
GFI LANguard Network Security Scanner 8.0 ReportPack

Manual

By GFI Software Ltd.



<http://www.gfi.com>
E-mail: info@gfi.com

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

Version 8.0 – Last updated March 20, 2007

Contents

Introduction	6
About GFI ReportCenter	6
About the GFI LANguard N.S.S. 8.0 ReportPack	7
Components of the GFI LANguard N.S.S. 8.0 ReportPack	7
Key features	10
License scheme and evaluation period	11
Installation	12
System requirements	12
Installation procedure.....	12
Launching the GFI LANguard N.S.S. reports for GFI ReportCenter	16
Selecting a product	16
Getting started: Default reports	17
Introduction	17
Generating a default report	17
Analyzing the generated report.....	20
Adding default reports to the list of favorite reports	21
Custom reports	23
Introduction	23
Creating a new custom report.....	23
Configuring data filter conditions.....	25
Run a custom report.....	31
Editing a custom report	31
Deleting a custom report.....	31
Adding custom reports to the list of favorite reports	32
Scheduling reports	33
Introduction	33
Scheduling a report.....	33
Configuring advanced settings.....	35
Configuring report export to file options	36
Configuring report emailing options	37
Viewing the list of scheduled reports	38
Viewing the scheduled reports activity.....	39
Enable/disable a scheduled report.....	40
Editing a scheduled report	40
Deleting a scheduled report	41
Example: Scheduling a report.....	41
Configuring default options	46
Introduction	46
Configuring database source: Microsoft SQL Server	47
Configuring database source: Microsoft Access.....	47
Viewing the current database source settings	49

Configuring default scheduling settings	49
Importing/Exporting the configuration	49
General options	53
Entering your license key after installation	53
Viewing the current licensing details.....	54
Viewing the product ReportPack version details	54
Checking the web for newer builds	54
Appendix: GFI LANguard Network Security Scanner default reports	56
Vulnerabilities scanning reports	56
Network vulnerability summary	56
Network vulnerability trend.....	59
Vulnerability distribution by host	60
Vulnerability distribution by operating system.....	61
Security scans history	62
Vulnerability listing by category.....	63
Vulnerability listing by host.....	64
Vulnerability listing by product	65
Vulnerability listing by severity	66
Open trojan ports by host.....	67
Open trojan ports	67
Top SANS vulnerabilities status.....	68
Vulnerable hosts based on open ports	69
Vulnerable hosts based on vulnerability level.....	69
Patch management reports.....	70
Network patching status.....	70
Missing patches grouped by host	72
Missing patches grouped by operating system.....	73
Missing patches grouped by severity	73
Installed patches grouped by host	74
Installed patches grouped by operating system	74
Installed patches grouped by severity	75
Deployment history by host.....	75
Deployment history by date	76
Deployment history by patch.....	76
System information reports	77
Software audit	77
Operating system and service pack distribution	78
System information	80
Computer properties	84
Uptimes	84
Disk utilization	85
Groups and users	85
SNMP information.....	86
Services	86
Processes	87
Devices	88
Shares.....	88
Open ports	89
Installed applications.....	89
Policies.....	90
Registry information	90
Results comparison.....	92
Network security log by date.....	92
Network security log by host	93
Baseline changes comparison	94
Troubleshooting	95

Introduction 95
Knowledge Base 95
Request technical support via email 95
Request technical support via web chat 96
Request technical support via phone..... 96
Web Forum 96
Build notifications 96

Index

97

Introduction

About GFI ReportCenter

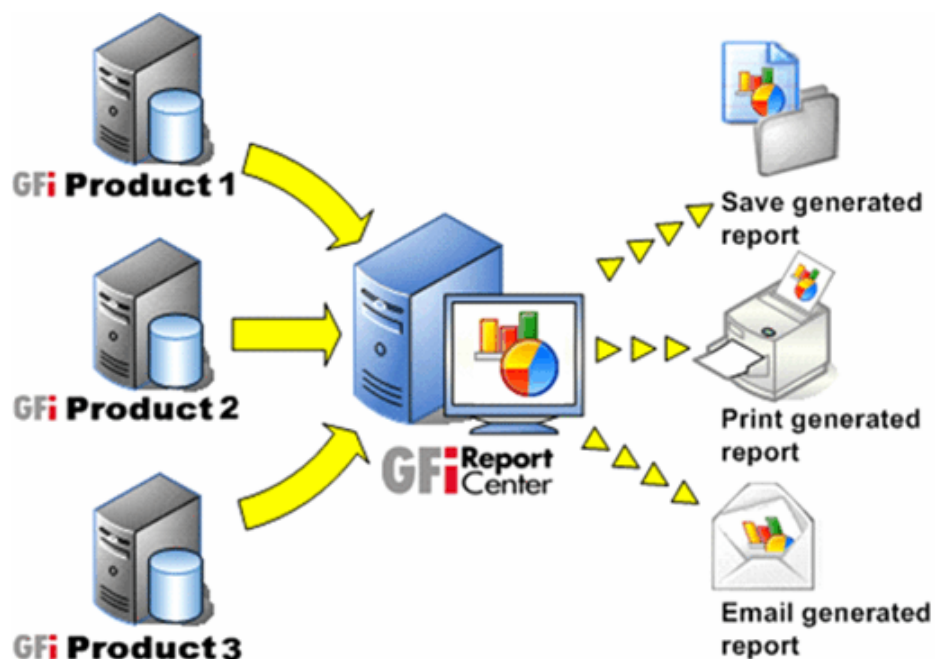


Figure 1 - Centralized reporting framework

GFI ReportCenter is a centralized reporting framework that allows you to generate various reports using data collected by different GFI products. GFI releases specialized reports for each of its products, referred to as a ReportPack; for example, the GFI LANguard Network Security Scanner ReportPack. A ReportPack can be purchased as an add-on to the GFI product.

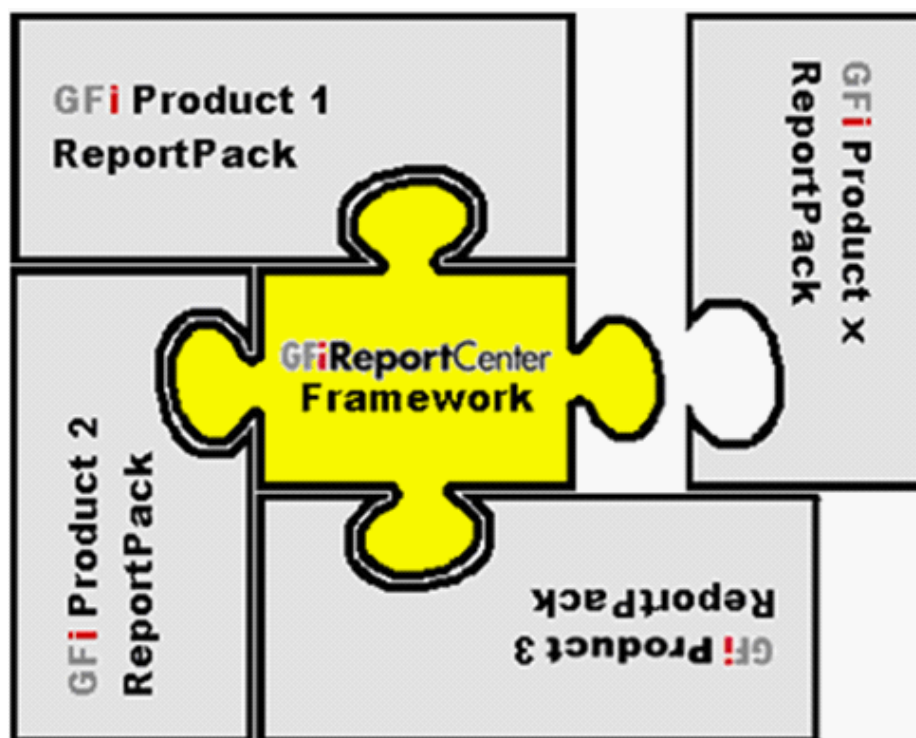


Figure 2 – Several ReportPacks plugged into the GFI ReportCenter framework

A ReportPack plugs into the GFI ReportCenter framework; allowing you to generate, analyze, export and print the information generated through these reports.

About the GFI LANguard N.S.S. 8.0 ReportPack

The GFI LANguard Network Security Scanner ReportPack is a full-fledged reporting companion to GFI LANguard Network Security Scanner (GFI LANguard N.S.S.). It allows you to generate graphical IT-level, technical and management reports based on the network security audits carried out by GFI LANguard N.S.S.

From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI LANguard N.S.S. ReportPack provides you with the easy-to-view information required, to fully identify any vulnerability on your corporate network.

The GFI LANguard N.S.S. ReportPack allows for the creation of various graphical and text based reports related to:

- Vulnerabilities scanning reports
- Patch management reports
- System information reports
- Results comparison reports.

Components of the GFI LANguard N.S.S. 8.0 ReportPack

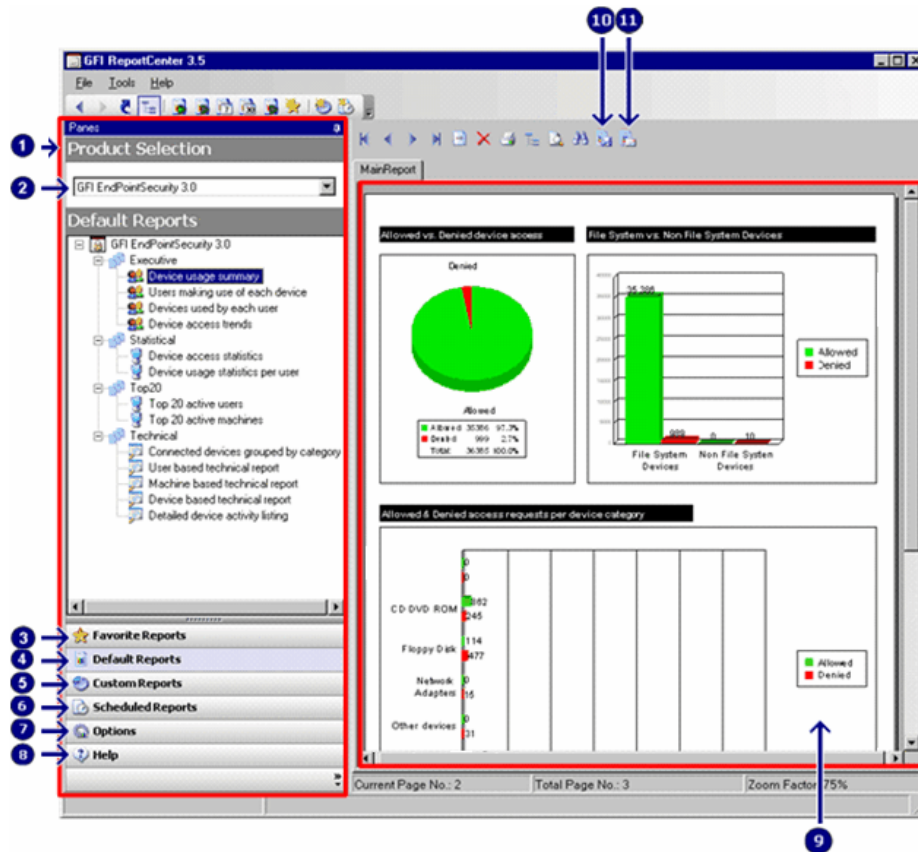
When you install the GFI LANguard N.S.S. 8.0 ReportPack, the following components are installed:

- GFI ReportCenter framework
- GFI LANguard N.S.S. 8.0 default reports

- Report scheduling service.

GFI ReportCenter framework

The GFI ReportCenter framework is the management console through which you can generate the specialized product reports which are shipped with a product ReportPack. The GFI ReportCenter framework offers a common application interface through which you can navigate, generate, customize and schedule reports.



Screenshot 1 – The GFI ReportCenter management console

The GFI ReportCenter management console is organized as follows:

1	Navigation Pane – Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
2	Product Selection drop-down list – Use this drop-down list to select the GFI product for which to generate reports. The Product Selection drop-down list displays all the products for which you have installed a ReportPack.
3	Favorite Reports – Use this navigation button to access your favorite/most used reports. For more information on how to add reports to this list refer to the ‘Adding default reports to the list of favorite reports’ and ‘Adding custom reports to the list of favorite reports’ sections in this manual.
4	Default Reports – Use this navigation button to access the default list of reports which can be generated for the selected product. For more information on default reports refer to the ‘GFI LANguard N.S.S. default reports’ section in this manual.
5	Custom Reports – Use this navigation button to access the list

	of customized reports which can be generated for the selected product. For more information on how to create custom reports refer to the 'Custom reports' chapter in this manual.
6	Scheduled Reports – Use this navigation button to access the list of scheduled reports for automatic generation and distribution. For more information on how to create scheduled reports refer to the 'Scheduling reports' chapter in this manual.
7	Options – Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.
8	Help – Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
9	Report Pane - Use this multi-functional pane to: <ul style="list-style-type: none"> • View and analyze generated reports • Maintain the scheduled reports list • Explore samples and descriptions of default reports.
10	Export – Use this button to export generated reports to various formats including HTML, Adobe Acrobat (PDF), Excel (XLS), Word (DOC), and Rich Text Format (RTF).
11	Send email – Use this button to instantly distribute the last generated report via email.

GFI LANguard N.S.S. 8.0 default reports

The GFI LANguard N.S.S. 8.0 default reports are a collection of specialized pre-configured reports which plug into the GFI ReportCenter framework. These reports present the results of network security scans performed by GFI LANguard N.S.S. and allow for the generation of both graphical and tabular IT-Level, technical and management reports. Default reports can also serve as the base template for the creation of customized reports which fit specific network-reporting requirements.

Report scheduling service

The report scheduling service controls the scheduling and automatic distribution of reports by email. Reports generated by this service can also be saved to a specific hard disk location in a variety of formats which include DOC, PDF, RTF and HTML.

Key features

Centralized reporting

GFI ReportCenter is a one-stop, centralized reporting framework which enables the generation and customization of graphical and tabular reports for a wide array of GFI products.

Wizard assisted configuration

Wizards are provided to assist you in the configuration, scheduling and customization of reports.

Report scheduling

With GFI ReportCenter you can schedule reports to be generated on a pre-defined schedule as well as at specified intervals. For example, you can schedule lengthy reports to be generated after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Distribution of reports via email

GFI ReportCenter allows you to automatically distribute generated reports via email. In scheduled reports, this can be achieved automatically after the successful generation of a scheduled report.

Report export to various formats

By default, GFI ReportCenter allows you to export reports to various formats. Supported formats include HTML, PDF, XLS, DOC and RTF. When scheduling reports, you can optionally configure the preferred report output format. Different scheduled reports can also be configured to output generated reports to different file formats.

Default reports

The GFI LANguard N.S.S. ReportPack ships with a default set of graphical and tabular reports. These reports can be generated without any further configuration effort immediately after the installation. The

default reports in this ReportPack are organized into four different report-type categories:

- Vulnerabilities scanning reports
- Patch management reports
- System information reports
- Results comparison reports.

Report customization

The default reports that ship with every ReportPack can serve as the base template for the creation of customized reports. Report customization is achieved by building up custom data filters which will analyze the data source and filter the information that matches specific criteria. In this way, you create reports tailored to your reporting requirements.

Favorites

GFI ReportCenter allows you to create bookmarks to your most frequently used reports – both default and custom.

Printing

By default, all reports generated by GFI ReportCenter are printer friendly and can be printed through the windows printing services provided by the system where GFI ReportCenter is installed.

License scheme and evaluation period

Evaluation period

The default evaluation period for this product is of 10 days. However you can apply for a 30-day product evaluation key by filling in our [online registration form](#). This will also qualify you for free email support. The 30-day evaluation period key will be emailed to you automatically after you download the product.

NOTE: During the evaluation period, you may use all the features available with GFI ReportCenter.

Purchasing a license key

You can purchase a license key online by visiting the GFI website (<https://www.gfi.com/pages/cart/orderform.aspx>). After purchasing a product license, you do not need to re-install the GFI ReportCenter framework and GFI LANguard N.S.S. ReportPack. Just key in the license key via the **Licensing** node provided in the management console. For more information refer to the 'Entering your license key after installation' section in this manual.

Installation

System requirements

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

- Windows 2000 (SP4) / XP (SP2) / 2003 operating system
- Internet Explorer 5.1 or higher
- .NET Framework version 1.1.

NOTE: The GFI LANguard N.S.S. ReportPack only allows you to generate reports for data contained in scan results databases which were created and maintained by GFI LANguard N.S.S.

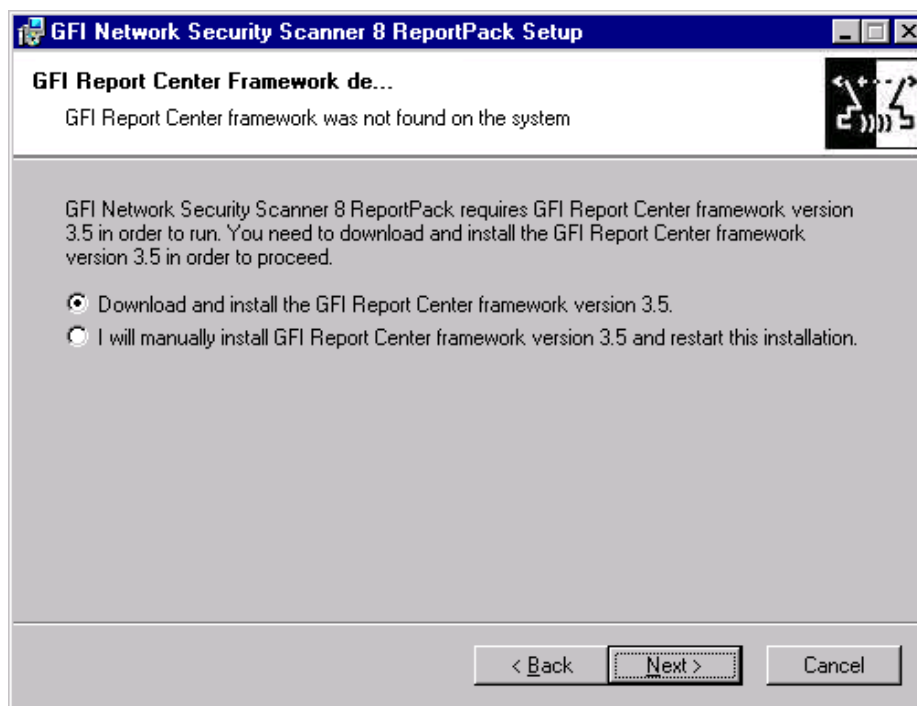
Installation procedure

The GFI LANguard N.S.S. ReportPack includes an installation wizard which will assist you through the installation process. During the installation process this wizard will:

- Verify that you are running the latest version of the GFI ReportCenter framework; if you are installing the framework for the first time or the currently installed framework version is outdated, the installation wizard will automatically download the latest one for you.
- Automatically install all the required components distributed including the GFI ReportCenter framework, the GFI LANguard N.S.S. default reports and the Report Scheduling service.

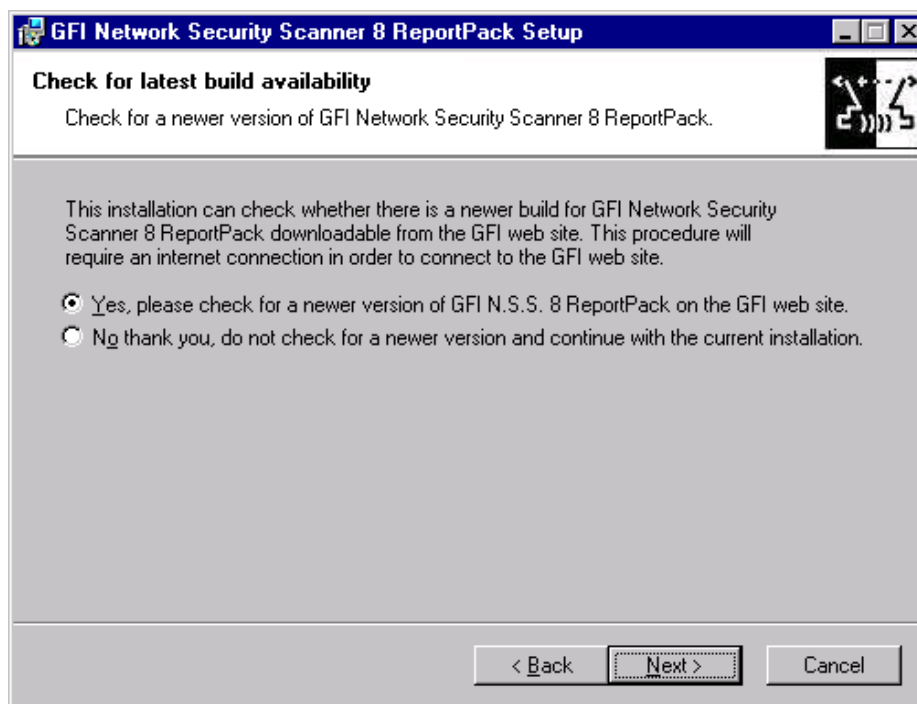
To start the installation:

1. Double-click on **languardnss7rp.exe**. As soon as the welcome dialog is displayed, click **Next** to start the installation.



Screenshot 2 - GFI ReportCenter framework detection dialog

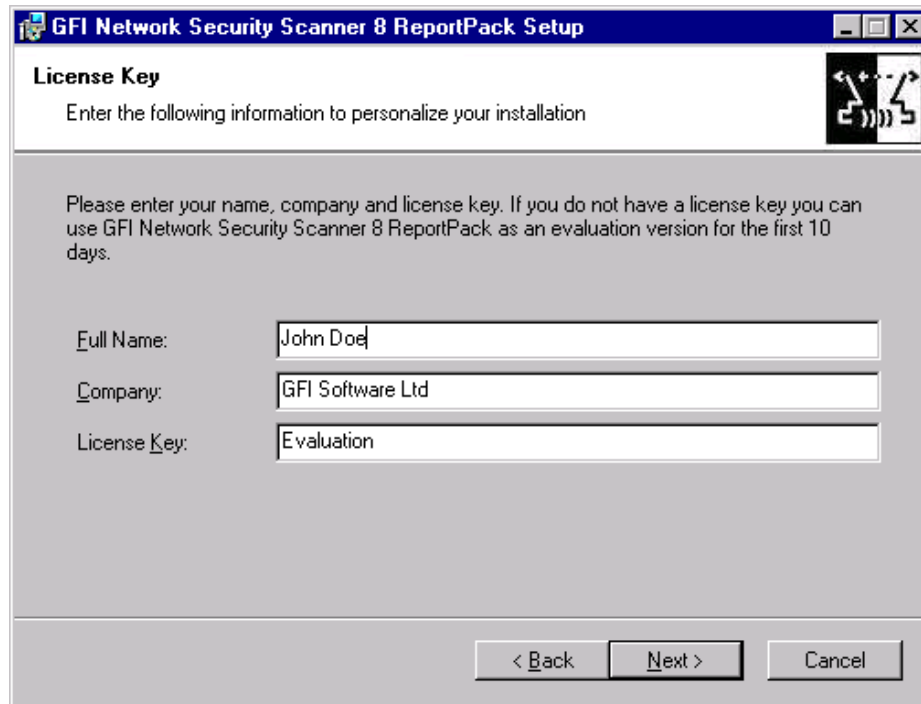
2. If the current version of your GFI ReportCenter framework is not compatible with the GFI LANguard N.S.S. ReportPack, you will be prompted to download and install an updated version. To automatically achieve this, leave the dialog options as default and click on the **Next** button.



Screenshot 3 - Check for latest build availability

3. Choose whether you want the installation wizard to search for a newer build of the GFI LANguard N.S.S. 8.0 ReportPack on the GFI website. Then, click on the **Next** button to proceed with the installation.

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



License Key

Enter the following information to personalize your installation

Please enter your name, company and license key. If you do not have a license key you can use GFI Network Security Scanner 8 ReportPack as an evaluation version for the first 10 days.

Full Name:

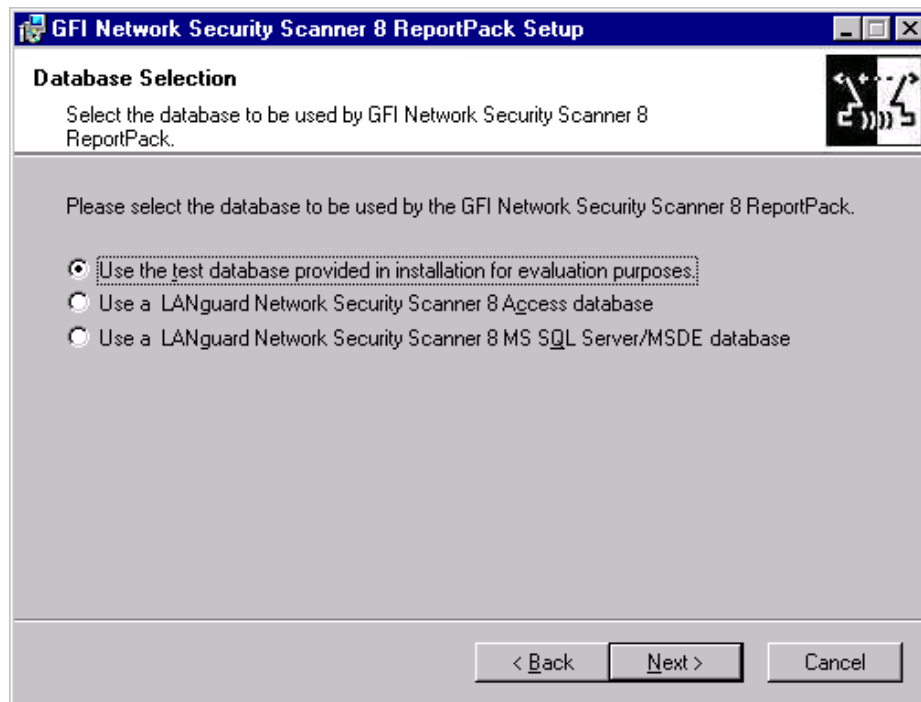
Company:

License Key:

< Back Next > Cancel

Screenshot 4 - Licensing details dialog

5. Specify the full user name, the company name and the license key. If you will be evaluating the product for 10 days, leave the evaluation key as default (i.e. "Evaluation"). Click on **Next** to continue.



Database Selection

Select the database to be used by GFI Network Security Scanner 8 ReportPack.

Please select the database to be used by the GFI Network Security Scanner 8 ReportPack.

Use the test database provided in installation for evaluation purposes.

Use a LANguard Network Security Scanner 8 Access database

Use a LANguard Network Security Scanner 8 MS SQL Server/MSDE database

< Back Next > Cancel

Screenshot 5 – SQL Server selection dialog

6. Specify which database backend is being used by your GFI LANguard N.S.S. installation.

NOTE 1: For evaluation purposes you can also use the sample database that is distributed with this installation.

NOTE 2: If a MS Access database is being used and you are not installing the GFI LANguard N.S.S. ReportPack on the same computer that is running GFI LANguard N.S.S., click Browse and specify the path to your MS Access database backend using UNC (e.g. \\LNSS Server\GFI\ScanResults.mdb).

GFI Network Security Scanner 8 ReportPack Setup

SQL Server selection

Please enter the requested information

Please specify an SQL server containing a valid LANguard Network Security Scanner 8 database, and the necessary logon information.

SQL server details:

Server:

Use Windows authentication.

Login using the following credentials (SQL Account):

User:

Password:

< Back

Screenshot 6 - Database configuration dialog

7. If an MS SQL Server/MSDE database backend is being used, specify the SQL server details (name, authentication method and credentials). Click on **Next** to continue.

GFI Network Security Scanner 8 ReportPack Setup

Mail Settings

Enter administrator email and SMTP mail server settings

Please enter the details of the SMTP server and email address that are to be used by GFI Network Security Scanner 8 ReportPack for email reporting.

From:

To:

SMTP server: Port:

SMTP server does not require authentication.
 SMTP server requires authentication.

< Back

GFI ReportCenter

8. Specify the default email settings that will be used for report distribution.
9. Specify the product installation path or click **Next** to leave as default. The installation will need approximately 100 MB of free disk space.
10. The installation wizard is now ready to copy the required files and finalize the installation. To proceed click on the **Next** button.

Launching the GFI LANguard N.S.S. reports for GFI ReportCenter

Following the installation, launch the GFI LANguard N.S.S. Reports for GFI ReportCenter from **Start ▶ Programs ▶ GFI ReportCenter ▶ LANguard Network Security Scanner 8 ReportPack**.

NOTE: GFI ReportCenter will run with limited functionality upon expiry of the evaluation period. This will also occur if the license key you entered is not a valid GFI ReportCenter license key.

Selecting a product

When more than one product ReportPack is installed, use the **Product Selection** drop down list to select the GFI product ReportPack to be used.



Screenshot 8 – Product Selection drop down list

For example, to run the reports provided in the GFI LANguard N.S.S. ReportPack:

1. Launch GFI ReportCenter from **Start ▶ Program Files ▶ GFI ReportCenter**.
2. Select 'GFI LANguard Network Security Scanner 8.0' from the **Product Selection** drop down list.

NOTE: Select the 'ALL PRODUCTS' option to display and navigate all the ReportPacks that are currently installed in GFI ReportCenter.

Getting started: Default reports

Introduction

After installing the GFI LANguard N.S.S. ReportPack, a number of specialized pre-configured reports can immediately be generated on the data stored in the database backend of GFI LANguard N.S.S. These default reports are organized into the following categories:

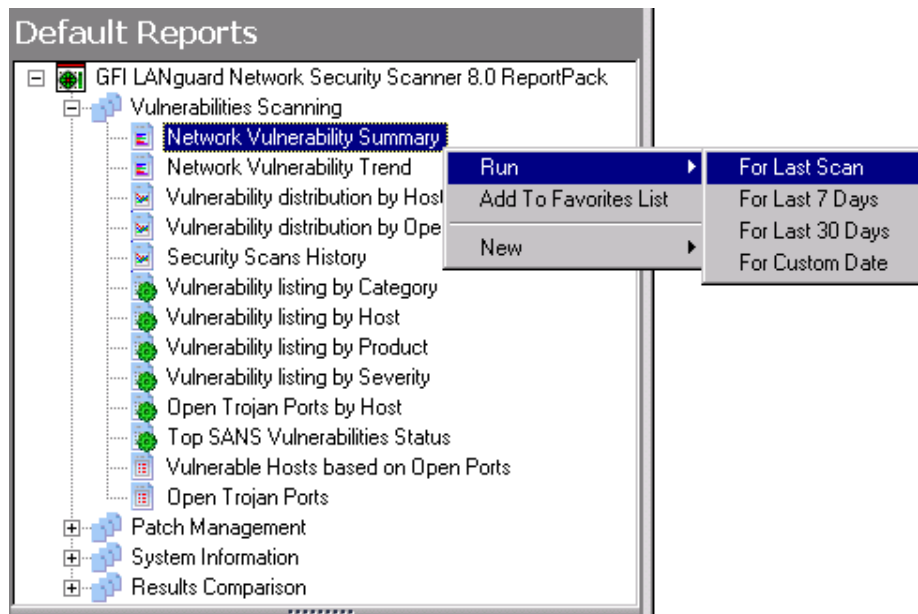
- **Vulnerabilities scanning reports:** Use the reports in this category to identify vulnerabilities detected on the network. The reports include vulnerability details such as host machines, operating systems affected and severity.
- **Patch management reports:** Use the reports in this category to display information on network patches and service packs installed as well as those still requiring deployment.
- **System information reports:** Use the reports in this category to display detailed information on hardware and software present on the network. These reports help management in analyzing conformance with corporate security policy.
- **Results comparison reports:** Use the reports in this category to compare results of consecutive network scans that have a common profile and target, and of computer scans against a computer used as benchmark.

GFI LANguard N.S.S. default reports are accessed by clicking on the **Default Reports** navigation button provided in the navigation pane.

Generating a default report

To generate a default report:

1. Click on the **Default Reports** navigation button to bring up the list of default reports available.



Screenshot 9 – Selecting the data set

2. Right-click on the report to be generated, select **Run** and specify the scan date/time period that will be covered by the report.

Example 1: Generating a “Network Vulnerability Summary” report based on the last scan.

This example demonstrates how to generate a network vulnerability summary report based on the last network security scan carried out:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.
2. Right-click on **Network Vulnerability Summary** and select **Run ▶ For Last Scan**.

Example 2: Generating a “Network Vulnerability Summary” report based on scans made on a particular day.

This example demonstrates how to generate a network vulnerability summary report based on the scan performed on January 14, 2007.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.
2. Right-click on **Network Vulnerability Summary** and select **Run ▶ For Custom Date**.

Specify Custom Date

Date Time
Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found during these scans.

Relative
Today

Day
Sunday, January 14, 2007

[Month] [Year] 2007

Sun	Mon	Tue	Wed	Thu	Fri	Sat
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

Today: 1/29/2007

< Back Next > Cancel

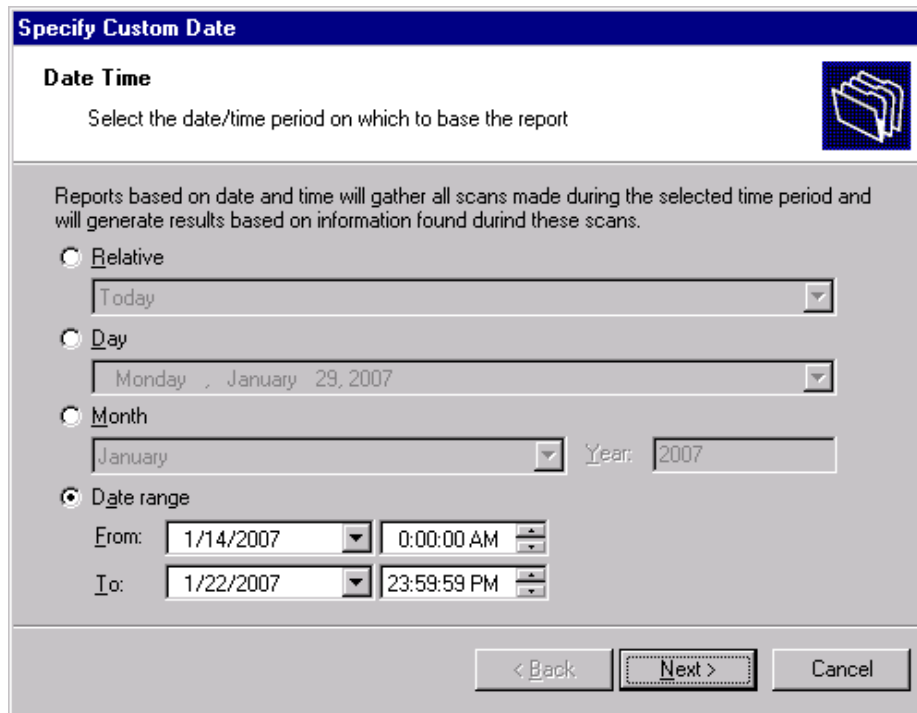
Screenshot 10 - Configuring custom date/time period

3. Select the 'Day' option and expand the provided drop down. This will bring up the date selection calendar.
4. Navigate to the required month (i.e. January) and select the required day (i.e. 14).
5. Click **Finish** to generate the report.

Example 3: Generating a “Network Vulnerability Summary” report based on data collected over a specific date/time period.

This example demonstrates how to generate a network vulnerability summary report based on network security scans carried out between January 14, 2007 and January 22, 2007.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.
2. Right-click on **Network Vulnerability Summary** and select **Run ▶ For Custom Date**.



Screenshot 11 - Configuring custom date/time period

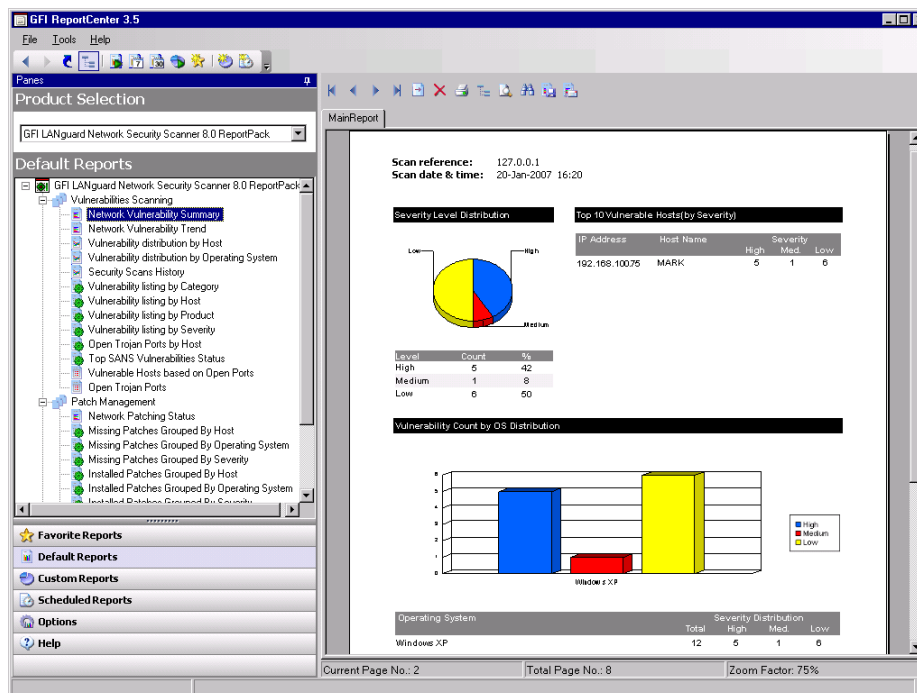
3. Select the 'Date range' option and specify the required parameters:

- 'From' – 01/14/2007 0:00:00.
- 'To' – 01/22/2007 23:59:59.

NOTE: Date and time format are based on the regional settings configured on your computer.

4. Click **Finish** to generate the report.







Analyzing the generated report





Screenshot 12 – Generated reports are displayed in the right pane of the management console

Generated reports are shown in the right pane of the GFI ReportCenter. Use the toolbar at the top of the report pane to access common report related functions:

Report browsing options

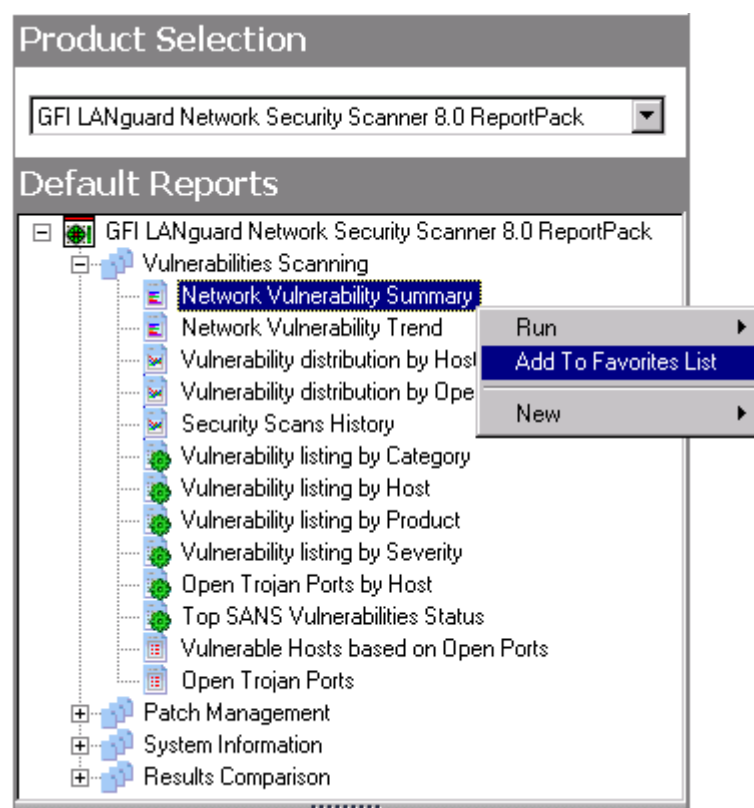
-  Browse the generated report page by page.
-  Zoom in/Zoom out.
-  Search the report for particular text or characters.
-  Go directly to a specific page.
-  Breakdown the report into a group tree (e.g. by date/time).
-  Print report.

Report storage and distribution options

-  Export the generated report to a specific file format.
-  Distribute the generated report via email.

NOTE: For information on how to configure report storage and distribution options refer to the 'Configuring Advanced Settings' section in this manual.

Adding default reports to the list of favorite reports



Screenshot 13 – Favorite Reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a default report to the list of favorite reports:

1. Click on the **Default Reports** navigation button to bring up the list of available reports.
2. Right-click on the default report that you to be added to favorites and select **Add to favorites list**.
3. Click Yes to confirm.

Custom reports

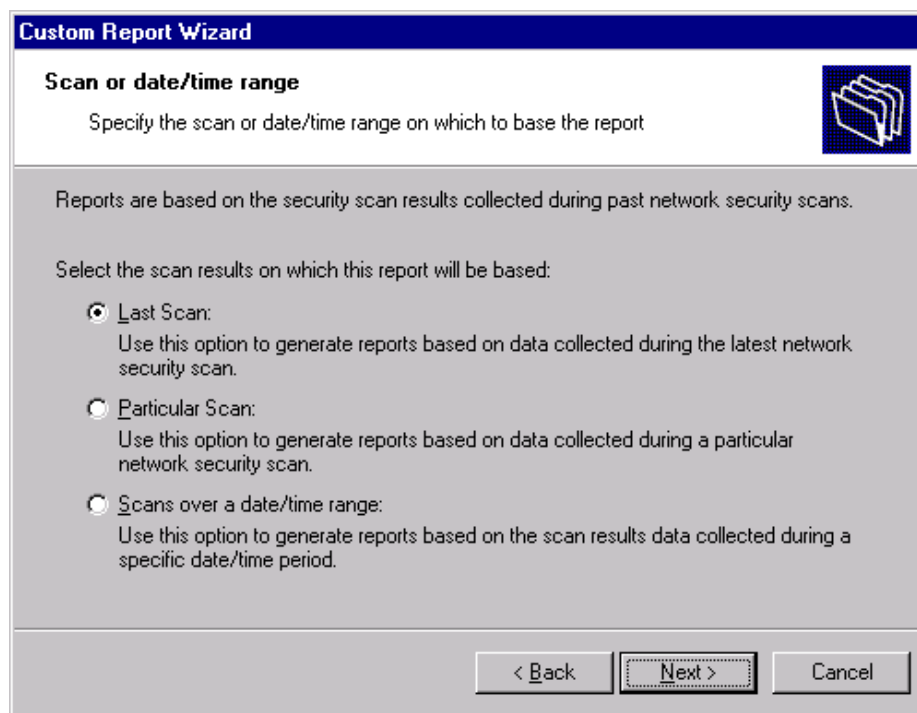
Introduction

GFI ReportCenter allows you to create custom reports which are tailored to your reporting requirements. This is achieved by building up custom data filters which will analyze the data source and filter out the information that matches the specified criteria.

Creating a new custom report

To create a custom report:

1. Click on the **Default Reports** navigation button.
2. Right-click on the default report to be used as template and select **New ► Custom Report**. This will bring up the 'Custom Report Wizard'.

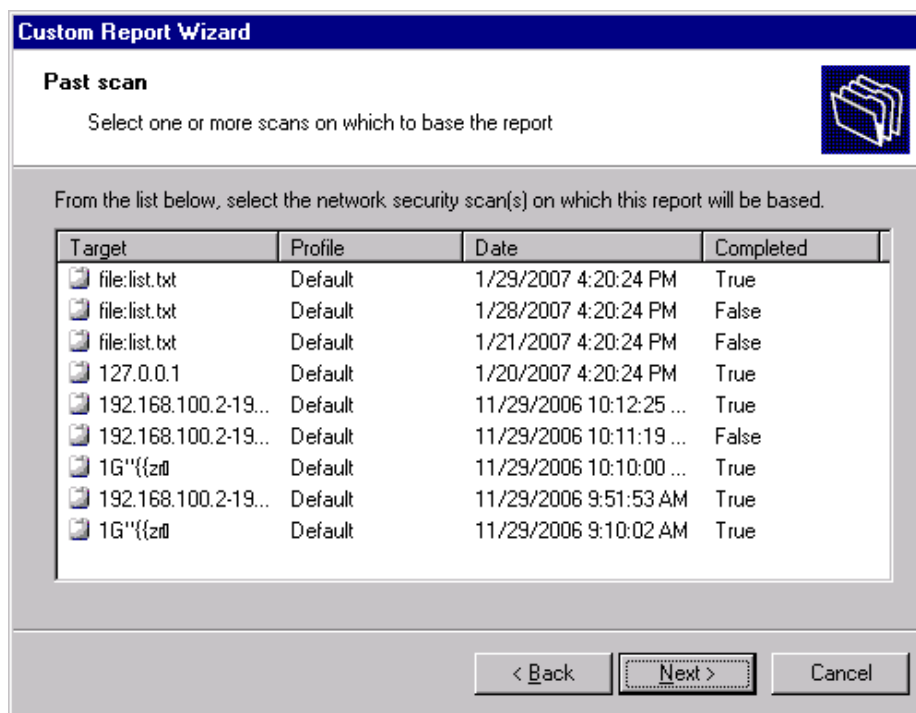


Screenshot 14 - Selecting the scan data source to use

3. Specify the data source option that will be used to generate the custom report. This data source refers to scan results from:

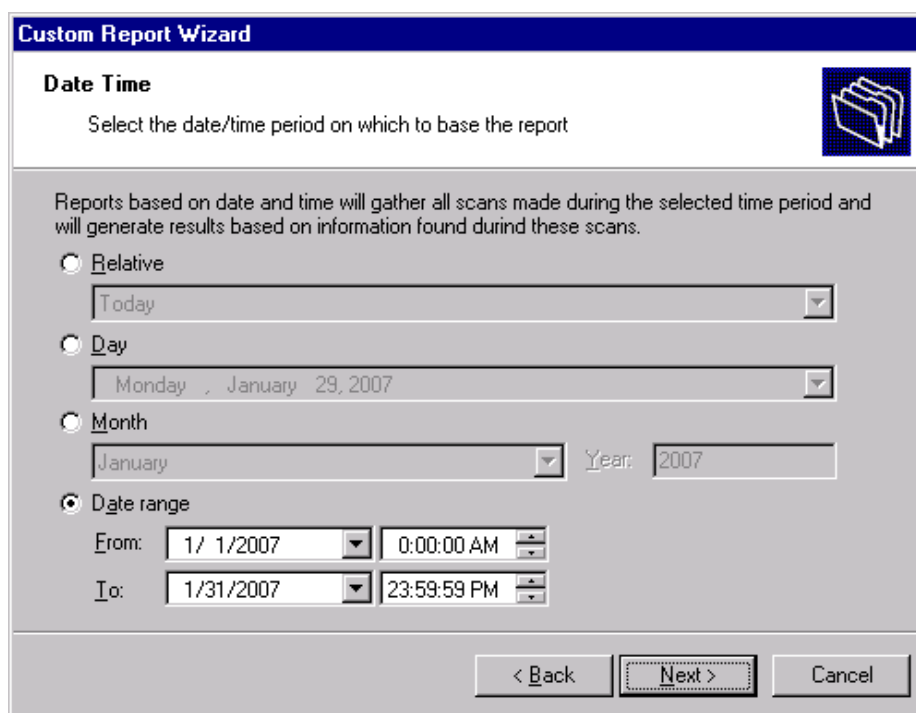
- the last scan
- particular scan(s)
- scans carried out over a specific date/time period.

Click on **Next** to continue.



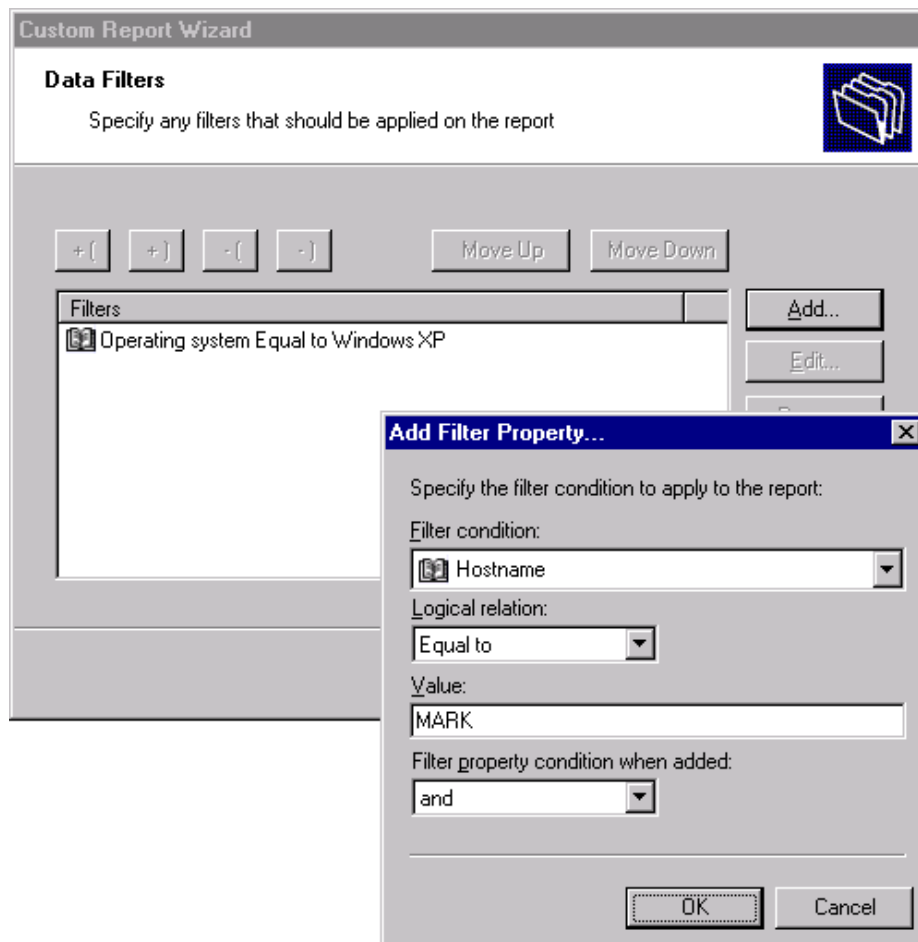
Screenshot 15 – Selecting the scan data source to use

4. If using the ‘Particular Scan’ option, select the required scan(s) from the list of network security scans carried out on the corporate network. Click on **Next** to continue.



Screenshot 16 - Configuring custom date/time period

5. If using the ‘Scans over a date/time range’ option, select the date/time period from which network security scan results will be gathered. Click on **Next** to continue.



Screenshot 17 – Specifying data filter conditions

6. Configure the data filter conditions that will be applied against the selected data source. Click on **Next** to continue.

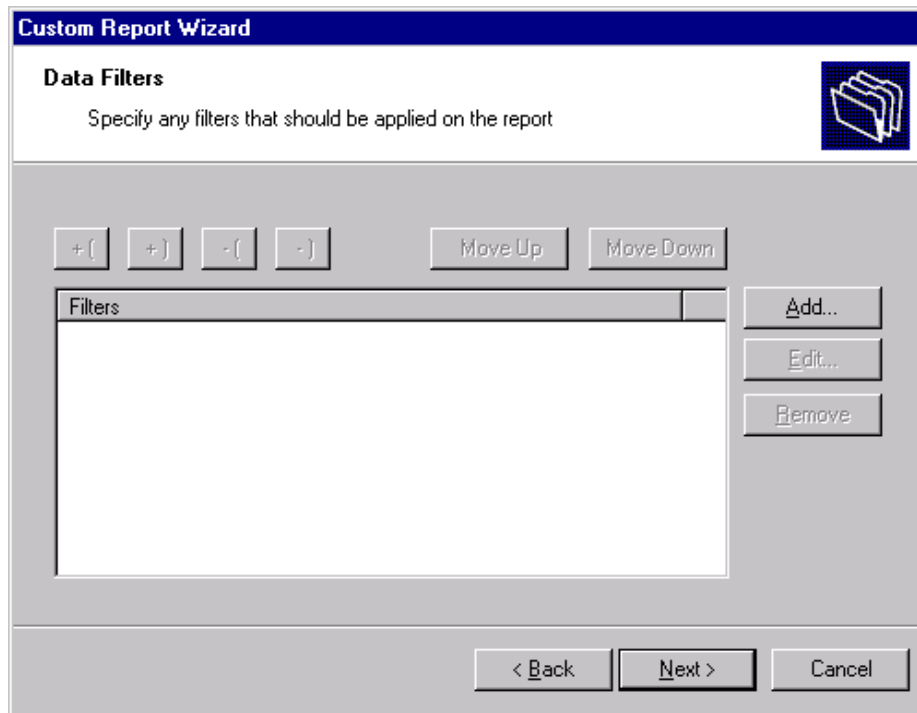
NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this manual.

7. Specify a name and description for the customized report. Click on **Next** to continue.

8. Click on **Finish** to finalize your configuration settings.

Configuring data filter conditions

Use data filter conditions to specify which network security scan data/results will be included in the report. Only scans which match the specified criteria will be processed and presented within the report.

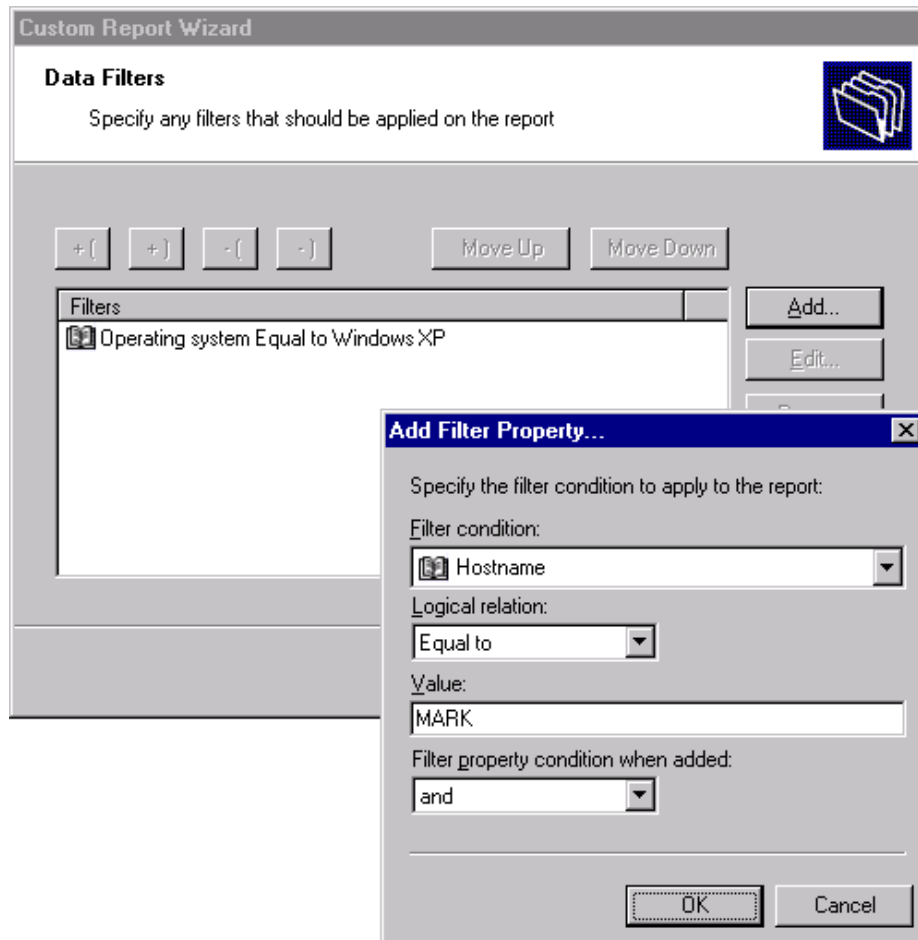


Screenshot 18 - Custom Report Wizard: Filters dialog

Click on the **Add...** button to bring up the 'Edit filter properties' dialog and configure the following conditions:

- '*Filter condition*' – Specify the data source area on which the filter will focus (for example, select 'Operating System' to filter the events data related to a specific operating system).
- '*Condition*' – Specify the condition comparison parameter.
- '*Value*' – Specify the string to which source data will be compared.

For example to generate a report which contains only information related to Windows XP, configure your filter parameters as shown below:



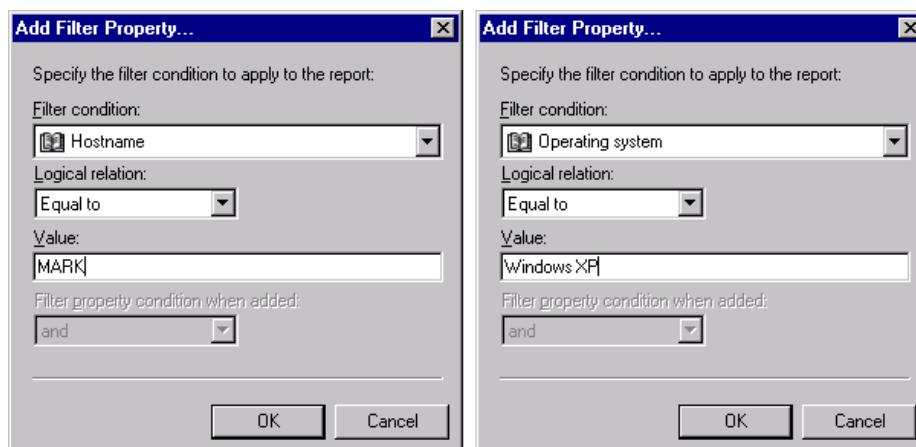
Screenshot 19 - Filter conditions configuration dialog

For more specific reports, you can limit the range of information to be displayed by tightening your conditions/search criteria. This is achieved by configuring and applying multiple data filters against the selected data source. When more than one filter is used, specify how these filters will be logically linked. This is achieved by selecting a logical grouping condition from 'Filter property condition...' drop down list.

- Select **And** to include ALL the scan data information that satisfies ALL of the conditions specified in the filters.
- Select **Or** to include ALL the scan data information that matches at least one of the specified filter conditions.

Example: Using multiple filters

Consider the situation where a custom report has 2 filters configured as follows:



Screenshot 20 - Using multiple filters

Parameters	Filter 1	Filter 2
Filter condition	Hostname	Operating System
Logical relation	Is equal to	Is equal to
Value	'Mark'	'Windows XP'

The data which will be included in this custom report will vary according to how these filters will be applied against your data. This is defined through the 'Filter property condition... ' drop-down.

Filters applied			Data output
Filter 1	and	Filter 2	The report will show: <ul style="list-style-type: none"> All scan data which is related to a host called 'Mark' which runs on 'Windows XP'.
Filter 1	or	Filter 2	The report will show: <ul style="list-style-type: none"> All scan data related to 'Windows XP' – (no matter which host it belongs to) AND <ul style="list-style-type: none"> All scan data related to a host called 'Mark' – (no matter which operating system it has installed).

Example: Creating a custom report based on network security scans performed during a particular month

This example demonstrates how to generate a network vulnerabilities summary report called 'Network vulnerabilities summary on hostname Mark for January 2007'. This report will be based on scans:

- Related to a host named 'Mark'
- Corresponding to operating system 'Windows XP'
- Performed during the month of 'January 2007'.

To create this report:

1. Click on the **Default Reports** navigation button.
2. Right-click on the report to be customized and select **New ► Custom Report**. This will bring up the 'Custom Reports Wizard'.
3. As soon as the welcome dialog is displayed, click **Next**.

Custom Report Wizard

Scan or date/time range

Specify the scan or date/time range on which to base the report

Reports are based on the security scan results collected during past network security scans.

Select the scan results on which this report will be based:

Last Scan:
Use this option to generate reports based on data collected during the latest network security scan.

Particular Scan:
Use this option to generate reports based on data collected during a particular network security scan.

Scans over a date/time range:
Use this option to generate reports based on the scan results data collected during a specific date/time period.

< Back Next > Cancel

Screenshot 21 – Selecting the data source to use

4. Select the ‘Scans over a date/month range’ option and click Next.

Custom Report Wizard

Date Time

Select the date/time period on which to base the report

Reports based on date and time will gather all scans made during the selected time period and will generate results based on information found during these scans.

Relative
Today

Day
Monday, January 29, 2007

Month
January Year: 2007

Date range
From: 1/29/2007 17:43:22 PM
To: 1/29/2007 17:43:22 PM

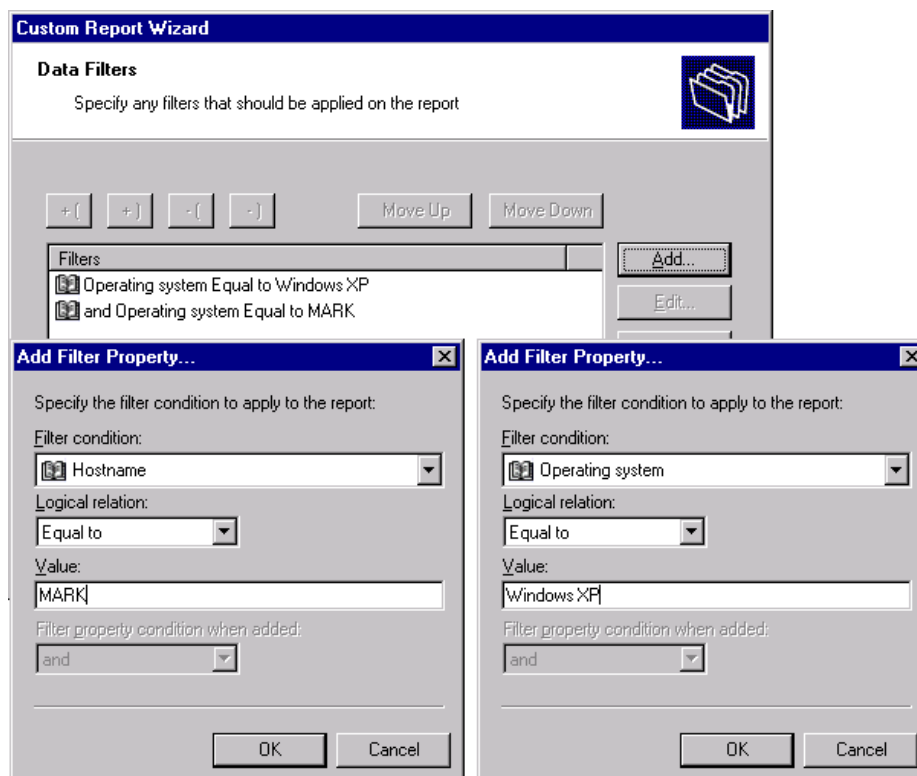
< Back Next > Cancel

Screenshot 22 – Selecting the date/time period

5. Select the ‘Month’ option and specify the following parameters:

- **Month:** ‘January’.
- **Year:** ‘2007’.

6. Click on **Next** to proceed to the data filters dialog.



Screenshot 23 - Filter conditions dialog(s)

6. Click on the **Add...** button and configure the parameters of filter 1 as follows:

- **Filter condition:** 'Hostname'
- **Condition:** 'Equal to'
- **Value:** 'Mark'.

7. Click **OK** to finalize your filter configuration settings.

8. Click again on the **Add...** button and configure the parameters of filter 2 as follows:

- **Filter condition:** 'Operating system'
- **Condition:** 'is equal to'
- **Value:** 'Windows XP'
- **Filter Property condition...:** 'and'.

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

10. Click **Next** and specify the following parameters:

- **Report Name:** 'Network Vulnerability summary for January 2007'
- **Report Title:** 'Network security scans of hostname Mark'
- **Report Description:** 'This report shows a summary of vulnerabilities found on hostname Mark during January 2007.'

11. Click **Next** to proceed to the final dialog.

12. Click **Finish** to finalize your custom report configuration settings.

Run a custom report

To run a custom report:

1. Click on the **Custom Reports** navigation button.
2. Right-click on the custom report to be generated and select **Generate**.

Editing a custom report

To edit the configuration settings of a custom report:

1. Click on the **Custom Reports** navigation button.



Screenshot 24 - Custom Report Wizard: Welcome dialog

2. Right-click on the custom report to be modified and select **Edit**. This will bring up the 'Custom Reports Wizard' through which you can make the required changes.

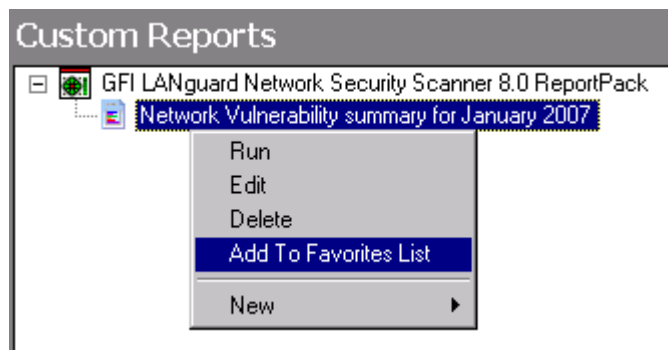
NOTE: For more information on how to configure the parameters of a custom report refer to the 'Creating a custom report' section in this chapter.

Deleting a custom report

To delete a custom report:

1. Click on the **Custom Reports** navigation button.
2. Right-click on the custom report to be permanently removed from the list and select **Delete**.
3. Click **Yes** to confirm.

Adding custom reports to the list of favorite reports



Screenshot 25 - Favorite reports navigation button

You can group and access frequently used reports through the **Favorite Reports** navigation button. To add a custom report to the list of favorite reports:

1. Click on the **Custom Reports** navigation button to bring up the list of available reports.
2. Right-click on the custom report to be added to favorites and select **Add to Favorites List**.
3. Click Yes to confirm.

Scheduling reports

Introduction

GFI ReportCenter allows you to generate reports on a pre-defined schedule as well as at specified intervals. This way you can automate the generation of reports that are required on regular basis/periodically.

Further to this, GFI ReportCenter can also be configured to automatically distribute scheduled reports via email. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format (e.g. PDF) in which the report will be attached to the email.

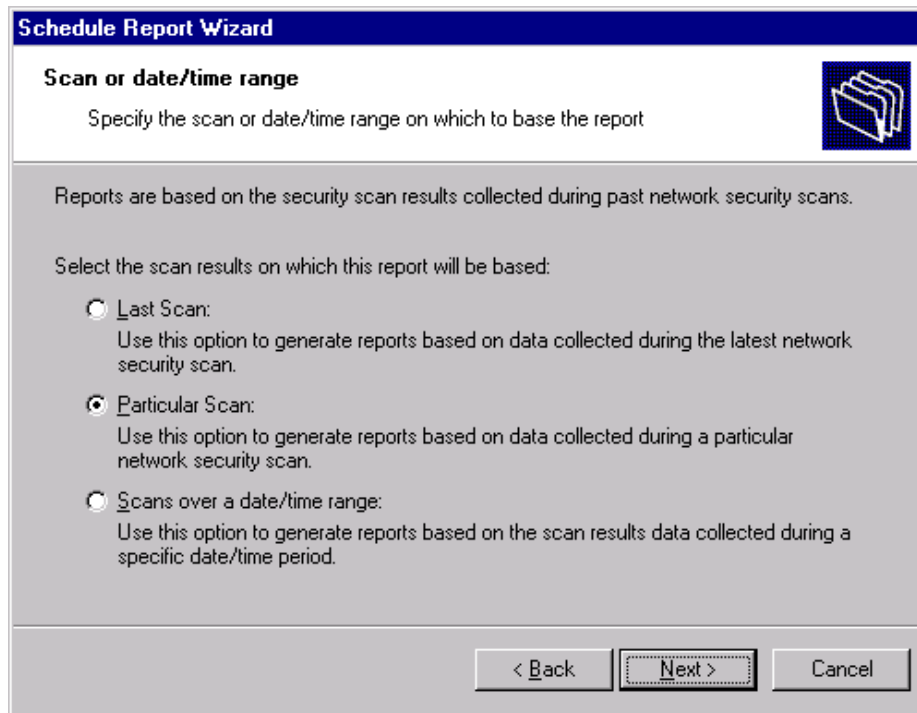
Use the report scheduling feature to automate your report generation requirements. For example, you can schedule lengthy reports after office working hours and automatically email them to the intended recipients. This way, you maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

Both default and custom reports can be scheduled for automatic generation.

Scheduling a report

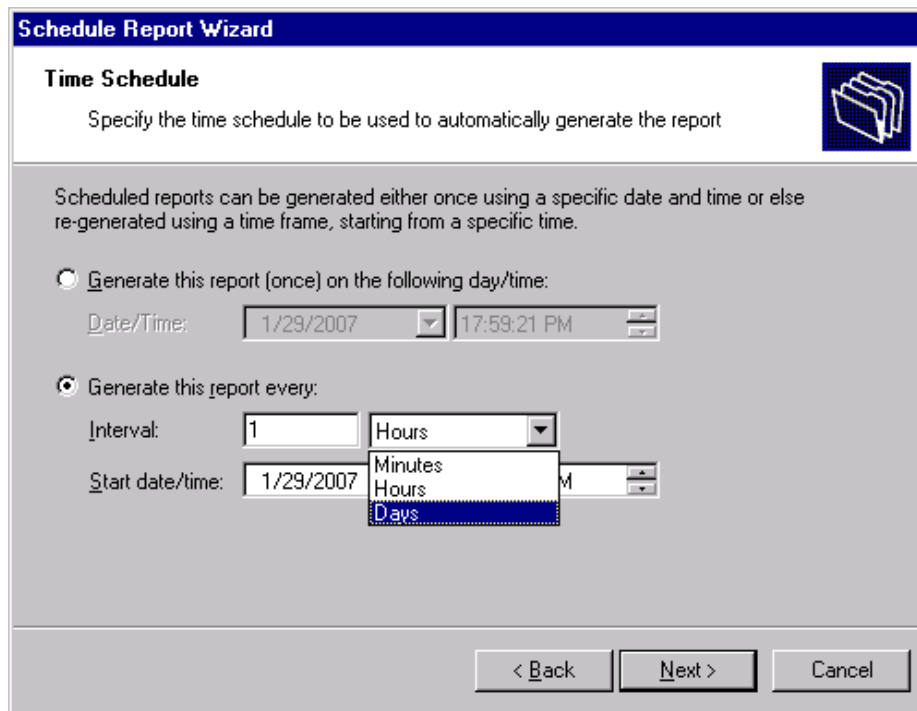
To schedule a report:

1. Click on the **Default/Custom Reports** option pane.
2. Right-click on the report to be scheduled and select **New ▶ Scheduled report**. This will bring up the 'Scheduled Report Wizard'. Click on **Next** to continue.



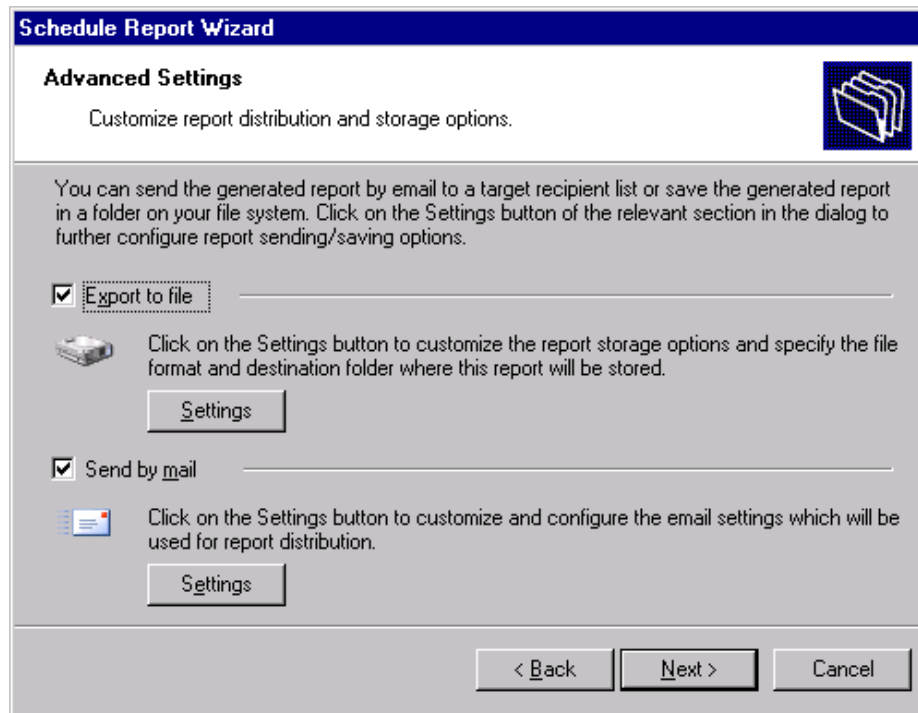
Screenshot 26 - Report Scheduling Wizard: Data-set selection dialog

3. Select the network security scan(s) data to be covered by this report.



Screenshot 27 – Report Scheduling Wizard: Time schedule dialogue

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.



Screenshot 28 – Report Scheduling Wizard: Advanced Settings dialog

5. To export the generated report to file, select the ‘*Export to file*’ option. To customize the report export configuration settings click on the **Settings** button underneath this option.

NOTE: For information on how to configure export-to-file settings refer to the ‘Configuring report export to file options’ section in this chapter.

6. To automatically distribute generated reports via email, select the ‘*Send by mail*’ option. To customize the email settings used for report distribution click on the **Settings** button underneath this option.

NOTE: For information on how to configure email settings refer to the ‘Configuring report emailing options’ in this chapter.

7. Specify a name and description for this scheduled report. Click on **Next** to continue.

8. Click on **Finish** to finalize your settings.

Configuring advanced settings

GFI LANguard N.S.S. ReportPack allows you to export scheduled reports to a specific file format as well as to automatically distribute these reports via email. This is achieved using either a set of parameters (e.g. recipient’s email addresses) which are specified on the fly during scheduled report configuration or using the default set of report export and distribution parameters configured during the ReportPack installation.

NOTE: The Report Scheduling Wizard is by default configured to use the default set of report export and distribution parameters.

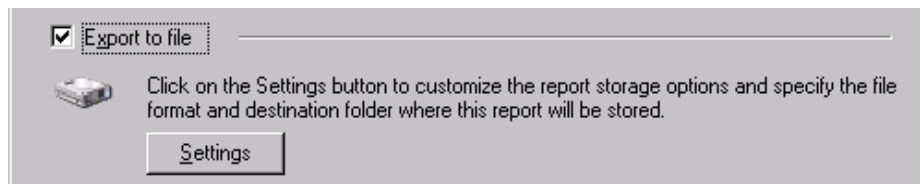
Report export formats

Scheduled reports can be exported in a variety of formats. Supported file formats include:

	Format	Description
1	Adobe Acrobat (.PDF)	Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.
2	MS Excel (.XLS)	Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.
3	MS Word (.DOC)	Use this format if you want to access this report using Microsoft Word.
4	Rich text format (.RTF)	Use this format to save the report in a format that is small in size and which allows accessibility through different word processors in different operating systems.

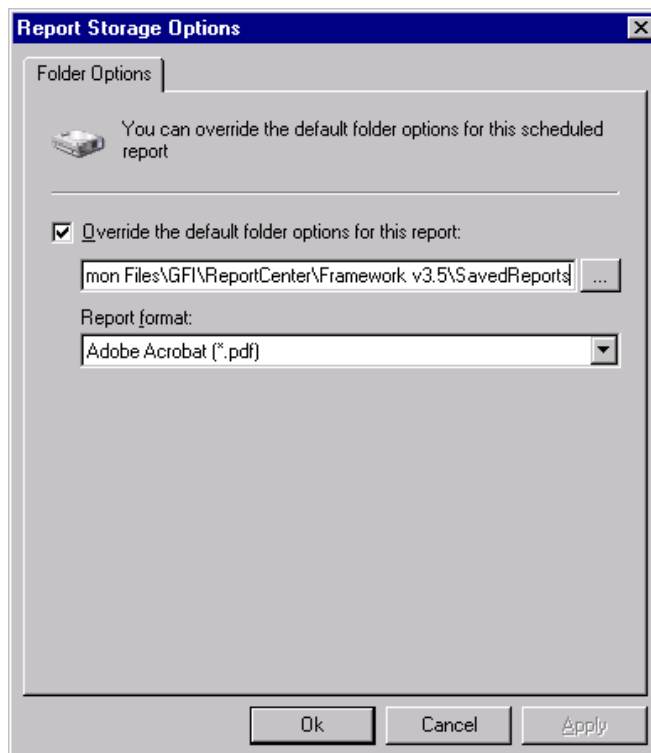
Configuring report export to file options

To configure the report export to file settings of a scheduled report do as follows:



Screenshot 29 - Advanced Settings dialog: Export to file settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the 'Export to file' option.



Screenshot 30 - Advanced Settings: Export to file options

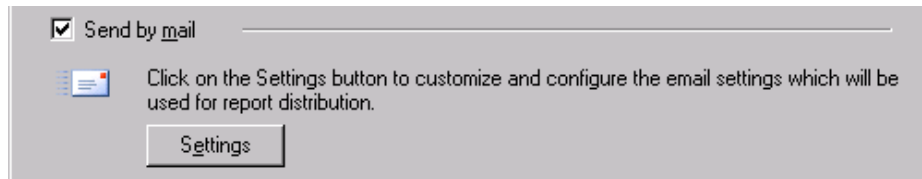
2. Select the option 'Override the default folder options for this report:'

3. Specify the complete path where the exported report will be saved.
4. Specify the file format in which the exported report will be saved.
5. Click **OK** to finalize your configuration settings.

NOTE: For information on how to configure the default export to file settings refer to the 'Configuring default scheduling options' section in this manual.

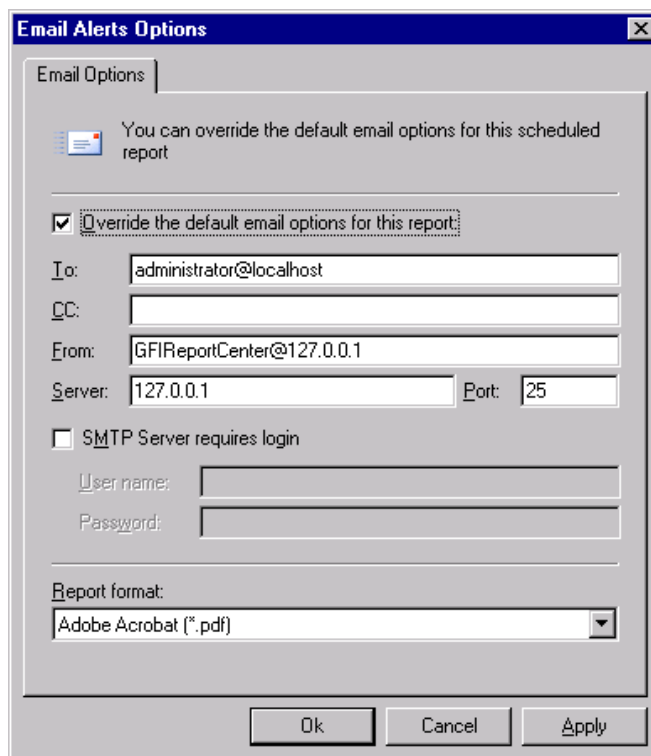
Configuring report emailing options

To configure the report emailing options of a scheduled report do as follows:



Screenshot 31 - Advanced Settings dialog: Send by email settings button

1. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the 'Send by email' option.

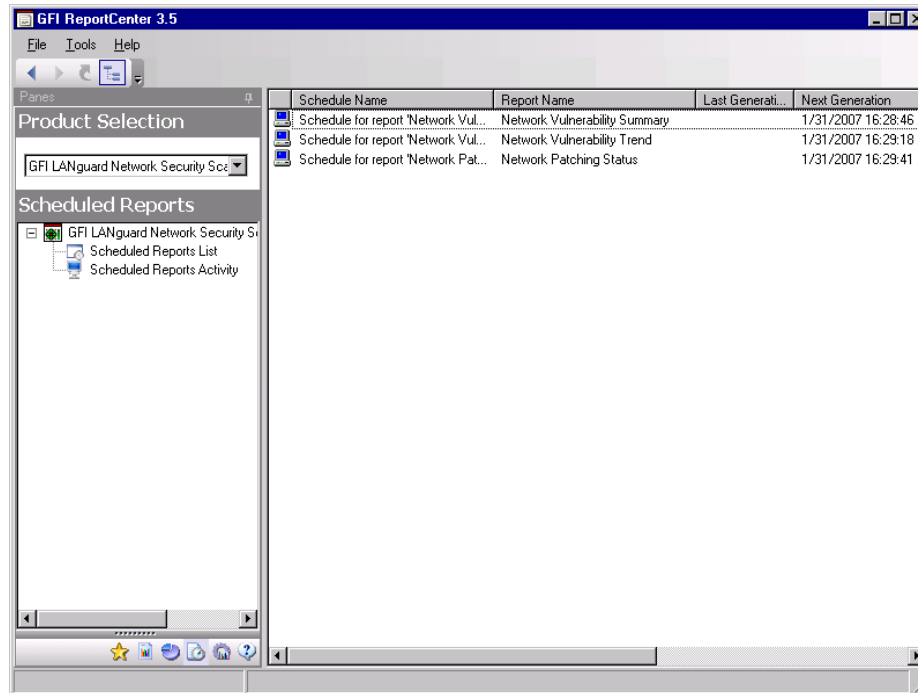


Screenshot 32 - Report distribution options

2. Select the option 'Override the default email options for this report:'
3. Specify the following parameters:
 - **To/CC:** Specify the email address(es) where the generated report will be sent.
 - **From:** Specify the email account that will be used to send the report.

- **Server:** Specify the name/IP of your SMTP (outbound) email server. If the specified server requires authentication, select the option 'SMTP Server requires login' and specify the logon credentials in the 'User name' and 'Password' fields.
 - **Report format:** Reports are sent via email as attachments. Select the file format in which to send out your report.
4. Click **OK** to finalize your configuration settings.

Viewing the list of scheduled reports

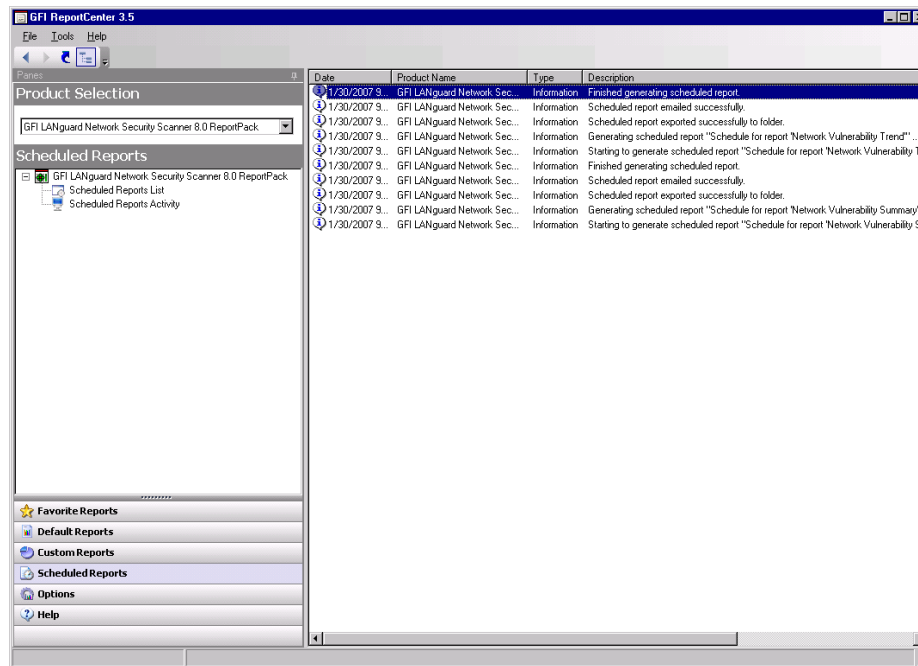


Screenshot 33 - List of Scheduled reports

Click on the **Scheduled Reports** navigation button to show the list of scheduled reports which are currently configured for automatic generation. This information is displayed in the right pane of the management console and includes the following details:

- **Schedule Name:** The custom name that was specified during the creation of the new scheduled report.
- **Report Name:** The names of the default or custom report(s) that will be generate.
- **Last Generation:** Indicates the date/time when the report was last generated.
- **Next Generation:** Indicate the date/time when the report is to be next generated.
- **Description:** The description that you have entered for each schedule.

Viewing the scheduled reports activity





Screenshot 34 - Schedule activity monitor


GFI ReportCenter also includes a schedule activity monitor through which you can view events related to all scheduled reports that have been executed.

To open the schedule activity monitor, click on the **Scheduled Reports** navigation button and select the **Scheduled Reports Activity** node. This will bring up the activity information in the right pane of the GFI ReportCenter management console.

The activity monitor displays the following events:

 - **Information:** The scheduled report was successfully executed and sent by email and/or saved to disk.

 - **Warning:** The scheduled report was not executed because product license is invalid or has expired.

 - **Error:** The scheduled report was not executed due to a particular condition/event. Typical conditions include:

- Errors when attempting to save the generated report to a specific folder (for example, out of disk space).
- Errors when attempting to send the generated report via email (for example, the SMTP server configured in the GFI ReportCenter settings is not reachable).

The activity monitor records and enumerates the following information:

- **Date:** The date and time when the scheduled report was executed.
- **Product name:** The name of the GFI product to which the report belongs.
- **Type:** The event classification - error, information, or warning.
- **Description:** Information related to the state of a scheduled report that has been executed. The format and contents of the activity description vary, depending on the event type.

NOTE: The description is often the most useful piece of information, indicating what happened during the execution of a scheduled report or the significance of the event.

Enable/disable a scheduled report

Scheduled reports can be enabled or disabled as required. Use the **Scheduled Reports** navigation button to view the list of scheduled reports as well as to identify their current status. The status of scheduled reports is shown through the icon included on the left hand side of each schedule:



- Indicates that the scheduled report is disabled.



- Indicates that the scheduled report is enabled/pending.

To enable or disable a scheduled report, right-click on the respective report and select **Enable/Disable** accordingly.

Editing a scheduled report

To make changes to the configuration settings of a scheduled report:

1. Click on the **Scheduled Reports** navigation button.
2. Right-click on the scheduled report to be re-configured and select **Properties**. This will bring up the 'Scheduled Reports Wizard'.



Screenshot 35 - Scheduled Reports wizard

3. Click on **Next** and perform the required changes. For information on how to configure the parameters of a scheduled report refer to the 'Creating a scheduled report' section in this chapter.

Deleting a scheduled report

To delete a scheduled report:

1. Click on the **Scheduled Reports** navigation button.
2. Right-click on the scheduled report to be permanently removed from the list and select **Delete**.

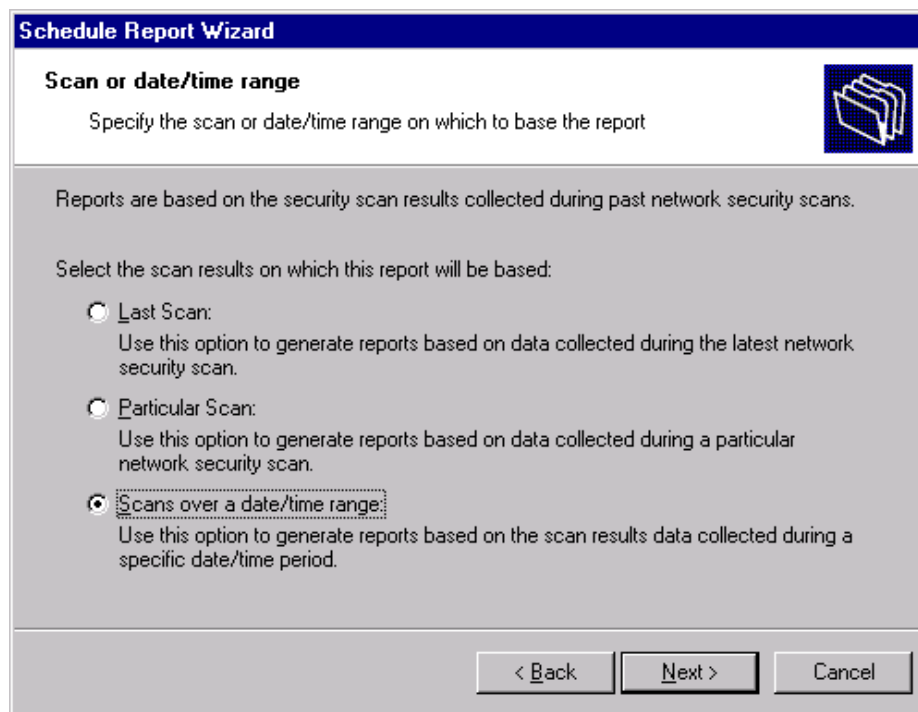
Example: Scheduling a report

This example demonstrates how to schedule a network vulnerability summary report which will:

- Generate the first report on 02/01/2007 at 20:00.
- Continue generating the same report on a monthly basis.
- Export the generated report(s) to folder 'C:\Monthly Reports' in PDF format.
- Email the generated report using the following custom parameters:
 - Send from email account: 'RC_Admin@gfi.com'
 - Send to email account: 'IT_manager@gfi.com'
 - SMTP server details: '120.11.120.11'.

To create the scheduled report:

1. Click on the **Default Reports** navigation button.
2. Right-click on 'Network Vulnerability Summary' and select **New ► Scheduled Report**. As soon as the welcome dialog is displayed click **Next**.



Screenshot 36 - Select network security scan(s) data

3. Select the option '**Scans over a date/time range**' for data to be covered by this report and click **Next**.

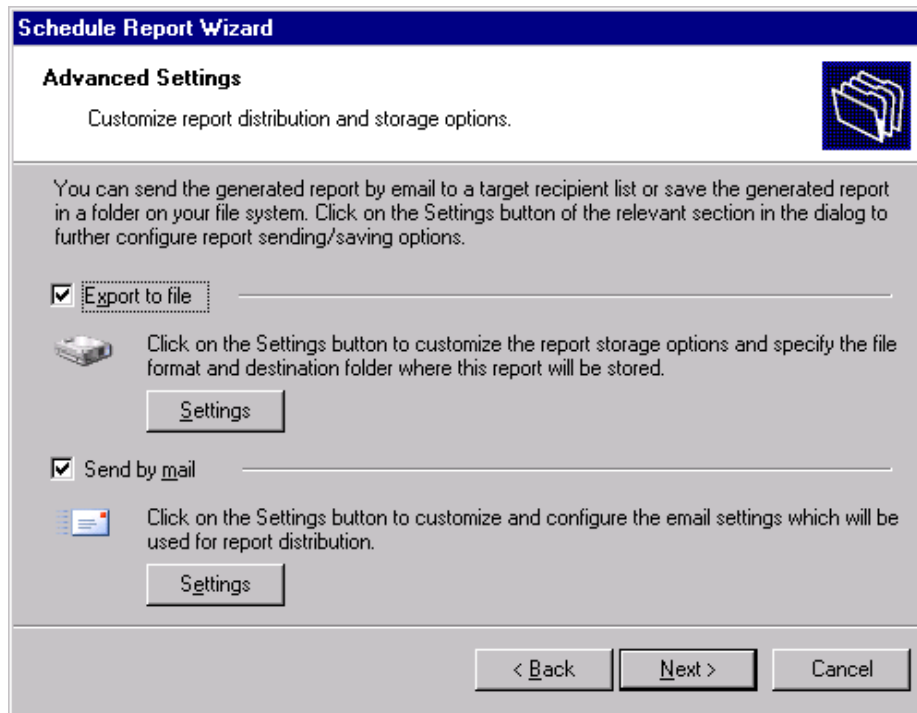
Screenshot 37 - Select date/time of network scan

4. Select the option **'Relative'** and from the provided drop down list select **'Last month'**. Click on **Next** to proceed to the next dialog.

Screenshot 38 – Specifying the scheduling options

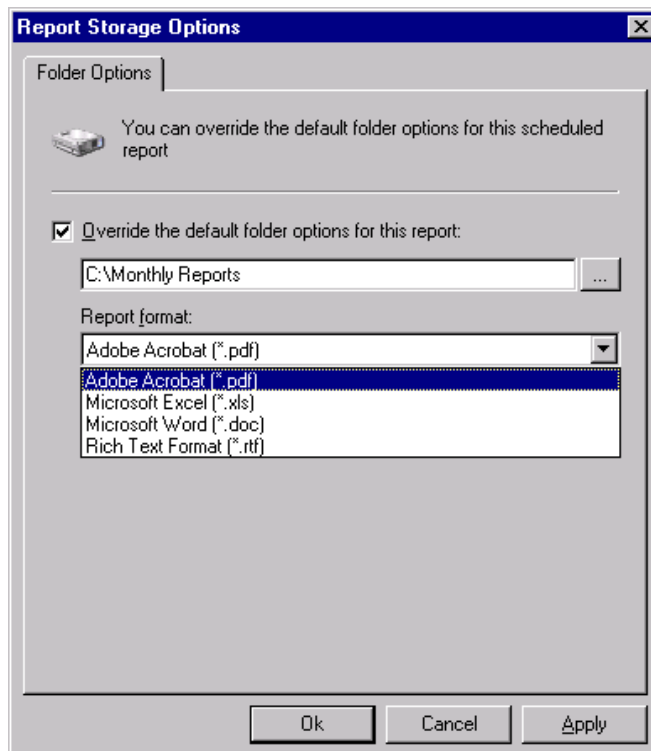
5. To generate this report on a monthly basis, select the option **'Generate this report every:'** and set the interval to **'30 Days'**.

6. Set the start date to **'02/01/2007'** and time to **'20:00'**. Click **Next** to continue.



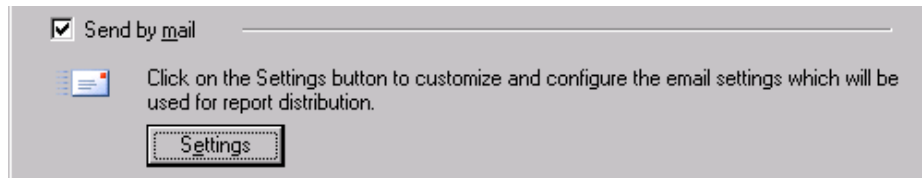
Screenshot 39 - Advanced Settings dialog

7. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the 'Export to file' option.



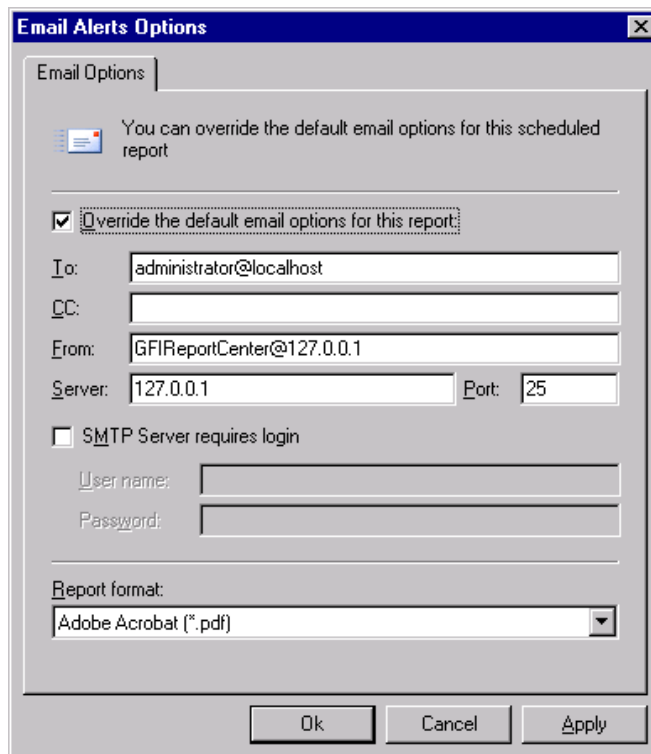
Screenshot 40 - Advanced Settings: Export to file options

8. Select the option 'Override the default folder options for this report:'
9. Specify the complete path where this report will be saved i.e. 'C:\Monthly Reports'.
10. From the report format drop down select 'PDF' and click **OK**.



Screenshot 41 - Advanced Settings dialog: Send by email settings button

11. From the 'Advanced Settings' dialog, click on the **Settings** button underneath the 'Send by email' option.



Screenshot 42 - Report distribution options

12. Select the option 'Override the default email options for this report:'

13. Specify the following parameters:

- **To:** 'RC_Admin@gfi.com'
- **From:** 'IT_manager@gfi.com'
- **Server:** '120.11.120.11'.

14. From the report format drop down select 'PDF' and click **OK** to finalize your email settings.

The screenshot shows a dialog box titled "Schedule Report Wizard" with a blue header bar. Below the header, the section is titled "Name and Description" and includes a folder icon. The instruction reads: "Specify the name and description for this custom report". A paragraph explains: "The name, title and description of a custom report will be used to uniquely identify the report through the set of custom reports. The custom report name must be unique." There are three input fields: "Report name:" with the text "Monthly network vulnerability summary report", "Report Title:" with the same text, and "Report description:" with a text area containing "This report is generated on a monthly basis. It shows a summary of network vulnerabilities on scan carried out during the previous month." A checkbox labeled "Show Cover Page" is checked. At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a dashed border), and "Cancel".

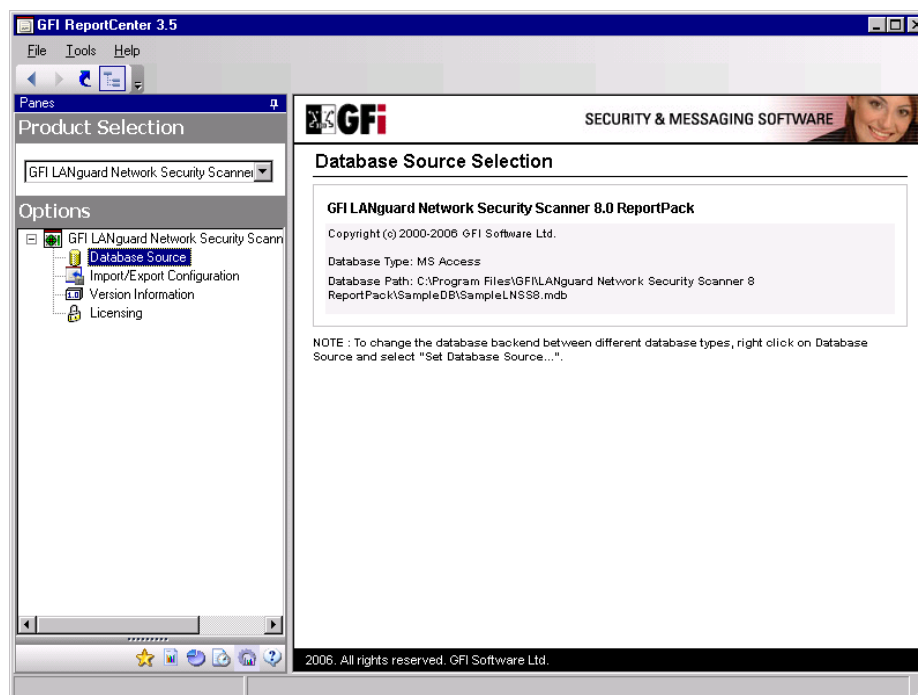
Screenshot 40 – Custom report name and description

15. Click **Next** and specify the following parameters:
 - **Report Name:** *'Monthly network vulnerability summary report'*
 - **Report Title:** *'Monthly network vulnerability summary report'*
 - **Report Description:** This report is generated on a monthly basis. It shows a summary of network vulnerabilities on scans carried out during the previous month.
16. Click **Next** to proceed to the final dialog.
17. Click **Finish** to finalize your custom report configuration settings.

Configuring default options

Introduction

The GFI LANguard N.S.S. ReportPack allows you to configure a default set of parameters which can be used when generating reports. These parameters are first set during installation. However, you can still reconfigure any of these parameters via the **Options** navigation button and the **Tools** menu provided in the GFI ReportCenter management console.



Screenshot 43 - Options navigation button and Tools menu

Through the **Options** navigation button you can configure the following parameter:

- **Database source:** Use this node to specify the database backend from where the ReportPack will extract the required reporting data.

Through the **Tools** menu you can configure the following parameters:

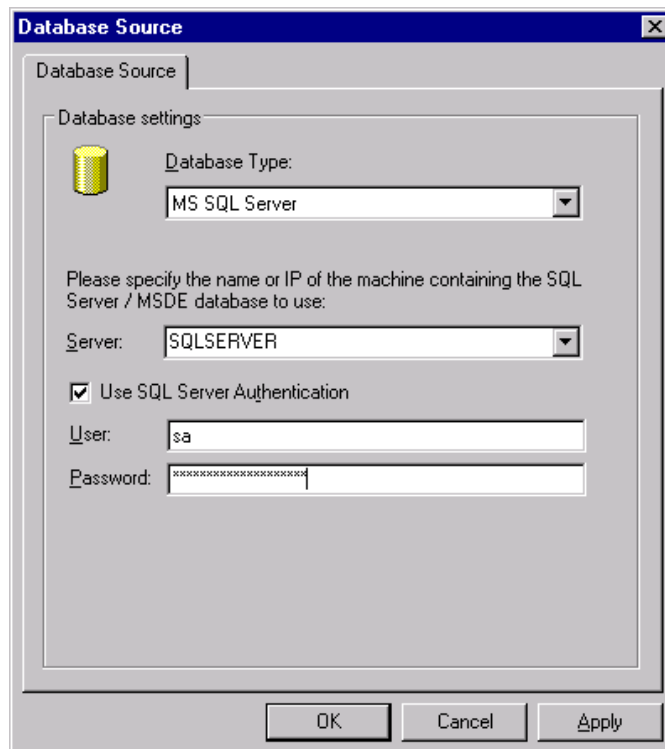
- **Default scheduling settings:** Use this menu option to configure the default export to file parameters and report emailing parameters of scheduled reports.

You can also backup your configuration settings for the ReportPack through the **Import/Export Configuration** node in the **Options** section. Exported configurations may be imported into a separate GFI ReportCenter instance, provided that the same ReportPacks are installed on both instances.

Configuring database source: Microsoft SQL Server

To configure MS SQL Server your database source:

1. Click on the **Options** navigation button.
2. Right-click on the **Database Source** node and select **Set Database Source...** This will bring up the database source configuration dialog.



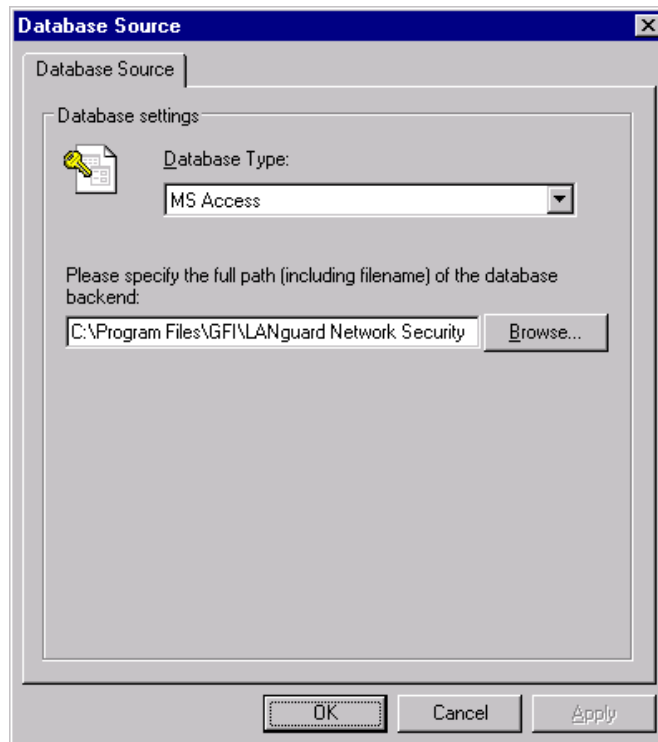
Screenshot 44 - Database source configuration dialog: SQL Server

3. Select 'MS SQL Server' as the database type from the provided list of supported databases.
 4. Specify the name or IP address of your MSDE/MS SQL Server database backend.
 5. To use the credentials of an SQL Server account, select the 'Use SQL Server authentication' option and specify the user name and password in the provided fields.
- NOTE:** By default, the GFI LANguard N.S.S. ReportPack uses Windows logon credentials to authenticate to the SQL Server.
6. Click on **OK** to finalize your configuration settings.

Configuring database source: Microsoft Access

To configure Microsoft Access as your database source:

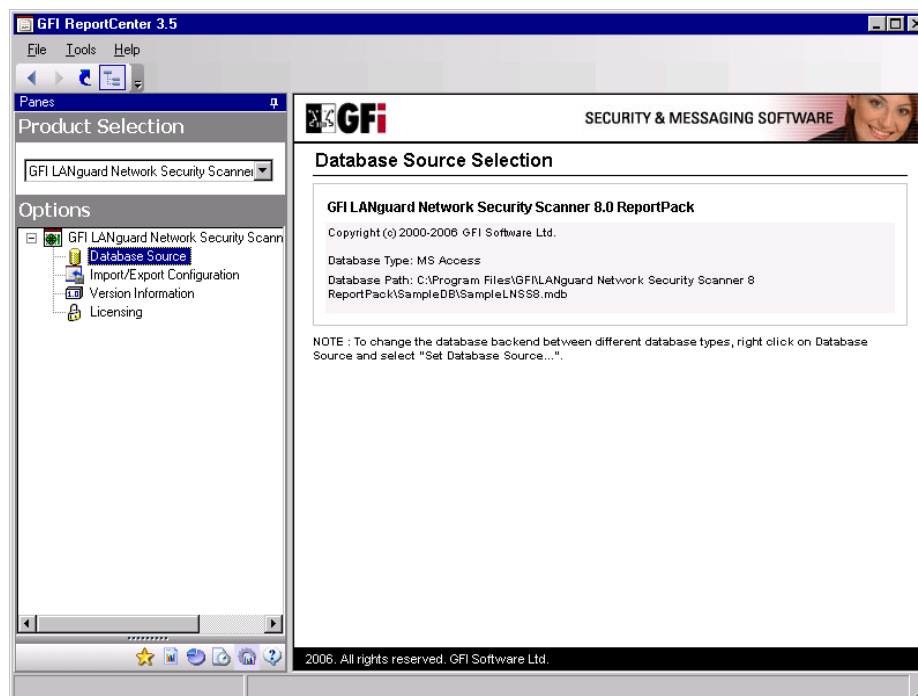
1. Click on the **Options** navigation button.
2. Right-click on the **Database Source** node and select **Set Database Source...** This will bring up the database source configuration dialog.



Screenshot 45 - Database source configuration dialog: MS Access

3. Select 'MS Access' as the database type from the provided list of supported databases.
4. Specify the complete path to the database backend. If the database source is not stored locally, specify the complete path using Universal Naming Convention (UNC).
(e.g., `\\Security_Server\Program Files\GFI\LANguard Network Security Scanner 8.0\Data\scanresults.mdb`).
5. Click on **OK** to finalize your configuration settings.

Viewing the current database source settings

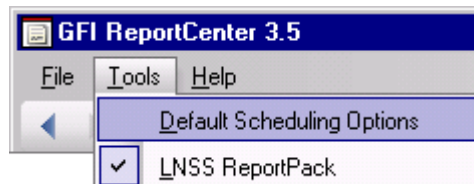


Screenshot 46 - Database source configuration settings

After configuration, you can view the current database source settings by clicking on the **Database Source** node.

Configuring default scheduling settings

To configure the default settings to be used by scheduled reports:



Screenshot 47 - Default scheduling options node

1. From the pull-down menu, click on the **Tools ► Default Scheduling Options**.
2. Configure the required parameter as described in the 'Configuring Advanced Settings' section of the Scheduling Reports chapter.

Importing/Exporting the configuration



Screenshot 48 – Import/Export Configuration node

The GFI ReportCenter allows you to backup your configuration settings for the ReportCenter and all ReportPacks through **Import/Export Configuration...** in the **File** pull-down menu. Settings are exported for:

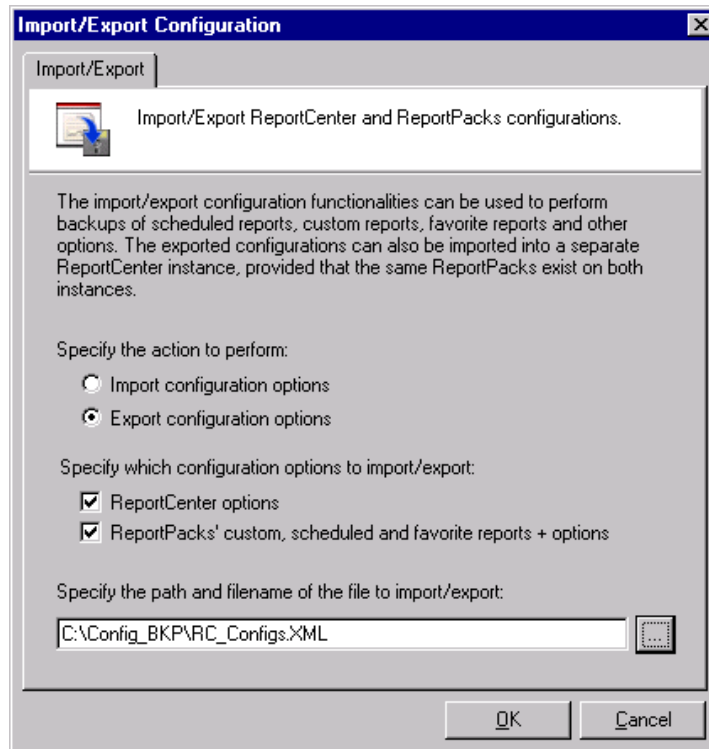
- Default scheduling options
- Custom reports
- Scheduled reports
- Favorite reports.

The configuration is backed up into an XML file which may be imported into a separate GFI ReportCenter instance, provided that the same ReportPacks are installed on both instances.

You can also import/export the configuration for a particular ReportPack through the **Import/Export Configuration** node in the **Options** section of the ReportPack.

Exporting the configuration

To export the GFI LANguard N.S.S. configuration:



Screenshot 49 – Import/Export configuration dialog

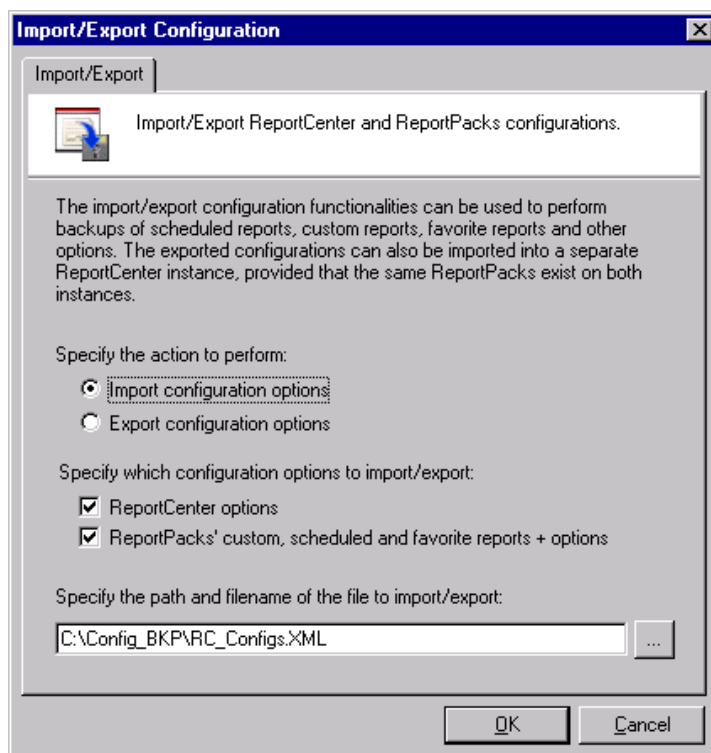
1. From the pull-down menu, click on the **File ▶ Import/Export Configuration...** . This will bring up the configuration dialog.
2. Select the option '**Export configurations options**'.
3. Specify which configuration options to export.
4. Specify the path and filename of the XML file to export. Click on **OK** to proceed with the export.



Screenshot 50 – Export configuration success

Importing the configuration

To import the GFI LANguard N.S.S. configuration:



Screenshot 51 – Import configurations dialog

1. From the pull-down menu, click on the **File ► Import/Export Configuration...** . This will bring up the configuration dialog.
2. Select the option '**Import configurations options**'.
3. Specify which configuration options to import.
4. Specify the path and filename of the XML file to import. Click on **OK** to proceed with the import.



Screenshot 52 – Import configuration success

5. Close and restart GFI ReportCenter to activate the imported items.

General options

Entering your license key after installation

If you have purchased a ReportPack, enter your license key using the **Options ▶ Licensing** node (no re-installation/re-configuration required)

NOTE 1: You must purchase a different license key for every product ReportPack to be installed and accessed through the GFI ReportCenter framework.

For example, to install both the GFI Network Security Scanner 8.0 ReportPack and the GFI EventsManager 7.0 ReportPack, you must purchase 2 separate license keys, one for each product ReportPack.

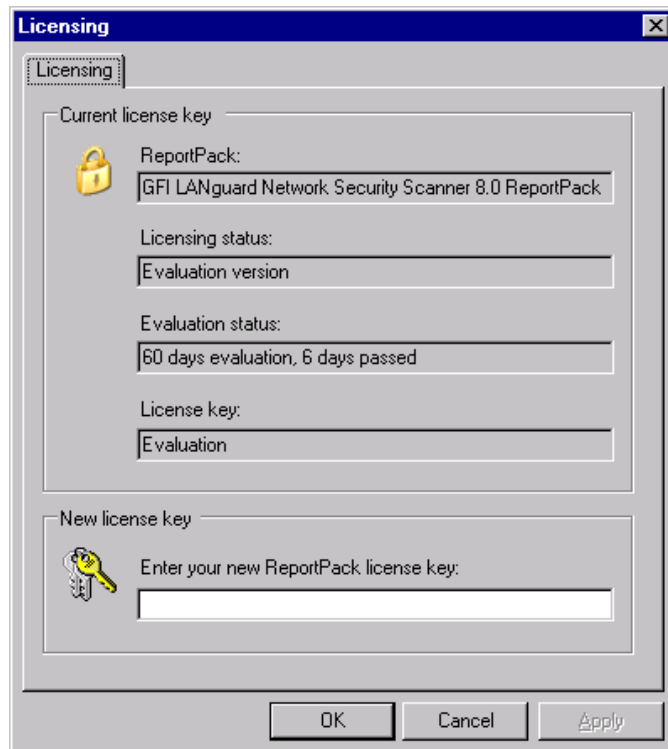
NOTE 2: Entering the license key should not be confused with the process of registering your company details on our website. This is important since it allows us to give you support and notify you of important product news. You may register and obtain your GFI customer account from: <http://www.gfi.com/pages/regfrm.htm>.

To input your product ReportPack license key:



Screenshot 53 – Product Selection drop down list

1. Select the respective product (e.g. 'GFI LANguard N.S.S. 8.0') from the **Product Selection** drop down list.
2. Click on the **Options** navigation button.
3. Right-click on the **Licensing** node and select **Set Licensing...** This will bring up the 'Licensing' dialog.



Screenshot 54 - Licensing dialog

4. Type in the ReportPack license key.
5. Click on **OK** to finalize your entry.

Viewing the current licensing details

To view your current licensing details, click on the **Options** navigation button and select the **Licensing** node. The licensing details will be displayed in the right pane of the management console.

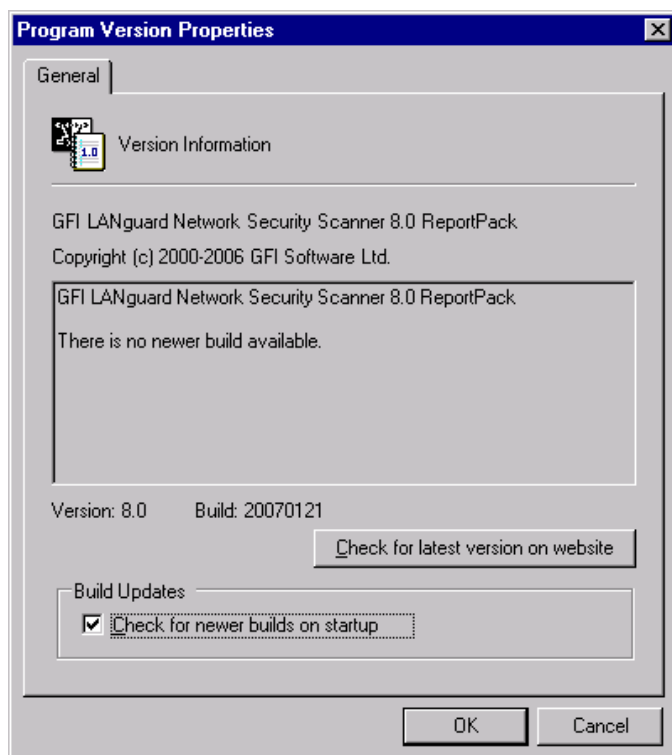
Viewing the product ReportPack version details

To view the version information of your product ReportPacks:

1. Select the product ReportPack from the **Product Selection** drop down list.
2. Click on the **Options** navigation button and select the **Version Information** node. The version details will be displayed in the right pane of the management console.

Checking the web for newer builds

Periodically GFI releases product and ReportPack updates which can be automatically downloaded from the GFI website. To check if a newer built is available for download:



Screenshot 55 - Version Properties: Check for newer builds dialog

1. Select the respective product (for example, GFI LANguard N.S.S. 8.0 Reports) from the **Product Selection** drop down list.
2. Click on the **Options** navigation button.
3. Right-click on the **Version Information** node and select **Checking for newer builds...**

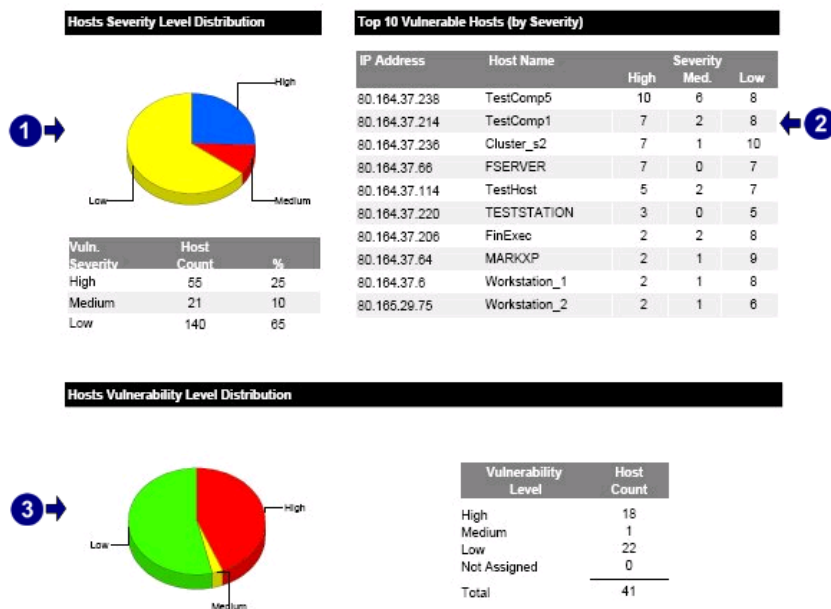
NOTE: GFI LANguard Network Security Scanner 8.0 ReportPack is configured by default to check for newer builds on startup.

Appendix: GFI LANguard Network Security Scanner default reports

Vulnerabilities scanning reports

Network vulnerability summary

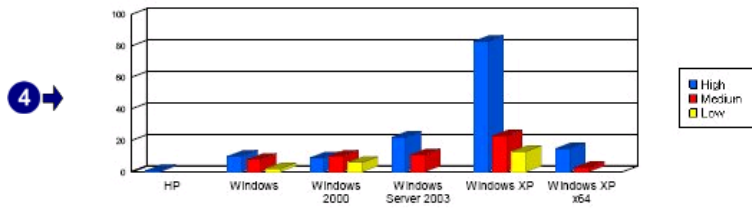
Scan reference : 192.168.100.2-192.168.100.254
 Scan date & time : 29-Nov-2006 10:12



Screenshot 56 – Sample report showing network vulnerability summary

1	Chart displaying vulnerability severity distributions
2	List showing the top 10 most vulnerable host machines ordered by severity
3	Chart displaying vulnerability level distributions across host machines on the network

Vulnerability Count by OS Distribution

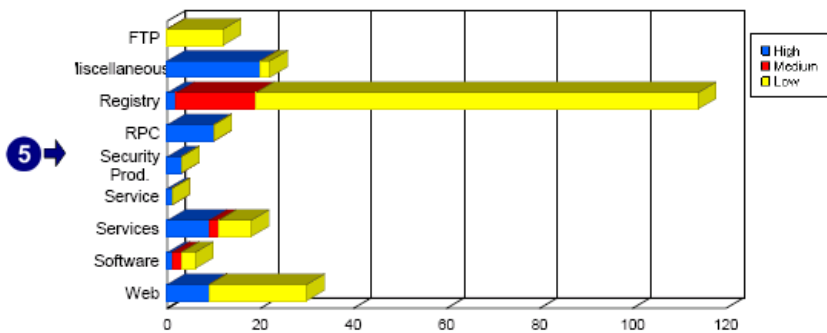


Operating System	Total	Severity Distribution		
		High	Med.	Low
HP	1	0	0	1
Windows	20	8	2	10
Windows 2000	25	10	6	9
Windows Server 2003	33	11	0	22
Windows XP	119	23	13	83
Windows XP x64	18	3	0	15

Screenshot 57 – Sample report showing network vulnerability summary

4 Chart displaying the vulnerability distribution for each operating system on the network

Vulnerability Distribution (by Category)

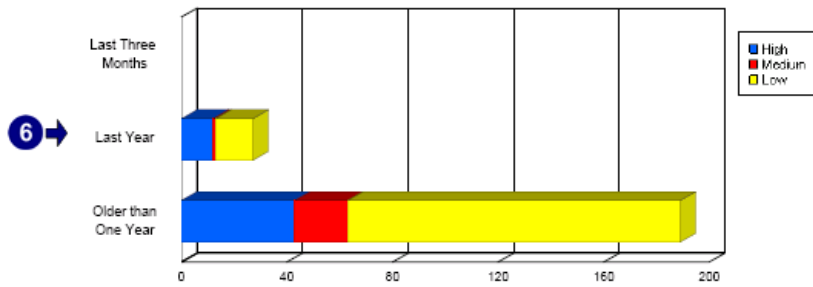


Vulnerability Category	Total	Severity Distribution		
		High	Med.	Low
FTP	12	0	0	12
Miscellaneous	22	20	0	2
Registry	114	2	17	95
RPC	10	10	0	0
Security Prod.	3	3	0	0
Service	1	1	0	0
Services	18	9	2	7
Software	6	1	2	3
Web	30	9	0	21

Screenshot 58 – Sample report showing network vulnerability summary

5 Chart displaying vulnerability categories and their distribution

Vulnerability Distribution (by Timestamp)



Vulnerability Category	Severity Distribution			
	Total	High	Med.	Low
Last Three Months	0	0	0	0
Last Year	27	12	1	14
Older than One Year	189	43	20	126

Screenshot 59 – Sample report showing network vulnerability summary

6 Chart displaying the vulnerability distribution over time

Top 10 Most Common Vulnerabilities

Vulnerability : AutoShareWKS						
Product	Timestamp	References	Type	Severity	Count	
Unknown	2002-01-01	Unknown	Registry	Low	19	
Vulnerability : Cached Logon Credentials						
Unknown	2002-01-01	Unknown	Registry	Low	19	
Vulnerability : AutoShareServer						
Unknown	2002-01-01	Unknown	Registry	Low	18	
Vulnerability : DCOM is enabled						
Unknown	1999-06-07	CVE-1999-0658	Registry	Low	18	
Vulnerability : Last logged-on username visible						
Unknown	2002-01-01	Unknown	Registry	Low	18	
Vulnerability : LM Hash						
Unknown	2002-01-01	Unknown	Registry	Medium	13	
Vulnerability : FTP anonymous access allowed						
Unknown	Unknown	Unknown	FTP	Low	11	
Vulnerability : OVAL:999: Hyperlink Object Buffer Overflow Vulnerability						
Unknown	2006-08-11	CVE-2006-3088	Services	High	8	
Vulnerability : Netscape: Netscape PageServices						
Unknown	1999-09-11	CVE-1999-0269	Web	Low	8	
Vulnerability : OVAL:894: Server 2003 RPCSS DCOM Buffer Overflow						
Unknown	2004-04-20	CVE-2003-0813	RPC	High	8	

Top 10 Most Vulnerable Products

Products	Severity Distribution			
	Total	High	Med.	Low
Product 2	34	11	2	21
Product3	22	5	1	16
Product1	18	3	1	14

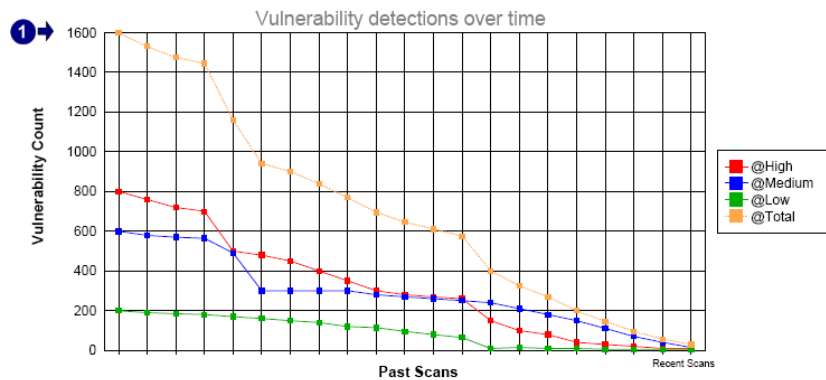
Screenshot 60 – Sample report showing network vulnerability summary

7	Chart displaying the 10 most common vulnerabilities
8	Chart displaying the 10 most vulnerable products

Use this report to:

- Display vulnerability counts for different categories
- Identify the 10 most vulnerable host machines
- Identify the 10 most vulnerable products
- Identify the 10 most common vulnerabilities.

Network vulnerability trend



This trend report was generated from data in the following scans :

2 →

Scan Date & Time	Scan Profile	Scan target reference
1/2/2007 11:00:00AM	Default	80.134.200.10 - 80.134.200.157
1/3/2007 11:23:00AM	Default	80.134.200.10 - 80.134.200.157
1/4/2007 1:05:00PM	Default	80.134.200.10 - 80.134.200.157
1/5/2007 5:00:23PM	Default	80.134.200.10 - 80.134.200.157
1/6/2007 3:21:42PM	Default	80.134.200.10 - 80.134.200.157
1/7/2007 10:43:30AM	Default	80.134.200.10 - 80.134.200.157
1/8/2007 11:31:22AM	Default	80.134.200.10 - 80.134.200.157
1/9/2007 6:31:10PM	Default	80.134.200.10 - 80.134.200.157
1/10/2007 1:34:52PM	Default	80.134.200.10 - 80.134.200.157
1/11/2007 4:43:44PM	Default	80.134.200.10 - 80.134.200.157
1/12/2007 11:43:40AM	Default	80.134.200.10 - 80.134.200.157
1/13/2007 11:10:21AM	Default	80.134.200.10 - 80.134.200.157
1/14/2007 11:00:40AM	Default	80.134.200.10 - 80.134.200.157
1/15/2007 10:43:43AM	Default	80.134.200.10 - 80.134.200.157
1/16/2007 10:20:17AM	Default	80.134.200.10 - 80.134.200.157
1/17/2007 10:31:59AM	Default	80.134.200.10 - 80.134.200.157
1/18/2007 12:40:58PM	Default	80.134.200.10 - 80.134.200.157
1/19/2007 6:23:25PM	Default	80.134.200.10 - 80.134.200.157
1/20/2007 2:23:49PM	Default	80.134.200.10 - 80.134.200.157
1/21/2007 11:50:53AM	Default	80.134.200.10 - 80.134.200.157
1/22/2007 10:32:47AM	Default	80.134.200.10 - 80.134.200.157

Screenshot 61 – Sample report showing network vulnerability trend

1	Chart displaying past scans and vulnerability totals for each scan
2	List of past scans and respective scan profiles

Use this report to:

- Graphically illustrate how the number of vulnerabilities on the network has changed over a given time span.

Vulnerability distribution by host

Scan reference : 192.168.100.2-192.168.100.254
 Scan date & time: 29-Nov-2006 9:51

IP / Hostname	Severity Distribution			Vulnerability Categories													
	Total	Low	Med	High	CGI	FTP	Mail	Misc	Reg	Services	DNS	RPC	Bkdoor	S.Prod.	Applic.	USB	Network
192.168.100.11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.12 BOGDAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.13 STELI	6	5	0	1	0	0	0	0	5	0	0	1	0	0	0	0	0
192.168.100.14 SORIN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.15 CRISTI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.16 BOGDY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.17 BOBBY	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.19 NSM_XP264	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.20 CALDEV	8	5	1	2	0	0	0	0	6	0	0	0	0	1	0	0	0
192.168.100.23 MASTERSERV	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
192.168.100.24 HORI	6	5	0	1	0	0	0	0	5	0	0	1	0	0	0	0	0
192.168.100.26 CB	2	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.28 CB1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.29 MIHAI	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.100.30 MASTER	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
192.168.100.31 NSM2K3STD	8	7	0	1	0	0	0	0	6	0	0	1	0	0	0	0	0

① ② ③

Screenshot 62 – Sample report showing vulnerability distribution by host

1	List of IP addresses and host names on which vulnerabilities were detected
2	The number of low, medium and high severity vulnerabilities detected on each host
3	The number of vulnerabilities detected on each host distributed by vulnerability category

Use this report to:

- Generate statistics showing vulnerability counts for each host machine.

Vulnerability distribution by operating system

Scan reference : 192.168.100.2-192.168.100.254
 Scan date & time: 29-Nov-2006 10:12

Operating System/ SP	Total	Severity Distribution			Vulnerability Categories													
		Low	Med	High	CGI	FTP	Mail	Misc.	Reg.	Services	DNS	RPC	Ekdoor	S.Prod.	Applic.	USB	Network	
D-Link DWL-2100AP (2100AP SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
HP SP: None	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Unknown SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows SP: None	20	10	2	8	2	3	0	0	6	1	0	1	0	0	0	0	0	0
Windows2000 SP: 4	24	8	6	10	4	1	0	0	9	0	0	1	0	0	0	0	0	0
Windows2000 SP: None	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows9X/XP SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
WindowsNT SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Windows Server2003 SP: Gold	14	7	0	7	2	0	0	0	5	0	0	1	0	0	0	0	0	0
Windows Server2003 SP: 1	17	13	0	4	1	0	0	0	11	0	0	2	0	0	0	0	0	0
Windows Server2003 SP: None	2	2	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0
WindowsXP SP: None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
WindowsXP SP: 1	18	10	1	7	4	1	0	0	6	0	0	1	0	0	0	0	0	0
WindowsXP SP: Gold	14	7	2	5	0	0	0	0	6	0	0	1	0	0	0	0	0	0
WindowsXP SP: 2	87	66	10	11	15	6	0	0	56	0	0	0	0	3	0	0	0	0

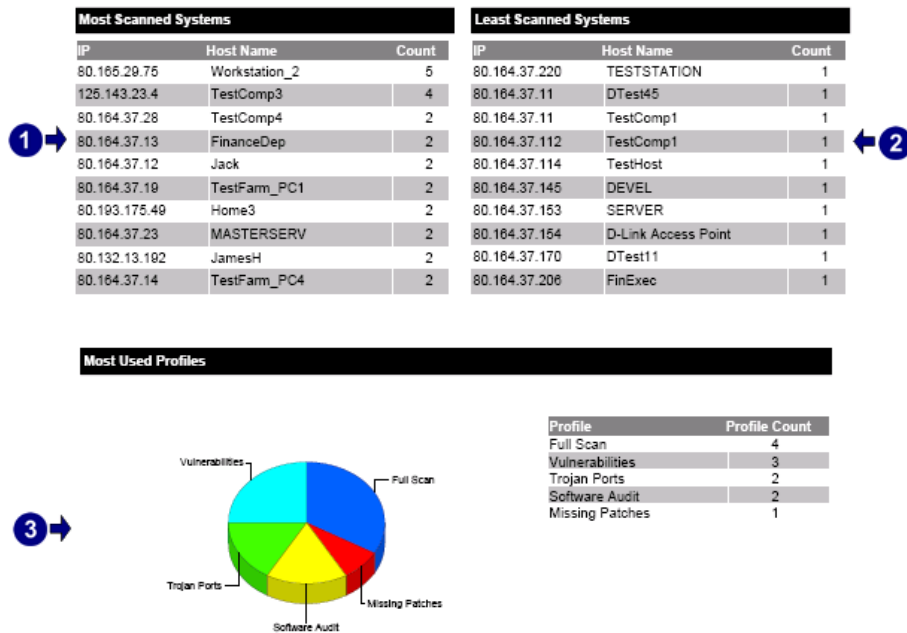
Screenshot 63 – Sample report showing vulnerability distribution by operating system

1	List of operating systems and service packs affected by one or more vulnerabilities
2	The number of low, medium and high severity vulnerabilities detected on each operating system
3	The number of vulnerabilities detected on each operating system distributed by vulnerability category

Use this report to:

- Generate statistics showing vulnerability counts for each operating system.

Security scans history



Screenshot 64 – Sample report showing security scans history

1	List showing the host machines with the highest number of scans and the respective scan count
2	List showing the host machines with the lowest number of scans and the respective scan count
3	Chart displaying scan profile usage

Last Scan for Each System		
IP	Host Name	Last Scan Date
192.168.100.6	N/A	11/29/2006 9:51:53AM
192.168.100.11	N/A	11/29/2006 9:51:53AM
192.168.100.49	N/A	11/29/2006 10:11:19AM
192.168.100.15	CRISTI	11/29/2006 10:12:25AM
192.168.100.220	TESTSTATION	11/29/2006 10:12:25AM
192.168.100.214	N/A	11/29/2006 10:12:25AM
192.168.100.211	ZVIRTUAL2	11/29/2006 10:12:25AM
192.168.100.206	V206A	11/29/2006 10:12:25AM
192.168.100.20	CALDEV	11/29/2006 10:12:25AM
192.168.100.19	NSM_XPB64	11/29/2006 10:12:25AM
192.168.100.170	BOGVXP	11/29/2006 10:12:25AM
192.168.100.17	BOBBY	11/29/2006 10:12:25AM
192.168.100.16	BOGDY	11/29/2006 10:12:25AM
192.168.100.153	SERVER	11/29/2006 10:12:25AM

Scans Listing			
Start Date/Time	Target	Profile	Ended
11/28/2006 3:37:44PM	127.0.0.1	Default	Yes
11/28/2006 3:42:33PM	file:list.txt	Default	No
11/28/2006 3:43:10PM	file:list.txt	Default	No
11/28/2006 3:47:54PM	file:list.txt	Default	Yes
11/29/2006 9:10:02AM	10"{{zrδ	Default	Yes
11/29/2006 9:51:53AM	192.168.100.2-192.168.100.254	Default	Yes
11/29/2006 10:10:00AM	10"{{zrδ	Default	Yes
11/29/2006 10:11:19AM	192.168.100.2-192.168.100.254	Default	No
11/29/2006 10:12:25AM	192.168.100.2-192.168.100.254	Default	Yes

Screenshot 65 – Sample report showing security scans history

4	List showing date and time of the last scan performed on each host
5	List showing all scans performed

Use this report to:

- Display information and statistics on all network security scans performed.

Vulnerability listing by category

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

CATEGORY: FTP

1 → Vulnerability: FTP anonymous access allowed—
 Product: N/A
 Severity: Low
 Timestamp: N/A

2 →

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.17	BOGVXP	Windows XP	2
192.168.100.21	ZVIRTUAL2	Windows XP	2
192.168.100.21		Windows	
192.168.100.23	MASTERSERV	Windows	
192.168.100.23	MG1	Windows XP	2
192.168.100.23	MG4	Windows XP	1
192.168.100.23	CB3	Windows 2000	4
192.168.100.24	XPDELPHI2005	Windows XP	2
192.168.100.30	MASTER	HP	
192.168.100.49	STEFAN	Windows	
192.168.100.6	LUCIANP	Windows XP	2
192.168.100.64	MARKXP	Windows XP	2

CATEGORY: Information

Vulnerability: A modem is installed on this computer—
 Product: N/A
 Severity: N/A
 Timestamp: 2002-01-01

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.17	BOGVXP	Windows XP	2

Screenshot 66 – Sample report showing vulnerability listing by category

1	Vulnerability details including name, description and severity
2	List of host machines affected by each vulnerability detected

Use this report to:

- List detected vulnerabilities grouped by category, and the host machines affected by each vulnerability.

Vulnerability listing by host

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM



Screenshot 67 – Sample report showing vulnerability listing by host

1	Host machine details on which vulnerabilities were detected
2	Vulnerability count for each host, also shown as a percentage of total vulnerabilities detected on the network
3	List of vulnerability details for each host, including name, description and severity
4	Chart displaying percentage of vulnerabilities detected on each host compared to total vulnerabilities detected on the network

Use this report to:

- List the vulnerabilities detected for each host machine on the network.

Vulnerability listing by product

Scan reference: 192.168.100.2-192.168.100.254

Scan date & time: 11/29/2006 10:12:25AM

1 → PRODUCT: N/A

Vulnerability: A connection could be opened using account Administrator without password —

2 →

Category: Service

Severity: High

Timestamp: N/A

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.49	STEFAN	Windows	

Vulnerability: A modem is installed on this computer —

Category: Information

Severity: N/A

Timestamp: 2002-01-01

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.170	BOGVXP	Windows XP	2

Vulnerability: Administrator account exists —

Category: Information

Severity: N/A

Timestamp: N/A

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.6	LUCIANP	Windows XP	2
192.168.100.206	V206A	Windows XP	2
192.168.100.31	NSM2K3STD	Windows Server 2003	1
192.168.100.247	VXPDELPHI2005	Windows XP	2
192.168.100.21	EVIRTUAL2	Windows XP	2
192.168.100.64	MARKXP	Windows XP	2
192.168.100.238	CB3	Windows 2000	4
192.168.100.238	MG4	Windows XP	1
192.168.100.232	MG1	Windows XP	2
192.168.100.13	STELI	Windows XP x64	1
192.168.100.66	FSERVER	Windows Server 2003	Gold
192.168.100.220	TESTSTATION	Windows Server 2003	1
192.168.100.170	BOGVXP	Windows XP	2
192.168.100.76	MARK-TESTING	Windows XP x64	1
192.168.100.75	MARK	Windows XP	2
192.168.100.24	HORI	Windows XP x64	1
192.168.100.114	VSORIN-D2005	Windows XP	Gold
192.168.100.20	CALDEV	Windows XP	2

3 →

Name: User ASPNET never logged on
 Description: It is recommended to remove this account if not used
 Product:

Screenshot 68 – Sample report showing vulnerability listing by product

1	Name of product for which vulnerabilities were detected
2	Vulnerability details for each product, including name, description and severity
3	List of host machines affected by each product vulnerability detected

Use this report to:

- List detected vulnerabilities grouped by product, and the host machines affected by each vulnerability.

Vulnerability listing by severity

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

1 SEVERITY : High

Vulnerability: A connection could be opened using account Administrator without password —

2 → **Category:** Service
Product: N/A
Timestamp: N/A

Affected Hosts:

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.49	STEFAN	Windows	

Vulnerability: Application not up to date: Ad-Aware SE Personal Edition —

Category: Security Products
Product: N/A
Timestamp: N/A

Affected Hosts:

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.20	CALDEV	Windows XP	2

Vulnerability: Application not up to date: F-Prot Antivirus for Windows —

Category: Security Products
Product: N/A
Timestamp: N/A

Affected Hosts:

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.64	MARKXP	Windows XP	2

SEVERITY : Low

Vulnerability: Alerterservice enabled —

Category: Services
Product: N/A
Timestamp: 1997-12-01

3 → **Affected Hosts:**

IP Address	Host Name	Operating System	Serv. Pack
192.168.100.153	SERVER	Windows 2000	Unknown
192.168.100.31	NSM2K3STD	Windows Server 2003	1
192.168.100.6	LUCIANP	Windows XP	2
192.168.100.170	BOGVXP	Windows XP	2
192.168.100.238	CB3	Windows 2000	4
192.168.100.75	MARK	Windows XP	2

Screenshot 69 – Sample report showing vulnerability listing by severity

1	Severity level
2	Vulnerability details for each severity level, including name and description
3	List of host machines affected by vulnerabilities detected for each security level

Use this report to:

- List detected vulnerabilities grouped by severity, and the host machines affected by each vulnerability.

Open trojan ports by host

Open Port Listing by Host

This report shows a list of Open Ports found on each host that could serve as a backdoor for trojans.

Created date: 21/12/2005 14:21:04

Scan reference: file:SampleHostList.txt

Scan date & time: 21/12/2005 10:58:55

192.168.20.35 - KeithTest

1 → Operating System: Windows XP
Service Pack: 2
Open Port Count: 3

2 → Open Ports
DummyTrojan.B1Q (500)
DummyTrojan.A.YY (1025)
DummyTrojan.B.SSS (1026)

192.168.20.40 - KeithMain

Operating System: Windows XP
Service Pack: Unknown
Open Port Count: 2

Open Ports
DummyTrojan.A.YY (1025)
DummyTrojan.XB5.T (1134)

192.168.25.10 - KeithServe2K3

Operating System: Windows Server 2003
Service Pack: 1
Open Port Count: 2

Open Ports
DummyTrojan.B.SSS (1026)
DummyTrojan.B1Q (500)

Screenshot 70 – Sample report showing open trojan ports by host

1	Details of host machines having open ports associated with trojans
2	List of open ports for each host and the names of trojans targeting each port

Use this report to:

- List open ports, grouped by host machine, which could potentially serve as a backdoor for trojans.

Open trojan ports

Top 20 Open Trojan Ports

This report shows the Top20 most common open trojan ports(backdoors) found on the network.

Created date: 21/12/2005 14:25:10

Scan reference: file:SampleHostList.txt

Scan date & time: 21/12/2005 10:58:55

Top 20 most common backdoors

Port Description	Open Port Count
DummyTrojan.A.YY (1025)	2
1 → DummyTrojan.B.SSS (1026)	2
DummyTrojan.B1Q (500)	2
DummyTrojan.XB5.T (1134)	1

Screenshot 71 – Sample report showing open trojan ports

1	List showing the most common open trojan ports detected on the network
----------	--

Use this report to:

- List the 20 most common open ports found on the network, which could potentially serve as a backdoor for trojans.

Top SANS vulnerabilities status

Scan reference: 127.0.0.1
Scan date & time: 28-Nov-2006 15:37

1 → 192.168.100.75 - MARK

Operating System	Service Pack
Windows XP	2

TopSANS Year : 2004
TopSANS Chapter : Custom SANS Chapter

2 →

Name:	AutoShareWKS
Description:	The administrative shares (C\$, D\$, ADMIN\$, etc) are available on this machine. For internal networks these are normally turned on for administrative purposes. For Web server(s) these are normally turned off in order to solidify the possible entry points (since it is more exposed to attacks). If you don't use them set HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks to 0 to prevent creation of these shares. For more information, visit http://support.microsoft.com/support/kb/articles/Q246/1/17.asp
Product:	
Name:	Cached Logon Credentials
Description:	Microsoft Windows NT caches the logon information of users who would have logged on, so that they would be able to logon when the server is unavailable. When a domain controller is unavailable and a user's logon information is cached, the user will still be allowed to logon. The cache can hold up from 0 to 50 logon attempts, with the value of 0 disabling logon caching. If the value is set to a high value and an administrator logs in to computers to solve specific problems, an attacker might obtain the credentials of the administrator at a later stage, and logon with such an account, having powerful privileges. The registry value for setting this type of caching is: HKKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ld
Product:	early it should be set to either 0 to disable caching, or else it should be set to 1 to provide for functionality (allowing the last user to logon immediately next time) and security.
Name:	DCCOM is enabled
Description:	Distributed Component Object Model (DCCOM) is similar to Component Object Model (COM) but it is distributed across several networked computers to communicate with each other. COM on Windows 95 had no security, however, DCCOM does. In order to enable DCCOM, EnableDCCOM found in HKKEY_LOCAL_MACHINE\Software\Microsoft\OLE registry key, should be set to 'Y'. This would enhance the system's security features.
Product:	
Name:	Last logged-on username visible
Description:	By default, NT/2k displays the last logged-on user. For more information, visit http://support.microsoft.com/support/kb/articles/q1144/6/3.asp
Product:	
Name:	LM Hash
Description:	It is recommended to use NTLM authentication instead of LM. For more information, visit http://support.microsoft.com/support/kb/articles/q1477/0/6.asp
Product:	

TopSANS Chapter : New SANS Chapter

Name:	A connection could be opened using account Administrator without password!
Description:	You MUST set a password for the administrator account and/or disable guest logons.
Product:	
Name:	Administrator account exists
Description:	It is recommended to rename this account
Product:	
Name:	User ASPNET never logged on
Description:	It is recommended to remove this account if not used
Product:	

Screenshot 72 – Sample report showing top SANS vulnerabilities status

1	Host machine details on which vulnerabilities reported by SANS were detected
2	List showing SANS vulnerability details, including name, description and product affected. SANS vulnerabilities are grouped by year and chapter

Use this report to:

- List the vulnerabilities detected for each host machine, based on the SANS top-20 report of vulnerabilities.

Vulnerable hosts based on open ports

Top 20 Most Vulnerable Hosts (by Open Ports)

This report shows the Top20 most vulnerable hosts based on the number of open trojan port (backdoors) found on each machine.

Created date: 21/12/2005 14:25:07

Scan reference: file:SampleHostList.txt

Scan date & time: 21/12/2005 10:58:55

Top 20 most vulnerable hosts

IP Address	Host Name	Operating System	Serv. Pack	Open Ports
192.168.20.35	KeithTest	Windows XP	2	3
192.168.20.40	KeithMain	Windows XP	Unknown	2
192.168.25.10	KeithServer2K3	Windows Server 2003	1	2

Screenshot 73 – Sample report showing vulnerable hosts based on open ports

1	List showing the top 20 host machines most likely to be compromised by trojans
----------	--

Use this report to:

- List the 20 most vulnerable host machines, based on the number of open trojan ports found.

Vulnerable hosts based on vulnerability level

Scan reference: 80.143.32.1/24
Scan date & time: 05-Feb-2007 19:04

Top 20 hosts based on Vulnerability Level

IP / Host Name	Vuln. Level	Operating System	Service Pack	Total	Vulnerabilities			Missing Patches				
					High	Medium	Low	Total	Critic.	Imprt.	Moder.	Low
80.143.32.211 Andrew	High	Windows 2000	4	24	10	6	8	79	35	34	9	0
80.143.32.233 Andy	High	Windows XP	1	13	5	1	7	81	38	30	11	2
80.143.32.221 Jose	High	Windows XP	Gold	12	3	1	8	41	31	7	3	0
80.143.32.140 Jane	High	Windows XP	2	8	2	1	5	60	27	22	8	3
80.143.32.226 GamesPC	High	Windows XP	2	9	3	1	5	1	1	0	0	0
82.188.102.175 Julia	Medium	Windows XP	2	6	0	1	5	0	0	0	0	0
82.188.102.176 Steve	Low	Windows XP x04	1	5	0	0	5	0	0	0	0	0

Screenshot 74 – Sample report showing vulnerable hosts based on vulnerability level

1	Host machine details showing the number of vulnerabilities and missing patches detected according to criticality
----------	--

Use this report to:

- List the 20 most vulnerable host machines for each network security scan, based on vulnerability level.

Patch management reports

Network patching status

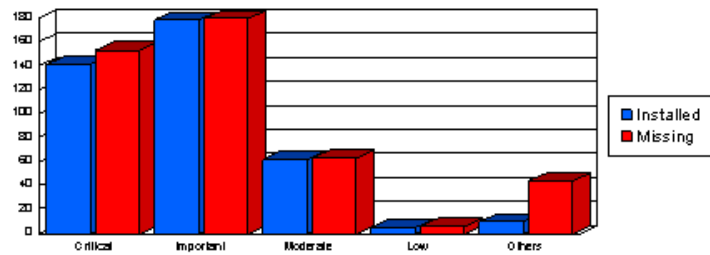
Scan reference: 192.168.100.2-192.168.100.254

Scan date & time: 29-Nov-2006 10:12

Patches and Service Packs Status

1 →

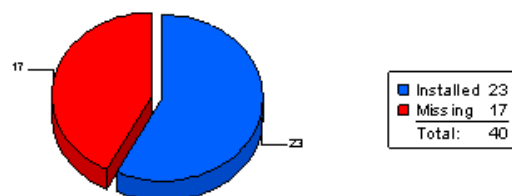
Missing And Installed Patches by Severity



Status	Totals	Severity				
		Critical	Important	Moderate	Low	Others
Installed	396	141	178	62	5	10
Missing	445	153	179	63	6	44
Totals	841	294	357	125	11	54

2 →

Missing And Installed Service Packs



Screenshot 75 – Sample report showing network patching status

1	Chart displaying the number of installed and missing patches, grouped by severity
2	Chart displaying the number of installed and missing service packs

3 → **Top 10 missing security updates**

Bulletin ID	Description	Post Date
MS06-006	Security Update for Windows Media Player Plug-in (KB911564)	2006-02-14
Not Available	Windows Malicious Software Removal Tool - July 2006 (KB890830)	2006-07-11
Not Available	MDAC 2.8 Service Pack 1	2006-02-01
MS04-043	Security Update for Windows XP (KB873339)	2004-12-15
MS04-044	Security Update for Windows XP (KB885835)	2005-04-13
MS04-041	Security Update for Windows XP (KB885836)	2004-12-15
MS05-015	Security Update for Windows XP (KB888113)	2005-02-08
MS05-007	Security Update for Windows XP (KB888302)	2005-02-08
MS05-032	Security Update for Windows XP (KB890046)	2005-06-10
MS05-018	Security Update for Windows XP (KB890859)	2005-07-26

4 → **Top 20 most vulnerable hosts**

IP	Host Name	Severity					N/A
		Critical	High	Important	Moderate	Low	
192.168.100.238	MG4	25	0	30	8	1	7
192.168.100.238	CB3	22	0	29	7	0	8
192.168.100.66	FSERVER	21	1	23	13	1	6
192.168.100.75	MARK	16	1	21	6	1	3
192.168.100.6	LUCIANP	16	1	15	5	1	2
192.168.100.206	V206A	16	0	21	5	1	2
192.168.100.20	CALDEV	14	0	20	7	1	5
192.168.100.220	TESTSTATION	12	0	13	8	0	1
192.168.100.114	VSQRIN-D2005	10	0	7	3	0	19
192.168.100.24	HORI	1	0	0	0	0	0
192.168.100.31	NSM2K3STD	0	1	0	0	0	0
192.168.100.13	STELI	0	0	0	1	0	0
192.168.100.211	ZVIRTUAL2	0	0	0	0	0	1
192.168.100.247	VXPDELPHI2005	0	0	0	0	0	1
192.168.100.232	MG1	0	0	0	0	0	1
192.168.100.64	MARKXP	0	0	0	0	0	1
192.168.100.46	PROJECT	0	0	0	0	0	0
192.168.100.17	BOBBY	0	0	0	0	0	0
192.168.100.19	NSM_XP64	0	0	0	0	0	0
192.168.100.23	MASTERSERV	0	0	0	0	0	0

Screenshot 76 – Sample report showing network patching status

3	List showing the top 10 missing security updates
4	List showing the top 20 most vulnerable host machines, as a result of missing patches and service packs. The number of vulnerabilities detected is split according to severity

Use this report to:

- Illustrate the status of patches and service packs for host machines on the network.

Missing patches grouped by host

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1 → 192.168.100.114 - VSORIN-D2005				
Operating System		Service Pack	Patch Count	
Windows XP		Gold	39	
Bulletin ID	Description	Posted Date	Severity	
2 → Not Available	Windows Malicious Software Removal Tool July 2006 (KB890830)	2006-07-11	N/A	
Not Available	Windows XP Service Pack2	2006-04-25	N/A	
MS04-032	Security Update for Windows XP (KB840987)	2006-04-12	Critical	
MS04-018	Cumulative Security Update for Outlook Express6 SP1 (KB823353)	2006-04-11	Moderate	
Not Available	Update Rollup 1 for Microsoft Windows XP (KB826839)	2005-04-13	N/A	
MS02-051	Q324380: Security Update (Windows XP)	2005-03-25	Moderate	
MS03-018	Q811114: Security Update(Windows XP or Windows XP Service Pack1)	2005-03-25	Important	
MS04-011	Security Update for Windows XP (KB835732)	2005-02-19	Critical	
MS04-015	Security Update for Windows XP (KB840374)	2005-02-19	Important	
MS04-037	Security Update for Windows XP (KB841356)	2005-02-17	Critical	
MS04-003	Security Update for Microsoft Data Access Components (KB832483)	2005-02-17	Important	
MS04-023	Security Update for Windows XP (KB840315)	2005-02-12	Critical	
MS04-024	Security Update for Windows XP (KB839645)	2005-02-08	Important	
MS04-028	Security Update for Windows XP (KB833987)	2004-12-15	Critical	
MS04-022	Security Update for Windows XP (KB841873)	2004-12-15	Critical	
MS04-031	Security Update for Windows XP (KB841533)	2004-11-20	Important	
MS04-038	Cumulative Security Update for Internet Explorer6 Service Pack 1 (KB834707)	2004-11-20	Critical	
MS04-030	Security Update for Windows XP (KB824151)	2004-11-20	Important	
MS04-034	Security Update for Windows XP (KB873376)	2004-11-20	Critical	
MS03-051	Security Update for Windows XP (KB810217)	2004-10-04	Critical	
MS04-016	Security Update for Windows XP (KB839643)	2004-07-26	Moderate	
MS04-014	Security Update for Windows XP (KB837001)	2004-07-23	Important	
MS04-012	Security Update for Windows XP (KB828741)	2004-07-06	Critical	
MS03-008	814078: Security Update(Microsoft Jscript version 5.6, Windows 2000, Windows XP)	2003-11-21	N/A	
MS03-043	Security Update for Microsoft Windows XP (KB828035)	2003-11-20	N/A	
MS02-046	Q326830: Security Update (Windows XP)	2003-11-14	N/A	
MS02-043	Q323172: Security Update (Windows XP)	2003-11-14	N/A	
MS02-008	Security Update, February 13, 2002 (MSXML 2.6)	2003-10-21	N/A	
MS02-000	Security Update for Microsoft Windows XP (KB328940)	2003-10-16	N/A	
MS03-041	Security Update for Microsoft Windows (KB823182)	2003-10-13	N/A	
MS03-044	Security Update for Microsoft Windows XP (KB825119)	2003-10-13	N/A	
MS02-008	Security Update, February 13, 2002 (MSXML 4.0)	2003-09-30	N/A	
MS03-030	Security Update for Windows XP (819696)	2003-09-16	N/A	
MS03-034	Security Update for Microsoft Windows (KB824105)	2003-09-09	N/A	
MS02-029	Q318138: Security Update (Windows XP)	2003-08-05	N/A	
MS02-032	Q320920: Security Update(Windows Media Player for Windows XP)	2003-06-18	N/A	
MS02-012	Q313450: Security Update	2003-02-18	N/A	
MS02-017	Q311967: Security Update	2003-02-18	N/A	
MS01-059	Security Update, December 17, 2001	2003-02-18	N/A	

Screenshot 77 – Sample report showing missing patches grouped by host

1	Host machine details on which missing patches were detected
2	List of missing patch details for each host, including severity and URL link for further information

Use this report to:

- List missing patches grouped by host machine, including URL links providing further information on each missing patch.

Missing patches grouped by operating system

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Windows 2000

1	Patch: 914388 Bulletin ID: MS06-036 Posted Date: 2006-07-11 Severity: Critical Description: Security Update for Windows 2000 (KB914388)								
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.238</td> <td>CB3</td> <td>4</td> </tr> </tbody> </table>	Host IP	Host Name	Service Pack	192.168.100.238	CB3	4		
Host IP	Host Name	Service Pack							
192.168.100.238	CB3	4							
	Patch: 890830 Bulletin ID: Not Available Posted Date: 2006-07-11 Severity: N/A Description: Windows Malicious Software Removal Tool - July 2006 (KB90830)								
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.238</td> <td>CB3</td> <td>4</td> </tr> </tbody> </table>	Host IP	Host Name	Service Pack	192.168.100.238	CB3	4		
Host IP	Host Name	Service Pack							
192.168.100.238	CB3	4							
2	Patch: 917344 Bulletin ID: MS06-023 Posted Date: 2006-06-13 Severity: Moderate Description: Security Update for Windows Server 2003 (KB917344)								
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.220</td> <td>TESTSTATION</td> <td>1</td> </tr> <tr> <td>192.168.100.66</td> <td>FSERVER</td> <td>Gold</td> </tr> </tbody> </table>	Host IP	Host Name	Service Pack	192.168.100.220	TESTSTATION	1	192.168.100.66	FSERVER
Host IP	Host Name	Service Pack							
192.168.100.220	TESTSTATION	1							
192.168.100.66	FSERVER	Gold							

Screenshot 78 – Sample report showing missing patches grouped by operating system

1	Missing patch details for each operating system
2	List of host machines on which specific patches were found to be missing

Use this report to:

- List missing patches grouped by operating system, including the host machine names for each missing patch.

Missing patches grouped by severity

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Critical

1	Patch: 917159 Bulletin ID: MS06-035 Posted Date: 2006-07-11 Description: Security Update for Windows Server 2003 (KB917159)											
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Operating System</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.220</td> <td>TESTSTATION</td> <td>Windows Server 2003</td> <td>1</td> </tr> </tbody> </table>	Host IP	Host Name	Operating System	Service Pack	192.168.100.220	TESTSTATION	Windows Server 2003	1			
Host IP	Host Name	Operating System	Service Pack									
192.168.100.220	TESTSTATION	Windows Server 2003	1									
	Patch: 914388 Bulletin ID: MS06-036 Posted Date: 2006-07-11 Description: Security Update for Windows Server 2003 (KB914388)											
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Operating System</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.220</td> <td>TESTSTATION</td> <td>Windows Server 2003</td> <td>1</td> </tr> </tbody> </table>	Host IP	Host Name	Operating System	Service Pack	192.168.100.220	TESTSTATION	Windows Server 2003	1			
Host IP	Host Name	Operating System	Service Pack									
192.168.100.220	TESTSTATION	Windows Server 2003	1									
	Patch: 914388 Bulletin ID: MS06-036 Posted Date: 2006-07-11 Description: Security Update for Windows XP (KB914388)											
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Operating System</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.75</td> <td>MARK</td> <td>Windows XP</td> <td>2</td> </tr> </tbody> </table>	Host IP	Host Name	Operating System	Service Pack	192.168.100.75	MARK	Windows XP	2			
Host IP	Host Name	Operating System	Service Pack									
192.168.100.75	MARK	Windows XP	2									
2	Patch: 917159 Bulletin ID: MS06-035 Posted Date: 2006-07-11 Description: Security Update for Windows XP (KB917159)											
	<table border="1"> <thead> <tr> <th>Host IP</th> <th>Host Name</th> <th>Operating System</th> <th>Service Pack</th> </tr> </thead> <tbody> <tr> <td>192.168.100.75</td> <td>MARK</td> <td>Windows XP</td> <td>2</td> </tr> <tr> <td>192.168.100.236</td> <td>MG4</td> <td>Windows XP</td> <td>1</td> </tr> </tbody> </table>	Host IP	Host Name	Operating System	Service Pack	192.168.100.75	MARK	Windows XP	2	192.168.100.236	MG4	Windows XP
Host IP	Host Name	Operating System	Service Pack									
192.168.100.75	MARK	Windows XP	2									
192.168.100.236	MG4	Windows XP	1									

Screenshot 79 – Sample report showing missing patches grouped by severity

1	Missing patch details for each severity level
2	List of host machines on which specific patches were found to be missing

Use this report to:

- List missing patches grouped by severity, including the host machine names for each missing patch.

Installed patches grouped by host

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1 → 192.168.100.6 - LUCIANP

Operating System	Service Pack	Patch Count
Windows XP	2	17

2 →

Bulletin ID	Description	Posted Date	Severity	Uninstallable
MS06-005	Security Update for Windows Media Player 9 (KB911566)	2006-02-14	Critical	No
Not Available	MDAC 2.8 Service Pack 1	2006-02-01	High	No
MS05-018	Security Update for Windows XP (KB890859)	2005-07-26	Important	Yes
MS04-044	Security Update for Windows XP (KB885835)	2005-04-13	Important	Yes
MS05-020	Cumulative Security Update for Internet Explorer for Windows XP Service Pack 2 (KB890923)	2005-04-12	Critical	Yes
MS05-016	Security Update for Windows XP (KB893086)	2005-04-12	Important	Yes
MS05-011	Security Update for Windows XP (KB885250)	2005-02-23	Critical	Yes
MS05-007	Security Update for Windows XP (KB888302)	2005-02-08	Important	Yes
MS05-009	Security Update for Windows Messenger (KB887472)	2005-02-08	Moderate	Yes
MS05-012	Security Update for Windows XP (KB873333)	2005-02-08	Important	Yes
MS05-015	Security Update for Windows XP (KB888113)	2005-02-08	Important	Yes
MS05-013	Security Update for Windows XP (KB891781)	2005-02-08	Important	Yes
MS05-001	Security Update for Windows XP (KB890175)	2005-01-18	Critical	Yes
MS04-043	Security Update for Windows XP (KB873339)	2004-12-15	Important	Yes
MS04-041	Security Update for Windows XP (KB885836)	2004-12-15	Important	Yes
Not Available	Microsoft .NET Framework 1.1 Service Pack 1	2004-09-01	N/A	No
MS03-011	316093: Security Update Microsoft Virtual Machine (Microsoft VM)	2004-06-08	Critical	No

Screenshot 80 – Sample report showing installed patches grouped by host

1	Host machine details on which installed patches were detected
2	List of installed patch details for each host, including severity, URL link for further information and indication if the patch can be uninstalled

Use this report to:

- List installed patches grouped by host machine, including URL links providing further information on each installed patch.

Installed patches grouped by operating system

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

Windows Server2003

1 → Patch: 889101 Bulletin ID: [Not Available](#) Posted Date: 2006-07-11
Severity: N/A Uninstallable: No
Description: Windows Server 2003 Service Pack 1

Host IP	Host Name	Service Pack
192.168.100220	TESTSTATION	1
192.168.10031	NSM2K3STD	1

2 → Patch: 890830 Bulletin ID: [Not Available](#) Posted Date: 2006-07-11
Severity: N/A Uninstallable: No
Description: Windows Malicious Software Removal Tool - July 2006 (KB890830)

Host IP	Host Name	Service Pack
192.168.10031	NSM2K3STD	1

Screenshot 81 – Sample report showing installed patches grouped by operating system

1	Installed patch details for each operating system
2	List of host machines on which specific patches were found to be installed

Use this report to:

- List installed patches grouped by operating system, including the host machine names for each installed patch.

Installed patches grouped by severity

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

High

1 → Patch: 899456 Bulletin ID: [NotAvailable](#) Posted Date: 2006-02-01
 Uninstallable: No
 Description: MDAC 2.8 Service Pack 1

Host IP	Host Name	Operating System	Service Pack
192.168.100.13	STELI	Windows XP x64	1
192.168.100.64	MARKXP	Windows XP	2
192.168.100.247	VXPDELPHI2005	Windows XP	2
192.168.100.24	HORI	Windows XP x64	1
192.168.100.170	BOGVXP	Windows XP	2
192.168.100.20	CALDEV	Windows XP	2
192.168.100.75	MARK	Windows XP	2

Screenshot 82 – Sample report showing installed patches grouped by severity

1	List of installed patches grouped by their severity level, including information on each patch
2	List of host machines on which specific patches were found to be installed

Use this report to:

- List installed patches grouped by severity, including the host machine names for each installed patch.

Deployment history by host

1 → Target Host: 192.168.100.149

Deployments						
Date Started	Date Ended	Completed Status	Type	Is Scheduled		
11/20/2006 2:45:26PM	11/20/2006 2:45:52PM	With errors.	Custom	No		
2 → Files: AnotherFile.exe.config						
Date Started	Date Ended	Completed Status	Type	Is Scheduled		
11/20/2006 2:46:58PM	11/20/2006 2:47:05PM	Successfully.	Custom	No		
Files: NOTEPAD.EXE;						

Screenshot 83 – Sample report showing deployment history by host

1	Host machine on which deployments were made
2	List of deployment details for each host, including file names deployed, and deployment status

Use this report to:

- Display patch deployment information grouped by host machine, including deployment details such as date and status.

Deployment history by date

1 → Date Started: 11/20/2006 2:45:26PM

Deployments					
Target	Date Ended	Completed Status	Type	Is Scheduled	
192.168.100.149	11/20/2006 2:45:52PM	With errors.	Custom	No	

2 → Files: AnotherFile.exe.config

Target	Date Ended	Completed Status	Type	Is Scheduled	
TestHost2	11/20/2006 2:45:52PM	Erroneous.	Custom	No	

Files: out.txt; T29.txt; vssver.scc;

Screenshot 84 – Sample report showing deployment history by date

1	Deployment starting date
2	List of deployment details grouped by host, including file names deployed, and deployment status

Use this report to:

- Display patch deployment information by date and time, including details such as host machine names for each deployment.

Deployment history by patch

1 → Patch: AnotherFile.exe.config

Deployments					
Date Started	Date Ended	Completed Status	Type	Is Scheduled	
11/20/2006 2:45:26PM	11/20/2006 2:45:52PM	With errors.	Custom	No	

2 → Target: 192.168.100.149

Screenshot 85 – Sample report showing deployment history by patch

1	Name of patch deployed
2	List of host machines on which the patch was deployed and deployment details, including deployment status

Use this report to:

- Display patch deployment information grouped by patch applied, including details such as host machine names for each deployment.

System information reports

Software audit

Scan reference : 80.143.32.1/24
 Scan date & time : 2/3/2007 2:30:23PM

Top 10 Systems with Unauthorized Applications

IP	Host Name	Unauthorized Applications
80.143.32.211	Andrew	2
80.143.32.233	Andy	1

Top 10 Unauthorized Applications

Application Name	Application Count
Yahoo! Toolbar	2
Nero Suite	1

Systems with Security Applications



Category of Systems	Systems Count
Systems With Security Applications Not Updated	1
Systems Without Any Security Application	1

Top 20 Most Installed Applications

Adobe Flash Player 9		
Publisher : Adobe Systems Inc.		
Occurance : 2		
IP	Host Name	Operating System
80.143.32.211	Andrew	Windows 2000
80.143.32.233	Andy	Windows XP
VMware Tools		
Publisher : VMware, Inc.		
Occurance : 1		
IP	Host Name	Operating System
80.143.32.211	Andrew	Windows 2000
VMware Workstation		
Publisher : VMware, Inc.		
Occurance : 1		
IP	Host Name	Operating System
80.143.32.211	Andrew	Windows 2000

Screenshot 86 – Sample report showing software audit

1	List showing the top 10 host machines with unauthorized applications
2	List showing the top 10 unauthorized applications
3	Chart displaying the status of security applications on host machines
4	List showing the top 20 installed applications

Use this report to:

- Identify unauthorized applications installed on host machines, detected during network security scans

- Identify the top 10 host machines with unauthorized applications
- Identify the top 10 unauthorized applications with highest number of installations
- Identify the top 20 installed applications
- Graphically represent the number of host machines without security applications, or with security applications not updated.

Operating system and service pack distribution

Operating System and Service Pack Distribution

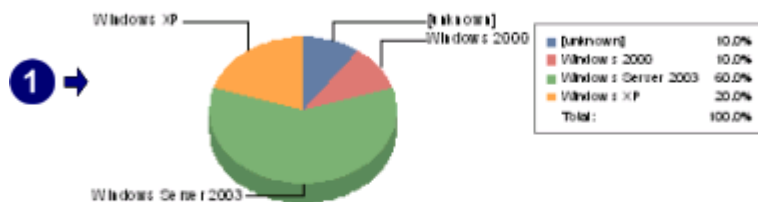
A graphical and textual representation of operating system distributions together with their related service packs.

Created date: 21/12/2005 14:19:30

Scan reference : file:SampleHostList.txt

Scan date & time : 21/12/2005 10:58:55

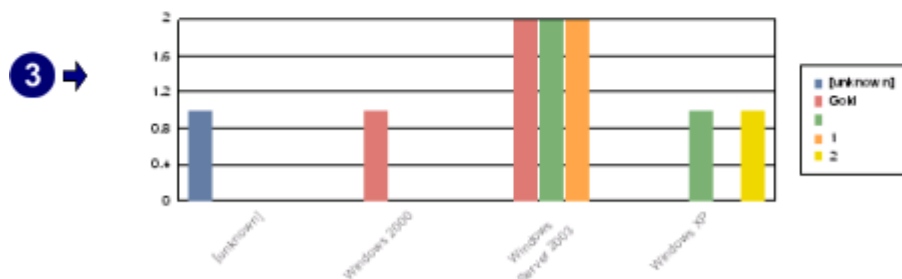
Operating System distribution



2 →

Operating System	Number of Hosts
[unknown]	1
Windows 2000	1
Windows Server 2003	6
Windows XP	2

Service Pack distribution



4 →

Operating System	Service Pack	Number of Hosts
[unknown]	[unknown]	1
Windows 2000	Gold	1
Windows Server 2003		2
Windows Server 2003	1	2
Windows Server 2003	Gold	2
Windows XP		1
Windows XP	2	1

Screenshot 87 – Sample report showing operating system and service pack distribution

1	Chart displaying distribution percentage of each operating system on the network
2	List of operating systems, including the number of host machines on which they are installed
3	Chart displaying service pack distribution for each operating system
4	List of operating system service packs, including the number of host machines on which they are installed

Use this report to:

- Graphically represent operating systems detected on the network
- List the number of host machines for each operating system
- Graphically represent service packs detected on the network for each operating system
- List the number of host machines for each service pack installed.

System information

Scan reference: file:list.txt
Scan date & time: 1/8/2007 2:38:18PM

1 → 192.168.100.75- MARK

Operating System	Service Pack
Windows XP	2

2 → Computer Properties

MAC Address: 00-0E-0C-3C-A8-36 (Intel Corporation)
 Time to live: 128 (128)
 Network role: Workstation
 Domain: WORKGROUP
 LAN manager: Windows2000 LAN Manager

3 → Uptimes

Time of Day	Up Time
22	2 seconds, 321 ms
543	653 ms

4 → Disk Utilization

Name	Total Space	Free Space	File System Type
C:	343434	33242424	FAT 32

5 → Groups and Users

Groups	
Name	Description
Administrators	Administrators have complete and unrestricted access to the computer/domain Members: MARKLNSS_MONITOR_USR, MARKroot, MARKAdministrator
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted Members: MARKoba_anonymous, MARKGuest
Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications Members: NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authenticated Users, MARKASPNET, MARKImtest, MARKroot
HelpServicesGroup	Group for the Help and Support Center Members: MARKSUPPORT_388945a0
vmware	VMware User Group Members: MARK_vmware_user_

Users	
Administrator()	Privilege: Administrator(*) Flags: SCRIPT, NORMAL_ACCOUNT Comment: Built-in account for administering the computer/domain LastLogon: 28 Nov 2006, 15:41:58 PasswordAge: 19 days, 30 minutes, 16 seconds # Logons: 2,229 BadPasswordCount: 4

Screenshot 88 – Sample report showing system information

1	Host machine IP and name
2	Host machine details, including MAC address and domain
3	Uptime details for each host machine, including time of day and uptime value
4	Disk utilization details for each host machine, including drive name, file system type, total storage space and free storage space
5	Group and user details for each host machine, including group name, group members, user privileges and user bad password count

6 → **SNMP Information**

Name	Description
Object_ID	1.3.6.1.4.1.311.1.1.3.1.3 (NT Domain Controller)
sysDescr	Hardware: x86 Family 15 Model 4 Stepping 1 AT/AT COMPATI
sysName	PROJECT
sysUpTime	18 minutes, 45 seconds
Vendor	Microsoft

7 → **Services**

Service Name	Status	Startup Type	Account Name
Alerter			
Alerter	Running	Automatic	NT AUTHORITY\LocalService
ALG			
Application Layer Gateway Service	Running	Manual	NT AUTHORITY\LocalService
AppMgmt			
Application Management	Stopped	Manual	LocalSystem
aspnet_state			
ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService
AudioSrv			
Windows Audio	Running	Automatic	LocalSystem
BITS			
Background Intelligent Transfer Service	Stopped	Manual	LocalSystem
Browser			
Computer Browser	Running	Automatic	LocalSystem

8 → **Processes**

alg.exe
PID : 2404
PPID : 1048
User Name : LOCAL SERVICE
Domain : NT AUTHORITY
Handle Count : 107
Thread Count : 5
Priority : 8
atiptaxx.exe
PID : 2236
PPID : 2072
User Name : Administrator
Path : C:\WINDOWS\system32\atiptaxx.exe
Domain : MARK
Command Line : "C:\WINDOWS\system32\atiptaxx.exe"
Handle Count : 53
Thread Count : 1
Priority : 8

Screenshot 89 – Sample report showing system information

6	SNMP details for each host machine, including name and description
7	Service details for each host machine, including name, description, status, startup type and account name
8	Process details for each host machine, including process ID and account name

9 → **Devices**

USB Devices

USB Root Hub	
Description:	USB Root Hub
Manufacturer:	(Standard USB Host Controller)
USB Root Hub	
Description:	USB Root Hub
Manufacturer:	(Standard USB Host Controller)
USB Root Hub	
Description:	USB Root Hub
Manufacturer:	(Standard USB Host Controller)

There were no Blacklisted USB Devices vulnerabilities detected

Virtual Devices

WAN Miniport (L2TP)	
DHCP Set:	False
WAN Miniport (PPTP)	
MAC Address:	50:50:54:50:30:30
DHCP Set:	False
WAN Miniport (PPPOE)	
MAC Address:	33:50:8F:45:30:30
DHCP Set:	False

There were no Blacklisted Wireless Devices vulnerabilities detected

10 → **Shares**

Name	Remark
ADMIN\$	Remote Admin
c	share
C\$	Defaultshare
CD Drive (F)	N/A
D	share
D\$	Defaultshare
E	share
E\$	Defaultshare
IPC\$	Remote IPC
XP Prof- SP2 - VXPGE	N/A

11 → **Open Ports**

TCP Ports

3,593 [Full Port List]
2,107 [Full Port List]
2,105 [Full Port List]
2,103 [Full Port List]
1,801 [Full Port List]
139 [Netbios-ssn => NETBIOS Session Service]

UDP Ports

1,900 [Full Port List]
1,943 [Full Port List]
138 [Full Port List]

Screenshot 90 – Sample report showing system information

9	List showing USB devices, blacklisted USB devices, network cards and black listed wireless devices
10	Share folder details for each host machine, including name and remarks
11	Open port details for each host machine, including port number and name

12 Installed Applications				
Installed Applications				
Application Name	Publisher	Version		
Ad-Aware SE Personal Edition	Lavasoft	1.06		
Adobe Flash Player9 ActiveX	Adobe Systems	9		
Adobe Reader7.08	Adobe Systems Incorporated	7.0.8		
ATI Display Driver				
CCleaner(remove only)				
F-Prot Antivirus for Windows				
Gadwin PrintScreen	Gadwin Systems, Inc.	3.5		
GFI EventsManager 7 Report Pack	GFI Software Ltd	1.0.2006.0907		
GFI LANguard Network Security Scanner8.0	GFI	8.0		
GFI Report Center Framework	GFI Software	3.5		
Unauthorized Applications				
Application Name	Publisher	Version		
Ad-Aware SE Personal Edition	Lavasoft	1.06		
Adobe Flash Player9 ActiveX	Adobe Systems	9		
ATI Display Driver				
CCleaner(remove only)				
Gadwin PrintScreen	Gadwin Systems, Inc.	3.5		
13 Policies				
Password Policy				
Minimum Password Length	Maximum Password Age	Minimum Password Age	Force Logoff	Password History
0 chars	42 days, 22 hours, 47 minutes, 31 seconds	no delay	never force	no history
Security Audit Policy				
Auditing Policy	Success	Failure		
Audit account logon events	True	True		
Audit account management	True	True		
Audit directory service access	False	False		
Audit logon events	True	True		
Audit object access	False	False		
Audit policy change	True	True		
Audit privilege use	True	True		
Audit process tracking	True	True		
Audit system events	True	True		
14 Registry Information				
Node Name	Registry Entry			
	~MHz : 2793			
	CSDVersion : Service Pack 2			
	CurrentBuildNumber : 2600			
	CurrentType : Multiprocessor Free			
	CurrentVersion : 5.1			
	Default : 0409			
	DriverDesc : Media Control Devices			
	DriverDesc : RAGE XL PCI			
	Identifier : x86 Family 15 Model 4 Stepping 3			
Run	ATIP TA : atiptax.exe			
Run	FRISK FP-Scheduler: C:\Program Files\F-SIN\F-Pro\F-Sched.exe STARTUP			
Run	F-StopW: C:\Program Files\F-SIN\F-Pro\F-StopW.EXE			
Run	Intel Server Manager: C:\program files\intel\ServerManager\Server\bin\usm.exe			
Run	ISUSPM: "C:\Program Files\Common Files\InstallShield\UpdateService\ISUSPM.exe" -scheduler			
Run	MsmqIntCrt: regsvr32 /s mqrt.dll			
Run	PRONoMgrWired: C:\program Files\Intel\PROSetWired\NC\S\PROSet\PRONoMgr.exe			

Screenshot 91 – Sample report showing system information

12	Installed application details for each host machine, including name, publisher and version
13	List showing password policy details security audit policy details
14	List of registry entry details for each host machine

Use this report to:

- List detailed technical information for each host machine, including services, installed applications, policies and devices.

Computer properties

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:12:25AM

CATEGORY: FTP

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:11

1 → 192.168.100.11- [Z] Service Pack

MAC Address: 00-0F-EA-F0-FF-1E ("GigaByte Technology Co.,LTD.")

2 → Time to live: 128 (128)
 Network role: N/A
 Domain: N/A
 LAN manager: N/A

192.168.100.12- [BOGDAN] Service Pack

MAC Address: 00-11-D8-9D-BA-7C (ASUSTek Computer Inc.)

Time to live: 128 (128)
 Network role: N/A
 Domain: N/A
 LAN manager: N/A

Screenshot 92 – Sample report showing computer properties

1	Host machine IP and name
2	Host machine details, including MAC address and domain

Use this report to:

- List information for each host machine, including MAC address, network role and domain.

Uptimes

Scan reference: 127.0.0.1
Scan date & time: 28-Nov-2006 15:37

1 → 192.168.100.75- MARK

Operating System	Service Pack
Windows XP	2
Time of Day	Up Time
00	100 ms
23	123 ms
156	1 hours, 13 minutes, 2 seconds, 735 ms

192.168.100.26- CB

Operating System	Service Pack
Windows Server2003	
Time of Day	Up Time
4	44 ms

Screenshot 93 – Sample report showing uptimes

1	Host machine IP and name
2	Uptime details for each host machine, including time of day and uptime value

Use this report to:

- List uptime for each host machine, grouped by network scan.

Disk utilization

Scan reference: 127.0.0.1
Scan date & time: 28-Nov-2006 15:37

1	192.168.100.75 - MARK			
	Operating System	Service Pack		
	Windows XP	2		
2	Name	Total Space	Free Space	File System Type
	C:	36263662	1212121	NTFS
	D:	433423423	33333	NTFS

Screenshot 94 – Sample report showing disk utilization

1	Host machine IP and name
2	Disk utilization details for each host machine, including drive name, file system type, total storage space and free storage space

Use this report to:

- List disk utilization information for each host machine, including file system type, total space and free space.

Groups and users

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1	192.168.100.6 - LUCIANP	
	Operating System	Service Pack
	Windows XP	2
	Groups	
	Name	Description
	__vmware__	VMware User Group
	Members: LUCIANP__vmware_user__	
2	192.168.100.6 Admins	192.168.100.6 Admins - Members can create and manage Webs
	Members: BUILTIN\Administrators	
	Administrators	Administrators have complete and unrestricted access to the computer\domain
	Members: DEVELOPMENT\Domain Admins, LUCIANP\User, LUCIANP\Administrator, LUCIANP\wok	
	Debugger Users	Debugger users can debug processes on this machine, both locally and remotely
	Members: LUCIANP\User	
	Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
	Members: LUCIANP\USR_LUCIANP, LUCIANP\Guest	
	HelpServicesGroup	Group for the Help and Support Center
	Members: LUCIANP\SUPPORT_388945a0	
	Users	Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications
	Members: DEVELOPMENT\Domain Users, NT AUTHORITY\INTERACTIVE, NT AUTHORITY\Authenticated Users, LUCIANP\ASPNET, LUCIANP\wok, LUCIANP\ACTUser, LUCIANP\SQLDebugger	
	Users	
3	ACTUser(Application Center Test Account)	
	Full Name: Application Center Test Account	
	Privilege: User	
	Flags: SCRIPT,PASSWORD_CANNOT_BE_CHANGED,NORMAL_ACCOUNT	
	Comment: Account used to launch the Application Center Test Broker and Controller services	
	LastLogon: 14 Aug 2006, 16:32:58	
	PasswordAge: 106 days, 17 hours, 38 minutes, 45 seconds	
	# Logons: 3	

Screenshot 95 – Sample report showing groups and users

1	Host machine IP and name
2	List showing group details for each host machine, including name, description and members
3	List of user details for each group, including user name, privilege, last logon and bad password count

Use this report to:

- List group and user information for each host machine.

SNMP information

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:11

1	192.168.100.17 - BOBBY													
	Operating System	Service Pack												
	Windows XP													
2	<table border="1"> <thead> <tr> <th>Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Object_ID</td> <td>1.3.6.1.4.1.311.1.1.3.1.1 (NT Workstation)</td> </tr> <tr> <td>sysDesor</td> <td>Hardware: x86 Family 15 Model 3 Stepping 3 AT/AT COMPATI</td> </tr> <tr> <td>sysName</td> <td>BOBBY</td> </tr> <tr> <td>sysUpTime</td> <td>52 minutes, 23 seconds</td> </tr> <tr> <td>Vendor</td> <td>Microsoft</td> </tr> </tbody> </table>		Name	Description	Object_ID	1.3.6.1.4.1.311.1.1.3.1.1 (NT Workstation)	sysDesor	Hardware: x86 Family 15 Model 3 Stepping 3 AT/AT COMPATI	sysName	BOBBY	sysUpTime	52 minutes, 23 seconds	Vendor	Microsoft
Name	Description													
Object_ID	1.3.6.1.4.1.311.1.1.3.1.1 (NT Workstation)													
sysDesor	Hardware: x86 Family 15 Model 3 Stepping 3 AT/AT COMPATI													
sysName	BOBBY													
sysUpTime	52 minutes, 23 seconds													
Vendor	Microsoft													

Screenshot 96 – Sample report showing SNMP information

1	Host machine IP and name
2	SNMP details for each host machine, including name and description

Use this report to:

- List SNMP information for each host machine, including name, description and uptime.

Services

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:11

1	192.168.100.8 - LUCIANP																																																																				
	Operating System	Service Pack																																																																			
	Windows XP	2																																																																			
2	<table border="1"> <thead> <tr> <th colspan="5">Services</th> </tr> <tr> <th colspan="5">Alerter</th> </tr> <tr> <th>Service Name</th> <th>Status</th> <th>Startup Type</th> <th colspan="2">Account Name</th> </tr> </thead> <tbody> <tr> <td>Alerter</td> <td>Running</td> <td>Automatic</td> <td colspan="2">NT AUTHORITY\LocalService</td> </tr> <tr> <th colspan="5">ALG</th> </tr> <tr> <th>Service Name</th> <th>Status</th> <th>Startup Type</th> <th colspan="2">Account Name</th> </tr> <tr> <td>Application Layer Gateway Service</td> <td>Running</td> <td>Manual</td> <td colspan="2">NT AUTHORITY\LocalService</td> </tr> <tr> <th colspan="5">AppMgmt</th> </tr> <tr> <th>Service Name</th> <th>Status</th> <th>Startup Type</th> <th colspan="2">Account Name</th> </tr> <tr> <td>Application Management</td> <td>Stopped</td> <td>Manual</td> <td colspan="2">LocalSystem</td> </tr> <tr> <th colspan="5">aspnet_state</th> </tr> <tr> <th>Service Name</th> <th>Status</th> <th>Startup Type</th> <th colspan="2">Account Name</th> </tr> <tr> <td>ASP.NET State Service</td> <td>Stopped</td> <td>Manual</td> <td colspan="2">NT AUTHORITY\NetworkService</td> </tr> </tbody> </table>				Services					Alerter					Service Name	Status	Startup Type	Account Name		Alerter	Running	Automatic	NT AUTHORITY\LocalService		ALG					Service Name	Status	Startup Type	Account Name		Application Layer Gateway Service	Running	Manual	NT AUTHORITY\LocalService		AppMgmt					Service Name	Status	Startup Type	Account Name		Application Management	Stopped	Manual	LocalSystem		aspnet_state					Service Name	Status	Startup Type	Account Name		ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService	
Services																																																																					
Alerter																																																																					
Service Name	Status	Startup Type	Account Name																																																																		
Alerter	Running	Automatic	NT AUTHORITY\LocalService																																																																		
ALG																																																																					
Service Name	Status	Startup Type	Account Name																																																																		
Application Layer Gateway Service	Running	Manual	NT AUTHORITY\LocalService																																																																		
AppMgmt																																																																					
Service Name	Status	Startup Type	Account Name																																																																		
Application Management	Stopped	Manual	LocalSystem																																																																		
aspnet_state																																																																					
Service Name	Status	Startup Type	Account Name																																																																		
ASP.NET State Service	Stopped	Manual	NT AUTHORITY\NetworkService																																																																		

Screenshot 97 – Sample report showing services

1	Host machine IP and name
2	Service details for each host machine, including name, description, status, startup type and account name

Use this report to:

- List service information for each host machine, including description, status, startup type and account name.

Processes

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1 → 192.168.100.114 - VSDRIN-D2005

Operating System	Service Pack
Windows XP	Gold

System Idle Process
Thread Count 1

2 → System

PID: 4
User Name: SYSTEM
Domain: NT AUTHORITY
Handle Count 640
Thread Count 49
Priority: 8

mdm.exe

PID: 208
PPID: 1216
User Name: SYSTEM
Path: C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe
Domain: NT AUTHORITY
Command Line: "C:\Program Files\Common Files\Microsoft Shared\VS7Debug\mdm.exe"
Handle Count 70
Thread Count 4
Priority: 8

Screenshot 98 – Sample report showing processes

1	Host machine IP and name
2	Process details for each host machine, including process ID and account name

Use this report to:

- List process properties for each host machine.

Devices

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1 → 192.168.100.114 - VSORIN-D2005

Operating System	Windows XP	Service Pack	Gold
------------------	------------	--------------	------

2 → USB Devices

USB Root Hub	Description:	USB Root Hub
	Manufacturer:	(Standard USB Host Controller)

3 → There were no Blacklisted USB Devices vulnerabilities detected

4 → Network Devices

Virtual Devices

Packet Scheduler Miniport	MAC Address:	00:0C:29:10:A3:D7
	DHCP Set:	False
	Status:	Plugged in

WAN Miniport (L2TP)	DHCP Set:	False
	Status:	Plugged in

Software Enumerated Devices

RAS Async Adapter	DHCP Set:	False
	Status:	Plugged in

Unknown devices

AMD PCNET Family PCI Ethernet Adapter - Packet Sched	MAC Address:	00:0C:29:10:A3:D7
	IP Address(es):	192.168.100.114, 192.168.18.29, 192.168.18.21, 192.168.18.29
	Hostname:	VSorin-D2005
	DHCP Set:	False
	DNS Server(s):	212.93.140.1
	Gateway(s):	192.168.100.1
	Status:	Plugged in

5 → There were no Blacklisted Devices vulnerabilities detected

Screenshot 99 – Sample report showing devices

1	Host machine IP and name
2	List showing USB devices detected for each host machine
3	List showing blacklisted USB devices detected for each host machine
4	List showing network cards detected for each host machine
5	List showing blacklisted wireless devices detected for each host machine

Use this report to:

- List information on devices detected on the network including host information and whether the devices are blacklisted.

Shares

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1 → 192.168.100.114 - VSORIN-D2005

Operating System	Windows XP	Service Pack	Gold
------------------	------------	--------------	------

2 →

Name	Remark
ADMIN\$	Remote Admin
C\$	Defaultshare
IPC\$	Remote IPC

Screenshot 100 – Sample report showing shares

1	Host machine IP and name
2	Share folder details for each host machine, including name and remarks

Use this report to:

- List information on shared folders for each host machine.

Open ports

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 11/29/2006 10:11:19AM

1	192.168.100.6 - LUCIANP
	Operating System: Windows XP Service Pack: 2
2	TCP Ports 21 [FTP => File Transfer Protocol] 25 [SMTP => Simple Mail transfer Protocol] 135 [epmap => DCE endpoint resolution] 139 [Netbios-ssn => NETBIOS Session Service] 443 [HttpS => Secure HTTP] 445 [Microsoft-Ds] 1,433 [Microsoft SQL server]

Screenshot 101 – Sample report showing open ports

1	Host machine IP and name
2	Open port details for each host machine, including port number and name

Use this report to:

- List open ports detected for each host on the network including port number and name.

Installed applications

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1	192.168.100.114 - VSDRIND2005																											
	Operating System: Windows XP Service Pack: Gold																											
2	Installed Applications <table border="1"> <thead> <tr> <th>Application Name</th> <th>Publisher</th> <th>Version</th> </tr> </thead> <tbody> <tr> <td>GFI LANguard S.E.L.M. 5</td> <td>GFI Software Ltd.</td> <td>5.0.0</td> </tr> <tr> <td>Microsoft .NET Framework 2.0</td> <td>Microsoft Corporation</td> <td></td> </tr> <tr> <td>Microsoft Internet Explorer 6 SP1</td> <td></td> <td></td> </tr> <tr> <td>MSXML4.0 SP2 Parser and SDK</td> <td>Microsoft Corporation</td> <td>4.20.9818.0</td> </tr> <tr> <td>Notepad++</td> <td></td> <td></td> </tr> <tr> <td>Total Commander (Remove or Repair)</td> <td></td> <td></td> </tr> <tr> <td>VMware Tools</td> <td>VMware, Inc.</td> <td>3.1.0000</td> </tr> <tr> <td>Windows Installer 3.0 (KB884016)</td> <td>Microsoft Corporation</td> <td>3.0</td> </tr> </tbody> </table>	Application Name	Publisher	Version	GFI LANguard S.E.L.M. 5	GFI Software Ltd.	5.0.0	Microsoft .NET Framework 2.0	Microsoft Corporation		Microsoft Internet Explorer 6 SP1			MSXML4.0 SP2 Parser and SDK	Microsoft Corporation	4.20.9818.0	Notepad++			Total Commander (Remove or Repair)			VMware Tools	VMware, Inc.	3.1.0000	Windows Installer 3.0 (KB884016)	Microsoft Corporation	3.0
Application Name	Publisher	Version																										
GFI LANguard S.E.L.M. 5	GFI Software Ltd.	5.0.0																										
Microsoft .NET Framework 2.0	Microsoft Corporation																											
Microsoft Internet Explorer 6 SP1																												
MSXML4.0 SP2 Parser and SDK	Microsoft Corporation	4.20.9818.0																										
Notepad++																												
Total Commander (Remove or Repair)																												
VMware Tools	VMware, Inc.	3.1.0000																										
Windows Installer 3.0 (KB884016)	Microsoft Corporation	3.0																										

Screenshot 102 – Sample report showing installed applications

1	Host machine IP and name
2	Installed application details for each host machine, including name, publisher and version

Use this report to:

- List installed applications detected for each network host scanned, including publisher and version details.

Policies

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1	192.168.100.6 - LUCIANP				
	Operating System	Service Pack			
	Windows XP	2			
2	Password Policy				
	Minimum Password Length	Maximum Password Age	Minimum Password Age	Force Logoff	Password History
	0 chars	42 days, 22 hours, 47 minutes, 31 seconds	no delay	never force	no history
3	Security Audit Policy				
	Auditing Policy			Success	Failure
	Audit account logon events		True	True	
	Audit account management		True	True	
	Audit directory service access		True	True	
	Audit logon events		False	False	
	Audit object access		False	False	
	Audit policy change		True	True	
	Audit privilege use		True	True	
	Audit process tracking		True	True	
	Audit system events		True	True	

Screenshot 103 – Sample report showing policies

1	Host machine IP and name
2	Password policy details for each host machine, including minimum password length and password history
3	List showing security audit policy details for each host machine

Use this report to:

- List password and security audit policy settings for each network host scanned.

Registry information

Scan reference: 192.168.100.2-192.168.100.254
Scan date & time: 29-Nov-2006 10:12

1	192.168.100.114 - VSDRIN-D2005	
	Operating System	Service Pack
	Windows XP	Gold
2	Node Name	Registry Entry
		~MHz : 2992
		CurrentBuildNumber : 2600
		CurrentType : Uniprocessor Free
		CurrentVersion : 5.1
		Default : 0409
		DriverDesc : Creative AudioPCI (ES1371,ES1373)(WDM)
		DriverDesc : VMware SVGA II
		Identifier : x86 Family 15 Model 3 Stepping 8
		InstallLanguage : 0409
		PathName : C:\WINDOWS
		ProductId : 55274-338-0879281-22184
		ProductName : Microsoft Windows XP
		RegisteredOrganization : ts
		RegisteredOwner : ts
		SoftwareType : SYSTEM
		SourcePath : D:\ENGLISH\WINXP\PRO\386
		SystemRoot : C:\WINDOWS
		VendorIdentifier : GenuineIntel
	Run	MsmqIntCert : regsvr32 /s mqrt.dll
	Run	VMware Tools: C:\Program Files\VMware\VMware Tools\VMwareTray.exe
	Run	VMware User Process: C:\Program Files\VMware\VMware Tools\VMwareUser.exe

Screenshot 104 – Sample report showing registry information

1	Host machine IP and name
2	List of registry entry details for each host machine

Use this report to:

- List system related registry information for each network host scanned.

Results comparison

Network security log by date

1 → **Compare Scans from Dates:** 11/28/2006 3:42:33PM and 11/28/2006 3:43:10PM
Scan reference: file:list.txt
Scan profile: Default

2 → **MARK**
 Missing hotfixes

3 → A new patch needs to be installed: Security Update for Windows XP (KB899589).
 A new patch needs to be installed: Security Update for Windows XP (KB899591).
 A new patch needs to be installed: Security Update for Windows XP (KB900725).
 A new patch needs to be installed: Security Update for Windows XP (KB901017).
 A new patch needs to be installed: Security Update for Windows XP (KB901214).
 A new patch needs to be installed: Security Update for Windows XP (KB902400).
 A new patch needs to be installed: Security Update for Windows XP (KB904706).
 A new patch needs to be installed: Security Update for Windows XP (KB905414).
 A new patch needs to be installed: Security Update for Windows XP (KB905749).
 A new patch needs to be installed: Security Update for Windows XP (KB908519).
 A new patch needs to be installed: Security Update for Windows XP (KB908531).
 A new patch needs to be installed: Security Update for Windows XP (KB911280).
 A new patch needs to be installed: Security Update for Windows XP (KB911280).
 A new patch needs to be installed: Security Update for Windows XP (KB911562).
 A new patch needs to be installed: Security Update for Windows XP (KB911927).
 A new patch needs to be installed: Security Update for Windows XP (KB912919).
 A new patch needs to be installed: Security Update for Windows XP (KB913580).
 A new patch needs to be installed: Security Update for Windows XP (KB914388).
 A new patch needs to be installed: Security Update for Windows XP (KB914389).
 A new patch needs to be installed: Security Update for Windows XP (KB917159).
 A new patch needs to be installed: Security Update for Windows XP (KB917344).
 A new patch needs to be installed: Security Update for Windows XP (KB917953).
 A new patch needs to be installed: Security Update for Windows XP (KB918439).
 A new patch needs to be installed: SQL Server 2000 Service Pack 4 for Database Components.
 A new patch needs to be installed: Windows Malicious Software Removal Tool - July 2006 (KB890830).
 Hotfix/patch has been installed: MDAC 2.8 Service Pack 1.
 Hotfix/patch has been installed: Security Update for Windows Media Player9 (KB911565).
 Hotfix/patch has been installed: Security Update for Windows XP (KB901190).
 Hotfix/patch has been installed: Windows XP Service Pack 2.

Screenshot 105 – Sample report showing network security log by date

1	Network security scans to be compared
2	Host machine on which the comparison was made
3	List of differences found between comparisons for each host machine. Differences are grouped by category, including backdoors, missing hotfixes, password policy, USB devices and applications

Use this report to:

- Compare results of consecutive scans that have a common profile and target, grouped by scan date.

Network security log by host

1 → MARK

2 → **Compare Scans from Dates :** 11/28/2006 3:42:33PM and 11/28/2006 3:43:10PM
Scan reference : file:list.txt
Scan profile : Default

3 → **General Host**
 At least one of the two scans was not completed.

TCP Ports
 New TCP port is open: 9593.
 New TCP port is open: 9594.
 New TCP port is open: 9595.
 New TCP port is open: 31770.

UDP Ports
 New UDP port is open: 123.
 New UDP port is open: 123.
 New UDP port is open: 137.
 New UDP port is open: 137.
 New UDP port is open: 138.
 New UDP port is open: 138.
 New UDP port is open: 445.
 New UDP port is open: 445.
 New UDP port is open: 500.
 New UDP port is open: 1032.
 New UDP port is open: 1038.
 New UDP port is open: 1900.
 New UDP port is open: 1900.
 New UDP port is open: 1943.
 New UDP port is open: 2431.
 New UDP port is open: 3527.
 New UDP port is open: 4500.
 New UDP port is open: 9595.

Network Cards
 The virtual device 'VMware Virtual Ethernet Adapter for VMnet8' (MAC: '00:50:56:C0:0008') was added.
 The virtual device 'VMware Virtual Ethernet Adapter for VMnet1' (MAC: '00:50:56:C0:0001') was added.
 The virtual device 'Packet Scheduler Miniport' (MAC: '00:0E:0C:3C:A8:35') was added.
 The physical wired device 'Generic Marvell Yukon Chipset based Gigabit Ethernet Controller' (MAC: '00:0E:0C:3C:A8:35') was added.
 The virtual device 'Packet Scheduler Miniport' (MAC: '00:0E:0C:3C:A8:36') was added.
 The physical wired device 'Intel(R) PRO/1000 MT Network Connection' (MAC: '00:0E:0C:3C:A8:36') was added.
 The virtual device 'Packet Scheduler Miniport' (MAC: '20:FF:20:52:4153') was added.
 The virtual device 'WAN Miniport (IP)' (MAC: '') was added.
 The virtual device 'Direct Parallel' (MAC: '') was added.
 The virtual device 'WAN Miniport (PPPOE)' (MAC: '33:50:6F:45:30:30') was added.
 The virtual device 'WAN Miniport (PPTP)' (MAC: '50:50:54:50:30:30') was added.
 The virtual device 'WAN Miniport (L2TP)' (MAC: '') was added.
 The software enumerated device 'RAS Async Adapter' (MAC: '') was added.

Screenshot 106 – Sample report showing network security log by host

1	Host machine on which the comparison was made
2	Network security scans which were compared
3	List of differences found between comparisons for each host machine. Differences are grouped by category, including backdoors, missing hotfixes, password policy, USB devices and applications

Use this report to:

- Compare results of consecutive scans that have a common profile and target, grouped by host machine.

Baseline changes comparison

The computer used as Comparison Standard

192.168.100.26 - CB

- 1 → **Scan Date:** 11/28/2006 3:47:54PM
Scan reference: file:list.txt
Scan Profile: Default

Operating System: Windows Server 2003
Service Pack:

Comparing Standard Computer with hosts from scan session

- 2 → **Scan date & time:** 11/28/2006 3:42:33PM
Scan reference: file:list.txt
Scan profile: Default

3 → 192.168.100.75 - MARK

Operating System	Service Pack
Windows XP	2

General Host

At least one of the two scans was not completed.
 Hostname has been changed: CB; before was: MARK.
 MAC has been changed: 00-02-44-5A-0E-DB; before was: 00-0E-0C-3C-A8-36.
 LAN manager has been changed: ; before was: Windows2000 LAN Manager.
 Another domain is being used now: ; before was: WORKGROUP.
 Computer usage has been changed: Member Server; before was: Workstation.
 Another service pack has been installed: ; before was: 2.

Screenshot 107 – Sample report showing security settings comparison

1	Details of the computer used as comparison standard, including scan date, and scan profile
2	List showing host machines with which the standard computer was compared
3	List of differences found when comparing the host machines with the standard computer. Differences are grouped by category, including backdoors, missing hotfixes, password policy, USB devices and applications

Use this report to:

- Compare results between a choused computer, used as benchmark, and host machines scanned with the same profile and having the same target.

Troubleshooting

Introduction

The troubleshooting chapter explains how you should go about resolving issues you have. The main sources of information available to users are:

- The manual – most issues can be solved by reading the manual.
- The GFI Knowledge Base – accessible from the GFI website.
- The GFI technical support site.
- Contacting the GFI technical support team by email at support@gfi.com.
- Contacting the GFI technical support team using our live support service at <http://support.gfi.com/livesupport.asp>.
- Contacting our technical support team 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 technical 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 technical support team. 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 click the troubleshooter\support folder, located under the main program directory, compress the files in ZIP format, and send the generated ZIP file to 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 technical support via web chat

You may also request technical support via 'LiveSupport (web chat)'. You can contact the GFI technical 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 technical support via phone

You can also contact GFI by phone for technical support. Please check our website for the correct numbers to call, depending on where you are located, and for our opening times.

Technical 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 technical 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

C

configuration settings 49, 95
custom reports 8, 11, 23, 32,
33

D

data filters 11, 23
database backend 15
database source 47, 49
default reports 8, 17, 21
distribution of reports 10

E

email settings 16
export reports 10

F

favorite reports 8, 21, 32
filter conditions 25
framework 6, 7, 8, 10, 12

I

installation 10, 12, 16, 46, 53

L

license 11, 14, 16, 39, 53, 54

N

navigation button 8, 9, 17,
18, 19, 22, 23, 28, 31,
32, 36, 37, 38, 39, 40,
41, 43, 44, 46, 47, 53,
54, 55

P

product ReportPack 8
Product Selection drop down
list 16, 53, 54, 55

R

Report scheduling 8, 10

S

schedule activity monitor 39
scheduled reports 9, 10, 38,
40
security scan 25
System requirements 12

T

Troubleshooting 95

U

user interface 8, 38, 39, 46

W

wizard 12, 16, 41, 95