover how:

1. GFI LANguard N.S.S. 8.0 stores scan results

2. To modify scan results storage parameters e.g. the format in which scan results will be saved

3. To reload saved scan results data in the GFI LANguard N.S.S. 8 management console.

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. Nevertheless, you can also save these results to an external XML file. To achieve this:

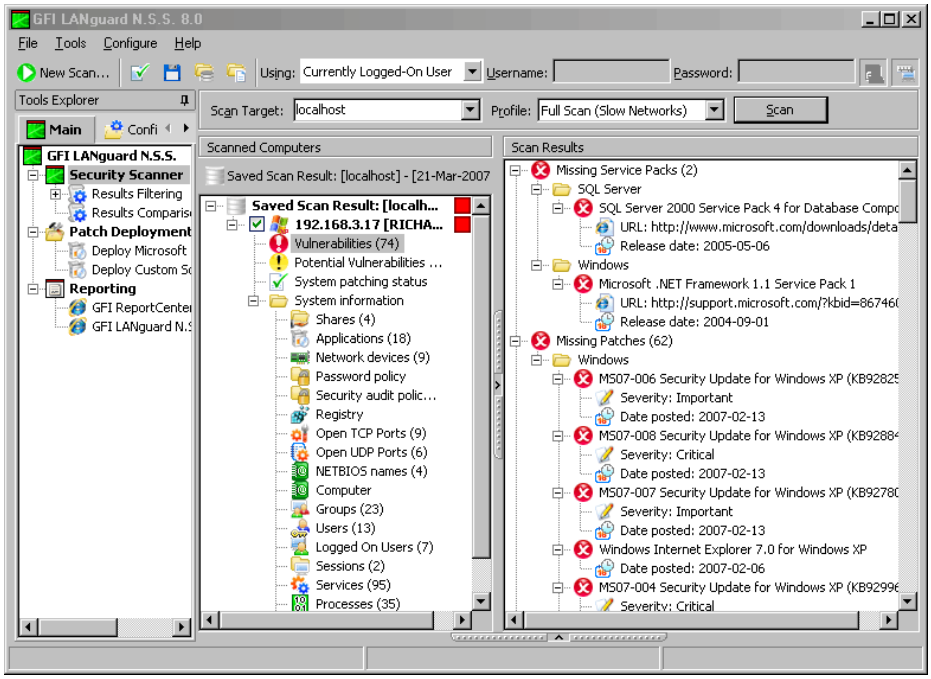
1. Go to **File ▸ Save scan results…**

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 49 - Reloaded scan results

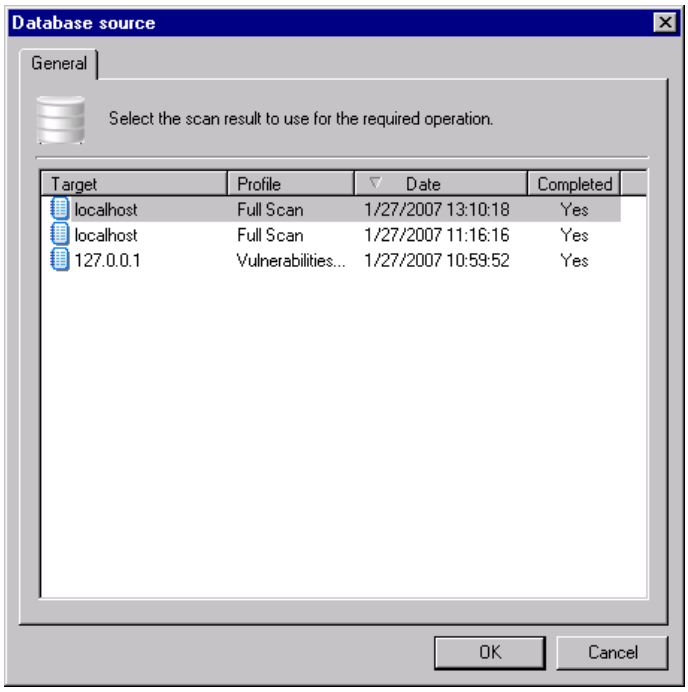
GFI LANguard N.S.S. can store scan results in a Microsoft Access or Microsoft SQL Server database backend as well as to an XML file. By default, saved scan results are organized in a database containing the results data of the last 10 scans performed per scanning profile.

NOTE: You can configure the number of scan results that are stored in a database file. For more information on how to achieve this please refer to the 'Manage saved scan results' section in the 'Database Maintenance Options' chapter.

Saved scan results can also be re-loaded from XML file for further processing and analysis. To load saved scan results from the database backend:

1. Click on the **Main** button

2. Right-click on the **Security Scanner (default)** node and select **Load saved scan results from… ▸ Database**.



Screenshot 50 - Saved Scan Results dialog

3. Select the scan results to load and click **OK**.

Loading saved scan results from an XML file

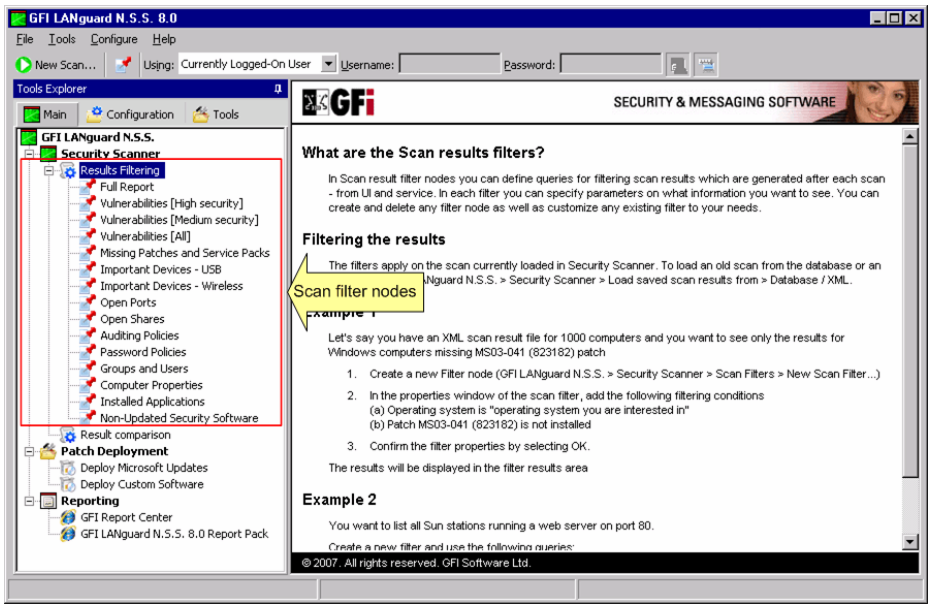
Loading saved scan results from an XML file is identical to loading results from database.

1. Click on the **Main** button
2. Right-click on the **Security Scanner (default)** node and select **Load saved scan results from… ▸ XML**.
3. Select the XML containing the scan results to load and click **OK**.

7. Filtering scan results

Introduction

Scan results contain an wide-ranging amount of information. Even though all of this information is important, there are times when you will require only specific information in order to achieve a particular scope - such as, for example, identifying only which patches are missing in your system.



Screenshot 51 - Scan filter nodes

GFI LANguard N.S.S. 8 provides you with a default set of scan results filters. Using them you can sift out trivial information and display only the relevant information.

In this chapter you will discover how to apply scan result filters and display only the information that you want to analyze

About default scan results filters

The following is a brief description of the scan results filters which are included with GFI LANguard N.S.S. 8.

- **Full report:** Use this scan results filter to display all the information that was collected during a network vulnerability scan including system information, outdated anti-virus signatures, and missing security updates.
- **Vulnerabilities [high security]:** Use this default scan filter to display only severe vulnerabilities such as missing critical security patches and service packs.

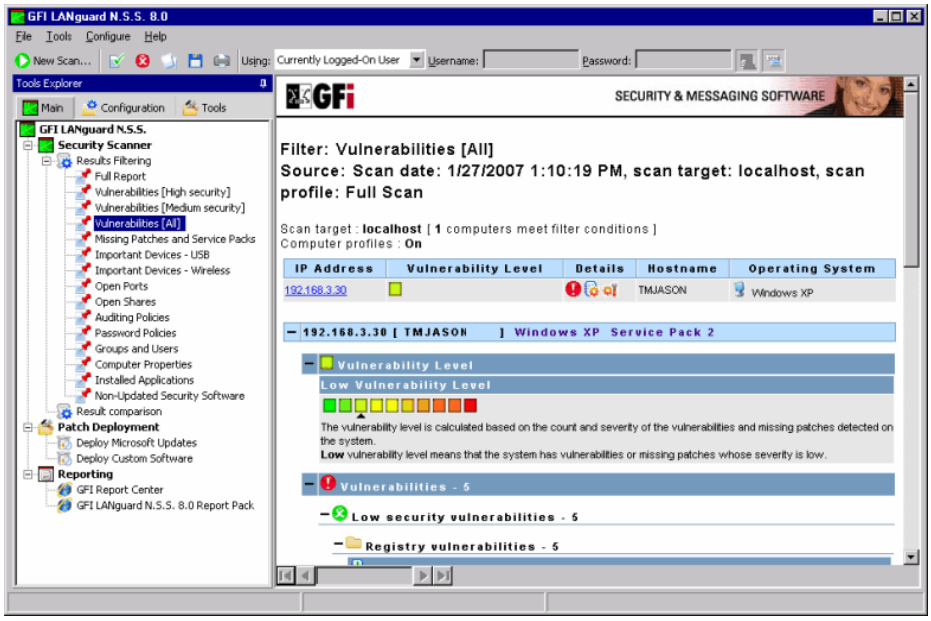
- **Vulnerabilities [medium security]:** Use this default scan filter to display only moderate severity vulnerabilities which may need to be addressed by the administrator such as average threats and medium vulnerability patches.
- **Vulnerabilities [All]:** Use this default scan filter to display all vulnerability categories only all High and Medium vulnerabilities discovered during a security scan such as missing patches, and missing service packs.
- **High vulnerability level computers:** Use this default scan filter to display computers and vulnerability details for which vulnerability level is high.
- **Missing patches and service packs:** Use this default scan filter to display only all missing service packs and patch files discovered on the scanned target computer(s).
- **Missing critical patches:** Use this default scan filter to display all missing patches marked as critical.
- **Missing service packs:** Use this scan filter to display a list of all computers and computer details of computers which have a missing service pack.
- **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).
- **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.
- **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 52 - Scan filters: Full report

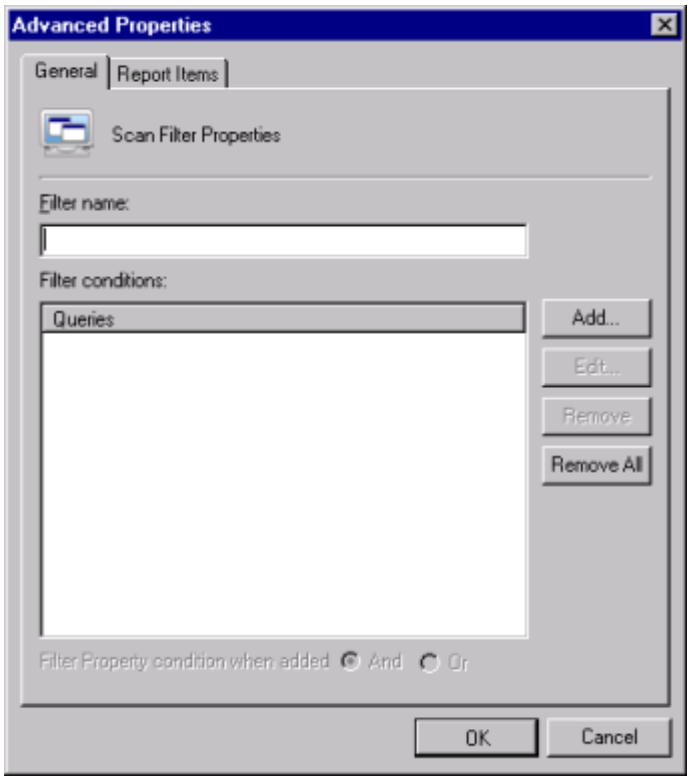
2. Expand the **Security Scanner ▸ Results Filtering** node.

3. Select the scan filter that you want to apply (e.g. Vulnerabilities [All]).

Creating a custom scan filter

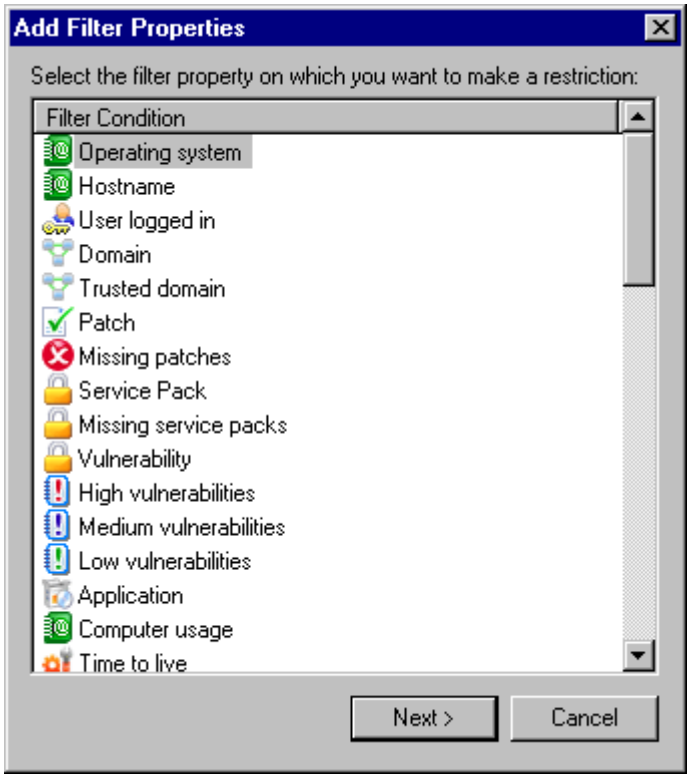
To create a custom scan filter:

1. Click on the **Main** button, right-click the **Security Scanner ▸ Results Filtering** node and select **New ▸ Filter…**.



Screenshot 53 - The new Scan filter properties dialog: General tab-page

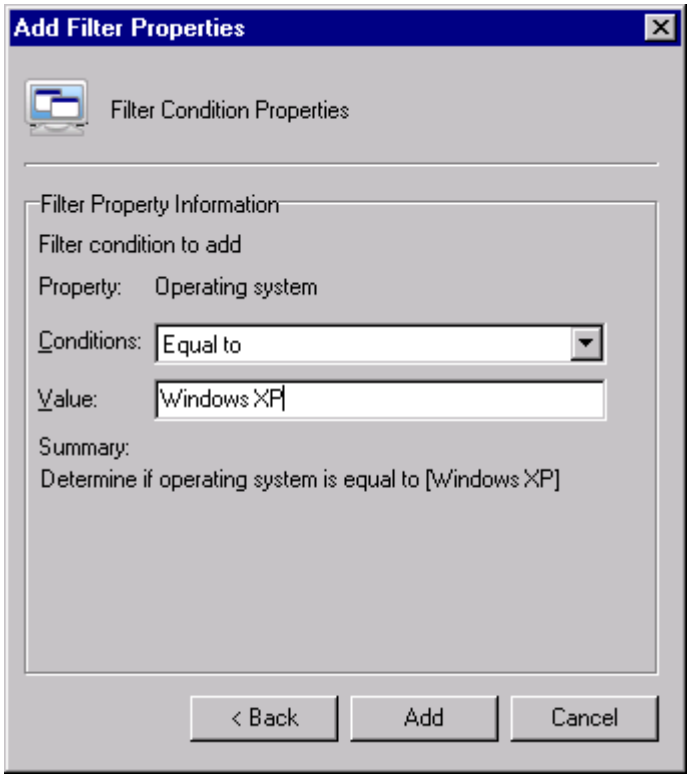
2. In the **General** tab specify the name of the new scan filter.



Screenshot 54 - Filter properties dialog

3. Click on **Add** and select the required filter property from the provided list (for example, operating system). This 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.

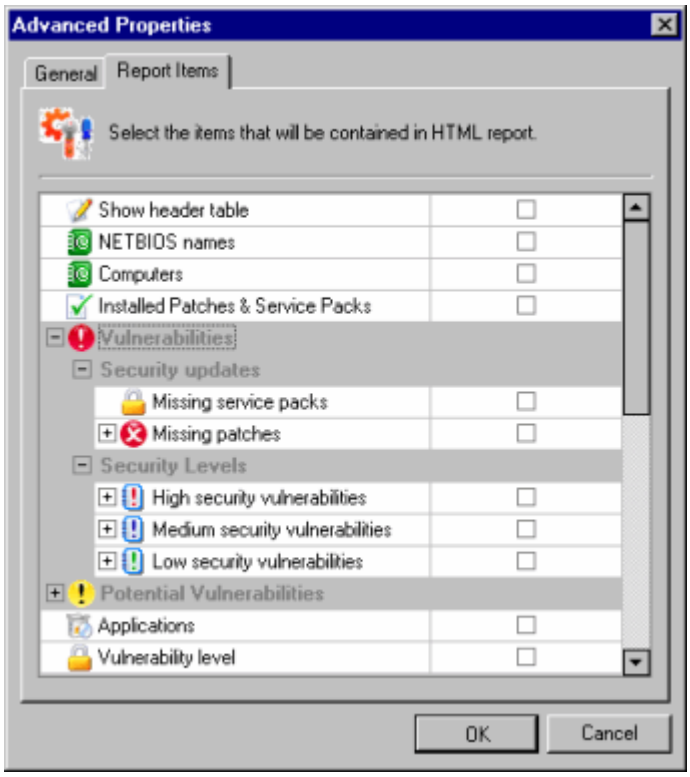


Screenshot 55 - Filter condition properties dialog

5. Select the required filter condition from the *'Conditions'* drop down and specify the filter value. The filter value is the reference string to be used with the specified condition to filter 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 that more accurately isolate the scan results information that you may want to analyze.



Screenshot 56 - The new Scan-Filter properties dialog: Report Items tab-page

7. Click on the **Report Items** tab and select the information categories/sub-nodes that will be displayed in the configuration interface. Click on **OK** to save and create the new filter.

The new filter will be added as a new permanent sub-node under the **Security Scanner ▸ Results Filtering** node.

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

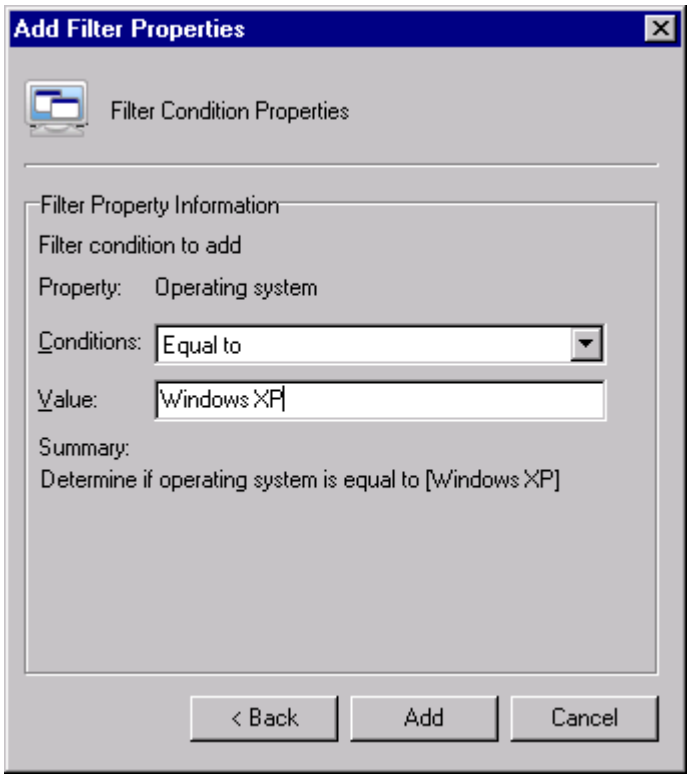
Example 1 – Create a filter which displays all computers that have a particular patch missing

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

1. Click on the **Main** button, right-click on the **Security Scanner ▸ Results Filtering** node and select **New ▸ Filter…**

2. In the filter name field type in *'Missing Blaster Patch'* and click on the **Add** button.

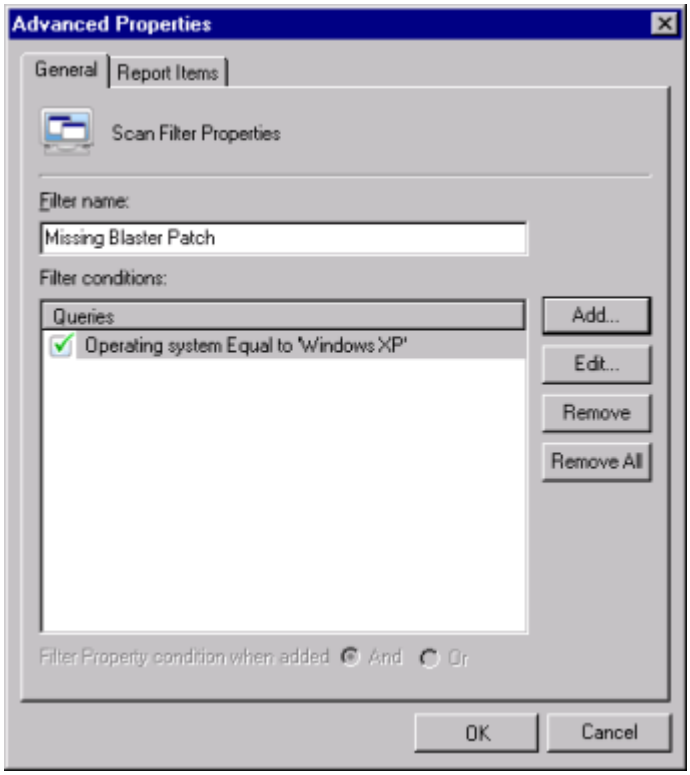
3. Select the *'operating system'* option and click on **Next**.



Screenshot 57 - Filter conditions dialog

4. From the conditions drop down box select *'Equal to'* and in the value field type in *'Windows XP'*.

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



Screenshot 58 - The new Scan Filter properties dialog: General tab-page

6. Click on **Add** to create another filter condition in which you will specify the required patch name (i.e. MS03-026).

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

8. From the conditions drop down select *'is not installed'* and in the value field type in *'MS03-026'*. Click on the **Add** button to include this condition in the scan filter.

9. Click **OK** to finalize the configuration and create the filter. The new filter is added as a new permanent sub-node. (**Security Scanner ▸ Results Filtering ▸ Missing Blaster Patch)**.

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

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

1. Click on the **Main** button, right-click on the **Security Scanner ▸ Results Filtering** node and select **New ▸ Filter…**.

2. In the filter name field key in *'Sun WS web servers on port 80'* and click on the **Add** button.

3. From the list of filter properties select *'operating system'* and then click on **Next**.

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

5. Click on the **Add** button.

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

7. Select '*TCP Port'* and click on **Next**.

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

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

10. Click on **OK** to finalize the configuration. The new filter will be added as a new permanent node. (**Security Scanner ▸ Results Filtering ▸ Sun WS web servers on port 80**).

8. Configuring GFI LANguard N.S.S.

Introduction

GFI LANguard N.S.S. 8 allows you to run vulnerability scans straight out of the box – using the default settings configured prior to shipping. However, if required you can also customize these settings to suit any particular vulnerability management requirements that your organization might need. You can customize and configure various aspects of GFI LANguard N.S.S. including scan schedules, vulnerability checks, scan filters and scan profiles.

In this chapter you will discover how to:

- Create and configure scheduled scans
- Configure email alerts
- Configure computer profiles
- Configure automatic patch downloads
- Configure the database backend settings.

Creating and configuring scheduled scans

Network vulnerability scans can be scheduled to be executed automatically on specific date/time periods as well as regularly on a daily, weekly, monthly schedule.

By default, scheduled scan results are stored in the Microsoft Access or Microsoft SQL Database backend. However, you can also configure GFI LANguard N.S.S. 8 to:

- Save scan results as XML or HTML files and store them in a specific location to be used further on for report comparison operations.
- Automatically generate a scan results report and send it to the administrator via email.

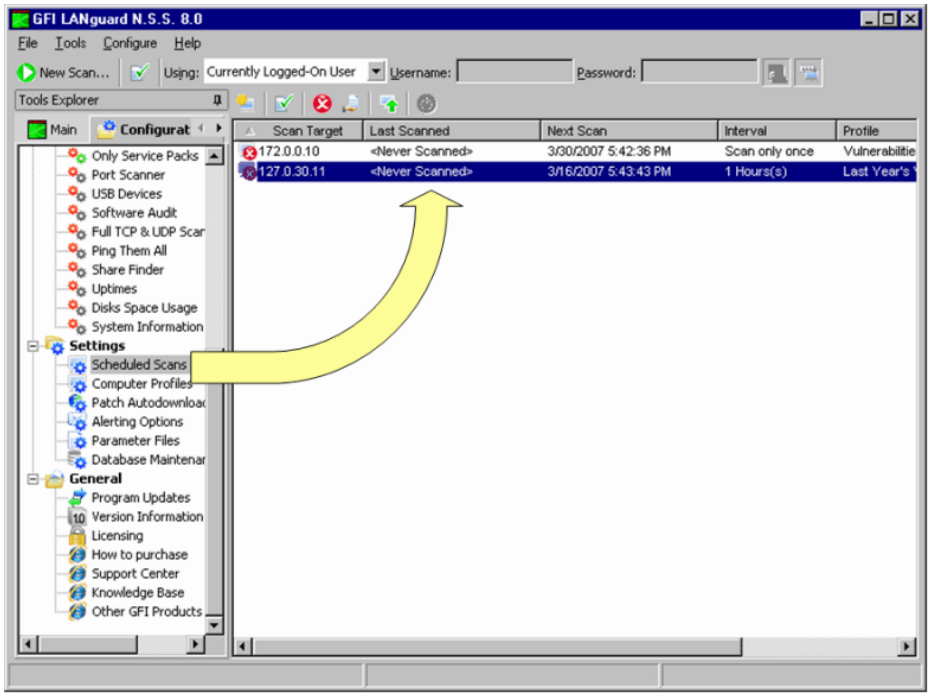
NOTE: For information on how to configure mail server settings or administrator email address refer to the alerting options section in this chapter.

GFI LANguard N.S.S. 8 can automatically generate and email two types of reports following the completion of a scheduled scan; the ‘Full Scan’ report and the ‘Results Comparison’ report.

- The ‘Full Scan Report’ includes all the information collected or generated during the execution of a scheduled scan.
- The ‘Results Comparison’ report enumerates only the differences identified between the last scheduled scan results and the preceding one.

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.

Creating a scheduled scan

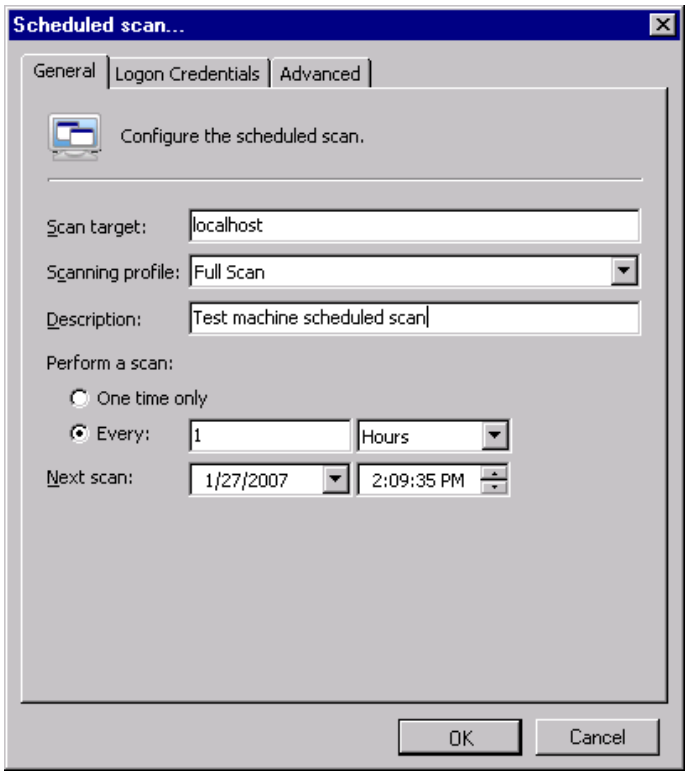


Screenshot 59 - List of configured scheduled scan

To create a scheduled scan:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings sub-node**

2. Right-click on the Scheduled Scans sub-node and select **New ▸ Scheduled scan…** This will bring up the 'New Scheduled Scan' configuration dialog.



Screenshot 60 - New Scheduled Scan dialog

3. In the **General** tab which opens by default, specify the target computers (i.e. hostname, IP or IP range).

NOTE: For more information on how to specify which target computers to be scanned refer to the "Scheduled scan: Configuring scan targets" section below.

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

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

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

7. If alternative logon credentials are required, click on the **Logon Credentials** tab. For instructions on how to achieve this refer to the 'Scheduled scan: Configuring Logon Credentials' section in this chapter.

8. When scanning targets that are normally offline such as laptops, click on the **Advanced** tab. Follow the instructions provided in the 'Scheduled scan: Configuring Advanced options' section in this chapter.

9. Click **OK** to finalize your settings.

Scheduled scan: Configuring scan targets

When configuring the list of target computers you can specify:

- The fully qualified domain name to scan all machines making part of a specific domain
- Computer names to denote scanning of particular machines.
- The URL (ex. computer.corporation.com)

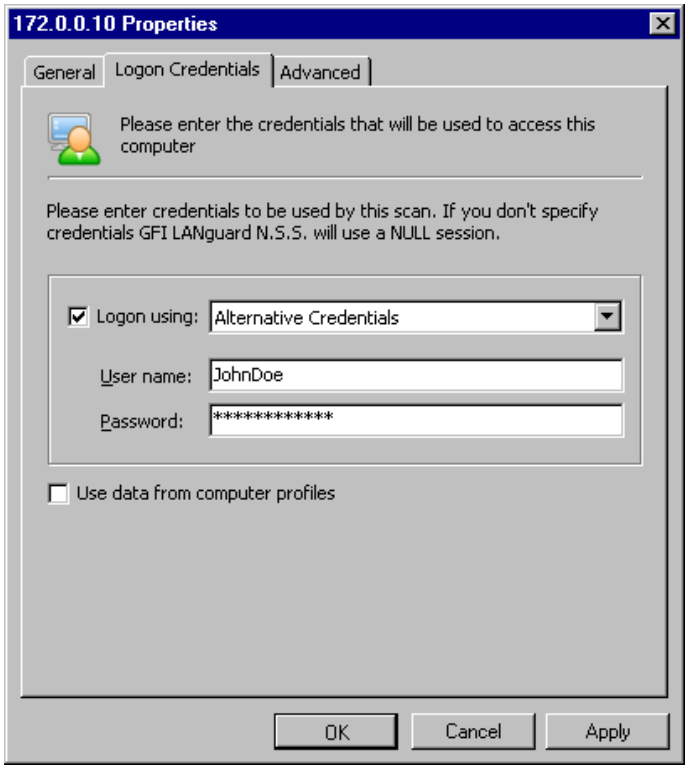
- The I.P. addresses (ex. 192.168.100.5) of all machines to be scanned
- An I.P. address range (ex. 192.168.100.5 – 192.168.100.50)
- CIDR subnets (ex. 192.168.100.0/24)
- The name and full path of the text file which contains target computer details using the following syntax:

  file:<*filename*>

  NOTE: The file must contain one target computer name per line.

Scheduled scan: Configuring logon credentials

As with normal vulnerability scans, scheduled scans will require to logon to target computers with administrator credentials in order to perform a vulnerability scan. By default, scheduled scans will use the credentials of the currently logged on user account. However if required, you can also specify a different set of logon credentials to be used during a scheduled scan.

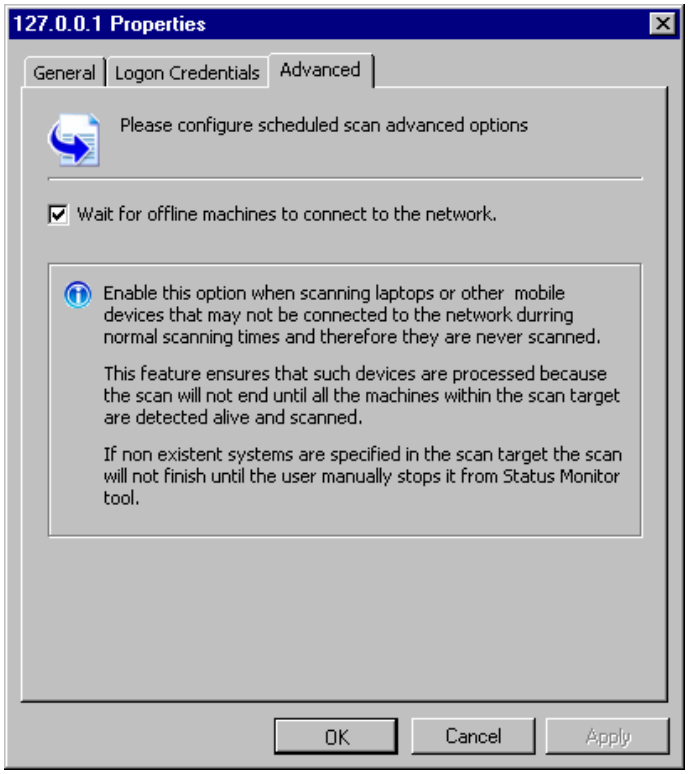


Screenshot 61 - Configuring logon credentials

To configure logon credentials for a scheduled scan select one of the following options from the provided drop down list:

- *'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.

Scheduled scans: Configuring advanced options

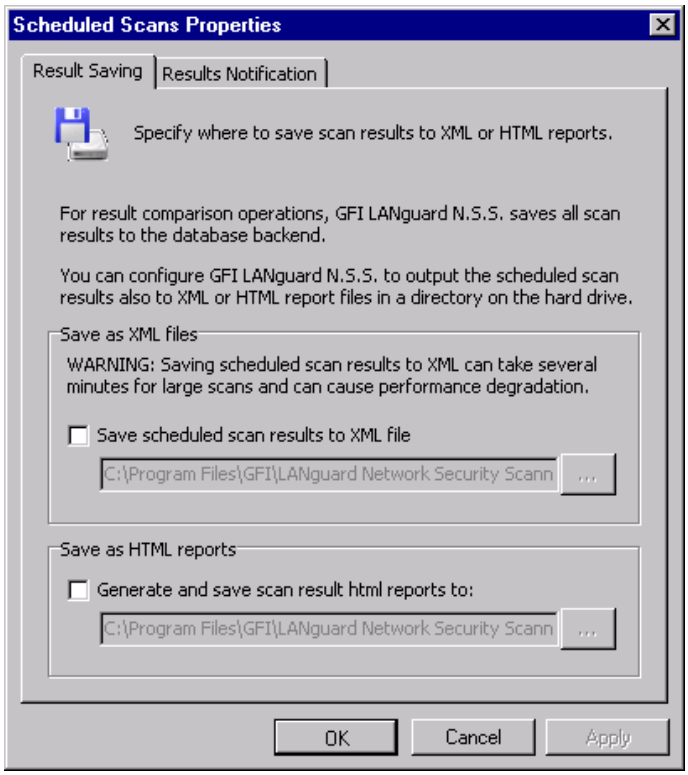


Screenshot 62 - Configuring advanced options

GFI LANguard N.S.S. can automatically keep track of scan targets that were "missing" (e.g. switched off) during the execution of a vulnerability scan; and attempt to re-scan these machines as soon as these are reachable over the network.

To achieve this, click on the **Advanced** tab and select the "**Wait for offline machines to connect to network**" option.

Scheduled scan: Configuring the scan results saving options



Screenshot 63 - Scheduled Scans properties dialog

To save scheduled scan results in an XML/HTML file:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

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

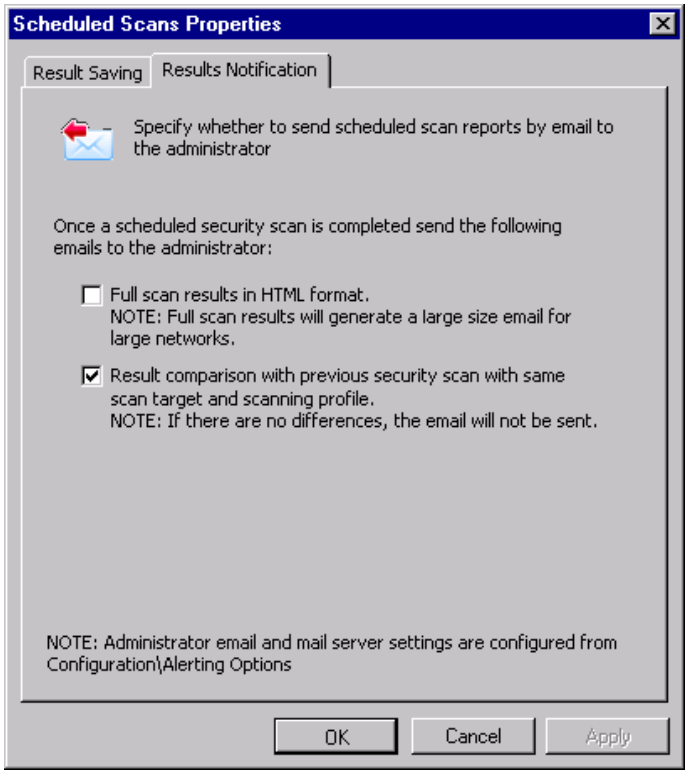
3. Specify file-type preferences by selecting:

'Save scheduled scan results to XML file' – Select this option to save scan results to XML file.

'Generate and save scan result HTML reports to:' - Select this option to save scan results to HTML file.

4. Click **OK** to finalize your settings.

Scheduled scan: Configuring results notifications



Screenshot 64 - Scheduled Scan properties: Results Notification tab

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

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

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

3. Click on the **Results Notifications** tab and select the report(s) that will be emailed upon completion of the scheduled scan.

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

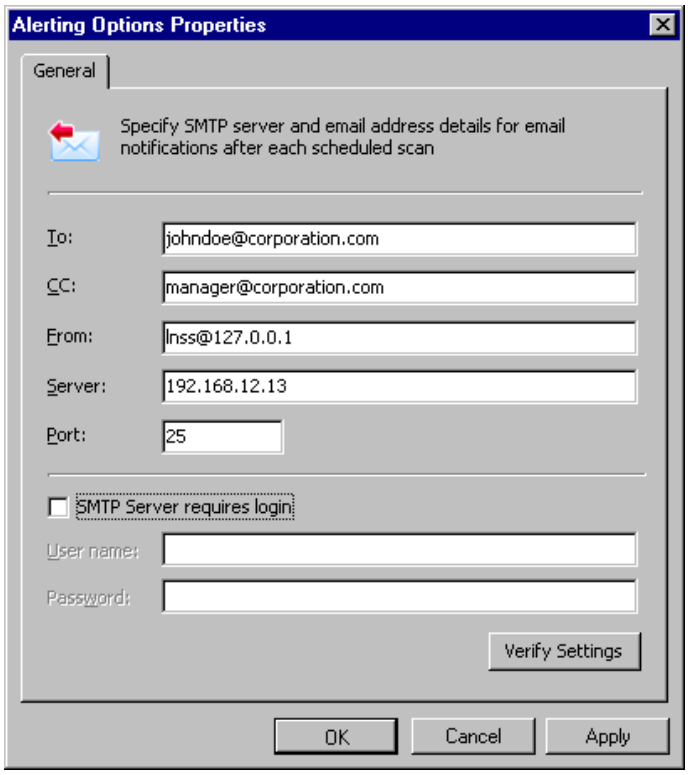
NOTE: For information on how to configure mail server settings or administrator email address refer to the alerting options section in this chapter.

Configuring alerting options

To configure mail server settings or administrator email address:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Alerting Options** sub-node and select **Properties**. This will bring up the scheduled scans properties dialog.



Screenshot 65 - Configuring Alerting Options

3. Configure the following parameters:

- 'To – Email address where email notification will be sent.
- 'CC' – Carbon-copy email address details
- 'From' - Display name that will be shown in email sent to addressee
- 'Server' - SMTP server details
- 'Port' – SMTP port details
- 'Username' – (optional) SMTP login name details
- 'Password' – (optional) SMTP password

4. Click on the **Verify** settings button to verify email settings.

5. Click **OK** to finalize your settings.

Computer profiles

When working in both large and smaller-sized networks, you will inevitably have to log in with different sets of credentials on different computers. 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 every target computer. The scanning engine can then refer to the logon credentials stored in these computer profiles when authenticating to target computers. This way you will not need to specify a default set of logon credentials prior to starting a network scan. It also makes it possible to scan target computers that require

different logon credentials and authentication methods in the same (single) session. 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 authentication

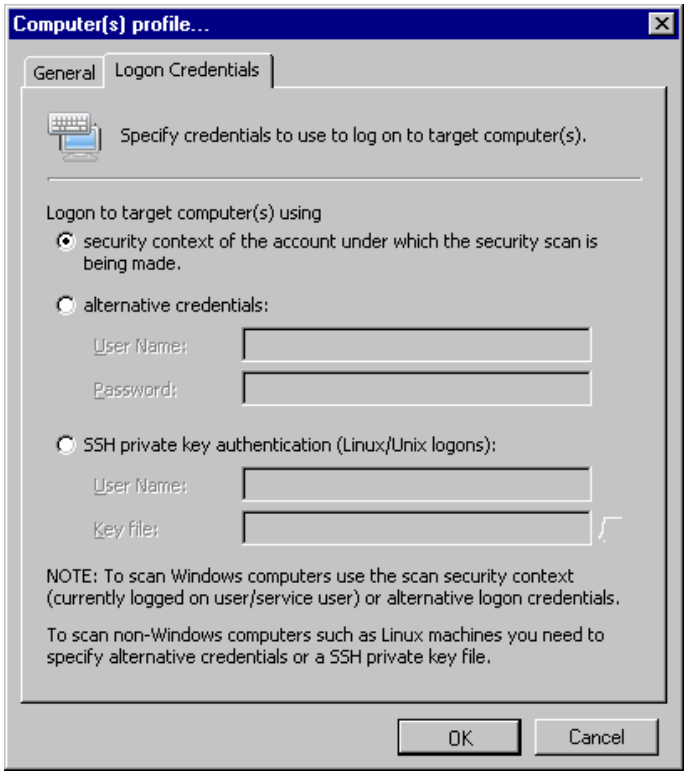
GFI LANguard N.S.S. connects to Linux-based target computers through SSH connections. In public key cryptography, two keys (in the form of text files) are used to verify the authenticity of an SSH connection request. These keys are identified as the 'SSH private key' and 'SSH public key'.

The SSH 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).

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).

Creating a new computer profile



Screenshot 66 - Computer profile properties dialog

To create a new computer profile:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Computer Profiles** sub-node and select **New ▸ Computer(s) Profile…** This will bring up the Computer Profile properties dialog.

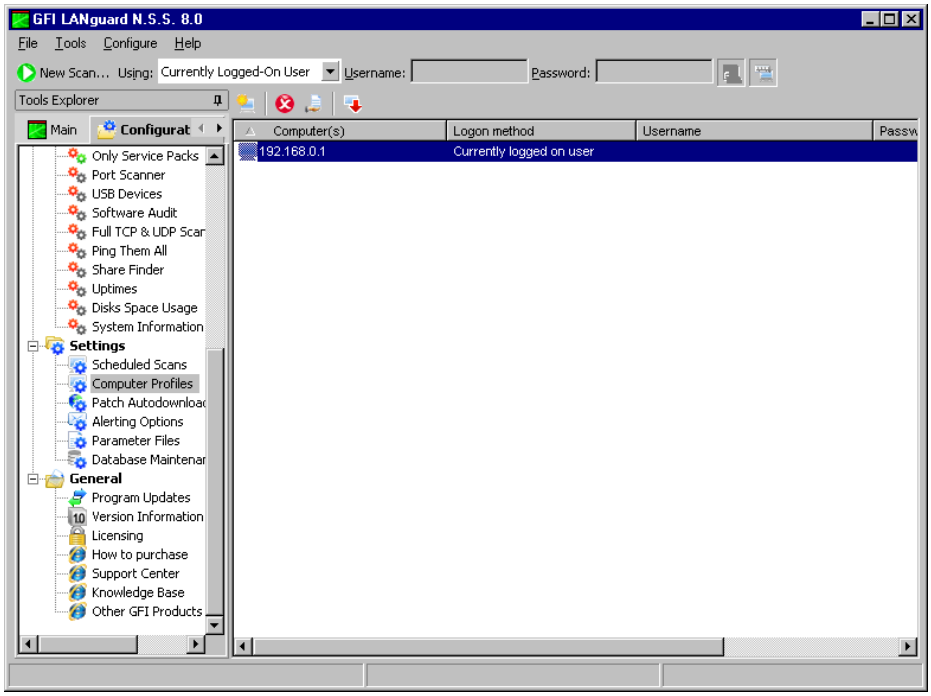
3. In the **General** tab which opens by default specify the target computer name.

3. Click on the **Logon Credentials** tab, select the required authentication method and specify the respective logon credentials.

4. Click **OK** to finalize your settings.

NOTE: In GFI LANguard N.S.S. 8, newly created computer profiles are disabled by default. For information on how to enable newly created computer profiles, refer to the 'Enabling/Disabling computer profiles' section in this chapter.

Configuring computer profile parameters



Screenshot 67 - List of existing computer profiles

To configure/change the parameters of an existing computer profile:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings ▸ Computer Profiles** sub-node

2. Right-click the computer profile to configure and select **Properties**.

3. Configure the required parameters and click **OK** to finalize your settings.

Enabling/Disabling Profiles

By default all the newly created computer profiles are disabled. In practice this means that GFI LANguard N.S.S. 8 will not use these profiles during vulnerability scans.

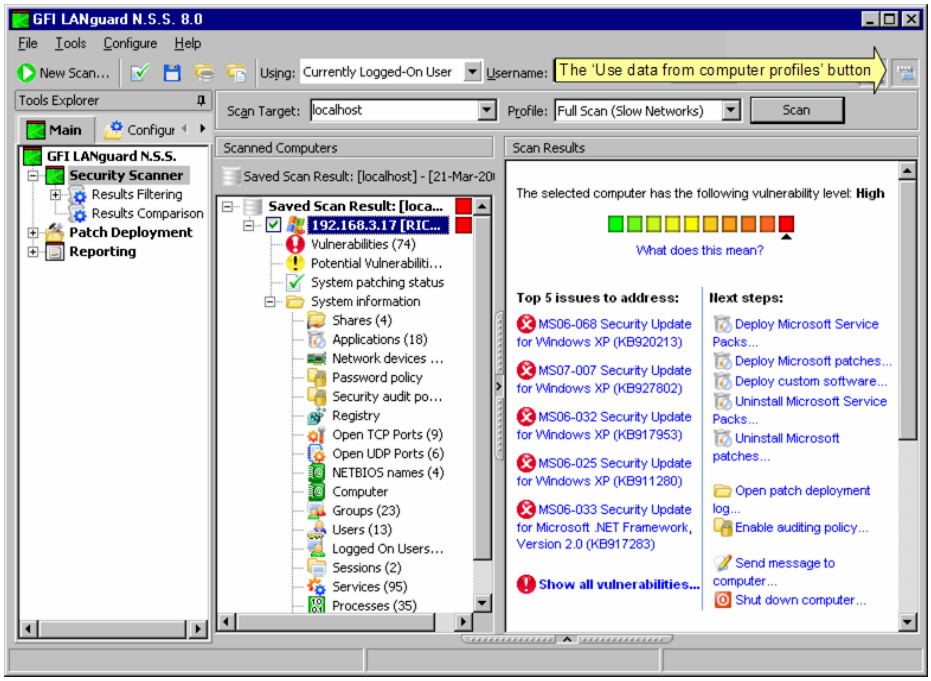
To enable (or disable) profiles:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings ▸ Computer Profiles** sub-node

2. Select one or more profiles to be enabled/disable.

3. Right-click on these profiles and select **enable** /**disable** accordingly.

Using computer profiles in a scan



Screenshot 68 - The 'Use data from computer profiles' button

To scan target computers using computer profiles, click on the **Use data from computer profiles** button included in the GFI LANguard N.S.S. 8 tool bar.

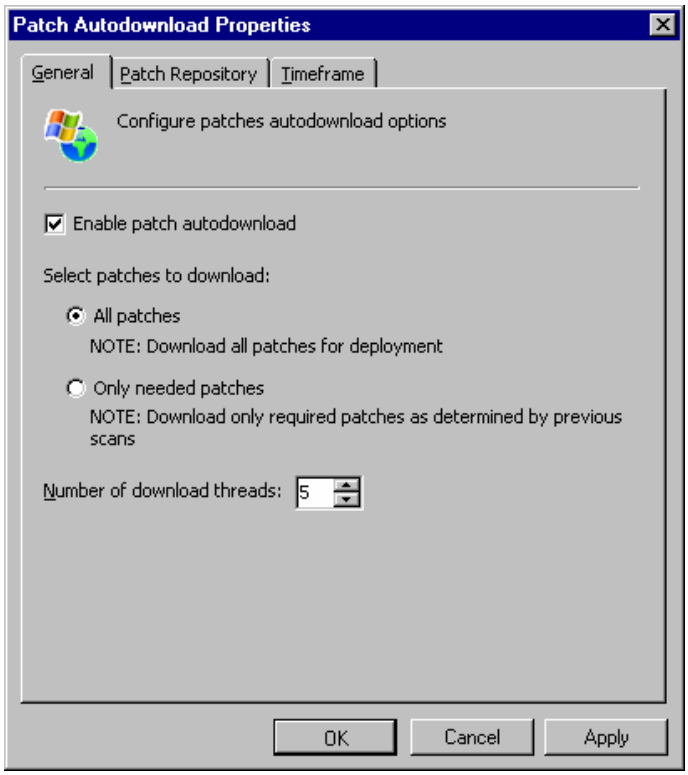
Configuring Patch Autodownload

GFI LANguard N.S.S. 8 ships with a patch autodownload feature which allows you to automatically download missing Microsoft patches and service packs in all 38 languages supported by Microsoft products. In addition you can also schedule patch autodownload by specifying the timeframe within which the download of patches is to be performed.

To configure patch autodownload:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Patch Autodownload** sub-node and select **Properties**.



Screenshot 69- Configuring Patch Autodownload Properties

3. In the **General** tab which opens by default, select one of the following options:

- 'All patches' – Select this option to download all available patches.
- 'Only needed patches' – Select this option to download only the missing patches as determined during vulnerability scanning.

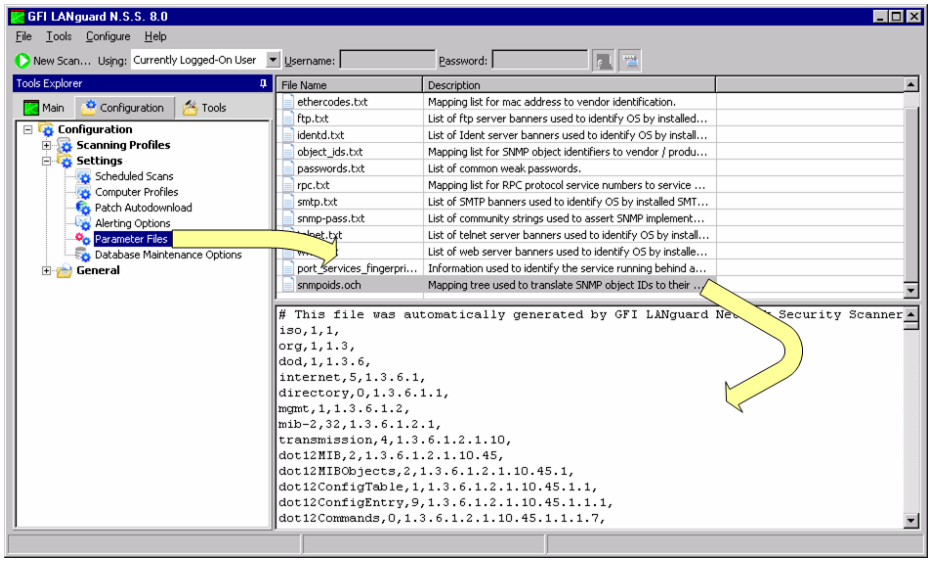
4. To change the path were downloaded patches are stored click on the **Patch Repository** tab and specify the required details.

5. To change the timeframe during which patch downloads are performed click on the **Timeframe** tab and specify the required details.

NOTE: GFI LANguard N.S.S. 8.0 can use patch files downloaded by Microsoft WSUS when deploying missing patches and service packs on target computers. To enable use of Microsoft WSUS downloaded files select the *'Use files downloaded by Microsoft WSUS when available'* option and specify the path from where the Microsoft WSUS downloaded patches will be retrieved.

6. Click **OK** to finalize your settings.

Parameter files



Screenshot 70 - List of Parameter Files

During vulnerability scanning, GFI LANguard N.S.S. extracts parameters from a number of text files known as 'Parameter Files'. These parameter files can be modified in order to improve the performance of GFI LANguard N.S.S. 8.

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 **Configuration ▸ Settings ▸ Parameter Files** sub-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.

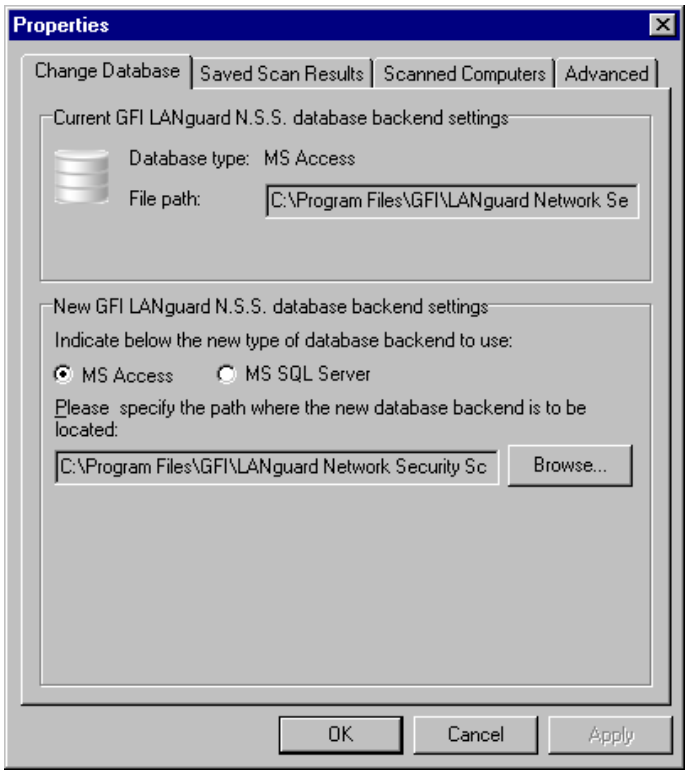
- **Object_ids.txt** – This file contains the SNMP object_ids as well as the associated vendor(s) and product(s). When a device responds to an SNMP query, GFI LANguard N.S.S. will compare the Object ID information (sent by the target computer) to the OID information stored in this file.
- **Passwords.txt** – This file has a list of passwords that, during a scan, are used to perform dictionary attacks on target computers in order to identify weak passwords.
- **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 N.S.S. 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.
- **Port_services_fingerprint.xml** – This file contains a copy of the data sent while trying to recognize the type of the servers that are listening behind an open port (HTTP, FTP, SMTP, POP3, SSH, TELNET, etc.)
- **Snmpoids.och** – This file contains a map between SNMP object IDs and their display name and it is used to browse SNMP info by the SNMP Walk tool.

Database maintenance

GFI LANguard N.S.S. ships with a set of database maintenance options through which you can maintain your scan results database backend in good shape. For example you can improve product performance and prevent your scan results database backend by getting excessively voluminous by automatically deleting scan results that are older than a specific number of months.

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; hence ensure the integrity of your scan results database.

Selecting a database backend



Screenshot 71 - The database maintenance properties dialog

GFI LANguard N.S.S. 8 supports both MS Access and MS SQL Server (2000 or higher) based database backend.

Storing scan results in an MS Access database backend

To store scan results in a Microsoft Access database:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node.

2. Right-click the **Database Maintenance Options** sub-node and select **Properties**.

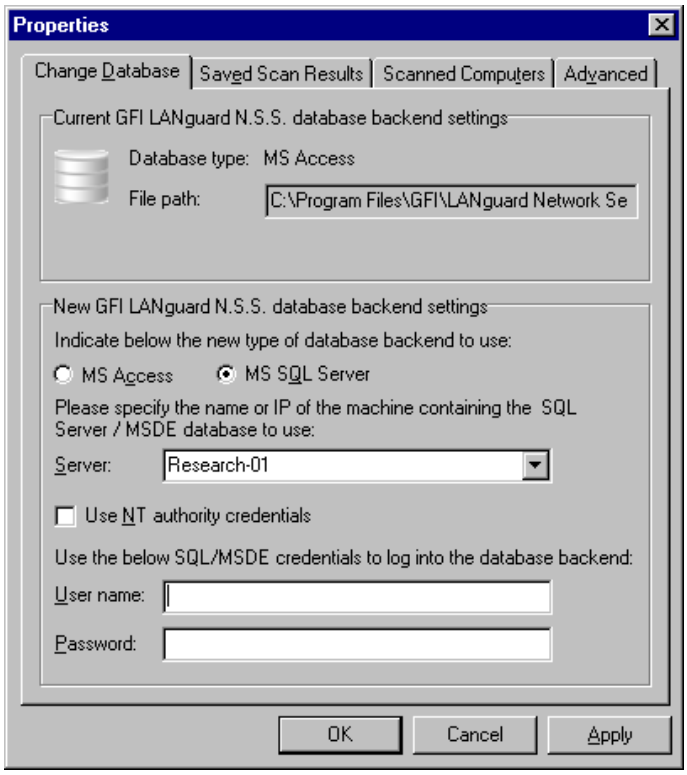
3. Select the *'MS Access'* option and specify the full path (including the file name) of your Microsoft Access database backend.

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. you will be asked whether you wan to over-write the existing information.

4. Click **OK** to finalize your settings.

Storing scan results in an MS SQL Server database



Screenshot 72 - Microsoft SQL Server database backend options

To store scan results in a Microsoft SQL Server database:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Database Maintenance Options** sub-node and select **Properties**.

3. Select the *'MS SQL Server'* option and choose the SQL Server that will be hosting the database from the provided list of servers discovered on your network.

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 finalize your settings.

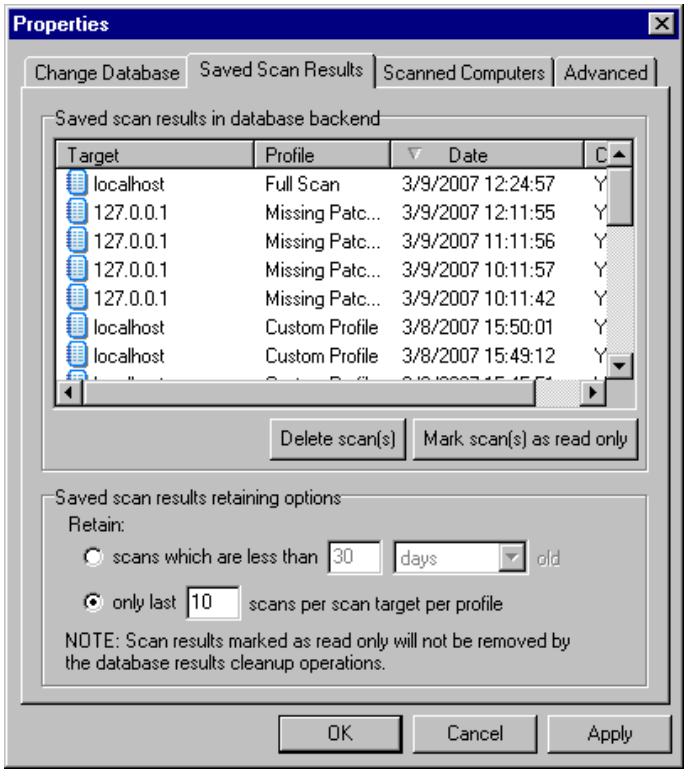
NOTE 1: If the specified server and credentials are correct, GFI LANguard N.S.S. will automatically log on to your SQL Server and create the necessary database tables. If the database tables already exist it will re-use them.

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

Database maintenance: Managing saved scan results

Use the **Saved Scan Results** tab to maintain your database backend and delete saved scan results that are no longer required. Deletion of non-required saved scan results can be achieved manually as well as automatically through scheduled database maintenance.

During scheduled database maintenance GFI LANguard N.S.S. automatically deletes saved scan results that are older than a specific number of days/weeks or months. You can also configure automated database maintenance to retain only a specific number of recent scan results for every scan target and scan profile.



Screenshot 73 - Database maintenance properties: Managed saved scan results tab

To manage saved scan results:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Database Maintenance Options** sub-node and select **Properties**.

3. Click the **Saved Scan Results** tab.

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

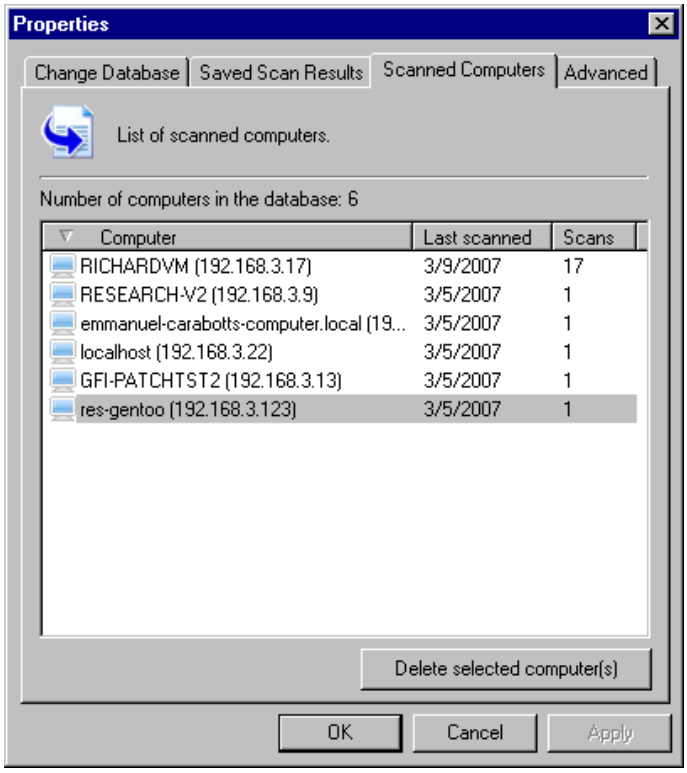
5. To let GFI LANguard N.S.S. manage database maintenance for you, select one of the following options:

- *'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: List of scanned computers

GFI LANguard N.S.S. incorporates a mechanism where a global list of scanned computers is maintained for licensing purposes. This enables GFI LANguard N.S.S. to enforce its licensing details, where a larger range of scanned computers than what is specified in the licensing information will not be scanned.

GFI LANguard N.S.S. enables systems administrators to delete previously scanned computers (nodes) so that that node licenses taken by computers that are no longer present on the network, or which should no longer be scanned, can be reutilized.



Screenshot 74 - Database maintenance properties: Scanned Computers tab

To delete computers previously scanned:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node.

2. Right-click the **Database Maintenance Options** sub-node and select **Properties**.

3. Click the **Scanned Computers** tab.

4. Select the computers to delete by holding the control key and clicking on the computers.

5. Click on the **Delete selected computer(s)** button to delete scanned computer data.

NOTE 1: Deleting computers from the database is a one-way operation that will also delete all computer related data from the database. **Once deleted, this data is no longer recoverable.**

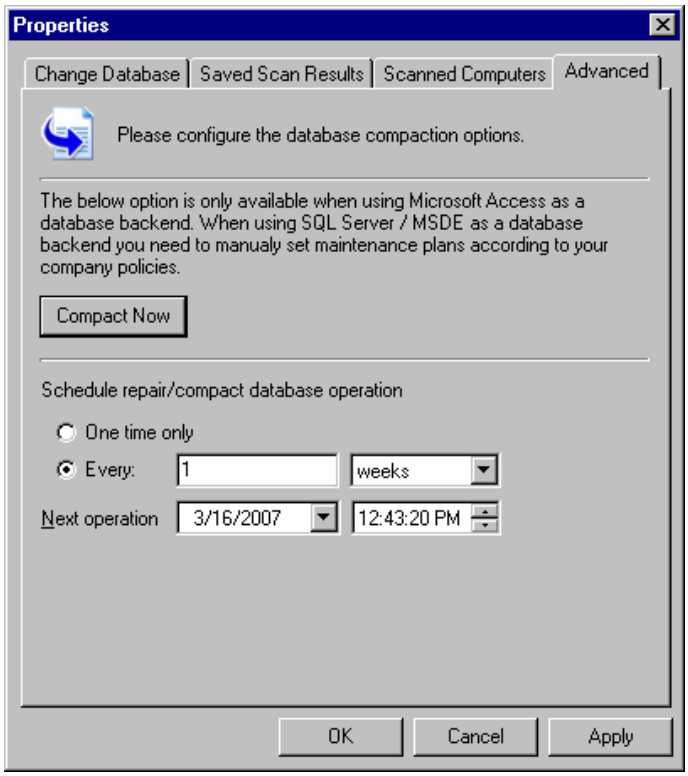
NOTE 2: While this is a very efficient mechanism for freeing up licenses previously occupied by unused nodes, kindly note that this impacts the long term security reporting capabilities of GFI LANguard N.S.S. Where long term security reporting must be ascertained, or in

environments where security databases must be intact, it is highly advisable to not delete any data whatsoever. In such scenarios, it is advisable that more licenses are acquired to cater for network growth or expansion.

Database maintenance: Advanced options

To improve the performance of your MS Access based database backend you must regularly repair and compact it; two functions that GFI LANguard N.S.S. allows you to automate.

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 this 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 is corrupted when the database is unexpectedly closed before records are saved (for example, due to a power failure, hung up processes, forced reboots, etc.).



Screenshot 75 - Database Maintenance properties: Advanced tab

To compact and repair a Microsoft Access based database backend:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Database Maintenance Options** sub-node and select **Properties**.

3. Click the **Advanced** tab

4. To manually launch a repair and compact process on an MS Access database backend, on the **Compact Now** button.

5. To automate the repair and compact process on an MS Access database backend select one of the following options:

- *'One time only'* - Select this option to schedule a one time MS Access database repair and compact.
- *'Every'* - Select this option to execute a repair and compact process on a regular schedule. Specify the date, time and frequency in days/weeks or months at which the compact and repair operations will be executed on your database backend.

9. Scanning Profiles

Introduction

A typical IT infrastructure is constantly under attacks from various attack vectors. GFI LANguard N.S.S. 8 allows you to scan your IT infrastructure for particular vulnerabilities using pre-configured sets of vulnerability checks known as 'scanning profiles'. A scanning profile allows you to scan your network targets and enumerate only specific information. 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.

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

With 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.

In this chapter you will discover how to:

- Use the default scanning profiles that ship with GFI LANguard N.S.S.
- Configure and customize default scanning profiles
- Create new/customized scanning profiles.

About OVAL

Open Vulnerability and Assessment Language (OVAL™) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the OVAL community. The language standardizes the three main steps of the assessment process:

- Representing configuration information of systems for testing
- Analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.)
- Reporting the results of this assessment.

The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three XML schemas to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process:

- An OVAL System Characteristics schema for representing system information
- An OVAL Definition schema for expressing a specific machine state
- An OVAL Results schema for reporting the results of an assessment

Content written in OVAL Language is located in one of .the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that the OVAL, which is funded by US-CERT at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

GFI LANguard N.S.S. OVAL Support

GFI LANguard N.S.S. supports all checks defined in the XML file issued by OVAL, with the exception of HP-UX checks.

GFI LANguard N.S.S. does not support HP-UX based machines and therefore it is beyond the scope of this product to include these checks within its check definition database.

About OVAL Compatibility

OVAL Compatibility is a program established to develop consistency within the security community regarding the use and implementation of OVAL. The main goal of the compatibility program is to create a set of guidelines that will help enforce a standard implementation. An offshoot of this is that users are able to distinguish between, and have confidence in, compatible products knowing that the implementation of OVAL coincides with the standard set forth.

For a product or service to gain official OVAL Compatibility, it must adhere to the "Requirements and Recommendations for OVAL Compatibility" and complete the formal OVAL Compatibility Process.

OVAL Compatibility means that GFI LANguard N.S.S. incorporates OVAL in a pre-defined, standard way and also uses OVAL for communicating details of vulnerabilities, patches, security configuration settings, and other machine states.

Submitting OVAL listing error reports

Any issues with the GFI LANguard N.S.S. or the listing of the OVAL checks included with GFI LANguard N.S.S. should be reported to GFI through its official support lines. Please refer to the troubleshooting section within this document for more information regarding email, web chat, phone or web forum support channels.

GFI Software Ltd will endeavor to look into any issues reported and if any inconsistency or error is ascertained, it will issue updates to fix such issues. Vulnerability check updates are usually released on monthly basis.

Scanning profile description

Out of the box GFI LANguard N.S.S. 8 includes an extensive list of scanning profiles:

- **Vulnerabilities, Patches and Service Packs:** Use this scanning profile to enumerate particular network vulnerabilities such as open TCP/UDP ports commonly exploited by Trojans as well as missing patches and service packs. The list of vulnerabilities enumerated by this profile can be customized through the Vulnerabilities tab.

  NOTE 1: Installed USB devices and applications are not enumerated by this profile.

  NOTE 2: This profile will scan for all vulnerabilities. This includes vulnerabilities which have an associated Microsoft patch to them and which are considered to be missing patches.

- **Vulnerabilities:** Use this scanning profile to enumerate all network vulnerabilities except missing patches and service packs. This includes open TCP/UDP ports commonly exploited by Trojans. The list of vulnerabilities enumerated by this profile can be customized through the Vulnerabilities tab.

  NOTE 1: Missing patch scanning and network audit operations are not performed through this profile.

  NOTE 2: All vulnerabilities (including OVAL vulnerabilities) which have a Microsoft issued patch associated with them will not be scanned for if this profile is selected. These vulnerabilities are considered to be missing patches and are scanned in profiles that include missing patch detection.

- **SANS Top 20 Vulnerabilities:** Use this scanning profile to enumerate all vulnerabilities reported in the SANS top 20 list.

  NOTE: Missing patch scanning and network audit operations are not performed through this profile.

- **High Security Vulnerabilities:** Use this scanning profile to enumerate open TCP/UDP ports and high security vulnerabilities. The list of TCP/UDP ports and high security vulnerabilities that will be enumerated by this profile can be customized through the TCP/UDP Ports tabs and the Vulnerabilities tab respectively.

  NOTE: Missing patch scanning and network audit operations are not performed through this profile.

- **Last Year's Vulnerabilities:** Use this scanning profile to network vulnerabilities which emerged during the last 12 months.

NOTE: Missing patch scanning and network audit operations are not performed by this profile.

- **Only Web:** Use this scanning profile to identify web-server specific vulnerabilities. This includes scanning and enumerating open TCP ports which are most commonly used by web-servers such as port 80.

  NOTE: Only TCP ports commonly used by web-servers are scanned by this profile. Network auditing operations as well as enumeration of vulnerabilities and missing patches are not performed using this profile.

- **Trojan Ports:** Use this scanning profile to enumerate open TCP/UDP ports which are commonly exploited by known Trojans. The list of TCP/UDP ports to be scanned can be customized through the TCP Ports and UDP Ports tabs respectively.

  NOTE: Only the TCP/UDP ports commonly exploited by known Trojans are scanned by this profile. Network auditing operations as well as enumeration of other open TCP/UDP ports and missing patches are not performed by this profile.

- **Only SNMP:** Use this scanning profile to perform network discovery and retrieve information regarding hardware devices (routers, switches, printers, etc.) that have SNMP enabled. This enables you to monitor network attached devices for conditions that require administrative attention.

  NOTE: No network audit operations or vulnerability checks other than those used for SNMP scanning are performed by this profile.

- **Protection from Portable Storage:** Use this scanning profile to check if GFI EndPointSecurity is installed or if GFI EndPointSecurity's security agent is deployed on scan targets.

  NOTE 1: No vulnerability checks, missing patch scans or network audit operations other than those related to GFI EndPointSecurity are performed by this profile.

  NOTE 2: You can customize this profile to enumerate only unauthorized/blacklisted software or vice-versa. For more information refer to the user manual.

- **Missing Patches:** Use this scanning profile to enumerate missing Microsoft patches. The list of missing patches that will be enumerated by this profile can be customized through the Patches tab.

  NOTE: No network audit operations or vulnerability checks other than those related to missing Microsoft patches are performed by this profile.

- **Critical Patches:** Use this scanning profile to enumerate only missing Microsoft patches that are tagged as critical. The list of critical patches that will be enumerated by this profile can be customized through the Patches tab.

  NOTE: No network audit operations or vulnerability checks other than those related to missing critical Microsoft patches are performed by this profile.

- **Last Month's Patches:** Use this scanning profile to enumerate only missing Microsoft patches that were released last month. The

list of missing patches that will be enumerated by this profile can be customized through the Patches tab.

NOTE: No network audit operations or vulnerability checks other than those related to missing Microsoft patches released last month are performed by this profile.

- **Only Service Packs:** Use this scanning profile to enumerate missing Microsoft service packs. The list of service packs that will be enumerated by this profile can be customized through the Patches tab.

  NOTE: No network audit operations or vulnerability checks other than those related to missing Microsoft service packs are performed by this profile.

- **Port Scanner:** Use this scanning profile to enumerate open TCP/UDP ports including those most commonly exploited by Trojans. The list of ports that will be enumerated by this profile can be customized through the TCP/UDP ports tab.

  NOTE: No network audit operations or vulnerability checks other than open port scanning are performed by this profile.

- **USB Devices:** Use this scanning profile to audit your network and enumerate all USB devices currently connected to your network computers.

  NOTE 1: No vulnerability checks are performed by this profile. You can customize this profile to enumerate only unauthorized/blacklisted USB Devices or vice-versa.

- **Software Audit:** Use this scanning profile to enumerate all software applications installed on scan targets. This includes security software such as anti-virus and anti-spyware.

  NOTE 1: No vulnerability checks and missing service pack enumeration are performed using this profile. You can customize this profile to enumerate only unauthorized/blacklisted software or vice-versa.

- **Full TCP & UDP Scan:** Use this scanning profile to audit your network and enumerate all open TCP and UDP ports.

  NOTE: No vulnerability checks are performed by this profile.

- **Ping Them All:** Use this scanning profile to audit your network and enumerate all computers that are currently connected and running.

  NOTE: No vulnerability checks are performed by this profile.

- **Share Finder:** Use this scanning profile to audit your network and enumerate all open shares either hidden or visible.

  NOTE: No vulnerability checks are performed by this profile.

- **Uptimes:** Use this scanning profile to audit your network and identify how long each computer has been running since the last reboot.

  NOTE: No vulnerability checks are performed by this profile.

- **Disks Space Usage:** Use this scanning profile to audit your network and retrieve system information on available storage space.

- **System Information:** Use this scanning profile to retrieve system information such as operating system details, wireless/virtual/physical network devices connected, USB devices connected, installed applications and more..

  NOTE: No vulnerability checks or missing patch detection are performed using this scanning profile.

- **Full Scan:** Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including: open TCP/UDP ports, missing patches and service packs, USB devices connected and more. The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with LAN environments.

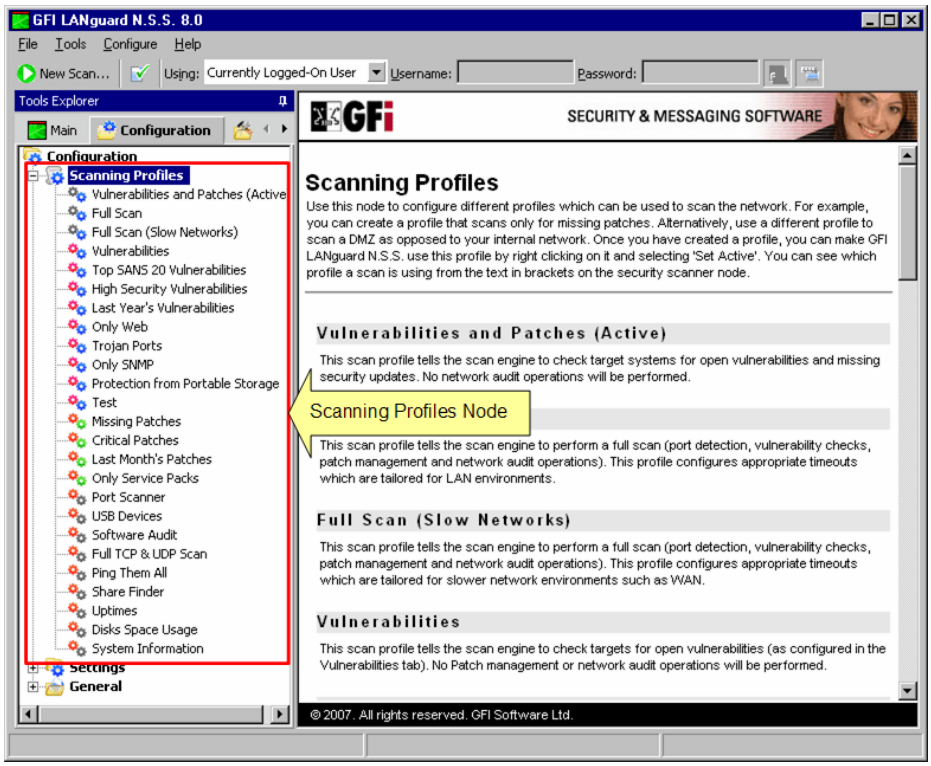
- **Full Scan (Slow Networks):**Use this scanning profile to retrieve system information as well as scan your network for all supported vulnerabilities including: open TCP/UDP ports, missing patches and service packs, USB devices connected and more… The vulnerability check timeouts in this profile are specifically preconfigured to suite the network traffic and transmission delays usually associated with WAN environments.

Which scanning profile shall I use?

Select the scanning profile to be used for network vulnerability scanning based on the:

1. The scope of your vulnerability analysis i.e. what you want to achieve out of your vulnerability scan. Based on these factors, you can determine the type of vulnerability checks to be performed and the information that you want to retrieve from your scan targets.

2. Time you have at your disposal for target vulnerability scanning. Obviously the more vulnerability checks you run the longer it will take for the scan process to complete.



Screenshot 76 - The Scanning Profiles node

Scanning profiles in action

Example 1: Using the 'Vulnerabilities & Patches' profile to scan your local host

1. Click on **New Scan…** button

2. Select *'Complete/Combination Scans'* option and click on the **Next** button to proceed.

3. Select the *'Vulnerabilities and Patches'* option from the scanning profile selection box. Click on the **Next** button to proceed.

4. Select *'Scan single computer'* option. Click on the **Next** button to proceed.

5. Select the *'Scan this computer'* option. Click on the **Next** button to proceed.

6. Provide the credentials under which the scan will be performed and click on the **Scan** button to start the scan.

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

Example 2: Using the 'Vulnerabilities' profile to scan the local host

1. Click on **New Scan…** button

2. Select *'Vulnerability scanning'* option and click on the **Next** button to proceed.

3. Select *'Vulnerabilities'* option and click on the **Next** button to proceed.

4. Select *'Scan single computer'* option. Click on the **Next** button to proceed.

5. Select the *'Scan this computer'* option. Click on the **Next** button to proceed.

6. Provide the credentials under which the scan will be performed and click on the **Scan** button to start the scan.

Important consideration

As you can see the time taken to complete a vulnerability scan using the *'Vulnerabilities'* scanning profile is less than that of the *'Vulnerabilities and Patches'* scanning profile previously performed. This is because the 'Vulnerabilities' scanning profile only performs specific vulnerability checks which analyze and report which vulnerabilities are present on the system. Hence no other patch related checks are run against the target(s) and no extra data is retrieved from the target computer(s).

On the other hand, the 'V*ulnerabilities and patches*' scanning profile performs vulnerability checks on all vulnerable areas of your network as well as all checks for all missing patches. Hence it takes more time to complete the scan. More information is also retrieved from the scanned targets and reported in the scan results.

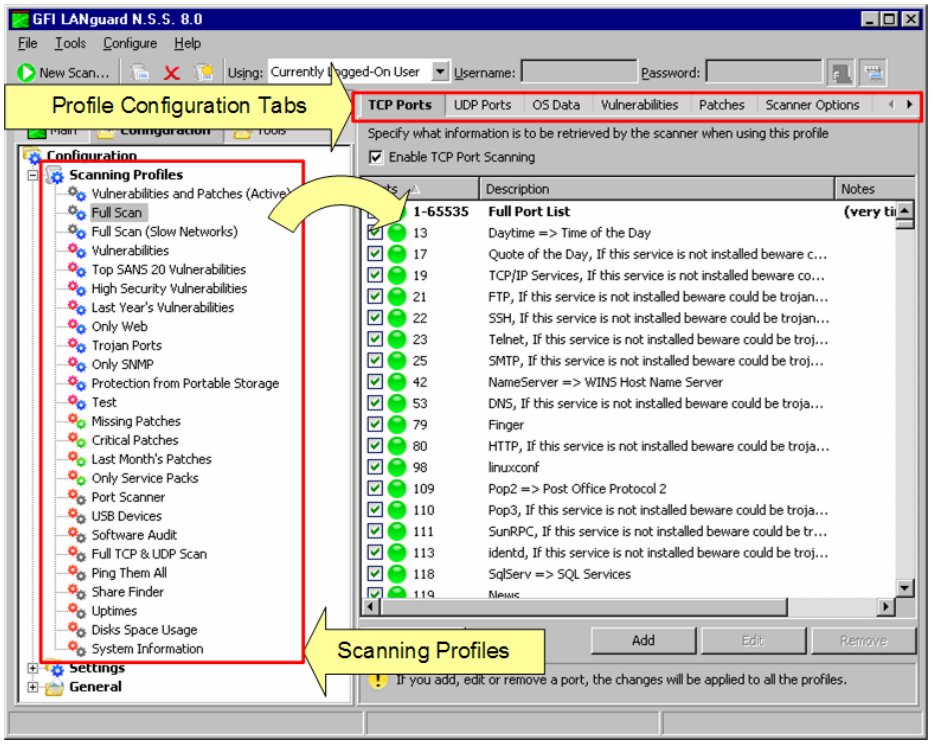
Creating a new scanning profile

To create a new scanning profile:

1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

2. Right-click the **Scanning Profiles** sub-node and select **New ▸ Profile…**

3. Specify the name of the new profile and click **OK**.



Screenshot 77 - The Scanning Profile configuration page

4. Use the tabs presented in the right pane of the management console to 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 this tab to configure TCP port scanning parameters and options (e.g. specify which TCP ports to be scanned).
- **UDP ports** tab – Use this tab to configure UDP port scanning parameters and options (e.g. specify which UDP ports to be scanned).
- **OS data** tab – Use this tab to specify which operating system data will be extracted from scanned targets (e.g. open shares, user accounts and currently logged on user details).
- **Vulnerabilities** tab – Use this tab to specify which vulnerability checks will be run against your target computers (e.g. Web Server vulnerability checks)
- **Patches** tab – Use this tab to specify which missing security updates will be scanned for on target computers.
- **Scanner Options** tab – Use this tab to configure the operational parameters of the vulnerability scanning engine (e.g. target discovery parameters such as timeout values, query methods).
- **Devices** tab – Use this tab to configure the required parameters and enable scanning for installed network and USB devices connected to target computers.
- **Applications** tab – Use this tab to configure the required parameters and enable scanning for applications installed on target computers.

Customizing a scanning profile

To customize a scanning profile:

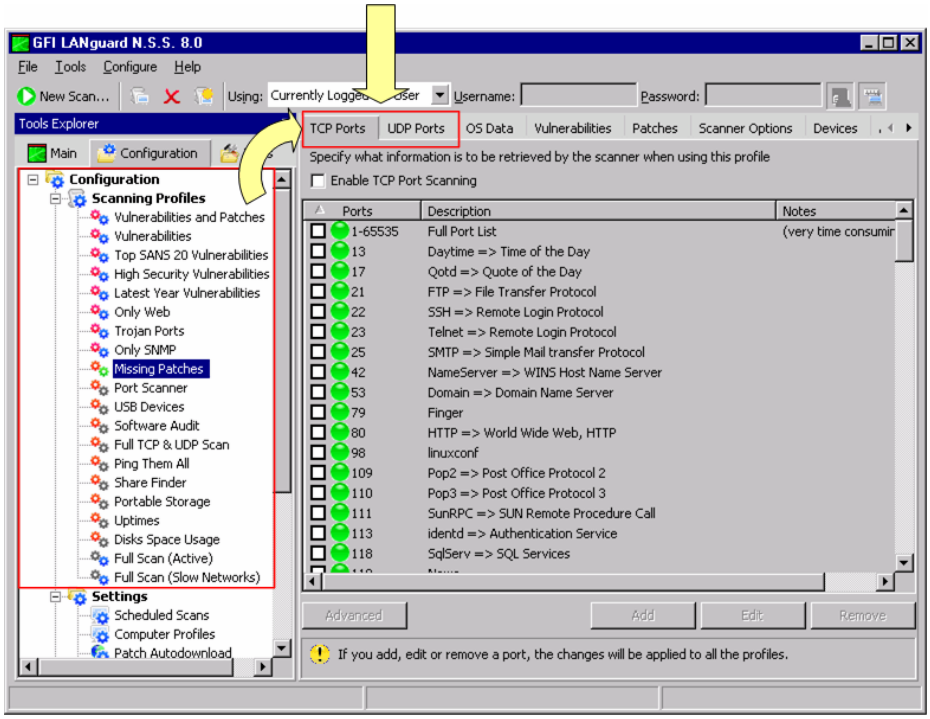
1. Click on the **Configuration** button and expand the **Configuration ▸ Settings** sub-node

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 updates.

NOTE: Changes in scanning profiles will become effective in the next new scan.

Configuring TCP/UDP ports scanning options



Screenshot 78 - Scanning Profiles properties: TCP Ports tab options

Enabling/disabling TCP/UDP Port scanning

To enable TCP Port Scanning in a particular scanning profile,

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. From the right pane click on the **TCP/UDP Ports** tab(s) accordingly.

3. Select the *'Enable TCP Port Scanning' and/or 'Enable UDP Port Scanning'* option(s) accordingly.

NOTE: TCP/UDP Ports scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable TCP/UDP port scanning in all profiles where TCP/UDP port scanning is required.

Configuring the list of TCP/UDP ports to be scanned

To configure which TCP/UDP ports will be processed by a scanning profile during vulnerability scanning :

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. Select the scanning profile that you wish to customize and from right pane, click on the **TCP Ports/UDP Ports** tab(s) accordingly.

3. Select the TCP/UDP ports that will be analyzed by this scanning profile.

Customizing the list TCP/UDP ports

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

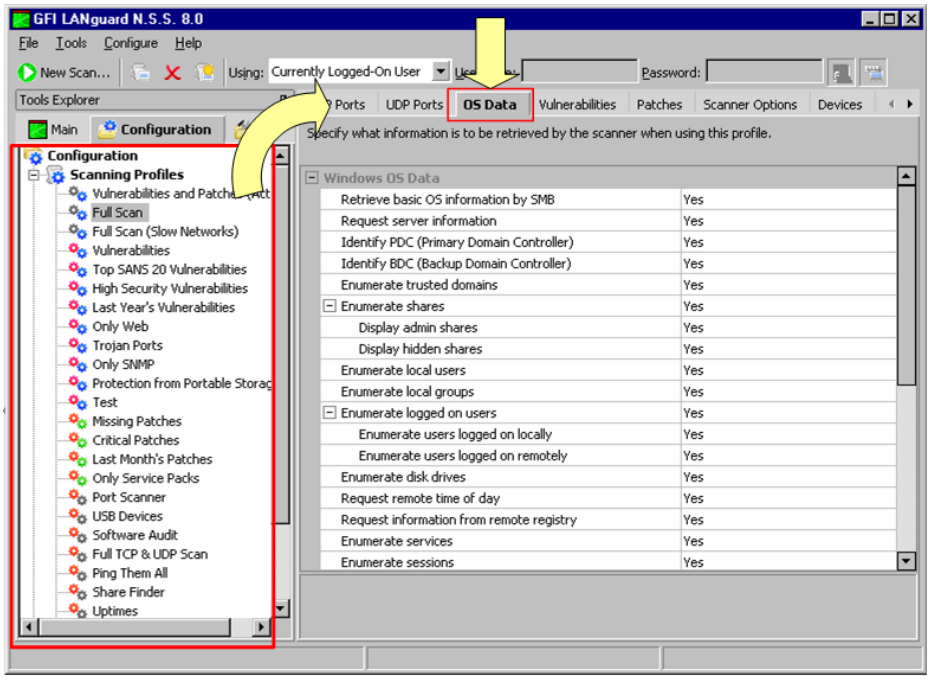
2. Select the scanning profile that you wish to customize and from right pane, click on the **TCP Ports/UDP Ports** tab(s) accordingly.

3. Customize the list of TCP/UDP Ports as follows:

- Use the **Add** button to add new TCP/UDP ports to the list. Specify the port number/range/description. Select the '*Is a Trojan port'* option if the new ports are commonly exploited by Trojans.
- Use the **Edit** button to modify TCP/UDP port parameters (i.e. port number and description).
- Use the **Remove** button to remove TCP/UDP ports from the list. To achieve this select the port(s) to be removed and click **Remove**.

NOTE: The list of supported TCP/UDP Ports is common for all profiles. Deleting a port from the list will make it unavailable for all scanning profiles. To exclude particular ports from scanning follow the procedure described in the 'Configuring the list of TCP/UDP ports to be scanned' section in this chapter.

Configuring OS data retrieval options



Screenshot 79 - Scanning Profiles properties: OS Data tab options

To specify which OS Data will be enumerated by a particular scanning profile during vulnerability scanning:

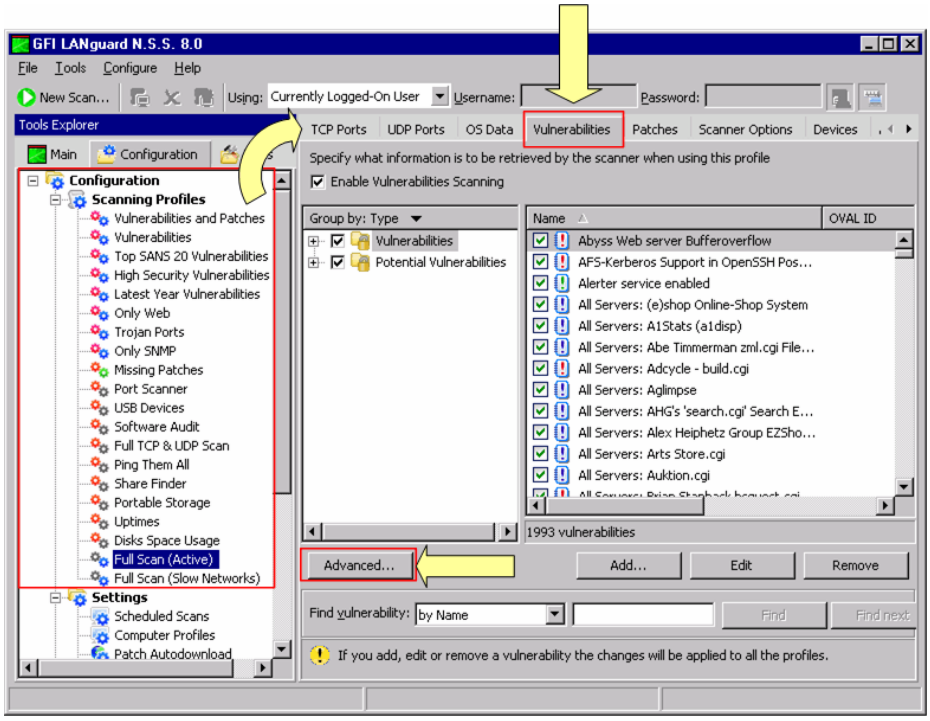
1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. Select the scanning profile that you wish to customize and from right pane, click on the **OS Data** tab.

3. From the right pane, expand the *'Windows OS Data' group and 'Linux OS Data'* group accordingly.

4. Select which Windows/Linux OS information will be retrieved by the security scanner from scanned targets. For example, to enumerate administrative shares in scan results, expand the *'Enumerate shares'* option and set the 'Display admin shares' option to *'Yes'.*

Configuring vulnerabilities scanning options



Screenshot 80 - Scanning Profiles properties: Vulnerabilities tab options

The scanning profiles that ship with GFI LANguard N.S.S. 8 are already pre-configured to execute a number of vulnerability checks on selected target. Nevertheless you can still disable vulnerability scanning as well as customize the list of vulnerability checks to be executed during a scan.

Enabling/disabling vulnerability scanning

To enable vulnerability scanning in a particular scanning profile,

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

2. Select the scanning profile that you wish to customize and from right pane, click on the **Vulnerabilities** tab.

3. Select the *'Enable Vulnerability Scanning'* option.

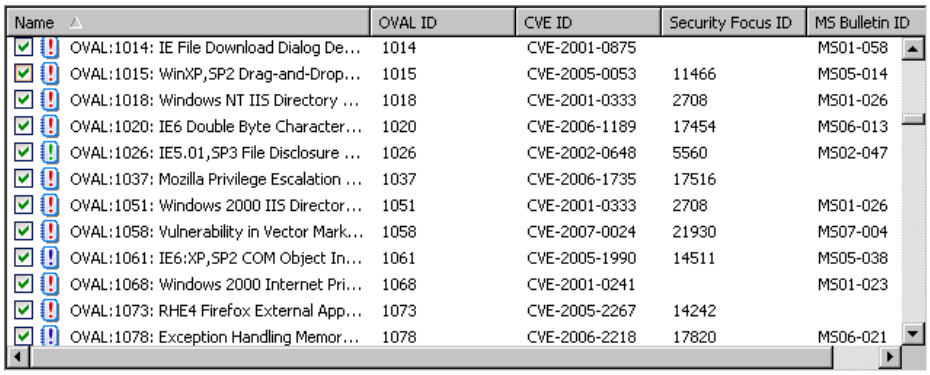
NOTE: Vulnerability scanning is configurable on a scan profile by scan profile basis. If in a particular profile this option is not selected, no vulnerability tests will be performed in the security audits carried out by this scanning profile.

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. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

2. Select the scanning profile to be customize and from right pane, click on the **Vulnerabilities** tab.



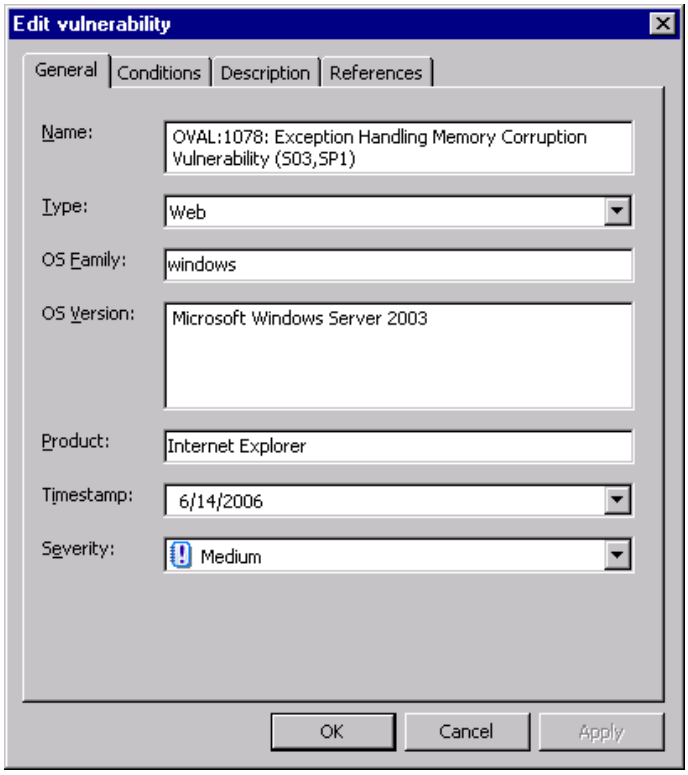
Name	OVAL ID	CVE ID	Security Focus ID	MS Bulletin ID
OVAL:1014: IE File Download Dialog De...	1014	CVE-2001-0875		MS01-058
OVAL:1015: WinXP,SP2 Drag-and-Drop...	1015	CVE-2005-0053	11466	MS05-014
OVAL:1018: Windows NT IIS Directory ...	1018	CVE-2001-0333	2708	MS01-026
OVAL:1020: IE6 Double Byte Character...	1020	CVE-2006-1189	17454	MS06-013
OVAL:1026: IE5.01,SP3 File Disclosure ...	1026	CVE-2002-0648	5560	MS02-047
OVAL:1037: Mozilla Privilege Escalation ...	1037	CVE-2006-1735	17516	
OVAL:1051: Windows 2000 IIS Director...	1051	CVE-2001-0333	2708	MS01-026
OVAL:1058: Vulnerability in Vector Mark...	1058	CVE-2007-0024	21930	MS07-004
OVAL:1061: IE6:XP,SP2 COM Object In...	1061	CVE-2005-1990	14511	MS05-038
OVAL:1068: Windows 2000 Internet Pri...	1068	CVE-2001-0241		MS01-023
OVAL:1073: RHE4 Firefox External App...	1073	CVE-2005-2267	14242	
OVAL:1078: Exception Handling Memor...	1078	CVE-2006-2218	17820	MS06-021

Screenshot 81 - Select the vulnerability checks to be run by this scanning profile

3. Select the vulnerability checks that you wish to execute through this scanning profile.

Customizing the properties of vulnerability checks

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



Screenshot 82 - Vulnerability properties dialog: General tab

To change the properties of a vulnerability check:

1. Right click on the vulnerability to customize and select **Properties**.

2. Customize the selected vulnerability check through the following tabs:

- **General** - Use this tab to customize the general details of a vulnerability check including vulnerability check name, vulnerability type, OS family, OS version, Product, Timestamp and Severity.
- **Conditions**: Use this tab to configure the operational parameters of this vulnerability check. These parameters will define whether a

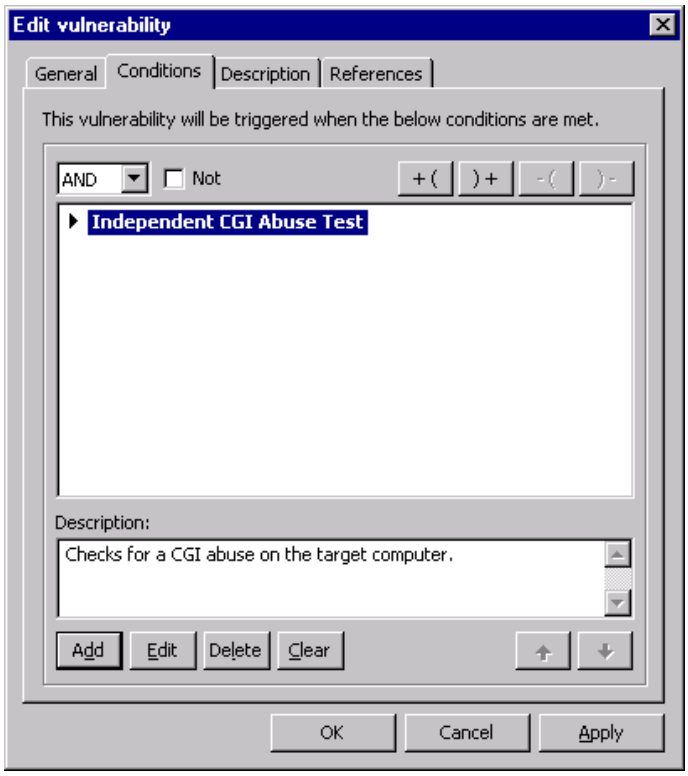
vulnerability check is successful or not. For information on how to configure vulnerability check conditions refer to the 'Vulnerability check conditions setup' section in this chapter.

- **Description:** Use this tab to customize the vulnerability check description.
- **References:** Use this tab to customize references and links which lead to relevant information in the OVAL, CVE, MS Security, Security Focus and SANS TOP 20 reports.

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

Vulnerability check conditions setup

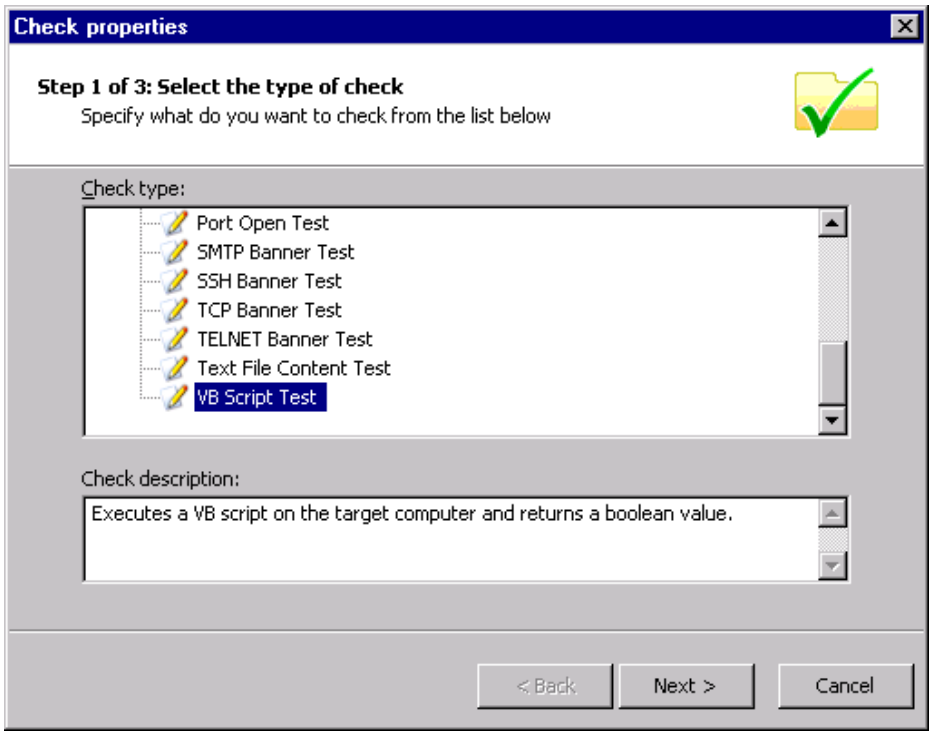
The **Conditions** tab enables you to add or customize conditions which define whether the computer(s) or network(s) being scanned are vulnerable or not. It is therefore of paramount importance that any custom checks defined in this section are set-up by qualified personnel that are aware of the ramifications of their actions.



Screenshot 83 - Vulnerability conditions setup tab

To add a vulnerability check condition:

1. Click on the **Add** button.

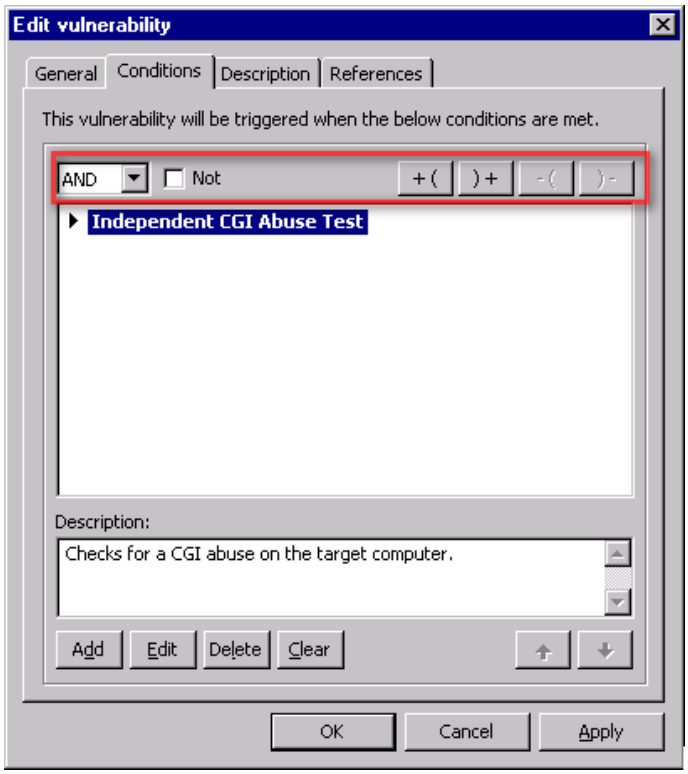


Screenshot 84 - Check properties wizard

2. Select the type of check to be configured and click **Next**.

3. Define the object to examine and click **Next**.

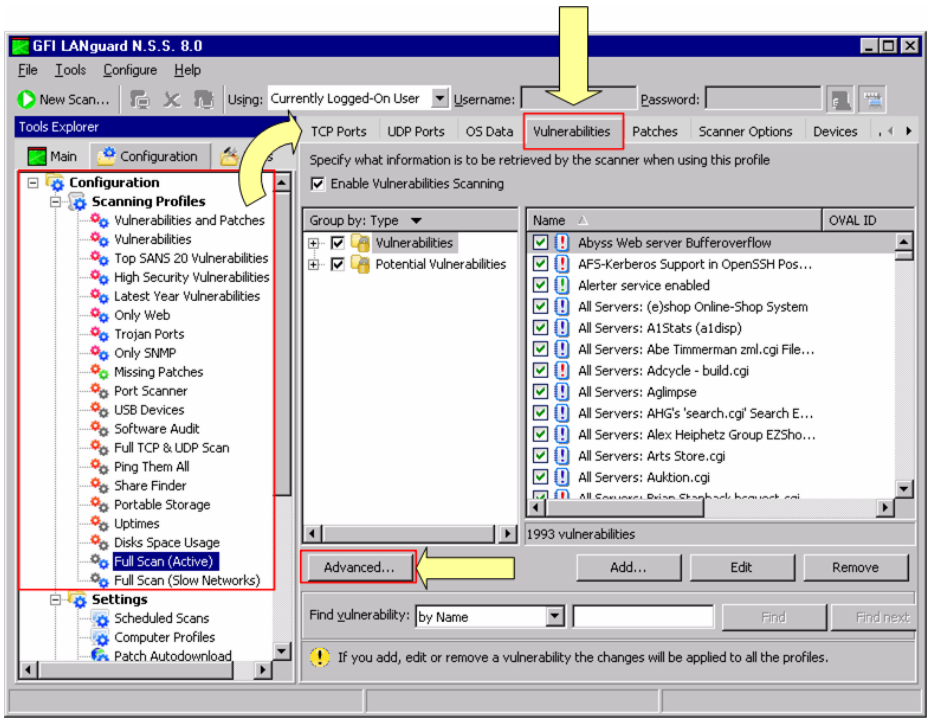
4. Set attributes/desired parameters and click **Finish** to finalize your settings.



Screenshot 85 - Edit vulnerability

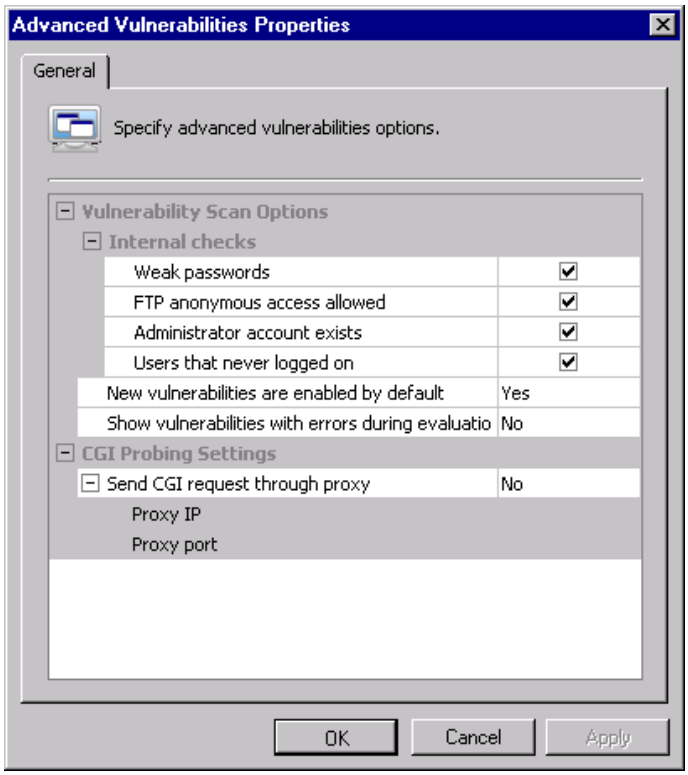
5. If more than one condition is setup, define conditional operators and click **OK** to finalize your configuration settings.

Vulnerability checks - advanced options



Screenshot 86 - Scanning Profiles properties

Use the **Advanced** button included in the **Vulnerabilities** tab to bring up the advanced vulnerabilities scanning options.

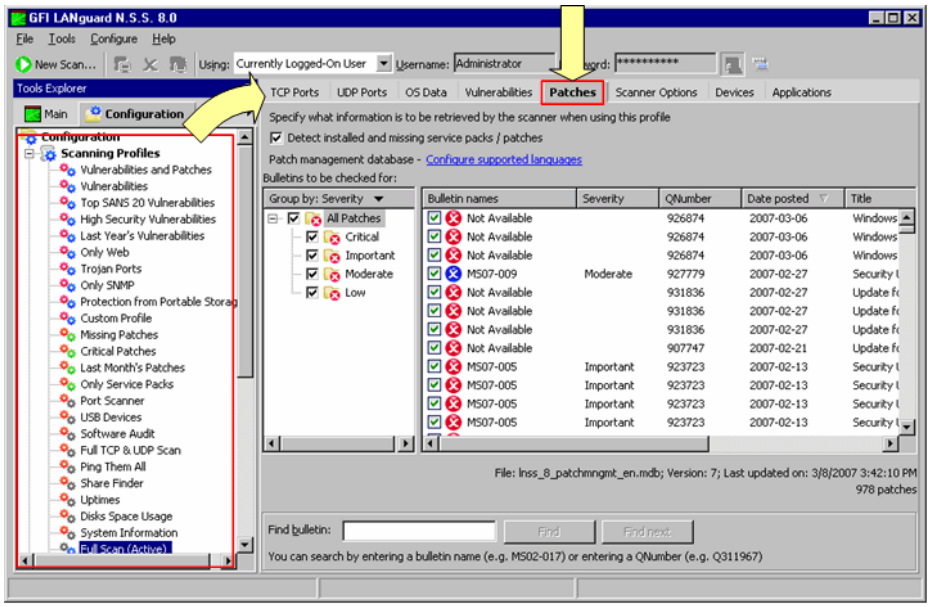


Screenshot 87 - Advanced vulnerability scanning dialogs

Use these options to:

- Configure extended vulnerability scanning features that check your target computers for weak passwords, anonymous FTP access, and unused user accounts.
- Configure how GFI LANguard N.S.S. will handle newly created vulnerability checks.
- 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 that is behind a firewall to a target web server that is 'outside' the firewall (for example, Web servers that are on a DMZ). The firewall will generally block all the CGI requests that are directly sent by GFI LANguard N.S.S. to a target computer that is in front of the firewall. To avoid this, set the *'Send CGI requests through proxy'* option to *'Yes'* and specify the name/IP address of your proxy server and the communication port which be used to convey the CGI request to the target.

Configuring patch scanning options



Screenshot 88 - Scanning Profiles properties: Patches tab options

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

Enabling/disabling missing patch detection checks

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

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

2. Select the scanning profile that you wish to customize and from right pane, click on the **Patches** tab.

3. Select the *'Detect installed and missing service packs/patches'* option.

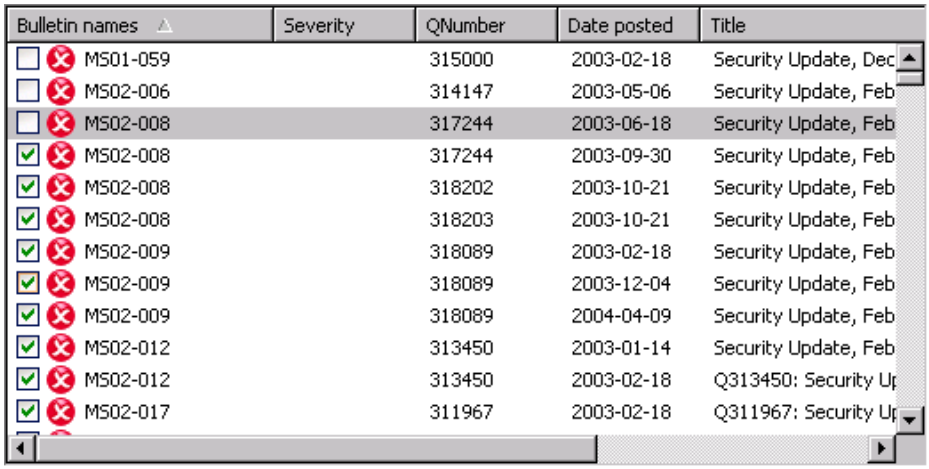
NOTE: Missing patch scanning parameters are configurable on a scan profile by scan profile basis. Make sure to enable missing patch scanning in all profiles where missing patch scanning is required.

Customizing the list of software patches to be scanned

To specify which missing security updates will be enumerated and processed by a scanning profile:

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

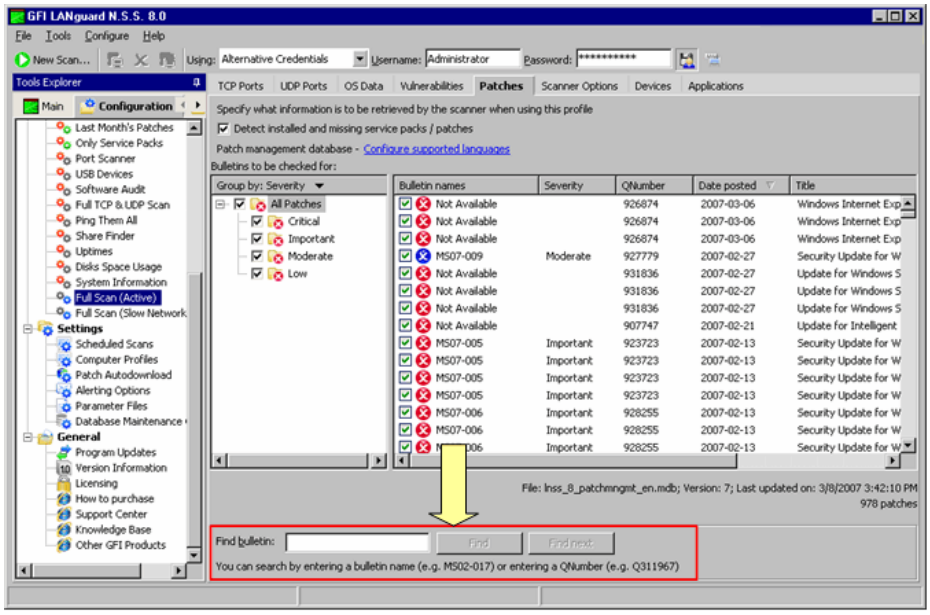
2. Select the scanning profile that you wish to customize and from right pane, click on the **Patches** tab.



Screenshot 89 - Selecting the missing patches to be enumerated

3. Select/unselect which missing patches will be enumerated by this scanning profile.

Searching for bulletin information

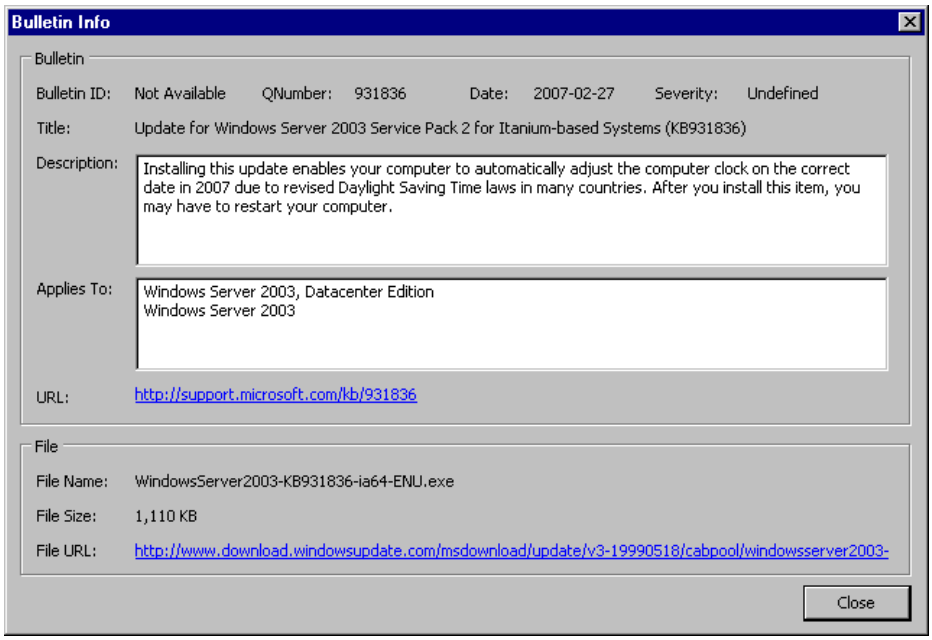


Screenshot 90 – Searching for bulletin information

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.

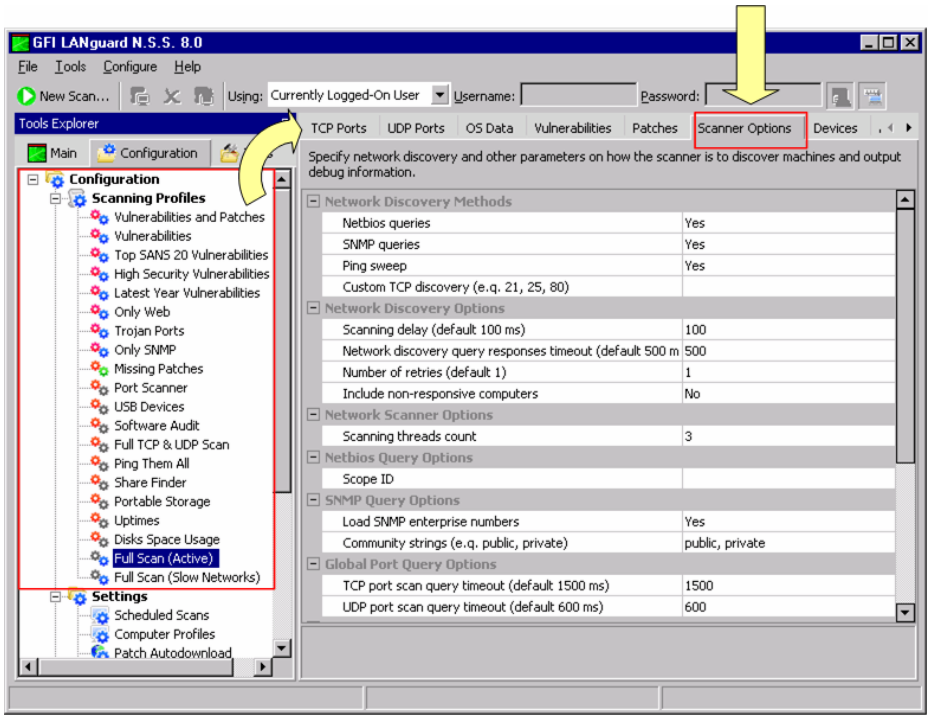
2. Click on **Find** to start searching for your entry.



Screenshot 91 - Extended bulletin information

Configuring the security scanning options

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.

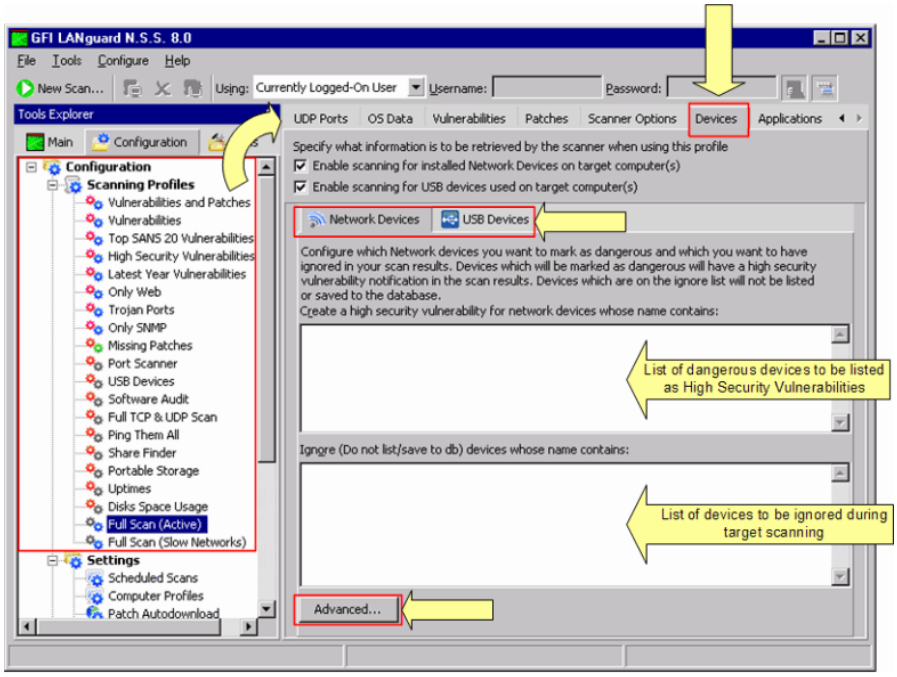


Screenshot 92 - Scanning Profiles properties: Scanner Options tab

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

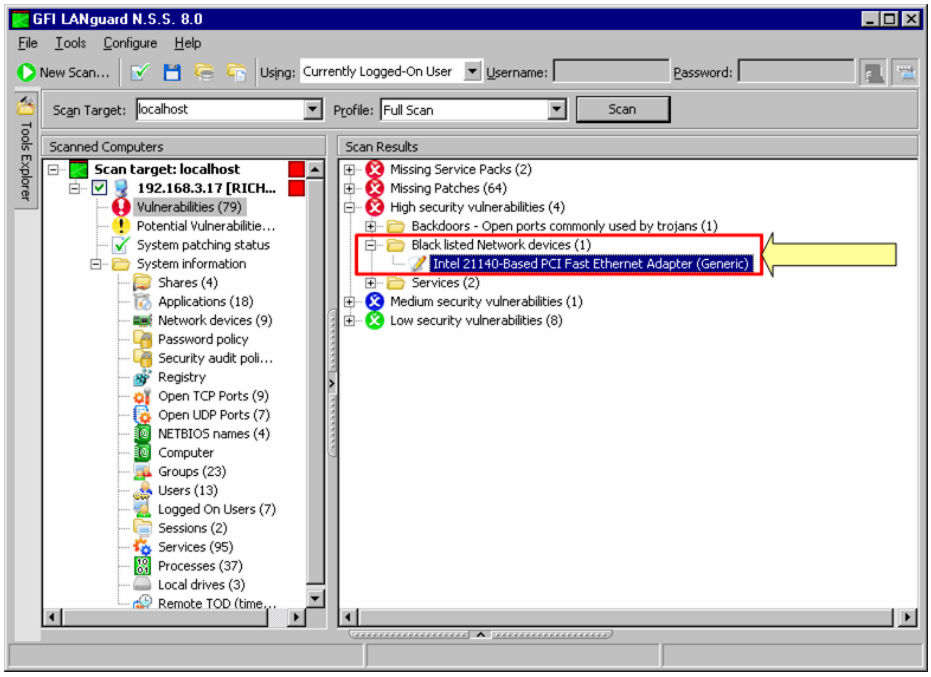
NOTE: Configure these parameters with extreme care! An incorrect configuration can affect the security scanning performance of GFI LANguard N.S.S.

Configuring the attached devices scanning options



Screenshot 93 - The Devices configuration page: Network Devices tab options

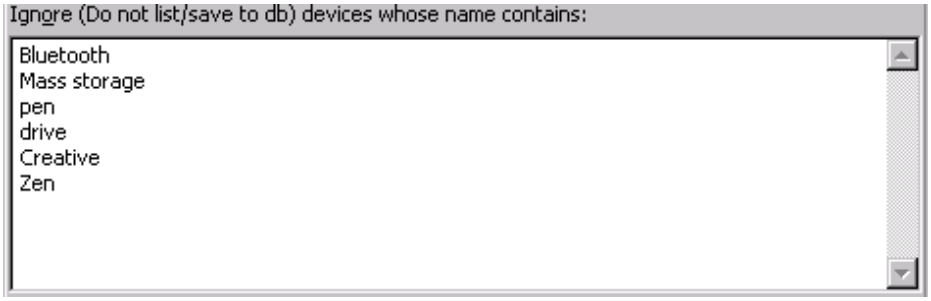
Use the **Devices** tab to enable the scanning and reporting of network and USB devices installed on your target computers.



Screenshot 94 - Dangerous network devices are listed as High Security Vulnerabilities

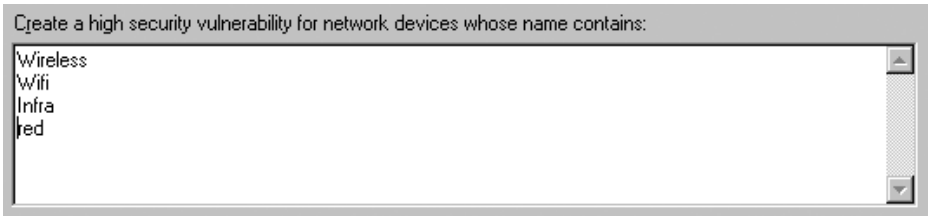
Together with device enumeration, you can further configure GFI LANguard N.S.S. to generate high security vulnerability alerts whenever particular USB and network hardware is detected. This is achieved by compiling a list of unauthorized/blacklisted network and USB devices that you want to be alerted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

You can also configure GFI LANguard N.S.S. to exclude from the scanning process particular USB devices that you consider as 'safe' such as USB keyboards. This is achieved by compiling a safe/whitelist of USB devices to be ignored during scanning.



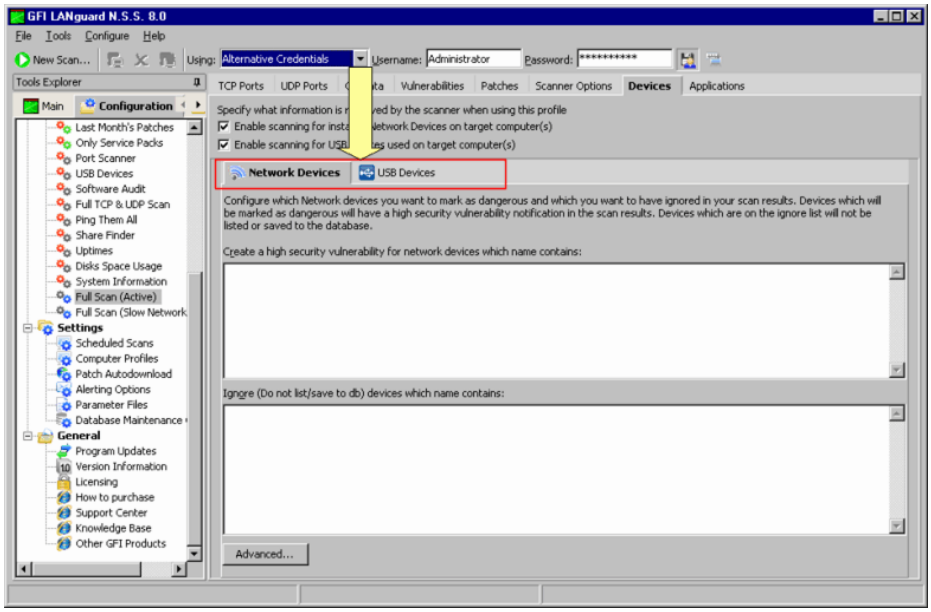
Screenshot 95 - List of authorized network devices

For example, you can create a generic USB device scanning profile that 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..



Screenshot 96 - List of unauthorized/blacklisted network devices

Similarly you can create a separate scanning profile that enumerates only Bluetooth dongles and wireless NIC cards connected to your target computers However, in this case you must specify 'Bluetooth' and 'Wireless' or 'WiFi' in the unauthorized network and USB lists of your scanning profile.

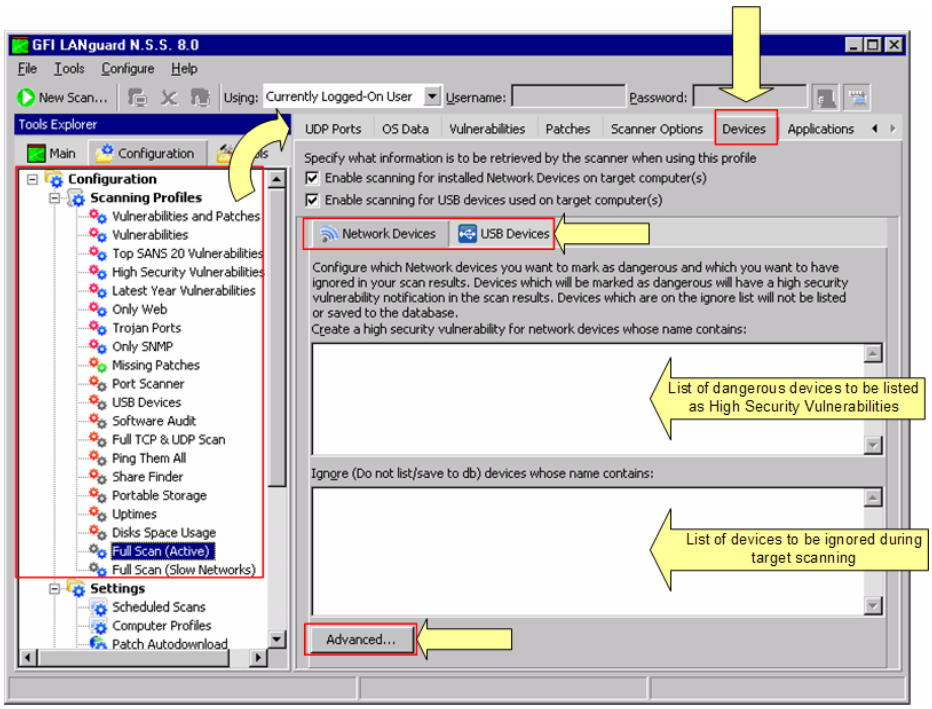


Screenshot 97 - Network and USB Devices tabs

All the device scanning configuration options are accessible through the two sub-tabs contained in the devices configuration page. These are the **Network Devices** tab and the **USB Devices** tab.

- Use the **Network Devices** sub-tab to configure the attached network devices scanning options and blacklisted (unauthorized)/whitelisted (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 98 - Device configuration page: Network Devices tab options

Enabling/disabling checks for installed network devices

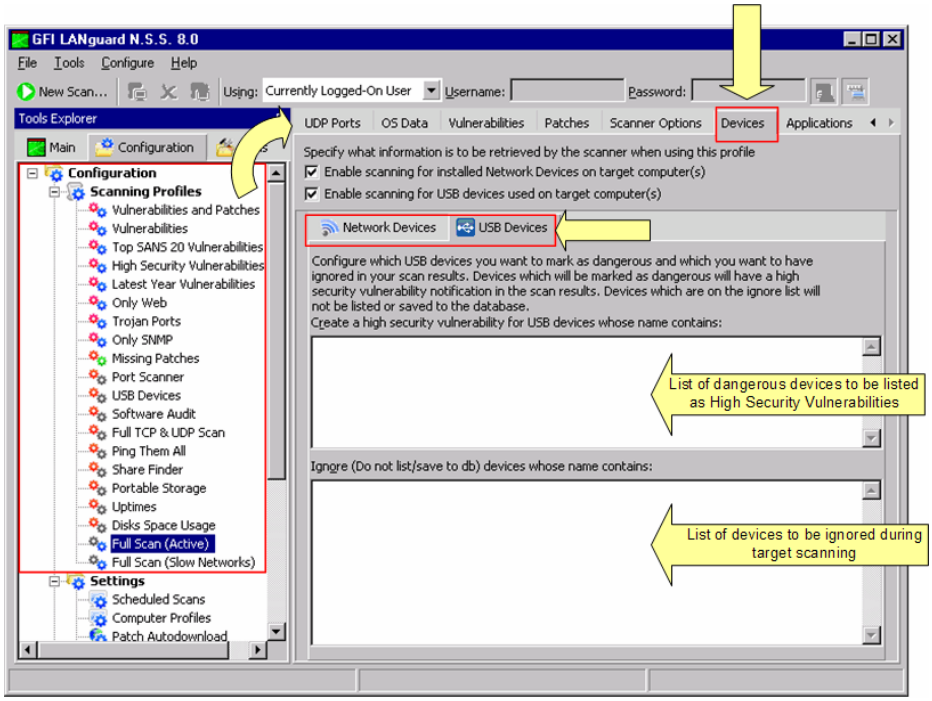
To enable network device scanning in a particular scanning profile:

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. Select the scanning profile that you wish to customize and from right pane, click on the **Devices** tab.

3. Select 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. Make sure to enable network device scanning in all profiles where this is required.



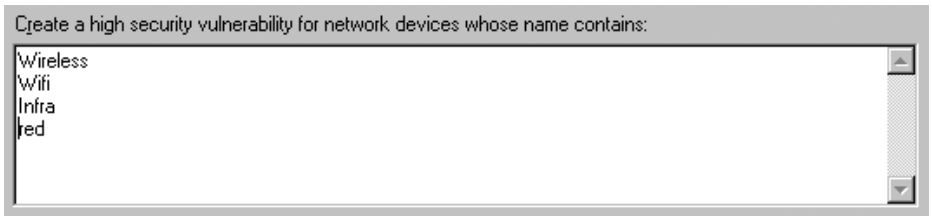
Screenshot 99 - Devices configuration page: Unauthorized devices and Ignore devices lists

Compiling a network device blacklist/whitelist

To compile a network device blacklist/whitelist:

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. Select the scanning profile that you want to customize and from the right pane, click on the **Devices** tab.



Screenshot 100 - List of unauthorized/blacklisted network devices

3. Click on the **Network Devices** tab and do as follows:

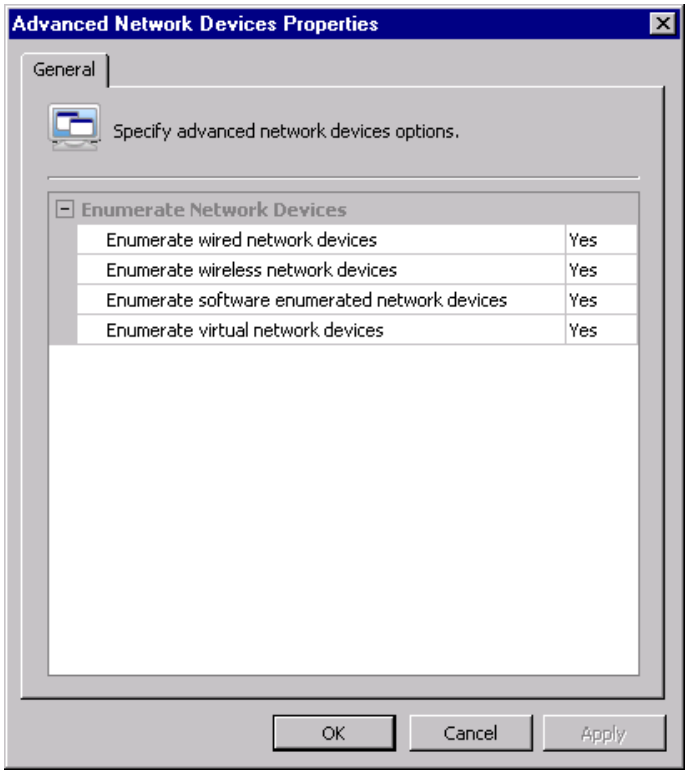
- To create a network device blacklist, specify which devices you want to classify as high security vulnerabilities in the space

provided under *'Create a high security vulnerability for network devices whose name contains:'* For example, if you enter the word "wireless" you will be notified through a high security vulnerability alert when a device whose name contains the word "wireless' is detected.

- To create a network device whitelist, specify which devices you want to ignore during network vulnerability scanning in the space provided under '*Ignore devices (Do not list/save to db) whose name contains*:'.

NOTE: Include only one network device name per line.

Configuring advanced network device scanning options



Screenshot 101 - 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:

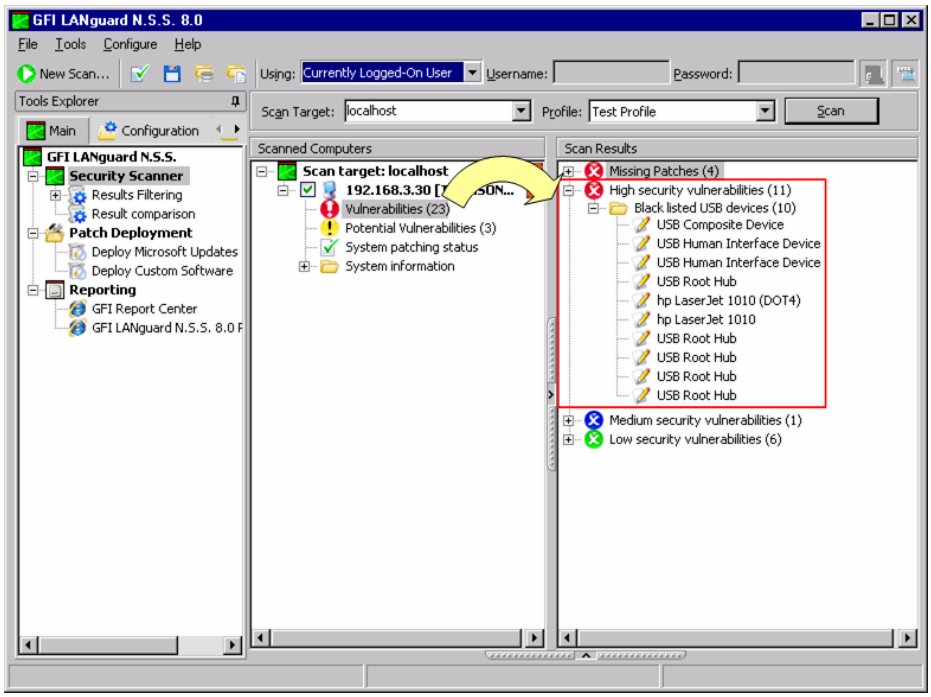
1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

2. Select the scanning profile that you wish to customize and from right pane, click on the **Devices** tab.

3. From the **Network Devices** tab which opens by default, click the **Advanced** button at the bottom of the page.

4. Set the required options to *'Yes'* and on completion click **OK** to finalize your settings.

Scanning for USB devices



Screenshot 102 - 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. Select the **Configuration** button and expand the **Configuration** ▸ **Scanning Profiles** sub-node

2. Select the scanning profile that you wish to customize and from right pane, click on the **Devices** tab.

3. Select the *'Enable scanning for USB Devices installed on the target computer(s)'* option.

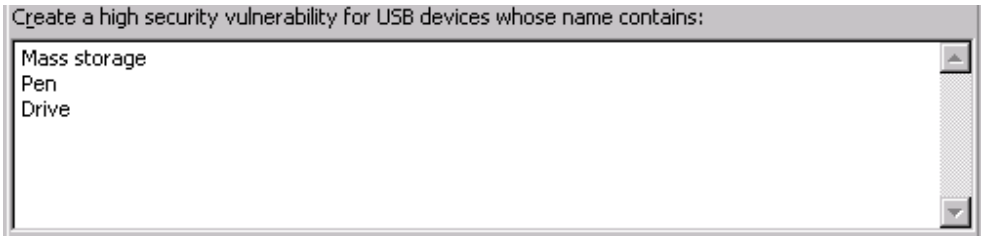
NOTE: USB device scanning is configurable on a scan profile by scan profile basis. Make sure to enable USB device scanning in all profiles where this is required.

Compiling a USB devices blacklist/whitelist

To compile a list of unauthorized/dangerous USB devices:

1. Select the **Configuration** button, expand **Configuration** ▸ **Scanning Profiles** node and select the scanning profile that you wish to customize.

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



Screenshot 103 - List of unauthorized/blacklisted USB devices

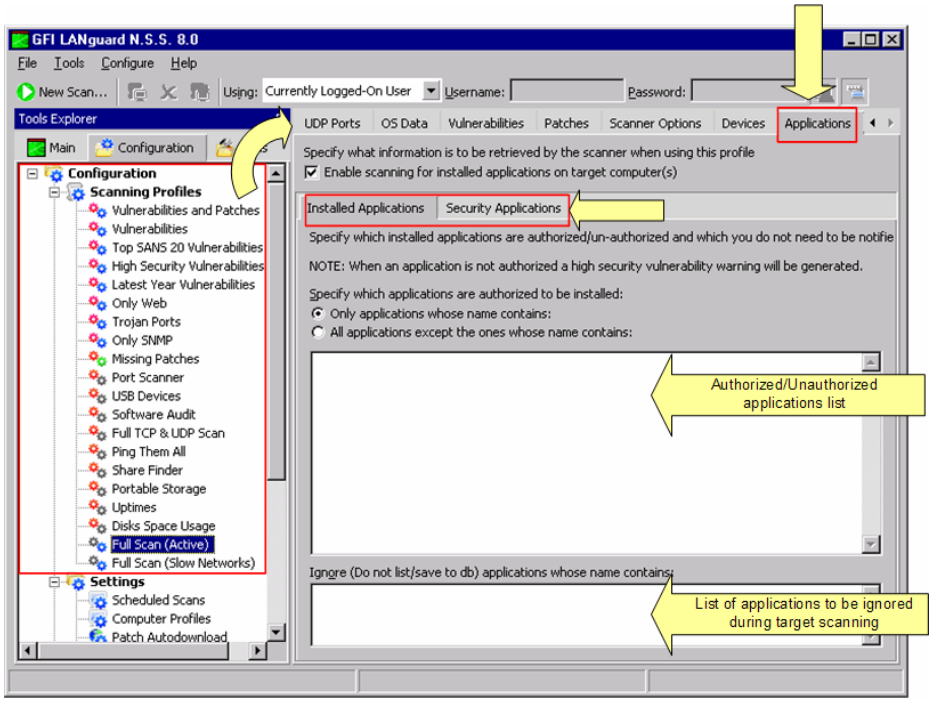
3. Click on the **USB Devices** sub-tab and do as follows:

- To create a USB device blacklist, specify which devices you want to classify as high security vulnerabilities in the space provided under *'Create a high security vulnerability for USB devices whose name contains:'* For example, if you enter the word "iPod" you will be notified through a high security vulnerability alert when a USB device whose name contains the word "iPod' is detected.
- To create a USB device whitelist, specify which USB devices you want to ignore during network vulnerability scanning in the space provided under '*Ignore devices (Do not list/save to db) whose name contains*:'.

NOTE: Include only one USB device name per line.

Configuring 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 104 - 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.

Scanning installed applications

Screenshot 105 - 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

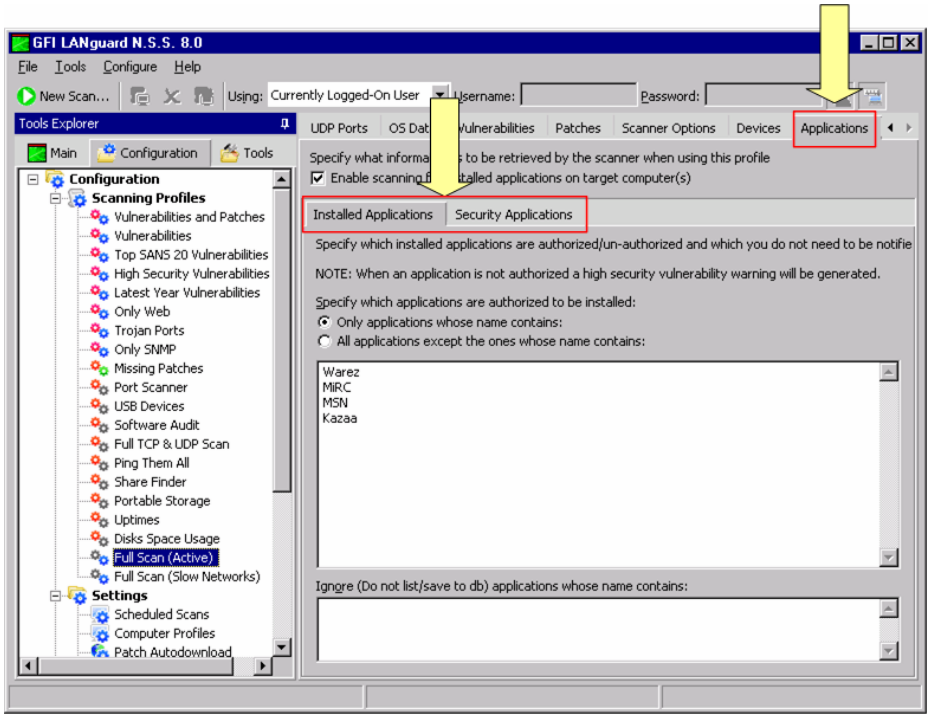
To enable installed applications scanning in a particular scanning profile:

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. Select the scanning profile that you wish to customize and from right pane, click on the **Applications** tab.

3. Select the *'Enable scanning for installed applications on target computers'* option.

NOTE: Installed applications scanning is configurable on a scan profile by scan profile basis. Make sure to enable installed applications scanning in all profiles where this is required.



Screenshot 106 - The Applications tab: Installed Applications tab options

Compiling an installed applications blacklist/whitelist

To compile an installed applications blacklist/whitelist:

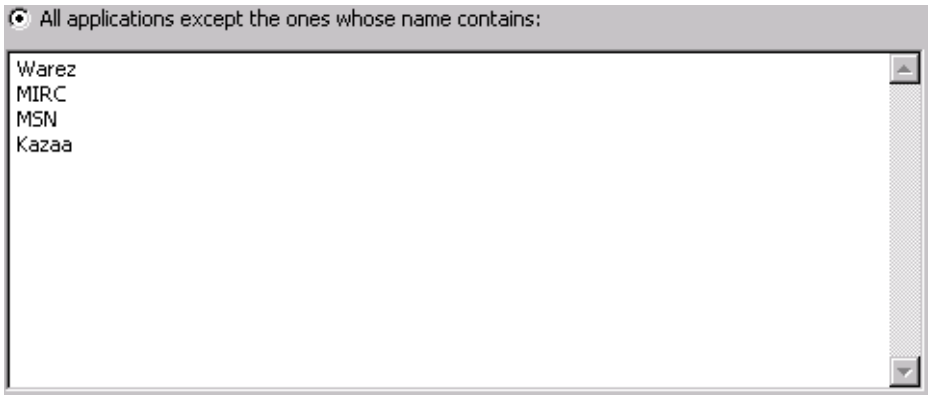
1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node

2. Select the scanning profile that you wish to customize and from right pane, click on the **Applications** tab.

3. Click the **Installed Applications** tab and select one of the following options::

- *'Only applications whose name contains:'* – Select this option to setup a blacklist/whitelist of applications whose name matches specific criteria.
- *'All applications except the ones whose name contains:'* - Select this option to setup a blacklist/whitelist of applications whose name does not match specific criteria.

4. Define application blacklist/whitelist by doing as follows:

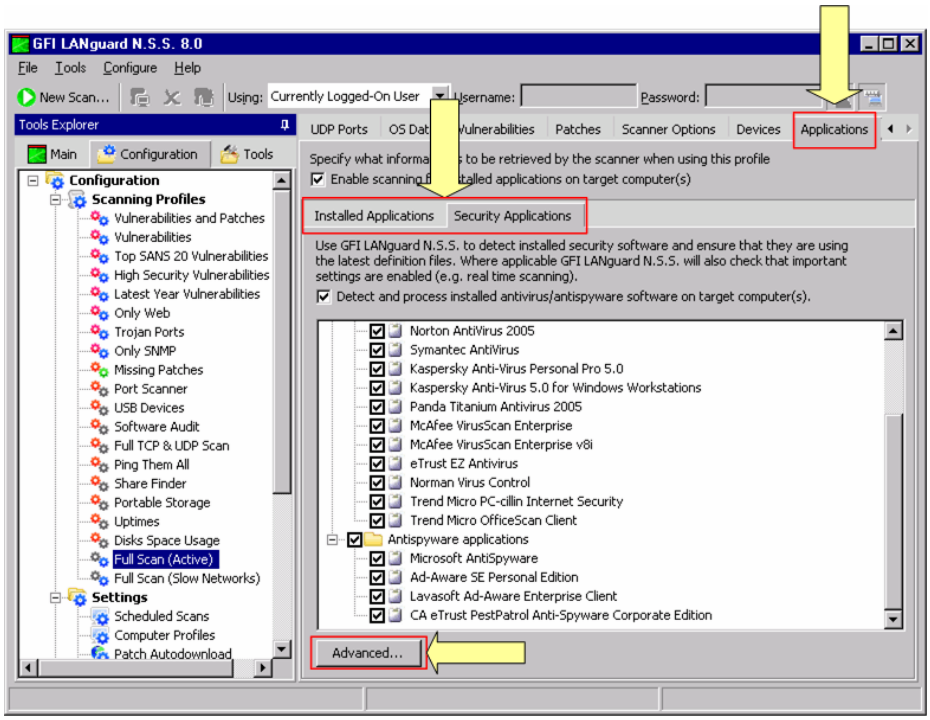


Screenshot 107 - List of unauthorized applications

- To create an applications blacklist, specify which applications you want to classify as high security vulnerabilities in the space provided under *'Only applications whose name contains:'.* 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.
- To create a applications whitelist, specify which applications you want to ignore during network vulnerability scanning in the space provided under '*Ignore (Do not list/save to db) applications whose name contains*:'.

NOTE: Include only one application name per line.

Scanning security applications



Screenshot 108 - The Applications configuration page: Security Applications tab options

GFI LANguard N.S.S. ships with a default list of anti-virus and anti-spyware applications that 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. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

2. Select the scanning profile that you wish to customize and from right pane, click on the **Applications** tab.

3. Click the **Security Applications** tab and select the '*Detect and process installed anti-virus/anti-spyware software on target computers'* option.

NOTE: Security applications scanning is configurable on a scan profile by scan profile basis. Make sure to enable security applications scanning in all profiles where this is required.

Customizing the list of security application for scanning

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

1. Select the **Configuration** button and expand the **Configuration ▸ Scanning Profiles** sub-node.

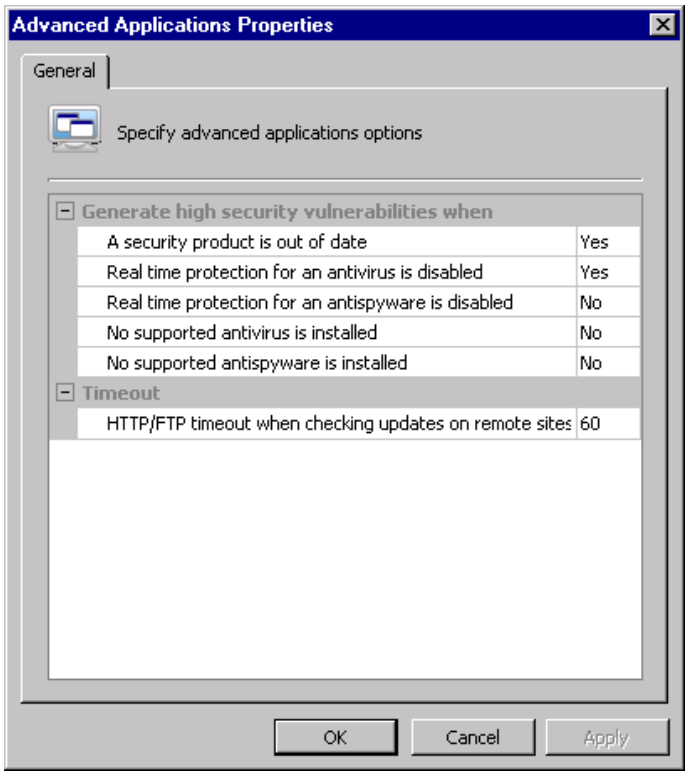
2. Select the scanning profile that you wish to customize and from right pane, click on the **Applications** tab.

Screenshot 109 - Selecting the security applications to be investigated

3. Click on the **Security Applications** tab and select the security applications that you wish investigate.

4. Click **OK** to finalize your settings.

Configuring security applications - advanced options



Screenshot 110 - Advanced configuration options dialog

Use the **Advanced** button included in the **Security Applications** configuration page to configure extended security product checks that 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 anti-spyware application is found disabled.
- None of the selected anti-virus or anti-spyware software is currently installed on the scanned target computer.

10. GFI LANguard N.S.S. updates

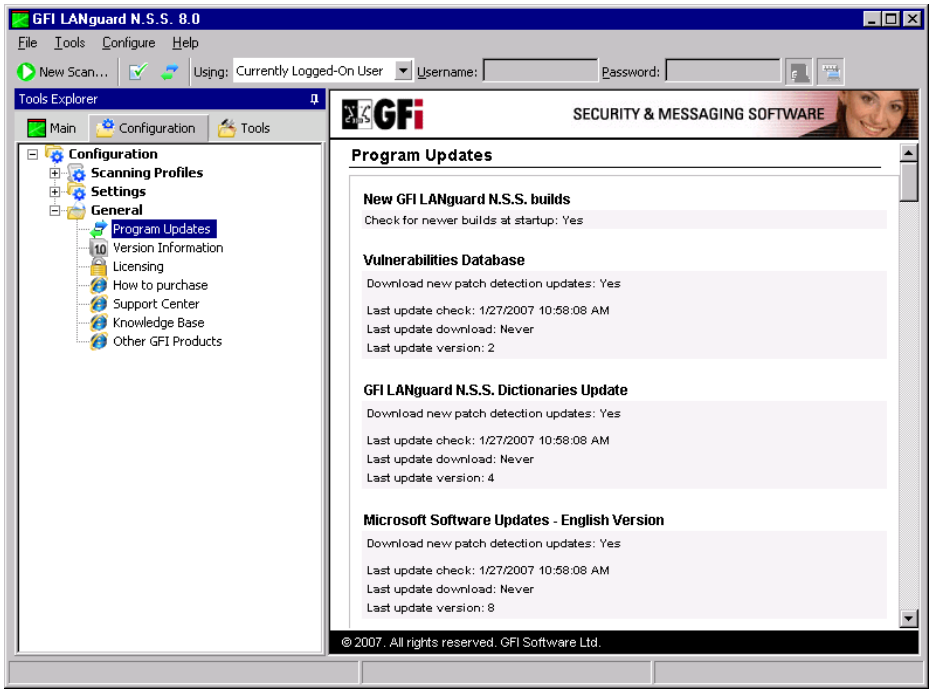
Introduction

Periodically GFI releases program updates aimed at enhancing the performance and functionality of the product such as the addition of new vulnerability checks.

Apart from its own program updates, GFI LANguard N.S.S. 8 can also download Microsoft product updates including missing patches and service packs for operating systems as well as desktop applications such as MS Office XP/2007.

In this chapter you will learn how to check, download and update GFI LANguard N.S.S. You will also learn how to configure GFI LANguard N.S.S. so to enable/disable automatic checking for newer builds at application startup.

Checking the version of current installed updates

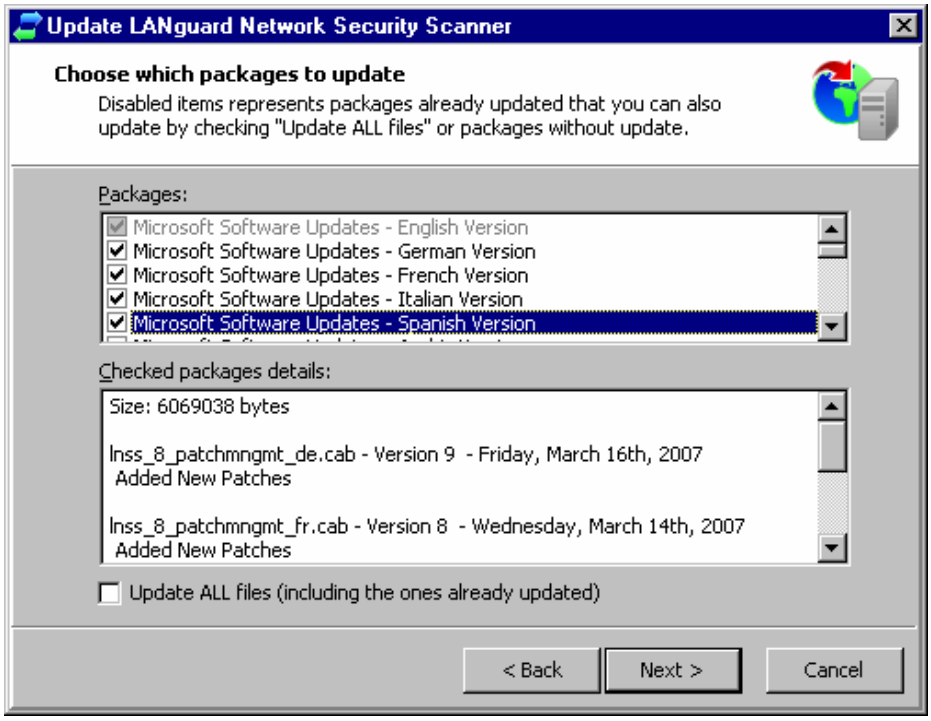


Screenshot 111 - Details on the currently installed updates

Select the **Configuration** button and click on **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 the GFI LANguard N.S.S. management console. Every 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 Microsoft product updates in different languages



Screenshot 112 - Selecting the Microsoft update files

Out of the box, GFI LANguard N.S.S. supports multilingual patch management for all Unicode compliant languages. 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, Portuguese/Brazilian, Russian, Swedish, Chinese, Chinese (Taiwan), Greek, and Turkish.

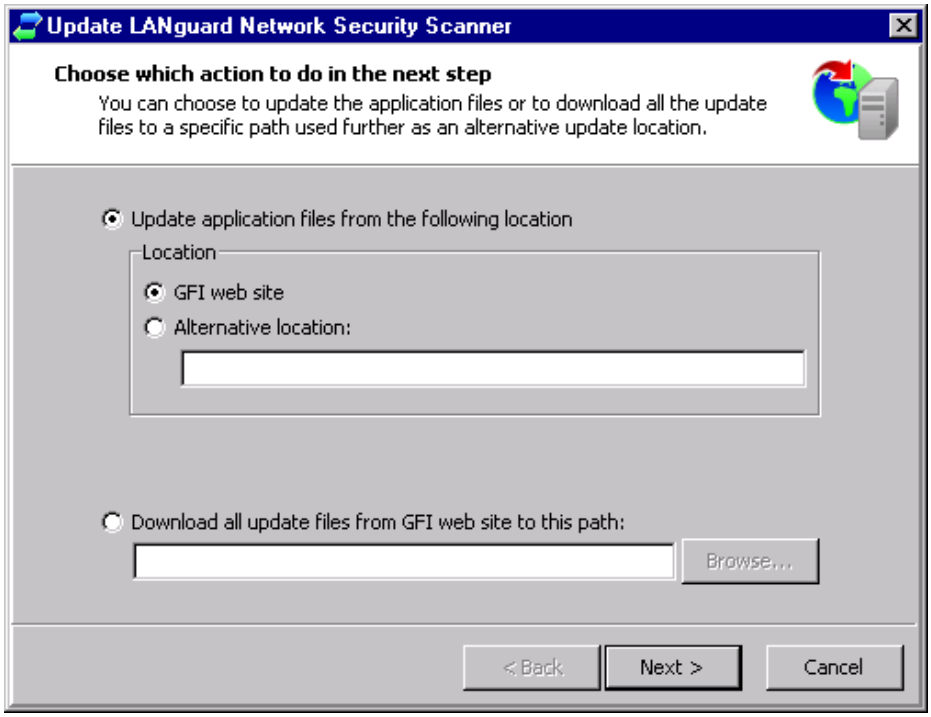
Information on how to download and deploy multilingual 'Microsoft Update Files' is provided further on in this chapter.

Starting program updates manually

To manually start GFI LANguard N.S.S. program updates:

1. Select the **Configuration** button right click and expand the **General** node

2 Right-click the **Program Updates** sub-node and select **Check for Updates…**. This will bring up the 'Check for updates wizard'.

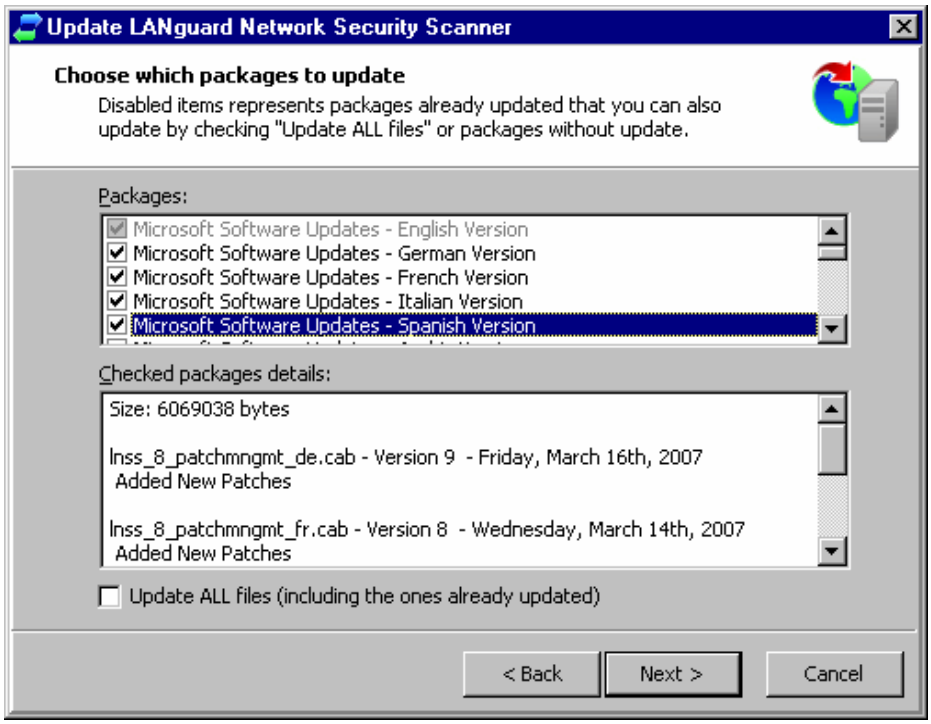


Screenshot 113 - The Check for Updates wizard: Stage 1

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

4. To change the default download path, select the *'Download all update files… to this path'* option and provide the alternate download path.

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



Screenshot 114 - The Check for updates Wizard: Stage 2

6. Select the updates to be downloaded and click **Next**. 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, including other ones already updated.

7. Click on **Start** to initiate the update process.

Check for software updates at program startup

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

1. Select the **Configuration** button right click and expand the **General** node.

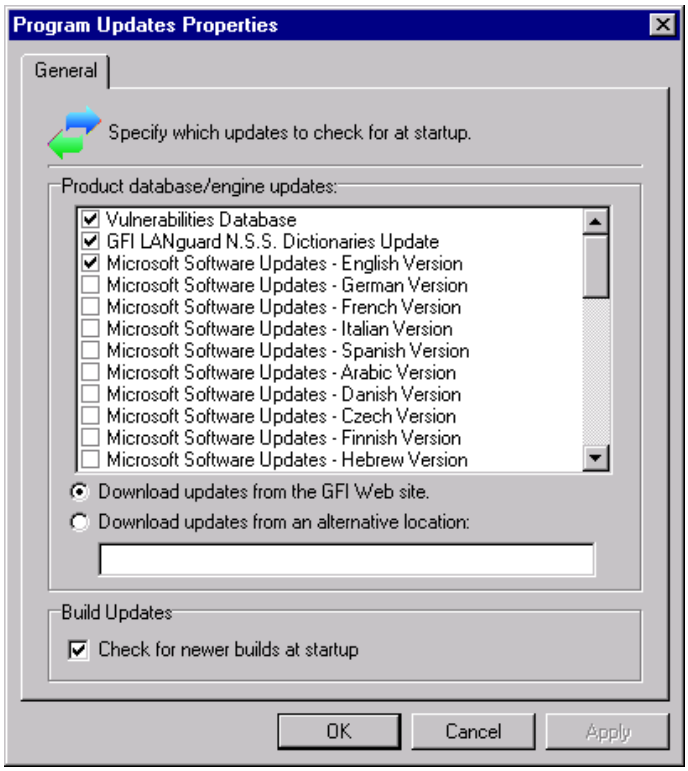
2 Right-click the **Program Updates** sub-node and select **Properties**. This will bring up the Program Updates Properties dialog.

Screenshot 115 - The 'Check for newer builds at startup' option

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

Configure which updates to check on program startup

To configure which updates are checked at program startup:



Screenshot 116 - Program Updates Properties dialog

1. Select the **Configuration** button right click and expand the **General** node.

2 Right-click the **Program Updates** sub-node and select **Properties**. This will bring up the Program Updates Properties dialog.

3. Select the updates to be downloaded and specify the location from where the selected program updates will be downloaded.

4. Click **OK** to finalize your settings.

11. Patch management: Deploying Microsoft Updates

Introduction

Apart from automatically downloading Microsoft patches and service packs, GFI LANguard N.S.S. can also deploy downloaded updates network-wide as well as recall any patches that have already been deployed. Patches are generally recalled due to newly discovered vulnerabilities or problems caused by the installation of these updates such as conflict issues with present software or hardware. Examples of updates recalled by the manufacturer include patches MS03-045 and MS03-047 for Exchange that were released by Microsoft on October 15, 2006.

Both patch deployment and patch rollback operations are managed by an agent service which handles all file transfers between GFI LANguard N.S.S. and the remote targets. This service is silently (and automatically) installed on the remote target computer during patch deployment process.

NOTE 1: To successfully deploy missing patches ensure that GFI LANguard N.S.S. is running under an account that has administrative privileges.

NOTE 2: Ensure that the 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.

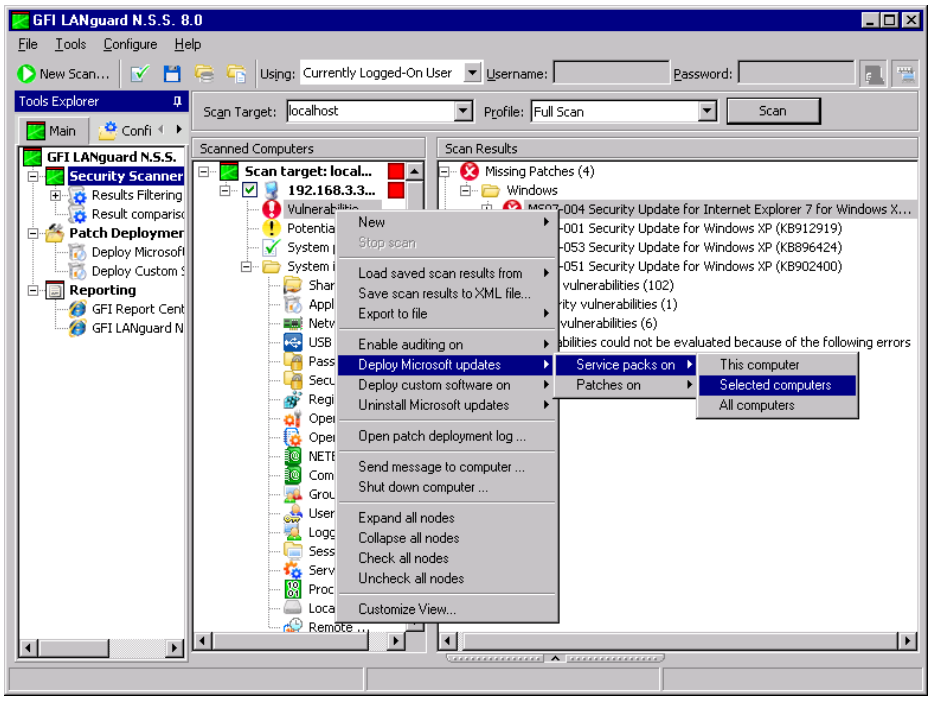
NOTE 3: A complete list of Microsoft products for which GFI LANguard N.S.S. can download and deploy patches is available on http://kbase.gfi.com/showarticle.asp?id=KBID001820.

In this chapter you will learn how to:

- Specify target computers for patch deployment
- Specify which Microsoft patches/updates must be deployed
- Sort patches and change download priorities
- Download patches and service packs
- Start the deployment process and monitor its progress.
- Recall patches that were already deployed on target computers.

Selecting target computers for patch deployment

After scanning your network, you can start the deployment of missing patches and service packs on target computers.



Screenshot 117 - Deploying missing service packs and patches

To specify on which target computers patches and service packs will be deployed do as follows:

To deploy 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

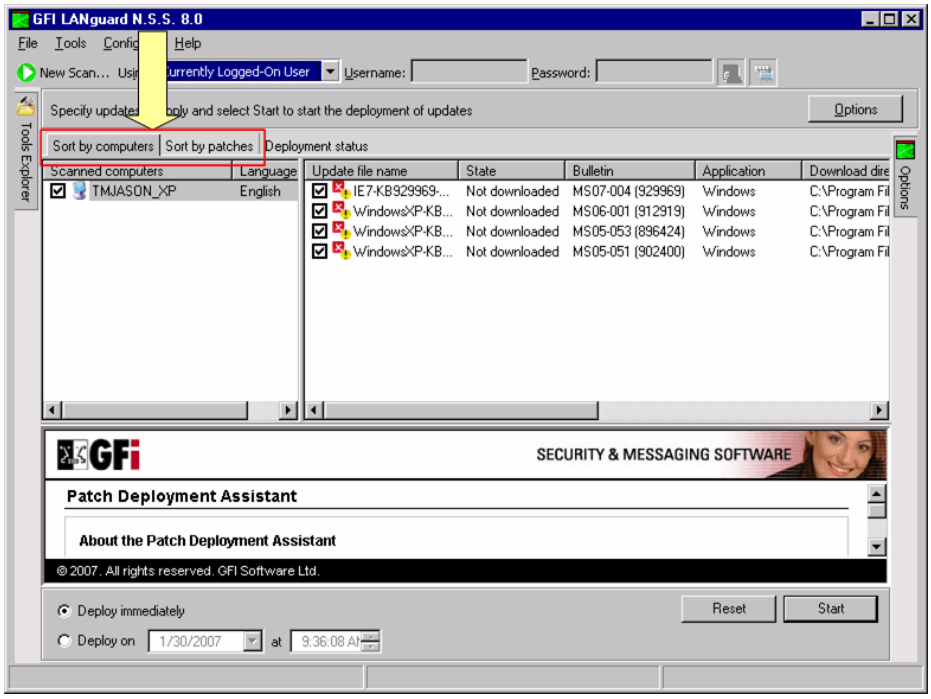
1. From the 'Scanned Computers' (middle) pane, select the computers to be updated.

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

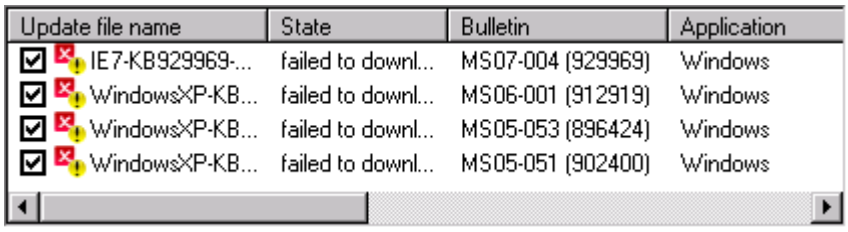
From the 'Scanned Computers' (middle) pane, right-click on any of the listed target computers and select **Deploy Microsoft updates ▸ [Service packs on** or **Patches on] ▸ All computers.**

Selecting which patches to deploy



Screenshot 118 - 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 management console together with the list of target computers selected and the English/non-English updates that will be downloaded and deployed on the enumerated targets.



Screenshot 119 - Selecting patches to be downloaded and deployed

NOTE: GFI LANguard N.S.S. can be configured to automatically download and any missing patches and service packs discovered during a network security scan. For more information please refer to the 'Configuring Patch Autodownload' section in the 'Configuring GFI LANguard N.S.S.' chapter of this manual.

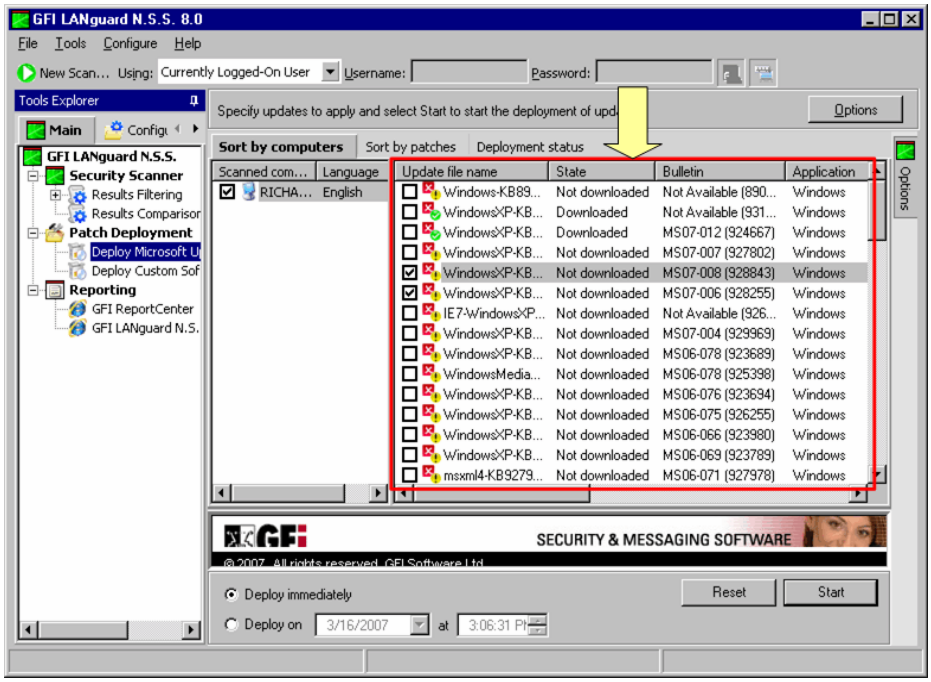
Sorting the list of pending software updates

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.

Download patches and service pack files

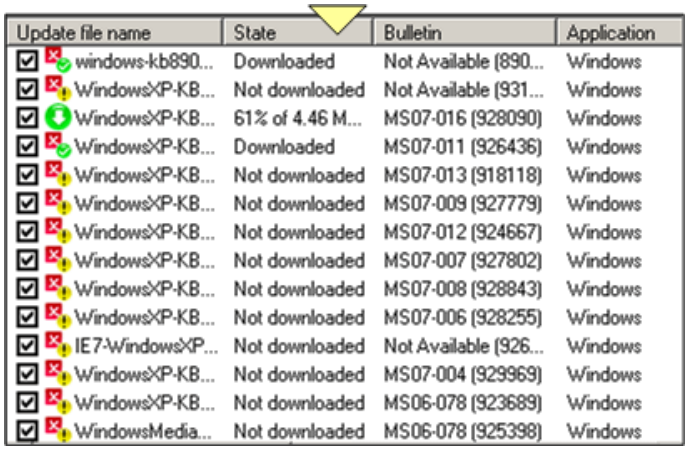


Screenshot 120 - A list of patches to be downloaded

To initiate the download of selected patches and service packs do as follows:

- To download a specific patch or service pack, right-click on the respective patch file and select **Download File**.
- To download all selected patches and service packs, right-click on any patch file and select **Download all checked files**.

Identifying the download queue status



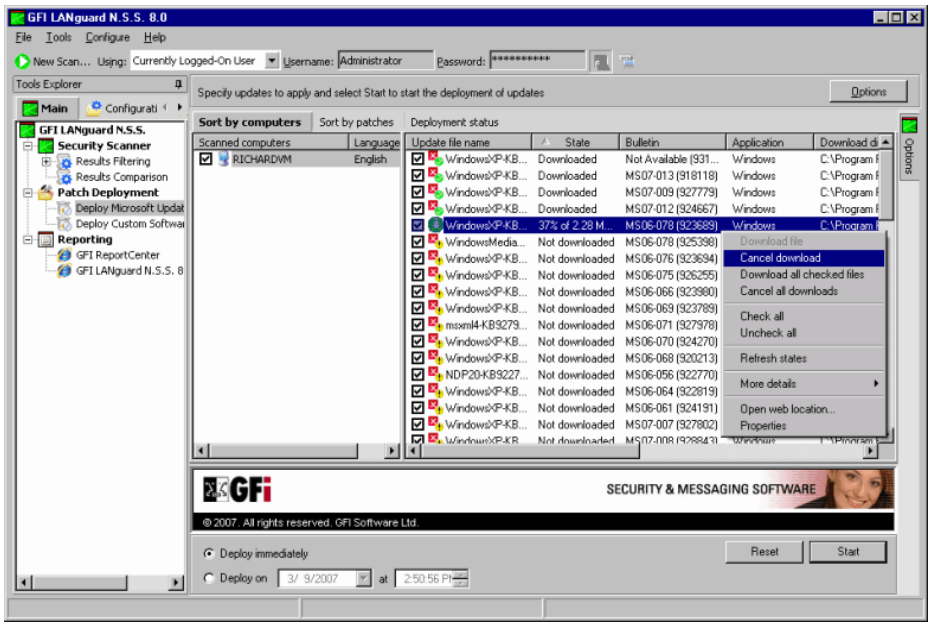
Screenshot 121 - Identifying the download queue status

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

- Downloaded

- Currently being downloaded
- Not downloaded.

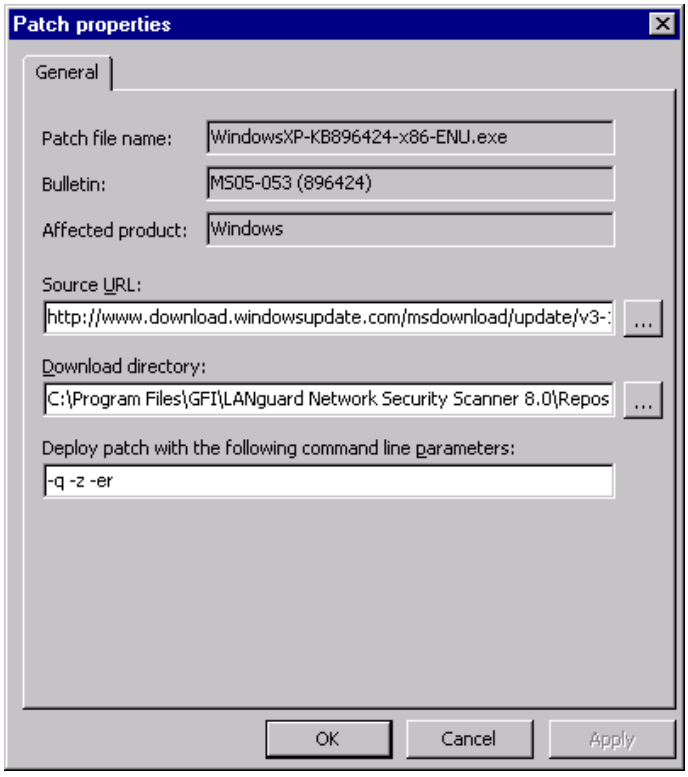
Stopping active downloads



Screenshot 122 - 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



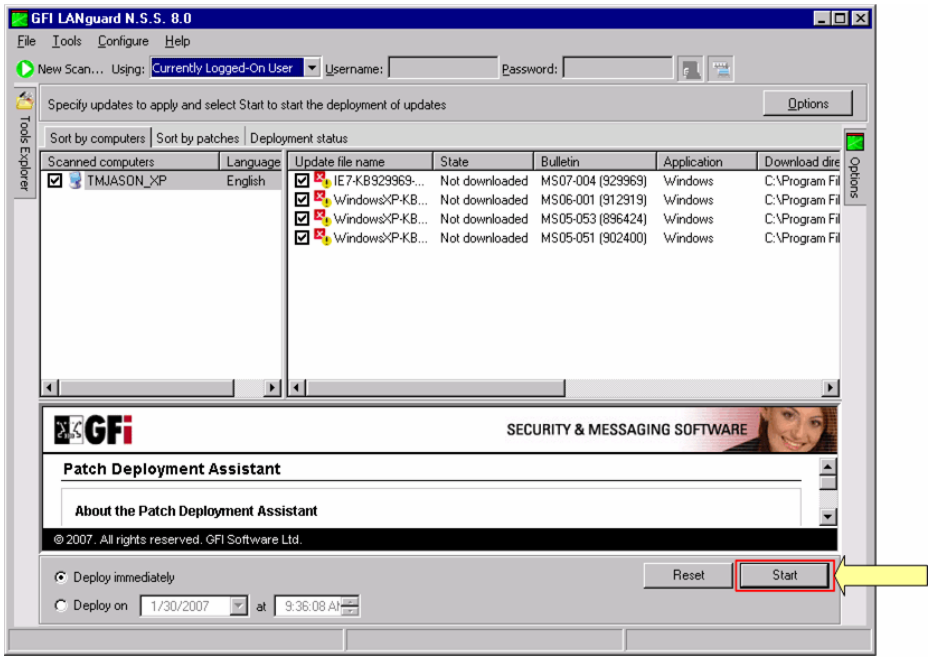
Screenshot 123 - Patch file properties dialog

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 **OK** to finalize your settings.

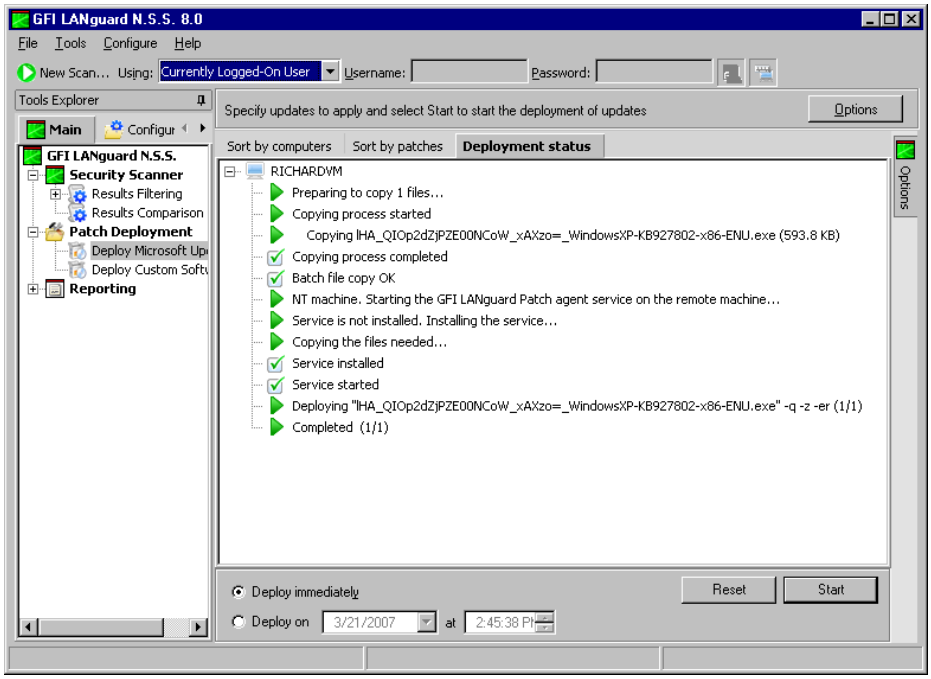
Deploy downloaded patches on selected targets



Screenshot 124 - Patch deployment options

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.

Monitor the patch deployment process



Screenshot 125 - Monitoring the deployment process

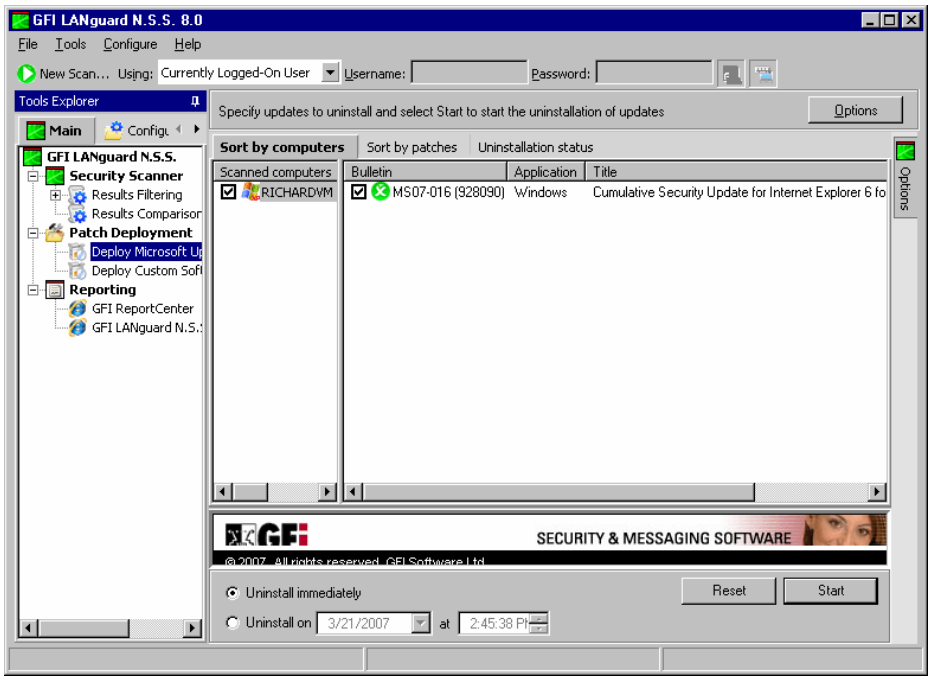
To view the patch deployment activity in progress, click on the **Deployment Status** tab located next to the **Sort by patches** tab at the top of the right pane.

Uninstall patches already deployed on targets

To uninstall patches or service pack previously installed on target computers:

1. Perform a scan on the computer(s) from which you need to uninstall (roll back) patches previously deployed.

2. From the scan results, right click on listed computers and select **Uninstall Microsoft updates ▸ [Service packs from** or **Patches from] ▸ [This computer or Selected computers or All computers}**.



Screenshot 126 – Uninstalling a patch

3. Select the patches or service packs to be uninstall from selected targets.

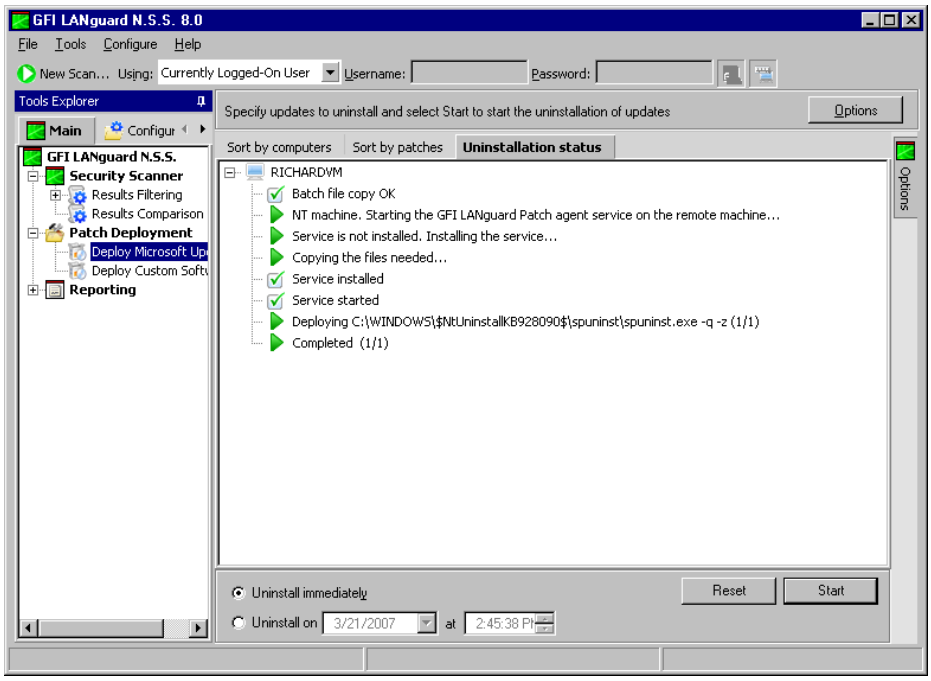
NOTE 1: Some patches or service packs cannot be rolled back since uninstalling them could impair the functionality of your systems. Patches that cannot be uninstalled will not be displayed for selection.

NOTE 2: You can sort the list of patches currently on display by clicking on the **Sort by computers** and **Sort by patches** tabs accordingly.

4. Click **Start** to initiate the uninstall process.

Monitoring the patch uninstall process

To view the patch roll-back progress, click on the **Uninstallation Status** tab located next to the **Sort by patches** tab at the top of the right pane.



Screenshot 127 - Monitoring the patch rollback process

12. Patch management: Deploying custom software

Introduction

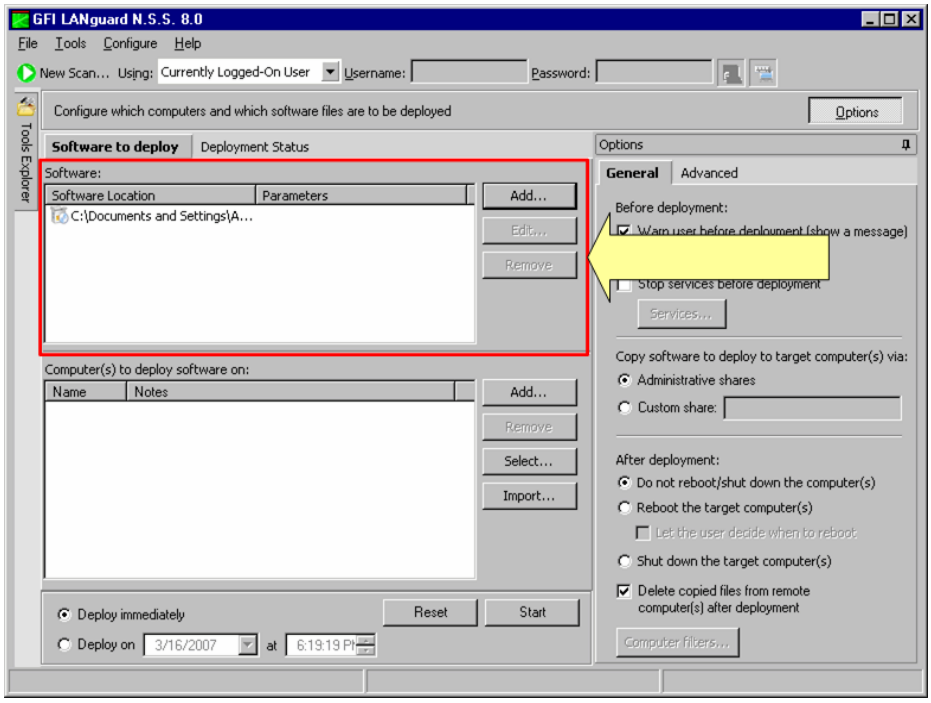
In addition to Microsoft security updates (i.e. patches, etc…), the versatile deployment engine that ships with GFI LANguard N.S.S. 8 also allows you to remotely deploy third party or custom software network-wide. Software that can be remotely deployed via this engine includes:

- Security applications such as complete anti-virus/anti-spyware solutions, software firewalls, etc.
- Third party software updates and patches such as anti-virus/anti-spyware signature file updates
- Custom code such as scripts and batch-files
- Desktop applications such as MS Office 2007 and more.

In this chapter you will learn how to:

- Specify which software must be deployed
- Specify on which target computers the software will be deployed
- Configure file deployment preferences
- Start the deployment process and monitor its progress.

Enumerating the software to be deployed

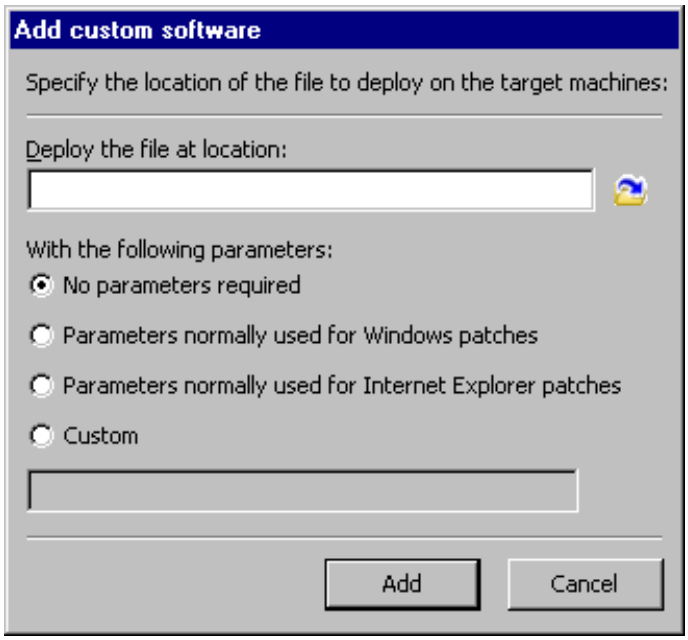


Screenshot 128- Selecting the software to deploy

To specify which software needs to be deployed:

1. From the left pane of the management console, click on the **Main** button and expand the **Patch Deployment** node.

2. Click the **Deploy Custom Software** node and from the 'Software' area in the right pane (see image above) click **Add.**



Screenshot 129 - Specifying the software to deploy

3. Specify the complete path to the file/software to be deployed.

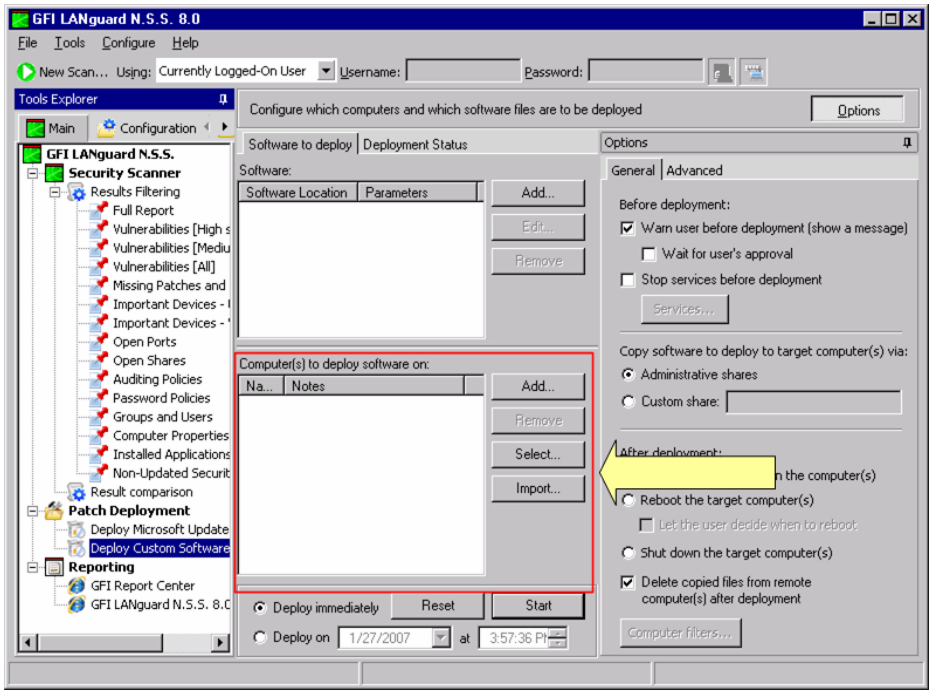
4. Specify any command line parameters to pass on during deployment by select one of the following options:

- *'Parameters normally used for Windows patches'* – Select this option if you want to pass parameters normally supplied during the installation of Windows patches.
- *'Parameters normally used for Internet Explorer patches'* – Select this option if you want to pass parameters normally supplied during the installation of 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.

5. Click **Add** to finalize your settings.

Repeat the process described above for every file/software that you want to deploy. On completion, proceed on configuring the list of target computer(s) where the selected files will be deployed. A description on how to achieve this is provided below.

Selecting target computers for file deployment



Screenshot 130 - Selecting the target computers

From the 'Computer(s) to deploy software on:' area (see image above), specify target computers using one of the following options:

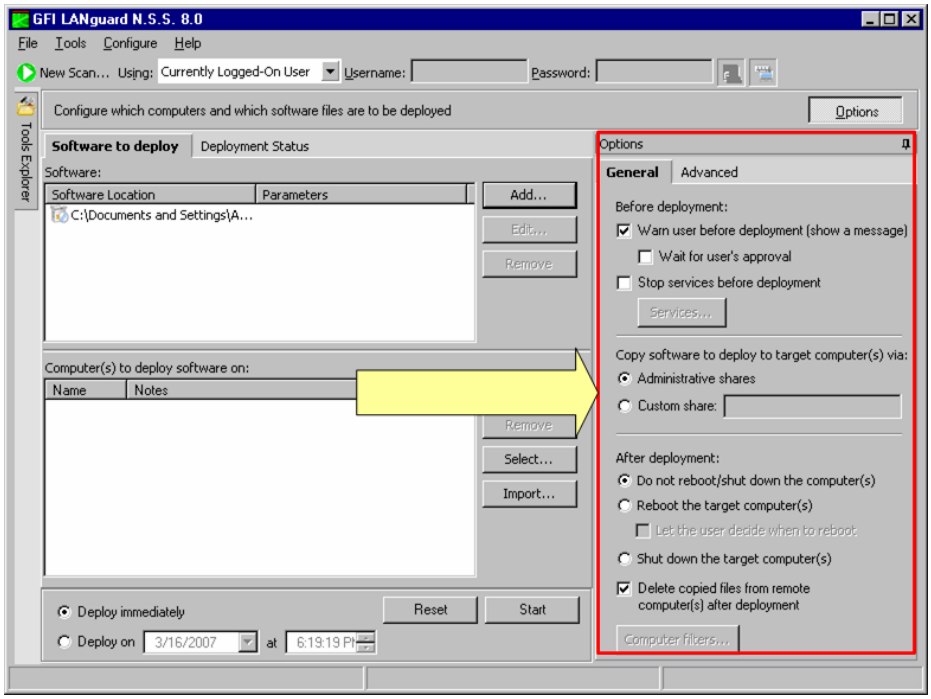
- Click **Add** to input the IP/name of your target computer(s)
- Click **Select** to select target computer(s) from the list of machines currently connected to your domain
- Click **Import** to import the list of target computers from a text file.

Deployment options

General deployment options

The general deployment options allow you to configure the actions and processes that must be triggered prior and post-deployment of the

selected file. Supported actions include sending a file deployment request to the user that is currently logged on to the target computer and the automated reboot of target computer following a successful deployment operation.

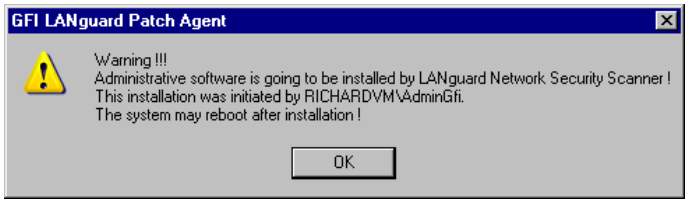


Screenshot 131 - General deployment options

Configuring pre-deployment options

Configure the 'Before deployment' options as follows:

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



Screenshot 132 - Deployment Warning: Informs that a deployment process is about to start

The message is intended to inform target computer users that a deployment will take place; hence give them time to save their work and close all running programs before the deployment process takes place.

- *'Wait for user's approval'* – Select this option to request an approval from the target computer user before starting the deployment process. Target computer users can opt to put on hold the deployment process in case some other important process (for example, a system backup) is already under way. This way other processes can be left to finish prior to the deployment, just in case

the target computer requires a reboot after the deployment process.

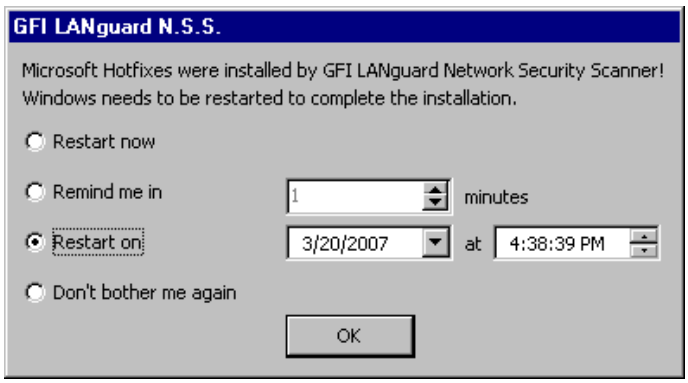
- *'Stop services before deployment'* – Select this option to stop specific services before starting the deployment. To specify the services to be stopped, click on the **Services…** button.

Configuring post-deployment options

Configure the 'After deployment' options as follows:

- *'Do not reboot/shut down the computer(s)'* – Select this option if you do NOT want to (remotely) reboot target computers on completion of the deployment process.
- *'Reboot the target computers'* – Select this option to automatically reboot target computers on completion of the deployment process.
- *'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, a message will be automatically sent to target computers on completion of the deployment process.

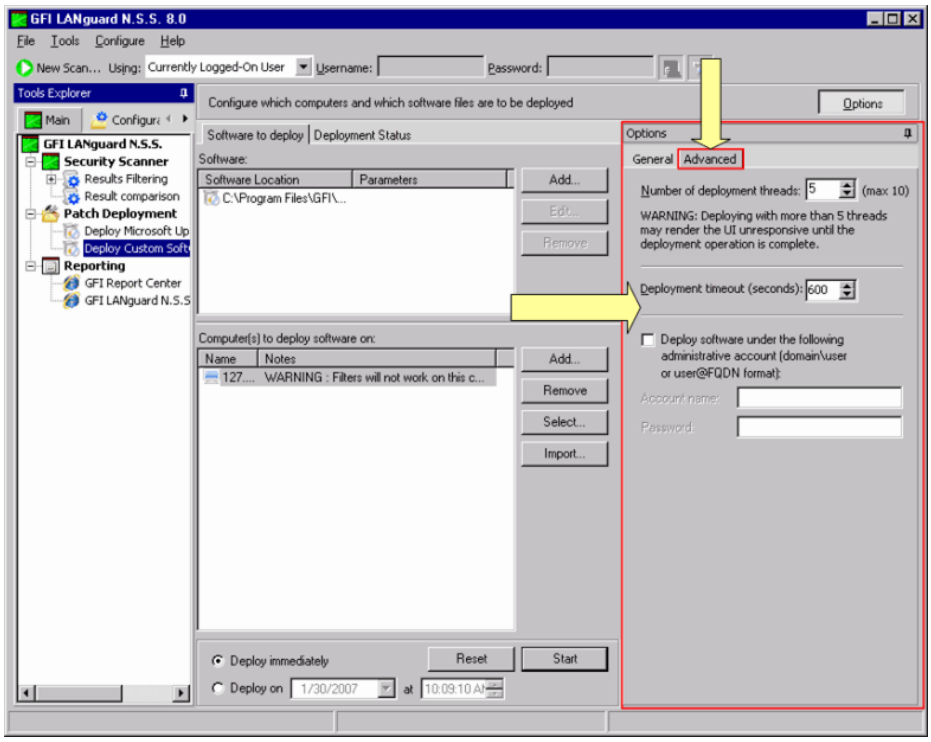


Screenshot 133 - Post deployment options dialog: Decide when to reboot the target computer

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

- *'Restart Now'* – Select this option for an 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 at a 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 completion of the deployment process.
- *'Delete copied files on the remote computers after deployment'* – Select this option to delete the source/installation file from target computer(s) on successful deployment.
- *"Computer filters"* - Click on the **Computer filters** button to configure particular target filtering conditions such as deploy only on targets running Windows XP.

Configuring advanced deployment options

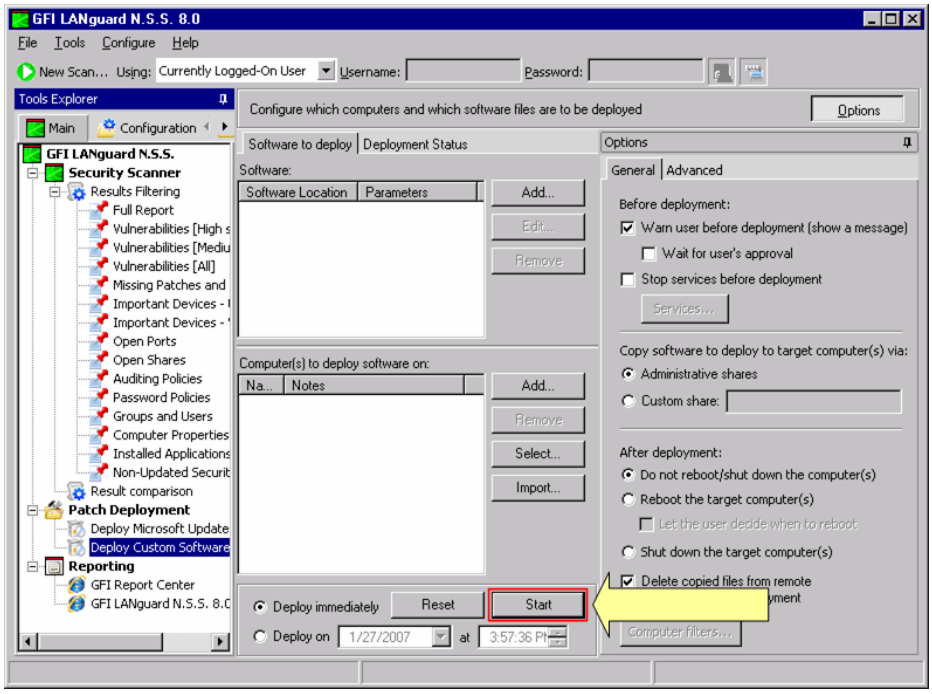


Screenshot 134 - Advanced deployment options

Use the **Advanced** tab to configure advanced options including:

- The number of patch deployment threads that will be used.
- Deployment timeout.
- Authentication credentials for the deployment agent service.

Start the deployment process



Screenshot 135 - Software deployment details

Once you have configured the required parameters you can:

- Initiate the deployment process by clicking on the **Start** button.

Schedule the deployment process. To achieve this, select the *'Deploy on'* option, specify the preferred date/time and click **Start**.

13. Results comparison

Introduction

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.

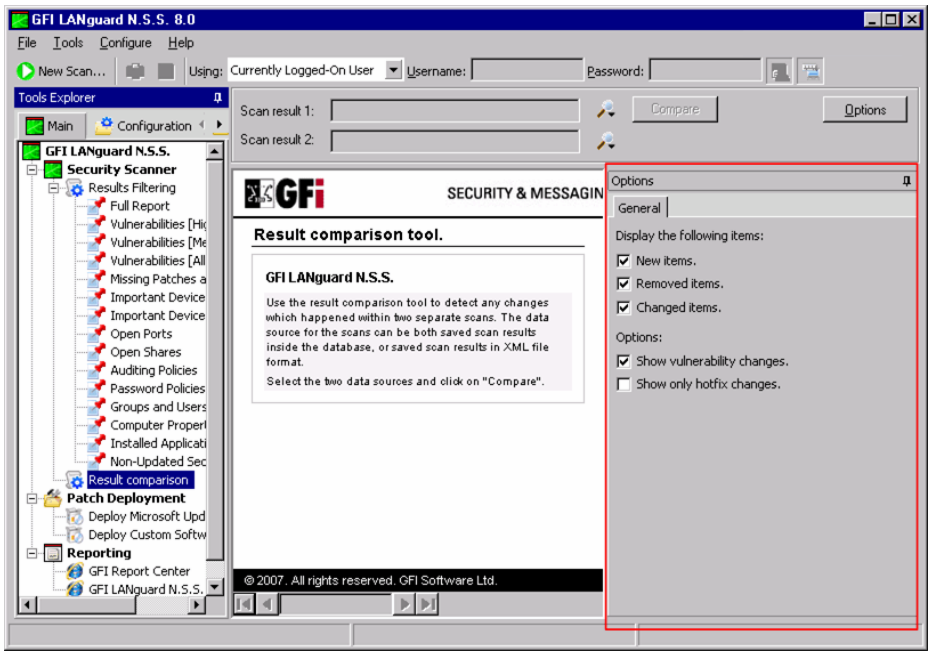
In this section you will discover how to:

- Configure what scan results changes will be reported
- Manually generate a results comparison report
- Automatically generate a results comparison report
- Analyze the results in the comparison report.

Configuring what scan results changes will be reported

The result comparison tool can report various information discovered during the comparison of two saved scan results. To configure what changes will be included in a comparison report:

1. Select the **Main** button, click on **Security Scanner** ▸ **Result comparison** node.



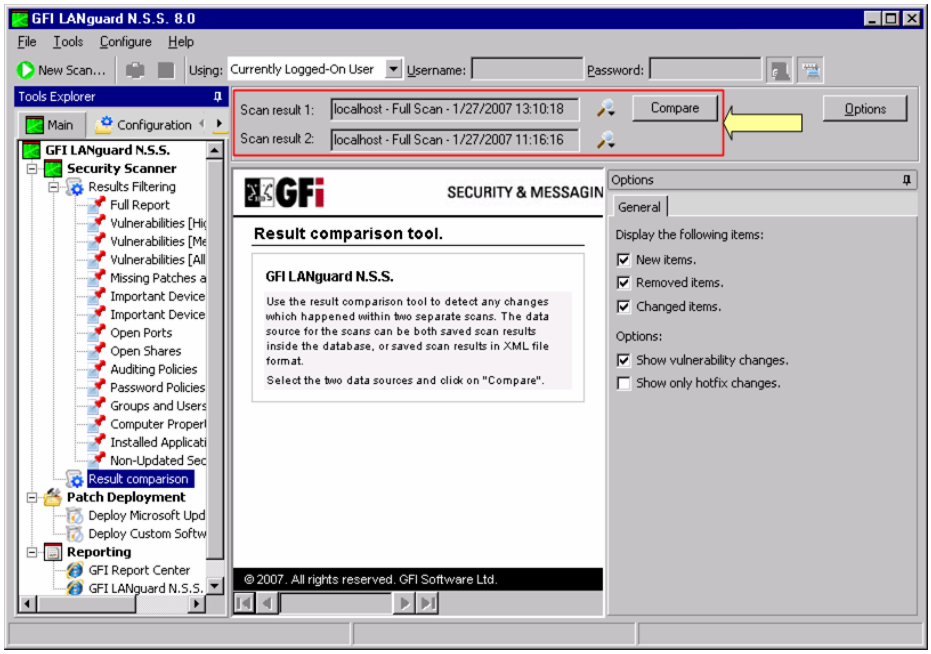
Screenshot 136 - Results comparison configuration options

2. From the right pane, click on the **Options** button and select the information item(s) to be reported from the following:

- *'New items:'* – Select this option to include all new security issues that emerged since the previous vulnerability scan.

- *'Removed items:'* Select this option to include 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 results.
- *'Changed items:'* Select this option to include all result items that have changed, such as a service that were enabled or disabled in between scans.
- *'Show vulnerability changes:'* Select this option to include all vulnerabilities identified during the 2 scans being compared.
- *'Show only hot-fix changes:'* Select this option to include all missing and installed patches identified between the compared scan results.

Generating a Results Comparison Report



Screenshot 137 - Comparing scan results

To generate a scan results comparison report:

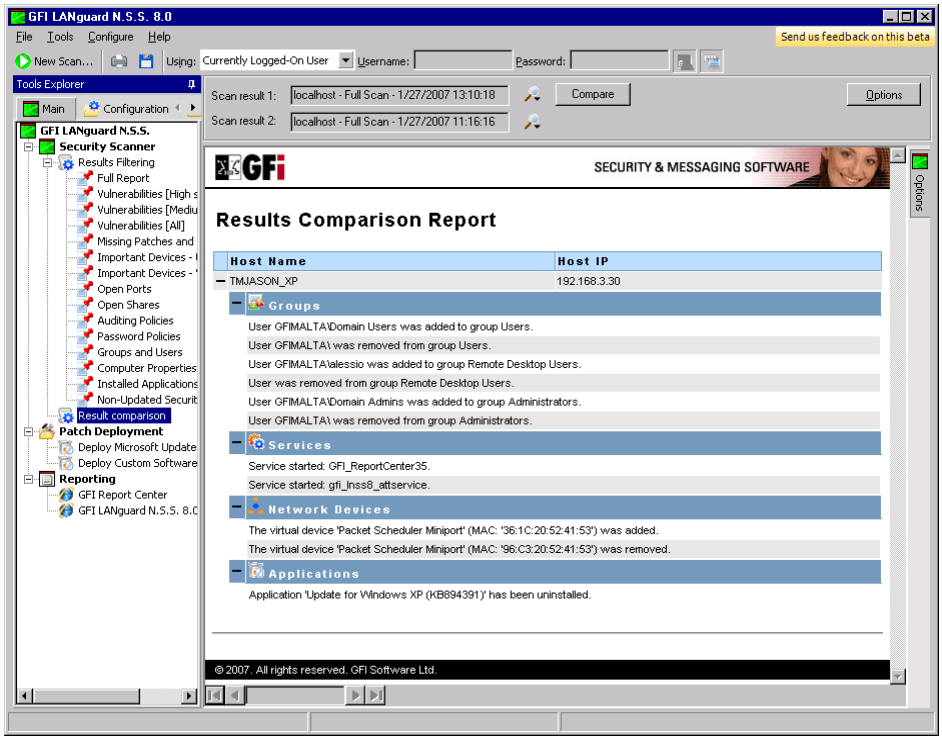
1. Select the **Main** button, click on the **Security Scanner ▸ Result comparison** node.

2. Click on the search file buttons to select the scan result files that you wish to compare.

NOTE: 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 138 - Results Comparison Report

On completion, the results comparison report is displayed in the right pane of the management console.

14. GFI LANguard N.S.S. Status Monitor

Introduction

GFI LANguard N.S.S. 8 ships with a state of the art status monitor which graphically indicates the status of various operations that might be currently active or scheduled such as patch download queue.

Screenshot 139 - GFI LANguard N.S.S. Status Monitor icon shown in the Windows system tray

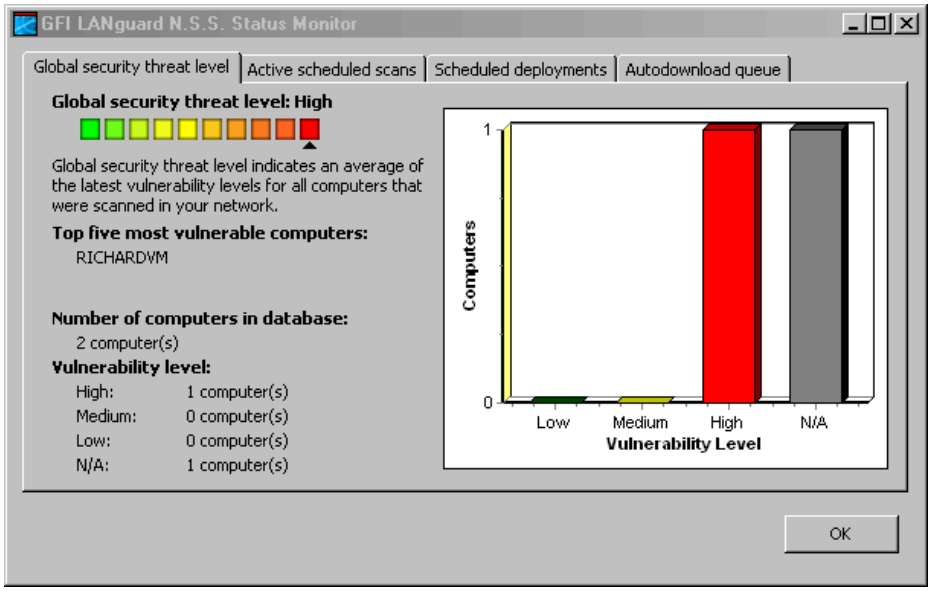
The Status Monitor is automatically loaded in the Windows system tray whenever the GFI LANguard N.S.S. management console is started.

NOTE: Bring up the Status Monitor without opening the GFI LANguard N.S.S. management console from **Start ▸ Program files ▸ GFI LANguard Network Security Scanner 8.0 ▸ LNSS Status Monitor**.

In this chapter you will discover how to use the GFI LANguard N.S.S. 8 Status Monitor to view:

- The global security threat level
- The state of active scheduled scans
- Scheduled update deployments
- Patch autodownload queue.

Viewing the global security threat level



Screenshot 140 - Status Monitor: Global security threat level tab

The global security threat level tab provides you with extensive security information based on data acquired during scans. This enables you to determine at a glance the current network vulnerability level, the top five most vulnerable computers, the number of computers in the database. It also provides you with a breakdown of the vulnerable computers according to their vulnerability level.

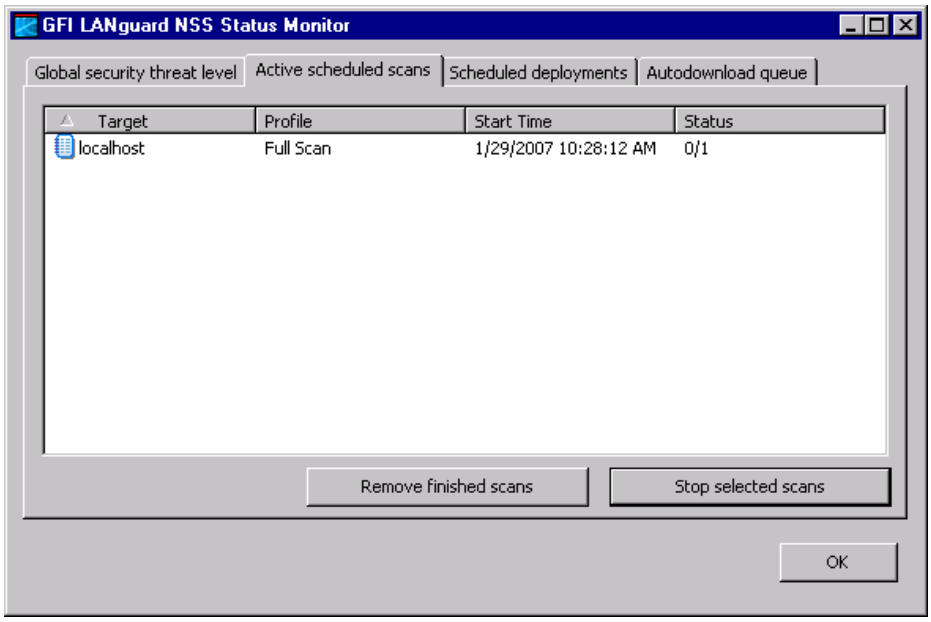
NOTE 1: The data displayed in the **Global security threat level** tab is dynamically worked out by GFI LANguard N.S.S. based on previous scans.

To view the global security threat level:

1. Bring up the status monitor by right-clicking on the icon located in your Windows system tray and select **Status**.
2. Click on the **Global security threat level** tab.

Viewing the progress of scheduled scans

Scheduled scans are scans that have been set up to trigger at a later date and time. Through the Active Scheduled scans tab in GFI LANguard N.S.S's Status Monitor, you can monitor these scans and stop current scans in progress or remove finished scan details.



Screenshot 141 - Status Monitor: Active scheduled scans tab.

To view scheduled scans in progress:

1. Bring up the status monitor by right-clicking on the icon located in your Windows system tray and select **Status**.
2. Click on the **Active scheduled scans** tab.
3. If required, trigger any one of the following operations:

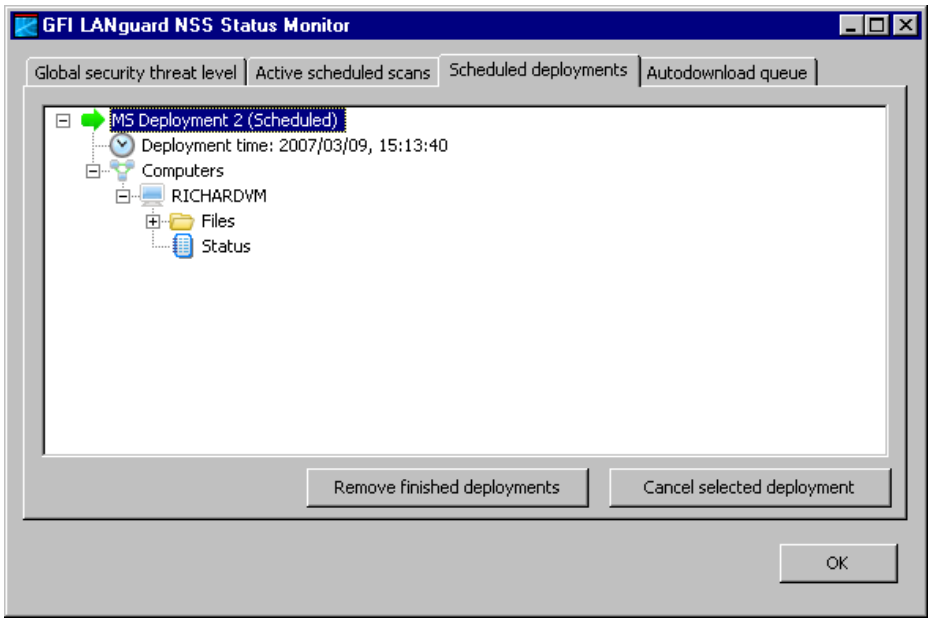
- To cancel any scheduled scan that is in progress, click **Stop Selected Scans**.
- To remove any finished scan details, click **Remove finished scans**.

NOTE: From the **Active Scheduled Scans** tab you can only view and cancel scheduled scans that are in progress. To view or cancel scheduled scans that have not yet started launch the GFI LANguard N.S.S. management console and go to **Configuration ▸ Scheduled Scans**.

Viewing the progress of scheduled deployments

Scheduled deployments are patch or service pack deployments that have been set up to trigger at a later date/time combination. Through this feature you can set-up GFI LANguard N.S.S. to deploy missing patches and service pack during times of the day when users are not using their computer, therefore not stopping them when computers need to restart to complete some update.

Through the Scheduled deployments tab available with GFI LANguard N.S.S's status monitor, you can monitor these scheduled patch or service pack deployments and cancel deployments or remove finished deployments.



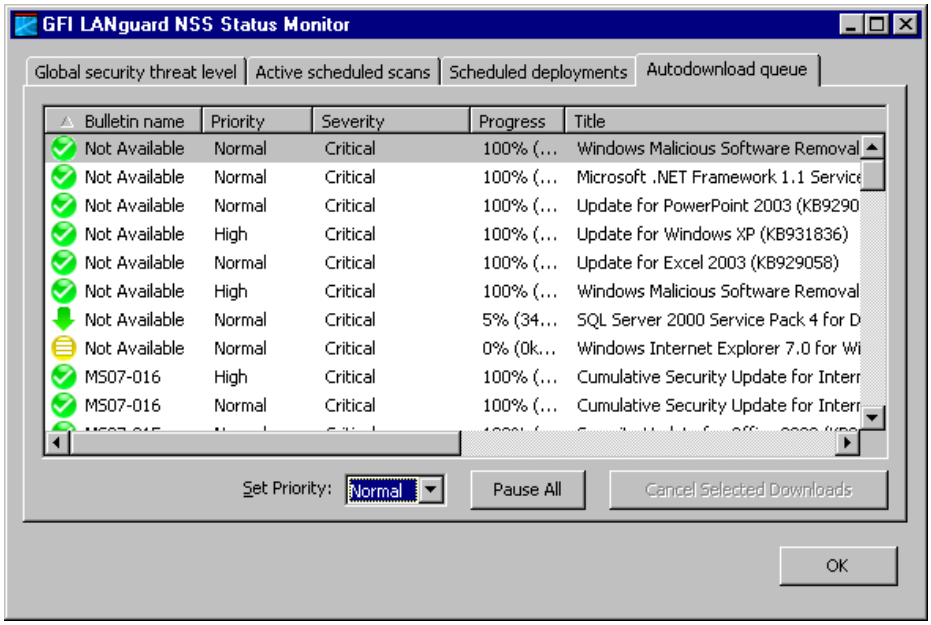
Screenshot 142 - Status Monitor: Scheduled deployments

To view scheduled deployments in progress:

1. Bring up the status monitor by right-clicking on the icon located in your Windows system tray and select **Status**.
2. Click on the **Scheduled deployments** tab.
3. If required, trigger any one of the following operations:

- To cancel any scheduled deployment that is in progress, click **Cancel selected deployment**.
- To remove any finished deployment details, click **Remove finished deployments**.

Viewing the autodownload queue



Screenshot 143 - Status Monitor: Autodownload queue tab

To view the autodownload queue:

1. Bring up the status monitor by right-clicking on the  icon located in your Windows system tray and select **Status**.

2. Click on the **Autodownload queue** tab.

3. If required, trigger any one of the following operations:

- To pause all downloads that are in progress, click **Pause All**.
- To cancel a particular download that is in progress click **Cancel Selected downloads**.
- Change the priority of a downloads via the Set Priority selection box.

15. Tools

Introduction

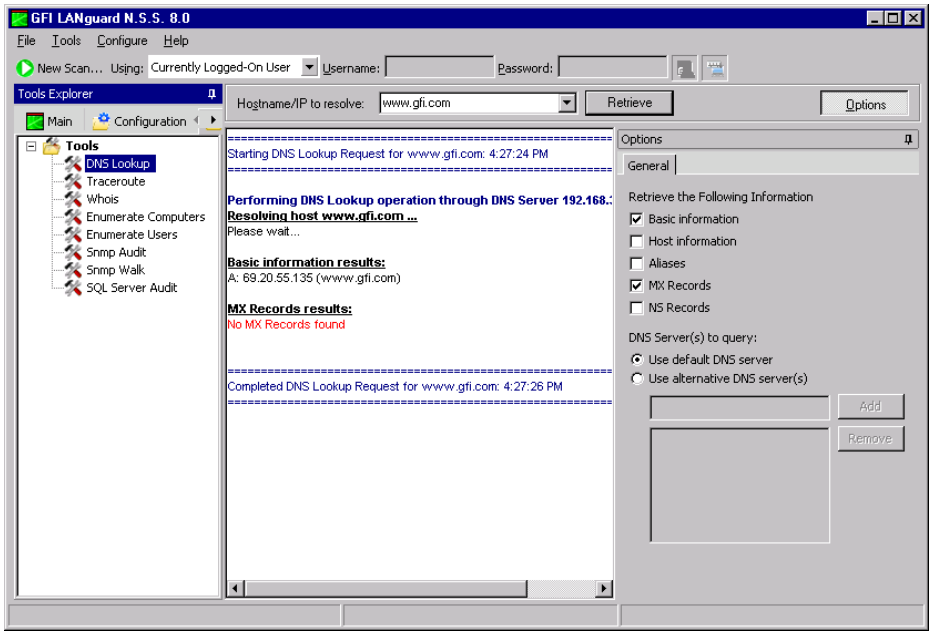
In this chapter you will discover how to use the default set of network tools that troubleshoot common network problems and assist you in the administration of your network.

Use the **Tools** button to access the following list of default network tools:

- DNS Lookup
- Traceroute
- Whois
- Enumerate Computers
- Enumerate Users.
- SNMP Audit
- SNMP Walk
- SQL Server Audit

DNS lookup

Click on the **Tools** button, and select 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 144 - The DNS Lookup tool

To resolve a domain/host name:

1. Click on the **Tools** button, and select the **Tools ▸ DNS lookup** node.

2. Specify the hostname to resolve.

3. Specify the information that you wish to retrieve:

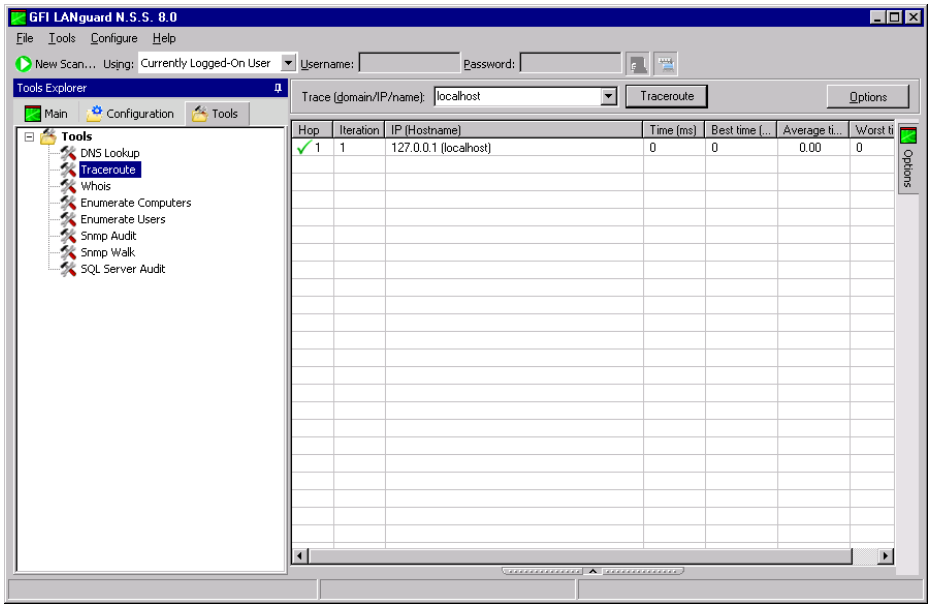
- *'Basic Information'* – Select this option to retrieve the host name and the relative IP address.
- *'Host Information'* – Select this option to retrieve HINFO details. The host information (known as HINFO) generally includes target computer information such as hardware specifications and OS details.

  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.

Traceroute



Screenshot 145 - Trace route tool

Click on the **Tools** button, and select the **Tools ▸ Traceroute** tool to identify the path that GFI LANguard N.S.S. followed to reach a target computer. To use this tool:

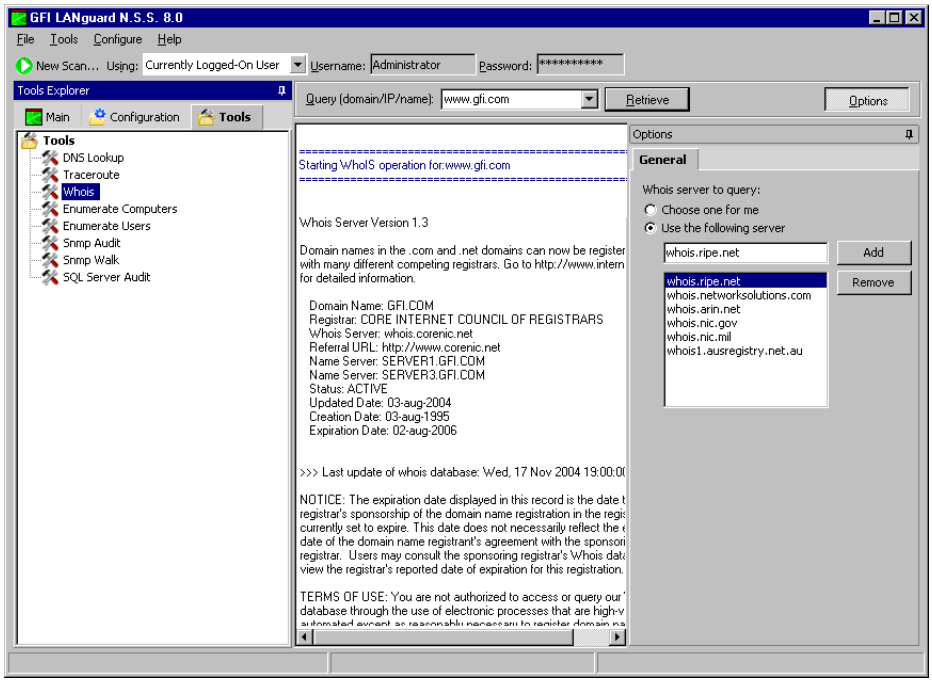
1. In the 'Trace' dropdown, specify the name/IP or domain to reach.

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:

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

Whois



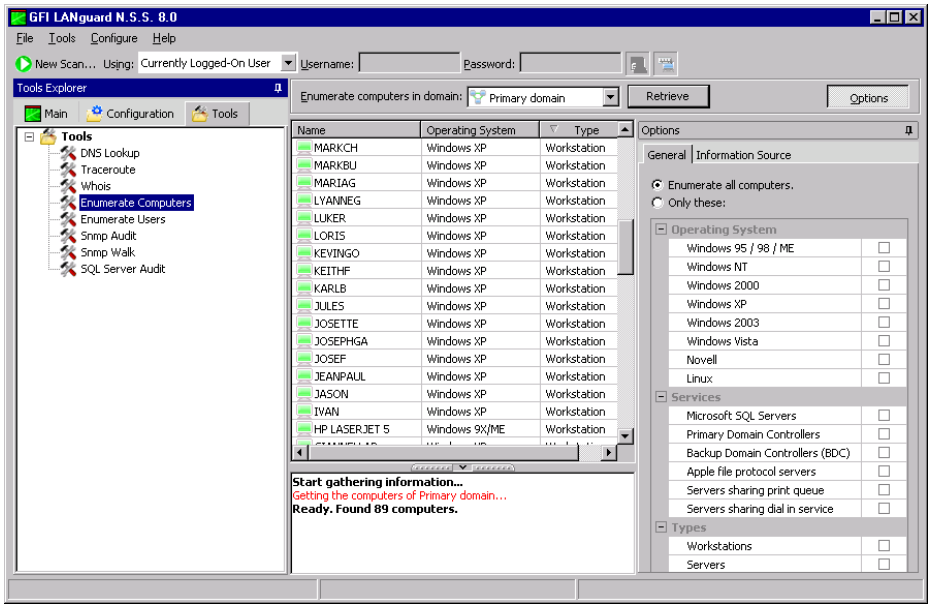
Screenshot 146 - Whois tool

Click on the **Tools** button, and select 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 management console, 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.

Enumerate computers



Screenshot 147 - Enumerate Computers tool

Click on the **Tools** button, and select 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 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 that 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.

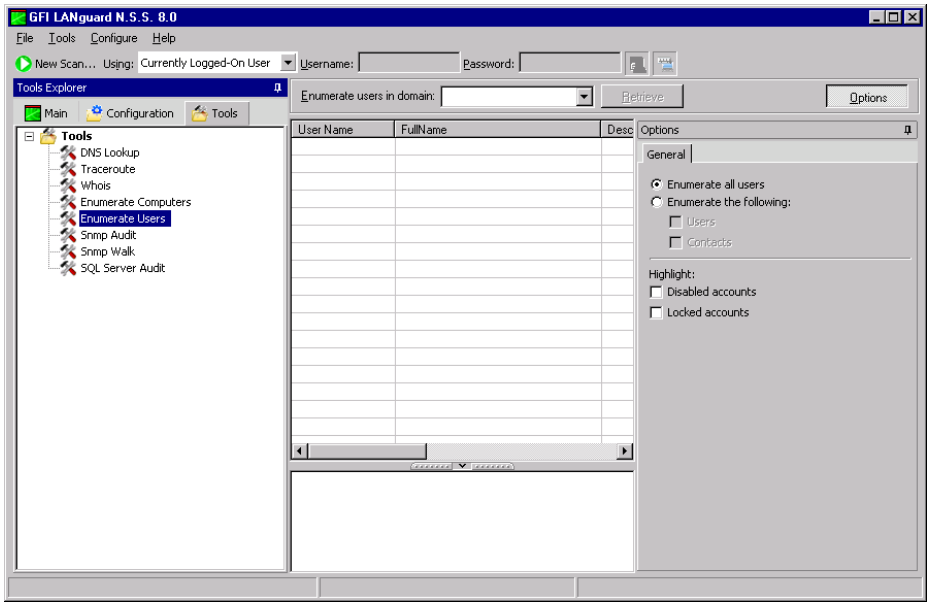
2. Right click on any of the selected computers and select **Deploy Custom Patches**.

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 that 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



Screenshot 148 - The Enumerate Users tool dialog

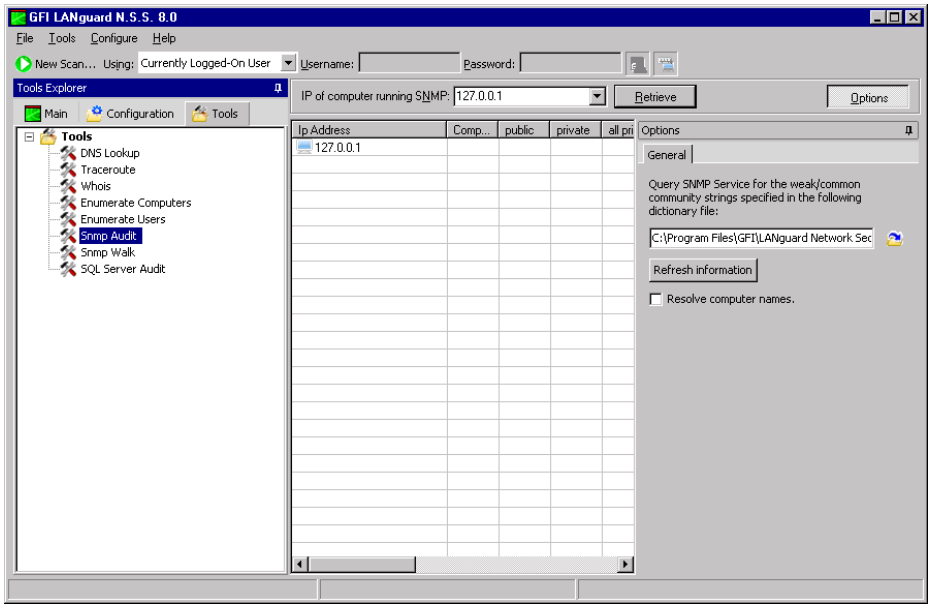
Click on the **Tools** button, and select the **Tools ▸ Enumerate Users** tool to scan the Active Directory and retrieve the list of all users and contacts included in this database.

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.

SNMP Auditing



Screenshot 149 - SNMP Audit tool

Click on the **Tools** button, and select 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 management console.

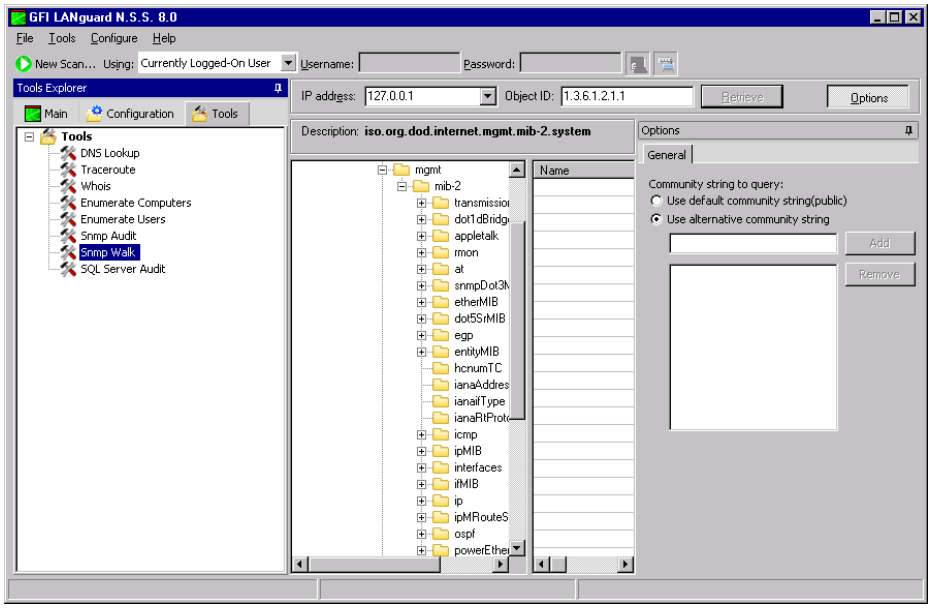
To perform an SNMP Audit:

1. Click on the **Tools** button, and select 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.

SNMP Walk



Screenshot 150 - 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** button, and select 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.

Microsoft SQL Server Audit

Click on the **Tools** button, and select 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** button, and select 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.

16. Using GFI LANguard N.S.S. from the command line

Introduction

In this chapter you will discover how to use the two command line tools bundled with GFI LANguard N.S.S; *'lnsscmd.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. management console.

Configured through a set of command line switches, the complete list of supported switches together with a description of the respective function is provided below.

Using 'lnsscmd.exe' - the command line scanning tool

The *'lnsscmd.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 *'lnsscmd.exe'* command line tool supports the following switches:

lnsscmd [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 management console, 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 management console).
- **/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 '***lnss@127.0.0.1***'

The command line tool instruction for this particular security scan is:

lnsscmd.exe 130.16.130.1 /Profile="Default" /Output="c:\out.xml" /Report="c:\result.html" /email="lnss@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 that will be shown on screen immediately before the deployment session is started.
- **/useraproval** – (Optional) Include this switch to request the user's approval before starting the file/patch 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 management console. 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.

- **/?** - (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

17. Adding vulnerability checks via custom conditions or scripts

Introduction

In this section you will learn how to add new custom vulnerability checks created either through 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 that 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 that can be run against your network targets.

Security auditing scripts can be developed using the script editor that ships with GFI LANguard Network Security Scanner. This built-in script editor includes syntax highlighting capabilities as well as debugging features that support you during script development. Open the script editor from **Start ▸ Programs ▸ GFI LANguard Network Security Scanner 8.0 ▸ LNSS Script Debugger**.

NOTE: For more information on how to develop scripts using the built-in script editor, refer to the 'Scripting documentation' help file included in **Start ▸ Programs ▸ GFI LANguard Network Security Scanner 8.0 ▸ GFI LANguard N.S.S. 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 http://forums.gfi.com/. 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 that adds results to the vulnerability check report (i.e. scan results). These results are shown in the GFI LANguard N.S.S. management console 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 that 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 8.0 ▸ GFI LANguard N.S.S. 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 8.0\Data\Scripts\myscript.vbs'*.

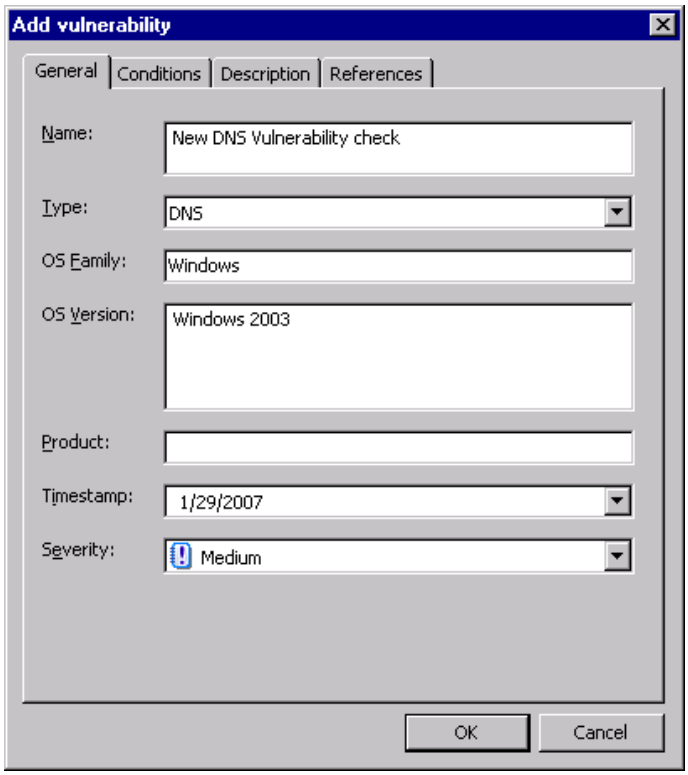
Step 2: Add the new vulnerability check:

1. Open the GFI LANguard N.S.S. management console.

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).

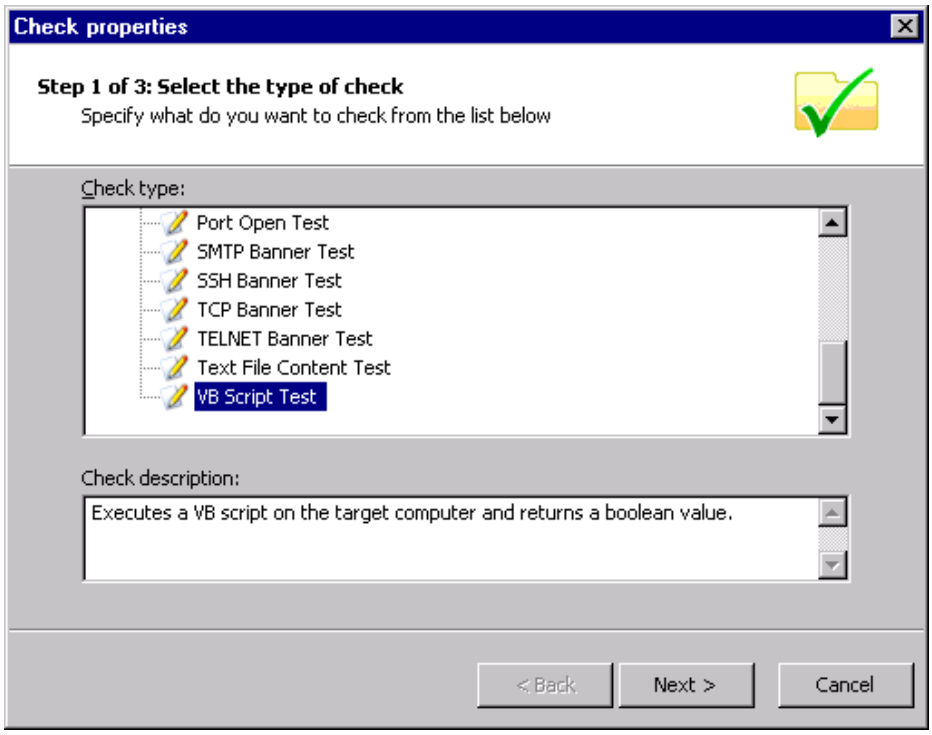


Screenshot 151 - The new vulnerability check dialog

5. Click on the **Add** button. This will bring up the “Add Vulnerability” dialog box.

6. Go through the **General**, **Description** and **Reference** tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

7. Choose the **Conditions** tab and click on the **Add…** button. This will bring up the check properties wizard.



Screenshot 152 - The check triggering conditions dialog

8. Select **Independent checks ▸ VBScript** node and click on **Next** button to continue setup.

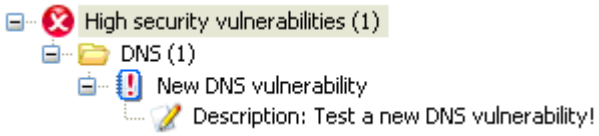
9 Click on the **Choose file** button and select the custom VBscript file that will be executed by this check (For this example select '*myscript.vbs*'). Click on **Next** to proceed.

10. Select the relative condition setup in the wizard to finalize script selection. Click on **Finish** to exit wizard.

11. Click on **OK** to save new vulnerability check.

Testing the vulnerability check/script used in example

Scan your local host computer using the scanning profile where the new check was added.



Screenshot 153 - High security vulnerabilities

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 that 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

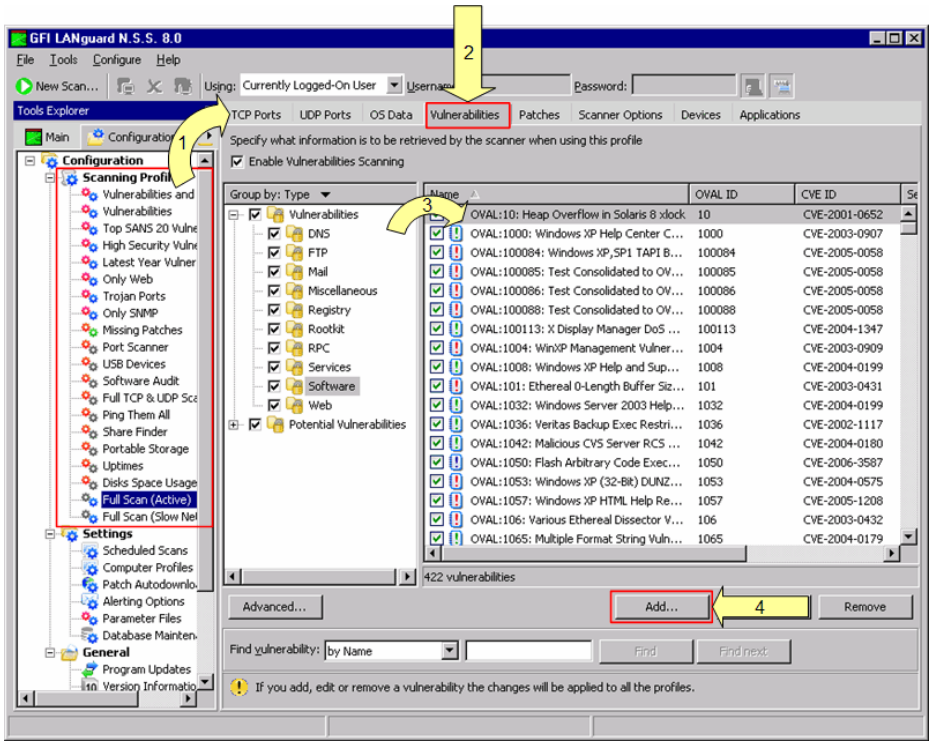
1. Launch your favorite text file editor.

2. Create a new script using the following code:

```
#!/bin/bash
if [ -e test.file ]
then
        echo "TRUE:"
else
        echo "FALSE:"
fi
echo "!!SCRIPT_FINISHED!!"
```

3. Save the file in '*C:\Program Files\GFI\LANguard Network Security Scanner 8.0\Data\Scripts\myscript.sh*"

Step 2: Add the new vulnerability check:



Screenshot 154 - Adding a new vulnerability check

1. Click on the **Main** button, select the **Configuration ▸ Scanning Profiles** node and select the scanning profile where you wish to add the new vulnerability check.

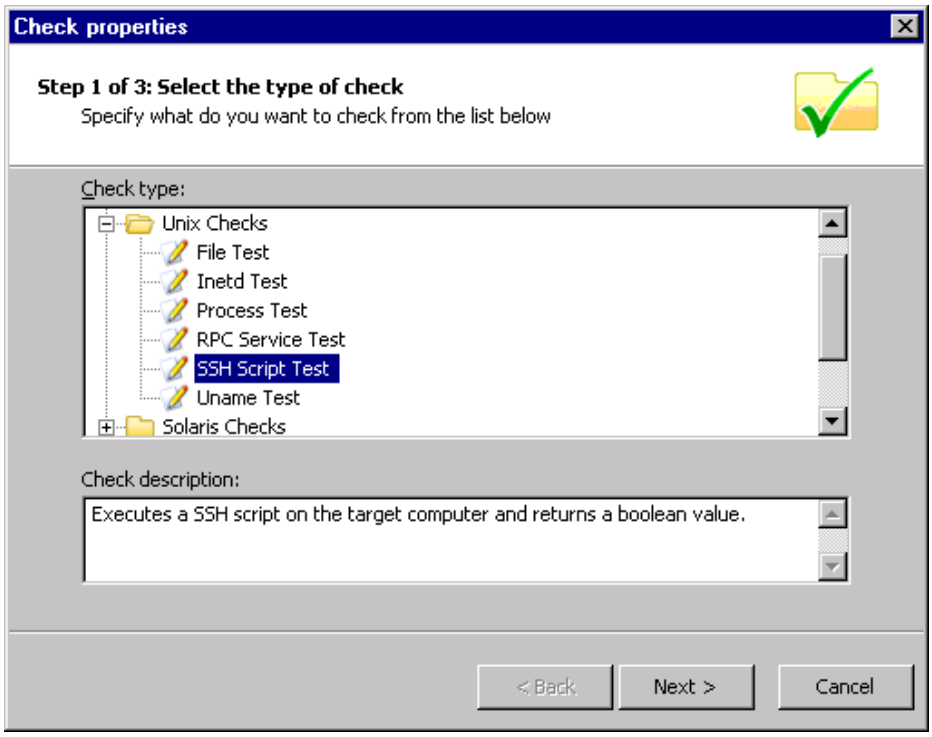
2. Click on the **Vulnerabilities** tab.

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 “Add Vulnerability” dialog box.

5. Go through the General, Description and Reference tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Choose the **Conditions** tab and click on the **Add…** button. This will bring up the check properties wizard.



Screenshot 155 - The check triggering conditions dialog

7. Select **Unix checks ▸ SSH Script test** node and click on Next button to continue setup.

8 Click on the **Choose file** button and select the custom SSH Script file that will be executed by this check (For this example select '*myscript.sh*'). Click on **Next** to proceed.

9. Select the relative condition setup in the wizard to finalize script selection. Click on **Finish** to exit wizard.

10. Click on **OK** to save new vulnerability check.

Testing the vulnerability check/script used in our example

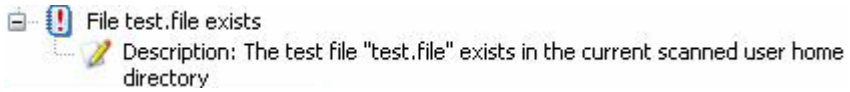
Scan your local host computer using the scanning profile where the new check was added.

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.

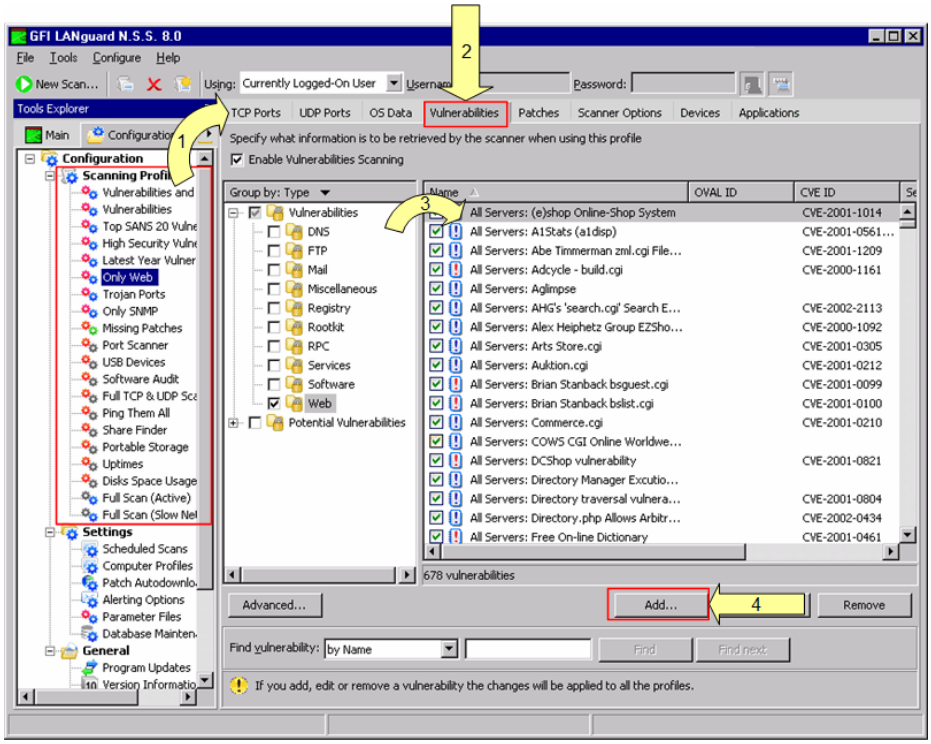
3. Check you scan results. The **Vulnerabilities** node will the vulnerability warning shown below.



Screenshot 156 - Testing the vulnerability check/script

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.



Screenshot 157 - Creating a CGI vulnerability check

To create a new CGI vulnerability check:

1. Click on the **Configuration** button and select the **Configuration ▸ Scanning Profiles ▸ Only Web** node.

2. Click on the **Vulnerabilities** tab.

3. From the middle pane, select the **Web** node.

4. Click on the **Add** button. This will bring up the **Add vulnerability** dialog box.

5. Go through the General, Description and Reference tabs while specifying the basic details such as the vulnerability name, short description, security level and OVAL ID (if applicable).

6. Choose the **Conditions** tab and click on the **Add…** button. This will bring up the check properties wizard.

7. Select **Independent checks ▸ CGI Abuse test** node and click on **Next** button to continue setup.

8. Specify:

- *'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 that 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.

- *'Directories:'* – Specify the directories where the CGI script is located.

Click on the **Next** button to continue setup..

9. Specify the conditions for the CGI vulnerability check. Click **Finish** to save the custom condition settings.

10. Click on **OK** button to save new CGI vulnerability check.

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'.

18. Miscellaneous

Introduction

In this section you will find information on:

- How to enable 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

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.

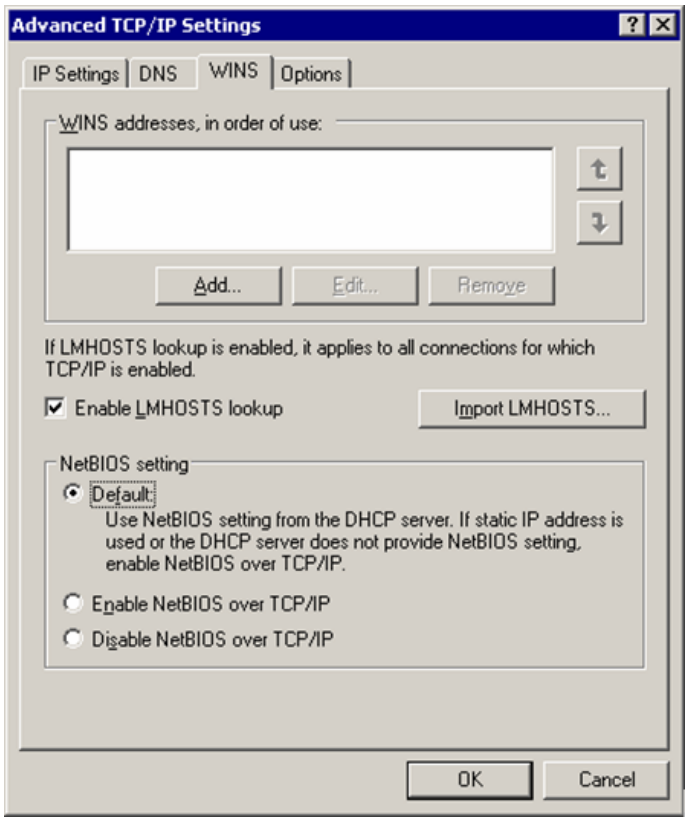
Local Areas Connection icon

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.



Screenshot 158 - 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).

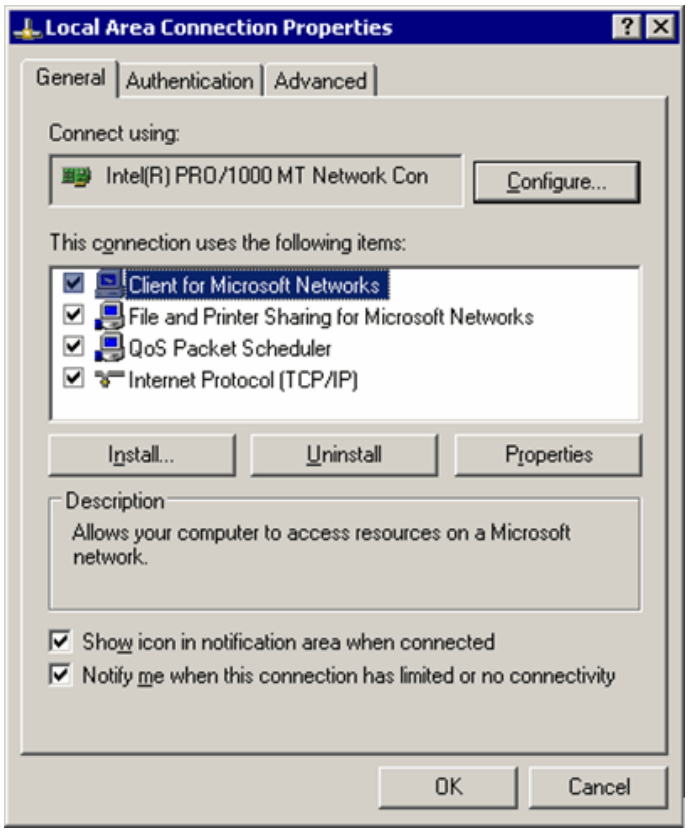
Installing the Client for Microsoft Networks component on Windows 2000 or higher

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.



Screenshot 159 - 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.

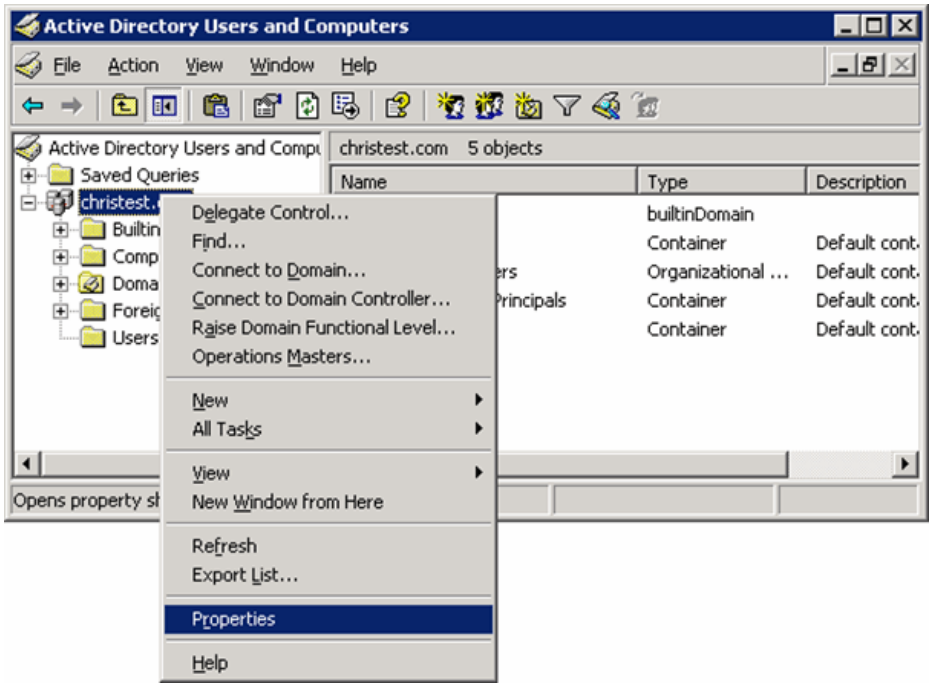
6. To finalize the installation, click on the **OK** button and reboot the computer. After the computer has restarted, Client for Microsoft Windows will be automatically installed.

Configuring Password Policy Settings in an Active Directory-Based Domain

NOTE: You must be logged on as a member of the Domain Admin group.

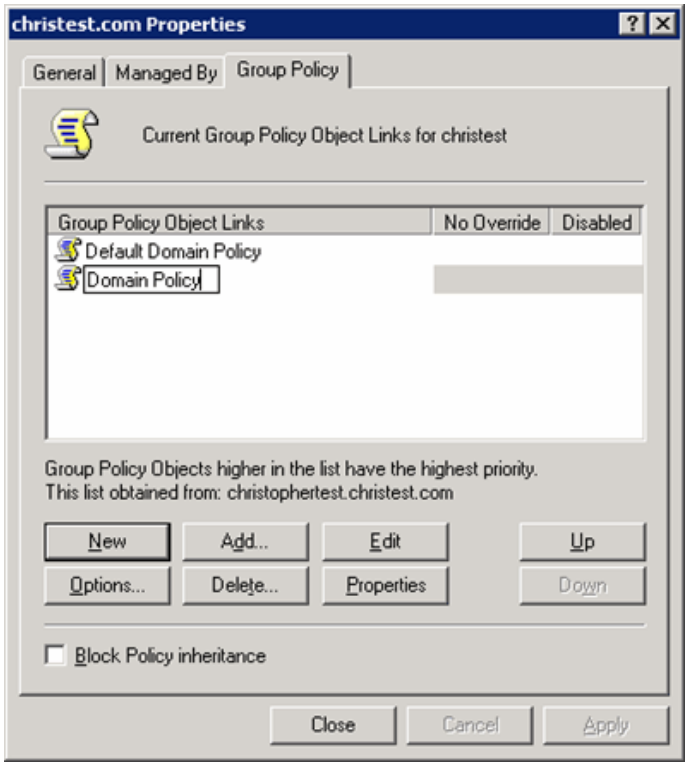
To implement password policies on network computers belonging to an Active Directory domain:

1. Navigate to the Control Panel (**Start ▸ Settings ▸ Control Panel**) and open the 'Administrative Tools'.



Screenshot 160 - 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**.



Screenshot 161 - 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.

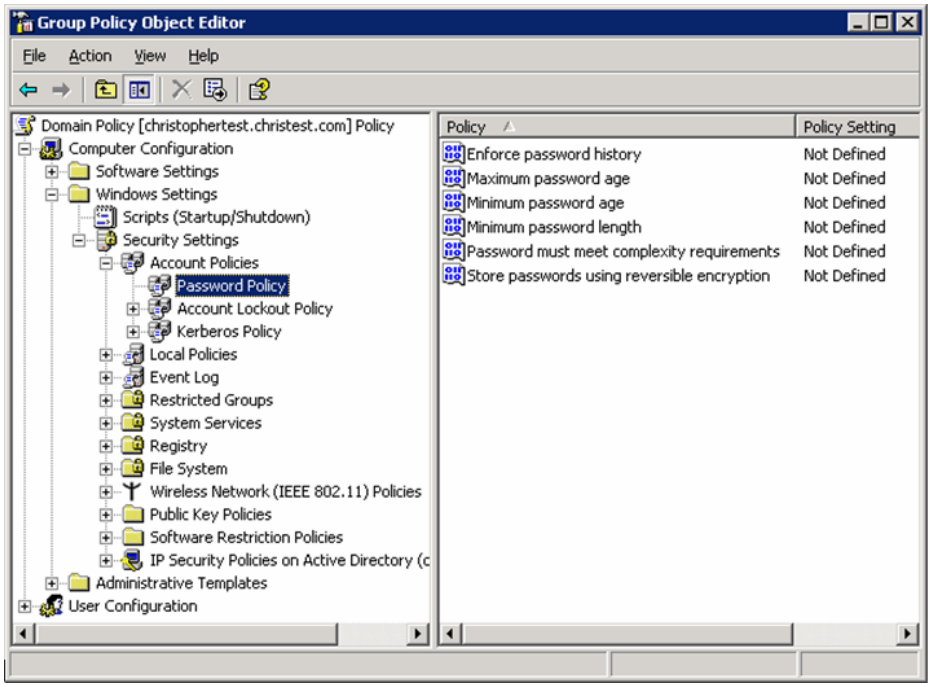
4. Specify the name of the new group policy (for example, 'Domain Policy') and then click on **Close**.

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.



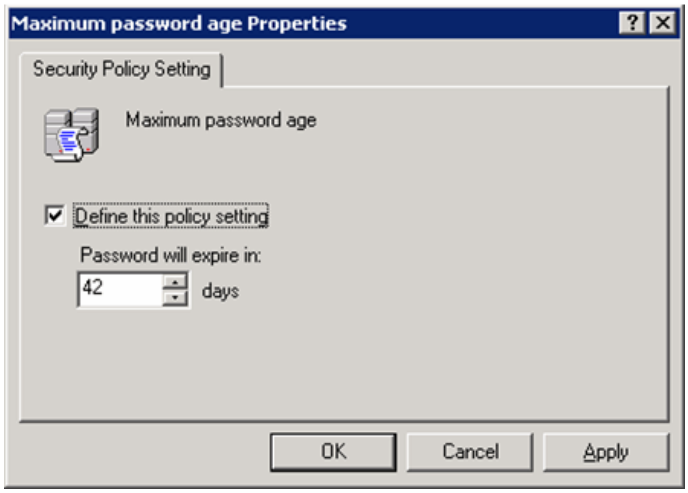
Screenshot 162 - The Group Policy Object Editor

8. Expand the **Computer Configuration** node and navigate to **Windows Settings** ▸ **Security Settings** ▸ **Account Policies** ▸ **Password Policy** folder.

Screenshot 163 - 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'.

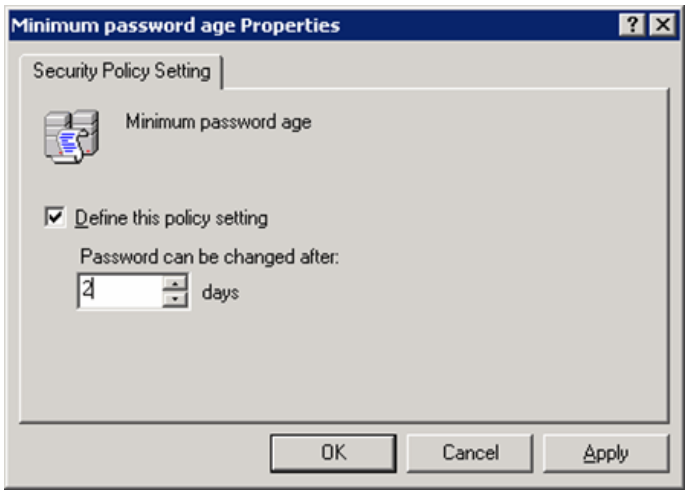
10. Click on the **OK** button to close the dialog.



Screenshot 164 - 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.

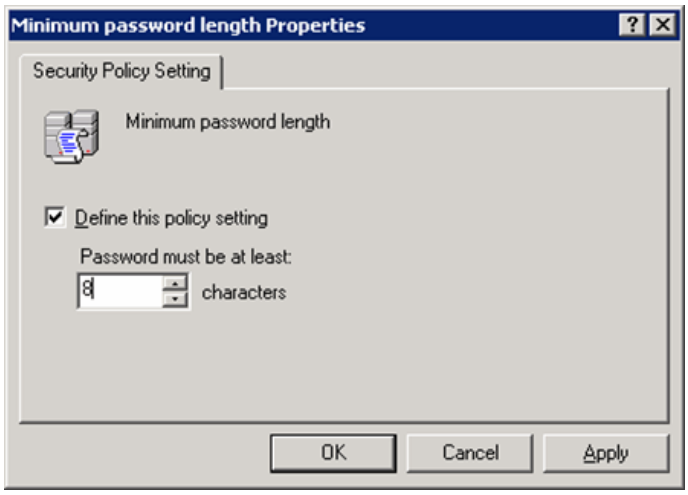
12. Click on **OK** to close the properties dialog.



Screenshot 165 - 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'.

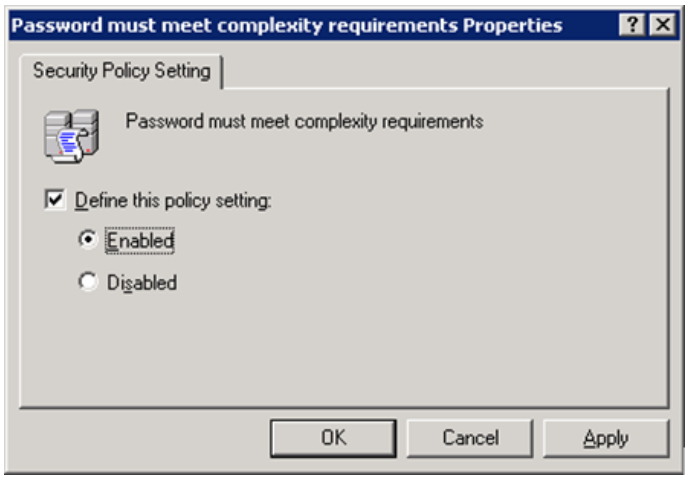
14. Click on the **OK** button to close the dialog.



Screenshot 166 - 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 167 - 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 Admin 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.

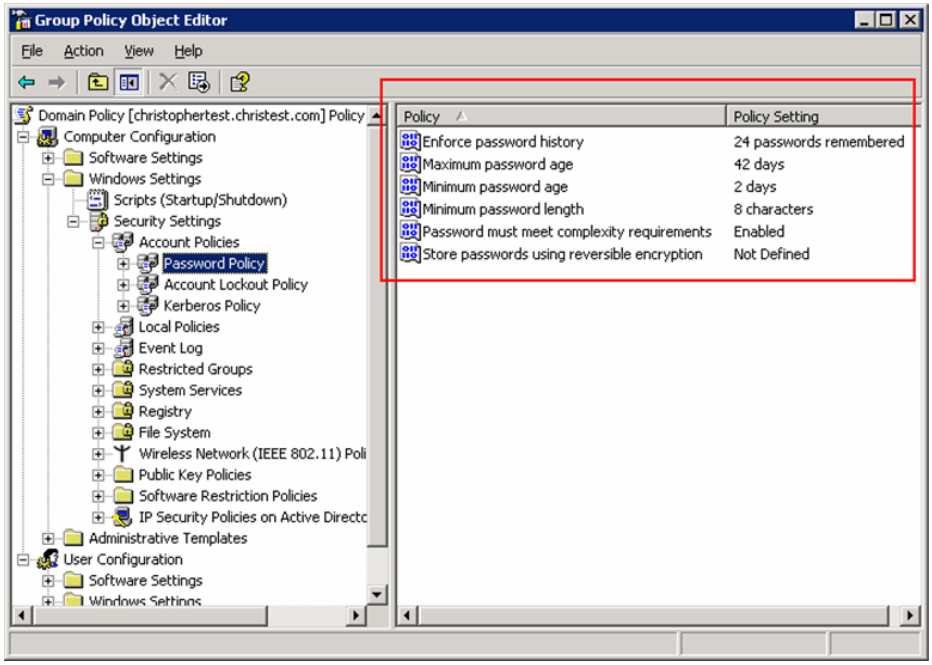
To verify password policy settings for an Active Directory domain

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 168 - 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 that are not older than two days.

19. Troubleshooting

Introduction

This 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 mailto:support@gfi.com
- Contacting the GFI support department using our live support service at http://support.gfi.com/livesupport.asp
- 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 up-to-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 mailto:support@gfi.com.

Ensure that you have registered your product on our website first, at http://customers.gfi.com/.

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 http://support.gfi.com/livesupport.asp

Ensure that you have registered your product on our website first, at http://customers.gfi.com/

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 http://customers.gfi.com/

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

T

U

V

W