GFI Product Manual

GFI EndPointSecurity™

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, frequency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

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

All product and company names herein may be trademarks of their respective owners.

Document Version: 1.1.1

Last updated (month/day/year): 1/28/2014

Contents

1 Introduction

GFI EndPointSecurity includes a reporting feature which enables you to generate text and graphical reports based on information obtained from security scans. This chapter provides you with an overview of the available reports as well as how to create your own reports for a tailored solution.

Topics in this chapter

1.1 About GFI ReportCenter

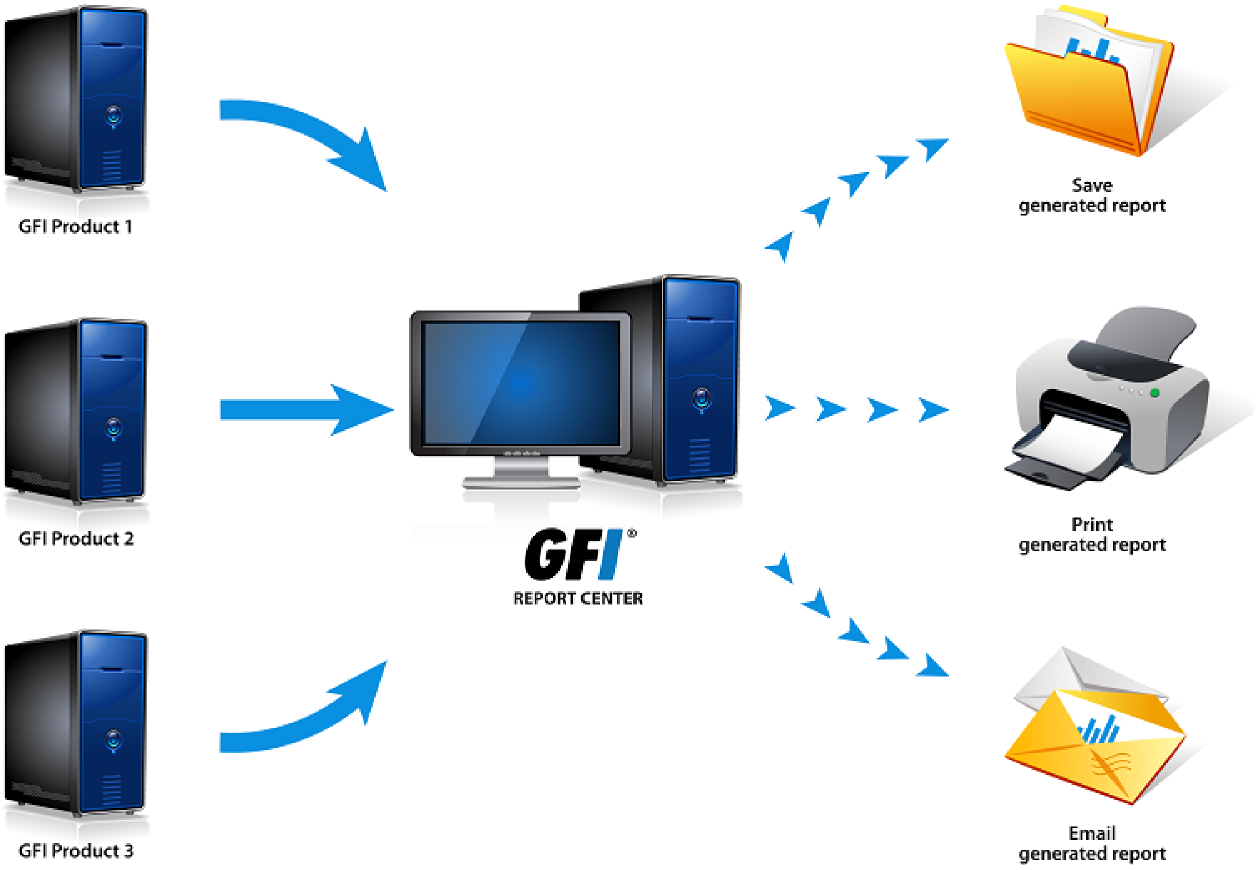


Figure 1: Centralized reporting framework

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

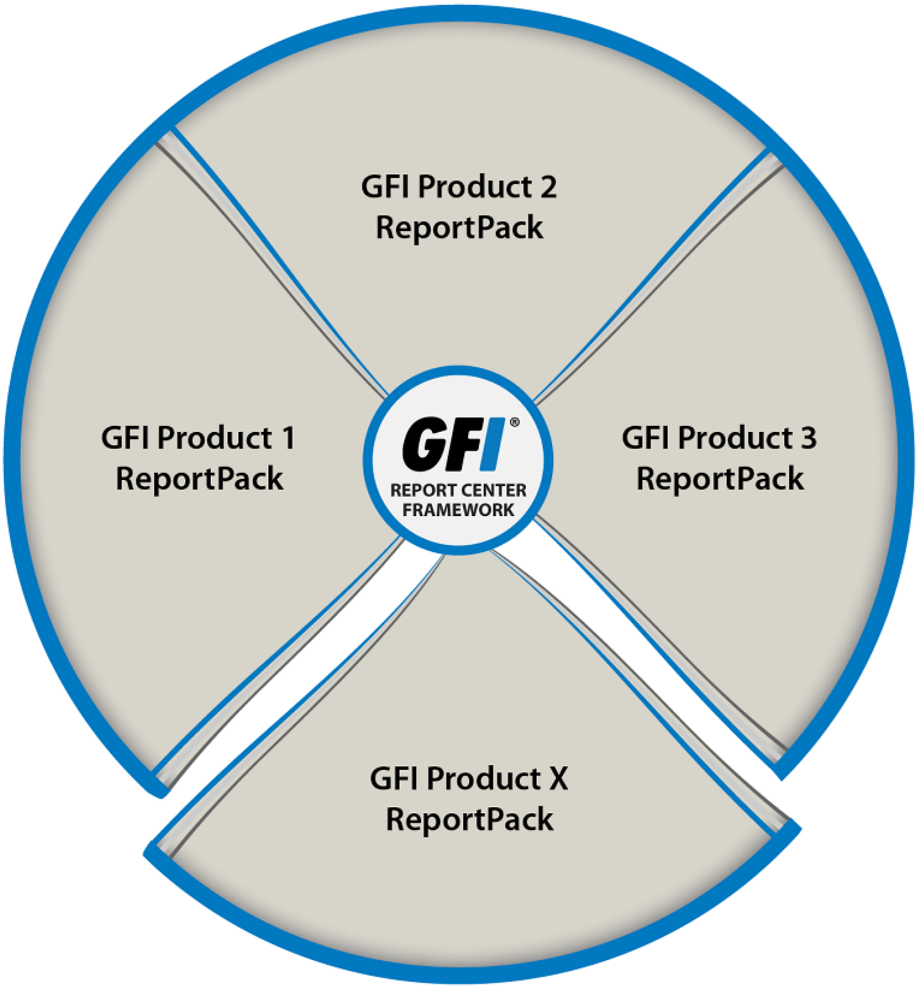


Figure 2: GFI ReportCenter framework

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

1.2 About the GFI EndPointSecurity GFI ReportPack

The GFI EndPointSecurity GFI ReportPack is a full-fledged reporting companion to GFI EndPointSecurity. It allows you to generate graphical IT-level, technical and management reports based on the portable device usage events recorded by GFI EndPointSecurity.

From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI EndPointSecurity GFI ReportPack provides you with the easy-to-view information required, to fully understand the ever-changing portable device activity on your corporate network.

The GFI EndPointSecurity GFI ReportPack allows for the creation of various graphical and text based reports including: Executive summaries, Statistical reports, Technical reports and Top reports.

1.3 Components of the GFI EndPointSecurity GFI ReportPack

When you install the GFI EndPointSecurityGFI ReportPack, the following components are installed:

- GFI Report Center Framework
- GFI EndPointSecurity default reports
- Report scheduling service

1.3.1 GFI Report Center Framework

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

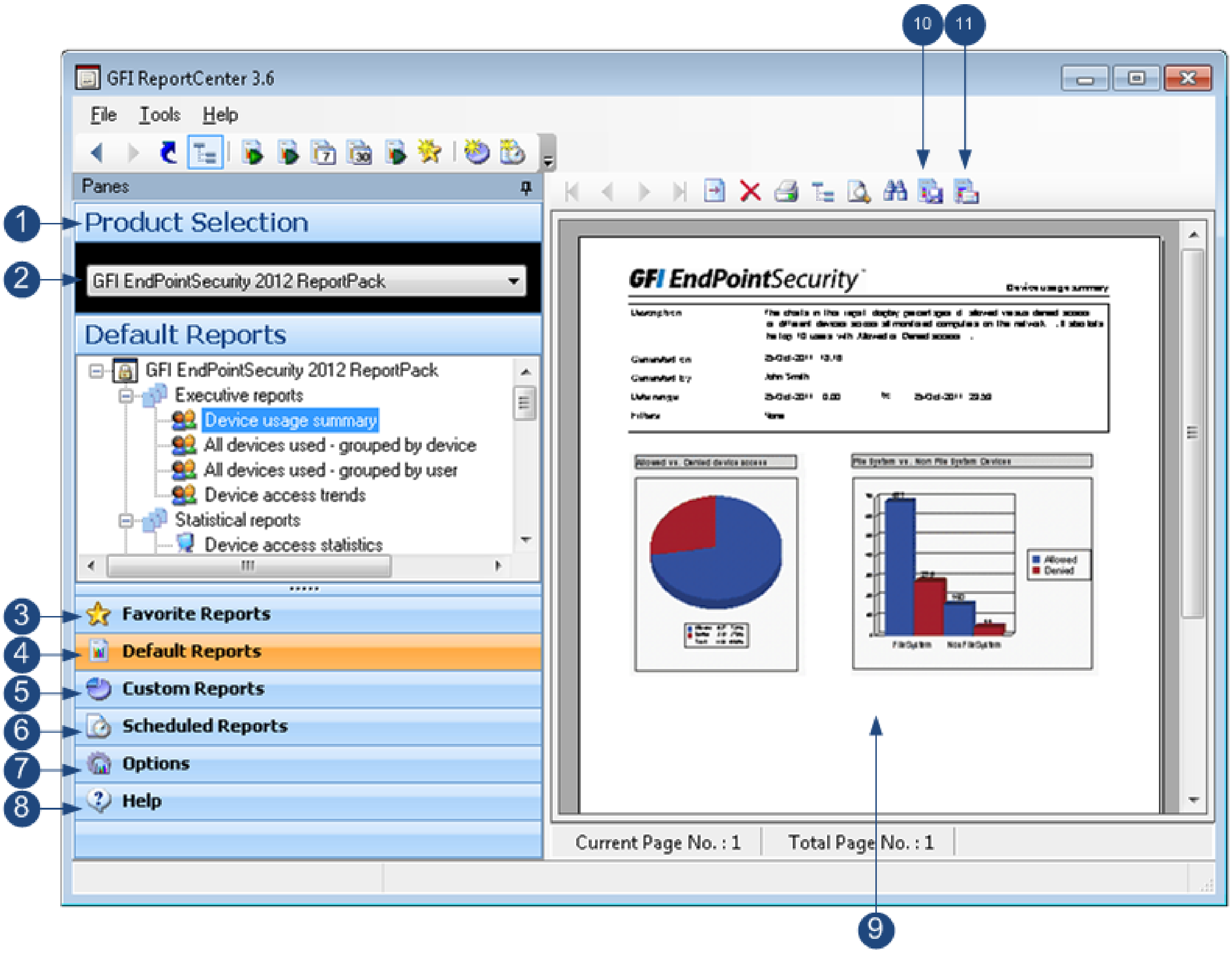


Figure 3: The GFI ReportCenter management console

The GFI ReportCenter management console is organized as follows:

Navigation Pane	Use this pane to access the navigation buttons/configuration options provided with GFI ReportCenter.
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 GFI ReportPack.
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.
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 EndPointSecurity default reports’ section in this manual.
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 ‘Getting Started: Entertaining custom reports’ section in this manual.

Scheduled Reports	Use this navigation button to access the list of scheduled reports for automatic generation and distribution. For more information on how to create scheduled reports refer to the 'Scheduling of reports' chapter in this manual.
Options	Use this navigation button to access the general configuration settings for the GFI product selected in the Product Selection drop down list.
Help	Use this navigation button to show this Quick Reference Guide in the Report Pane of the GFI ReportCenter management console.
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.

1.3.2 GFI EndPointSecurity default reports

The GFI EndPointSecurity default reports are a collection of specialized pre-configured reports which plug into the GFI ReportCenter framework. These reports present the portable device usage activity recorded by GFI EndPointSecurity 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.

1.3.3 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.

1.4 Key Features

This section contains information about:

- Centralized reporting
- Wizard assisted configuration
- Report scheduling
- Distribution of reports via email
- Reports export to various formats
- Default reports
- Reports customization
- Favorites
- Printing

1.4.1 Centralized reporting

GFI ReportPack 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.

1.4.2 Wizard assisted configuration

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

1.4.3 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.

1.4.4 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.

1.4.5 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.

1.4.6 Default reports

The GFI EndPointSecurity GFI 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 GFI ReportPack are organized into three different report-type categories: Executive, Statistical and Technical. For a detailed description of every report refer to **Appendix 1** in this manual.

1.4.7 Report customization

The default reports that ship with every GFI 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.

1.4.8 Favorites

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

1.4.9 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.

2 Installation

Topics in this chapter

2.1 System Requirements

Install the GFI EndPointSecurity GFI ReportPack on a computer that meets the following requirements:

- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2011 (Standard edition)
- Microsoft Windows Server 2008 R2 (Standard or Enterprise edition)
- Microsoft Windows Server 2008 (Standard or Enterprise edition)
- Microsoft Windows Small Business Server 2008 (Standard edition)
- Microsoft Windows Server 2003 (Standard, Enterprise or Web edition)
- Microsoft Windows Small Business Server 2003
- Microsoft Windows 8 (Professional or Enterprise)
- Microsoft Windows 7 (Professional, Enterprise or Ultimate edition)
- Microsoft Windows Vista (Enterprise, Business or Ultimate edition)
- Microsoft Windows XP Professional Service Pack 3.

> **Note**
>
> The GFI EndPointSecurity GFI ReportPack only allows you to generate reports for data contained in the SQL Server database backend of GFI EndPointSecurity.

2.2 Installation procedure

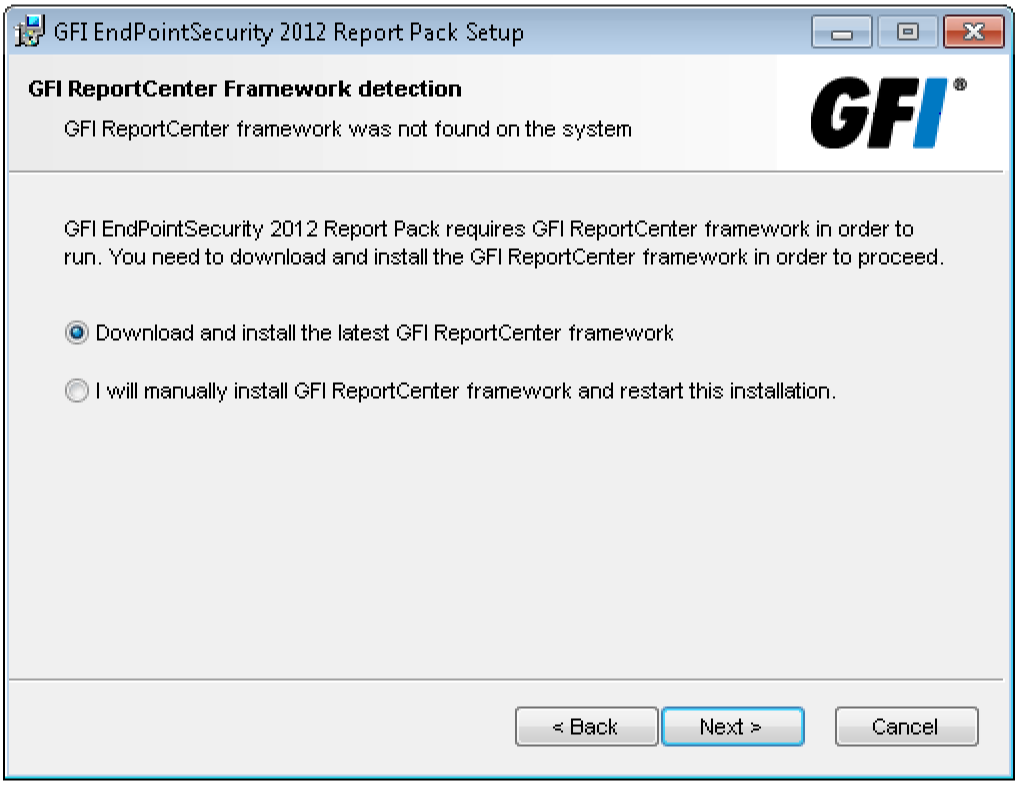
The GFI EndPointSecurity GFI ReportPack includes an installation wizard that will assist you through the installation process. During the installation process, this wizard will:

Note

- 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 EndPointSecurity default reports and the Report Scheduling service.

To start the installation:

1. Double-click on the GFI ReportPack executable file and in the welcome screen, click **Next** to start the installation.



GFI ReportCenter Framework detection

GFI ReportCenter framework was not found on the system

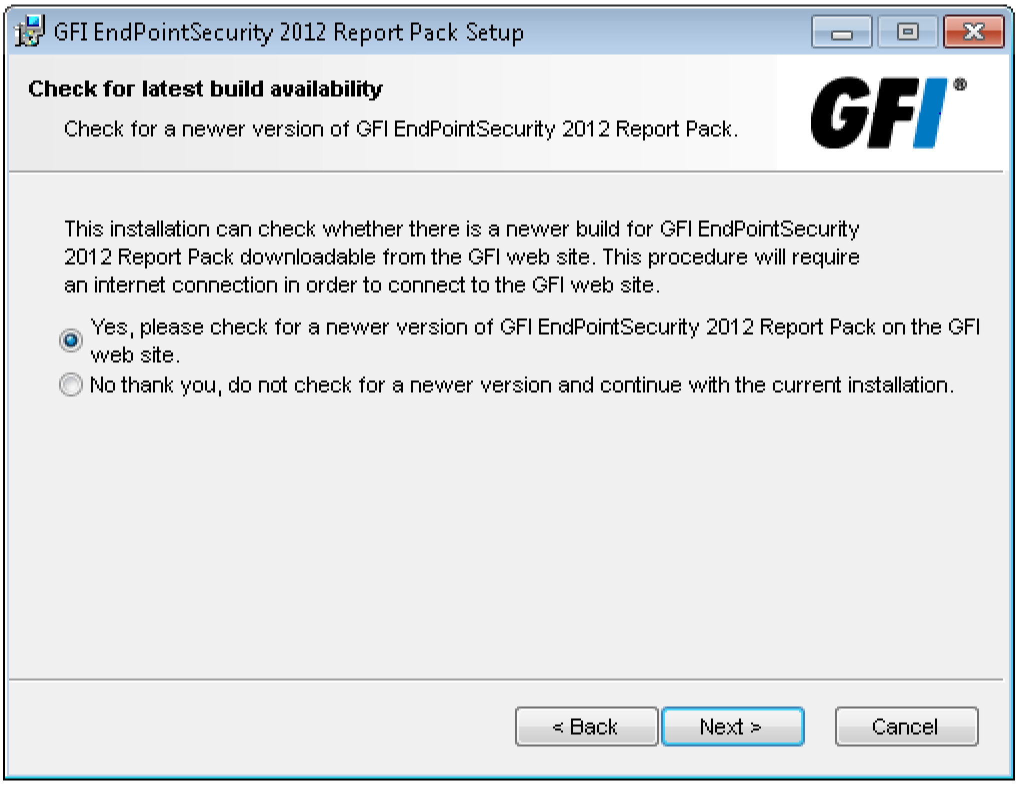
GFI EndPointSecurity 2012 Report Pack requires GFI ReportCenter framework in order to run. You need to download and install the GFI ReportCenter framework in order to proceed.

● Download and install the latest GFI ReportCenter framework

○ I will manually install GFI ReportCenter framework and restart this installation.

Screenshot 1: GFI ReportCenter framework detection dialog

2. If the current version of GFI ReportCenter framework is not compatible with the GFI EndPointSecurity GFI ReportPack, you will be prompted to download and install an updated version. Select **Download and install the GFI ReportCenter…** and click **Next**.



Check for latest build availability

Check for a newer version of GFI EndPointSecurity 2012 Report Pack.

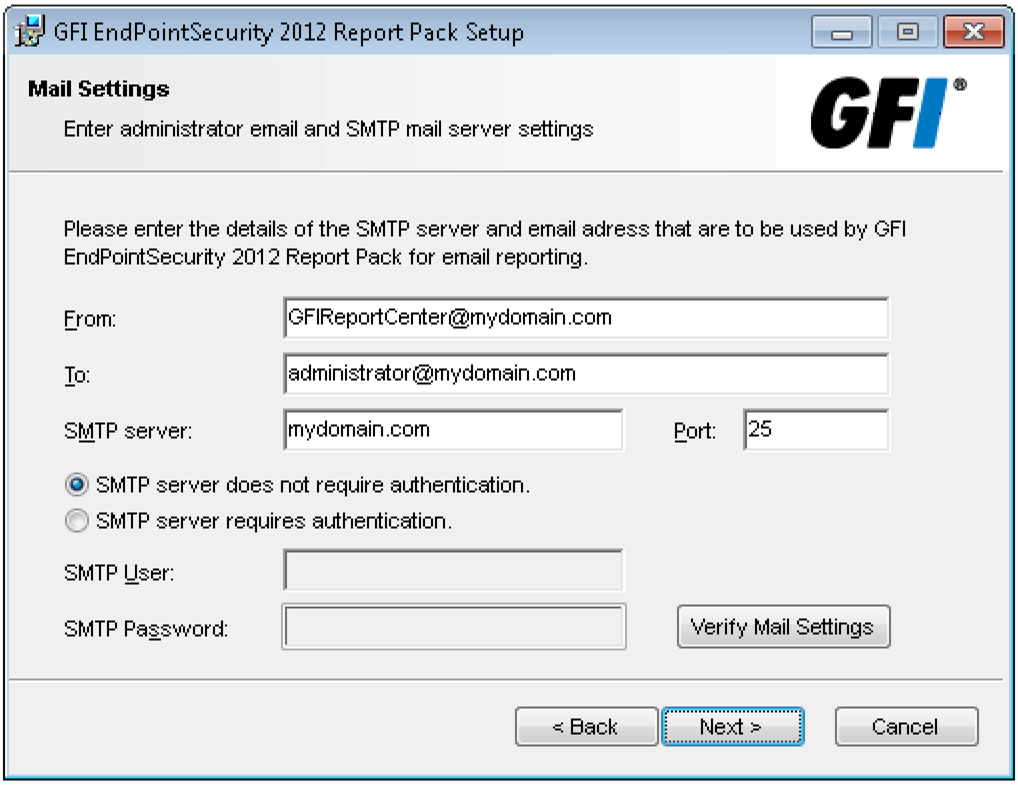
This installation can check whether there is a newer build for GFI EndPointSecurity 2012 Report Pack downloadable from the GFI web site. This procedure will require an internet connection in order to connect to the GFI web site.

● Yes, please check for a newer version of GFI EndPointSecurity 2012 Report Pack on the GFI web site.

○ No thank you, do not check for a newer version and continue with the current installation.

Screenshot 2: Check for latest build availability

3. Choose whether you want the installation wizard to search for a newer build of the GFI EndPointSecurity GFI ReportPack on the GFI website and click **Next**.
4. In the license dialog, read the licensing agreement carefully. Select the **I accept the Licensing agreement** option and click **Next**.
5. Specify the details of the SQL Server that is hosting your GFI EndPointSecurity database backend, and click **Next**.



GFI EndPointSecurity 2012 Report Pack Setup

Mail Settings

Enter administrator email and SMTP mail server settings

Please enter the details of the SMTP server and email adress that are to be used by GFI EndPointSecurity 2012 Report Pack for email reporting.

From: GFIReportCenter@mydomain.com

To: administrator@mydomain.com

SMTP server: mydomain.com Port: 25

● SMTP server does not require authentication.

○ SMTP server requires authentication.

SMTP User:

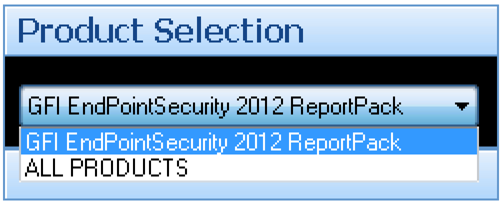
SMTP Password:

Screenshot 3: Email configuration dialog

6. Specify the default email settings that will be used for report distribution and click **Next**.
7. Specify the product installation path or click **Next** to install GFI Report Pack in the default path. The installation will need approximately 100 MB of free disk space.
8. The installation wizard is now ready to copy the required files and finalize the installation. Click **Next**.

2.3 Selecting a Product

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



Product Selection
GFI EndPointSecurity 2012 ReportPack
GFI EndPointSecurity 2012 ReportPack
ALL PRODUCTS

Screenshot 4: Product Selection drop down list

For example, to run the reports provided in the GFI EndPointSecurity GFI ReportPack:

1. Launch GFI ReportCenter from **Start** > **Program Files** > **GFI ReportCenter**.
2. Select **GFI EndPointSecurity GFI ReportPack** from the Product Selection drop down list.

Note

Select the **All Products** option to display and navigate all the GFI ReportPackthat are currently installed in GFI ReportCenter.

2.4 Launching the GFI EndPointSecurityreports for GFI ReportCenter

Following the installation, launch the GFI EndPointSecurity Reports for GFI ReportCenter from **Start > Programs > GFI ReportCenter > GFI EndPointSecurity GFI ReportPack.**

3 Getting Started: Default Reports

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

Report Type	Description
Executive Reports	Use the reports in this category to generate a high-level activity summary of all devices being controlled across the network. The information presented in these executive reports is mostly graphical and includes: » The percentage amount of allowed versus denied device access requests. » Device usage activity by user, machine and device class. » Trend reports such as device access attempts per day. » The top 10 device users who have been mostly allowed and denied access to controlled devices.
Statistical Reports	Use the reports in this category to generate a statistical overview of the device usage activity on a user and/or device basis.
Top active users/machines reports	Use the reports in this category to pinpoint top authorized/unauthorized device users as well as to enumerate the devices which were most frequently accessed across a network.
Technical Reports:	Use the reports in this category to generate detailed technical information related to controlled devices. This includes the number of times that each device was connected to computers protected by GFI EndPointSecurity. Technical reports allow you to generate report grouped by; users accessing each device, computers to which the devices were connected and the device class to which every connected device belongs.
Security reports:	Use the reports in this category to generate a list of; » users that connected devices during weekends or outside working hours » users that tried to access devices on multiple machines. » machines used to access devices by multiple users. GFI EndPointSecurity default reports are accessed by clicking on the Default Reports navigation button provided in the management console.

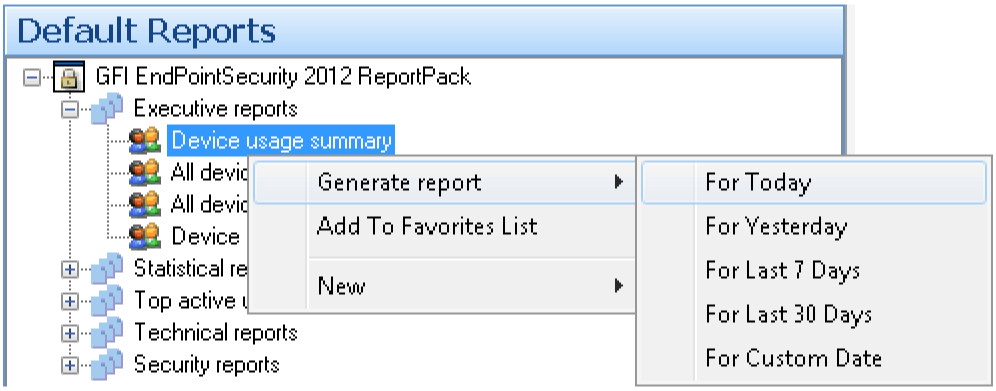
Note

Click a **report node** to view a description and a sample output of what the selected report will contain.

3.1 Generating Default Reports

To generate a default report:

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



Screenshot 5: Selecting the data set period

2. Right-click on the report that you wish to generate, select **Generate report** and specify which device activity data will be represented in the report.

> **Note:**
>
> Default reports can be based on the device activity data collected today, yesterday, during the last 7 days or over the last 30 days. Further to this, you can also base your reports on data collected during a particular day, month or date/time period.

Example 1: Generating a "Device usage summary" report based on yesterday's data.

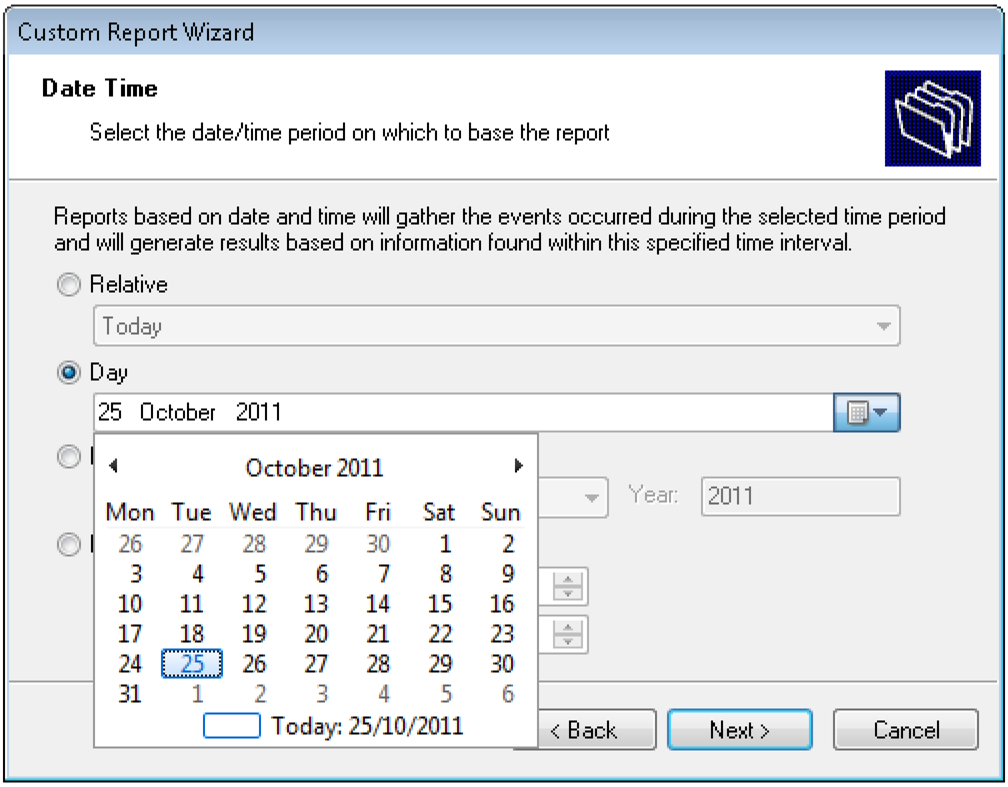
This example demonstrates how to generate a "Device usage summary" report based on the data collected by GFI EndPointSecurity during the previous day.

1. Click on the **Default Reports** navigation button to bring up the list of available reports.
2. Right-click on **Device usage summary** and select **Generate report** > **For Yesterday**.

Example 2: Generating a "Device usage summary" report based on that data collected on a particular day.

This example demonstrates how to generate a Device usage summary report based on the data collected by GFI EndPointSecurityon September 15, 2009.

1. Click on the **Default Reports** navigation button to launch the list of available reports.
2. Right-click on **Device usage summary** and select **Generate report** > **For Custom Date**.


Custom Report Wizard

Date Time

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

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

○ Relative

Today

● Day

25 October 2011

October 2011

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

Today: 25/10/2011

Year: 2011

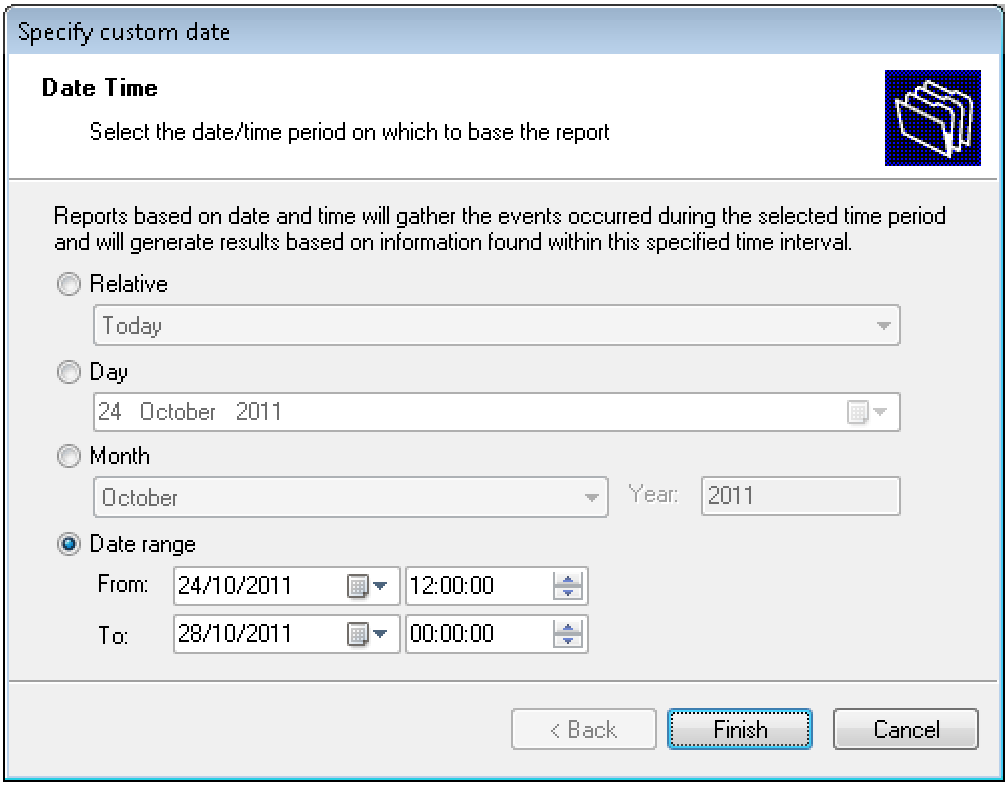
Screenshot 6: Selecting date and time

3. Select **Day** option and expand the provided drop down. This will launch the **date selection calendar**.
4. Navigate to the required month (For Example. September) and select the required day (i.e. 15).
5. Click **Finish** to generate the report.

Example 3: Generating a "Device usage summary" report based on data collected over a specific date/time period.

This example demonstrates how to generate a Device usage summary report based on the data collected by GFI EndPointSecurity between August 18, 2009 and September 1, 2009.

1. Click on the **Default Reports** navigation button to launch the list of available reports.
2. Right-click on **Device usage summary** and select **Generate report > For Custom Date**.



Specify custom date

Date Time

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

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

○ Relative

Today

○ Day

24 October 2011

○ Month

October Year: 2011

● Date range

From: 24/10/2011 12:00:00

To: 28/10/2011 00:00:00

Screenshot 7: Selecting date range

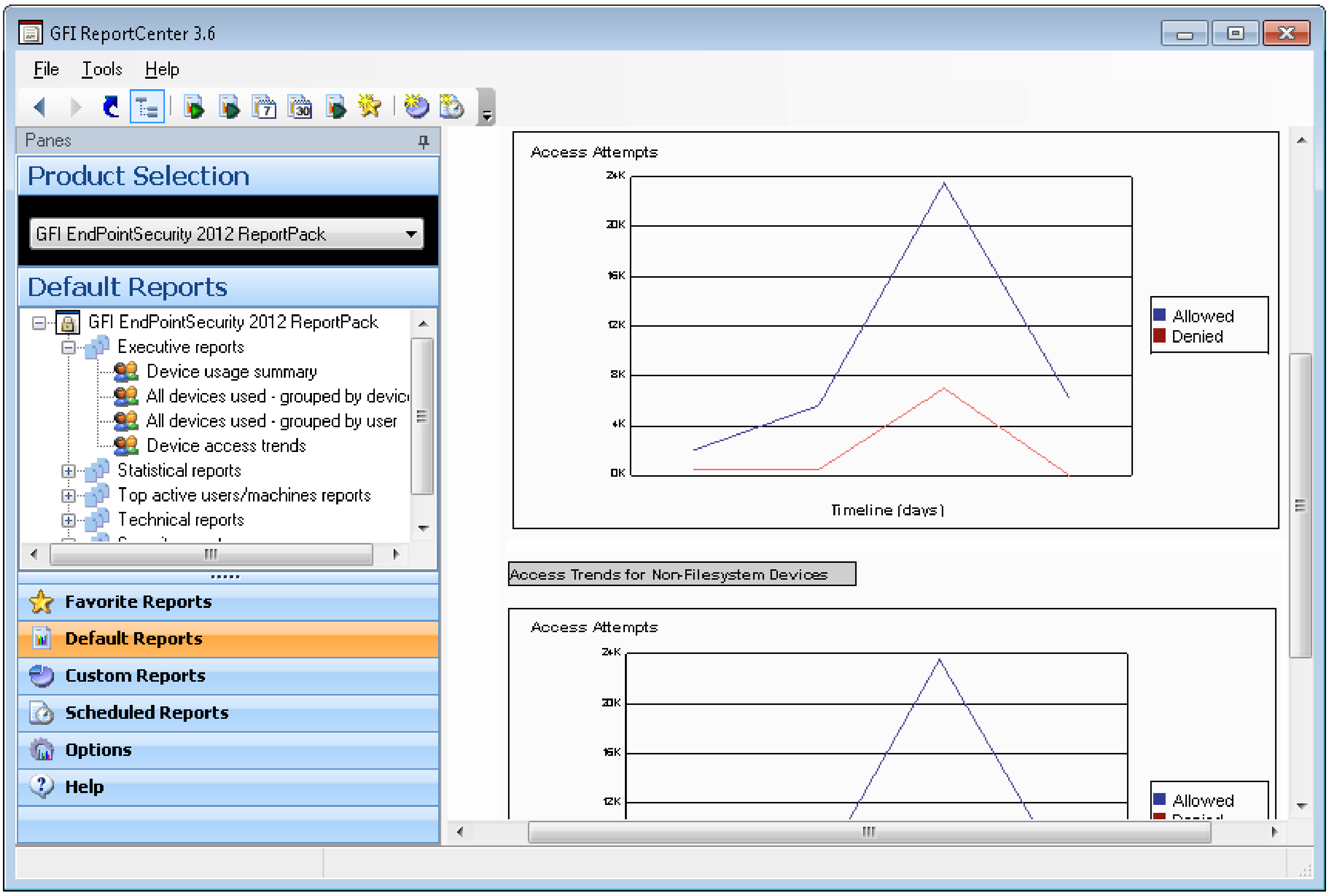
1. Select **Date range** option and specify the required parameters:

- From - 24/10/2011 12:00:00
- To - 28/10/2011 0:00:00

> **Note:**
>
> Date and time format are based on the regional settings configured on your computer.

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

3.2 Analyzing the generated report



Screenshot 8: Generated reports are displayed in the right pane of the management console

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

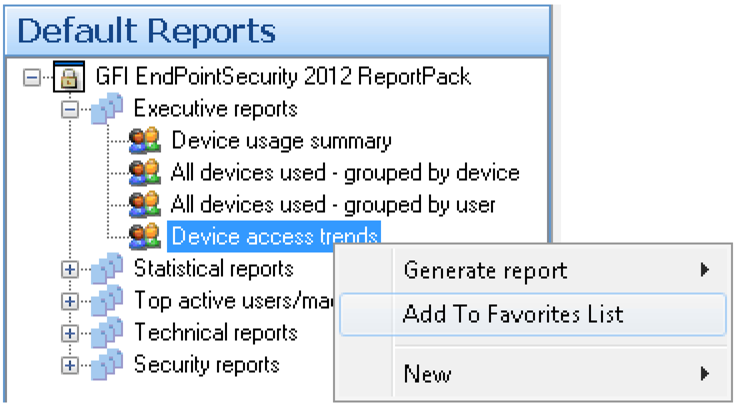
Report browsing options	
⏮◀▶⏭	Browse the generated report page by page.
🔍	Zoom in/Zoom out.
🔭	Search the report for particular text or characters.
→	Go directly to a specific page.
☰	Breakdown the report into a group tree (For example. By date/time).
🖨	Print report.

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.

3.3 Adding Default Reports to the list of Favorite Reports



Screenshot 9: Favorite Reports navigation button

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

1. Click on the **Default Reports** navigation button to launch the list of available reports.
2. Right-click on the default report that you wish to add to favorites and select **Add to favorites list**.

4 Custom Reports

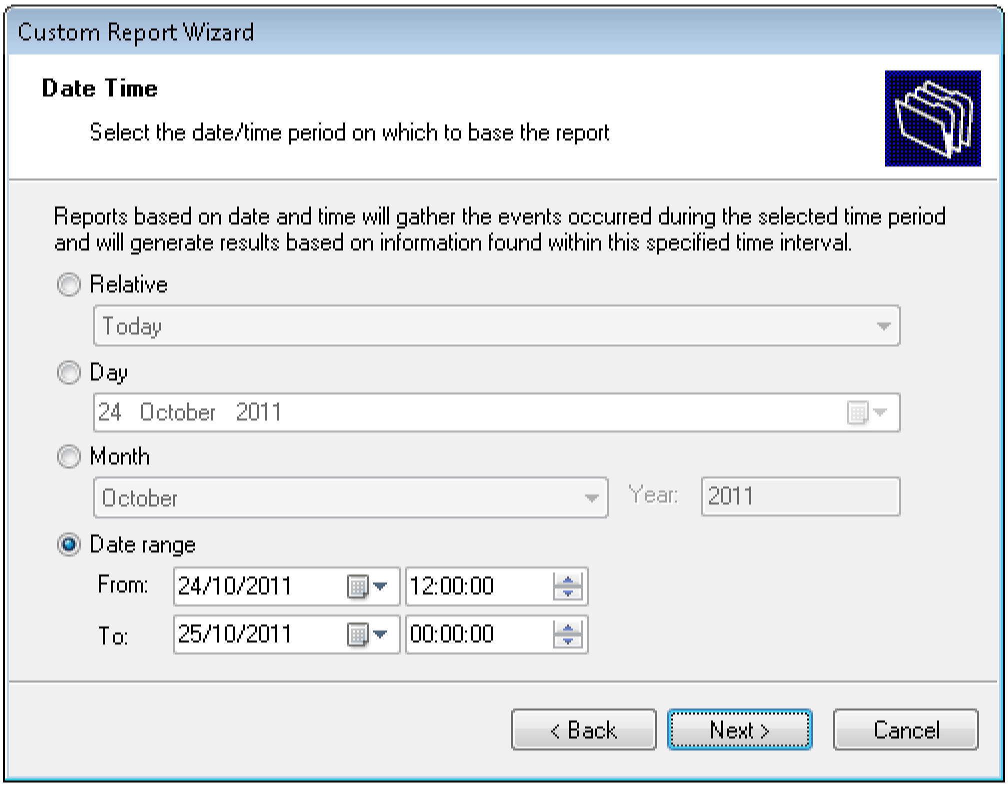
GFI ReportCenter allows you to create custom reports which are tailored to your reporting requirements. This is achieved by building up custom data filters which will analyze the data source and filter out the information that matches the specified criteria.

Topics in this chapter

4.1 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 that will be used as a custom report template and select **New > Custom Report.** This will launch the Custom Report Wizard.Click **Next**.



Custom Report Wizard

Date Time

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

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

○ Relative: Today

○ Day: 24 October 2011

○ Month: October Year: 2011

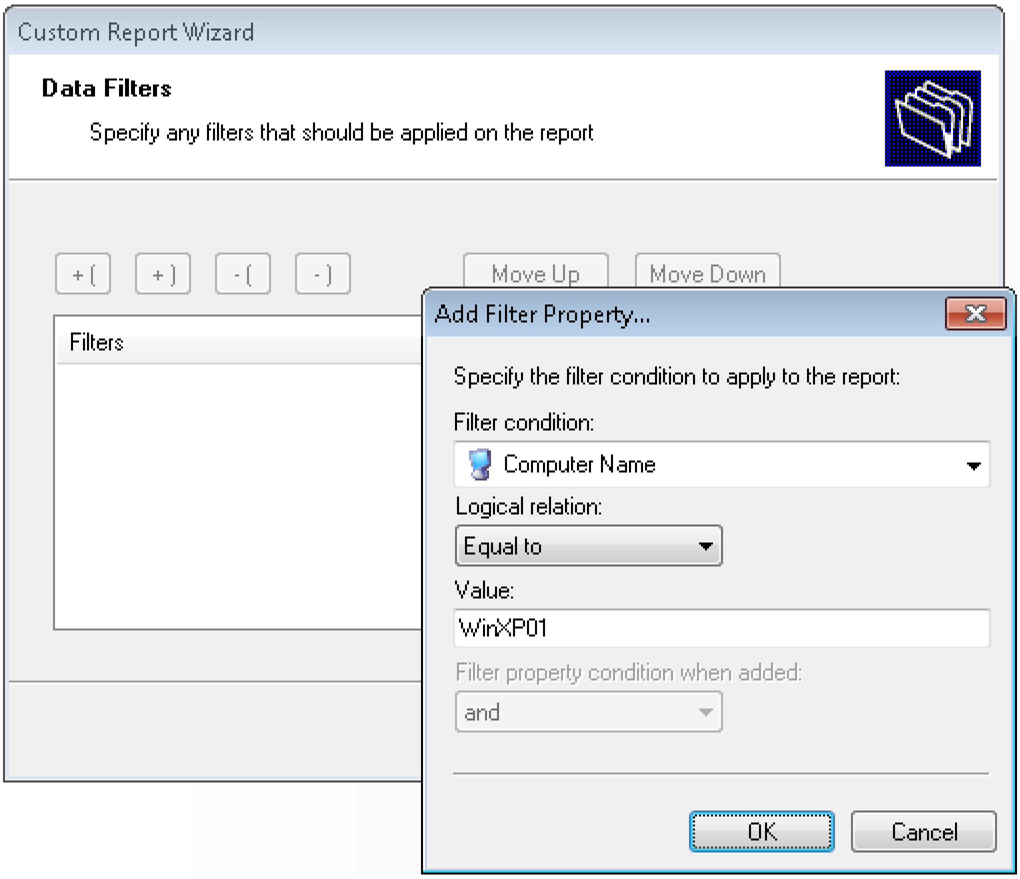
● Date range

From: 24/10/2011 12:00:00

To: 25/10/2011 00:00:00

Screenshot 10: Selecting the data source to use

3. Select the data source that will be used to generate the custom report.



Specify the filter condition to apply to the report:

Filter condition: Computer Name

Logical relation: Equal to

Value: WinXP01

Filter property condition when added: and

Screenshot 11: Specifying data filter conditions

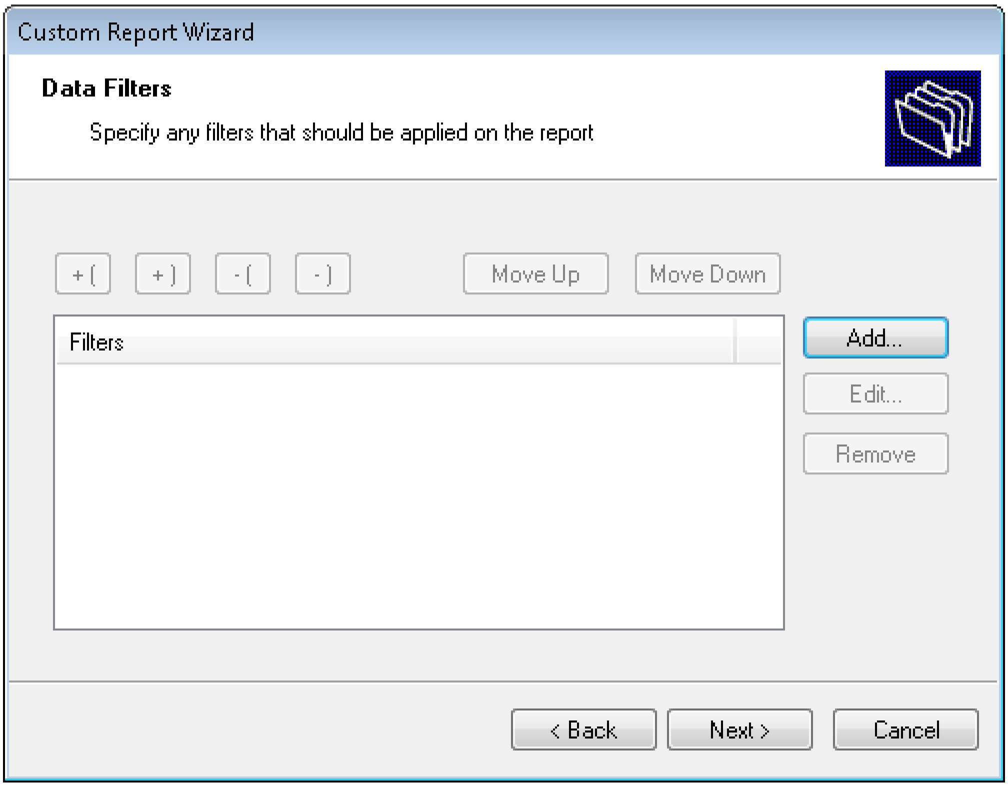
4. Configure the data filter conditions that will be applied against the selected data source. Click on Next to continue.

> **Note**
>
> For more information on how to configure filter conditions, refer to the section **Configuring data filter conditions** in this manual.

5. Specify a name and description for the customized report. Click on **Next** to continue.
6. Click on Finish to finalize your configuration settings.

4.2 Configuring Data Filter Conditions

Use data filter conditions to specify which device usage activity will be included in the report. Only the device usage activity which matches the specified criteria will be processed and presented within the report.

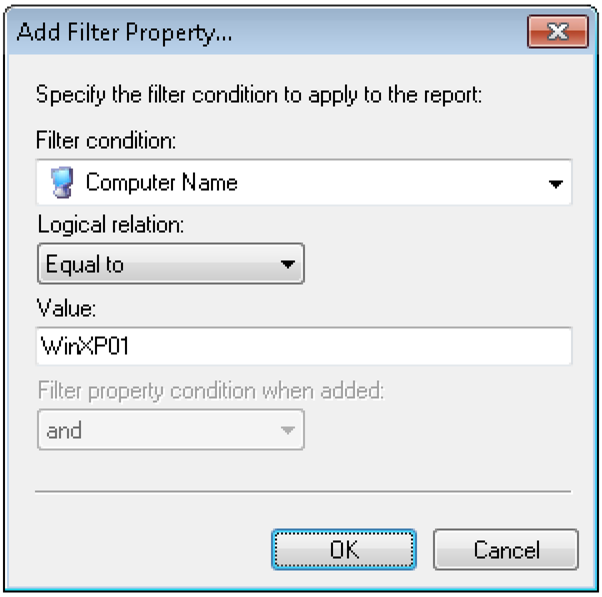


Screenshot 12: Custom Report Wizard: Filters dialog

Click **Add...** to launch the **Edit filter properties** dialog. Configurable options in this dialog include:

- **Filter condition** - This is the data source area on which the filter will focus (for example, select **Computer Name** to filter the device activity data that is related to a particular computer).
- **Logical relation** - The condition comparison parameter.
- **Value** - The string to which source data will be compared.

For example to generate a report which contains only information related to a workstation called “WinXp01”, configure your filter parameters as shown below:



Filter condition: Computer Name

Logical relation: Equal to

Value: WinXP01

Filter property condition when added: and

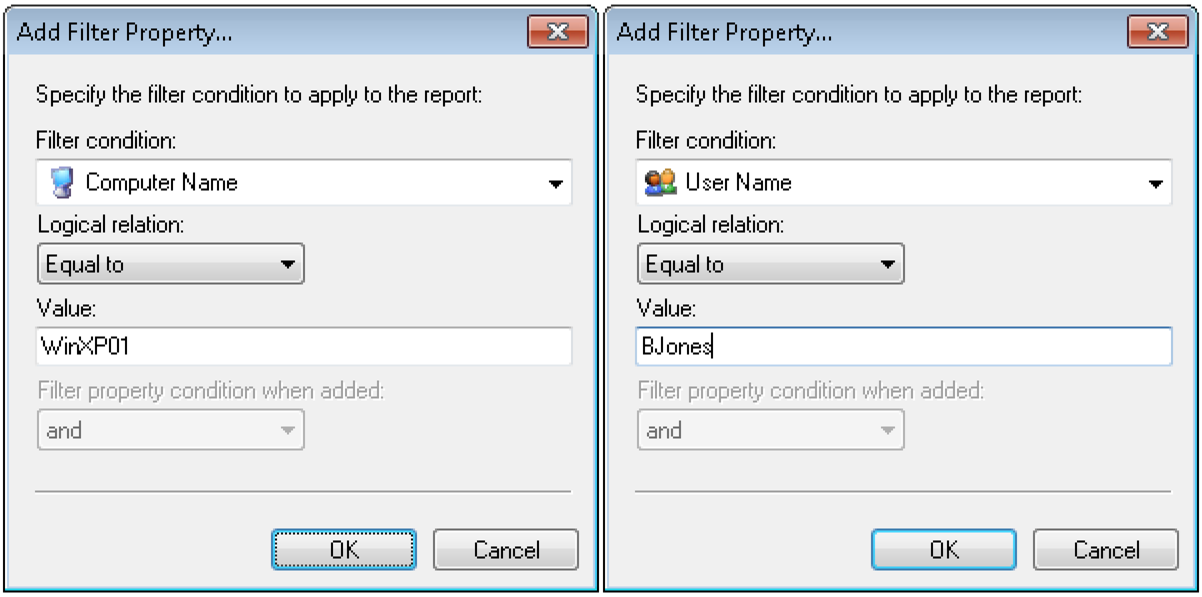
Screenshot 13: Filter conditions configuration dialog

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

- 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.

4.2.1 Example: Using multiple filters

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



Add Filter Property...

Specify the filter condition to apply to the report:

Filter condition: Computer Name

Logical relation: Equal to

Value: WinXP01

Filter property condition when added: and

Add Filter Property...

Specify the filter condition to apply to the report:

Filter condition: User Name

Logical relation: Equal to

Value: BJones

Filter property condition when added: and

Screenshot 14: Using multiple filters

Parameters	Filter 1	Filter 2
Filter condition	Computer Name	User Name
Logical relation	Is equal to	Includes
Value	'WinXP01'	'BJones'

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.

Filter 1	and	Filter 2	The report will show: » All the device usage activity made by users called 'BJones' on the computer called 'WinXP01'.
Filter 1	and	Filter 2	The report will show: » All the device usage activity made by users called 'Bjones' - (no matter on which computer the connections were made) AND » All device connections made to the computer called 'WinXp01' - (no matter who the users are).

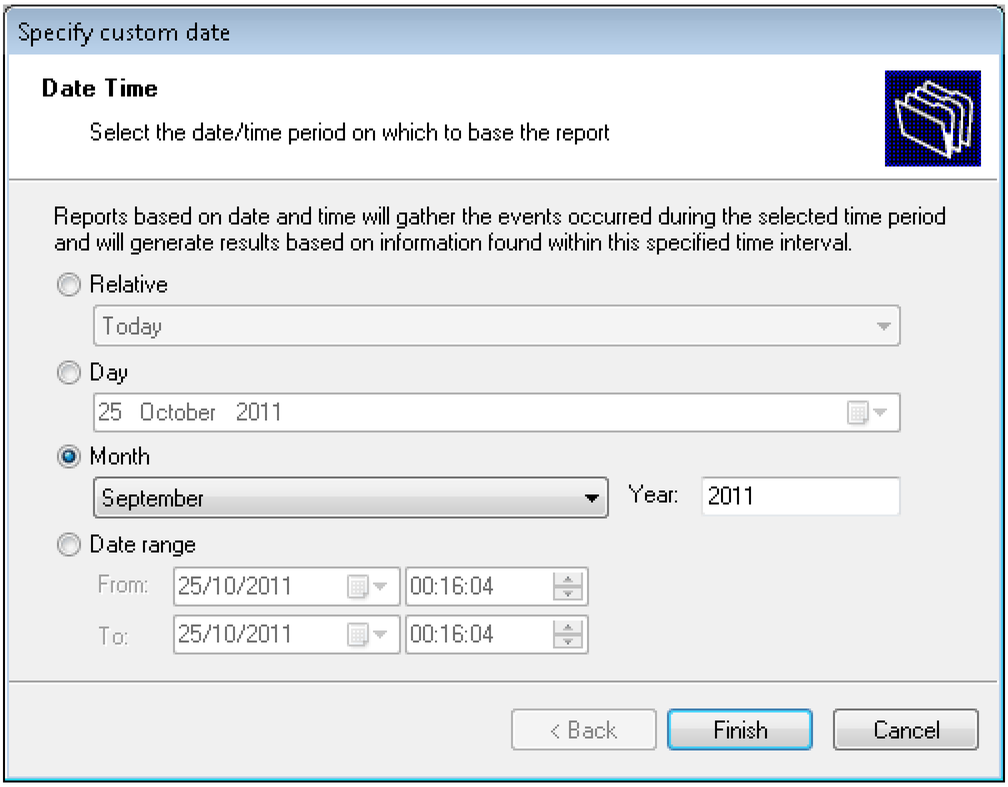
4.2.2 Example: Creating a custom report based on data collected during a particular month

This example demonstrates how to generate a device usage summary report called **Device Usage on September 2009**. This report will be based on the device usage activity:

- Collected from the computer called **WinXp01**
- Made by a particular user called **Bob Jones**
- Recorded during the month of **September 2009**.

To create this report:

1. Click on the **Default Reports** navigation button.
2. Right-click on the report that you wish to customize and select **New > Custom Report**. This will launch the **Custom Reports Wizard**.
3. As soon as the welcome dialog is displayed, click **Next**.



Specify custom date

Date Time

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

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

○ Relative

Today

○ Day

25 October 2011

● Month

September Year: 2011

○ Date range

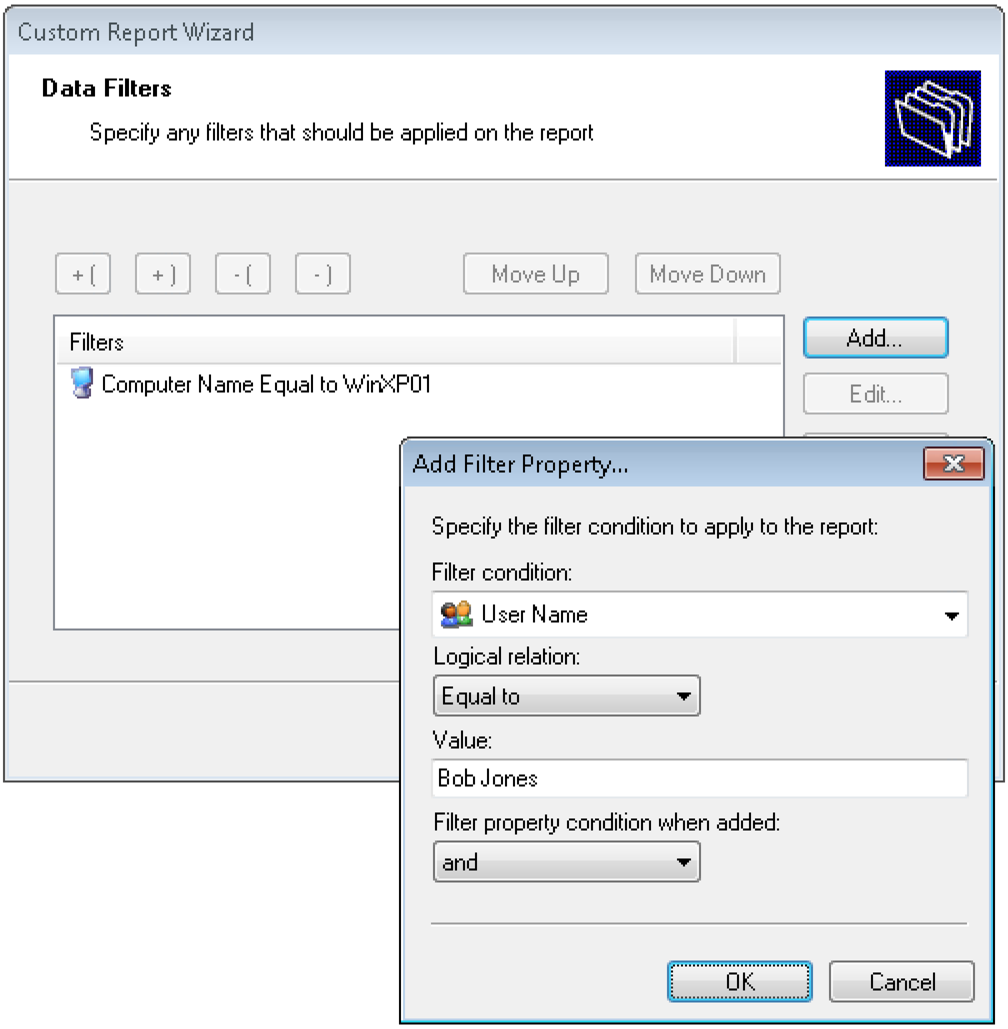
From: 25/10/2011 00:16:04

To: 25/10/2011 00:16:04

4. Select Month option and specify the following parameters:

- Month : **September**.
- Year : **2011**.

5. Click on Next to proceed to the data filters dialog.



Data Filters

Specify any filters that should be applied on the report

Filters

Computer Name Equal to WinXP01

Specify the filter condition to apply to the report:

Filter condition: User Name

Logical relation: Equal to

Value: Bob Jones

Filter property condition when added: and

Screenshot 15: Filter conditions dialog(s)

6. Click on the **Add...** button and configure the parameters of filter 1 as follows:
   - **Filter condition** : Computer Name
   - **Condition** : Equal to
   - **Value** : WinXp01
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** : User Name
   - **Condition** : Equal to
   - **Value** : Bob Jones
   - **Filter Property condition... : and**
9. Click **OK** to finalize your filter configuration settings.
10. Click **Next** and specify the following parameters:
    - **Report Name** : Device usage on September 2009
    - **Report Title** : Device usage by Bob Jones on computer WinXp01

- **Report Description**: This report shows the device connections made by user Bob Jones on computer WinXp01 during September 2009.

11. Click **Next** to proceed to the final dialog.
12. Click **Finish** to finalize your custom report configuration settings.

4.3 Run a custom report

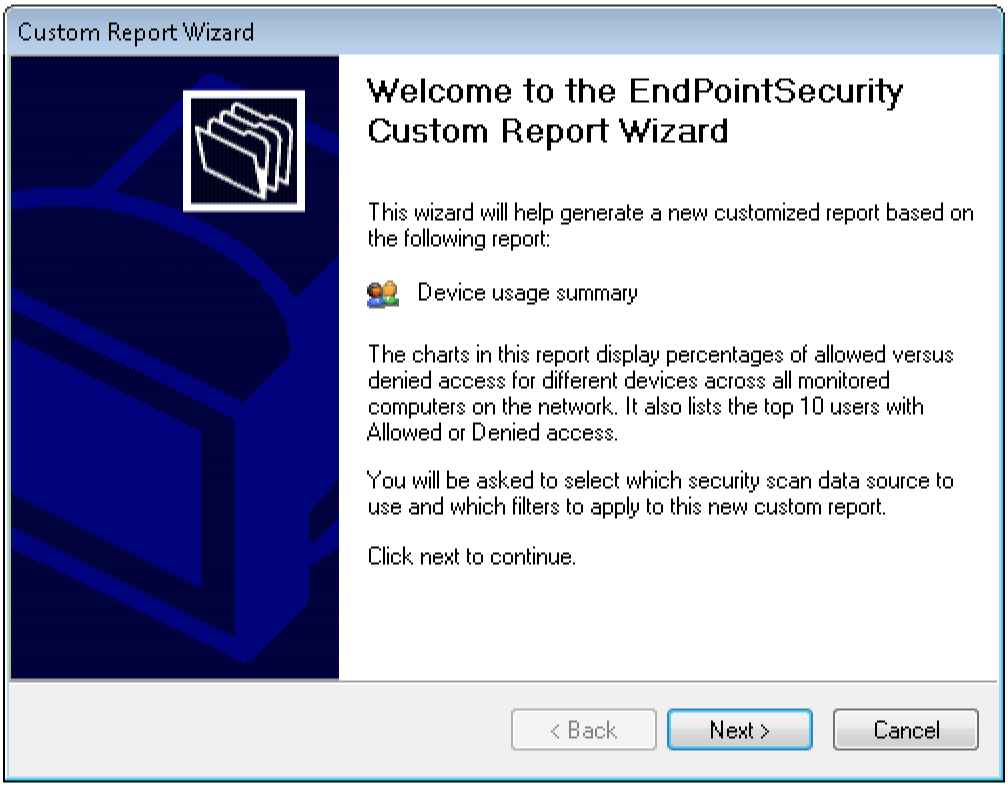
To run a custom report:

1. Click on the **Custom Reports** navigation button.
2. Right-click on the custom report that you wish to generate and select **Generate**.

4.4 Editing a Custom Report

To edit the configuration settings of a custom report:

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



Welcome to the EndPointSecurity Custom Report Wizard

This wizard will help generate a new customized report based on the following report:

Device usage summary

The charts in this report display percentages of allowed versus denied access for different devices across all monitored computers on the network. It also lists the top 10 users with Allowed or Denied access.

You will be asked to select which security scan data source to use and which filters to apply to this new custom report.

Click next to continue.

Screenshot 16: Custom Report Wizard: Welcome dialog

2. Right-click on the custom report that you wish to modify and select **Edit**. This will launch the **Custom Reports Wizard** through which you can make the required changes.

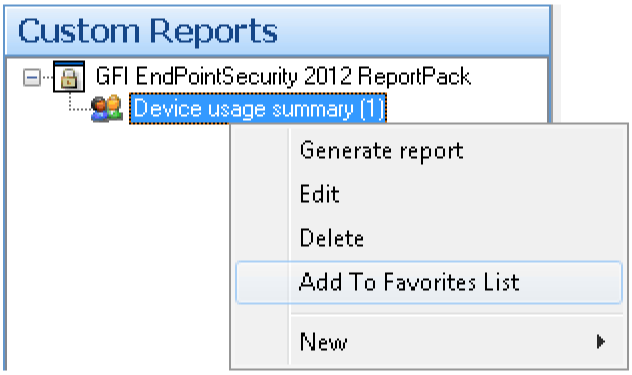
> **Note**
>
> For more information on how to configure the parameters of a custom report refer to the Creating a custom report section in this chapter.

4.5 Deleting a custom report

To delete a custom report:

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

4.6 Adding custom reports to the list of favorite reports



Screenshot 17: Favorite reports navigation button

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

1. Click on the **Custom Reports** navigation button to launch the list of available reports.
2. Right-click on the custom report that you wish to add to favorites and select **Add to Favorites List**.

5 Scheduling Reports

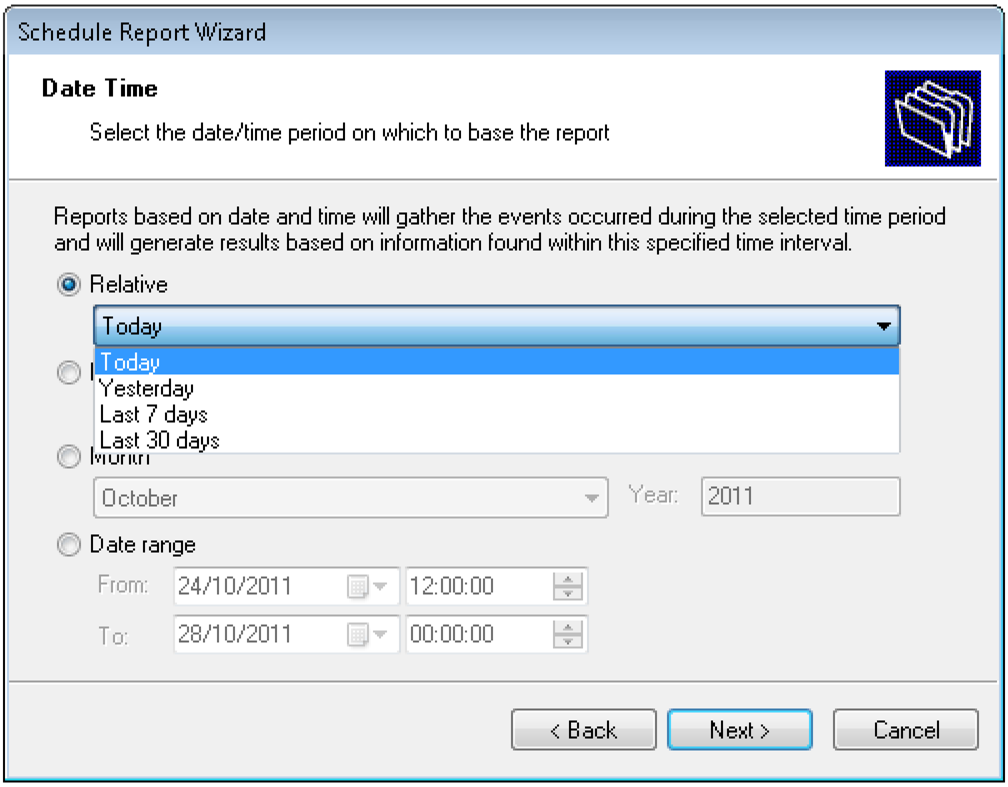
GFI ReportPack allows you to generate reports on a pre-defined schedule as well as at specified intervals. In this way you can automate the generation of reports which need to be created and delivered on a regular basis. Further to this, GFI ReportPack can also be configured to automatically distribute scheduled reports via email. For every scheduled report, you can configure custom emailing parameters including the list of report recipients and the file format (example: 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. In 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.

Topics in this chapter

5.1 Scheduling a report

To schedule a report

1. Click on the Default or Custom Reports option pane.
2. Right-click on the report to be scheduled and select New > Scheduled report. This will launch the **Scheduled Report Wizard**. Click on **Next** to continue.



Schedule Report Wizard

Date Time

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

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

● Relative

Today

○ Month

October Year: 2011

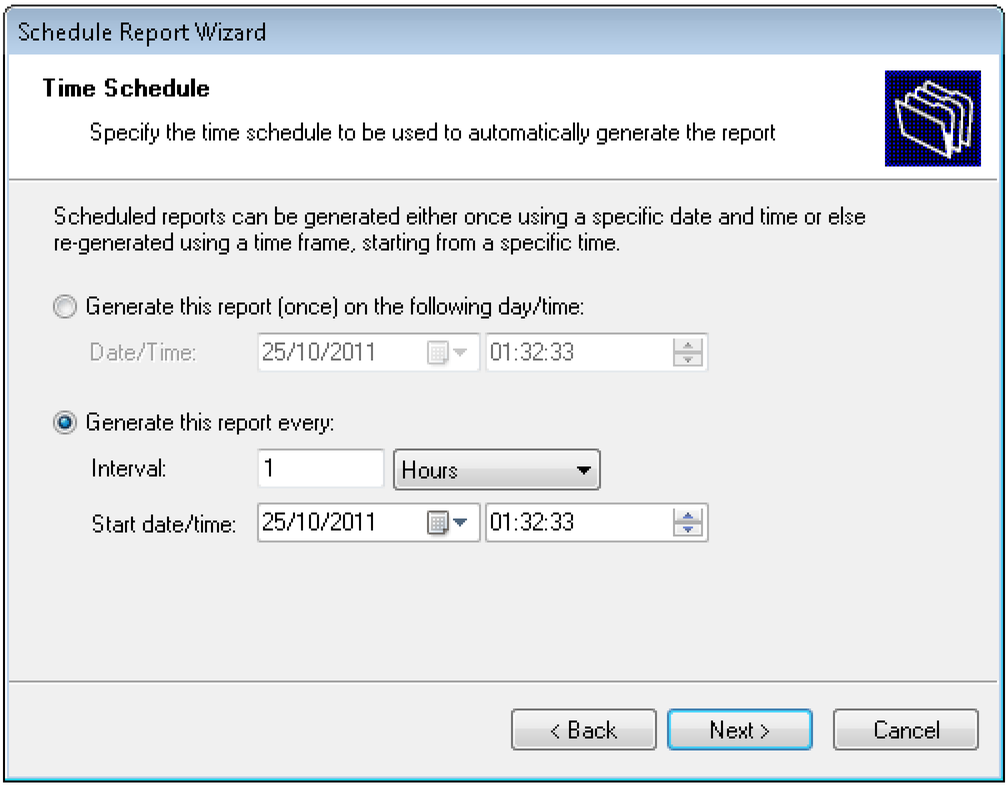
○ Date range

From: 24/10/2011 12:00:00

To: 28/10/2011 00:00:00

Screenshot 18: Report Scheduling Wizard: Data-set selection dialog

3. Select the device usage period to be covered by this report.



Schedule Report Wizard

Time Schedule

Specify the time schedule to be used to automatically generate the report

Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.

○ Generate this report (once) on the following day/time:

Date/Time: 25/10/2011 01:32:33

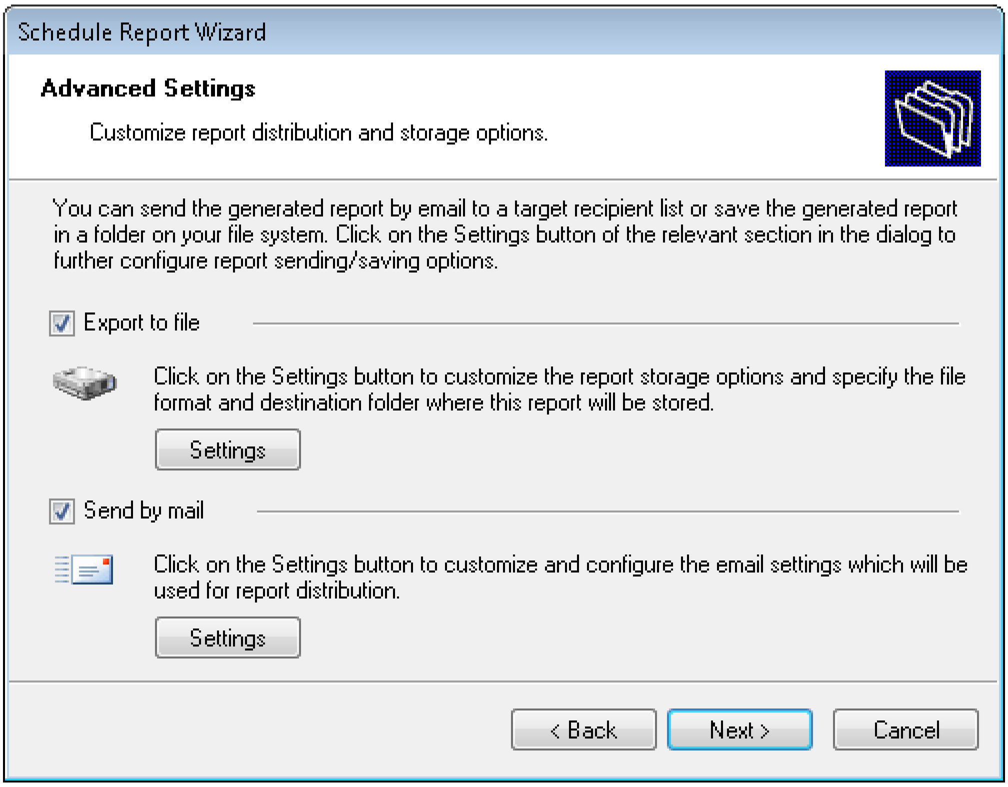
● Generate this report every:

Interval: 1 Hours

Start date/time: 25/10/2011 01:32:33

Screenshot 19: Report Scheduling Wizard: Time schedule dialogue

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



Schedule Report Wizard

Advanced Settings

Customize report distribution and storage options.

You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.

☑ Export to file

Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

5. To export the generated report to file, select **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 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.

5.2 Configuring Advanced Settings

GFI EndPointSecurity GFI 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 GFI ReportPack installation.

Note:

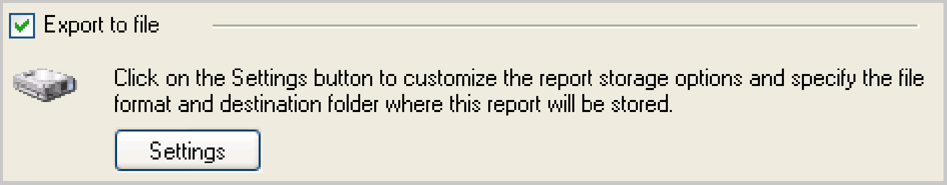
The Report Scheduling Wizard is by default configured to use the default set of report export and distribution parameters.

5.2.1 Report Export Formats

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

Format	Description
Adobe Acrobat (.PDF)	Use this format to allow distribution of a report on different systems such as Macintosh and Linux while preserving the layout.
MS Excel (.XLS)	Use this format if you want to further process the report and perform more advance calculations using another (external) program such as Microsoft Excel.
MS Word (.DOC)	Use this format if you want to access this report using Microsoft Word.
Rich text format (.RTF)	Use this format to save the report in a format that is small in size and which allows accessibility through different word processors in different operating systems.
HTML (.HTM)	Use this format to save the report in a platform independent format which can be viewed through a web browser. For example, you can include reports exported in html format directly on your website or intranet.

5.2.2 Configuring report export to file options



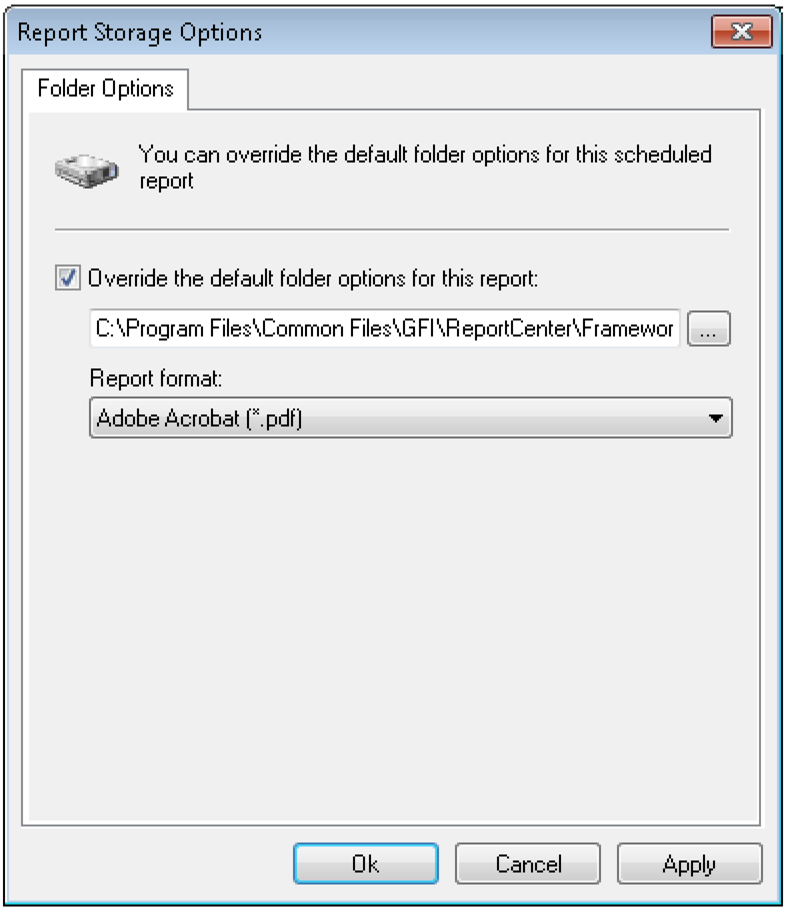
☑ Export to file

Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

Screenshot 20: Advanced Settings dialog: Export to file settings button

To configure the report Export to file settings of a scheduled report;

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



Report Storage Options

Folder Options

You can override the default folder options for this scheduled report

☑ Override the default folder options for this report:

C:\Program Files\Common Files\GFI\ReportCenter\Framewor

Report format:

Adobe Acrobat (*.pdf)

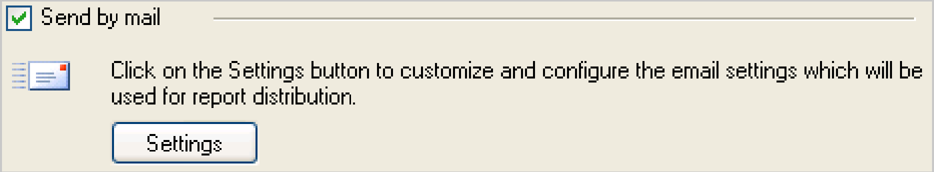
Screenshot 21: Advanced Settings: Export to file options

2. Select the **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.

5.2.3 Configuring report emailing options

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

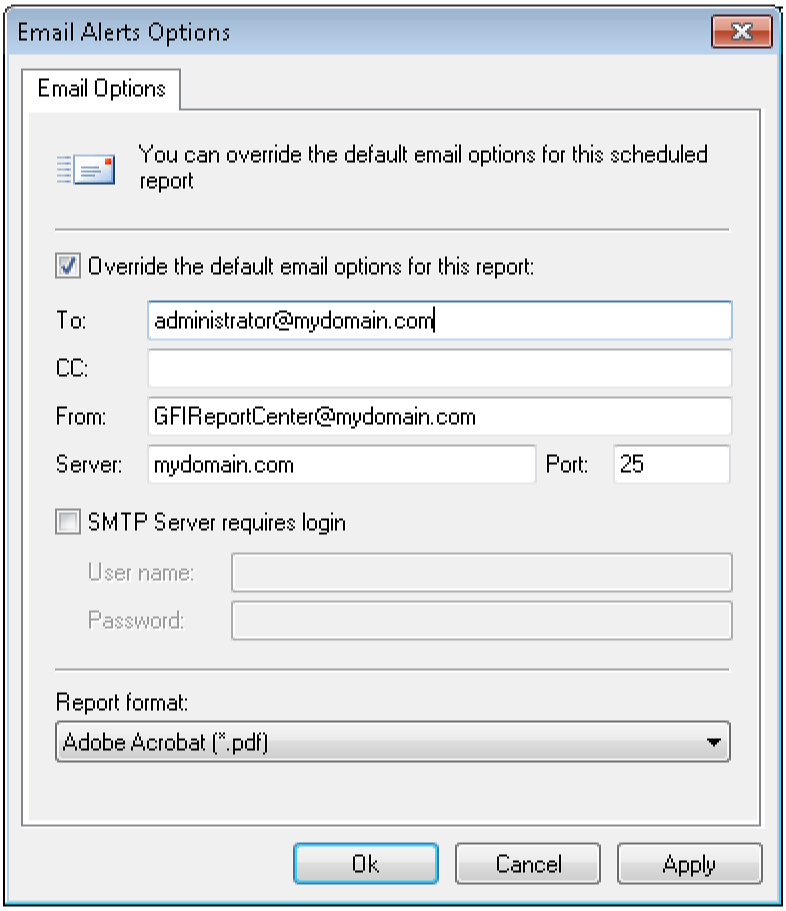


☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

Screenshot 22: Advanced Settings dialog: Send by email settings button

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



Email Alerts Options

Email Options

You can override the default email options for this scheduled report

☑ Override the default email options for this report:

To: administrator@mydomain.com

CC:

From: GFIReportCenter@mydomain.com

Server: mydomain.com Port: 25

□ SMTP Server requires login

User name:

Password:

Report format: Adobe Acrobat (*.pdf)

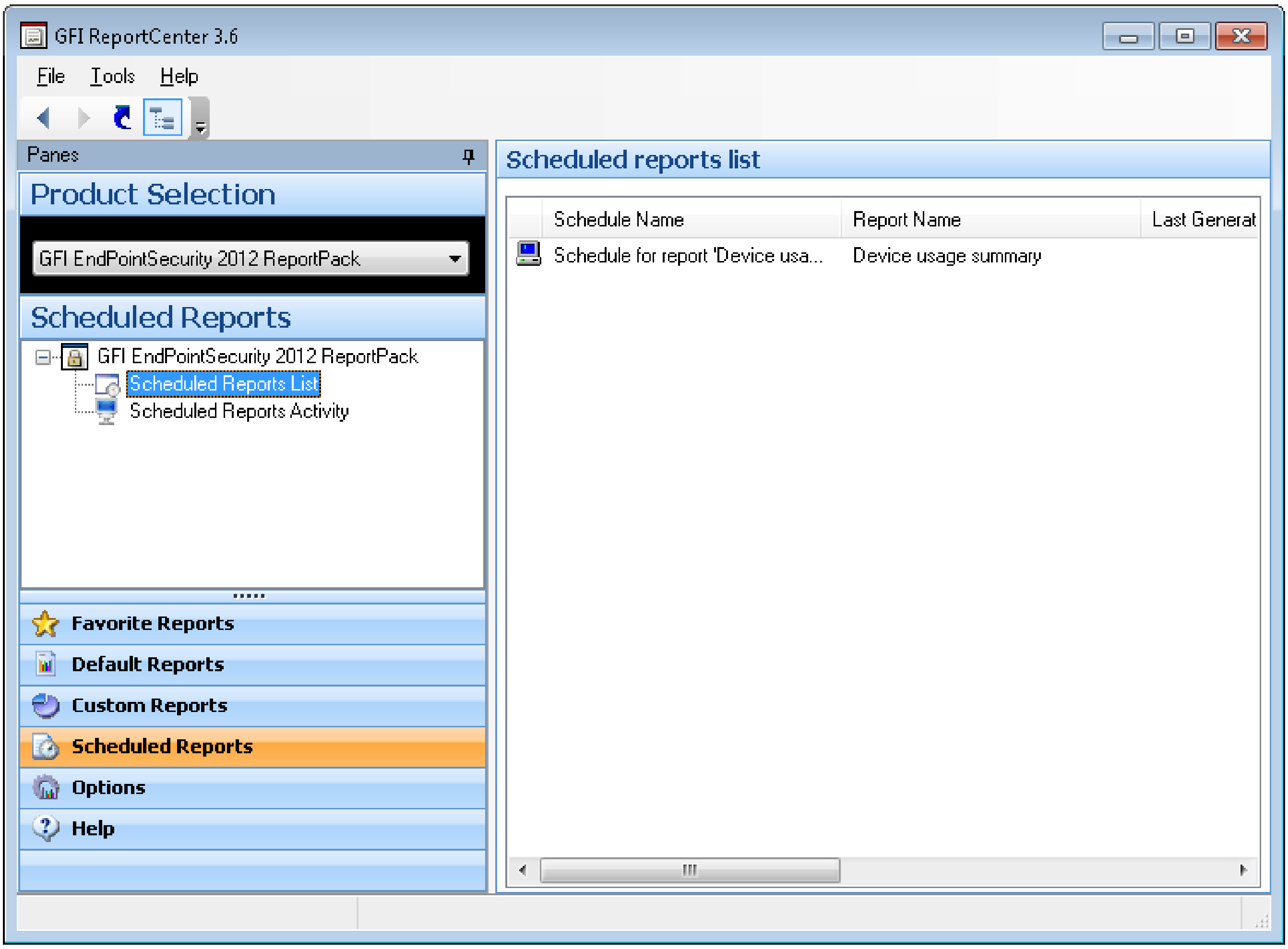
Screenshot 23: Report distribution options

1. Select **Override the default email options** for this report.
2. 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 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.

3. Click **OK** to finalize your configuration settings.

5.3 Viewing a list of Scheduled Reports



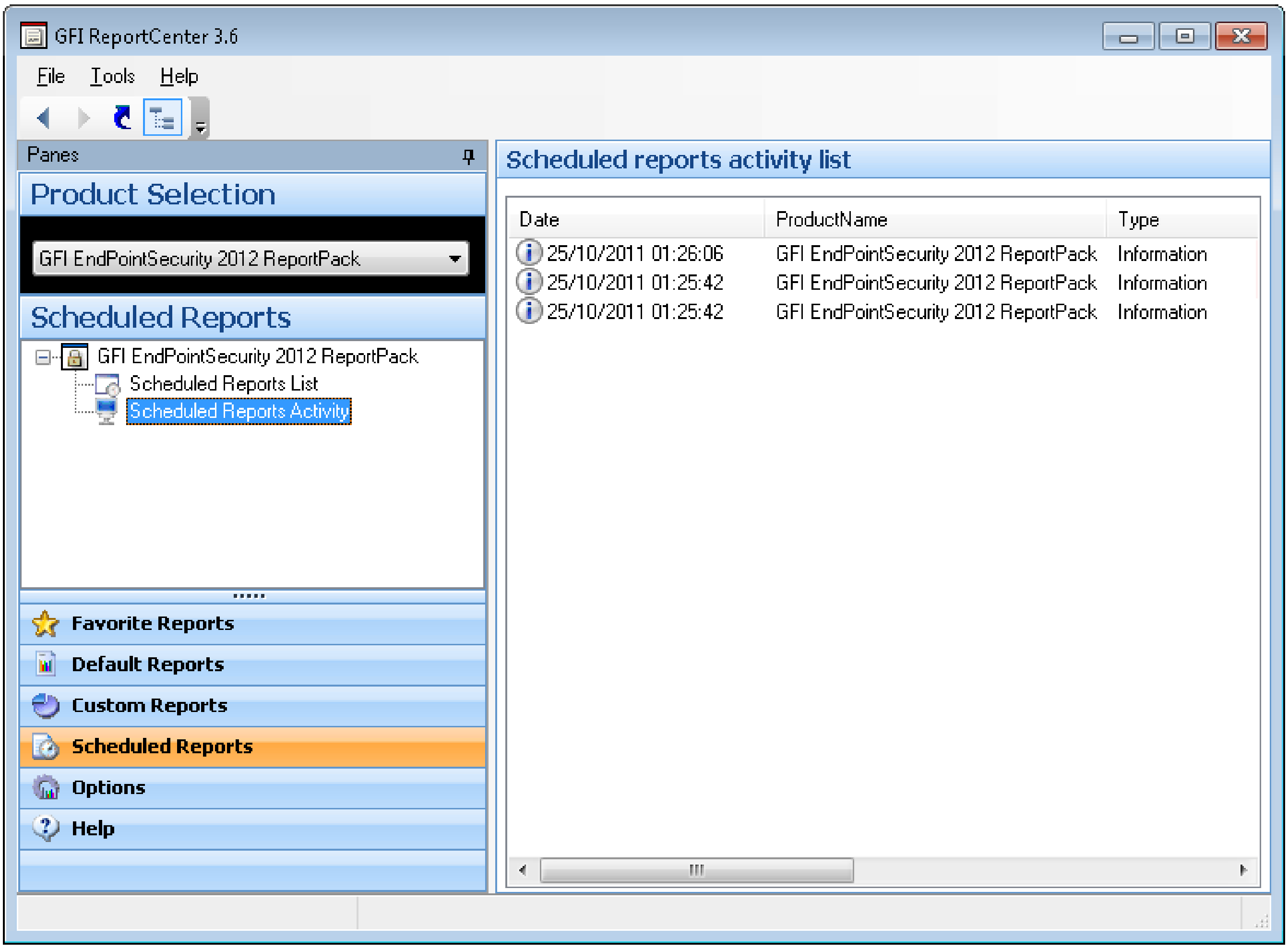
Schedule Name	Report Name	Last Generat
Schedule for report 'Device usa...	Device usage summary	

Screenshot 24: List of Scheduled reports

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

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

5.4 Viewing the Scheduled Reports activity



Date	ProductName	Type
25/10/2011 01:26:06	GFI EndPointSecurity 2012 ReportPack	Information
25/10/2011 01:25:42	GFI EndPointSecurity 2012 ReportPack	Information
25/10/2011 01:25:42	GFI EndPointSecurity 2012 ReportPack	Information

Screenshot 25: Schedule activity monitor

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

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

The activity monitor displays the following events:

Note:

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

Warning:

The scheduled report was not executed because product license is invalid or has expired.

Warning

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.

5.5 Enable or disable a scheduled report

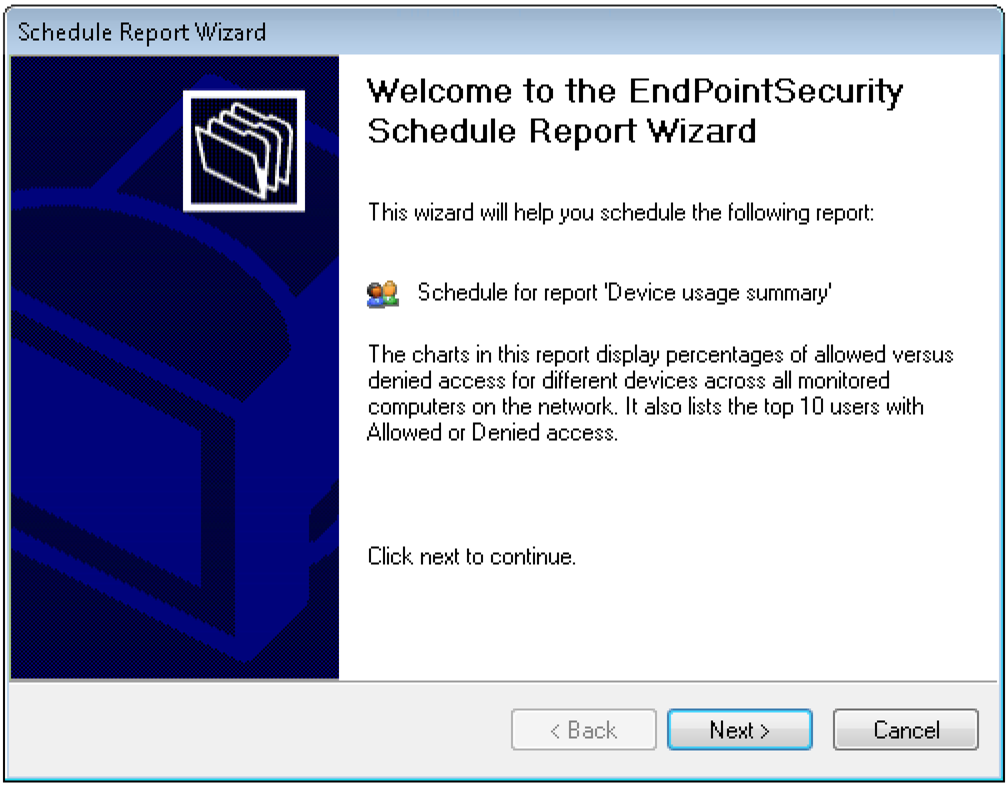
🖥✖	Indicates that the scheduled report is disabled.
🖥	Indicates that the scheduled report is enabled or pending.

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

5.6 Editing a Scheduled Report

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

1. Click **Scheduled Reports** > **Scheduled Reports list** navigation button.
2. **Right-click** on the scheduled report that you wish to re-configure and select **Properties**. This will launch the Scheduled Reports Wizard.



Welcome to the EndPointSecurity Schedule Report Wizard

This wizard will help you schedule the following report:

Schedule for report 'Device usage summary'

The charts in this report display percentages of allowed versus denied access for different devices across all monitored computers on the network. It also lists the top 10 users with Allowed or Denied access.

Click next to continue.

Screenshot 26: Scheduled Reports wizard

3. Click **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.

5.7 Deleting a Scheduled Report

To delete a scheduled report:

1. Click on the Scheduled Reports navigation button.
2. Right-click on the scheduled report that you wish to permanently remove from the list and select Delete.

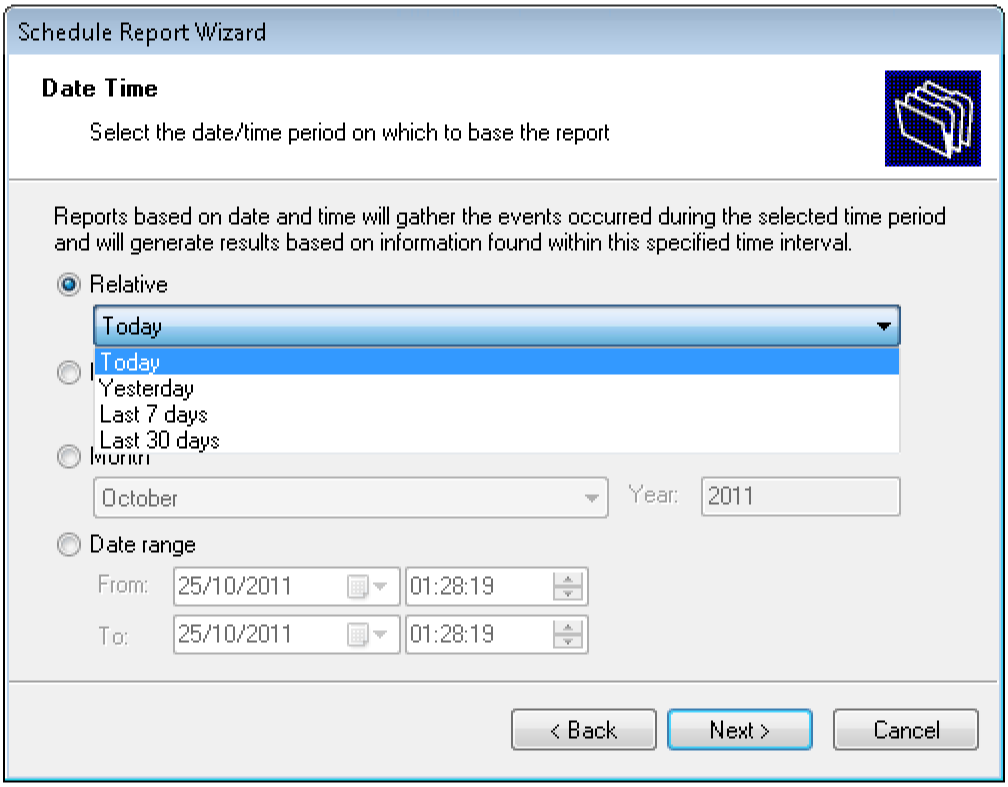
5.8 Example Scheduling a Report

This example demonstrates how to schedule a device usage summary report called Daily Device Usage Report. This schedule will be configured to:

- Generate the first report on 09/16/2009 at 12:00.
- Continue generating the same report on daily basis.
- Export the generated report(s) to folder 'C:\Daily Reports' in PDF format.
- Email the generated report using the following custom parameters:
  - Send from email account: **administrator@masterdomain.com**
  - Send to email account: **gfireportcenter@masterdomain.com**
  - SMTP server details: **Win2k3serv**

To create the scheduled report:

1. Click on the **Default Reports** navigation button.
2. Right-click on **Device Usage Summary** and select **New > Scheduled Report**.
3. In the welcome dialog, click **Next**.



Schedule Report Wizard

Date Time

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

Reports based on date and time will gather the events occurred during the selected time period and will generate results based on information found within this specified time interval.

● Relative: Today

○ Month: October Year: 2011

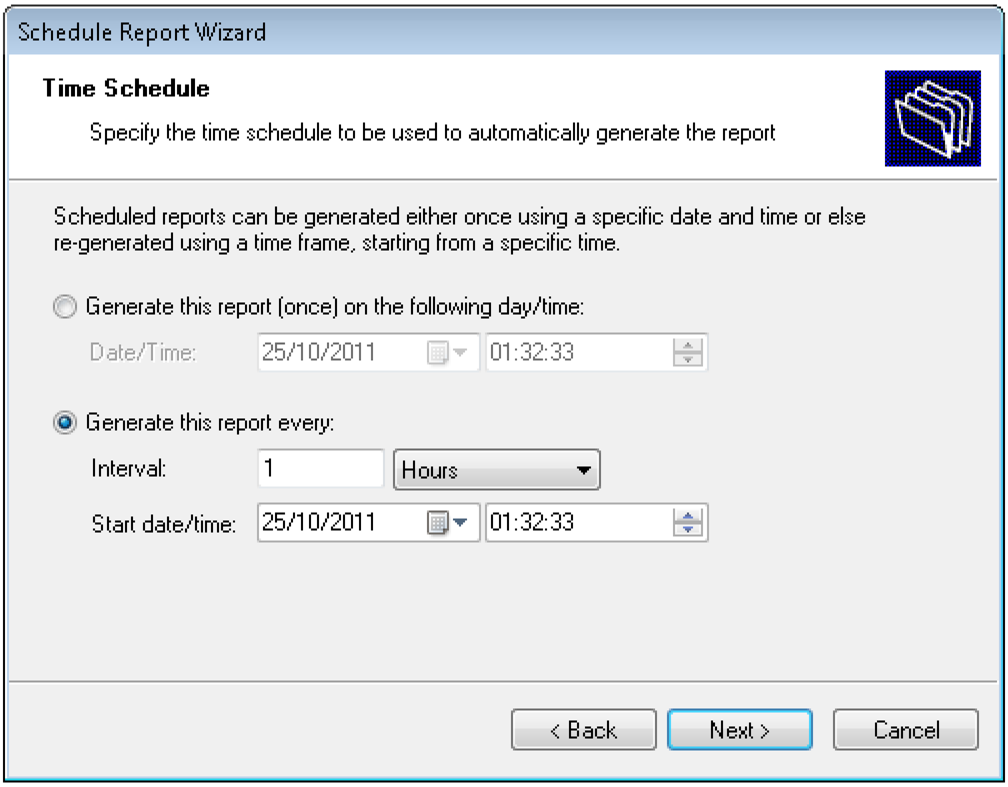
○ Date range

From: 25/10/2011 01:28:19

To: 25/10/2011 01:28:19

Screenshot 27: Select device usage period

4. Select the option **Relative** and from the provided drop down list select **Today**. Click on **Next** to proceed to the next dialog.
5. Since no data filters will be applied in this example, click **Next** to proceed to the next dialog.



Schedule Report Wizard

Time Schedule

Specify the time schedule to be used to automatically generate the report

Scheduled reports can be generated either once using a specific date and time or else re-generated using a time frame, starting from a specific time.

○ Generate this report (once) on the following day/time:

Date/Time: 25/10/2011 01:32:33

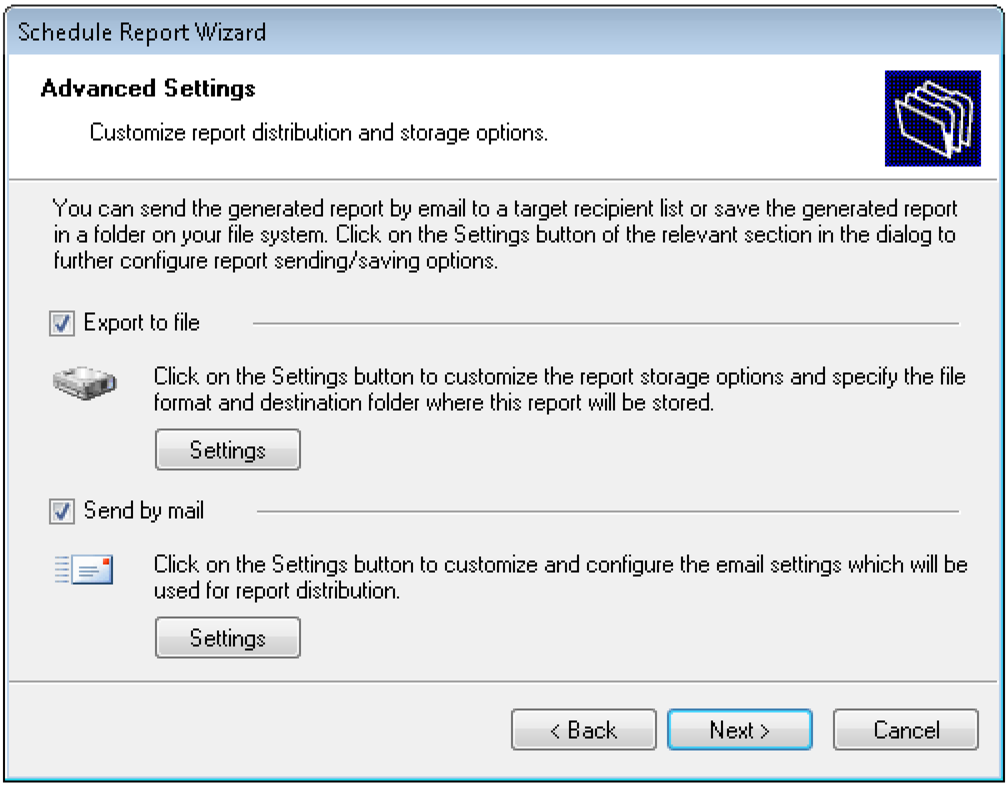
● Generate this report every:

Interval: 1 Hours

Start date/time: 25/10/2011 01:32:33

Screenshot 28: Specifying the scheduling options

6. To generate this report on daily basis, select the option **Generate this report every:** and set the interval to 1 Day.
7. Set the start date to **09/16/2009** and time to **12:00:00 AM**. Click **Next** to proceed to the next dialog.



Schedule Report Wizard

Advanced Settings

Customize report distribution and storage options.

You can send the generated report by email to a target recipient list or save the generated report in a folder on your file system. Click on the Settings button of the relevant section in the dialog to further configure report sending/saving options.

☑ Export to file

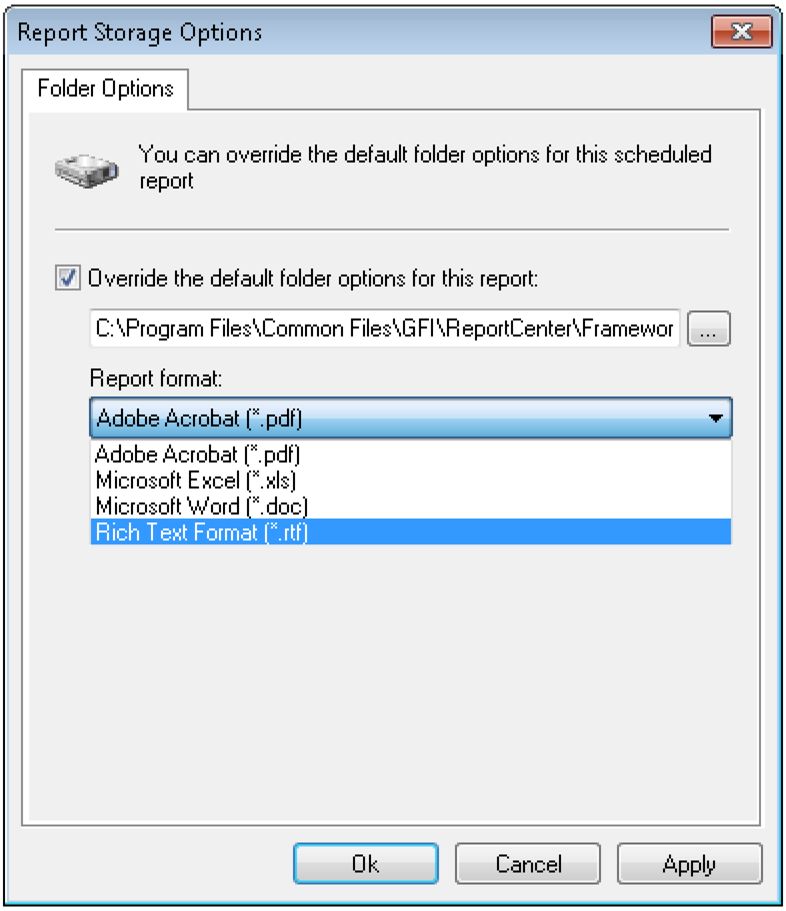
Click on the Settings button to customize the report storage options and specify the file format and destination folder where this report will be stored.

☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

Screenshot 29: Advanced Settings dialog

8. From the **Advanced Settings** dialog, click **Settings** under **Export to file** option.



Report Storage Options

Folder Options

You can override the default folder options for this scheduled report

☑ Override the default folder options for this report:

C:\Program Files\Common Files\GFI\ReportCenter\Framewor

Report format:

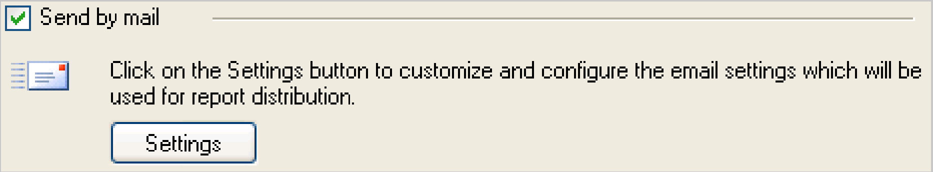
Adobe Acrobat (*.pdf)

Screenshot 30: Advanced Settings: Export to file options

9. Select **Override the default folder** options for this report:

10. Specify the complete path where this report will be saved i.e. **C:\Daily Reports**.

11. From the report format drop down select **PDF** and click **OK.**

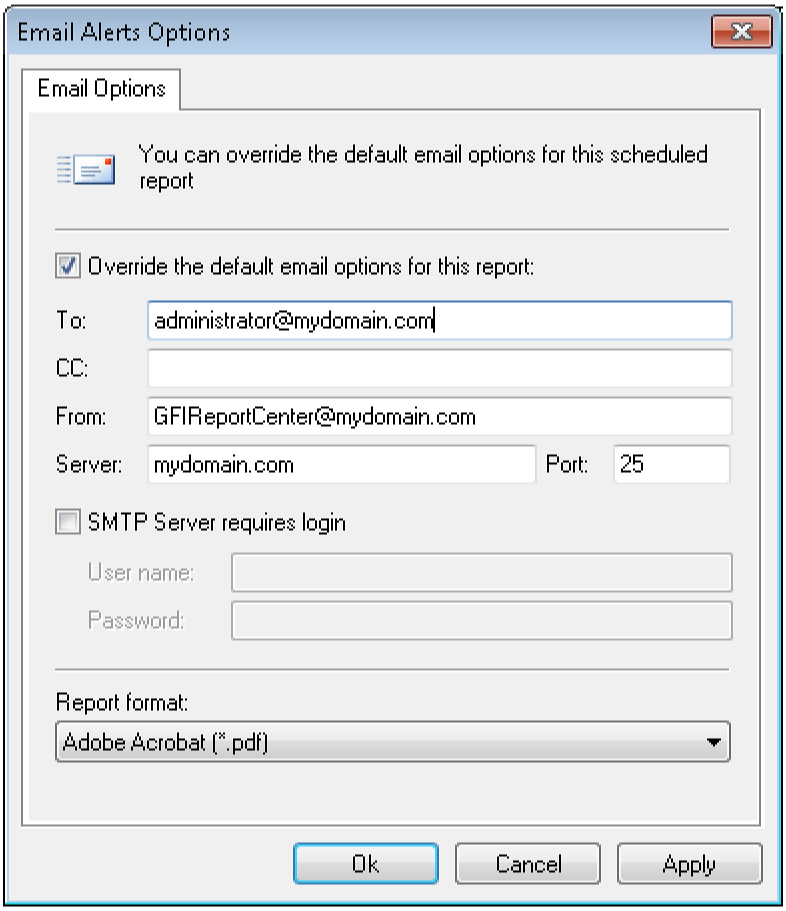


☑ Send by mail

Click on the Settings button to customize and configure the email settings which will be used for report distribution.

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

12. From **Advanced Settings** dialog, click **Settings** button under **Send by email** option.



You can override the default email options for this scheduled report

☑ Override the default email options for this report:

To: administrator@mydomain.com

CC:

From: GFIReportCenter@mydomain.com

Server: mydomain.com Port: 25

□ SMTP Server requires login

User name:

Password:

Report format:

Adobe Acrobat (*.pdf)

Screenshot 32: Report distribution options

13. Select **Override** the default email options for this report:

14. Specify the following parameters:

   - To : **administrator@masterdomain.com**
   - From : **gfireportcenter@masterdomain.com**
   - Server : **Win2k3serv**

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

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

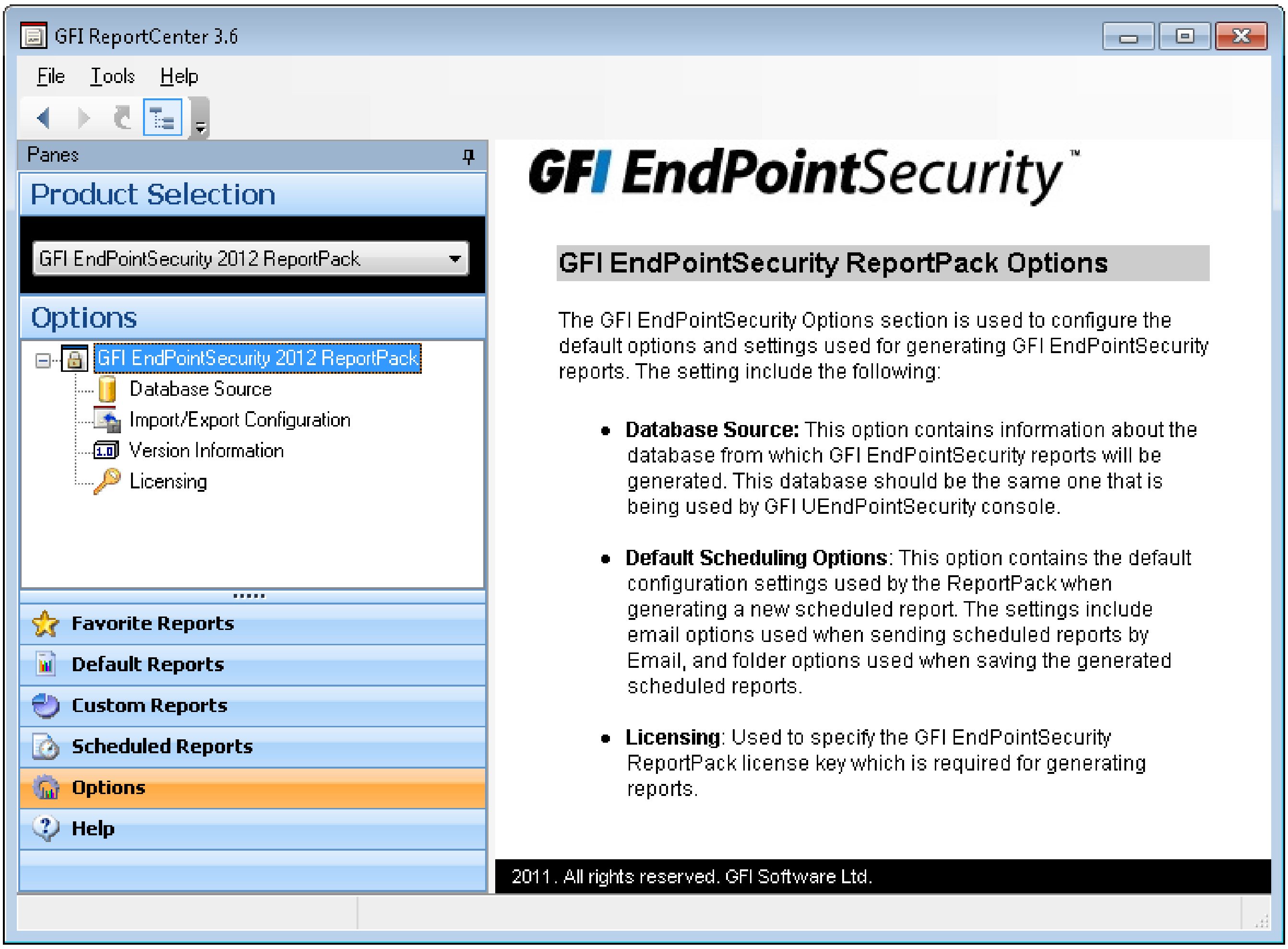
   - Report Name : **Daily device usage report**
   - Report Title : **Daily device usage report**
   - Report Description: This report is generated on a daily basis at 12:00 AM. It shows all device usage activity recorded throughout the day.

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

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

6 Configuring default options

The GFI EndPointSecurity GFI 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 provided in the GFI ReportCenter management console.



GFI EndPointSecurity ReportPack Options

The GFI EndPointSecurity Options section is used to configure the default options and settings used for generating GFI EndPointSecurity reports. The setting include the following:

- **Database Source:** This option contains information about the database from which GFI EndPointSecurity reports will be generated. This database should be the same one that is being used by GFI UEndPointSecurity console.
- **Default Scheduling Options**: This option contains the default configuration settings used by the ReportPack when generating a new scheduled report. The settings include email options used when sending scheduled reports by Email, and folder options used when saving the generated scheduled reports.
- **Licensing**: Used to specify the GFI EndPointSecurity ReportPack license key which is required for generating reports.

2011. All rights reserved. GFI Software Ltd.

Screenshot 33: Options navigation button

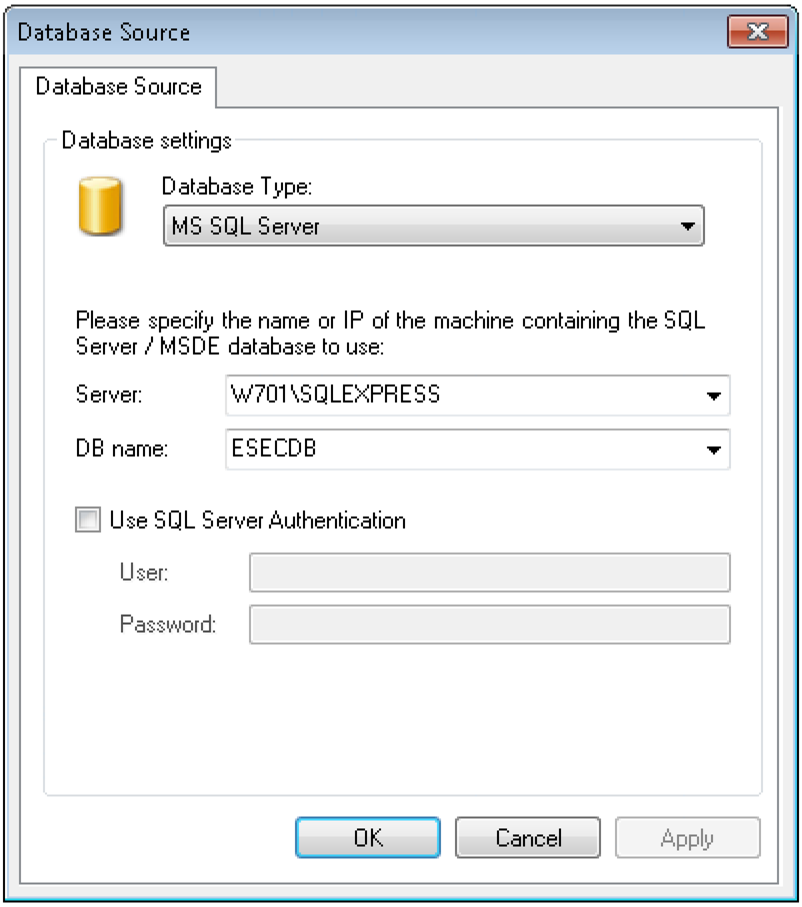
Through the **Options** navigation button you can configure the following parameters:

- **Database source:** Use this node to specify the database backend from where the GFI ReportPack will extract the required reporting data.
- **Default scheduling settings:** Use this node to configure the default export to file parameters and report emailing parameters of scheduled reports.

6.1 Configuring Database Source

To configure your database source:

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



Database Source

Database settings

Database Type: MS SQL Server

Please specify the name or IP of the machine containing the SQL Server / MSDE database to use:

Server: W701\SQLEXPRESS

DB name: ESECDB

□ Use SQL Server Authentication

User:

Password:

Screenshot 34: Database source configuration dialog

3. Select the **database type** (For example. MS SQL Server) from the provided list of supported databases.

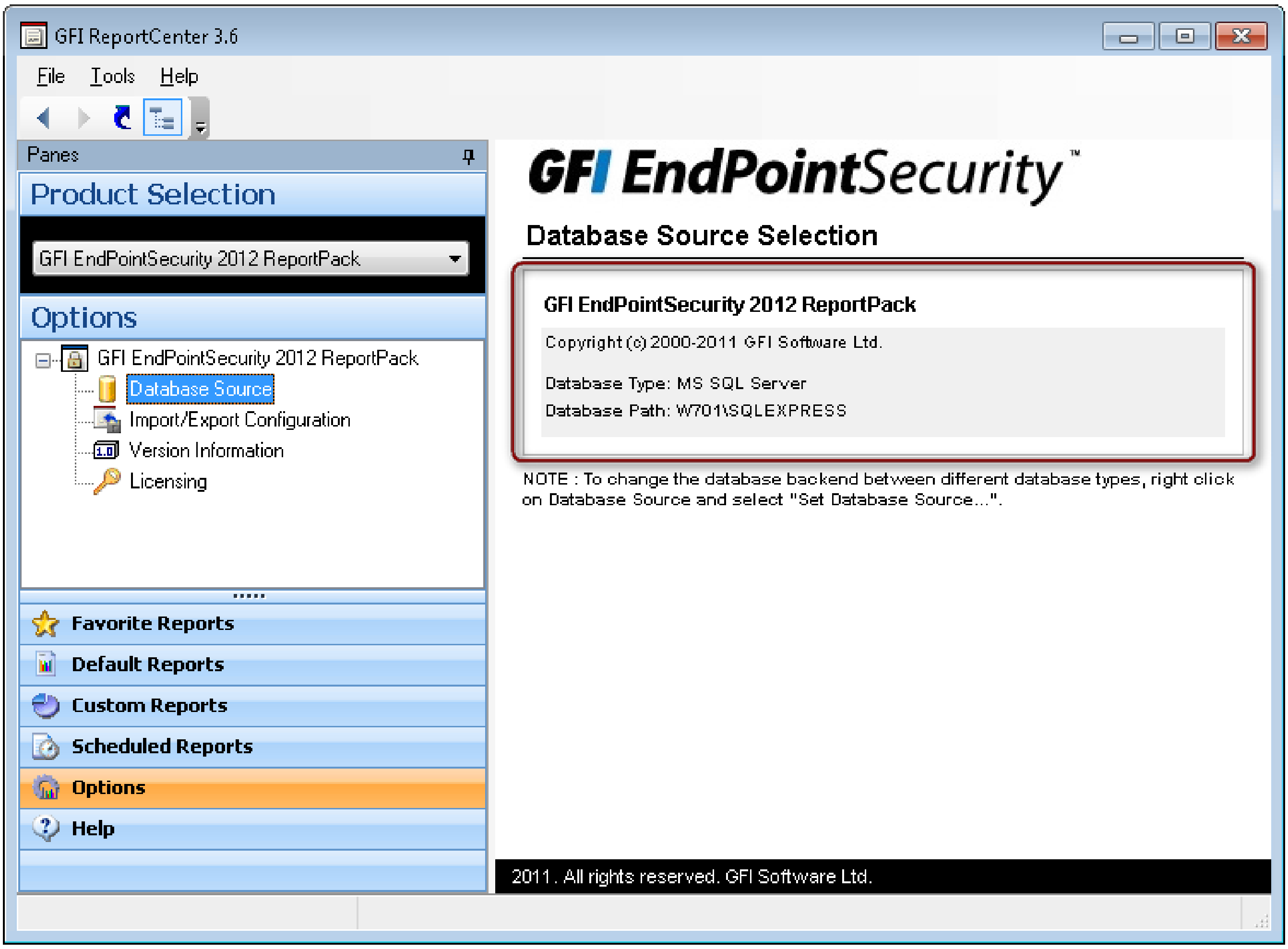
> **Note:**
>
> GFI EndPointSecurity database backend supports only MSDE/MS SQL Server.

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 **Use SQL Server authentication** option and specify the user name and password in the provided fields.

> **Note:**
>
> By default, the GFI EndPointSecurity GFI ReportPack uses Windows logon credentials to authenticate to the SQL Server.

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

6.2 Viewing the current Database Source settings



Database Source Selection

GFI EndPointSecurity 2012 ReportPack

Copyright (c) 2000-2011 GFI Software Ltd.

Database Type: MS SQL Server

Database Path: W701\SQLEXPRESS

NOTE : To change the database backend between different database types, right click on Database Source and select "Set Database Source...".

2011 . All rights reserved. GFI Software Ltd.

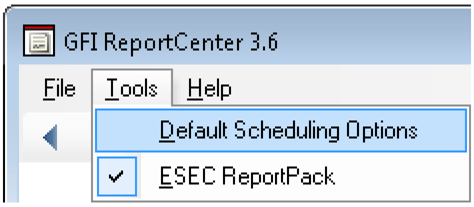
Screenshot 35: Database source configuration settings

Click **Database Source** to view in the right pane window the current database source settings.

7 Configuring default scheduling settings

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

1. Click on the **Options** navigation button.



Screenshot 36: Default Scheduling Options node

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

8 General Options

This chapter enables you to configure and view the GFI ReportPack general options. If you have purchased GFI EndPointSecurity, this chapter provides detailed information about how to enter your purchased license key, view the GFI ReportPack version details and also check for newer versions.

Topics in this chapter

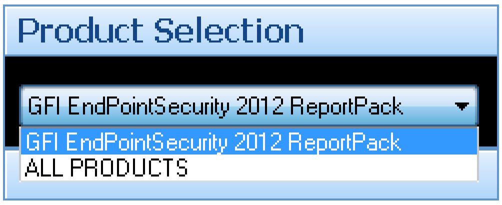
8.1 Entering your license key after installation

If you have purchased GFI EndPointSecurity, enter your License key using the **Options** > **Licensing node** (no re-installation/re-configuration required)

Note:

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 GFI EndPointSecurity license key in the GFI ReportPack:



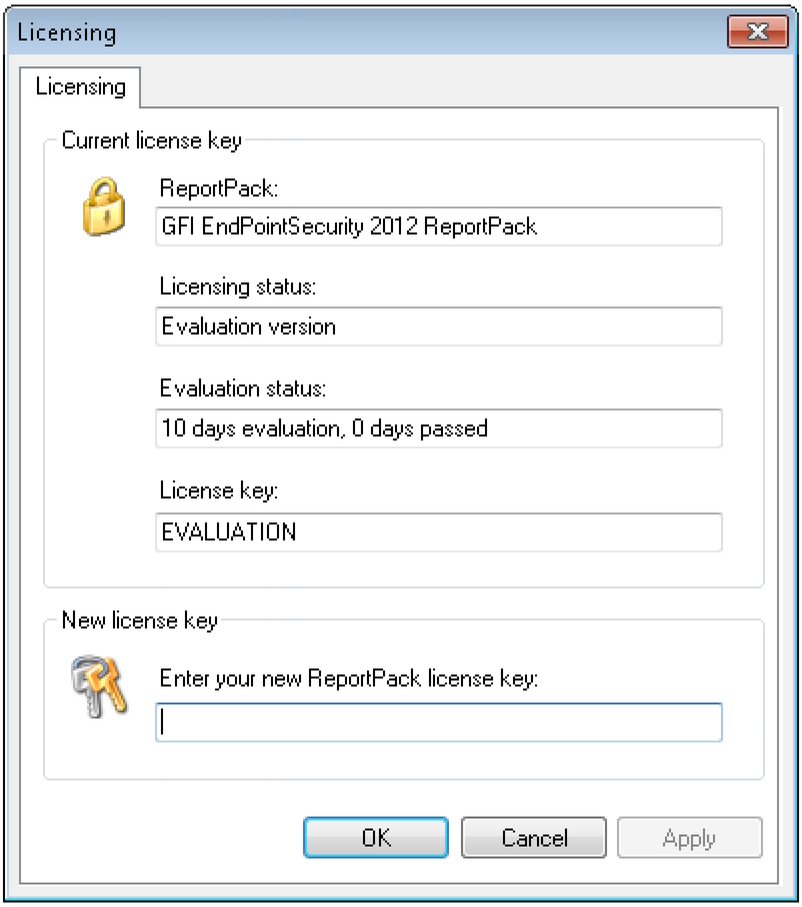
Product Selection
GFI EndPointSecurity 2012 ReportPack
GFI EndPointSecurity 2012 ReportPack
ALL PRODUCTS

Screenshot 37: Product Selection drop down list

1. Select the respective product (e.g. **GFI EndPointSecurity**) 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 launch the **Licensing** dialog.



ReportPack:
GFI EndPointSecurity 2012 ReportPack

Licensing status:
Evaluation version

Evaluation status:
10 days evaluation, 0 days passed

License key:
EVALUATION

Screenshot 38: Licensing dialog

4. Type the **GFI EndPointSecurity license key** in the space provided.
5. Click on **OK** to finalize license key entry.

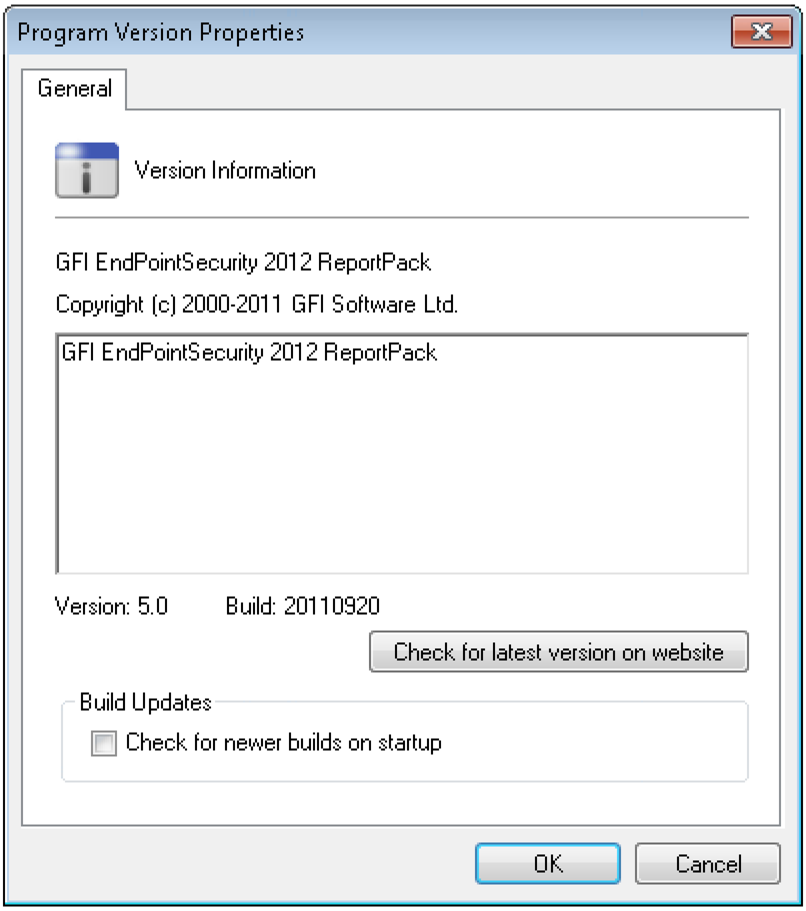
8.2 Viewing product Report Pack version details

To view the version information of a currently installed product GFI ReportPack:

1. Select the product report from the **Product Selection** drop down list.
2. Click on the **Options** navigation button.
3. Click on the **Version Information** node. The version details are displayed in the right pane of the GFI ReportCenter management console.

8.3 Checking the web for newer builds

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



Program Version Properties
General
Version Information

GFI EndPointSecurity 2012 ReportPack

Copyright (c) 2000-2011 GFI Software Ltd.

GFI EndPointSecurity 2012 ReportPack

Version: 5.0 Build: 20110920

Check for latest version on website
Build Updates

□ Check for newer builds on startup

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

> **Note:**
>
> You can configure GFI EndPointSecurity GFI ReportPack to check for newer builds on startup.

9 Appendix GFI EndPointSecurity default reports

Topics in this chapter

9.1 Executive Reports

Report	Description
Device usage summary	The charts in this report display percentages of allowed versus denied access for different devices across all monitored computers on the network. It also lists the top 10 users with Allowed or Denied access.
All devices used - grouped by device	This report shows a list of devices detected by GFI EndPointSecurity agents across the network together with a list of users that have in some way made use of each device.
All device used - grouped by user	This report shows a list of users monitored by GFI EndPointSecurityagents across the network together with a list of devices that each user has used.
Device access trends	This is a trend report showing the change in device access attempts over time. The graphs plot both the allowed and denied access counts per day.

9.2 Statistical Reports

Report	Description
Device access statistics	This report shows the number of allowed and denied access requests made by each user for each device, grouped by file system and non file system devices. Each row shows Read-Only and Read-Write (full) access requests that were allowed or denied.
Device usage statistics per user	This report shows a list of external devices connected by each user together with the number of allowed and denied access requests for each device.

9.3 Top active users or machine reports

Report	Description
Top 20 active users	This report shows a list of monitored users who have the highest amount of device activity.
Top 50 active users	This report shows a list of monitored users who have the highest amount of device activity
Top 20 active machines	This report lists those monitored machines with the highest amount of device activity.
Top 50 active machines	This report lists those monitored machines with the highest amount of device activity.

9.4 Technical reports

Report	Description
Connected devices grouped by category	This report shows a list of external devices that were plugged in to machines monitored by GFI EndPointSecurityAgents. All devices are grouped under their category.
User based technical report	This report lists all device access requested by users. Activity is grouped by user name and event type and also lists the application that attempted the access, and for file system devices, also the path and filename.
Machine based technical report	This report shows a list of device access requests made from each machine. Each activity is grouped by machine name and event type and includes the application that attempted the accessed. In case of file system devices, the accessed path and filename are also provided.
Device based technical report	This report shows a list of events originating from devices monitored by GFI EndPointSecurity. Events are sorted in chronological order and grouped by device description.
Detailed device activity listing	This report lists all details of all Agent Activity across monitored Computers.
Encryption activity report	Use this report in order to determine the status of encryption across the network.

9.5 Security reports

Report	Description
Users who accessed devices on more than one machine	This report displays the users who were accessing devices on more than one machine.
Machines which had more than one user accessing devices	This report displays the machines which had more than one user accessing the devices.
Connected devices outside working hours	This report show the devices which were connected outside the working hours.
Connected devices during weekends	This report show the devices which were connected during weekends.
Suspicious user activity	This report shows all the denied file access events where the real file types were different from the file extensions. These accesses could indicate suspicious user activities - users might have tried to overcome the protection policies by altering file extensions.

9.6 Troubleshooting

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

The manual – most issues can be solved by reading this manual.

- GFI Knowledge Base articles
- Web forum
- Contacting GFI Technical Support

9.7 Knowlegebase

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 technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

9.8 Web forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

9.9 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

» Online: Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.

» Phone: To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

Note:

Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

9.10 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, visit: http://www.gfi.com/pages/productmailing.htm.

10 Glossary

A

Access permissions

A set of permissions (access, read and write) that are assigned to users and groups per device category, connectivity port or a specific device.

Active Directory

A technology that provides a variety of network services, including LDAP-like directory services.

Alert recipient

A GFI EndPointSecurity profile account to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.

Alerts

A set of notifications (e-mail alerts, network messages or SMS messages) that are sent to alert recipients when particular events are generated.

Alerts administrator account

An alert recipient account that is automatically created by GFI EndPointSecurity upon installation.

Automatic discovery

A GFI EndPointSecurity feature to search and discover computers that were newly connected to the network at configured scheduled times.

B

BitLocker To Go

A Microsoft Windows 7 feature to protect and encrypt data on removable devices.

C

Connectivity port

An interface between computers and devices.

Create Protection Policy wizard

A wizard to guide you in the creation and configuration of new protection policies. Configuration settings include the selection of device categories and ports to be controlled and whether to block or allow all access to them. This wizard also allows the configuration of file-type based filters, encryption permissions as well as logging and alerting options.

D

Database backend

A database used by GFI EndPointSecurity to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on target computers.

Deployment error messages

Errors that can be encountered upon deployment of GFI EndPointSecurity agents from the GFI EndPointSecurity management console.

Device blacklist

A list of specific devices whose usage is blocked when accessed from all the target computers covered by the protection policy.

Device category

A group of peripherals organized in a category.

Device scan

A GFI EndPointSecurity feature to search for all devices that are or have been connected to the scanned target computers.

Device whitelist

A list of specific devices whose usage is allowed when accessed from all the target computers covered by the protection policy.

Digest report

A summary report giving an account of the activity statistics as detected by GFI EndPointSecurity.

E

Event logging

A feature to record events related to attempts made to access devices and connection ports on target computers and service operations.

F

File-type filters

A set of restrictions that are assigned to users and groups per file-type. Filtering is based on file extension checks and real file type signature checks.

G

GFI EndPointSecurity agent

A client-side service responsible for the implementation/enforcement of the protection policies on the target computer(s).

GFI EndPointSecurity application

A server-side security application that aids in maintaining data integrity by preventing unauthorized access and transfer of content to and from devices and connection ports.

GFI EndPointSecurity management console

The user interface of the GFI EndPointSecurity server-side application.

GFI EndPointSecurity Temporary Access tool

A tool which is available on the target computers. It is used by the user to generate a request code and later to enter the unlock code in order to activate the temporary access once it is granted by the administrator. Upon activation, the user will have access to devices and connection ports (when such access is normally blocked) on his protected target computer for the specified duration and time window.

Global permissions

A Create Protection Policy wizard step that prompts the user to either block or else to allow access to all devices falling in a category or which are connected to a port of the target computers covered by the protection policy.

GPO

See Group Policy Objects.

Group Policy Objects

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

H

Human Interface Devices

A specification that is part of the universal serial bus (USB) standard for a class of peripheral devices. These devices, such as a mice, keyboards, and joysticks, enable users to input data or to interact directly with the computer.

M

MSI file

A file generated by GFI EndPointSecurity for later deployment using GPO or other deployment options. It can be generated for any protection policy and contains all the relevant configured security settings, including installation settings for unprotected target computers.

P

Power user

A power users is automatically given full access to devices connected to any target computer covered by the protection policy.

Protection policy

A set of device access and connectivity port permissions that can be configured to suit your company’s device access security policies.

Q

Quick Start wizard

A wizard to guide you in the configuration of GFI EndPointSecurity with custom settings. It is launched upon the initial launch of GFI EndPointSecurity management console and is intended for first time use.

S

Security encryption

A set of restrictions configured to either block or else to allow users/groups to access specific file-types stored on devices that are encrypted with BitLocker To Go. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy.

T

Target computer

A computer that is protected by a GFI EndPointSecurity protection policy.

Temporary access

A period of time during which users are allowed to access devices and connection ports (when such access is normally blocked) on protected target computers, for a specified duration and time window.

U

User message

A message that is displayed by GFI EndPointSecurity agents on target computers, when devices are accessed.

11 Index

USA, CANADA AND CENTRAL AND SOUTH AMERICA

4309 Emperor Blvd, Suite 400, Durham, NC 27703, USA
Telephone: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK
Telephone: +44 (0) 870 770 5370
Fax: +44 (0) 870 770 5377
sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, Territorials Street, Mriehel, BKR 3000, Malta
Telephone: +356 2205 2000
Fax: +356 2138 2419
sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia
Telephone: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfiap.com