# Contents

## Introduction
- 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
- 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
- Introduction ....................................................................................... 17
- Generating a default report ................................................................. 17
- Analyzing the generated report .......................................................... 20
- Adding default reports to the list of favorite reports ......................... 21

## Custom reports
- 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
- 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
- Introduction ....................................................................................... 46
- Configuring database source: Microsoft SQL Server .......................... 47
- Configuring database source: Microsoft Access .................................. 47
- Viewing the current database source settings .................................... 49
General options

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 host .................................................................................. 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

About GFI ReportCenter

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.
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.

<table>
<thead>
<tr>
<th>Scheduled Reports</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.</td>
</tr>
<tr>
<td>Help</td>
<td>Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.</td>
</tr>
</tbody>
</table>
| Report Pane | Use this multi-functional pane to:  
  - View and analyze generated reports  
  - Maintain the scheduled reports list  
  - Explore samples and descriptions of default reports. |
| 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). |
| 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 the online registration form on the GFI website ([http://www.gfi.com/downloads/register.aspx?pid=lanssrp&vid=8rp&lid=en](http://www.gfi.com/downloads/register.aspx?pid=lanssrp&vid=8rp&lid=en)) when downloading the product. 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/purchasing.htm](https://www.gfi.com/pages/purchasing.htm)). 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, 2008, VISTA (SP1), XP (SP3) 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 `languardnss8rp.exe`. As soon as the welcome dialog is displayed, click **Next** to start the installation.
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.

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.

![Screenshot 4 - Licensing details dialog](image)

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.

![Screenshot 5 – SQL Server selection dialog](image)

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. `\LNSServer\GFI\ScanResults.mdb`).

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.
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.

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.
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.
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.
Getting started: Default reports

GFI ReportCenter

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

- Day

- Month

- Date range

- ‘From’ – 01/14/2007 0:00:00.

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

3. Select the ‘Date range’ option and specify the required parameters:
   - ‘From’ – 01/14/2007 0:00:00.

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

4. Click Finish to generate the report.
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

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 want 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’.

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.
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.

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.
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.
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:
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:
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.

<table>
<thead>
<tr>
<th>Filters applied</th>
<th>Data output</th>
</tr>
</thead>
</table>
| Filter 1 and Filter 2 | The report will show:  
  - 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:  
  - All scan data related to 'Windows XP' – (no matter which host it belongs to)  
  AND  
  - 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.
4. Select the ‘Scans over a date/month range’ option and click Next.

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.
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.

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

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

4. Specify the report scheduling parameters (date/time/frequency). Click on **Next** to continue.
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:
<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Adobe Acrobat (.PDF)</td>
<td>Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.</td>
</tr>
<tr>
<td>2  MS Excel (.XLS)</td>
<td>Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.</td>
</tr>
<tr>
<td>3  MS Word (.DOC)</td>
<td>Use this format if you want to access this report using Microsoft Word.</td>
</tr>
<tr>
<td>4  Rich text format (.RTF)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Configuring report export to file options

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

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

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:

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

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](image-url)

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

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 the 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'.

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.

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

- Last Scan
- Particular Scan
- Scans over a date/time range

3. Select the option ‘Scans over a date/time range’ for data to be covered by this report and click Next.
4. Select the option ‘Relative’ and from the provided drop down list select ‘Last month’. Click on **Next** to proceed to the next dialog.

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

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

![Screenshot 41 - Advanced Settings dialog: Send by email settings button](image1)

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.

![Screenshot 42 - Report distribution options](image2)
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.

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.

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.
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\GFILANguard Network Security Scanner 8.0\Data\scanresults.mdb`).

5. Click on **OK** to finalize your configuration settings.
Viewing the current database source 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:

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
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:

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.
Importing the configuration

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

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.
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:

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.
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:
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-2005 10:12]

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
Screenshot 57 – Sample report showing network vulnerability summary

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

Vulnerability Distribution (by Category)

Screenshot 58 – Sample report showing network vulnerability summary

Chart displaying vulnerability categories and their distribution
Appendix: GFI LANguard Network Security Scanner default reports

GFI ReportCenter

Screenshot 59 – Sample report showing network vulnerability summary

Chart displaying the vulnerability distribution over time

Top 10 Most Common Vulnerabilities

Vulnerability: Access Denied (NAT)
Product: Unknown
Timestamp: 2002-01-01
References: Unknown
Type: Registry
Severity: Low
Count: 10

Vulnerability: Session Logon Credentials
Product: Unknown
Timestamp: 2002-01-01
References: Unknown
Type: Registry
Severity: Low
Count: 18

Vulnerability: ACL/TunnelServer
Product: Unknown
Timestamp: 2002-01-01
References: Unknown
Type: Registry
Severity: Low
Count: 18

Vulnerability: DCOM is enabled
Product: Unknown
Timestamp: 1994-05-07
References: CVE-1993-0558
Type: Registry
Severity: Low
Count: 18

Vulnerability: Last logged-in username visible
Product: Unknown
Timestamp: 2002-01-01
References: Unknown
Type: Registry
Severity: Low
Count: 18

Vulnerability: LM hash
Product: Unknown
Timestamp: 2002-01-01
References: Unknown
Type: Registry
Severity: Medium
Count: 13

Vulnerability: FTP anonymous access allowed
Product: Unknown
Timestamp: Unknown
References: Unknown
Type: FTP
Severity: Count
Count: 11

Vulnerability: DCOM-Admin: Hyperlink Object Remote OLE/COM Vulnerability
Product: Unknown
Timestamp: 2003-08-11
References: CVE-2003-0696
Type: Sandbox
Severity: High
Count: 8

Vulnerability: Netscape: Netscape PageServices
Product: Unknown
Timestamp: 1994-02-11
References: CVE-1998-0255
Type: Web
Severity: Count
Count: 8

Vulnerability: DCOM-94: Server 2005 RPC/DCOM Buffer Overflow
Product: Unknown
Timestamp: 2004-04-03
References: CVE-2003-0693
Type: RPC
Severity: High
Count: 6

Top 10 Most Vulnerable Products

<table>
<thead>
<tr>
<th>Product</th>
<th>Severity Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product 1</td>
<td>16</td>
</tr>
<tr>
<td>Product 2</td>
<td>34</td>
</tr>
<tr>
<td>Product 3</td>
<td>22</td>
</tr>
</tbody>
</table>

Screenshot 60 – Sample report showing network vulnerability summary
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

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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Total</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
<th>VSS</th>
<th>VMS</th>
<th>VSS/MS</th>
<th>FTS</th>
<th>VMS/FTS</th>
<th>AppIS</th>
<th>GSS</th>
<th>GSS/IS</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10.100.100.10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10.100.100.10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>192.168.100.15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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:** 20-Nov-2006 10:52

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Severity Distribution</th>
<th>Vulnerability Category</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>D-LINK DP-300X405</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SP D-Link</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Windows</td>
<td>28</td>
<td>10</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>24</td>
<td>6</td>
</tr>
<tr>
<td>Windows 95</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Windows 95/98/4.0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Windows NT</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>Windows Server 2003 SP 1</td>
<td>17</td>
<td>13</td>
</tr>
<tr>
<td>Windows Server 2003 SP 2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Windows XP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Windows XP SP 1</td>
<td>18</td>
<td>10</td>
</tr>
<tr>
<td>Windows XP SP 2</td>
<td>14</td>
<td>7</td>
</tr>
<tr>
<td>Windows XP SP 3</td>
<td>127</td>
<td>68</td>
</tr>
</tbody>
</table>

**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.
Appendix: GFI LANguard Network Security Scanner default reports

GFI ReportCenter

Security scans history

<table>
<thead>
<tr>
<th>Most Scanned Systems</th>
<th>Least Scanned Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Host Name</td>
</tr>
<tr>
<td>00.186.32.16</td>
<td>Windows2000</td>
</tr>
<tr>
<td>192.168.23.4</td>
<td>TestComp</td>
</tr>
<tr>
<td>00.184.37.38</td>
<td>TestComp</td>
</tr>
<tr>
<td>00.184.37.13</td>
<td>FinanceDep</td>
</tr>
<tr>
<td>00.184.37.12</td>
<td>Jack</td>
</tr>
<tr>
<td>00.184.37.19</td>
<td>TestFirewall_PC1</td>
</tr>
<tr>
<td>00.185.37.42</td>
<td>HomeA2</td>
</tr>
<tr>
<td>00.184.37.23</td>
<td>MASTERSERV</td>
</tr>
<tr>
<td>00.184.37.10</td>
<td>Jamoplit</td>
</tr>
<tr>
<td>00.184.37.14</td>
<td>TestFirewall_PC4</td>
</tr>
</tbody>
</table>

Most Used Profiles

<table>
<thead>
<tr>
<th>Profile</th>
<th>Profile Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Scan</td>
<td>4</td>
</tr>
<tr>
<td>Webcheck</td>
<td>2</td>
</tr>
<tr>
<td>Trojan Ports</td>
<td>2</td>
</tr>
<tr>
<td>Software Audit</td>
<td>3</td>
</tr>
<tr>
<td>Missing Patches</td>
<td>1</td>
</tr>
</tbody>
</table>

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 Scanner for Each System

<table>
<thead>
<tr>
<th>IP</th>
<th>Host Name</th>
<th>Last Scan Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.186.100.5</td>
<td>N/A</td>
<td>11/2006 07:15 AM</td>
</tr>
<tr>
<td>192.186.100.11</td>
<td>N/A</td>
<td>11/2006 09:51 AM</td>
</tr>
<tr>
<td>192.186.100.15</td>
<td>CRISTI</td>
<td>11/2006 09:11 AM</td>
</tr>
<tr>
<td>192.186.100.20</td>
<td>TESTATION</td>
<td>11/2006 09:12 AM</td>
</tr>
<tr>
<td>192.186.100.21</td>
<td>N/A</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>VIRTUAL2</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>QADEV2</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>N/A</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
<tr>
<td>192.186.100.220</td>
<td>NA</td>
<td>11/2006 10:25 AM</td>
</tr>
</tbody>
</table>

Scan Listing

<table>
<thead>
<tr>
<th>Scan Date/Time</th>
<th>Target</th>
<th>Profile</th>
<th>Profile</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/2006 03:37 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>11/2006 03:42 AM</td>
<td>127.6.0.11</td>
<td>Default</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
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: 1/29/2008 10:12:25AM

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>FTP</th>
</tr>
</thead>
</table>

| Vulnerability | FTP anonymous access allowed— |
| Product       | N/A |
| Severity      | Low |
| Timestamp     | N/A |

Affected hosts:
- 192.168.100.79: Windows XP
- 192.168.100.81: Windows 2000
- 192.168.100.82: Windows XP

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 10:12:58AM

1. Operating System: Windows XP
   Service Pack: 26

2. Total Host Vulnerabilities: 18
   Total Network Vulnerabilities: 102
   Total Host / Total Network: 5.64%

3. Category: Information
   Product: N/A
   Timestamp: N/A
   Severity: N/A

4. Category: Registry
   Product: N/A
   Timestamp: 2002-01-01
   Severity: Low

Use this report to:
- List the vulnerabilities detected for each host machine on the network.
- Vulnerability count for each host, also shown as a percentage of total vulnerabilities detected on the network.
- List of vulnerability details for each host, including name, description and severity.
- Chart displaying percentage of vulnerabilities detected on each host compared to total vulnerabilities detected on the network.

Screenshot 67 – Sample report showing vulnerability listing by host
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: NA

Vulnerability: A connection could be opened using account Administrator without password —
Category: Service
Severity: High
Timestamp: NA
Affected Hosts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.24</td>
<td>STEFAN</td>
<td>Windows</td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability: A modem is installed on this computer—
Category: Information
Severity: NA
Timestamp: 2002/01/01
Affected Hosts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.12</td>
<td>BOOGIE</td>
<td>Windows XP</td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability: Administrator account exists—
Category: Information
Severity: NA
Timestamp: NA
Affected Hosts

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.169.100.8</td>
<td>LUCIAN</td>
<td>Windows XP</td>
<td>2</td>
</tr>
</tbody>
</table>

Name: User ASPNET never logged on
Description: This account should be removed 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 10:12:25 AM

1. SEVERITY: High

Vulnerability: A connection could be opened using account Administrator with password —
Category: Service
Product: N/A
Timestamp: N/A
Affected Hosts:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.2</td>
<td>STEFAN</td>
<td>Windows</td>
<td></td>
</tr>
</tbody>
</table>

2. SEVERITY: High

Vulnerability: Application not up to date Ad-Aware SE Personal Edition —
Category: Security Products
Product: N/A
Timestamp: N/A
Affected Hosts:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.20</td>
<td>DABRVA</td>
<td>Windows X.P</td>
<td>2</td>
</tr>
</tbody>
</table>

Vulnerability: Application not up to date F-Prot AntiVirus for Windows —
Category: Security Products
Product: N/A
Timestamp: N/A
Affected Hosts:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.99</td>
<td>MARKOP</td>
<td>Windows X.P</td>
<td>2</td>
</tr>
</tbody>
</table>

3. SEVERITY: Low

Vulnerability: Alert service enabled —
Category: Services
Product: N/A
Timestamp: 10/07/2001
Affected Hosts:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Serv. Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.150</td>
<td>150SERVER</td>
<td>Windows 2000</td>
<td>Unknown</td>
</tr>
<tr>
<td>192.168.100.99</td>
<td>LUCAND</td>
<td>Windows XP</td>
<td>2</td>
</tr>
<tr>
<td>192.168.100.9</td>
<td>LUCAND</td>
<td>Windows XP</td>
<td>2</td>
</tr>
<tr>
<td>192.168.100.90</td>
<td>LUCAND</td>
<td>Windows XP</td>
<td>4</td>
</tr>
</tbody>
</table>

Screenshot 69 – Sample report showing vulnerability listing by severity

<table>
<thead>
<tr>
<th>Severity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability details for each severity level, including name and description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List of host machines affected by vulnerabilities detected for each severity level</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
</tr>
</tbody>
</table>

Use this report to:

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

Screenshot 70 – Sample report showing open trojan ports by cost

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

Screenshot 71 – Sample report showing open trojan ports
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**

<table>
<thead>
<tr>
<th>Scan reference:</th>
<th>127.0.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan date &amp; time:</td>
<td>29-Nov-2006 15:37</td>
</tr>
</tbody>
</table>

**Host machine details on which vulnerabilities reported by SANS were detected**

1. Screenshot 72 – Sample report showing top SANS vulnerabilities status

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

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

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

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

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-Mar-2006 10:12

![Chart displaying the number of installed and missing patches, grouped by severity](image)

<table>
<thead>
<tr>
<th>Status</th>
<th>Total</th>
<th>Critical</th>
<th>Important</th>
<th>Moderate</th>
<th>Low</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>936</td>
<td>141</td>
<td>179</td>
<td>62</td>
<td>4</td>
<td>70</td>
</tr>
<tr>
<td>Missing</td>
<td>695</td>
<td>153</td>
<td>119</td>
<td>68</td>
<td>5</td>
<td>42</td>
</tr>
<tr>
<td>Totals</td>
<td>1631</td>
<td>294</td>
<td>298</td>
<td>130</td>
<td>11</td>
<td>112</td>
</tr>
</tbody>
</table>

**Chart displaying the number of installed and missing service packs**

![Chart displaying the number of installed and missing service packs](image)

*Screenshot 75 – Sample report showing network patching status*

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Chart displaying the number of installed and missing patches, grouped by severity</td>
</tr>
<tr>
<td>2</td>
<td>Chart displaying the number of installed and missing service packs</td>
</tr>
</tbody>
</table>
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: 192.168.100.1:192.168.100.254
Scan date & time: 29-Nov-2006 10:12

GFI LANguard Network Security Scanner default reports
GFI ReportCenter

Bulletin ID Description Posted Date Severity

Not Available Windows Malicious Software Removal Tool July 2006 2006-07-11 N/A
Not Available Windows XP Service Pack 2 2006-04-25 N/A
MS04-022 Security Update for Windows XP (KB903807) 2006-04-12 Critical
MS04-024 Security Update for Internet Explorer 5 SP1 (KB822052) 2006-04-11 Moderate
Not Available Update Roll Up 1 for Microsoft Windows XP (KB826255) 2006-04-13 N/A
MS04-021 Security Update for Windows XP (KB903222) 2005-03-25 Moderate
MSS01-051 QR11142 Security Update for Windows XP Service Pack 1 2005-02-01 Important
MS04-011 Security Update for Windows XP (KB903722) 2005-02-10 Critical
MS04-012 Security Update for Windows XP (KB904716) 2005-02-10 Important
MS04-013 Security Update for Microsoft Data Access Components (KB902953) 2005-02-07 Critical
MS04-014 Security Update for Windows XP (KB904016) 2005-02-12 Critical
MS04-015 Security Update for Windows XP (KB903546) 2005-02-08 Important
MS04-016 Security Update for Windows XP (KB903877) 2004-12-15 Critical
MS04-017 Security Update for Windows XP (KB903193) 2004-12-15 Critical
MS04-018 Security Update for Windows XP (KB903522) 2004-11-20 Important
MS04-019 Cumulative Security Update for Internet Explorer 5 Service Pack 1 (KB864347) 2004-11-20 Critical
MS04-020 Security Update for Windows XP (KB902971) 2004-11-20 Important
MS04-021 Security Update for Windows XP (KB810247) 2004-10-04 Critical
MS04-022 Security Update for Windows XP (KB835945) 2004-07-20 Important
MS04-023 Security Update for Windows XP (KB837193) 2004-07-23 Important
MS04-024 Security Update for Windows XP (KB823844) 2004-07-06 Critical

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: 014909
   Bulletin ID: MS00-080
   Posted Date: 2000-07-11
   Severity: Critical
   Description: Security Update for Windows 2000 (KB940058)

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Host Name</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.254</td>
<td>CB0</td>
<td>4</td>
</tr>
</tbody>
</table>

2. Patch: 8806603
   Bulletin ID: Not Available
   Posted Date: 2000-07-11
   Severity: N/A
   Description: Windows Update for Software Removal Tool – July 2000 (KB806603)

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Host Name</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.160.100.200</td>
<td>CB0</td>
<td>4</td>
</tr>
</tbody>
</table>

3. Patch: 017394
   Bulletin ID: MS08-022
   Posted Date: 2008-06-12
   Severity: Moderate
   Description: Security Update for Windows Server 2003 (KB917394)

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Host Name</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.160.100.200</td>
<td>TESTATION</td>
<td>1</td>
</tr>
<tr>
<td>192.160.100.200</td>
<td>FSERVER</td>
<td>Gold</td>
</tr>
</tbody>
</table>

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: 917519
   Bulletin ID: MS09-059
   Posted Date: 2009-07-11
   Description: Security Update for Windows Server 2003 (KB917519)

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.200</td>
<td>TESTATION</td>
<td>Windows Server 2003</td>
<td>1</td>
</tr>
</tbody>
</table>

2. Patch: 914599
   Bulletin ID: MS09-032
   Posted Date: 2009-07-11
   Description: Security Update for Windows Server 2003 (KB914599)

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Host Name</th>
<th>Operating System</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.200</td>
<td>TESTATION</td>
<td>Windows Server 2003</td>
<td>1</td>
</tr>
</tbody>
</table>

3. Patch: 914988
   Bulletin ID: MS09-065
   Posted Date: 2009-07-11
   Description: Security Update for Windows Server 2003 (KB914988)

<table>
<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>

4. Patch: 917519
   Bulletin ID: MS09-059
   Posted Date: 2009-07-11
   Description: Security Update for Windows Server 2003 (KB917519)

<table>
<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>

Screenshot 79 – Sample report showing missing patches grouped by severity
Appendix: GFI LANguard Network Security Scanner default reports

GFI ReportCenter

Use this report to:

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

### Installed patches grouped by host

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack</th>
<th>Patch Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td>2</td>
<td>17</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bulletin ID</th>
<th>Description</th>
<th>Date</th>
<th>Severity</th>
<th>Uninstallable</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS04-006</td>
<td>Security Update for Windows Media Player (KB8411059)</td>
<td>2006-02-14</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>MS05-015</td>
<td>Security Update for Windows XP (KB926406)</td>
<td>2005-05-15</td>
<td>Important</td>
<td>Yes</td>
</tr>
<tr>
<td>MS06-001</td>
<td>Security Update for Internet Explorer (KB961545)</td>
<td>2006-04-12</td>
<td>Critical</td>
<td>Yes</td>
</tr>
<tr>
<td>MS06-020</td>
<td>Microsoft Security Update for Internet Explorer (KB9682160)</td>
<td>2006-04-12</td>
<td>Important</td>
<td>Yes</td>
</tr>
<tr>
<td>MS06-022</td>
<td>Security Update for Internet Explorer (KB923798)</td>
<td>2006-02-06</td>
<td>Important</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Screenshot 80 – Sample report showing installed patches grouped by host

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Patch ID</th>
<th>Bulletin ID</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>569401</td>
<td>Not Available</td>
<td>N/A</td>
<td>Windows Server 2003 Security Update 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Patch ID</th>
<th>Bulletin ID</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>569401</td>
<td>Not Available</td>
<td>N/A</td>
<td>Windows Server 2003 Security Update 2</td>
</tr>
</tbody>
</table>

74 • 7B Appendix: GFI LANguard Network Security Scanner default reports
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: 192.168.100.2-192.168.100.354
Scan date & time: 29-Nov-2006 10:12

1. Patch: 098498  Bulletin ID: NotAvailable  Posted Date: 2000-02-01
   Uninstallable: No
   Description: NDAC 2.8 Service Pack 1
   Host IP        Host Name     Operating System   Severity   Service Pack
   192.168.100.13  STELU         Windows XP   64        1
   192.168.100.54  MACHINE       Windows XP   64        2
   192.168.100.24  BORISI         Windows XP   64        1
   192.168.100.170 BOGISXP        Windows XP   64        2
   192.168.100.26  CALDEV         Windows XP   64        2
   192.168.100.75  MARKS          Windows XP   64        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   IsScheduled
   Files: Attached file.exe.config

2. Date Started  Date Ended  Completed Status  Type   IsScheduled
   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

*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

*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: 80.143.32.21/2
Scan date & time: 2/3/2007 2:30:23PM

Top 10 Systems with Unauthorized Applications

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
<th>Unauthorized Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>80.143.32.211</td>
<td>Andrew</td>
<td>2</td>
</tr>
<tr>
<td>80.143.32.233</td>
<td>Andy</td>
<td>1</td>
</tr>
</tbody>
</table>

Top 10 Unauthorized Applications

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Application Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samba Tools</td>
<td>2</td>
</tr>
<tr>
<td>Note Suite</td>
<td>1</td>
</tr>
</tbody>
</table>

Systems with Security Applications

<table>
<thead>
<tr>
<th>Security Applications</th>
<th>Systems Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems with Security Applications Not Updated</td>
<td>1</td>
</tr>
<tr>
<td>Systems without Any Security Application</td>
<td>1</td>
</tr>
</tbody>
</table>

Top 20 Most Installed Applications

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Publisher</th>
<th>Occurrence</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader</td>
<td>Adobe Systems Inc.</td>
<td>2</td>
<td>Windows XP</td>
</tr>
<tr>
<td>80.143.32.211</td>
<td>Andrew</td>
<td>Windows 2000</td>
<td></td>
</tr>
<tr>
<td>80.143.32.233</td>
<td>Andy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| VMware Tools     | VMware, Inc. | 1 | Windows 2008 |
| 80.143.32.211 | Andrew |

| VMware Workstation | VMware, Inc. | 1 | Windows 2008 |
| 80.143.32.211 | Andrew |

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 10:50:55

---

**Operating System**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Number of Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>[unknown]</td>
<td>1</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>1</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>2</td>
</tr>
<tr>
<td>Windows XP</td>
<td>2</td>
</tr>
</tbody>
</table>

---

**Service Pack distribution**

---

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack</th>
<th>Number of Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>[unknown]</td>
<td>[unknown]</td>
<td>1</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>Gold</td>
<td>1</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Windows XP</td>
<td>Gold</td>
<td>2</td>
</tr>
</tbody>
</table>

---

*Screenshot 87 – Sample report showing operating system and service pack distribution*
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:** No list.txt  
**Scan date & time:** 1/9/2007 2:30:10PM

### System Details

<table>
<thead>
<tr>
<th>Host machine IP and name</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.100.75: MARKIK</td>
</tr>
</tbody>
</table>

### Computer Properties

- **MAC Address:** 00:06:00:2C:A6:20 (Intel Corporation)  
- **Time to live:** 120 (020)  
- **Network & role:** Workstation  
- **Domain:** WORKGROUP  
- **LAN manager:** Windows 2000 LAN Manager

### Uptime

<table>
<thead>
<tr>
<th>Time of Day</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>321 ms</td>
</tr>
<tr>
<td>603</td>
<td>955 ms</td>
</tr>
</tbody>
</table>

### Disk Utilization

<table>
<thead>
<tr>
<th>Name</th>
<th>Total Space</th>
<th>Free Space</th>
<th>File System Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>394MB</td>
<td>294MB</td>
<td>FAT 32</td>
</tr>
</tbody>
</table>

### Groups and Users

- **Administrators:**  
  - Members: MARKILIN, MONITOR, USER, MARKILIN, MARKILIN/Administrator

- **Guests:**  
  - Members: MARKILIN, MONITOR, USER, MARKILIN, MARKILIN/Administrator

- **Users:**  
  - Members: MARKILIN, MONITOR, USER, MARKILIN, MARKILIN/Administrator

  **Help Services Group:**  
  - Members: MARKILIN, MONITOR, USER, MARKILIN, MARKILIN/Administrator

  **VMware:**  
  - Members: MARKILIN, VMware User Group

- **Administrators:**  
  - Privileges: Administrator(1)  
  - Flags: SCRIPT_NORMAL_ACCOUNT  
  - Comment: Built in account for administering the computer  
  - Last logon: 26 Nov 2000, 15:41:50  
  - Passwordage: 10 days, 30 minutes, 10 seconds  
  - # Logins: 2,225  
  - Bad Password Count: 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
### SNMP Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object ID</td>
<td>1.3.6.1.4.1.111.1.3.1.3 (NT Domain Controller)</td>
</tr>
<tr>
<td>System</td>
<td>Hardware: 080 Family 15 Model 4 Stepping 1 AT/AT COMPATI</td>
</tr>
<tr>
<td>System Name</td>
<td>PROJECT</td>
</tr>
<tr>
<td>Setup Time</td>
<td>10 minutes 45 seconds</td>
</tr>
<tr>
<td>Vendor</td>
<td>Microsoft</td>
</tr>
</tbody>
</table>

### Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Status</th>
<th>Startup Type</th>
<th>Account Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Running</td>
<td>Automatic</td>
<td>NT AUTHORITY\LocalService</td>
</tr>
<tr>
<td>Application Layer Gateway</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Management</td>
<td></td>
<td>Manual</td>
<td>NT AUTHORITY\LocalService</td>
</tr>
<tr>
<td>HTTP Service</td>
<td></td>
<td>Stopped</td>
<td>NT AUTHORITY\NetworkService</td>
</tr>
<tr>
<td>ASP .NET State Service</td>
<td></td>
<td>Stopped</td>
<td>NT AUTHORITY\NetworkService</td>
</tr>
<tr>
<td>Windows Audio</td>
<td></td>
<td>Running</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>IRC</td>
<td></td>
<td>Stopped</td>
<td>LocalSystem</td>
</tr>
<tr>
<td>Desktop Broker</td>
<td></td>
<td>Running</td>
<td>LocalSystem</td>
</tr>
</tbody>
</table>

### Processes

<table>
<thead>
<tr>
<th>PID</th>
<th>User Name</th>
<th>Command Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>LOCALSERVICE</td>
<td>C:\WINNT\System32\calc.exe</td>
</tr>
<tr>
<td>2005</td>
<td>Administrator</td>
<td>C:\WINNT\System32\calc.exe</td>
</tr>
</tbody>
</table>

**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
### Devices

<table>
<thead>
<tr>
<th>USB Devices</th>
<th>Description</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Root Hub</td>
<td>USB Root Hub</td>
<td>Standard USB Host Controller</td>
</tr>
<tr>
<td>USB Root Hub</td>
<td>USB Root Hub</td>
<td>Standard USB Host Controller</td>
</tr>
<tr>
<td>USB Root Hub</td>
<td>USB Root Hub</td>
<td>Standard USB Host Controller</td>
</tr>
</tbody>
</table>

There were no Blacklisted USB Devices vulnerabilities detected.

### Virtual Devices

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>DHCP</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Minipub (LZTP)</td>
<td></td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>WAN Minipub (PPPoE)</td>
<td></td>
<td>False</td>
<td>60:50:50:50:50:50</td>
</tr>
<tr>
<td>WAN Minipub (PPTP)</td>
<td></td>
<td>False</td>
<td>90:80:40:40:40:40</td>
</tr>
</tbody>
</table>

There were no Blacklisted Wireless Devices vulnerabilities detected.

### Shares

<table>
<thead>
<tr>
<th>Name</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0M$</td>
<td>Remote Admin</td>
</tr>
<tr>
<td>C0</td>
<td>share</td>
</tr>
<tr>
<td>C0</td>
<td>Default share</td>
</tr>
<tr>
<td>C0</td>
<td>NA</td>
</tr>
<tr>
<td>D</td>
<td>share</td>
</tr>
<tr>
<td>E</td>
<td>Default share</td>
</tr>
<tr>
<td>F</td>
<td>share</td>
</tr>
<tr>
<td>IP:0</td>
<td>Remote IPC</td>
</tr>
<tr>
<td>IP:0</td>
<td>Remote IPC</td>
</tr>
</tbody>
</table>

### Open Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>Full Port List</td>
</tr>
<tr>
<td>2002</td>
<td>Full Port List</td>
</tr>
<tr>
<td>2003</td>
<td>Full Port List</td>
</tr>
<tr>
<td>2004</td>
<td>Full Port List</td>
</tr>
<tr>
<td>1000</td>
<td>Full Port List</td>
</tr>
<tr>
<td>1000</td>
<td>Netbios Session Service</td>
</tr>
</tbody>
</table>

### Screenshot 90 – Sample report showing system information

- List showing USB devices, blacklisted USB devices, network cards and blacklisted wireless devices
- Share folder details for each host machine, including name and remarks
- Open port details for each host machine, including port number and name
GFI ReportCenter 7BAppendix: GFI LANguard Network Security Scanner default reports

• 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

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

Use this report to:
• List uptime for each host machine, grouped by network scan.

Host machine IP and name

Host machine details, including MAC address and domain

Host machine IP and name

Host machine details, including MAC address and domain

Operating System
Windows XP Service Pack 2

Time of Day
Up Time
00
100 ms
23
123 ms
05
1 hour, 13 minutes, 2 seconds, 735 ms

Screenshot 92 – Sample report showing computer properties

Host machine IP and name

Host machine details, including MAC address and domain

Operating System
Windows Server2003 Service Pack

Time of Day
Up Time
4
44 ms

Screenshot 93 – Sample report showing uptimes

Host machine IP and name

Uptime details for each host machine, including time of day and uptime value

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

Scan reference: 127.0.0.1
Scan date & time: 20-Nov-2006 15:37

1. 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: 20-Nov-2006 10:12

1. Use this report to:
   - List showing group details for each host machine, including name, description and members.
   - 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**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>obi-090.ep478</td>
<td>1.0.3.6.1.4.1.311.1.1.1.1.1 (NT Workstation)</td>
</tr>
<tr>
<td>hwRevision</td>
<td>Hardware id50 Family 15 Model 3 Stepping 3 AT/AT COMPAT</td>
</tr>
<tr>
<td>sysName</td>
<td>BOBY</td>
</tr>
<tr>
<td>sysUpTime</td>
<td>62 minutes, 29 seconds</td>
</tr>
<tr>
<td>Vendor</td>
<td>Microsoft</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Service Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Status</th>
<th>Startup Type</th>
<th>Account Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Service</td>
<td>Running</td>
<td>Automatic</td>
<td>NT AUTHORITY\LocalService</td>
</tr>
<tr>
<td>Application Layer Gateway Service</td>
<td>Status</td>
<td>Startup Type</td>
<td>Account Name</td>
</tr>
<tr>
<td>Application Management</td>
<td>Status</td>
<td>Startup Type</td>
<td>Account Name</td>
</tr>
<tr>
<td>SMTP</td>
<td>Status</td>
<td>Manual</td>
<td>NT AUTHORITY\LocalService</td>
</tr>
<tr>
<td>GC</td>
<td>Status</td>
<td>Manual</td>
<td>LocalSystem</td>
</tr>
</tbody>
</table>

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: 23-Nov-2006 10:12

1 192.168.100.14 - VSOPX04-22005

- Operating System: Windows XP
- Service Pack: Gold

- System Idle Process
- Thread Count: 1

2 192.168.100.14 - VSOPX04-22005

- Process ID: 4
- User Name: SYSTEM
- Domain: NT AUTHORITY
- Handle Count 340
- Thread Count: 49
- Priority: 6

Reference
- PID: 248
- PPID: 1216
- User Name: SYSTEM
- Path: C:\Program Files\Common Files\Microsoft Shared\WINDEBUG\debugmd.exe
- Domain: NT AUTHORITY
- Command Line: "C:\Program Files\Common Files\Microsoft Shared\WINDEBUG\debugmd.exe"
- Handle Count: 70
- Thread Count: 8
- Priority: 8

Screenshot 98 – Sample report showing processes

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host machine IP and name</td>
</tr>
<tr>
<td>2</td>
<td>Process details for each host machine, including process ID and account name</td>
</tr>
</tbody>
</table>

Use this report to:

- List process properties for each host machine.
Appendix: GFI LANguard Network Security Scanner default reports

GFI ReportCenter

Devices

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

1. **Operating System**
   - Windows XP
   - Service Pack: Gold

2. **USB Devices**
   - USB Root Hub
     - Description: USB Root Hub
     - Manufacturer: (Standard USB Host Controller)
     - Status: Plugged in

3. There were no Blacklisted USB Devices vulnerabilities detected.

4. **Network Devices**
   - **Wireless Devices**
     - Wireless Adapter: 00:0C:29:10:0A:07
     - MAC Address: 00:0C:29:10:0A:07
     - DHCP Set: False
     - Status: Plugged in

   - **Blacklisted wireless devices**
     - Status: Plugged in

   - **Active Devices**
     - **AMD PCIET 1000 NIC Ethernet Adapter - Packet Scheduler**
       - MAC Address: 00:0C:29:10:0A:07
       - DHCP Set: False
       - 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. **Operating System**
   - Windows XP
   - Service Pack: Gold

2. **Network Devices**
   - **Shares**
     - Admins
     - CS
     - IPC

**Screenshot 100 – Sample report showing shares**
Use this report to:

- List information on shared folders for each host machine.

### Open ports

<table>
<thead>
<tr>
<th>Scan reference:</th>
<th>192.168.100.2-192.168.100.254</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan date &amp; time:</td>
<td>11/23/2006 10:11:19PM</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Operating System: Windows XP</th>
</tr>
</thead>
</table>

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.
Appendix: GFI LANguard Network Security Scanner default reports

## Policies

**Scan reference:** 192.168.100.2-192.168.100.299  
**Scan date & time:** 29-Nov-2006 10:12

1. **Operating System:** Windows XP  
2. **Service Pack:** 2

### Password Policy

<table>
<thead>
<tr>
<th>Minimum Password Length</th>
<th>Maximum Password Age</th>
<th>Minimum Password History</th>
<th>Force Logoff</th>
<th>Password History</th>
</tr>
</thead>
<tbody>
<tr>
<td>40 characters, 10 lower case + 10 upper case + 10 numbers + 10 symbols</td>
<td>32 days, 32 hours, 32 minutes, 32 seconds</td>
<td>never</td>
<td>never force</td>
<td>no history</td>
</tr>
</tbody>
</table>

### Security Audit Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Success</th>
<th>Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Audit account management</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Audit file system access</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>Audit system events</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

**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:** 192.168.100.2-192.168.100.299  
**Scan date & time:** 29-Nov-2006 10:12

1. **Operating System:** Windows XP  
2. **Service Pack:** Gold

<table>
<thead>
<tr>
<th>Node Name</th>
<th>Registry Entry</th>
</tr>
</thead>
</table>
| CurrentType: LiU processormodel:  
| CurrentVersion: 6.1  
| Driver: OSE2  
| Driver: Creative Audio Chipset  
| Driver: Microsof SWG  
| Driver: IBM Family: 15 Model: 3 Speed:  
| Driver: Language: 0005  
| PathName: C:\Windows\Fonts  
| Product: 02274-336-6579081-22164  
| ProductName: MicrosoftWindowsAXP  
| RegistryLocation:  
| RegistryOwner:  
| SoftwareType: SYSTEM  
| SourcePath: C:\Windows\Fonts  
| System: Computer  
| Version: C:\Windows|

**Screenshot 104 – Sample report showing registry information**
Use this report to:

- List system related registry information for each network host scanned.
Appendix: GFI LANguard Network Security Scanner default reports

Results comparison

Network security log by date

   
   **Scan reference**: Host.a.b.c
   
   **Scan profile**: Default

2. **MARK**

   **Missing hotfixes**:
   - An exp. patch needs to be installed: Security Update for Windows XP (KB869059)
   - An exp. patch needs to be installed: Security Update for Windows XP (KB868715)
   - An exp. patch needs to be installed: Security Update for Windows XP (KB869176)
   - An exp. patch needs to be installed: Security Update for Windows XP (KB869176)
   - An exp. patch needs to be installed: Security Update for Windows XP (KB869176)
   - An exp. patch needs to be installed: Security Update for Windows XP (KB869176)
   - An exp. patch needs to be installed: Security Update for Windows XP (KB869176)

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.

**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
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

192.168.100.28 - CB

Scan Date: 1/1/2003 3:17:54PM
Scan reference: Net List.txt
Scan Profile: Default

Operating System: Windows Server 2003
Service Pack:

Comparing Standard Computer with hosts from scan session

Scan date & time: 1/1/2003 3:42:30PM
Scan reference: Net List.txt
Scan profile: Default

192.168.100.75 - MATRIK
Operating System: Windows XP
Service Pack: 2

Details of the computer used as comparison standard, including scan date, and scan profile

1 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 chosen computer, used as benchmark, and host machines scanned with the same profile and having the same target.

Screenshot 107 – Sample report showing security settings comparison
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 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:
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:

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:
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
e-mail 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